Universidade Federal de Mato Grosso
Instituto de Cências Exatas e da Terra
Departamento de Matemática

TEOREMA CHINÊS DO RESTO:
Sua aplicação no ensino médio

Adriano Sales Nascimento

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Junho - 2014

TEOREMA CHINÊS DO RESTO:
Aplicações no Ensino Médio

Dissertação apresentada ao curso de Metrado Profissional em Matemática - PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título em MESTRE em Matemática.

Cuiabá, 16 de Junho de 2014

Prof. Dr. Martinho da Costa Araújo Orientador

Banca examinadora:

Prof. Dr.

Prof. Dr.

Prof. Dr.

A minha Avó (in memorian) minha fonte de inspiração. Aos meus filhos e esposa que nos momentos difíceis tiveram paciência e compreensão para me ajudar a concluir mais uma etapa de vida.

Agradecimentos

Gostaria de agradecer aos meus avós, Nuporanga (*in memorian*) e Alvarina (*in memorian*) aos qual devo todo incentivo e orientação no início do estudo na minha vida. Agradeço aos meus filhos e esposa por me incentivarem e compreenderem a minha ausência devido os estudos e aulas para conclusão de mais uma etapa da minha vida acadêmica.

Agradeço o apoio dos grandes amigos que fiz nesse mestrado, em especial aos companheiros Moacir, Wilson, Giseli, Nayara e Liliana com muitas horas de estudo e de boas discussões para um melhor aprendizado.

Devo agradecer ao meu orientador, Prof. Dr. Martinho da Costa Araújo pelo apoio a realização deste trabalho, bem como aos professores Moíses e André fonte de inúmeras consultas no decorrer do mestrado, que contribuíram e muito para meu aperfeiçoamento na formação matemática. Agradeço a Deus por colocar todas essas pessoas maravilhosas no meu caminho e me auxiliar nessa grande etapa da minha vida.

"Não existe ramo da matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real".(Nicolai Lobachevsky)

Resumo

Este trabalho pretende mostrar que o Teorema Chinês do Resto é um tema atual e que pode ser introduzido no Ensino Médio, por meio de uma proposta de ensino de um minicurso com ênfase na resolução de exercícios contextualizados. Para o minicurso inicialmente é apresentado uma fundamentação teórica sobre o assunto, revisão de divisibilidade, mínimo múltiplo comum, máximo divisor comum e números primos, bem como a introdução a congruência linear e algumas de suas propriedades apresentando aplicações para solução de problemas contextualizados de olimpíadas de matemática, e processos seletivos para faculdades e universidades. O minicurso é sobre teorema Chinês do resto e sua aplicabilidade em resolução de exercícios contextualizados, de grande importância para os alunos do Ensino Médio.

Palavra Chave: Divisibilidade, congruência linear, ensino médio exercícios contextualizados, Teorema Chinês do Resto.

Abstract

This paper has intention to show that the Reminder Chinese Theorem is a nowadays issue which can be introduced into the Hight School Program through the idea of an extra-curricular course giving emphasis to solving problems with context in the student's everyday.

The course, at a first approach, the theory can be taught over the subject, lookimg back on divisibility, least common multiple, highest common divider, prime mumbers as well as the introduction to linear congruity and some of it's property, showing their applications on solving problems related specifically to the Math Olympics and on solving problems given on universities' admittance exams. The course would bring up the Reminder Chinese Theorem and it's use on solving contextualized math problems that are of great importance to Hight School students.

Key Words: Divisibility, linear congruity, contextualized Hight School Math problems, Reminder Chinese Theorem.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

O Teorema Chinês do Resto é um item de sistemas de equações envolvendo congruência linear. O teorema examina a existência de soluções para tais sistemas. Utilizamos o teorema para resolver vários problemas dentro do Ensino Médio na área da Matemática, muitos deles, relacionados ao nosso cotidiano.

Esse trabalho tem como objetivo **uma proposta de criação de um minicurso sobre Teorema Chinês do Resto e suas aplicações no Ensino Médio**, visto a grande importância desse assunto para solução de alguns exercícios envolvendo progressão aritmética e divisibilidade e apesar disso é comum a ausência em alguns componentes curriculares. O minicurso é baseado no Teorema Chinês do Resto e a proposta é abordar o tema com uma linguagem mais acessível ao aluno do Ensino Médio. Alguns tópicos para a resolução do Teorema Chinês do Resto, necessitam de propriedades e de alguns conceitos de Aritmética, para isso no capítulo 2 apresentaremos fundamentação teórica necessária a introdução do assunto. No capítulo 3 abordaremos o **Teorema Chinês do Resto e suas aplicações no Ensino Médio**, cujo conteúdo foi organizado para um melhor entendimento do aluno do Ensino Médio e no capítulo 4 faremos um breve relato do minicurso que já foi aplicado em duas escolas com turmas do Ensino Médio:

-Colégio Maxi(turma do $3^{\underline{o}}$ ano do Ensino Médio privado) - Escola Estadual Liceu Cuiabano (turma do 2° ano do Ensino Médio público Estadual)

Existe uma grande quantidade de material sobre o assunto, principalmente nos livros sobre teoria dos números, mas a grande maioria não é voltada para os alunos do Ensino Médio. Grande parte do referencial teórica neste trabalho tem suporte em Elementos de Aritmética- Hefez(2011) e no Tópico de Matemática Elementar volume 5 Teoria dos Números Muniz Neto(2012).

Serve, também, de referência para este trabalho, a dissertação de mestrado profissional de Marco Antonio de Oliveira Barros, o trabalho final de conclusão de curso em

matemática de Cleice de Cássia F Cidade e um artigo interessante do Professor Ilydio Pereira de Sá intitulado "Aritmética Modular e algumas de suas aplicações", no qual o mesmo ressalta que o assunto em questão "é um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental e é gerador de excelentes oportunidades de contextualizações no processo de ensino e aprendizagem da matemática".

Ressaltamos ainda que, embora, também pretenda servir de apoio a professores e estudantes de nível superior de ensino, este trabalho é direcionado para professores e alunos do Ensino Médio. Muitos dos alunos dessa faixa etária ainda não tem a maturidade ou não possui pré-requisitos necessário para compreender todas as demonstrações referentes a fundamentação teórica. O minicurso é fundamentado na necessidade de solução de exercícios contextualizados para alunos do Ensino Médio em processos seletivos de universidades e olimpíadas de matemática.

Capítulo 1

Apresentação do Trabalho

O teorema Chinês do resto é um conceito muito importante que esta relacionado com divisibilidade e os restos da divisão de números inteiros. Alguns alunos e professores podem relacionar o tema com mínimo múltiplo comum (MMC) ou Congruência linear. Muito se tem escrito sobre o assunto em livros de teoria dos números, mas, apesar de utilizarmos os restos de divisão para solucionarmos vários exercícios, encontramos pouco material sobre o TCR para aluno nessa fase do ensino.

Essa dissertação é uma proposta de criar um minicurso de teorema chinês do resto e suas aplicações no ensino médio, com ênfase na resolução de exercícios contextualizados de diversos assuntos da matemática tais como: Progressões Aritméticas, Matrizes, Números com parte imaginária entre outros com o objetivo de mostrar a aplicação do TCR no ensino médio. As questões foram retiradas de livros didáticos utilizados no ensino médio, olimpíadas de matemática para o ensino médio e processos seletivos pós ensino médio para faculdades e universidades, mostrando assim que é um tema com muita aplicação nas séries do ensino médio.

1.1 Como Aplicar o Teorema Chinês do Resto

O teorema chinês do resto é um assunto com várias aplicações: divisibilidade, números primos, MDC e MMC são alguns dos conteúdos matemáticos que encontramos no ensino médio e que podem ser ministrados para os alunos.

A linguagem para a aplicação do teorema chinês do resto pode ser a formal dos livros de aritmética, mas exemplos e suas aplicações facilita para o aluno a visão mais

contextualizada, mais próxima da linguágem dos livros do ensino médio.

A aplicação será mostrada com problemas contextualizados sobre satélites, reposição salarial, doságem de remédios e outros. Ainda podemos aplicar na resolução de sistema de congruência ou na solução simultânea de sistema de equações.

No decorrer do curso de mestrado profissional vários assuntos foram abordados e discutidos pelos professores e mestrandos. Um deles que se destacou pela ausência nas escolas da nossa região foi o tema abordado. A princípio alguns dos mestrandos diria que a aplicação seria apenas na resolução de congruências linear. No decorrer das aulas várias aplicações foram surgindo, e outras foram comparadas com o teorema.

A dissertação sobre a aplicação de teorema, surge da necessidade de mostrar para o aluno do ensino médio algumas desses aplicações.

O minicurso foi uma ideia para colocar em prática conceitos de aplicações.

Algumas foram colocadas no minicurso e outras ficaram como sugestão.

O teorema necessita de assuntos da matemática que o estudante deve ter como fundamento teórico e que será visto no capitulo 2. Veremos a seguir alguns assuntos que são utilizados no ensino médio e servem de ponto de partida para que o aluno utilize na aplicação do teorema.

1.1.1 Divisibilidade e Divisão Euclidiana

O minicurso necessita de um conceito de divisibilidade que não é muito abordado no ensino fundamental, o ensino da divisibilidade no minicurso foi de maneira formal e apresentado para alguns alunos do ensino médio pela primeira vez, visto que alguns não conheciam a abordagem formal de divisibilidade. Foi normal o questionamento de alguns alunos sobre os símbolos usados. Ocorreu o questionamento de alguns, para que utilizar essa simbologia? Isso não torna o assunto mais confuso?

Alguns critérios de divisibilidade foram vistos e revistos para melhor conceituação e compreensão dos alunos. As regras de divisibilidade dos primeiros números primos 2, 3, 5, 7, 9 e 11 foram revisada e complementada com as regras de divisibilidade de números compostos 4, 6, 8, 10, 12 e 14.

A Divisão Euclidiana se torna muito útil no minicurso para uma formalização mais aproximada com o tipo encontrada nos livros didáticos utilizados pelos alunos que participaram do minicurso. A formalização $X \equiv a \mod b$ é mais aceita ao ser escrita

$X = b \cdot q + a$

Exemplo 1.1.1. Mostrar que o resto da $10n - 1$ por 9 sempre é 0, qualquer que seja o número natural n.

Solução. Utilizando uma das propriedades do algoritmo da Divisão. Dados a e b inteiros e k natural, temos que: Se $a \neq b$, então $a - b|(a^k - b^k)$. Sendo $a = 10$ e $b = 1$ temos que $10 - 1|(10^k - 1^k)$ logo $9|(10^k - 1)$ ou seja $10^n = 9 \cdot q + 1$.

Exemplo 1.1.2. Qual o maior número natural n que dividido por 11 deixa quociente igual ao resto?

Solução. $X = 11 \cdot q + r$, sendo $q = r$ temos que $X = 11 \cdot r + r = 12r$.

Os valores de r é uma variação de $0 \leq r \leq 10$. Sendo o maior valor de $r = 10$, $X = 120$. De fato dividindo 120 por 11, encontramos quociente igual ao resto.

Exemplo 1.1.3. Todo quadrado perfeito deixa resto 0 ou 1 quando dividido por 3.

Solução. Pelo algoritmo da divisão, o resto da divisão de n por 3 é 0, 1 ou 2, de modo que $n = 3q$, $n = 3q + 1$ ou $n = 3q + 2$ para algum q inteiro.

Se $n = 3q$ então $n^2 = (3q)^2 = 9k = 3m$

Se $n = 3q + 1$ então $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3m + 1$

Se $n = 3q + 2$ então $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3m + 3 + 1 = 3n + 1$.

Os exemplos são melhores compreendidos quando no minicurso surge alguns exemplos numéricos. Não deixando a demonstração formal como a única maneira de demonstração para os alunos do ensino médio.

Exemplo 1.1.4. Sendo n ímpar, então $n^2 - 1$ é divisível por 8.

Solução. Sendo n ímpar então pode ser escrito como $2m + 1$.

