Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

Uma Abordagem da Aritmética Modular no Ensino Básico [†]

por

Tércio das Neves Almeida

sob orientação do

Prof. Bruno Henrique Carvalho Ribeiro

Trabalho de conclusão de curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

agosto/2014
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Uma Abordagem da Aritmética Modular no Ensino Básico

por

Tércio das Neves Almeida

Trabalho de conclusão de curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática.

Aprovada por:

Prof. Dr. Bruno Henrique Carvalho Ribeiro -UFPB (Orientador)

Prof. Dr. Uberlandio Batista Severo - UFPB

Profa.Dra. Maria Isabelle Silva - UEPB

agosto/2014

Agradecimentos

Agradeço primeiramente a Deus, que me propiciou saúde e força de vontade para que eu pudesse chegar até aqui.

A minha mãe, Rosilda das Neves Almeida, por ter tido paciência e dedicação em lidar comigo e insistir nos meus estudos.

Minha falecida avó, Maria Luíza Alves das Neves, que cuidava de todos os meus irmãos e a mim enquanto minha mãe trabalhava, nos dando educação doméstica e cuidados de uma segunda mãe.

A Minha esposa, Ana Karla Miranda de Luna, quem me incentivou a fazer e a concluir o Profmat, estando ao meu lado em todos os momentos do curso.

Ao meu orientador, Bruno Henrique Carvalho Ribeiro, que me acolheu neste projeto.

Aos meus amigos e colegas que estiveram comigo nesta jornada, em especial ao amigo Francisco do Nascimento Lima, que, além de me incentivar, teve paciência para ajudar na construção deste projeto.

A todos os professores que fazem o Profmat acontecer, pois sem eles não haveria este sonho de mestrado profissionalizante; sei que se esforçaram para que todos saíssem com mais embasamento teórico.

Ao meu falecido pai, Fernando José Barreto, sempre se preocupou com os estudos de todos em minha casa.

Aos colegas de trabalho da Escola Estadual João José da Costa que sempre estavam dando força para que fosse possível a conclusão do Profmat.

Aos meu alunos que participaram das aulas, mesmo os que tiveram de desistir por motivos adversos, em especial a eles: Ana Beatriz Mesquita da Silva, Letícia Raquel Medeiros de Lima Barbosa, Rikelme Escócio Pereira da Silva e Viviane Veríssimo de Paiva, que foram até o fim, mesmo com todas as dificuldades.

Dedicatória

Dedico este trabalho a minha esposa que está grávida de uma menina a quem tanto amo, Luíza Karla Miranda de Almeida, minha mãe que esteve sempre comigo.

Resumo

Este trabalho consiste em uma aplicação em sala de aula de Aritmética voltada para as Olimpíadas Brasileiras de Matemática com alunos da Rede Pública de Ensino Fundamental, apresentando a teoria como os teoremas, definições, corolários e proposições; para que o aluno possa construir e compreender regras de divisibilidade, assim como resolver problemas que podem se apresentar no dia a dia ou os propostos em sala de aula do Ensino Médio.

Abstract

...

Sumário

Introdução

Este trabalho trata de uma pesquisa de campo sobre a Aritmética e resoluções de questões voltadas para a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) usando embasamento teórico: definições, Proposições, Teoremas, Lemas e Corolários. A pesquisa também mostra a falta de incentivo aos profissionais de Matemática e aos estudantes, embora tenhamos estudantes com grandes potenciais para o trabalho com a Matemática.

A Matemática, em particular a Aritmética, se apresenta com uma das maiores vilãs, junto com a disciplina de português, nos índices de reprovação e abandono escolar. É uma disciplina pouco apreciada pela maioria dos estudantes nas escolas, apesar de seu uso diário em nossas vidas: passar ou receber o troco de uma determinada compra, o tempo que falta para realizar tarefas ou de um determinado programa começar ou terminar, contagem e outras aplicações. Sendo assim, cabe ao professor de Matemática encontrar formas de despertar a curiosidade e a vontade do estudante de querer aprender e de fazer novas descobertas na área da Matemática e ao Governo de dar incentivo aos estudantes para desenvolver a Matemática, pois aqui se trata da disciplina básica das ciências e do desenvolvimento tecnológico.

O trabalho que aqui se apresenta está dividido em dois capítulos, em que iremos demonstrar toda a teoria passo a passo e citar exemplos e, também, discutir uma análise da aplicação em sala de aula dos assuntos envolvidos.

O Capítulo 1 trata da Matemática formal, definições, notações, demonstrações de teoremas, lemas, corolários e proposições, seguido de exemplos, assim como traremos demonstrações de algumas regras de divisibilidade usando congruência e deixando a ideia para que se possa construir outras regras.

O Capítulo 2 trata de relatos em sala de aula com uma turma formada especificamente para este trabalho, relatando o interesse ou a falta dele nos estudantes, falta de incentivo e de apoio para formar um grupo de estudo voltado para a OBMEP ou qualquer outra finalidade, e para o desenvolvimento do estudante comparando seu desempenho antes, durante e depois das aulas.

Capítulo 1

Teoria dos Números

Neste capítulo, discutiremos acerca dos conceitos, definições e proposições da Teoria dos Números, baseados nas obras de [1] e [3], que servirão de suporte nas atividades propostas no capítulo subsequente.

1.1 Divisibilidade

Definição 1 *Dados dois números inteiros a e b com $a \neq 0$, diremos que a divide b, escrevendo $a \mid b$, quando existir $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é múltiplo de a.*

Note que a notação $a \mid b$ não representa operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$.

Exemplo: Dados 3 e 9, temos que $3 \mid 9$, pois podemos tomar $3 \in \mathbb{Z}$ tal que $9 = 3 \cdot 3$;

Dados 3 e 18, temos que $3 \mid 18$, pois podemos tomar $6 \in \mathbb{Z}$ tal que $18 = 3 \cdot 6$;

Dados 2 e 4, temos que $2 \mid 4$, pois podemos tomar $2 \in \mathbb{Z}$ tal que $4 = 2 \cdot 4$;

Dados 2 e 6, temos que $2 \mid 6$, pois podemos tomar $3 \in \mathbb{Z}$ tal que $6 = 2 \cdot 3$.

A negação da sentença $a \mid b$ é representada por $a \nmid b$ que significa dizer que não existe nenhum número inteiro $q \in \mathbb{Z}$ tal que $b = a \cdot q$.

Exemplo: Dados 3 e 5, temos que $3 \nmid 5$, pois tomando $1 \in \mathbb{Z}$, temos que $5 > 3 \cdot 1$ e, tomando $2 \in \mathbb{Z}$, temos que $5 < 3 \cdot 2$. Como sabemos que não existe nenhum número inteiro entre 1 e 2, tal que $5 = 3 \cdot q$, temos que $3 \nmid 5$.

Se $a \mid b$; seja $q \in \mathbb{Z}$ tal que $b = a \cdot q$. O número inteiro q é chamando de quociente de b por a e é denotado por $q = \frac{b}{a}$.

Exemplo: Dados 0 e 1, temos que $\frac{0}{1} = 0$

Dados 0 e 2, temos que $\frac{0}{2} = 0$

Dados 18 e 3, temos que $\frac{18}{3} = 6$.

Proposição 1.1 *Sejam $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$. Tem-se que:*

(i) $1 \mid c$, $-1 \mid c$, $a \mid a$ *e* $a \mid 0; \forall a \neq 0$;

(ii) *se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$;

(iii) *se* $a \mid 1$ *então* $a = \pm 1$;

(iv) $a \mid b$ *se, e somente se,* $a \mid -b$.

Demonstração:

(i) Pela definição de divisibilidade, dados 1, $c \in \mathbb{Z}$, temos que $1 \mid c$ se, e somente se, existir $k \in \mathbb{Z}$, tal que $c = 1 \cdot k$, logo $c = k$.

De mesmo modo, dados -1, $c \in \mathbb{Z}$, temos que $-1 \mid c$ se, e somente se, existir $t \in \mathbb{Z}$, tal que $c = (-1) \cdot t$, ou seja, $c = -t$ donde temos $t = -c$.

Dado o número $a \in \mathbb{Z}$, temos que de fato $a \mid a$, pois $1 \in \mathbb{Z}$ é tal que $a = 1 \cdot a$.

Dados os números a, $0 \in \mathbb{Z}$, temos que $a \mid 0$, pois como $0 \in \mathbb{Z}$ temos $0 = a \cdot 0$.

(ii) Pela definição de divisibilidade, dados a, b *e* $c \in \mathbb{Z}$ então $a \mid b$ se, e somente se, existir $q_1 \in \mathbb{Z}$ tal que

$$b = a \cdot q_1 \tag{1.1}$$

e $b \mid c$ se, e somente se, existir $q_2 \in \mathbb{Z}$ tal que $c = b \cdot q_2$.

Substituindo em (1.1) a primeira equação na segunda, temos $c = (a \cdot q_1) \cdot q_2$.

Então

$$c = a \cdot (q_1 \cdot q_2).$$

Como q_1 e $q_2 \in \mathbb{Z}$, temos que $q_1 \cdot q_2 = q \in \mathbb{Z}$. Assim temos $c = a \cdot (q_1 \cdot q_2)$ e $c = a \cdot q$, ou seja, $a \mid c$.

(iii) Dados os números $a,\ 1 \in \mathbb{Z}$, temos que $a \mid 1$, se e somente se, existir $q \in \mathbb{Z}$, tal que $1 = a \cdot q$. Como $a, q \in \mathbb{Z}$, tem-se que ou $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$.

(iv) Temos que se $a \mid b$, então existe $c \in \mathbb{Z}$, tal que $b = a \cdot c$. Multiplicando ambos os membros por -1, temos $-b = a \cdot (-c)$, isto é, $a \mid -b$.

□

Observação 1 *O item (i) da proposição acima nos diz que todo número inteiro é divisível por* ± 1 *e, se não nulo, por si mesmo.*

Proposição 1.2 *Se* $a, b, c, d \in \mathbb{Z}$, *com* $a \neq 0$ *e* $c \neq 0$, *tal que* $a \mid b$ *e* $c \mid d$, *então* $a \cdot c \mid b \cdot d$.

Demonstração: Pela definição de divisibilidade, dados $a,\ b,\ c$ e $d \in \mathbb{Z}$, temos que $a \mid b$ se, e somente se, existir $q_1 \in \mathbb{Z}$; $b = a \cdot q_1$ e $c \mid d$ se, e somente se, existir $q_2 \in \mathbb{Z}$, tal que $d = c \cdot q_2$. Multiplicando as duas equações, temos:

$$b \cdot d = (a \cdot q_1) \cdot (c \cdot q_2).$$

Assim, usando as propriedades comutativa e a associativa, temos

$$b \cdot d = (a \cdot c) \cdot (q_1 \cdot q_2)$$

$$b \cdot d = (a \cdot c) \cdot q.$$

Temos que $q_1 \cdot q_2 = q \in \mathbb{Z}$, ou seja,

$$a \cdot c \mid b \cdot d.$$

□

Em particular, se $a \mid b$, então $a \cdot c \mid b \cdot c$, para todo $c \in \mathbb{Z}$, $c \neq 0$.

Exemplo: Sabemos que $2 \mid 6$, pois $3 \in \mathbb{Z}$ é tal que $6 = 2 \cdot 3$ e $3 \mid 12$, pois $4 \in \mathbb{Z}$ é tal que $12 = 3 \cdot 4$. Dessa forma, substituindo a primeira equação na segunda, temos $3 \cdot 2 \mid 6 \cdot 12 \Rightarrow 6 \mid 72$.

Proposição 1.3 *Sejam* $a, b, c \in \mathbb{Z}$, *com* $a \neq 0$, *tal que* $a \mid (b + c)$. *Então* $a \mid b$ *se, e somente se,* $a \mid c$.

Demonstração: Se $a \mid (b + c)$, pela definição de divisibilidade, temos que existe um $q_1 \in \mathbb{Z}$, tal que $(b + c) = a \cdot q_1$.

Suponha agora que $a \mid b$, isto é, existe $q_2 \in \mathbb{Z}$, tal que $b = a \cdot q_2$.
Substituindo a segunda equação na primeira, temos

$$a \cdot q_2 + c = a \cdot q_1.$$

Assim,

$$c = a \cdot q_1 - a \cdot q_2,$$

ou seja,

$$c = a \cdot (q_1 - q_2).$$

Escrevendo $q = (q_2 - q_1) \in \mathbb{Z}$, temos:

$$c = a \cdot q.$$

Portanto,

$$a \mid c.$$

Suponha, agora, que $a \mid c$. Dessa forma, se $a \mid (b + c)$, pela definição de divisibilidade, existe um $q_1 \in \mathbb{Z}$, tal que $(b + c) = a \cdot q_1$. Por outro lado, como $a \mid c$, existe também $q_3 \in \mathbb{Z}$, tal que $c = a \cdot q_3$.
Substituindo esta c na equação anterior, temos

$$(b + a \cdot q_3) = a \cdot q_1,$$

isto é,

$$b = a \cdot q_1 - a \cdot q_3.$$

Dessa forma,

$$b = a \cdot (q_1 - q_3).$$

Novamente, temos que existe $(q_1 - q_3) = q' \in \mathbb{Z}$, tal que $b = a \cdot q'$, ou seja, $a \mid b$. □

Exemplo: Observe que $3 \mid 18$. Assim, $3 \mid (6 + 12)$. Dessa forma, $3 \mid 6$, se, e somente se, $3 \mid 12$. De fato temos que $3 \mid 6$, pois existe $2 \in \mathbb{Z}$, tal que $6 = 3 \cdot 2$ e $3 \mid 12$, pois existe $4 \in \mathbb{Z}$ tal que $12 = 3 \cdot 4$.

Proposição 1.4 *Sejam $a, b, c \in \mathbb{Z}$, com $a \neq 0$, tal que $a \mid (b - c)$. Então $a \mid b$ se, e somente se, $a \mid c$.*

A demonstração desta proposição é consequência da Proposição 1.3 e do item (iv) da Proposição 1.1.

Exemplo: Dados os números 3, 6 e $9 \in \mathbb{Z}$, temos que $3 \mid (6 - 9)$. Então $3 \mid 6$ se, e somente se, $3 \mid 9$. De fato, $3 \mid (6 - 9)$, isto é, $3 \mid -3$, pois existe $-1 \in \mathbb{Z}$, tal que $-3 = 3 \cdot (-1)$ e $3 \mid 6$, pois existe $2 \in \mathbb{Z}$, tal que $6 = 3 \cdot 2$. Então $3 \mid -9$, o que é

verdade, pois existe $-3 \in \mathbb{Z}$, tal que $-9 = 3 \cdot (-3)$.

Da mesma forma, temos que como $3 \mid (6-9)$, isto é, $3 \mid -3$, pois existe $-1 \in \mathbb{Z}$, tal que $-3 = 3 \cdot (-1)$ e $3 \mid -9$, pois existe $-3 \in \mathbb{Z}$, tal que $-9 = 3 \cdot (-3)$, então $3 \mid 6$.

Proposição 1.5 *Se $a, b, c \in \mathbb{Z}$, com $a \neq 0$, são tais que $a \mid b$ e $a \mid c$, então $a \mid (xb \pm yc)$, parta todo $x, y \in \mathbb{Z}$.*

Demonstração: Como $a \mid b$ e $a \mid c$, pela proposição 1.6, temos que $a \mid x \cdot b$ e $a \mid y \cdot c$.

Dessa forma, existem $q_1, q_2 \in \mathbb{Z}$, tais que, $x \cdot b = a \cdot q_1$ e $y \cdot c = a \cdot q_2$ Somando ou subtraindo estas duas equações, temos

$$x \cdot b \pm y \cdot c = a \cdot q \pm a \cdot q'.$$

Logo,

$$x \cdot b \pm y \cdot c = a \cdot (q \pm q').$$

Como existe $(q \pm q') = q_3 \in \mathbb{Z}$, temos

$$x \cdot b \pm y \cdot c = a \cdot q_3.$$

Portanto,

$$a \mid (x \cdot b \pm y \cdot c).$$

□

Exemplo: Temos que $7 \mid 7$ e $7 \mid 14$, então $7 \mid (7 \cdot x \pm 14 \cdot y)$.

Vimos, na Proposição 1.6, que se $a \mid b$ então $a \mid bx$, isto é, se $7 \mid 7$, então 7 dividirá todos os múltiplos de 7; da mesma forma, $7 \mid 14$, então 7 dividirá todos os múltiplos de 14.

Proposição 1.6 *Se $a, b \in \mathbb{Z}$, com $a \neq 0$, e $a \mid b$, então $a \mid b \cdot n, \forall\ n \in \mathbb{Z}$.*

Demonstração: Como $a \mid b$, então existe $q_1 \in \mathbb{Z}$ tal que $b = a \cdot q_1$. Multiplicando a última igualdade por n, temos

$$b \cdot n = a \cdot q_1 \cdot n \text{ ou } b \cdot n = a \cdot (q_1 \cdot n).$$

Como $q_1, n \in \mathbb{Z}$, temos que existe $q_1 \cdot n = q \in \mathbb{Z}$. Portanto,

$$b \cdot n = a \cdot q, \text{ isto é, } a \mid b \cdot n.$$

□

Exemplo: Se $5 \mid 15$, então $5 \mid 30$, pois $30 = 15 \cdot 2$.

Proposição 1.7 *Se $a, b \in \mathbb{Z}^*$, tem-se que $a \mid b$, então $|a| \leqslant |b|$.*

Demonstração: $a \mid b$ se, e somente se, $q \in \mathbb{Z}^*$, tal que $b = a \cdot q$, dessa forma, $|b| = |a \cdot q|$, assim, $|b| = |a| \cdot |q|$ e como $b \neq 0$, temos que $q \neq 0$, assim $|q| \geqslant 1$ e portanto: $|b| = |a| \cdot |q| \geqslant |a| \cdot 1 \geqslant |a|$. □

Exemplo: Claramente, a recíproca da proposição anterior não é válida, pois, por exemplo, $|3| \geqslant |2|$; e, no entanto, $2 \nmid 3$.
Note que a relação de divisibilidade em $\mathbb{Z}_+{}^*$ é uma relação de ordem, pois

(i) é reflexiva: $\forall a \in \mathbb{Z}^*, a \mid a$;

(ii) é antissimétrica: se $a \mid b$ e $b \mid a$, então $a = b$;

(iii) é transitiva: se $a \mid b$ e $b \mid c$, então $a \mid c$.

1.1.1 Divisão Euclidiana

Euclides, em sua obra Elementos, provou que mesmo quando $a \nmid b$, com a e $b \in \mathbb{N}$ é possível efetuar a divisão de b por a com o resto.

Teorema 1.8 *(Divisão Euclidiana) Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que*

$$b = a \cdot q + r;\ r < a.$$

Demonstração: Suponha que $b > a$ e considere, enquanto fizer sentido, os números $b,\ b-a,\ b-2\cdot a,\ \ldots,\ b-n\cdot a,\ \ldots$. Note que o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q \cdot a$. Vamos provar que r tem a propriedade requerida, ou seja, que $r < a$. Se $a \mid b$, então $r = 0$ e nada mais temos a provar. Se, por outro lado, $a \nmid b$, então $r \neq 0$, logo, basta mostrar que não pode ocorrer $r \geqslant a$. De fato, se isto ocorresse, existiria um número natural $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - q \cdot a$, teríamos $c = b - (q+1) \cdot a \in S$, com $c < r$, contradição com o fato de r ser o menor elemento de S.
Portanto, temos que $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.
Agora, vamos provar a unicidade.
Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a é pelo menos a. Logo, se $r = b - a \cdot q$ e $r' = b - a \cdot q'$, com $r < r' < a$, teríamos $r' - r \geqslant a$, o que acarretaria $r' \geqslant r + a \geqslant a$, absurdo. Portanto, $r = r'$. Daí segue-se que $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$ e, portanto, $q = q'$. □

1.1.2 Algoritmo da Divisão

Teorema 1.9 *Se a e b são dois números inteiros, com $b > 0$, então existem e são únicos os inteiros q e r que satisfazem às condições:*

$$a = b \cdot q + r \text{ com } 0 \leqslant r < b.$$

Primeiro vamos mostrar existência. Seja S o conjunto de todos os inteiros não negativos que são da forma $a - b \cdot x$, com $x \in \mathbb{Z}$, isto é

$$S = \{a - b \cdot x \mid x \in \mathbb{Z}, a - b \cdot x \geqslant 0\}.$$

Este conjunto S não é vazio ($S \neq 0$), pois, sendo $b > 0$, $0 \leqslant r < b$, temos que $b \geqslant 1$ e, portanto, para $x = -|a|$, temos

$$a - b \cdot x = a + b \cdot |a| \geqslant a + |a| \geqslant 0.$$

Assim sendo, existe o elemento mínimo r de S tal que $r \geqslant 0$ e $r = a - b \cdot a$ ou $a = b \cdot q + r$, com $q \in \mathbb{Z}$. Além disso, temos que $r < b$, pois, se fosse $r \geqslant b$, teríamos

$$0 \leqslant r - b = a - b \cdot q = a - b \cdot (q + 1) < r.$$

Isto é, r não seria o elemento mínimo de S.
Agora amos mostrar unicidade de q e r. Suponhamos que existem dois outros números inteiros q_1 e r_1 tais que

$$a = b \cdot q_1 + r_1 \text{ e } 0 \leqslant r_1 < b.$$

Então, teremos:

$$b \cdot q_1 + r_1 = b \cdot q + r,$$

logo

$$r_1 - r = b \cdot q - b \cdot q_1.$$

Assim temos

$$r_1 - r = b \cdot (q - q_1).$$

Portanto,

$$b \mid (r_1 - r).$$

Por outro lado temos:

$$-b < -r \leqslant 0 \; e \; 0 \leqslant r_1 < b,$$

o que implica:

$$-b < r_1 - r < b \; isto: \; |r_1 - r| < b.$$

Assim, $b \mid (r_1 - r)$, mas $|r_1 - r| < b$. Com isso $r_1 - r = 0$ e, portanto,

$$r_1 = r \text{ e } q_1 = q.$$

Exemplo: Dados 3 e 13, números naturais, temos que $3 \nmid 13$, mas existem 4 e $1 \in \mathbb{N}$, tal que $13 = 3 \cdot 4 + 1$. Dados os números 4 e 19, temos que $4 \nmid 19$, mas existem 4 e $3 \in \mathbb{N}$ tal que $19 = 4 \cdot 4 + 3$.

