
**UNIVERSIDADE ESTADUAL DO CEARÁ – UECE**
**CENTRO DE CIÊNCIAS E TECNOLOGIA**
**MESTRADO PROFISSIONAL EM MATEMÁTICA – PROFMAT**

Moésio Morais de Sales

# RESOLUÇÃO DE PROBLEMAS DE EQUAÇÕES DIOFANTINAS

**FORTALEZA – CEARÁ**
**2014**

Moésio Morais de Sales

# Resolução de Problemas de Equações Diofantinas

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, do centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do título de mestre em Matemática.

Orientador: Prof. Dr. José Othon Dantas Lopes

FORTALEZA – CEARÁ
2014

**Dados Internacionais de Catalogação na Publicação**

**Universidade Estadual do Ceará**

**Biblioteca Central Prof. Antônio Martins Filho**

**Bibliotecário(a) Responsável – Giordana Nascimento de Freitas CRB-3 / 1070**

S163r Sales, Moésio Morais de

Resolução de problemas de equações diofantinas / Moésio Morais de Sales. — 2014.

CD-ROM. 69 f. : il. (algumas color); 4 ¾ pol.

"CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico, acondicionado em caixa de DVD Slin (19 x 14 cm x 7 mm)".

Dissertação (mestrado) – Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Curso de Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2014.

Área de concentração: Matemática.

Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Teoria dos números. 2. Equações diofantinas. 3. Números inteiros. 4. Pari/GP. I. Título.

CDD: 510

**MOÉSIO MORAIS DE SALES**

**RESOLUÇÃO DE PROBLEMAS DE EQUAÇÕES DIOFANTINAS**

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia (CCT) da Universidade Estadual do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática, Área de Concentração Matemática.

Aprovada em: 13/03/2014.

BANCA EXAMINADORA

Prof. Dr. José Othon Dantas Lopes
Orientador e Presidente da Banca Examinadora
Universidade Estadual do Ceará – UECE/PROFMAT

Prof.Dr. Marcos Ferreira de Melo
Universidade Federal do Ceará – UFC

Prof. Dr. João Marques Pereira
Universidade Estadual do Ceará – UECE/PROFMAT

# *Agradecimentos*

A Deus pela vida.

A minha esposa e aos meus filhos, Jamile e Murilo

A todos meus familiares, amigos e irmãos.

A meu orientador , Professor José Othon Dantas Lopes.

Aos membros da banca e, de modo geral, a todos os docentes e colaboradores do Profmat - UECE, por sua valiosa colaboração e apoio, sem os quais este trabalho não teria sido realizado.

Ao nosso querido coordenador do Profmat UECE, Prof. Guilherme Ellery.

Aos meus pais, por terem acreditado na educação como elemento essencial para a minha vida e sempre buscaram me guiar neste caminho;

Outra vez, muito obrigado.

# *Resumo*

Vários problemas de matemática se resumem a resolver uma equação e em alguns casos o que nos interessa são as soluções inteiras destas equações e quando isto ocorre temos o que chamamos de uma Equação Diofantina. Nesta pesquisa é apresentado uma forma construtiva para resolução de problemas de teoria dos números que envolvem equações diofantinas, onde daremos especial atenção ao caso exponencial, além de apresentar uma aplicação na resolução de questões de ensino básico utilizando Pari/GP CALCULATOR Versão 2.5.0, também faremos um estudo sobre alguns teoremas pouco conhecidos mas que tem vital importância nas aplicações consideradas neste trabalho.

**Palavras-chave:** Teoria dos Números, Equações Diofantinas, Números Inteiros, Pari/GP.

# *Abstract*

Various math problems boil down to solve an equation and in some cases what interests us are the integer solutions of these equations and when this occurs we have what we call a Diophantine Equation. This research is presented a constructive way to solve problems involving number theory diophantine equations, where we will give special attention to the exponential case, and present an application in solving issues of basic education using Pari/GP CALCULATOR Version 2.5.0, we will also make a study of some theorems little known but which is vitally important in the applications considered in this work.

**Keywords:** Number Theory, Diophantine equations, Whole Numbers, Pari/GP.

# *Sumário*

# *Lista de Figuras*

# *Lista de Tabelas*

# 1 Introdução

Este trabalho tem como objetivo apresentar uma forma construtiva para resolução de questões de teoria dos números que envolvem equações diofantinas, onde trataremos casos em que as incógnitas estão nos expoentes.

Faremos inicialmente um estudo das equações diofantinas lineares e mostraremos algumas de suas aplicações de forma contextualizada, onde entendemos como contextualização algo que também pode esta inserido dentro de um contexto teórico, ou seja, que não está necessariamente vinculado a uma aplicação direta do cotidiano do aluno. Muitos acham que contextualizar é encontrar aplicações práticas para a Matemática a qualquer preço. Desta concepção resulta que um conteúdo que não se consegue contextualizar, não serve para ser ensinado.

Quando resolvemos problemas de teoria dos números, é muito importante os problemas em que é dada uma equação diofantina cujas incógnitas são expoentes. Há muitas maneiras de resolver tais equações: analisar módulo algum primo conveniente, utilizar métodos análogos à equação de Pell ou de Pitágoras, dentre estes consideraremos algumas técnicas como:

1. Fatoração;
2. Utilizar Congruências;
3. O uso do discriminante para equações quadráticas;
4. Método de descida infinita de Fermat;
5. Formas Especiais.

Neste trabalho faremos uma análise destas equações e aplicaremos as técnicas listadas acima. Também apresentaremos de forma mais detalhada o método através de congruências módulo algum primo ou potência de primos convenientes. Como auxilio utilizaremos uma ferramenta computacional o software Pari/GP o qual exploraremos suas vantagens no que tange a modelagem para situações de contorno que reduza o campo de solução para determinadas equações.

Trataremos, de fato, dois casos particulares de equações difantinas exponenciais que são:

$$a^x - b^y = c \tag{1.1}$$

e um caso mais particular

$$5^a 7^b + 4 = 3^c. \tag{1.2}$$

Aceitaremos em geral que vale a seguinte conjectura:

*" Considere a equação Diofantina exponencial*

$$a_1 b_{11}^{\alpha_1} \cdots b_{1l}^{\alpha_l} + \cdots + a_k b_{k1}^{\alpha_1} \cdots b_{kl}^{\alpha_l} = 0. \tag{1.3}$$

*Suponha que a equação 1.3 não tem solução em inteiros não negativos,* $\alpha_1, \cdots, \alpha_l, \cdots, \alpha_1, \cdots, \alpha_l$. *Então, a congruência*

$$a_1 b_{11}^{\alpha_1} \cdots b_{1l}^{\alpha_l} + \cdots + a_k b_{k1}^{\alpha_1} \cdots b_{kl}^{\alpha_l} \equiv 0 \pmod{m}$$

*não tem solução para algum inteiro* $m \geqslant 2$*."*

Discutiremos e levantaremos informações sobre as equações acima buscando fazer uma abordagem construtiva que favoreça o entendimento dos educandos em um contexto de educação básica.

No Capítulo 3, foi construído um comando no Pari/GP para análise das equações (1.1) e (1.2) módulo um inteiro $m$ e para alguns casos particulares das mesmas.

Finalmente, no Capítulo 4 apresentaremos algumas conclusões obtidas neste trabalho. Analisamos as vantagens da utilização do Pari/GP relativo a soluções de problemas de aritmética.

Este trabalho está dividido em quatro capítulos:

- Introdução
- Fundamentos de Teoria dos Números
- Aplicações nas Soluções de problemas
- Conclusões

## 1.1 Objetivo Geral

Fazer uma bordagem elementar das soluções das equações diofantinas lineares e exponenciais de forma intuitiva e construtiva utilizando o software Pari/GP CALCULATOR Versão 2.5.0, aplicando-o de forma a simular e explorar as situações de contorno que possa reduzir o conjunto domínio das soluções dessas equações.

## 1.2 Objetivos Específicos

As atividades de pesquisa bibliográfica e experimentos realizados durante a execução dos trabalhos descritos nessa dissertação foram distribuídos nos seguintes objetivos específicos:

- Realizar estudo sobre os teoremas fundamentais de teoria dos números que envolvem divisibilidade e conceitos de números inteiros e naturais.
- Realizar estudo sobre os teoremas fundamentais de congruência com ênfase nas equações diofantinas lineares e exponenciais.
- Explorar as situações de contorno das soluções das equações $a^x - b^y = c$ e $5^a 7^b + 4 = 3^c$ que favorecem as aplicações do software Pari/GP CALCULATOR Versão 2.5.0 como ferramenta de teste e análise.

## 1.3 Metodologia

Utilizaremos a pesquisa exploratória, pois não iremos fazer testes que comprovem que esse é o melhor método para solucionar as equações consideradas, iremos apenas nos aprofundar neste assunto.

"A pesquisa exploratória não requer a elaboração de hipóteses a serem testadas no trabalho, restringindo-se a definir objetivos e buscar mais informações sobre determinado assunto de estudo. [...] realiza descrições precisas da situação e quer descobrir as relações existentes entre seus elementos componentes". (CERVO,2009, p.63)

No Capítulo 2, apresentamos os conceitos de divisibilidade e congruência relativa a números inteiros e naturais e suas principais propriedades. Trataremos também alguns problemas sobre equações diofantinas lineares e teorema chinês dos restos e no Capítulo 3 desenvolveremos uma aplicação onde estudaremos e discutiremos a praticidade do método proposto. Para alcançar o objetivo final foi necessário utilizar diversos conceitos e resultados de Teoria de Números. Além disso, nos problemas sobre equações diofantinas exponenciais foi necessário considerarmos as conjecturas de Skolem e Pillai, baseado na aceitação destas utilizamos o Pari/GP para testar e encontrar um módulo adequado para solucionar as equações.

# 2 Fundamentos de Teoria dos Números

Neste capítulo veremos os tópicos básicos de teoria dos números, como propriedades de números inteiros, divisibilidade, congruências e aritmética módulo $m$, mostraremos também algumas aplicações do Teorema Chinês dos Restos e complementaremos com o estudo de equações diofantinas, mais especificamente das equações diofantinas exponenciais.

Todas as secções deste capítulo são adaptações baseadas em LANDAU(2002), HEFEZ(2011) e NIVEN, ZUCKERMAN(1960).

## 2.1 Relações de Equivalência

Chamamos de *Relações de Equivalência* as relações em um conjunto $X$ que satisfaz as propriedades:

- $\forall a \in X,\ a \sim a$ (reflexividade)
- $\forall a,b \in X,\ a \sim b \Rightarrow\ b \sim a$ (simetria)
- $\forall a,b,c \in X,\ a \sim b\ e\ b \sim c\ \Rightarrow a \sim c$ (transitividade)

Dada uma relação de equivalência $\sim$ sobre um conjunto $X$ e um elemento $x \in X$ definimos a *classe de equivalência* $\bar{x}$ de $x$ como

$$\bar{x} = \{y \in X | y \sim x\}.$$

MOREIRA(2005) observa que dada uma relação $\sim$, como descrito acima, temos que:

> " $x \sim y$ se, e somente se, $\bar{x} = \bar{y}$. As classes de equivalência formam uma partição de $X$, i.e., uma coleção de subconjuntos não vazios e disjuntos de $X$ cuja união é $X$. O conjunto $\{\bar{x} | x \in X\}$ das classes de equivalência é chamado o *quociente* de $X$ pela relação de equivalência $\sim$ e é denotado por $X/\sim$. "

## 2.2 Relação de Ordem

Para HALMOS(2001):

> ” Uma **Ordem Parcial** (ou, algumas vezes, ordem, simplesmente) em um conjunto $X$ é uma relação reflexiva, anti-simétrica, e transitiva. É costume usar somente um símbolo (ou algum outro tipograficamente próximo) para a maioria das ordens parciais na maior parte dos conjuntos; o símbolo de uso comum é sinal de desigualdade. Assim uma ordem parcial em $X$ pode ser definida pela relação $\leq$ em $X$ tal que, para todo $x$, $y$ e $z$ em $X$, temos **(i)** $x \leq x$**, (ii) se** $x \leq y$ **e** $y \leq x$**, então** $x = y$**, e (iii) se** $x \leq y$ **e** $y \leq z$**, então** $x \leq z$. [...] Se para todo $x$ e $y$ em $X$ acontece $x \leq y$ ou se $y \leq x$, então $\leq$ é dita uma **Ordem Total**. ”

## 2.3 Números Inteiros e Divisibilidade

A aritmética é o estudo sobre números naturais e suas propriedades. Os números naturais tiveram suas origens como modelo abstrato de contagem de objetos, eles aparecem naturalmente sempre que se quer dar ordem e contar objetos (um, dois, três, quatro, ....). Para LIMA(2007) isto foi uma evolução lenta que se deu a medida que a humanidade se civilizava.

Representaremos por $\mathbb{N}$ o conjunto dos números naturais. Uma construção consistente do Conjunto dos Números Naturais $(\mathbb{N})$ foi desenvolvida no século XIX por Giuseppe Peano. Essa construção, comumente chamada de Axiomas de Peano, é uma estrutura simples e elegante, servindo como um bom exemplo, de construção de conjuntos numéricos. Definimos sobre este conjunto as operações adição $(+)$ e multiplicação $(.)$, que possuem às seguintes propriedades:

1. São bem definidas, ou seja, para todos $a,\ b,\ a'\ e\ b' \in \mathbb{N}$, se $a = b$ e $a' = b'$ então $a+b = a'+b'$ e $a \cdot b = a' \cdot b'$;
2. São comutativas, ou seja, para todos $a,\ b \in \mathbb{N}$ tem-se que $a+b = b+a\ e\ a \cdot b = b \cdot a$;
3. São associativas, ou seja, para todos $a,\ b,\ e\ c \in \mathbb{N}$ tem-se que $a+(b+c) = (a+b)+c$ e $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
4. Possuem elementos neutros, ou seja, para todo $a \in \mathbb{N}$, $a+0 = a$ e $a \cdot 1 = a$;
5. A multiplicação é distributiva com relação à adição, ou seja, para todos $a,\ b,\ c\ \in \mathbb{N}$ tem-se $a \cdot (b+c) = (a \cdot b)+(a \cdot c)$.

   Considera-se ainda que os números naturais possuem as seguintes propriedades:

6. **Integridade**, ou seja, dados $a,\ b \in \mathbb{N}$, com $a$, $b$ diferentes de zero, tem-se que $a \cdot b$ é diferente de zero.
   De maneira equivalente pode-se dizer que se $a \cdot b = 0$ então $a = 0$ ou $b = 0$;
7. **Tricotomia**: Dados $a,\ b \in \mathbb{N}$ se verifica apenas uma das seguintes possibilidades:
   (a) $a = b$;
   (b) existe $c \in \mathbb{N}$, com $c \neq 0$, $b = a+c$;
   (c) existe $c \in \mathbb{N}$, com $c \neq 0$, $a = b+c$

**Definição 2.3.1.** *Diz-se que $a$ é menor do que $b$ e simboliza-se por $a < b$, sempre que se verifica a propriedade $(b)$. Diz-se que $a$ é maior do que $b$, e simboliza-se por $a > b$, sempre que se verifica a propriedade $(c)$. Adicionalmente, conclui-se, das definições acima, que $0 < a$ para todo número natural.*

Assim, segundo HEFEZ(2007):

> "[...] a tricotomia nos diz que, dados $a,\ b\ \in \mathbb{N}$, uma, e somente uma, das seguintes condições é verificada:
>
> (i) $a = b$
>
> (ii) $a < b$
>
> (iii) $a > b$ "

Com relação definição 2.3.1, HEFEZ(2007) observa que:

> "para $a$ e $b$, números naturais, se $a+b=0$ então, $a=b=0$. Realmente, se $a>0$ tem-se que $b<0$, o que é absurdo. Portanto, $a=0$. De maneira similar mostra-se que $b=0$. Logo, se $a>0$ ou $b>0$ então $a+b>0$."