$(2m + 1)^2 - 1 = 4m^2 - 4m + 1 - 1 = 4m^2 - 4m = 4m(m + 1) = 4$(par)(ímpar) ou 4(ímpar)(par) $= 8.k$

1.1.2 Números Primos

Um tópico que gera sempre questionamento é o conjunto dos números primos. A fatoração em número primo é muito bem conceituado como revisão para divisibilidade. Nesta unidade recordamos o conceito de número primo e número composto que é

muito importante para solucionarmos problemas contextualizados e aplicarmos algumas propriedades nos Mínimo Múltiplo Comum (MMC), Máximo Divisor Comum (MDC) e congruência linear.

Um inteiro $p \geq 2$ é primo se seus únicos divisores positivos forem ele mesmo e 1. O número p que não for primo é composto e formado pelo produto de números primos. Citamos alguns números do conjunto dos números primos

$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \cdots\}$

A primeira pergunta no minicurso sobre os primos é "Professor, como descobrir se o número é primo?"

Exemplo 1.1.5. Sendo $n \geq 2$ for composto então existe um divisor primo p de n tal que $p \leq \sqrt{n}$.

Solução. Seja $n = ab$ com $2 \leq a \leq b$. Sendo p um divisor primo de a, segue que $p|nk$.

$$p^2 \leq a^2 \leq ab = n, \qquad p \leq \sqrt{n}$$

A representação de um inteiro $n \geq 2$ como um produto de potências de primos é sua fatoração ou decomposição canônica em fatores primos.

Exemplo 1.1.6. Prove que um natural n é quadrado perfeito se e só se o número de divisores naturais $d(n)$ for ímpar. Se $n = p_i^{x_i} \cdot \ldots \cdot p_k^{x_k}$ é decomposição canônica do inteiro $n \geq 2$, então os divisores positivos de n são os números da forma $p_i^{y_i} \cdot \ldots \cdot p_k^{y_k}$ onde $0 \leq y_i \leq x_i$ para todo i.

Podemos representar os divisores naturais como $d(n) = \prod (y_i + 1)$

Solução. Se $d \geq 2$ é divisor de n e p é um primo que divide d, então p também divide n logo p é igual a um dos primos $p_i \cdot \ldots \cdot p_k$ válido para todo divisor primo de d, assim $d = p_i^{y_i} \cdot \ldots \cdot p_k^{y_k}$, com $y_i \geq 0$ para todo i. Sendo q natural então $n = dq$.

Se $n = p_1^{x_1} \cdot \ldots \cdot p_k^{x_k} q$ e $d = p_1^{y_1} \cdot \ldots \cdot p_k^{y_k}$, $y_i \leq x_i$ para todo i. Como $0 \leq y_i \leq x_i$ para $1 \leq i \leq k$, é um divisor positivo de n há $y_i + 1$ possibilidades para x_i.

Exemplo 1.1.7. Sendo $n! = 1 \times 2 \times 3 \times 4 \times \cdot \times n$, qual o valor de n para $n! = 215 \times 36 \times 53 \times 72 \times 11 \times 13$.

Solução. Sendo $n = 1 \times 2 \times 3 \times (2 \times 2) \times 5 \times (2 \times 3) \times 7 \times (2 \times 2 \times 2) \times \cdots$, basta descobrir qual a quantidade de números primos 2 usamos para decompor n. Sendo $2, 4, 6, 8, \cdots$ os números pares que utilizam 2 apenas uma vez e $4, 8, 16, \cdots$ os números pares que utilizam 2 duas vezes e assim sucessivamente $215 = 2 \times 22 \times 2 \times 23 \times 2 \times 22 \times 2 \times 24$ ou seja até 16. $N = 16$.

Exemplo 1.1.8. Quantos divisores naturais tem o número 144?

Solução. Como 144 pode ser escrito de forma canônica $2^4 \times 3^2$ ou seja $d(144) = 5 \times 3 = 15$.

Podemos concluir com o exemplo (1.1.6) que n possui uma quantidade ímpar de divisores se, e somente se, cada x_i é par, ou seja, um quadrado perfeito. Relaciona a isso existe uma brincadeira que é muito bem aceita pelos alunos.

No vestiário de uma escola com n alunos, numerados de 1 a n, há n armários enfileirados em um corredor, também numerados de 1 a n. Um dia , os alunos resolvem fazer a seguinte brincadeira:

O primeiro aluno abre todos os armários, em seguida, o aluno 2 fecha todos os armários de número par, o aluno 3 inverte as posições dos armários de número múltiplo de 3 e assim por sucessivamente. Propõe para a turma se alguém consegue dizer , quais armários ficaram abertos?

Os armários com números de divisores ímpares ficaram abertos, os armários de divisores pares ficaram fechados. Concluímos para os alunos que os abertos serão os QUADRADOS PERFEITOS.

1.1.3 Máximo Divisor Comum e Mínimo Múltiplo Comum

Um dos conceitos com boa aceitação no minicurso foram a aplicabilidade de Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC). Foi apresentado para a os alunos uma nova nomenclatura para a maioria deles.

Máximo Divisor Comum entre a e b: $(a; b)$

Mínimo Múltiplo Comum entre a e b: $[a; b]$

MDC- Dados dois números naturais a e b, não simultaneamente nulos, diremos que o número natural não nulo é um divisor comum de a e b se $d|a$ e $d|b$. A definição dada por Euclides nos Elementos e se constitui um dos pilares da sua aritmética. Diremos que d é um máximo divisor comum de a e b se possuir as seguintes propriedades:

i) d é um divisor comum de a e de b

ii) d é divisível por todo divisor comum de a e b

Calculemos MDC de 372 e 162 pelo algoritmo de Euclides:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Tabela 1.1: MDC de 372 e 162

Observe que acima nos fornece

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ 12 &= 48 - 2 \cdot 18 \\ 18 &= 162 - 3 \cdot 48 \\ 48 &= 372 - 2 \cdot 162 \end{aligned}$$

Assim segue que $6 = 18 - 1 \cdot (48 - 2 \cdot 18) = 3 \cdot 18 - 48 = 3 \cdot (162 - 3 \cdot 48) - 48 = 3 \cdot 162 - 10 \cdot 48 = 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) = 23 \cdot 162 - 10 \cdot 372$

Escrevemos o 6 como a diferença de dois múltiplos de 162 e 372

$$(372, 162) = 6$$

Exemplo 1.1.9. Uma sala retangular 18 metros $\times$ 12 metros possui pisos em forma quadrada que não serão colocados se não for inteiro. Qual a menor quantidade de pisos que poderão ser utilizados com pisos idênticos?

Solução. Se $18 = 2^1 \times 3^2$ e $1^2 = 2^2 \times 31$ logo $(18, 12) = 2^1 \times 3^1$.

Como o piso quadrado terá 6 metros de lado, a quantidade de piso será de 6 pisos com 36 m^2 de área.

Exemplo 1.1.10. Para levar os alunos de duas escolas a uma aula prática um professor em comum resolveu separar os grupos em quantidade igual e maior possível. Cada grupo

possui um único professor responsável. Se na primeira escola tem 1350 alunos e na próxima 1224 alunos, Qual o número de professores para acompanhar esse grupo?

Solução. $1350 = 2^1 \times 3^3 \times 5^2$ e $1224 = 2^3 \times 3^2 \times 17$ $(1350, 1224) = 2^1 \times 3^2 = 18$. O número de alunos por grupo é de exatamente 18.

Como $1350 = 18 \times 75$ e $1224 = 18t \times 68$, o número de professores será de $75 + 68 = 143$

MMC- Dados dois números naturais a e b, diremos que $[a, b]$ é o menor múltiplo comum entre eles. Em qualquer caso ab é um múltiplo comum de a e b. Se $m = [a, b]$ é o menor múltiplo comum então:

i) m é múltiplo comum de a e b.

ii) se c é um múltiplo comum de a e b então $m|c$.

Exemplo 1.1.11. Uma árvore de natal tem lâmpadas de duas cores verdes e vermelhas. As lâmpadas de cor verde pisca 5 vezes por minuto e as lâmpadas de cor vermelha pisca 4 vezes por minuto. Se as lâmpadas forem ligadas juntas, em uma hora quantas vezes as lâmpadas piscarão juntas?

Solução. Sendo 5 vezes por minuto, a cada 12 segundos as lâmpadas de cor verde voltam a piscar. Sendo 4 vezes por minuto, a cada 15 segundos as lâmpadas de cor vermelha voltam a piscar. Se $12 = 2^2 \times 3^1$ e $15 = 3^1 \times 5^1$ $[12, 15] = 2^2 \times 3^1 \times 5^1 = 60$. A primeira vez que elas piscam juntas é após 60 segundos. Como 1 hora = 60 minutos = 360 segundos, as lâmpadas piscarão juntas 60 vezes.

Exemplo 1.1.12. Três automóveis disputam uma corrida em uma pista circular. O $1^{\underline{o}}$ a sair dá uma volta em 3 minutos, o $2^{\underline{o}}$ a sair dá uma volta em 5 minutos e o $3^{\underline{o}}$ a sair dá uma volta em 11 minutos. Se saírem juntos, qual o tempo após a saída que passam os três juntos na linha de saída pela primeira vez?

Solução. O valor $[3, 5, 11] = 3 \times 5 \times 11 = 165$, ou seja, após 165 minutos passarão pela primeira vez juntos.

1.1.4 Congruência Lineares

A Congruência é uma das noções mais usadas na aritmética, introduzida por Gauss no seu livro *Disquisitiones Arithmeticae*, de 1801, trata-se de uma aritmética com

os restos da divisão euclidiana por um número fixado e compatível com as operações de adição, subtração, multiplicação e divisão muito utilizadas em exercícios contextualizados, que o objetivo principal do minicurso. Nesta unidade apresentamos exemplos de problemas que envolvem alguns tópicos utilizado pelos alunos do ensino médio como Geometria, Sequência, Progressão Aritmética, Progressão Geométrica entre outros.

Seja m um número natural não nulo, diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m. Escrito assim: $a \equiv b \mod m$.

$$23 \equiv 3(\mod 5) \text{ ou seja } 23 = 5 \cdot x + 3$$

Observação. Quando a relação $a \equiv b(\mod m)$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m.

i) Dois números são côngruos módulo m quando diferem de um múltiplo m.

ii) Se dois números são côngruos módulo m, eles deixam o mesmo resto na divisão por m.

iii) $a \equiv a \mod m$.

iv) $a \equiv b \mod m$ e $b \equiv c \mod m$ então $a \equiv c \mod m$.

v) $a \equiv b \mod m$ então $a + c \equiv b + c \mod m$.

vi) $a \equiv b \mod m$ e $c \equiv d \mod m$ então $a + c \equiv b + d \mod m$.

vii) $a \equiv b \mod m$ então $a \cdot c \equiv b \cdot c \mod m$.

viii) $a \equiv b \mod m$ e $c \equiv d \mod m$ então $a \cdot c \equiv b \cdot d \mod m$.

ix) $a \equiv b \mod m$ então $a^n \equiv b^n \mod m$.

x) $a \equiv b \mod m$,se e somente se, $a = m \cdot k + b$ para k inteiro.

Exemplo 1.1.13. O dia 01 de janeiro de 2014 foi quarta-feira, Qual dia da semana será no próximo $1^{\underline{o}}$ de janeiro?

Solução. Como há 365 dias no ano de 2014, $365 \equiv 1(\mod 7)$ o próximo dia 1° será na quinta-feira.

Exemplo 1.1.14. O dia 01 de janeiro de 2016 foi sexta-feira, Qual dia da semana será no próximo $1^{\underline{o}}$ de janeiro?

Solução. Como há 366 dias no ano de 2016, $366 \equiv 2(\mod 7)$ o próximo dia 1° será na domingo.

Exemplo 1.1.15. (FUVEST) O ano de 2007 começa na segunda-feira. Qual o próximo ano começará em uma segunda-feira?

$a)$ 2012 $b)$ 2011 $c)$ 2014 $d)$ 2018 $e)$ 2024

Solução. Temos um casa de congruência no módulo 7. Vamos construir a tabela da primeira semana do ano de 2007.

