UNIVERSIDADE FEDERAL DO PARANÁ

ELISANGELA DE CAMPOS

A noção de congruência algébrica no Curso de Matemática: uma análise das respostas dos estudantes

CURITIBA

2009

ELISANGELA DE CAMPOS

A noção de congruência algébrica no Curso de Matemática: uma análise das respostas dos estudantes

Tese de doutorado, requisito parcial para a obtenção do grau de Doutor em Educação, Linha de Pesquisa Educação Matemática, Curso de Pós Graduação em Educação, Setor de Educação, Universidade Federal do Paraná.

Orientadora: Prof.ª Dr.ª Maria Tereza Carneiro Soares.

CURITIBA
2009

Catalogação na publicação
Sirlei do Rocio Gdulla – CRB 9ª/985
Biblioteca de Ciências Humanas e Educação - UFPR

Campos, Elisangela de
A noção de congruência algébrica no Curso de Matemática: uma análise das respostas dos estudantes / Elisangela de Campos. – Curitiba, 2009.
207 f.

Orientadora: .Profª. Drª. Maria Tereza Carneiro Soares
Tese (Doutorado em Educação) – Setor de Educação, Universidade Federal do Paraná.

1. Matemática – estudo e ensino. 2. Álgebra abstrata. 3. Matemática – ensino superior . 4. Álgebra – ensino superior. I. Titulo.

CDD 512.02
CDU 512

MINISTÉRIO DA EDUCAÇÃO E DO DESPORTO
UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE EDUCAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO

UNIVERSIDADE FEDERAL DO PARANÁ M E C PROGRAMA DE PÓS GRADUAÇÃO EM EDUCAÇÃO MESTRADO E DOUTORADO SETOR DE EDUCAÇÃO

PARECER

Defesa de Tese de **ELISANGELA DE CAMPOS** para obtenção do Título de DOUTORA EM EDUCAÇÃO. Os abaixo-assinadas: DRª MARIA TEREZA CARNEIRO SOARES, DRª HELENA NORONHA CURY, DRª ÂNGELA MARTA PEREIRA DAS DORES SAVIOLI, DR. JOSÉ CARLOS CIFUENTES e DR. MARCELO MUNIZ SILVA ALVES argüiram, nesta data, a candidata acima citada, a qual apresentou a seguinte Tese: "**A NOÇÃO DE CONGRUÊNCIA ALGÉBRICA NO CURSO DE MATEMÁTICA: UMA ANÁLISE DAS RESPOSTAS DOS ESTUDANTES**".

Procedida a argüição, segundo o Protocolo aprovado pelo Colegiado, a Banca é de Parecer que a candidata está apta ao Título de DOUTORA EM EDUCAÇÃO, tendo merecido as apreciações abaixo:

BANCA	ASSINATURA	APRECIAÇÃO
DRª MARIA TEREZA CARNEIRO SOARES		APROVADA
DRª HELENA NORONHA CURY		APROVADA
DRª ÂNGELA MARTA PEREIRA DAS DORES SAVIOLI		APROVADA
DR. JOSÉ CARLOS CIFUENTES		APROVADO
DR. MARCELO MUNIZ SILVA ALVES		APROVADA

Curitiba, 29 de janeiro de 2009.

Prof. Dr. Ângelo Ricardo de Souza
Coordenador do Programa de Pós-Graduação em Educação

Em tempo, o professor Gert Schubring, da Universität Bielefeld, Alemanha, participou por vídeo conferência e aprovou o trabalho!

Dedico este trabalho a minha querida filha Mariana e ao meu amado esposo Márcio.

Agradecimentos

- Aos meus pais, Sebastião e Hélia, e aos meus irmãos, Ana Eliza e Sandro, que, mesmo longe, me deram apoio e torceram para que eu finalizasse este estudo.
- À minha orientadora Profª. Drª. Maria Tereza Soares Carneiro, pela orientação, atenção e paciência.
- Ao amigo Cifuentes, por ter colaborado com esta pesquisa, com conversas esclarecedoras sobre Álgebra e Filosofia.
- À amiga Mariângela Setti, com quem eu pude dividir todas as alegrias, angústias e dúvidas, durante estes anos de estudo.
- Ao amigo Marcelo, pelas conversas e por ter cedido suas aulas para a aplicação dos questionários.
- À amiga Ximena, pela amizade, pelas dicas sobre o Latex e pelos momentos de descontração nos lanchinhos no meio da tarde.
- Aos membros da banca examinadora que contribuíram muitíssimo para melhorar a versão final deste trabalho.
- A todos os estudantes do Curso de Matemática da UFPR, que participaram desta pesquisa.
- A todos os professores, colegas e funcionários do Programa de Pós-Graduação em Educação, que me ajudaram de alguma forma na realização deste estudo.
- Ao Departamento de Matemática da UFPR, por ter permitido que eu pudesse me dedicar exclusivamente a esta pesquisa.

Sumário

Resumo

Este trabalho tem como objetivo geral identificar e analisar as dificuldades apresentadas por estudantes de um Curso de Matemática, ao responderem questões sobre congruência algébrica no contexto da Teoria de Números e da Teoria de Anéis. Foram elaborados dois questionários, o primeiro, contendo questões sobre congruência módulo m e o segundo, contendo questões sobre anel quociente $\mathbb{Z}_m$, ambos aplicados a estudantes do curso de Matemática, matriculados na disciplina de Álgebra A ou Teoria de Anéis. Após as respostas serem classificadas e analisadas, foram feitas entrevistas com três estudantes do mesmo curso, matriculados na disciplina Teoria de Grupos. Das análises dos questionários, com apoio dos dados das entrevistas, foi possível identificar dificuldades no reconhecimento da partição induzida pela relação de congruência módulo m sobre $\mathbb{Z}$, no entendimento da natureza dos elementos do anel quociente $\mathbb{Z}_m$, em construir e entender o anel quociente, em identificar dois anéis isomorfos e em trabalhar com o representante da classe. Entre as possíveis razões para que estas dificuldades ocorram, pode-se destacar a falta de conhecimentos básicos de teoria de conjuntos envolvidos na noção de congruência e aspectos didáticos e cognitivos.

Palavras-chave: Educação Matemática, Ensino Superior, Álgebra Abstrata

Abstract

The general purpose of this work is to identify and analyze difficulties that mathematics students present, when answering questions on algebraic congruence in the contexts of Number Theory and Ring Theory. To that end, two tests were prepared. The first one presented questions on congruence modulo m, and the second one questions on the $\mathbb{Z}_m$ quotient ring. Both tests were applied to mathematics students attending the courses of Algebra A or Ring Theory. The answers to those tests were classified and analyzed. After that, three students that were attending a course on Group Theory, were interviewed. By analyzing the answers to the tests, with the support of the interviews, it was possible to identify the following difficulties: on recognizing the induced partition by the congruence modulo m on $\mathbb{Z}$; on understanding the nature of the elements of the $\mathbb{Z}_m$ quotient ring; on building and understanding the quotient ring; on recognizing isomorphic rings; on working with a class representing element. There are many reasons that may cause those difficulties. One points out the lack of basic knowledge on set theory regarding the notion of congruence as well as pedagogic and cognitive aspects.

Apresentação

Este trabalho começou com minhas observações sobre os erros cometidos por estudantes em disciplinas de Matemática do ensino superior. Depois de conhecer algumas pesquisas sobre ensino e aprendizagem em Cálculo, Álgebra Linear e Teoria de Grupos, e observar que a maioria delas era sobre Cálculo, considerei que seria interessante explorar o ensino e a aprendizagem de Álgebra Abstrata, já que os trabalhos nesta área eram poucos e as dificuldades dos estudantes aparentemente muitas.

A pesquisa, agora apresentada, tem a seguinte questão norteadora:

O que os estudantes de um Curso de Matemática respondem sobre congruência algébrica em questões formuladas no contexto da Teoria de Números e Teoria de Anéis? O que se pode inferir destas respostas?

Ao buscar respostas para estas questões espero contribuir para uma reflexão sobre o ensino e a aprendizagem de Álgebra Abstrata, além de contribuir para a formação de um banco de dados sobre este tema, para que outros pesquisadores possam utilizar esses resultados em suas investigações.

O Capítulo 1 é dedicado a delimitar e justificar o tema desta pesquisa. Neste capítulo, também faço uma breve descrição da evolução do projeto e defino alguns termos para este estudo.

As noções matemáticas envolvidas nesta pesquisa, são detalhadas no Capítulo 2, quando são definidas as noções de congruência, congruência módulo m e anel quociente $\mathbb{Z}_m$. Também são apresentadas as notações utilizadas para estas noções.

No capítulo 3, são descritos e discutidos resultados de algumas pesquisas que foram utilizados neste trabalho, seja para construção dos instrumentos e coleta de dados, seja para análise dos dados.

O capítulo 4 é dedicado à descrição dos procedimentos metodológicos. Nele, os sujeitos da pesquisa são definidos, bem como os instrumentos de coleta de dados, o tratamento e a forma de análise destes dados, tomando como base as pesquisas sobre análise de erros.

No capítulo 5, são apresentadas a classificação e a análise das respostas dos estudantes, resultados que são discutidos levando em conta também as entrevistas feitas

com outros estudantes.

O capítulo final traz as conclusões e considerações sobre os resultados, e o que, a partir deles, ainda pode ser explorado em pesquisas futuras.

Capítulo 1

Justificativa e Delimitação do Tema

Neste capítulo será feita a delimitação do tema e a justificativa desta pesquisa. Uma breve descrição das modificações que o projeto de pesquisa foi sofrendo durante seu desenvolvimento será apresentada. No final, alguns termos serão estabelecidos e os objetivos da pesquisa, definidos.

1.1 Introdução

Desde 1999, trabalho com ensino de Matemática na Universidade Federal do Paraná, UFPR, principalmente nas disciplinas de Álgebra, Cálculo, Geometria Analítica e Projetos Integrados em Educação Matemática, e tenho notado certas dificuldades nos alunos em lidar com determinados conceitos matemáticos. Entre eles o tema "limite", que é trabalhado na disciplina de Cálculo, os temas "dependência e independência linear", na disciplina de Álgebra Linear, e os temas "isomorfismo e grupo quociente", em Álgebra Abstrata. Encontrei várias pesquisas desenvolvidas para identificar e amenizar estas dificuldades ou obstáculos, como, por exemplo, as realizadas por Cornu(1991), Sierpinska (1985), Dias (1993). Encontrei, também, em menor número, trabalhos sobre ensino e aprendizagem, dedicados a conceitos estudados na disciplina de Álgebra Abstrata, como é o caso de Asiala et al. (1997), Lajoie (2000) e Findell (2001). E é nesta disciplina que se encontra o foco de minha pesquisa.

A disciplina "Álgebra Abstrata" ou "Estruturas Algébricas" ou simplesmente "Álgebra" é uma disciplina do curso de graduação em Matemática que, no caso da UFPR, é ministrada tanto para o bacharelado quanto para a licenciatura, veja Apêndice A. Nesta disciplina são trabalhadas as estruturas algébricas: grupo, anel e corpo, de

forma genérica, dando enfoque às suas propriedades, independentemente do conjunto envolvido. A escolha pela Álgebra se deu por um gosto pessoal, já que fiz mestrado nesta área, e por esta ser umas das disciplinas do Curso de Matemática da UFPR na qual existe um número relativamente alto de reprovação e evasão de alunos.

Em geral, esta disciplina não é a preferida dos estudantes, que reclamam da sua abstração e seu formalismo; é o que pude constatar com minha experiência como professora da mesma. Este formalismo e abstração, dos quais os estudantes reclamam, são consequências, entre outros fatores, da progressiva abstração pela qual passou a noção de operação algébrica, que fez com que se ampliasse a noção de número, a ponto de fazermos cálculos com objetos matemáticos que não têm nenhum caráter numérico, como as permutações de um conjunto, apontada por Bourbaki (1970) no prefácio do livro *Éléments de Mathématiques: Algèbre*.

Além disso, os conceitos algébricos são, em geral, apresentados aos estudantes a partir das definições formais, tomadas em sua forma geral e apoiados na linguagem da teoria de conjuntos, em que as relações entre os objetos são mais importantes do que o próprio objeto e em que o conhecimento é apresentado na forma axiomática. Somente depois, nos exemplos, é que se dá significação a esta definição, quando se trabalha com um conjunto particular. Pode-se perceber este fato em praticamente todos os livros de Álgebra destinados ao ensino universitário.

Dentre os conteúdos ensinados na disciplina de Álgebra analisada, busquei um que estivesse presente em vários momentos. Em conversas informais com os professores da disciplina, eles relataram alguns problemas que seus alunos têm ao trabalharem com conceitos de grupo quociente, anel quociente e subgrupo normal. Eles disseram que os estudantes não entendem, por exemplo, o que são os elementos do grupo quociente, ou não entendem por que o subgrupo tem que ser normal para a construção de um grupo quociente.

Mas o que tem em comum o grupo quociente e o anel quociente? Um grupo quociente G/N pode ser definido como o conjunto de classes laterais módulo N, sendo N um subgrupo normal, munido de uma operação $*$, definida de $G/N \times G/N$ em G/N satisfazendo as três condições que caracterizam um grupo[1]. Um anel quociente A/I

[1] Definição de grupo: Seja G um conjunto não vazio onde está definida a operação entre pares de G, denotada por $*$. Dizemos que o par $(G, *)$ é um gupo se são válidas as seguintes propriedades: i) $a*(b*c) = (a*b)*c, \forall\, a, b, c \in G$; ii) $\exists\, e \in G$ tal que $a*e = e*a$, $\forall\, a \in G$; iii) $\forall\, a \in G, \exists\, b \in G$

é definido como o conjunto de classes de congruência módulo um ideal, que também é um anel. Estas definições trazem consigo uma série de outras noções que são importantes para o seu entendimento, tais como: relação de equivalência, estrutura quociente, operação entre classes de equivalência, partição de um conjunto. Pode-se reunir todas estas noções em um só conceito, o de relação de congruência em uma estrutura algébrica, ou simplesmente congruência.

A relação de congruência algébrica (ou simplesmente congruência) pode ser definida, utilizando a linguagem de teoria de conjuntos, como sendo uma relação de equivalência em um conjunto, compatível com alguma operação algébrica neste mesmo conjunto. O exemplo tradicional desta relação é a congruência módulo m, que é uma congruência no anel dos inteiros, e que pode ser generalizada para congruência módulo um ideal, por exemplo. Além disso, encontramos a congruência em outras disciplinas, como em Geometria Analítica, quando definimos um vetor por meio de segmentos equipolentes e também usamos a congruência na construção lógico-formal dos números inteiros, racionais e reais.

Vale notar que a construção de uma estrutura quociente $E/\equiv$, em que E é um conjunto qualquer, pode ser feita usando apenas a relação de equivalência $\equiv$. Mas no caso em que existem operações envolvidas, quando queremos que a estrutura quociente tenha operações que satisfaçam algumas propriedades, a relação de equivalência em questão deve ser uma congruência, tem que existir a compatibilidade da operação, como é o caso da construção de um anel quociente $\mathbb{Z}_m$, que será detalhado mais adiante.

A relação de congruência é um conceito matemático que está presente em vários ramos da Matemática e por meio dela pode-se construir uma estrutura quociente, ou seja, é possível construir um novo objeto matemático, utilizando este conceito. Em geral, a relação de congruência é utilizada para construção de novos objetos matemáticos[2], quando o conjunto envolvido possui pelo menos uma operação entre os seus elementos, como é o caso do grupo quociente e do anel quociente.

Sendo assim, entendo que a relação de congruência é uma ferramenta poderosa para a construção de novos objetos matemáticos a partir de outros já existentes. Acredito também que, apesar deste conceito não estar explicitamente colocado como objeto de estudo em alguma disciplina do Curso de Matemática da UFPR, ele pode ser fonte

tal que $a * b = b * a = e$ (Gonçalves, 1979).

[2] Tema do Capítulo 2

de erros dos estudantes ao trabalharem com conteúdos matemáticos a ela relacionados, como, por exemplo, o de anel quociente.

Entender as dificuldades que os estudantes possam apresentar ao estudar as estruturas construídas, utilizando a relação de congruência, é importante para refletir sobre o ensino de Álgebra Abstrata e sobre as possíveis falhas no currículo deste curso.

Inicialmente, decidi apresentar um projeto de pesquisa que tinha como objetivo identificar os obstáculos da noção de congruência. O projeto de pesquisa foi se modificando, conforme me aprofundava nos estudos de texto e artigos encontrados.

1.2 Projeto inicial e suas modificações

O projeto inicial, que foi apresentado para o ingresso no programa de doutorado, tinha como objetivo identificar e classificar os obstáculos na aprendizagem da noção de congruência, em particular da congruência módulo m. Para aprofundar os estudos sobre a noção de obstáculo epistemológico e obstáculo didático, estudei textos de Bachelard(1996), Cornu (1983), Brousseau (1983), Schubring (2002, 2006), Artigue(1990) e Malisani (1999).

A noção de obstáculo epistemológico foi introduzida por Bachelard (1996), como sendo a causa de lentidões e inércia no desenvolvimento científico. A ideia central desta noção é que "... no fundo o ato de conhecer dá-se contra um conhecimento anterior, destruindo conhecimentos já estabelecidos..." (BACHELARD, 1996, p. 17). Ou seja, para Bachelard, o desenvolvimento científico acontece por meio de rupturas epistemológicas, com o conhecimento sensível, conhecimentos já estabelecidos. Ele indica que os obstáculos epistemológicos podem ser encontrados no desenvolvimento histórico do pensamento científico e na prática da educação, embora seu livro aborde os obstáculos no desenvolvimento científico.

A noção de ruptura epistemológica pode ser entendida como uma ruptura com um conhecimento anterior, seja com a negação ou com a contradição com experiências do senso comum ou com alguma crença, seja em relação a conceitos científicos formalizados. Assim, uma ruptura pode ser entendida não somente com a rejeição da ciência do passado, mas, também, como uma preservação por meio de reformulações de velhas ideias em um novo e mais amplo contexto do pensamento.

Um exemplo disso é o desenvolvimento da Geometria não Euclidiana. Este

modelo rejeita a ideia de que os axiomas euclidianos expressam a única verdade acerca da geometria e, ao mesmo tempo, apresenta postulados definindo uma classe mais geral de geometria. Estes processos de reposição ao geral são caracterizados, por Bachelard, como dialéticos, no sentido de que um processo de expansão conceitual, pelo qual o que previamente parece oposto, é visto como possível de ser complementar, como, por exemplo a geometria Euclidiana e a Lobachevskiana (Bachelard, 2000).

A noção de obstáculo epistemológico foi desenvolvida para as ciências naturais. Em relação à Matemática, Bachelard afirma que esta noção não se aplica, pois sua evolução apresenta uma regularidade em seu desenvolvimento, conhecendo períodos de paradas, mas não etapas de erros ou rupturas que destruíssem o saber estabelecido anteriormente. Sendo assim, entendi ser necessário adaptar esta noção para o contexto da Matemática e também estabelecer como estes obstáculos seriam encontrados na História da Matemática. Uma possibilidade de aplicação da noção de obstáculo epistemológico segundo Bachelard, seria "ver" a Matemática como uma ciência experimental, em que os experimentos seriam experimentos mentais, como propõe Cifuentes e Negrelli (2006), para "traduzir" os obstáculo epistemológicos categorizados por Bachelard para a Matemática. Percebi que uma outra possibilidade seria a utilização de uma historiografia da Matemática, que não se guiasse apenas pelas contribuições de matemáticos famosos, mas de toda a comunidade matemática que tivesse se empenhado para desenvolver um conceito. Porém isso não é o que acontece atualmente, como indica Schubring (2002, 2006). O fato é que não encontrei uma formulação explícita do uso desta noção na análise do desenvolvimento da Matemática.

Em seu trabalho sobre obstáculos na aprendizagem da noção de limite, Cornu (1983) toma como obstáculo um conhecimento que faz parte do conhecimento do aluno e "traduz" o obstáculo da experiência primeira, apresentada por Bachelard, como sendo as concepções espontâneas, as ideias anteriores, que não são o fruto de um ensinamento organizado.

Para Cornu (1983, p. 31), o desenvolvimento de uma noção matemática é constituído pela superação de obstáculos, de conflitos e recuos, assim como acontece com o estudante quando adquire um novo conhecimento.

Sobre a noção de limite, ele afirma que: "... a história da noção de limite é rica em obstáculos, e as reflexões de Bachelard a propósito de obstáculos se aplicam muito bem a Matemática. O que ele chama " a experiência primeira", pode se ver de outra

forma. Em particular, o que chamamos de concepções espontâneas é uma variante deste obstáculo " (CORNU, 1983, p. 31, tradução da autora). No entanto, ele não indica de quem são essas concepções espontâneas, se dos matemáticos que desenvolveram esta noção ou dos estudantes que participaram de sua pesquisa, deixando ainda sem uma definição clara o que ele entende por obstáculo epistemológico na aprendizagem e na evolução histórica do conceito matemático. Nesse mesmo trabalho, Cornu adverte que não se trata de saber se os obstáculos encontrados na história são os mesmos encontrados pelos alunos de hoje, mas que o estudo dos obstáculos na história apenas facilitam a pesquisa dos obstáculos atuais na aprendizagem da noção de Limite.

Em sua tese de doutorado, citada acima, Cornu, a partir da análise histórica da evolução do noção de Limite, classifica quatro obstáculos epistemológicos na história desta noção, a saber: i) falha a relação entre números e geometria; ii) a noção de infinitamente grande e infinitamente pequeno; iii) o aspecto metafísico da noção de limite; iv) questionamento se o limite é atingido ou não.

A partir dessa classificação, ele propõe algumas estratégias pedagógicas, mas com a ressalva de que esta não é a solução para todos os problemas, devido à complexidade do assunto.

Para estabelecer a noção de obstáculo epistemológico na Didática da Matemática, Guy Brousseau, segundo Schubring (2002), valeu-se de uma analogia da ideia de Bachelard, de que um novo conhecimento não consegue integrar-se de uma só vez; o saber já existente não admite o novo, seja parcial ou inteiramente. Dessa forma, tem-se a noção de obstáculo na Didática da Matemática dada por Brousseau, como sendo:

> O obstáculo está constituído como um conhecimento, com os objetos, as relações, os métodos de apreensão, as previsões, com as evidências, as consequências esquecidas, as ramificações imprevistas,... Ele vai resistir à rejeição, ele tentará, como se deve, adaptar-se localmente, modificar-se, otimizar-se sobre um campo reduzido, seguindo um processo de acomodação bem conhecido. (BROUSSEAU, 1983, p. 175, tradução da autora).

Brousseau indica, ainda, que os erros mais frequentes dos alunos podem ser indícios de obstáculos didáticos e os classifica em:

1. obstáculos de origem ontogenética, que estão relacionados a aspectos psicológicos do aluno;

2. obstáculos de origem didática, que estão ligados aos aspectos institucionais de ensino, como currículo e escolha da estratégia de ensino;

3. obstáculos didáticos de origem epistemológica, que estão relacionados com o aspecto do desenvolvimento histórico do conceito.

Neste mesmo trabalho, Brousseau, em um comentário sobre o trabalho de Cornu (1983), diz que o mesmo coloca em evidência a hipótese geral, por ele formulada, de que "... algumas dificuldades dos alunos podem reunir-se em torno de obstáculos atestados pela história." (BROUSSEAU, 1983, p. 193, tradução da autora).

Em um trabalho mais recente, Brousseau (1997, p. 99, apud Schubring, 2002 p. 27), afirma que os passos para se encontrar um obstáculo epistemológico são os seguintes:

1. encontrar os erros recorrentes e mostrar que tais erros são agrupados ao redor de conceitos;

2. encontrar obstáculos na História da Matemática;

3. comparar obstáculos históricos com obstáculos para aprendizagem e estabelecer seu caráter epistemológico.

É importante observar que Brousseau apresenta primeiro a noção de obstáculo, para, depois classificá-lo, o que indica que, para ele, nem todo erro freqüente cometido pelos estudantes pode ser considerado um obstáculo epistemológico e nem toda dificuldade é causada por um obstáculo. Porém, ele não diz como encontrar estes obstáculos na História da Matemática.

Artigue (1990) afirma que o que fundamenta, de alguma maneira, um obstáculo epistemológico é mais a aparição e a resistência na história de certos conceitos, bem como a observação de concepções análogas entre os alunos, não a constatação da resistência a estes conceitos entre os estudantes da atualidade. Ou seja, ela defende que um obstáculo epistemológico é aquele encontrado na história do desenvolvimento do conceito em questão e que não é possível comprovar que um obstáculo em matemática é epistemológico apenas pela resistência de algum conceito ou erros recorrentes apresentados por estudantes de hoje.

A autora ainda identifica alguns processos produtores de obstáculos tanto historicamente quanto para os alunos da atualidade, como sendo: 1) a generalização

abusiva; 2) a regularização formal abusiva; 3) a fixação sobre uma contextualização ou uma modelização familiares; 4) a aderência exclusiva a um único ponto de vista.

Em Cornu (1991, p. 158), encontra-se, ainda a noção de obstáculo cognitivo. Ele considera que esta noção é interessante, pois ela pode ajudar a identificar as dificuldades dos estudantes na aprendizagem desse conceito e a formular estratégias de ensino. Este autor diz ainda que é possível distinguir vários tipos de obstáculos, como o "...genético ou psicológico, que ocorre por causa do desenvolvimento pessoal do estudante; o didático, que ocorre pela natureza do ensino e do professor; e os obstáculos epistemológicos, que ocorrem pela natureza dos conceitos matemáticos mesmo."

Um dos objetivos das pesquisas sobre obstáculo na aprendizagem (Cornu, 1983; Brosseau, 1983), além de detectá-lo, é encontrar estratégias para superá-los, seja ele didático ou de origem epistemológica. Para isso é necessário destruir o conhecimento mal formulado ou o conhecimento já estabelecido pelo aluno, que, por vezes, torna-se contraditório com o novo conhecimento. É necessário que ocorra uma "ruptura" com os conhecimentos já estabelecidos, sejam eles matemáticos ou do senso comum.

Apesar da noção de obstáculo ser utilizada nas pesquisas seja sobre aprendizagem ou sobre o desenvolvimento histórico de conceitos matemáticos, tais como: Cornu(1983), Sierpinska(1985), Malisani (1999), Schubring (2002), não existe um consenso sobre esta noção. Em Schubring (2002) é apontado que nem mesmo com a presença de especialistas no simpósio internacional *Obstacles et conflits cognitifs, 1988, em Québec*, chegou-se a um consenso de como esta noção deva ser utilizada na História da Matemática e na Didática da Matemática, devido não terem sido exploradas questões como: "Qual realidade corresponde ao conceito de obstáculo? Como reconhecer os obstáculos? Podem-se evitar os obstáculos na aprendizagem? Como se pode ultrapassar um obstáculo?" (BEDNARZ, 1989, p. 16, apud SCHUBRING, 2002).

Do estudo desses textos (Cornu, 1983, Brousseau, 1983, Artique, 1990, Schubring, 2002), pude observar que, para encontrar os "candidatos" a obstáculos na aprendizagem, é necessário identificar os erros recorrentes cometidos pelos estudantes na aprendizagem do conceito que está em jogo.

No caso do projeto inicial que pretendia desenvolver, para alcançar os objetivos propostos, seria feito um estudo histórico-epistemológico do conceito de congruência, evidenciando o uso do mesmo pelos matemáticos ao longo do tempo, buscando enten-

der as rupturas epistemológicas que ocorreram neste desenvolvimento, caso existissem[3]. Como ocorreu no uso da ideia do conceito de congruência módulo m, por Euler, antes que ela fosse definida e sistematizada por Gauss (Frei, 1994; Campos e Soares, 2006). O levantamento histórico realizado, até então, procurava entender as rupturas epistemológicas (Bachelard, 2000), que podem ocorrer na passagem de um tipo de fazer matemático para outro, seguindo as ideias de Lorenzo (2005).

Segundo Lorenzo (2005), o fazer matemático é uma prática dinâmica que vai se transformando e na qual se produzem rupturas epistemológicas, rupturas estas que têm suas consequências ontológicas, epistemológicas e metodológicas associadas, o que traz uma concepção de Matemática "... na qual se admite que nem tudo está dado de uma vez e para sempre, no universo da Matemática, no mundo sempre aberto da razão conceitual". (LORENZO 2005 p. 398, tradução da autora). No mesmo trabalho, o autor relata algumas de suas experiências, como aluno e como professor de Matemática, de algumas mudanças de fazeres matemáticos, por exemplo, a mudança da álgebra "clássica" para álgebra "moderna". A primeira, se dedica à resolução de equações algébricas, enquanto que a segunda, se dedica ao estudo das estruturas algébricas por si mesmas. Duas "versões" da álgebra que exigem organizações teórica e metodológica diferentes "... uma se mostra como saber produtivo ou artístico e a outra como um saber epistêmico" (ibid, 2005 p. 404, tradução da autora).

Este é um exemplo de mudança de um fazer matemático clássico para um fazer matemático moderno. Esta mudança traz uma nova linguagem, novos objetos matemáticos, e requer do matemático um novo tipo de raciocínio. A Álgebra passa a ser mais demonstrativa, seus objetos são, agora, mais abstratos, um exemplo muito ilustrativo da mudança do fazer matemático figural para o global, conforme Lorenzo (2005). O fazer matemático figural é aquele que está apoiado no concreto, que tende a ser mais prático e formulado para resolver problemas particulares, como, por exemplo, a teoria da divisibilidade de Euclides. Já o fazer matemático global é aquele que pode ser formulado de forma geral, apoiado na linguagem da Teoria de Conjuntos, em que as relações entre os objetos são mais importantes do que o próprio objeto e onde o conhecimento é apresentado na forma axiomática, como, por exemplo, a Teoria de Grupos.

Ainda, para alcançar os objetivos do projeto inicial, com base em Brousseau

[3] O resultado deste estudo histórico inicial pode ser encontrado no Apêndice C

(1997, apud Schubring, 2002), deveria também identificar os erros recorrentes dos estudantes em questões sobre congruência módulo m e comparar os obstáculos históricos com os obstáculos para aprendizagem e estabelecer seu caráter epistemológico.

Nesse percurso, ao buscar pesquisas sobre o ensino e a aprendizagem de Álgebra Abstrata no ensino universitário, que pudessem ajudar a fundamentar a minha pesquisa, encontrei os trabalhos de Dubynski et al. (1994), Asiala et al. (1997), Lajoie (2000), Lajoie e Mura (2004). Dentre estes trabalhos, chamou-me a atenção o de Lajoie e Mura (2004) sobre as dificuldades na aprendizagem dos conceitos de subgrupo normal e grupo quociente.

Para Lajoie (2000), uma dificuldade pode ser traduzida pela incapacidade de tratar de maneira eficaz ou de dar sentido a certos problemas, que ela entende poder se manifestar através dos erros cometidos pelos estudantes e também pelas hesitações e insegurança no momento de falar sobre determinado assunto.

Para caracterizar o sentido do termo "dificuldade", Lajoie (2000), partiu do significado corrente da palavra que se encontra nos dicionários e do significado dado por dicionários dedicados à educação, como, por exemplo, de que uma dificuldade é "a característica de um item ou de um instrumento de medida percebidos sob os aspectos de esforços, de capacidade necessária, de importância do desafio revelado para obter a ou as respostas certas" (LEGENDRE, 1988, apud LAJOIE, 2000, p. 30)[4]. Ela distinguiu a presença de dois pontos de vista para a abordagem das dificuldades: um que se prende mais ao caráter intrínseco de dificuldade sobre a essência de uma tarefa ou de uma noção e outro, que insiste mais sobre o mal-estar sentido por uma pessoa diante de uma situação considerada por ela difícil, da seguinte forma:

> O primeiro desses pontos de vista coloca foco sobre o caráter "intrínseco" de dificuldade que faz parte da essência de uma tarefa ou de uma noção, falamos então de uma complexidade, de uma sutileza desta tarefa, de um obstáculo, de uma barreira. O segundo insiste mais sobre o mal-estar sentido (mais ou menos consciente eu diria) por uma pessoa diante de uma situação considerada, por ela, difícil, falamos então de incômodo, de confusão, de aflição. (LAJOIE, 2000, p. 31, tradução da autora).

Observei nestes dois pontos de vista, um mais subjetivo, que está ligado ao

[4] Le Dictionnaire actuel de l´éducation (Legendre, 1988) define uma dificuldade como "caractère d´un item ou d´un instrument de mesure perçu sous l´aspect de l´effort, des capacités nécessaires, de l´importance du défi à relever pour obtenir la ou las réponses acceptées"

sentimento do sujeito; outro mais objetivo, que está vinculado à tarefa proposta ou a alguma noção.

Em Lajoie (2000), o termo dificuldade foi utilizado colocando estes dois pontos de vista como complementares, sendo que uma dificuldade é intrínseca a uma tarefa quando ela é suscetível de ser sentida pela maioria das pessoas que a realizam pela primeira vez.

Lajoie (2000) observa no uso do termo dificuldade por alguns educadores matemáticos, os dois pontos de vista mencionados acima, como em Glaeser (1981), em que o termo dificuldade, segundo esta autora, é também usado como "inaptidão", "estagnação ao nível de", sendo utilizado no sentido subjetivo do termo. O que já é diferente em Vergnaud (1988), em que a autora observa o outro ponto de vista, que no meu entender, é o mais objetivo do termo, pois descreve as dificuldades não em termos das pessoas que as encontra, mas, sim, em termos das noções matemáticas por elas mesmas. De acordo com Lajoie (2000), Vergnaud enumera as dificuldades relativas à aprendizagem da multiplicação e da divisão como sendo: "a concatenação de adições reiteradas, o produto cartesiano de dois espaços de medida e a possibilidade de dividir um número menor por um número maior". (VERGNAUD, 1988, apud LAJOIE, 2000, p. 32, tradução da autora). Às duas primeiras ele chama de dificuldade conceitual e à última, de obstáculo epistemológico, pois requer do estudante um salto de compreensão.

No trabalho de Lajoie e Mura (2004) o termo dificuldade é utilizado da mesma forma que em Lajoie (2000) e estas autoras não se preocuparam em estabelecer uma demarcação entre estes dois pontos de vista, por considerarem impossível determinar com certeza a causa de uma dificuldade. De fato, é possível observar em seu trabalho que estes dois aspectos foram levados em conta, os aspectos subjetivos, como por exemplo, a confusão entre as definições de subgrupo normal, subgrupo comutativo e subgrupo central, causada principalmente pela semelhança das notações desses conceitos. Já o aspecto, por mim denominado objetivo, aparece, por exemplo, no fato de os estudantes não reconhecerem o papel do subgrupo normal na construção do grupo quociente, quando para os estudantes a operação induzida no grupo quociente está intimamente ligada à operação do grupo de partida, o que faz o estudante não se preocupar em verificar se ela está bem definida.

Depois de estudar o artigo de Lajoie e Mura (2004), minhas suspeitas de que os erros dos estudantes nas respostas a questões sobre grupo quociente estivessem rela-

cionados com a noção de congruência, e a todos os conceitos ligados a ela, foi reforçada. Por exemplo, a dificuldade em entender a natureza dos elementos e da operação de um grupo quociente, em que, embora grande parte dos estudantes reconhecessem que os elementos do grupo quociente são classes de equivalência, eles consideraram que estes podiam ser elementos do grupo de partida ou que o grupo quociente podia ser um subgrupo do grupo de partida.

Entendo que isso possa ter acontecido porque, quando se trabalha com estes elementos, que são classes de equivalência, o que se utiliza é o representante desta classe. Como este representante é um elemento do grupo de partida, os estudantes parecem ter acreditado que classe e representante eram a mesma coisa, fazendo com que aceitassem a ideia de que os elementos do grupo quociente eram elementos do grupo de partida. O que, no meu entender, pode justificar o fato da maioria dos estudantes terem respondido na pesquisa de Lajoie e Mura (2004) que os elementos de G/N eram os mesmos de G.

Apliquei em março de 2006, o questionário elaborado por Lajoie e Mura (2004) e aplicado aos estudantes canadenses, para verificar se os estudantes do curso de Licenciatura e Bacharelado da UFPR apresentavam as mesmas dificuldades identificadas por elas. No Curso de Matemática da UFPR, o questionário foi respondido por dezessete (17) estudantes voluntários, que já haviam cursado a disciplina Álgebra A, na qual o conteúdo de Teoria de Grupos é ensinado. O resultado desta análise pode ser encontrado no Apêndice B.

Da análise das respostas destes estudantes, foi possível identificar, no que diz respeito ao uso de noções da teoria de conjuntos, um dos erros mais frequentes dos alunos ao trabalharem com a partição de um conjunto, esse erro foi identificado nas respostas à seguinte questão: *Seja* $\{S_1, S_2, ..., S_n\}$ *uma partição de um conjunto* E *e seja* x *um elemento de* E*. Podemos afirmar que* $x \in \{S_1, S_2, ..., S_n\}$*? Justifique sua resposta.*

Dos sete (7) estudantes que responderam "não" a esta questão, apenas um justificou corretamente a sua resposta, outros três (3) deram justificações errôneas, como, por exemplo, o estudante T_3, que escreveu: " Não, pois $\{x\} \in$ ao conjunto $\{S_1, S_2, ..., S_n\}$, pois para algum $S_i = \{x\}$, e não o elemento x". Esta resposta levou-me a pensar que o estudante entende as relações de pertinência e de inclusão e aceita o fato de um conjunto ser elemento de outro conjunto, mas não compreendeu o que é

uma partição. Os outros três (3) estudantes não justificaram suas respostas.

Dentre os seis (6) estudantes que responderam sim a esta questão, quatro (4) deles, T_6, T_4, N_5, B_2, justificaram da seguinte forma:

"Se $\{S_1, S_2, ..., S_n\}$ é uma partição de um E, então $E = S_1 \bigcup S_2 \bigcup ... \bigcup S_n$, logo $x \in S_i$, para algum $i = 1, 2, ...n$."

Esta resposta indica confusão entre as relações de pertinência e inclusão, pois, para eles, se $x \in S_i$, para algum $i = 1, 2, ..., n$, então $x \in \{S_1, S_2, ..., S_n\}$.

Um estudante, T_1, não conseguiu dizer se a afirmativa era verdadeira ou falsa, e justificou da seguinte forma: "Pode ser que sim ou que não, pois uma partição de um conjunto não é o conjunto todo". Uma resposta como esta indica que ele também não compreendeu o que é partição de um conjunto.

As respostas destes estudantes apontam que existe uma confusão entre as relações de inclusão e pertinência, que eles não compreenderam o que é partição de um conjunto e, também, que eles não conseguiram entender conjunto de conjuntos. O fato destes estudantes não entenderem o que é partição de um conjunto, parece explicar as respostas que deram a outras questões do mesmo questionário, veja Apêndice B, como, por exemplo, ao afirmarem que o grupo quociente G/N é um subgrupo do grupo G.

A análise das respostas destes estudantes ao questionário por mim aplicado e elaborado por Lajoie e Mura (2004) mostrou-me que as dificuldades encontradas foram as mesmas indicadas pelas referidas autoras, e assim, como elas, pude identificar que o entendimento de noções de Teoria de Conjuntos tem um papel importante para a aprendizagem de grupo quociente.

Diante da minha insegurança em trabalhar com os obstáculos epistemológicos na História da Matemática, por entender que para isso seria necessário o acesso aos textos históricos, como cartas entre matemáticos, rascunhos ou memórias de matemáticos que de alguma forma tivessem contribuído para o desenvolvimento do conceito de congruência, aos quais dificilmente teria acesso, caso existissem, optei por não desenvolver o projeto inicialmente proposto. E mais ainda, por considerar ser necessário justificar o porquê de usar a noção de obstáculo epistemológico na análise do desenvolvimento da Matemática, uma vez que o próprio Bachelard (1996) diz que ele não se aplica a esta Ciência, optei, então em identificar as dificuldades dos estudantes ao trabalharem com questões sobre congruência, no contexto da Teoria de Grupos, entendendo por

dificuldade o mesmo que Lajoie (2000) e Lajoie e Mura (2004).

A opção por identificar as dificuldades dos estudantes foi feita também por entender que as explicações de por que elas podem acontecer são abrangentes. Por exemplo, elas podem sim envolver obstáculos epistemológicos nas noções matemáticas focadas nesta pesquisa. Mas, deveriam envolvem também obstáculos didáticos e cognitivos a elas relacionados e até mesmo a falta ou falha em algum conhecimento necessário para a resolução de uma tarefa proposta. O que poderia contribuir com a reflexão sobre o ensino e aprendizagem de Álgebra no Ensino Superior.

Uma outra alteração no projeto inicial foi em relação ao conteúdo matemático escolhido. O Curso de Matemática, em que o projeto estava sendo desenvolvido, passava por uma mudança curricular. Até o ano de 2005 a disciplina do curso de Matemática da UFPR que tratava das estruturas algébricas, chamada de Álgebra A, era anual (veja ementa da disciplina no Apêndice A). Com a reformulação curricular pela qual o curso passou, esta disciplina foi substituída por três disciplinas semestrais: Teoria de Números, Teoria de Anéis e Teoria de Grupos, veja Apêndice A, nesta ordem. Embora não haja um consenso entre professores de Álgebra sobre se deve ser ministrado primeiro disciplina que trate de Grupos ou de Anéis, no novo currículo optou-se por ministrar primeiro a disciplina de Anéis e não de Grupo, como em geral é feito, com o objetivo de aproveitar os conhecimentos adquiridos sobre números inteiros na disciplina Teoria de Números e continuar trabalhando com o anel dos inteiros como exemplo, em Teoria de Anéis. De acordo com Rotmam (1996), a escolha de qual assunto deveria ser abordado primeiro, tanto em um livro quanto em um curso de graduação, depende mesmo é do professor, ou do autor, conforme a estratégia pedagógica a ser seguida. Assim, se por um lado, ao iniciar com grupos, tem-se a facilidade por trabalhar apenas com uma operação algébrica, por outro, ao iniciar pela teoria de anéis, tem-se a possibilidade de utilizar exemplos e fazer analogias com o anel dos inteiros.

Como no semestre em que seria feita a coleta de dados, a disciplina de Grupos não seria oferecida, ao invés de investigar as dificuldades na aprendizagem da noção de grupo quociente, como proposto anteriormente, passei a focar meu objeto matemático de estudo nas noções de congruência módulo m e anel quociente $\mathbb{Z}_m$, ensinadas nas disciplinas Teoria de Números e de Anéis. Um dos pontos positivos desta mudança foi que estas noções são os exemplos mais simples de congruência, por envolverem em suas definições inicialmente os números inteiros.

As pesquisas encontradas sobre ensino e aprendizagem de Álgebra, no nível universitário, são em sua maioria sobre conceitos de Teoria de Grupos, provavelmente por este conteúdo ser o primeiro conteúdo de uma disciplina sobre Álgebra Abstrata, das instituições onde as pesquisas foram desenvolvidas, como se pode verificar nas pesquisas de Lajoie (2000), Asiala et al. (1997), Lajoie (2004) e Findell (2001).

Assim, os objetivos apresentados no projeto submetido ao exame de qualificação eram os seguintes:

1. identificar as dificuldades dos estudantes ao trabalharem com uma relação de congruência módulo m;

2. identificar as dificuldades dos estudantes na aprendizagem do conjunto quociente Z_m;

3. identificar as dificuldades dos estudantes ao trabalharem com anel quociente. Em particular com anel Z_m;

4. analisar as relações entre as dificuldades anteriores.

No entanto, mesmo com esta alteração os referenciais teóricos permaneceram, uma vez que, tanto para construir o anel quociente quanto para construir o grupo quociente, a relação de congruência é necessária e um anel $\mathbb{Z}_m$ é também um grupo aditivo.

Naquele momento, com base no referencial teórico construído, observei que tanto para identificar os obstáculos didáticos de origem epistemológia (Brousseau, 1997, apud Schubring, 2002, p. 27), quanto para identificar as dificuldades na aprendizagem de subgrupo normal e grupo quociente (Lajoie e Mura, 2004), os autores mencionados partem da análise dos erros cometidos pelos estudantes. O que nos deu uma ideia de como o erro tem um papel importante nestas pesquisas, o que anteriormente não era visto dessa forma, pois o erro cometido pelos estudantes, em suas avaliações, nem sempre foi visto como indicativo de algo que pudesse ser estudado.

A partir do último quarto do século XX, com a influência do construtivismo, o erro passou a ser aceito e interpretado de forma diversa por professores, a ser considerado como analisável e a ser investigado, sendo a ele atribuídas determinadas dificuldades dos alunos na apreensão do conhecimento. O erro passou a "... ser encarado como

ferramenta para a aprendizagem ou construtor do conhecimento..." (CURY 2004, p. 2). Um resultado decisivo neste tipo de pesquisa, de acordo com Schubring (2002), é a importância dada às pré-concepções, ou seja, aos "...conhecimentos já estabelecidos no aluno, quando confrontado com um novo conhecimento..." (SCHUBRING, 2002, p. 28). Portanto, para este autor, os erros não são apenas atribuídos à falta de atenção ou à incapacidade cognitiva do aluno, mas podem estar relacionados a conhecimentos já estabelecidos, que entram em conflito com o novo conhecimento.

Atualmente, os erros cometidos pelos estudantes em suas avaliações tem sido estudados sob o ponto de vista psicológico, técnico, ou de ensino ou de aprendizagem, dependendo da teoria educacional vigente, como mencionado por Cury (2003). A ideia de anotar erros cometidos pelos alunos, classificá-los e analisá-los, tem sido utilizada como objeto de pesquisa, cujos resultados têm apontado alternativas para aprimorar estratégias de ensino, adaptação de currículos (Batista, 1995; Cury, 2003) e como metodologia de ensino (Cury e Konzen, 2006).

Para Cury , "...na análise das respostas dos alunos, o importante não é o acerto ou o erro em si..., mas as formas de se apropriar de um determinado conhecimento, que emergem na produção escrita e que podem evidenciar dificuldades de aprendizagem"(CURY, 2007, p. 63). Ou seja, o importante não é saber quantos acertaram ou erraram determinado problema, mas entender as formas como o aluno produziu esta resposta. Isso pode contribuir para que as dificuldades dos alunos sejam reconhecidas e, então, pode-se construir novos patamares de conhecimento, novas estratégias de ensino. É possível, também, compreender que conhecimento está funcionando "... como obstáculo para a superação da dificuldade e o que suas respostas decoradas estão encobrindo em termos de não-conhecimento." (ibid, p. 48).

Dessa forma, entendo que o erro, ou melhor, a resposta dos estudantes a determinada questão, seja ela certa ou errada, pode dar pistas de como eles estão compreendendo os conceitos; quais são as suas dificuldades e quais conhecimentos (matemáticos ou da prática social) podem estar funcionando como obstáculos na superação desta dificuldade.

Considerando estas breves reflexões sobre obstáculos na aprendizagem, erros e dificuldades, estabeleci alguns termos para esta pesquisa.

1.3 Delimitação de termos para pesquisa

Considero que a aprendizagem da Matemática não se dá pelo acúmulo de conhecimento, que ela pode não acontecer de forma linear e que a aprendizagem de um conceito tem aspectos subjetivos e objetivos. Os subjetivos podem ser entendidos como psicológicos ou afetivos e os objetivos são os aspectos ligados ao conceito matemático estudado.

Entendo que uma noção matemática foi aprendida de forma integral, quando o estudante é capaz de aplicá-la adequadamente em várias situações; quando ele consegue coordenar definição, notação, propriedades e exemplos; e quando ele faz ligações desta noção com outros conceitos. Por exemplo, considero que um estudante aprendeu a noção de congruência módulo m, quando ele consegue trabalhar tanto com a definição em termos de relação de equivalência; quanto com a definição via resto da divisão, quando ele utiliza suas propriedades e notação corretamente, e consegue visualizá-la em situações como na aritmética do relógio.

Concordo com as ideias de Brousseau (1993) que no processo de aprendizagem podem existir alguns conhecimentos do estudante, que funcionem como obstáculos na aprendizagem de algum conceito, causando dificuldades e levando o estudante a cometer erros.

O termo dificuldade, no sentido comum da palavra, é a qualidade do que é difícil, problema, impedimento, obstáculo, complicação e complexidade.

Por vezes, dizer que um estudante tem dificuldade na aprendizagem de algum conteúdo matemático parece levar em conta apenas os aspectos subjetivos, emocionais e afetivos da aprendizagem, deixando de lado os aspectos relacionados à noção matemática que ele está aprendendo. Ou ainda, que essa dificuldade acontece porque ele não gosta do assunto ou do professor.

Entendo que quando se diz que um aluno do ensino superior tem dificuldade de entender ou aprender algum conteúdo matemático, devido estar em jogo conteúdos matemáticos realmente complexos, pode-se pensar que ele não está desenvolvendo noções matemáticas de uma forma suficiente para compreendê-lo.

Na presente pesquisa, assim como em Lajoie (2000), entendo que uma dificuldade pode ser traduzida pela incapacidade de tratar de maneira eficaz ou de dar sentido a certos problemas, e que esta dificuldade pode se manifestar através dos erros

cometidos pelos estudantes e, também, pelas hesitações e inseguranças no momento de falar sobre determinado assunto.

Em Lajoie e Mura (2004), as autoras caracterizam melhor os dois pontos de vista sobre o termo dificuldade apresentado por Lajoie (2000), da seguinte forma:

> Por um lado, pode-se colocar o enfoque sobre o aspecto subjetivo da dificuldade, sobre que reação uma pessoa tem frente a uma situação considerada, por ela, difícil. Por outro lado, pode-se insistir mais no carácter intrínseco de dificuldades inerentes a uma tarefa, sobre a complexidade ou a sutileza desta tarefa. Certamente, a dificuldade de uma tarefa continua relativa à pessoa que deve realizá-la, mas qualificamos uma dificuldade de intrínseca quando é susceptível de ser sentida pela maioria das pessoas que a realizam pela primeira vez. (Lajoie e Mura, 2004, p. 48, tradução da autora).

Pelo que foi dito acima, estas autoras estão considerando um caráter intrínseco de dificuldade referente à complexidade da tarefa, que pode ser tomado como inerente ao conteúdo matemático em questão, que estou chamando de aspecto mais objetivo do termo dificuldade.

Na presente pesquisa, as interpretações e as explicações da origem dessas dificuldades estarão focadas no aspecto mais objetivo do termo; serão feitas visando estabelecer a falta ou a falha no conteúdo matemático necessário para a resolução das questões propostas. Não será considerado se o estudante gosta ou não da disciplina e do professor, ou se estava com algum problema de ordem, afetiva, emocional ou física ao responder as questões, pois entendo que não é possível precisar o quanto isso influenciou em suas respostas.

Em seu trabalho, Cury (2007) parece utilizar a palavra dificuldade preocupando-se mais com o aspecto objetivo do termo. Por exemplo, ao relatar as questões escolhidas para o teste que seria aplicado a estudantes de Cálculo, ela diz "...teve-se o cuidado de elencar questões cujos conteúdos estivessem de alguma forma relacionados com as dificuldades encontradas, em geral, no ensino de tópicos de Cálculo,...; dificuldades estas que não dependem do conhecimento de conteúdos específicos do Cálculo..." (CURY, 2007, p. 50). Ela procura determinar quais são os conteúdos da Matemática Básica do Ensino Fundamental e Médio que causam dificuldade na aprendizagem de Cálculo Diferencial e Integral.

Assim, para a presente pesquisa, o erro cometido por vários alunos pode ser indício de dificuldade em relação aos conceitos matemáticos envolvidos. Dificuldades estas que podem reunir-se ao redor de um obstáculo epistemológico ou não, de acordo com as ideias de Brousseau (1983).

Outra noção utilizada nesta pesquisa é a de obstáculo na aprendizagem que é entendida de acordo com as ideias de Brousseau (1983), isto é, um conhecimento que pode causar dificuldades na aprendizagem de algum conceito. Por exemplo a multiplicação de números naturais pode ser considerada um obstáculo na aprendizagem da multiplicação de números decimais, porque para números naturais o resultado desta multiplicação sempre é maior do que seus fatores e isso pode não acontecer nos números decimais, causando conflitos com conhecimentos até então estabelecidos pelo aluno.

Entendo que, para superar este obstáculo, deve haver uma "ruptura" com o conhecimento anterior, isto é, é necessário que o estudante aceite uma nova regra, e identifique que ela contradiz uma outra já estabelecida, a qual ele provavelmente acreditava ser única. O aluno vai, então, ampliar o seu conhecimento, mas não sem conflitos e contradições com o conhecimento anterior.

Com esses termos estabelecidos, elaborei minha questão de pesquisa e os objetivos da mesma, apresentados na próxima seção.

1.4 Questão norteadora e objetivos do trabalho

Depois das mudanças e ajustes no projeto, a questão norteadora desta pesquisa é:

O que os estudantes de um Curso de Matemática respondem sobre congruência algébrica em questões formuladas no contexto da Teoria de Números e Teoria de Anéis? O que se pode inferir destas respostas?

Tenho como hipótese de pesquisa que essas respostas podem estar relacionadas com a compreensão que eles têm de noções relacionadas à congruência algébrica como partição de um conjunto, relação de equivalência, estrutura quociente, entre outros.

O objetivo geral do projeto é :

Identificar e analisar as dificuldades dos estudantes, do curso de Matemática da UFPR, ao responderem questões sobre congruência algébrica no contexto da Teoria de Números e Teoria de Anéis.

Os objetivos específicos são:

1. identificar e analisar as dificuldades dos estudantes ao trabalharem a relação de congruência módulo m e o conjunto quociente $\mathbb{Z}_m$;

2. identificar e analisar as dificuldades dos estudantes ao trabalharem com anel quociente, no caso particular do anel quociente $\mathbb{Z}_m$.

O capítulo seguinte será dedicado a explorar os objetos matemáticos envolvidos nesta pesquisa, ou seja, a relação de congruência, a congruência módulo m e o anel quociente módulo ideal.

Capítulo 2

O Objeto Matemático

Neste capítulo será feita uma breve discussão sobre a noção de congruência, como objeto matemático e como ferramenta na construção de novos objetos matemáticos.

Para esta pesquisa, a noção de objeto matemático e ferramenta matemática será entendida como em Douady (1986). Em que um objeto matemático é um objeto cultural, reconhecido socialmente. E uma ferramenta matemática é um conceito focado na resolução de algum problema, no caso, na construção de novos objetos matemáticos.

Serão discutidas as possíveis definições de congruência módulo m e algumas de suas propriedades, além da construção do conjunto quociente $\mathbb{Z}_m$. O mesmo será feito para a noção de anel quociente e, em particular, para o anel quociente $\mathbb{Z}/m\mathbb{Z}$.

O objetivo deste capítulo não é fazer um estudo aprofundado destas noções, mas, sim, discutir alguns aspectos conceituais que considero importantes para esta pesquisa. Este estudo é necessário para conhecer os objetos matemáticos que estão envolvidos nesta pesquisa, uma vez que minhas suspeitas são que as dificuldades que os estudantes possam apresentar estão ligadas aos conceitos envolvidos nestas noções.

2.1 Congruência como objeto e como ferramenta matemática

2.1.1 Relação de congruência

Em Álgebra Abstrata, entende-se relação de congruência como uma relação de equivalência em um conjunto compatível com algumas operações algébricas.

Pelo que foi dito acima, é possível perceber que existem vários conceitos ligados a uma congruência, entre eles, a 'relação de equivalência', 'operação binária', 'classe de equivalência' e 'conjunto quociente'. No presente trabalho, quando me referir ao conceito de congruência, estarei englobando todos estes conceitos, como já foi dito anteriormente.

Mas o que significa esta relação de congruência? O que é uma relação de equivalência? Qual a necessidade da compatibilidade de operação? Nos próximos parágrafos pretendo responder ou, pelo menos, discutir estas questões.

Dizer que dois elementos de um conjunto são equivalentes significa dizer que eles são "os mesmos" em certos aspectos. A relação de equivalência revela um aparente paradoxo, "iguais mas diferentes", pois os elementos equivalentes são iguais sobre certos aspectos, mas em outros não.

Por exemplo, a relação R definida sobre os números inteiros da seguinte forma: para todo x, $y \in \mathbb{Z}$, xRy, se e somente se, $|x| = |y|$, que é uma relação de equivalência sobre $\mathbb{Z}$. Dessa forma, pode-se pensar que -1 e 1 são os mesmos (ou, são iguais) segundo a relação R. Pode-se interpretar esta relação como sendo a de que a distância de n a um ponto O é a mesma de $-n$ ao mesmo ponto.

Do mesmo modo, pode-se pensar nas equivalências de frações: uma fração $\frac{a}{b}$ pode ser vista como o par ordenado (a, b), onde a e b são inteiros e $b \neq 0$, e a equivalência de frações é dada por $(a, b)R(a', b')$ se e somente se $ab' = a'b$. Assim, pode-se dizer que $\frac{1}{2}$ e $\frac{4}{8}$ são equivalentes, ou que elas são iguais segundo esta relação, $\frac{1}{2} = \frac{4}{8}$, por isso podemos substituir uma pela outra.

Usando linguagem matemática, formalmente, pode-se definir uma relação de congruência da seguinte maneira:

Definição 1 *Dado um conjunto E munido de uma operação algébrica n-ária σ, $n \geqslant 1$, diz-se que R é uma relação de congruência sobre E com respeito a σ, se e somente se,*

1. *R é uma relação de equivalência;*

2. *para todo $x_1, ..., x_n, y_1, ..., y_n \in E$, se $x_k \, R \, y_k$ para $k = 1, 2, ..., n$ então $\sigma(x_1, ..., x_n) \, R \, \sigma(y_1, ..., y_n)$.*

Esta definição geral é feita usualmente no campo da Matemática chamado Álgebra Universal.

Por esta definição, tomando $E = \mathbb{Z}$, com as operações de adição $(+)$ e multiplicação $(\cdot)$ usuais, tem-se que uma relação de congruência R em $\mathbb{Z}$, compatível com as operações dadas, satisfaz:

1. se $a\,R\,b$ e $a'\,R\,b'$, então $a + a'\,R\,b + b'$.