Corolário 1.9.1 *Se a e b são dois inteiros, com $b \neq 0$, existem e são únicos os inteiros q e r que satisfazem as condições*

$$a = b \cdot q + r \text{ com } 0 \leqslant r < |b|.$$

Demonstração: com efeito, se $b > 0$, nada há que demonstrar, e se $b < 0$, então $|b| > 0$, e por conseguinte existem e são únicos os inteiros q_1 e r, tais que

$$a = |b| \cdot q_1 + r, \text{ com } 0 \leqslant r < |b|.$$

Ou seja,

$$|b| = -b.$$

Logo,

$$a = -b \cdot q_1 + r,$$

então

$$a = b \cdot (-q_1) + r$$

e

$$0 \leqslant r < |b|.$$

Dessa forma, temos que $q = -q_1$, ou seja:

$$a = b \cdot q + r \text{ e } 0 \leqslant r < |b|.$$

Os inteiros q e r chamam-se, respectivamente, o quociente e o resto na divisão de a por b. □

Exemplo: Encontre o quociente e o resto da divisão de 19 por -3.
Pelo algoritmo da divisão, na divisão de 19 por $3 \in \mathbb{Z}_+$, temos

$$19 = 3 \cdot 6 + 1.$$

O que implica: $19 = -3 \cdot (-6) + 1$.
Logo, $q = -6$ e $r = 1$.
Exemplo: Encontre o quociente e o resto na divisão de -19 por 3.
Pelo algoritmo de Euclides na divisão de 19 por $3 \in \mathbb{Z}_+$, temos

$$19 = 3 \cdot 6 + 1.$$

Multiplicando tudo por -1, temos

$$-19 = -3 \cdot 6 - 1.$$

Como $r = -1 < 0$, isto é, não satisfaz a condição $0 \leqslant r < 3$, temos

$$-19 = -3 \cdot 6 - 1 = -3 \cdot 6 - 3 + 2.$$

Com isso, $-19 = -3 \cdot 7 + 2 \Rightarrow -19 = 3 \cdot (-7) + 2$, ou seja:

$$q = -7 \text{ e } r = 2.$$

Observe que b é divisor de a se, e somente se, $r = 0$. Neste caso, temos $a = b \cdot q$ e o quociente q na divisão exata de a por b, indicado também por $\frac{a}{b}$ ou a/b $\left(q = \frac{a}{b} = a/b\right)$, e lê-se "$a$ sobre b".

1.1.3 Paridade de um Número Inteiro

Na divisão de um inteiro qualquer a por $b = 2$ os possíveis restos são $r = 0$ ou $r = 1$. Se $r = 0$, então o inteiro $a = 2 \cdot q$ é denominado par; e se $r = 1$, então o inteiro será escrito da seguinte forma $a = 2 \cdot q + 1$ e, consequentemente, denominado ímpar. Observe-se que:

(i) Se a for par, isto é, $a = 2k$, em que $k \in \mathbb{Z}$, então a^2 é par.

(ii) Se a for ímpar, isto é, $a = 2k \pm 1$, em que $k \in \mathbb{Z}$, então a^2 é ímpar.

Demonstração: (i) De fato, suponha que $a = 2k$, assim , $a^2 = (2k)^2$, ou seja, $a^2 = 4k^2$, logo, $a^2 = 2 \cdot (2k^2)$. Portanto $a^2 = 2n$, em que $2k^2 = n \in \mathbb{Z}$

(ii) Suponha que $a = 2k \pm 1$, dessa forma, $a^2 = (2k \pm 1)^2$, ou seja, $a^2 = 4k^2 \pm 4k + 1$. Assim, temos que, $a^2 = 2 \cdot (2k^2 + 2k) + 1$, isto é, $a^2 = 2t + 1$, em que $2k^2 + 2k = t \in \mathbb{Z}$. □

Exemplo: Observe que o quadrado de qualquer inteiro ímpar é da forma $8k + 1$. Pelo algoritmo da divisão, temos que dado um número $a \in \mathbb{Z}$, só temos quatro possibilidades de escrever a em função de 4, ou seja:

$$a = 4q,\ a = 4q + 1,\ a = 4q + 2 \text{ ou } a = 4q + 3.$$

Dessa forma, temos que

i' Temos que $a^2 = (4q)^2$, assim, $a^2 = 16q^2$, o que implica em $a^2 = 8 \cdot (2q^2)$. Dessa forma, como $(2q^2) = n \in \mathbb{Z}$, $a^2 = 8n$ que é um número par;

ii' Temos que $a^2 = (4q+1)^2$, assim, $a^2 = 16q^2 + 8q + 1$ que podemos escrever da seguinte forma: $a^2 = 8 \cdot (2q^2 + q) + 1$. Dessa forma, como $(2q^2 + q) = k \in \mathbb{Z}$, $a^2 = 8k + 1$ que é um número ímpar;

iii' Temos que $a^2 = (4q+2)^2$, assim, $a^2 = 16q^2 \pm 16q + 4$, que podemos escrever da seguinte forma: $a = 8(2 \cdot q^2 + 2 \cdot q) + 4 = 2[4(2 \cdot q^2 + 2 \cdot q) + 2]$, isto é, a é par.

iv' Temos que $a^2 = (4q+3)^2$, assim, $a^2 = 16q^2 + 24q + 9$, isto é, $a^2 = 8 \cdot (2q^2) + 8 \cdot (3q) + 8 + 1$, que podemos escrever da seguinte forma: $a^2 = 8 \cdot (2q^2 + 3q + 1) + 1$ $a^2 = 8k + 1$, isto é, como $(2q^2 + 3q + 1) = k \in \mathbb{Z}$, a^2 é ímpar.

Assim, por exemplo, 7 e 13 são inteiro ímpares, pois:

$$7^2 = 49 = 8 \cdot 6 + 1$$

$$13^2 = 169 = 8 \cdot 21 + 1.$$

1.1.4 Conjunto dos Divisores de um Número Inteiro

Definição 2 *: Seja $a \in \mathbb{Z}$, diremos que $D(a)$ é o conjunto dos divisores inteiros de a, se para todo $d \in D(a)$ d dividir a, isto é, $D(a) = \{x \in \mathbb{Z}^*;\ x \mid a\}$.*

Exemplo: Seja $2 \in \mathbb{Z}^*$, então $D(2) = \{-2,\ -1,\ 1,\ 2\}$, pois $-2 \mid 2$, $-1 \mid 2$, $1 \mid 2$ e $2 \mid 2$. Note, também, que não existe nenhum outro número inteiro que divide 2.

Exemplo: Seja $9 \in \mathbb{Z}^*$, então $D(9) = \{-9,\ -3,\ -1,\ 1,\ 3,\ 9\}$, pois $-9 \mid 9$, $-3 \mid 9$, $-1 \mid 9$, $1 \mid 9$, $3 \mid 9$ e $9 \mid 9$. Da mesma forma que no exemplo acima, não existe nenhum outro número inteiro que divida 9.

Observação 2 *: Note que, sabendo quais são os divisores naturais de um número $a \in \mathbb{Z}$, para encontrar os divisores inteiros basta tomar os divisores naturais e os seus simétricos.*

Observação 3 *$D(a) = D(-a)$, $\forall a \in \mathbb{Z}$, pois $a = a \cdot 1 = (-a) \cdot (-1)$. 1, -1, a e $-a$, são ditos divisores triviais de a.*

Qualquer que seja o inteiro $a \neq 0$, se $x \mid a$, então: $-a \leqslant x \leqslant a$, ou seja, $D(a) \subset [-a, a]$, isto implica que, $\forall\ a \in \mathbb{Z}^*$ existe um número finito de divisores de a.

1.1.5 Divisores Comuns de Dois Números Inteiros

Definição 3 *Dados $a,\ b \in \mathbb{Z}$, com um deles não nulo, diremos que o número $d \in \mathbb{Z}^*$ é um divisor comum de a e b se $d \mid a$ e $d \mid b$.*

Exemplo: Sejam 3 e $0 \in \mathbb{Z}$, temos $D(3) = \{-3,\ -1,\ 1,\ 3\}$ e $D(0)$ é formado por todos os números inteiros não nulos. No entanto, apenas os números $-3,\ -1,\ 1$ e 3 são divisores comuns de 3 e 0.

Sejam -4 e $12 \in \mathbb{Z}$, temos: $D(-4) = \{-4,\ -2,\ -1,\ 1,\ 2,\ 4\}$ e $D(12) = \{-12,\ -6,\ -4,\ -3,\ -2,\ -1,\ 1,\ 2,\ 3,\ 4,\ 6,\ 12\}$. No entanto, apenas os números $-4,\ -2,\ -1,\ 1,\ 2$ e 4 são divisores comuns de -4 e 12.

1.1.6 Máximo Divisor Comum

Definição 4 *Diremos que $d \in \mathbb{N}$ é o maior divisor comum, ou o máximo divisor comum (mdc), de a e b, em que um deles seja não nulo, se possuir as seguintes propriedades:*

i) *d é um divisor comum de a e b;*

ii) *d é divisível por todos divisores comuns de a e b.*

Exemplo: Temos que $D(12) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12\}$ e $D(8) = \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 8\}$ e que $(12, 8) = 4$, pois o conjunto dos divisores comuns de 12 e 8 são $\{\pm 1,\ \pm 2,\ \pm 4\}$ e tomando qualquer outro divisor comum deles irá dividir 4, ou seja, se $x \in \{\pm 1,\ \pm 2,\ \pm 4\}$, temos que $x \mid 4$.

Note que $-3,\ -1,\ 1$ e 3 são divisores comuns de 3 e 0, ou seja, todos estes números satisfazem a condição i).No entanto, apenas o 3 satisfaz as duas condições.

A condição (ii) pode ser escrita da seguinte forma: ii') Se c é um divisor comum de a e b, então $c \mid d$.

Portanto, se d é um mdc de a e b, e se c é um divisor comum desses dois números, então $c \leqslant d$. 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 d' são dois mdc de um mesmo par de números, então $d \leqslant d'$ e $d' \leqslant d$, e, consequentemente, $d = d'$. Isto é, há unicidade do mdc. O mdc de a e b será denotado por (a, b). Como o mdc de a e b não depende da ordem em que a e b são tomados, temos que $(a, b) = (b, a)$.

No Teorema 1.11 a frente mostraremos a existência do mdc de dois números a e b em que um dele é diferente de zero. Para tanto faremos algumas observações abaixo.

Agora vamos mostrar existência do mdc de dois a e b, em que um deles não seja nulo.

Como, por definição, a e b são números inteiros tais que $a \neq 0$ ou $b \neq 0$, temos:

(i) Se um deles for nulo: $(0, b) = |b|$ ou $(a, 0) = |a|$;

(ii) Se um deles for igual a 1: $(1, b) = 1$ ou $(a, 1) = 1$;

(iii) Se $a = b$: $(a, a) = |a|$;

(iv) Se $a \mid b$ então $a = (a, b)$. Reciprocamente, se $(a, b) = a$ então $a \mid b$.

Para provar a existência do máximo divisor comum de dois números, utilizaremos, essencialmente, o resultado abaixo.

Se $a < 0$ temos que $-a > 0$ e $-a \mid a$, pois existe $-1 \in \mathbb{Z}$, tal que $a = -a \cdot (-1)$. Reciprocamente, se $-a < 0$ temos que $a > 0$ e $a \mid -a$.

Da mesma forma podemos estender o Lema de Euclides apresentado.

Lema 1.10 *Se existir* $(a, b - n \cdot a)$, *então* (a, b) *existe e* $(a, b) = (a, b - n \cdot a)$, *para* $a, b, n \in \mathbb{Z}$.

Demonstração: Como $(a, b - n \cdot a) = d \in \mathbb{N}$, então $d \mid a$ e, com isso, $d \mid n \cdot a$; temos também que $d \mid b - n \cdot a$. Portanto, $d \mid b - n \cdot a + n \cdot a \Rightarrow d \mid b$. Supondo, agora, que c seja um divisor comum de a e de b; logo, $c \mid na$ e, com isso, $c \mid b - n \cdot a$. Dessa forma, $c \mid d$. Logo, $d = (a, b)$. $\square$ A existência do mdc de (a, b) para a e $b \in \mathbb{Z}$, em que $a \neq 0$ ou $b \neq 0$, dá-se da mesma forma:

(i) Se um deles for nulo: $(0, b) = b$, para $b > 0$ ou $(0, b) = -b$, para $b < 0$, sendo $b = 0$, $(a, 0) = a$, para $a > 0$ ou $(a, 0) = -a$, para $a < 0$;

(ii) Se um deles for igual a 1: $(1, b) = 1$ ou $(a, 1) = 1$;

(iii) Se $a = b$: $(a, a) = a$, para $a > 0$ ou $(a, a) = -a$, para $a < 0$;

(iv) Se $a \mid b$ então $(a, b) = a$, para $a > 0$ ou será $(a, b) = -a$, para $a < 0$. Temos que a é um divisor comum de a e de b, e, se c é um divisor comum de a e b, então $c \mid a$, o que nos mostra que $a = (a, b)$.

Reciprocamente, se $(a, b) = a$ então $a \mid b$.

Teorema 1.11 *Se a e b são dois inteiros em que um deles não é nulo ($a \neq 0$ ou $b \neq 0$), então existe e é único o mdc de a e b; além disso, existem inteiros x e y tais que: $(a, b) = a \cdot x + b \cdot y$, isto é, o mdc é uma combinação linear de a e b.*

Demonstração: Seja S o conjunto de todos os inteiros positivos da forma $a \cdot u + b \cdot v$, com $u, v \in \mathbb{Z}$, isto é: $S = \{a \cdot u + b \cdot v \mid a \cdot u + b \cdot v > 0 \text{ e } u, v, \mathbb{Z}\}$. Este conjunto S não é vazio, pois a ou b tem que ser diferente de zero, suponha que $a \neq 0$, então um dos inteiros: $a = a \cdot 1 + b \cdot 0$, se $a > 0$, ou $-a = a \cdot (-1) + b \cdot 0$, se $a < 0$ é positivo e pertence a S. Logo, pelo "Princípio da Boa Ordenação", existe e é único o elemento mínimo $d \in S$. E, consoante a definição de S, existem inteiros x e y tais que $d = a \cdot x + b \cdot y$. Posto isso, vamos mostrar que $d = (a, b)$. Com efeito, pelo algoritmo da divisão, temos: $a = d \cdot q + r$, com $0 \leqslant r \leqslant d$ o que dá

$r = a - d \cdot q = a - (a \cdot x + b \cdot y) \cdot q = a(1 - q \cdot x) + b \cdot (-q\dot{v})$, isto é, o resto r é uma combinação linear de a e de b. Com $0 \leqslant r \leqslant d$ e $d > 0$ é o elemento mínimo de S, segue-se que $r = 0$ e $a = d \cdot q$, ou seja, $d \mid a$. De maneira análoga, prova-se que também $d \mid b$. Portanto, d é um divisor comum positivo de a e de b. Suponha que c é um divisor comum positivo qualquer de a e de b, ou seja, $c \mid a$ e $c \mid b$, então

$c \mid (a \cdot x + b \cdot y)$ então $c \mid d$, isto é, d é o maior divisor comum positivo de a e b, ou seja, $(a, b) = d = a \cdot x + b \cdot y$, com $x, y \in \mathbb{Z}$. □

Observação 4 *Este teorema mostra que:*

(i) *(a, b) é o menor inteiro positivo, tal que $(a, b) = a \cdot x + b \cdot y$, isto é, o mdc de a e b pode ser escrito como combinação linear dos mesmos e que essa representação como combinação linear não é única, pois temos:*

$$(a, b) = d = a \cdot x + b \cdot y.$$

Assim

$$d = a \cdot x + a \cdot b \cdot t - a \cdot b \cdot t + b \cdot y.$$

Portanto

$$d = a \cdot (x + b \cdot t) + b \cdot (y - a \cdot t), \ \forall t \in \mathbb{Z}.$$

(ii) *Se $d = a \cdot r + b \cdot s$, para algum par de inteiros r e s, então d não é necessariamente o mdc de a e b. Assim, por exemplo, se:*

$$(a, b) = a \cdot x + b \cdot y,$$

ou seja,

$$t \cdot (a, b) = a \cdot t \cdot x + b \cdot t \cdot y, \ \forall t \in \mathbb{Z},$$

isto é,

$$d = a \cdot r + b \cdot s,$$

em que

$$d = t \cdot (a, b).$$

Portanto,

$$r = t \cdot x \ \ e \ \ s = t \cdot y.$$

Dessa forma, podemos concluir que $d \in \mathbb{Z}$, tal que $d = a \cdot x + b \cdot y$ não é necessariamente o mdc de a e b, entretanto, será um múltiplo de (a, b).

1.1.7 Algoritmo de Euclides

Aqui, traremos uma prova construtiva da existência do mdc de a e b, atribuído a Euclides em sua obra Elementos.
Dados $a, b \in \mathbb{N}$, podemos supor $a \leqslant b$. se $a = 1$ ou $a = b$, ou ainda $a \mid b$, já vimos que $(a, b) = a$. Suponhamos, então, que $1 < a < b$ e que $a \nmid b$. Logo, pela divisão euclidiana, podemos escrever $b = a \cdot q_1 + r_1$, com $r_1 < a$.

Temos duas possibilidades:

(i) $r_1 \mid a$, então, $r_1 = (a, r_1) = (a, b - q_1 \cdot a) = (a, b)$, (Lema 1.10);

(ii) $r_1 \nmid a$, e, em tal caso, podemos efetuar a divisão de a por r_1, obtendo $a = r_1 q_2 + r_2$, com $r_2 < r_1$.

Novamente, duas possibilidades:

i') $r_2 \mid r_1$ e, novamente, teríamos: $r_2 = (r_1, r_2) = (r_1, a - r_2 \cdot q_2) = (r_1, a) = (b - q_1 \cdot a, a) = (a, b - q_1 \cdot a) = (a, b)$, e paremos, pois termina o algoritmo, ou

ii') $r_2 \nmid r_1$, e, em tal caso, podemos efetuar a divisão de r_1 por r_2, obtendo $r_1 = r_2 \cdot q_3 + r_3$, com $r_3 < r_2$.

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > r_3 > \ldots$ o que contradiz o Principio da Boa Ordenação nos naturais. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$.

Exemplo: Vamos calcular $(372, 162)$.
$(162, 372) = (162, 372 - 2 \cdot 162) = (162, 48) = (48, 162) = (48, 162 - 48 \cdot 3) = (48, 18) = (18, 48) = (18, 48 - 18 \cdot 2) = (18, 12) = (12, 18) = (12, 18 - 12 \cdot 1) = (12, 6) = (6, 12) = (6, 12 - 6 \cdot 2) = (6, 0) = 6$

1.1.8 Propriedades do mdc

Sejam $a, b \in \mathbb{Z}_+$, em que um deles seja diferente de zero. Definimos o conjunto $J(a,b) = \{x \in \mathbb{Z}_+^*; \exists\ u, v \in \mathbb{Z}_+, x = u \cdot a - v \cdot b\}$ e $J(b,a) = \{y \in \mathbb{Z}_+^*; \exists\ u, v \in \mathbb{Z}_+, y = v \cdot b - u \cdot a\}$.

Lema 1.12 *Tem-se que* $J(a,b) = J(b,a) \neq \emptyset$.