Segunda	Terça	Quarta	Quinta	Sexta	Sábado	Domingo
1	2	3	4	5	6	7

Tabela 1.2: Primeira Semana do Ano de 2007

Observe que $365 \equiv 1 \mod 7$ ou seja um ano não bissexto o último dia do ano é o mesmo dia do início do próximo ano, com isso o próximo ano se inicia um dia após o ano anterior se iniciou.

Com isso no ano bissexto $366 \equiv 2 \mod 7$ ou seja uma ano bissexto o último dia do ano é um dia a mais que o dia do início do próximo ano, com isso o próximo ano se inicia dois dias após o ano anterior se iniciou. Chamamos de Y um número divisível por 4, ou seja, anos bissextos e X um número X que deixa resto 1 quando dividido por 4.

Ano	Congruência	Primeiro dia	Início do próximo ano
2007	$x \equiv 1 \mod 7$	segunda-feira	terça-feira
2008	$y \equiv 2 \mod 7$	terça-feira	quinta-feira
2009	$x \equiv 1 \mod 7$	quinta-feira	sexta-feira
2010	$x \equiv 1 \mod 7$	sexta-feira	sábado
2011	$x \equiv 1 \mod 7$	sábado	domingo
2012	$y \equiv 2 \mod 7$	domingo	terça-feira
2013	$x \equiv 1 \mod 7$	terça-feira	quarta-feira
2014	$x \equiv 1 \mod 7$	quarta-feira	quinta-feira
2015	$x \equiv 1 \mod 7$	quinta-feira	sexta-feira
2016	$y \equiv 2 \mod 7$	sexta-feira	domingo
2017	$x \equiv 1 \mod 7$	domingo	segunda-feira

Tabela 1.3: Primeiro dia da Semana do Ano de 2007 a 2017

Conclusão o próximo ano será 2018. Letra d.

Exemplo 1.1.16. (OBMEP- Olimpíadas de Matemática) Os pontos A, B, C, D, E, F, G e H são os fios de apoios que uma aranha usa para construir sua teia, conforme a figura. Qual fio estará o número 118?

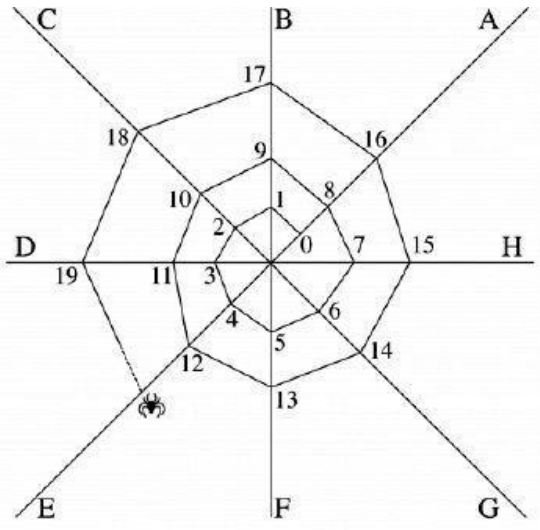

Figura 1.1: Teia da Aranha

Solução. Fio A segue $x \equiv 0 \mod 8$

Fio B segue $x \equiv 1 \mod 8$

Fio C segue $x \equiv 2 \mod 8$

Fio D segue $x \equiv 3 \mod 8$

Fio E segue $x \equiv 4 \mod 8$

Fio F segue $x \equiv 5 \mod 8$

Fio G segue $x \equiv 6 \mod 8$

Fio H segue $x \equiv 7 \mod 8$

Sendo $118 \equiv 6 \mod 8$ ou seja o fio G.

Exemplo 1.1.17. (OBMEP-2012) Cinco cartas, inicialmente dispostas como na figura serão embaralhadas. Em cada nova posição a primeira passa a ser a segunda, a segunda passa ser a quarta, a terceira passa a ser a primeira, a quarta passa ser a quinta e a quinta passa ser a terceira. Qual será a primeira carta após o 2012° posição?

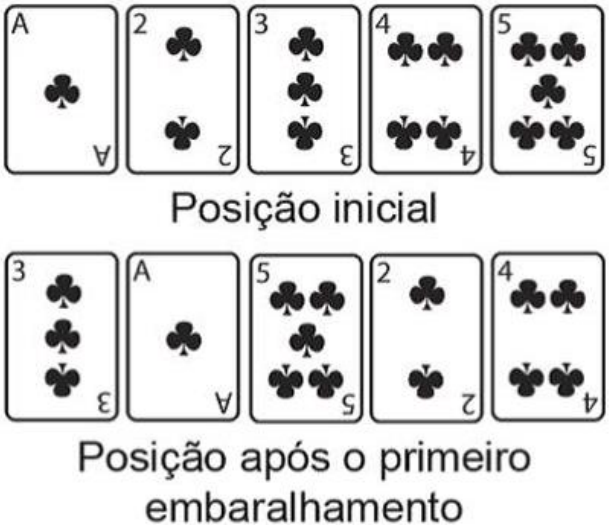

Figura 1.2: Posições das Cartas

Solução. 1° posição: A 2 3 4 5

2^{o} posição: 3 A 5 2 4

3^{o} posição: 5 3 4 A 2

4^{o} posição: 2 4 A 5 3

5^{o} posição: A 2 3 4 5

Com isso temos um caso de congruência módulo 5

$x \equiv 0 \mod 5$, a primeira carta será A

$x \equiv 1 \mod 5$, a primeira carta será 3

$x \equiv 2 \mod 5$, a primeira carta será 5

$x \equiv 3 \mod 5$, a primeira carta será 4

$x \equiv 4 \mod 5$, a primeira carta será 2

Sendo $2012 \equiv 2 \mod 5$, a primeira carta será 5 .

1.2 Sugestão de um Minicurso Sobre o Teorema Chinês do Resto

Nessa proposta de minicurso os conteúdos foram organizados em unidades para facilitar aos alunos a teoria e suas aplicações. Os minicurso foram aplicados no Colégio Maxi para alunos do 3^{o} ano do ensino médio e na Escola Estadual Liceu Cuiabano para alunos do 2^{o} ano do ensino médio.

Nos assuntos abordados no minicurso, as demonstrações dos teoremas e propriedades foram de maneira formal conforme a fundamentação teórica do capítulo posterior. A grande maioria dos alunos do Ensino Médio, para quais é direcionado o minicurso não tem pré-requisitos necessários para compreender toda essa fundamentação teórica da forma como foi apresentada. Para suprir essa dificuldade dos alunos do ensino médio colocamos alguns exemplos do cotidiano, exercícios contextualizados e exemplos numéricos para uma melhor compreensão do assunto abordado no minicurso.

Apresentamos então a proposta do minicurso apostilado e como foi trabalhado com as turmas do 2^{o} ano e do 3^{o} ano. As unidades de 01 a 04 são pré-requisitos necessários à introdução do assunto das unidades 05 a 07. A unidade 05 é o Teorema Chinês do Resto e suas aplicações em exercícios para o ensino médio. As unidades de 01 a 04 são pré-requisitos mas visto a necessidade e a falta de conhecimento de alguns alunos, se tornaram parte do minicurso e com isso alguns exercícios foram feitos para demonstração e melhor compreensão das unidades. Cada unidade contém uma lista de exercícios propostos ao final de cada unidade. (Anexo)

Capítulo 2

Fundamentação Teórica

2.1 Divisibilidade

Dados dois números a e b com a não nulo, diremos que a divide b, escrevendo $a|b$, quando existir c natural tal que $b = a \times c$. Neste caso, diremos que a é um divisor ou fator de b ou, ainda que b é um múltiplo de a.

Observe que $a|b$, não representa nenhuma operação nos naturais, nem representa uma fração. Trata de uma sentença que diz ser verdade que existe c tal que $b = ac$.

Seja b um inteiro não nulo. Se b dividir a, dizemos que b é um divisor de a, que a é divisível por p ou ainda que a é um múltiplo de b. se $b|a$ e $b \geq 1$, então b é um divisor positivo de a. Note que todo inteiro não nulo é um divisor de si mesmo e de 0.

Propriedades 2.1.1. Dados a, b inteiros e k natural, temos que:

a) Se $a \neq b$ então $(a - b)|(a^k - b^k)$.

b) Se $a \neq -b$ e k for ímpar, então $(a + b)|(a^k + b^k)$.

Propriedades 2.1.2. Sejam a, b, c inteiros não nulos e x, y inteiros quaisquer.

a) Se $b|a$ e $a|b$, então $a = b$ ou $a = -b$.

b) Se $c|b$ e $b|a$, então $c|a$.

c) Se $c|a$ e $c|b$, então $c|(ax + by)$.

d) Se $c|b$ e $c|ab$, então $c|a$.

e) Se $b|a$ então $bc|ac$.

f) Se $b|a$ então $|b| \leq |a|$.

Propriedades 2.1.3. Dados inteiros a_1, a_2, b sendo b não nulo, temos que $b|(a_1, a_2)$ se e só se a_1 e a_2 deixam restos iguais na divisão por b.

2.2 Divisão Euclidiana

Mesmo quando um número natural a não divide o número natural b, Euclides no livro Elementos, utiliza, sem enuncia-lo explicitamente, o fato de que é sempre possível efetuar a divisão de b por a, com resto. Este resultado, não só é um importante instrumento na obra de Euclides, como também é um resultado central da teoria.

Sejam a e b dois números naturais $0 \leq a \leq b$. Existem dois únicos números naturais q e r tais que $b = aq + r$, com $r \leq a$.

2.3 Máximo Divisor Comum (MDC)

O MDC dos inteiros não nulos a_1, a_2, a_3, $\cdot$, a_n denotado $\text{mdc}(a_1, a_2, a_3, \cdots, a_n)$ é o maior dentre os divisores comuns de $a_1, a_2, a_3, \cdots, a_n$ Os inteiros a_1, a_2, a_3, $\cdots$, a_n são primos entre si ou relativamente primos se $\text{mdc}(a_1, a_2, a_3, \cdots, a_n) = 1$

Diremos que d é um máximo divisor comum (mdc) de a e b se possuir as seguintes propriedades:

a) d é um divisor comum de a e de b, e

b) d é divisível por todo divisor comum de a e b. Portanto, se d é um mdc de a e b, c é um divisor comum desses números, então $c \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números. Em particular, isto nos mostra que se d e f são dois mdc de um mesmo par de números, $d \leq f$ e $f \leq d$, e, consequentemente $d = f$. Ou seja, o mdc de dois números, quando existe, é único.

c) Como o mdc de a e b não depende da ordem em que a e b são tomados, temos que: $(a, b) = (b, a)$ Em alguns casos particulares, é fácil verificar a existência do mdc. Por

exemplo, se a e b são números naturais, tem-se claramente que (0,a) = a, (1,a) = 1 e que (a,a) = a

d) Sejam a, b e n naturais com $a \leq na \leq b$. Se existe $(a, b - na)$ então (a, b) existe, e $(a, b) = (a, b - na)$,

e) Sejam a e b naturais. Definimos o conjunto $J(a, b) = \{x$ natural não nulo: existe u e v natural onde $x = ua - vb\}$ e $J(b, a) = \{y$ natural não nulo: existe v e u natural onde $y = vb - ua\}$ e $J(a, b) = J(b, a)$

f) Sejam a e b natural não nulo e seja $d = min\{J(a, b)\}$. Tem-se que:

$$-d \text{ é o mdc de } a \text{ e } b \qquad -J(a, b) = \{nd : n \text{ natural}\}$$

g) Quaisquer que sejam a, b e n naturais não nulos, $(na, nb) = n(a, b)$

h) Dois números naturais a e b são primos entre si, ou coprimos, se $(a, b) = 1$; ou números naturais n e m tais que $na - mb = 1$

i) Sejam a, b e c números naturais. Se $a|bc$ e $(a, b) = 1$ então $a|c$

j) Dados números naturais a_1, a_2, a_3, $\cdots$, an existe o seu mdc e $(a_1, a_2, a_3, \cdots, an) = (a_1, a_2, a_3, \cdots, ak, \cdots, (an - 1, an))$.