2. se $a\,R\,b$ e $a'\,R\,b'$, então $a \cdot a'\,R\,b \cdot b'$.

Certamente, nem toda relação de equivalência em $\mathbb{Z}$ é uma relação de congruência a respeito das operações usuais. Veja o seguinte exemplo: seja R uma relação em $\mathbb{Z}$, definida por xRy, se e somente se, $|x| = |y|$. R é uma relação de equivalência sobre $\mathbb{Z}$, R é compatível com a multiplicação, pois se $|x| = |x'|$ e $|y| = |y'|$, então $|xy| = |x||y| = |x'||y'| = |x'y'|$, o que significa que $xy\,R\,x'y'$, mas R não é compatível com a adição, pois $-1\,R\,1$ e $2\,R\,2$, mas $(-1+2)\not{R}\,(1+2)$. Logo R não é uma congruência para adição (Warner, 1965).

Como uma relação de congruência no conjunto E é uma relação de equivalência, esta relação também produz uma partição em E, isto é, "divide" o conjunto E em subconjuntos dois a dois disjuntos e que, unidos, resulta no próprio E. É possível, então, definir para uma relação de congruência as respectivas classes de equivalência e o conjunto de classes de equivalência.

O método de construção dos conceitos envolvidos na relação de congruência, como classe de congruência e conjunto das classes, pode ser considerado uma ferramenta poderosa para a construção de novos objetos matemáticos a partir de outros já existentes. A utilização desta ferramenta pode ser reconhecida, por exemplo, na construção de espaços vetoriais, na construção dos números inteiros, racionais e reais, na construção de grupos quocientes e anéis quocientes, entre outros.

Considere um conjunto E e uma relação de equivalência R sobre E.

Definição 2 *A classe de equivalência de a, $\overline{a}$, é definida pelo conjunto*

$$\overline{a} = [a] = \{x \in E | xRa\}$$

ou seja, o conjunto de todos os elementos de E que se relacionam segundo R com a.

Embora a definição acima fale da classe de equivalência de a, este elemento é apenas um dos representantes dessa classe. Qualquer elemento da classe pode ser tomado como representante da mesma, ou seja, se $b \in \overline{a}$, então aRb , e teremos $\overline{a} = \overline{b}$.

Dessa forma, tomando E o conjunto dos números inteiros $\mathbb{Z}$ e a relação R definida por

$$xRy, \text{ se e somente se, } x - y \text{ é múltiplo de 2,}$$

teremos $\overline{0} = \{x \in \mathbb{Z} | x\, R\, 0\} = \{x \in \mathbb{Z} | x = 2k, \text{ para algum } k \in \mathbb{Z}\}$, é o conjunto dos números pares.

O conjunto das classes de equivalência de E pela relação de equivalência R é chamado *conjunto quociente* e é denotado por E/R. No exemplo anterior, o conjunto quociente é $\mathbb{Z}/R = \{\overline{0}, \overline{1}\}$, onde $\overline{0}$ é o conjunto dos números pares e $\overline{1}$ o conjunto dos números ímpares.

Usando a relação de equivalência constroem-se então, novos objetos matemáticos, a saber, as classes de equivalências e o conjunto quociente E/R, cujos elementos são também conjuntos, as classes de equivalência $\overline{a} = [a]$, símbolo utilizado por Rotman (1996).

O conjunto quociente E/R pode "herdar" operações algébricas análogas as de E e algumas de suas propriedades. Para isso, é necessário a garantia de que as operações em E/R estejam bem definidas. O que garante isso é a compatibilidade da relação de equivalência com as operações de E. Só assim, as operações entre as classes de equivalências podem ser feitas.

O que se espera dessa construção é que, dados $(E, *)$, um conjunto munido de operação binária e "$\equiv$" uma relação de congruência, se possa definir uma operação $\circledast$ também binária em $E/\equiv$, de forma que as propriedades dessa operação possam ser verificadas utilizando as propriedades já conhecidas de $*$, a fim de encontrar a estrutura algébrica de $(E/\equiv, \circledast)$. A operação $\circledast$ deve ser definida da forma mais "natural" possível, diz-se, então, que $\circledast$ é a operação induzida por $*$.

Se em $(E, *)$ tem-se que se $a \equiv a'$ e $b \equiv b'$, implica que $a * b \equiv a' * b'$, pode-se definir em $E/\equiv$ a operação $\circledast$ de forma que $\overline{a} \circledast \overline{b} = \overline{a * b}$, ou seja, a operação $*$ é utilizada na definição de $\circledast$, pois já se sabe quais as propriedades que a primeira satisfaz. Portanto, para que E/R tenha uma estrutura algébrica análoga à de E, é necessário que a relação R seja uma relação de congruência.

O exemplo a seguir ilustra como a compatibilidade das operações pode ser usada. No que se segue será feita a construção de $\mathbb{Q}$, a partir de $\mathbb{Z}$. Considere o

conjunto

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) | a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}$$

com as operações de adição e multiplicação definidas da seguinte forma:

$$(a, b) + (c, d) = (ad + cb, bd)$$

$$(a, b) \cdot (c, d) = (ac, bd)$$

Em $\mathbb{Z} \times \mathbb{Z}^*$ define-se a relação $\equiv$ da seguinte forma: $(a, b) \equiv (c, d) \Leftrightarrow ad = cb$ em $\mathbb{Z}$. Pode-se mostrar que esta relação é uma relação de equivalência e que para todo $(a, b), (c, d), (a', b'), (c', d') \in \mathbb{Z} \times \mathbb{Z}^*$, se $(a, b) \equiv (a', b')$ e $(c, d) \equiv (c', d')$, então $(a, b) + (c, d) \equiv (a', b') + (c', d')$ e $(a, b) \cdot (c, d) \equiv (a', b') \cdot (c', d')$.

Ou seja, esta relação preserva a operação, o que significa que essa relação é uma congruência.

As classes de congruência são

$$\overline{(a, b)} = \frac{a}{b} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* | (x, y) \equiv (a, b)\} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^* | xb = ay\},$$

ou seja, a classe de equivalência de (a, b) é o conjunto de todos os elementos de $\mathbb{Z} \times \mathbb{Z}^*$ que estão relacionados com (a, b). O par (a, b) é o representante da classe $\frac{a}{b}$, mas poderia ser (a', b'), desde que $(a, b) \equiv (a', b')$.

O conjunto $\mathbb{Q}$ é formado por todas as classes de equivalência de elementos de $\mathbb{Z} \times \mathbb{Z}^*$, isto é $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$. Em $\mathbb{Q}$ tem-se o seguinte: $\frac{a}{b} = \frac{c}{d}$ se e somente se $ad = bc$. Definem-se em $\mathbb{Q}$ as operações:

1. Adição: $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$.

2. Multiplicação $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

Estas operações estão bem definidas, ou seja, dados $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$ em $\mathbb{Q}$, tem-se que $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$.

De fato, de $\frac{a}{b} = \frac{a'}{b'}$, tem-se que $(a, b) \equiv (a', b')$ e de $\frac{c}{d} = \frac{c'}{d'}$, que $(c, d) \equiv (c, d)$. Como a relação $\equiv$ é uma congruência, tem-se $(a, b) + (c, d) \equiv (a', b') + (c', d')$, se e somente se $(ad+cb, bd) \equiv (a'd' + c'b', b'd')$, se e somente se $(ad+cb)b'd' = (a'd' + c'b')bd$, ou seja, $\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'}$. Portanto $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$.

Com estas operações, o conjunto $\mathbb{Q}$ é o corpo dos números racionais $\mathbb{Q}$, cujos elementos, as classes de equivalência, são os números racionais, que têm como representantes os pares ordenados ou as frações. Assim tem-se, por exemplo, que o número racional $3/2 = \{(3, 2), (6, 4), (9, 6), ...\} = \frac{6}{4} = \frac{9}{6}$.

A próxima seção será dedicada ao estudo da congruência módulo m e do conjunto quociente $\mathbb{Z}_m$, no contexto da Teoria de Números.

2.2 Congruência módulo m e o conjunto quociente $\mathbb{Z}_m$

O conceito de congruência módulo m pode ser identificado em diversas situações, tais como: no calendário, nas horas, na segurança de informação (criptografia); também pode-se reconhecer este conceito na matemática escolar, nos critérios de divisibilidade, na construção dos números módulo m, entendidos como restos da divisão por m, entre outros.

A congruência módulo m foi definida por Gauss em seu livro *Disquisitiones Arithmeticae* (1801), mas a ideia de trabalhar com restos da divisão de um número por m já era conhecida e utilizada por outros matemáticos, e o próprio Gauss reconhece isto neste seu livro.

Pode-se reconhecer a ideia da congruência módulo m em alguns trabalhos de Euler, por exemplo, no artigo *Theoremata circa residua ex divisione potestatum relicta* (1758/59, apud Wussing, 1984) sobre restos obtidos na divisão de potências a^v , onde v é um número natural, por um número primo p. De acordo com Wussing (1984), Euler assume que a não é divisível por p e conclui que a^v também não é. Assim ele investiga o que acontece com os restos das divisões dos termos da sequência infinita a^v, v número natural, por p.

Para Euler, mais importante que o resto r, tal que $0 < r < p$, é que todos os restos da forma $m + np$ (n um número natural) podem ser considerados como o mesmo resto r. Assim, como não existem mais que $p - 1$ restos não equivalentes, um número infinito de termos da sequência a^v deve deixar o mesmo resto. Em particular, muitos dos infinitos termos de a^v deixam resto 1 quando divididos por p.

Se a^γ é a menor potência que deixa resto 1 na divisão por p, então todas as potências a^γ que deixam resto 1 são da forma $a^{\gamma m}$, em que m é um número natural. Então, os restos da divisão por p das potências

$$1,\ a,\ a^2, ...,\ a^{\gamma-1}$$

são todos distintos.

Euler verificou que

$$1, a, a^2, ..., a^{\gamma-1},\ a^{\gamma},\ a^{\gamma+1}, a^{2\gamma-1},\ a^{2\gamma},\ a^{2\gamma+1}, ..., a^{3\gamma-1}$$

deixam o mesmo resto na mesma ordem, basta, portanto, investigar os restos das potências

$$1,\ a,\ a^2, ..., a^{\gamma-1}.$$

A congruência módulo m foi definida por Gauss da seguite maneira: "Se um número divide a diferença de dois números b e c, b e c são chamados congruentes relativos a a, ... O número a é chamado *modulus*. Se b e c são congruentes, cada um é chamado resíduo do outro. ... Designaremos congruência pelo símbolo $\equiv$ e colocaremos em parênteses o modulus..." (GAUSS, 1986, p. 1, tradução da autora).

Com esta definição Gauss estuda os resíduos dos termos das potências, obtendo os mesmos resultados de Euler, como, por exemplo: Se $a^t \equiv 1$ teremos $a^{t+1} \equiv a, a^{t+2} \equiv a^2$, etc., até chegar o termo a^{2t}. Seu resíduo será novamente congruente a 1 e o período dos resíduos começará de novo. Em geral teremos $a^{mt} \equiv 1$ e $a^{mt+n} \equiv a^n$.

O trabalho de Gauss(1801), *Disquisitiones Arithmeticae*, foi uma contribuição essencial para a Teoria de Números, que, segundo Ore (1988), inspirou a fase moderna dessa área da Matemática. Também foi considerado um dos seus maiores trabalhos, tanto pelos resultados apresentados como pela profundidade de suas novas ideias. Ainda de acordo com Ore (1988), o novo cálculo proposto por Gauss, a teoria das congruências, foi aceita quase imediatamente e, desde então, colocou seu nome em toda a terminologia da Teoria de Números. Os termos congruente e módulo são derivados do Latim: congruente significa "o que concorda" ou "o que corresponde", enquanto módulo significa "molde", "modelo", "pouca medida".

A definição e a notação utilizadas por Gauss (1986) são as mesmas usadas atualmente. A diferença está na linguagem utilizada que está apoiada na teoria de conjuntos e na lógica matemática.

Uma indicação da influência desta noção para a Teoria de Grupos está na definição e notação que Jordan (1873, apud Nicholson, 1993) utilizou para definir sua congruência módulo um subgrupo H,"...duas substituições s e t, que comutam com um grupo H, são chamadas congruentes segundo o grupo H, se podem ser escritas da seguinte forma $s = th$, onde h é uma substituição de H. Podemos expressar esta relação

pela fórmula análoga à das congruências ordinárias: $s \equiv t \pmod{H}$..." (JORDAN, 1873, apud NICHOLSON, 1993, p. 74, tradução da autora). Esta analogia pode ser encontrada também na Teoria de Anéis, quando se define a congruência módulo um ideal I.

Atualmente, esta mesma definição é utilizada nos textos sobre Teoria de Números empregados em cursos sobre o tema. Veja por exemplo a definição encontrada em Milies e Coelho (2003).

A congruência módulo m é definida da seguinte forma, Milies e Coelho (2003, p. 104):

Definição 3 *Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulo m se m divide a diferença $a - b$.*

A notação adotada pela maioria dos livros que tratam desta congruência é $a \equiv b \pmod{m}$ ou $a \equiv_m b$, que se lê como "a e b são *congruentes módulo* m" e $a \not\equiv b \pmod{m}$ para dizer que a e b não são congruentes módulo m; veja Milies e Coelho (2003), Santos (1998), Domingues (1991).

Assim tem-se, por exemplo, que $12 \equiv 5 \pmod{7}$, pois $7 \mid 12 - 5$. No entanto, $30 \not\equiv 4 \pmod{7}$, pois $7 \nmid 30 - 4$.

Uma caracterização de congruência módulo m, encontrada em Milies e Coelho (2003, p. 104) que facilita a resolução de muitos exercícios, é a seguinte:

Definição 4 *Seja m um inteiro fixo. Dois inteiros a e b são congruentes módulo m, se e somente se, eles têm como resto o mesmo inteiro quando divididos por m.*

Estas definições são matematicamente equivalentes e utilizamos uma ou outra, dependendo do que se pretende. Por exemplo, a definição 3 pode facilitar a demonstração de algumas propriedades, como a seguinte: Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$. De fato, sendo $a \equiv b \pmod{m}$, tem-se que $m|a - b$, ou seja, existe $k \in \mathbb{Z}$, tal que $a = b + km$, mas $b = a - km = a + tm$, isto é, $m|b - a$, ou seja, $b \equiv a \pmod{m}$.

Já a definição 4, facilita a resolução de exercícios numéricos, como, por exemplo, encontrar um número inteiro $b \neq 50121$, tal que $b \equiv 50121 \pmod{13}$. Como sabemos que dois inteiros são congruentes módulo m se tem o mesmo resto na divisão por m, basta encontrar o resto da divisão de 50121 por 13 e encontraremos b, assim $50121 \div 13 = 3855 \cdot 13 + 6$ e, então, $b = 6$. Na verdade, podemos encontrar um conjunto

de números que são congruentes a 50121, que são todos os números inteiros da forma $b = 6 + 13k$.

A congruência módulo m satisfaz algumas propriedades, entre elas as que mostram que esta é uma relação de congruência em $\mathbb{Z}$, ou seja, dados $a, b, c, d \in \mathbb{Z}$ valem as seguintes propriedades:

1. $a \equiv a \pmod{m}$ (reflexividade).
2. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$ (simetria).
3. Se $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$ (transitividade).
4. Se $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, então $a+c \equiv b+d \pmod{m}$ (compatibilidade com a adição).
5. Se $a \equiv b \pmod{m}$, $c \equiv d \mod m$, então $ac \equiv bd \pmod{m}$ compatibilidade com a multiplicação).

As três primeiras propriedades revelam que a congruência módulo m é uma relação de equivalência e as duas últimas garantem a compatibilidade desta relação com as operações de adição e multiplicação usuais de $\mathbb{Z}$. Estas cinco propriedades garantem que a congruência módulo m é uma relação de congruência sobre $\mathbb{Z}$ a respeito das operações mencionadas.

Como a congruência módulo m é uma relação de equivalência, pode-se definir a classe de equivalência, ou, neste caso, *classe de congruência de a módulo m*, como sendo o conjunto cujos elementos são todos os inteiros congruentes a a módulo m, ou seja,

$$\overline{a} = \{x \in \mathbb{Z} | x \equiv a \pmod{m}\} = \{a + tm \mid t \in \mathbb{Z}\}.$$

Como a relação de congruência módulo m é uma relação de equivalência, a congruência entre números a e b nos dá a igualdade entre as classes, isto é, $a \equiv b \pmod{m}$, se e somente se, $\overline{a} = \overline{b}$. Dessa forma, por exemplo, para $m = 4$, temos a igualdade das classes $\overline{0} = \overline{4} = \overline{16} = ...$ ou $\overline{3} = \overline{15} = \overline{-1} = \overline{55}$. Cada inteiro pertencente a uma classe é chamado *representante* da classe, como já foi dito anteriormente; assim, $3, 15$ e -1, são representantes da classe $\overline{3}$ na congruência módulo 4.

Encontrando todas as classes de congruência módulo m dos elementos de $\mathbb{Z}$, ou seja, particionando o conjunto dos números inteiros, o conjunto quociente $\mathbb{Z}_m =$

$\{\overline{a} \mid a \in \mathbb{Z}\}$ é o conjunto de todas estas classes e é também denotado por $\mathbb{Z}/\equiv_m$ ou $\mathbb{Z}/mZ$.

Em geral, o conjunto $\mathbb{Z}_m$ é escrito com os menores representantes não negativos de cada classe, que corresponde aos restos da divisão de qualquer inteiro por m, assim, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$. Por exemplo, para $m = 8$, $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{7}\}$.

No conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ podemos definir as operações de adição e multiplicação da seguinte forma:

1. Adição.

   $\overline{a} + \overline{b} = \overline{a+b}$, $\forall \overline{a}, \overline{b} \in \mathbb{Z}_m$.

2. Multiplicação.

   $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$,$\forall \overline{a}, \overline{b} \in \mathbb{Z}_m$.

O fato da relação de congruência módulo m ser uma congruência garante, como vimos na seção anterior, que estas operações estão bem definidas. Podemos ainda mostrar que estas operações têm, salvo algumas adaptações, as mesmas propriedades da adição e multiplicação de $\mathbb{Z}$, ou seja, o $\mathbb{Z}_m$ "herdou" a estrutura de $\mathbb{Z}$.

As propriedades da adição de $\mathbb{Z}$, que valem para $\mathbb{Z}_m$, são as seguintes: associatividade, existência do elemento neutro ($\overline{0}$), existência do elemento oposto ($\overline{-a}$) e comutatividade. E as propriedades da multiplicação de $\mathbb{Z}$ que valem para $\mathbb{Z}_m$, são as seguintes: associatividade, comutatividade, existência do elemento identidade ($\overline{1}$) e distributividade.

No entanto, a propriedade cancelativa, ou a lei do cancelamento, da multiplicação precisa de alguma adaptação para funcionar em $\mathbb{Z}_m$, para ela vale o seguinte: "A propriedade cancelativa do produto vale em $\mathbb{Z}_m$ se e somente se m é primo." (MILIES e COELHO, 2003, p. 143). Isto porque $\mathbb{Z}_m$ pode ter *divisores de zero*, isto é, se $\overline{a}, \overline{b} \in \mathbb{Z}_m$, onde $\overline{a}, \overline{b}$ são não nulos, pode ocorrer $\overline{a}\overline{b} = \overline{0}$, como, por exemplo, em $\mathbb{Z}_8$, onde $\overline{2} \cdot \overline{4} = \overline{8} = \overline{0}$ e $\overline{6} \cdot \overline{4} = \overline{24} = \overline{0}$; neste caso, temos $\overline{2} \cdot \overline{4} = \overline{6} \cdot \overline{4}$ mas $\overline{2} \neq \overline{6}$.

Para ilustrar todo o procedimento de construção do $\mathbb{Z}_m$, será construído em detalhes o conjunto quociente $\mathbb{Z}_4$.

A congruência módulo 4 é definida por: $a \equiv b \pmod 4$ se e somente se $4 \mid a - b$. Por exemplo, $6 \equiv 2 \pmod 4$, pois $4 \mid 6 - 2 = 4$, mas $13 \not\equiv 2 \pmod 4$, pois $4 \nmid 13 - 2 = 11$.

As classes de congruência módulo 4, isto é, $\overline{a} = \{x \in \mathbb{Z} | x \equiv a \pmod 4\}$, são:

$$\overline{0} = \{..., -8, -4, 0, 4, 8, ...\} = \{4k | k \in \mathbb{Z}\}.$$
$$\overline{1} = \{..., -5, -3, 1, 5, 9, ...\} = \{1 + 4k | k \in \mathbb{Z}\}.$$
$$\overline{2} = \{..., -6, -2, 2, 6, 10, ...\} = \{2 + 4k | k \in \mathbb{Z}\}.$$
$$\overline{3} = \{..., -3, -1, 3, 7, 11, ...\} = \{3 + 4k | k \in \mathbb{Z}\}.$$

O conjunto de todas as classes de congruência módulo 4, $\mathbb{Z}_4$, é o conjunto quociente $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, com apenas quatro elementos, já que $\overline{4} = \overline{0}$, $\overline{5} = \overline{1}$, $\overline{6} = \overline{2}$ e assim por diante. Neste conjunto, é possível somar e multiplicar os elementos de acordo com as operações definidas para $\mathbb{Z}_m$. Para o exemplo que está sendo trabalhado, tem-se as seguintes tabelas de operação:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Um aspecto da congruência módulo m interessante de ser observado é o da periodicidade ou circularidade, que pode ser representado por uma circunferência dividida em m partes, em que cada um dos m pontos corresponde a uma classe de congruência. Assim para m = 12, a estrutura algébrica de

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{910}, \overline{11}\}$$

pode ser representada pelas horas do mostrador do relógio e, questões como a de calcular o horário de chegada em uma viagem podem ser utilizadas como exemplo de aplicação desse conteúdo matemático.

Nesta seção, por meio da congruência módulo m, foram construídos novos objetos matemáticos, a saber, a classe de congruência módulo m e o conjunto quociente $\mathbb{Z}_m$, cujas operações satisfazem algumas propriedades das operações usuais de $\mathbb{Z}$. Exemplos de objetos matemáticos, construídos a partir de outros já existentes, com a utilização da relação de congruência podem ser encontrados, como, por exemplo o anel quociente que será abordado na próxima seção.

2.3 Congruência módulo I e o anel quociente A/I

Nesta seção será definido o anel quociente A/I, mostrando a possível generalização da congruência módulo m, estudada na seção anterior. Um aspecto importante a ser tratado aqui é que a construção de um anel quociente pode ser vista como algo análogo à construção do anel $\mathbb{Z}_m$ feita na seção anterior.

Em Teoria dos Anéis, o anel quociente é uma forma de construir novos anéis a partir de um anel dado, tratando como "iguais" elementos distintos do anel. Para isso, considera-se subconjuntos do anel que possuem certas propriedades especiais (que serão determinadas com mais cuidado a seguir), chamados ideais do anel. Cada ideal I determina uma congruência no anel A e, como já vimos, o conjunto quociente A/I determinado por congruência tem operações bem definidas - e também é um anel.

Com isso, de acordo com Fraleigh (2002, p. 220), é possível mostrar por exemplo, que se um polinômio $f(x) \in \mathbb{Z}[x]$ de grau n é tal que $\overline{\sigma_m}(f(x))$ é irredutível em $\mathbb{Z}_m[x]$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$, onde $\overline{\sigma_m} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_m[x]$, é definido por $\overline{\sigma_m}(a_0 + a_1x + \cdots + a_nx^n) = \sigma_m(a_0) + \sigma_m(a_1)x + \cdots + \sigma_m(a_n)x^n$, onde $\sigma_m(a) = \overline{a}$.

As próximas seções mostram quais as propriedades que o subconjunto I de A deve ter para que A/I seja o mais parecido possível com A.

2.3.1 Anel comutativo com unidade

O objetivo desta seção é fazer um breve estudo da construção do anel quociente, que generaliza o anel quociente $\mathbb{Z}/m\mathbb{Z}$. Para isso será dada a definição de anel.

De acordo com Gonçalves (1979) define-se anel da seguinte maneira:

Definição 5 *Seja A um conjunto não vazio, no qual estejam definidas duas operações, as quais chamaremos de soma e produto e denotaremos por $+$ e $\cdot$ respectivamente.*

Chamaremos $A, +, \cdot$ de anel se as seguintes propriedades são verificadas quaisquer que sejam $a, b, c \in A$:

1. *$(a + b) + c = a + (b + c)$, associatividade da soma;*
2. *existe $0 \in A$ tal que $a + 0 = 0 + a = a$, existência do elemento neutro para soma;*
3. *para todo $x \in A$ existe um único $y \in A$, denotado por $y = -x$, tal que $x + y = y + x = 0$, existência de inverso aditivo;*
4. *$a + b = b + a$, comutatividade da soma;*
5. *$(ab)c = a(bc)$, associatividade do produto;*
6. *$(a + b)c = ac + bc$ e $a(b + c) = ab + ac$, distributividade à direita e à esquerda;*

Se um anel $A, +, \cdot$ satisfaz a propriedade:

Existe $1 \in A, 1 \neq 0$, tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in A$, diz-se que $A, +, \cdot$ é um *anel com unidade* 1.

Se um anel $A, +, \cdot$ satisfaz a propriedade:

Para todo $a, b, \in A$, $a \cdot b = b \cdot a$, diz-se que $A, +, \cdot$ é um *anel comutativo.*

Tem-se como exemplos de anel os conjuntos seguintes com suas operações usuais: os inteiros $\mathbb{Z}$, os racionais $\mathbb{Q}$. O conjunto quociente $\mathbb{Z}_m$ definido na seção anterior, é um anel para as operações de adição $\overline{a} + \overline{b} = \overline{a + b}$ e multiplicação $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$..

Alguns subconjuntos não vazios de um anel A, têm algumas propriedades que os tornam subconjuntos especiais, como no caso de um subanel que é definido a seguir, de acordo com Gonçalves (1979).

Definição 6 *Seja $A, +, \cdot$ um anel e B subconjunto não vazio de A. Suponhamos que B seja fechado para as operações $+$ e $\cdot$ de A, isto é,*

a) $x, y \in B \Rightarrow x + y \in B$

b) $x, y \in B \Rightarrow x \cdot y \in B$.

Assim podemos também considerar a soma e o produto como operações em B. Se $B, +, \cdot$ for um anel com as operações de A dezemos que B é um subanel de A.

Um critério utilizado para verificar se um subconjunto é um subanel, é dado pela seguinte proposição.

Proposição 1 *Seja $(A, +, \cdot)$ um anel e seja B um subconjunto não vazio de A. Então B é um subanel de A se e somente se as seguintes condições são verificadas:*

1. $0 \in B$;
2. $x, y \in B \Rightarrow x - y \in B$;
3. $x, y \in B \Rightarrow x \cdot y \in B$.

Uma demonstração desta proposição pode ser vista no livro (Gonçalves, 1979).

Pode-se verificar que $2\mathbb{Z} = \{2k, k \in \mathbb{Z}\}$ é um subanel de $\mathbb{Z}$, já que ele satisfaz as seguintes condições:

1. $0 \in 2\mathbb{Z}$, neste caso $k = 0$;
2. se $x, y \in 2\mathbb{Z}$, então $x = 2k$ e $y = 2s$, com $k, s \in \mathbb{Z}$, assim, $x - y = 2k - 2s = 2(k - s) = 2t$, portanto $x - y \in \mathbb{Z}$;
3. se $x, y \in 2\mathbb{Z}$, então $x = 2k$ e $y = 2s$, com $k, s \in \mathbb{Z}$, assim, $x \cdot y = 2k \cdot 2s = 2(k \cdot 2s) = 2t$, portanto $x \cdot y \in \mathbb{Z}$.

2.3.2 Ideal e Anel Quociente

Em Teoria dos Anéis, um ideal é um subconjunto especial de um anel. O conceito generaliza de uma maneira apropriada algumas importantes propriedades dos inteiros, como "número par" e "múltiplo de 3".

Por exemplo, em anéis estuda-se ideais primos ao invés de números primos, define-se ideais coprimos como generalização de números coprimos entre si e pode-se provar um teorema do resto chinês para ideais. Um ideal pode ainda ser usado para a construção de um anel quociente da mesma forma que um subgrupo normal pode ser usado para a construção de um grupo quociente.

Um ideal pode ser definido da seguinte maneira, de acordo com Rotman (1996):

Definição 7 *Seja A um anel comutativo e diz-se que um subconjunto I de A, é um* ideal *de A se:*

1. $0 \in I$;
2. *se $a, b \in I$, então $a - b \in I$;*

3. se $b \in I$ e $a \in A$ então $ab \in I$.

Pode-se observar que o item 3 acima, difere do item 3 da proposição 2.3.1, nos conjuntos aos quais os fatores pertencem.

Outra definição de ideal também pode ser dada da seguinte forma: um subanel I de A é um ideal de A se $A \cdot I \subset I$ e $I \cdot A \subset I$, de acordo com Gonçalvez (1979); sendo $A \cdot I = \{c \in A | c = a \cdot x, \forall\, a \in A \text{ e } x \in I\}$.

Por exemplo $3\mathbb{Z} = \{x \in \mathbb{Z} |\, x = 3k, \text{ para algum } k \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$, pois:

1. $0 \in 3\mathbb{Z}$, de fato, basta tomar $k = 0$;

2. $x, y \in 3\mathbb{Z} \Rightarrow x - y \in 3\mathbb{Z}$. De fato, sendo $x = 3k$ e $y = 3t$, para algum $k, t \in \mathbb{Z}$, $x - y = 3k - 3t = 3(k - t) \in 3\mathbb{Z}$;

3. $x \in 3\mathbb{Z}, y \in \mathbb{Z} \Rightarrow xy \in 3\mathbb{Z}$, de fato, sendo $x = 3k$, $xy = 3ky \in 3\mathbb{Z}$.

Os ideais I tais que $I \neq A$ são chamados ideais próprios de A. Pode-se mostrar que se $A = \mathbb{Z}$, então existe $m \in \mathbb{Z}$ tal que $I = m\mathbb{Z}$, onde $m\mathbb{Z} = \{km |\, k \in \mathbb{Z}\}$. Veja, por exemplo, no caso $m = 2$, onde $I = \{2a |\, a \in \mathbb{Z}\} = 2\mathbb{Z}$, ou seja, o conjunto dos números inteiros pares.

Esta definição de ideal permite generalizar a noção de congruência módulo m, $\equiv \pmod m$, em $\mathbb{Z}$ da seguinte maneira: considere $I = m\mathbb{Z}$, então, para $x, x' \in \mathbb{Z}$, temos $x \equiv x' \pmod m \Leftrightarrow x - x' \in m\mathbb{Z}$ define uma relação de equivalência. Assim, se $x \equiv x^{'} \pmod m$, então $x - x^{'} = mk$ para algum $k \in \mathbb{Z}$, mas $mk \in m\mathbb{Z}$, logo $x - x^{'} \in m\mathbb{Z}$. Por outro lado, se $x - x^{'} \in m\mathbb{Z}$, então $x - x^{'} = mk$ para algum $k \in \mathbb{Z}$, o que significa que $x \equiv x^{'} \pmod m$.

No que se segue, será feita a generalização desta ideia para um anel qualquer.

Seja A um anel qualquer e seja I um ideal de A. Define-se a seguinte relação em A, para todo $x, x^{'} \in A$,

$$x \equiv x^{'} \pmod I \Leftrightarrow x - x^{'} \in I.$$

Primeiramente, prova-se que congruência módulo I define uma relação de equivalência em A.

De fato, quaisquer que sejam $x, x^{'}, x^{''} \in A$, tem-se

i) $x \equiv x \pmod I$, pois $x - x = 0 \in I$.

ii) $x \equiv x^{'} \pmod{I} \Rightarrow x^{'} \equiv x \pmod{I}$, pois se $x - x^{'} \in I$, então $x^{'} - x = -(x - x^{'}) \in I$.

iii) $x \equiv x^{'} \pmod{I}$ e $x^{'} \equiv x^{''} \pmod{I} \Rightarrow x \equiv x^{''} \pmod{I}$, pois $x - x^{'} \in I$ e $x^{'} - x^{''} \in I \Rightarrow x - x^{''} = (x - x^{'}) + (x^{'} - x^{''}) \in I$

Denota-se por $\overline{x} = \{y \in A | y \equiv x \pmod{I}\}$ a qual chama-se de *classe de equivalência* do elemento $x \in A$ relativamente à relação $\equiv \pmod{I}$.

Agora, observe que $y \in \overline{x} \Leftrightarrow y - x \in I$, e, por isso, também denota-se a classe $\overline{x}$ por $\overline{x} = x + I = \{x + z | z \in I\}$. Chama-se de *conjunto quociente de A pelo ideal I* ao conjunto $A/I = \{\overline{x} = x + I | x \in A\}$.

Como exemplo, será encontrada as classes de $x \in \mathbb{Z}$, relativamente à relação $\equiv \pmod{3\mathbb{Z}}$, isto é $x + 3\mathbb{Z} = \{y \in \mathbb{Z} | y \equiv x \pmod{3\mathbb{Z}}\}$.

$$0 + 3\mathbb{Z} = \{x \in \mathbb{Z} |\, x - 0 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} |\, x = 3k, k \in \mathbb{Z}\}$$
$$1 + 3\mathbb{Z} = \{x \in \mathbb{Z} |\, x - 1 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} |\, x = 1 + 3k, k \in \mathbb{Z}\}$$
$$2 + 3\mathbb{Z} = \{x \in \mathbb{Z} |\, x - 2 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} |\, x = 2 + 3k, k \in \mathbb{Z}\}.$$

Neste caso, $3 + 3\mathbb{Z} = \{x \in \mathbb{Z} |\, x - 3 \in 3\mathbb{Z}\} = \{x \in \mathbb{Z} |\, x = 3 + 3k, k \in \mathbb{Z}\} = \{x \in \mathbb{Z} |\, x = 3t, t \in \mathbb{Z}\} = 0 + 3\mathbb{Z}$.

Assim, o conjunto quociente $\mathbb{Z}/3\mathbb{Z}$ possui três elementos, as classes $0+3\mathbb{Z}, 1+3\mathbb{Z}$ e $2 + 3\mathbb{Z}$ ou pode-se escrever $\overline{0}, \overline{1}$ e $\overline{2}$.

A proposição a seguir permitirá definir as operações $+$ e $\cdot$ no conjunto quociente A/I de modo a torná-lo um anel.

Proposição 2 *Sejam A um anel e I um ideal em A. Se* $x \equiv x^{'} \pmod{I}$ *e* $y \equiv y^{'} \pmod{I}$*, então:*

$$(a)\, x + y \equiv x^{'} + y^{'} \pmod{I}$$

$$(b)\, x \cdot y \equiv x^{'} \cdot y^{'} \pmod{I}$$

Para provar (a), basta observar que $(x+y)-(x^{'}+y^{'}) = (x-x^{'})+(y-y^{'}) \in I$, pois $(x - x^{'})$ e $(y - y^{'}) \in I$.

Agora, para provar (b), considere $x = x^{'} + a, a \in I$ e $y = y^{'} + b, b \in I$. Então,

$x \cdot y - x^{'} \cdot y^{'} = (x^{'} + a) \cdot (y^{'} + b) - x^{'} \cdot y^{'} = x^{'} \cdot y^{'} + x^{'} \cdot b + a \cdot y^{'} + a \cdot b - x^{'} \cdot y^{'} = x^{'} \cdot b + a \cdot y^{'} + a \cdot b$

e como $a, b \in I$ e I é um ideal de A segue que $x \cdot y - x^{'} \cdot y^{'} \in I$.

Como corolário imediato desta Proposição, segue a seguinte proposição.

Proposição 3 *Sejam A um anel, I um ideal de A. Se $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$ então*

$$(a)\, \overline{x+y} = \overline{x'+y'}$$

$$(b)\, \overline{x \cdot y} = \overline{x' \cdot y'}$$

O item (a) diz que a classe da soma independe dos representantes das duas classes das parcelas, enquanto o item (b) diz que a classe do produto independe dos representantes das classes dos fatores.

Proposição 4 *Seja A um anel e I um ideal de A. Se $\overline{x} = x + I$ e $A/I = \{\overline{x} : x \in A\}$, então:*

$$+ : A/I \times A/I \longrightarrow A/I \quad e \quad \cdot : A/I \times A/I \longrightarrow A/I$$

$$(\overline{x}, \overline{y}) \rightsquigarrow \overline{x} + \overline{y} = \overline{x+y} \qquad (\overline{x}, \overline{y}) \rightsquigarrow \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

definem as operações (denominadas soma e produto) em A/I, que é um anel com estas operações.

2.3.3 $\mathbb{Z}_m$ ou $\mathbb{Z}/m\mathbb{Z}$?

Na seção 2.2 foi construído o conjunto quociente $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$, que munido das operações definidas na referida seção é um anel comutativo. Na seção anterior, foi construído o anel quociente $\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, ..., m - 1 + m\mathbb{Z}\}$, como uma generalização da congruência módulo m, o que faz com que $\mathbb{Z}_m$ seja o próprio $\mathbb{Z}/m\mathbb{Z}$. Sendo assim, pode-se utilizar qualquer uma das notações $\mathbb{Z}_m$ ou $\mathbb{Z}/m\mathbb{Z}$ para esse anel quociente.

Embora estes conjuntos sejam matematicamente iguais, suas construções requerem objetos matemáticos diferentes; enquanto para construir os elementos de $\mathbb{Z}_m$, que são classes de congruência módulo m, os objetos matemáticos envolvidos são divisibilidade, ou resto da divisão, para construir os elementos de $\mathbb{Z}/m\mathbb{Z}$, que são classes de congruência módulo ideal, as noções envolvidas são anel, subanel, operação entre elementos do anel e do ideal. Esta diferença, no caso dos anéis em questão, pode não fazer sentido para o professor, mas para o estudante, que está aprendendo estas estruturas, esta diferença pode dificultar a aprendizagem da noção de anel quociente, pois o nível de abstração é maior quando os conceitos de Teoria de Anéis estão presentes.

Alguns autores definem $\mathbb{Z}_m$ como conjunto de resíduos (ou restos) módulo m, como é o caso de Domingues (1991), Fraleigh (2002), Birkhoff e Maclane (1980), isto é, $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ é o conjunto de restos da divisão de inteiros por m, este conjunto é um subconjunto de $\mathbb{Z}$. O conjunto de resíduos $\mathbb{Z}_m$ com as operações adição e multiplicação módulo m, é um anel comutativo.

É possível mostrar então, veja Fraleigh (2002), que $\mathbb{Z}_m$ definido dessa forma é isomorfo ao anel quociente $\mathbb{Z}/m\mathbb{Z}$ usando o Teorema do Isomorfismo (Gonçalves, 1979; Rotmam, 1996; Fraleigh, 2002). E assim pode-se entender $\mathbb{Z}_m$ como anel de resíduos módulo m e abusando da notação pode-se escrever $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

Temos então duas maneiras distintas de entender o conjunto $\mathbb{Z}_m$: uma como conjunto de restos da divisão de inteiros por m e outra como conjunto de classes de congruência módulo m. A escolha de uma ou outra definição depende do objetivo do curso, do professor e dos textos utilizados para as aulas, e as implicações dessa escolha na aprendizagem do estudante podem ser diferentes, pois se pode, por exemplo, entender $\mathbb{Z}_m$ como subconjunto de $\mathbb{Z}$ ou não.

Uma outra questão a ser levantada é sobre o isomorfismo[1]. Em Álgebra Abstrata, o que interessa são as propriedades algébricas dos conjuntos e suas operações, e não os nomes dos seus elementos e operações. Assim dizer que um anel é isomorfo a outro significa que suas propriedades algébricas são as mesmas, ou seja, que eles são essencialmente os mesmos, diferindo somente na notação para os seus elementos e operações. Veja por exemplo, os conjuntos $R = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{R}$ e $R' = \{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \,|\, a, b \in \mathbb{Z}\} \subset M_2(\mathbb{Z})$. Estes dois conjuntos são isomorfos[2], mas seus elementos e operações são bem diferentes entre si.

A próxima seção mostra como a congruência está inserida no currículo do Curso de Matemática da UFPR.

---

[1] Dizemos que uma função bijetiva $f : A \to A'$, sendo A e A' anéis é um isomorfismo de A sobre A', se as satisfaz as seguintes condições: (i) $f(x + y) = f(x) + f(y), \forall x, y \in A$; (ii) $f(x \cdot y) = f(x) \cdot f(y), \forall x, y \in A$

[2] Considere o isomorfismo $f : R \to R'$ difinido por $f(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$

2.4 A noção de congruência no Curso de Matemática da UFPR

Nesta seção, será feita uma breve discussão de como a noção de congruência está inserida no currículo do Curso de Matemática da UFPR.

A construção de um novo objeto matemático, utilizando uma relação de congruência, é chamada de construção quociente, e é resumida pelos matemáticos na expressão "passar ao quociente", construção esta que nem sempre é entendida pelos estudantes. Esta construção não é simples, os conceitos envolvidos exigem do estudante um nível de abstração e de conhecimento matemático que nem sempre ele tem, mas ela está presente, mesmo que, implicitamente, em algumas disciplinas.

A congruência módulo m é apresentada para os estudantes pela primeira vez, na disciplina Complementos de Matemática (CM100), no currículo anterior ela era apresentada em Fundamentos da Matemática C (CM430), as ementas dessas disciplinas podem ser encontradas no Apêndice A, quando se estudam relações de equivalência e a congruência módulo m era dada como um exemplo deste tipo de relação. É na disciplina Teoria de Números que os alunos deveriam trabalhar pela primeira vez com a congruência módulo m do ponto de vista algébrico, sendo utilizada para construir o conjunto quociente $\mathbb{Z}_m$, quando o conjunto dos números inteiros ainda não é tratado como um anel. Da mesma forma que o $\mathbb{Z}_m$ também não é tratado como anel quociente; isto será feito apenas na disciplina Teoria de Anéis.

No currículo atual do curso de Matemática não existe uma disciplina obrigatória na qual se estude a noção de congruência do ponto de vista da Álgebra Universal, ou que se estude a congruência por ela mesma. Esta noção é trabalhada nas disciplinas de Álgebra, no contexto da Teoria de Números, quando se estuda congruência módulo m, da Teoria de Anéis, quando se estuda ideais e anéis quocientes e, também, em Teoria de Grupos quando se estuda subgrupos normais e grupos quocientes. No currículo anterior, até o ano de 2005, ela era trabalhada nos mesmos contextos em uma única disciplina, Álgebra A.

Os livros indicados como texto para a disciplina Teoria de Números são: Milies e Coelho (2003), Santos (1998), Domingues (1991), Rotman (1996) entre outros. Em geral, eles trazem o conteúdo de congruência módulo m, com o objetivo de resolver as congruências lineares. Dos livros citados acima, apenas Milies e Coelho (2003) fazem

a construção de $\mathbb{Z}_m$ como conjunto de classe de congruência módulo m, e depois volta aos resultados das congruências lineares com esta nova linguagem, para mostrar como estes ficam mais simples. Os outros livros, ou não fazem esta construção, como Santos (1998), ou o fazem em outro contexto, como é o caso de Rotman (1996), em que esta construção é feita no contexto de Teoria de Grupos, quando trabalha grupo quociente.

Na disciplina Teoria de Anéis do curso de Matemática da UFPR, são estudados: a estrutura de anel e suas propriedades, o anel quociente, anel de polinômios e homomorfismos. Os livros textos indicados para isso são: Gonçalves (1979), Fraleigh (2002), Rotman (1996), Garcia e Lequain (2005), entre outros.

No caso da turma pesquisada neste trabalho, os textos seguidos mais de perto pelo professor das disciplinas Teoria de Números e Teoria de Anéis, investigada nesta pesquisa, foram Miles e Coelho(2003) e Gonçalves(1979), por este motivo foram mais citados nas seções precedentes e, no que segue neste trabalho, as notações e definições utilizadas nos questionários, entrevistas e análises, serão as desses autores, ou seja, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ como conjunto de classes. Quando o anel $\mathbb{Z}_m$ for entendido como conjunto de restos, isto será feito expressamente.

Capítulo 3

Algumas Pesquisas

Neste capítulo serão apresentadas algumas considerações sobre pesquisas em Matemática do Ensino Superior que ajudaram na formulação deste trabalho, seja para elaboração e análise de questões, seja para entender outros trabalhos.

3.1 Em Ensino Superior

Em seu artigo sobre as investigações em Educação Matemática, no nível universitário, Artigue (2003), destaca três tendências de perspectivas teóricas que ocorrem neste campo de pesquisa, são elas: "...a primeira, em termos da dualidade processo-objeto; a segunda em termos de obstáculos epistemológicos; a terceira, em termos de reconstruções de relações com objetos do conhecimento". (ARTIGUE, 2003, p. 120).

Segundo Lajoie (2000), as pesquisas em didática da matemática no âmbito da Matemática do Ensino Superior estão relacionadas em sua maioria, à compreensão de determinados conceitos matemáticos.

No que se refere à pesquisa sobre ensino e aprendizagem de Álgebra Abstrata, Hazzam (1999) categoriza as pesquisas em dois grupos: métodos de ensino e, aprendizagem, compreensão e desenvolvimento de conceitos em Álgebra Abstrata.

No Brasil, as pesquisas apresentadas no III SIPEM (Simpósio Internacional de Pesquisa em Educação Matemática), de acordo com o relatório do grupo de trabalho sobre Matemática no Ensino Superior, GT4, dos dezesseis trabalhos apresentados, dez deles eram sobre o ensino e aprendizagem de Cálculo ou Análise. Este relatório revela, ainda, que as tendências neste tipo de pesquisa, levantadas durante a discussão dos trabalhos, foram relativas à pertinência das abordagens intuitiva e formal e suas inter-

relações no ensino de um determinado conceito; a inserção da resolução de problemas e da investigação matemática como metodologias de ensino nas Licenciaturas; a presença da História da Matemática no desenvolvimento de conteúdos; a presença de aspectos afetivos no ensino-aprendizagem da Matemática (psicologia e psicanálise); a análise de erros e estilos de aprendizagem; integração da Matemática em cursos de serviço; a importância da publicação de livros nacionais para o ensino superior, que estejam de acordo com pontos levantados por pesquisas (GT4-SIPEM, 2006). As pesquisas realizadas em Álgebra são no âmbito da Álgebra Linear, ensino e aprendizagem de equações e estrutura curricular.

No XIII EBRAPEM (Encontro Nacional dos Estudantes de Pós-graduação em Educação Matemática), realizado no ano de 2008, no grupo de trabalho sobre Matemática no Ensino Superior, os trabalhos apresentados eram sobre ensino e aprendizagem, história do ensino e tecnologia na disciplina de Cálculo; cônicas na formação de professores e indução finita. Certamente, em outros grupos também havia trabalhos sobre Matemática no Ensino Superior, como formação de professor e tecnologia. No XI EBRAPEM, realizado em 2006, um trabalho sobre história e ensino de teoria de grupos foi apresentado, Brandemberg (2006); este trabalho de doutorado estava ainda no início.

No Brasil, não encontrei, nos bancos de teses da Capes e nas bibliotecas de algumas universidades, trabalhos sobre ensino e aprendizagem de estruturas algébricas, exceto a pesquisa de Kluth (2005), que faz uma investigação fenomenológica sobre a construção das estruturas algébricas. Embora este seja um trabalho interessante e bastante complexo, não será usado na presente pesquisa, por não estar ligado aos nossos objetivos. Por isso, os artigos utilizados nesta pesquisa são, em sua maioria, internacionais.

Descreverei, a seguir, os resultados de alguns trabalhos que, de alguma forma, contribuíram para a realização desta pesquisa. Estes artigos trazem como resultados algumas dificuldades que os estudantes podem encontrar quando estudam os conceitos de classe lateral, subgrupo normal e grupo quociente, alguns artifícios utilizados por eles para compreender estes conceitos e uma descrição de como se dá a aprendizagem destes conceitos. Os resultados destes trabalhos me forneceram indicações de como as congruências podem ser fonte de dificuldades na aprendizagem destes conceitos e de como amenizar estas dificuldades, que me ajudaram a reconhecer as outras dificuldades

na aprendizagem do conjunto quociente $\mathbb{Z}_m$ e do anel quociente.

3.1.1 Sobre ensino e aprendizagem em Teoria de Grupos

De acordo com Lajoie (2000), as pesquisas sobre ensino e aprendizagem em Teoria de Grupos tiveram um forte impulso com os trabalhos de Dubinsky e seus colaboradores , e com o projeto internacional sobre ensino e aprendizagem de Matemática no Ensino Universitário, o projeto *RUMEC* (*Research in Undergraduate Mathematics Education Community*).

A influência destas pesquisas nesta área é tão forte que Findell (2001) as categoriza em duas: as que estão ligadas a Dubinsky e as que não estão.

Um dos primeiros artigos, considerado o marco inicial, é o de Dubinsky et al. (1994). O objetivo desta pesquisa era entender a natureza do conhecimento sobre Teoria de Grupo e como um indivíduo pode desenvolver uma compreensão de vários tópicos desse domínio, e verificar se é possível mapear a decomposição genética destes tópicos, isto é, fazer uma descrição das construções mentais específicas que uma pessoa deve desenvolver para o entendimento de um conceito. Apresenta, também, uma breve discussão sobre as estratégias pedagógicas para o ensino destes tópicos.

A perspectiva teórica utilizada é uma aproximação construtivista baseada nas ideias de Piaget, de abstração reflexionante (Dubinsky, 1991). A partir dessa perspectiva ele tenta analisar as construções mentais que podem intervir no processo de desequilibração/reequilibração que acontecem quando um indivíduo é posto em uma situação (ou um problema) que exige a construção de esquemas mais sofisticados do que ele tem disponível no momento. Estas construções foram categorizadas em quatro tipos: *actions, processes, objects, schemas* (ações, processos, objetos e esquemas), a chamada teoria *APOS*.

São analisadas a compreensão dos tópicos grupo, subgrupo, classe e normalidade e grupo quociente. Os autores concluíram que, aparentemente, o encapsulamento de dois objetos, um conjunto e uma função (operação binária), coordenados em par, pode ser o primeiro entendimento real de um grupo pelo estudante, ou seja, a partir do momento que o estudante combina estes dois conceitos, ele começa a entender o que é um grupo. Os pesquisadores perceberam, também, que o entendimento de grupo e de subgrupo, em geral, se dá ao mesmo tempo. A descrição dos autores para a

aprendizagem de classe lateral (coset), de acordo com a teoria *APOS*, é a seguinte:

1. Formação de classes como uma ação: A formação de classes como uma ação é possível somente em situações familiares e onde fórmulas explícitas estão disponíveis.

2. Formação de classes como um processo: a formação de uma classe como processo acontece quando o estudante é capaz de aplicar em várias situações, fazendo cálculos. Ele pode não apenas construir uma classe aH, sendo H um subgrupo do grupo G, mas todas as outras, para todo $a \in G$, usando como critério de parada a repetição dos elementos.

3. Formação de classe como objeto: A formação de classe como objeto se dá quando o estudante for capaz de escrever e operar com os representantes das classes.

Dubinsky e seus colaboradores (1994) observaram que encapsular o processo de formação de classes em objeto é muito difícil. Eles acreditam, ainda, que as dificuldades no entendimento da Teoria de Grupos começam quando os conceitos relacionados ao Teorema de Lagrange e grupo quociente, ou seja, classes laterais, operações entre classes e normalidade são apresentados aos estudantes.

Segundo Asiala et al. (1997), o conceito de grupo quociente é uma coordenação de três esquemas: classe, operação e grupo. Esta coordenação consiste em selecionar construções específicas destes esquemas e aplicar à situação quociente. A perda da propriedade comutativa é uma dificuldade para os estudantes que, em geral, não conseguiram responder as questões relativas ao grupo D_3 (grupo de todas as simetrias de um triângulo equilátero com a operação de composição).

Nos trabalhos vinculados a este projeto, é utilizada, também, uma estratégia pedagógica menos tradicional, a *ACE-teaching cycle (Activities, Class discussion, and Exercises)*. O principal atrativo deste método é que se pode ter acesso à construção das ideias matemáticas dos estudantes, por meio da realização de atividades feitas no computador, usando a linguagem de programação *ISETL (Interactive SET Language)*. O trabalho é feito em grupos de aprendizagem cooperativos e discute-se os resultados das atividades no computador.

Os objetivos da pesquisa, desenvolvida por Asiala et al. (1997), foram: a) determinar o quanto a perspectiva teórica *APOS* é útil para a compreensão das cons-

truções mentais feitas pelos estudantes que aprendem sobre os tópicos estudados; b) aumentar a compreensão de como a aprendizagem sobre estes tópicos pode acontecer e aplicar esta compreensão para o ensino; c) avaliar como o tratamento instrutivo utilizado, conduz os estudantes a executarem com sucesso as tarefas matemáticas que requerem uma compreensão destes conceitos; d) desenvolver uma base de informações que lance luz sobre a epistemologia e a pedagogia associadas com estes assuntos.

As conclusões da pesquisa realizada por Asiala et al. (1997) reforçam a análise epistemológica feita por Dubinsky et al. (1994). O tratamento instrucional, ou seja, a estratégia pedagógica adotada parece ajudar os estudantes a fazerem uma construção satisfatória dos conceitos analisados, embora os autores avaliem que algumas atividades devam ser consideradas em outras disciplinas, como, por exemplo, atividades que incluam subconjuntos de S_n (grupo das Permutações do conjunto S), ou seja, atividades que incluam grupos não comutativos e atividades que envolvam todos os componentes da construção de um grupo quociente.

De um modo geral, estes trabalhos trazem resultados sobre como o estudante pode entender conceitos de Teoria de Grupos, de forma que se pode pelas respostas dos estudantes, perceber se eles estão entendendo uma classe como uma ação ou objeto, por exemplo, e propor atividades ou situações de ensino para ajudá-los a alcançarem o esquema sobre o conceito estudado. Certamente, não se pode tomar os resultados destes estudos como verdades absolutas. O processo de aprendizagem não é o mesmo para todas as pessoas, o que eles descreveram foi uma forma aproximada de como aquele grupo de pessoas respondeu a determinadas questões. Mesmo assim, estes resultados parecem interessantes, pois possibilitam ampliar a forma como podemos interpretar determinadas respostas dos estudantes da presente pesquisa. Por exemplo, quando um estudante, ao trabalhar com vários representantes das classes, não apenas com os canônicos, entende a classe como objeto.

Em sua tese de doutorado, Findell (2001), por meio de um estudo exploratório, busca identificar as características e componentes do conceito imagem (Tall e Vinner, 1981) dos estudantes que se destacam quando eles estão aprendendo as noções de teoria de grupo, como grupo, subgrupo, isomorfismo, classe e grupo quociente. Ao mesmo tempo, considerando a dialética processo objeto desses conceitos, Findell observou em seu estudo que, conceber classes como objetos, ou seja, encapsular o processo de construção das classes em objeto, não foi muito problemático, como sugere Dubinsky et al.

(1994).

As pesquisas desenvolvidas por Dubinsky et al. (1994) e Asiala et al. (1997) ajudaram a compreender outros textos, como, por exemplo, Leron, Hazzan e Zazkis (1995), Findell (2001), Lajoie (2000). Também, os resultados encontrados por eles contribuíram para a construção dos questionários.

Os trabalhos prioritários para fundamentar esta pesquisa foram os trabalhos de Lajoie (2000) e Lajoie e Mura (2004), como foi dito anteriormente no capítulo 1. Nestes trabalhos, as autoras identificam as dificuldades ligadas à aprendizagem de conceitos de Teoria de Grupos.

Em ambos, o termo dificuldade é utilizado, tomando os dois pontos de vista mais correntes na literatura como complementares. Para elas, uma dificuldade pode estar ligada a características intrínsecas, inerente a uma noção ou à complexidade e sutileza de uma tarefa, e ao aspecto subjetivo. Elas não se preocuparam em estabelecer uma demarcação entre estes dois pontos de vista por considerarem impossível determinar, com certeza, a causa de uma dificuldade, como já foi dito na seção 1.2.

Em sua tese de doutorado, Lajoie (2000), identifica quatorze (14) dificuldades ligadas à aprendizagem das noções de grupo, subgrupo, grupo ciclico e isomorfismo. Para exemplificar, apresentamos uma para cada uma das noções:

1. Dificuldade de discernir as propriedades essenciais de um grupo. Os estudantes não verificaram todos os axiomas que deteminam se um conjunto com uma operação é ou não um grupo.

2. Dificuldade de mostrar (formalmente) que dois grupos são isomorfos. Os estudantes não conseguiram escrever a função que determina o isomorfismo, ou apenas se detinham na cardinalidade do conjunto para dizer que dois grupos são isomorfos.

3. Dificuldade para construir um subgrupo de um grupo infinito. Os estudantes encontraram como subgrupo de um grupo infinito $G =< a >$, conjuntos munidos com a operação de G, mas que não eram subgrupos, como o conjunto $\{a^u | u \in \mathbb{N}\}$.

4. Dificuldade para considerar que um grupo infinito possa ser cíclico. Os estudantes se apegaram ao significado comum do termo cíclico, não se atentando para a definição de um grupo cíclico.

Embora, a autora utilize o termo dificuldade, é possível reconhecer neste trabalho alguns traços da noção de obstáculo didático de origem epistemológica, idealizado por Brousseau (1983), pois, além de identificar as dificuldades dos alunos ela, tenta utilizar a história para apoiar suas interpretações.

Já em Lajoie e Mura (2004), as autoras identificaram três dificuldades ligadas à aprendizagem de subgrupo normal e grupo quociente.

Elas buscam na análise das respostas identificar o conceito imagem e o conceito definição (Tall e Vinner, 1981), que estes estudantes manifestam sobre as noções de subgrupo normal e grupo quociente. Para elas, o conceito imagem não se refere unicamente à visualização de um conceito, mas toda a interpretação subjetiva que uma pessoa faz de um determinado conceito. Nele estão presentes as ideias, os exemplos, as imagens, as concepções, as definições pessoais, ou conceito definição pessoal, que são as palavras usadas para especificar o conceito. Esta definição pessoal do estudante pode ter partes que não são coerentes entre si e pode ser diferente da definição formal do conceito. Umas das explicações que elas têm para as dificuldades identificadas é a fragilidade das definições pessoais, ou seja, quando as definições pessoais são diferentes ou mesmo contraditórias com as definições formais do conceito, como, por exemplo, ter a definição de subgrupo normal como se fosse a comutatividade dos elementos do subgrupo.