**Proposição 2.3.1.** *Para todo $a \in \mathbb{N}$ tem-se que $a \cdot 0 = 0$.*

**Demonstração 2.3.1.** *De fato, $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Se $a \cdot 0 > 0$ então, da afirmação anterior, segue que $a \cdot 0 > a \cdot 0$, o que é absurdo. Logo $a \cdot 0 = 0$.*

**Proposição 2.3.2.** *Para relação "menor do que" vale a lei do cancelamento para a adição, ou seja, para todo $a,\ b,\ c \in \mathbb{N}$, $a < b$ se, e somente se, $a + c < b + c$.*

**Demonstração 2.3.2.** *Suponha $a < b$. Isso significa que existe $d > 0$, tal que $b = a + d$. Somando $c$ a ambos os lados desta igualdade tem-se, pelas propriedades da adição:*

$$b + c = c + b = c + (a + d) = (c + a) + d = (a + c) + d,$$

*o que mostra que $a + c < b + c$.*

*Reciprocamente, suponha que $a + c < b + c$. Pela tricotomia, temos três possibilidades:*

*(i) $a = b$. Isto acarretaria $a + c = b + c$, portanto falso.*

*(ii) $b < a$. Isto acarretaria, pela primeira parte da demonstração, que $b + c < a + c$; também é falso.*

*(iii) $a < b$. Esta é única possibilidade que resta.*

**Proposição 2.3.3.** *No que se refere à relação "menor do que" vale a lei do cancelamento para a multiplicação, ou seja, para todo $a,\ b,\ e\ c \in \mathbb{N}$ com $c > 0$, tem-se que $a < b$ se, e somente se, $a \cdot c < b \cdot c$.*

**Demonstração 2.3.3.** *Suponha $a < b$. Isso significa que existe $d > 0$, tal que $b = a + d$. Multiplicando por $c > 0$ a ambos os lados desta igualdade tem-se, pelas propriedades comutativa e distributiva da multiplicação, decorre:*

$$b \cdot c = c \cdot b = c \cdot (a + d) = (c \cdot a) + (c \cdot d) = (a \cdot c) + (c \cdot d),$$

*o que mostra que $a \cdot c < b \cdot c$, pois, pela integridade, $c \cdot d$ é diferente de zero.*

*Reciprocamente, suponha que $a \cdot c < b \cdot c$. Pela tricotomia, temos três possibilidades a analisar:*

*(i) $a = b$. Isto acarretaria $a \cdot c = b \cdot c$, o que é falso.*

*(ii) $b < a$. Isto acarretaria, pela primeira parte da demonstração, que $b \cdot c < a \cdot b$, o que também é falso.*

*(iii) $a < b$. Esta é única possibilidade válida.*

**Proposição 2.3.4.** *No que se refere à igualdade vale a lei do cancelamento para a adição, ou seja, para todo $a,\ b,\ c \in \mathbb{N}$, $a = b$ se, e somente se, $a + c = b + c$.*

**Demonstração 2.3.4.** *Pelo fato da adição ser bem definida vale que, se $a = b$ então $a + c = b + c$.*

*Reciprocamente, supondo que $a + c = b + c$ existem três possibilidades:*

1. *$a < b$. Pela proposição 2.1.2, $a + c = b + c$ o que é absurdo.*
2. *$b < a$. Pela mesma proposição, $b + c = a + c$, o que também é absurdo.*
3. *Logo, $a = b$.*

Note que relação ”menor do que” não é reflexiva, pois não vale $a < a$. No entanto a relação ”menor ou igual a”, descrita abaixo, o é.

Diz-se que $a$ é menor ou igual a $b$, e simboliza-se por $a \leqslant b$, sempre que $a < b$ ou $a = b$. Diz-se que $a$ é maior ou igual a $b$, e simboliza-se por $a \geqslant b$ sempre que $a > b$ ou $a = b$.

A relação ”menor ou igual a” é, de fato, uma relação de ordem, pois,

1. É reflexiva: para todo $a$, $a \leqslant a$.
2. É antissimétrica: para todos $a,\ b$, se $a \leqslant b$ e $b \leqslant a$ então $a = b$.
3. É transitiva: para todos $a,\ b$, e $c$, se $a \leqslant b$ e $b \leqslant c$ então $a \leqslant c$.

**Princípio 2.3.1. (Boa Ordem)** *Todo conjunto não-vazio de números naturais possui um menor elemento.*

### 2.3.1 O Conjunto dos Números Inteiros ($\mathbb{Z}$)

Chama-se conjunto dos números inteiros, que representaremos por $\mathbb{Z}$, a reunião $\mathbb{N} \cup \{0\} \cup (-\mathbb{N})$, dos números naturais com o zero e o conjunto $-\mathbb{N}$ dos números negativos.

## 2.4 Divisão euclidiana e o teorema fundamental da aritmética

A divisão euclidiana, ou divisão com resto, é uma das quatro operaçoes que toda criança aprende na escola. Sua formulação precisa é: dados $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ existem $q, r \in \mathbb{Z}$ com $0 \leq r < |b|$ e $a = bq + r$. Tais $q$ e $r$ estão unicamente determinados e são chamados o *quociente* e *resto* da divisão de $a$ por $b$. Se $b > 0$ podemos definir $q = \lfloor a/b \rfloor$ e se $b < 0$, $q = \lceil a/b \rceil$; em qualquer caso, $r = a - bq$. O resto $r$ é ás vezes denotado por $a \pmod{\mathrm{b}}$; definimos $a \pmod{0} = a$. Lembramos que $\lfloor x \rfloor$ denota o único inteiro $k$ tal que $k \leq x < k+1$ e $\lceil x \rceil$ o único inteiro $k$ tal que $k - 1 < x \leq k$.

**Definição 2.4.1.** *Dados dois inteiros $a$ e $b$ (em geral com $b \neq 0$) dizemos que $b$ divide $a$, ou que $a$ é um múltiplo de $b$, e escrevemos $b|a$, se existir $q \in \mathbb{Z}$ com $a = qb$. Se $a \neq 0$, também dizemos que $b$ é um divisor de $a$.*

**Proposição 2.4.1.** *Dados $a, b \in \mathbb{Z}$ existe um único $d \in \mathbb{N}$ tal que $d|a$, $d|b$ e, para todo $c \in \mathbb{N}$, se $c|a$ e $c|b$ então $c|d$. Além disso existem $x, y \in \mathbb{Z}$ com $d = ax + by$.*

Esse natural $d$ é chamado o *máximo divisor comum*, ou mdc, entre $a$ e $b$. Escrevemos $d = (a, b)$.

**Demonstração 2.4.1.** *O caso $a = b = 0$ é trivial (temos $d = 0$). Nos outros casos, seja $I(a,b) = \{ax + by; x, y \in \mathbb{Z}\}$ e seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a,b)$. Como $d \in \mathbb{N}^*$, existem $q, r \in \mathbb{Z}$ com $a = dq + r$ e $0 \leq r < d$. Temos $r = a - dq = a(1 - qx_0) + b(-qy_0) \in I(a,b)$; como $r < d$ e $d$ é o menor elemento positivo de $I(a,b)$, $r = 0$ e $d|a$. Analogamente, $d|b$. Suponha agora que $c|a$ e $c|b$; temos $c|ax + by$ para quaisquer valores de $x$ e $y$ donde, em particular, $c|d$.* □

**Proposição 2.4.2.** *Se $(a,b) = 1$ e $a|bc$ então $a|c$.*

**Demonstração 2.4.2.** *Como $(a,b) = 1$, existem $x, y \in \mathbb{Z}$ com $ax + by = 1$, logo $a|c = acx + bcy$.* □

Quando $(a,b) = 1$ dizemos que $a$ e $b$ são *primos entre si*. Um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de $p$ são $1$ e $p$. Um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e $n$.

Claramente, se $p$ é primo e $p \nmid a$ temos $(p,a) = 1$.

No que fizemos acima na proposição 2.4.1, temos uma forma mais próxima do que se faz no ensino fundamental que segundo HEFEZ(2011, p.54):

> "[...]como se faz usualmente no ensino fundamental definir o máximo divisor comum de dois números $a$ e $b$ como sendo o maior elemento do conjunto de todos os divisores comuns desses números, o que de imediato garantiria a sua existência."

Hefez destaca que seria necessário provar como fizemos na Proposição 2.4.1 que para todo $c \in \mathbb{N}$, se $c|a$ e $c|b$ então $c|d$. Tal propriedade é fundamental para provar propriedades subsequêntes.

**Lema 2.4.1** (**Lema de Euclides).** *Sejam $a$, $b$, $n \in \mathbb{N}$ com $a < na < b$. Se existe $(a, b-na)$, então $(a,b)$ existe e*

$$(a,b) = (a,b-na)$$

**Demonstração 2.4.3.** *Seja $d = (a,b-na)$. Como $d \mid a$ e $d \mid (b-na)$, segue que $d$ divide $b = b-na+na$. Logo, $d$ é um divisor comum de $a$ e $b$. Suponhamos agora que $c$ seja um divisor comum de $a$ e $b$; logo, $c$ é divisor comum de $a$ e $b-na$ e, portanto, $c \mid d$. Isso prova que $d = (a,b)$.* □

Com a mesma técnica usada para provar o Lema de Euclides segundo HEFEZ(2011) poderíamos provar:

**Observação 2.4.1.** *Para todo $a$, $b$, $n \in \mathbb{N}$,*

$$(a,b) = (a,b+na)$$

*ou que, se $na > b$, então*

$$(a,b) = (a,na-b).$$

Agora faremos uma prova que traz um algoritmo incluso que será útil para encontrar soluções de uma equação diofantina linear, a qual estudaremos mais a frente.

Para HEFEZ(2011, p. 56) trata-se de uma:

> "[..] prova construtiva da existência do $mdc$ dada por Euclides (Os Elementos, Livro VII, Proposição 2). O método chamado Algoritmo de Euclides, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios."

A prova que apresentaremos encontra-se em HEFEZ(2011, p. 56-57).

## Algoritmo de Euclides

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

$$b = aq_1 + r_1, \text{com } r_1 < a.$$

Temos duas possibilidades:

1. $r_1 \mid a$, em tal caso, pela proposição 2.4.1 e pelo Lema 2.4.1,

$$r_1 = (a,r_1) = (a,b-q_1a) = (a,b),$$

e termina o algoritmo, ou

2. $r_1 \nmid a$, e, em tal caso, podemos efetuar a divisão de $a$ por $r_1$, obtendo

$$a = r_1 q_2 + r_2, \text{com } r_2 < r_1.$$

Novamente temos duas possibilidades:

(a) $r_2 \mid r_1$, e, em tal caso, novamente, pela proposição 2.4.1 e pelo Lema 2.4.1,

$$r_2 = (r_1, r_2) = (r_1, a - q_2 r_1) = (r_1, a) = (b - q_1 a, a) = (b, a) = (a, b),$$

e paramos, pois termina o algoritmo, ou

(b) $r_2 \nmid r_1$, e, em tal caso, podemos efetuar a divisão de $r_1$ por $r_2$, obtendo

$$r_1 = r_2 q_3 + r_3, \text{com } r_3 < r_2.$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pela propriedade da Boa Ordem. Logo para algum $n$, temos que $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$.

□

O algoritmo acima pode ser sintetizado e realizado na prática, como mostraremos a seguir.

Inicialmente, efetuamos a divisão $b = aq_1 + r_1$ e colocamos os números envolvidos em um diagrama conforme a Tabela 2.1.

| | $q_1$ | |
|---|---|---|
| $b$ | $a$ | |
| $r_1$ | | |

**Tabela 2.1:** *Algoritmo de Euclides I*

A seguir, continuamos efetuando a divisão $a = r_1 q_1 + r_2$ e colocamos os números envolvidos no diagrama da Tabela 2.2.

| | $q_1$ | $q_2$ | |
|---|---|---|---|
| $b$ | $a$ | $r_1$ | |
| $r_1$ | $r_2$ | | |

**Tabela 2.2:** *Algoritmo de Euclides II*

Prosseguindo, enquanto for possível, teremos o resultado conforme a Tabela 2.3.

| | $q_1$ | $q_2$ | $q_3$ | $\cdots$ | $q_{n-1}$ | $q_n$ | $q_{n+1}$ |
|---|---|---|---|---|---|---|---|
| $b$ | $a$ | $r_1$ | $r_2$ | $\cdots$ | $r_{n-2}$ | $r_{n-1}$ | $r_n = (a, b)$ |
| $r_1$ | $r_2$ | $r_3$ | $r_4$ | $\cdots$ | $r_n$ | | |

**Tabela 2.3:** *Diagrama do Algoritmo de Euclides*

Supondo então que $r_{n+1}$ seja o primeiro resto nulo, tem-se: $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$ Desse modo, verifica-se que, nesse processo, o $(a, b)$ é o último resto diferente de zero.

## 2.5 Equações Diofantinas

Diofanto foi um matemático que acredita-se que viveu por volta de 250, em Alexandria. O único dado pessoal sobre Diofanto encontra-se, sob forma de problema, na chamada Antologia Grega do $5^o$ ou $6^o$ século:

> "Deus lhe concedeu ser menino pela sexta parte de sua vida, e somando uma dou décima. parte a isso cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma. sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! infeliz criança; depois de viver a metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida." (BOYER, 1991, p.121)

No que segue faremos uma breve revisão sobre alguns dos principais fatos relativos as equações diofantinas e suas propriedades. Faremos observações, enunciaremos as propriedades e algumas conjecturas relevantes para o estudo das equações diofantinas exponenciais. A definição que adotaremos para equação diofantinas está em MAIER(2005, p. 30).

**Definição 2.5.1.** *Uma equação em $n$ incógnitas $x_1,\ x_2,\ \cdots,\ x_n$ da forma*

$$f(x_1,x_2,\cdots,x_n)=0 \tag{2.1}$$

*é considerada uma equação* **Diofantina**, *quando temos interesse nas soluções inteiras $x_1, x_2,\ \cdots,\ x_n \in \mathbb{Z}$ dela.*

As relações

$$a_1x_1+a_2x_2+\cdots+a_nx_n=b \tag{2.2}$$

$$a_1{}^{x_1}+a_2{}^{x_2}+\cdots+a_n{}^{x_n}=b \tag{2.3}$$

$$A_1^{x_1}\cdots A_n^{x_n}-B_1^{y_1}\cdots B_m^{y_m}=C \tag{2.4}$$

são alguns exemplos de equações diofantinas, quando as $n,m$-uplas de coordenas inteiras $x_1,\ x_2,\ \cdots,\ x_n$ e $y_1,\ y_2,\ \cdots,\ y_m$ são procuradas.

Em particular a equação da forma 2.2 é chamada Diofantina Linear de grau $n$.

## 2.6 A equação Diofantina Linear de grau $2$

Trataremos agora da equação diofantina linear do tipo

$$ax+by=c$$

onde $a$, $b$ e $c \in \mathbb{Z}$.

**Teorema 2.6.1.** *Sejam $a$, $b$ e $c \in \mathbb{Z}$ não ambos zero.*

*a) A equação* **Diofantina**

$$ax + by = c \tag{2.5}$$

*admite solução* $x, y \in \mathbb{Z}$ *se, e somente se,* $d = (a,b) \mid c$.

*b) Suponha que* $d \mid c$ *e seja* $(x_o, y_o)$ *uma solução(particular) de 2.5. Então a solução geral (isto é, o conjunto de todas as soluções) de 2.5 é dada por*

$$\begin{cases} x &= x_o + \frac{b}{d}t \\ y &= y_o - \frac{a}{d}t \end{cases}$$

*com* $t \in \mathbb{Z}$.