2.4 Mínimo Múltiplo Comum (MMC)

Diremos que um número é um múltiplo comum de dois números naturais dados se ele é simultaneamente múltiplo de ambos os números. Nomenclatura de MMC de a e b é denominada $[a, b]$.

Em qualquer caso, o número ab é sempre um múltiplo comum de a e b.

Diremos que um número m é um mínimo múltiplo comum (mmc) de a e b se possuir as seguintes propriedades:

a) m é um múltiplo comum de a e b, e

b) se c é um múltiplo comum de a e b, então $m|c$.

c) Dados dois números naturais a e b, temos $[a, b]$ existe, ou seja o MMC existe e $[a, b](a, b) = ab$

d) Se a e b são números naturais primos entre si, então $[a, b] = ab$.

2.5 Números Primos

Teorema Fundamental da Aritmética- Um número maior do que 1 e que só é divisível por 1 e por si próprio é chamado de número primo. Dados dois números primos p e q e um número natural a qualquer, decorrem da definição acima os seguintes fatos:

a) Se $p|q$, então $p = q$

b) Se $p|q$, então $(p, q) = 1$

c) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

d) Se um inteiro $n \geq 2$ for composto, então existe um divisor primo p de n tal que $p \leq \sqrt{n}$.

Conjuntos dos números primos $\{2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots\}$

e) O conjunto dos números primos é infinito

2.6 Congruência Linear

Introduzida por Gauss no seu livro Disquisitiones Arithmeticae, de 1801, trata-se de uma aritmética com os restos da divisão euclidiana por um número fixado.

2.7 Aritmética dos RESTOS

Seja m um número um número natural diferente de zero. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m, são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se $a \equiv b \mod m$

Exemplo 2.7.1. $21 \equiv 13 \mod 2$, já que os restos de 21 e 13 por 2 são iguais a 1.

Como o resto da divisão de um número natural qualquer por 1 é sempre nulo, temos que $a \equiv b \mod 1$, quaisquer que sejam a e b natural. Isto torna desinteressante a aritmética dos restos módulo 1.

A relação de Congruência é muito importante para solucionar alguns problemas com resto das divisões naturais.

Definição 2.7.1. Sejam a, b, e n inteiros dados, sendo $n \geq 2$, dizemos que a é congruente a b, módulo n, e denotamos $a \equiv b(\mod n)$, se $n|(a-b)$

Exemplo 2.7.2. $3 \equiv 5(\mod 2)$, $-1 \equiv 11(\mod 12)$, $2 \equiv -1(\mod 3)$

Propriedades 2.7.1. a) $a \equiv a(\mod m)$

b) Se $a \equiv b(\mod m)$ então $b \equiv a(\mod m)$

c) Se $a \equiv b(\mod m)$ e $b \equiv c(\mod m)$, então $a \equiv c(\mod m)$

d) Sendo a e b naturais e $b \geq a$. Tem-se que a $a \equiv b(\mod m)$, se, e somente se, $m|b-a$

e) Se $a \equiv b(\mod m)$ e $c \equiv d(\mod m)$, então $a+c \equiv b+d(\mod m)$

f) Se $a \equiv b(\mod m)$ e $c \equiv d(\mod m)$, então $ac \equiv bd(\mod m)$

g) Se $a \equiv b(\mod m)$ então $(a,m) = (b,m)$

Exemplo 2.7.3. Vamos achar o menor múltiplo de 7 que deixa resto 1 quando dividido por 2, 3, 4, 5 e 6. Portanto, queremos achar a menor solução do seguinte sistema de congruências :

$$7x \equiv 1 \mod 2, \quad \mod 3, \quad \mod 4, \quad \mod 5 \text{ e } \quad \mod 6.$$

Solução. $7x \equiv 1(\mod [2,3,4,5,6])$, logo devemos resolver $7x \equiv 1(\mod 60)$. Isto se traduz como $60|7x-1$, o que equivale a resolver $7x - 60y = 1$.

$$\begin{aligned} 60 &= 7 \cdot 8 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 1 &= (p60 - 17)7 - (p7 - 2)60 \end{aligned}$$

e portanto $x = p60 - 17$ e $y = p7 - 2$.

Tomando $p = 1$, temos $x = 43$ e $y = 5$ é a solução minimal, segue então que o número procurado é $7 \cdot 43 = 301$.

2.8 Classes Residuais

Nesta unidade, introduzimos o conceito de classe residual módulo m e apresentado pelo conjunto $\mathbb{Z}_m$ formado por todas essas classes. Para introduzir o conceito de classes residuais, utilizamos a tabela utilizada abaixo:

A	0	6	12	18	24	30	36	42	48
B	1	7	13	19	25	31	37	43	49
C	2	8	14	20	26	32	38	44	50
D	3	9	15	21	27	33	39	45	51
E	4	10	16	22	28	34	40	46	52
F	5	11	17	23	29	35	41	47	53

Tabela 2.1: Classes Residuais

Sendo adição temos

$B \equiv 1 \mod 6$, $C \equiv 2 \mod 6$ e assim $B + C \equiv 1 + 2 \mod 6$, ou seja, $B + C \equiv 3 \mod 6$

$D \equiv 3 \mod 6$.

Sendo multiplicação temos

$D \equiv 3 \mod 6$, $C \equiv 2 \mod 6$ e assim $D \cdot C \equiv 3 \cdot 2 \mod 6$, ou seja, $D \cdot C \equiv 6 \mod 6$

$A \equiv 0 \mod 6$

Observe que a tabela apresenta o conjunto dos números naturais divididos em seis subconjuntos, ou seja, cada linha contém elementos que apresentam a mesma propriedade em relação a divisão euclidiana pelo número 6, a saber:

Na linha A: temos o subconjunto formados pelos números que divididos por 6 deixam restos 0, ou seja, $A = \{ x \in \mathbb{N} : x \equiv 0 \mod 6\}$

Na linha B: temos o subconjunto formados pelos números que divididos por 6 deixam restos 0, ou seja, $B = \{ x \in \mathbb{N} : x \equiv 1 \mod 6\}$

Na linha C: temos o subconjunto formados pelos números que divididos por 6 deixam restos 0, ou seja, $C = \{ x \in \mathbb{N} : x \equiv 2 \mod 6\}$

Na linha D: temos o subconjunto formados pelos números que divididos por 6 deixam restos 0, ou seja, $D = \{ x \in \mathbb{N} : x \equiv 3 \mod 6\}$

Na linha E: temos o subconjunto formados pelos números que divididos por 6 deixam restos 0, ou seja, $E = \{ x \in \mathbb{N} : x \equiv 4 \mod 6\}$

Na linha F: temos o subconjunto formados pelos números que divididos por 6 deixam restos 0, ou seja, $F = \{ x \in \mathbb{N} : x \equiv 5 \mod 6\}$

Verificamos também, através das propriedades das congruências modulares, que somando, por exemplo, qualquer elemento do subconjunto B com qualquer elemento do subconjunto E, obteremos um elemento do subconjunto F, ou, em outro exemplo, se multiplicarmos qualquer elemento do subconjunto C por um elemento do subconjunto F obteremos sempre um elemento do subconjunto E.

Da mesma forma, veremos a seguir que o conjunto dos números inteiros também pode ser repartido em m subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m e que o conjunto dos números inteiros, assim subdivididos e munidos das operações de adição e multiplicação com algumas de suas propriedades, permitem definir novas aritméticas que encontram inúmeras aplicações em várias partes da matemática e que servem de base para quase todos os procedimentos de cálculo, possuindo muitas aplicações tecnológicas.

Então, fixado um número inteiro $m > 1$, podemos repartir o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números

inteiros que possuem o mesmo resto quando divididos por m; isto nos dá a seguinte partição de $\mathbb{Z}$:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \mod m\} \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \mod m\} \\
&\vdots \\
[m-1] &= \{x \in \mathbb{Z} : x \equiv m-1 \mod m\}
\end{aligned}$$

Observe que $[m] = [0]$, pois $m \equiv 0 \mod m$. Desta forma, podemos obter apenas m subconjuntos distintos da maneira como foi definida acima.

O conjunto $[a] = \{x \in \mathbb{Z} : x \equiv a \mod m\}$ é chamado de classe residual módulo m do elemento a de $\mathbb{Z}$. O conjunto de todas as classes residuais de módulo m será representado por $\mathbb{Z}_m$, ou seja:

$$\mathbb{Z}_m = \{[0]; [1]; [2]; \cdots [m-1]\}$$

Exemplo 2.8.1. Seja $m = 2$. Então:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \mod 2\} \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \mod 2\}
\end{aligned}$$

Logo $\mathbb{Z}_2 = \{[0], [1]\}$.

Neste caso, dizemos que qualquer número par é um representante da classe residual [0] e qualquer número ímpar é representante da classe residual [1].

Exemplo 2.8.2. Seja $m = 3$. Então:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \mod 3\} \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \mod 3\} \\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \mod 3\}
\end{aligned}$$

Logo $\mathbb{Z}_3 = \{[0], [1], [2]\}$

Neste caso, dizemos que qualquer múltiplo de 3 é representante da classe residual [0], enquanto que $1, 4, 7, 10, \cdots$ são representantes da classe residual [1] e $2, 5, 8, \cdots$ são representantes da classe residual [2].

Na tabela apresentada no exemplo inicial, temos:

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

Após definir o anel das classes residuais da forma como foi apresentada na fundamentação teórica, as tabelas de adição e multiplicação em $\mathbb{Z}_2 = \{[0], [1]\}$, $\mathbb{Z}_3 = \{[0], [1], [2]\}$ e $\mathbb{Z}_4 = \{[0], [1], [1], [3]\}$ ficaram da seguinte forma:

$+$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$\times$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Tabela 2.2: Adição e Multiplicação em $\mathbb{Z}_2$

$+$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\times$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Tabela 2.3: Adição e Multiplicação em $\mathbb{Z}_3$

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Tabela 2.4: Adição e Multiplicação em $\mathbb{Z}_4$

Neste ponto, solicitamos aos alunos que elaborem as tabelas de adição e multiplicaçao em $\mathbb{Z}_5$ e $\mathbb{Z}_6$ e respondam as seguintes perguntas:

a) Identifiue nas tabelas de multiplicação em $\mathbb{Z}_2$, $\mathbb{Z}_3$, Z_4, $\mathbb{Z}_5$ e $\mathbb{Z}_6$; os pares de elementos $[a]$ e $[b]$ de cada conjunto, onde $[a] \cdot [b] = [1]$.

   O objetivo deste item é apresentar a definição do elemento invertível, ou seja: Um elemento $[a] \in \mathbb{Z}_m$ é invertível, se existir $[b] \in \mathbb{Z}_m$ tal que $[a] \cdot [b] = [1]$.

b) Em quais desses conjuntos, todo elemento distinto de [0] é invertível?

   O aluno deve perceber, por exemplo, que em $\mathbb{Z}_4$, [0] e [2] não são invertíveis e que $(4, 0) = 4$ e $(4, 2) = 2$. Já [1] e [3] são invertíveis em $\mathbb{Z}_4$ e que $(4, 1) = (4, 3) = 1$. Deve notar também que em $\mathbb{Z}_5$, todo elemento distinto de [0] é invertível, que $(5, 1) = (5, 2) = (5, 3) = (5, 4) = (5, 5) = 1$ e que isto também ocorre em Z_2 e Z_3.

   O objetivo desse item é levar o aluno a concluir que $[a] \in \mathbb{Z}_m$ invertível se, e somente se, $(a, m) = 1$ e que $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$ são chamados de corpos, ou seja, são anéis onde todo elemento não nulo possui um inverso multiplicativo.

O aluno deve notar também que 2, 3 e 5 são primos e chegar à conclusão que $\mathbb{Z}_m$ é um corpo, se e somente se, m é primo.