O modelo de compreensão em Matemática, que as autoras utilizam, é o de Hiebert e Carpenter (1992), segundo o qual a compreensão de uma noção matemática pode ser concebida em termos das ligações que se criam, em particular entre as diversas representações internas que o indivíduo integra à estrutura cognitiva associada a esta noção. Se estas ligações não forem feitas ou forem mal feitas, isto pode levar os estudantes a cometerem erros ao trabalharem com as noções que estão em jogo. Para as autoras, estas duas teorias (Tall e Vinner, 1981; Hiebert e Carpenter, 1992) se completam e assim, por exemplo, elas explicam as dificuldades sobre grupo quociente pela presença no conceito imagem de componentes incompletas ou conflitantes, pela falta de ligações entre certas componentes do conceito imagem.

A pesquisa relatada foi realizada em dois momentos. Em um primeiro momento foram feitas entrevistas individuais, em que as autoras identificaram três dificuldades:

1. reconhecer a definição de subgrupo normal;

2. entender a natureza dos elementos e a operação de um grupo quociente;

3. reconhecer o papel do subgrupo normal na construção de um grupo quociente.

Estas dificuldades foram analisadas e elas consideraram que as mesmas ocorreram devido às seguintes hipóteses:

1. Fragilidade das definições pessoais.

   As pessoas haviam se esquecido desses conceitos, principalmente da definição de subgrupo normal. De acordo com as autoras, isto se deve provavelmente porque elas não fizeram as relações entre estes conceitos e outros cursos, ou porque não entenderam verdadeiramente estes conceitos. Para lembrar-se das definições formais, os estudantes recorriam a exemplos familiares ou, ainda, às impressões visuais das notações utilizadas. Isso pôde ser notado na definição de subgrupo normal quando os estudantes escreveram $NG = GN$ ou $Gn = nG$, ao invés de $Ng = gN$. Dessa forma, as definições pessoais enunciadas durante as entrevistas não eram equivalentes às definições formais.

2. Falha nas noções básicas da teoria de conjuntos.

   As autoras afirmam que, apesar de não ter na entrevista questões relacionadas diretamente com a Teoria de Conjuntos, elas conseguiram identificar algumas dificuldades em relação a este tópico, como, por exemplo, algumas pessoas parecem não entender que uma partição A de um grupo G contém o elemento neutro de G; que AB contém B, ou seja, que o produto de quaisquer dois subgrupos de G contém os dois subgrupos de G; e que o produto de um grupo G por qualquer um dos seus subgrupos, é igual a G. Outra dificuldade identificada é a confusão entre as relações pertinência e inclusão.

No segundo momento, foi aplicado um questionário para confirmar ou não as dificuldades encontradas na análise das entrevistas. Este questionário foi elaborado de acordo com as dificuldades e com as hipóteses levantadas anteriormente e foi aplicado para 24 pessoas que já tinham feito um primeiro curso de Álgebra Abstrata, das universidades de Quebec e Montreal.

As análises desse questionário apontaram que os alunos têm dificuldades em:

1. reconhecer a definição de um subgrupo normal: uma dificuldade confirmada;

2. saber a natureza dos elementos e da operação de um grupo quociente: uma dificuldade realçada pela análise dos questionários;

3. reconhecer o papel de um subgrupo normal na construção de um grupo quociente: uma dificuldade realçada na análise do questionário.

A interpretação das dificuldades encontradas na análise das entrevistas e questionários escritos foi realizada pelas autoras à luz do quadro teórico proposto por Tall e Vinner (1981), conceito imagem e conceito definição, e Hiebert e Carpenter (1992), utilizando ainda a análise conceitual de subgrupo normal e grupo quociente e os resultados de pesquisas em Didática da Matemática.

As interpretações das dificuldades relatadas por Lajoie e Mura (2004) foram:

1. Reconhecer a definição de um subgrupo normal: um perigo de confusão criada pela proximidade com outras definições. As autoras apontam o perigo de confusão entre as definições de subgrupo normal, subgrupo comutativo e subgrupo central, causada principalmente pela semelhança das notações desses conceitos. Para os estudantes, o subgrupo normal lembra alguma coisa sobre comutatividade.

2. Entender a natureza dos elementos e da operação de um grupo quociente: uma tarefa difícil, mas que não se pode evitar. Para as autoras, as relações entre os conceitos de subgrupo normal e grupo quociente são falhas ou inexistentes para os alunos. Elas apontam que, para os estudantes, é difícil considerar simultaneamente um conjunto como um objeto e como uma coleção de objetos. Como, por exemplo, o caso em que "...um subgrupo normal N pode ser considerado como um subrupo de G, como um subconjunto contendo em particular o elemento neutro de G, e como ele mesmo sendo elemento neutro do grupo quociente G/N...". (LAJOIE e MURA, 2004, p. 69).

   Para as autoras, alguns fatores que podem contribuir para que esta dificuldade seja difícil de ser superada, entre outros, é o uso dos representantes para realizar as operações do grupo quociente, o que pode induzir a uma confusão sobre a natureza dos elementos e a operação de grupo quociente. Isso pode levar pessoas inexperientes a pensar que os representantes, que eles manipulam, são elementos do grupo quociente, e não classes de equivalência, e que a operação do grupo quociente seja a mesma do grupo de partida.

Uma conclusão a que elas chegaram, da análise das entrevistas, levou-as a entender que alguns estudantes não têm consciência de que os elementos de G/N formam uma partição de G, o que pode contribuir para a dificuldade de entender a natureza dos elementos e da operação do grupo quociente.

3. Reconhecer o papel de um subgrupo normal na construção de um grupo quociente: uma armadilha da compatibilidade da operação de um grupo com a partição produzida por um subgrupo. Os alunos tomam esta compatibilidade como adquirida, não sentem a necessidade de assegurar que a operação nas classes está bem definida. Eles recorrem aos representantes das classes para efetuar as operações com os elementos do conjunto quociente G/N, sem mesmo verificar se o subgrupo N é normal. As autoras justificam isso dizendo que os estudantes podem supor que a operação esteja bem definida, porque ela está intimamente ligada àquela do grupo de partida, ou por acreditarem que ela coincide com a operação do grupo de partida.

Apesar de as autoras procurarem explicar suas hipóteses à luz da teoria de conceito imagem e conceito definição (Tall e Vinner, 1981), muito do que foi dito em suas interpretações das dificuldades identificadas está ligado às dificuldades dos estudantes em Teoria de Conjuntos. Não somente com as relações pertinência e inclusão, mas também com as noções envolvidas na relação de congruência. Como no caso em que os estudantes não entendem a natureza dos elementos do grupo quociente, em que as autoras afirmam: "...nós acreditamos também que para eles é efetivamente difícil considerar o conjunto - uma classe - como um objeto, quer dizer, de considerá-lo como um elemento de um outro conjunto...". (LAJOIE e MURA, 2004 p. 68, tradução da autora).

Uma crítica que pode ser feita em relação ao trabalho de Lajoie e Mura é que não fica claro se as notações e definições utilizadas na entrevista e questionário, são as usadas pelos estudantes, pois se as notações, por exemplo, são diferentes, isso pode levar o estudante a cometer erros. Como na questão sobre a definição de subgrupo, que pode ser encontrada no Apêndice B, que parece mais uma questão sobre quantificadores, que pode induzir a erro pela semelhança de símbolos utilizados. Se o estudante não foi apresentado à definição de subgrupo normal daquela forma, dificilmente responderá corretamente à questão, já que não foi alertado pelo professor sobre as possíveis formas

de defini-lo. Esses cuidados foram tomados no desenvolvimento da presente pesquisa.

A metodologia utilizada nos trabalho de Lajoie (2000) e Lajoie e Mura (2004) para análise dos dados foi a *théorisation ancrée* elaborada por Paillé (1994), que é uma variação da *grounded theory*, teoria fundamentada nos dados (Glaser e Strauss, 1967, Strauss e Corbin, 1990, apud Lajoie, 2000). Segundo Lajoie (2000) a análise por esta teoria é um tipo de análise qualitativa empírica e dedutiva, que tem como objetivo gerar uma teoria sobre um fenômeno cultural, psicológico ou social.

Quanto à presente pesquisa, apenas farei a análise dos erros apresentados por estudantes ao responderem instrumentos elaborados a partir dos instrumentos utilizados por Lajoie e Mura (2004) prioritariamente e, alguns dos resultados dessa pesquisa e de Lajoie (2000).

Considero que os resultados destes estudos, embora tenham como objeto matemático a Teoria de Grupos, podem servir de base ao contexto matemático da presente pesquisa, uma vez que o anel quociente, assim como grupo quociente, pode ser definido como o conjunto das classes de equivalência, e, portanto, trata-se de uma partição de um anel. Além disso, o anel quociente $\mathbb{Z}_m$ é também um grupo aditivo.

3.1.2 Sobre dificuldades em conceber conjunto como um objeto

A partir dos resultados da pesquisa de Lajoie e Mura (2004), principalmente as explicações das dificuldades encontradas, ligadas à Teoria de Conjuntos, as pesquisadoras Traoré, Lajoie e Mura (2007) tematizaram a dificuldade de não conceber um conjunto como objeto distinto de seus elementos, ou seja, particularmente quando não se consegue, por exemplo, entender ou aceitar um conjunto como elemento de outro conjunto. Segundo as autoras, essa dificuldade levaria os estudantes a afirmarem que os elementos de um grupo quociente G/N são elementos do grupo G; a confundirem as relações $\in$ e $\subset$ e escreverem que $gN \in G$ ao invés de $gN \subset G$, sendo G um grupo e N um subgrupo normal de G.

Da análise das respostas de vinte e um (21) estudantes a uma questão de uma lista discutida em uma aula de resolução de exercícios, as autoras encontraram três tipos de erros matemáticos, que foram atribuídos à dificuldade de conceber um conjunto como objeto distinto de seus elementos. São eles:

1. T1: confusão entre as relações " pertencer a" e " inclusão" (ou entre os conceitos de elemento e subconjunto). Este erro consiste em trocar os sentidos destas duas relações.

2. T2: confusão entre a reunião (união) de conjuntos $A, B, C, ...$ e o conjunto onde os elementos são $A, B, C, ...$, isto é, $A \cup B \cup C \cup ... = \{A, B, C, ...\}$. Este erro ocorre quando o estudante assume, por exemplo, que o conjunto com dois elementos $\{\{x, y\}, \{a, b, c\}\}$ é igual ao conjunto $\{x, y, a, b, c\}$, ou seja $\{A, B\} = A \cup B$.

3. T3: adição ou supressão de chaves. As chaves têm como função reagrupar os elementos. Para os estudantes que cometem este tipo de erro, o papel das chaves não seria essencial e colocar ou tirá-las não mudaria fundamentalmente a natureza de um conjunto, que permaneceria sempre composto das mesmas partes.

Em seus resultados, elas destacam que uma das razões que levam à dificuldade encontrada é a de que os estudantes têm como concepção de conjunto um modelo primitivo, ou seja, o de uma coleção de objetos físicos.

Outros fatores também por elas identificados como podendo influenciar nestes erros foram: a interferência da linguagem corrente na linguagem matemática, como acontece com a relação de inclusão e de pertinência e a abordagem dada à Teoria de Conjuntos no curso, por exemplo, de que "tudo é conjunto", o que pode fazer desaparecer um marcador que não é muito usado em uma aproximação formal, a ideia de que "pertence" está ligado a um elemento de um conjunto, enquanto a "inclusão" está ligada a dois conjuntos.

As autoras também fazem uma ressalva, a de que alguns estudantes podem cometer um tipo de erro em um exercício e em outro não. Para elas, uma das principais conclusões que podem tirar deste estudo é o fato de que erros apresentados, que envolvem noções elementares de Teoria de Conjuntos, já haviam sido encontrados anteriormente no trabalho sobre conceitos de Álgebra Abstrata por Lajoie e Mura (2004), o que as levou a entender ser necessário manter a reflexão sobre as causas destes erros. Ainda, de acordo com as autoras, isso pode acontecer, entre outros fatores, porque as noções de Teoria de Conjuntos são ensinadas, em geral, de maneira informal no nível secundário, e são tidas como adquiridas na universidade, sem que seja feito um ensino sistemático delas. Outro argumento apresentado pelas autoras é que a própria noção de conjunto não é tão simples como se acredita, e que alguns estudos (Fischbein e Baltsan,

1999; Zazkis e Gunn, 1997, apud Traoré, Lajoie e Mura (2007)), sugerem que se trata de uma noção difícil.

3.1.3 Sobre congruência de inteiros

As pesquisas em Teoria de Números são, em sua maioria, sobre as noções básicas como divisibilidade, máximo divisor comum e mínimo múltiplo comum, como pode ser visto nos livros de Zazkis e Campbell (2006, 2002). Os textos encontrados sobre congruência módulo m ou a aritmética modular foram os de Findell (2001) e Smith (2006).

Em Smith (2006), a autora tem como objetivo identificar as concepções dos estudantes sobre a congruência módulo m. Ela fez entrevistas com seis estudantes da disciplina de introdução a Álgebra e Teoria de Números, de uma universidade dos Estados Unidos. A participação da pesquisadora foi de observadora participante e como professora assistente, durante as aulas desssa disciplina.

O professor encarregado de ministrar a disciplina fez uma abordagem de congruência de inteiros, utilizando os conhecimentos dos estudantes sobre divisibilidade para chegar que dois inteiros são congruentes módulo n se deixam o mesmo resto na divisão por n, para, depois, apresentar a definição de congruência como encontrada em geral nos livros, ou seja, $a \equiv b \pmod{n}$ se e somente se $n|a-b$. Ele queria, com esta abordagem, que a noção de congruência fizesse sentido para os estudantes, e não que eles simplesmente aceitassem esta definição, porque ela é apresentada dessa forma.

De acordo com a forma como os estudantes se referiam a congruência módulo m e trabalhavam com ela, a autora definiu duas categorias de interpretação da congruência de inteiros: a relacional e a operacional. Segundo ela, os argumentos utilizados pelos estudantes se apresentam, para cada categoria, da seguinte forma (Smith, 2006):

1. Argumentos que revelam uma visão operacional do estudante da congruência módulo m:

   - Interpreta a congruência frequentemente, se não exclusivamente, com a afirmação do tipo a/n deixa resto b.
   - Reduz o lado direito de uma congruência como uma exigência para que a congruência seja verdadeira, deixando o lado direito sempre menor que n.

- Vê a congruência como uma transformação de $\mathbb{Z}$ para o " (mod n) *world*". Este termo foi utilizado pelo professor da disciplina analisada pela autora, como uma forma intuitiva de se referir ao anel $\mathbb{Z}_n$, o conjunto das classes de congruência módulo n.
- Vê o termo mod n como se fosse parte do número inteiro. Como, por exemplo, escrevendo 3 (mod 7) $\equiv x$, ou substituindo (mod n) por $+nk$ nas equações.

2. Argumentos que revelam uma visão relacional do estudante da congruência módulo m:

   - Interpreta a congruência de várias formas, mas a divisão é sempre vista como a e b, deixando o mesmo resto na divisão por n.
   - Reduz o lado direito da congruência como um problema de convenção ou como uma estratégia para resolver um problema.
   - Vê a congruência formalmente ou informalmente como uma relação de equivalência definida em $\mathbb{Z}$, de modo que as quantidades de ambos os lados da congruência são vistas como elementos de um mesmo conjunto, ou seja, da mesma classe de congruência.
   - Vê o termo mod n modificando toda a congruência, não apenas um dos inteiros.

Assim, se o estudante tem a tendência a pensar sobre congruência módulo m em termos de um processo que transforma um inteiro em outro, adicionando ou subtraindo múltiplos de m, ou quando não consegue ver a e b na mesma classe de congruência, este estudante tem a visão operacional da congruência de inteiros. No entanto, se o estudante trabalha com o símbolo $\equiv$ indicando que duas quantidades são consideradas as mesmas, ou seja, vê a e b na mesma classe de congruência, ou que na divisão pelo módulo ambos os números deixam o mesmo resto, ou que a diferença entre qualquer dois inteiros congruentes é múltiplo do módulo; então, estes estudantes têm uma visão relacional da congruência de inteiros.

Muitos estudantes participantes da pesquisa de Smith entendiam o número do lado esquerdo da congruência como um número inteiro ordinário, enquanto que o lado direito da congruênca era visto como um elemento do *"mod n world"*, ou como uma

classe de congruência ou como um número entre 0 e $n-1$. Argumentos que fornecem uma interpretação operacional da congruência módulo n.

A autora constatou que, na primeira entrevista, os estudantes entenderam a congruência como uma propriedade sobre divisões e restos, com o número da esquerda da congruência sendo o dividendo e o da direita o resto da divisão. Já na segunda entrevista, a maioria dos estudantes viu a congruência como uma transformação de números inteiros em números existentes, no *mod n world*. Na maioria dos casos, a congruência linear foi resolvida, colocando a variável do lado esquerdo da congruência, por exemplo, $3x \equiv 13 \pmod 7$, como se faz, geralmente, com a equação linear em Álgebra.

Os resultados obtidos das análises, dos questionários e das entrevistas, revelaram que os estudantes tendem a ver a relação de congruência operacionalmente, ao invés de relacionalmente, e que os participantes demonstraram uma tendência a resolver congruências lineares usando um complicado processo memorizado, ao invés de utilizar as propriedades da relação de congruência e a estrutura algébrica encontrada no anel finito dos inteiros, $\mathbb{Z}_n$, em que a congruência existe. A autora compara estes resultados aos encontrados em pesquisa (Kieran, 1981, apud, Smith, 2006) sobre como as crianças veem o sinal de igualdade e sobre as dificuldades delas em resolver equações lineares em álgebra.

Em suas reflexões sobre os resultados encontrados, a autora apresenta que uma dificuldade conceitual inerente à aprendizagem de congruência é o fato de que os números indicados em uma congruência podem representar diferentes objetos matemáticos. Por um lado, pode-se pensar em congruência, explicitamente como relação de equivalência definida em $\mathbb{Z}$ e, então, tem-se uma infinidade de números inteiros que podem ser substituídos em ambos os lados da congruência, que seriam os representantes de uma mesma classe de equivalência. Por outro, pode-se pensar também na congruência como uma equação em $\mathbb{Z}/n\mathbb{Z}$, e olhar as classes de equivalência como objetos a serem manipulados. Outra possível interpretação é a de pensar no conjunto $\{0, 1, 2, 3, ..., n-1\}$, como um anel finito de inteiros, com adição e multiplicação definidos módulo n.

Assim, de acordo com estas três formas de pensar a congruência módulo m, tem-se soluções diferentes para uma congruência linear, por exemplo, para a equação $5x \equiv 1 \pmod{11}$, as soluções são as seguintes: i) infinitas soluções da forma $9 + 11k$,

para $k \in \mathbb{Z}$, se pensarmos em congruência explicitamente como relação de equivalência definida em $\mathbb{Z}$; ii) uma única solução, a classe denotada por 9, congruência como uma equação em $\mathbb{Z}/n\mathbb{Z}$; iii) uma única solução, o inteiro 9, se pensarmos no conjunto $\{0, 1, 2, 3, ..., n-1\}$, como um anel finito de inteiros, com adição e multiplicação definidos módulo n.

Smith afirma ainda que, para os matemáticos, estas perspectivas não causam dificuldades e muitos não aceitam que existam estas formas de pensar a congruência modulo m. Porém para o estudante que está iniciando seus estudos sobre este conceito, a distinção entre estas três perspectivas não é simples, ela é real e confusa.

Um resultado parecido foi observado por Findell (2001) sobre a utilização do termo $\bmod n$. Ele notou que os estudantes utilizavam este símbolo como uma operação binária entre inteiros, como resto da divisão de um inteiro por m, e como um modificador de uma relação de equivalência, o que poderia causar ambiguidades na afirmação, por exemplo, $15 \equiv 7 \bmod 4$, que é verdadeira para a relação de congruência módulo 4, pois $4|15-7$, mas não é verdadeira se considerarmos $\bmod$ como operação binária, pois o resto da divisão de 15 por 4, não é igual a 7. Estas duas formas também podem ser vistas como relacional e operacional, respectivamente.

É a partir do referencial teórico até aqui apresentado que os dados da presente pesquisa serão analisados, juntamente com a análise conceitual feita no Capítulo anterior.

Capítulo 4

Procedimentos metodológicos

Para alcançar o objetivo desta pesquisa, que é identificar e analisar as dificuldades dos estudantes, do curso de Matemática da UFPR, ao responderem questões sobre congruência algébrica no contexto da Teoria de Números e Teoria de Anéis, a metodologia de pesquisa escolhida foi a análise das respostas dos estudantes a questões sobre congruência módulo m e sobre o anel quociente $\mathbb{Z}_m$.

Diferentemente de Lajoie e Mura (2004), que utilizaram como metodologia uma variação da teoria fundamentada nos dados, optei por usar a análise das respostas dos estudantes, por entender que os resultados apresentados por elas e por outros pesquisadores, como os das pesquisas apresentadas no Capítulo anterior, poderiam ser utilizados nas análises destas respostas, já que os temas destas pesquisas são semelhantes aos meus.

Neste capítulo serão detalhados os procedimentos metodológicos adotados.

4.1 Sujeitos e procedimentos de coleta de dados

Os estudantes participantes desta pesquisa são estudantes voluntários do Curso de Matemática, matriculados na disciplina Teoria de Anéis ou Álgebra A, do período noturno, e são, em sua maioria, do curso de Licenciatura. Como o curso de Matemática da Universidade Federal do Paraná estava passando pelo período de mudança curricular, os estudantes que estavam matriculados na disciplina Álgebra A cursaram as disciplinas Teoria de Números e Teoria de Anéis, formando uma única turma com setenta e um (71) alunos matriculados em uma ou outra disciplina. Dessa forma, os conteúdos matemáticos vistos por estes estudantes são os relacionados nas ementas

destas disciplinas, veja Apêndice A, e eles ainda não tinham estudado Teoria de Grupos.

Embora a maioria dos estudantes fosse estudantes de Licenciatura, por se tratar do período noturno, não houve a necessidade de diferenciar estes dos alunos do Bacharelado, pois estas disciplinas são as mesmas e o conteúdo matemático foi apresentado da mesma forma para as duas modalidades. Não estou com isso dizendo que esta seja a melhor forma de tratar estes tópicos, ou que seja necessário fazer distinção da forma como estes conteúdos devem ser apresentados para a Licenciatura e para o Bacharelado, este é apenas o cenário em que a pesquisa se desenvolveu.

O primeiro questionário foi aplicado no dia 14 de agosto de 2007; começou às 20h e terminou por volta de 21h, durante a aula da disciplina Teoria de Anéis. Quarenta e um (41) estudantes se dispuseram a responder ao questionário, sendo que quinze (15) deles identificaram-se como alunos de Álgebra A, foram nomeados por A1, A2,..., A15; quatro (4) como alunos de Teoria de Anéis, e foram identificados por T1, T2,..., T4; e vinte e dois (22) não identificaram em qual disciplina estavam matriculados e foram nomeados por S1, S2... S22. Este questionário foi aplicado no início do primeiro semestre, antes que fosse apresentado aos estudantes o anel quociente. Estes estudantes tinham cursado a disciplina de Teoria de Números no semestre anterior, em que a noção congruência módulo m foi estudada.

O segundo questionário foi aplicado no dia 13 de novembro de 2007, durante a aula da disciplina Teoria de Anéis, a mesma do questionário anterior, começou às 20h15 e terminou às 21h e foi aplicado depois da avaliação sobre anel quociente. Vinte e oito (28) estudantes matriculados na disciplina Teoria de Anéis ou Álgebra A se dispuseram a responder ao questionário. Destes, dez (10) disseram ter respondido ao questionário anterior sobre congruências e foram identificados como Q1, Q2,..., Q10, os outros dezoito (18) estudantes, que não escreveram esta informação, foram identificados por N1, N2,..., N18.

As entrevistas foram feitas no final do primeiro semestre de 2008, com três alunos voluntários, identificados por E1, E2 e E3 que estavam cursando a disciplina Teoria de Grupos, do período diurno[1]. A escolha por esta turma se deu porque os estudantes que responderam aos questionários não estavam cursando disciplinas de Teoria de Grupos que, para o período noturno, seria ofertada no primeiro semestre

[1] Devido ter sido voluntária a identificação dos estudantes aos questionários, poucos foram os que fizeram isso, não sendo possível contatá-los para entrevistas

de 2009. Outro motivo desta escolha é que estes alunos já teriam cursado as disciplinas que tratam de Álgebra Abstrata do curso de Matemática e, assim, teriam mais experiência em trabalhar com estes conceitos, e se acreditava que as respostas poderiam ser diferentes das dos questionários, com argumentações mais precisas matematicamente. Também levou-se em conta que seria interessante observar o que estes estudantes diriam sobre os argumentos utilizados pelos estudantes que responderam aos questionários em suas respostas. As entrevistas foram audiogravadas e transcritas posteriormente.

4.2 Instrumentos de coleta de dados

Para coleta de dados foram aplicados dois questionários (quarenta e um (41) responderam ao primeiro e vinte e oito (28) ao segundo) e foram realizadas entrevistas individuais com três (3) estudantes.

O primeiro questionário foi elaborado com o objetivo de se obter e analisar respostas dos estudantes em questões sobre congruência módulo m. Da mesma forma, o segundo questionário foi elaborado com o objetivo de se obter e analisar respostas dos estudantes em questões sobre anel quociente $\mathbb{Z}_n$, sua construção e suas propriedades. A escolha de questionários como instrumento para a coleta de dados foi, principalmente, pela facilidade de aplicação e pelo número de pessoas que poderiam ser envolvidas na pesquisa.

Para apoiar ou refutar os resultados encontrados nas análises preliminares das respostas aos questionários, realizei três entrevistas individuais, semiestruturadas. Nessas entrevistas, primeiro solicitei ao estudante entrevistado que respondesse a um questionário, veja Apêndice D, pedi a seguir para que ele explicasse suas respostas e, conforme as explicações, perguntei-lhe sobre algum detalhe, procedimento ou conceito envolvido na mesma. Na transcrição das entrevistas, o que está escrito entre colchetes [ ] são comentários que esclarecem sobre o que está se falando e nos diálogos a letra P identifica o pesquisador.

4.2.1 Elaboração dos instrumentos de coleta de dados

A ideia inicial para a elaboração das questões para estes questionários, foi o questionário elaborado por Lajoie e Mura (2004) e os resultados por elas encontrados.

Em um primeiro estudo exploratório, apliquei aos estudantes do Curso de Matemática o mesmo questionário aplicado aos estudantes do Canadá pelas pesquisadoras Lajoie e Mura (2004), com o objetivo de verificar se as dificuldades identificadas por elas poderiam ser reconhecidas pelas respostas dos estudantes do curso de Matemática da UFPR, veja Apêndice B.

Na análise das respostas, identifiquei as mesmas dificuldades que elas, e destaquei as dificuldades em relação aos conceitos ligados à congruência, como partição de um conjunto e classe de equivalência. Observei que alguns aspectos do questionário elaborado por Lajoie e Mura (2004) podem ter levado os estudantes a se confundirem, como, por exemplo, na questão sobre a definição de subgrupo normal, devido à quantidade de símbolos e definições muito parecidas em uma questão de múltipla escolha. Neste caso, talvez uma questão discursiva com um enunciado objetivo, tal como, *defina (ou descreva) subgrupo normal*, fosse mais indicado.

Este primeiro estudo exploratório que realizei com os estudantes, replicando o mesmo instrumento de coleta de dados da pesquisa de Lajoie e Mura(2004), foi uma experiência importante para a minha pesquisa, pois me ajudou na elaboração dos instrumentos de coleta de dados e na condução da sua aplicação.

Para elaborar os questionários aplicados aos estudantes, além da pesquisa de Lajoie e Mura (2004), foram levados em conta os livros textos utilizados pelo professor da disciplina, as notas de aulas, e, principalmente, as conversas informais com o referido professor, ocasião em que ele relatava as dúvidas dos estudantes, o andamento da disciplina, a notação e abordagem utilizadas em aula. Além disso, antes de cada aplicação dos questionários, as questões elaboradas foram discutidas com o professor, para que não houvesse distorções sobre o que se pedia e o que os estudantes haviam aprendido. A exceção foi a questão 4 do primeiro questionário, em que optei por deixar - mesmo sendo alertada pelo professor de que os seus alunos não tinham estudado ainda a construção do conjunto quociente $\mathbb{Z}_m$ - para verificar se era possível que eles a respondessem utilizando conhecimentos prévios sobre Teoria de Conjuntos, por supor que eles já tivessem aprendido esse conteúdo.

O primeiro questionário elaborado teve questões relativas à congruência módulo m e ao conjunto quociente $\mathbb{Z}_m$.

Neste questionário, um dos objetivos gerais era identificar o quê e como os estudantes aprenderam a noção de congruência, por isso uma das questões pedia para que eles explicassem o que é a congruência módulo m a um colega do curso. A opção por este tipo de pergunta foi por acreditar que, para explicar algo para outra pessoa, é necessário mobilizar mais aspectos de um conceito do que somente a definição formal.

Para identificar como eles lidam com as propriedades de congruência, questões em que deveriam utilizá-las para resolvê-las, foram colocadas. Estas questões poderiam ser resolvidas utilizando não apenas a congruência, mas também a aritmética. Esta escolha foi proposital, para identificar qual a estratégia utilizada, e se os estudantes preferem utilizar recursos mais ou menos elaborados para resolver a questão.

O segundo questionário foi elaborado com questões sobre anel quociente, seus elementos e suas propriedades; o anel utilizado para estas questões foi o anel quociente $\mathbb{Z}_m$. Questões que visavam identificar se e como os estudantes conseguiam construir e reconhecer a natureza dos elementos do anel quociente, foram colocadas. Nele, algumas questões elaboradas por Lajoie e Mura (2004) foram adaptadas, principalmente para o contexto da Teoria de Anéis, como, por exemplo, a questão:

" Os elementos de G/N podem ser elementos de G? Justifique sua resposta." (LAJOIE e MURA, 2004, p. 61, tradução da autora).

Já no questionário aplicado na presente pesquisa, tornou-se:

Os elementos de $\mathbb{Z}/3\mathbb{Z}$ podem ser elementos de $\mathbb{Z}$? Justifique sua resposta.

Esta questão teve como objetivo identificar se os estudantes reconhecem a diferença da natureza dos elementos dos conjuntos e, se não for este o caso, conhecer as razões.

As questões utilizadas para as entrevistas foram elaboradas levando em conta os erros, as justificativas e o raciocínio, que apareceram nas respostas dos questionários anteriores. Como, por exemplo, a questão:

Você concorda com algum destes argumentos? Justifique sua resposta. Se não concorda, justifique também.

i) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ são elementos de $\mathbb{Z}$, pois $\mathbb{Z}/5\mathbb{Z}$ são múltiplos de 5, e, portanto, são números inteiros.

ii) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ não são elementos de $\mathbb{Z}$, porque eles são do tipo $\frac{n}{5}$

e, portanto, pertencem a $\mathbb{Q}$.

iii) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ *não são elementos de* $\mathbb{Z}$*, porque eles são classes de equivalência e não números inteiros.*

Se você não concorda com nenhum desses argumentos, como você responderia a questão: elementos de $\mathbb{Z}/5\mathbb{Z}$ *podem ser elementos de* $\mathbb{Z}$*?*

Depois da primeira entrevista realizada, foi necessário um ajuste no questionário, pois não foi possível verificar se o estudante entrevistado conhecia partição de um conjunto. Portanto, a questão de número três foi modificada, ficando com o seguinte enunciado:

Seja $\{S_1, S_2, ..., S_n\}$ *uma partição de um conjunto* E *e seja* x *um elemento de* E*. Podemos afirmar que* $x \in \{S_1, S_2, ..., S_n\}$*? Justifique sua resposta.*

Sendo $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$*, podemos afirmar que:*

a) $10 \in \mathbb{Z}_7$*;*

b)$\overline{10} \in \mathbb{Z}_7$.

Colocar explicitamente a questão sobre partição deu mais ênfase a esta noção e foi possível, na análise, verificar o que os estudantes entendem sobre ela. Este questionário pode ser encontrado no Apêndice D.

4.3 Organização, análise e interpretação dos dados

Para organizar e analisar os dados, tomei a forma de apresentação da análise de erros, nos trabalhos de Cury,(2006, 2007).

Como foi visto no Capítulo 1, os erros cometidos pelos estudantes deixaram de ser vistos apenas como um equívoco do aluno ou falta de atenção ao resolver um problema, uma vez que os erros podem ser considerados como indicadores dos processos cognitivos na aprendizagem da Matemática na sala de aula e que podem ser analisados e investigados.

Para organizar os dados, as questões foram analisadas separadamente. No canto de folha de resposta, foi colocada uma sigla que identificava em qual classe a resposta de uma determinada questão estava. Por exemplo, se o estudante não respondesse a quarta questão, teria no canto superior direito de sua folha de resposta a sigla 4-NF, ou se na resposta à questão 1 aparecesse um argumento utilizando a definição de congruência, seria colocada a sigla 1-DC. Dessa forma, considerei ser mais

fácil localizar a resposta de alguma questão caso fosse necessário.

A forma de classificação e de análise das respostas foi baseada em Cury (2007). As respostas de cada questão foram classificadas em A, B, C, e assim por diante, de acordo com as justificativas ou erros cometidos pelos estudantes. Em cada classe foi feita uma descrição detalhada dos tipos de respostas e, a seguir, realizada uma análise visando ao objetivo de cada questão.

Para esta pesquisa estou considerando que uma dificuldade pode ser traduzida pela incapacidade de tratar de forma eficaz ou de dar sentido a certos problemas, ou seja, pode ser observada pelas respostas incorretas dadas pelos estudantes. O termo dificuldade foi utilizado nesta pesquisa, da mesma forma como foi utilizado por Lajoie e Mura (2004), como foi apresentado na seção 1.3 do Capítulo 1 e que pode ser percebida pelos erros cometidos por várias pessoas.

As entrevistas foram utilizadas para reforçar ou refutar estas dificuldades.

A interpretação dos resultados foi feita levando em conta a revisão de literatura a respeito de pesquisas sobre ensino e aprendizagem em Teoria de Grupos e Teoria de Números, como, por exemplo, Lajoie (2000), Lajoie e Mura (2004), Dubinsky et al. (1994), Findell (2001), Smith (2006) e os conteúdos matemáticos envolvidos. As explicações para essas dificuldades estão focadas no aspecto mais objetivo do termo dificuldade, visando estabelecer a falta, ou falha, no conteúdo matemático necessário para a resolução das questões propostas.

Capítulo 5

Análise e discussão dos resultados

Neste capítulo, será apresentada a classificação e a análise das respostas dos estudantes ao questionário sobre congruência módulo m e anel quociente $\mathbb{Z}_m$. As respostas foram agrupadas e classificadas, pela semelhança dos argumentos utilizados, por meio dos quais foram identificados os erros na aprendizagem desta congruência.

5.1 Das questões sobre congruência módulo m

A análise apresentada nessa seção tem como objetivo responder à seguinte questão, referente ao primeiro objetivo específico desta pesquisa, apresentado na seção 1.4:

Quais as dificuldades encontradas pelos estudantes ao responderem questões sobre congruência módulo m e sobre o conjunto das classes de congruência módulo m?

5.1.1 Classificação e primeira análise das respostas dos estudantes

Nesta seção, será apresentada uma descrição detalhada das respostas dos estudantes a cada questão e algumas considerações sobre as mesmas, de acordo com o objetivo de cada uma delas. Para as análises destas questões, para considerá-las corretas ou não, foram levados em conta o que foi ensinado em sala de aula, utilizando as notações e as definições dadas pelo professor e pelo livro texto utilizado. Não se está com isso afirmando que estas sejam mais adequadas ou não, este é apenas o cenário em que os dados foram colhidos.

Questão 1

Como você explicaria, para um aluno do primeiro ano do Curso de Matemática, o que é a congruência módulo m? Justifique sua resposta.

O objetivo desta questão era identificar o que o aluno entende por congruência módulo m.

Para esta questão não existia uma resposta correta, eles poderiam responder definindo a relação de congruência módulo m, ou utilizando a ideia de resto da divisão, ou mesmo utilizando um exemplo numérico em que a ideia do conceito fosse utilizada corretamente.

Dos quarenta e um (41) estudantes que responderam a este questionário, trinta e seis (36) deles responderam esta questão e cinco (5) (A14, S10, S12, S13, T3) deixaram de responder. As respostas foram agrupadas em cinco classes, de acordo com a definição utilizada. O quadro abaixo mostra um resumo das classes e dos tipos de respostas; para isso, considere $a, b, \in \mathbb{Z}$ e m um número inteiro fixo.

Classe	Subclasse	Estudantes	Tipo de resposta
A	A1	S2, S5, S16, S14, S18, S21, A6, A8, A11, A13, A15, T2	$a \equiv b \pmod{m} \Leftrightarrow m\|a-b$
	A2	S8, S20, A10, T4	$a \equiv b \pmod{m} \Leftrightarrow a-b=mk, k \in \mathbb{Z}$
	A3	S7, S11, S19, A12	as duas notações anteriores
B		S4, S6, T1, A4, A5	$a \equiv b \pmod{m} \Leftrightarrow a$ e b deixam o mesmo resto na divisão por m
C		S1, S9, S15, A7	$a \equiv b \pmod{m} \Leftrightarrow m\|a-b$ e a e b deixam o mesmo resto na divisão por m
D		S3, A3	base numérica
E		A1, A2, A9, S17, S22	incorreta ou incompleta

Quadro 5.1: Classes da questão 1

Classe A: Corresponde a vinte (20) respostas corretas, nas quais foram utilizadas a definição 3, Capítulo 2 sobre objeto matemático, da relação de congruência módulo m. Pode-se dividir esta classe em três subclasses.

Subclasse A1: Corresponde às respostas dadas, usando a notação de divisibilidade. Doze (12) estudantes responderam esta questão, utilizando a notação de divisibilidade, como no livro texto indicado pelo professor, Milies e Coelho(2003), mas escrevendo com suas próprias palavras, como, por exemplo, o estudante S5, que escreveu: "Explicaria que seria dois números $a, b, \in \mathbb{Z}$, que subtraídos são divididos por m sem deixar resto".

Outro aluno, A6, embora tenha escrito corretamente a definição, ao continuar o raciocínio de como explicaria para um colega, escreveu: "Mostraria que congruência é sinônimo de igualdade na divisão e que trabalha com os restos, facilitando a operação". Ele entende a ideia de trabalhar com restos da divisão, mas o que se tem é a igualdade de classes de congruência módulo m, não na divisão.

O estudante T2 respondeu: "Se escolher dois números a e b e se m dividir a diferença $a - b$ então a será congruente a b módulo m". Para justificar a escolha por esta definição, ele escreveu: "Por ser um aluno do primeiro ano, explicaria envolvendo conceitos que com certeza, esse aluno tem, como a divisão e diferença, creio que é a forma mais clara de enxergar a definição de congruência".

O estudante A8 apresenta a congruência como uma notação utilizada para um caso particular de divisibilidade, e escreve corretamente a definição, da seguinte forma: "Congruência módulo m está diretamente relacionado à divisibilidade. É uma notação de algum caso de divisibilidade: $a \equiv b \pmod{m} \Leftrightarrow m|a - b$".

O estudante S2 escreveu corretamente a definição de congruência, e escreveu em seguida: "...depois destacaria que m é o resto na divisão de a por b, se tomarmos a e b convenientemente". Apesar de escrever corretamente a definição, este estudante parece ter uma ideia de congruência equivocada; a noção de congruência, não foi bem entendida, dando a impressão de que a definição foi decorada.

Subclasse A2: Corresponde a quatro (4) respostas que estão escritas utilizando a notação de múltiplo. Os estudantes responderam a questão dizendo que $a \equiv b \pmod{m} \Leftrightarrow a - b = mk, k \in \mathbb{Z}$. Um dos estudantes, A10, ainda relacionou os múltiplos e a ideia da divisão, mostrando que b pode ser o resto da divisão de a por m.

Outro estudante, T4, escreveu:"$a, b, m, \in \mathbb{Z}$, dizemos que $a \equiv b \pmod{m}$ se a diferença de a e b é múltipla de m, i.é: $a - b = mk, k \in \mathbb{Z}$. No primeiro ano do curso de Matemática, um aluno deve ser capaz de aceitar essa definição".

Subclasse A3: Corresponde às quatro (4) respostas em que as duas notações

são utilizadas. Respostas como a do estudante, S7, que escreveu: "... dado a, b e $n \in$ aos inteiros a é congruente a $b \mod m$ se: $a - b$ for múltiplo de n, ou seja, n divide $a - b$".

De um modo geral, as respostas dadas a esta questão, que estão nesta classe, foram satisfatórias. Pode-se dizer que estes estudantes, de alguma forma, entenderam a definição de congruência módulo m.

Classe B: Corresponde a cinco (5) respostas, em que a ideia de congruência como resto de divisão é utilizada. Duas destas respostas, dos estudantes S4 e T1, utilizaram a ideia de resto mencionando as classes laterais, da seguinte forma: "Dois números são congruentes módulo m quando têm restos iguais na divisão por m. Daí decorre o fato de existirem m possibilidade de classes de congruência...", foi a resposta de S4.

Outro aluno, A4, respondeu que "$a \equiv b \pmod{m}$ é o mesmo que a e b terem o mesmo resto na divisão por m", mas em seguida, afirmou que b é o resto da divisão de a por m, isto está correto, como um caso particular, para valores convenientes de a e b, como por exemplo 15 e 1 módulo 2, mas isso não ocorre sempre. As outras duas (2) respostas, dos estudantes S6 e A5, correspondem ao caso particular em que $a \equiv r \pmod{m}$, em que r é o resto da divisão de a por m. Mas estas respostas foram dadas em termos numéricos, módulo 5 e módulo 7. Pode-se considerar que estas respostas estão parcialmente corretas, porque isso não acontece sempre. Tome por exemplo os números inteiros 15 e 30, $15 \equiv 30 \pmod{5}$; porém 30 não é o resto da divisão de 15 por 5.

Classe C: Corresponde a quatro (4) respostas que utilizaram a ideia de congruência como relação de inteiros e como resto da divisão. Apenas esses quatro (4) estudantes, S15, S9, S1 e A7, usaram as ideias de resto da divisão e definição de congruência módulo m, a definição 3 do Capítulo 2, de forma correta, sendo que apenas um deles, S1, referiu-se em termos de relação entre inteiros, da seguinte forma: "Congruência módulo m é uma relação entre inteiros tal que

$$a, b \in \mathbb{Z}\ a \equiv b \pmod{m}\ se\ a - b$$

é múltiplo de m. Ou: a e b possuem o mesmo resto na divisão por m".

O estudante A7, no entanto, mesmo utilizando corretamente a definição, ao tentar explicá-la cometeu alguns erros com as notações de dividir e divisibilidade; os

símbolos de divisibilidade "$a \mid m$" e os símbolos de divisão "a/m" foram empregados de maneira equivalente. Ele escreveu o seguinte:

$$\text{“}a \equiv b \pmod{m} \Rightarrow m \mid a-b \therefore \quad a-b=mk, \;\; a=mk+b.$$
$$4 \equiv 8 \pmod{2},\ 4 \div 2 = 2 \text{ e } 8 \div 2 = 4.$$

A congruência módulo m é quando $a \mid m$ e $b \mid m$ tem o mesmo resto." Entende-se que este estudante quis dizer que $a \div m$ e $b \div m$ deixam o mesmo resto, mas os símbolos utilizados dizem outra coisa.

Classe D: Corresponde às duas (2) respostas em que foram utilizadas a ideia de base númérica. Dois estudantes A3 e S3, usaram a noção de base de um sistema de numeração para explicar a ideia da congruência módulo m, A3 escreveu "O módulo m age como uma base de um sistema de numeração. Por exemplo, o módulo 2 seria equivalente ao código binário". Esta resposta traz uma característica importante da congruência módulo m que é a periodicidade, e está relacionada com o resto da divisão. Eles mencionaram como exemplo as horas, $a \equiv b \pmod{12}$ e o código binário $\overline{0}$ e $\overline{1}$, ou seja, $a \equiv b \pmod{2}$.

Classe E: Referente às cinco (5) resoluções incorretas ou incompletas. Das cinco respostas consideradas erradas, em todas elas as divisões e o resto destas divisões, estão envolvidos. Isto está presente na resposta do aluno A2 que escreveu, "eu enunciaria o teorema de euclides para explicar congruência".

O estudante, S17, escreveu que m é o resto da divisão de a por b e por isso $a \equiv b \pmod{m}$. Outro aluno, A1, respondeu que a " congruência módulo m é uma relação $a \equiv b \pmod{m}$ tal que $b \mid (a-m)$, ou seja, $bs = a-m, s \in \mathbb{Z}$.", que foi a mesma ideia utilizada pelo estudante A9. Estes estudantes parecem se lembrar que a definição de congruência envolve um número dividindo uma diferença, mas não compreenderam quais eram estes números, e o que eles significavam. Mesmo nas respostas incorretas as noções de múltiplo e divisibilidade apareceram.

Primeiras Análises

As respostas à questão 1 foram, em sua maioria, trinta e duas (32), consideradas corretas e mostraram que os estudantes conseguiram definir a relação de congruência módulo m, seja utilizando a definição padrão, definição número 3 do Capítulo 2 sobre o objeto matemático, com variação da utilização de múltiplos ao

invés da divisibilidade, como na resposta do estudante A10, que escreveu: "$a \equiv b \pmod{m} \Leftrightarrow a - b = mk, k \in \mathbb{Z}$", ou utilizando a definição de congruência, usando a ideia de resto de divisão, como a definição 4 também do Capítulo 2. As ideias de periodicidade e de agrupar elementos que estão relacionados, também foram mencionadas na utilização de exemplos, como o das horas do relógio analógico (congruência módulo 12) e o código binário (congruência módulo 2) da **classe D**.

Em uma pesquisa sobre a interpretação dos estudantes da congruência módulo m, Smith (2006) divide estas interpretações em duas categorias, que ela chamou de relacional e operacional, dependendo de como o estudante define e utiliza as propriedades da congruência módulo m. Por exemplo, se o estudante consegue expressar que dois números são congruentes, se deixam o mesmo resto na divisão por m, então pode-se interpretar esta resposta como relacional. Se, por outro lado, o estudante diz que a e b são congruentes, se b é o resto da divisão de a por m, então a interpretação de congruência módulo m deste estudante é operacional.

De acordo com esta categorização e levando em conta as respostas dos estudantes a esta questão, pode-se entender que eles interpretam a congruência módulo m de forma relacional, pois a maioria das respostas, vinte e nove delas, foi feita em termos de relação de equivalência.

Nas respostas consideradas erradas, cinco (5) delas, a ideia de resto da divisão e divisibilidade também foram utilizadas, mas de forma equivocada; esses estudantes lembravam-se de que estes conteúdos matemáticos estavam de alguma forma envolvidos na definição de congruência módulo m, mas não souberam expressar como eles estavam envolvidos, como na resposta do estudantes A1 da **classe E**. O que sugere a dificuldade desses estudantes com a definição da relação de congruência módulo m e com a ideia intuitiva de tomar o resto da divisão.

As respostas desses estudantes a essa primeira questão indicam que esta definição foi apreendida pela maioria dos estudantes, ou seja, eles conseguiram definir a congruência módulo m, e alguns deles mencionaram a característica de periodicidade; outros, ainda, relacionaram as duas definições, dizendo que elas podem ser equivalentes.

Questão 2

Qual o resto da divisão de $n = (121 \cdot 35 + 282 \cdot 75)$ *por* 4. *Justifique sua resposta.*

O objetivo desta questão era verificar se os estudantes utilizariam a congruência módulo m para resolver a questão e identificar qual definição seria utilizada.

A resposta da questão é que o resto desta divisão é 1. Os estudantes poderiam responder esta questão usando a ideia de congruência como resto da divisão, ou poderiam fazer as contas, embora esta estratégia não fosse a esperada, dado os objetivos da questão. Foram consideradas erradas as questões em que a resposta ou as justificativas estavam incorretas.

Trinta e dois (32) estudantes responderam esta questão e nove (9) (T2, T3, A11, S13, S14, S16, S17, S21, S22) não responderam. De acordo com as estratégias e notações utilizadas nestas respostas, foi possível dividi-las em cinco classes resumidas no quadro abaixo e detalhadas a seguir:

Classe	Subclasse	Estudantes	Tipo de resposta
A	A1	S3, S15, S18, S19, A1, A3, A8, A9, A13	resto da divisão e separando em múltiplos de 4
	A2	S6, S8, A4, A12	resto de divisão e notação de congruência
	A3	S5, S12, A14, T1	dividiu as parcelas por quatro e usou resto da divisão
B		S1, S2, S9, A5, A6, A15	notação e propriedades da congruência módulo m
C		A2, A7, T4	fez as contas indicadas
D		S4	usou classes de congruência
E		S7, S10, S11, S20, A10	parciais

Quadro 5.2: Classes da questão 2

Classe A: Corresponde a dezessete (17) respostas, em que os estudantes utilizaram a ideia de resto da divisão, separando os números múltiplos de quatro, visando eliminar as divisões exatas e deixando os restos. Esta classe pode ser, ainda, dividida em subclasses:

Subclasse A1: Corresponde a nove (9) respostas, em que os estudantes usaram soma de resto da divisão para resolver a questão. Como o aluno A1 que diz que sendo $n = (121 \cdot 35 + 282 \cdot 75)$, então "$(30 \cdot 4 + 1)(4 \cdot 8 + 3) + (4 \cdot 7 + 2)(4 \cdot 18 + 3); r = 3 + 6 = 9/4 \Rightarrow r = 1$".

Apesar da notação deste aluno não ser rigorosa, entendeu-se que ele dividiu 9 por 4 para obter a resposta da questão.

Subclasse A2: Corresponde a quatro (4) respostas, em que os estudantes utilizaram a ideia de resto, separando os múltiplos de quatro e usaram a notação de congruência módulo m para dar a resposta.

Como o estudante A4, que escreveu:

$$\text{“}121 = 120 + 1 = 4 \cdot 30 + 1 \quad 35 = 8 \cdot 4 + 3$$

$$282 = 280 + 2 = 4 \cdot 70 + 2 \;\; 75 = 18 \cdot 4 + 3 ... 3 + 6 = 99 \equiv 1 \pmod 4\text{”}.$$

Depois, para explicar o que tinha feito para resolver o problema, ele escreveu: “Decompus os números, separei os restos e os somei, deu 9, mas quando dividido por 4 dá resto 1, que é o resto de toda a divisão”.

Subclasse A3: Corresponde a quatro (4) respostas, em que os estudantes dividiram cada parcela da soma por 4 e usaram a soma do resto da divisão para resolver a questão. Um exemplo desse tipo de resposta é a do estudante T1, que escreveu:“(121.35 + 282.75) Dividindo cada número por 4 e obtendo resto da divisão, os restos de $121, 35, 282$ e 75 são respectivamente $1, 3, 2$ e 3, no lugar dos números coloco os seus restos e obtenho $(1 \cdot 3 + 2 \cdot 3) = 9$, 9 dividindo por 4 tem resto 1”.

A ideia de congruência módulo m como resto da divisão está presente nestas respostas, pois utilizaram as relações com resto da divisão.

Classe B: Corresponde a seis (6) respostas, em que os estudantes utilizaram a notação e as propriedades de congruência módulo 4. Como, por exemplo, o aluno S2, que escreveu em sua resposta:

$$\begin{gathered}
\text{“}121 \equiv 1 \mod 4 \qquad 282 \equiv 2 \mod 4 \\
35 \equiv -1 \mod 4 \qquad 75 \equiv -1 \mod 4 \\
121.35 \equiv 1(-1) \mod 4 \qquad 282.75 \equiv 2(-1) \mod 4 \\
\text{então } 121.35 + 282.75 \equiv -1. - 2 \mod 4 \\
\equiv -3 \mod 4 \\
\equiv 1 \mod 4\text{”}.
\end{gathered}$$

Esses estudantes conseguiram utilizar a notação e as propriedades de congruência módulo 4 e parece que eles conseguiam coordenar a ideia de congruência e sua notação.

Classe C: Corresponde a três (3) respostas, em que os alunos fizeram as contas, ou seja, eles multiplicaram 121 por 35, 282 por 75, somaram estes resultados e dividiram por 4, obtendo, assim, o resto da divisão que se pedia na questão.

O estudante A7, para justificar sua estratégia, escreveu: "Não me recordo de nenhuma teoria de Álgebra para me auxiliar de maneira imediata. Então, fiz as contas mesmo".

Classe D: Corresponde a uma (1) resposta, em que o estudante utilizou as classes de congruência módulo 7, para resolver a questão. O estudante S4 escreveu: "$n = 121 \cdot 35 + 282 \cdot 75 = \overline{1} \cdot \overline{-1} + \overline{2} \cdot \overline{-1} = \overline{-1} - \overline{2} = \overline{-3} = \overline{1}$ resto 1".

Classe E: Corresponde a cinco (5) respostas a esta questão, em que os estudantes usaram a notação e propriedades de congruência, mas não terminaram de resolver a questão. Eles esboçaram em suas respostas a ideia de que, usando a congruência módulo 4, resolveriam o problema proposto, mas não deram continuidade a seus raciocínios, como o aluno A10, que respondeu: "Para o resto da divisão, utilizaria a ideia de módulo, visto que o resto "r" $n \equiv r \pmod 4$ $(121.35 + 282.75 \equiv r \pmod 4)$". E terminou sua resolução neste ponto. Pode-se entender que estes estudantes pareciam saber que poderiam resolver este tipo de problema, usando a congruência módulo m, mas talvez eles não soubessem como utilizar esta noção, ou eles apenas utilizaram esta noção por se tratar de um questionário sobre a congruência módulo m, e então eles podem ter concluído que, com essa noção, resolveriam o problema, mas não sabem como fazer isso.

Primeiras Análises

As respostas à questão dois foram, em sua maioria, corretas, já que vinte e sete (27) delas foram consideradas assim. As estratégias utilizadas foram variadas, mas em geral elas consistiam em fazer algumas contas, seja efetuando as operações indicadas e fazendo a divisão por 4, ou dividindo as parcelas e somando os restos, resoluções aritméticas. Poucos estudantes utilizaram a relação de congruência módulo 4 para resolver esta questão.

Dentre as respostas em que a ideia de congruência módulo 4 foi utilizada, sua notação e propriedades, notou-se que a interpretação relacional da congruência módulo m permaneceu, pois os estudantes conseguiram "ver o termo $\pmod m$ modificando toda a congruência, não apenas um dos inteiros", (SMITH 2006, p. 261, tradução da

autora), como, por exemplo, na resposta do aluno S2 da **classe B**.

Embora a maioria das respostas apresente a noção de congruência módulo m, principalmente as respostas das **classes A** e **C**, a definição mais utilizada foi a de que dois números são congruentes se deixam o mesmo resto da divisão. Também se pode notar a ideia de que $a \equiv r \pmod{m}$. Dessa forma, pode-se pensar que o objetivo desta questão não foi alcançado.

Questão 3

Mostre que $2^{13} \equiv 2 \pmod{7}$. *Justificando sua resposta.*

O objetivo desta questão era verificar se os alunos conseguiriam aplicar as propriedades da congruência módulo m e o Pequeno Teorema de Fermat[1].

Ela poderia ser resolvida utilizando o Pequeno Teorema de Fermat ou as propriedades básicas de congruência módulo m, ou, ainda, desenvolvendo a potência e efetuando a divisão, embora esta última estratégia não fosse esperada como resposta, dados os objetivos da questão. Foi considerada correta qualquer uma destas alternativas, ou, ainda, uma outra que tenha levado à resposta correta. Foram consideradas parciais aquelas respostas que não completaram corretamente a demonstração, mas que, pelo menos, parte dela estivesse correta. As respostas erradas foram aquelas em que não havia indícios de que os estudantes estivessem na direção correta para demonstrar o que foi pedido, ou quando a apresentação da demonstração não estivesse correta.

Trinta e quatro (34) estudantes responderam esta questão e sete (7) (S16, S17, A2, A7, A10, A11, T2) não responderam. De acordo com as respostas dos estudantes, foi possível encontrar cinco classes, que estão resumidas no quadro abaixo e detalhadas a seguir:

Classe	Subclasse	Estudantes	Tipo de resposta
A		S7, S11, S14, S18, T3, T4, A4, A5, A9, A12, A15,	usou o Pequeno Teorema de Fermat e propriedades de congruência
B		S1, S2, S6, S9, S10, S12, S20, S21, S22, A6, A14, A13, T1	usou propriedades de congruência módulo m

[1] Pequeno Teorema de Fermat: Seja p primo. Se p não divide a então $a^{p-1} \equiv 1 \pmod{p}$. (Santos, 1998).

Classe	Subclasse	Estudantes	Tipo de resposta
C	C1	S3, S13, A3, A8,	usou a tese na argumentação
	C2	A1, S8	usou $2^6 \equiv 2 \pmod 7$
D		S5, S19	respostas incompletas
E		S4, S15	definição de congruência; classe de congruência.

Quadro 5.3: Classes da questão 3

Classe A: Corresponde a onze (11) respostas, nas quais foram utilizados o Pequeno Teorema de Fermat e propriedades de congruência. O uso desse teorema foi considerado, mesmo que não fosse mencionado, isto é, foi considerado como uso do teorema a relação $2^6 \equiv 1 \pmod 7$. Como pode ser visto na resposta dada pelo estudante A12, que fez a seguinte demostração:

$$\text{“}2^6 \equiv 1 \pmod 7) \uparrow^2$$
$$(2^6)^2 \equiv 1^2 \pmod 7$$
$$2^{12} \equiv 1 \pmod 7) \times 2$$
$$2^{12}.2 \equiv 1.2 \pmod 7$$
$$2^{13} \equiv 2 \pmod 7\text{”}$$

Ele partiu do Pequeno Teorema de Fermat e, utilizando as propriedades de potência e multiplicação, chegou ao resultado.