**Demonstração 2.6.1.** *a) Como* $d \mid a$ *e* $d \mid b$ *temos também* $d \mid c$ *para qualquer possível solução* $(x,y)$ *de 2.5. Logo,* $d \mid c$ *é uma condição necessária para a solubilidade de 2.5. Reciprocamente, seja* $d \mid c$, *digamos* $dk = c$ *para algum* $k \in \mathbb{Z}$. *Pela proposição 2.4.1 sabemos que existem* $x_1$ , $y_1 \in \mathbb{Z}$ *com* $d = ax_1 + by_1$ . *Segue* $c = a(kx_1) + b(ky_1)$ *e vemos que* $(kx_1, ky_1)$ *é uma solução particular de 2.5.*

*b) Seja* $(x_0, y_0)$ *uma solução particular e* $t \in \mathbb{Z}$. *Primeiro, note que qualquer par de números* $\begin{cases} x &= x_o + \frac{b}{d}t \\ y &= y_o - \frac{a}{d}t \end{cases}$ *com* $t \in \mathbb{Z}$ *satisfaz a equação 2.5 também. De fato,*

$$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c.$$

*Seja reciprocamente* $(x,y)$ *uma solução qualquer de 2.5. Temos então* $ax_0 + by_0 = c = ax + by$ *e daí*

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

*Existem* $r,\ s \in \mathbb{Z}$ *tais que* $a = rd$ *e* $b = ds$ *e vale* $(r,s) = (\frac{a}{d}, \frac{b}{d}) = 1$. *Segue* $dr(x - x_0) = ds(y_0 - y)$ *e daí*

$$r(x - x_0) = s(y_0 - y),$$

*pois* $d \neq 0$. *Podemos supor* $a \neq 0$. *Concluímos* $r \mid s(y_0 - y)$ *e daí* $r \mid y_0 - y$ *pois* $(r,s) = 1$. *Logo existe* $t \in \mathbb{Z}$ *tal que* $rt = y_0 - y$ *de onde vem* $y = y_0 - rt = y_0 - \frac{a}{d}t$. *Segue* $r(x - x_0) = s(y_0 - y) = srt$ *e então* $x - x_0 = st$, *pois* $r \neq 0$. *Isto nos dá* $x = x_0 + st = x_0 + \frac{d}{b}t$. *Logo temos*

$$\begin{cases} x &= x_o + \frac{b}{d}t \\ y &= y_o - \frac{a}{d}t \end{cases}$$

*para algum* $t \in \mathbb{Z}$, *demonstrando assim a afirmação.*

□

**Corolário 2.6.1.** *Se* $(a,b) = 1$, *isto é, se* $a$ *e* $b$ *são relativamente primos (ou primos entre si), então a equação* $ax + by = c$ *sempre tem soluções inteiras, qualquer que seja* $c$.

**Demonstração 2.6.2.** *Basta tomar* $d = 1$ *no teorema 2.6.1.*

□

A demonstração do **ítem b)** do Teorema 2.6.1 constitui um algoritmo que é de fundamental importância prática na busca de soluções como afirma LA ROCQUE e PITOMBEIRA(1991, p. 41):

> "Para efeito de encontrar as soluções inteiras, o caso que interessa é só esse do corolário, em que $(a,b)=1$. De fato, se existir solução e esse máximo divisor comum for $d \neq 1$, basta dividir ambos os membros da equação por $d$ que se chega ao caso de coeficientes $a$ e $b$ relativamente primos, com um segundo membro ainda inteiro."

## 2.7 Congruências

Sejam $a,b,n \in \mathbb{Z}$. Dizemos que *$a$ é congruente a $b$ módulo $n$*, e escrevemos $a \equiv b \pmod{n}$[1], se $n|b-a$. Como a congruência módulo 0 é a igualdade e quaisquer inteiros são côngruos módulo 1, em geral estamos interessados em $n > 1$.

**Proposição 2.7.1.** *Para quaisquer $a,a',b,b',c,n \in \mathbb{Z}$ temos:*

*(a)* $a \equiv a \pmod{n}$*;*

*(b) se* $a \equiv b \pmod{n}$ *então* $b \equiv a \pmod{n}$*;*

*(c) se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$ *então* $a \equiv c \pmod{n}$*;*

*(d) se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a+b \equiv a'+b' \pmod{n}$*;*

*(e) se* $a \equiv a' \pmod{n}$ *então* $-a \equiv -a' \pmod{n}$*;*

*(f) se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a \cdot b \equiv a' \cdot b' \pmod{n}$.

**Demonstração 2.7.1.** *Para o item (a) basta observar que $n|a-a=0$. Em (b), se $n|b-a$ então $n|a-b=-(b-a)$. Em (c), se $n|b-a$ e $n|c-b$ então $n|c-a=(c-b)+(b-a)$. Em (d), se $n|a'-a$ e $n|b'-b$ então $n|(a'+b')-(a+b)=(a'-a)+(b'-b)$. Em (e), se $n|a'-a$ então $n|(-a')-(-a)=-(a'-a)$. Em (f), se $n|a'-a$ e $n|b'-b$ então $n|a'b'-ab=a'(b'-b)+b(a'-a)$.*

□

Os itens (a), (b) e (c) da Proposição 2.7.1 dizem, nesta ordem, que a relação "$\equiv \pmod{n}$" é uma relação reflexiva, simétrica e transitiva.

Utilizando a noção de classe de equivalência visto no inicio, definimos o quociente $\mathbb{Z}/(\equiv \pmod{n})$, que chamaremos por simplicidade de notação de $\mathbb{Z}/(n)$. Dado $a \in \mathbb{Z}$, definimos $\overline{a}$ como um subconjunto de $\mathbb{Z}$,

$$\overline{a} = \{x \in \mathbb{Z} |\ x \equiv a \pmod{n}\}.$$

[1] Essa notação foi introduzida por Gauss, que foi também o primeiro matemático a usar de forma sistemática a noção de congruência, em seu livro Disquisitiones Arithmeticae, publicado em 1801.

Temos que $\overline{a} = \overline{a'}$ se e somente se $a \equiv a' \pmod{n}$. Se $n > 0$, a divisão euclidiana diz que todo inteiro $a$ é côngruo a um único inteiro $a'$ com $0 \leq a' < n$ e estes são incongruentes entre si; podemos reescrever este fato na nosso nova linguagem como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Quando não houver possibilidade de confusão omitiremos as barras e chamaremos os elementos de $\mathbb{Z}/(n)$ simplesmente de $0, 1, \ldots, n-1$.

Os itens (d), (e) e (f) da Proposição 2.7.1 tem grande importância dentro da teoria, segundo MOREIRA(2005), eles dizem que:

> " [...] as operações de soma, diferença e produto são compatíveis com a relação de congruência. É esta propriedade que torna congruências tão úteis, nos possibilitando fazer contas módulo $n$."

**Proposição 2.7.2.** *Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod{n}$ se e somente se $(a,n) = 1$.*

**Demonstração 2.7.2.** *Se $ab \equiv 1 \pmod{n}$ temos $nk = 1 - ab$ para algum $k$, donde $(a,n) | ab + nk = 1$ e $(a,n) = 1$. Se $(a,n) = 1$ temos $ax + ny = 1$ para certos inteiros $x$ e $y$, donde $ax \equiv 1 \pmod{n}$.*

□

Dizemos portanto que $a$ é *invertível* módulo $n$ quando $(a,n) = 1$ e chamamos $b$ com $ab \equiv 1 \pmod{n}$ de *inverso* de $a$ módulo $n$. O inverso é sempre único módulo $n$: se $ab \equiv ab' \equiv 1 \pmod{n}$ temos $b \equiv ab^2 \equiv abb' \equiv b' \pmod{n}$.

**Proposição 2.7.3.** *Se $(a,n) = 1$ e $ab \equiv ab' \pmod{n}$ então $b \equiv b' \pmod{n}$.*

**Demonstração 2.7.3.** *Basta escrever $b \equiv abc \equiv ab'c \equiv b' \pmod{n}$ onde $c$ é o inverso de $a$ módulo $n$.*

□

**Teorema 2.7.1.** *Qualquer número inteiro é congruente $(\mathrm{mod\ n})$ com um e só um dos elementos de $\{0,\ 1,\ \cdots,\ n-1\}$.*

**Demonstração 2.7.4.** *Dados $n \in \mathbb{N}$ e $x \in \mathbb{Z}$, pelo teorema, existem $q$ e $r$ únicos tais que*

$$x = qn + r \quad 0 \leqslant r < n;$$

*portanto $x \equiv r \pmod{n}$ e $0 \leqslant r < n-1$. A unicidade resulta da unicidade do resto do algoritmo de Euclides.*

□

**Definição 2.7.1.** *Um conjunto $\{r_1, \cdots, r_n\}$ diz-se um sistema completo de resíduos módulo $n$, se para cada número inteiro $x$ existe um e um só $r_i$ tal que $x \equiv r_i \pmod{n}$.*

**Exemplo 2.7.1.** *O conjunto $14,\ 17,\ 18,\ 19,\ 22,\ 23,\ 34$ é um sistema completo de resíduos módulo $7$ pois, dividindo estes números por $7$ obtêm-se, respectivamente, $0,\ 3,\ 4,\ 5,\ 1,\ 2,$ e $6$.*

**Proposição 2.7.4.** *Todos os sistemas completos de resíduos para um mesmo módulo têm o mesmo número de elementos.*

**Demonstração 2.7.5.** *Consideremos um sistema completo de resíduos, digamos* $R = \{r_1, r_2, \cdots, r_k\}$*, para um módulo fixo* $n > 1$*; seja ainda* $R_0 = \{1, 2, \cdots, n-1\}$*. Como vimos acima, no Teorema 2.7.1, para cada* $j = 1, \cdots, k$*, existe um e só um* $i(j) \in R_0$ *tal que* $r_j \equiv i(j) \pmod{n}$*, portanto* $R_0$ *tem pelo menos o mesmo número de elementos que* $R$*; por outro lado,* $R$ *também um sistema completo de resíduos e, por definição, para cada elemento de* $R_0$ *existe um e só um elemento de* $R$ *com o qual aquele é congruente* $\pmod{n}$*, donde* $R$ *tem pelo menos tantos elementos como* $R_0$*. Em suma:* $R$ *e* $R_0$ *têm o mesmo número* $n$ *de elementos.*

□

## 2.8 A função de Euler e o pequeno teorema de Fermat

Discutiremos agora alguns resultados sobre a função $\phi$(fi) de Euler[2] e o Teorema de Fermat. A primeira é uma função aritmética que tem diversas aplicações em teoria dos números. O conteúdo desta secção é baseado em HEFEZ(2011), com algumas modificações.

**Definição 2.8.1.** *Um sistema de reduzido de resíduos módulo* $m$ *é um conjunto de números naturais* $r_1, r_2, \cdots, r_s$ *tais que*

*a)* $(r_i, m) = 1$*, para todo* $i = 1, 2, \cdots, s$*;*

*b)* $r_i \not\equiv r_j \pmod{\mathrm{m}}$*, se* $i \neq j$*;*

*c) Para cada* $n \in \mathbb{N}$ *tal que* $(n, m) = 1$*, existe* $i$ *tal que* $n \equiv r_i \pmod{\mathrm{m}}$*.*

Designaremos por $\phi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m$ , que corresponde à quantidade de números naturais entre $0$ e $m-1$ que são primos com $m$. Defini-se:

$$\phi : \mathbb{N}^* \longrightarrow \mathbb{N},$$

onde $\phi(m) = \#\{x \in \mathbb{N}; 1 \leq x \leq m \ e \ (x, m) = 1\}$ chamada de função *fi de Euler*. De acordo com a definição

$$\phi(m) \leqslant m - 1.$$

**Proposição 2.8.1.** *Seja* $m \in \mathbb{N}^*$ *,* $\phi(m) = m - 1$ *se, e somente se,* $m$ *é um número primo.*

**Demonstração 2.8.1.** *Como* $m$ *é primo se, e somente se,* $1, 2, \cdots, m-1$ *formam um sistema reduzido de resíduos módulo* $m$*, o que equivale a dizer que* $\phi(m) = m - 1$*.*

□

**Proposição 2.8.2.** *Sejam* $r_1, \cdots, r_{\phi(m)}$ *um sistema reduzido de resíduos módulo* $m$ *e seja* $a \in \mathbb{N}$ *tal que* $(a, m) = 1$*. Então,* $ar_1, \cdots, ar_{\phi(m)}$ *é um sistema reduzido de resíduos módulo* $m$*.*

[2] Leonhard Paul Euler foi um grande matemático suíço ele trabalhou em quase todas as áreas da matemática: geometria, cálculo infinitesimal, trigonometria, álgebra e teoria dos números, bem como deu continuidade na física, newtoniana, teoria lunar e outras áreas da física.

**Demonstração 2.8.2.** *Seja $a_1, \cdots, a_m$ um sistema completo de resíduos módulo $m$ do qual foi retirado o sistema reduzido de resíduos $r_1, \cdots, r_{\phi(m)}$. Do fato de que $(a,m) = 1$ se, e somente se, $(aa_i, m) = 1$, o resultado segue.*

□

**Teorema 2.8.1** (Euler)**.** *Sejam $m,\ a \in \mathbb{N}$ com $m > 1$ e $(a,m) = 1$. Então,*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

**Demonstração 2.8.3.** *Seja $r_1, \cdots, r_{\phi(m)}$ um sistema reduzido de resíduos módulo $m$. Logo, pela Proposição 2.8.2, $ar_1, \cdots, ar_{\phi(m)}$ formam um sistema reduzido de resíduos módulo $m$. Portanto,*

$$a^{\phi(m)} r_1 \cdot r_2 \cdots r_{\phi(m)} = ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} \pmod{m}$$

*Como $(r_1 \cdot r_2 \cdots r_{\phi(m)}, m) = 1$, segue-se da Proposição 2.7.3 que*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

□

**Corolário 2.8.1** (Pequeno Teorema de Fermat)**.** *Sejam $a,\ p \in \mathbb{N}$ onde $p$ é um número primo e $(a,p) = 1$. Tem-se que*

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Demonstração 2.8.4.** *Pelo teorema anterior $a^{\phi(p)} \equiv 1 \pmod{p}$ e como $\phi(p) = p - 1$, segue-se o resultado.*

□

Nos problemas que abordaremos no Capítulo 3 deste trabalho geralmente precisaremos encontrar um número natural $h$ tal que $a^h \equiv 1 \pmod{m}$, porém nem sempre esse número existe. No que segue mostraremos como utilizar e determinar esse número $h$.

Em primeiro lugar, e também como veremos no próximo capítulo isto será um fato bastante utilizado, para calcular o resto da divisão de uma potência $a^n$ por um número natural $m > 1$, é conveniente achar um número natural $h$ tal que $a^h \equiv 1 \pmod{m}$, pois se $n = hq + r$ pela divisão euclidiana de $n$ por $h$, teremos $a^n = a^{hq+r} = a^{hq} a^r \equiv a^r \pmod{m}$.

Agora, na proposição seguinte, veremos quando é possível determinar tal número $h$.

**Proposição 2.8.3.** *Dado $a \in \mathbb{N}^*$, existe $h \in \mathbb{N}^*$ tal que $a^h \equiv 1 \pmod{m}$ se, e somente se, $(a,m) = 1$.*

**Demonstração 2.8.5.** *Se $(a,m) = 1$, temos, pelo Teorema de Euler, que $a^{\phi(m)} \equiv 1 \pmod{m}$, mostrando a existência do expoente desejado. Por outro lado, se $(a,m) \neq 1$ do Teorema 2.6.1 temos que a equação $aX - mY = 1$ não possui solução e, portanto $aX \equiv 1 \pmod{m}$ não possui solução.*

*Consequentemente, não pode existir* $h > 1$ *tal que* $a^h \equiv 1 \pmod{m}$.

□

Na Proposição 2.8.3 foi caracterizado quando da existência de um número $h$ tal que $a^h \equiv 1 \pmod{m}$, mas é de importante valia saber qual o menor valor desse $h$. No que segue definiremos o conceito de ordem.