Uma vantagem das classes residuais é transformar a congruência $a \equiv b \mod m$ na igualdade $[a] = [b]$. Dessa forma, elas permitem resolver congruências lineares do tipo $ax \equiv b(\mod m)$, reduzindo-as, em $[a] \in \mathbb{Z}_m$, à seguinte equação:

$$[a] \cdot z = [b]$$

Podemos notar a importância de determinar o elemento invertível no exemplo abaixo:

Exemplo 2.8.3. N é um múltiplo de 4 que possui três algarismos. Dividindo N por 5 encontramos resto igual a 3. Determine o menor valor de N. Observe que $N = 4 \cdot x$. Dessa forma devemos ter:

Resolver essa congruência equivale a resolver em $\mathbb{Z}_5$ a seguinte equação:

$$[4] \cdot z = [3]$$

Observe que $[4]$ é invertível em $\mathbb{Z}_5$, pois $[4] \cdot [4] = [1]$. Logo, basta multiplicar ambos os membros da equação por $[4]$ e obtemos:

$$[4] \cdot [4] \cdot z = [4] \cdot [3] \Rightarrow [1] \cdot z = [2] \Rightarrow z = [2]$$

Em $\mathbb{Z}_5$, $[2]$ é o conjunto dos números inteiros que divididos por 5 deixam resto 2, ou seja: $X = 5 \cdot t + 2$

Como $N \geq 100 \Rightarrow 4 \cdot x \geq 100 \Rightarrow x \geq 25 \Rightarrow 5t + 2 \geq 25 \Rightarrow t \geq 4,6 \Rightarrow t = 5$. Assim:

$$x = 5.5 + 2 \Rightarrow x = 27. \text{ Logo: } N = 4.27 \Rightarrow N = 108$$

Capítulo 3

Teorema Chinês do Resto

Observação 3.1. Sejam a_1, a_2, a_3, ..., a_r, $c \in \mathbb{Z}$. Temos a seguinte propriedade :

1. Se $a_1|c$, $a_2|c$, ..., $a_r|c$, então $m = mmc(a_1, a_2, \ldots, a_r)|c$.

Proposição 3.2. Se $a \equiv b(\mod m_1)$, $a \equiv b(\mod m_2)$, ..., $a \equiv b(\mod m_k)$ com a, b inteiros e m_1, m_2, ..., m_k inteiros positivos, então $a \equiv b(\mod mmc(m_1, m_2, \ldots, m_k))$.

Demonstração. Por hipótese $m_1|(a-b)$, $m_2|(a-b)$, ..., $m_k|(a-b)$ pela observação 3.1 temos $mmc(m_1, m_2, \ldots, m_k)|(a-b)$, consequentemente $a \equiv b(\mod mmc(m_1, m_2, \ldots, m_k))$. □

Corolário 3.3. Se $a \equiv b(\mod m_1)$, $a \equiv b(\mod m_2)$, ..., $a \equiv b(\mod m_k)$ com a, b inteiros e m_1, m_2, ..., m_k inteiros positivos tais que $mdc(m_i, m_j) = 1$ para todo $i \neq j$, então $a \equiv b(\mod (m_1 \cdot m_2 \cdot \ldots \cdot m_k))$.

Demonstração. Como $mdc(m_i, m_j) = 1$ para todo $i \neq j$, pela observação 3.1 temos

$$mmc(m_1, m_2, \ldots, m_k) = m_1 \cdot m_2 \cdot \ldots \cdot m_k$$

Pela proposição 3.2 segue que $a \equiv b(\mod (m_1 \cdot m_2 \cdot \ldots \cdot m_k))$.

Teorema 3.4. (Teorema Chinês dos Restos): Sejam $m_1, m_2, \ldots, m_k$ inteiros positivos tais que $mdc(m_i, m_j) = 1$, sempre que $i \neq j$ e a_1, a_2, a_3, $\cdots$, a_k inteiros. Então o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \vdots \\ x \equiv a_k \mod m_k \end{cases}$$

tem solução que é única módulo $m = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot, m_k$.

Demonstração. Nosso objetivo é construir uma solução simultanea para o sistema de congruências. Consideremos o conjunto de r números $M_k = \left(\frac{m}{m_k}\right) = m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_{k-1} \cdot m_{k+1} \cdot \ldots \cdot m_r$. para $k = 1, 2, 3, \ldots, r$. Como o $d = mdc(m_i, m_j) = 1$ para $i \neq j$ temos

$$\begin{aligned} mdc(m_1, m_k) &= mdc(m_2, m_k) = \ldots = mdc(m_{k-1}, m_k) \\ &= mdc(m_{k+1}, m_k) = \ldots = mdc(m_r, m_k) \\ &= 1 \end{aligned}$$

o que implica

$$mdc(m_1 \cdot m_2 \cdot \ldots \cdot m_{k-1} \cdot m_{k+1} \cdot \ldots \cdot m_r, m_k) = mdc(M_k, m_k) = 1$$

logo existem inteiros u, v tais que $u \cdot M_k + v \cdot m_k = 1$, o que significa que existe $u = s_k$ tal que

$$s_k \cdot M_k \equiv 1(\mod m_k)$$

Como $\text{mdc}(M_k, m_k) = 1|1$ segue que $s_k \cdot M_k \equiv 1(\mod m_k)$ tem solução única y_k, ou seja,

$$M_k \cdot y_k \equiv 1(\mod m_k)$$

Então

$$a_k \cdot M_k \cdot y_k \equiv a_k(\mod m_k)$$

Uma vez que $m_k|M_j$ quando $j \neq k$, temos $M_j \equiv 0(\mod m_k)$; então $a_j \cdot M_j \cdot y_j \equiv 0(\mod m_k)$ para todos os termos, exceto o k-ésimo. Portanto $x = a_k \cdot M_k \cdot y_k \equiv a_k(\mod m_k)$, para $k = 1, 2, 3, \ldots, r$ é uma solução do sistema de r congruências, ou seja,

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots + a_r \cdot M_r \cdot y_r \equiv a_k(\mod m_k)$$

Agora mostraremos que quaisquer duas soluções do sistema de r congruências são congruentes módulo m. Sejam x_0 e x_1 soluções do sistema. Então para cada k, segue que $x_0 \equiv x_1 \equiv a_k(\mod m_k)$ isto implica que $m_k|(x_0 - x_1)$. Mas $x_0 \equiv x_1(\mod m_1)$, $x_0 \equiv x_1(\mod m_2)$, ..., $x_0 \equiv x_1(\mod m_k)$, então pelo corolário 3.3 segue que

$$x_0 \equiv x_1(\mod mmc(m_1, m_2, \ldots, m_k))$$

Como $d = mdc(m_i, m_j) = 1$ sempre que $i \neq j$ temos que

$$mmc(m_1, m, \ldots, m_k) = m_1 \cdot m_2 \cdot m_2 \cdot \ldots \cdot m_k = m$$

logo $m|(x_0 - x_1)$, ou seja, $x_0 \equiv x_1(\mod m)$, o que significa que as soluções são únicas módulo m.

Exemplo 1. Resolva o sistema

$$\begin{cases} x \equiv 1(\mod 3) \\ x \equiv 2(\mod 5) \\ x \equiv 3(\mod 7) \end{cases}$$

Solução. Note que $m = 3 \cdot 5 \cdot 7 = 105$ e

$$\begin{cases} M_1 = \frac{105}{3} = 35 \\ M_2 = \frac{105}{5} = 21 \\ M_3 = \frac{105}{7} = 15 \end{cases} ; \begin{cases} M_1 y_1 \equiv 1(\mod 3) \\ M_2 y_2 \equiv 1(\mod 5) \\ M_3 y_3 \equiv 1(\mod 7) \end{cases} ; \begin{cases} 35 y_1 \equiv 1(\mod 3) \\ 21 y_2 \equiv 1(\mod 5) \\ 15 y_3 \equiv 1(\mod 7) \end{cases}$$

$$\begin{cases} 2 y_1 \equiv 1(\mod 3) \\ y_2 \equiv 1(\mod 5) \\ y_3 \equiv 1(\mod 7) \end{cases} ; \begin{cases} y_1 \equiv 2(\mod 3) \\ y_2 \equiv 1(\mod 5) \\ y_3 \equiv 1(\mod 7) \end{cases}$$

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157 \equiv 52(\mod 105)$$

Exemplo 2. Resolva a equação $17 \cdot x \equiv 9(\mod 276)$.

Solução. Note que $276 = 2^2 \cdot 3 \cdot 23 = 3 \cdot 4 \cdot 23$.

$$\begin{cases} 17x \equiv 9(\mod 3) \\ 17x \equiv 9(\mod 4) \\ 17x \equiv 9(\mod 23) \end{cases} ; \begin{cases} 2x \equiv 0(\mod 3) \\ x \equiv 1(\mod 4) \\ 17x \equiv 9(\mod 23) \end{cases}$$

Como $d = mdc(17, 23) = 1$ a congruência $17x \equiv 9(\mod 23)$ tem uma única solução que pode ser obtida escrevendo $d = mdc(17, 23) = 1 = -4(17) + 3(23)$, ou seja, $-4(17) \equiv 1(\mod 23) \Rightarrow -36(17) \equiv 9(\mod 23)$, finalmente temos $10(17) \equiv 9(\mod 23)$.Então basta resolver o sisema de congruências

$$\begin{cases} x \equiv 0(\mod 3) \\ x \equiv 1(\mod 4) \\ x \equiv 10(\mod 23) \end{cases} ; \begin{cases} M_1 = \frac{276}{3} = 92 \\ M_2 = \frac{276}{4} = 69 \\ M_3 = \frac{276}{23} = 12 \end{cases} ; \begin{cases} M_1 y_1 \equiv 1(\mod 3) \\ M_2 y_2 \equiv 1(\mod 4) \\ M_3 y_3 \equiv 1(\mod 23) \end{cases}$$

$$\begin{cases} 92y_1 \equiv 1(\mod 3) \\ 69y_2 \equiv 1(\mod 4) \\ 12y_3 \equiv 1(\mod 23) \end{cases} ; \begin{cases} 2y_1 \equiv 1(\mod 3) \\ y_2 \equiv 1(\mod 4) \\ 12y_3 \equiv 1(\mod 23) \end{cases} ; \begin{cases} y_1 \equiv 2(\mod 3) \\ y_2 \equiv 1(\mod 4) \\ y_3 \equiv 2(\mod 23) \end{cases}$$

Portanto,

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 = 0 \cdot 92 \cdot 2 + 1 \cdot 69 \cdot 1 + 10 \cdot 12 \cdot 2 = 309 \equiv 23(\mod 276)$$

3.1 O Teorema Chinês dos Restos e suas Aplicações

3.1.1 Problema sobre Satélite

Três satélites passarão sobre o Rio de Janeiro à noite. O primeiro a 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra; o segundo, 15 horas e, o terceiro, 19 horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio de Janeiro.

Matematicamente formulando o problema: será chamado de x o número de horas, a partir da meia-noite. Sabe-se que o primeiro passa a cada 13 horas, a contar da 1 da 16 madrugada, representado por $x = 1 + 13t$, para algum inteiro t, equivalente a dizer $x \equiv 1($ mod 13). Aplicando para os outros satélites: $x \equiv 4(\mod 15)$ e $x \equiv 8(\mod 19)$.

Para saber qual o horário exato de passagem dos três satélites, deve ser encontrado o valor de x que satisfaça as três equações simultaneamente.

$$x \equiv 1(\mod 13)$$
$$x \equiv 4(\mod 15)$$
$$x \equiv 8(\mod 19)$$

Observando as equações não se pode adicionar nem subtrair, pois os módulos são diferentes, então a equação de congruência deve ser convertida em identidade de inteiros.