Outros estudantes, A9 e A4, embora tenham demonstrado corretamente o que se pedia no problema, identificaram o teorema usado como sendo Teorema de Euclides, não de Fermat. A resposta do estudante A9, foi a seguinte:

$$\text{“ Por Euclides, temos } 2^6 \equiv 1 \pmod 7)$$
$$\text{elevando ao quadrado, } 2^{12} \equiv 1 \pmod 7)$$
$$\text{multiplicando por 2, } 2^{13} \equiv 2 \pmod 7\text{”}$$

Isso não está rigorosamente correto para uma demonstração, mas no caso desta pesquisa foi considerado correto, pois as propriedades de congruência e mesmo o teorema foram utilizados corretamente.

Classe B: Corresponde a treze (13) respostas, em que os estudantes utilizaram as propriedades da congruência módulo m. Em geral, os alunos utilizaram as propriedades de potência e multiplicação de congruência módulo m, mas alguns alunos,

como S1, utilizaram as propriedades de potência de número inteiro juntamente com as de congruência, da seguinte maneira: " $2^{13} = (2^3)^4.2$, como $2^3 \equiv 1(7) \rightarrow 2^{13} \equiv 2(7)$".

A maioria dos estudantes dessa classe, oito (8), usou como argumento que $2^3 \equiv 1 \pmod 7$ e utilizou depois as propriedades de potência e multiplicação, como o estudante S9, que escreveu:

"$2^3 \equiv 1 \pmod 7$ elevando à 4

$(2^3)^4 \equiv 1^4 \pmod 7$

$2^{12} \equiv 1 \pmod 7$ multiplicando por 2 lado a lado

$2^{13} \equiv 2 \pmod 7$"

Classe C: Corresponde a sete (7) provas, em que as respostas estão incorretas. Estas respostas foram consideradas incorretas, porque a demonstração apresentada está incorreta, seja em sua argumentação ou na forma da apresentação, utilizando a tese como hipótese. Assim, pode-se dividir esta classe em duas subclasses:

Subclasse C1: Corresponde a cinco (5) respostas, em que os estudantes utilizaram a tese, $2^{13} \equiv 2 \pmod 7$, como hipótese e, depois, utilizaram as propriedades de congruência para completar a demonstração. Como, por exemplo, o estudante A3 que respondeu:

" $2^{13} \equiv 2 \pmod 7$

$2^{6+6+1} \equiv 2 \pmod 7$

$2^6 2^6 2^1 \equiv 2 \pmod 7$, por Fermat:

$2 \equiv 2 \pmod 7$"

Pode-se observar que a utilização das propriedades, e até mesmo do Pequeno Teorema de Fermat, estão corretos, mas a forma de apresentação da demonstração não está.

Subclasse C2: Corresponde a duas (2) respostas, em que o argumento utilizado para a demonstração estava incorreto.

Em uma delas, o Pequeno Teorema de Fermat, foi enunciado e utilizado de forma incorreta; nesta resposta, o estudante, A1, usou este Teorema, no caso particular desta questão, como sendo $2^6 \equiv 2 \pmod 7$.

Na outra resposta, o estudante, S8, usou a congruência $2^3 \equiv 2 \pmod 7$, que não está correta, para fazer sua demonstração.

Classe D: Corresponde a duas (2) respostas, em que os estudantes não concluíram a demonstração. Esses estudantes começaram a desenvolver suas respostas, mas não terminaram a demonstração, como o aluno S5, que escreveu: "$2^{13} \equiv 2 \pmod 7$. Sei que $2^4 \equiv 2 \pmod 7$, pois $7|(2^4 - 2)$ $7|(16 - 2)$ $7|14$", terminando assim sua argumentação.

Certamente, ele não mostrou o que foi pedido, mas a utilização da congruência está correta. Esta resposta indica que este estudante conhece a definição de congruência módulo m, mas não sabe como trabalhar com ela a ponto de mostrar que $2^{13} \equiv 2 \pmod 7$.

Classe E: Corresponde a duas (2) respostas, que não se encaixam nas anteriores. O estudante, S15, fez a demonstração utilizando a definição de congruência módulo m, mostrando que $2^{13} - 2 = 7k$ e usando propriedades dos números inteiros como distributiva e de potências, conseguindo demonstrar o que se pedia. Apesar de utilizar também propriedades de potência, como outros estudantes, esta resposta é diferente por se referir à definição de congruência módulo m.

O estudante S4 usou classes de congruência módulo 7 e as propriedades da potenciação: "$2^{13} = 2^3 \cdot 2^3 \cdot 2^3 \cdot 2 = \overline{1} \cdot \overline{1} \cdot \overline{1} \cdot \overline{2} = 2 \mod 7$". Notou-se, nessa resposta, a igualdade da classe $\overline{1}$ com o número 2, o que pode não ser verdadeiro, dependendo de como o anel Z_m foi definido.

Primeiras Análises

A questão de número três foi respondida corretamente por vinte e seis (26) estudantes, dos trinta e cinco (35) que responderam esta questão, utilizando estratégias diversas. Doze (12) deles utilizaram as propriedades de congruência módulo m e o Pequeno Teorema de Fermat, onze (11) utilizaram somente as propriedades e um (1) deles fez a demonstração a partir da definição. Em geral, a notação foi utilizada de forma correta. As sete (7) respostas consideradas incorretas, continham erros em suas demonstrações, como a do estudante S8, que usou, em sua argumentação, que o Pequeno Teorema de Fermat para este caso seria $2^6 \equiv 2 \pmod 7$, o que não está correto. Outros estudantes utilizaram a tese, ou seja, $2^{13} \equiv 2 \pmod 7$, como hipótese, como o estudante A3, cuja resposta está na **subclasse C1**.

Quanto à utilização das propriedades e definição da congruência módulo m, nota-se que os estudantes conseguiram, ainda, utilizá-las algumas vezes de forma cor-

reta, substituindo números congruentes, como o estudante A1, que escreveu:

$$\text{“Sabemos que } 2^3 \equiv 2 \pmod 7$$
$$2^{13} = 2^3.2^{10} = 2^3.2^3.2^3.2^3.2^1 \ldots 2^{13} \equiv 2.2.2.2.2 \pmod 7 \ldots\text{”}$$

Esse estudante, apesar de utilizar a congruência $2^3 \equiv 2 \pmod 7$, que está errada, fez as substituições corretamente.

Nas respostas da **subclasse C1**, observa-se uma tentativa de análise, em que o estudante, partindo da tese, por meio de uma sequência lógica de argumentos, chegou a uma sentença verdadeira. Esta é uma prática válida para fazer uma demonstração em Matemática. O problema é que a apresentação de uma demonstração, aceita pela Comunidade Matemática, é a síntese desta argumentação, ou seja, parte-se de uma sentença verdadeira para se chegar à tese. Por isso, estas respostas foram consideradas erradas.

Nesta questão, os estudantes parecem, em geral, saber utilizar as propriedades de congruência: de multiplicar um mesmo número dos dois lados e elevar a potência dos dois lados. Embora muitos não tenham utilizado a notação de congruência, a ideia de resto da divisão está presente nas respostas, mostrando que os estudantes preferiram ainda utilizar resoluções aritméticas.

Questão 4

Considere o conjunto $\overline{a} = \{x \in \mathbb{Z}; x \equiv a \pmod m\}$*, este conjunto é chamado* classe de congruência de a módulo m*, ou seja, o conjunto cujos elementos são todos os inteiros congruentes a a módulo* m*.*

As classes de congruência módulo 4*, isto é,* $\overline{a} = \{x \in \mathbb{Z} | x \equiv a \pmod 4\}$*, são:*

$$\overline{0} = \{0, 4, 8, ..., 4k\}, \text{ com } k \in \mathbb{Z}.$$
$$\overline{1} = \{1, 5, 9, ..., 1 \pm 4k\}, \text{ com } k \in \mathbb{Z}.$$
$$\overline{2} = \{2, 6, 10, ..., 2 \pm 4k\}, \text{ com } k \in \mathbb{Z}.$$
$$\overline{3} = \{3, 7, 11, ..., 3 \pm 4k\}, \text{ com } k \in \mathbb{Z}.$$

Encontrando todas as classes de congruência módulo m *dos elementos de* $\mathbb{Z}$*, temos o conjunto quociente* $\mathbb{Z}_m = \{\overline{a} \,|\, a \in \mathbb{Z}\}$ *é o conjunto de todas estas classes e é denotado por* $\mathbb{Z}/\equiv_m$ *ou* $\mathbb{Z}_m$*.*

O conjunto de todas as classes de congruência módulo 4, $\mathbb{Z}_4$ *é o conjunto* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, *com apenas quatro elementos, já que* $\overline{4} = \overline{0}$, $\overline{5} = \overline{1}$, $\overline{6} = \overline{2}$ *e assim por diante.*

Considerando, agora, o conjunto de classes de congruência módulo 7, *isto é,* $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, *podemos dizer que:*

(a) $10 \in \mathbb{Z}_7$. *Justifique sua resposta.*

(b)$\overline{10} \in \mathbb{Z}_7$. *Justifique sua resposta.*

O objetivo desta questão era verificar se os alunos reconheciam a partição induzida pela relação congruência módulo m em $\mathbb{Z}$, e se conseguiam fazer distinção entre a e sua classe $\overline{a}$.

Ela tem como resposta: a) Não é verdadeira, pois 10 é um número inteiro e não uma classe de congruência módulo 7.

b) É verdadeiro, pois $\overline{10} = \overline{3}$ e, portanto, $\overline{10} \in \mathbb{Z}_7$.

Esta questão trata de um assunto que não foi trabalhado na disciplina Teoria de Números, que os estudantes já tinham cursado anteriormente; a construção das classes de congruência módulo m e do conjunto quociente foram feitas somente na disciplina Teoria de Anéis, nas aulas subsequentes à aplicação deste questionário. Mesmo assim, ela foi aplicada pois se esperava que os estudantes conseguissem respondê-la, utilizando conhecimentos prévios de partição de conjunto e classes de equivalência, estudados em disciplinas anteriores.

Dos quarenta e um estudantes (41) que responderam a este questionário, dezoito (18) deles (T2, S2, S3, S16, S17, S18, S19, S20, S21, S22, A1, A2, A3, A6, A8, A12, A13, A14) não responderam a esta questão. As vinte e três (23) respostas desta questão foram agrupadas em cinco classes, como mostra o quadro abaixo e que serão detalhadas a seguir:

Classe	Estudantes	Tipo de resposta
A	S1, S14, S15, A11	a) $10 \notin \mathbb{Z}_7$, pois $10 \in \mathbb{Z}$ e b) $\overline{10} \in \mathbb{Z}_7$ pois $\overline{10} = \overline{3}$
B	S7, S11, S12, S13, A4, A9, A10, T4,	a) $10 \in \mathbb{Z}_7$, pois $10 \in \overline{3}$ e $\overline{3} \in \mathbb{Z}_7$ e b) $\overline{10} \in \mathbb{Z}_7$, pois $\overline{10} = \overline{3}$
C	S5, S6, S8, S9, S10, A5, A7, A15, T1	a)$10 \in \mathbb{Z}_7$, pois $10 \in \overline{3}$ e b) $\overline{10} \notin \mathbb{Z}_7$, pois $\mathbb{Z}_7$ tem apenas 7 elementos.
D	T3, S4	$10 \notin \mathbb{Z}_7$ e $\overline{10} \notin \mathbb{Z}_7$. Não respondeu item a)

Quadro 5.4: Classes da questão 4

Classe A: Corresponde a quatro (4) respostas consideradas corretas. Nestas, os argumentos usados para justificar que $10 \notin \mathbb{Z}_7$ é que 10 não é classe de congruência módulo 7, como a resposta do estudante S15, que diz que $10 \notin \mathbb{Z}_7$, "pois $\mathbb{Z}_7$ é o conjunto das classes de congruência módulo 7 e 10 não é uma congruência". Na verdade, esse estudante deveria dizer que 10 não é uma classe de congruência. Já o argumento mais utilizado para justificar que $\overline{10} \in \mathbb{Z}_7$ é que $\overline{10} = \overline{3}$, como por exemplo o do estudante S14, que escreveu: "$\overline{10} \in \mathbb{Z}$, pois $\overline{10} = \overline{3}$ e $\overline{3} \in \mathbb{Z}_7$. Este argumento mostra que a noção de representante de classe de congruência foi usada de forma correta.

Classe B: Corresponde a oito (8) respostas, em que o item a) da questão foi considerado incorreto e o item b) correto. O argumento utilizado por três estudantes para justificar que $10 \in \mathbb{Z}_7$, é que $10 \in \overline{3}$ e que $\overline{3} \in \mathbb{Z}_7$. Essa resposta indica que estes estudantes não entenderam o que é e como se trabalha com partição de um conjunto, ou seja, o que é elemento e o que é subconjunto de um conjunto.

Outros dois (2) estudantes, A9 e T4, justificaram que $10 \in \mathbb{Z}_7$, porque $10 \equiv 3 \pmod 7$, portanto, $10 \in \overline{3}$, o que leva a concluir que também, para esses estudantes, o fato que $10 \in \overline{3}$ implica que $10 \in \mathbb{Z}_7$, e novamente a noção de partição de um conjunto não foi utilizada de forma correta por eles.

Um outro aluno, A4, concluiu que $10 \in \mathbb{Z}_7$, porque $10 \in \overline{3}$ e que $\overline{3} \subset \mathbb{Z}_7$, que é um argumento parecido com os demais, mas ele não entendeu $\overline{3}$, como elemento de um conjunto. Isso indica que a ideia de conjunto como sendo elemento de outro conjunto não foi entendida pelo aluno.

Já o argumento justificando que $\overline{10} \in \mathbb{Z}_7$ foi o mesmo da classe anterior, ou seja, que $\overline{10} = \overline{3}$.

Classe C: Corresponde a nove (9) respostas consideradas incorretas. A maioria dos estudantes que responderam errado o item a) desta questão, fizeram a seguinte argumentação: $10 \in \overline{3}$, como $\overline{3} \subset \mathbb{Z}_7$, então $10 \in \mathbb{Z}_7$. Esse é um raciocínio que mostra que a ideia de partição de um conjunto não está bem entendida pelos estudantes; eles não demonstram entender um conjunto $\overline{3}$ como elemento de outro conjunto, o $\mathbb{Z}_7$.

Das respostas erradas do item b), a justificativa que mais foi encontrada foi a de que $\mathbb{Z}_7$ tem apenas 7 elementos e que, portanto, $\overline{10} \notin \mathbb{Z}_7$. Como a resposta do estudante S5, que entende que $\overline{10} = \overline{3}$, mas diz que $\mathbb{Z}_7$ tem apenas 7 elementos e que, portanto, $\overline{10} \notin \mathbb{Z}_7$. Isso indica que estes estudantes não entenderam o que significa $\overline{10} = \overline{3}$ e que $\overline{10} \in \mathbb{Z}_7$. Este tipo de resposta sugere que a escolha do representante para a classe, não foi bem compreendida por esses alunos. Por outro lado, o enunciado da questão pode ter induzido esta justificativa, já que mostra $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ com os elementos canônicos.

Classe D: Corresponde a duas (2) respostas, que não se encaixam nas demais. Em uma delas, o estudante S4 respondeu no item a) que "Não. Z_7 é um conjunto de classes e 10 é um número". O argumento utilizado no item b) "... as classes em $\mathbb{Z}_7$ são $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}$". Este argumento é semelhante a dizer que $\mathbb{Z}_7$ tem apenas 7 elementos, que assim como na **Classe C** anterior indica que o aluno não compreendeu as classes de congruência e seus representantes.

O estudante T3 não respondeu o item a) e respondeu no item b) que $\overline{10} \notin \mathbb{Z}_7$, pois "... se dividirmos 7 por qualquer $\overline{a}$ o conjunto, o resto não será igual quando 7 é dividido por 10".

Primeiras Análises

Embora nem todos os estudantes tivessem estudado classe de congruência módulo m, a questão de número quatro (4) tratava sobre ela, explicou-se primeiramente o que era uma classe de congruência e exemplificou-se com o conjunto das classes módulo 4, ou seja, o $\mathbb{Z}_4$. Esperava-se que os estudantes respondessem esta questão com conhecimentos prévios, sobre partição de conjunto e relação de equivalência, que se supõem apreendidos por um estudante que cursa a disciplina de Álgebra. Mas dos vinte e três (23) estudantes que responderam esta questão, apenas quatro (4) deles o fizeram corretamente, eles conseguiram explicar que $10 \notin \mathbb{Z}_7$, pois 10 é um número inteiro e que $\overline{10} \in \mathbb{Z}_7$, pois $\overline{10} = \overline{3}$. Foi considerado nesta questão o $\mathbb{Z}_7$ como o conjunto

das classes de congruência módulo 7, excluindo assim a possibilidade de entender este conjunto como o conjunto dos restos da divisão por 7.

Nos argumentos utilizados para justificar que $10 \in \mathbb{Z}_7$, encontrou-se indícios de que a noção de partição de conjunto não foi entendida por estes estudantes, pois eles argumentaram que $10 \in \mathbb{Z}_7$, pois $10 \in \overline{3}$ e que $\overline{3} \in \mathbb{Z}$.

Outros estudantes parecem não entender a classe de congruência, no caso $\overline{3}$, como um conjunto que é elemento de outro conjunto. Estes estudantes escreveram que $10 \in \mathbb{Z}_7$, pois $10 \in \overline{3}$ e que $\overline{3} \subset \mathbb{Z}$. O que se pode pensar é que eles entenderam que $\overline{3}$ é um conjunto, mas não conseguiram vê-lo como elemento de um outro conjunto, pois parecem empregar uma 'regra' utilizada quando se ensina noções básicas da Teoria de Conjuntos, que é 'se é conjunto está contido, então usa $\subset$; se é elemento, então pertence a um conjunto, então usa $\in$'; que pode levar o estudante a entender que não é possível que um conjunto seja elemento de outro conjunto.

Quanto aos argumentos para justificar que $\overline{10} \notin \mathbb{Z}_7$, a maioria dos estudantes escreveu que $\mathbb{Z}_7$ tem apenas sete elementos. Esta resposta talvez se deva ao fato do $\mathbb{Z}_7$ ter sido apresentado, no enunciado da questão, em sua forma canônica, ou seja, $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Este argumento também está ligado ao representante da classe e à natureza dos elementos do conjunto, pois $\overline{10} = \overline{3}$ e poder-se-ia ter $\mathbb{Z}_7 = \{\overline{7}, \overline{8}, \overline{16}, \overline{10}, \overline{18}, \overline{19}, \overline{27}\}$, o que muda neste caso é o número inteiro que representa a classe de congruência, que permanece a mesma, ou seja, o conjunto de inteiros congruentes a $0, 1, 2, 3, 4, 5, 6$ módulo 7, respectivamente.

Pelas respostas dos estudantes, pode-se entender que eles não reconheceram a partição de $\mathbb{Z}$ induzida pela relação de congruência módulo m. E não conseguiram diferenciar o número inteiro a da classe de congruência $\overline{a}$, já que dezessete(17) dos vinte e três (23) estudantes disseram que $10 \in \mathbb{Z}_7$.

5.1.2 Análise e discussão dos resultados: o apoio nas entrevistas

Esta seção será dedicada a discutir os resultados apresentados na seção anterior. Para esta discussão serão utilizadas, também, para reforçar ou refutar as hipóteses geradas pelas respostas do questionário, as respostas das entrevistas que os estudantes deram a questões elaboradas para isso.

As respostas deste questionário apontam que, em geral, os estudantes conseguem trabalhar com a definição de relação de congruência e com suas propriedades, pois as questões $1, 2$ e 3 foram respondidas corretamente pela maioria deles. Fica evidente, também, que alguns estudantes empregam ainda resoluções aritméticas, como os estudantes que efetuaram as operações indicadas na questão 2 para resolvê-la, ao invés de usarem a noção de congruência módulo m.

Notou-se, que mesmo que a noção de congruência módulo m não tenha sido escrita corretamente, alguns estudantes, cujas respostas estão na **classe E** da questão 1, conseguiram responder as questões 2 e 3 de forma satisfatória, sugerindo que a ideia intuitiva de tomar o resto da divisão por m e as propriedades dessa relação foram, de certa forma, compreendidas pelos estudantes, embora a definição formal não. Veja, por exemplo, o que respondeu o estudante A9, na questão 1: "$a \equiv x \pmod{m}$ equivale afirmar que $a = mb + x$, sendo b um fator multiplicativo de m e x o resto da divisão de a por b". Já na resposta à questão 2, sua resolução foi aritmética, "usando somas, buscando encontrar múltiplos de 4, visando eliminar divisões exatas. Logo se encontra resto 1". Já na questão 3 utilizou a notação e as propriedades de congruência módulo m corretamente, confundindo apenas o nome do teorema utilizado na resolução, como pode ser visto na **classe A** da questão 3.

Pode-se verificar alguns erros no uso de algumas notações, como na de divisibilidade na resposta do estudante A7, da **classe C** da questão 1.

Embora os objetivos das questões 2 e 3 tenham sido atingidos, pode-se observar que alguns estudantes utilizaram a notação de congruência módulo m de forma equivocada, ou apenas para dar a resposta da questão, ou não a utilizaram. Certamente, o uso da notação de um conceito não é garantia de que ele tenha sido bem compreendido, mas saber usar a notação faz parte da aprendizagem de qualquer conceito.

Findell (2001) enfatiza que a compreensão dos conteúdos matemáticos pelos estudantes está intimamente ligada à linguagem, notação e metáforas utilizadas por eles e por seus professores. A notação $\pmod{m}$, segundo este autor, tem uma ambiguidade em seu significado: por um lado denota uma relação de equivalência, $a \equiv b \pmod{m}$; por outro, uma operação binária, $a \bmod m = b$. Ele considera, ainda, um terceiro uso, que seria uma generalização da congruência módulo m, a congruência módulo H, sendo H um subgrupo normal, e que esta ambiguidade pode dificultar o entendimento da construção do grupo quociente $\mathbb{Z}/n\mathbb{Z}$.

No caso desta pesquisa, esta ambiguidade parece não ter afetado os estudantes pesquisados, pois, diferentemente da pesquisa de Findell, eles utilizaram o termo *mod* significando uma relação de equivalência, como pode-se verificar principalmente nas respostas da questão 1 e 3. Isso se deve ao fato de que, nos livros textos utilizados e nas aulas, esta ambiguidade não aconteceu, o termo mod m foi utilizado apenas para denotar a congruência módulo m.

Agora, quando a noção de classe de equivalência está envolvida, nota-se dificuldades para responder a questão, já que apenas quatro estudantes responderam a questão 4 corretamente. As respostas dessa questão sugerem que existe dificuldade na compreensão da noção de partição de conjunto, na escolha do representante da classe e no uso de símbolos básicos de Teoria de Conjuntos.

O fato de as dificuldades começarem a aparecer quando a noção de classe de equivalência ou, no caso, de congruência está envolvida, vem ao encontro do que foi constatado por Dubinsky e seus colaboradores (1994) e Asiala e seus colaboradores (1997), que concordam que encapsular o processo de formação de classes em objeto é muito difícil. Os primeiros acreditam, ainda, que as dificuldades no entendimento da Teoria de Grupos começam quando os conceitos relacionados ao Teorema de Lagrange e grupo quociente, ou seja, classes laterais, normalidade e operações entre classes laterais, são apresentadas aos estudantes. Apesar desses conceitos não estarem envolvidos na presente pesquisa, o que se chama de classes laterais são, na verdade, classes de equivalência, como é o caso das classes de congruência módulo m. Asssim pode-se considerar os resultados apresentados por estes autores.

Embora as respostas das **classes C** e **D** da questão 4 sugiram uma dificuldade em trabalhar com os representantes da classe, pois a maioria dos estudantes responderam que $\overline{10} \notin \mathbb{Z}_7$, pois $\mathbb{Z}_7$ tem apenas 7 elementos, mesmo admitindo que $\overline{10} = \overline{3}$, esta dificuldade não será considerada, pois o enunciado da questão pode ter induzido esta resposta, e porque os estudantes, provavelmente, não trabalharam com representantes de classe dessa forma, mesmo em disciplinas anteriores.

Considerando, então, que uma dificuldade pode ser percebida pelos erros cometidos por várias pessoas, pode-se considerar, de acordo com as respostas dos estudantes, que foi possível identificar a seguinte dificuldade:

Dificuldade em reconhecer a partição induzida pela relação de congruência módulo m sobre $\mathbb{Z}$.

As respostas que sugerem esta dificuldade são as da questão 4, principalmente nas respostas do item a), quando, para justificar que $10 \in \mathbb{Z}_7$, os estudantes afirmaram que $10 \in \mathbb{Z}_7$, pois $10 \in \overline{3}$ e $\overline{3} \in \mathbb{Z}_7$. Este argumento é semelhante ao que os estudantes da pesquisa de Lajoie e Mura (2004) usaram para responder a questão: *Seja* $\{S_1, S_2, ..., S_n\}$ *uma partição de um conjunto* E *e seja* x *um elemento de* E*. Podemos afirmar que* $x \in \{S_1, S_2, ..., S_n\}$*? Justifique sua resposta.* (ibid, p. 61).

Este argumento também é semelhante aos das respostas a esta mesma questão, dadas por estudantes da UFPR, veja Apêndice B. Uma das respostas obtidas nestas duas ocasiões foi que o elemento x do conjunto E pertence a $\{S_1, S_2, ..., S_n\}$, pois sendo $\{S_1, S_2, ..., S_n\}$ uma partição de um conjunto E, então $E = S_1 \bigcup S_2 \bigcup ... \bigcup S_n$, logo $x \in S_i$, para algum $i = 1, 2, ...n$, e portanto $x \in \{S_1, S_2, ..., S_n\}$. Esta resposta indica confusão entre as relações de pertinência e inclusão, pois, para eles, se $x \in S_i$, para algum $i = 1, 2, ..., n$, então $x \in \{S_1, S_2, ..., S_n\}$.

Eles não se deram conta de que os elementos da partição são subconjuntos de E, ou seja, que uma partição de E está contida no conjunto das partes de E.

Lajoie e Mura (2004) referem-se a estes erros como sendo a dificuldade em distinguir as relações de pertinência (de um elemento para um conjunto) e inclusão (de um conjunto para outro conjunto). Elas entendem que mais do que uma simples confusão, estes erros podem ser explicados, pois é difícil considerar um conjunto, no caso uma classe, como um objeto, ou seja, como um elemento de outro conjunto.

Observei esta mesma confusão, com os símbolos $\in$ e $\subset$, nas respostas das **classes B** e **C** questão 4. Este tipo de erro, segundo Traoré, Lajoie e Mura (2007) acontece devido à dificuldade de conceber um conjunto como objeto distinto de seus elementos. Este erro categorizado pelas autoras é um erro do tipo T1, que consiste em trocar o sentido das relações de pertinência e inclusão, apresentado no Capítulo 3, reforçando a ideia de Lajoie e Mura (2004) sobre considerar um conjunto como objeto.

De minha parte, entendo que estes erros não acontecem apenas por uma confusão com os símbolos ($\in$ e $\subset$), mas porque os estudantes podem não saber a definição de partição de um conjunto, ou não reconhecem as classes de congruência módulo m como uma partição de $\mathbb{Z}$, ou não conhecem a relação entre a relação de equivalência e a partição de um conjunto.

Isso pode ser notado nas respostas de dois estudantes entrevistados, para os quais a questão descrita acima foi apresentada, veja questão 3 no Apêndice D; elas

foram as seguintes:

> **E2:** "Eu acredito que não necessariamente, porque, se por exemplo você tem um conjunto e você pega esse complementar. Se a gente diz que x é um elemento de E e a gente pega uma certa partição, a gente pode ter tanto elemento de E coincidentemente caindo lá ou fora. Então a gente calcula o complementar em relação a esta partição. Essa parte que nos resta pode conter o x se não for especificado nenhuma propriedade adicional...."
>
> **P:** "O que você está entendendo por partição?"
>
> **E2:** "Aqui o caso, como partição estou entendendo como uma subdivisão desse conjunto, como se fosse um subconjunto".

Este estudante entende que partição de um conjunto é um subconjunto do mesmo, e que é possível, então, calcular o seu complementar, e, neste caso, o elemento x pode ou não pertencer à partição. Já o estudante E3 parece entender a noção de partição, pois ele respondeu:

> **E3:** "Não ele não é. x é um elemento do conjunto E, agora esse conjunto aqui $[\{S_1, S_2, ..., S_n\}]$ é um conjunto de conjunto, de subconjuntos de E, então não faz sentido".

Observei por estas respostas e pelas respostas da questão 4 do questionário, principalmente das **classes B e C**, que os estudantes podem, de fato, não saber a definição de partição de um conjunto. Isso pode levá-los a não compreender integralmente a noção de anel quociente e grupo quociente. Segundo Lajoie e Mura (2004), não entender a noção de partição pode levar o estudante a não entender que os elementos de G/N, do grupo quociente, formam uma partição do gupo G. No caso da presente pesquisa, pode-se pensar que, se o estudante não entende a noção de partição de um conjunto, ele não entenderá $\mathbb{Z}_m$ como partição de $\mathbb{Z}$, o que poderá levá-lo a entender, por exemplo, que $10 \in \mathbb{Z}_7$, que foi o que ocorreu neste questionário.

Isso sugere, então que existe uma falha no conhecimento dos estudantes sobre as noções preliminares de teoria de conjunto, noções que estão envolvidas na noção de congruência, o que reforça a hipótese de pesquisa.

5.2 Das questões sobre o anel quociente $\mathbb{Z}/m\mathbb{Z}$

Esta seção tem como objetivo responder a seguinte questão associada ao segundo objetivo específico desta pesquisa, apresentado na seção 1.4:

Quais as dificuldades encontradas pelos estudantes, ao responderem questões sobre anel quociente $\mathbb{Z}_m$?

5.2.1 Classificação e primeira análise das respostas dos estudantes

Nesta seção, será apresentada uma descrição detalhada das respostas dos estudantes a cada questão e as considerações sobre as mesmas, de acordo com o objetivo de cada uma delas. Nas análises destas questões, para considerá-las corretas ou não, foi levado em conta, o que foi ensinado em sala de aula, utilizando as notações e as definições dadas pelo professor e pelo livro texto utilizado. Não estou com isso afirmando que estas sejam mais adequadas ou não, este é apenas o cenário em que os dados foram colhidos.

Questão 1

Considere o anel $\mathbb{Z}_{18}$ e seu subanel $J = \overline{3}\mathbb{Z}_{18} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$. Justifique suas respostas.

i) Quais são os elementos do anel quociente $\mathbb{Z}_{18}/J$?

ii) Qual é o elemento identidade de $\mathbb{Z}_{18}/J$?

iii) Encontre um anel familiar que seja isomorfo a $\mathbb{Z}_{18}/J$.

Os objetivos desta questão eram verificar se os estudantes conseguem construir um anel quociente, identificar alguns dos seus elementos e reconhecer um anel isomorfo a outro.

A escolha do anel quociente $\mathbb{Z}_{18}/J$ foi feita por ele ser isomorfo a $\mathbb{Z}_3$, sua construção requer que o estudante tenha entendido o conceito de classe de congruência e o processo de construção de um anel quociente.

A resposta dessa questão é $\mathbb{Z}_{18}/J = \{\overline{0} + J, \overline{1} + J, \overline{2} + J\}$. Os elementos desse anel são as classes cujos elementos são:

$$\overline{0} + J = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$$

$$\overline{1} + J = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}, \overline{13}, \overline{16}\}$$

$$\overline{2} + J = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}, \overline{14}, \overline{17}\}$$

O elemento identidade é o elemento $\overline{1}+J$. O anel quociente $\mathbb{Z}_{18}/J$ é isomorfo ao anel $\mathbb{Z}_3$.

Dos vinte e sete (27) estudantes que responderam este questionário, apenas nove (09) responderam esta questão e dezoito (18) estudantes (Q2, Q6, Q7, Q8, Q9, Q10, N6, N7, N8, N9, N10, N11, N12, N13, N14, N15, N16, N17) não responderam.

O quadro abaixo, a seguir, mostra os estudantes que responderam a todos os itens desta questão ou apenas alguns deles.

Respondeu aos itens	i), ii), iii)	i) e ii)	i) e iii)	apenas i)
Estudante	N1, N2, Q3	N4, N3	Q1	Q4, Q5, N5

Quadro 5.5: Distribuição dos estudantes de acordo com os itens respondidos da questão 1

Dos estudantes que responderam esta questão, oito (8) deles responderam ao item i) da questão, estas respostas foram agrupadas nas **classes A** e **B**; as cinco (5) respostas ao item ii) nas **classes C** e **D**; e as quatro (4) respostas, ao item iii) nas **classes E** e **F**, como mostra o quadro abaixo.

Classe	Subclasse	Estudantes	Tipo de resposta
A		N2, N3	item a) $\mathbb{Z}_{18}/J=\{\overline{0},\overline{1},\overline{2}\}$
B	B1	Q5, N5	item a) $\mathbb{Z}_{18}/J=\overline{3}\mathbb{Z}_{18}$
	B2	Q4, N4	item a) $\frac{\mathbb{Z}_{18}}{\overline{3}\mathbb{Z}}=\frac{\{\overline{0},\overline{3},\overline{4}...,\overline{17}\}}{\{\overline{0},\overline{3},\overline{6}...,\overline{15}\}}=\{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8},\overline{10},\overline{11},\overline{13},\overline{14}\}$
	B3	Q1, Q3	item a) ideia de interseção de $\mathbb{Z}_{18}$ com $\overline{3}\mathbb{Z}$
C		N4, N1	item b) identidade é $\overline{0}$ ou $\overline{3}$
D		Q3, N2, N3	item b) a identidade é $\overline{1}$
E		Q1, N2	item c) $\mathbb{Z}_{18}/J\cong\mathbb{Z}_3$
F		N1, Q3	item c) $\mathbb{Z}_{18}/J\cong\mathbb{Z}_6$ ou $\mathbb{Z}_{18}/J\cong\mathbb{Z}$

Quadro 5.6: Classes da questão 1

Classe A: Corresponde a duas (2) respostas ao item a) consideradas parcialmente corretas. Nestas duas respostas, os estudantes N2 e N3, escreveram $\mathbb{Z}_{18}/J=\{\overline{x},x\in\mathbb{Z}_{18}\}=\{\overline{0},\overline{1},\overline{2}\}$, N2 ainda explicou que: "$\overline{1}\in\mathbb{Z}_{18}$, $\overline{4}\in\mathbb{Z}_{18}$ e $\overline{4}-\overline{1}=\overline{3}\in J\Rightarrow\overline{4}$ e $\overline{1}$ são as mesmas classes". Essas respostas apontam que esses estudantes compreenderam o processo de construção de um conjunto quociente.

A notação utilizada por eles, $\mathbb{Z}_{18}/J = \{\overline{0}, \overline{1}, \overline{2}\}$, não é adequada, pois $\overline{0} \in \mathbb{Z}_{18}/J$ não é o mesmo $\overline{0} \in \mathbb{Z}_{18}$, eles deveriam ter feito esta diferenciação.

Classe B: Corresponde a seis (6) respostas ao item a) consideradas incorretas. Estas respostas podem ainda ser agrupadas em subclasses em que as justificativas são semelhantes.

Subclasse B1: Corresponde a duas (2) respostas, dos estudantes Q5 e N5, que responderam "$\mathbb{Z}_{18} = (\overline{0}, \overline{3}, ..., \overline{15})$" e que "$\mathbb{Z}_{18}/J = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$", respectivamente, mas este conjunto é o próprio $J = \overline{3}\mathbb{Z}_{18}$.

Subclasse B2: Corresponde a duas (2) respostas, dos estudantes Q4 e N4, que entenderam o anel quociente $\mathbb{Z}_{18}/J$ como sendo o "quociente" dos elementos destes dois conjuntos, N4 escreveu: "$\frac{\mathbb{Z}_{18}}{3\mathbb{Z}} = \frac{\{\overline{0},\overline{3},\overline{4}...,\overline{17}\}}{\{\overline{0},\overline{3},\overline{6}...,\overline{15}\}} = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{14}\}$".

Esses estudantes cancelaram os elementos comuns nestes dois conjuntos. Eles fizeram um quociente entre dois conjuntos, como se estivessem fazendo o quociente entre dois números.

Subclasse B3: Corresponde a duas (2) respostas, que não se encaixam nas demais. O estudante Q1 respondeu que $\mathbb{Z}_{18}/J = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, porque são os elementos comuns a $\mathbb{Z}_{18}$ e J. Este estudante entendeu a noção de conjunto quociente como sendo a interseção entre dois conjuntos. E o estudante Q3 respondeu apenas que "$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \mathbb{Z}_{18}/J$", sem dar nenhuma justificativa. O anel descrito acima pelo estudantes Q3 é o anel $\mathbb{Z}_6$, que não é isomorfo ao anel quociente em questão.

Classe C: Corresponde a duas (2) respostas dadas ao item ii). Esses estudantes disseram que o elemento identidade é $\overline{0}$ ou $\overline{3}$; apenas um deles, N1, justificou dizendo que era porque $mdc(18, 3) = 3$. Essas respostas podem ter ocorrido porque $\overline{0}$ é o elemento neutro dos anéis do tipo $\mathbb{Z}_m$, e então seria deste também.

Classe D: Corresponde a três (3) respostas em que os estudantes encontram a unidade de $\mathbb{Z}_{18}/J$, isto é, o elemento $\overline{1}$. Das respostas agrupadas nesta classe, apenas o estudante N2 justificou sua resposta da seguinte forma:

$$\text{" } \overline{1} \text{ pois } a \in \mathbb{Z}_{18}/J, a \neq \overline{0} \Rightarrow a = \overline{1} \text{ ou } \overline{2} \text{ e}$$
$$\overline{1} \cdot \overline{1} = \overline{1} \cdot \overline{1} = \overline{1}$$
$$\overline{2} \cdot \overline{1} = \overline{1} \cdot \overline{2} = \overline{2}\text{".}$$

Classe E: Corresponde a duas (2) respostas ao item c) da questão. Estes estudantes responderam que $\mathbb{Z}_{18}/J \cong \mathbb{Z}_3$, mas apenas um deles, Q1, justificou que eles

"têm os mesmos elementos".

Classe F: Corresponde a duas (2) respostas consideradas incorretas. As respostas desta classe foram dadas pelos estudantes Q3 e N3, que responderam, respectivamente, que $\mathbb{Z}_{18}/J$ é isomorfo a $\mathbb{Z}_6$ e a $\mathbb{Z}$, ambas sem justificativas. Essas respostas não esclarecem como os estudantes pensaram para resolver esta questão. Pode-se pensar que eles não entenderam o que é um conjunto quociente, nem o processo para sua construção, por isso responderam dessa forma.

Primeiras Análises

Esperava-se que mais pessoas respondessem a esta questão, pois a construção deste anel quociente é análoga à construção do anel $\mathbb{Z}/3\mathbb{Z}$, por exemplo, a diferença está nos elementos do conjuntos envolvidos. Este baixo número de respostas pode ter acontecido por ter sido utilizado em seu enunciado o anel $\mathbb{Z}_{18}$ do qual se quer encontrar o anel quociente $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18}$. Esta questão pode ter sido considerada difícil por alguns estudantes, pois os elementos do anel de partida são classe de congruência módulo 18, e os elementos do anel quociente seriam então classes de congruência cujos elementos também são classes. E este raciocínio não é usual para eles, já que este anel quociente não é, em geral, utilizado nos livros e em sala de aula.

Para resolver essa questão, era necessário que estivesse claro para o aluno o que é um anel quociente, seus elementos e a sua construção, para que ele pudesse fazer a analogia para construção do anel quociente, cujos elementos do anel de partida, $\mathbb{Z}_{18}$, são classes de congruência.

As respostas das **classes C** e **D**, em que os estudantes afirmam que a identidade de $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18}$ é $\overline{0}$ e $\overline{1}$, respectivamente, podem estar refletindo um problema com a nomenclatura do elemento neutro.

Alguns autores, como Rotman e Gonçalves, utilizam o termo identidade para nomear o elemento neutro de um grupo com qualquer operação. No caso do $\mathbb{Z}_m$, como ele é um grupo aditivo, o elemento $\overline{0}$ é a identidade do grupo. Gonçalves (1979), na definição de anel, chama de unidade o elemento neutro da multiplicação e de elemento neutro da adição o $\overline{0}$.

Outros autores, como Garcia e Domingues, utilizam o termo identidade para nomear o elemento neutro da multiplicação. Um exemplo ilustrativo desse elemento é a matriz identidade. No caso do anel $\mathbb{Z}_m$, a identidade é o elemento $\overline{1}$.

Em ambos os casos, o termo identidade está relacionado ao elemento neutro das operações e o que se deve fazer para provar que um elemento do anel A é o neutro (tanto da adição quanto da multiplicação), é mostrar que para todo $a \in A$ existe um elemento $\varepsilon \in A$, tal que $a * \varepsilon = a = \varepsilon * a$. Esta semelhança na definição e no procedimento, para demonstração, pode ter contribuído para as respostas das **classes C** e **D**.

Como os estudantes, que responderam esta questão, ainda não estudaram grupos, o termo identidade está ligado ao elemento neutro da multiplicação, como no caso da matriz identidade e identidade da multiplicação no conjunto dos números reais, as respostas consideradas corretas são as da **classe D**.

Nas respostas a esta questão pode se observar alguns erros na linguagem matemática, como, por exemplo, escrever um conjunto utilizando parênteses, **subclasse B1**. Algumas respostas indicam, ainda, que alguns estudantes entenderam um anel quociente como interseção de conjuntos, como na **subclasse B3**, como quociente numérico como nas respostas da **subclasse B2**, e mesmo como sendo o próprio ideal.

Em Lajoie e Mura (2004), as autoras chamam a atenção para a fragilidade das definições pessoais de seus estudantes, e que podem ser agravadas por estratégias como fixar-se em exemplos familiares ou apegar-se as impressões visuais das definições, podendo gerar controvérsias com as definições formais. Outra estratégia identificada por elas é fazer ligações com noções familiares, como, por exemplo, fazer relações entre grupo quociente e o quociente aritmético, como um de seus estudantes, que disse que $\mathbb{Z}/2\mathbb{Z}$ é como se fosse $\mathbb{Z}$ dividido em dois, ou, ainda, que compondo $\mathbb{Z}/2\mathbb{Z}$ por $2\mathbb{Z}$ tem-se como resultado o próprio $\mathbb{Z}$. Na pesquisa que realizei, pude observar respostas semelhantes a estas, em que o anel quociente foi entendido como quociente aritmético, como, por exemplo, em algumas respostas da **classe B**.

Considerando que apenas dois estudantes responderam a questão 1 de forma satisfatória, conclui que os objetivos da questão de construir um anel quociente, identificar alguns dos seus elementos e reconhecer um anel isomorfo a outro, não foram alcançados. Isso porque que os estudantes não entenderam o processo de construção de um anel quociente, a ponto de conseguirem construir o anel $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18}$. Também não conseguiram verificar qual o elemento unidade do anel quociente e identificar um anel isomorfo a ele.

Questão 2

Qual polinômio abaixo é igual ao polinômio $f(x) = \overline{3}x^4 + \overline{2}x^3 + \overline{1}x^2 + \overline{4}$ *de* $\mathbb{Z}_5[x]$*? Justifique sua resposta.*

i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \overline{1}x^2 + \overline{0}$ *de* $\mathbb{Z}_5[x]$.

ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ *de* $\mathbb{Z}_5[x]$.

iii) $l(x) = \overline{8}x^4 - \overline{3}x^3 + \overline{16}x^2 + \overline{9}$ *de* $\mathbb{Z}_5[x]$.

O objetivo desta questão era verificar se o aluno consegue trabalhar com os elementos do anel quociente e reconhecer os elementos do anel quociente como objetos, isto é, trabalhar com as classes de congruência módulo 5, independente do representante.

A resposta dessa questão é o polinômio *iii)* $l(x) = \overline{8}x^4 - \overline{3}x^3 + \overline{16}x^2 + \overline{9}$ *de* $\mathbb{Z}_5[x]$, pois tem-se a igualdade das classes $\overline{3} = \overline{8}$, $\overline{2} = -\overline{3}$, $\overline{1} = \overline{16}$ e $\overline{4} = \overline{9}$.

Esta questão foi respondida corretamente pelos vinte e sete (27) estudantes que responderam este questionário. As justificativas encontradas estão organizadas nas classes a seguir:

Classe	Estudantes	Tipo de resposta
A	Q1, Q2, Q3, Q4, Q7, Q10, N1, N3, N4, N6, N9, N11, N12, N13, N16, N17	igualdade de classes de congruência módulo 5
B	Q5, Q9, N1, N7, N8, N14, N15	noção ou notação de congruência módulo 5
C	Q6, Q8, N5, N10	resto de divisão por 5

Quadro 5.7: Classes da questão 2

Classe A: Corresponde a dezesseis (16) respostas, em que foi utilizada a igualdade de classes de congruência para a justificativa. Como, por exemplo, a de N13 que respondeu: "...em $\mathbb{Z}_5 \rightarrow \overline{8} = \overline{3}, \overline{-3} = \overline{2}, \overline{16} = \overline{1}, \overline{9} = \overline{4}$...". Respostas como esta mostram que o estudante consegue trabalhar com as classes de congruência. Já o estudante N2, apesar de usar igualdade de classes, escreveu " $\overline{8} = \overline{3}$ (mod 5)" e também errou ao afirmar que as classes de congruência estavam em "$\mathbb{Z}_5(x)$", quando o correto seria $\mathbb{Z}_5$. Este erro pode ter ocorrido porque os polinômios estão em $\mathbb{Z}_5[x]$ e ele concluiu que os coeficientes também estão. O estudante N9, para justificar que não poderia ser o

polinômio $h(x)$, escreveu: " $\overline{1}x^3 \neq \overline{2}x^3$", o que indica, que apesar de usar a classe corretamente, a igualdade de polinômios não foi utilizada corretamente.

Classe B: Corresponde a sete (7) respostas, em que a justificativa foi feita utilizando a noção e a notação de congruência módulo 5. Como, por exemplo, o estudante Q9, que escreveu em sua resposta "Temos que $8 \equiv 3 \pmod 5$, pois $8-3$ divide 5, pelo mesmo argumento, $-3 \equiv 2 \pmod 5, 16 \equiv 1 \pmod 5, 9 \equiv 4 \pmod 5$..." então $f(x) = l(x)$.

Os estudantes N7 e N14 usaram congruência, mas utilizando as classes de congruência e não os números inteiros, da seguinte maneira, $\overline{8} \equiv \overline{3} \pmod 5$. Esta resposta indica uma confusão entre as classes e seus representantes.

Classe C: Corresponde a quatro (4) respostas, em que os estudantes utilizaram o resto da divisão para justificar a sua escolha, como a do estudante N5, que escreveu: "iii) pois os restos das divisões dos coeficientes por 5 têm restos iguais ao polinômio $f(x)$", ou seja, ele dividiu os coeficientes por 5 e viu que os restos são iguais aos restos da divisão dos coeficientes do polinômio $f(x)$ por 5, embora sua afirmação tenha ficado confusa.

O estudante Q6 escreveu "...é a (iii) porque o polinômio $l(x)$ de $\mathbb{Z}_5[x]$, analisando seus coeficientes, terão os mesmos restos com os respectivos coeficientes de $f(x)$ quando divididos por 5". Já o estudante N10 usou, também, o resto da divisão, mas utilizou para divisor e resto a notação de classe e para dividendo e quociente a notação de número inteiros, ou seja, $\overline{8} \div 5 = 1 + \overline{3}$. Ele parece ter entendido que é o resto da divisão que justifica o que ele pensou, mas parece não entender a diferença entre números e classes, ou seja, a natureza destes objetos, já que está efetuando a divisão com os dois.

Primeiras Análises

Chama a atenção nestas respostas o fato de alguns estudantes terem utilizado a notação de classe de congruência, como $\overline{8}$ e a de números inteiros, como 5, para efetuar as operações, como, por exemplo, $\overline{8} \div 5 = 1 + \overline{3}$, ou quando o estudante escreveu congruência de classes módulo 5, como $\overline{8} \equiv \overline{3} \pmod 5$. Certamente, entende-se que ele está dividindo oito por cinco para tomar o resto, e que $\overline{8} = \overline{3}$ em $\mathbb{Z}_5$. O problema é se o estudante entende o que está escrito e o que ele está querendo dizer.

Se o estudante tomasse $\mathbb{Z}_5$ como o conjunto dos restos da divisão de números

inteiros por 5, não teria problema com a notação, pois estaria trabalhando sempre com números inteiros. Mas pensando $\mathbb{Z}_5$ como conjunto das classes de congruência módulo 5 (ou como classe de congruência módulo $5\mathbb{Z}$), como foi apresentado aos estudantes em sala de aula, ele está lidando com objetos matemáticos diferentes, um é um conjunto de números inteiros e outro é um número inteiro, e, então, pode-se perguntar, se faz sentido o que estes estudantes escreveram.

Embora todos os estudantes tenham respondido esta questão corretamente, ou seja, responderam que o polinômio do item *iii)* é igual a $f(x) = \overline{3}x^4 + \overline{2}x^3 + \overline{1}x^2 + \overline{4}$ em $\mathbb{Z}_5[x]$, suas justificativas mostram que eles podem não estar utilizando a classe de congruência módulo m corretamente. O objeto classe de congruência parece não ter sido aprendido por eles, pois eles tomaram a igualdade $\overline{a} = a$. No entanto, entendo que o objetivo desta questão de trabalhar com as classes de congruência módulo 5, independente do representante foi atingido, porém, deve-se observar que eles não empregaram uma notação adequada.

Questão 3

Os elementos de $\mathbb{Z}/3\mathbb{Z}$ podem ser elementos de $\mathbb{Z}$? Justifique sua resposta.

O objetivo desta questão era verificar se o aluno consegue distinguir classe de equivalência de números inteiros do conjunto dos números inteiros.

A resposta para esta questão é que os elementos de $\mathbb{Z}/3\mathbb{Z}$ não podem ser elementos de $\mathbb{Z}$, pois os elementos de $\mathbb{Z}/3\mathbb{Z}$ são classes de congruência módulo 3, enquanto os elementos de $\mathbb{Z}$ são números inteiros.

Esta questão foi respondida por onze (11) estudantes e dezesseis (16) (N4, N5, N7, N8, N10, N12, N13, N14, N15, N16, N17, Q2, Q6, Q7, Q9, Q10) deixaram de responder. As respostas foram agrupadas em classes de acordo com o tipo de justificativa utilizado pelo aluno.

Classe	Estudantes	Tipo de resposta
A	N2, N3, Q4	os elementos de $\mathbb{Z}/3\mathbb{Z}$ são classes de congruência módulo 3 enquanto, os elementos de $\mathbb{Z}$ são números inteiros
B	N1, N9	os elementos de $\mathbb{Z}/3\mathbb{Z}$ pertencem a $\mathbb{Q}$
C	N6, N11, Q1, Q3, Q5, Q8	os elementos de $\mathbb{Z}/3\mathbb{Z}$ são elementos de $\mathbb{Z}$, pois $\mathbb{Z}/3\mathbb{Z} = 3\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$ é subanel de $\mathbb{Z}$

Quadro 5.8: Classes da questão 3

Classe A: Corresponde a três (3) respostas com justificativa considerada correta. Estes estudantes responderam que não, pois os elementos dos conjuntos não são os mesmos. O estudante Q4 respondeu: "Não. Os elementos do anel quociente são classes de equivalência e não inteiros". Os estudantes N2 e N3 escreveram " Não, pois $\mathbb{Z}$ contém inteiros e $\mathbb{Z}_3$ contém classes". Este tipo de resposta indica que esses alunos parecem entender a natureza destes objetos.

Classe B: Corresponde a duas (2) respostas, em que os estudantes, apesar de responderem que não é possível que os elementos de $\mathbb{Z}/3\mathbb{Z}$ sejam elementos de Z, suas justificativas estão equivocadas. Os estudantes N1 e N9 deram o mesmo tipo de justificativa. Ambos responderam que não, pois os elementos de $\mathbb{Z}/3\mathbb{Z}$ pertencem a $\mathbb{Q}$, como na resposta de N9: "$\mathbb{Z}/3\mathbb{Z}$ não podem se elementos, pois alguns elementos de $\mathbb{Z}/3\mathbb{Z} \notin \mathbb{Z} \Rightarrow \mathbb{Z}/3\mathbb{Z}[3] = \frac{1}{3} \notin \mathbb{Z}$", ou seja, para eles este anel quociente está contido no conjunto dos números racionais, o que indica que, provavelmente, eles não entenderam o que é um anel quociente. Ou, ainda, pode-se pensar que a notação utilizada nos livros textos usados como referência nas aulas Álgebra (Gonçalves, 1979; Rotman, 1996), pode ter induzido a este erro.

Classe C: Corresponde a seis (6) respostas consideradas incorretas. Estes estudantes responderam sim a esta questão, ou seja, que os elementos de $\mathbb{Z}/3\mathbb{Z}$ podem ser elementos de $\mathbb{Z}$. As justificativas para esta resposta foram variadas. Dois estudantes, Q1 e Q3, justificaram que os elementos de $\mathbb{Z}/3\mathbb{Z}$ seriam os múltiplos de 3, como o estudante Q3 ao dizer que sim e justificar que " serão coincidentes com os múltiplos de 3", ou seja, para ele $\mathbb{Z}/3\mathbb{Z} = 3\mathbb{Z}$ e, portanto, são elementos de $\mathbb{Z}$. Outros disseram que sim, porque $\mathbb{Z}$ é ideal ou subanel de $\mathbb{Z}/3\mathbb{Z}$, como Q5 que justificou escrevendo "... pois é subanel". O estudante Q8 respondeu sim à questão e escreveu que " $\mathbb{Z}$ é ideal de $\mathbb{Z}/3\mathbb{Z}$ ". Já o estudante N11 justificou dizendo que: "Os elementos $\mathbb{Z}/3\mathbb{Z}$ são

$$\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3...\}$$

$$3\mathbb{Z} = \{... - 6, -3, 0, 3, 6, 9, ...\}$$

$$\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$$

$\mathbb{Z}_3$ está contido em $\mathbb{Z}$, dessa forma todos os elementos do $\mathbb{Z}_3$ pertencem a $\mathbb{Z}$". Se este estudante estiver entendendo $\mathbb{Z}_3$ como conjunto dos restos da divisão de inteiros por 3, a igualdade $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$ não está correta, pois o que se tem aqui é um isomorfismo de anéis.

Primeiras Análises

Nota-se nas respostas da **classe C** confusão entre classes de congruência que são os elementos do anel quociente e números inteiros que são os elementos do anel de partida. Estes estudantes parecem não diferenciar a natureza destes objetos matemáticos.

Novamente aqui, como na questão anterior, pode-se notar problemas quanto à definição do anel $\mathbb{Z}_m$. No caso desta questão, a confusão está entre $\mathbb{Z}_m$ (como conjunto de restos) e $\mathbb{Z}/m\mathbb{Z}$, como no caso do estudante N11, da **classe C**, o que não deveria ocorrer, uma vez que o enunciado da questão está colocado em termos do anel quociente $\mathbb{Z}/3\mathbb{Z}$ que é definido como o conjunto das classes de congruência módulo ideal $3\mathbb{Z}$. Dessa forma, as respostas afirmativas a esta questão foram consideradas incorretas.

Ainda na **classe C**, outros estudantes afirmaram que $\mathbb{Z}/3\mathbb{Z} = 3\mathbb{Z}$, dizendo que $\mathbb{Z}/3\mathbb{Z}$ é subanel de $\mathbb{Z}$ e, portanto, seus elementos são também elementos de $\mathbb{Z}$, parecendo não entender o que é um anel quociente, quais e o que são seus elementos.

Nas respostas da **classe B**, os estudantes entendem o anel quociente como quociente numérico, já que dois estudantes escreveram que $\mathbb{Z}/3\mathbb{Z} \subset \mathbb{Q}$, da mesma forma que na **subclasse B2**, da questão 1. Isso sugere que estes estudantes viram o anel quociente apenas como quociente aritmético, que é algo familiar para eles, pois até agora quociente era o resultado da divisão de números. O que também foi observado por Lajoie e Mura (2004), como já foi dito anteriormente.

Pode-se inferir pelas respostas das **classes B** e **C** que a maioria dos estudantes não faz distinção entre os elementos de $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}$. Apenas três (3) dos onze (11) estudantes que responderam a questão atingiram o objetivo da mesma.

Questão 4

Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta.

O objetivo era verificar se os estudantes conseguiam diferenciar os elementos e as operações envolvidas em cada anel. E verificar se os estudantes conseguiam reconhecer um subanel de um anel.

A resposta desta questão é que $\mathbb{Z}_3$ não é subanel do anel $\mathbb{Z}_6$, pois os elementos e as operações dos anéis são diferentes.

Vinte e um (21) estudantes responderam esta questão e seis (6) estudantes (N3, N5, N13, N16, Q5, Q7) não responderam. As respostas foram agrupadas em classes que foram elaboradas de acordo com o tipo de justificativa apresentada, conforme o quadro abaixo e descritas em seguida.

Classe	Estudantes	Tipo de resposta
A	Q4, Q8, N2, N15	as classes de $\mathbb{Z}_3$ são de congruência módulo 3, enquanto as classes do $\mathbb{Z}_6$ são módulo 6
B	N1, N4, N8, N9, N10, N11, Q10	$\mathbb{Z}_6 \subset \mathbb{Z}_3$ ou $\mathbb{Z}_6 = 2\mathbb{Z}_3$
C	Q2, N6, N7	não é subanel, pelo fechamento das operações
D	Q1, Q3, Q9, Q6, N14, N12	é subanel, pois $\mathbb{Z}_3 \subset \mathbb{Z}_6$
E	N17	é subanel, pelo fechamento da operação

Quadro 5.9: Classes da questão 4

Classe A: Corresponde a quatro (4) respostas, em que as justificativas são consideradas corretas. Estes estudantes, Q4, Q8, N2 e N15, justificaram suas respostas, usando como argumento que os elementos dos conjuntos são diferentes, como, por exemplo, o estudante N2, que escreveu "$\overline{0}^3 \neq \overline{0}^6$, logo $\mathbb{Z}_3 \not\subset \mathbb{Z}_6$". Já o aluno Q4 justificou que "...as classes de $\mathbb{Z}_3$ são de congruência módulo 3, enquanto as classes do $\mathbb{Z}_6$ são módulo 6".