Demonstração: Inicialmente, mostraremos que os dois conjuntos são iguais. Basta mostrar que $J(a,b) \subset J(b,a)$. Seja $x \in J(a,b)$, então $x = u \cdot a - v \cdot b$, com $u, v \in \mathbb{Z}$. Dessa forma, existem $\lambda, \theta \in \mathbb{Z}_+^*$, tais que $\lambda \cdot a > v$ e $\theta \cdot b > u$. Tomando $\rho = max\{\lambda, \theta\}$, tem-se que $\rho \cdot a > v$ e $\rho \cdot b > u$. Dessa forma,

$$x = u \cdot a - v \cdot b.$$

Somando e subtraindo $\rho \cdot a \cdot b$, temos

$$x = u \cdot a - \rho \cdot a \cdot b + \rho \cdot a \cdot b - v \cdot b.$$

Assim,

$$x = -a \cdot (\rho \cdot b - u) + b \cdot (\rho \cdot a - v)$$

e, portanto,

$$x = b \cdot (\rho \cdot a - v) - a \cdot (\rho \cdot b - u) \in J(b,a).$$

Note que $a \in J(a,b)$, pois basta tomar $v = 0$ e $u = 1$ teremos $x = u \cdot a - b \cdot v = a$, portanto $J(a,b) \neq \emptyset$. □

Teorema 1.13 *Sejam* $a, b \in \mathbb{Z}_+^*$, *e seja* $d = minJ(a,b)$. *Tem-se que:*

i) $d = (a,b)$;

ii) $J(a,b) = \{n \cdot d; n \in \mathbb{Z}_+^*\}$.

Demonstração: (i) Suponha que c divida a e b; logo, $c \mid u \cdot a$ e $c \mid v \cdot b$, ou seja, $c \mid a \cdot u - b \cdot b$. Dessa forma, $c \mid x$, para todo $x \in J(a,b)$ e, consequentemente, $c \mid d$. Suponha, por absurdo, que $d \nmid x$. Portanto, pela divisão Euclidiana $x = d \cdot q + r$, em que $0 \leqslant r < d$. Como $x = a \cdot u - b \cdot v$ e $x = d \cdot q + r$, temos que $d \cdot q + r = a \cdot u - b \cdot v$, ou seja, $r = a \cdot u - b \cdot v - d \cdot q$. Temos que $d \in J(a,b)$, ou seja, $d = b \cdot m - a \cdot n$, para algum $m, n \in \mathbb{Z}_+^*$. Portanto:

$$r = a \cdot u - b \cdot v - b \cdot m \cdot q + a \cdot n \cdot q.$$

Assim, temos

$$r = a \cdot u + a \cdot n \cdot q - b \cdot v - b \cdot m \cdot q.$$

Dessa forma

$$r = a \cdot (u + n \cdot q) - b \cdot (v + q \cdot m),$$

ou seja, $r \in J(a,b)$, o que é um absurdo, pois $d = minJ(a,b)$ e $r < d$. Em particular $d \mid a$ e $d \mid b$.

(ii) Dado que $l \cdot d = l \cdot (n \cdot a - m \cdot b) = (l \cdot n) \cdot a - (l \cdot m) \cdot b \in J(a,b)$ é claro que $\{l \cdot d; l \in \mathbb{Z}_+^*\} \subset J(a,b)$. Por outro lado, já provamos que todo $x \in J(a,b)$ é tal que $d \mid x$, e, portanto, $J(a,b) \subset \{l \cdot d; l \in \mathbb{Z}_+^*\}$ □

Corolário 1.13.1 *Quaisquer que sejam* $a, b, n \in \mathbb{Z}_+^*$, $(n \cdot a, n \cdot b) = n \cdot (a,b)$.

Demonstração: Note que $J(n \cdot a, n \cdot b) = n \cdot J(a,b) = \{n \cdot x; x \in J(a,b)\}$. Como $d = (a,b) = minJ(a,b)$, temos que $n \cdot (a,b) = min\ [n \cdot J(a,b)] = min\ J(n \cdot a, n \cdot b) \ni (n \cdot a, n \cdot b)$, ou seja, $n \cdot (a,b) = (n \cdot a, n \cdot b)$. □

Corolário 1.13.2 *Dados* $a, b \in \mathbb{Z}_+^*$, *tem-se que* $\left(\frac{a}{(a,b)} \frac{b}{(a,b)}\right) = 1$.

Demonstração: Pelo Corolário 1.2, temos

$$(a,b) \cdot \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \left((a,b) \cdot \frac{a}{(a,b)}, (a,b) \cdot \frac{b}{(a,b)}\right) = (a,b).$$

□

Definição 5 *Dois números naturais* a *e* b *serão ditos primos entre si, ou coprimos, se* $(a,b) = 1$*; ou seja, se o único divisor comum positivo de ambos é o número* 1.

Proposição 1.14 *Dois números naturais* a *e* b *são primos entre si se, e somente se, existem números naturais* n *e* m *tais que* $m \cdot a - n \cdot b = 1$.

Demonstração: Suponha que $(a,b) = 1$. Dessa forma, pelo teorema temos que existem números naturais m e n, tais que $m \cdot a - n \cdot b = (a,b) = 1$. Reciprocamente, suponha que existam números naturais m e n tais que $m \cdot a - n \cdot b = 1$. Se $d = (a,b)$, temos que $d \mid (m \cdot a - n \cdot b)$, o que mostra que $d \mid 1$, e, portanto, $d = 1$. □

Teorema 1.15 *Sejam* $a, b, c \in \mathbb{Z}_+^*$. *Se* $a \mid b \cdot c$ *e* $(a,b) = 1$, *então* $a \mid c$.

Demonstração: Se $a \mid b \cdot c$, então existe $e \in \mathbb{Z}$, tal que $b \cdot c = a \cdot e$. Se $(a,b) = 1$, então existem $m, n \in \mathbb{Z}_+^*$, tal que $m \cdot a - n \cdot b = 1$. Multiplicando os dois membros por c temos

$$m \cdot a \cdot c - n \cdot b \cdot c = c.$$

Como $b \cdot c = a \cdot e$, podemos fazer

$$m \cdot a \cdot c - n \cdot a \cdot e = c,$$

ou seja,

$$a \cdot (m \cdot c - n \cdot e) = c.$$

Portanto, $a \mid c$. □

Corolário 1.15.1 *Dados $a \in \mathbb{Z}$ e $b, c \in \mathbb{Z}^*$, temos que $b \mid a$ e $c \mid a$ se, e somente se, $\dfrac{b \cdot c}{(b,c)} \mid a$.*

Demonstração: Sejam $a \in \mathbb{Z}$ e $b, c \in \mathbb{Z}^*$. Suponhamos que $b \mid a$ e $c \mid a$, deste modo existem $q_1,\ q_2 \in \mathbb{Z}$, tais que $a = b \cdot q_1$ e $a = c \cdot q_2$. Além disso, $(b,c) \mid b$ e $(b,c) \mid c$.

Sendo assim, $\dfrac{a}{(b,c)} = \dfrac{b}{(b,c)} \cdot q_1$ e $\dfrac{a}{(b,c)} = \dfrac{c}{(b,c)} \cdot q_2$, ou seja, $\dfrac{b}{(b,c)} \cdot q_1 = \dfrac{c}{(b,c)} \cdot q_2$. Pelo Corolário 1.13.2, $\left(\dfrac{b}{(b,c)}, \dfrac{c}{(b,c)}\right) = 1$, logo $\dfrac{b}{(b,c)} \mid q_2$ e $\dfrac{c}{(b,c)} \mid q_1$ e, com isso, $c \cdot \dfrac{b}{(b,c)} \mid c \cdot q_2$ e $b \cdot \dfrac{c}{(b,c)} \mid b \cdot q_1$, ou seja, $\dfrac{c \cdot b}{(b,c)} \mid a$ e $\dfrac{b \cdot c}{(b,c)} \mid a$.

Portanto,

$$\frac{b \cdot c}{(b,c)} \mid a.$$

Suponhamos, agora, que $\dfrac{b \cdot c}{(b,c)} \mid a$, ou seja, existe $q_3 \in \mathbb{Z}$ tal que $a = \dfrac{b \cdot c}{(b,c)} \cdot q_3$, isto é, $a = b \cdot \left[\dfrac{c}{(b,c)} \cdot q_3\right]$. Sabemos que $\left[\dfrac{c}{(b,c)} \cdot q_3\right] = q \in \mathbb{Z}$, logo $a = b \cdot q$, ou seja, $b \mid a$.

De maneira análoga, podemos escrever $a = c \cdot \left[\dfrac{b}{(b,c)} \cdot q_3\right]$, assim, $a = c \cdot q'$, onde $\dfrac{b}{(b,c)} \cdot q_3 = q' \in \mathbb{Z}$, e portanto $c \mid a$. □

1.1.9 Mínimo Múltiplo Comum

Definição 6 *Diremos que um número $m \in \mathbb{N}$ é um mínimo múltiplo comum (mmc) de a e de b se possuir as seguintes propriedades:*

(i) *m é um múltiplo de a e de b ao mesmo tempo;*

(ii) *Se c é um múltiplo de a e de b, então $m \mid c$.*

Exemplo: Sabemos que 12 é um múltiplo comum de 2 e de 3, mas não é o mmc destes números, pois $6 \in \mathbb{N}$ também é múltiplo e $6 \mid 12$.

Se c é um múltiplo comum de a e b, então, do item (ii) da definição acima, temos que $m \mid c$. Portanto $m \leqslant c$, o que nos diz que o mínimo múltiplo comum, se existir, é único e é o menor dos múltiplos comuns de a e b. Denotaremos o mmc de a e b, da seguinte forma: $[a, b]$.

Proposição 1.16 *Dados dois números naturais a e b, temos que $[a, b]$ existe e*

$$[a, b] \cdot (a, b) = a \cdot b.$$

Demonstração: Suponha que $m = \dfrac{a \cdot b}{(a, b)}$. Logo, podemos escrever m das seguintes formas:

$$m = a \cdot \frac{b}{(a, b)} \text{ ou } m = b \cdot \frac{a}{(a, b)},$$

isto é:

$$m = a \cdot \frac{b}{(a, b)} = b \cdot \frac{a}{(a, b)}.$$

Assim, temos que $a \mid m$ e $b \mid m$, pois $\dfrac{a}{(a, b)}$ e $\dfrac{b}{(a, b)} \in \mathbb{Z}$. Seja c um múltiplo comum de a e b; logo, $c = n \cdot a = n' \cdot b$.
Segue daí que

$$n \cdot \frac{a}{(a, b)} = n' \cdot \frac{b}{(a, b)}.$$

Como $\left(\dfrac{a}{(a, b)}, \dfrac{b}{(a, b)}\right) = 1$, temos que $\dfrac{a}{(a, b)} \mid n'$. Assim obtemos $\dfrac{a \cdot b}{(a, b)} \mid n' \cdot b$, ou seja, $\dfrac{a \cdot b}{(a, b)} \mid c$. Logo $[a, b] = \dfrac{a \cdot b}{(a, b)}$ por definição de mmc.

□

Corolário 1.16.1 *Se a e $b \in \mathbb{Z}$, tal que $(a, b) = 1$, então $[a, b] = a \cdot b$.*

Demonstração: Temos que $[a, b] \cdot (a, b) = a \cdot b$ e que $(a, b) = 1$, logo, $[a, b] \cdot 1 = a \cdot b$, então $[a, b] = a \cdot b$. □

1.2 Equações Diofantinas Lineares

Generalidades

O tipo mais simples de equações diofantinas é a equação diofantina linear com duas incógnitas X e Y:

$$a \cdot X + b \cdot Y = c$$

Onde a, b e c são inteiros dados, sendo $a, b \neq 0$.

Todo par de inteiros X_0, Y_0 tais que $a \cdot X_0 + b \cdot Y_0 = c$ diz-se uma solução inteira ou apenas uma solução da equação $a \cdot X + b \cdot Y = c$.

Consideremos, por exemplo, a equação diofantina linear com duas incógnitas:

$$3 \cdot X + 6 \cdot Y = 18$$

Temos:

$3 \cdot 4 + 6 \cdot 1 = 18$
$3 \cdot (-6) + 6 \cdot 6 = 18$
$3 \cdot 10 + 6 \cdot (-2) = 18$

Logo, os pares de inteiros: 4 e 1, -6 e 6, 10 e -2 são soluções da equação $3 \cdot X + 6 \cdot Y = 18$.

Existem equações diofantinas lineares com duas incógnitas que não têm solução. Assim, por exemplo, a equação diofantina linear: $2 \cdot X + 4 \cdot Y = 7$ não tem solução, porque $2 \cdot X + 4 \cdot Y$ é um inteiro par para quaisquer que sejam os valores inteiros de X e Y, enquanto que 7 é um inteiro ímpar (observe-se que $2 = (2, 4)$ não divide 7).

De modo geral, a equação diofantina linear $a \cdot X + b \cdot Y = c$ não tem solução todas as vezes que $d = (a, b)$ não divide c.

Condição de Existência de Solução

Teorema 1.17 *A equação diofantina linear $a \cdot x + b \cdot Y = c$ tem solução se, e somente se, d divide c, sendo $d = (a, b)$.*

Demonstração: Suponha que a equação $a \cdot X + b \cdot Y = c$ tem uma solução, isto é, que existe um par de inteiros x_0 e y_0 tal que

$$a \cdot x_0 + by_0 = c.$$

Como $(a, b) = d$, existem inteiros q_1 e q_2 tais que $a = d \cdot q_1$ e $b = d \cdot q_2$, ou seja: $c = d \cdot q_1 \cdot x_0 + d \cdot q_2 \cdot y_0$. Podemos escrever da seguinte forma: $c = d \cdot (q_1 \cdot x_0 + q_2 \cdot y_0)$, isto é: $d \mid c$, pois existe q inteiro, tal que $(q_1 \cdot x_0 + q_2 \cdot y_0) = q$, ou seja, $c = d \cdot q$. Suponha que $(a, b) = d$ e que $d \mid c$, ou seja, $c = d \cdot q$, onde $q \in \mathbb{Z}$. Então, pelo resultado obtido, existem x_0 e $y_0 \in \mathbb{Z}$, tais que, $d = a \cdot x_0 + b \cdot y_0$ e, dessa forma, $c = d \cdot q$. Assim, substituindo d por $a \cdot x_0 + b \cdot y_0$, temos: $c = (a \cdot x_0 + b \cdot y_0) \cdot q$, ou seja, $c = a \cdot (x_0 \cdot q) + b \cdot (y_0 \cdot q)$, isto é,

$$X = x_0 \cdot q \text{ e } Y = y_0 \cdot q.$$

Como, $c = d \cdot q$, temos que $\dfrac{c}{d} = q$, ou seja,

$$X = x_0 \cdot \frac{c}{d} \text{ e } Y = y_0 \cdot \frac{c}{d},$$

logo é uma solução da equação

$$a \cdot X + b \cdot Y = c.$$

□

Teorema 1.18 *Se d divide c, sendo $d = (a, b)$ e se o par de inteiros x_0 e y_0 é uma solução particular da equação diofantina linear $a \cdot X + b \cdot Y = c$, então todas as outras soluções desta equação dadas pelas fórmulas:*

$$x = x_0 + \frac{b}{d} \cdot t \text{ e } y = y_0 - \frac{a}{d} \cdot t$$

onde t é um inteiro arbitrário.

Demonstração: Suponhamos que o par de inteiros x_0 e y_0 é uma solução particular da equação $a \cdot X + b \cdot Y = c$, e seja x e y uma outra solução qualquer desta equação. Então, temos:

$$c = a \cdot x + b \cdot y = a \cdot x_0 + b \cdot y_0,$$

ou seja,

$$a \cdot x - a \cdot x_0 = b \cdot y_0 - b \cdot y.$$

Assim, temos

$$a \cdot (x - x_0) = b \cdot (y_0 - y).$$

Como $(a, b) = d$, temos que existem $q_1,\ q_2 \in \mathbb{Z}$ tais que $a = d \cdot q_1$ e $b = d \cdot q_2$, com q_1 e q_2 primos entre si, isto é, $(q_1, q_2) = 1$. Substituindo estes valores de a e b na última igualdade, temos:

$$d \cdot q_1 \cdot (x - x_0) = d \cdot q_2 \cdot (y_0 - y),$$

dessa forma,

$$q_1 \cdot (x - x_0) = q_2 \cdot (y_0 - y).$$

Assim, como $q_1 \nmid q_2$, temos que $q_1 \mid (y_0 - y)$ e $q_2 \mid (x - x_0)$, isto é, existe $t \in \mathbb{Z}$ tal que:

$$y_0 - y = q_1 \cdot t \text{ e } x - x_0 = t \cdot q_2.$$

Dessa forma, temos:

$$x = x_0 + q_2 \cdot t \text{ e } y = y_0 - q_1 \cdot t,$$

e, como $q_1 = \dfrac{b}{d}$ e $q_2 = \dfrac{a}{d}$, podemos escrever esta última equação da seguinte forma:

$$x = x_0 + \frac{b}{d} \cdot t, \text{ e } y = y_0 - \frac{a}{d} \cdot t$$

Estes valores de x e y satisfazem realmente a equação $a \cdot X + b \cdot Y = c$, qualquer que seja o inteiro t, pois, temos:

$$a \cdot x + b \cdot y = a \cdot \left[x_0 + \frac{b}{d} \cdot t\right] + b \cdot \left[y_0 - \frac{a}{d} \cdot t\right],$$

assim, temos

$$a \cdot x + b \cdot y = a \cdot x_0 + \frac{a \cdot b}{d} \cdot t + b \cdot y_0 - \frac{b \cdot a}{d} \cdot t.$$

Assim, concluímos

$$a \cdot x_0 + b \cdot y_0 + \frac{a \cdot b}{d} \cdot t - \frac{b \cdot a}{d} \cdot t = c,$$

visto que $a \cdot x_0 + b \cdot y_0 = c$. □

Sendo assim, a equação diofantina linear $a \cdot x + b \cdot y = c$ admite infinitas soluções, uma para cada valor do inteiro arbitrário t.

Corolário 1.18.1 *Se $(a, b) = 1$ e se x_0 e y_0 é uma solução particular da equação diofantina linear $a \cdot X + b \cdot Y = c$, então todas as outras soluções desta equação são dadas pelas fórmulas:*

$$x = x_0 + b \cdot t \text{ e } y = y_0 - a \cdot t, \text{ onde } t \text{ é um inteiro arbitrário.}$$

Uma solução particular da equação diofantina linear se obtém por tentativas ou pelo algoritmo de Euclides. E em ambos os casos a solução geral se pode obter usando o Teorema 1.18, conforme se vai ver nos exemplos a seguir.

Exemplo: Determinar todas as soluções da equação diofantina linear

$$172 \cdot X + 20 \cdot Y = 1000.$$

Vamos encontrar $(172, 20)$ pelo algoritmo de EUCLIDES e verificar se $(172, 20) \mid 1000$.

	8	1	1	2
172	20	12	8	4
12	8	4	0	

Portanto, $(172, 20) = 4$ e como $4 \mid 1000$, segue-se que a equação dada tem solução. Temos que:

$$172 = 20 \cdot 8 + 12$$
$$20 = 12 + 8$$
$$12 = 8 + 4.$$

Isolando os restos, temos:

$$172 - 20 \cdot 8 = 12$$
$$20 - 12 = 8$$
$$-20 + 12 = -8$$
$$12 - 8 = 4.$$

Substituindo as duas primeiras equações na última, temos:

$$172 - 20 \cdot 8 - 20 + 12 = 4$$
$$172 - 20 \cdot 9 + 12 = 4.$$

Como $12 = 172 - 20 \cdot 8$, temos:

$$172 - 20 \cdot 9 + 172 - 20 \cdot 8 = 4$$
$$172 \cdot 2 - 20 \cdot 17 = 4$$
$$172 \cdot (2) + 20 \cdot (-17) = 4.$$

Multiplicando ambos os membros desta igualdade por

$$\frac{1000}{4} = 250.$$

Obtemos:

$$172 \cdot (2 \cdot 250) + 20 \cdot (-17 \cdot 250) = 4 \cdot 250$$

$$172 \cdot (500) + 20 \cot(-4250) = 1000.$$

Portanto, o par de inteiros $x_0 = 500$ e $y_0 = -4250$ é uma solução particular da equação proposta, e todas as outras soluções são dadas pelas fórmulas:

$$x = 500 + \frac{20}{4} \cdot t \text{ e } y = -4.250 - \frac{172}{4} \cdot t$$

ou seja,

$$x = 500 + 5 \cdot t \; e \; = -4250 - 43 \cdot t,$$

em que t é um inteiro arbitrário. **Exemplo:** Determinar todas as soluções inteiras positivas da equação diofantina linear.

$$18 \cdot X + 5 \cdot Y = 48$$

Note que $(18, 5) = 1$, pois 5 é primo e 18 não é um múltiplo de 5, e $(18, 5) \mid 48$, isto é, $18 \cdot X + 5 \cdot Y = 48$ tem solução.