$x \equiv 1(\mod 13)$, isto é, $x-1 = 13t$, logo $x = 1+13t$, se substituir o x na segunda equação de congruência, tem-se:

$$\begin{aligned} x &\equiv 4(\mod 15) \\ 1 + 13t &\equiv 4(mod 15) \\ 13t \equiv 3(\mod 15) &\rightarrow \text{ em } \mathbb{Z}_{15} \text{ os } I = 2, 4, 7, 11, 13 \end{aligned}$$

Resolvendo através do inversível:

$$\begin{aligned} 13x &\equiv 1(\mod 15) \\ 13 \cdot 7 &\equiv 1(\mod 15) \\ 91 : 15 = 6 \cdot 15 + 1 &(\text{ este é o resto}) \end{aligned}$$

Substituído este resultado:

$$\begin{aligned} 13 \cdot 7 \cdot t &\equiv 3 \cdot 7(\mod 15) \\ t &\equiv 21(\mod 15) \\ t &\equiv 21 \equiv 6(\mod 15) \\ t \equiv 6(\mod 15), &\text{ donde } t - 6 = 15u \\ t &= 15u + 6 \end{aligned}$$

Então substituindo em $x = 1 + 13t$.

$$\begin{aligned} x &= 1 + 13(15u + 6) \\ x &= 1 + 78 + 195u \\ x &= 79 + 195u \end{aligned}$$

Com este resultado, substitui-se na equação $x \equiv 8(\mod 19)$, assim:

$$79 + 195u \equiv 8(\mod 19)$$
$$195u \equiv -71(\mod 19)$$
$$195 \equiv 5(\mod 19) \rightarrow 190|19$$
$$-71 \equiv 5(\mod 19) \rightarrow -76|19$$

Ou seja:

$$5u \equiv 5(\mod 19) \rightarrow em\mathbb{Z}_{19} \Rightarrow 5x \equiv 1(\mod 19)$$
$$5 \cdot 4 \equiv 1(\mod 19)$$
$$20 : 19 = 19.1 + 1$$

Logo $(5.4)u \equiv 5 \cdot 4(\mod 19)u \equiv 1(\mod 19)$.
Portanto, $u = 1 + 19v$. Substituindo na equação do x.

$$x = 79 + 195u$$
$$x = 79 + 195(1 + 19v)$$
$$x = 79 + 195 + 3705v$$
$$x = 274 + 3705v.$$

Conclui-se que a primeira hora que os 3 satélites passarão juntos sobre a cidade do Rio de Janeiro é o menor valor de x na equação acima que é 274, pois o valor do x representa o tempo contado a partir da meia-noite. Além do mais o problema acima foi resolvido em duas a duas equações como no algoritmo, representando que é concreta a resolução do Teorema Chinês do Resto.

3.1.2 Problema do Camponônês e os Ovos

Um camponês tem um certo número de ovos; quandos os divide por 3, sobra-lhe 1; quando os divide por 4, sobram 2 ovos; e quando os divide por 5, sobram 3. Quantos ovos tem o camponês? O que queremos aqui é a solução simultânea de um sistema de equações modulares

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 4 \\ x \equiv 3 \mod 5 \end{cases}$$

Começando pela primeira equação, temos que qualquer solução x do sistema tem que satisfazer

$$x = 1 + 3y$$

para algum $y \in \mathbb{Z}$; substituindo na segunda equação ficamos com

$$3y + 1 \equiv 2 \mod 4 \Leftrightarrow 3y \equiv 1 \mod 4 \Leftrightarrow y \equiv 3 \mod 4$$

e portanto $y = 3 + 4z$ e $x = 1 + 3(3 + 4z) = 10 + 12z$, onde, mais uma vez, z representa uma nova incógnita inteira; substituindo de novo na terceira equação

$$12z + 10 \equiv 3 \mod 5 \Leftrightarrow 2z \equiv 3 \mod 5 \Leftrightarrow z \equiv 4 \mod 5$$

Concluímos que $z = 4 + 5w$ e portanto a solução do nosso sistema

$$x = 10 + 12(4 + 5w) = 58 + 60w$$

A resposta pergunta é portanto que o camponês poderia ter 58 ovos ou 118 ou 178, etc.

Que a solução do sistema são fica determinada módulo 60 é evidente, uma vez que se x for solução, qualquer inteiro da forma $x + 60w$ também seria solução. Por outro lado, se x e y forem duas soluções do sistema, então $x - y$ será divisível por 3, por 4 e por 5, e como estes são primos dois a dois, $x - y$ tem que ser divisível pelo seu produto 60.

Podemos também observar que o facto de 3, 4 e 5 serem primos entre si dois a dois nos garantiu que ao substituir o valor de x na segunda e depois na terceira equação,

ficaríamos sempre com uma equação com soluções, uma vez que o coeficiente de y e depois de z é primo com o módulo da equação respectiva.

Vamos agora enunciar um resultado fundamental para a simplificação da resolução de equações modulares:

3.1.3 Aplicar o Teorema Chinês do Resto para resolver equações diofantinas lineares

$$327x \equiv 171 \mod 520;$$

Calculando $mdc(327; 520) = 1$ podemos deduzir que existe uma única solução e aplicar o método explicado mais atrás. No entanto, notando que $520 = 5 \cdot 8 \cdot 13$, passamos ao sistema

$$\begin{cases} 327x \equiv 171 \mod 5 \\ 327x \equiv 171 \mod 8 \\ 327x \equiv 171 \mod 13 \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 1 \mod 5 \\ 7x \equiv 3 \mod 8 \\ 2x \equiv 4 \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 8 \\ x \equiv 2 \mod 13 \end{cases}$$

Qualquer solução da equação inicial terá que ser também solução de cada uma das equações do sistema e reciprocamente, pelo Teorema Chinês dos Restos, qualquer solução do sistema é solução da equação inicial.

Usamos o mesmo método de solução do exemplo anterior: pela primeira equação $x = 3 + 5y$; substituindo na segunda temos

$$5y \equiv 2 \mod 8, y \equiv 2(\mod 8)$$

portanto $y = 2 + 8z$ e $x = 13 + 40z$, o que nos dá, na última equação,

$$40z \equiv 2 \mod 13, z \equiv (2 \mod 13)$$

donde se deduz finalmente que $x = 93 + 520w$

É possível demonstrar o teorema de outra forma, que nos fornece igualmente um método prático de solução: Dado o sistema no enunciado, calcula-se, para cada $1 \leq i \leq k$, um inteiro b_i tal que

$$\frac{m}{m_i} b_i \equiv 1 \mod m_i$$

Note-se que isto é possível, uma vez que $mdc\left(\frac{m}{mi}, mi\right) = 1$, ficando b_i determinado naturalmente módulo m_i.

Verificamos que x definido por

$$x = \sum_{i=1}^{k} \frac{m}{m_i} b_i a_i$$

é solução do sistema; fixemos um índice $1 \leq j \leq k$; nas parcelas do somatório com $i \neq j$ temos que $m_j | \frac{m}{m_i}$ (m_i e m_j são primos entre si) e portanto essas parcelas anulam-se módulo m_j; na parcela de índice j, devido ao modo como escolhemos b_j, temos

$$\frac{m}{m_i} b_j a_j \equiv a_j \mod m_j$$

Este método de solução torna-se mais útil quando temos que resolver não um mas vários sistemas de equações com os mesmos módulos $m_1, \cdots, m_k$, como veremos a seguir.

O próximo exemplo envolve equações modulares de grau maior que 1 para pôr em evidência as vantagens do segundo método de solução de um sistema.

3.1.4 Soluções Simultâneas de Sistema de Equaçôes

$$\begin{cases} x^2 \equiv 2 \mod 7 \\ x^3 \equiv 1 \mod 9 \\ x^4 \equiv 3 \mod 11 \end{cases}$$

Como não temos (por enquanto) nenhuma forma mais eficaz de tratar estas equações, procuramos as suas soluções directamente, calculando a^2 em que a percorre

todas as classes de congruência módulo 7, e do mesmo modo para as outras equações. Concluímos que a primeira equação tem duas soluções 3 e 4 módulo 7, a segunda tem três soluções módulo 9: 1, 4 e 7, e a terceira tem duas soluções 4 e 7. Teríamos portanto que resolver os 12 sistemas de 3 equações da forma

$$\begin{cases} x^2 \equiv a_1 \mod 7 \\ x^3 \equiv a_2 \mod 9 \\ x^4 \equiv a_3 \mod 11 \end{cases}$$

onde $a_1 \in \{3\}$, $\{a_2\} \in \{1, 4, 7\}$ e $a_3 \in \{4, 7\}$.

Em alternativa, podemos usar o outro método: resolvemos as equações da forma

$$\frac{m}{m_i} y \equiv 1 \mod m_i$$

Temos

$$99y \equiv 1(\mod 7) \Leftrightarrow y \equiv 1(\mod 7)$$

e portanto podemos escolher $b_1 = 1$. As outras equações são

$$77y \equiv 1(\mod 9) \Leftrightarrow 5y \equiv 1(\mod 9) \Leftrightarrow y \equiv 2(\mod 9)$$

e

$$63y \equiv 1(\mod 11) \Leftrightarrow 8y \equiv 1(\mod 11) \Leftrightarrow y \equiv 7(\mod 11)$$

e portanto $b_2 = 2$ e $b_3 = 7$. Substituindo os valores dos ai na expressão

$$x = \sum_{i=1}^{3} \frac{m}{m_i} b_i a_i = 99a_1 + 154a_2 + 441a_3$$

obtemos as doze soluções pretendidas.

Recorde-se que os b_i são calculados módulo m_i; podemos portanto, por exemplo, pôr $b_3 = -4$; as soluções obtidas são as mesmas módulo $m = 7 \times 9 \times 11 = 693$, ainda que representadas por outros inteiros.

O Teorema Chinês dos Restos pode ser enunciado alternativamente do seguinte modo:

Teorema 3.5. Se $M = m_1 \times \cdots \times m_k$ e $mdc(m_i; m_j) = 1$ se $i \neq j$, então a aplicação

$$\psi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

definida por

$$\psi(a) = (a \mod m_1, \cdots, a \mod m_k)$$

é uma bijecção.

A existência de solução para qualquer sistema da forma

$$\begin{cases} x \equiv a_1 (\mod m_1) \\ x \equiv a_2 (\mod m_2) \\ \vdots \\ x \equiv a_k (\mod m_k) \end{cases}$$

e equivalente a ψ ser sobrejetiva; por outro lado, a propriedade de ψ ser injetiva é equivalente a aquela solução ser única módulo M.

Quando enunciado desta forma, o Teorema Chinês dos Restos é de demonstração ainda mais simples: de fato, basta provar que ψ é injetiva, sendo a sobrejetividade uma consequência imediata de o domínio e o contra-domínio desta aplicação terem o mesmo número de elementos. Mas ψ é injetiva uma vez que

$$x \equiv y (\mod m_i) \ \forall i \in \{1, \cdots, k\} \Leftrightarrow x \equiv y \mod M$$

Por outro lado, este raciocínio não nos indica como resolver na prática um sistema, ou seja, dados $a_i \in \mathbb{Z}_{m_i}$, como determinar

$$\psi^{-1}(a_i, \cdots, a_k)$$

É isso que as outras demonstrações fazem. De facto, a segunda dessas demonstrações dá-nos uma fórmula para a função inversa de ψ:

$$\psi^{-1}(a_i, \cdots, a_k) = \sum_{i=1}^{k} \frac{m}{m_i} b_i a_i$$

ou mais precisamente a classe congruência módulo M deste inteiro.

3.1.5 O Problema do Matemático Chinês Sun-Tsu

Começamos o minicurso propondo o problema do primeiro século do matemático chinês Sun-Tsu. Qual o número que deixa restos 2,3 e 2 quando dividido, respectivamente, por 3, 5 e 7?

Alguns alunos "testam" alguns números e encontram o número 23 como primeira resposta.

A proposta a seguir é a mesma, mas utilizando Progressão Aritmética.

$A = \{2, 5, 8, 11, 14, \cdots\}$; $B = \{3, 8, 13, 18, \cdots\}$ e $C = \{2, 9, 16, 23, 30, \cdots\}$ Qual número aparece primeiro nas três sequências?

Solução. Os termos gerais são $3n + 2$, $5m + 3$ e $7p + 2$. Mas isso trás um problema pois n, m e p serão diferentes. Os alunos com isso foram preenchendo as sequências buscando número comum.