Esses estudantes perceberam que os elementos destes conjuntos são classes de congruência de módulos diferentes, e que, portanto, um não poderia estar contido no outro.

Classe B: Corresponde a sete (7) respostas, em que os estudantes, apesar de responderem não à questão, justificaram de diferentes formas que $\mathbb{Z}_6 \subset \mathbb{Z}_3$, e, portanto, $\mathbb{Z}_3$ não pode ser subanel de $\mathbb{Z}_6$, como na resposta do estudante Q10, que escreveu "Não. É ao contrário pois os elementos de $\mathbb{Z}_6$ é que estarão dentro de $\mathbb{Z}_3$". Mesmo afirmando isso, esse aluno não verificou as outras condições para que um subconjunto de um anel seja subanel.

Outro estudante, N8, disse que não "... pois $\mathbb{Z}_6$ é maior que $\mathbb{Z}_3$", provavelmente com o termo "maior que" ele se refere ao número de elementos de cada conjunto.

N10 justificou que "... $\mathbb{Z}_6$ é subanel de $\mathbb{Z}_3$, pois $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ é o conjunto dos divisores de 3. 3 é divisor de $9 \Rightarrow \overline{0}$, no entanto 6 não é divisor de 9". Este estudante, apesar de escrever os elementos de $\mathbb{Z}_3$ corretamente, ao afirmar que estes elementos são divisores de 3, demonstra que não entendeu o que é o anel $\mathbb{Z}_m$.

Já o estudante N11 disse que $\mathbb{Z}_6$ é subanel de $\mathbb{Z}_3$, "...uma vez que $\mathbb{Z}_6 = 2\mathbb{Z}_3$", provavelmente se referindo aos subanéis $3\mathbb{Z}$ e $6\mathbb{Z}$ de $\mathbb{Z}$, que são usados na construção dos anéis quocientes $\mathbb{Z}_3$ e $\mathbb{Z}_6$, respectivamente. Observa-se que esse estudante não diferenciou estes conjuntos.

Classe C: Corresponde a três (3) respostas negativas, justificadas pelo fechamento da operação, como na resposta do estudante N7: " $3 \in \mathbb{Z}_3$, $6 \in \mathbb{Z}_3$ mas $3 + 6 = 9 \notin \mathbb{Z}_6$, não é subanel", e também na resposta do estudante Q2: "Não, um contra exemplo seria $\overline{3} + \overline{3} = \overline{6} \notin \mathbb{Z}_3$ assim $\mathbb{Z}_3$ não é fechado para soma."

Classe D: Corresponde a seis (6) respostas, em que os estudantes responderam sim, e usaram como justificativa que $\mathbb{Z}_3 \subset \mathbb{Z}_6$, como, por exemplo, a do estudante Q9, que respondeu:" $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ e $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Logo $\mathbb{Z}_3 \subset \mathbb{Z}_6$ e, portanto, é subanel".

Classe E: Corresponde a uma (1) resposta afirmativa, justificada pelo fechamento da operação. O estudante N17 afirmou que Z_3 é subanel de $\mathbb{Z}_6$, pois é fechado para adição e multiplicação, embora ele não mostre nenhum argumento que o leve a concluir isso.

Primeiras Análises

Nas respostas desta questão, pode-se identificar alguns problemas na forma de escrever de alguns estudantes, como, por exemplo, nas respostas da **classe C**, em que não é possivel saber se $\overline{3} \in \mathbb{Z}_3$ ou $\mathbb{Z}_6$, e, dessa forma, não há como saber se as respostas

estão corretas, embora a ideia de testar o fechamento da operação seja correta. Outro problema observado é quanto ao representante da classe, dizer que $\overline{9} \notin \mathbb{Z}_3$, não está correto, pois $\overline{9} = \overline{0}$ em $\mathbb{Z}_3$ que é o mesmo problema encontrado na questão 4 do capítulo anterior, e está ligado ao entendimento da partição induzida sobre $\mathbb{Z}$ e ao uso do representante da classe.

Nas respostas da **classe D**, os estudantes concluíram que $\mathbb{Z}_3$ é subanel de $\mathbb{Z}_6$ apenas comparando os representantes em comum dos conjuntos, ou seja, os inteiros $0, 1, 2$. Eles não verificaram que os elementos desses conjuntos são diferentes, apesar de os representantes serem os mesmos. Também não verificaram as condições para que um subconjunto de um anel seja subanel do mesmo; mesmo que esta inclusão fosse verdadeira isso não é garantia de que o subconjunto seja subanel.

As respostas negativas a esta questão trouxeram como argumento que $\mathbb{Z}_6 \subset \mathbb{Z}_3$, e, por isso, $\mathbb{Z}_3$ não poderia ser subanel de $\mathbb{Z}_6$. O que se observa nessas respostas é que eles podem ter confundido esses conjuntos com os conjuntos $6\mathbb{Z}$ e $3\mathbb{Z}$.

As respostas da questão 4 indicam que os estudantes, em geral, não sentem necessidade de verificar as condições para que um subconjunto de um anel seja um subanel deste anel, pois nenhum estudante fez esta verificação, agindo como se a inclusão fosse condição necessária e suficiente para que um subconjunto fosse um subanel.

Pode-se concluir, então, que os estudantes não conseguiram diferenciar os elementos dos anéis quocientes e nem as operações desses anéis.

Questão 5

Como você explicaria para um aluno do primeiro ano do Curso de Matemática o que é um anel quociente? Justifique sua resposta.

Esta questão visava identificar o que os alunos entenderam sobre anel quociente. Uma resposta possível seria dizer que o anel quociente é o conjunto das classes de congruência módulo ideal I.

Dos vinte e sete (27) estudantes que responderam a este questionário, apenas onze (11) estudantes responderam esta questão e dezesseis (16) estudantes (N1, N3, N5, N6, N7, N8, N9, N10, N14, N15, N16, Q5, Q8, Q10, Q9, Q6) não responderam. As respostas foram agrupadas em classes que foram elaboradas de acordo com a explicação apresentada, conforme o quadro abaixo e descritas em seguida.

Classe	Estudantes	Tipo de resposta
A	Q2, N13, N17	não sabe o que é anel quociente
B	N2 N11, N12, Q3	noção de congruência
C	Q1, Q4	resto da divisão
D	Q7, N4	respostas que se encaixam nas anteriores

Quadro 5.10: Classes da questão 5

Classes A: Corresponde a três (3) respostas, em que os estudantes disseram que não sabem o que é anel quociente, como a resposta do estudante N13: "não sei o que é anel quociente". Os estudantes dessa classe não responderam as questões 1 e 3 desse questionário, em que era necessário que a noção de anel quociente estivesse bem estabelecida para que a resposta fosse correta, o que indica fortemente que eles, de fato, não entenderam o que é o anel quociente.

Classe B: Corresponde a quatro (4) respostas, em que a noção de congruência módulo m está presente, como na resposta do estudante N12, que escreveu: "Começaria explicando relação de congruência". Outro estudante, Q3, escreveu: "Sem dúvida, fazer primeiro uma comparação e/ou analogia à "congruência módulo m", da teoria de anéis". Dois outros estudantes não formularam corretamente suas respostas, por exemplo, N13 escreveu que " Tomemos como exemplo $\mathbb{Z}_3$, $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Anel quociente será o conjunto dos números irredutíveis em 3. Qualquer outro número adicionado a este conjunto será reduzido a algum destes elementos, quando dividido por 3 e tomado o seu resto". Este aluno descreveu como encontrar os elementos do anel quociente $\mathbb{Z}_3$, porém, usou termos como "irredutível" e "número adicionado ao conjunto", que podem ter outro significado matemático.

Classe C: Corresponde a duas (2) respostas em que a explicação é feita usando o resto da divisão, como na resposta do estudante Q4, que escreveu: "A/zA é o conjunto dos conjuntos dos restos das divisões de A pelo zA, que é o conjunto dos múltiplos de z em A", e do estudante Q1 que respondeu: "É o conjunto dos restos das divisões dos elementos dos anéis".

Estas respostas estão relacionadas, de certa forma, com a ideia de congruência módulo m, de tomar os restos da divisão por m, mas esta ideia se limita a alguns anéis, o que pode causar problemas, quando o anel em questão não for desse tipo, como, por exemplo, o anel das matrizes 2×2 com coeficientes reais.

Classe D: Corresponde a duas (2) respostas, que não se encaixam nas anteriores. São as respostas dos estudantes N4 e Q7, que escreveram, respectivamente: "Anel é um conjunto de elementos que satisfazem determinadas propriedades em operações bem definidas" e "É o conjunto com elementos de $\mathbb{Z}$, que são primos com elementos de J". Estes estudantes, provavelmente, não entenderam o que é um anel quociente; o primeiro, escreveu o que sabia sobre anel e o outro, usou a noção de número primo, que não corresponde à ideia de anel quociente.

Primeiras Análises

Como esta questão pedia para que fosse explicado para um estudante do primeiro ano o que é um anel quociente, parece que alguns destes estudantes sentiram dificuldade em explicar o que é um anel quociente no contexto do primeiro ano do curso, uma vez que sabem que um aluno do primeiro ano não teria conhecimentos matemáticos suficientes para entender o que é anel quociente, como indica o estudante Q4, cuja resposta está na **classe B**, ao escrever "...imagino que o aluno do 1^o ano não saiba o que é anel...". Mesmo assim, o que estas respostas indicam é que os estudantes que responderam ao questionário, em geral, parecem também não ter desenvolvidas as noções necessárias para o entendimento do que é um anel quociente.

Considero, porém, que as respostas a esta questão poderiam ser mais reveladoras se o enunciado pedisse para o estudante escrever o que ele entende sobre um anel quociente, ou até mesmo que definisse um anel quociente. Talvez isso pudesse trazer mais indicações de como e se os estudantes entendem esta noção.

A referência de $\mathbb{Z}/m\mathbb{Z}$ como anel quociente ocorreu pois este é o exemplo de anel mais trabalhado durante a disciplina, um outro exemplo é o anel de polinômio $\mathbb{Z}[x]$, em que a construção do anel quociente é feita de forma análoga.

Das onze (11) respostas a essa questão, a maioria delas, sete (7), relacionou o anel quociente com a congruência modulo m ou com o resto da divisão, o que sugere que o exemplo padrão de anel quociente que estes estudantes têm é o do anel quociente $\mathbb{Z}/m\mathbb{Z}$.

5.2.2 Análise e discussão dos resultados: o apoio nas entrevistas

Pretendia neste capítulo fazer uma análise das respostas dos estudantes, estando elas corretas ou não, mas os erros cometidos pelos estudantes destacaram-se sobre as respostas corretas, o que me levou a delimitar esta análise apenas aos erros identificados.

O que será feito agora é uma análise das respostas dos estudantes aos questionários, para identificar o que eles entenderam por anel quociente.

Embora, nas questões formuladas, os anéis $\mathbb{Z}_m$ e $\mathbb{Z}/m\mathbb{Z}$ tenham sido considerados iguais, conforme foi visto no capítulo 2, as respostas dos estudantes mostram que nem todos os estudantes têm esta ideia sobre o anel quociente.

Como nas respostas à questão 1 do questionário sobre congruências módulo m, a definição de congruência módulo m foi escrita pelos estudantes, esperava-se como resposta na questão 5, deste questionário, que os estudantes definissem o anel quociente. A resposta mais simples e objetiva que se esperava é que um anel quociente é o conjunto das classes de congruência módulo um ideal I. No entanto, as respostas a esta questão revelaram que os estudantes têm como exemplo padrão de anel quociente o anel $\mathbb{Z}_m$, pois a maioria dos estudantes fez referência à congruência módulo m, ou ao resto da divisão, como mostram as respostas da **classe B**, da referida questão.

O fato dessa referência ao anel quociente $\mathbb{Z}_m$ ter ocorrido, deve-se provavelmente, porque eles foram apresentados a este conceito dessa forma, ou seja, primeiro eles estudaram a congruência módulo m, depois a generalização desta relação para a congruência módulo um ideal, em que o principal exemplo é o anel $\mathbb{Z}_m$, como em Gonçalves (1979). Também pode ter sido porque os exemplos mais usados na disciplina Teoria de Anéis são o $\mathbb{Z}_m$ e os anéis quocientes construídos a partir de anéis e polinômios, que envolvem o resto da divisão.

Na **classe B** da questão 1, encontrei respostas que me levam a crer que os estudantes entendem um anel quociente como sendo um "quociente " dos elementos desses conjuntos, e esta mesma ideia de anel quociente pode ser identificada nas respostas da **classe B** da questão 3, em que o anel $\mathbb{Z}/3\mathbb{Z}$ é visto como um subconjunto de $\mathbb{Q}$. Outros estudantes, cujas respostas estão nesta mesma classe, entendem o anel quociente como o próprio ideal.

A compreensão da noção de anel quociente também foi explorada por meio de entrevista com três estudantes que cursavam a disciplina de Teoria de Grupos, no ano de 2008. No decorrer da entrevistas, para explorar mais o entendimento desses estudantes sobre esta noção, foi feita a questão "o que você entende por anel quociente". Abaixo seguem os extratos das entrevistas em que eles explicam isso:

> "**E1:** O quociente é alguma coisa relacionada com classes laterais, alguma coisa assim, que eu não..."
>
> **E2:** "Eu entendi o seguinte, quando a gente obtém um anel que é quociente de dois anéis, a gente está querendo estabelecer o seguinte, é os representantes que no caso a gente pode chamar de classes. E qual seria a função de cada uma dessas classes? De certa forma representar qual a nossa operação, que a gente está fazendo aqui, por exemplo, a gente tem um conjunto dos inteiros e a gente está quocientando por $6\mathbb{Z}$, aqui em baixo, a gente já tem um conjunto de todos os números inteiros que passariam a ser múltiplos de seis [referindo-se ao anel quociente $\mathbb{Z}_6$ construído anteriormente]. Então quando a gente tivesse esse quociente a gente teria uma ideia parecida então a gente está dividindo..."
>
> **E3:** "Eu entendo como sendo um conjunto formado por elementos onde cada elemento é um subconjunto de uma partição, uma célula da partição e esse cara tem uma estrutura algébrica, alguma estrutura."

Observei nesses extratos que a ideia do que seja um anel quociente parece estar clara apenas para o estudante E3, poi ele conseguiu verbalizar de forma geral a ideia do que seja um anel quociente; o estudante E1 parece se lembrar que a definição tem algo a ver com classes laterais, mas não soube dar uma ideia do que fosse esta noção. No extrato da entrevista do estudante E2, há também a ideia de que é necessário haver uma classe para se ter um anel quociente, embora esse estudante recorra ao anel $\mathbb{Z}/6\mathbb{Z}$, e à necessidade de dividir dois números e tomar o resto para encontrar a classe, ele não manifesta um entendimento geral sobre o assunto.

A pesquisa de Hazzan (1999) destaca a tendência dos estudantes em tornar algo não familar em algo familiar. Ele verificou que esta tendência em relação à noção de grupos é a de se referir a um grupo qualquer, por meio de números e operações numéricas, que são objetos matemáticos com os quais eles têm mais familiaridade. Segundo esse autor isso se deve por um tentativa do estudante de tornar mais familiar (concreto) o que lhe é desconhecido (abstrato), para reduzir o nível de abstração e assim se tornarem capazes de manipulá-los cognitivamente. Esta redução não deve ser vista como um processo mental que resulta em uma ideia equivocada ou em erros

matemáticos, embora isso possa ocorrer. Esta tentativa de reduzir o nível de abstração foi identificada nesta pesquisa no caso dos estudantes que recorreram ao anel quociente $\mathbb{Z}/m\mathbb{Z}$ ou à congruência módulo m para responder a questão 5.

Do que foi discutido acima e nas respostas à questão 5, a maioria dos estudantes apresentou como padrão de anel quociente o anel $\mathbb{Z}_m$, cujos elementos são classes, que podem ser pensadas como números inteiros, obtidas encontrando o resto da divisão de um número por m. Ou seja, eles parecem não ter entendido o anel quociente como classe de congruência módulo ideal I. Essa ideia do que é um anel quociente parece ter influenciado na forma como as questões foram respondidas, tanto nos questionários quanto nas entrevistas.

No capítulo 2 o anel $\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$ foi apresentado como isomorfo ao anel quociente $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, .., \overline{m-1}\}$, e os elementos do anel quociente puderam ser vistos como classe de congruência módulo m ou módulo ideal $m\mathbb{Z}$. Nesta pesquisa, durante todo o processo de formulação de questões e coleta de dados, o $\mathbb{Z}_m$ foi por mim usado como anel quociente, mas durante as análises observei que os estudantes, mesmo tendo sido apresentados a este anel dessa forma, ora o viam como conjunto de inteiros, ora como conjunto de classes de congruência, o que pode ter causado várias confusões.

As respostas dos estudantes, classificadas na seção anterior, sugerem que os erros cometidos dizem respeito à natureza dos elementos do anel quociente, do que é um anel quociente, do que é um subanel, do processo de construção de um anel quociente e dos representantes da classe de congruência.

Considerando, então, que uma dificuldade pode ser percebida pelos erros cometidos por várias pessoas, nas respostas dos estudantes aos questionários e também nas manifestações orais dos estudantes entrevistados, foi possível identificar as seguintes dificuldades:

1. *Dificuldade em entender a natureza dos elementos do anel quociente $\mathbb{Z}_m$.*

   Esta dificuldade pode ser identificada principalmente nas respostas dadas às questões 3 e 4 dos questionários.

   A **classe C** da questão 3 refere-se às respostas em que os estudantes escreveram que os elementos do anel quociente $\mathbb{Z}/3\mathbb{Z}$ são elementos de $\mathbb{Z}$, por considerarem que $\mathbb{Z}$ é subanel ou ideal de $\mathbb{Z}/3\mathbb{Z}$, o que não está correto, pois se isso fosse verdadeiro, ter-se-ia que $\mathbb{Z} \subset \mathbb{Z}/3\mathbb{Z}$, o que não garante que os elementos do

anel quociente são elementos de $\mathbb{Z}$. Outra justificativa encontrada foi a de que $\mathbb{Z}/3\mathbb{Z} = 3\mathbb{Z}$.

Para investigar um pouco mais sobre o que os estudantes entendem em relação à natureza dos elementos do anel quociente, a partir das respostas encontradas nos questionários, formulei a questão 2 da entrevista, a seguir apresentada:

Você concorda com algum destes argumentos? Justifique sua resposta. Se não concorda, justifique também.

i) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ *são elementos de* $\mathbb{Z}$*, pois* $\mathbb{Z}/5\mathbb{Z}$ *são múltiplos de* 5*, e, portanto, são números inteiros.*

ii) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ *não são elementos de* $\mathbb{Z}$*, porque eles são do tipo* $\frac{n}{5}$ *e, portanto, pertencem a* $\mathbb{Q}$*.*

iii) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ *não são elementos de* $\mathbb{Z}$*, porque eles são classes de equivalência e não números inteiros.*

Se você não concorda com nenhum desses argumentos, como você responderia a questão: elementos de $\mathbb{Z}/5\mathbb{Z}$ *podem ser elementos de* $\mathbb{Z}$*?.*

Sobre essas justificativas, os estudantes entrevistados disseram:

> **E3:** "O primeiro argumento [os elementos de $\mathbb{Z}/5\mathbb{Z}$ podem ser elementos de $\mathbb{Z}$, pois $\mathbb{Z}/5\mathbb{Z}$ são múltiplos de 5] para mim é falso, porque isso [$\mathbb{Z}/5\mathbb{Z}$] é um conjunto de classes e isso aqui [$\mathbb{Z}$] é um conjunto de números. O segundo também não faz sentido porque $\mathbb{Z}/5\mathbb{Z}$ não tem nada a ver com $\frac{n}{5}$. Não é essa a cara do conjunto, isso aqui é um conjunto de classes e $\mathbb{Q}$ é o conjunto de números. O terceiro [os elementos de $\mathbb{Z}/5\mathbb{Z}$ não são elementos de $\mathbb{Z}$ porque eles são classes de equivalência e não números inteiros] eu concordo porque ela é a contradição da primeira. "
>
> **E2:** "O primeiro,... o equívoco aqui é porque ele utiliza essa justificativa aqui, são mútiplos de 5,.... Agora de fato são elementos de $\mathbb{Z}$, porque a gente está tomando essa barra aqui, mas no fundo é o resto de uma divisão inteira, é um número inteiro. O segundo,... ao meu ver não podem ser escritos dessa forma $\frac{n}{5}$, não teria como. Eles [elementos de $\mathbb{Z}/5\mathbb{Z}$] podem pertencer a $\mathbb{Q}$ se a gente considerar que são $\frac{n}{1}$ mas por esta justificativa eu não concordo. [O terceiro] aí ficou aquela minha dúvida de considerar ou não, eu penso assim que como a classe de equivalência é apenas uma representação, que no fundo são restos da divisão de uma divisão inteira, eu acho que faz sentido considerar que são elementos de $\mathbb{Z}$. Porque se já não fossem elementos de $\mathbb{Z}$, não faria sentido dizer que $\mathbb{Z}$ quociente $5\mathbb{Z}$, são os restos da divisão inteira por cinco, bom se são classes de equivalência, se não são inteiros são o quê?"

O estudante E3 entende o anel quociente como conjunto de classes de congruência módulo ideal $5\mathbb{Z}$; por isso não concorda com a afirmação de que os elementos do anel quociente podem ser elementos de $\mathbb{Z}$. Enquanto o estudante E2 entende o anel quociente como conjunto de restos da divisão por 5; portanto, concorda com tal afirmação. A ideia de classe de equivalência que ele tem é que estas classes são elementos que podem ser dispostos em ciclos. E o anel quociente seria o conjunto das classes, ou seja, "os restos da divisão inteira pelo nosso cinco" (estudante E2).

Existe aqui uma confusão quanto à definição de anel quociente $\mathbb{Z}/m\mathbb{Z}$ e o anel comutativo $\mathbb{Z}_m$, como conjunto de números inteiros, que são isomorfos e que este estudante E2 vê como sendo o mesmo.

As respostas da **classe D**, da questão 4 do segundo questionário, também são indícios dessa dificuldade, pois os estudantes afirmaram que $\mathbb{Z}_3 \subset \mathbb{Z}_6$, e que, portanto, $\mathbb{Z}_3$ é subanel de $\mathbb{Z}_6$. Pensando novamente em $\mathbb{Z}_m$ como conjunto de restos, esta inclusão pode ser considerada correta, mas não a afirmação de que $\mathbb{Z}_3$ é subanel de $\mathbb{Z}_6$, pois as operações destes anéis são diferentes e $\mathbb{Z}_3$ não é fechado em relação à adição módulo 6, isto é, $2 +_{(mod6)} 2 = 4 \notin \mathbb{Z}_3$.

Agora, tomando $\mathbb{Z}_m$ como conjunto das classes de equivalência módulo m, a inclusão $\mathbb{Z}_3 \subset \mathbb{Z}_6$ não é verdadeira, uma vez que os elementos destes conjuntos são diferentes, ou seja, $\overline{0} \in \mathbb{Z}_3$ é o conjunto dos múltiplos de 3, enquanto $\overline{0} \in \mathbb{Z}_6$ é o conjunto dos múltiplos de 6, que não são os mesmos e as operações destes anéis também são diferentes.

A questão 4, formulada para a entrevista, é apresentada a seguir:

Descreva os anéis $\mathbb{Z}_4$ e $\mathbb{Z}_8$. Indique alguma diferença entre eles. Podemos afirmar que $\mathbb{Z}_4$ é subanel de $\mathbb{Z}_8$?

Os extratos a seguir são das respostas a esta questão:

> **E1:** "Não porque o zero barra do $\mathbb{Z}_4$ não é o mesmo do $\mathbb{Z}_8$."
>
> **E3:** "$\mathbb{Z}_4$ não é subanel de $\mathbb{Z}_8$. Ele pode ser subconjunto no sentido de colocar os elementos dentro. Mas a estrutura, o $\mathbb{Z}_4$ como subcojunto de $\mathbb{Z}_8$ não tem a mesma estrutura de subanel."
>
> **E2:** "Eu creio que sim, porque a gente tem que o conjunto $\mathbb{Z}_4$ está contido no $\mathbb{Z}_8$, e no caso para o próprio subanel a gente tem que satisfazer as propriedades, ser fechado para a adição, a identidade ser a mesma e de fato é para os dois conjuntos.

P:"... e quais são as operações que estão envolvidas?"

E2: "...no caso é módulo 8... fazendo as contas assim de cabeça, creio que é fechado."

P: "Bom, mas se você pega dois e três módulo 8. Dois mais três módulo 8 é cinco. E cinco está em $\mathbb{Z}_4$?"

E2: "É verdade. É realmente a gente não pode considerar subanel."

Este entrevistado, E2, disse que $\mathbb{Z}_4$ é subanel de $\mathbb{Z}_8$, e assim como os estudantes que responderam a questão 4 do segundo questionário, não se preocupou em testar as condições que garantem que um subconjunto seja um subanel, e quando o fez, percebeu que não era possível afirmar tal coisa. Já o entrevistado E3, pareceu confuso com o uso dos representantes, na sequência do trecho de sua resposta apresentado acima ele disse o seguinte:

P: "O $\mathbb{Z}_4$ está contido em $\mathbb{Z}_8$?"

E3: "Olha eu não sei, se eu olhar para cada elemento aqui $[\mathbb{Z}_4]$, eu digo que ele tem elementos aqui $[\mathbb{Z}_8]$, graficamente olhando tem, mas eu não tenho certeza se você pode colocar um dentro do outro. ... Não eu acho que não. Porque estes caras são diferentes. Mesmo a classe do um, se for olhar enquanto classe mesmo, olhar os elementos que fazem parte de uma classe, a classe do um aqui $[\mathbb{Z}_4]$ e do um aqui $[\mathbb{Z}_8]$ são elementos diferentes, então eu não posso colocar um dentro do outro."

As respostas dos estudantes E2 e E3 mostram que, dependendo de como se entende o anel $\mathbb{Z}_m$, tem-se uma resposta diferente para esta inclusão, mas em qualquer um dos casos, $\mathbb{Z}_4$ não é subanel de $\mathbb{Z}_8$. O estudante E2 entende como já foi dito anteriormente, o anel $\mathbb{Z}_m$ como conjunto de restos da divisão por m, enquanto E3 entende como sendo conjunto de classes de equivalência módulo ideal $m\mathbb{Z}$.

O estudante E3 considerou, inicialmente, apenas os representantes da classe, e depois de pensar um pouco mais, percebeu que sendo os elementos classes de equivalência, esta inclusão não seria possível. Olhar apenas para o representante da classe pode confundir o estudante sobre a natureza dos elementos em questão.

No trabalho de Lajoie e Mura (2004), as autoras identificaram a dificuldade de entender a natureza dos elementos e das operações do grupo quociente. Mesmo a maioria dos estudantes tendo respondido que os elementos do grupo quociente são classes de equivalência, eles admitem que estes elementos são também elementos

do grupo de partida, ou que o grupo quociente é um subgrupo deste. Para as autoras alguns fatores podem contribuir para que esta dificuldade seja difícil de ser superada, entre outros, o uso dos representantes para realizar as operações do grupo quociente, o que pode induzir a uma confusão sobre a natureza dos elementos e a operação de grupo quociente.

No caso do anel quociente $\mathbb{Z}/m\mathbb{Z}$, que é também um grupo comutativo aditivo, pode-se pensar que esta confusão, com os representantes, torna-se mais fácil de acontecer, pois os representantes são números inteiros que são muito familiares para os estudantes. Considerando, ainda, a dificuldade dos estudantes em entender a partição induzida pela relação de equivalência, de noções de teoria de conjunto como a partição e classe de equivalência, observados na seção anterior, isso pode colaborar ainda mais para que a dificuldade em entender a natureza dos elementos de $\mathbb{Z}/m\mathbb{Z}$ aconteça.

Outro fator que pode contribuir para que esta dificuldade não seja facilmente superada é o que Duval (1983) chama de *obstacle du dedoublement*, obstáculo do desdobramento de um objeto matemático, que é uma característica de alguns objetos matemáticos de terem várias propriedades em um mesmo contexto, neste caso, os números inteiros como representantes de classe, como elementos de um conjunto e como números inteiros mesmo. Este obstáculo também parece agir para causar a confusão com os representantes da classe, pois, por exemplo, 1 é representante, tanto da classe $\overline{1} \in \mathbb{Z}_3$, quanto da classe $\overline{1} \in \mathbb{Z}_6$, representando coisas diferentes. De acordo com Duval (1983), parte dos estudantes sempre encontraram este obstáculo nas diversas situações de aprendizagem, em que são colocados.

2. *Dificuldade em construir e entender o anel quociente.*

   Ao observar que poucos estudantes responderam o item a) da questão 1 de forma satisfatória, veja as **classes A** e **B** desta questão, pude inferir que os estudantes tiveram dificuldade para construir o anel quociente em questão.

   Lajoie e Mura (2004) já haviam identificado a dificuldade dos seus estudantes em entender por que o subgrupo tem que ser normal na construção do grupo quociente; seus estudantes conseguiram construir o grupo quociente G/S, encontrando as classes laterais $a * S$, para todo $a \in G$, sendo G um grupo e $*$ sua

operação, sem verificar, no entanto, se S era um subgrupo normal. Na presente pesquisa, observei que os estudantes não conseguiram construir o anel quociente $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18}$, não encontrando seus elementos, as classes laterais, ou as classes de congruência módulo ideal $\overline{3}\mathbb{Z}_{18}$, isto é, as classes $a + \overline{3}\mathbb{Z}_{18}$.

Pode-se pensar que este resultado aconteceu devido ao fato de o anel envolvido na questão ser o $\mathbb{Z}_{18}$, e este não ser um anel que os estudantes estivessem familiarizados a utilizar para construir um anel quociente. O que, nesse caso, poderia ser um problema isolado, com este anel particular.

Por outro lado, pode-se pensar que estes estudantes não responderam esta questão porque não entenderam o processo de construção de um anel quociente, uma vez que este processo é o mesmo para qualquer anel. Neste processo de construção, dado um ideal de um anel, deveriam ter sido encontradas as classes de congruência módulo este ideal e no conjunto destas classes deveriam ser definidas as operações para estas classes.

Para explorar a construção de um anel quociente, foi elaborada a seguinte questão, de número 5, para os estudantes entrevistados:

Construa, passo-a-passo, o anel quociente $\mathbb{Z}_6$.

ii) Encontre um ideal deste anel com 3 elementos.

iii) Faça o quociente de $\mathbb{Z}_6$ *com o ideal que você encontrou.*

iv)Encontre um anel que seja isomorfo ao quociente encontrado.

v) O que seria $\mathbb{Z}_6/\overline{8}\mathbb{Z}_6$*?*

Apenas um dos três estudantes, E3, respondeu encontrando as classes de congruência módulo o ideal I. Ele construiu $\mathbb{Z}_6$ como conjunto de classes de congruência módulo 6 e, depois, como conjunto de classes módulo ideal $6\mathbb{Z}$, como mostra o extrato abaixo:

> **E3:** "Tinha duas formas que eu pensei em fazer. A primeira usando a relação de equivalência, congruência módulo 6. ... Uma outra forma de construir esse cara é definir um ideal $6\mathbb{Z}$. ... E daí fazer o quociente com esses conjuntos [$\mathbb{Z}$ e $6\mathbb{Z}$]. O quociente desses caras é $0 + 6\mathbb{Z}$, $1 + 6\mathbb{Z}$ até $5 + 6\mathbb{Z}$, onde os inteiros em cada uma dessas classes são os caras que são congruentes módulo $6\mathbb{Z}$".

Para construir o anel quociente $\mathbb{Z}_6/I$, o estudante E3 ficou em dúvida sobre qual das duas ideias de construção, mencionadas acima, ele havia usado, mas depois de examinar o que ele tinha escrito, ele mesmo chegou à conclusão de que havia construído as classes módulo ideal $I = \{\overline{0}, \overline{2}, \overline{4}\}$. Como pode ser visto no extrato abaixo.

> **E3:** "Eu peguei esse ideal e somei. Se eu pegar só o ideal e somar com zero é ele próprio. Se eu somar com 1 agora vai ficar 1, 3 e 5 e não sobra mais ninguém. Então fico com esses dois representantes [0 e 1]."

Já a construção do $\mathbb{Z}_6$ foi feita pelos estudantes E1 e E2, que encontraram as classes de congruência módulo 6. Abaixo, o trecho da entrevista do estudante E1, descrevendo como construiu o $\mathbb{Z}_6$:

> **P:** "Como você fez para construir estas classes?"
>
> **E1:** "É como se você pegasse os números inteiros e fosse dividindo por 6. Aí os restos das divisões você ia colocar, se era zero barra, um barra, assim."
>
> **P:** "Você usa a divisão?"
>
> **E1:** "Eu pego, sei lá, o $\mathbb{Z}$ que são os $0, \pm 1, \pm 2$, etc, porque tanto faz pegar positivo ou negativo. Aí você pega os inteiros e vai dividindo por 6. ..., 7 dividido por 6 vai dar 1 e vai sobrar 1, ... então 7 eu não sei se fala pertence a classe? O 7 pertence a classe um barra, por exemplo, e assim para os outros."

Mas ao construir o anel quociente $\mathbb{Z}_6/I$, sendo $I = \{\overline{0}, \overline{2}, \overline{4}\}$, E1 e não percebeu que a construção por ele realizada anteriormente não funcionaria para este caso, como pode ser observado no trecho abaixo:

> **P:** "O que é o anel quociente para você?"
>
> **E1:** "O quociente é alguma coisa relacionada com classes laterais, alguma coisa assim, que eu não..."
>
> **P:** "Então?"
>
> **E1:** "É um conceito que eu não sei, assim. O que é quociente? É tal coisa. Eu olho para a notação $[\mathbb{Z}_6/I]$ e não sei dizer o que eu tenho que fazer. "
>
> **P:** "Você se lembra como construiu o $\mathbb{Z}_6$?"
>
> **E1:** "Eu construí dividindo os elementos de $\mathbb{Z}$. No caso eu vou ter que pegar os elementos de $\mathbb{Z}_6$ e vou ter que dividir por esses [elementos de I]. Não sei."

Este estudante, E1, construiu o anel $\mathbb{Z}_6$ encontrando as classes de congruência módulo m, dividindo os inteiros por 6 e encontrando a classe em que cada um está.

Para construir as classes de congruência módulo ideal I, ele tentou usar o mesmo procedimento, mas parece não ter se sentido seguro de que era esse o procedimento correto, e só conseguiu construir as classes depois que a pesquisadora induziu, utilizando uma analogia com a construção de $\mathbb{Z}/6\mathbb{Z}$.

O mesmo ocorreu com o estudante E2, que também construiu o anel $\mathbb{Z}_6$ considerando a divisão de inteiros por 6 e tomando os restos. Mas para construir o anel quociente pedido, ele tentou usar o mesmo procedimento, como mostra o seguinte trecho:

> **E2:** "...eu já fiquei um pouco com dúvida, assim, foi $\mathbb{Z}_6$ quociente $2\mathbb{Z}_6$, mas eu tentei pensar de forma análoga ao que a gente faz aqui [referindo-se à construção de $\mathbb{Z}_6$]. ...eu tentei buscar uma ideia análoga, que foi pegar os restos da divisão inteira por dois, mas percorrendo agora o conjunto $\mathbb{Z}_6$."

Estes estudantes, E1 e E2, tentam utilizar a mesma ideia de tomar o resto da divisão por m na construção dos dois anéis. O anel $\mathbb{Z}_6$, para o estudante E2, é o anel comutativo, cujos elementos são números inteiros, resto da divisão por 6. Para o anel quociente $\mathbb{Z}_6/2\mathbb{Z}$, E2 faz a mesma divisão, só que com elementos de $\mathbb{Z}_6$, a ideia de quociente que ele apresenta é a de resto da divisão.

O que pude concluir destas entrevistas é que estes dois estudantes, E1 e E2, não compreenderam a construção de um anel quociente e não encontraram as classes de congruência módulo ideal I. Isso pode ter ocorrido devido a eles estarem muito ligados à ideia de quociente como resto da divisão, ou seja, eles estavam associando a construção de um anel quociente à necessidade de encontrar os restos da divisão por um número m, mas no caso do anel quociente, em questão, não é possível utilizar esta ideia.

O que concluo após as análises dos questionários, e apoiada nas entrevistas, é que o que pode ter levado estes estudantes a tomarem a construção do anel $\mathbb{Z}_m$, cujos elementos são classes de congruência módulo m, como padrão, é a familiaridade que eles tinham com este anel. Como o anel $\mathbb{Z}_m$ é igual ao anel quociente $\mathbb{Z}/m\mathbb{Z}$, veja Capítulo 2, e como este anel é o exemplo utilizado em praticamente toda a disciplina de Teoria de Anéis cursada pelos estudantes, estes podem ter ficado com a impressão de que todos os outros anéis quocientes podem ser construídos da mesma forma.

Outra possível explicação para os erros mencionados, que são indícios da dificuldade em construir e entender o anel quociente, é que estes estudantes não reconheceram a partição induzida pela relação de congruência módulo ideal I, da mesma forma como a dificuldade em reconhecer a partição induzida pela congruência módulo m identificada na subseção 5.1.2. Esses estudantes parecem não saber que uma relação de equivalência induz uma partição do conjunto sobre o qual ela está definida, o que pode ter dificultado o entendimento da construção de um anel quociente. Concluo portanto, que os estudantes participantes da presente pesquisa não demonstraram ter aprendido o algoritmo ou processo de construção do anel quociente.

3. *Dificuldade em identificar dois anéis isomorfos.*

   As respostas das **classes E** e **F**, da questão 1, sugeriram esta dificuldade, pois apesar de, na **classe E** os estudantes terem dito corretamente que o anel quociente $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18} \cong \mathbb{Z}_3$, a justificativa dada foi a de que os elementos eram iguais, que não está correta. Já nas respostas da **classe F**, os estudantes colocaram que $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18}$ é isomorfo a $\mathbb{Z}_6$ e a $\mathbb{Z}$; porém, eles não verificaram, por exemplo, que a ordem desses anéis é diferente, não mostrando que os anéis utilizados não são isomorfos a $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}_{18}$.

   Segundo Leron, Hazzan e Zazkis (1995), os estudantes trabalham bem com a definição de isomorfismo, que eles chamaram de "versão ingênua", ou seja, a de que dois grupos são isomorfos se eles são os mesmos, exceto pela notação de seus elementos. Quanto à definição formal de isomorfismo, que envolve a existência de uma função f injetiva satisfazendo algumas propriedades, eles consideraram ser mais difícil de ser entendida, já que dois grupos são isomorfos se existe um isomorfismo de um para outro. De acordo com esses autores, a construção de grupos isomorfos nesta definição formal envolve a construção de função e de isomorfismo como objeto (desde suas primeiras quantificações).

   Os mesmos autores destacam, ainda, a necessidade de distinção da relação "ser isomorfo a" entre dois grupos e do objeto do isomorfismo, o que para o processo ensino/aprendizagem é importante, pois as operações mentais que estão envolvidas em cada um são diferentes. Enquanto a "relação ser isomorfo é simétrica, intuitiva e não necessita do conceito de função para o seu entendimento, o objeto

do isomorfismo é direcional, "funcional", e muito difícil de ser entendido, e nós não temos uma versão intuitiva para isso" (LERON, HAZZAN e ZAZKIS. 1995, p. 155, tradução da autora).

Os estudantes entrevistados tiveram que encontrar um anel isomorfo a um outro para responder o item *iv)Encontre um anel que seja isomorfo ao quociente encontrado* da questão 5 já apresentada, veja também no Apêndice D.

O que se esperava como resposta para esta questão é que os estudantes utilizassem a versão ingênua de isomorfismo, como na resposta do estudante E3:

> **E3:** "Como esse cara [referindo-se a $\mathbb{Z}_6/I$] tem dois elementos, ele tem que ser isomorfo a $\mathbb{Z}_2$, não tem outra coisa. Daí dá para mostrar definindo o isomorfismo."

Uma explicação para os erros encontrados tanto nos questionários quanto nas entrevistas, que demonstraram a dificuldade em identificar dois anéis isomorfos, é a de que os estudantes provavelmente não têm a noção de isomorfismo bem compreendida, nem a formal, nem a ingênua.

Esta noção parece ser um enigma para os estudantes. As dúvidas sobre como e quando considerar uma estrutura isomorfa a outra, em Álgebra, pode ser percebida nos trechos das entrevistas dos estudantes E3 e E2, transcritas abaixo:

> **E3:** "Quando a gente estuda Álgebra, a gente tem a ideia às vezes de fazer isomorfismo, e a gente olha só para o cara, né? Ah não! Tem o mesmo símbolo aqui tal, mantém a estrutura então é igual, quer dizer isomorfo, mas se você olhar igual mesmo, não são iguais. "

Ou a fala do entrevistado E2, que depois de ter dito que $\mathbb{Z}_6/2\mathbb{Z}_6$ era igual a $\mathbb{Z}_2$, e ser questionado pela pesquisadora, ele disse:

> **E2:** "É porque na Álgebra é bem difícil dizer que é igual... a gente tem que dizer que eles têm a mesma estrutura, se comportam com a mesma função, então justamente tem que dizer é que são isomorfos."

Leron, Hazzan e Zazkis (1995), afirmam que o conceito de isomorfismo é uma expressão formal de uma ideia mais geral sobre semelhanças e diferenças.

Isso pode gerar um obstáculo cognitivo (Cornu, 1991), pois se deve romper com a ideia de igualdade que temos interiorizada, em que coisas iguais são as mesmas

sob todos os aspectos. A ideia que temos sobre igualdade é de um padrão, de uniformidade, que podemos trocar um elemento por outro, de que tudo vale para todos. Mas estas também são as mesmas "essências" de uma relação de equivalência, e não poderia deixar de ser, já que a igualdade é também uma relação de equivalência. Assim, o que temos do senso comum é que os símbolos:

$=$ (igualdade) significa: os mesmos sob todos os aspectos.

$\equiv$ (equivalência) significa: os mesmos sob alguns aspectos.

Em sua tese de doutorado, Lajoie (2000) identificou, nas respostas dos seus estudantes, a dificuldade de entender que grupos isomorfos são semelhantes, no mesmo sentido que os matemáticos entendem a relação de isomorfismo entre dois grupos. Segundo a autora, seus estudantes tinham a ideia de semelhança entre grupos isomorfos, mas isso só acontecia para alguns aspectos do grupo, por exemplo, eles percebiam a semelhança em um ou vários dos seguintes aspectos: nos próprios elementos; na natureza da composição ou dos elementos; na ordem dos elementos do grupo, na ordem do grupo e no fato dos grupos serem ou não comutativos ou cíclicos. Ou seja, os estudantes mencionados verificaram alguns desses aspectos para dizer se os grupos são isomorfos, mas eles não apresentaram um isomorfismo entre os grupos. Lajoie (2000) destacou, também, que fazendo estas verificações nem sempre se obtém respostas erradas; é possível, verificando estes aspectos, concluir que dois grupos não são isomorfos, o que está correto.

Na presente pesquisa, os estudantes investigados detiveram-se em alguns dos aspectos mencionados acima para dizer que os anéis em questão eram isomorfos. Por exemplo, o estudante Q1, disse que $\mathbb{Z}_{18}/J \cong \mathbb{Z}_3$, pois eles "têm os mesmos elementos", ou como o estudante E3, que justificou que dois anéis são congruentes pois eles têm o mesmo número de elementos. Parece haver nesta última afirmação, uma confusão entre dizer que se dois anéis (ou grupos) são isomorfos eles têm o mesma ordem, o que é considerado verdadeiro, e dizer que se dois anéis (ou grupos) têm a mesma ordem então são isomorfos, o que nem sempre é considerado verdadeiro.

4. *Dificuldade em trabalhar com o representante da classe*

O representante de uma classe de equivalência, ou no caso, de congruência, é um

elemento da classe de congruência. No caso do anel $\mathbb{Z}_m$, que está sendo estudado, foram tomados para representantes os menores inteiros positivos de cada classe, como, por exemplo em $\mathbb{Z}_3$, que tem como representantes os inteiros $0, 1, 2$, mas que poderiam ser $9, 13, 26$, já que estes números são congruentes a $0, 1, 2$ módulo 3, respectivamente. Estes números foram utilizados pela comodidade de se trabalhar com números 'pequenos' e positivos e por estes números darem a ideia de resto da divisão por m, o que é usual ao denotar os elementos de $\mathbb{Z}_3$ por $\overline{0}, \overline{1}, \overline{2}$. A barra em cima destes números mostra que se está trabalhando com as classes de congruência módulo 3, e não com os números inteiros. Mas qual a diferença entre eles? Pode-se utilizar os números sem as barras? O que se quer dizer quando se escreve $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ e quando se escreve $\mathbb{Z}_3 = \{0, 1, 2\}$? Estas questões foram observadas nas respostas aos questionários e também foram levantadas pelos estudantes nas entrevistas, o que demonstrou a dificuldade dos estudantes em trabalhar com o representante da classe.

Em Lajoie e Mura (2004), o uso dos representantes da classe em aulas de Álgebra, sem as devidas explicações do porquê, isso pode ser feito foram tomados como fonte de dificuldade. Na presente pesquisa observei, assim como essas autoras, que os representantes podem também ter sido fonte de dificuldade, mas além disso observei a dificuldade dos estudantes investigados em trabalhar com o representante. As respostas dos estudantes, que demonstram esta dificuldade, podem ser encontradas na **classe B** da questão 2, em que os estudantes N7 e N14 escreveram $\overline{8} \equiv \overline{3} \pmod 5$ e o estudante N10 escreveu $\overline{8} \div 5 = 1 + \overline{3}$ e na **classe C** da questão 4, em que o estudantes N7 escreveu $\overline{9} \notin \mathbb{Z}_6$. Estes estudantes parecem não diferenciar o representante da classe de uma classe, pois eles utilizaram a igualdade $\overline{a} = a$.

Nas entrevistas, foram encontrados outros indícios dessa dificuldade, como, por exemplo, no trecho da entrevista com o estudante E3:

> **E3:** Esse cara aqui [referindo-se ao item c) da questão 5, Apêndice D] eu fiquei com uma dúvida aqui, porque eu peguei $\overline{8}$ em $\mathbb{Z}_6$, só que $\overline{8}$ não está lá. Supondo que $\overline{8}$ é igual a $\overline{2}$, que eu acho que é ..."
>
> **P:** "Mas por que você ficou com dúvida?"
>
> **E3:** " É uma questão só de notação, o oito. É que nem nessa questão aqui do $\overline{10}$ estar no $\mathbb{Z}_7$. Tá a classe do 10, apesar dela não estar escrita dentro do conjunto

> aqui, ela é igual a classe do três. Então eu usei essa ideia, oito barra vezes $\mathbb{Z}_6$ é igual a dois barra vezes $\mathbb{Z}_6$. ... Não é que para mim esta é a ideia certa, só que eu tava, eu fiquei inseguro na hora que eu olhei para esse símbolo [$\overline{8}\mathbb{Z}_6$]. Na hora que eu olhei para o símbolo eu pensei 'será que faz sentido o símbolo?'...".

As razões para que os erros que sugiram a dificuldade em trabalhar com o representante da classe tenham ocorrido, podem ter sido a familiaridade com os números inteiros e o obstáculo do desdobramento, assim como ocorreu na primeira dificuldade identificada nesta seção, a de entender a natureza dos elementos do anel quociente $\mathbb{Z}_m$.

Outra razão pode ter sido devido à forma com que os representantes das classes de congruência, em questão, são tratados em sala de aula e nos livros de Álgebra. Em geral, os representantes utilizados são os canônicos, isto é, os menores inteiros positivos de cada classe, o que pode levar o estudante a pensar que existem apenas estes e a questionar se faz sentido pensar em $\overline{8} \in \mathbb{Z}_6$, por exemplo, como no caso do estudante E3. Estes representantes são utilizados em sala de aula porque é mais prático trabalhar com eles e com a notação para classes $\overline{a}$ do que com a notação $a + I$; porém parecem gerar dificuldades.

Considero, ainda, ser possível pensar que a dificuldade em trabalhar com o representante da classe pode ter acontecido porque estes estudantes não entenderam as noções e as propriedades ligadas a uma relação de equivalência. Por exemplo, no caso do representante de uma classe, que pode ser qualquer elemento da classe de equivalência, e no caso do $\mathbb{Z}_m$, em que, identificando-se um elemento da classe, pode-se reconstruir a classe inteira.

Capítulo 6

Considerações finais

Esta pesquisa buscou, por meio da análise das respostas dos estudantes a questões sobre congruência algébrica no contexto das disciplinas de Teoria de Números e Teoria de Anéis, responder a seguinte questão:

O que os estudantes de um Curso de Matemática respondem sobre congruência algébrica em questões formuladas no contexto da Teoria de Números e Teoria de Anéis? O que podemos inferir destas respostas?

Nas seções 5.1 e 5.2 deste trabalho, foi feita a classificação das respostas dos estudantes aos dois questionários elaborados sobre questões de congruência módulo m e anel quociente $\mathbb{Z}_m$. Tais seções apresentam o quê e de que modo os estudantes investigados responderam às questões formuladas, seus erros e acertos.

A partir da análise das respostas dos questionários e com o apoio das respostas obtidas nas entrevistas, considero ser possível inferir as seguintes dificuldades:

1. dificuldade em reconhecer a partição induzida pela relação de congruência módulo m sobre $\mathbb{Z}$. Muitos estudantes não reconheceram a partição induzida pela congruência módulo m, pois escreveram, por exemplo, que a classe $\overline{3} \subset \mathbb{Z}_7$;

2. dificuldade em construir e entender o anel quociente. A maioria dos estudantes não conseguiu construir um anel quociente, apenas encontrando por meio de cálculos os seus elementos, que são as classes de congruência módulo um ideal;

3. dificuldade em entender a natureza dos elementos do anel quociente $\mathbb{Z}_m$. A maioria dos estudantes disse que os elementos do anel quociente $\mathbb{Z}/m\mathbb{Z}$ são elementos do anel $\mathbb{Z}$;

4. dificuldade em identificar dois anéis isomorfos. A maioria dos estudantes não conseguiu identificar o anel isomorfo a $\mathbb{Z}_{18}/\overline{3}\mathbb{Z}$;

5. dificuldade em trabalhar com o representante da classe. A quase totalidade dos estudantes se apegou aos representantes canônicos de $\mathbb{Z}_n$ e afirmou que $\mathbb{Z}_3$ é subanel de $\mathbb{Z}_6$.

Não se pretende, com esta lista de dificuldades, afirmar que estas sejam as únicas, nem que elas sejam as mesmas para todos os estudantes.

Nesta pesquisa, alguns aspectos identificados como fonte dessas dificuldades foram:

1. os ligados a noções preliminares, uma vez que a maioria dos estudantes demonstrou não saber noções de teoria de conjuntos, como, por exemplo, partição de conjunto, classe de equivalência, assim como a impossibilidade de estabelecer relações entre elas. Houve estudantes que, inclusive, confundiram as relações de pertinência e de inclusão;

2. os inerentes ao conceito, como, por exemplo, no caso do obstáculo do desdobramento de um conceito matemático Duval (1983), o que ocorreu devido ao fato de o representante da classe poder significar um número inteiro e uma classe módulo m ou n, no mesmo contexto, dependendo do anel que está em jogo;

3. os didáticos, como o tratamento em sala de aula dado ao representante da classe, às estruturas isomorfas e à definição dada a $\mathbb{Z}_m$;

4. os cognitivos, por exemplo, a noção de anel quociente exige do estudante a coordenação de alguns esquemas (Dubinsky, 1994), que podem não estar interiorizados, fazendo com que a aprendizagem desta noção fique comprometida.

A hipótese de trabalho desta pesquisa era que as dificuldades na aprendizagem de congruência módulo m e anel quociente $\mathbb{Z}_m$, estavam ligadas aos conceitos envolvidos na noção de congruência, entre eles, a 'relação de equivalência', 'operação binária', 'classe de equivalência' e 'conjunto quociente'. Pensei, inicialmente, que estas dificuldades estariam ligadas, principalmente, se não exclusivamente, às noções matemáticas preliminares da Teoria de Conjuntos.

Embora as dificuldades apresentadas pareçam estar vinculadas à ideia de falta de pré-requisito por parte do estudante, ou seja, falha nas noções básicas de Teoria de Conjuntos, os resultados demonstram que as origens dessas dificuldades podem ser também didáticas ou cognitivas.

Os resultados apresentados, analisados e discutidos no Capítulo 5 mostram que as dificuldades identificadas estão, sim, ligadas à noção de congruência, como, por exemplo, na dificuldade demonstrada pelos estudantes no reconhecimento da partição de uma congruência sobre o conjunto em questão, o que parece ter levado os estudantes a não entenderem a construção do anel quociente, nem mesmo a natureza dos elementos desse conjunto.

Já a dificuldade dos estudantes em trabalhar com o representante da classe, ao tomarem o representante da classe como classe, também demonstra uma incompreensão da noção de congruência, uma vez que a propriedade de tomar qualquer elemento da classe para representá-la é uma propriedade de toda relação de equivalência . A identificação de anéis isomorfos também está ligada à noção de congruência, pois podemos construir o anel quociente por meio, do Teorema do Isomorfismo, cujo núcleo do isomorfismo é um ideal.

Tais resultados permitem concluir os limites de minha hipótese de trabalho ao destacar na aprendizagem do conceito de congruência algébrica apenas os aspectos matemáticos das noções matemáticas envolvidas, sem considerar os aspectos didáticos e cognitivos que interferem no processo de ensino e aprendizagem.

Para finalizar, farei algumas considerações sobre o ensino de Álgebra no ensino superior e apresentarei algumas sugestões para pesquisas futuras.

6.1 O ensino de Álgebra Abstrata

O que estes resultados mostraram é que a linguagem da Teoria de Conjuntos não está interiorizada pelos estudantes investigados. Isso, considerando que esses estudantes estavam matriculados no 4º ou 6º período de curso de Licenciatura ou Bacharelado em Matemática, do período noturno, é preocupante.

Expressar-se matematicamente faz parte da aprendizagem matemática; se os estudantes não escrevem ou não falam o que querem dizer, como farão para comunicar aos seus futuros alunos as noções matemáticas?

O que nós professores do ensino superior, esperamos dos nossos alunos, ou que seria 'ideal', é que os estudantes tivessem as noções básicas de Teoria de Conjuntos e sua respectiva linguagem bem compreendidas e interiorizadas, para que pudessem se dedicar apenas à aprendizagem de conceitos da Álgebra Abstrata, por exemplo.

Mas o que esta e outras pesquisas, como, por exemplo, a de Cury (2006), mostram é que as falhas nas noções preliminares estão cada vez mais presentes no contexto do ensino superior. Não podemos mais supor que os estudantes cheguem à universidade com as noções básicas de teoria de conjuntos, de funções, manipulações algébricas e outras, bem apreendidas. O que algumas universidades têm feito, para preencher, estas lacunas é oferecer disciplinas com estes conteúdos, com nomes como Pré-Cálculo, ou, no caso da universidade em que esta pesquisa foi realizada, Complementos de Matemática e Funções, o que parece não estar surtindo o efeito desejado, como pode ser visto pelos resultados desta pesquisa.

Assim, concordo com Lajoie e Mura (2004) de que "não é suficiente ensinar as noções de conjuntos, fora de um contexto, mas que é necessário também situá-las no contexto da Álgebra Abstrata." (LAJOIE e MURA, 2004, p. 74). Entendo ser necessária essa ampliação para outras disciplinas, incluindo o mesmo para outras noções consideradas "básicas" no ensino universitário. Assim, quando as classes de congruência módulo ideal forem estabelecidas, o professor pode fazer a ligação destas classes com a partição do conjunto; pode, também, lembrar aos estudantes que os elementos dessa partição são conjuntos, e relembrar os símbolos matemáticos envolvidos.

Certamente, esta sugestão fará com que as sessenta horas programadas para desenvolver os conteúdos dessas disciplinas não sejam suficientes, mas pode-se considerar que estas falhas nas noções preliminares podem formar um círculo vicioso. Os estudantes das disciplinas de Álgebra são os futuros professores de futuros estudantes universitários, e estes poderão chegar à universidade com falhas nas noções matemáticas básicas também. Sendo assim, valeria a pena dedicar um tempo dessa disciplina para discutir estas noções neste contexto.

Não compete apenas aos professores do ensino superior quebrar este círculo, são necessárias políticas públicas para que haja uma melhoria da qualidade de ensino em todos os níveis. Mas os professores de Álgebra Abstrata, por exemplo, podem "gastar" um tempo com seus alunos, para discutir, no contexto de sua disciplina, as noções matemáticas básicas, ou a natureza dos elementos do anel ou grupo quociente,

ou ainda destacar o porquê de se poder utilizar os representantes da classe como o fazemos.

De minha experiência como professora de Matemática do Ensino Superior, acredito que possa ser difícil para os professores, em geral, deixarem de fazer algumas demonstrações que fazem parte da cultura desta ciência, e dedicarem mais tempo à reflexão, juntamente com seus estudantes, sobre estes conceitos, o que poderá ser mais vantajoso do que apenas ver os estudantes tentando acompanhar demonstrações a eles apresentadas. Porém, considero, após minha revisão de literatura, serem necessárias muito mais pesquisas sobre como se dá a aprendizagem dos estudantes do ensino superior, particularmente quando são provocados a pensar sobre os conceitos de Álgebra Abstrata, por exemplo.