**Definição 2.8.2.** *Seja* $a,\ m \in \mathbb{N}^*$*, com* $m > 1$ *e* $(a,m) = 1$*. Chamaremos de* Ordem de $a$ com respeito a $m$ *o número natural*

$$ord_m(a) = \min\{i \in \mathbb{N}^*;\ a^i \equiv 1 \pmod{m}\}.$$

**Proposição 2.8.4.** *Temos que* $a^n \equiv 1 \pmod{m}$ *se, e somente se,* $ord_m(a)|n$.

**Demonstração 2.8.6.** *Suponha que* $ord_m(a)|n$*. Logo,* $n = r \cdot ord_m(a)$ *e, portanto,*

$$a^n = a^{r \cdot ord_m(a)} = \left(a^{ord_m(a)}\right)^r \equiv 1^r = 1 \pmod{m}.$$

*Reciprocamente, suponha que* $a^n \equiv 1 \pmod{m}$*. Queremos provar que* $ord_m(a)|n$*. Pela divisão euclidiana, podemos escrever* $n = ord_m(a)q + r$*, onde* $r < ord_m(a)$*. Suponha, por absurdo, que* $r \neq 0$*. Então,*

$$1 \equiv a^n \equiv a^{ord_m(a)q+r} = \left(a^{ord_m(a)}\right)^q a^r \equiv a^r,$$

*que é absurdo, pois* $0 < r < ord_m(a)$ *e* $ord_m(a)$ *é o menor expoente não nulo* $i$ *tal que* $a^i \equiv 1 \pmod{m}$.

□

**Corolário 2.8.2.** *Sejam* $a,\ m \in \mathbb{N}$*, com* $(a,m) = 1$*. Temos que* $ord_m(a)|\phi(m)$.

**Demonstração 2.8.7.** *Sendo* $(a,m) = 1$ *temos, pelo Teorema de Euler,* $a^{\phi(m)} \equiv 1 \pmod{m}$*, daí pela Proposição 2.8.4 resulta que* $ord_m(a)|\phi(m)$.

□

**Definição 2.8.3.** *Se* $ord_m(a) = \phi(m)$ *dizemos que* $a$ *é uma raiz primitiva módulo* $m$.

**Teorema 2.8.2.** *Sejam* $a,\ m \in \mathbb{N}$*, com* $(a,m) = 1$*. Temos que* $a^j \equiv a^k \pmod{m}$ *se, e somente se,* $ord_m(a)|j-k$.

**Demonstração 2.8.8.** *Suponhamos sem perda de generalidade que* $j > k$ *logo a congruência* $a^j \equiv a^k \pmod{m}$ *é equivalente a* $a^{j-k} \equiv 1 \pmod{m}$*, então pela Proposição 2.8.4, isso é verdade se, e somente se,* $ord_m(a)|j-k$.

□

É claro que $ord_m(a)|j-k$ é equivalente, por definição de congruência, a $j \equiv k \pmod{\mathrm{ord_m(a)}}$ ou $j \equiv k \pmod{\phi(\mathrm{m})}$.

Considere exemplo retirado de BURTON(1980, p.159):

**Exemplo 2.8.1.** *Vamos mostrar que se $F_n = 2^{2^n}+1$, $n>1$, é um primo, então $2$ não é uma raiz primitiva módulo $F_n$. (Claramente, $2$ é raiz primitiva módulo $5 = F_1$.) Nós temos*

$$2^{2^{n+1}} \equiv 1 \pmod{F_n}$$

*que implica que a ordem de $2$ módulo $F_n$ não excede $2^{n+1}$. Mas se $F_n$ é primo por hipótese,*

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

*e um argumento de indução simples confirma que $2^{2^n} > 2^{n+1}$, sempre que $n>1$. Assim a ordem de $2$ módulo $F_n$ é menor do que $\phi(F_n)$; pela Definição 2.8.3 vemos que $2$ não pode ser uma raiz primitiva de $F_n$.*

**Corolário 2.8.3.** *Sejam $a,\ m \in \mathbb{N}$, com $(a,m)=1$. Se $k = ord_m(a)$, então os números $1,a,a^2,\cdots,a^{k-1}$ são incongruentes módulo $m$.*

**Demonstração 2.8.9.** *Vamos supor que dois destes números sejam congruentes módulo $m$, isto é, $a^x \equiv a^y \pmod{m}$, $0 \leqslant x \leqslant k-1$, $0 \leqslant y \leqslant k-1$. Pelo Teorema 2.8.2, devemos ter $k|x-y$. Como ambos $x$ e $y$, são não-negativos e menores do que $k$, isto só poderá ocorrer se eles forem iguais. Assim concluímos que os números $1,a,a^2,\cdots,a^{k-1}$ são incongruentes módulo $m$.*

□

**Teorema 2.8.3.** *Se $a$ é uma raiz primitiva, então os números $a,a^2,\cdots,a^{\phi(m)}$ formam um sistema reduzido de resíduos módulo $m$ e que representaremos como $S^a_{(\mathrm{mod\ m})}$.*

**Demonstração 2.8.10.** *Como $a$ é uma raiz primitiva $k = ord_m(a) = \phi(m)$. Pelo Corolário 2.8.3, $1,a,a^2,\cdots,a^{\phi(m)-1}$ são todos incongruentes módulo $m$. Como $(a,m)=1$ a Proposição 2.8.2 nos garante que $a,a^2,\cdots,a^{\phi(m)}$ formam um sistema reduzido de resíduos módulo $m$.*

□

**Corolário 2.8.4.** *Sejam $a,\ m$ e $b \in \mathbb{N}$. Se $a$ é uma raiz primitiva módulo $m$ e $(b,m)=1$, então existe um e somente um $a^i \in \{a,a^2,\cdots,a^{\phi(m)}\}$ tal que $a^i \equiv b\,(\mathrm{mod\ m})$.*

**Demonstração 2.8.11.** *(**Existência**). Como $(b,m)=1$ por euclides temos para algum $q \in \mathbb{N}$ que $b = mq+r$, onde $0 \leqslant r \leqslant m-1$, logo $r \in \{0,1,\cdots,m-1\}$ e sendo $(b,m) = (mq+r,m) = (r,m) = 1$ assim $r$ pertence ao sistema reduzido de resíduos módulo $m$ e portanto para algum $a^i \in \{a,a^2,\cdots,a^{\phi(m)}\}$ temos que $a^i \equiv r\,(\mathrm{mod\ m})$.*

*(**Unicidade**). Se $a^j \in \{a,a^2,\cdots,a^{\phi(m)}\}$ é tal que $a^j \equiv r\,(\mathrm{mod\ m})$, então teríamos por transitividade que $a^i \equiv a^j\,(\mathrm{mod\ m})$ mais isso é verdade se, e somente se, $i=j$*

□

O expoente $i$ tal que $a^i \equiv b\,(\mathrm{mod\ m})$ se chama índice de $a$. Segundo NIVEN e ZUCKERMAN (1960), o índice depende de $m$ assim como de $b$ e seu comportamento é muito semelhante aos logarítmos.

**Observação 2.8.1.** *A Proposição 2.8.4, Corolário 2.8.2 e o Teorema 2.8.2 serão utilizados constantemente nos problemas do Capítulo 3 onde, em geral aplicaremos quando for necessário levantar informações sobre os expoentes de equações difantinas, como, por exemplo:*

$$a^x - b^y = c. \tag{2.6}$$

*Especificamente, quando tivermos algo como*

$$a^x \equiv b \pmod{m}, \tag{2.7}$$

*onde* $(a,m) = 1$ *e tomando* $h = ord_m(a)$*, então pela Proposição 2.8.3 , teremos duas situações:*

**a)** *se* $\phi(m) = ord_m(a) = h$*, ou seja, se a for raiz primitiva módulo* $m$*, então pelo Teorema 2.8.3*

$$S^a_{(\text{mod m})} = \{a, a^2, \cdots, a^{\phi(m)} \equiv 1\} \tag{2.8}$$

*é um sistema reduzido de resíduos módulo* $m$*. Daí temos, pelo Corolário 2.8.4, se* $(b,m) > 1$*, então não existe* $a^i \in S^a_{(\text{mod m})}$ *tal que* $a^i \equiv b \pmod{\text{m}}$*. Se, por outro lado,* $(b,m) = 1$*, então existe* $a^i \in S^a_{(\text{mod m})}$ *tal que* $a^i \equiv b \pmod{\text{m}}$*.*

*Dessa foma se tivermos interessados em levantar informações sobre o expoente* $x$ *da equação 2.6, como* $a^h \equiv 1 \pmod{\text{m}}$ *e supondo* $(b,m) = 1$*, logo existe* $r \in \{1, 2, \cdots, \phi(m)\}$ *tal que* $a^r \equiv b \pmod{\text{m}}$ *e portanto para todo* $k \in \mathbb{N}$*, temos*

$$a^{hk+r} \equiv b \pmod{\text{m}}$$

*e por transitividade*

$$a^{hk+r} \equiv a^x \pmod{\text{m}},$$

*então pelo Teorema 2.8.2, temos que*

$$x \equiv r \pmod{\text{h}}^{3}.$$

**b)** *se* $\phi(m) \neq ord_m(a) = h$*. Neste caso o conjunto* $I = \{1, a, a^2, \cdots, a^{h-2}, a^{h-1}\}$ *são formados por elementos incongruentes módulo* $m$ *(Corolário 2.8.3) e como* $ord_m(a) \mid \phi(m) \Rightarrow ord_m(a) < \phi(m)$ *este conjunto não é um sistema completo de resíduos. Nesta situação as soluções se tornam mais restritas, pois dado*

$$a^x \equiv b \pmod{m},$$

*e* $b \equiv r \pmod{\text{m}}$*, temos:*

**(i)** *se* $r \in I$ *então exite* $k$ *tal que*

$$a^k \equiv r \pmod{m},$$

[3] De fato, $h|hk + r - x \Longleftrightarrow hw = hk + r - x$ para algum $w \in \mathbb{N}$. Portanto, $x = h(k-w) + r$, com $0 \leqslant r < h$, que significa que $x \equiv r \pmod{\text{h}}$.

**(ii)** *se $r \notin I$, então para todo $k$*

$$a^k \not\equiv r \pmod{m}.$$

## 2.9 O Pari/GP

O software que usaremos ao longo deste trabalho chama-se o Pari/GP, distribuído segundo a licença GPL[4]. Pode ser obtido no sítio http://pari.math.u-bordeaux.fr. Existem binários para MSWindows e está disponível nos repositórios das distribuições mais importantes de Linux.

Para construirmos as funções precisaremos de um editor de texto ou, no nosso caso utilizaremos diretamente o *Prompt de Comando* ou *Shell*[5] dentro do *Terminal* que são as janelas onde rodamos o Shell.

Em geral o Pari/GP trabalha com inteiros de Gauss e Eisenstein e muito mais, e tem várias funções avançadas. Para o trabalho em teoria elementar dos números conta com ferramentas como: fatoração em primos, resolução de Pell, Bezout, sistemas de congruências, função phi de Euler, entre outros.

Para STEIN(2001, p. 1)

> ”Muito do progresso na teoria dos números tem sido impulsionada por tentativas de provar conjecturas. É razoavelmente fácil de brincar com números inteiros, ver um padrão, e fazer uma conjectura. Frequentemente provar uma conjectura é extremamente difícil. Nesse sentido, os computadores ajudam-nos a:
>
> - encontrar mais conjecturas
> - refutar conjecturas
> - aumentar a nossa confiança em uma conjectura”.

Ainda segundo STEIN(2001) os software como o Pari/GP também frequentemente podem ajudar a resolver um problema específico. Por exemplo,

> Determine todos os inteiros $n < 100$ tal que $n$ seja a área de um triângulo retângulo de lado inteiro.

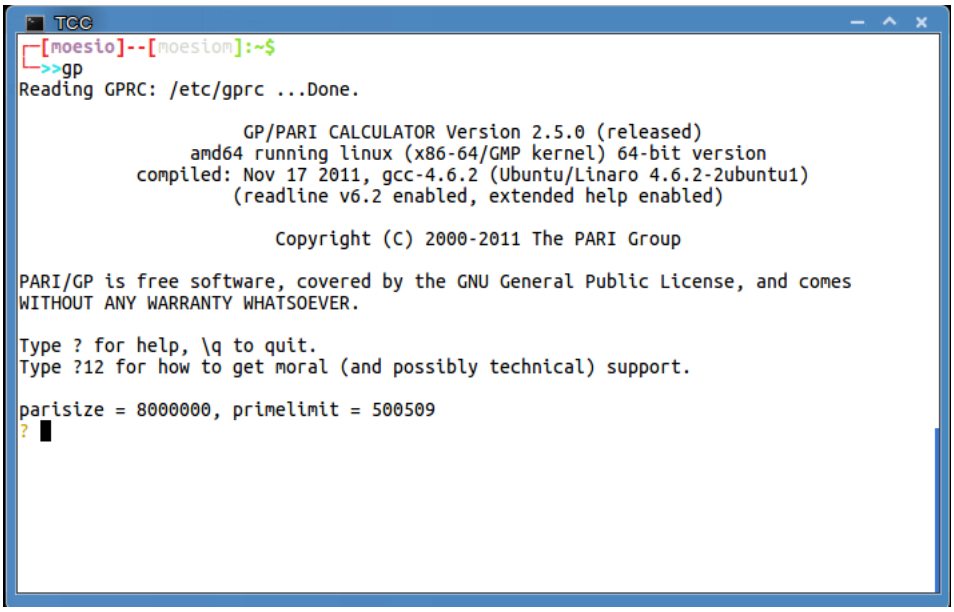
O problema acima demanda um tempo considerável para ser resolvido manualmente.

Para iniciar uma sessão do Pari/GP digitamos o comando ”gp” no terminal, na figura 2.1 temos uma sessão do Pari/GP.

[4] General Public License (Licença Pública Geral) é a licença com maior utilização por parte de projetos de software livre.

[5] Um programa que processa comandos.

**Figura 2.1:** *Tela inicial da sessão do Pari/GP*




### 2.9.1 Funções Definidas Pelo Utilizador

Nos casos que trataremos aqui neste trabalho combinaremos funções existentes no Pari/GP para formar outras funções. Esta é uma característica do Pari/GP conforme afirma PATRÍCIO(2009, p. 5):

> "É possível definir novas funções no Pari/GP. A sintaxe é
>
> `nome(lista de vari\'aveis formais) =`
> `local(lista de vari\'aveis locais); sequencia de comandos`"

**Exemplo 2.9.1.** *No exemplo queremos determinar a ordem de* $10$ *módulo* $17389$.

```
? znorder(Mod(10,17389))
%1 = 17388
```

No exemplo anterior 2.9.1, `Mod(10, 17389)` faz com que o programa considere $10$ como elemento do grupo das unidades do semigrupo multiplicativo do anel[6] $(Z/17389, +, \times)$, e `znorder` calcula a ordem deste elemento.

O Pari/GP foi utilizado neste trabalho para construções de algoritmos computacionais que facilitaram a simulação e teste de soluções e, por outro lado, este caráter exploratório de modelar os problemas aqui apresentados tem grande valia para o ensino do conteúdo.

[6] Detalhes sobre anéis e grupos podem ser visto em MOREIRA(2005) e NIVEN e ZUCKERMAN(1960).

## 2.10 Aplicações das Equações Diofantinas Lineares de Grau 2

No que segue apresentaremos uma uma proposta para trabalhar o tema ”equações diofantinas lineares” no Ensino Médio utilizando recursos computacionais. Faremos tal proposta sempre focando suas aplicações que é muito comum neste nível ensino como veremos nos problemas apresentados. Destacamos o tema como uma algo que transcende a sala de aula, pois segundo MACHADO(2009, p. 13):

> ”As matérias a serem estudadas não constituem um fim em si mesmo: elas são apenas um meio necessário para que a escola realize sua função de formação pessoal. A finalidade da Educação, em qualquer situação, sempre será a formação de pessoas e de profissionais competentes para a vida em sociedade e para a atuação no universo de trabalho”.

Ao contrário do que poderia parecer não é tão difícil desenvolver esse tema com os alunos do Ensino Médio. O desenvolvimento do tema não implica amplos conhecimentos teóricos, isto é, envolve conhecimentos já tratados no Ensino Fundamental e, portanto, trata-se de um objeto do saber passível de se tornar um objeto de ensino. Desejamos incentivar e sensibilizar os professores do Ensino Médio a incorporar esse conhecimento em suas aulas, dada a sua utilidade e a simplicidade de seu desenvolvimento.

Muitos problemas de Matemática são provenientes de situações concretas que envolvem número de pessoas, peças, etc. e requerem soluções inteiras positivas. Nesses casos, deve-se buscar entre as soluções possíveis do modelo matemático, aquelas que satisfaçam as condições do problema proposto. Ressaltamos porém que contextualizar um problema, depois é claro que o aluno adquiriu certas competências, pode se referir também a ele está inserido dentro de um contexto teórico.