	3	1	1	2
18	5	3	2	1
3	2	1	0	

Temos que:

$$18 = 5 \cdot 3 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1.$$

Isolando os restos, temos:

$$18 - 5 \cdot 3 = 3$$

$$5 - 3 = 2$$

$$3 - 2 = 1.$$

Substituindo a segunda equação na última, temos:

$$3 - 2 = 1$$

$$3 - 5 + 3 = 1$$

$$3 \cdot 2 - 5 = 1$$

Substituindo, agora, a primeira equação nesta última encontrada, temos:

$$(18 - 5 \cdot 3) \cdot 2 - 5 = 1$$

$$18 \cdot 2 - 5 \cdot 6 - 5 = 1$$

$$18 \cdot 2 - 5 \cdot 7 = 1$$

$$18 \cdot 2 + 5 \cdot (-7) = 1$$

Multiplicando esta última equação encontrada por 48, temos:

$$18 \cdot (2 \cdot 48) + 5 \cdot (-7 \cdot 48) = 48$$

$$18 \cdot (96) + 5 \cdot (-336) = 48.$$

Logo, o par de inteiros $x_0 = 96$ e $y_0 = -336$ é uma solução particular da equação proposta, e todas as demais soluções são dadas pela fórmulas:

$$x = 96 + 5 \cdot t, \;\; y = -336 - 18 \cdot t,$$

em que t é um inteiro arbitrário. As soluções inteiras e positivas se encontram escolhendo t de modo que sejam satisfeitas as desigualdades:

$$96 + 5 \cdot t > 0, \;\; -336 - 18 \cdot t > 0,$$

isto é,

$$t < -19 \cdot \frac{1}{5} \text{ e } t < -18 \cdot \frac{2}{3},$$

o que implica $t = -19$ e , portanto:

$$x = 96 + 5 \cdot (-19) = 1, \;\; y = -336 - 18 \cdot (-19) = 6.$$

Exemplo: Determine o menor inteiro positivo que tem restos 11 e 35 quando dividido, respectivamente, por 37 e 48.

Suponha que este inteiro seja A e que X e Y sejam os cocientes para as respectivas divisões. Dessa forma, teríamos:

$$A = 37 \cdot X + 11 \; e, \;\; A = 48 \cdot Y + 35.$$

Logo, teríamos a seguinte igualdade:

$$37 \cdot X + 11 = 48 \cdot Y + 35$$

$$37 \cdot X - 48 \cdot Y = 35 - 11$$

$$37 \cdot X - 48 \cdot Y = 24.$$

	1	3	2	1	3
48	37	11	4	3	1
11	4	3	1	0	

Temos que $(48, 37) = 1$ e como $1 \mid 24$, segue-se que a equação dada tem solução. Temos que

$$48 = 37 + 11$$

$$37 = 11 \cdot 3 + 4$$

$$11 = 4 \cdot 2 + 3$$

$$4 = 3 + 1$$

Isolando os restos temos

$$48 - 37 = 11$$

$$37 - 11 \cdot 3 = 4$$

$$11 - 4 \cdot 2 = 3$$

$$4 - 3 = 1.$$

Substituindo a terceira igualdade na última:

$$4 - 11 + 4 \cdot 2 = 1$$

$$4 \cdot 3 - 11 = 1.$$

Substituindo, agora, a segunda igualdade nesta última encontrada:

$$(37 - 11 \cdot 3) \cdot 3 - 11 = 1$$

$$37 \cdot 3 - 11 \cdot 9 - 11 = 1$$

$$37 \cdot 3 - 11 \cdot 10 = 1.$$

E substituindo a primeira nesta última, temos:

$$37 \cdot 3 - (48 - 37) \cdot 10 = 1$$

$$37 \cdot 3 - 48 \cdot 10 + 37 \cdot 10 = 1$$

$$37 \cdot (13) - 48 \cdot (10) = 1.$$

Multiplicando esta igualdade por 24, temos:

$$37 \cdot (13 \cdot 24) - 48 \cdot (10 \cdot 24) = 24$$

$$37 \cdot (312) - 48 \cdot (240) = 24.$$

Logo, $x_0 = 312$ e $y_0 = 240$ é uma solução particular da equação diofantina $37 \cdot X - 48 \cdot Y = 24$, como queremos $A \in \mathbb{Z}_+$, temos:

$$x = x_0 + b \cdot t \text{ e } y = y_0 + a \cdot t,$$

ou seja:

$$x = 312 + 48 \cdot t \text{ e } y = 240 + 37 \cdot t.$$

Para obter um $A \in \mathbb{Z}_+$, basta resolver as inequações, abaixo.

$$312 + 48 \cdot t > 0 \text{ e } 240 + 37 \cdot t > 0.$$

Ou seja,

$$48 \cdot t > -312$$
$$t > -\frac{312}{48},$$
$$t > -6\frac{24}{48}$$

e

$$240 + 37 \cdot t > 0$$
$$37 \cdot t > -240$$
$$t > -\frac{240}{37}$$
$$t > -6\frac{18}{37}$$

Logo $t \geqslant -5$. Mas, como queremos o menor valor para A, temos que tomar $t = -5$.

$$x = 312 + 48 \cdot (-5)$$
$$x = 312 - 240$$
$$x = 72$$
$$y = 240 + 37 \cdot (-5)$$
$$y = 240 - 185$$
$$y = 55.$$

Como A é dado por $A = 37 \cdot x + 11$ ou $A = 48 \cdot y + 35$, basta substituir em uma delas para encontrá-la. Se substituirmos na primeira:

$$A = 37 \cdot 72 + 11$$
$$A = 2664 + 11$$
$$A = 2675.$$

Se substituirmos na segunda:

$$A = 48 \cdot 55 + 35$$

$$A = 2640 + 35$$

$$A = 2675$$

Exemplo: De quantas maneiras podem-se comprar selos de 3 reais e de 5 reais de modo que se gastem 50 reais? Chamando de X a quantidade de selos que custa 3 reais e de Y a quantidade de selos que custa 5 reais, temos:

$$3 \cdot X + 5 \cdot Y = 50.$$

	1	1	2
5	3	2	1
2	1	0	

Portanto, $(5, 3) = 1$ e como $1 \mid 50$, segue-se que a equação dada tem solução.
Temos que:

$$5 = 3 + 2$$

$$3 = 2 + 1.$$

Isolando os restos temos:

$$5 - 3 = 2$$

$$3 - 2 = 1.$$

Substituindo a primeira equação na segunda, temos:

$$3 - 5 + 3 = 1$$

$$3 \cdot 2 + 5 \cdot (-1) = 1.$$

Multiplicando esta última equação por 50, temos:

$$3 \cdot (2 \cdot 50) + 5 \cdot (-1 \cdot 50) = 50$$

$$3 \cdot (100) + 5 \cdot (-50) = 50.$$

Logo, $x_0 = 100$ e $y_0 = -50$ é uma solução particular para a equação diofantina linear $3 \cdot X + 5 \cdot Y = 50$. No entanto, não podemos ter soluções negativas nesta questão. Portanto, teremos que encontrar uma outra solução que seja positiva, ou seja:

$$x = 100 - 5 \cdot t > 0 \qquad y = -50 + 3 \cdot t > 0$$
$$100 > 5 \cdot t \qquad 3 \cdot t > 50$$
$$\frac{100}{5} > t \qquad t > \frac{50}{3}$$
$$20 > t. \qquad t > 16\frac{2}{3}.$$

Dessa forma

$$17 \leqslant t < 20,$$

isto é,

$$t \in \{17,\ 18,\ 19\}.$$

Para $t = 17$, temos

$$x = 100 - 5 \cdot 17 \text{ e } y = -50 + 51.$$

Daí temos

$$x = 15 \text{ e } y = 1.$$

É uma solução que satisfaz a $3 \cdot x + 5 \cdot y = 50$, pois

$$3 \cdot 15 + 5 \cdot 1 = 50$$

$$45 + 5 = 50.$$

Para $t = 18$, temos

$$x = 100 - 5 \cdot 18 \text{ e } y = -50 + 3 \cdot 18 \; x = 100 - 90 \text{ e } y = -50 + 54 \; x = 10 \text{ e } y = 4.$$

É uma solução que satisfaz a $3 \cdot x + 5 \cdot y = 50$, pois $3 \cdot 10 + 5 \cdot 4 = 50$, logo $30 + 20 = 50$.
Para $t = 19$, temos

$$x = 100 - 5 \cdot 19 \text{ e } y = -50 + 3 \cdot 19 \; x = 100 - 95 \text{ e } y = -50 + 57 \; x = 5 \text{ e } y = 7.$$

É uma solução que satisfaz a $3 \cdot x + 5 \cdot y = 50$, pois $3 \cdot 5 + 5 \cdot 7 = 50$, logo $15 + 35 = 50$.

1.3 Congruências

Definição 7 *Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que a é congruente a b módulo m se, e somente se, m divide a diferença $a-b$. Em outros temos, a é congruente a b módulo m se, e somente se, existe um inteiro q tal que $a - b = q \cdot m$. Notação: $a \equiv b \ mod \ m$.*

Dessa forma, temos que $a \equiv b \; mod \; m$ se, e somente se, $m \mid (a-b)$, ou seja: $a \equiv b \; mod \; m$ se, e somente se, existir $q \in \mathbb{Z}$, tal que $a - b = q \cdot m$.
Exemplo: Note que $3 \equiv 24 \; mod \; 7$, pois $7 \mid (3-24)$, ou seja, $7 \mid -21$. De fato, pois $-3 \in \mathbb{Z}$ tal que $-21 = 7 \cdot (-3)$.

Se m não divide $a-b$, então diz-se que a é incongruente a b módulo m, que pela notação se escreve: $a \not\equiv b \; modo \; m$
Exemplo: Dados os números 25, 12 e 7, temos que $25 \not\equiv 12 \; mod \; 7$, pois $7 \nmid (25-12)$
Note que:

i Dados $a, \; b, \; 1 \in \mathbb{Z}$, temos que $a \equiv b \; mod \; 1$, para quaisquer a e b, pois 1 é divisor de todo e qualquer número;

ii Dados $a, \; b, \; 2 \in \mathbb{Z}$, temos que $a \equiv b \; mod \; 2$ se ambos forem pares ou se ambos forem ímpares, pois 2 é divisor de todos os números pares e qualquer número ímpar deixar resto 1 quando dividido por 2.

Exemplo: Mostraremos que $n \equiv 7 \; mod \; 12$ se, e somente se, $n \equiv 3 \; mod \; 4, \; \forall \; n \in \mathbb{Z}$
Usando a definição temos

$$n \equiv 3 \; mod \; 4, \text{ se, e somente se,} 4 \mid (n-3), \text{ ou seja, } (n-3) = 4 \cdot q_1.$$

Como $n \equiv 7 \; mod \; 12$, se, e somente se,$12 \mid (n-7)$, ou seja, $(n-7) = 12 \cdot q_2$. Podemos escrever da seguinte forma:

$$(n-3-4) = 12 \cdot q_2,$$

ou seja,

$$(n-3) - 4 = 12 \cdot q_2$$
$$(n-3) = 12 \cdot q_2 + 4$$
$$(n-3) = 4 \cdot (3 \cdot q_2 + 1),$$

fazendo $(3 \cdot q_2 + 1) = q \in \mathbb{Z}$ temos: $(n-3) = 4 \cdot q$.

Exemplo: Mostraremos que $n^2 \equiv 0 \; mod \; 4$ ou $n^2 \equiv 1 \; mod \; 4, \; \forall n \in \mathbb{Z}$.
Só existem duas possibilidades para n: ou n é par, ou n é ímpar. Portanto:

i) $n = 2 \cdot t$
$n^2 = 4 \cdot t^2$
$4 \mid 4 \cdot t^2, \; \forall \; t \in \mathbb{Z}.$

ii) $n = 2 \cdot t \pm 1$
$n^2 = 4 \cdot t^2 \pm 4 \cdot t + 1$
$n^2 = 4 \cdot (t^2 \pm t) + 1$
$n^2 \equiv 1 \; mod \; 4.$

Teorema 1.19 *Dois números inteiros a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.*

Demonstração: Por hipótese, $a \equiv b \; mod \; m$ se, e somente se, $m \mid (a-b)$, isto é, $a - b = m \cdot q$, onde $q \in \mathbb{Z}$.

Pelo algoritmo da divisão, temos que $b = m \cdot q_1 + r_1$, em que r_1 é o resto da divisão de b por m, isto é,

$$0 \leq r_1 < m$$

e $a = m \cdot q_2 + r_2$, em que r_2 é o resto da divisão de a por m, isto é,

$$0 \leq r_2 < m.$$

Como $a - b = m \cdot q$, temos que

$$m \mid [(m \cdot q_2 + r_2) - (m \cdot q_1 + r_1)]$$

$$m \mid [m \cdot q_2 - m \cdot q_1 + r_2 - r_1]$$

$$m \mid [m \cdot (q_2 - q_1) + (r_2 - r_1)].$$

Ou seja,

$$m \mid m \cdot (q_2 - q_1) \; e \; m \mid (r_2 - r_1)$$

. Como $0 \leq r_1 < m$ e $0 \leq r_2 < m$, então $r_2 - r_1 < m$ e, ainda, $|r_2 - r_1| < m$. Portanto só há uma forma para que $m \mid (r_2 - r_1)$ que é quando $r_2 - r_1 = 0$, ou seja, $r_2 = r_1$. Suponha que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever: $a = m \cdot q_1 + r$ e $b = m \cdot q_2 + r$, com $0 \leqslant r < m$ e, portanto:

$$a - b = m \cdot q_1 + r - (m \cdot q_2 + r)$$

$$a - b = m \cdot q_1 + r - m \cdot q_2 - r$$

$$a - b = m \cdot q_1 - m \cdot q_2 + r - r$$

$$a - b = m \cdot (q_1 - q_2),$$

ou seja,

$$m \mid a - b.$$

Logo,

$$a \equiv b \; mod \; m.$$

□

Exemplo: Sejam os inteiros -56 e -11. Pelo algoritmo da divisão, temos:

$-56 = 9 \cdot (-7) + 7$ e $-11 = 9 \cdot (-2) + 7$, isto é, -56 e -11 quando divididos por 9 deixam o mesmo resto que é 7. Logo, pelo teorema 1.8: $-56 \equiv -11 \; mod \; 9$.

Exemplo: Sejam, agora, os inteiros -31 e 11. Temos a congruência $-31 \equiv 11 \ mod \ 7$ de modo que, pelo teorema 1.8 e pela definição de congruência, -31 e 11 quando divididos por 7 deixam o mesmo resto. De fato temos que:

$$-31 = 7 \cdot (-5) + 4 \ e \ 11 = 7 \cdot 1 + 4.$$

1.3.1 Propriedades das Congruências

Teorema 1.20 *Seja m um inteiro positivo fixo maior que zero e sejam a, b e c inteiros quaisquer. Subsistem as seguintes propriedades:*

(i) *$a \equiv a \ mod \ m$ (Reflexiva);*

(ii) *Se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$ (Simétrica);*

(iii) *Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$ (Transitiva).*

Demonstração: (i) Como $m \neq 0$, temos que $m \mid 0$, isto é, $m \mid a - a$ que, por sua vez significa, $a \equiv a \ mod \ m$.

(ii) Se $a \equiv b \ mod \ m$, então existe $q \in \mathbb{Z}$ tal que $a - b = q \cdot m$. Multiplicando a equação por -1, temos

$$-(a - b) = -q \cdot m$$
$$-a + b = (-q) \cdot m$$
$$b - a = (-q) \cdot m,$$

isto é,

$$b \equiv a \ mod \ m.$$

(iii) Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então existem q_1 e $q_2 \in \mathbb{Z}$, tais que:

$$a - b = q_1 \cdot m \ e \ b - c = q_2 \cdot m.$$

Somando membro a membro das duas equações, temos:

$$(a - b) + (b - c) = q_1 \cdot m + q_2 \cdot m$$
$$a - b + b - c = (q_1 + q_2) \cdot m$$
$$a - c = q \cdot m,$$

isto é,

$$a \equiv c \ mod \ ml.$$

□

Observação 5 *Pelo fato de que a relação apresentada ser reflexiva, simétrica e transitiva, temos que $a \equiv b$ mode m, nos inteiros, é uma relação de equivalência, denominada de congruência módulo m.*

Teorema 1.21 *Seja m um inteiro positivo fixo maior que 0 e sejam a e b dois inteiros quaisquer. Valem as seguintes propriedades:*

(1) *Se $a \equiv b \ mod \ m$ e se $n \mid m$, com $n > 0$, então $a \equiv b \ mod \ n$;*

(2) *Se $a \equiv b \ mod \ m$ e se $c > 0$, então $a \cdot c \equiv b \cdot c \ mod \ m \cdot c$;*

(3) *Se $a \equiv b \ mod \ m$ e se a, b, m são todos divisíveis pelo inteiro $d > 0$, então $\frac{a}{d} \equiv \frac{b}{d} \ mod \ \frac{m}{d}$.*

Demonstração: (1) Por hipóteses temos que $a \equiv b \ mod \ m$ e $n \mid m$, ou seja, $a - b = q_1 \cdot m$ e $m = q_2 \cdot n$, em que q_1 e $q_2 \in \mathbb{Z}^*$. Dessa forma, substituindo a segunda equação na primeira, temos

$$a - b = q_1 \cdot (q_2 \cdot n)$$

$$a - b = (q_1 \cdot q_2) \cdot n.$$

Como existe $q \in \mathbb{Z}$ tal que $q = q_1 \cdot q_2$, temos que $a - b = q \cdot n$, isto é, $a \equiv b \ mod \ n$.
(2) Temos que $a \equiv b \ mod \ m$, ou seja, $a - b = q \cdot m$.
Multiplicando tudo por c, obtemos

$$c \cdot (a - b) = c \cdot q \cdot m$$

$$a \cdot c - b \cdot c = q \cdot (c \cdot m).$$

Portanto,

$$a \cdot c \equiv b \cdot c \ mod \ m \cdot c.$$

(3) Temos que $a \equiv b \ mod \ m$, isto é, $a - b = q \cdot m$ e que $d \mid a$, $d \mid b$ e $d \mid m$, temos:

$$\frac{(a-b)}{d} = q \cdot \frac{m}{d}$$

$$\frac{a}{d} - \frac{b}{d} = q \cdot \frac{m}{d}$$

$$\frac{a}{d} \equiv \frac{b}{d} \ mod \ \frac{m}{d}.$$

□

Exemplo: Temos que $-15 \equiv 9 \ mod \ 8$ e $4 \mid 8$, logo, temos que $-15 \equiv 9 \ mod \ 4$;
Temos que $7 \equiv -8 \ mod \ 3$, então, $7 \cdot 5 \equiv -8 \cdot 5 \ mod \ 3 \cdot 5$, ou seja, $35 \equiv -40 \ mod \ 15$;
Temos que $36 \equiv -24 \ mod \ 12$ e como $4 \mid 36$, $4 \mid 24$ e $4 \mid 12$, podemos concluir que $9 \equiv -6 \ mod \ 3$.

Teorema 1.22 *Seja m um inteiro positivo fixo maior que zero e seja a, b, c, d inteiros quaisquer. Subsistem as seguintes propriedades:*

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

(ii) *Se $a \equiv b \ mod \ m$, então $a + c \equiv b + c \ mod \ m$;*

(iii) *Se $a \equiv b \ mod \ m$ então $a^n \equiv b^n \ mod \ m$ para todo inteiro positivo n.*

Demonstração: (i) Temos que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, dessa forma existem q_1 e $q_2 \in \mathbb{Z}$ tais que $a - b = q_1 \cdot m$ e $c - d = q_2 \cdot m$. Se somarmos as duas equações membro a membro, teremos

$$(a - b) + (c - d) = q_1 \cdot m + q_2 \cdot m$$

$$(a + c) - (b + d) = (q_1 + q_2) \cdot m.$$

Como

$$(q_1 + q_2)) \ni \mathbb{Z},$$

temos que existe um

$$(q_1 + q_2) = q \in \mathbb{Z},$$

ou seja,

$$(a + c) - (b + d) = q \cdot m.$$

Portanto,

$$a + c \equiv b + d \ mod \ m.$$

Note, agora, que

$$a \cdot c - b \cdot d = a \cdot c - a \cdot d + a \cdot d - b \cdot d = a \cdot (c - d) + d \cdot (a - b).$$

Como

$$m \mid (c - d) \ e \ m \mid (a - b),$$

temos que

$$m \mid a \cdot (c - d) \ e \ m \mid d \cdot (a - b),$$

ou seja,

$$m \mid a \cdot (c - d) + d \cdot (a - b)$$

$$m \mid a \cdot c - a \cdot d + a \cdot d - b \cdot d$$

$$m \mid a \cdot c - b \cdot d.$$

Portanto

$$a \cdot c \equiv b \cdot d \ mod \ m.$$

(ii) Temos que

$$a \equiv b \ mod \ m,$$

ou seja,

$$a - b = m \cdot q_1, \ com \ q_1 \in \mathbb{Z}.$$

Basta agora multiplicar a equação por $c \in \mathbb{Z}$, ou seja,

$$(a - b) \cdot c = m \cdot q_1 \cdot c$$

$$a \cdot c - b \cdot c = m \cdot (q_1 \cdot c)$$

$$a \cdot c - b \cdot c = m \cdot q, \text{ em que } q = (q_1 \cdot c) \in \mathbb{Z}.$$

Dessa forma, temos que

$$a \cdot c \equiv b \cdot c \ mod \ m$$

. (iii) Vamos utilizar indução matemática para provar este item.