Deve ficar claro, porém, que nem todos os problemas do ensino de Álgebra estarão resolvidos, simplesmente "tapando os buracos" das noções matemáticas básicas nesta disciplina. Os conceitos matemáticos ensinados exigem dos estudantes uma abstração, que eles podem não conseguir alcançar. Uma explicação possível pode ser dada por meio da abordagem das rupturas epistemológicas que devem acontecer, de acordo com Lorenzo (2005), na passagem de um fazer matemático concreto para o abstrato, assim como da matemática escolar para a matemática universitária. Foi o que observei na presente pesquisa nas respostas dos estudantes às questões 2 e 3 do primeiro questinário, quando, por exemplo, identifiquei estudantes que empregaram procedimentos aritméticos (contas), ao invés de utilizarem a congruência módulo m para resolver. Romper com o pensamento aritmético, até então exigido dele no ensino básico, pode demorar mais do que as sessenta horas programadas para a disciplina. Não podemos esquecer também que a aprendizagem não depende apenas do professor, do livro texto escolhido, mas também do empenho do estudante, ele também deve fazer a sua parte. No entanto, o professor deve dar condições para que o estudante consiga romper com conhecimentos e raciocínios que podem dificultar este "salto" no nível de abstração.

De acordo com Asiala et al. (1997), a aprendizagem do grupo quociente se dá quando os estudantes conseguem coordenar os esquemas de classe, operação binária e grupo. No desenvolvimento da aprendizagem de classe, as noções de partição e a ideia de conjunto podem também ser desenvolvidas. Como foi visto no capítulo 3, a análise epistemológica, de acordo com a Teoria *APOS* para formação da noção de

classe como objeto, permite propor para os estudantes alguns exercícios específicos, em que estes passos sejam explorados, como, por exemplo, pedir para que eles calculem explicitamente as classes módulo ideal, sobre anéis familiares e, depois, sobre anéis um pouco mais complexos como $\mathbb{Z}_8$, sendo possível discutir ao mesmo tempo a natureza desses conjuntos, chamando a atenção para o uso dos representantes.

Outra alternativa é a abordagem apresentada por Fraleigh (2002, p. 98), na definição de classe, pois utiliza a tabela de operações, por exemplo de $\mathbb{Z}_6$ em cores diferentes para cada classe, tornando visível para o estudante o que acontece com o grupo quando as classes são construídas, dando a ideia de partição de conjunto, e, também, do fechamento da operação destas classes.

Quanto ao ensino de anel quociente, $\mathbb{Z}_m$, como ele pode ser definido como anel quociente cujos elementos são classes de congruência módulo m ou como anel de inteiros módulo m, o professor deve estar atento para as possíveis confusões que isso pode causar, por exemplo, ao entender os elementos do anel quociente $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ como elementos de $\mathbb{Z}$.

Os resultados da presente pesquisa mostram que o uso do representante da classe é algo que não foi bem entendido pelos estudantes. É comum, em salas de aula de disciplinas de Álgebra no ensino superior, que os professores utilizem, por exemplo, os representantes, os números inteiros com a barra ou não acima deles. Para o professor, isso pode ser considerado apenas como um problema de notação, pois no caso do $\mathbb{Z}/m\mathbb{Z}$ é isomorfo a $\mathbb{Z}_m$ (como resto da divisão), e ele pode não se dar conta das dúvidas e confusões que esta diferença na notação pode gerar nos estudantes, já que isso se refere à natureza dos elementos desses conjuntos.

O problema é que os estudantes, que estão iniciando os estudos destas noções, podem não entender o porquê de se colocar ou não a barra, por não entenderem a natureza dos elementos em jogo, o que pode levá-los a pensar como o estudante E2, que, ao não concordar que $10 \in \overline{3}$ em $\mathbb{Z}_7$, demonstra entender classe como um número e o anel quociente $\mathbb{Z}/m\mathbb{Z}$ como um subconjunto de $\mathbb{Z}$.

Destaco, a seguir, o momento da entrevista do estudante E2 em que ele expressa suas dúvidas em colocar ou não a barra sobre o representante da classe e o que isso significa.

> **E2:** "Então o nosso professor [de outra instituição], fazia isso, ele considerava tanto com a barra ou sem a barra, mas eu sempre ficava meio intrigado. ... Será que todo

mundo concorda com isso, será que é a visão do professor?"

O que mostra que a forma como o professor apresenta estas noções e trabalha com elas em sala de aula pode causar dúvidas e dificuldades na aprendizagem dos estudantes.

Mas o que pode acontecer se a aprendizagem de uma estrutura quociente ou da noção de congruência não for satisfatória? Depende da ênfase do curso que o estudante segue? Um exemplo disso é que, para o estudante do Bacharelado em Matemática, o não entendimento da noção de congruência pode fazer com que a aprendizagem de conceitos, como quocientes de variedades, ou de espaços topológicos, que requerem do estudante habilidades com as noções envolvidas na estrutura quociente, não sejam possíveis. Para o estudante da Licenciatura em Matemática pode ser que o entendimento de noções, como a equivalência de frações e as construções lógico-formais dos números inteiros, números reais e complexos, fiquem comprometidas.

6.2 E a partir de agora...

Esta pesquisa teve algumas limitações, como, por exemplo, não ter apresentado um estudo histórico do desenvolvimento das noções de congruência, congruência módulo m e de anel quociente, o que não permitiu abordar os erros cometidos pelos estudantes em termos de obstáculos epistemológicos. Assim, tomando a noção de obstáculo epistemológico dada por Brousseau (1983), o que foi feito neste trabalho, foi encontrar os erros recorrentes e mostrar que tais erros são agrupados ao redor de conceitos. Considero que ainda poderei continuar a utilizar esta abordagem, em pesquisa para detectar os obstáculos no desenvolvimento histórico destas noções, para verificar se são de fato obstáculos epistemológicos. Um trabalho que indica que conjunto de conjunto é um obstáculo epistemológico para a aprendizagem de grupo quociente é o trabalho de Brenton e Edwars (2003), em que eles encontram no desenvolvimento histórico da Teoria de Conjuntos, indícios desse obstáculo.

Poderei, também, a partir das dificuldades encontradas, propor atividades de ensino ou uma sequência didática para ajudar o estudante a superar estas dificuldades. Como, por exemplo, analisar experiências com o ISETEL, que é uma linguagem de programação, relatada por Dubinsky (1994), Asiala (1997), e outros.

Outra pesquisa que ainda poderá ser proposta, de acordo com os dados levantados por este trabalho, seria, por exemplo, para identificar as concepções dos estudantes sobre isomorfismo, o que não foi abordado nesta pesquisa, mas que encontrei indícios de que este conceito pode causar dificuldades na aprendizagem de Álgebra Abstrata, como foi comentado na seção anterior.

Neste trabalho, não foi feita distinção se os estudantes que responderam os questionários e entrevistas eram do curso de Bacharelado ou Licenciatura em Matemática, nem nos preocupamos se essas noções eram relevantes ou não para a formação profissional de cada uma das ênfases do curso, pois, na instituição em que esta pesquisa foi desenvolvida não existe tal separação, mas em alguns eventos em que este trabalho foi apresentado, como por exemplo no EBRAPEM, estas questões foram levantadas. Sendo assim, parece-me importante um estudo que contemple estas questões, e também pesquisas que analisem a relação professor, aluno e os conceitos matemáticos na sala de aula nas disciplinas de Álgebra tanto, no Curso de Licenciatura, quanto no de Bacharelado.

Para finalizar, espero que este trabalho contribua para a uma reflexão sobre ensino e aprendizagem de Álgebra Abstrata.

Referências Bibliográficas

[1] ARTIGUE, M. Épistémologie et Didactique. *Recherches en Didactique des Mathèmatiques*, Vol. 10, n. 23, p. 241-286. Grenoble: La Pensée Sauvage-Éditions, 1990.

[2] ARTIGUE, M. Qué se puede aprender de la investigación educativa en el nível universitario? *Boletin de al Associación matemática Venezolane*, Vol.X, n. 2, p. 117-134, 2003.

[3] ASIALA M. et al. Development of students´ understanding os cosets, normality, and quotient groups. *Jornal Mathematical Behavior.* 16(3) p. 241-309, 1997.

[4] BACHELARD, G. *O Novo espírito científico.* Tradução: Juvenal H. Júnior, 3 ed. Rio de Janeiro: Tempo Brasileiro, 2000.

[5] BACHELARD, G. *A formação do espírito científico.* Tradução: Estela dos Santos Abreu, 1 ed. Rio de Janeiro: Editora Contraponto, 1996.

[6] BATISTA, C. G. Fracasso escolar: análise de erros em operações matemáticas. *Zetetiké*, v. 3, n. 4, p. 61-72, 1995.

[7] BIRKHOFF, G., MACLAINE, C. *Álgebra Moderna Básica.* Tradução: Carlos A. A. de Cavalho. 4 ed. Rio de Janeiro: Ed.Guanabara Dois S.A. 1980.

[8] BRANDERMGERG, J. C. Uma análise histórico-epistemológica do conceito de Grupo: caminhos para uma nova transposição didática. In: X EBRAPEM - *X Encontro Brasileiro de Estudantes de Pós-graduação em Educação Matemática*, CD do evento. Belo Horizonte, 2006.

[9] BROUSSEAU, G. Les obstacles epistemologiques et les problemes en mathematiques. *Recherches en Didactique des Mathématiques*, v. 4, n. 2, p. 165-168. Grenoble, 1983.

[10] BOURBAKI, N. *Élémentes de Mathématique: Algèbre*. Cap. 1-3, Hermann, Paris, 1970.

[11] CAMPOS, E.; SOARES, M. T. C. Algumas reflexões sobre o desenvolvimento histórico dos conceitos congruências e grupo quociente e sobre o ensino deste conceito. In: VII Reunião de Didática da Matemática do Cone Sul, 2006, Águas de Lindóia. *Anais VII Reunião de Didática da Matemática do Cone Sul*, 2006.

[12] CAMPOS, E. Congruência Algébrica: uma poderosa feramenta na construcão de objetos matemáticos. In: EBRAPEM- *Encontro Brasileiro de Estudantes de Pós-graduação em Educacão Matemática*, São Paulo. *Atas do Ebrapem*, 2005.

[13] CAMPBELL, S. R., ZAZKIS R. *Learning and teaching number theory: research in cognition and instruction.* Westport,Ct: Ablex Publishing. 2002.

[14] CAMPBELL, S. R., ZAZKIS R. *Number Theory in Mathematics Education: perspectives an prospects.* New Jersey: Lawrence Erlbaum Associates, 2006.

[15] CIFUENTES, J. C.; NEGRELLI, L. G. Perpectivas Epistemológicas e Metafísicas na Educação Matemática. In: *IIISIPEM- Seminário Internacional de Pesquisa em Educação Matemática*. CD Ron. Águas de Lindóia, 2006.

[16] CORNU, B. *Apprentissage de la notion de limite: conceptions et obstacles*. Thèse de doctorat de troisième cycle. L'Université Scientifique et Medicale Grenoble, 1983.

[17] CORNU, B. Limits. In: Tall D., ed. *Advanced Mathematical Thinking*. Kluwer, p. 153-166, 1991.

[18] CURY, H. N. *Análise de erros - o que podemos aprender com as respostas dos alunos*. Belo Horizonte: Ed. Autêntica, 2007.

[19] CURY, H. N. Análise de erros em cálculo diferencial e integral: resultados de investigação em cursos de engenharia. In: CONGRESSO BRASILEIRO DE ENSINO DE ENGENHARIA, *Anais do congresso*, Cd-rom. Rio de Janeiro , 2003.

[20] CURY, H. N.Análise de erros em Educação Matemática. *Verati* Salvador, v. 3, n. 4. p. 95-107, 2004.

[21] CURY, H. N. KONZEN, B. Classificação e Análise de erros em Álgebra. 2006. In: ccet.ucs.br/eventos/outros/egem/cientificos/cc26.pdf. Último em acesso 13/11/2007.

[22] DIAS, M. A. *Contribuition à alalyse d'un enseignement expérimental d'álgèbre linéaire en DEUG, A première année*. Mémoire de DEA. Paris: Université de Paris 7, 1993.

[23] DOUADY, R. Jeux des cadres et dialectique outil-objet. *Recherches en Didactique des Mathématiques*. v. 7(2), p. 5-31, 1986.

[24] DOMINGUES, H. H. *Fundamentos da Aritmética*. São Paulo: ed. Atual, 1991.

[25] DUBINSKY, E. et al. On learning fundamental concepts of group theory. *Educational Studies in Mathematics*, vol. 27, p.267- 305, 1994.

[26] DUBINSKY, E. Reflective Abstraction. In: Tall D., ed. *Advanced Mathematical Thinking.* Kluwer, p. 95-126, 1991.

[27] DUVAL, R. L´obstacle du dédoublement des objets mathématiques. *Educational Studies in Mathematics* 14(4), p. 385-414, 1983.

[28] FINDELL, B. *Learning and understanding in Abstract Algebra*, Doctoral dissertation, University of New Hampshire, Durham, 2001.

[29] FOWLER, D. Equivalence classes as objects. Disponível em: http://sunsite.utk.edu/matharchives/.http/hypermail/historia/aug98/0106.html. Último acesso em:28/03/2006.

[30] FRALEIGH, J.B. *A first Course in Abstract Algebra*. Hardcover, 7 ed., 2002.

[31] FREI, G. Number Theory. *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, Vol. 1, I. Grattan-Guiness, London, 1994.

[32] GARCIA, A., LEQUAIN, Y. *Elementos de Álgebra*. 3 ed. Rio de Janeiro: IMPA -Instituto de Matemática Pura e Aplicada, 2005.

[33] GAUSS, C. F. *Disquisitiones Arithmeticae*, Trad. Arthur A. Clarke; Spinger-Verlag, New York, 1986.

[34] GLASER, G. Épistémologie des nombres relatifs. *Recherches en didactique des mathématiques*, 2(3), p. 303-346, 1981.

[35] GONÇALVES, A. *Introdução à Álgebra*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1979.

[36] GT4-SIPEM. Relatório do GT4 - Educação Matemática no Ensino Superior. III Simpósio Internacional de Educação Matemática, 2006. In: www.sbem.com.br/files/RelatorioGT4.pdf. Último acesso em 12/12/2008.

[37] HAZZAN, O. Reducing abstraction level when learning abstract algebra concepts. *Educational Studies in Mathematics*. 40(1), p. 71-90, 1999.

[38] HIEBERT, J.; CAPENTER, T. P. Learning and teaching with understanding. In: Grouws D. A. (ed) *Handbook of Research on Mathematics teaching and Learnig* p. 65-97. New York: Macmillan, 1992.

[39] KLUTH, V. S.; *Estruturas da álgebra: investigação fenomenológica sobre a construção do seu conhecimento*. Tese Dutorado, 2005. Unesp - Rio Claro.

[40] LAJOIE, C. *Difficultés liées aus premiers apprentissages em théorie des groupes*. Tese (Doutorado), 2000. Faculte des études supérieures de l´Université Laval. Québec, Canadá, 2000.

[41] LAJOIE, C. MURA, R. Difficultés liées à l'aprentissage des concepts de sous-groupe normal et de groupe quotient. *Recherches en Didactique des Mathématiques*, Grenoble, vol. 24, n. 1, p. 47-80, 2004.

[42] LORENZO, J. Del hacer matemático, su historia y su plasmación educativa. *La Gaceta de la RSME*, Vol. 8, n. 2, p. 397-417, 2005.

[43] LERON, U.; HAZZAN, O.; ZAZKIS, R. Learning group isomorphism: A crossroads of many concepts. *Educational Studies in Mathematics.* 29(2) 153-174, 1995.

[44] MALISANI, E. Los obstaculos epistemologicos en el desarrolo del pensamiento algebrico: vision historica. *Revista IRICE*, nº 13. Argentina, 1999.

[45] MILIES, C. P.; COELHO, S. P. *Números: Uma introdução à Matemática*. 3 ed. São Paulo: Editora da Uniersidade de São Paulo, 2003.

[46] NICHOLSON, J. The development and understanding of the concept of quotient group. *Historia Mathematica*, n. 20, p. 68-88, 1993.

[47] ORE, O. *Number Theory and its History*. Dover, New York, 1988.

[48] Paillé, P. L´analyse par théorisation ancrée. *Cahiers de recherche sociologique*, 23, p. 148-181, 1994.

[49] ROTMAN J. *A First Course in Abstract Algebra*. Prentice Hall, New Jersey, 1996.

[50] SANTOS, J. P. O. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 1998.

[51] SCHUBRING, G. A noção de Multiplicação: um "obstáculo" desconhecido na História da Matemática. *Bolema*, Ano 15, nº18, p. 26-52, 2002.

[52] SCHUBRING, G.;Ontogeny and Phylogeny - Categories for Cognitive Development. Proceedings HPM 2004 e ESU 4, F. Furinghetti, S. Kaijser, C. Tzanakis (eds.), Iraklion, Greece: University of Crete, 2006 (678 pages in one volume), ISBN 960-88712-8-X.

[53] SFARD, A.; Operational origins of mathamtical objects and the quandry os reification- the case of function. In Dubinsky, E., Guershon, H.(ed), *The Concept of Function. Aspects of Epstemology and Pedagogy*, MAA NOtes, p. 44-45, 1992.

[54] SMITH, J. C. Revisiting Algebra in a Number Theoretical Setting. In Zazkis R., Campbell S. R.(ed), *Number theory in Mathematics Education: perspectives an prospects.* Lawrence Erlbaum Associates, New Jersey, 2006.

[55] TALL, D. O.; VINNER, S. Concept image and concept definition in mathematics with particular reference to limit and continuity. *Educational Studies in Mathematics*, 22(2), p. 125-147, 1981.

[56] TRAORÉ, K.; LAJOIE, C.; MURA, R. Quelques erreurs pouvant être liées à une difficulté à concevoir un ensemble comme un objet distinct de ses éléments chez des étudiants et des étudiantes universitares. *Educational Studies in Mathematics*, 64, p. 247-264, 2007.

[57] VERGNAUD, G. Difficultés conceptuelles, erreurs didactiques et vrais obstacles épistémologiques dans l´apprentissage des mathématiques. *Obstacle épistémologique et conflit socio-cognitif*. Colloque international. CIRADE, Université du Québec à Montreal, Montréal, p. 9-14, 1988.

[58] WARNER, S. *Modern Algebra*. Vol. 1, Prentice-Hall, Englewood Cliffs, N.J. 1965.

[59] WUSSING, H. *The genesis of the Abstract Group Concept*. Trad. Abe Shenitzer. Cambrige: The MIT Press, 1984.

Apêndice A

Ementa das disciplinas

A partir de 2006, entrou em vigência um novo Projeto Político Pedagógico[1], PPP, e um novo modelo de grade curricular, para os Cursos de Licenciatura e Bacharelado em Matemática da Universidade Federal do Paraná. Algumas mudanças que podem ser notadas são: a semestralização das disciplinas do curso e o processo de seletivo estendido[2].

Neste novo PPP, o curso de Bacharelado em Matemática existe para preparar profissionais para a carreira de ensino superior e para a pesquisa, enquanto o curso de Licenciatura em Matemática tem como objetivo principal a formação de professores para a educação básica e para a pesquisa sobre o ensino. Então, algumas escolhas como disciplinas mais específicas e dedicadas à Educação Matemática foram elaboradas para a Licenciatura. Outras, como as que compõem o eixo de Álgebra (Teoria de Números, Anéis e Grupos), por exemplo, foram concebidas para que pudessem ser ministradas tanto para o Bacharelado quanto para Licenciatura, deixando a cargo do professor a forma como lidar com as especificidades de cada uma das ênfases do curso.

A grade curricular anterior a esta mudança era a mesma para os dois períodos do curso, isto é, tanto para o período noturno quanto para o diurno. As disciplinas estavam distribuídas da seguinte forma:

1º ano: CM430 - Fundamentos da Matemática C; CM405 - Cálculo Diferencial e Integral C; CM412 - Geometria Analítica A; CI208 - Programação de Computadores (1º sem); CI202 - Métodos Numéricos (2º sem).

[1] O projeto pode visto no site http://www.mat.ufpr.br/graduacao/matematica

[2] Os detalhes sobre o funcionamento do processo seletivo estendido podem ser encontrados no site www.nc.ufpr.br

2º ano: CF406 - Física Geral A; CM406 - Cálculo Diferencial e Integral D; CM413 - Algebra Linear A; CD405 - Desenho Geométrico A; EP431 - Estrutura e Func. do ensino 1º e 2º Graus; ET401 - Psicologia da Educação A; Optativa 1; Optativa 2.

3º ano: CM415 - Análise Matemática A; CM419 - Álgebra A; CD415 - Elementos de Geometria; EM401 - Didática A; EM402 - Metodologia do Ensino de Matemática; CM036 - Tópicos de História da Matemática I (1º sem); CD025 - Projetos Integrados em Geometria (1º sem); CMP001 - Projetos Integrados em Educação Matemática I (2º SEM); CMP002 - Projetos Integrados em Educação Matemática II (2º sem).

4º ano: CF407 - Física Geral B; CM431 - Fundamentos da Matemática D; CD404 - Geometria Descritiva A; EM403 - Prática de Ensino e Estágio Supervisionado de Matemática A; CM432 - Fundamentos da Matemática Elementar A; EM061 - Prática de Ensino e Estágio Supervisionado de Matemática I (1ºsem); Optativa 3 (1º sem); Optativa 4 (2º sem).

Com novo currículo algumas adaptações na grade curricular, para o Curso de Licenciatura Noturno, o curso passou a ser feito em 9 semestre. As disciplinas dessa grade curricular estão distribuídas ao longo destes semestres da seguinte forma:

1º Semestre: CM118 - Geometria Analítica; CM119 - Funções.

2º Semestre: CM047 - Cálculo Diferencial e Integral I; CM100 - Complementos de Matemática; CM120 - Álgebra Linear I; CM127 - Fundamentos de Geometria.

3º Semestre: CD031 - Desenho Geométrico I; CF059 - Física I; CM048 - Cálculo Diferencial e Integral II; CM124 - Teoria de Números.

4º Semestre: CD030 - Geometria Dinâmica; CF060 - Física II; CM125 - Teoria de Anéis; CM139 - Cálculo Diferencial e Integral III.

5º Semestre: CD036 - Geometria no Ensino; CM121 - Equações Diferenciais e Aplicações; CM122 - Fundamentos de Análise; EP073 - Políticas e Planejamento da Educação. Brasileira; ET053 Psicologia da Educação.

6º Semestre: CE003 - Estatística II; CM123 - Análise na Reta; CM132 - Matemática no Ensino Fundamental; EP074 - Organização do Trabalho Pedagógico; ET054 - Processos Interativos na Escola.

7º Semestre: CF061 - Física III; CM126 - Teoria de Grupos; CM133 - Matemática no Ensino Médio; EM126 - Metodologia do Ensino de Matemática; EM200 - Didática I.

8º Semestre: CE068 - Cálculo de Probabilidades A; CM128 - Geometrias

Euclidianas e não-Euclidianas; CM134 - Trabalho de Conclusão de Curso para Licenciatura I; EM127 - Prática de Docência em Matemática I; Optativa 1.

9º Semestre: CM135 - Trabalho de Conclusão de Curso para Licenciatura. II; EM128 - Prática de Docência em Matemática II; Optativa 2; Optativa 3; Optativa 4; Optativa 5.

A.1 Ementas das disciplinas envolvidas nesta pesquisa

As ementas das disciplinas, que serão descritas nesta seção, são aquelas que estão ligadas a esta pesquisa[3], a saber: as disciplinas do currículo antigo Álgebra A e Fundamentos da Matemática C são disciplinas anuais e as disciplinas do novo currículo são Complementos de Matemática, Teoria de Números, Teoria de Anéis e de Grupo, sendo estas semestrais.

- **CM419 - Álgebra A**

  Carga horária: 120h (4 horas por semana)

  Ementa: Grupos. Homomorfismos de grupos. Anéis. Homomorfismos de anéis. Ideais de um anel. Anel quociente. Anéis de integridade. Corpo de frações de um anel de integridade. Anéis euclidianos. Polinômios sobre um anel.

- **CM430 - Fundamentos da Matemática C**

  Carga horária: 120h (4 horas por semana)

  Ementa: Noções de Lógica. Conjuntos e operações com conjuntos. Relações. Relações de Ordem. Relações de equivalência. Funções. Números naturais. Números inteiros, racionais, reais e complexos. Noções sobre Números Cardinais e Ordinais.

- **CM100 - Complementos de Matemática**

  Carga horária: 60h (4 horas por semana)

  Ementa: Introdução à lógica proposicional. Quantificadores. Técnicas de demonstração matemática. Relações. Funções. Indução matemática.

[3] As ementas das outras disciplinas podem ser encontradas no site http://www.mat.ufpr.br/graduacao/matematica

- **CM124 - Teoria de Números**

  Carga horária: 60h (4 horas por semana)

  Pré-requisito: CM100 - Complementos de Matemática

  Ementa: Apresentação Axiomática dos inteiros. Divisibilidade. Congruências. Números algébricos e transcendentes. Representações decimais finitas e infinitas. Aplicações.

- **CM125 - Teoria de Anéis**

  Carga horária: 60h (4 horas por semana)

  Pré-requisito: CM120 - Álgebra Linear I

  Ementa: Anéis, ideais, anéis quocientes e homomorfismos. Domínios de ideais principais, domínios de fatoração única, domínios euclidianos e aplicações. Polinômios, divisibilidade e fatoração em anéis de polinômios e raízes de polinômios. Corpos e extensões algébricas. Problemas clássicos. Aplicações.

- **CM126 - Teoria de Grupos**

  Carga horária: 60h (4 horas por semana)

  Pré-requisito: CM124 - Teoria de Anéis

  Ementa: Grupos, subgrupos e homomorfismos. Grupos de permutações. Grupos abelianos finitamente gerados. Ações de Grupos e aplicações a contagem. Extensões algébricas. Grupo de Galois de uma extensão. Correspondência de Galois e suas aplicações. Grupos solúveis. Resolução de equações por radicais. Aplicações.

Apêndice B

Dificuldades ligadas à aprendizagem dos conceitos de subgrupo normal e grupo quociente

B.1 Introdução

Este texto mostra os resultados obtidos pela aplicação do questionário elaborado pelas pesquisadoras Lajoie e Mura (2004) em um estudo apresentado no artigo *Difficultés liées à l´apprentisage des concepts de sous-groupe normal e de groupe quocient* (2004), para alunos que já cursaram a disciplina de Álgebra A, na Universidade Federal do Paraná (UFPR). O objetivo em replicar este estudo é o de verificar se os estudantes de UFPR apresentam as mesmas dificuldades identificadas por elas. Como este estudo foi realizado no Canadá, entendemos que é importante fazer esta réplica, para observar o que acontece com alunos da UFPR. Neste momento optou-se por aplicar somente o questionário, pois este estudo exploratório foi feito para nos dar ou não subsídios para justificar a hipótese do trabalho de tese de doutorado, que é a de que estas dificuldades estão relacionadas com o entendimento do conceito de congruências e dos conceitos relacionados a ela. Também por considerar que as dificuldades identificadas por Lajoie e Mura(2004) são pertinentes, levando em consideração a minha experiência como professora desta disciplina.

No referido artigo, as autoras apresentam as três dificuldades dos alunos, identificadas por elas, na aprendizagem dos conceitos de grupo quociente e subgrupo normal.

Para este estudo, o termo dificuldade está sendo entendido da mesma forma que o termo utilizado por Lajoie (2000) e Lajoie e Mura (2004), considerando como pista para identificar uma dificuldade, raciocínios incompletos ou incorretos e erros cometidos por várias pessoas.

Esta pesquisa de Lajoie e Mura foi feita em dois momentos, sendo que em um primeiro momento foram feitas entrevistas individuais com nove estudantes. As autoras utilizaram para análise das respostas dos alunos a perspectiva teórica de conceito imagem e conceito definição, proposta por Tall e Vinner (1981). De acordo com estas análises, elas apontam três dificuldades ligadas à aprendizagem dos conceitos subgrupo normal e grupo quociente, são elas:

1. reconhecer a definição de subgrupo normal;
2. entender a natureza dos elementos e a operação de um grupo quociente;
3. reconhecer o papel do subgrupo normal na construção de um grupo quociente.

Estas dificuldades foram analisadas e levantadas as hipóteses para justificá-las. Elas podem acontecer por:

1. fragilidade das definições pessoais;
2. falha nas noções básicas da teoria de conjuntos.

No segundo momento, foi aplicado um questionário para confirmar ou não as dificuldades encontradas na análise das entrevistas. Este questionário foi elaborado de acordo com as dificuldades e com as hipóteses levantadas anteriormente. Foi aplicado para 24 pessoas que já tinham feito um primeiro curso de álgebra abstrata, das universidades de Quebec e Montreal. As análises desses questionários apontaram o seguinte:

1. Reconhecer a definição de um subgrupo normal: uma dificuldade confirmada. Os estudantes não reconhecem a definição de subgrupo normal. Eles confundem esta definição com a definição de subgrupo central, ou comutativo, além de escolher mais de uma alternativa, como se fossem definições equivalentes.
2. Entender a natureza dos elementos e da operação de um grupo quociente: uma dificuldade com nuances realçadas pela análise dos questionários. Apesar de grande parte dos estudantes reconhecerem que os elementos do grupo quociente

são classes de equivalência, consideram que estes podem ser elementos do grupo de partida e/ou que o grupo quociente pode ser subgrupo do grupo de partida.

3. Reconhecer o papel de um subgrupo normal na construção de um grupo quociente: uma dificuldade com nuances realçada na análise do questionário. Apesar de a maioria dos estudantes afirmarem que o subgrupo N deva ser normal para que se possa construir um grupo quociente, eles não conseguem justificar satisfatoriamente porque isso deva acontecer.

Algumas diferenças com o estudo replicado devem ser apontadas. As pesquisadoras canadenses aplicaram este questionário para vinte e quatro (24) estudantes do primeiro ciclo da universidade, em Quebec. Dentre esses estudantes, dez (10) estavam fazendo o segundo curso de Álgebra, obrigatório para o curso de bacharelado em Matemática. Os outros quatorze (14) estudantes tinham terminado no semestre anterior o primeiro curso de Álgebra.

No caso desta pesquisa, dezessete (17) estudantes voluntários responderam o mesmo questionário proposto por Lajoie e Mura(2004). Dentre estes, quatro (4) eram estudantes do bacharelado em Matemática e estão cursando a segunda disciplina de Álgebra, obrigatória para esta modalidade. Os outros treze (13) estudantes terminaram o primeiro curso de Álgebra, em sua maioria, em 2006, com exceção de dois (2), um terminou em 2005 e outro em 1999.

O questionário foi aplicado em três turmas, duas durante a aula da disciplina Fundamentos da Matemática D, para sete (7) estudantes no período noturno, que foram chamados $N_1, N_2, ...N_7$ e para seis (6) estudantes no período vespertino, que foram identificados por $T_1, T_2, ..., T_6$, e outra durante a aula da disciplina Álgebra B para quatro (4) estudantes identificados por $B_1, ...B_4$.

Outros aspectos a serem observados são relativos ao tempo transcorrido entre o término desta disciplina Álgebra A e a aplicação deste questionário; e o fato desta disciplina ser uma disciplina de final de curso, em que os conceitos estudados não foram mais utilizados pela maioria dos estudantes, exceto pelos estudantes da disciplina Álgebra B.

B.2 Análise dos dados

Para esta análise, foram consideradas as respostas das questões de número 3 a número 10, que estão relacionadas com o conteúdo da pesquisa em questão. Os estudantes res- ponderam a outras duas questões, sobre a nota na disciplina Álgebra, se estavam ou não matriculados em Álgebra B e sobre suas impressões gerais sobre a disciplina.

As respostas a estas questões foram categorizadas inicialmente em números de estudantes que responderam ou não res- ponderam, ou seja, que responderam sim ou não, com ou sem justificativa a questão. Depois foi feito um refinamento desta categoria com as respostas corretas e justificativas parciais ou incorretas, exceto a questão 4 que foi categorizada acordo com a quantidade de alternativa escolhida.

A análise das questões foi feita em dois momentos. Primeiramente, uma análise foi feita somente pela pesquisadora. Depois de categorizadas as respostas, houve uma segunda análise com a participação do Prof. Marcelo Muniz Silva Alves, professor do Departamento de Matemática da UFPR e que, no momento em que este questionário foi aplicado, era o professor da disciplina Álgebra A. Com esta segunda análise, algumas respostas receberam outras interpretações que serão relatadas no decorrer desta seção.

- Questão 3: *Seja* $\{S_1, S_2, ..., S_n\}$ *uma partição de um conjunto* E *e seja* x *um elemento de* E*. Podemos afirmar que* $x \in \{S_1, S_2, ..., S_n\}$*? Justifique sua resposta.*

  Objetivo: Observar as eventuais dificuldades para distinguir entre as relações de inclusão e pertinência e para distinguir um conjunto da união de seus conjuntos.

  A resposta desta questão é "não", pois o x é um elemento de E e não um conjunto de sua partição.

  O quadro abaixo mostra como estão distribuídos os estudantes de acordo com a resposta dada a esta questão:

Resposta	Estudante
sim com just.	$B_3, B_2, N_7, T_4, N_5, T_6$
não com just.	B_4, T_2, N_4, T_3
não sem just.	N_1, N_2, N_3
não fez e outros	$B_1, T_5, N_6\ T_1$

Dos sete (7) estudantes que responderam "não" a esta questão, apenas um justificou corretamente a sua resposta; outros três (3) deram justificativas errôneas como por exemplo T_3, que escreveu: "Não, pois $\{x\} \in$ ao conjunto $\{S_1, S_2, ..., S_n\}$, pois para algum $S_i = \{x\}$, e não o elemento $x´´$. Esta resposta nos leva a pensar que o aluno entende as relações de pertinência e de inclusão e aceita o fato de um conjunto ser elemento de outro conjunto, mas não compreendeu o que é uma partição. Os outros três (3) estudantes não justificaram suas respostas.

Dentre os seis (6) estudantes que responderam sim a esta questão, quatro (4) deles justificaram da seguinte forma:

se $\{S_1, S_2, ..., S_n\}$ é uma partição de um E, então $E = S_1 \bigcup S_2 \bigcup ... \bigcup S_n$, logo $x \in S_i$, para algum $i = 1, 2, ...n$.

Esta resposta indica confusão entre as relações de pertinência e inclusão, pois, para eles, se $x \in S_i$, para algum $i = 1, 2, ..., n$, então $x \in \{S_1, S_2, ..., S_n\}$.

Um aluno T_1 não conseguiu dizer se a afirmativa era verdadeira ou falsa, e justificou da seguinte forma: "Pode ser que sim ou que não, pois uma partição de um conjunto não é o conjunto todo". Uma resposta como esta indica que este aluno também não compreendeu o que é partição de um conjunto.

As respostas destes estudantes apontam que existe aqui a confusão entre as relações de inclusão e pertinência, não compreenderam o que é partição de um conjunto e também que os estudantes não conseguiram entender conjunto de conjunto.

- Questão 4: *Diga se cada uma das afirmações abaixo é verdadeira ou falsa: N é um subgrupo normal de G se e somente se...*

  (i)$\forall a \in N, \forall b \in G : ab = ba$

  (ii)$\forall a \in N, \forall b \in N : ab = ba$

  (iii)$\forall a \in N, \forall b \in G, \exists c \in G : ab = bc$

  (iv)$\forall a \in N, \forall b \in G, \exists c \in N : ab = bc$

  Objetivo desta questão era verificar se os estudantes podem reconhecer a definição de subgrupo normal, (iv), e se eles podem diferenciar esta definição da de subgrupo central, (i), da de subgrupo comutativo, (ii), ou de um enunciado que se

aplica não importa qual seja o subgrupo, (iii).

Nesta questão, a resposta correta é a (iv). Três (3) estudantes, N_6, B_1, T_2, não responderam esta questão. A tabela abaixo mostra a distribuição de respostas de acordo com a alternativa escolhida como verdadeira pelos estudantes:

Resposta	Estudante
item i) verdadeiro	$N_2, N_3, N_4, N_5, N_7, T_1, T_3, T_4, T_5, T_6, B_4$
item ii) verdadeiro	$N_1, N_2, N_3, N_4, T_4, T_5, T_6$
item iii) verdadeiro	B_4
item iv) verdadeiro	N_1, N_3, N_4, B_2, B_4

Observamos que alguns estudantes escolheram mais de uma alternativa como verdadeira. Embora cinco (5) estudantes escolheram somente uma alternativa, apenas um aluno, B_2, escolheu a alternativa correta (iv), os outros quatro (4) responderam a alternativa (i), que é, na verdade, a definição de subgrupo central. Esta escolha pode ter sido feita pela semelhança da notação utilizada nos livros, que diz que um subgrupo N de G é normal quando $Nb = bN, \forall b \in G$ (veja Garcia e Lequain, 2005). Os estudantes podem ter pensado que, se simplesmente substituíssem N por um elemento $a \in N$, ou seja, verificassem esta comutatividade, teriam N um subgrupo normal. Esta interpretação foi feita com a participação do Professor Marcelo. Dentre todos os estudantes que responderam esta questão, onze (11) escolheram a alternativa (i), o que pode servir de indício de que a notação contribuiu para o resultado das respostas obtidas.

Outros quatro (4) estudantes escolheram a alternativa correta, (iv). Porém, também outras alternativas foram escolhidas, que pode ser um indício de que os estudantes não conseguiram fazer distinção entre as definições de subgrupo central, comutativo e normal, além de pensarem nestas definições como equivalentes.

Outros quatro (4) estudantes escolheram mais de uma alternativa, mas sem incluir a correta, e três (3) estudantes deixaram de responder esta questão.

Levando em conta o resultado geral, podemos entender que os estudantes têm a ideia de que a definição de subgrupo normal tem algo a ver com a comutatividade; contudo, eles não foram capazes de distinguir os elementos envolvidos.

- Questão 5: *Para construir o grupo quociente G/N, N deve ser necessariamente um subgrupo normal de G? Justifique sua resposta.*

  Objetivo: Determinar se os estudantes sabem que um subgrupo deve ser normal para construir um grupo quociente e se eles podem explicar por quê.

  A resposta a esta questão deveria ser "sim". A justificativa é que o subgrupo ser normal, garante que a operação do grupo quociente esteja bem definida.

  O quadro abaixo mostra como estão distribuídos os estudantes de acordo com a resposta dada a esta questão:

Tipo de resposta	Estudante
sim com just.	T_3, B_4, B_3, N_4, N_5
não com just.	N_1
sim sem just.	$T_1, T_5, T_6, B_2, N_2, N_7$
não fez	T_2, T_4, B_1, N_3, N_6

  Das pessoas que responderam sim, apenas um (1) respondeu corretamente, as outras não lembram o porquê desta necessidade (dois (2) estudantes) ou deram justificativas incorretas como, por exemplo, N_4, que justificou da seguinte forma: "... Sim, pois G e N devem satisfazer as mesmas propriedades", provavelmente fazendo referência às propriedades de grupo. Ou como B_4, que justificou da seguinte maneira: "... para que possamos dividir em classe de equivalências, usando a relação mod N". O que não está correto, pois, para "dividir" em classes de equivalência, basta que N seja subgrupo, não é necessário que o subgrupo N seja normal. Podemos perceber aqui que o papel desta relação na construção de um subgrupo normal não está bem entendido, bem como o papel do subgrupo normal na construção do grupo quociente.

  A justificativa dos dois (2) estudantes que responderam não a esta questão, é que eles não se lembravam o porquê do subgrupo não ser necessariamente normal.

  Observamos que, apesar de entenderem que o subgrupo deve ser normal para a construção do grupo quociente, a maioria não conseguiu justificar o porquê desta exigência, o que parece indicar que o papel do subgrupo normal na construção do grupo quociente não foi compreendido pelos estudantes.

- Questão 6: *Os elementos de G/N podem ser elementos de G? Justifique sua resposta.*

  Objetivo: Determinar se encontramos a ideia de que os elementos de um grupo quociente G/N são elementos de G e, se for este o caso, conhecer as razões.

  A resposta a esta questão deve ser "não", pois os elementos do grupo quociente não são da mesma natureza que os elementos do grupo.

  O quadro abaixo mostra como estão distribuídos os estudantes de acordo com a resposta dada a esta questão:

Tipo de resposta	Estudante
sim com just.	T_3, N_4, T_1, T_5
não com just.	B_1, B_2, B_3, B_4
não sem just.	N_2
sim sem just.	N_1, N_5, N_7, T_6
não fez	T_2, T_4, N_3, N_6

  Dentre as pessoas que responderam e justificaram sua resposta, quatro (4) responderam corretamente e quatro (4) responderam sim com justificativas diversas, como os três (3) estudantes que deram a seguinte justificativa: "...se $N \subset G$, N é subgrupo de G e os elementos de G/N podem ser elementos de G". O outro estudantes, T_5, escreveu o seguinte: "...sim, pois "passar" o quociente é como restringir os elementos de G a um determinado conjunto, e essa restrição pode cair dentro de G", isto pode indicar uma confusão entre as classes e seus representantes, como, por exemplo, $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ e seus representantes $0, 1, 2 \in Z$ esta interpretação foi feita em conjunto como professor Marcelo. Anteriormente havíamos entendido que esta resposta indicava apenas problemas com partição de um conjunto.

  Podemos observar que o fato de N ser subgrupo de G levou estes estudantes a entenderem que os elementos de G/N serem elementos de G, e podemos pensar, então, que a natureza do elemento de G/N, não foi bem compreendida.

  Apenas um estudante respondeu "não", mas não justificou e outros três (3) responderam afirmativamente, mas não justificaram.

Os estudantes que justificaram esta questão corretamente foram os estudantes matriculados em Álgebra B. A maioria não conseguiu entender a diferença na natureza dos elementos.

- Questão 7: *Você pode estabelecer uma relação entre a expressão "grupo quociente" e o sentido de "quociente" aritmético?*

  Objetivo: Determinar se relações impróprias foram estabelecidas entre os grupos quocientes e os quocientes aritméticos.

  Esta questão faz mais sentido no contexto da pesquisa das professoras canadenses, pois, durante as entrevistas, alguns estudantes disseram sobre grupo quociente que: "... um grupo quociente é "a divisão do grupo por seu subgrupo..." Assim $Z/2Z$ ele considera como sendo Z " dividido por dois" e $Z/3Z$ "separado em três"..." (LAJOIE e MURA, 2004, p. 58), por este motivo elas colocaram esta questão no questionário.

  O quadro abaixo mostra como estão distribuídos os estudantes de acordo com a resposta dada a esta questão:

Tipo de resposta	Estudante
sim com just.	N_7, B_1, B_3, B_4
não sem just.	T_1, T_3, T_5
sim sem just.	N_1, N_2
não fez	$N_3, N_4, N_5, N_6, T_2, T_4, T_6, B_2$

  Dentre as pessoas que responderam, mas não justificaram sua resposta, três (3) não estabelecem relação e duas (2) estabelecem, mas não especificam qual.

  Nesta questão não há, no nosso entendimento, uma resposta correta, ela pode mostrar as estratégias que os estudantes utilizam para entender algum conceito, como por exemplo, B_1 que respondeu: "... é como se você tivesse dividindo os elementos de um corpo entre conjuntos, os quais são as classes de equivalência".

- Questão 8: *Um grupo quociente G/N pode ser um subgrupo de G? Justifique sua resposta.*

  Objetivo: Determinar se G/N é considerado um subgrupo de G e encontrar, caso seja, as razões que levaram as pessoas a responderem que sim.

A resposta para esta questão é "não"; novamente a justificativa está na natureza diferente dos elementos de G/N e G.

O quadro abaixo mostra como estão distribuídos os estudantes de acordo com a resposta dada a esta questão:

Tipo de resposta	Estudante
sim com just.	T_6
não com just.	B_1, B_2, B_3, B_4
sim sem just.	$N_1, N_2, N_5, N_7, T_1, T_4, T_6$
não sem just.	T_5
não fez	N_3, N_4, N_6, T_2

Vemos que sete (7) estudantes responderam sim, que o grupo quociente G/N pode ser subgrupo G, apesar de não justificarem sua resposta. O aluno T_3, que respondeu sim e justificou sua resposta, dizia o seguinte: "... N é um subgrupo de G, logo G/N pode ser subgrupo de G (G/N é formado pelos elementos de G)". Por esta resposta, podemos pensar que o aluno não entendeu a natureza dos elementos de um grupo quociente, e, mais ainda, que não compreendeu que o grupo quociente não é subconjunto de G.

Dos quatro (4) estudantes que responderam "não" a esta questão, três (3) justificaram corretamente, e um deles deu uma justificativa que podemos considerar parcial, pois se nota que o estudante entende que a natureza do elementos de G/N é diferente dos elementos de G. O estudante B_3 escreveu: "... Não, a soma de classes no grupo quociente é uma classe, não um elementos de G".

Pode-se pensar que a natureza dos elementos do grupo quociente não está bem entendida para os estudantes que não responderam corretamente.

- Questão 9: *Seja G/N um grupo quociente. É verdade que efetuando o produto de G/N por N, encontramos G? Justifique sua resposta.*

  A resposta a esta questão é "não"; este "quociente" não é uma operação.

  O objetivo era determinar se os estudantes veem sentido no "produto" de G/N por N e se eles aceitam a ideia desse produto ser G. Esclarecer, caso possível, qual o sentido para esta afirmação.

Novamente esta questão faz mais sentido no contexto da pesquisa canadense, pois, durante as entrevistas alguns estudantes entenderam como Dominic que "... visualizou o grupo quociente G/N como aquele que "multiplicado" por N dá G..." (LAJOIE e MURA, 2004, p. 58).

O quadro abaixo mostra como estão distribuídos os estudantes de acordo com a resposta dada a esta questão:

Tipo de resposta	Estudante
não com just.	N_7
não sem just.	T_1, N_2
sim sem just.	T_5
não fez	$T_2, N_4, N_1, N_6, N_3, N_5, B_2, T_6, T_4, N_5$
outros	T_3, B_4, B_3, B_1

Nesta questão, dois estudantes responderam que depende do produto para que isso possa acontecer, apenas uma justificou corretamente, uma justificativa incorreta foi dada por N_7, que disse: "Não. Pois estaremos apenas encontrando os mesmos divisores de G/N".

Entre os dezessete (17) estudantes que responderam ao questionário, dez (10) deles não responderam esta questão, parece que a maioria não entendeu o enunciado, por isso não respondeu. Os estudantes que responderam corretamente a maioria das questões anteriores, hesitaram ao responder esta; estes estudantes disseram não ver sentido na pergunta ou que dependia do produto.

- Questão 10: *Os elementos de um grupo quociente G/N são classes de equivalência? Se você respondeu sim, diga qual a relação de equivalência definida.*

  Objetivo: Determinar se os estudantes reconhecem que os elementos de um grupo quociente são classes de equivalência e se eles podem descrever a relação de equivalência Correspondente.

  A resposta a esta questão é sim, a relação que define as classes é: $\forall x, y \in G, x \equiv y \Leftrightarrow \exists h \in N$, tal que $x = yh$ ou $y^{-1}x \in H$ esta relação define a classe lateral à esquerda, também poderiam responder a classe lateral à direita.

  O quadro abaixo mostra como estão distribuidos os estudantes de acordo com a resposta dada a esta questão:

Tipo de resposta	Estudantes
sim com just.	B_1, B_2, B_3, B_4, N_5, N_7
sim sem just.	T_1, T_3, T_5, T_6, N_2, N_3
não fez	T_2, T_4, N_1, N_4, N_6

Dos doze (12) estudantes que responderam sim a esta questão, nenhum deles escreveu a relação de equivalência correta, três (3) escreveram a relação correta para o caso em que G é um grupo abeliano, como por exemplo B_2 que respondeu: "$g_1 \equiv g_2 \bmod N \Leftrightarrow g_1 - g_2 \in N$", três (3) escreveram uma relação que não é a correta, e quatro (4) disseram não lembrar qual a relação envolvida e dois (2) não justificaram sua resposta.

Doze das dezessete (17) pessoas que responderam este questionário, entendem que os elementos de G/N são classes de equivalência, mas não conseguem explicitar a relação que define estas classes. Esta questão deve ser relacionada com as questões 6 e 8 que tratam dos elementos de G/N.

B.3 As dificuldades encontradas

De acordo com os dados levantados nesta pesquisa, pode-se reconhecer as mesmas dificuldades identificadas por Lajoie e Mura (2004). Ou seja:

1. Reconhecer a definição de subgrupo normal. Os estudantes da pesquisa canadense não reconhecem a definição de subgrupo normal. Eles confundem esta definição com a definição de subgrupo central, ou comutativo, além de escolherem mais de uma alternativa, como se fossem definições equivalentes.

   Da mesma forma, os estudantes que responderam esta questão, apenas um deles respondeu corretamente, os outros estudantes escolheram mais de uma alternativa ou apenas a alternativa (i). Como a maior parte destes estudantes escolheu mais de uma alternativa, podemos considerar que para eles a definição de subgrupo normal parece, lembra, algo sobre a comutatividade, mas eles não conseguiram reconhecer os elementos e os conjuntos envolvidos nesta definição.

   Devemos atentar para o fato de que a notação utilizada pelas pesquisadoras, neste questionário, é diferente da usada pelos livros adotados no curso de Álgebra

da UFPR, veja Gonçalves (1979) e Garcia e Lequain (2005). Além disso, o apelo visual das definições favorece estas confusões e a linguagem utilizada nestas definições também contribui para isso, vejamos as definições destes subgrupos apresentadas nos livros:

Definição de subgrupo central: N é um subgrupo central de G se e somente se $\forall g \in G$, $\forall n \in N : gn = ng$.

Definição de subgrupo normal: N é um subgrupo normal de G se e somente se $\forall g \in G : gN = Ng$.

Definição de subgrupo comutativo: N é um subgrupo comutativo de G se e somente se $\forall a \in N$, $\forall b \in N : ab = ba$.

Nota-se que estas definições, como dito anteriormente, são na linguagem e no aspecto visual muito parecidas; no entanto, entendemos que o estudante que realmente entendeu estas definições, saberia responder corretamente a questão.

2. Entender a natureza dos elementos e a operação de um grupo quociente.

   Novamente esta dificuldade também está presente no nosso trabalho. No caso da pesquisa realizada no Canadá, apesar de a grande parte das estudantes reconhecerem que os elementos do grupo quociente são classes de equivalência, consideraram que estes podem ser elementos do grupo de partida ou que o grupo quociente pode ser subgrupo do grupo de partida. No caso desta pesquisa, os estudantes responderam que os elementos do grupo quociente G/N são classes de equivalência, mas também admitem que eles podem ser elementos de G, ou que G/N pode ser um subgrupo de G. É o que nos indica as respostas das questões 6, 8 e 10, vistas em conjunto.

   Dos dezessete (17) estudantes que responderam o questionário, cinco (5) deles responderam sim as questões 6, 8 e 10, ou seja, os elementos do grupo quociente G/N são classes de equivalência, mas também admitem que eles são elementos de G e que G/N pode ser um subgrupo de G. Um deles respondeu sim às questões 8 e a 10 e não à questão 6; outro respondeu sim à 6 e à 10 e não à questão 8 e quatro (4) estudantes responderam corretamente a 6 e 8 e sim à questão 10, embora a relação de equivalência descrita por eles é verdadeira apenas para o caso em que G é um grupo abeliano.

3. Reconhecer o papel do subgrupo normal na construção de um grupo quociente. Também esta dificuldade pode ser reconhecida nesta pesquisa, assim como os estudantes canadenses, os estudantes pesquisados afirmam ser necessário que o subgrupo N de G, seja normal para a construção do grupo quociente G/N, mas a maioria não consegue explicar por quê. No entanto, não temos dados suficientes para verificar o que os estudantes fariam com a operação no grupo quociente, se eles sentiram a necessidade de verificar se elas estão bem definidas ou se tomariam esta operação como algo adquirido, assim como os estudantes canadenses. Isso porque o questionário aplicado para os estudantes nesta pesquisa não tem nenhum exemplo em que os estudantes tenham que realizar operações com os elementos do grupo quociente.

Com isso, pode-se concluir que a análise dos dados coletados apontaram que as mesmas dificuldades encontradas por Lajoie e Mura (2004), entre seus estudantes no Canadá, também foram encontradas entre os estudantes na UFPR.

Entretanto, os dados coletados nesta pesquisa revelaram ainda uma dificuldade diferente das relatadas por Lajoie e Mura(2004), que está relacionada com os conceitos envolvidos na construção de um grupo quociente, conceito de partição de um conjunto.

As respostas encontradas para a questão 3 indicam que os estudantes não compreendem o que é uma partição, como se dá a formação das classes de equivalência como objeto, já que 4 das 17 pessoas que responderam esta questão entenderam que: o elemento x do conjunto E pertence a $\{S_1, S_2, ..., S_n\}$, onde $S_1, S_2, ...S_n$ é uma partição de E. Dubinsky et al. (1994) e Asiala et al. (1997),entendem que encapsular o processo de formação de classes em objeto é muito difícil. No entanto, este processo é importante na construção de vários outros conceitos, como, por exemplo, os conceitos de grupo e anel quociente.

Apêndice C

Estudo Histórico

C.1 Estudo histórico e epistemológico: mudanças nos fazeres matemáticos

Para fazer esta análise epistemológica procuraramos entender as rupturas epistemológicas (Bachelard, 2000) que ocorrer na passagem de um tipo de fazer matemático para outro, seguindo as ideias de Lorenzo (2005).

Consideramos que uma ruptura epistemológica acontece com a negação ou com a contradição com experiências do senso comum ou com alguma crença, e também em relação a conceitos científicos formalizados, ou seja, ruptura não é somente a rejeição da ciência do passado, senão também uma preservação por meio de reformulações de velhas ideias em um novo e mais amplo contexto do pensamento. Um exemplo disso é o desenvolvimento da Geometria não Euclidiana, este modelo rejeita a ideia de que os axiomas Euclidianos expressam a única verdade acerca da geometria e ao mesmo tempo apresentam postulados definindo uma classe mais geral de geometria. Estes processos de reposição ao geral são caracterizados, por Bachelard, como dialéticos, no sentido de que de um processo de expansão conceitual pelo qual o que previamente parece oposto é visto como possibilidade complementar, como, por exemplo, a geometria Euclidiana e a Lobachevskiana, que fazem parte como casos particulares de uma pangeometria (Bachelard, 2000).

Segundo Lorenzo (2005), o fazer matemático é uma prática dinâmica que vai se transformando e na qual se produzem rupturas epistemológicas, rupturas estas que têm suas consequências ontológicas, epistemológicas e metodológicas associadas, e isso nos

traz uma concepção de Matemática "...na qual se admite que nem tudo está dado de uma vez e para sempre, no universo da Matemática, no mundo sempre aberto da razão conceitual" (LORENZO, 2005, p. 398, tradução da autora). No mesmo trabalho, o autor relata algumas de suas experiências, como aluno e como professor de Matemática, de algumas mudanças de fazeres matemáticos, por exemplo, a mudança da álgebra "clássica" para álgebra "moderna". A primeira se dedica à resolução de equações algébricas, enquanto a segunda se dedica ao estudo das estruturas algébricas por si mesmas. Estas duas "versões" da álgebra exigem organizações teórica e metodológica diferentes "... uma se mostra como saber produtivo ou artístico e a outra como um saber epistémico" (LORENZO, 2005, p. 404, tradução da autora). Temos aqui, um exemplo de mudança de um ,fazer matemático clássico para um fazer matemático moderno. Esta mudança traz uma nova linguagem, novos objetos matemáticos, e requer do matemático um novo tipo de raciocínio. A Álgebra passa a ser mais demonstrativa, seus objetos são agora mais abstratos. Este é um exemplo muito ilustrativo da mudança do fazer matemático que Lorenzo chama de Figural para o Global.

Entendemos que o fazer matemático figural é aquele que está apoiado no concreto, que tende a ser mais prático e formulado para resolver problemas particulares, como, por exemplo, a teoria da divisibilidade de Euclides. Já por fazer matemático global entendemos aquele que pode ser formulado de forma geral, apoiado na linguagem da teoria de conjuntos, em que as relações entre os objetos são mais importantes do que o próprio objeto e cujo conhecimento é apresentado na forma axiomática, como, por exemplo, a teoria de grupos.

Um outro exemplo de mudança e fazer matemático do figural para o global, acontece na Geometria, quando Hilbert formula seus fundamentos de Geometria, ciência que deixa de ser concreta e material como a Geometria de Euclides e passa a ser formal e abstrata. Enquanto para a Geometria Euclidiana os axiomas são verdades absolutas e os objetos matemáticos são pontos, retas e planos, para a Geometria de Hilbert não há pontos de partida e nem objetos, o que importa são as relações entre eles.

São mudanças, como as descritas acima, que queremos identificar no desenvolvimento histórico da relação de congruência.

C.2 Um breve estudo histórico e epistemológico dos conceitos de congruência e grupo quociente

Nesta seção, faremos um breve estudo da trajetória histórica e epistemológica do conceito de congruência e como ele se apresenta no desenvolvimento do conceito de grupo quociente.Veremos algumas mudanças nos fazeres matemáticos pelas quais passaram estes conceitos. Nesta trajetória do fazer figural ao fazer global, estes conceitos passam por algumas 'fases' que identificaremos como uma fase instrumental, outra mais organizada e sistematizada, entre outras.

Uma relação de congruência é definida, atualmente, como uma relação de equivalência que é compatível com alguma operação. Esta definição nos indica que devemos considerar também o desenvolvimento da relação de equivalência.

De acordo com Fowler (1998), a relação de equivalência ou similaridade, pode ser explicitada como uma generalização da igualdade, que já era conhecida desde antes de Euclides. Podemos reconhecer, então, a ideia da relação de equivalência quando Euclides define igualdade entre números.