> ”Embora não se trate de reduzir os problemas escolares ao formato das tarefas e situações cotidianas, [...] para [se caracterizar] as tarefas escolares como verdadeiros problemas é necessário que elas tenham relação com os contextos de interesse dos alunos ou, pelo menos, adotem um formato interessante no sentido literal do termo. Parece, então, imprescindível ampliar o âmbito dos problemas escolares, tanto na sua natureza, incluindo problemas abertos [...] como no seu conteúdo, abrangendo também alguns dos problemas e situações que causam inquietação nos alunos” (ECHEVERRÍA; POZO, 1998, p. 42).

Com base no estudo feito no presente capítulo trataremos agora de uma situação-problema em que aplicaremos os conceitos estudados na busca de soluções para o problema considerado. Aqui devemos enfatizar que tanto os problemas abertos como as situações-problema possibilitam situar o aluno em posição análoga à do matemático no exercício da profissão, pois ”[...] o aluno deve, diante desses problemas, realizar tentativas, estabelecer hipóteses, testar essas hipóteses e validar seus resultados” (BRASIL, 2006, p.84).

Objetivo final será o de transformar o aluno em aluno pesquisador e, como ferramenta para explorar os problemas considerados usaremos o PARI como auxiliar para buscar, testar, analisar, refutar ou aceitar soluções para os problemas, pois acreditamos que

> "[...] a aprendizagem da solução de problemas somente se transformará em autônoma e espontânea se transportada para o âmbito do cotidiano, se for gerada no aluno a atitude de procurar respostas para suas próprias perguntas/problemas, se ele se habituar a questionar-se ao invés de receber somente respostas já elaboradas por outros, seja pelo livro-texto, pelo professor ou pela televisão. O verdadeiro objetivo final da aprendizagem da solução de problemas é fazer com que o aluno adquira o hábito de propor-se problemas e de resolvê-los como forma de aprender."(ECHEVERRÍA e POZO, 1998, p. 15)

Também temos o objetivo de além desenvolver as soluções através de propriedades, explorar o campo em que teremos que usar os recursos computacionais (no nosso caso o PARI) para encontrar soluções de equações diofantinas pois segundo LA ROCQUE e PITOMBEIRA(1991), ao propor um desses problemas, a escolha dos coeficientes $a$, $b$ e $c$ da equação diofantina linear $ax+by=c$ importa, não só para maior ou menor dificuldade nos cálculos, como também para a existência de uma solução (desde que sejam inteiras ou inteiras positivas).

Se considerarmos as equações diofantinas lineares:

$$15x+25y=2000 \tag{2.9}$$

$$10x+12y=80 \tag{2.10}$$

$$10x+12y=77 \tag{2.11}$$

e se estamos interessados apenas em pares de soluções inteiras positivas, então equação (2.9) apresenta $27$ soluções inteiras positivas, a equação (2.10) apresenta apenas duas soluções inteiras, enquanto a equação (2.11) não apresenta soluções.

Considere o problema:

**Problema 2.10.1.** *Se um trabalhador recebe* $510$ *reais em tíquetes de alimentação, com valores de* $20$ *reais ou* $50$ *reais cada tíquete, de quantas formas pode ser formado o carnê de tíquetes desse trabalhador?*

**Solução 2.10.1.** *Sejam* $x$ *a quantidade de tíquetes de 20 reais e* $y$ *a quantidade de tíquetes de* $50$ *reais então a equação é:*

$$20x+50y=510 \tag{2.12}$$

*Como* $(20,50)=10$ *e* $10 \mid 510$*, então a equação 2.12 tem solução. Utilizando o Corolário 2.6.1 e dividindo a equação* $20x+50y=510$ *por* $10$*, obtemos a equação equivalente:*

$$2x+5y=51 \text{ onde } (5,2)=1. \tag{2.13}$$

*Primeiro encontraremos uma solução para* $2x+5y=1$.

*Pelo algoritmo de Euclides:*

| | | |
|---|---|---|
| | 2 | 2 |
| 5 | 2 | 1 |
| 1 | 0 | |

**Tabela 2.4:** *Algoritmo de Euclides para* $(2,5)$

*Deste algoritmo construímos as seguintes expressões:*

$$5 = 2\cdot 2+1 \tag{2.14}$$
$$2 = 1\cdot 2+0 \tag{2.15}$$

*Apartir da expressão 2.14:*

$$1 = 5-2\cdot 2$$
$$1 = 2(-2)+5(1) \tag{2.16}$$

*Multiplicando a equação por* $51$*, obtemos:*

$$2\cdot(-102)+5\cdot(51)=51.$$

*Onde* $x_0=-102$ *e* $y_0=51$ *é uma solução particular da equação 2.12 , e utilizando teorema 2.6.1 na equação 2.12 as soluções são:*

$$\begin{cases} x = x_o+bt = -102+5t \\ y = y_o-at = 51-2t \end{cases}$$

*com* $t\in\mathbb{Z}$*.*

*Como estamos interessado em soluções não negativa, então devemos ter* $x\geqslant 0$ *e* $y\geqslant 0$ *assim* $-102+5t\geqslant 0$ *e* $51-2t\geqslant 0$*. Isto é:*

$$t\geqslant 20{,}4 \text{ e } t\leqslant 25{,}5$$

*que nos dá* $t\in\{21,22,23,24,25\}$*. Portanto o carnê pode ser formado de* $5$ *formas diferentes.*

Considere agora o problema que retiramos de LA ROCQUE e PITOMBEIRA(1991, p.39):

**Problema 2.10.2.** *Um laboratório dispõe de 2 máquinas para examinar amostras de sangue. Uma delas examina 15 amostras de cada vez, enquanto a outra examina 25. Quantas vezes essas máquinas devem ser acionadas para examinar 2 mil amostras?*

**Solução 2.10.2.** *Sejam* $x$ *e* $y$*, o número de vezes que a primeira e a segunda máquinas, foram acionadas, respectivamente. Temos portanto a equação diofantina linear:*

$$15x+25y=2000 \tag{2.17}$$

*essa equação é equivalente a*

$$3x+5y=400 \tag{2.18}$$

*como* $(5,3) = 1$*, esta equação (diofantina) tem solução. Tem-se agora que encontrar uma solução particular para* $3x + 5y = 400$*. Utilizando o método sugerido, primeiramente deve-se encontrar a solução da equação* $3x + 5y = 1$*, pelo algoritmo de Euclides:*

| | 1 | 1 | 2 |
|---|---|---|---|
| 5 | 3 | 2 | 1 |
| 2 | 1 | 0 | |

**Tabela 2.5:** *Algoritmo de Euclides para* $(5,3)$*.*

*Este algoritmo permite construir as seguintes expressões:*

$$5 = 3 \cdot 1 + 2 \tag{2.19}$$
$$3 = 2 \cdot 1 + 1 \tag{2.20}$$
$$2 = 1 \cdot 2 + 0 \tag{2.21}$$

*A partir da expressão 2.20:*

$$1 = 3 - 2 \cdot 1 \tag{2.22}$$

*A partir da expressão 2.19 obtém-se:*

$$2 = 5 - 3 \cdot 1 \tag{2.23}$$

*Substituindo 2.23 em 2.22*

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

*aplicando a propriedade distributiva obtém-se*

$$1 = 3.2 + 5.(-1) \tag{2.24}$$

*A expressão 2.24 indica que* $x = 2$ *e* $y = -1$ *é uma solução particular da equação* $3x + 5y = 1$*. Multiplicando ambos os lados da expressão 2.24 por* $400$*:*

$$\begin{aligned} 1 \cdot (400) &= 3 \cdot 2 \cdot 400 + 5 \cdot (-1) \cdot 400 \\ 400 &= 3 \cdot 800 + 5 \cdot (-400) \end{aligned} \tag{2.25}$$

*Logo* $800$ *e* $-400$ *é uma solução particular da equação 2.18 e também será da equação original 2.17 :* $2000 = 15 \cdot 800 + 25 \cdot (-400)$*. Consequentemente, a solução geral da equação 2.17 que apresenta* $mdc(25,15) = 5$ *se expressa por:*

$$\begin{aligned} x &= 800 + 25/5t \\ y &= -400 - 15/5t, \ para\ t \in \mathbb{Z}. \end{aligned} \tag{2.26}$$

*Considerando o problema que levou a essa equação, vê-se que só interessam respostas não-negativas para $x$ e para $y$, assim, deve-se impor que:*

$$800+5t \geqslant 0 \implies t \geqslant -160 \tag{2.27}$$

$$-400-3t \geqslant 0 \implies t \leqslant -133,3 \tag{2.28}$$

*portanto,*

$$-160 \leqslant t \leqslant -133,$$

*para $t \in \mathbb{Z}$.*

*Substituindo os valores de $t$ em $x$, obtêm-se $27$ soluções (que apresentam valores $x$ e $y$ inteiros positivos) para o problema, desde a primeira máquina parada e a outra sendo acionada $80$ vezes, até o caso em que a primeira trabalha $130$ vezes e a outra só $2$.*

**Problema 2.10.3.** *Subindo uma escada de dois em dois degraus, sobra um degrau. Subindo a mesma escada de três em três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o seu número é múltiplo de $7$ e está compreendido entre $40$ e $100$. HEFEZ(2011, p. 73)*

**Solução 2.10.3.** *Seja $N$ a quantidade de degraus. Então pelas condições do problema temos:*

$$\begin{cases} N = 2x+1 \\ N = 3y+2 \end{cases}$$

*de onde obtemos a equação diofantina*

$$2x-3y=1 \tag{2.29}$$

*Como $(3,2)=1$ a equação tem solução.*

*Utilizando algoritmo de Euclides.*

*Obtemos a solução particular*

$$2(2)-3(1) = 1 \tag{2.30}$$

*A expressão 2.30 indica que $x_0=2$ e $y_0=1$ é uma solução para equação 2.29*

*Pelo teorema 2.6.1 as soluções são:*

$$\begin{cases} x = 2-3t \\ y = 1-2t \end{cases}$$

*com $t \in \mathbb{Z}$.*

*Queremos as soluções não negativa, então devemos ter $x \geqslant 0$ e $y \geqslant 0$ assim $2-3t \geqslant 0$ e $1-2t \geqslant 0$. Isto é:*

$$t \leqslant 1,3 \text{ e } t \leqslant 0,5 \Rightarrow t \leqslant 0,5.$$

*Tomando* $x = 2 - 3t$ *e substituindo em* $N = 2x + 1$ *obtemos* $N = 5 - 6t$ *e como* $40 \leqslant N \leqslant 100$*, temos*

$$\begin{aligned} 40 \leqslant 5 - 6t \leqslant 100 \Leftrightarrow \\ 35 \leqslant -6t \leqslant 95 \Leftrightarrow \\ -15,8 \leqslant t \leqslant -5,8 \end{aligned} \tag{2.31}$$

*que significa que* $t \in \{-15, -14, -13, -12, -11, -10, -9, -8, -7, -6\}$*. Como* $N$ *é múltiplo de* $7$ *devemos* $t = -12$ *o que nos dá* $N = 77$ *degraus.*

## 2.11 Resolução de Congruências Lineares

Nesta secção pretendemos resolver equações do tipo

$$ax \equiv b \,(\mathrm{mod\ m}), \tag{2.32}$$

em que $a$, $b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Uma vez que, se $x_0$ é solução da equação, então $x_0 + mt$ (com $t \in \mathbb{Z}$) também é, só precisamos de encontrar as soluções no conjunto $\{0, 1, ..., m-1\}$ ou em qualquer outro sistema completo de resíduos módulo $n$. Assim, qualquer congruência deste tipo, ou não tem solução ou tem uma infinidade de soluções. Ao tratarmos estas congruências com infinitas soluções e olharmos para elas como restos módulo $m$ teremos não mais infinitas soluções mas no máximo $n$ soluções incongruentes. Por exemplo, a equação $2x \equiv 0 \,(\mathrm{mod}\ 6)$ tem duas soluções (incongruentes módulo 6) $x = 0$ e $x = 3$. Todo conteúdo desta secção é quase todo baseado em HEFEZ(2011) com algumas adaptações.

Para SANTOS(2007, p. 36):

> "[...] se $x_0$ é umas solução, i. e., $ax_0 \equiv b \,(\mathrm{mod\ m})$ e $x_1 \equiv x_0 \,(\mathrm{mod\ m})$ então $x_1$ também é uma solução. Isto é óbvio pois se $x_1 \equiv x_0 \,(\mathrm{mod\ m})$ então $ax_1 \equiv ax_0 \equiv b \,(\mathrm{mod\ m})$. O que acabamos de verificar é que se um membro de uma classe de equivalência é solução então todo membro desta classe é solução. Destas observações surge uma questão natural: no caso de existir alguma solução, quantas soluções incongruentes existem?"

Para dar respostas para as perguntas apresentadas enunciaremos algumas proposições.

**Proposição 2.11.1.** *Sejam* $a$*,* $b$ *inteiros e* $m \in \mathbb{N}^*$*, com* $m > 1$ *e* $d = (a, m)$*. No caso em que* $d \nmid b$ *a congruência* $ax \equiv b \,(\mathrm{mod\ m})$ *não possui solução e quando* $d \mid b$*, possui exatamente* $d$ *soluções incongruentes.*

**Demonstração 2.11.1.** *Temos que se* $x$ *é uma solução de* $ax \equiv b \,(\mathrm{mod\ m})$ *significa que* $m \mid ax - b$*, logo existe um inteiro* $y$ *tal que* $ax - my = b$*. Do teorema 2.6.1 sabemos que esta equações não possui nenhuma solução caso* $d \nmid b$*,que se* $d \mid b$ *ela possui infinitas soluções dadas por* $x = x_0 - (m/d)t$ *e* $y = y_0 - (a/d)t$ *onde* $(x_0, y_0)$ *é uma solução particular de* $ax - my = b$*. Logo a congruência* $ax \equiv b \,(\mathrm{mod\ m})$ *possui infinitas soluções dadas por* $x = x_0 - (\frac{m}{d})t$*. Agora para saber o número de*

*soluções incongruentes considere* $x_1 = x_0 - (m/d)t_1$ *e* $x_2 = x_0 - (m/d)t_2$*. Queremos saber as condições que tornam estas soluções incongruentes, temos que se*

$$x_0 - (m/d)t_1 \equiv x_0 - (m/d)t_2 \,(\mathrm{mod\ m}),$$

*então*

$$(m/d)t_1 \equiv (m/d)t_2 \,(\mathrm{mod\ m}),$$

*e como* $(m/d) \mid m$*, temos* $(m/d, m) = m/d$ *que implica*

$$t_1 \equiv t_2 \,(\mathrm{mod\ d}),$$

*Mostrando que as soluções incongruentes são obtidas tomando* $x = x_0 - (m/d)t$*, onde* $t$ *percorre um sistema completo de resíduos módulo* $d$*.*

□

**Corolário 2.11.1.** *Se* $(a,m) = 1$*, então a congruência* $ax \equiv b \,(\mathrm{mod\ m})$ *possui uma única solução módulo* $m$*.*

**Demonstração 2.11.2.** *Basta tomar* $d = 1$ *na proposição 2.11.1.*

□

**Definição 2.11.1.** *Uma solução* $\overline{a}$ *de* $ax \equiv 1 \,(\mathrm{mod\ m})$ *é chamada de um inverso de* $a$ *módulo* $m$*.*

**Observação 2.11.1.** *Se a congruência*

$$aX \equiv b \,(\mathrm{mod\ m})$$

*possui solução, então* $d = (a,m)$ *divide* $b$*. Pondo*

$$a' = \frac{a}{d}\ ,\ b' = \frac{b}{d}\ ,\ n = \frac{m}{d},$$

*temos que a congruência acima é equivalente a*

$$a'X \equiv b' \,(\mathrm{mod\ n}),$$

*temos que* $(a', n) = 1$*, logo exite um inverso módulo* $n$ *para* $a'$*, então esta última congruência é equivalente à*

$$X \equiv c \,(\mathrm{mod\ n})$$

*onde* $c = b'a''$*, sendo* $a''$ *o inverso multiplicativo de* $a'$ *módulo* $n$*.*

## 2.12 Teorema Chinês dos Restos

O chamado Teorema Chinês dos Restos dá um método sistemático de resolução de sistemas de congruências do tipo $ax \equiv b \,(\mathrm{mod\ m})$. Segundo Coutinho:

> "[...]um dos primeiros lugares em que apareceu foi no livro do mestre Sun, chamado Manual de Aritmética do mestre Sun, escrito entre 287 d. C. e 473 d.C. "(COUTINHO, 1997, p. 120)

Aparentemente a ideia surgiu com a necessidade de contar o número de soldados numa parada. Suponhamos que sabemos que o número de soldados é no máximo $1000$. Mandamos ordenar os soldados em filas de $7$ e depois em filas de $11$ e depois em filas de $13$ (o que é mais simples do que contar os soldados) e contamos o número de soldados que sobraram em cada um dos casos.