Note que $a^n \equiv b^n \ mod \ m$, será verdade para $n = 1$, pois $a \equiv b \ mod \ m$ é verdade. Suponha, agora, que $a^n \equiv b^n \ mod \ m$ seja verdade para $n \in \mathbb{Z}_+$ e vamos provar que será verdade para $n + 1$. Temos, por hipótese, que $a^n \equiv b^n \ mod \ m$ e $a \equiv b \ mod \ m$ são verdadeiras. Então, pelo item (i), temos que $a^n \cdot a \equiv b^n \cdot b \ mod \ m$ também é verdade, ou seja, $a^{n+1} \equiv b^{n+1} \ mod \ m$ é verdadeira. □

Exemplo:

(i) Como $12 \equiv 22 \ mod \ 5$ e $8 \equiv 13 \ mod \ 5$, então, $12 + 8 \equiv 22 + 13 \ mod \ 5$, ou seja, $20 \equiv 35 \ mod \ 5$. Temos também que: $12 \cdot 8 \equiv 22 \cdot 13 \ mod \ 5$, ou seja, $96 \equiv 286 \ mod \ 5$.

(ii) Temos que $12 \equiv 5 \ mod \ 7$ o que implica em $12 + 6 \equiv 5 + 6 \ mod \ 7$, ou seja, $18 \equiv 11 \ mod \ 7$. Temos, também, que $12 \cdot (-9) \equiv 5 \cdot (-9) \ mod \ 7$, isto é, $-108 \equiv -45 \ mod \ 7$.

(iii) Se $-5 \equiv 2 \ mod \ 7$, temos que $(-5)^3 \equiv (2)^3$, ou seja, $-125 \equiv 8 \ mod \ 7$.

Teorema 1.23 *Se* $a \cdot c \equiv b \cdot c \ mod \ m$ *e se* $(c, m) = d$, *então* $a \equiv b \ mod \ \frac{m}{d}$.

Demonstração: Como $(c, m) = d$, então existem q_1 e $q_2 \in \mathbb{Z}$ tais que

$$c = d \cdot q_1 \ e \ m = d \cdot q_2,$$

com $(q_1, q_2) = 1$. Temos também que se $a \cdot c \equiv b \cdot c \ mod \ m$, então $a \cdot c - b \cdot c = m \cdot q$. Dessa forma

$$a \cdot c - b \cdot c = m \cdot q$$

$$c \cdot (a - b) = m \cdot q$$

$$d \cdot q_1 \cdot (a - b) = d \cdot q_2 \cdot q$$

Dividindo ambos os membros desta última igualdade por d temos

$$q_1 \cdot (a - b) = q_2 \cdot q.$$

Note que $q_1 \nmid q_2$, pois $(q_1, q_2) = 1$. Dessa forma $q_2 \mid (a - b)$, ou seja, $a \equiv b \ mod \ q_2$
Temos que $m = q_2 \cdot d$, ou seja, $q_2 = \dfrac{m}{d}$. Logo $a \equiv b \ mod \ q_2$ e, portanto,

$$a \equiv b \ mod \ \frac{m}{d}$$

□

Corolário 1.23.1 *Se $a \cdot c \equiv b \cdot c \ mod \ m$ e $(c, m) = 1$, então $a \equiv b \ mod \ m$.*

Demonstração: Por hipótese temos que $a \cdot c \equiv b \cdot c \ mod \ m \Rightarrow a \cdot c - b \cdot c = m \cdot q \Rightarrow c \cdot (a - b) = m \cdot q$.
Como $m \nmid c$, temos que $m \mid (a - b)$, ou seja, $(a - b) = m \cdot q_1 \Rightarrow a \equiv b \ mod \ m$. □

Corolário 1.23.2 *Se $a \cdot c \equiv b \cdot c \ mod \ p$, com p primo, e se $p \nmid c$, então $a \equiv b \ mod \ p$.*

Demonstração: Como $p \nmid c$, isto é, $(p, c) = 1$. O resultado segue do corolário anterior. □

Exemplo: Se $33 \equiv 15 \ mod \ 9$, podemos escrever da seguinte forma: $3 \cdot 11 \equiv 3 \cdot 5 \ mod \ 9$.
Como $(9, 3) = 3$, temos que $11 \equiv 5 \ mod \ 9$. Se $-35 \equiv 45 \ mod \ 8$, podemos escrever da seguinte forma: $5 \cdot (-7) \equiv 5 \cdot 9 \ mod \ 8$.
Como $(5, 8) = 1$, temos que $-7 \equiv 9 \ mod \ 8$.

Observação 6 *No que $4 \cdot 11 \equiv 4 \cdot 15 \ mod \ 8$, mas não é verdade que $11 \equiv 15 \ mod \ 8$, pois $(4, 8) = 4 \neq 1$. No entanto $11 \equiv 15 \ mod \ 2$.*

1.3.2 Algumas Regras de Divisibilidade

Como no sistema decimal, todo número é representado por uma sequência formada pelos algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9, acrescidos dos símbolos 0, que representa a ausência de algarismo. Dessa forma, podemos escrever um número n da seguinte maneira:

$$n = a_k a_{k-1} a_{k-2} \ldots a_3 a_2 a_1 a_0,$$

em que $a_i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$, com i variando entre $k, k-1, \ldots, 1, 0$, podemos representar n também da seguinte forma:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0.$$

Com isso, vamos mostrar algumas regras de divisibilidade.
Divisibilidade por 2

Temos que

$$\begin{aligned} 10^0 &\equiv 1 \ mod\ 2 \\ 10^1 &\equiv 0 \ mod\ 2 \\ 10^2 &\equiv 0 \ mod\ 2 \\ \vdots &\equiv \vdots \end{aligned}$$

Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, temos:

$$\begin{aligned} a_0 \cdot 10^0 &\equiv a_0 \cdot 1 \ mod\ 2 \\ a_1 \cdot 10^1 &\equiv a_1 \cdot 0 \ mod\ 2 \\ a_2 \cdot 10^2 &\equiv a_2 \cdot 0 \ mod\ 2 \\ \vdots &\equiv \vdots \end{aligned}$$

Pelo Teorema 1.22, temos $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_0\ mod\ 2$, isto é, n só será divisível por 2, se, e somente se, $2 \mid a_0$.
Divisibilidade por 3

Temos que

$$\begin{aligned} 10^0 &\equiv 1 \ mod\ 3 \\ 10^1 &\equiv 1 \ mod\ 3 \\ 10^2 &\equiv 1 \ mod\ 3 \\ 10^3 &\equiv 1 \ mod\ 3 \\ \vdots &\equiv \vdots \end{aligned}$$

Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, temos

$$\begin{aligned} a_0 \cdot 10^0 &\equiv a_0 \cdot 1 \ mod\ 3 \\ a_1 \cdot 10^1 &\equiv a_1 \cdot 1 \ mod\ 3 \\ a_2 \cdot 10^2 &\equiv a_2 \cdot 1 \ mod\ 3 \\ a_3 \cdot 10^3 &\equiv a_3 \cdot 1 \ mod\ 3 \\ \vdots &\equiv \vdots \end{aligned}$$

Pelo Teorema 1.22, temos: $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_0 + a_1 + a_2 + a_3 + \ldots + a_k \ mod\ 3$, isto é, n só será divisível por 3, se, e somente se, $3 \mid a_0 + a_1 + a_2 + a_3 + \ldots + a_k$.

Divisibilidade por 4

Temos que

$$\begin{gathered} 10^0 \equiv 1 \ mod\ 4 \\ 10^1 \equiv 2 \ mod\ 4 \\ 10^2 \equiv 0 \ mod\ 4 \\ 10^3 \equiv 0 \ mod\ 4 \\ \vdots \equiv \vdots \end{gathered}$$

Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, temos

$$\begin{gathered} a_0 \cdot 10^0 \equiv a_0 \cdot 1 \ mod\ 4 \\ a_1 \cdot 10^1 \equiv a_1 \cdot 2 \ mod\ 4 \\ a_2 \cdot 10^2 \equiv a_2 \cdot 0 \ mod\ 4 \\ a_3 \cdot 10^3 \equiv a_3 \cdot 0 \ mod\ 4 \\ \vdots \equiv \vdots \end{gathered}$$

Pelo Teorema 1.22, temos: $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_0 + 2 \cdot a_1 \ mod\ 4$, isto é, n só será divisível por 4, se, e somente se, $4 \mid a_0 + 2 \cdot a_1$.

Divisibilidade por 5

Temos que

$$\begin{gathered} 10^0 \equiv 1 \ mod\ 5 \\ 10^1 \equiv 0 \ mod\ 5 \\ 10^2 \equiv 0 \ mod\ 5 \\ 10^3 \equiv 0 \ mod\ 5 \\ \vdots \equiv \vdots \end{gathered}$$

Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, temos

$$\begin{gathered} a_0 \cdot 10^0 \equiv a_0 \cdot 1 \ mod\ 5 \\ a_1 \cdot 10^1 \equiv a_1 \cdot 0 \ mod\ 5 \\ a_2 \cdot 10^2 \equiv a_2 \cdot 0 \ mod\ 5 \\ a_3 \cdot 10^3 \equiv a_3 \cdot 0 \ mod\ 5 \\ \vdots \equiv \vdots \end{gathered}$$

Pelo Teorema 1.22, temos: $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_0 \ mod\ 5$, isto é, n só será divisível por 5, se, e somente se, $5 \mid a_0$.

Divisibilidade por 6

Temos que

$$\begin{aligned} 10^0 &\equiv 1 \ mod\ 6 \\ 10^1 &\equiv 4 \ mod\ 6 \\ 10^2 &\equiv 4 \ mod\ 6 \\ 10^3 &\equiv 4 \ mod\ 6 \\ \vdots &\equiv \vdots \end{aligned}$$

Como $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$, temos

$$\begin{aligned} a_0 \cdot 10^0 &\equiv a_0 \cdot 1 \ mod\ 6 \\ a_1 \cdot 10^1 &\equiv a_1 \cdot 4 \ mod\ 6 \\ a_2 \cdot 10^2 &\equiv a_2 \cdot 4 \ mod\ 6 \\ a_3 \cdot 10^3 &\equiv a_3 \cdot 4 \ mod\ 6 \\ \vdots &\equiv \vdots \end{aligned}$$

Pelo Teorema 1.22, temos: $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + a_{k-2} \cdot 10^{k-2} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \equiv a_0 + 4 \cdot a_1 + 4 \cdot a_2 + \ldots + 4 \cdot a_k \ mod\ 6$, que podemos escrever, $n \equiv -3 \cdot a_0 + 4 \cdot a_0 + 4 \cdot a_1 + 4 \cdot a_3 + \ldots + 4 \cdot a_k \ mod\ 6$. Assim, temos que $n \equiv -3 \cdot a_0 + 4 \cdot (a_0 + a_1 + a_3 + \ldots + a_k) \ mod\ 6$, isto é, n só será divisível por 6, se, e somente se, $6 \mid -3 \cdot a_0$ e $6 \mid 4 \cdot (a_0 + a_1 + a_3 + \ldots + a_k)$. Dessa forma, $2 \mid -a_0$ e $3 \mid 2 \cdot (a_0 + a_1 + a_3 + \ldots + a_k)$, ou seja, $-a_0$ tem que ser par e $3 \mid (a_0 + a_1 + a_3 + \ldots + a_k)$.

O leitor interessado pode consultar mais detalhes em [1] e [3].

Capítulo 2

Aritmética no Ensino Fundamental

Neste capítulo apresentaremos um pouco da experiência em sala de aula aplicada a uma turma de estudantes do Ensino Fundamental, da escola E.E.E.F.M.J.J.C., formada especialmente para a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP). Estas aulas envolveram todos os conteúdos apresentados no Capítulo 1: Divisibilidade, Máximo Divisor Comum (MDC), Mínimo Múltiplo Comum (MMC), Equações Diofantinas e Congruência Modular. Dois destes conteúdos, Equações Diofantinas e Congruência Modular, não estão contemplados na grade curricular do Ensino Básico de acordo com os Parâmetros Curriculares Nacionais (PCN). Citaremos também algumas barreiras ou dificuldades enfrentadas.

2.1 A Aritmética e o PCN

Para o PCN, a Aritmética, ramo da matemática que lida com números e as operações possíveis entre eles, tem como objetivo fazer com que o aluno venha a: "resolver situações-problemas, sabendo validar estratégias e resultados, desenvolvendo formas de raciocínio e de processos, como dedução, indução, intuição, analogia, estimativa, e utilizando conceitos e procedimentos matemáticos, bem como instrumentos tecnológicos disponíveis"[2]. Dessa forma, o assunto de congruência, que não é contemplado no PCN, foi ministrado voltado para a resolução de questões envolvendo divisão, para encontrar o resto da divisão de números com 3 ou mais algarismos, e para criar regras de divisibilidade, ou seja, para resolver situações-problemas usando estratégias e desenvolvendo formas de raciocínio lógico como mencionado no próprio PCN.

2.2 A Aritmética e a OBMEP

O conteúdo de Aritmética é estudado inicialmente no conjunto dos naturais e logo em seguida no conjunto dos inteiros. Visando resolver problemas que se assemelham com os apresentados em edições anteriores da OBMEP, o nosso objetivo é fazer com que o aluno aprenda as operações com os números inteiros e, posteriormente, resolver problemas que os envolvam como, também, fazer com que os alunos construam regras de divisibilidade e saibam calcular restos de números com três ou mais algarismos sem precisar efetuar a divisão, usando apenas congruências.

2.3 O Desenvolvimento do Trabalho

O trabalho foi executado durante cinco semanas, com duas aulas semanais nas quintas-feiras e sextas-feiras, tendo cada aula uma duração de três horas, das oito horas até às 11 horas, em uma escola estadual de João Pessoa, Paraíba. O convite para a realização de tal projeto foi feito de sala em sala, no período da tarde, do 7º ano ao 9º ano.

Os estudantes envolvidos cursavam o 7^o, 8^o ou 9^o ano alguns fora da faixa etária. Pude também perceber alunos com potencial para o estudo na área de exatas.

A maioria dos estudantes envolvidos mora em comunidades ou bairros carentes e afastados da escola. Outros, no bairro da própria escola.

O trabalho foi dividido em três momentos:

(a) No primeiro momento, foi realizado um questionário contendo dez questões com os assuntos já citados, ou seja: questões que envolviam assuntos da grade curricular; questões para diagnosticar dificuldades ou não, como, por exemplo, divisibilidade, algoritmo da divisão e com máximo divisor comum; questões que envolviam assuntos que não estão presentes na grade curricular do aluno, para, posteriormente, avaliar se houve aprendizado deste assunto, quais as dificuldades apresentadas durante as aulas e se há possibilidade de o assunto ser ministrado para alunos com a mesma maturidade.

(b) O segundo momento deste trabalho, consiste em aulas expositivas, em sala de aula, e resolução de questões orientadas, isto é, questões são colocadas para os estudantes após apresentação de conteúdo e resolução de exercício em sala de aula com a participação de todos os envolvidos. Esta parte do trabalho, em que o estudante é chamado a participar, tem como objetivo fazer com que

todos fiquem atentos às aulas e às resoluções de questões, dificultando a dispersão da atenção dos participantes.

(c) O terceiro e último momento tem a aplicação do mesmo questionário do primeiro momento para verificar se os estudantes que tinham alguma dificuldade naqueles assuntos da grade curricular conseguiram superá-lo e, consequentemente, se houve realmente aprendizado; se todos os envolvidos na pesquisa aprenderam os assuntos não pertencentes a grade curricular e qual foi o efetivo ganho para esta turma.

2.4 Das Aulas

No início, as aulas contavam com quinze participantes e logo na segunda semana foi tendo uma redução para nove participantes até que chegou ao número de quatro estudantes, os quais deram continuidade até o fim das atividades.

O primeiro dia do trabalho foi composto de dois momentos: no primeiro momento, foi aplicado um questionário contendo dez questões que abordavam os conteúdos de divisibilidade, algoritmo da divisão, máximo divisor comum, e congruência; no segundo momento foi dado início aos conteúdos, começando pelo conceito formal de divisibilidade e proposições. Estes primeiros conteúdos foram ministrados de acordo com a sequência natural dos livros consultados para elaboração das aulas: primeiro a teoria e logo em seguida citando exemplos. Foi possível perceber uma dificuldade de compreensão dos conteúdos pelos alunos e havia reclamação com relação ao uso de letras, dizendo que ficava mais difícil de se aprender. Então, nas aulas que se seguiram, foram citados exemplos numéricos para só então chegarmos ao conceito formal e, posteriormente, demonstrado.

Exemplo: sabemos que $2 \mid 6$, pois existe o $3 \in \mathbb{Z}$ tal que $6 = 2 \cdot 3$, e $5 \mid 15$, pois existe $3 \in \mathbb{Z}$ tal que $15 = 5 \cdot 3$, então, $2 \cdot 5 \mid 6 \cdot 15$, ou seja, $10 \mid 90$, pois existe $9 \in \mathbb{Z}$ tal que $90 = 10 \cdot 9$.

Se $a,\ b,\ c,\ d \in \mathbb{Z}$, com $a,\ c \neq 0$, então $a \mid b$ e $c \mid d \Rightarrow a \cdot c \mid b \cdot d$

2.4.1 Do Primeiro Momento das Aulas - Questionário

O questionário foi elaborado envolvendo questões de baixa complexidade, em que estávamos buscando saber qual é o conhecimento que este estudante tem em relação aos inteiros e as operações aritméticas; de média complexidade, em que queremos

saber se o estudante consegue interpretar problemas de aritmética e se são capazes de resolvê-las; e de alta complexidade, em que os assuntos não são ministrados nas escolas.

O que se esperava com a aplicação deste questionário era que o alunos conseguissem responder às questões de baixa complexidade e que, possivelmente, alguns desses estudantes resolvessem as de média complexidade ou tentassem resolvê-las.

Vamos observar o que foi feito pelos alunos neste questionário de aplicação e comentar aluno por aluno:

1. Com relação aos critérios de divisibilidade:
   a) Quando um número é divisível por 2? Dê um exemplo.
   b) Quando um número é divisível por 6? Dê um exemplo.
   c) O que seria necessário para que se obtenha um critério de divisibilidade por 11?

2. Sendo a um número inteiro positivo que, dividido por b, nos dá como quociente o número q e resto r. Então:
   a) Determine o valor de a em função de b, q e r.
   b) Sabendo que $a = bq + r$, dê um exemplo numérico com r diferente de zero.

   Dado os números abaixo, responda:

   i. 3271

   ii. 2799

   iii. 3306

   iv. 2841

   a) Quais destes números, quando dividido por 7, deixa resto 2.
   b) Quais deste números, quando dividido por 6, deixa resto 3.

3. Seja m 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 $a \equiv b \; mod \; m$. por exemplo $21 \equiv 13 \; mod \; 2$, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.
   a) Escreva dois exemplos em que você pode utilizar a ideia apresentada.
   b) Faça o mesmo utilizando as letras a) e b) da questão anterior.

4. Em uma fábrica são empilhados e embalados 12 produtos por caixa. Tendo produzido 2.841 produtos em certo dia, quantas caixas serão necessárias?

5. O número de alunos de uma escola, do turno da tarde, é de 231 alunos. Sabe-se que a escola pretende fazer uma excursão levando todos os seus 231 alunos em vans que comportam apenas 11 alunos. A escola dispõe de 7 vans. Quantas viagens, da escola para o ponto de destino, serão necessárias para que as 7 vans transportem todos os 231 alunos?

6. De quantas maneiras podem-se comprar selos de 3 reais e de 5 reais de modo que se gastem 50 reais?

7. Verifique, abaixo, quais das sentenças são verdadeiras:
   a) $13 \mid 2^{13} - 2$
   b) $13 \mid 5^{13} - 5$
   c) $13 \mid 3^{13} - 3$

8. Ache o resto da divisão de:
   a) 5^{60} por 26
   b) 3^{100} por 10

9. Tendo que $25 \equiv 3 \ mod \ 11$, determine o resto da divisão de 25^4 por 11.

O estudante B, que está cursando o 9^o ano do Ensino Fundamental, não consegue atingir o esperado na primeira aplicação do questionário, pois, como podemos ver na Figura 2.1 da página 56, na resposta dada à primeira questão, ela não sabe da regra de divisibilidade por 6. Esquece de citar exemplos que foram pedidos na questão e não desenvolve nenhum outro exercício que exija conhecimento do 6^o ano do Ensino Fundamental.

O estudante L, que está cursando o 7^o ano do Ensino Fundamental, não conseguiu atingir o esperado para este questionário neste primeiro momento, pois a primeira questão é do assunto do ano anterior. O estudante até inverteu a posição do divisor com o dividendo, fez uma mistura de conhecimentos de MDC e cometeu erros com a operação de multiplicação, como podemos ver na Figura 2.5 da página 60.

O estudante V, que cursa o 9^o ano do Ensino Fundamental, conseguiu uma parte do esperado na aplicação do primeiro questionário, como mostra a Figura 2.18 da página 68. O aluno ainda se mostrou com déficit de conhecimento anteriores, pois se espera que um aluno do 9^o ano seja capaz de resolver problemas algébricos de matemática.

O estudante R, que também cursa o 9^o ano do Ensino Fundamental, atingiu a expectativa esperada, mostrando-se com conhecimento esperado para um aluno do 9^o ano, sabendo resolver problemas de aritmética, conforme podemos ver na Figura 2.10 e Figura 2.11 da página 64.