Observamos, também, a ideia de relação de equivalência no trabalho de Gauss Disquisitiones Arithmeticae, quando define congruência módulo m, denotada por $\equiv$, de dois inteiros a e b, da seguinte forma: "$...a \equiv b(mod\, m)$ se e somente se m divide $b - a$" GAUSS (1801). Neste trabalho, ele faz a primeira prova completa da lei da reciprocidade quadrática. Ele também mostrou que, para os restos, junto com a relação $\equiv$, satisfazem essencialmente as mesmas propriedades da relação $=$ para inteiros, ou seja Gauss mostrou que esta relação de equivalência é uma congruência. Em termos modernos isso significa que as classes de equivalência com respeito a relação $\equiv$ formam um anel. De acordo com Frei (1994), estes resultados já tinham sido obtidos por Euler em seu trabalho "Tractatus de numerorum doctrina", de 1750, mas de forma menos concisa.

Assim, temos uma mudança no fazer matemático, de fazer instrumental, em que as noções eram utilizadas apenas para resolver um determinado problema, sem a formulação da teoria, a um fazer racional, onde podemos encontrar definições e demonstrações de propriedades sobre congruência módulo m. No entanto, Lorenzo (2005) afirma que, apesar de sistematizada e organizada, a teoria de Gauss ainda não está formulada de forma axiomática, no sentido do fazer global, o que nos leva a entender

que este ainda é um fazer figural; mesmo assim, a noção de relação de congruência é mais abstrata.

O desenvolvimento do conceito de relação de congruência pode ser encontrado também no desenvolvimento do conceito de grupo quociente, como podemos reconhecer em Nicholson (1993), em cujo artigo a autora analisa as contribuições dos matemáticos Galois, Betti, Jordan, Dedekind, Dyck e Hölder no desenvolvimento deste conceito de grupo quociente.

De acordo com artigo de Nicholson (1993), podemos reconhecer o conceito de congruência mais fortemente nos trabalhos de Jordan, quando ele, fazendo uma analogia com a congruência módulo m, definida por Gauss, define congruência segundo um grupo H, que dá origem à definição atual de subgrupo normal. Sua definição foi a seguinte: "...duas substituições s e t, que comutam com um grupo H, são chamadas congruentes segundo o grupo H, se podem ser escrita da seguinte forma $s = th$, onde h é uma substituição de H. Podemos expressar esta relação pela fórmula análoga a das congruências ordinárias: $s \equiv tmodH$ ..." (JORDAN, 1873, apud NICHOLSON, 1993, p. 74, tradução da autora).

Jordan mostrou ainda que, se $s \equiv tmod\,H$ e $s' \equiv t'mod\,H$, então $ss' \equiv tt'\,mod\,H$, provando que a multiplicação em sua estrutura quociente estava bem definida e, portanto, podia ser considerada como um grupo. Sendo G um grupo gerado por $s_1, s_2, ...$ na forma normal, então, ele denotou por G/H (notação moderna) o grupo das substituições da forma $mod\,H$, ou seja, o grupo quociente de Jordan consiste de todas as classes de congruência dos elementos $s_1, s_2, ...$ do qual G é formado. Dessa forma, os elementos do grupo quociente não são os mesmos elementos de G, eles são os representantes de cada uma das classes de congruência.

Apesar das ideias de Jordan serem bastante abstratas, ele ainda manteve seus trabalhos dentro dos limites da teoria de grupo das substituições, ou seja, ele estava trabalhando com um grupo particular, o que nos leva a crer que este conceito deve ser considerado ainda dentro do fazer figural. Depois desses trabalhos, o processo da construção do grupo quociente, que entendemos hoje como sendo a utilização da relação de equivalência para construir uma partição do conjunto inicial, que são ideias mais abstratas, foram incorporadas ao estudo de grupos, a tal ponto que podemos ver o desenvolvimento e o entendimento do papel da relação de equivalência refletido no desenvolvimento do conceito de grupo quociente.

No desenvolvimento do conceito de relação de equivalência, principalmente no uso de classes de equivalência como objetos matemáticos, encontramos nomes como Dedekind, Cantor, Frege, Hölder e outros, veja Nichonson (1993, p. 76). Destes matemáticos, tanto Nicholson (1993), quanto Fowler (1998), creditam a Dedekind a utilização mais geral destes conceitos, não só no contexto da teoria de grupos, passando então a relação de equivalência ser formulada dentro do fazer global. A Hölder é creditado a explicitação e sistematização do conceito de grupo quociente. Hölder mostrou, por exemplo, que os elementos do grupo podem ser divididos entre as classes de qualquer subgrupo H e que se H é um subgrupo normal, então a multiplicação de duas classes teria como resultado uma terceira, ou seja, ele mostrou que, neste caso, a multiplicação de classes está bem definida.

Este breve estudo nos dá pistas de como os desenvolvimentos históricos dos conceitos de relação de congruência e grupo quociente estão ligados.

Apêndice D

Questionário para entrevista

Questionário para entrevista.

Nome:

Período:

1. i) Mostre que $2^4 \equiv 2(mod 7)$.

   ii) Mostre que $2^{45} \equiv 1(mod 7)$.

   Quais propriedades usadas para resolver o item i) você usou para resolver o item ii)?

2. Você concorda com algum destes argumentos? Justifique sua resposta. Se não concorda justifique também.

   i) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ são elementos de $\mathbb{Z}$, pois $\mathbb{Z}/5\mathbb{Z}$ são múltiplos de 5, e, portanto, são números inteiros.

   ii) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ não são elementos de $\mathbb{Z}$, porque eles são do tipo $\frac{n}{5}$ e, portanto, pertencem a $\mathbb{Q}$.

   iii) Os elementos de $\mathbb{Z}/5\mathbb{Z}$ não são elementos de $\mathbb{Z}$, porque eles são classes de equivalência e não números inteiros.

   Se você não concorda com nenhum desses argumentos, como você responderia a questão: elementos de $\mathbb{Z}/5\mathbb{Z}$ podem ser elementos de $\mathbb{Z}$?

3. Seja $\{S_1, S_2, ..., S_n\}$ uma partição de um conjunto E e seja x um elemento de E. Podemos afirmar que $x \in \{S_1, S_2, ..., S_n\}$? Justifique sua resposta.

   Sendo $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, podemos afirmar que:

a) $10 \in \mathbb{Z}_7$;

b)$\overline{10} \in \mathbb{Z}_7$.

4. Descreva os anéis $\mathbb{Z}_4$ e $\mathbb{Z}_8$. Indique alguma diferença entre eles. Podemos afirmar que $\mathbb{Z}_4$ é subanel de $\mathbb{Z}_8$?

5. i) Construa, passo-a-passo, o anel quociente $\mathbb{Z}_6$.

   ii) Encontre um ideal deste anel com 3 elementos.

   iii) Faça o quociente de $\mathbb{Z}_6$ com o ideal que você encontrou.

   iv)Encontre um anel que seja isomorfo ao quociente encontrado.

   v) O que seria $\mathbb{Z}_6/\overline{8}\mathbb{Z}_6$?

6. Se um colega de curso pedisse para você explicar o que é conguência módulo m, como você explicaria? E se ele perguntasse o que é um anel quociente, como você explicaria?

Apêndice E

Respostas aos questionários

Este apêndice traz as respostas dos estudantes as dois questionários aplicados aos estudantes.

E.1 Primeiro questionário

O questionário sobre congruência módulo m era composto pelas seguintes questões:

1. Como você explicaria, para um aluno do primeiro ano do Curso de Matemática, o que é a congruência módulo m? Justifique sua resposta.

2. Qual o resto da divisão de $n = (121 \cdot 35 + 282 \cdot 75)$ por 4. Justifique sua resposta.

3. Mostre que $2^{13} \equiv 2 \pmod 7$. Justificando sua resposta.

4. Considere o conjunto $\overline{a} = \{x \in \mathbb{Z}; x \equiv a \pmod m\}$.E este conjunto é chamado *classe de congruência de a módulo m*, ou seja, o conjunto cujos elementos são todos os inteiros congruentes a a módulo m.

   As classes de congruência módulo 4, isto é, $\overline{a} = \{x \in \mathbb{Z} | x \equiv a \pmod 4\}$, são:

$$\overline{0} = \{0, 4, 8, ..., 4k\}, \text{ com } k \in \mathbb{Z}.$$
$$\overline{1} = \{1, 5, 9, ..., 1 \pm 4k\}, \text{ com } k \in \mathbb{Z}.$$
$$\overline{2} = \{2, 6, 10, ..., 2 \pm 4k\}, \text{ com } k \in \mathbb{Z}.$$
$$\overline{3} = \{3, 7, 11, ..., 3 \pm 4k\}, \text{ com } k \in \mathbb{Z}.$$

Encontrando todas as classes de congruência módulo m dos elementos de $\mathbb{Z}$, temos o conjunto quociente $\mathbb{Z}_m = \{\overline{a} \,|\, a \in \mathbb{Z}\}$ é o conjunto de todas estas classes e é denotado por $\mathbb{Z}/\equiv_m$ ou $\mathbb{Z}_m$.

O conjunto de todas as classes de congruência módulo 4, $\mathbb{Z}_4$ é o conjunto $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, com apenas quatro elementos, já que $\overline{4} = \overline{0}$, $\overline{5} = \overline{1}$, $\overline{6} = \overline{2}$ e assim por diante.

Considerando, agora, o conjunto de classes de congruência módulo 7, isto é, $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, podemos dizer que:

(a) $10 \in \mathbb{Z}_7$. Justifique sua resposta.

(b)$\overline{10} \in \mathbb{Z}_7$. Justifique sua resposta.

E.1.1 As respostas

Respostas do estudante A1

1. Como você explicaria para um aluno do primeiro ano do Curso de Matemática o que é a congruência módulo m? Justifique sua resposta. Congruência módulo m é uma relação $a \equiv b \pmod m$ tal que $b/(a-m)$, ou seja, $b \cdot s = a - m$, $s \in \mathbb{Z}$.

2. Qual o resto da divisão de $n = (121 \cdot 35 + 282 \cdot 75)$ por 4. Justifique sua resposta.
$(30 \cdot 4 + 1)(4 \cdot 8 + 3) + (4 \cdot 70 + 2)(4 \cdot 18 + 3)$
$r = 3 + 6 = 9/4 \Rightarrow r = 1$

3) Sabemos que $2^3 \equiv 2 \pmod 7$

$2^{13} = 2^3 \cdot 2^{10} = 2^3 \cdot 2^3 \cdot 2^3 \cdot 2^3 \cdot 2^1$

mas $2^3 \equiv 2 \pmod 7$

$2^{13} \equiv 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \pmod 7$

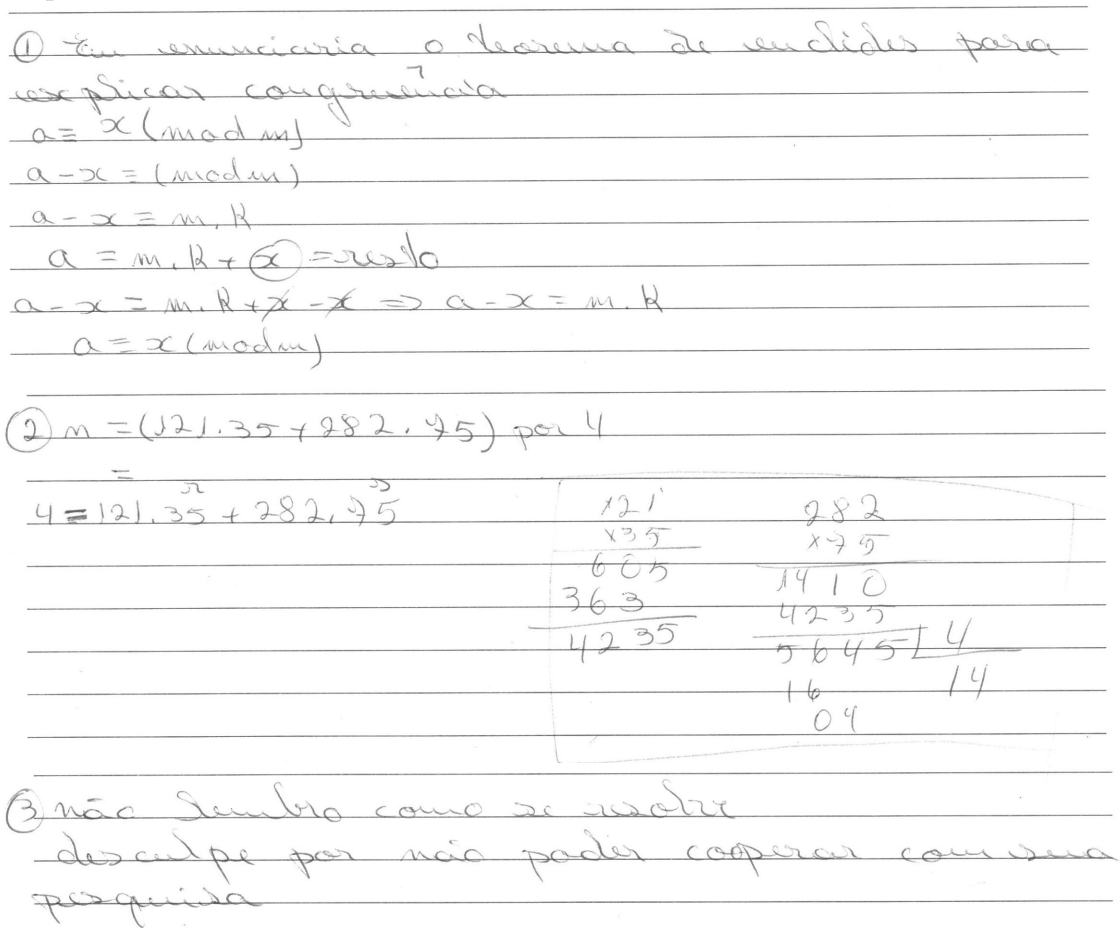
$2^{13} \equiv 2^3 \cdot 2 \cdot 2 \pmod 7$

$2^{13} \equiv 2 \cdot 2 \cdot 2 \pmod 7$

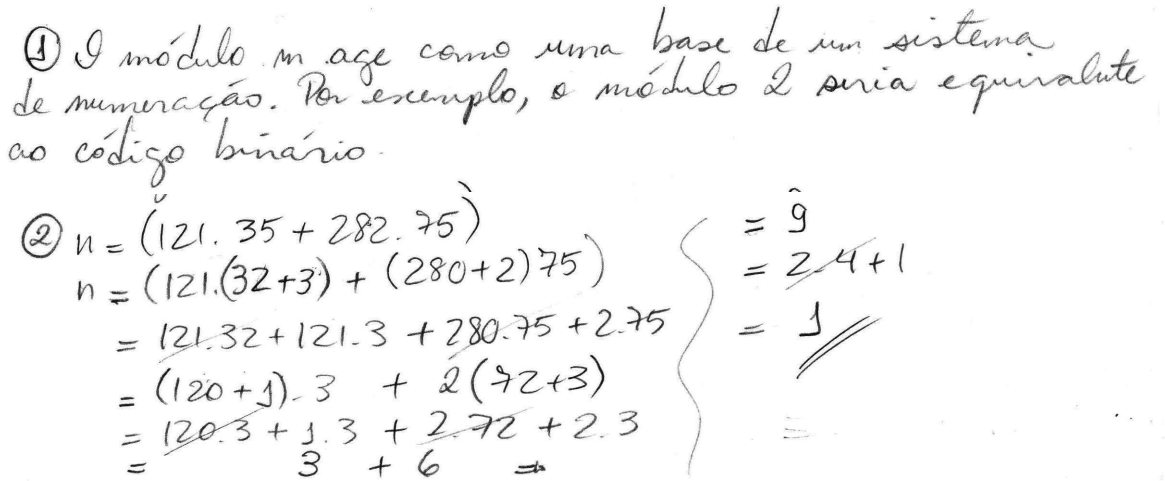
$2^{13} \equiv 2^3 \pmod 7$

$2^{13} \equiv 2 \pmod 7$

Respostas do estudante A2



Respostas do estudante A3



③

$2^{13} \equiv 2 \pmod 7$

$2^{6+6+1} \equiv 2 \pmod 7$

$2^6 . 2^6 . 2 \equiv 2 \pmod 7$

por fermat:

$2 \equiv 2 \pmod 7$

$a^{p-1} \equiv 1 \pmod p$

Respostas do estudante A4

(1) Sejam os grupos de números que, quando divididos por m, dão um mesmo valor como resto.

$a \equiv x \pmod m$ é o mesmo que $a = b.m + x$. $\begin{cases} b = \text{fator multiplicativo de } m \\ x = \text{resto} \end{cases}$

(2) $121.35 + 282.75$ dividido por 4.

$121 = 120+1 = 4.30+1$ $\quad 35 = 8.4+3$

$282 = 280+2 = 4.70+2.$ $\quad 75 = 18.4+3$

$(4.30+1)(8.4+3) + (4.70+2)(18.4+3)$

$3 + 6 = 9$ $\quad 9 \equiv 1 \pmod 4$

Decompus os números, separei os restos e os somei, deu 9, mas nove quando dividido por 4 dá resto 1, que é o resto de toda a divisão.

(3) $2^{13} \equiv 2 \pmod 7$

sei que $2^6 \equiv 1 \pmod 7$ → por 7 é primo (acho que pelo Teorema de Euclides)

$(2^6)^2 \equiv 1^2 \pmod 7$ → posso elevar ao quadrado que a congruência é preservada.

$2^{12} \equiv 1 \pmod 7$

$2.2^{12} \equiv 1.2 \pmod 7$ →

$2^{13} \equiv 2 \pmod 7$

(4) (a) Sim, pois $10 \equiv 3 \pmod 7$.

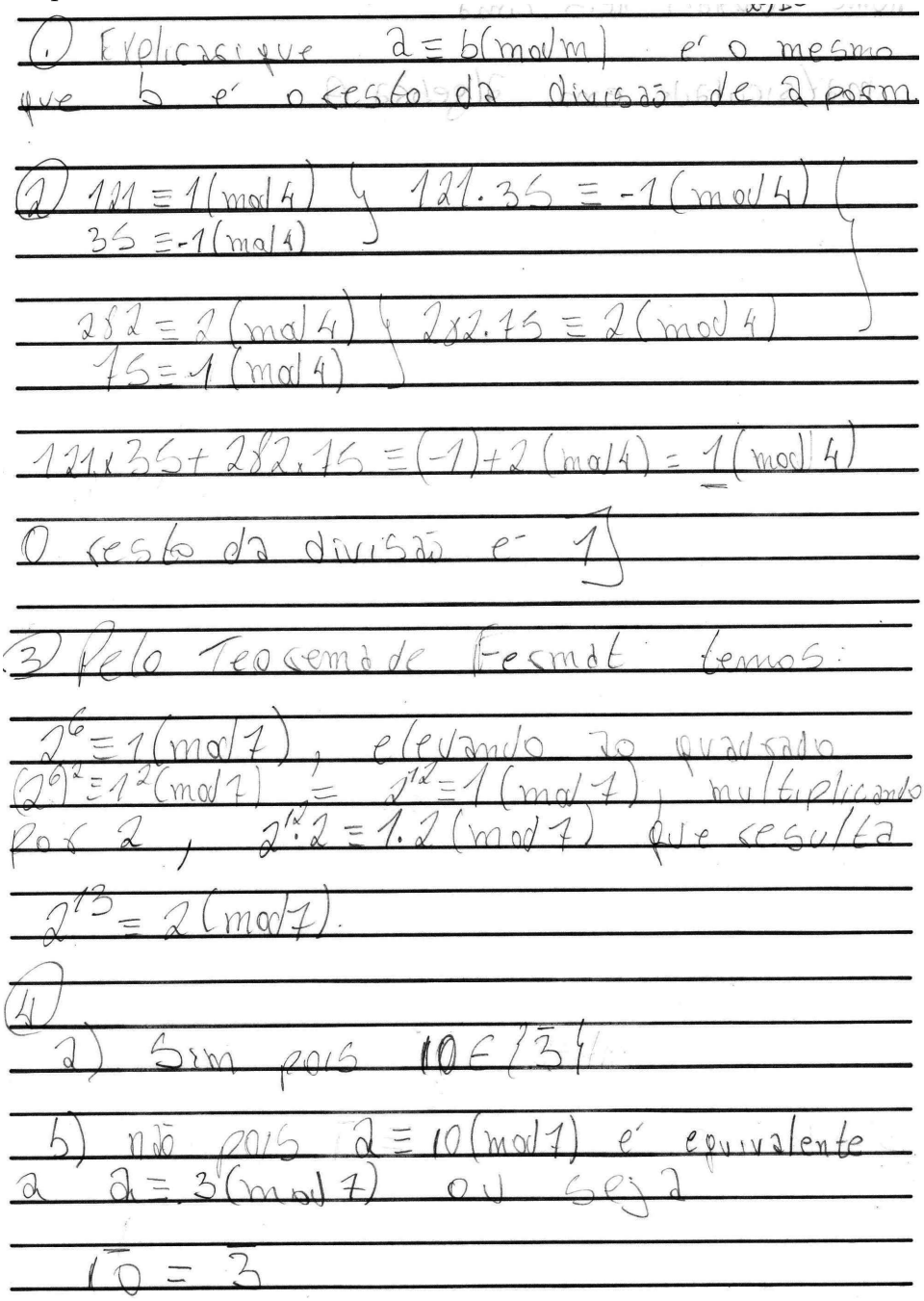
$\therefore 10 \in \overline{3} \subset \mathbb{Z}_7$.

O resto da divisão de 10 por 7 é 3, então 10 pertence a $\overline{3}$, isto é, os números congruentes a 3 módulo 7. Como este conjunto está contido em $\mathbb{Z}_7$, $10 \in \mathbb{Z}_7$.

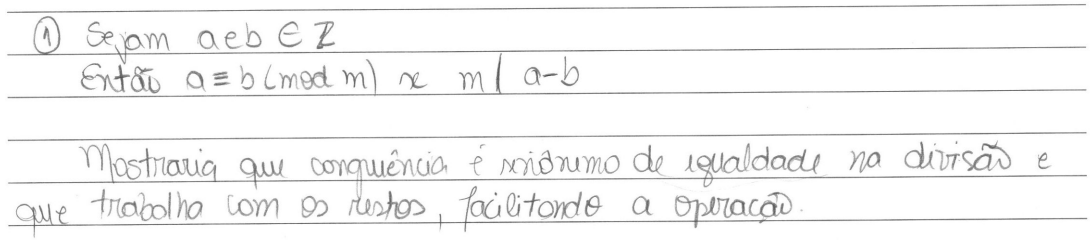
(b) Sim, pois $\overline{10} = \overline{3}$, isto é o número que apresenta 10 como resto da divisão por 7, quando divididos novamente dão resto 3.

Ao dividir a por 7 e ter resto 10, $10 > 7$ o resto deve ser menor que 7, se não dá pra dividir de novo, daí sai o resto 3.

Respostas do estudante A5



Respostas do estudante A6



② $n = (121 \cdot 35 + 282 \cdot 75)$

$121 \equiv 1 \pmod 4$ pois $4 | (121-1)$
$35 \equiv 3 \pmod 4$ pois $4 | (35-3)$
$282 \equiv 2 \pmod 4$ pois $4 | (282-2)$
$75 \equiv 3 \pmod 4$ pois $4 | (75-3)$

Assim $n = (1 \cdot 3 + 2 \cdot 3)$
$n = 9$

O resto da divisão de 9 por 4 é 1.

③ $2^{13} \equiv 2 \pmod 7$
Sabemos que $2^3 = 8$ e que $8 \equiv 1 \pmod 7$

$13 = 3.4 + 1$ então $2^{13} = 2^{3.4+1}$ ou $(2^3)^4 . 2^1$
Como $2^3 \equiv 1 \pmod 7$, temos
$1^4 . 2^1 = 2$, então
$2 \equiv 2 \pmod 7$ o que se confirma pois $7 | (2-2)$, pois $7 | 0$

Respostas do estudante A7

1) $a \equiv b \pmod m \Rightarrow m | (a-b) \therefore a - b = m.k$
$a = m.k + b$

$4 \equiv 8 \pmod 2$ 4 |2 → 0 2; 8 |2 → 0 4

a congruência módulo m é quando a/m e b/m tem o mesmo resto.

2) 121 × 35 = 605 + 363 = 4235; 282 × 75 = 1170 + 1974 = 20910; 20910 + 4235 = 25145

25145 |4 → 6286; 11, 34, 25, ①

não me recordo de nenhuma teoria de álgebra para me auxiliar de maneira imediata. Então, fiz as contas mesmo

3) Pelo que disse no item 1, sei que o resto da divisão de 2^{13} por 7 é 2, porém não me recordo como resolver algebricamente, ou melhor, lançando mão das ferramentas da álgebra que facilitariam as contas.

4) a) $\overline{10} \in \mathbb{Z}_7$, pertence pois o resto da divisão de 10 por 7 é 3.

b) $\overline{10} \in \mathbb{Z}_7$. Não, pois os únicos restos possíveis para a divisão com 7, são $0 < r < 7$.

Respostas do estudante A8

① Congruência módulo m está diretamente relacionado à divisibilidade. É uma notação de algum caso de divisibilidade:

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a-b$$

② $n = (121.35 + 282.75)$ por 4.

$n = 4q + r$

$121.35 + 282.75 = 4c + r$

$[(4.30+1).(4.8+3)] + [(4.70+2).(4.18+3)] = 4q + r$

$4.30.4.8 + 4.30.3 + 4.8 + 3 + 4.70.4.18 + 4.70.3 + 2.4.18 + 2.3 = 4q + r$

$4(30.8.4 + 30.3 + 8 + 70.4.18 + 70.3 + 2.18] + 9 = 4q + r$

$4.q + 2.4 + 1 = 4q + r$

$4(q+2) + \boxed{1} = 4q + r$

Logo o resto é 1.

③ $2^{13} \equiv 2 \pmod 7$

$2^{13}.2^{-1} \equiv 2.2^{-1} \pmod 7$

$2^{12} \equiv 1 \pmod 7$

$2^{12} \equiv 1^{12} \pmod 7 \Leftrightarrow 2 \equiv 1 \pmod 7$

$7k = 2 - 1$

$7k = 1$

$k = \frac{1}{7}$

Respostas do estudante A9

01. Dizer que um número $a \equiv r \pmod{m}$, equivale afirmar que $a = m.b + r$, sendo b um fator multiplicativo de m e r o resto da divisão de a por b, logo é uma ferramenta para encontrar restos de divisões.

02. $n = (121.35 + 282.75)$ por 4.

$121\,(32+3) + (280+2).(72+3)$

$(120+1).3 + 2.3$

$3 + 6 = 9/10 = 8+1 = 1/10$

O resto é $1/10$

Utilizando somas, buscando encontrar múltiplos de 4 visando eliminar divisões inteiras. Logo se encontra resto $1/10$

03. $2^{13} \equiv 2 \pmod{7}$

Por Euclides, temos $2^6 \equiv 1 \pmod{7}$

elevando ao quadrado, $2^{12} \equiv 1 \pmod{7}$

multiplicando por 2, $2^{13} \equiv 2 \pmod{7}$

04. $\bar{a} = \{ x \in \mathbb{Z} ; x \equiv a \pmod{m} \}$

$10 \in \mathbb{Z}_7$?

$\bar{0} = \{ 0, \pm 7, \pm 14, \ldots, \pm 7k \}$ $k \in \mathbb{Z}$

$\bar{3} = \{ 3, \pm 10, \pm 17, \ldots, 3 \pm 7k \}$ $k \in \mathbb{Z}$

$10 \in \mathbb{Z}_7$, pois $\bar{3} \in \mathbb{Z}_7$

$\overline{10} \in \mathbb{Z}_7$?

$\overline{10} = \{ 10, \pm 17, \pm 24, \ldots, 10 \pm 7k \}$, $k \in \mathbb{Z}$

$\bar{6} = \{ 6, \pm 13, \pm 20, \ldots, 6 \pm 7k \}$, $k \in \mathbb{Z}$

$\bar{4} = \{ 4, \pm 11, \pm 18, \ldots, 4 \pm 7k \}$, $k \in \mathbb{Z}$

Sim, ao unir $\bar{6}$ e $\bar{4}$, encontram-se os elementos de $\overline{10}$ e como $\bar{6}$ e $\bar{4} \in \mathbb{Z}_7$, então $\overline{10} \in \mathbb{Z}_7$.

Respostas do estudante A10

1 - Explicaria a partir $a \equiv x \pmod m \Rightarrow a - x = m \cdot k$ relacionando múltiplos e a idéia de divisão (mostrando até mesmo o algoritimo de euclides para divisão), que a partir de $a = m \cdot k + x \rightarrow$ resto

$a - x = m \cdot k + x - x \Rightarrow a - x = m \cdot k$

$a \equiv x \pmod m$.

2 - Bem, não lembrando exatamente, ou até mesmo não sabendo resolver, mas sabendo que minha maior dificuldade após entender é escrever ~~rigorosamente~~ a solução (isso ocorre em análise também).

Para o resto da divisão, utilizaria a idéia de módulo, visto que o resto "r"

$n \equiv r \pmod 4$

$(121 \cdot 35 + 282 \cdot 75) \equiv r \pmod 4$

3 - NÃO Lembro mesmo!

4 -

a) $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ Vaga lembrança!

10 neste caso seria $= \bar{2}$

então o próprio $10 \notin \mathbb{Z}_7$

b) $\bar{10} \in \mathbb{Z}_7 = \{10, \pm 17, \pm \dots\}$

neste caso $\bar{10} \in \mathbb{Z}_7$

Respostas do estudante A11

1. Começaria dando exemplos da utilização dessa teoria e aos poucos aplicar a definição (a congruência módulo $m = a \equiv b \pmod m = m/a - b$)

2. Não lembro pois o assunto passou "despercebido" por mim.

3. $2^{13} \equiv 2 \pmod 7$

$7 \mid 2^{13} - 2$

$2^{13} = 2^5 \cdot 2^8$

4. a) $10 \in \mathbb{Z}_7$ Não pois não faz parte da classe de congruência

b) $\bar{10} \in \mathbb{Z}_7$
$\bar{10} = \bar{3}$

Respostas do estudante A12

① Congruência módulo m é:
$a \equiv b \pmod{m} \Rightarrow m \mid a-b$

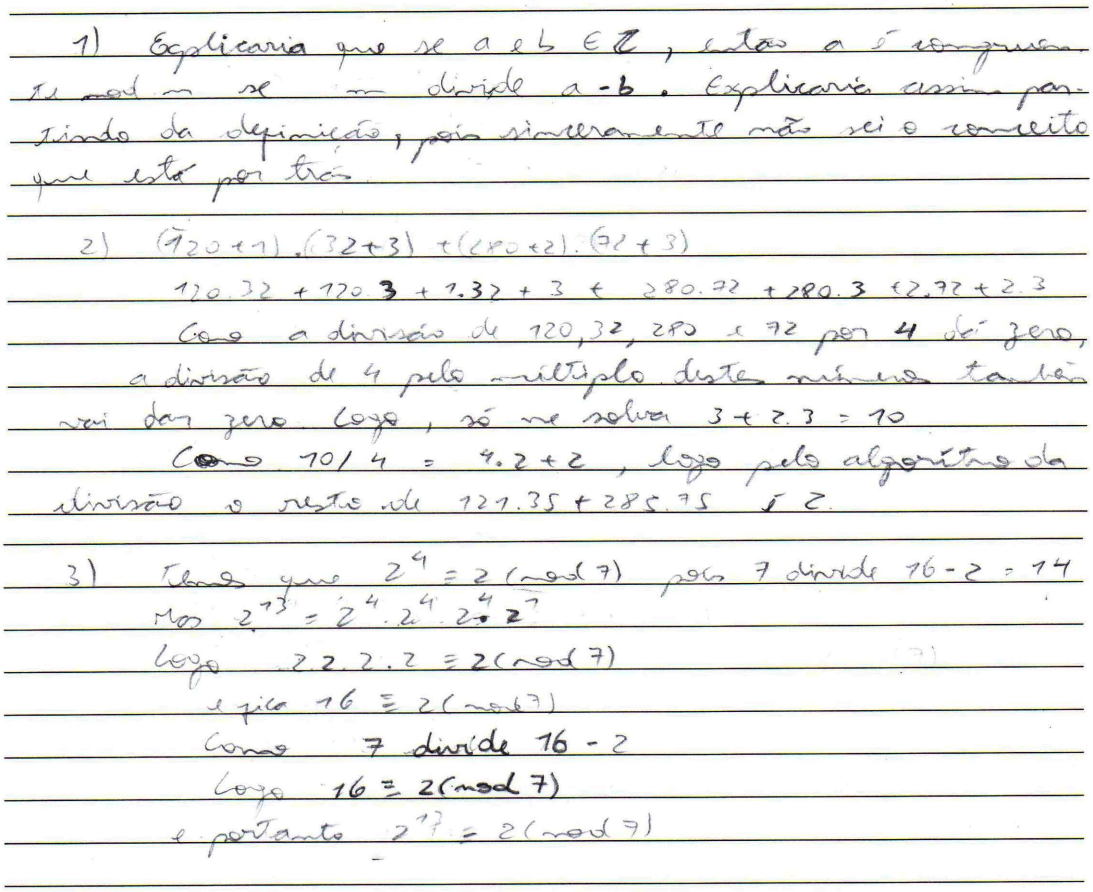
Explicaria que dois números são congruentes módulo outro número, se a diferença dos dois primeiros for múltiplo do módulo outro. Isto é,
$a - b = m.d$, com $d \in \mathbb{Z}$

②
$n = r \pmod 4$
$121.35 + 282.75 \equiv r \pmod 4$
$121.(32+3) + 75(280+2) \equiv r \pmod 4$
$(120+1).(32+3) + 75(280+2) \equiv r \pmod 4$
$120.32 + 3.120 + 32 + 3 + 75(280+2) \equiv r \pmod 4$
$3.120 + 75.280 + 75.2 \equiv r \pmod 4$
$3.120 + (72+3).280 + (72+3).2 \equiv r \pmod 4$
$3 + 3 + 72.2 + 3.6 \equiv r \pmod 4$
$9 \equiv r \pmod 4$

③ $2^{13} \equiv 2 \pmod 7$

$2^6 \equiv 1 \pmod 7$ $\quad 4^2$
$(2^6)^2 \equiv 1^2 \pmod 7$
$2^{12} \equiv 1 \pmod 7$ $\quad \times 2$
$2^{12}.2 \equiv 1.2 \pmod 7$
$2^{13} \equiv 2 \pmod 7$.

Respostas do estudante A13


1) Explicaria que se a e $b \in \mathbb{Z}$, então a é congruente b mod m se m divide $a-b$. Explicaria assim partindo da definição, pois sinceramente não sei o conceito que está por trás.

2) $(120+1).(32+3) + (280+2).(72+3)$

$120.32 + 120.3 + 1.32 + 3 + 280.72 + 280.3 + 2.72 + 2.3$

Como a divisão de 120, 32, 280 e 72 por 4 dá zero, a divisão de 4 pelo múltiplo destes mesmos também vai dar zero. Logo, só me sobra $3 + 2.3 = 10$

Como $10/4 = 4.2 + 2$, logo pelo algoritmo da divisão o resto de $121.35 + 282.75$ é 2.

3) Temos que $2^4 \equiv 2 \pmod 7$ pois 7 divide $16 - 2 = 14$

Mas $2^{13} = 2^4 . 2^4 . 2^4 . 2$

Logo $2.2.2.2 \equiv 2 \pmod 7$

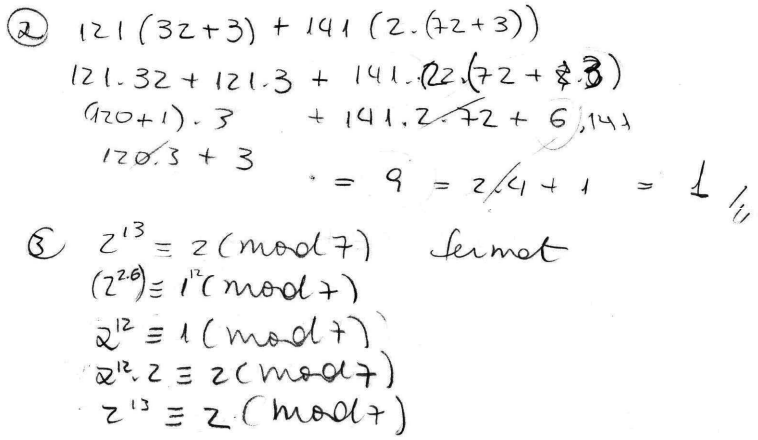
e pela $16 \equiv 2 \pmod 7$

Como 7 divide $16 - 2$

Logo $16 \equiv 2 \pmod 7$

e portanto $2^{13} \equiv 2 \pmod 7$

Respostas do estudante A14


② $121(32+3) + 141(2.(72+3))$

$121.32 + 121.3 + 141.2.(72+3)$

$(120+1).3 + 141.2.72 + 6,141$

$120.3 + 3$

$= 9 = 2.4 + 1 = 1$ //

③ $2^{13} \equiv 2 \pmod 7$ fermat

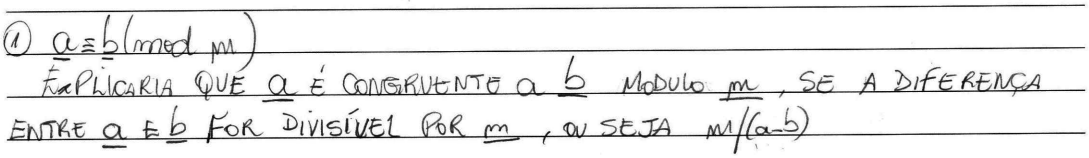
$(2^{2.6}) \equiv 1^{12} \pmod 7$

$2^{12} \equiv 1 \pmod 7$

$2^{12}.2 \equiv 2 \pmod 7$

$2^{13} \equiv 2 \pmod 7$

Respostas do estudante A15


① $a \equiv b \pmod m$

EXPLICARIA QUE a É CONGRUENTE A b MÓDULO m, SE A DIFERENÇA ENTRE a E b FOR DIVISÍVEL POR m, OU SEJA $m/(a-b)$

② $a \equiv 121.35 + 282.75 \pmod 4$

$a \equiv 1.3 + 2.3 \pmod 4$

$a \equiv 3 + 6 \pmod 4$

$a \equiv 9 \pmod 4$

$a \equiv 1 \pmod 4$

LOGO O RESTO DA DIVISÃO É IGUAL A 1.

③ PELO TEOREMA DE FERMAT, SABEMOS QUE $2^6 \equiv 1 \pmod 7$, ELEVANDO OS DOIS LADOS AO QUADRADO, TEMOS $(2^6)^2 \equiv (1)^2 \pmod 7 \Rightarrow 2^{12} \equiv 1 \pmod 7$
MULTIPLICANDO AMBOS OS LADOS POR DOIS TEMOS $2^{13} \equiv 2 \pmod 7$

④a) $10 \in \mathbb{Z}_7$.

ESSA AFIRMATIVA É VERDADEIRA POIS AS CLASSE DE CONGRUÊNCIA MODULO 4, ISTO É, $\bar{a} = \{x \in \mathbb{Z} / x \equiv a \pmod 7\}$, SÃO
$\bar{0} = \{0, \pm 7, \pm 14, \dots, \pm 7k\}, k \in \mathbb{Z}$, LOGO ENCONTRAMOS O 10
$\bar{1} = \{1, \pm 8, \pm 15, \dots, \pm 7k\}, k \in \mathbb{Z}$ DENTRE OS ELEMENTOS
$\bar{2} = \{2, \pm 9, \pm 16, \dots, 2 \pm 7k\}, k \in \mathbb{Z}$ DO QUOCIENTE.
$\bar{3} = \{3, \boxed{\pm 10}, \pm 17, \dots, 3 \pm 7k\}, k \in \mathbb{Z}$
$\bar{4} = \{4, \pm 11, \pm 18, \dots, 4 \pm 7k\}, k \in \mathbb{Z}$
$\bar{5} = \{5, \pm 12, \pm 19, \dots, 5 \pm 7k\}, k \in \mathbb{Z}$
$\bar{6} = \{6, \pm 13, \pm 20, \dots, 6 \pm 7k\}, k \in \mathbb{Z}$

b) $\bar{10} \in \mathbb{Z}_7$

NÃO PERTENCE, PORQUE O CONJUNTO DE TODAS CLASSES DE CONGRUENCIA MODULO 7, É O $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

Respostas do estudante S1

1) congruência é uma relação entre inteiros tal que
$a, b \in \mathbb{Z}$ $a \equiv b \pmod m$ sse $a - b$ é múltiplo de m

... ou: a e b possuem o mesmo resto na divisão por m

2) $121 = 120 + 1 \equiv 1 (4)$ $35 = 36 - 1 \equiv -1 (4)$ $282 = 280 + 2 \equiv 2 (4)$ $75 \equiv 76 - 1 \equiv -1 (4)$

logo $121.35 + 282.75 \equiv 1(-1) + 2(-1) \pmod 4$

$n \equiv -3 \pmod 4$

$n \equiv 1 \pmod 4$

3) $2^{13} = 2^{(3.4+1)} = (2^3)^4 . 2$

como $2^3 \equiv 1 (7) \rightarrow 2^{13} \equiv 2 (7)$

4) a) $10 \in \mathbb{Z}_7$: FALSO pois $10 \in \mathbb{Z}$ $\mathbb{Z}_7$ é um conjunto de conjuntos

$\mathbb{Z}_7$ não possui nenhum inteiro $\Rightarrow 10 \notin \mathbb{Z}_7$

4b) $\overline{10} = \{ x \in \mathbb{Z} \mid x \equiv 10 \pmod 7 \}$

se $x \equiv 10 \pmod 7$, como $10 = 7+3 \Rightarrow x \equiv 3 \pmod 7 \Rightarrow x \in \overline{3} \Rightarrow \overline{10} \subset \overline{3}$

$7 \equiv 0 (7)$

Reciprocamente, para qualquer $x \in \overline{3}$, $x \equiv 3 \pmod 7 \Rightarrow x \equiv 10 \pmod 7 \Rightarrow x \in \overline{10} \Rightarrow \overline{3} \subset \overline{10}$

logo $\overline{10} = \overline{3}$ logo $\overline{10} \in \mathbb{Z}_7$

Respostas do estudante S2

1) A congruência $a \equiv b \pmod m$ é um trio de números $a, b, m \in \mathbb{Z}$ tais que m divide $(a-b)$.

A seguir daria uns cinco exemplos de valores diferentes para a, b e m.

Depois destacaria que m é o resto na divisão de a por b, se tomarmos a e b convenientemente.

S2

2) $121 \equiv 1 \mod 4$ $\quad$ $282 \equiv 2 \mod 4$

$35 \equiv -1 \mod 4$ $\quad$ $75 \equiv -1 \mod 4$

$\Downarrow$ $\quad$ $\Downarrow$

$121 \cdot 35 \equiv 1(-1) \mod 4$ $\quad$ $282 \cdot 75 \equiv 2(-1) \mod 4$

$\Downarrow$

$121 \cdot 35 + 282 \cdot 75 \equiv -1 - 2 \mod 4$

$\equiv -3 \mod 4$

$\equiv 1 \mod 4$

$\downarrow$

RESTO = 1

3) $2^{13} = 2^{12+1} = 2^{12} \cdot 2 = (2^3)^4 \cdot 2$

$2^3 \equiv 1 \mod 7$ $\qquad 2 \equiv 2 \pmod 7$

$\therefore (2^3)^4 \equiv 1^4 \mod 7 \equiv 1 \mod 7$

$\therefore 2^{12} \cdot 2 \equiv 1 \cdot 2 \pmod 7$

$\therefore 2^{13} \equiv 2 \pmod 7$

4) Não foi visto no semestre anterior.

Respostas do estudante S3

① A congruência módulo m é uma maneira de reduzir a uma base conhecida. Ou seja no caso das horas: $a \equiv 5 \pmod{12}$.

② $n = \dfrac{(121 \cdot 35 + 282 \cdot 75)}{(121 \cdot 32 + 3) + (282(72+3))}$

$n = (120+1)(32+3) + (280+2)(72+3)$

$n = (120 \cdot 32 + 120 \cdot 3 + 32 + 32 \times 3 + 280 \cdot 72 + 280 \cdot 3 + 2 \times 72 + 2 \times 3)$

$n = 9 \quad | = 8+1 =$

$n = 9 \quad | = 8+1 =$

③ $2^{13} \equiv 2 \pmod 7$ Por fermat: $a^{p-1} = 1 \pmod p$

$2^{13} = 2^6 \cdot 2^7 \equiv 2 \pmod 7$

$2^7 \equiv 2 \pmod 7 \Rightarrow 1 \cdot 2^7 = 2 \pmod 7$

$2^6 \equiv 1 \pmod 7 \quad 2^7 = 2^6 \cdot 2^1 = 1 \cdot 2 = 2 \pmod 7$

Respostas do estudante S4

1. Dois números inteiros são congruentes módulo m quando tem restos iguais ao dividi-los por m. Daí decorre o fato de existirem m possibilidades (classes) de congruência. Com esse fato é possível partir para outras propriedades como multiplicação por um número, soma de classes e etc.

2. $n = 121 \cdot 35 + 282 \cdot 75 = \bar{1}.(\bar{-1}) + \bar{2}(\bar{-1}) = \bar{-1} - \bar{2} = \bar{-3} = \bar{1}$

resto 1

Simplesmente usei as propriedades de congruencia.

3.

$2^{13} = 2^3 . 2^3 . 2^3 . 2 = \bar{1} . \bar{1} . \bar{1} . \bar{2} = 2 \bmod 7$

Também pelas propriedades

4. a. NÃO. $\mathbb{Z}_7$ é um conjunto de classes e 10 é um número

b. NÃO. $\mathbb{Z}_7$ as classe em $\mathbb{Z}_7$ são $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ e $\bar{6}$.

Respostas do estudante S5

① Explicaria que seria dois números $a, b \in \mathbb{Z}^1$ que subtraídos são divididos por m sem deixar resto.

② Não me lembro mais como faz..

121 → r = 1
35 → r = 3
282 → r = 2
75 → r = 3

75 | 14
15 23
3

③ $2^{13} \equiv 2 \pmod 7$

sei que

$2^4 \equiv 2 \pmod 7$ pois $7 | (2^4 - 2)$
$7 | (16 - 2)$
$7 | 14$

④

(a) sim pois $10 \in \bar{3}$

$\bar{3} = \{3, \pm 10, \pm 14, \ldots, 3 \pm 7k\}$, onde k.
pois $\pm 10 \equiv 3 \pmod 7$

(b) não pois os restos possíveis nas divisões por 7 é no máximo 6, mas também $10 = \bar{3}$. mas $\mathbb{Z}_7$ só possui 7 elementos.

Respostas do estudante S6

Turma: _____ Data: ____ / ____ / ____

1) SE VOCÊ DIVIDISSE UM Nº INTEIRO QUALQUER DIGAMOS S POR OUTRO NÚMERO, QUAIS OS RESTOS QUE EU PODERIA TER?

5 | 5	6 | 5	7 | 5	8 | 5	9 | 5	10 | 5
0 1	1 1	2 1	3 1	4 1	0 2

PORTANTO UM NÚMERO x DIVIDIDO POR 5 PODE DEIXAR COMO RESTO 0, 1, 2, 3, 4 $\Rightarrow$ $0 \leq$ RESTO < 5
PODEMOS ESCREVER $x \equiv r \pmod 5$, $0 \leq r < 5$

2) $m = (121.35 + 282.75)$ POR $4 = 2^2$
$11^2 . 7.5 + 141 . 2 . \underline{5.5.3} \equiv x \pmod 4$
$3^2 . 3.1 + 2 . 3 \equiv x \pmod 4$
$1 . 3 . 1 + 2 = 5 \equiv 1 \pmod 4$

2) $m = (121.35 + 282.75)$ POR $4 = 2^2$
$11^2 . 7.5 + 141 . 2 . \underline{5.5.3} \equiv x \pmod 4$
$3^2 . 3.1 + 2 . 3 \equiv x \pmod 4$
$1 . 3 . 1 + 2 = 5 \equiv 1 \pmod 4$

NÃO LEMBRO

3) $2^{13} \equiv 2 \pmod 7$, como $2^3 = 8 \equiv 1 \pmod 7$
$13 = 3.4 + 1$ ENTÃO $(2^3)^4 . 2 \equiv 2 \pmod 7$ POIS
$1^4 . 2 \equiv 2 \pmod 7$ e $2^3 = 1 \pmod 7$

$\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\} \Rightarrow \mathbb{Z}/\equiv_m$ ou $\mathbb{Z}_m$ Ex $\mathbb{Z}_4 = \{\bar{0}\bar{1}\bar{2}\bar{3}\}$

b) $\bar{10} \in \mathbb{Z}_7$

NÃO Pois $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

ou seja $\bar{10} \not\in 7$

a) $10 \in \mathbb{Z}$ e $\mathbb{Z}_m = \{\bar{10} \mid 10 \in \mathbb{Z}\}$??

Respostas do estudante S7

(1) dado a, b e m $\in$ aos inteiros

a é congruente à b mod m se: a−b for um múltiplo de m

ou seja, m divide a−b.

(2) $n = 4t + r$

$n - r = 4t$

$n \equiv r \pmod 4$

$121.35 + 282.75 \equiv r \pmod 4$

$\begin{cases} 121.35 \equiv r \pmod 4 \\ 282.75 \equiv r \pmod 4 \end{cases}$ ... (não me lembro)

(3) $2^{13} \equiv 2 \pmod 7$

Pelo teorema de fermat.

$2^6 \equiv 1 \pmod 7$ elevando ao quadrado

$(2^6)^2 \equiv 1^2 \pmod 7$

$2^{12} \equiv 1 \pmod 7$

$2^{12}.2 \equiv 1.2 \pmod 7$ mult. por 2.

$2^{13} \equiv 2 \pmod 7$

(4) a) temos que $10 \equiv 3 \pmod 7$, logo $10 \in \bar{3}$ que por sua vez $\bar{3} \in \mathbb{Z}_7$

logo $10 \in \mathbb{Z}_7$

b) $\bar{10} = \{x \equiv 10 \pmod 7;\ x \in \mathbb{Z}\}$

Se $x \equiv 10 \pmod 7$

$x - 7 \equiv 10 - 7 \pmod 7$

$x - 7 \equiv 3 \pmod 7$

$x \equiv 3 \pmod 7$

$\forall\ x \in \mathbb{Z}$

logo $\bar{10} = \bar{3} \therefore \bar{10} \in \mathbb{Z}_7$

Respostas do estudante S8

1. Como você explicaria para um aluno do primeiro ano do Curso de Matemática o que é a congruência módulo m? Justifique sua resposta.

$n \equiv p \pmod m$. No caso $n - p$ é múltiplo de m.

(2) Justificativa.

$121 \equiv 1 \pmod 4$
$35 \equiv 3 \pmod 4$
$282 \equiv 2 \pmod 4$
$75 \equiv 3 \pmod 4$

Então

$9 \equiv (1) \pmod 4$
↳ resto.

Portanto

$n \equiv 1 \pmod 4$

(2) 121 | 4 resto 1 — 282 | 4 resto 2
35 | 4 resto 3 — 75 | 4 resto 3

$n = (121 \cdot 35 + 282 \cdot 75)$
$n = 1 \cdot 3 + 2 \cdot 3$
$n = 9$ — 9 | 4 → (1) resto.

---

por Fermat, temos

$2^6 \equiv 2 \pmod 7 \rightsquigarrow 2^6 \equiv 1 \pmod 7$.
$(2^6)^2 \equiv 2^2 \pmod 7$
$2^{12} \equiv 2^2 \pmod 7$
$2^{12} \cdot 2^1 \equiv 2^2 \cdot 2^1 \pmod 7$
$2^{12+1} \equiv 2^{2+1} \pmod 7$
$2^{13} \equiv 2^4 \pmod 7$

como

$2^4 \equiv 2 \pmod 7$

então

$\boxed{2^{13} \equiv 2 \pmod 7}$

a) Sim. $10 \in \mathbb{Z}_7$, pois

$\overline{0} = \{0, \pm 7, \ldots, \pm 7k\}$; onde $k \in \mathbb{Z}$

$\vdots$

$\overline{3} = \{3, \pm 10, \ldots, 3 \pm 7k\}$; onde $k \in \mathbb{Z}$

b) não. $\overline{10} \notin \mathbb{Z}_7$, pois $\overline{10} = \overline{3}$.

Respostas do estudante S9

① Que se um certo a é congruente a b módulo m ($a \equiv b \pmod m$), isto implica que $m|(a-b)$; logo $(a-b) = m \cdot q$. Então b é resto da divisão de a por m: $a = mq + b$

Isto significa que dizer que a é congruente b módulo m, é dizer que b é resto da divisão de a por m.

② Podemos aplicar mod m:

Quando dividimos por 4, podemos fazê-lo termo a termo: $\frac{121}{4}\frac{35}{} + \frac{282}{4}\frac{75}{}$

Logo $* \; 121 \cdot 35 \equiv d \pmod 4$

$\Rightarrow 121 \equiv d_1 \pmod 4 \Rightarrow d_1 = 1$

$35 \equiv d_2 \pmod 4 \Rightarrow d_2 = 3$

$* \; 282 \cdot 75 \equiv d' \pmod 4$

$282 \equiv d'_1 \pmod 4 \Rightarrow d'_1 = 2$

$75 \equiv d'_2 \pmod 4 \Rightarrow d'_2 = 3$

$\text{resto} = d + d' = d_1 + d_2 + d'_1 + d'_2 = 9/4 = 2$ e $n = 1$

Resto 1

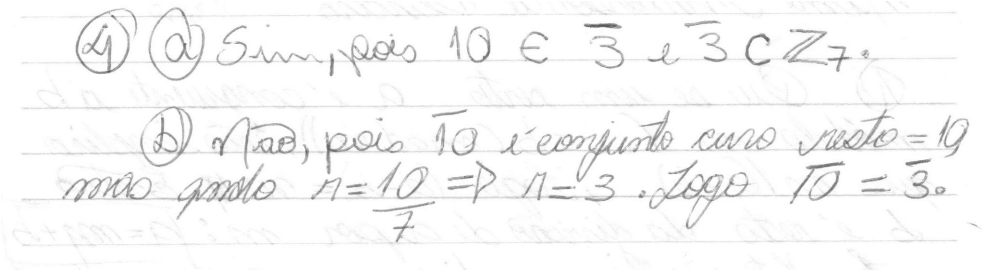
③ $2^{13} \equiv 2 \pmod 7$

$2^3 \equiv 1 \pmod 7$ elevando à 4

$(2^3)^4 \equiv 1^4 \pmod 7$

$2^{12} \equiv 1 \pmod 7$ multiplicando por 2 lado a lado

$2^{13} \equiv 2 \pmod 7$



④ (a) Sim, pois $10 \in \overline{3}$ e $\overline{3} \subset \mathbb{Z}_7$.

(b) Não, pois $\overline{10}$ é conjunto cuo resto = 10 mas gosto $n = \frac{10}{7} \Rightarrow n = 3$. Logo $\overline{10} = \overline{3}$.

Respostas do estudante S10

1. Teria que revisar a matéria, consultar algumas referências antes de responder a pergunta.

2. $n = (121 \cdot 35 + 282 \cdot 75)$ por 4

$121 \cdot 31 \equiv 3 \pmod 4$ $\qquad 282 \cdot 75 \equiv 6 \pmod 4$

Resto da divisão de n_1 por 4, multiplicado pelo resto da divisão de n_2 por 4, obtemos o resto.

Considere $n_1 \cdot n_2$

3 $\qquad 2^3 \equiv 1 \pmod 7$

$13 = 4 \cdot 3 + 1$

$2^{13} = (2^3)^4 \cdot 2$

$(2^3)^4 \cdot 2 \equiv (1)^4 \cdot 2 \equiv 1 \cdot 2 = 2 \pmod 7$

4. a. Sim, pois, $10 \equiv 3 \pmod 7$

b. Não, pois $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

Para que $\overline{10} \in \mathbb{Z}_7$, 10 teria que ser o resto de uma divisão por 7, mas 10 divide 7 e resta 3.