**Teorema 2.12.1.** *Considere o seguinte sistema de congruências com solução*

$$\begin{cases} a_1X & \equiv & b_1 \,(\mathrm{mod}\ \mathrm{m_1}) \\ a_2X & \equiv & b_2 \,(\mathrm{mod}\ \mathrm{m_2}) \\ \cdots & & \\ a_rX & \equiv & b_r \,(\mathrm{mod}\ \mathrm{m_r}) \end{cases}$$

*temos que* $(a_i, m_i) \mid b_i$*, com* $i \in \{1, 2, \cdots, r\}$*, pela observação 2.11.1 o sistema é equivalente à*

$$\begin{cases} X & \equiv & c_1 \,(\mathrm{mod}\ \mathrm{n_1}) \\ X & \equiv & c_2 \,(\mathrm{mod}\ \mathrm{n_2}) \\ \cdots & & \\ X & \equiv & c_r \,(\mathrm{mod}\ \mathrm{n_r}) \end{cases} \tag{2.33}$$

*onde* $(n_i, n_j) = 1$*, para todo par* $n_i,\ n_j$ *com* $i \neq j$*, possui uma única solução módulo* $N = n_1 n_2 \cdots n_r$*. Tal solução pode ser obtida como se segue:*

$$x = N_1 y_1 c_1 + \cdots + N_r y_r c_r,$$

*onde* $N_i = N/n_i$ *e* $y_i$ *é solução de* $N_i Y \equiv 1 \,(\mathrm{mod}\ \mathrm{n_i})$*,* $i = 1, 2, \cdots, r$*.*

**Demonstração 2.12.1.** *Vamos, inicialmente, provar que* $x$ *é uma solução simultaneamente do sistema 2.33. De fato, como* $n_i \mid N_j$*, se* $i \neq j$*, e* $N_i y_i \equiv 1 \,(\mathrm{mod}\ \mathrm{n_i})$*, segue-se que*

$$x = N_1 y_1 c_1 + \cdots + N_r y_r c_r \equiv N_i y_i c_i \equiv c_i \,(\mathrm{mod}\ \mathrm{n_i}).$$

*Por outro lado, se* $x'$ *é outra solução do sistema 2.33, então*

$$x \equiv x' \,(\mathrm{mod}\ \mathrm{n_i}),\ \forall i,\ i = 1, 2, \cdots, r.$$

*Como* $(n_i, n_j) = 1$*, para* $i \neq j$*, segue-se que* $[n_1, \cdots, n_r] = n_1 \cdots n_r = N$ *e, consequentemente, pela proposição, temos que* $x \equiv x' \,(\mathrm{mod}\ \mathrm{N})$*.*

□

Tomemos agora o seguinte exemplo.

**Problema 2.12.1.** *Três satélites passarão sobre o Rio esta noite. O primeiro à* $1$ *hora da madrugada, o segundo às 4 horas e o terceiro às* $8$ *horas da manhã. Cada satélite tem um período diferente. O primeiro leva* $13$ *horas para completar uma volta em torno da Terra, o segundo* $15$ *horas e o terceiro* $19$ *horas. Determine quantas horas decorrerão, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio.(COUTINHO, 1997, p. 116)*

**Solução 2.12.1.** *Seja $x$ o número de horas, contadas a partir da meia-noite de hoje, quando os três satélites passarão juntos sobre o Rio. O primeiro satélite passa sobre o Rio a cada $13$ horas, a contar da $1$ da madrugada. Logo precisamos ter que $x = 1 + 13n_1$ , para algum inteiro positivo $n_1$ , que representa o número de voltas que o satélite $1$ tem que dar em torno da Terra antes que passe junto com os dois outros satélites. As equações correspondentes aos outros dois satélites são*

$$x = 4 + 15n_2 \; e \; x = 8 + 19n_3;$$

*Estas equações podem ser reescritas como:*

$$\begin{cases} X & \equiv & 1 \pmod{13} \\ X & \equiv & 4 \pmod{15} \\ X & \equiv & 8 \pmod{19} \end{cases} \tag{2.34}$$

*Para este caso temos que $N = 13 \times 15 \times 19 = 3705$, $N_1 = N/n_1 = 285$, $N_2 = N/n_2 = 247$ e $N_3 = N/n_3 = 195$. Agora examinemos as congruências $N_i Y \equiv 1 \pmod{n_i}$,*

$$\begin{cases} 285Y & \equiv & 1 \pmod{13} \\ 247Y & \equiv & 1 \pmod{15} \\ 195Y & \equiv & 1 \pmod{19} \end{cases} \tag{2.35}$$

*esse sistema é equivalente a*

$$\begin{cases} 12Y & \equiv & 1 \pmod{13} \\ 7Y & \equiv & 1 \pmod{15} \\ 5Y & \equiv & 1 \pmod{19} \end{cases} \tag{2.36}$$

*que soluções $y_1 = 12$, $y_2 = 13$ e $y_3 = 4$, respectivamente.*

*Portanto, uma solução módulo $N = 3705$ é dada por*

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

$$x = 285 \cdot 12 \cdot 1 + 247 \cdot 13 \cdot 4 + 195 \cdot 4 \cdot 8 = 3420 + 12844 + 6240 = 22504$$

*Como $22504 \equiv 274 \pmod{3705}$, temos portanto, depois de passar juntos uma vez sobre o Rio $274$ horas depois da zero hora de hoje, os satélites passarão juntos novamente a cada $3705$ horas.*

É claro que o PARI tem funções específicas para esses cálculos que os tornam muito simples de realizar. Por exemplo se temos o sistema

$$\begin{cases} X & \equiv & 1 \pmod{13} \\ X & \equiv & 4 \pmod{15} \\ X & \equiv & 8 \pmod{19} \end{cases} \tag{2.37}$$

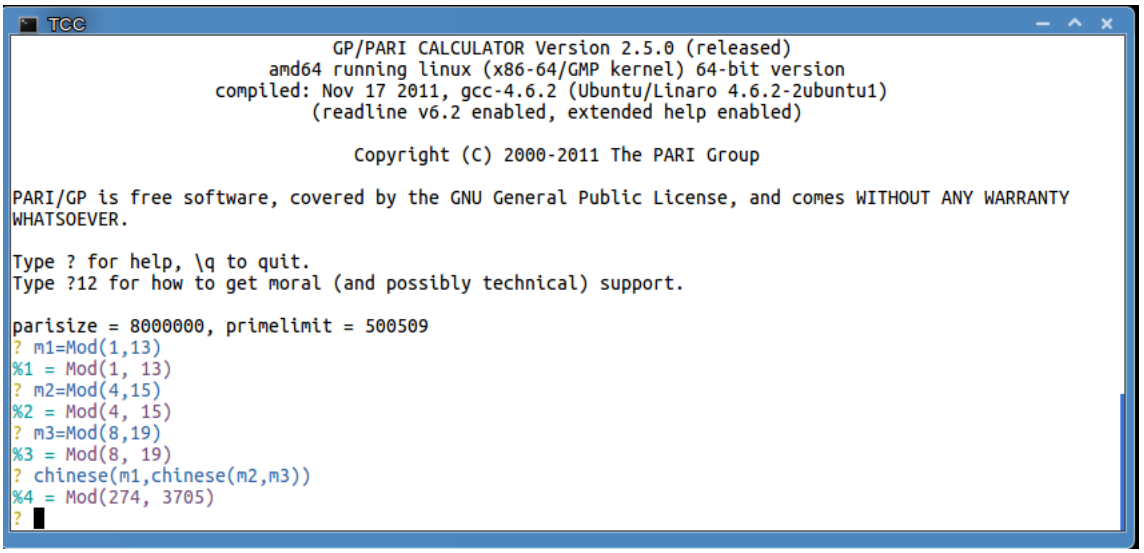
Definimos no Pari/GP as contantes, conforme a tabela 2.6 e aplicamos o comando "`chinese`".

Na figura 2.2, temos aplicação do comando e sua saída.

| Sistema | Comando |
|---|---|
| $X \equiv 1\,(\mathrm{mod}\ 13); X \equiv 4\,(\mathrm{mod}\ 15); X \equiv 8\,(\mathrm{mod}\ 19);$ | `m1=Mod(1,13); m2=Mod(4,15); m3=Mod(8,19)` `chinese(m1,chinese(m2,m3))` |

**Tabela 2.6:** *Comando para solução do sistema 2.37*

**Figura 2.2:** *Saída do comando:* `chinese(m1,chinese(m2,m3))`.



# 3 Aplicações na Solução de Problemas

*"Um método é um truque que funciona mais de uma vez."*
*George Pólya*

Neste capítulo daremos ênfase a aplicações que trabalham problemas que se destacam por ser necessário a compreensão e manipulação de conceitos teóricos mais elaborados. Conforme D'AMORE (2005):

> "A aprendizagem Matemática não é apenas construção de conceitos, mas envolve três tipologias de aprendizagens distintas, com intersecções, que são: aprendizagem conceitual, aprendizagem de estratégias (resolver, demonstrar,...) e aprendizagem algorítmica (calcular, operar,...)."

Um ensino comprometido com as necessidades atuais é fundamental a utilização de metodologias que possibilitem o desenvolvimento de competências para formar um aluno cidadão que utiliza cada vez mais conceitos matemáticos na sua rotina.

Não queremos de forma nenhuma diminuir a importância das aplicações prática, até porque elas estão presentes neste trabalho, e é importante salientar como afirma LIMA(2002, p. 141), "[...]as aplicações do conhecimento incluem a resolução de problemas, essa arte intrigante que, por meio de desafios, desenvolve a criatividade, nutre a auto-estima, estimula a imaginação e recompensa o esforço de aprender".

## 3.1 Pari/GP na Solução de Equações Diofantinas Exponenciais

Quando se tem um problemas que envolve equações diofantinas, encontrar todas as soluções (em números inteiros positivos) para tal equação não é uma tarefa fácil. Muitas dessas equações podem ser resolvidas usando aritmética modular.

Existem, porém, algumas equações exponenciais diofantinas que simplesmente não poderão ser resolvidas usando apenas a aritmética modular, e então ideias mais sofisticadas devem entram em jogo. O mais usual é o método de Baker, que usa formas lineares em logaritmos, esse método gera cotas efetivas para soluções de vários tipos de equações diofantinas, para maiores detalhes veja SHOREY,TIJDEMAN(1986) e WALDSCHMIDT(2009).

Conforme LOZANSKY, ROUSSEAU(1996) algumas equações diofantinas são muito fáceis de resolver quando se olha de um ângulo apropriado. No entanto, não há nenhum algoritmo geral e

eficaz para lidar com as equações Diofantinas. Temos portanto que cada equação diofantina pode ser um novo desafio que exige habilidade para ser solucionada. Por isso é desejável ter experiência com diversas estratégias para lidar com cada caso de equações diofantinas.

Ainda segundo LOZANSKY, ROUSSEAU(1996, p. 57) algumas das técnicas mais simples são:

1. Fatoração;
2. Utilizar Congruências;
3. O uso do discriminante para equações quadráticas;
4. Método de descida infinita de Fermat;
5. Formas Especiais.

A seguir ilustraremos alguns dos métodos acima.

### 3.1.1 Fatoração

Dada a equação $f(x_1,x_2,\cdots,x_n)=0$, se podermos escrevê-la sob a forma equivalente

$$f_1(x_1,x_2,\cdots,x_n)f_2(x_1,x_2,\cdots,x_n)\cdots f_k(_1,x_2,\cdots,x_n)=a,$$

onde $f_1,f_2,\cdots,f_k\in\mathbb{Z}[X_1,X_2,\cdots,X_n]$ e $a\in\mathbb{Z}$. Decompondo $a$ em fatores primos, obtemos um número finito de $k$ fatores inteiros $a_1,a_2,\cdots,a_k$. Cada uma dessas fatorações produz um sistema de equação

$$\begin{cases} f_1(x_1,x_2,\cdots,x_n)=a_1 \\ f_2(x_1,x_2,\cdots,x_n)=a_2 \\ \qquad\qquad\vdots \\ f_k(x_1,x_2,\cdots,x_n)=a_k. \end{cases} \tag{3.1}$$

Considere o exemplo retirado de ANDREESCU, ANDRICA e CUCUREZEANU(2010, p. 5)

**Exemplo 3.1.1.** *Sejam $p$ e $q$ primos. Determine a solução da equação*

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{pq}$$

*em inteiros positivos.*

**Solução 3.1.1.** *Esta equação é equivalente a equação diofantina*

$$(x-pq)(y-pq)=p^2q^2.$$

*Observe que $\frac{1}{x}<\frac{1}{pq}$, então nós temos que $x>pq$.*

*Considerando todos os divisores positivos de $p^2q^2$ nós obtemos os seguintes sistemas:*

$$\begin{cases} x-pq=1 \\ y-pq=p^2q^2 \end{cases} \quad \begin{cases} x-pq=p \\ y-pq=pq^2 \end{cases} \quad \begin{cases} x-pq=q \\ y-pq=p^2q \end{cases}$$

$$\begin{cases} x-pq=p^2 \\ y-pq=q^2 \end{cases} \quad \begin{cases} x-pq=pq \\ y-pq=pq \end{cases} \quad \begin{cases} x-pq=pq^2 \\ y-pq=p \end{cases}$$

$$\begin{cases} x-pq=p^2q \\ y-pq=q \end{cases} \quad \begin{cases} x-pq=q^2 \\ y-pq=p^2 \end{cases} \quad \begin{cases} x-pq=p^2q^2 \\ y-pq=1 \end{cases}$$

*resolvendo os sistemas obtemos as soluções:* $(1+pq, pq(1+pq))$, $(p(1+q), pq(1+q))$, $(q(1+p), pq(1+p))$, $(p(p+q), pq(1+pq))$, $(2pq, 2pq))$, $(pq(1+q), p(1+q))$, $(pq(1+p), q(1+p))$, $(q(p+q), p(p+q))$, $(pq(1+pq), 1+pq)$.

□

### 3.1.2 Método da Descida Infinita de Fermat

Segundo NETO(2000):

> "Esquematicamente, o método da descida (devido ao matemático francês Pierre Simon de Fermat) consiste então no seguinte:
>
> i. Supor que uma dada equação possui uma solução em inteiros não nulos.
>
> ii. Concluir daí que ela possui uma solução em inteiros positivos que seja, em algum sentido, mínima.
>
> iii. Deduzir a existência de uma solução positiva menor que a mínima, chegando a uma contradição."

Considere agora o exemplo retirado de ANDREESCU, ANDRICA e CUCUREZEANU(2010, p. 49):

**Exemplo 3.1.2.** *Resolva a equação* $2^x - 1 = xy$ *em inteiros positivos.*

**Solução 3.1.2.** *Note que* $(0,k)$, $k \in \mathbb{Z}_+$, $(1,1)$ *são soluções. Vamos provar que não existem outras soluções, usando Método da Descida de Fermat, sobre os fatores primos de* $x$. *Sejam* $p_1$ *um divisor primo de* $x$ *e* $q$ *o menor inteiro positivo tal que* $p_1 \mid 2^q - 1$. *Do pequeno Teorema de Fermat nós obtemos que* $p_1 \mid 2^{p_1-1} - 1$, *e portanto* $q \leq p_1 - 1 < p_1$.