Não posso afirmar, mas apenas um estudante tentou resolver a maioria das questões, que os quatro alunos envolvidos não tiveram o mínimo de conhecimento prévio, pois os estudantes que resolveram 2.18 e 2.1 da página 68 e 56, respectivamente, foram meus alunos do 9^o ano e foram bastante aplicados. Talvez tenham ficado ansiosos ou com medo, pois estes entregaram o questionário rapidamente, apesar de eu insistir para que eles tentassem.

2.4.2 Do Segundo Momento das Aulas

Como já foi mencionando, este é o momento em que o assunto é apresentado e estudado com a participação de todos e sob a orientação do professor mediador.

Antes mesmo de qualquer pergunta ou questão ser proposta aos estudantes, eram colocados exemplos resolvidos, fazendo com que os estudantes se sentissem mais confiantes e à vontade para responder perguntas ou citar algum outro exemplo.

Em todas as aulas, antes de dar início, eram feitos exemplos dos conteúdos estudados na aula anterior e colocado exercícios para que fossem feitos naquele exato momento com base na questão apresentada no quadro, o que deixou claro que estava havendo uma progressão significativa dos conteúdos e de sua assimilação por todos os envolvidos.

O objetivos aqui é estimular e dar mais confiança ao aluno, mostrando que, apesar das dificuldades providas pela falta de conhecimentos anteriores, é possível aprender e desenvolver questões.

Vejamos algumas dessas questões desenvolvidas pelos alunos a partir de um exemplo colocado no quadro e com o acompanhamento.

Vamos analisar algumas questões desenvolvidas em sala de aula a partir de um exemplo posto no quadro e com a intervenção do professor.

É possível perceber, através da Figura 2.1, Figura 2.6, Figura 2.19, Figura 2.12 e Figura 2.13 das respectivas páginas 56, 61, 69 e 65, que o estudante, tendo um exemplo a ser seguido, consegue obter êxito no desenvolvimento de sua questão, apesar de certas dificuldades em multiplicação e divisão que vêm sendo minimizadas com as aulas deste trabalho.

2.4.3 Do Terceiro Momento - Reaplicação do Questionário

Esta última aplicação do mesmo questionário aplicado no primeiro dia de aula teve como principal objetivo verificar se houve uma aprendizagem significativa e quais as dificuldades que os estudantes ainda apresentam.

Nesta aplicação, apenas a estudante L continuou com dificuldades para resolver as questões, mas, mesmo assim, é possível perceber um avanço com a aritmética. Não poderia deixar de lembrar que este estudante cursa o 7º ano do Ensino Fundamental, ano em que começa a ter um contato maior com a matemática abstrata de acordo com o PCN, e, mesmo nestas condições, se mostrou capaz de ter um aprendizado.

Nesta segunda aplicação, os estudantes B, R e V só não resolveram a sétima questão, ou porque não se lembravam como proceder ou por falta de tempo, pois já estava no final da aula.

Aqui, quero chamar atenção para a estudante V que na 3ª questão, encontrada na Figura 2.20 da página 70, do questionário, resolveu de maneira um pouco diferente e, de certa forma, mais rápida que os demais estudantes. A maneira com que os estudantes B e R resolveram foi a maneira ensinada durante as aulas; já a maneira com que V resolveu não foi comentada em sala de aula, mas é também uma maneira correta de resolver. Comparando com a Figura 2.2 e Figura 2.15 das páginas 57 e 66, podemos ver que a estudante V evitou a repetição da congruência ao contrário dos estudantes B e R.

Observação 7 *A 3ª questão foi resolvida usando congruência, mas poderia ter sido resolvida utilizando o Algoritmo da Divisão de Euclides. Porém, eu pedi que fosse usada a congruência como aplicação do conteúdo visto em nossas aulas.*

Na 9º questão, apesar de os estudantes terem visto, durante as aulas, a aplicação da função fi de Euler, eles não lembravam da função, mas, talvez por terem trabalhado muitas questões usando congruência com os números inteiros, conseguiram resolvê-la. A função fi não foi bem aceita pelos estudantes durante as aulas, pois eles reprovaram a ideia de ter que decorar a função para solucionar questões deste tipo. As figuras Figura 2.3, a Figura 2.17 e Figura 2.22, das respectivas páginas 58, 68 e 72 mostram que estes estudantes conseguem manipular as propriedades de congruência com os números inteiros.

Observação 8 *Foi dado, em sala de aula, um exemplo de grande utilidade da função fi de Euler através da questão presente no livro Elementos de Aritmética em*

que o estudante R começou à desenvolver de maneira correta, como podemos ver na Figura 2.14 da página 66.

Deixei, por fim, para apresentar e comparar as questões feitas pelo estudante L do 7º ano.

As questões consideradas de baixa e média complexidades, que se apresentam na Figura 2.7 da página 61, em que este estudante não havia obtido êxito, foram realizadas com sucesso; já a quinta questão este estudante cometeu um erro, talvez pela falta de organização, que comprometeu o resultado e realizou a sexta questão corretamente, como podemos ver na Figura 2.9 da página 63.

A terceira questão, considerada de média complexidade, foi feita parcialmente correta, pois o estudante L não conseguiu realizar o que foi pedido no item b), que deveria ser realizado da mesma forma que o item a). Este estudante gastou muito tempo realizando as contas no item a), se mostrando lento ao resolver contas de multiplicação e divisão. No entanto, mostrou ser capaz de resolver a questão usando congruência como podemos ver na Figura 2.8 da página 62.

A décima questão, apresentada na Figura 2.9 da página 63 considerada de alta complexidade, foi realizada corretamente, mostrando que este estudante já se mostra familiarizado com a definição de congruência e as propriedades.

Observação 9 *As perguntas que podemos fazer em relação da estudante L são:*

1 *Será que o estudante tem problemas realmente com o algoritmo da divisão ou será falta de atenção, organização e paciência, visto que já foi feito na 5ª questão apresentada na Figura 2.9 da página 63 ;*

2 *Será que o estudante demorou a realizar as contas porque tem problemas com multiplicação e divisão ou ele estava fazendo mais lentamente para que fossem evitado erros, e como o tempo estava terminando ele acabou errando as contas ao fazer com pressa.*

Uma coisa é certa, depois desta nova experiência com a matemática, em especial com a aritmética, os estudantes se mostram mais participativos em sala de aula e sempre questionando mais.

2.5 Das Barreiras ou Dificuldades Encontradas

Este trabalho enfrentou diversos problemas em que alguns poderão ser contornados e outros, infelizmente, não tivemos como saná-los. São eles:

1. Falta de interesse do estudante envolvido.
2. Falta de espaço físico adequado.
3. Falta de apoio e incentivo do governo.
4. Falta de base dos alunos.
5. Falta de material didático disponível.

2.5.1 Da Falta de Interesse do Estudante Envolvido

Alguns desses estudantes envolvidos, mais precisamente os que moravam no próprio bairro da escola ou nos bairros vizinhos, se mostraram desinteressados após a primeira semana de aula, deixando de comparecer nas seguintes.

Seus principais argumentos foram: ter que se acordar mais cedo, ter aula no período da manhã e depois à tarde, ter outros compromissos (este não mencionados de fato); e alguns diziam, simplesmente, não ter nenhum interesse em aprender os conteúdos da forma que foram vistos, com mais rigor na matemática e nas demonstrações.

Observação 10 *Muitas vezes o professor é questionado pelos seus estudantes o porquê de eles estudarem matemática. Para eles, bastavam aprender as quatro operações básicas: adição, subtração, multiplicação e divisão.*

2.5.2 Falta de Espaço Físico Adequado

A E.E.E.F.M.J.J.C. é uma escola de pequeno porte, pois tem, apenas, seis salas de aula, uma sala de refeitório, sala dos professores, uma pequena sala de vídeos, uma pequena sala de computação que comporta oito micro-computadores, sala de coordenação, duas pequenas salas (uma para a diretora e outra para a vice-diretora) secretaria, e uma pequena biblioteca.

A escola, tanto no turno da manhã como no turno da tarde, oferece os trabalhos de sexto, sétimo, oitavo, nono ano do ensino fundamental, primeiro ano do ensino médio e a correção de fluxo. Dessa forma, o trabalho foi ministrado na sala de vídeo (quando não era solicitada pelos outros professores) ou na biblioteca, ou seja, não se tem uma sala adequada para fazer um trabalho extra-classe voltado para a OBMEP; apesar de, tanto a sala de vídeo quanto a biblioteca, possuírem quadro branco.

2.5.3 Falta de Apoio e Incentivo do Governo

Aqui, podemos considerar uma das maiores barreiras para a realização de qualquer atividade fora do horário normal de aulas, pois um dos motivos de os alunos também terem abandonado o trabalho foi a falta de oferta da merenda e do almoço aos alunos que frequentavam este trabalho.

> O motivo da falta desta oferta é bem fácil de se compreender e, por incrível que pareça, é com base em preceitos legais. Apesar de a Lei 11.947, de 16 de Junho de 2009, em seu art. 3º dizer:
>
> Art. 3º A alimentação escolar é direito dos alunos da educação básica pública e dever do Estado e será promovida e incentivada com vistas no atendimento das diretrizes estabelecidas nesta Lei.

$(http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l11947.htm)$

O problema da falta de fornecimento da merenda e almoço aos alunos deste trabalho, fora do seu horário normal, é devido a outro sistema legal: o repasse da verba do Fundo Nacional de Desenvolvimento da Escola (Fundeb).

> Os recursos do Fundeb, Fundo Nacional de Desenvolvimento da Edução, são distribuídos de forma automática (sem necessidade de autorização ou convênios para esse fim) e periódica, mediante crédito na conta específica de cada governo estadual e municipal.
>
> A distribuição é realizada com base no número de alunos da educação básica pública, de acordo com dados do último censo escolar, sendo computados os alunos matriculados nos respectivos âmbitos de atuação prioritária, conforme art. 211 da Constituição Federal.

(http://www.fnde.gov.br/financiamento/fundeb/fundeb-funcionamento).

Ou seja, como o repasse do Fundeb não previa o aumento, em quase o dobro, do número de alunos matriculados este ano, a escola não poderia ofertar alimentos para esta turma ou qualquer outra que venha a trabalhar fora do horário normal de aula. Ela precisa dar conta do oferecimento de merenda aos que estão em curso normal. Portanto, muitos destes alunos deixaram de participar, pois ficaria economicamente impossível para seu pais pagar a alimentação dos seus filhos.

Não podemos esquecer, também, da falta de incentivo:

- Aos professores de matemática ao ministrar aulas voltados para OBMEP ou qualquer outro tipo de curso, como construção geométrica, a matemática aplicada no dia-a-dia, história da matemática, e outras que poderiam ser trabalhadas pelos profissionais da área, tornando a matemática mais atrativa; e

- Ao próprio aluno ao querer estudar matemática.

Aqui, refiro-me a premiar os professores e alunos por estarem fazendo um trabalho extra-classe que irá ter que disponibilizar mais de seu tempo e o segundo por estar buscando o conhecimento que será disponibilizado nos cursos.

Apesar de já existir a premiação da própria OBMEP junto ao CNPQ, não se pode ser vista como um incentivo significativo, pois o número de premiados com bolsa de estudo em relação ao número de participantes é praticamente insignificante. Ao contrário, chega a ser desestimulante devido à grande concorrência, como mostra a tabela abaixo.

Ano	N^o de Alunos Inscritos	N^o de Alunos Premiados	Premiados|Inscrito
2013	18.762.859	5.999	0,000319727
2012	19.166.371	4.504	0,000234995
2011	18.720.068	3.200	0,00017094
2010	19.665.928	3.208	0,000163125
2009	19.198.710	3.000	0,00015626
2008	18.326.029	3.005	0,000163974
2007	17.341.732	3.002	0,000173108
2006	14.181.705	1.110	7,82699E-05
2005	10.520.831	1.110	0,000105505

Disponível em: $http://www.obmep.org.br/obmep\_em\_numeros.html$

Vejamos, agora, qual o incentivo, de acordo com o próprio regulamento da OBMEP, é dado ao professor para desenvolver um trabalho, fora do horário normal de aula, voltado para a OBMEP:

i Um tablet, um diploma e uma assinatura anual de Revista do Professor de Matemática (RPM-SBM);

ii Excluídos os professores premiados no item anterior, serão concedidos 1 (um) diploma de homenagem e 1 (uma) assinatura anual da Revista do Professor de Matemática (RPM-SBM);

Toda essa premiação para que um profissional de matemática disponibilize tempo para lecionar aulas extras gratuitas. Aqui, vale lembrar, que o professor tem que trabalhar dois ou três turnos para conseguir um salário razoável para manter sua família, pois se não fosse o piso dado pelo governo federal em 2014 é 1.697,00 reais.

Contudo, OBMEP lançou um programa de incentivo aos professores da rede pública que queiram trabalhar com uma turma extra-classe direcionado para as provas das Olimpíadas Brasileiras de Matemática com bolsa promovida pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes).

OBMEP na escola:

a. Objetivo: apoiar e estimular o desenvolvimento de atividades extra-classe de professores de matemática da rede pública visando melhorar o desempenho de seus alunos nas provas da OBMEP.

b. De março a julho de 2015 a OBMEP promoverá oficinas mensais para familiarizar os Preparadores com o material didático elaborado pela OBMEP e para estimulá-los a utilizar este material em sala de aula.

c Da Bolsa: a partir de março de 2015, os Preparadores receberão por um ano uma bolsa da CAPES no valor mensal de R$ 765,00 (setecentos e sessenta e cinco reais) para realizarem suas atividades, que será renovada a cada ano mediante relatório das atividades realizadas ao longo do ano. Além das informações fornecidas nos relatórios mensais.

Vale lembra que serão 1.000 (mil) bolsas para os professores que fizerem mais ponto na prova de habilitação, e este número de bolsas sera distribuída tendo em vista a população de cada Estado.

Os requisitos para que um professor da rede pública venha a ter direito de participar deste projeto:

(i) Ser aprovado na prova de habilitação.

(ii) Elaboração de um Projeto de Atividades.

(iii) Realizar atividades extraclasse de preparação às provas da OBMEP.

(iv) Enviar relatórios mensais das atividades.

Entretanto, um profissional de matemática, efetivo da escola pública, que já tenha bolsa da Capes para realizar qualquer outro tipo de trabalho ou pesquisa não terá direito a esta bolsa promovida pela OBMEP, ou seja, o profissional de matemática, nestas condições mencionadas, que queira trabalhar com turmas extra-classe, terá de fazê-lo gratuitamente. Mas podemos dizer que já é um começo, pois, além de disponibilizar material para se trabalhar, o professor que entrar no programa terá seu trabalho extra-classe reconhecido e pago pelo seu feito.

2.5.4 Falta de Base dos Alunos

Pode ser inacreditável, mas um dos grandes vilões para que o aluno passe de ano sem merecimento, isto é, passar de ano sem dominar os conceitos básicos da série em que estava, é o Índice de Desenvolvimento da Educação Básica (Ideb).

O cálculo do Ideb é feito através das seguintes variáveis:

1- i = ano do exame (Saeb e Prova Brasil) e do Censo Escolar;

2- N_{ji} = média da proficiência em Língua Portuguesa e Matemática, padronizada para um indicador entre 0 e 10, dos alunos da unidade j, obtida em determinada edição do exame realizado ao final da etapa de ensino;

3- P_{ji} = indicador de rendimento baseado na taxa de aprovação da etapa de ensino dos alunos da unidade j;

Esta última variável faz com que as escolas aprovem os seus alunos mesmo sem ter o conhecimento necessário de prosseguir nos estudos, pois se o número de reprovação aumenta o Ideb da escola cai. Assim se explica o motivo de muitos alunos dos 6^{os}, 7^{os}, 8^{os} e 9^{os} anos do ensino fundamental não dominar as quatros operações básicas da matemática ou, quando sabem operar, não conseguem resolver problemas por falta de interpretação de textos.

Mas, por outro lado, a culpa não é apenas de um índice, ou dos professores, nem, muito menos, das escolas e dos pais dos alunos. Aqui, há todo um sistema por trás:

i Falta de acompanhamento dos pais, com relação às atividades dos alunos;

ii Falta de qualificação e remuneração digna de todos os profissionais da educação;

iii Falta de uma escola de alto padrão: alimentação, segurança, lazer, etc.;

iv Falta de incentivo dos governos ou de premiação a todos que busquem o conhecimento.

2.5.5 Falta de Material Didático Disponível

Apesar de o assunto, em sua grande parte, ser da grade curricular das escolas, ou seja, o assunto está presente em livros utilizados pelos alunos, faltam materiais mais específicos nas escolas, voltados para a OBMEP, pois as questões da Olimpíada Brasileira de Matemática são de níveis mais complexos restando aos alunos recorrer às provas de edições anteriores, sem resposta para conferir, e sob a responsabilidade do professor para resolver as questões de cada prova ou reproduzir as respostas encontradas no banco de questões. Isto faz com que o aluno se torne um bom colecionador de questões e métodos de resolver questões sem o conhecimento formal dos métodos e teorias.

2.5.6 Figuras

Nesta seção disponibilizamos, em sequência, as figuras citadas neste capítulo, que correspondem às atividades desenvolvidas pelos alunos dutrante o período da experiência.