Respostas do estudante S11

① Sendo 3 inteiros a, b e m, se $a-b$ é divisor de m (ou m divide $a-b$) então $(a-b) = mk$. Sendo $k = \frac{a-b}{m}$ como uma constante teremos que $a-b$ também deve ser de maneira proporcional a m. Ou seja $a \equiv b \pmod m$

② $n = 4t + r$

$n - r = 4t$

$n - r = 4t \Rightarrow n \equiv r \pmod 4$

$(121 \cdot 35 + 282 \cdot 75) \equiv r \pmod 4$

$\begin{cases} 121 \cdot 35 \equiv r \pmod 4 \\ 282 \cdot 75 \equiv r \pmod 4 \end{cases}$

③ $2^{13} = 2 \pmod 7$

como 7 é primo, por Teorema

$a^{7-1} \equiv 1 \pmod 7$

$2^6 \equiv 1 \pmod 7$

$(2^6)^2 \equiv 1^2 \pmod 7$

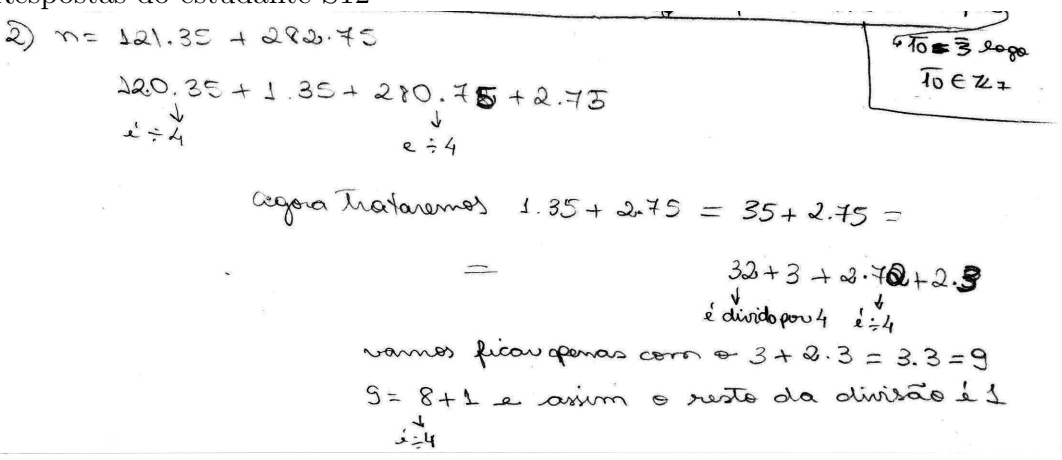
$2^{12} \equiv 1 \pmod 7$

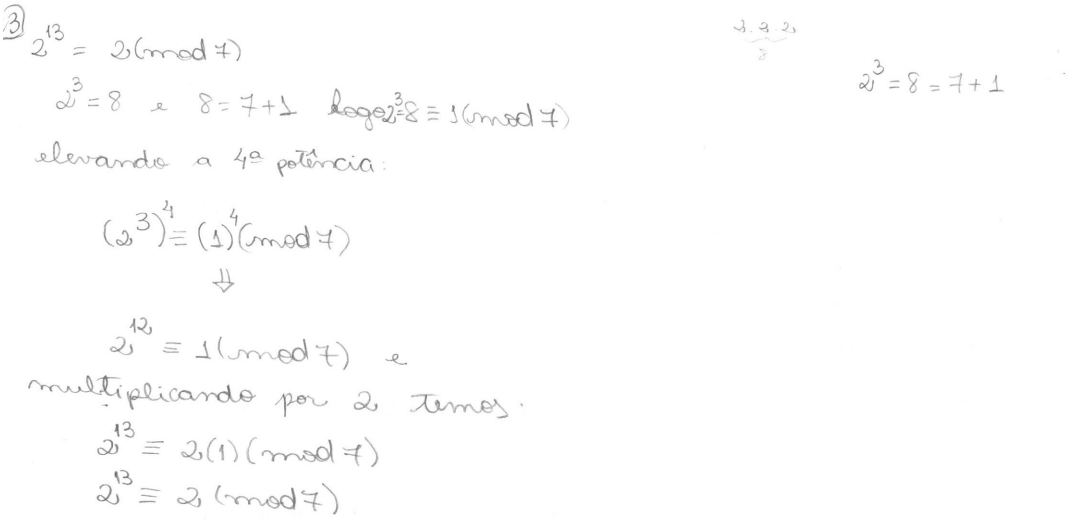
$2^{13} \equiv 2 \pmod 7$

4) Sendo
$\overline{3} = \{3, 10, \ldots\}$
Temos que $10 \in \mathbb{Z}_7$
já que $10 \equiv 3 \pmod 7$

b) $10 = 7 + \overline{3}$ =
logo $\overline{10} = \overline{3} \in \mathbb{Z}_7$

Respostas do estudante S12

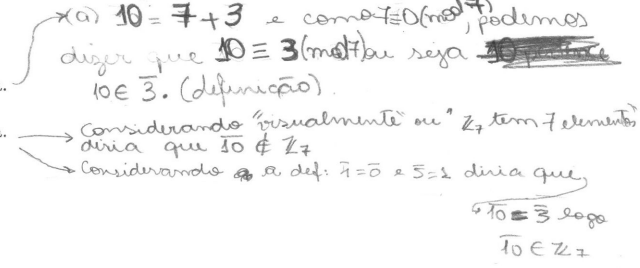




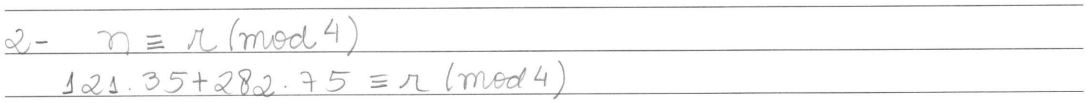
Considerando agora o conjunto de classes de congruência módulo 7, isto é, $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, podemos dizer que:

(a) $10 \in \mathbb{Z}_7$. Justifique sua resposta.

(b) $\overline{10} \in \mathbb{Z}_7$. Justifique sua resposta.



Respostas do estudante S13



3 - $2^{13} \equiv 2 \pmod 7$ $\quad 8 \equiv 1 \pmod 7$

$2^{(3+3+3+4)} \equiv 2 \pmod 7$ $\quad 13 = 3+3+3+4$

$2^3 \cdot 2^3 \cdot 2^3 \cdot 2^4 \equiv 2 \pmod 7$

$8 \cdot 8 \cdot 8 \cdot 2^4 \equiv 2 \pmod 7$, como $8 \equiv 1 \pmod 7$

$1 \cdot 1 \cdot 1 \cdot 2^4 \equiv 2 \pmod 7$

$16 \equiv 2 \pmod 7$ pois $7 \mid (16-2) = 14$

Considerando agora o conjunto de classes de congruência módulo 7, isto é, $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, podemos dizer que:

(a) $10 \in \mathbb{Z}_7$. Justifique sua resposta.

(b) $\overline{10} \in \mathbb{Z}_7$. Justifique sua resposta.

4, 8, 16, 32

$\overline{0} = \{0, \pm 7, \ldots, \pm 7k\}$

$\overline{1} = \{1, \pm 8, \ldots, \pm 1 \pm 7k\}$

$\overline{2} = \{2, \pm 9, \ldots, \pm 2 \pm 7k\}$

$\overline{3} = \{3, \pm 10, \ldots, \pm 3 \pm 7k\}$

$\overline{4} =$

$\overline{5} =$

$\overline{6} =$

a) $10 \in \mathbb{Z}_7$, pois $10 \equiv 3 \pmod 7$

b) $\overline{10} \in \mathbb{Z}_7$, pois $\overline{10} = \overline{3}$

Respostas do estudante S14

① Dois números a, b são congruentes módulo m se $m \mid (a-b)$

③ $2^7 \cdot 1 \equiv 2 \pmod 7 \Rightarrow 2^7 \cdot 2^6 \equiv 2 \pmod 7 \Rightarrow 2^{13} \equiv 2 \pmod 7$

$\star\ a^{p-1} \equiv 1 \pmod p$

④

a) $10 \notin \mathbb{Z}_7$ pois 10 não é uma classe de congruência (mod 7)

b) $\overline{10} \in \mathbb{Z}_7$, pois $\overline{10} = \overline{3} \in \overline{3} \in \mathbb{Z}_7$

Respostas do estudante S15

1. Dois números x e y são congruentes modulo m se e somente se $x - y = mk$ $k \in \mathbb{Z}$. De outra maneira x e y são congruentes modulo m $x \equiv y \pmod{m}$ se eles "deixam" o mesmo resto na divisão por m.

(2) $(121 \cdot 35) + (282 \cdot 75)$

$(120+1) \cdot 35 + (280+2) \cdot 75)$

$35 + 150$

$3 \cdot 2 + 3 + 748 \cdot 2$

$3 + 2 = 5 = 4 + 1 = (1)$

(3) $2^{13} = 2 \pmod{7}$

Basta provar que:

$2^{13} - 2 = 7k$.

De fato.

$2^{13} - 2 = 2^6 \cdot 2^6 \cdot 2 - 2 = 64 \cdot 64 \cdot 2 - 2 = (63+1) \cdot (63+1) \cdot 2 - 2$

$= ((7 \cdot 9)^2 + 2 \cdot 7 \cdot 9 + 1^2) 2 - 2 = 7 \cdot (7 \cdot 9^2 \cdot 2 + 2 \cdot 9 \cdot 2) + 2 - 2$

$= 7k + 0$.

C.Q.D.

(4) (A) não, pois $\mathbb{Z}_7$ é o conjunto das classes de congruência modulo 7 e 10 não é uma congruência.

(B) Sim pois $\bar{3} = \overline{10}$

Respostas do estudante S16

(1)

dois números distintos a e b são congruentes módulo m ($a \equiv b \bmod m$) quando m divide a diferença $a - b$

Respostas do estudante S17

(1) p e q são congruentes mod m, se o resto da divisão de p por q for igual a m.

② $n = (121.35 + 282.75)$ por 4

Sei que se eu utilizar congruência encontro a resposta, mas não me recordo como foi, porém tenho certeza de que se eu pudesse utilizar o livro agora para rever este método, eu conseguiria resolver

③ Eu lembro!!! (creio não ter entendido corretamente).

Respostas do estudante S18

① São elementos que respeitam a seguinte definição:
d é congruente a b módulo m se m divide a diferença entre d e b. Ou seja
$$d \equiv b \pmod{m} \Rightarrow m \mid d - b \quad , m, d, b \in \mathbb{Z}$$

② $n = (121.35 + 282.75)$
resto da divisão de n por 4?
$n = (120+1).35 + (280+2).75$
$= 120.35 + 35 + 280.75 + 2.75$
$= 120.35 + 280.75 + 150 + 35$
$= 120.35 + 280.75 + (148+2) + (32+3)$
$= 120.35 + 280.75 + 148 + 32 + 5$
$= \underbrace{120.35 + 280.75 + 148 + 32 + 4}_{\text{múltiplos de 4}} + 1$ // resto

③ $2^{13} \equiv 2 \pmod{7}$ Fermat: $a^{p-1} \equiv 1 \pmod{p}$
Por Fermat, temos:
$2^6 \equiv 1 \pmod{7}$
E
$2^{13} = 2^6 . 2^6 . 2^1$
Logo,
$2^{13} \equiv 2^6 . 2^6 . 2^1 \equiv 1 . 1 . 2^1 \equiv 2 \pmod{7}$
Portanto, $2 \equiv 2 \pmod{7}$

Respostas do estudante S19

① Suponha a e b inteiros não-nulos. Dizemos que a é congruente módulo m a b quando temos $m \in \mathbb{Z}$ múltiplo de $(a-b)$, ou seja,
$$a - b = m . k, k \in \mathbb{Z} \rightarrow m \mid (a-b)$$
→ podemos usar o conceito de divisibilidade, pois é no 1º ano que essa matéria é dada

(2) $n = (121.35 + 282.75)$ por 4:

$121.35 + 282.75 = 4.q + r$

$[(4.30+1).(4.8+3)] + [(4.70+2).(4.18+3)] = 4.q+r$

$(4.4.240 + 4.90 + 4.8 + 3) + (4.4.1260 + 4.210 + 4.36 + 6) = 4q+r$

$4.960 + 4.90 + 4.8 + 3 + 4.5040 + 4.210 + 4.36 + 6 = 4.q+r$

$4(960 + 90 + 8 + 5040 + 210 + 36) + 9 = 4.q+r$

$4(960 + 90 + 8 + 5040 + 210 + 36) + 4.2 + 1 = 4.q+r$

$4(\underbrace{960 + 90 + 8 + 5040 + 210 + 36 + 2}_{q}) + \underbrace{1}_{r} = 4.q+r$

Logo $r = 1$.

(3) $2^{13} \equiv 2 \pmod 7$

$2^{13}.2^{-1} \equiv 2.2^{-1} \pmod 7$

$2^{12} \equiv 1 \pmod 7$

$2^{12} \equiv 1^{12} \pmod 7$

Respostas do estudante S20

(01) falando da def de congruência mod m

$a \equiv b \pmod m \Rightarrow a - b = mf, \quad f \in \mathbb{Z}.$

ou seja $a = b + mf$.

(02) $121.35 + 282.75 \equiv n \pmod 4$

• O resto da divisão de n por 4 é obtido pela resolvendo a congruência acima.

Respostas do estudante S21

(1) $m \mid a - b$

$a \equiv b \pmod m$

$m \mid (a - b)$

$(a - b) = mK$

$a = mK + b$

③ $2^{13} \equiv 2 \pmod 7$

$7 \mid 2^{13} - 2$

$2^{13} \equiv 2 \pmod 7$

$2^4 \cdot 2^4 = 2 \cdot 2^4 \pmod 7$

$2^8 \equiv 2 \cdot 2 \pmod 7$

$2^8 \cdot 2^4 \equiv 2 \cdot 2 \cdot 2^4 \pmod 7$

$2^{12} \equiv 2 \cdot 2 \cdot 2 \pmod 7$

$2^{12} \cdot 2 \equiv 2 \cdot 2 \cdot 2 \cdot 2 \pmod 7$

$2^{13} \equiv 2^4 \pmod 7$

$2^{13} \equiv 2 \pmod 7$

Respostas do estudante S22

1) $ax \equiv b \pmod m$

Seria divisões por m, para determinar muitas vezes restos de divisões, que quando divisões exatas dizemos um número congruo ao outro na divisão por "m".

2)

$n = (121 \cdot 35 + 282 \cdot 75)$ por 4

$n = 5(121 \cdot 7 + 282 \cdot 15)$

$n =$ não sei

3) $2^{13} \equiv 2 \pmod 7$

$2^3 \equiv 1 \pmod 7$ pois $2^3 = 8$

e $8 \equiv 1 \pmod 7$ é igual à

$8 - 1 = 7$ e

$7 \equiv 0 \pmod 7$ divisão exata

então $(2^3)^4 \equiv 1^4 \pmod 7$ também é exata, e

portanto

$2^{12} \cdot 2 \equiv 1 \cdot 2 \pmod 7$

$2^{13} \equiv 2 \pmod 7$

Respostas do estudante T1

① Começaria mostrando tabelas, como por exemplo a do módulo 4, associando valores a cada coluna.

*	☆	□	○
0	1	2	3
4	5	6	7
⋮	⋮	⋮	⋮

, para cada elemento da coluna do 0, 1, 2 e 3, o resto da divisão se remete ao elemento.

No caso 7 dividido por 4 tem resto 3, portanto equivale ao elemento ○.

② $|121 \cdot 35 + 282 \cdot 75| = n$

Divido cada número por 4 e obtenho o resto da divisão os restos de 121, 35, 282 e 75 são respectivamente 1, 3, 2 e 3, no lugar dos números coloco os seus restos e obtenho $(1 \cdot 3 + 2 \cdot 3) = 9$, 9 dividido por 4 tem resto 1.

③ $2^{73} \equiv 2 \pmod 7$

Sei que $2^4 \equiv 2 \pmod 7$, ~~(multiplicando)~~ elevando os dois lados por 3 tem-se $2^{12} \equiv 2^3 \pmod 7$ e multiplicando por (2^1) $2^1 \cdot 2^{12} \equiv 2^1 \cdot 2^3 \pmod 7 \Rightarrow 2^{13} \equiv 2^4 \pmod 7$ e como eu sei que 2^4 é congruente $2 \pmod 7$, isso implica $2^{13} \equiv 2 \pmod 7$

④ a) $10 \in \mathbb{Z}_7$ pois se dividirmos 10 por 7 temos resto 3, logo $10 \in \bar{3}$ e $\bar{3} \in \mathbb{Z}_7$

b) $\bar{10}$ não pertence pois é igual ao $\bar{3}$, $\bar{10} = \bar{3}$, e pelo critério do enunciado considera-se apenas o $\bar{3}$.

Respostas do estudante T2

1) Se escolher dois números a, b e se m dividir a diferença a-b então a será congruente a b módulo m.
Por se tratar de aluno de 1° ano, explicaria involvendo conceitos que com certeza, esse aluno tem, como a divisão e diferença, pois é a forma mais clara de entregar a definição de congruência.

3) $a^n \equiv a \pmod m$
Não lembro!

Respostas do estudante T3

① • Mostrando a definição;
• Explicando a definição;
• Ensinando através da definição, aplicar técnicas
• Mostrando a aplicação de congruência
Através dessa maneira o aluno teria menos dificuldade em trabalhar com esse assunto.

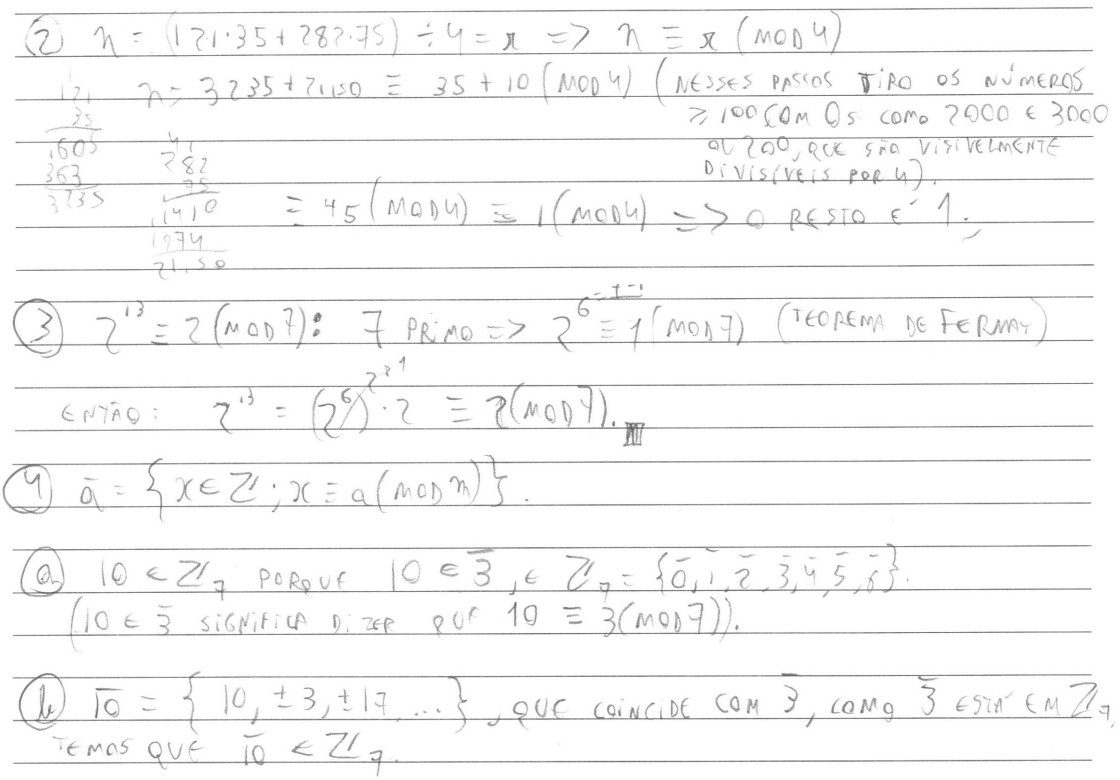
② Resto 5: $\left(\frac{A}{4}\right) + \left(\frac{B}{4}\right)$, $r_1 + r_2$
resto → r_1 r_2

③ $2^{13} \equiv 2 \pmod 7$
Por Fermat:
$2^7 \equiv 2 \pmod 7$
Multiplicando (2^6)
$2^6 \cdot 2^7 \equiv 2^6 \cdot 2 \pmod 7$
$2^{13} \equiv (2^7 \pmod 7)$
$\Rightarrow 2^{13} \equiv 2 \pmod 7$

④
a) Não pois se dividirmos 7 por qualquer ā do conjunto o resto não será igual quando 7 é dividido por 10 (Eu acho).

Respostas do estudante T4

① $a, b, m \in \mathbb{Z}$, DIZEMOS QUE $a \equiv b \pmod m$ SE A DIFERENÇA DE a E b É MÚLTIPLA DE m, ISTO É: $a - b = mk$, $k \in \mathbb{Z}$. NO PRIMEIRO ANO DO CURSO DE MATEMÁTICA, UM ALUNO DEVE SER CAPAZ DE ACEITAR ESSA DEFINIÇÃO.



E.2 Segundo questionário

O questionário sobre anel quociente era composto das seguintes questões:

1. Considere o anel $\mathbb{Z}_{18}$ e seu subanel $J = \overline{3}\mathbb{Z}_{18} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$. Justifique suas respostas.

   i) Quais são os elementos do anel quociente $\mathbb{Z}_{18}/J$?

   ii) Qual é o elemento identidade de $\mathbb{Z}_{18}/J$?

   iii) Encontre um anel familiar que seja isomorfo a $\mathbb{Z}_{18}/J$.

2. Qual polinômio abaixo é igual ao polinômio $f(x) = \overline{3}x^4 + \overline{2}x^3 + \overline{1}x^2 + \overline{4}$ de $\mathbb{Z}_5[x]$? Justifique sua resposta.

   i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \overline{1}x^2 + \overline{0}$ de $\mathbb{Z}_5[x]$.

   ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ de $\mathbb{Z}_5[x]$.

   iii) $l(x) = \overline{8}x^4 - \overline{3}x^3 + \overline{16}x^2 + \overline{9}$ de $\mathbb{Z}_5[x]$.

3. Os elementos de $\mathbb{Z}/3\mathbb{Z}$ podem ser elementos de $\mathbb{Z}$? Justifique sua resposta.

4. Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta.

5. Como você explicaria para um aluno do primeiro ano do Curso de Matemática o que é um anel quociente? Justifique sua resposta.

E.2.1 As respostas

Respostas do estudante N1

1. Considere o anel $\mathbb{Z}_{18}$ e seu subanel $J = \overline{3}\mathbb{Z} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$. Justifique suas respostas.
   i)Quais são os elementos do anel quociente $\mathbb{Z}_{18}/J$? $\{$
   ii) Qual é o elemento identidade de $\mathbb{Z}_{18}/J$? = é o $\overline{3}$ porque MDC(18,3)= 3
   iii) Encontre um anel familiar que seja isomorfo a $\mathbb{Z}_{18}/J$. $\cong \mathbb{Z}$

3. Os elementos de $\mathbb{Z}/3\mathbb{Z}$, podem ser elementos de Z? Justifique sua resposta. NÃO
   ELEMENTOS PERTENCEM A

4. Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta. NÃO
   $\mathbb{Z}_3 \subset \mathbb{Z}_6$ $\in$ $\overline{6} = \overline{3}.\overline{2}$

5) CLASSES DE EQUIVALÊNCIA PODEM SER EXPLICADAS FAZENDO ANALOGIAS COM "TABUADA" OU MÚLTIPLOS.

2) III é IGUAL POIS $\begin{cases} 8 \equiv 3 \pmod 5 \\ -3 \equiv 2 \pmod 5 \\ 16 \equiv 1 \pmod 5 \\ 9 \equiv 4 \pmod 5 \end{cases}$

Respostas do estudante N2

1i) $\mathbb{Z}_{18}/J = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{x}, x \in \mathbb{Z}_{18}\}$ logo $\bar{1} \in \mathbb{Z}_{18}$, $\bar{4} \in \mathbb{Z}_{18}$ e $\bar{4} - \bar{1} = \bar{3} \in J$
$\Rightarrow \bar{1}$ e $\bar{4}$ são as mesmas classes

1ii) $\bar{1}$ pois $a \in \mathbb{Z}_{18}/J$, $a \neq \bar{0} \Rightarrow a = \bar{1}$ ou $a = \bar{2}$ e $\bar{1}.\bar{1} = \bar{1}.\bar{1} = \bar{1}$
$\bar{2}.\bar{1} = \bar{1}.\bar{2} = \bar{2}$

1iii) $\mathbb{Z}_3 \cong \mathbb{Z}_{18}/J$

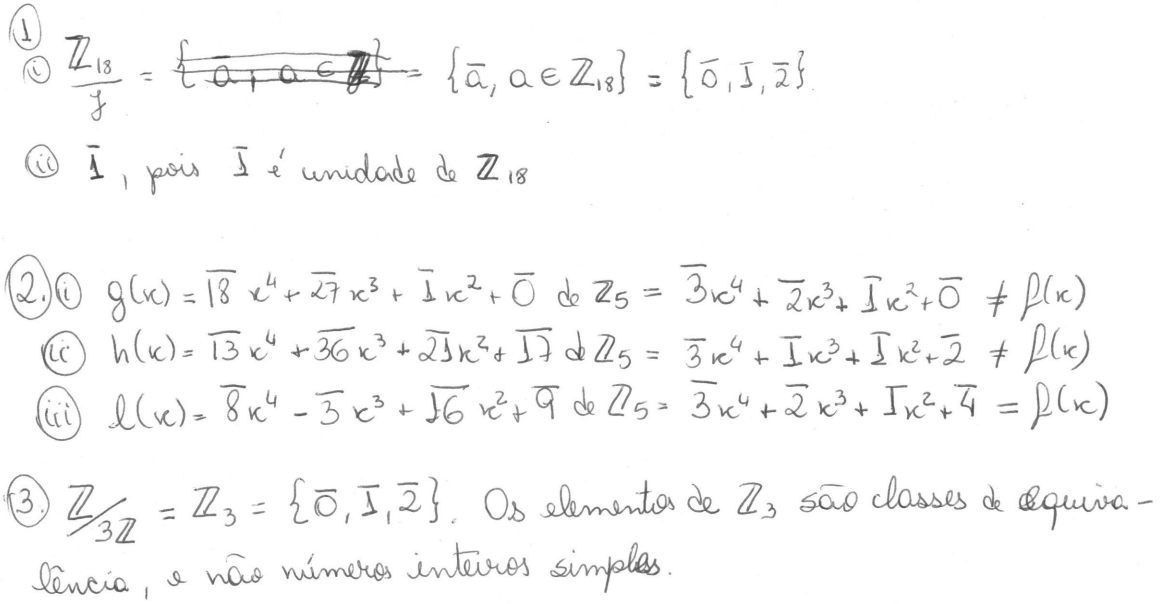
2) i) $g(x) = 3x^4 + 2x^3 + x^2$.
$h(x) = 3x^4 + x^3 + x^2 + 2$
$l(x) = 3x^4 + 2x^3 + x^2 + 4 = f(x)$

3) não pois $\mathbb{Z}$ contém inteiros e $\mathbb{Z}_3$ contém CLASSES

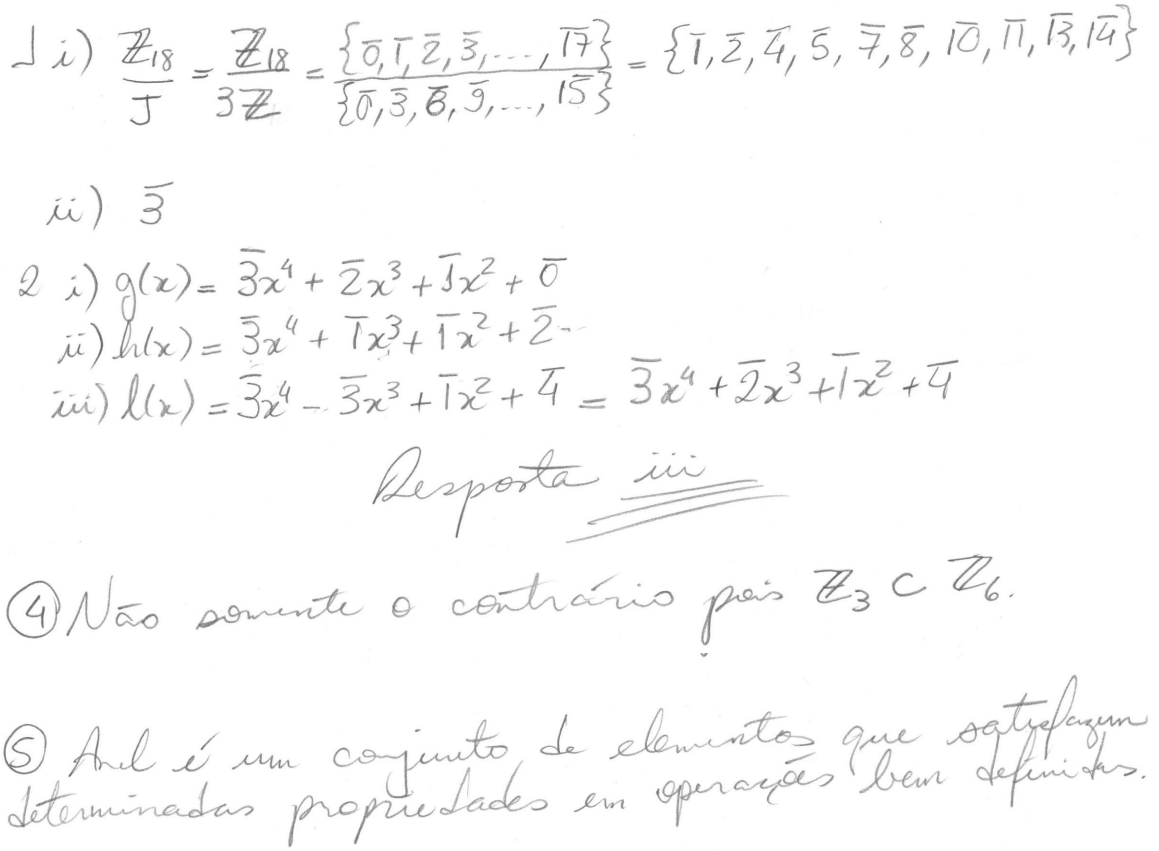
4) $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. $\bar{0}^3 \neq \bar{0}^6$ logo $\mathbb{Z}_3 \not\subset \mathbb{Z}_6$

5) é o conjunto de todas as classes de equivalência

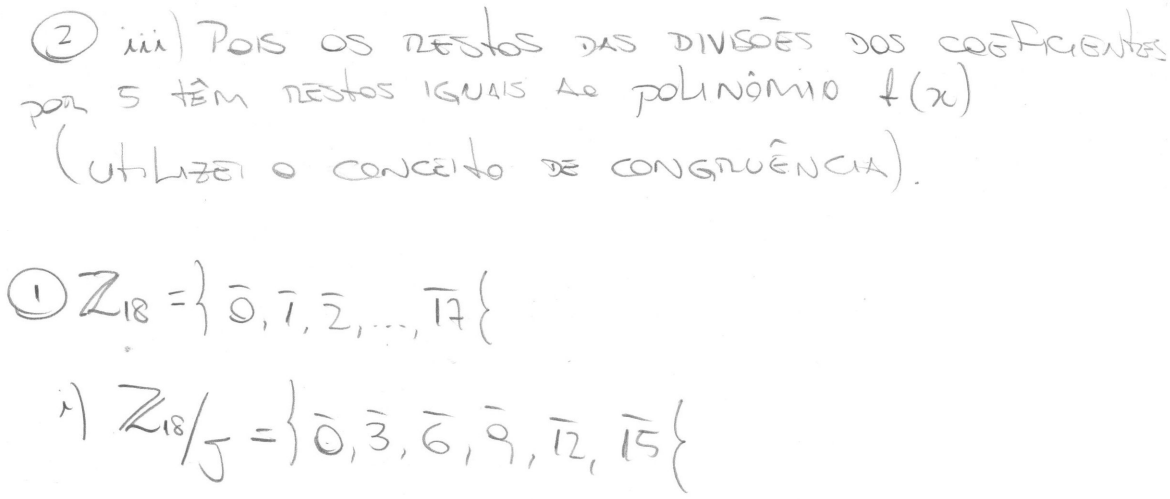
Respostas do estudante N3



Respostas do estudante N4



Respostas do estudante N5

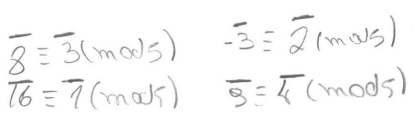


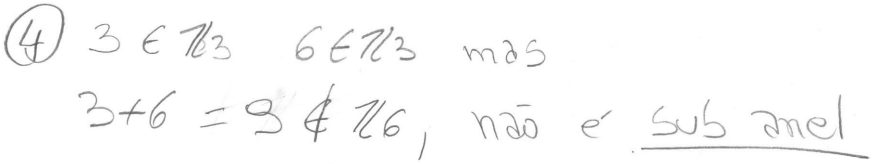
Respostas do estudante N6

2. Qual polinômio abaixo é igual ao polinômio $f(x) = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{4}$ de $\mathbb{Z}_5[x]$. Justifique sua resposta.
   i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \bar{1}x^2 + \bar{0}$ de $\mathbb{Z}_5[x]$. $\bar{0} \not\equiv \bar{4}$ em $\mathbb{Z}_5$
   ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ de $\mathbb{Z}_5[x]$ $\overline{36} \neq 2$ em $\mathbb{Z}_5$
   iii) $l(x) = \bar{8}x^4 - \bar{3}x^3 + \overline{16}x^2 + \bar{9}$ de $\mathbb{Z}_5[x]$.
3. Os elementos de $\mathbb{Z}/3\mathbb{Z}$, podem ser elementos de Z? Justifique sua resposta.
   Sim pois $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$
4. Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta.
   Não pois $\bar{2} + \bar{3} = \bar{5} \notin \mathbb{Z}_3$

Respostas do estudante N7

2. Qual polinômio abaixo é igual ao polinômio $f(x) = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{4}$ de $\mathbb{Z}_5[x]$. Justifique sua resposta.
   i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \bar{1}x^2 + \bar{0}$ de $\mathbb{Z}_5[x]$.
   ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ de $\mathbb{Z}_5[x]$
   iii) $l(x) = \bar{8}x^4 - \bar{3}x^3 + \overline{16}x^2 + \bar{9}$ de $\mathbb{Z}_5[x]$.





Respostas do estudante N8

2. Qual polinômio abaixo é igual ao polinômio $f(x) = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{4}$ de $\mathbb{Z}_5[x]$. Justifique sua resposta.
   i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \bar{1}x^2 + \bar{0}$ de $\mathbb{Z}_5[x]$.
   ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ de $\mathbb{Z}_5[x]$
   iii) $l(x) = \bar{8}x^4 - \bar{3}x^3 + \overline{16}x^2 + \bar{9}$ de $\mathbb{Z}_5[x]$. (classes) A diferença dos mi deve ser divisível por 5 //

4. Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta.

Acredito que não, pois $\mathbb{Z}_6$ é maior que $\mathbb{Z}_3$, não há como ser subanel

Respostas do estudante N9

(2) (i) $18 \,|\, 15 \,|\, 3 = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{0}$, no entanto $\bar{0} \neq \bar{4}$

(ii) $\bar{3}x^4 + \bar{1}x^3 + \bar{1}x^2 + \bar{2}x$ $\quad \bar{1}x^3 \neq \bar{2}x^3$ e

(iii) $\bar{3}x^4 + \bar{2}x^3 + 1x^2 + \bar{4}$, logo (iii) é igual a $f(x)$.

$-\bar{3} + \bar{5} = \bar{2}$

(3) $\mathbb{Z}_3\mathbb{Z}$ não podem ser elementos pois alguns elementos de $\mathbb{Z}_3\mathbb{Z} \notin \mathbb{Z} \Rightarrow \mathbb{Z}_3\mathbb{Z}[3] = \frac{1}{3} \notin \mathbb{Z}$

(4) Não $\mathbb{Z}_6$ é subanel de $\mathbb{Z}_3$ pois $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ é o conjunto dos divisores de 3. 3 é divisor de $9 \neq \bar{0}$, no entanto 6 não é divisor de 9.

Respostas do estudante N10

(2) $18 \,|\, 15 \,|\, 3 = \bar{3} + \bar{5} = \bar{1}$ $\quad \bar{16} \,|\, 15 \,|\, 3$ $\quad 9 \,|\, 15 \,|\, 4$

O polinômio $f(x) = f(x)$, pois as classes de equivalência são iguais

(4) $\mathbb{Z}_6$ $\mathbb{Z}_3$

$\bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}, \bar{18}, \in \mathbb{Z}_3$

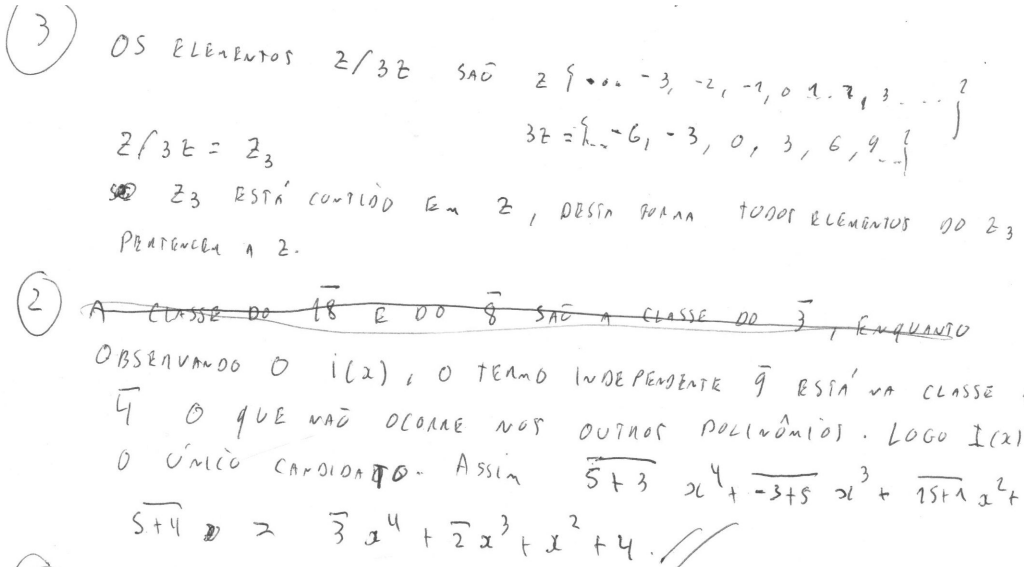
$\bar{6}, \bar{12}, \bar{18} \in \mathbb{Z}_6$

Não. Como $\mathbb{Z}_3 \supset \mathbb{Z}_6$, ou seja existem elementos que pertencem a $\mathbb{Z}_3$ mas que não pertencem a $\mathbb{Z}_6$, logo $\mathbb{Z}_3$ não é subanel de $\mathbb{Z}_6$.

Respostas do estudante N11

(5) TENHA DIFICULDADES. CONSEGUIA EXPLICANDO RELAÇÕES DE CONGRUÊNCIA.

(4) NÃO, $\mathbb{Z}_6$ É SUBANEL DE $\mathbb{Z}_3$, UMA VEZ QUE $\mathbb{Z}_6 = 2\mathbb{Z}_3$.



(3) OS ELEMENTOS $\mathbb{Z}/3\mathbb{Z}$ SÃO $\mathbb{Z}\{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

$3\mathbb{Z} = \{\ldots -6, -3, 0, 3, 6, 9 \ldots\}$

$\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$

$\mathbb{Z}_3$ ESTÁ CONTIDO EM $\mathbb{Z}$, DESTA FORMA TODOS ELEMENTOS DO $\mathbb{Z}_3$ PERTENCEM A $\mathbb{Z}$.

(2) ~~A CLASSE DO $\overline{18}$ E DO $\overline{8}$ SÃO A CLASSE DO $\overline{2}$, ENQUANTO~~ OBSERVANDO O $i(x)$, O TERMO INDEPENDENTE $\overline{9}$ ESTÁ NA CLASSE DO $\overline{4}$ O QUE NÃO OCORRE NOS OUTROS POLINÔMIOS. LOGO $I(x)$ É O ÚNICO CANDIDATO. ASSIM $\overline{5+3}\,x^4 + \overline{-3+5}\,x^3 + \overline{15+1}\,x^2 + \overline{5+4} = \overline{3}\,x^4 + \overline{2}\,x^3 + x^2 + 4$. //

Respostas do estudante N12

(2) i) $\overline{18} = \overline{3}$ em $\mathbb{Z}_5(x)$

$\overline{27} = \overline{2}$ em $\mathbb{Z}_5(x)$

$\overline{1} = \overline{1}$ em $\mathbb{Z}_5(x)$, mas $\overline{0} \neq \overline{4}$ em $\mathbb{Z}_5(x)$, então $g(x) \neq f(x)$

ii) $\overline{13} = \overline{3}$ em $\mathbb{Z}_5(x)$

$\overline{36} = \overline{1}$ em $\mathbb{Z}_5(x)$ e por aqui já vemos que $h(x) \neq f(x)$

iii) $\overline{8} = \overline{3}$ em $\mathbb{Z}_5(x)$

$-\overline{3} = \overline{2}$ em $\mathbb{Z}_5(x)$

$\overline{16} = \overline{1}$ em $\mathbb{Z}_5(x)$

$\overline{9} = \overline{4}$ em $\mathbb{Z}_5(x)$, então $l(x) = f(x)$

(4) $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$

$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

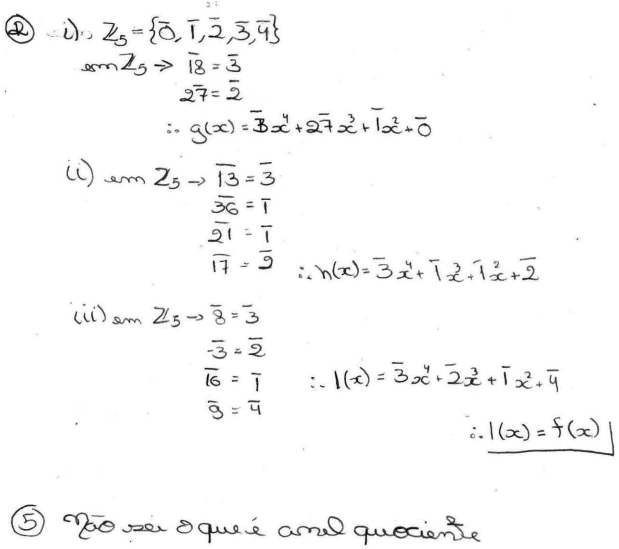
Então $\mathbb{Z}_3$ é subanel de $\mathbb{Z}_6$.

(5) Tomemos como exemplo $\mathbb{Z}_3$

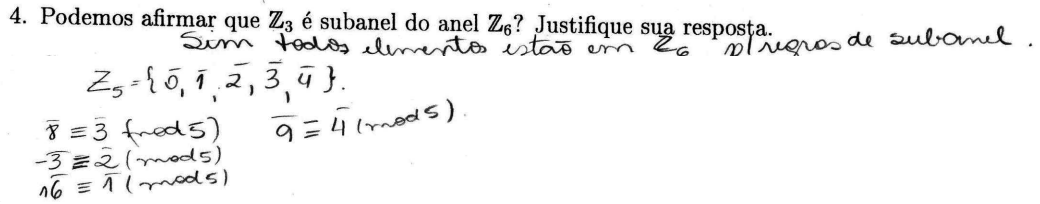
$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$

Anel quociente será o conjunto dos números irredutíveis em 3. Qualquer outro número adicionado à este conjunto será reduzido a algum destes elementos, quando dividido por 3 e tomado seu resto.

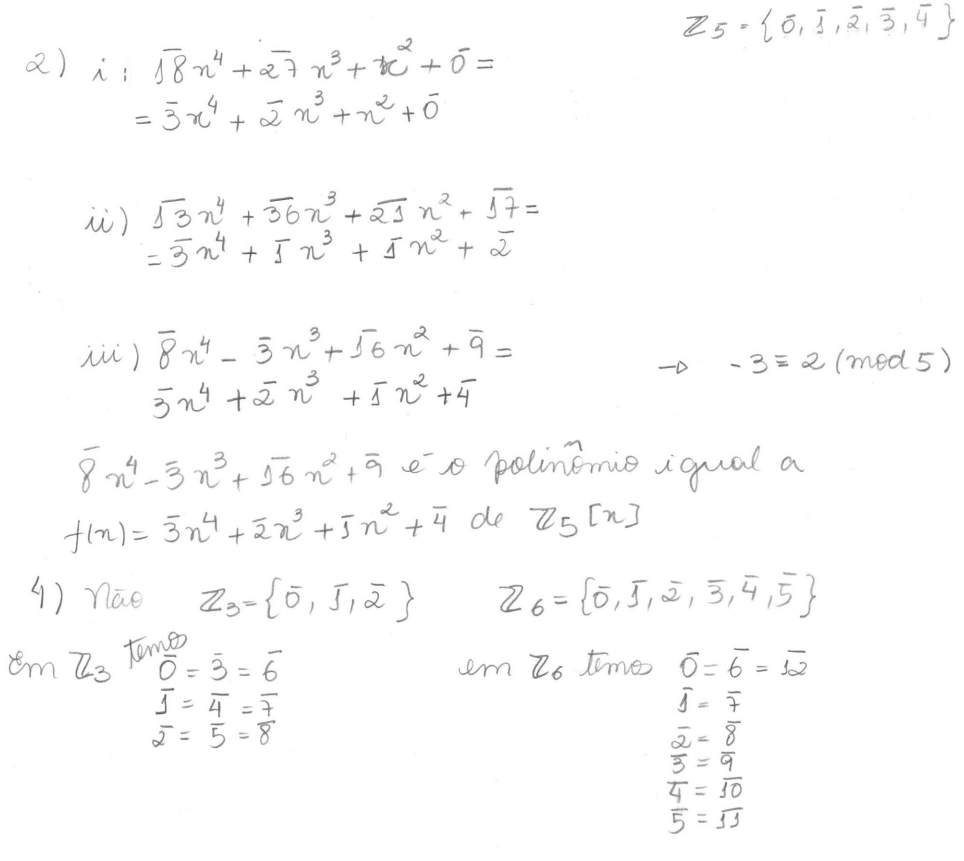
Respostas do estudante N13



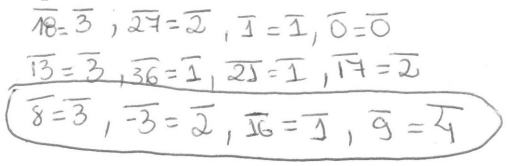
Respostas do estudante N14



Respostas do estudante N15



Respostas do estudante N16



(2) item (iii) pois :

$\overline{8}=\overline{3}$, $\overline{-3}=\overline{2}$, $\overline{16}=\overline{1}$, $\overline{9}=\overline{4}$.

Respostas do estudante N17

2. Qual polinômio abaixo é igual ao polinômio $f(x) = \overline{3}x^4 + \overline{2}x^3 + \overline{1}x^2 + \overline{4}$ de $\mathbb{Z}_5[x]$. Justifique sua resposta.

   i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \overline{1}x^2 + \overline{0}$ de $\mathbb{Z}_5[x]$. $\overline{3}x^4 + \overline{2}x^3 + \overline{1}x^2 + \overline{0}$

   ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ de $\mathbb{Z}_5[x]$ $\overline{3}x^4 + \overline{1}x^3 + \overline{1}x^2 + \overline{2}$

   iii) $l(x) = \overline{8}x^4 - \overline{3}x^3 + \overline{16}x^2 + \overline{9}$ de $\mathbb{Z}_5[x]$. $\overline{3}x^4 + \overline{2}x^3 + \overline{1}x^2 + \overline{4}$

4. Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta.

   Sim é fechado p/ adição e mult.

5. Como você explicaria para um aluno do primeiro ano do Curso de Matemática o que é um anel quociente? Justifique sua resposta.

   Não faço nem idéia

Respostas do estudante Q1

(1) i) $\mathbb{Z}_{18/J} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ → elementos comuns a $\mathbb{Z}_{18}$ e J.

ii)

iii) $\mathbb{Z}_3$ → mesmos elementos

(2) i) $g(x) = \overline{18}x^4 + \overline{27}x^3 + \overline{1}x^2 + \overline{0}$ $\mathbb{Z}_5$.
$= \overline{3}x^4 + \overline{2}x^3 + x^2$

ii) $h(x) = \overline{13}x^4 + \overline{36}x^3 + \overline{21}x^2 + \overline{17}$ $\mathbb{Z}_5$.
$= \overline{3}x^4 + x^3 + x^2 + \overline{2}$

iii) $l(x) = \overline{8}x^4 - \overline{3}x^3 + \overline{16}x^2 + \overline{9}$ ← esta sim é igual a $f(x)$
$= \overline{3}x^4 + \overline{2}x^2 + x^2 + \overline{4}$

(3) Sim, pois os elementos são múltiplos de $3n$, $n \in \mathbb{Z}$.
$3\mathbb{Z}$ é subanel de $\mathbb{Z}$

↳ $(\bar{0}, \bar{1}, \bar{2})$

(4) $\mathbb{Z}_3 \subset \mathbb{Z}_6 \rightarrow (\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5})$

sim, pois $\mathbb{Z}_3 \subset \mathbb{Z}_6$.

(5) É o conj. dos restos das divisões dos elementos dos anéis.

Respostas do estudante Q2

1) Até agora não entendi o que é anel comutativo

2) (iii). pois em $\mathbb{Z}_5[a]$ temos que $\overline{18} = \bar{3}$ $(18 = 3.5 + 3)$

assim como $-\bar{3} = \bar{2}$ pois $-3+5=2$

. $\overline{16} = \bar{1}$ pois $3.5 + 1 = 16$ e $\bar{9} = \bar{4}$ pois $4+5=9$

(4) não, um contra-exemplo seria $\bar{3} + \bar{3} = \bar{6} \notin \mathbb{Z}_3$

assim $\mathbb{Z}_3$ n é fechado p/ soma

5) Como eu disse, de anel comutativo não sei nada.

Respostas do estudante Q3

1) i) $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \mathbb{Z}_{18}/J$?

ii) $\bar{1}$

iii) $\mathbb{Z}_6$

2) $l(x) = \bar{8}x^4 - \bar{3}x^3 + \bar{16}x^2 + \bar{9}$

Porque $\bar{8}$ em $\mathbb{Z}_5$ é igual a $\bar{3}$

$-\bar{3}$ " " " " " $\bar{2}$

$\bar{16}$ " " " " " $\bar{1}$

$\bar{9}$ " " " " " $\bar{4}$

Por divisão.

3) Podem, serão coincidentes com os multiplos de 3.

4) Sim $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

Como os elementos de $\mathbb{Z}_3$ estão em $\mathbb{Z}_6$, então $\mathbb{Z}_3$ é subanel de $\mathbb{Z}_6$.

5) Sem dúvida, fazer primeiro uma comparação e/ou uma analogia a "congruência módulo m", da teoria de anéis

Respostas do estudante Q4

(1) (I) $\frac{\mathbb{Z}_{18}}{\bar{3}\mathbb{Z}}$ = CONJUNTO DAS CLASSES DE EQUIVALÊNCIA DE $\mathbb{Z}_{18}$ MOD 3 = $\frac{\{\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{18}\}}{\{\bar{0}, \bar{3}, \bar{6}, \ldots, \bar{15}\}} = \mathbb{Z}_3$?

(2) TESTANDO: $g(x)$: $\bar{18}x^4 + \bar{27}x^3 + \bar{1}x^2 + \bar{0}$ DE $\mathbb{Z}_5[x] = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{5}$.
MAS $\bar{3} \neq \bar{4}$, ENTÃO NÃO É IGUAL.
$h(x)$: $\bar{13}x^4 + \bar{36}x^3 + \bar{21}x^2 + \bar{17} = \bar{3}x^4 + \bar{1}x^3 + \bar{1}x^2 + \bar{2}$ (PARECE $\neq$)
$l(x) = \bar{8}x^4 - \bar{3}x^3 + \bar{16}x^2 + \bar{9} = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{4}$ ESSE É IGUAL AO $f(x)$.
(USA-SE QUE $\bar{0} = \bar{5} = \bar{10} = \ldots$ E $\bar{1} = \bar{6} = \bar{11} = \ldots$ ETC)

(3) NÃO OS ELEMENTOS DO ANEL QUOCIENTE SÃO CLASSES DE EQUIVALÊNCIA, E NÃO INTEIROS.

(4) $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ $\mathbb{Z}_3 \not\subset \mathbb{Z}_6$, POIS AS CLASSES DE $\mathbb{Z}_3$ SÃO DE CONGRUÊNCIA
$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ MÓDULO 3, ENQUANTO AS DO $\mathbb{Z}_6$ SÃO MÓDULO 6.

(5) $A/_{\mathbb{Z}}A$ É O CONJUNTO (IMAGINO QUE O ALUNO DO 1º ANO NÃO SAIBA O QUE É ANEL) DOS CONJUNTOS DOS RESTOS DAS DIVISÕES DOS ELEMENTOS DE A PELO $\mathbb{Z}A$ QUE É O CONJUNTO DOS MÚLTIPLOS DE $\mathbb{Z}$ EM A.

Respostas do estudante Q5

(02) O ítem (iii) é o polinômio igual ao polinômio proposto $l(x) = f(x)$, utilizando da congruência.

(01) $\mathbb{Z}_{18} = (\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{17})$

(i) $\mathbb{Z}_{18}/_{J} = (\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15})$

(03) Podem ser seus elementos de $\mathbb{Z}$, pois é seu subanel.

Respostas do estudante Q6

(2) É a (iii) porque Justificativa o polinômio $l(x) = \bar{8}x^4 - \bar{3}x^3 + \overline{16}x^2 + \bar{9}$ de $\mathbb{Z}_5[x]$, analisando seus coeficientes, terão os mesmos restos com os respectivos coeficientes de $f(x) = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{4}$ quando divididos por 5.

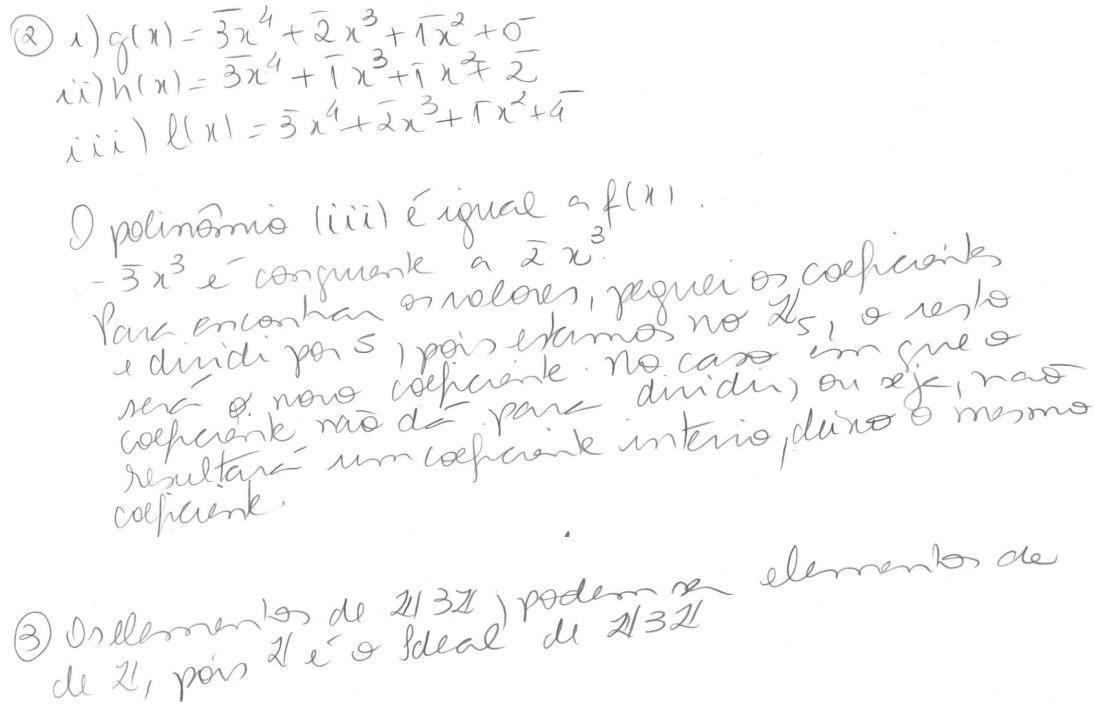
4. Podemos afirmar que $\mathbb{Z}_3$ é subanel do anel $\mathbb{Z}_6$? Justifique sua resposta.
Sim, porque $\mathbb{Z}_3 \subset \mathbb{Z}_6$.

Respostas do estudante Q7

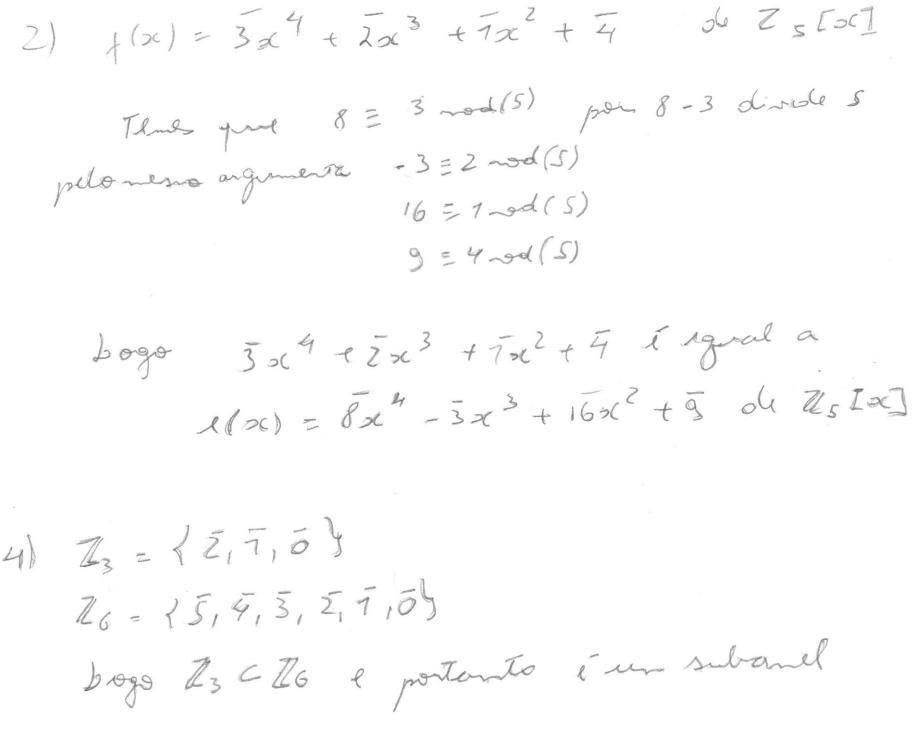
(2)(iii) Pois $\bar{8} = \bar{3}$ em $\mathbb{Z}_5[x]$
$-\bar{3} = \bar{2}$ em $\mathbb{Z}_5[x]$
$\overline{16} = \bar{1}$ em $\mathbb{Z}_5[x]$
$\bar{9} = \bar{4}$ em $\mathbb{Z}_5[x]$

(5) É o conjunto dos elementos de $\mathbb{Z}$ que são PRIMOS com elemento de J.

Respostas do estudante Q8



Respostas do estudante Q9



Respostas do estudante Q10

(2) apenas o iii é igual.
pois $g(x) = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{0} \neq f(x)$,
$h(x) = \bar{3}x^4 + \bar{1}x^3 + \bar{1}x^2 + 2 \neq f(x)$
$i(x) = \bar{3}x^4 + \bar{2}x^3 + \bar{1}x^2 + \bar{4} = f(x)$

(4) Não.
É ao contrário,
pois os elementos
de $\mathbb{Z}_6$ é que
estarão dentro de $\mathbb{Z}_3$.