*Provaremos agora que* $q \mid x$. *Suponha por absurdo que* $q$ *não divide* $x$, *então* $x = kq + r$, *com*

$0 < r < q$, *e*

$$\begin{aligned} 2^x - 1 &= 2^{kq}2^r - 1 \\ &= (2^q)^k.2^r - 1 \\ &= (2^q - 1 + 1)^k.2^r - 1 \\ &\equiv 2^r - 1 \,(\mathrm{mod}\ \mathrm{p}_1)\,. \end{aligned}$$

*Isto significa que* $p_1 \mid 2^r - 1$*, que é uma contradição com a minimalidade de* $q$*. Portanto* $q \mid x$ *e* $1 < q < p_1$*. Agora seja* $p_2$ *um primo divisor de* $q$*. Temos que* $p_2$ *é um divisor de* $x$ *e* $p_2 < p_1$*. Continuando este procedimento, nós construiremos uma sequência infinita de divisores primos decrescente de* $x$*:* $p_1 > p_2 > \cdots$ *que é uma contradição com o método da descida de Fermat.*

□

### 3.1.3 Formas Especiais

Ainda poderíamos citar outros métodos por exemplo o uso de desigualdades e formas paramétricas, então para concluir esta parte, considere o exemplo retirado de ANDREESCU, ANDRICA e CUCUREZEANU(2010, p. 26).

**Exemplo 3.1.3.** *Prove que a equação* $2^x + 1 = xy$ *tem infinitas soluções inteiros positivos.*

**Solução 3.1.3.** *Se tomarmos* $x = 3^k$*, é suficiente mostrar que* $3^k$ *divide* $2^{3^k} + 1$ *para todo* $k \geq 0$*. De fato, para todo* $k \geq 1$*,*

$$2^{3^k} + 1 = (2^{3^{k-1}})^3 + 1 = (2^{3^{k-1}} + 1)(2^{2.3^k} - 2^{3^{k-1}} + 1).$$

*O primeiro fator pode ser escrito como* $(3-1)^{3^{k-1}} + 1$*, e sendo* $(-1)^{3^k} + 1 = 0$*, temos que este fator é divisível por* $3^{k-1}$*. O segundo fator é igual a* $(2^{3^{k-1}} + 1)^2 - 3.2^{3k-1}$*, que é divisível por* $3$*. Portanto* $(3^k,\ \frac{2^{3^k}+1}{3^k})$*, com* $k \geq 0$*, são soluções da equação dada.*

□

## Utilização de Congruências

No que segue faremos uso do software Pari/GP e de congruências para resolver problemas que tratam de equações diofantinas na tentativa de expor uma forma construtiva que trabalhe os principais teoremas e propriedades estudadas no capítulo anterior.

Com exceção do Problema 3.3.3 no geral trabalharemos apenas com a equação diofantina exponencial

$$a^x - b^y = c \tag{3.2}$$

onde $a$, $b$ e $c$ são inteiros fixos e $x$ e $y$ são variáveis.

## 3.2 Equações Diofantinas Exponenciais sem Solução

Nas soluções utilizaremos a ideia de que se temos uma equação diofantina exponencial sem soluções, como

$$7^b + 4 = 3^c, \tag{3.3}$$

então queremos encontrar algum módulo $m \geqslant 2$, de modo que

$$7^b + 4 \equiv 3^c \pmod{\mathrm{m}} \tag{3.4}$$

não tenha soluções. Neste caso devemos, portanto, verificar todas as potências de $7 \pmod{\mathrm{m}}$, e de $3 \pmod{\mathrm{m}}$ (há um número finito de cada), e se nenhum delas nos der soluções, então não há soluções em inteiros positivos para a sua equação.

Aqui devemos destacar um fato muito importante no que foi dito acima que é:

> "Dada uma equação diofantina exponencial que não tem solução, então sempre existe um módulo $m \geqslant 2$ para qual equação não tenha solução."

esse fato é a chamada Conjectura de Skolem, que é devido a Thoralf Albert Skolem [1], que enunciaremos de forma mais precisa. A conjectura original de SKOLEM(1937) diz que:

**Conjectura 3.2.1.** *(Skolem). Considere a equação Diofantina exponencial*

$$a_1 b_{11}^{\alpha_1} \cdots b_{1l}^{\alpha_l} + \cdots + a_k b_{k1}^{\alpha_1} \cdots b_{kl}^{\alpha_l} = 0. \tag{3.5}$$

*Suponha que a equação 3.5 não tem solução em inteiros não negativos,* $\alpha_1, \cdots, \alpha_l, \cdots, \alpha_1, \cdots, \alpha_l$. *Então, a congruência*

$$a_1 b_{11}^{\alpha_1} \cdots b_{1l}^{\alpha_l} + \cdots + a_k b_{k1}^{\alpha_1} \cdots b_{kl}^{\alpha_l} \equiv 0 \pmod{m} \tag{3.6}$$

*não tem solução para algum inteiro* $m \geqslant 2$.

Essa conjectura, segundo HAJDU(2013), pode ser enunciada da forma como segue.

**Conjectura 3.2.2.** *(Nova Conjectura de Skolem). Dada um equação exponencial Diofantina*

$$a_1 b_{11}^{\alpha_{11}} \cdots b_{1l}^{\alpha_{1l}} + \cdots + a_k b_{k1}^{\alpha_{k1}} \cdots b_{kl}^{\alpha_{kl}} = c. \tag{3.7}$$

*e supondo que a equação 3.7 não tem solução em inteiros não negativos,* $\alpha_{11}, \cdots, \alpha_{1l}, \cdots, \alpha_{k1}, \cdots, \alpha_{kl}$. *Então, exite um inteiro* $m \geqslant 2$ *tal que a congruência*

$$a_1 b_{11}^{\alpha_1} \cdots b_{1l}^{\alpha_l} + \cdots + a_k b_{k1}^{\alpha_1} \cdots b_{kl}^{\alpha_l} \equiv c \pmod{m} \tag{3.8}$$

*não tem solução em inteiros não negativos* $\alpha_{11}, \cdots, \alpha_{1l}, \cdots, \alpha_{k1}, \cdots, \alpha_{kl}$

[1] Veja detalhes e alguns fatos de sua obra em:<http://pt.wikipedia.org/wiki/Thoralf_Skolem>

Note que na nova conjectura além do número $c$ temos que na conjectura original os expoentes dos $b_{ij}$ com $1 \leqslant i \leqslant k$ é mesmo $\alpha_j$ com $1 \leqslant j \leqslant l$.

Neste trabalho consideraremos o caso $k = 2$, para este caso específico podemos reescrever a equação 3.7 como

$$a_1 b_{11}^{\alpha_{11}} \cdots b_{1l}^{\alpha_{1l}} + a_2 b_{21}^{\alpha_{21}} \cdots b_{2l}^{\alpha_{2l}} = c. \tag{3.9}$$

conforme HAJDU(2013) no caso $k = 1$ a conjectura é verdadeira, para os casos em que $k = 2$ vários trabalhos corroboram no sentido que a conjectura é verdadeira, veja SHOREY,TIJDEMAN(1986) e HAJDU(2013).

## 3.3 Equações Diofantinas Exponenciais com Solução

Para o caso particular da equação 3.9, para $a_1 = a_2 = 1$ e $l = 1$, em que há solução temos uma interessante conjectura de SKOLEM(1945), que diz o seguinte:

**Conjectura 3.3.1.** *Se $a^x - b^y \equiv c \pmod{\mathrm{m}}$ tem solução para todo inteiro positivo $m$, então*

$$a^x - b^y = c \tag{3.10}$$

*tem solução inteiros positivos $x$ e $y$.*

Ainda neste contexto PILLAI(1936) mostrou que a equação 3.10 tem apenas um número finito de soluções inteiras $(x,y)$ e apenas uma solução se $c$ for suficientemente grande em relação a $a$ e $b$. Nos primeiros trabalhos de PILLAI e que de fato é o que nós utilizaremos, ele havia considerado as equações diofantinas $a^x - b^y = c$ onde $a$, $b$ e $c$ eram fixos, ou seja, apenas $x$ e $y$ eram variáveis, mas em trabalhos posteriores ele também consideraria o caso em que apenas um dos inteiros $(a,b,c,x,y)$ é fixo, para mais informações veja WALDSCHMIDT(2009).

Se considerarmos uma equação com solução como

$$5^a + 4 = 3^c \tag{3.11}$$

que tem uma solução $a = 1$ e $c = 2$. Então pela Proposição 2.8.3, se $m$ não é divisível por $3$ ou $5$ então existem $k$ e $k'$ tais que

$$\begin{aligned} 3^k &\equiv 1 \pmod{\mathrm{m}} \\ 5^{k'} &\equiv 1 \pmod{\mathrm{m}} \end{aligned}$$

daí não importa que valores inteiros escolhemos para $m$, o melhor que podemos concluir é que $a = 1$ e $c = 2$ é uma solução para equação 3.11 relativo ao módulo $m$, mas isso nunca será suficiente para concluir que $a = 1$ e $c = 2$ é a única solução, pois segundo a Conjectura 3.2.2 teríamos que mostrar que se, por exemplo $a \neq 1$, então existe $m \geqslant 2$ tal que a congruência $5^a + 4 = 3^c \pmod{\mathrm{m}}$ não tem solução. Como instrumento de auxílio, como já dissemos, utilizaremos o Pari/GP, por exemplo,

para equação 3.11 se queremos as soluções referentes a um módulo $m$ tal que $(m,5) = (m,3) = 1$ podemos construir o comando conforme apresentado na tabela 3.1 abaixo[2].

| Equação | Comando no Pari/GP |
|---|---|
| $5^a + 4 \equiv 3^c \pmod{m}$ | `r=znorder(Mod(5,m));t=znorder(Mod(3,m));for(a=0,r-1,for(c=0,t-1, if(Mod(5,m)^a-Mod(3,m)^c+4==0,print([a,c])));[r,t]]` |

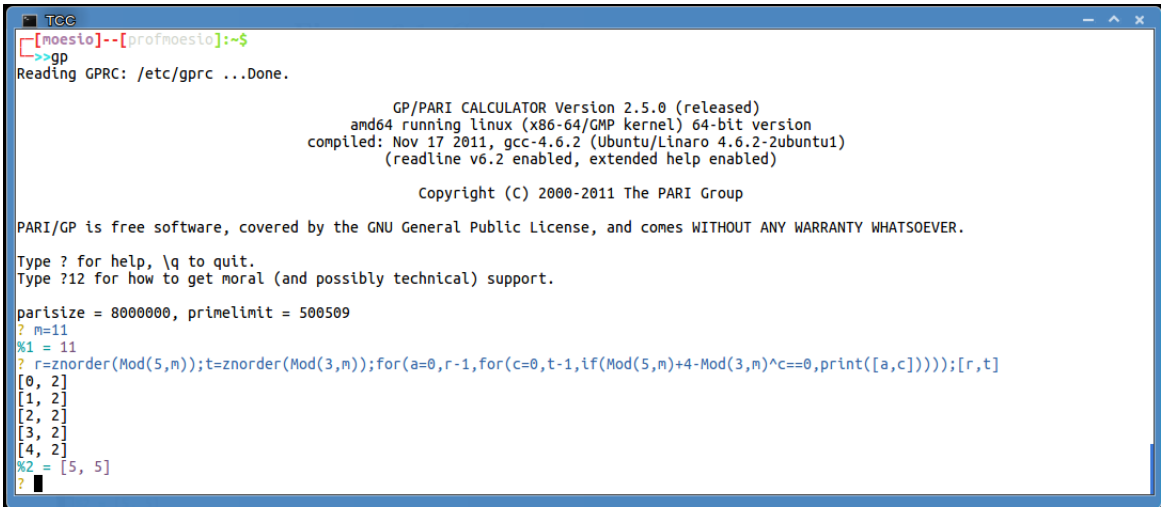
**Tabela 3.1:** *Comando para* $5^a + 4 = 3^c$

Utilizando o comando da tabela 3.1 relativo a módulo $11$, temos as soluções apresentadas na Tabela 3.2. Na figura 3.1 temos aplicação do comando e sua saída no Pari/GP.

| | Soluções | | | | |
|---|---|---|---|---|---|
| $[a,\ c]$ | $[0,\ 2]$ | $[1,\ 2]$ | $[2,\ 2]$ | $[3,\ 2]$ | $[4,\ 2]$ |

**Tabela 3.2:** *Soluções* $\pmod{11}$ *para* $5^a + 4 = 3^c$.

**Figura 3.1:** *Comando para* $5^a + 4 = 3^c$ *e soluções módulo* $11$




Assim, no procedimento que implementaremos neste trabalho determinaremos uma solução inicial para a equação $a^x - b^y = c$ por inspeção, $(x_0, y_0)$, e a partir desta vamos supor por absurdo a existência de uma outra solução maior que a solução considerada, ou seja, um $x > x_0$, por exemplo. Para a equação 3.11 temos que $a = 1$ e $c = 2$ é uma solução, portanto, temos de escolher algum $m$ que é divisível por uma potência de $5$ ou $3$, que deverá ser maior do que a maior potência cujo expoente seja solução para a equação. Como $a = 1$ e $c = 2$ isso significa que devemos começar com um $m = 3^3$ ou $m = 5^2$, pois $3^3 \mid 3^c$ para todo $c > 2$ e $5^2 \mid 5^a$ para todo $a > 1$, respectivamente.

Vamos considerar o mesmo exemplo de forma mais detalhada, no seguinte problema:

**Problema 3.3.1.** *Determine todas as soluções inteiras não negativas da equação* $3^n - 5^m = 4$.

**Solução 3.3.1.** *Esta equação tem somente uma solução nos inteiros não negativos, que é* $n = 2$ *e* $m = 1$. *De fato, se* $n = 0$, *temos que* $5^m = -3$, *que é falso para todo inteiro* $m$, *pois* $5^m$ *é positivo para todo* $m$. *Se* $n = 1$, *temos que* $5^m = -1$, *novamente pelo mesmo argumento está igualdade é falsa.*

[2] Ao inserir o comando no Pari/GP retire a quebra de linha.