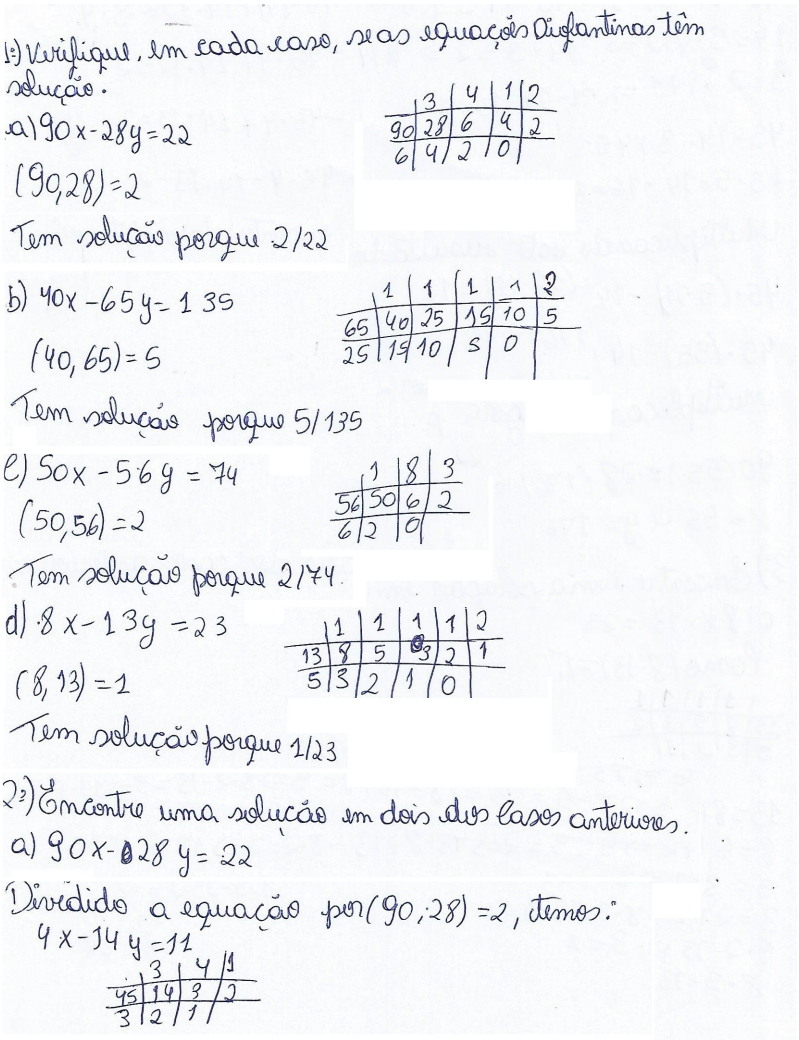


Figura 2.1: Estudante B

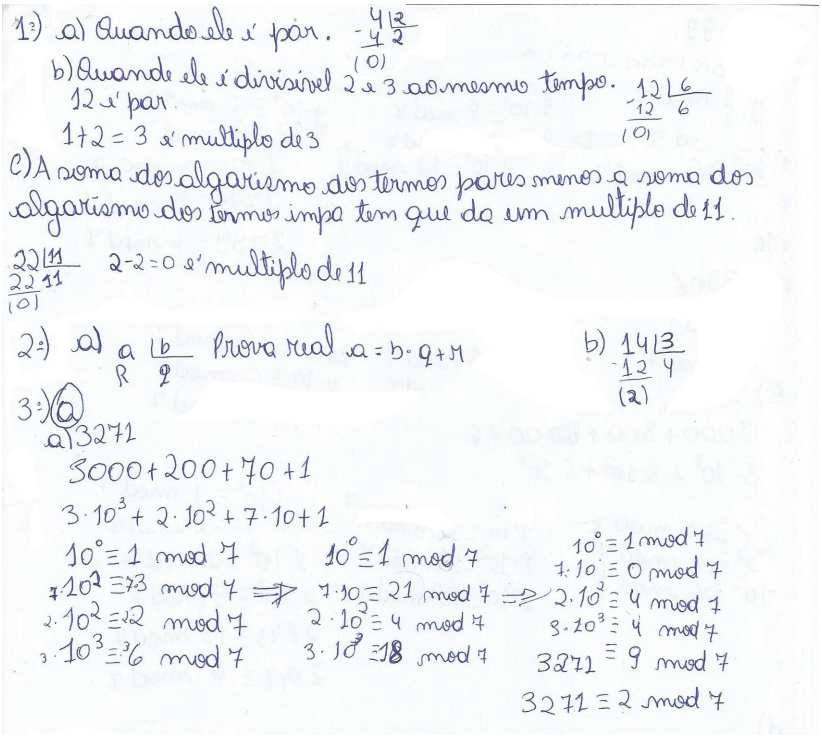


Figura 2.2: Estudante B

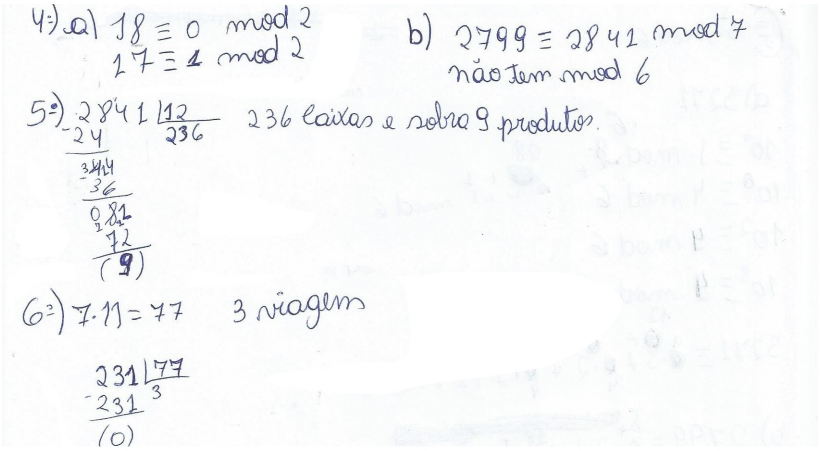


Figura 2.3: Estudante B

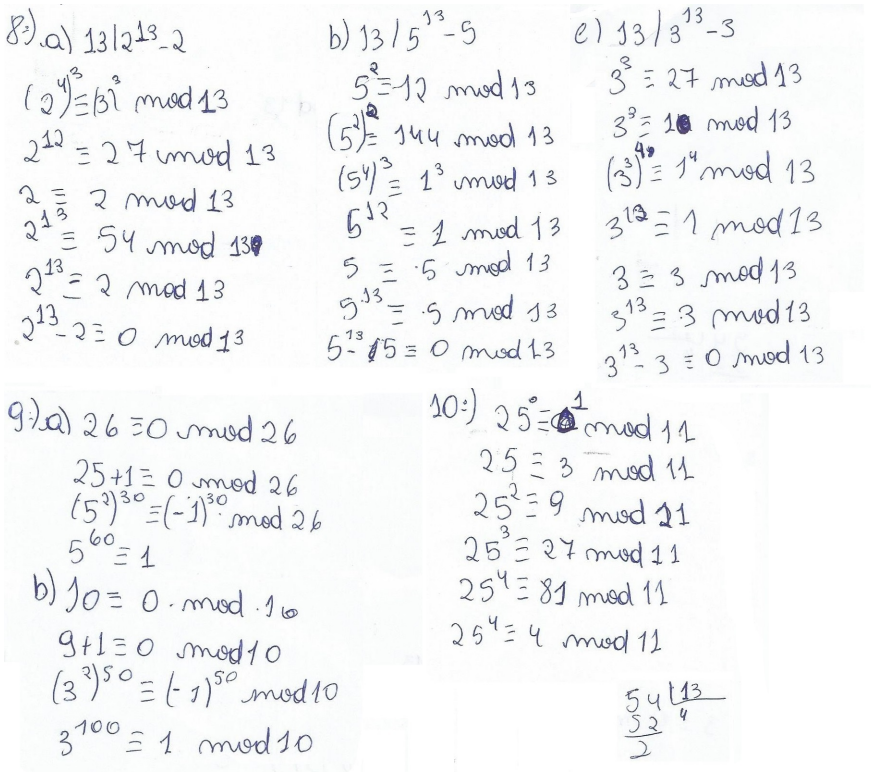
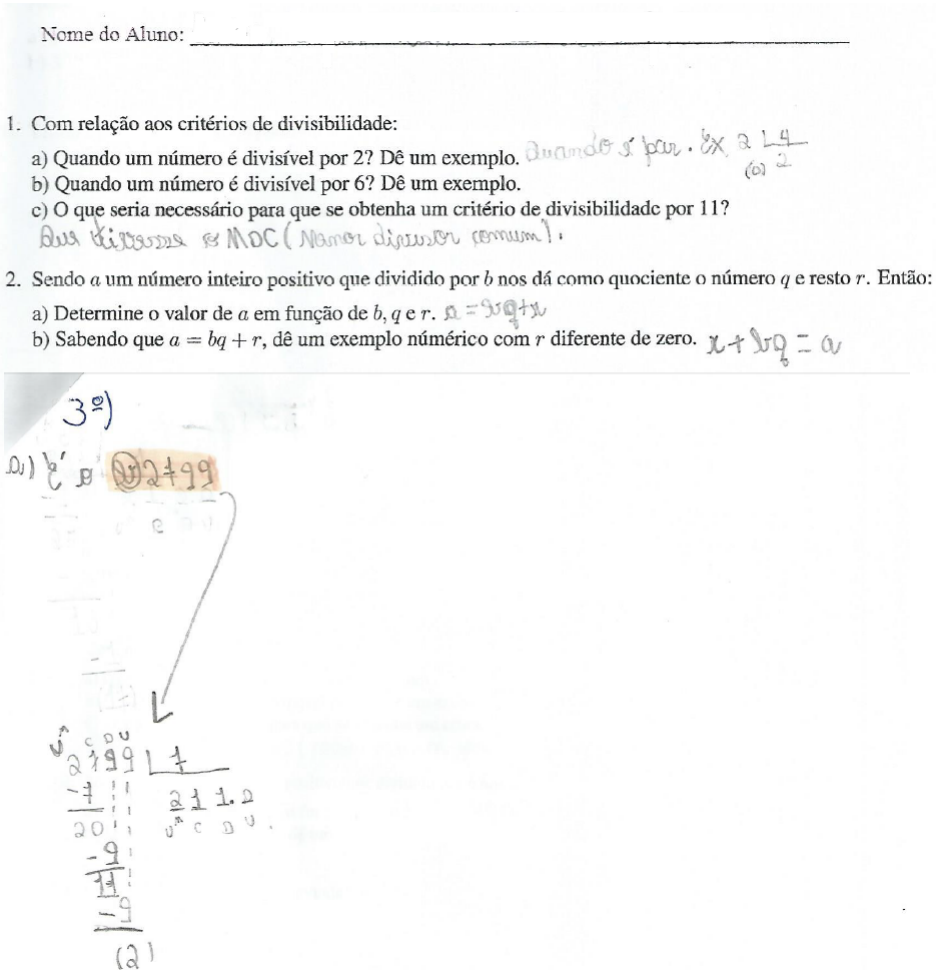


Figura 2.4: Estudante B



Nome do Aluno: _____

1. Com relação aos critérios de divisibilidade:
   a) Quando um número é divisível por 2? Dê um exemplo.
   b) Quando um número é divisível por 6? Dê um exemplo.
   c) O que seria necessário para que se obtenha um critério de divisibilidade por 11?
2. Sendo a um número inteiro positivo que dividido por b nos dá como quociente o número q e resto r. Então:
   a) Determine o valor de a em função de b, q e r.
   b) Sabendo que $a = bq + r$, dê um exemplo numérico com r diferente de zero.