O Teorema Chinês do Resto traduzindo em linguagem de aritmética procura o sistema de congruência para $x \equiv 2(\mod 3)$, $x \equiv 3(\mod 5)$, $x \equiv 2(\mod 7)$. Conforme a demonstração do Teorema Chinês do Resto $N = 3 \times 5 \times 7 = 105$, $N_1 = 35$, $N_2 = 21$, $N_3 = 15$ com isso $y_1 = 2$, $y_2 = 1$, $y_3 = 1$.

$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$x = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$ com isso $233 \equiv 23 \mod 105$.

Solução minimal é 23 e a solução é $23 + 105p$. As soluções das três sequências é uma outra sequência $\{23, 128, 203, 308, 413, \cdots\}$

3.1.6 Problema da Reposição Salarial

Uma empresa tem três cargos Junior, Office e Sênior. A cada 3 anos o cargo Junior tem reposição salarial, o cargo Office tem reposição salarial a cada 4 anos e o cargo Sênior a cada 5 anos. Se o cargo Junior teve aumento a primeira vez em 2002, o Office em 2003 e o Sênior em 2004, qual o primeiro ano que acontecerá reposição para os três cargos, e de quanto em quanto tempo terão reajustes juntos?

Solução. Usando o Teorema Chinês do Resto temos:

$x \equiv 2(\mod 3)$, $x \equiv 3(\mod 4)$, $x \equiv 4(\mod 5)$. Conforme a demonstração do Teorema Chinês do Resto $N = 3 \times 4 \times 5 = 60$, $N_1 = 20$, $N_2 = 15$, $N_3 = 12$ com isso $y_1 = 2$, $y_2 = 3$, $y_3 = 3$.

$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$x = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 4 = 359$ com isso $359 \equiv 59(\mod 60)$.

Solução minimal é 59 e a solução é $23 + 60p$. As soluções das três sequências vira uma outra sequência $\{59, 119, 179, 239, \cdots\}$ ou seja resposta é 2059 e o reajuste acontece junto de 60 em 60 anos.

3.1.7 Dosagem de Remédio

Um remédio A é dosado para o paciente na UTI de 10 em 10 horas, sendo o primeiro as 5 horas da manhã do dia 01 de maio de 2014, o mesmo paciente tem dosagem de 16 em 16 horas de um remédio B dosado a primeira vez as 11 horas do dia 01 de maio de 2014. O último remédio C foi dosado a primeira vez no mesmo dia 01 de maio de 2014 as 19 horas e será dosado 1 por dia, ou seja, a cada 24 horas. Qual a primeira vez que os remédios serão dosados juntos?

Solução. Sendo $x \equiv 5(\mod 10)$, $x \equiv 11(\mod 16)$, $x \equiv 19(\mod 24)$. Cuidado com a resolução pois o $mdc(10, 16, 24) = 2$. Faremos uma adaptação sendo a resolução para

$x \equiv 0(\mod 5)$

$x \equiv 1(\mod 2)$

$x \equiv 1(\mod 3)$

$x \equiv 0(\mod 5)$, $x \equiv 1(\mod 2)$, $x \equiv 1(\mod 3)$. Conforme a demonstração do Teorema Chinês do Resto $N = 5 \times 2 \times 3 = 30$, $N_1 = 6$, $N_2 = 15$, $N_3 = 10$ com isso $y_1 = 1$, $y_2 = 1$, $y_3 = 1$

$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$x = 6 \cdot 1 \cdot 0 + 15 \cdot 1 \cdot 1 + 10 \cdot 1 \cdot 1 = 25$ com isso $25 \equiv -5(\mod 30)$ ou seja $25 \equiv 25(\mod 30)$

Solução $(30p + 25)$. Para voltarmos na solução do nosso problema inicial

$(30p + 25) \times 8 + 11 + 19 + 5$ ou seja $X = 240p + 235$. A resposta é de 235 horas após 01 de maio de 2014 e de 240 horas em 240 horas. Solução 9 dias e 1 horas e a cada 10 dias. Resposta dia 9 de maio às 19 horas e a cada 10 dias no mesmo horário.

3.1.8 Problema dos Automóveis

Três automóveis Três automóveis disputam uma corrida em uma pista circular. O 1^{o} a sair dá uma volta em 3 minutos, o 2^{o} a sair dá uma volta em 5 minutos e o 3^{o} a sair dá uma volta em 11 minutos. Se o primeiro saiu após 1 minuto do início, o segundo após 2 minutos e o terceiro após 7 minutos do início, qual o tempo após a saída que passam os três juntos na linha de saída?

Solução. Usando o Teorema Chinês do Resto temos:

$x \equiv 1(\mod 3)$, $x \equiv 2(\mod 5)$, $x \equiv 7(\mod 11)$. Conforme a demonstração do Teorema Chinês do Resto $N = 3 \times 5 \times 11 = 165$, $N_1 = 55$, $N_2 = 33$, $N_3 = 15$ com isso $y_1 = 1$, $y_2 = 2$, $y_3 = 3$

$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$x = 55 \cdot 1 \cdot 1 + 33 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 7 = 502$ com isso $502 \equiv 7(\mod 165)$

Solução minimal é 7 e a solução é $7 + 165p$. As soluções das três sequências vira uma outra sequência $\{7, 172, 337, 502, \cdots\}$ ou seja resposta é 172 minutos ou 2 horas e 52 minuto, e a volta no início é de 165 em 165 minutos.

3.1.9 Problema dos Horários dos Ônibus

Uma estação de ônibus tem três linhas. Alvorada sai a cada 3 minutos, Baú a cada 5 minutos e Consil a cada 11 minutos. Se a linha Alvorada começa as 6h01min, a

Baú as 6h02min e a linha Consil as 6h06min . Qual o primeiro horário que sairão juntas as 3 linhas da estação?

Solução. Usando o Teorema Chinês do Resto temos:

$x \equiv 1(\mod 3)$

$x \equiv 2(\mod 5)$

$x \equiv 6(\mod 11)$.

Conforme a demonstração do Teorema Chinês do Resto $N = 3 \times 5 \times 11 = 165$, $N_1 = 55$, $N_2 = 33$, $N_3 = 15$ com isso $y_1 = 1$, $y_2 = 2$, $y_3 = 3$

$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$x = 55 \cdot 1 \cdot 1 + 33 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 6 = 457$ com isso $502 \equiv 127(\mod 165)$

Solução minimal é 127 e a solução é $127 + 165p$. As soluções das três sequências vira uma outra sequência $\{127, 292, 419, \cdots\}$ ou seja resposta é 127 minutos, 2 horas e 7 minutos ou 8h07min.

3.1.10 Problema da Logística para os Jogos da Copa

Na logística para a copa do mundo de 2014 foram destinados 3 linhas direto do aeroporto para o estádio de uma das sede da COPA. Linha A de 6 em 6 minutos, saindo a primeira linha 5h05min da manhã. Linha B de 5 em 5 minutos, saindo a primeira linha 5h da manhã e por último linha C de 11 em 11 minutos, saindo a primeira linha às 5h04 minutos. Qual a primeira vez no dia que sairão as 3 linhas juntas e de quanto em quanto minutos isso se repete?

Solução. Usando o Teorema Chinês do Resto temos:

$x \equiv 5(\mod 6)$

$x \equiv 0(\mod 5)$

$x \equiv 4(\mod 11)$.

Conforme a demonstração do Teorema Chinês do Resto $N = 6 \times 5 \times 11 = 330$, $N_1 = 55$, $N_2 = 66$, $N_3 = 30$ com isso $y_1 = 1$, $y_2 = 1$, $y_3 = 7$

$X = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$X = 55 \cdot 1 \cdot 5 + 66 \cdot 0 \cdot 1 + 30 \cdot 7 \cdot 4 = 457$ com isso $1115 \equiv 125(\mod 330)$

Solução minimal é 125 e a solução é $125 + 330p$. As soluções das três sequências vira uma outra sequência $\{125, 455, 785, \cdots\}$ ou seja resposta é 125 minutos, 2 horas e 5 minutos ou 7h05min.

3.1.11 Problema das Placas

Em uma estrada são colocadas placas de km a cada 3 km começando no km 2 e telefones a cada 5 km começando no km 3 . Qual a décima vez que o telefone ficará fixado junto a placa?

Solução. Usando o Teorema Chinês do Resto temos:

$x \equiv 2(\mod 3)$

$x \equiv 3(\mod 5)$

Conforme a demonstração do Teorema Chinês do Resto $N = 3 \times 5 = 15$, $N_1 = 5$, $N_2 = 3$ com isso $y_1 = 2$, $y_2 = 2$

$x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 5 \cdot 2 \cdot 2 + 3 \cdot 2 \cdot 3 = 38$ com isso $38 \equiv 8(\mod 15)$

Solução minimal é 8 e a solução é $8+15p$. A solução quando $p = 10$ é $8+15(10) = km$ 158.

3.1.12 Problema das Lâmpadas na Árvore de Natal

Em uma árvore de natal foram instalados 3 cores de lâmpadas. A lâmpada vermelha foi ligada às 8h02min e pisca de 11 em 11 minutos. A lâmpada branca foi ligada às 8h11min e pisca de 14 em 14 minutos e a lâmpada verde foi ligada às 8h03min e pisca de 15 em 15 minutos. Qual o primeiro horário que as lâmpadas piscaram juntas?

Solução. Usando o Teorema Chinês do Resto temos:

$x \equiv 2(\mod 11)$

$x \equiv 11(\mod 14)$

$x \equiv 3(\mod 15)$.

Conforme a demonstração do Teorema Chinês do Resto $N = 11 \times 14 \times 15 = 2310$, $N_1 = 210$,

$N_2 = 165$, $N_3 = 154$ com isso $y_1 = 1$, $y_2 = 9$, $y_3 = 4$

$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$

$x = 210 \cdot 1 \cdot 2 + 165 \cdot 9 \cdot 11 + 154 \cdot 4 \cdot 3 = 18603$ com isso $18603 \equiv 123(\mod 2310)$

Solução minimal é 123 e a solução geral é $123 + 2310p$. As soluções das três sequências vira uma outra sequência $\{123, 2433, 4743, \cdots\}$ ou seja resposta é 123 minutos ou seja 10h03min.

3.1.13 Aplicação em Compartilhamento de Senha

O compartilhamento de senhas é uma maneira segura e eficiente de se partilhar uma chave entre um grupo de pessoas. A ideia é dividir a senha sem que a pessoa tenha a senha completa e não seja necessário todas as pessoas para para descobrir a senha compartilhada. O número de integrantes que precisamos para descobrir a senha vai depender dos números primos escolhidos no grupo. será verificado que para um grupo de X elementos e que necessita de de Y elementos no grupo para descobrir a senha, escolhemos X números primos de forma que o produto dos y menores seja maior que $(y-1)$ maiores.

Exemplo: se escolhermos o conjunto de primos $\{11, 13, 29, 31, 43\}$ a solução poderia ser em conjuntos de 2 em 2 pois $11 \cdot 13$ é igual a 143 e isso é maior que 29, maior que 31 e maior que 43. Mas também poderia ser em conjuntos de 3 em 3 pois $11 \cdot 13 \cdot 29 = 4147$ é maior que $31 \cdot 43 = 1333$. o grupo de elementos para descobrir a senha é igual a quantidade de equações a serem resolvidas na congruência linear. A senha pode ser qualquer número menor que o produto dos dois menores elementos do conjunto dos números primos.

3.1.13.1 Exemplo de aplicação de compartilhamento de senhas

Um pai tem cinco filhos e resolve deixar de herança para os cinco filhos uma grande quantia dentro de um cofre com senha no banco da cidade. Para recuperar a senha completa necessitam de pelo menos duas delas para tal. Isso significa que o conjunto de cinco elementos tem pelo menos dois para encontrar a senha (chave) completa, o conjunto tem limiar 2 e nos permite agrupar quaisquer elementos 2 em 2.