Figura 2.5: Estudante L

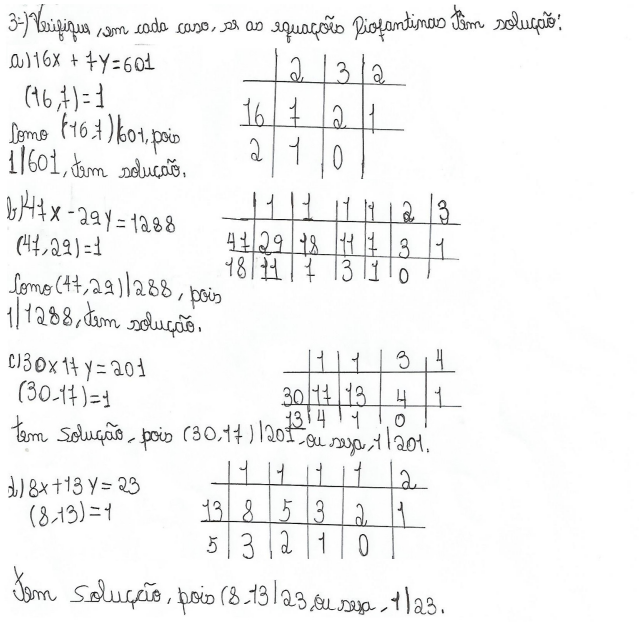


Figura 2.6: Estudante L

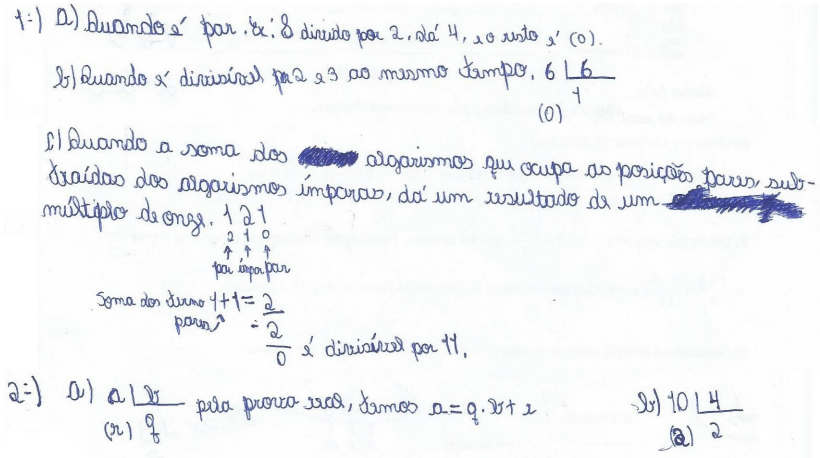


Figura 2.7: Estudante L

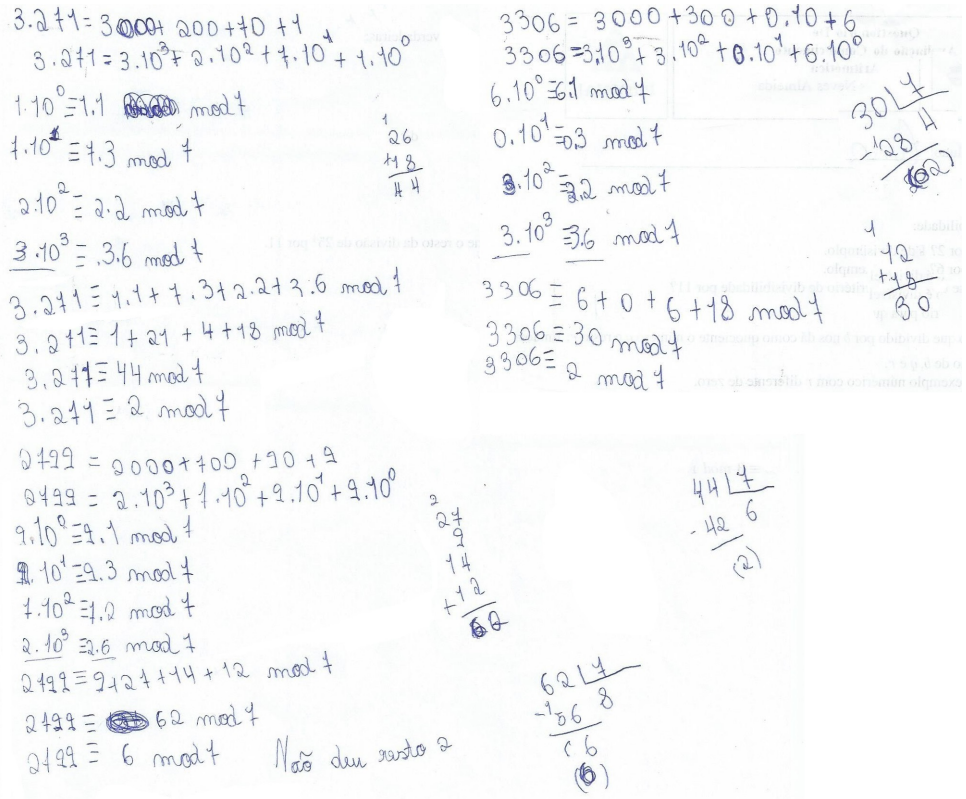


Figura 2.8: Estudante L

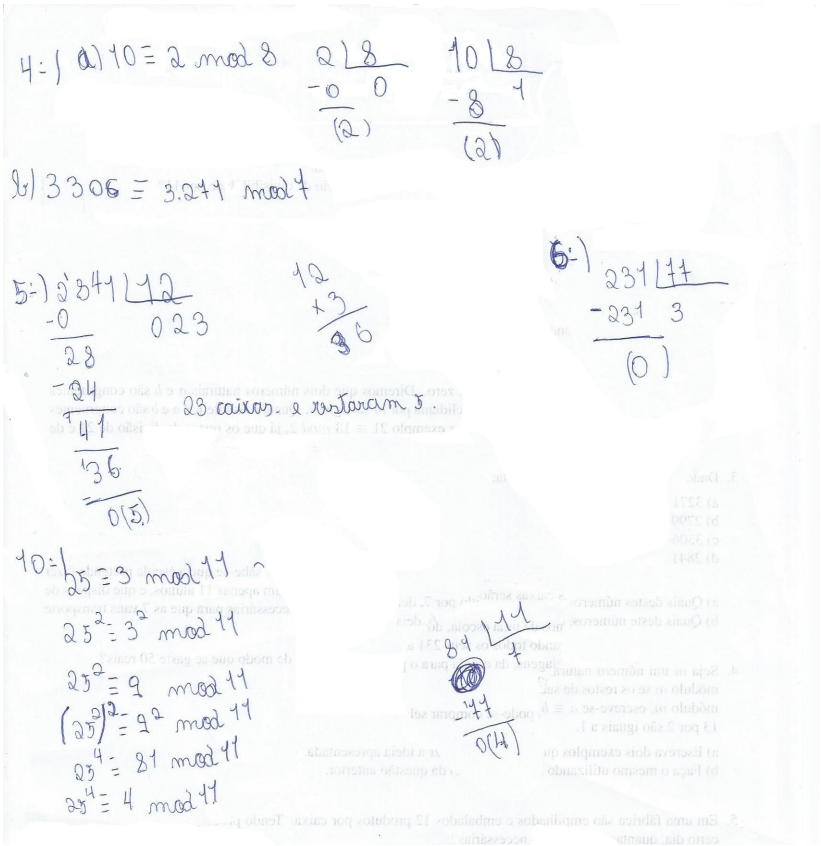


Figura 2.9: Estudante L

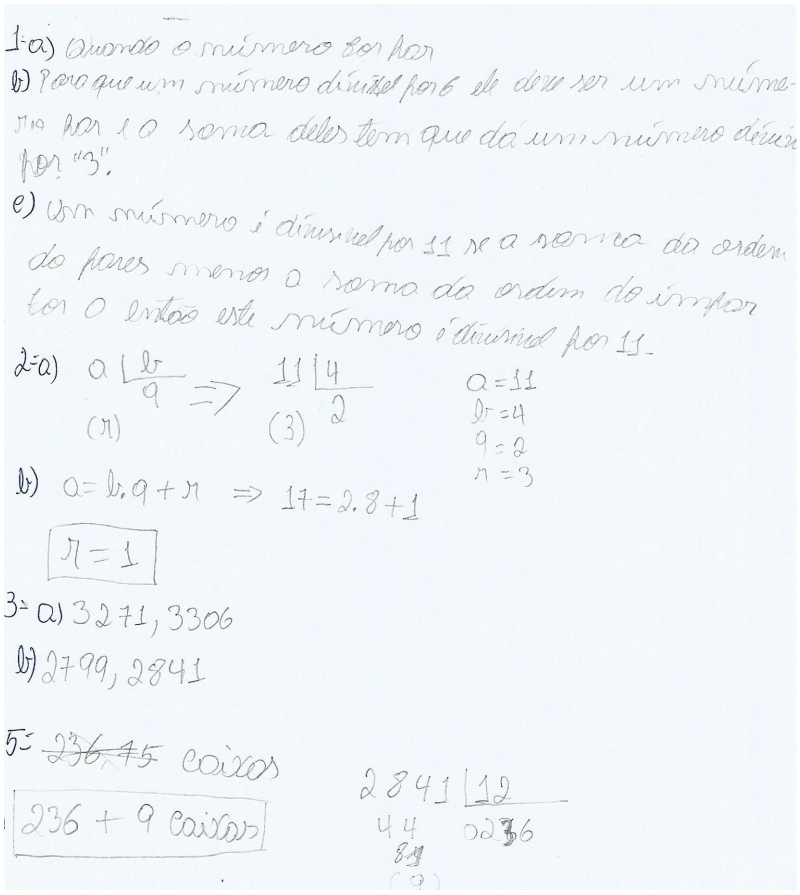


Figura 2.10: Estudante R

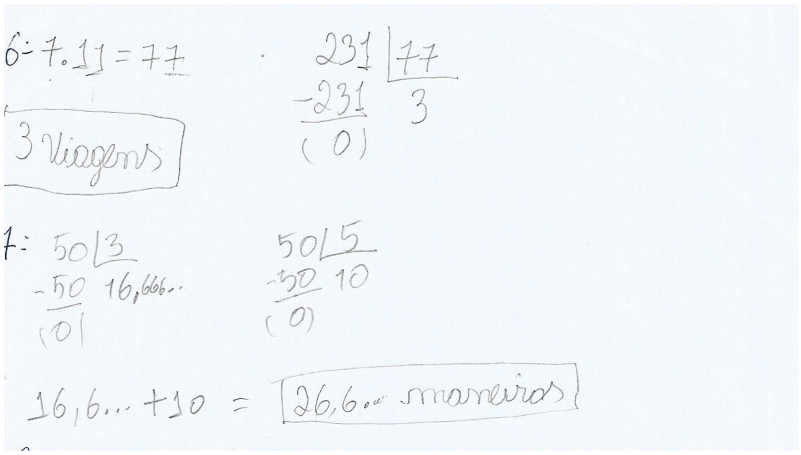


Figura 2.11: Estudante R

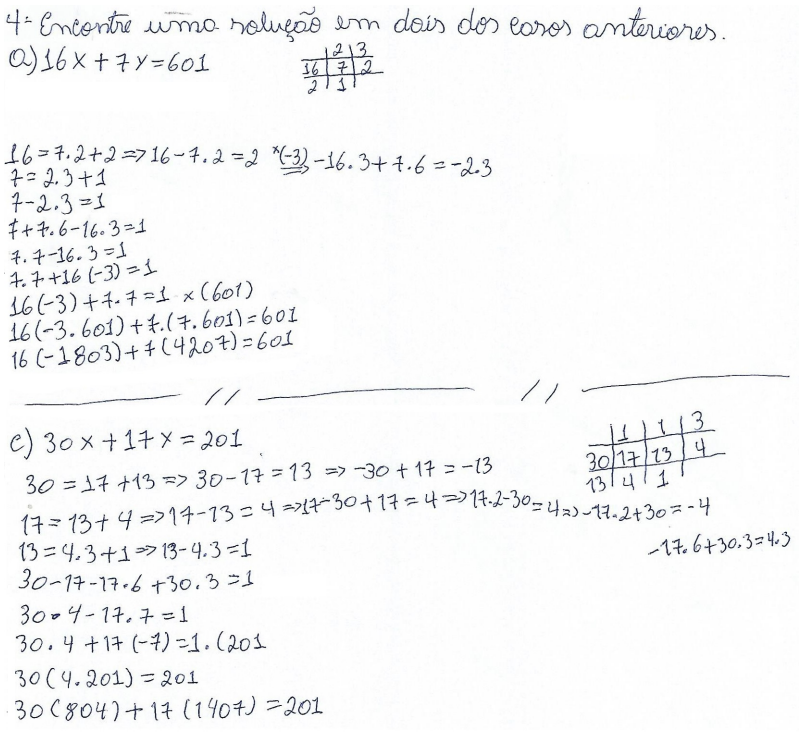


Figura 2.12: Estudante R

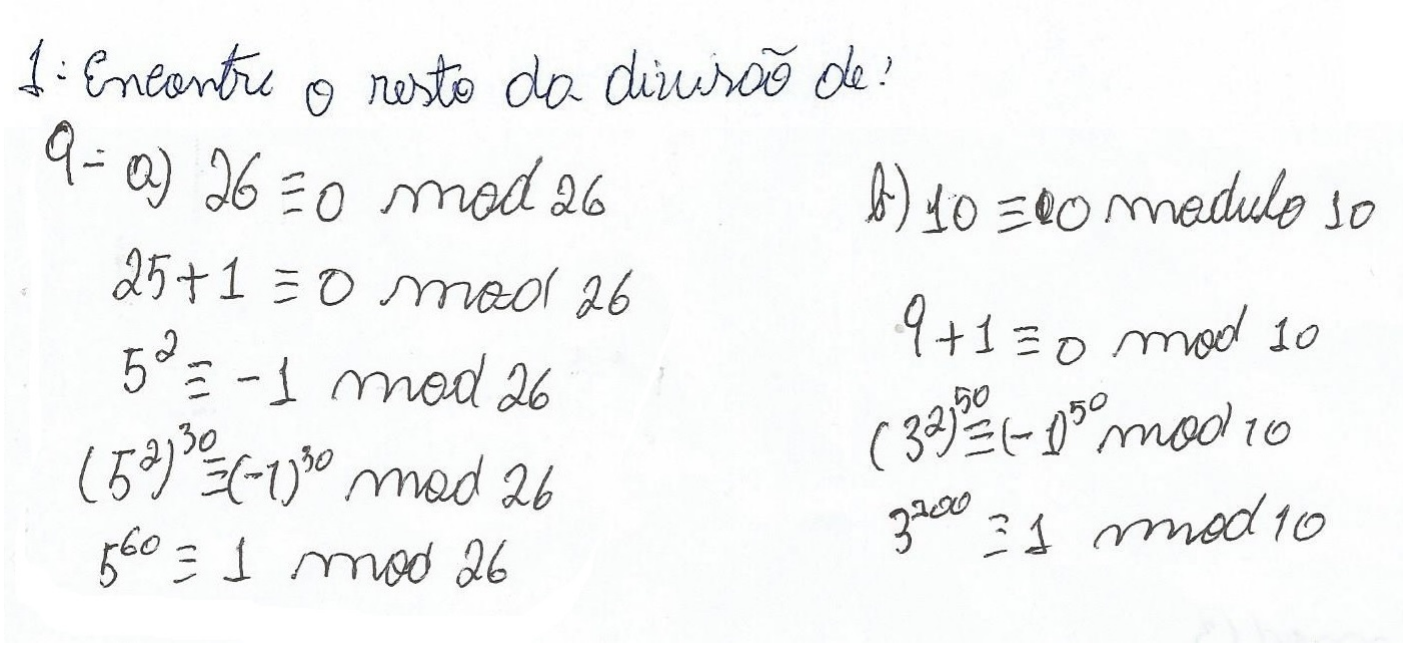


Figura 2.13: Estudante L

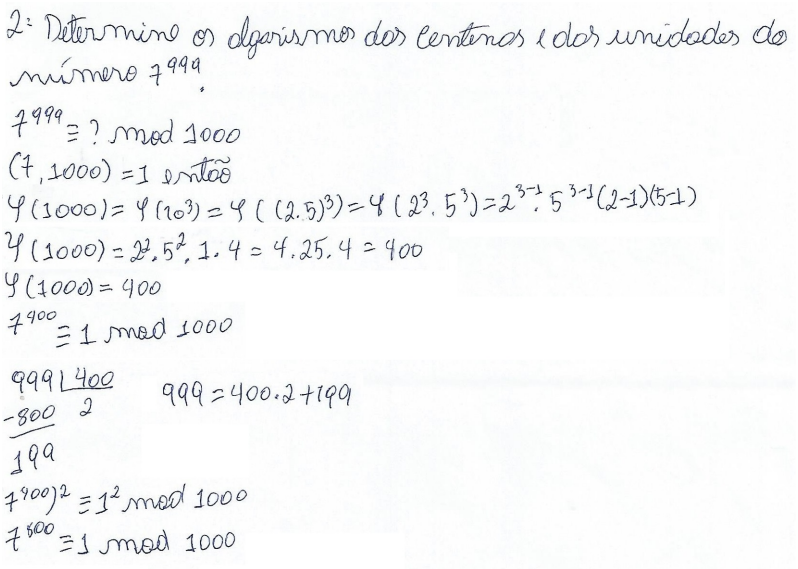


Figura 2.14: Estudante R

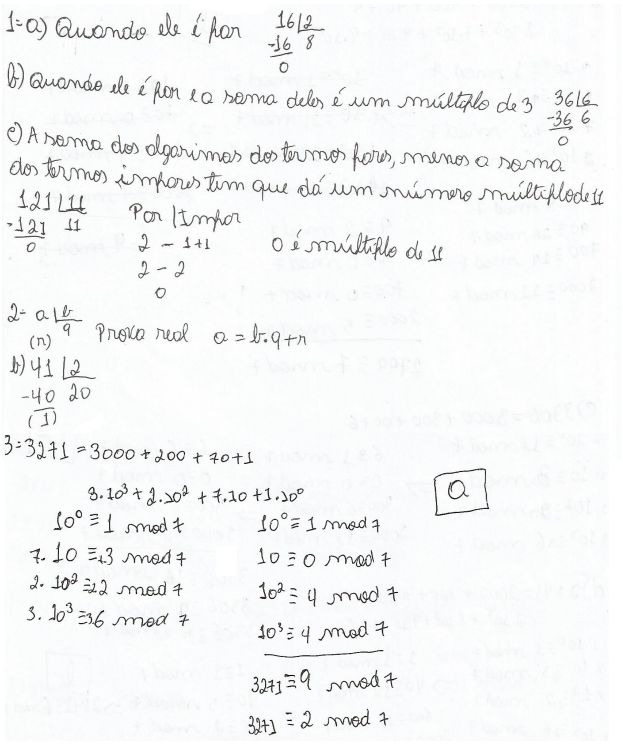


Figura 2.15: Estudante R

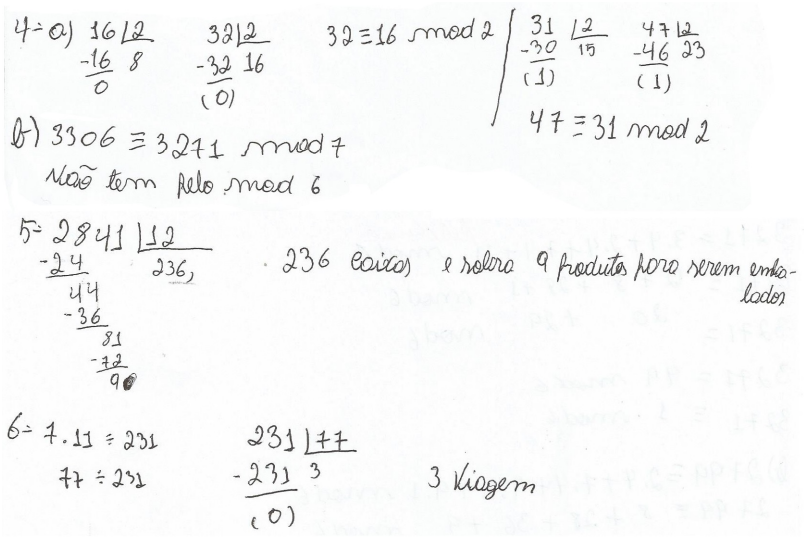


Figura 2.16: Estudante R

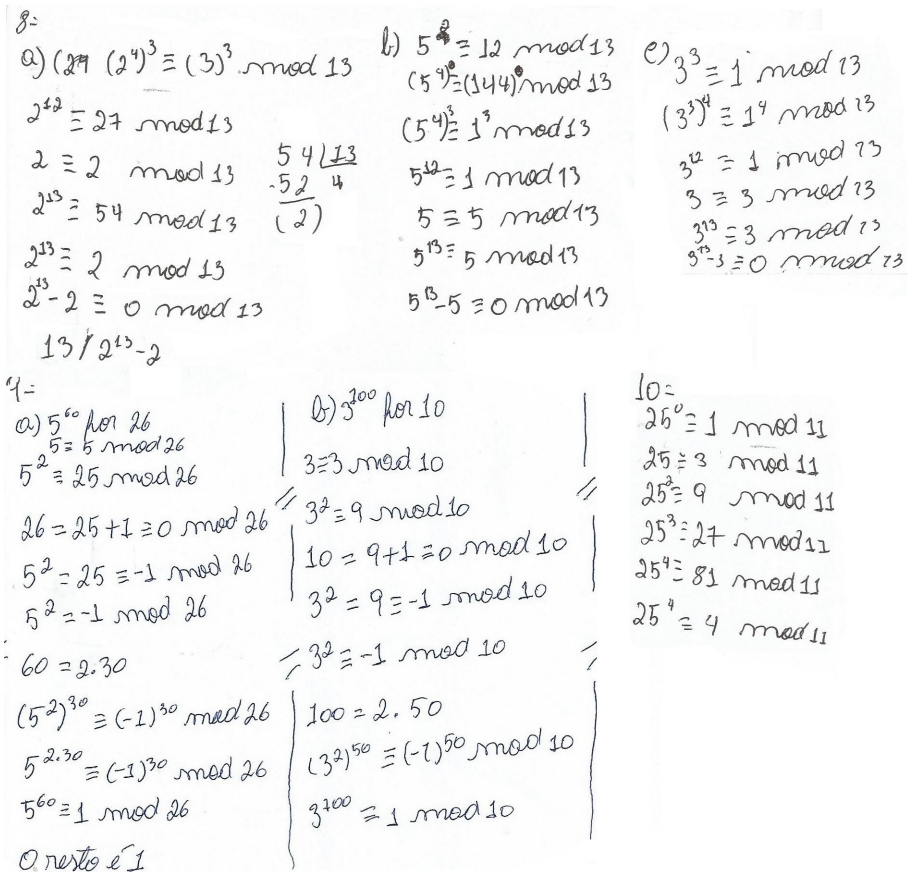


Figura 2.17: Estudante R

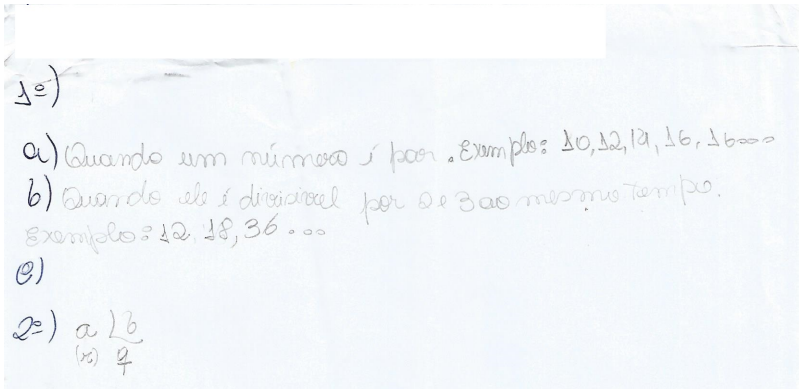


Figura 2.18: Estudante V

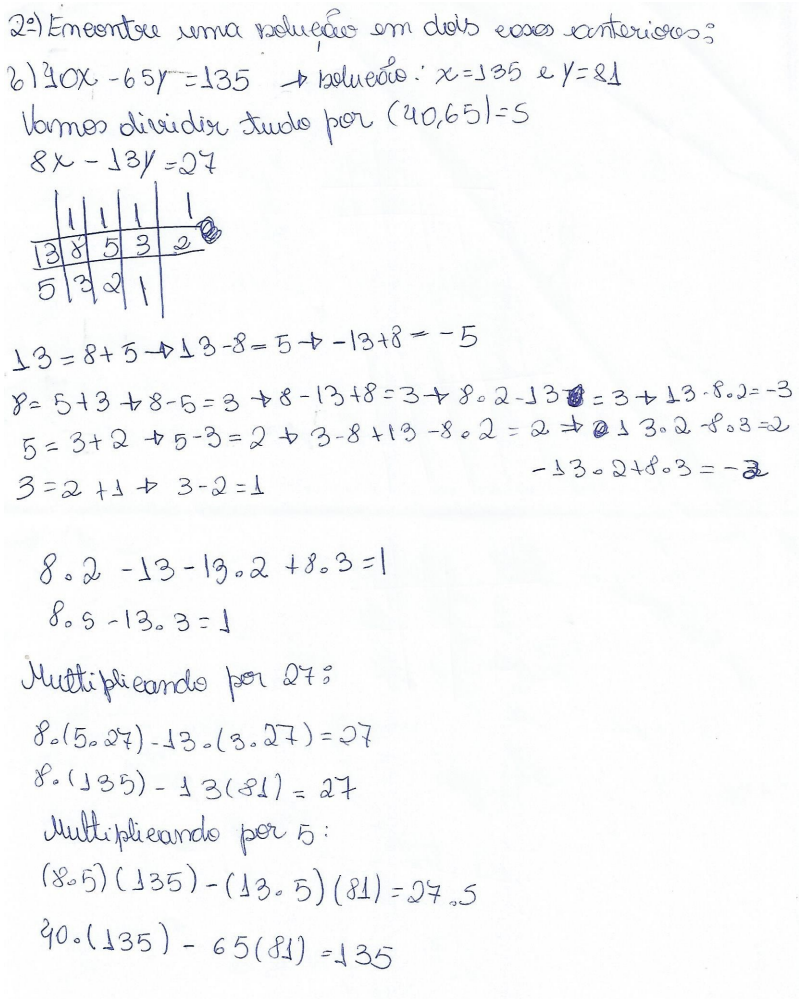


Figura 2.19: Estudante V

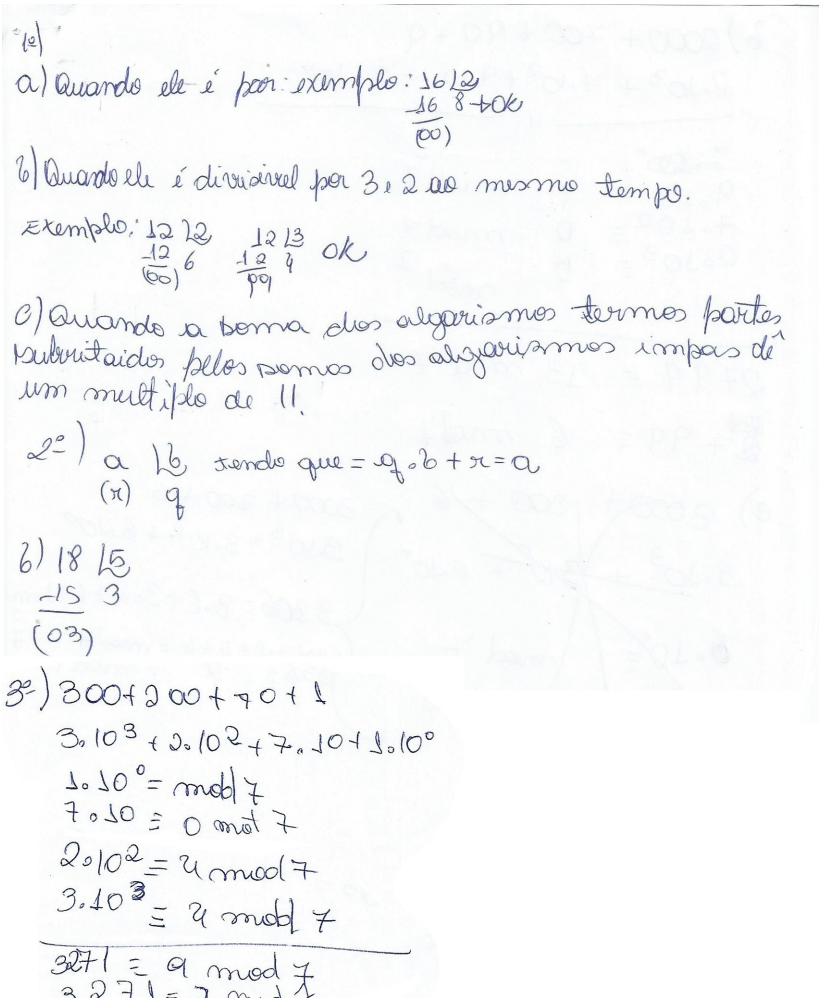


Figura 2.20: Estudante V

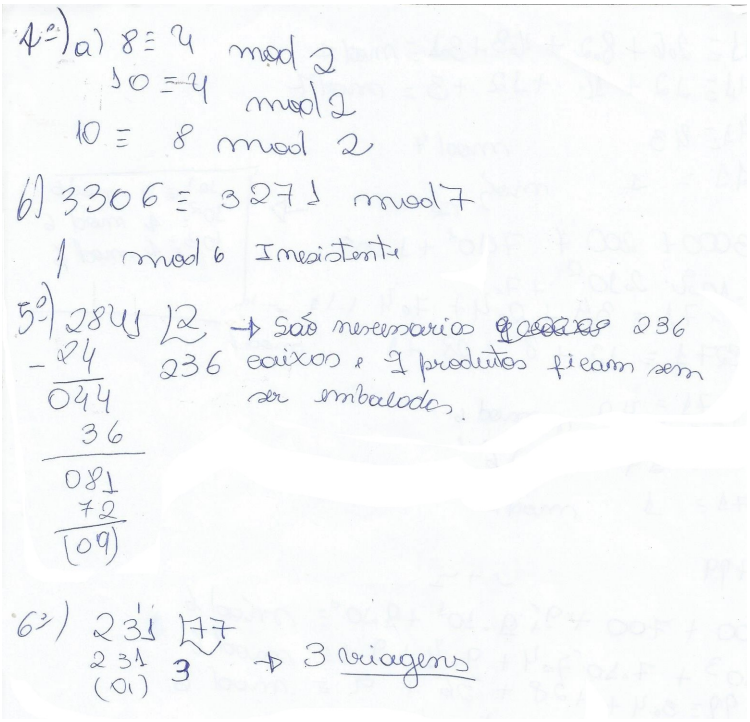


Figura 2.21: Estudante V

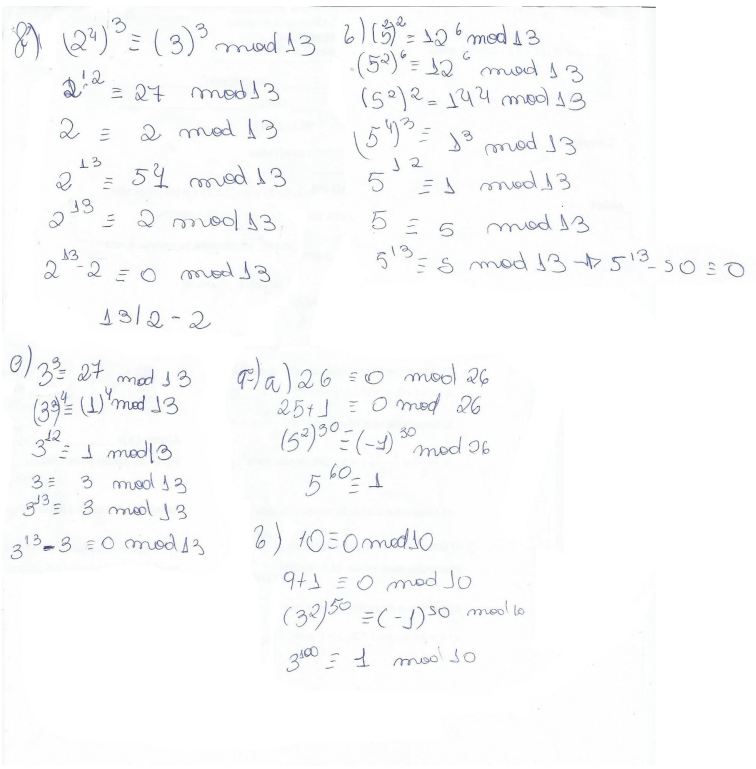


Figura 2.22: Estudante V

Referências Bibliográficas

[1] Alencar Filho, Edgard de, *Teoria elementar dos números*, 2ª edição, São Paulo: Nobel ,(1985).

[2] Brasil, Secretaria de Educação Fundamental, *Parâmetros curriculares nacionais* : Matemática, Brasília : MEC / SEF, (1998).

[3] Hefez, Abramo, *Elementos da Aritmética*, 2ª edição, Rio de Janeiro, (2006).

[4] Olimpíada Brasileira de Matemática das Escolas Públicas, Regulamentos da OBMEP, disponível em: *http://www.obmep.org.br/regulamentoOE.html*. Acesso em: 01/07/2014.

[5] Olimpíada Brasileira de Matemática das Escolas Públicas, OBMEP em números, disponível em: *http : //www.obmep.org.br/obmep_em_numeros.html*. Acesso em: 01/07/2014.

[6] BRASIL, Lei Nº 11.947, de 16 de junho de 2009. Dispõe sobre o atendimento da alimentação escolar e do Programa Dinheiro Direto na Escola aos alunos da educação básica; altera as Leis nos 10.880, de 9 de junho de 2004, 11.273, de 6 de fevereiro de 2006, 11.507, de 20 de julho de 2007; revoga dispositivos da Medida Provisória no 2.178-36, de 24 de agosto de 2001, e a Lei no 8.913, de 12 de julho de 1994; e dá outras providências. Diário Oficial [da União], Basília, 17 de junho de 2009.