Para resolver esse problema escolheremos cinco números primos, pois são cinco filhos $\{11, 13, 17, 19$ e $23\}$. A senha tem que ser um número entre 11 e 143, pois o produto entre os dois menores $11 \cdot 13$ é igual a 143. Escolhido a senha número 105, as senhas distribuídas aos filhos serão os números primos e os restos da divisão desses primos com 105. Outro conjunto dos restos da divisão do 105 pelos os números de cada filho seria $\{6, 1, 3, 10, 13\}$ os filhos receberiam os números $\{11, 6\}$, $\{13, 1\}$, $\{17, 3\}$, $\{19, 10\}$, $\{23, 13\}$.

O compartilhamento de senha utilizando o Teorema Chinês do Resto é a solução do sistema :

$$\begin{cases} C \equiv 6 \mod 11 \\ C \equiv 1 \mod 13 \\ C \equiv 3 \mod 7 \\ C \equiv 10 \mod 19 \\ C \equiv 13 \mod 23 \end{cases}$$

Utilizando o teorema Chinês do resto, precisamos encontrar a solução de duas equações do sistema de congruência linear acima.

$$\begin{cases} C \equiv 6 \mod 11 \\ C \equiv 1 \mod 13 \end{cases}$$

$N = 11 \cdot 13 = 143$ onde

$$\begin{cases} n_1 = 13 \\ n_2 = 11 \end{cases} ; \begin{cases} 13y_1 \equiv 1 \mod 11 \\ 11y_2 \equiv 1 \mod 13 \end{cases} ; \begin{cases} y_1 = 6 \\ y_2 = 6 \end{cases}$$

A solução é:

$$S = 6 \cdot 13 \cdot 6 + 6 \cdot 11 \cdot 1 = 534534 \equiv 105 \mod 143$$

Solução minimal é 105, a senha procurada.

Capítulo 4

Relatório sobre o Minicurso

Neste capítulo faremos um breve relato da aplicação da proposta do minicurso realizada em duas turmas. A primeira foi com vinte alunos no Colégio Maxi (turma do 3^{o} ano de um colégio particular de Cuiabá) e a segunda foi na Escola Liceu Cuiabano (turma do 2^{o} ano com quinze alunos de uma escola pública estadual de Cuiabá). Neste relato, incluímos observações sobre fatos importantes ocorridos durante os minicursos ministrados e a utilização dos conceitos aprendidos pelos alunos.

4.1 Proposta do minicurso

Identificação do minicurso- O curso é voltado para alunos do Ensino Médio e tem como tema o **Teorema Chinês do Resto e suas aplicabilidades** em exercícios contextualizados de olimpíadas de matemática e processos seletivos para faculdades e universidades.

Carga horária do minicurso - Total de 4 horas semanais e será ministrado pelo professor Adriano Sales.

Objetivo do minicurso- Instrumentalizar os discentes com ferramentas matemáticas na área de aritmética para solucionar problemas contextualizados bem como dar bases gerais para outros tipos de exercícios.

Conteúdo programático - Revisão sobre Divisibilidade, MDC, MMC e números primos. Introdução e conceituação de Congruência Linear, Aritmética do Resto e Teorema Chinês do Resto.

Procedimentos de Ensino - Minicurso com aulas expositivas e participativas; apre-

sentação e resolução de exercícios contextualizados sobre os conteúdos programáticos; leitura de exercícios; reflexão e discussão de situação problema; organização e realização de exercícios. Reunir em grupos para apresentação e solução de situações problemas sugeridos no decorrer do curso.

O minicurso pode ser aplicado no decorrer do ano letivo, ou como atividade de projeto fora do horário das aulas de matemática.

O minicurso faz parte da proposta elaborada pelo PROFMAT como uma aula sobre algum tópico ministrado no decorrer do mestrado profissional. O minicurso pode ser útil para o aluno do Ensino Médio.

Os dois minicursos aplicados tiveram como objetivo uma visualização sobre o tempo de aplicação, a abordagem com uma simbologia mais apropriada para o aluno do Ensino Médio e a assimilação sobre um assunto que para muitos era uma novidade.

O minicurso é uma proposta e deve ser aplicado em outras turmas para obtermos uma avaliação e tabulação dos resultados.

4.2 Observação sobre o minicurso

No início do curso é apresentado uma situação problema com dois exercícios contextualizados:

Exercício nº 1 Três automóveis disputam uma corrida em uma pista circular. O 1º a sair dá uma volta em 3 minutos, o 2º a sair dá uma volta em 5 minutos e o 3º a sair dá uma volta em 11 minutos. Se saírem juntos, qual o tempo após a saída que passam os três juntos na linha de saída?

Exercício nº 2 Três automóveis disputam uma corrida em uma pista circular. O 1º a sair dá uma volta em 3 minutos, o 2º a sair dá uma volta em 5 minutos e o 3º a sair dá uma volta em 11 minutos. Se o primeiro saiu após 1 minuto do início, o segundo após 2 minutos e o terceiro após 7 minutos do início, qual o tempo após a saída que passam os três juntos na linha de saída?

A pergunta feita nos dois minicursos que foram ministrados. Professor isso não é aquela matéria MMC? Não precisamos apenas achar o número que está na tabuada dos três automóveis?

Foi interessante responder o exercício nº 1 foi a ligação para a revisão de MMC, MDC e números primos.

O minicurso começa com a revisão de MMC, MDC e números primos. Logo após uma revisão sobre os conteúdos acima, eu pergunto. "O exercício n° 2 tem diferença em relação ao exercício nº 1 ?" Como aqui a revisão sobre divisibilidade e mostro que o deslocamento do referencial inicial do exercício 01 para o exercício 02 pode ser demonstrado com divisão euclidiana, o que também é visto no Ensino Médio com termo geral de uma Progressão Aritmética.

Mostra-se ao aluno que é necessário algo mais que MMC para resolver o exercício nº 2. Começa aqui após a revisão dos itens divisibilidade, divisão Euclidiana, MMC, MDC o minicurso e sua proposta inicial.

Começamos nos dois minicurso uma aula expositiva de Aritmética do resto, congruência linear. Com demonstrações, exemplos e propriedades trazemos nossos alunos para uma nova abordagem da matemática. Para muitos foi um primeiro contato para algumas simbologias da matemática, isso teve que ser feito com muito cuidado, pois foi comum o surgimento de perguntas, "Para que preciso fazer desse jeito", "não preciso escrever assim não", "nossa como isso me confunde"

O maior tempo do minicurso foi para conceitos e exemplos de congruência linear, aritmética do resto e o Teorema Chinês do Resto. O nosso objetivo era demonstrar para os alunos uma nova abordagem para um tema da matemática no Ensino Médio. Alguns concluíram que se tratava de Progressão Aritmética, outros concluíram que era sobre divisão e seu resto, afirmando que o quociente não iria muito influenciar no resultado. Aproveitando esse questionamento que demonstro as classes residuais e sua aplicabilidade.

Os exercícios tem a maioria apresentado como situação problema, e alguns alunos ficaram colocando números para resolver o Teorema Chinês do Resto, a pergunta que sempre indica para os alunos que resolviam dessa maneira era:

"Se o número for muito grande, perderemos um grande tempo?"

Após a solução do terceiro exercício utilizando Teorema Chinês do Resto, o quarto se torna um desafio para as duas turmas. Nesse momento surge questionamentos individuais, que são repassados para todos da turma e com isso o minicurso se torna mais desafiador para os alunos e professor.

No início da proposta do minicurso 3 horas seriam suficientes para esse assunto, no decorrer dos dois minicurso verificamos que o acrescer de 1 hora seria muito útil para que o aluno conseguisse resolver os últimos exercícios em grupo ou sozinho e na dúvida, solicitar auxilio teórico.

As dificuldades encontradas dos alunos foram de fundamentação teórica, argumentação para juntar o conteúdo matemático e a aplicabilidade no contexto.

Na dificuldade com a nomenclatura e reconhecimento de símbolos foi sugerido mais empenho na teoria, e uma resolução de exercícios com mais rigor técnico.

A leitura de símbolos e equações surge com o tempo de estudo e resolução de problemas. A interpretação dos exercícios contextualizados foi um obstáculo para os alunos. A sugestão foi a busca de texto matemático para melhor compreensão da formalização matemática após a leitura do problema. No decorrer do curso a simbologia se torna aliada para resolver e desenvolver problemas com aplicações no cotidiano.

Os dados avaliados e relatórios da aplicação do minicurso não serão colocados aqui, pois a proposta é de formação do minicurso e precisaria de uma quantidade maior de alunos para relatar esses dados.

Capítulo 5

Consideracoes Finais

Este trabalho teve como objetivo mostra que a Aritmética é um tema atual que pode ser introduzido no Ensino Fundamental e Ensino Médio através de uma proposta diferenciada, com ênfase em situações problemas, em exercícios contextualizados.

Para isto, mostramos para os alunos do minicurso a resolução de exercícios contextualizados com situações problemas, retirados de olimpíadas de matemática, livros didáticos ou processos seletivos de universidades. No minicurso abordamos alguns conteúdos como revisão e outros conteúdos com demonstração e propriedades que iria auxiliar em algumas resoluções. Mostramos que a Aritmética através da congruência, auxilia na solução de exercícios com vários assuntos ministrados no Ensino Médio. No decorrer do minicurso fica claro a dificuldade dos alunos do Ensino Médio com algumas nomenclaturas e simbologia, isso pode ser bem resolvido com exemplos e demonstrações com assuntos mais comuns ao aluno. Esse minicurso pode ser estendido com assuntos como equação diofantina e criptografia que são também itens da Aritmética que auxilia na solução de alguns exercícios contextualizados com situações problemas, retirados de olimpíadas de matemática, livros didáticos ou processos seletivos de universidades.

Finalmente, observamos nestes dois minicurso que a Aritmética é um assunto que motiva a aprendizagem e pode ser útil na elaboração e solução de vários exercícios no currículo matemático do Ensino Médio. Dessa forma acredito que o Teorema Chinês do Resto como outros assuntos da Aritmética seja de grande utilidade para os alunos do Ensino Médio.

Surge a necessidade de proposta de alguns minicursos:

- Equações Diofantinas

- Criptografia
- MMC, MDC e Propriedades
- Números Primos

Poderia ser criado ainda uma parte do curso para a formação de material concreto. Elaborar com os alunos o material, para que se crie o hábito de pesquisa e de modelagem matemática.

Faltou na proposta ainda uma avaliação do antes e depois, que seria de muita utilidade para pesquisas ou aprimoramento do curso.

O projeto com isso sairia de uma proposta para virar um minicurso com resultados catalogados e definidos.

O minicurso pode se tornar realidade, para poder auxiliar algumas perguntas que nesse primeiro teste não foram respondidas.

A proposta deve ser colocada em pratica em um número considerado de turmas para que seja tiradas algumas conclusões, o que não ocorreu nessa proposta.

Referências Bibliográficas

[1] HEFEZ, Abramo2011; **Elementos da Aritmética**, 2ª edição, SBM, Rio de Janeiro, 2011.

[2] MUNIZ NETO, Antonio Caminha; **Tópicos de matemática elementar: teoria dos números**, 1ª edição, SBM, Rio de Janeiro, 2012.

[3] MATTOS, Sergio R.P.de.; PUGGIAN, Cleonice.; LOZANO, Abel R.G; **Aritmética Modular e Suas Possibilidades Na Formação Continuada de Professores de Matemática**, Recife, 2011.

[4] http://magiadaatemática.com; **Autor: S A, llydio Pereira; Título: Aritmética Modular e algumas de suas aplicações**, Data de acesso: 15 maio de 2014.

[5] MALANGA, Umberto C.C; **Nosso trabalho consiste: Livros 1 e 2 Matemática Sistema de Ensino Poliedro Pré Vestibular**, Editora Poliedro, São Paulo, 2013.

[6] S A, IIydio, P.; **A magia da matemática**, Ciência Moderna, Rio de Janeiro, 2007.

[7] BARROS, Marco Antonio de Oliveira; **Congruência Modular**, Tese de Mestrado. Departamento de Matemática, UFMT,Cuiabá, 2014.

Anexo

APOSTILA PARA O MINICURSO

Adriano Sales Nascimento