*Note que, como* $5|5^m$*, temos, relativo ao módulos* $5$*, que*

$$\begin{aligned} 3^n - 5^m &\equiv 4 \pmod 5 \iff \\ 3^n &\equiv 4 \pmod 5 \end{aligned} \tag{3.12}$$

*Como* $\phi(5) = 4$ *e* $ord_5(3) = 4$ *, então pela Definição 2.8.3,* $3$ *é raiz primitiva módulo* $5$*, daí pelo Teorema 2.8.3 temos que*

$$S^3_{(\text{mod } 5)} = \{3,\ 3^2,\ 3^3,\ 3^4\}$$

*forma um sistema reduzido de resíduos módulo* $5$*, e portanto pelo Teorema 2.8.4, sendo* $(4,5) = 1$*, temos que deve existir* $x$ *tal que* $3^x \equiv 4 \pmod 5$*, com* $3^x \in S^3_{(\text{mod } 5)}$*. De fato, como*

$$3^2 \equiv 4 \pmod 5 \tag{3.13}$$

*e por transitividade, obtemos*

$$3^2 \equiv 3^n \pmod 5,$$

*pelo Teorema 2.8.2, resulta que*

$$n \equiv 2 \pmod 4. \tag{3.14}$$

*Analogamente, como* $n = 2$ *é uma solução, então* $3^2|3^n$*, temos relativo a módulo* $9$*, que*

$$\begin{aligned} 3^n - 5^m &\equiv 4 \pmod 9 \iff \\ -5^m &\equiv 4 \pmod 9 \iff \\ 5^m &\equiv -4 \pmod 9 \iff \\ 5^m &\equiv 5 \pmod 9 \end{aligned} \tag{3.15}$$

*Como* $\phi(9) = 6 = ord_9(5)$*, vem que* $5$ *é raiz primitiva módulo* $9$ *e o conjunto*

$$S^5_{(\text{mod } 9)} = \{5,\ 5^2,\ 5^3,\ 5^4,\ 5^5\} \tag{3.16}$$

*forma um sistema reduzido de resíduos módulo* $9$*, e sendo* $(5,9) = 1$ *temos que exite* $5^x \in S^5_{(\text{mod } 9)}$ *tal que* $5^x \equiv 5 \pmod 9$*. De fato, se tem*

$$5 \equiv 5 \pmod 9$$

*e por transitividade, vem*

$$5^m \equiv 5 \pmod 9$$

*do Teorema 2.8.2, obtemos*

$$m \equiv 1 \pmod 6 \tag{3.17}$$

*Das congruências 3.14 e 3.17 podemos concluir que $n$ é par e $m$ é ímpar.*

*Este procedimento feito até aqui não é suficiente para garantir que $n = 2$ e $m = 1$ é a única solução. Devemos então analisar a existência de soluções maiores que estas e comparar com a paridade de $n$ e $m$ que já determinamos.*

*Suponhamos, então que $n > 2$, logo devemos ter que $3^3 | 3^n$, assim relativo a módulo $27$,*

$$\begin{aligned} 5^m &\equiv -4 \pmod{27} \\ 5^m &\equiv 23 \pmod{27} \end{aligned} \tag{3.18}$$

*Como $\phi(27) = 18 = ord_{27}(5)$, temos que $5$ é raiz primitiva módulo $27$ e o conjunto*

$$S^5_{(\text{mod } 27)} = \{5,\ 5^2,\ \cdots,\ 5^{18}\} \tag{3.19}$$

*forma um sistema reduzido de resíduos módulo $27$, e sendo $(23, 27) = 1$ deve existir $t$ com $5^t \in S_{27}$ tal que $5^t \equiv 23 \pmod{27}$. De fato,*

$$5^{13} \equiv 23 \pmod{27}$$

*por transitividade e do Teorema 2.8.2, resulta*

$$\begin{aligned} 5^{13} &\equiv 5^m \pmod{27} \iff \\ m &\equiv 13 \pmod{18}. \end{aligned} \tag{3.20}$$

*O resultado da equivalência 3.20 não é necessariamente uma contradição com 3.17. Dessa forma, considerando a congruência*

$$3^m - 5^n \equiv 4 \pmod{\text{x}}$$

*queremos encontrar um primo $x$ de modo que $m = 18y + 13$ para algum $y \in \mathbb{N}$, que contradiga a hipótese de $n$ ser par.*

*Nesse momento testamos alguns primos para os valores de $x$ no comando abaixo:*

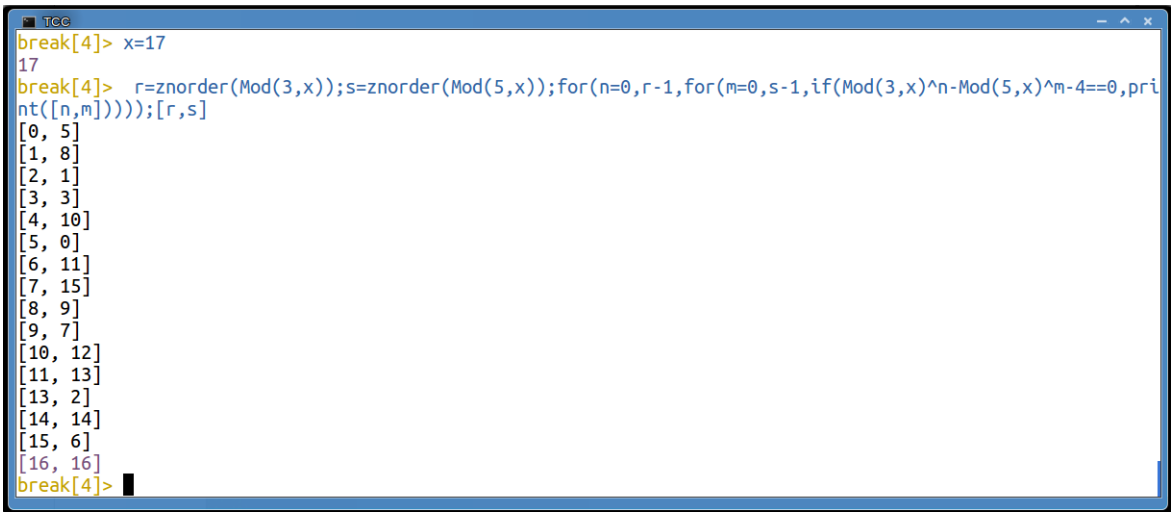
| Equação | Comando no Pari/GP |
|---|---|
| $3^n - 5^m = 4$ | `r=znorder(Mod(3,x));s=znorder(Mod(5,x));for(n=0,r-1,for(m=0,s-1,`<br>`if(Mod(3,x)^n-Mod(5,x)^m-4==0,print([n,m])));[r,s]]` |

**Tabela 3.3:** *Comando para $3^n - 5^m = 4$*

*Faremos alguns testes utilizando o comando da Tabela 3.3 acima afim de encontrarmos um $m$ tal que $m \equiv 13 \pmod{18}$ e que, como já dissemos, nos dê uma contradição relativo a paridade de $n$, que já sabemos ser "par".*

*Para $x = 17$ temos, conforme a saída do comando mostrado na figura 3.2, os seguintes resultados:*

**Figura 3.2:** *Comando para* $3^n - 5^m = 4$ *módulo* $x$




- *as ordens de* $3$ *e* $5$ *são iguais para este módulo;*
- *tanto* $3$ *como* $5$ *são raízes primitivas;*
- *a linha* $[11, 13]$ *é a única em que temos* $m \equiv 13 \pmod{18}$ *e como vemos nos dá um valor ímpar para* $n$*.*

*Faremos uma análise qualitativa relativa a módulo* $17$*. Temos, para este módulo que:*

$$3^n - 5^m \equiv 4 \pmod{17} \tag{3.21}$$

*Como* $\phi(17) = 16 = ord_{17}(3) = ord_{17}(5)$*, temos que* $3$ *e* $5$ *são raízes primitivas módulo* $17$ *e os conjuntos*

$$S^3_{(\text{mod } 17)} = \{3,\ 3^2,\ \cdots,\ 3^{16}\} \tag{3.22}$$

$$S^5_{(\text{mod } 17)} = \{5,\ 5^2,\ \cdots,\ 5^{16}\} \tag{3.23}$$

*forma um sistema reduzido de resíduos módulo* $17$*, daí por 3.20 devemos ter* $m = 18w + 13$ *para algum* $w \in \mathbb{N}$*, vem que, para todo* $x \in \mathbb{N}$*, temos*

$$\begin{aligned} 5^{16x} &\equiv 1 \pmod{17} \Longrightarrow \\ (5^{16x})^9 = 5^{18(8x)} &\equiv 1 \pmod{17} \Longrightarrow \\ 5^{18(8x)+13} &\equiv 3 \pmod{17} \end{aligned} \tag{3.24}$$

*e substituindo na relação 3.21, resulta*

$$\begin{aligned} 3^n - 3 &\equiv 4 \pmod{17} \Longleftrightarrow \\ 3^n &\equiv 7 \pmod{17} \end{aligned}$$

(3.25)

Agora, como $(7,17)=1$ deve existir $3^f \in S^3_{(\mathrm{mod}\ 17)}$ tal que $3^f \equiv 7\,(\mathrm{mod}\ 17)$, de fato

$$3^{11} \equiv 7\,(\mathrm{mod}\ 17)$$

e por transitividade,

$$3^{11} \equiv 3^n\,(\mathrm{mod}\ 17)$$

mas isso significa que $n \equiv 11\,(\mathrm{mod}\ 16)$, que é absurdo pois $n$ é par.

□

**Problema 3.3.2.** *Determine todas as soluções inteiras não negativas da equação* $3^x - 2^y = 7$.

**Solução 3.3.2.** *Primeiro faremos uma análise através do Pari/GP tomando alguns primos como módulo para obtermos qual o melhor a ser utilizado no problema. Faremos uso do seguinte comando conforme a Tabela 3.4 abaixo.*

| Equação | Comando no Pari/GP |
|---|---|
| $3^x - 2^y = 7$ | `r=znorder(Mod(3,m));s=znorder(Mod(2,m));for(x=0,r-1,for(y=0,s-1,if(Mod(3,m)^x-Mod(2,m)^y-7==0,print([x,y]))));[r,s]` |

**Tabela 3.4:** *Comando para* $3^x - 2^y = 7$

*Na Tabela 3.5 abaixo estão a saída para o comando relativo ao módulo* $m$ *e suas respectivas ordens.*

| $m$ | $[x,y]$ | | | | | **Ordem** |
|---|---|---|---|---|---|---|
| 5 | $[0,2]$ | $[1,0]$ | $[2,1]$ | | | $[4,4]$ |
| 7 | $[0,0]$ | $[2,1]$ | $[4,2]$ | | | $[6,3]$ |
| 11 | $[0,4]$ | $[1,7]$ | $[2,1]$ | $[3,6]$ | $[4,3]$ | $[5,10]$ |

**Tabela 3.5:** *Soluções módulo* $m$ *para* $3^x - 2^y = 7$.

*A equação*

$$3^x - 2^y = 7 \tag{3.26}$$

*tem somente uma solução nos inteiros não negativos, que é* $x=2$ *e* $y=1$. *De fato, se* $y=0$, *temos que* $3^x = 8$, *que é falso para todo* $x$ *inteiro.*

*Suponha* $y \geqslant 2$. *Dessa forma como* $2^2 | 2^y$, *temos, relativo ao módulo* $4$, *que*

$$3^x \equiv 7 \equiv 3 \pmod 4$$

*Como* $\phi(4) = ord_4(3) = 2$ *, então pela Definição 2.8.3,* $3$ *é raiz primitiva módulo* $4$, *daí pelo Teorema 2.8.3 temos que*

$$S^3_{(\mathrm{mod}\ 4)} = \{3,\ 3^2\}$$

*forma um sistema reduzido de resíduos módulo* $4$. *Neste caso, obviamente, temos:*

$$3^1 \equiv 3^x \pmod 4$$

*e pelo Teorema 2.8.2, resulta que*

$$x \equiv 1 \pmod 2. \tag{3.27}$$

*Portanto, $x$ é ímpar.*

*Por outro lado, se olharmos módulo 7 para a equação 3.26, temos:*

$$\begin{aligned} 3^x - 2^y &\equiv 7 \pmod 7 \Longleftrightarrow \\ 3^x &\equiv 2^y \pmod 7 \end{aligned} \tag{3.28}$$

*Agora como $6 = \phi(7) = ord_4(3) \neq ord_7(3) = 3$, temos que:*

- *o conjunto*

  $$\{2^0, 2^1, 2^2\}$$

  *é formado por elementos incongruentes módulo 7, ou seja, para todo $w \in \mathbb{Z}$: $2^{3w} \equiv 1 \pmod 7$, $2^{3w+1} \equiv 2 \pmod 7$ ou $2^{3w+2} \equiv 4 \pmod 7$;*

- *já o conjunto*

  $$S^3_{(\text{mod } 7)} = \{3, 3^2, \cdots, 3^6 \equiv 1\}$$

  *é um sistema completo de reduzido de resíduos módulo 7, daí para todo $b \in \mathbb{Z}$, existe $h$, tal que*

  $$3^h \equiv b \pmod 7, \tag{3.29}$$

  *onde $(b,7) = 1$ e $h \in \{1, \cdots, 6\}$.*

*Por 3.28, queremos $h$ de modo que $3^h \equiv 1, 2$ ou $4 \pmod 7$. Logo, sendo $3^6 \equiv 1 \pmod 7$, temos os seguintes casos:*

- *Se $y = 3w$, então $3^x \equiv 2^y \equiv 1 = 2^0 \pmod 7$ e obtemos $x \equiv 0 \pmod 6$.*
- *Se $y = 3w+1$, então $3^x \equiv 2^y \equiv 2 \pmod 7 \Rightarrow 3^x \equiv 9 = 3^2 \pmod 7$ e obtemos $x \equiv 2 \pmod 6$.*
- *Se $y = 3w+2$, então $3^x \equiv 2^y \equiv 4 \pmod 7 \Rightarrow 3^x \equiv 81 = 3^4 \pmod 7$ e obtemos $x \equiv 4 \pmod 6$.*

*Em qualquer caso, temos portanto $x$ par o que é uma contradição. Assim $y$ não pode ser maior do que ou igual a 2 e $X = 2$ e $y = 1$ é a única solução.*

□

Utilizaremos as mesmas estratégias utilizadas até aqui para resolver um problema que como poderemos observar trará outras dificuldades a serem contornadas. O problema seguinte foi retirado de ANDREESCU(2000, p. 86) e sua solução original está no Anexo A.

**Problema 3.3.3.** *Determine todas as soluções inteiras da equação* $5^a7^b+4=3^c$.

**Solução 3.3.3.** *Dada a equação*

$$5^a7^b+4=3^c \tag{3.30}$$

*por verificação podemos notar que* $a=1$, $b=0$ *e* $c=2$ *é uma solução.*

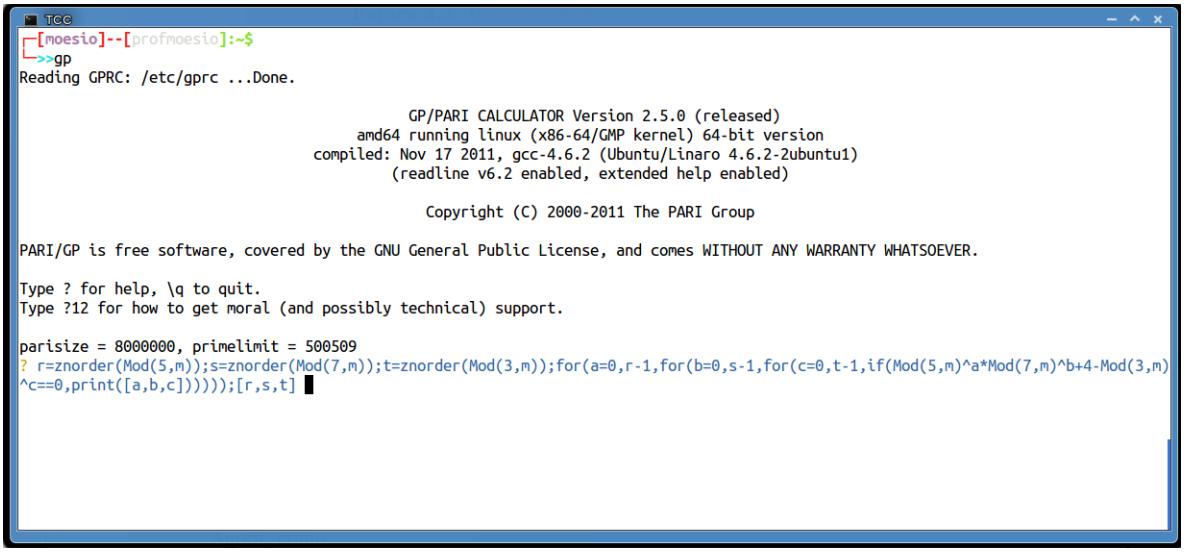
*Como dito acima precisaremos utilizar números relativamente primos com* $3$, $5$, *e* $7$, *para determinarmos aqueles cujas ordens sejam relativamente pequenas faremos uso do seguinte comando no Pari/GP:*

| Equação | Comando no Pari/GP |
|---|---|
| $5^a7^b+4=3^c$ | `r=znorder(Mod(5,m)),s=znorder(Mod(7,m));t=znorder(Mod(3,m));`<br>`for(a=0,r-1,for(b=0,s-1,for(c=0,t-1,if(Mod(5,m)^a*Mod(7,m)^b`<br>`+4-Mod(3,m)^c==0,print([a,b,c])))));[r,s,t]]` |

**Tabela 3.6:** *Comando para* $5^a7^b+4=3^c$ *módulo* $m$

*Na figura 3.3 temos a aplicação do comando da Tabela 3.6.*

**Figura 3.3:** *Comando para ordens e soluções módulo* $m$.

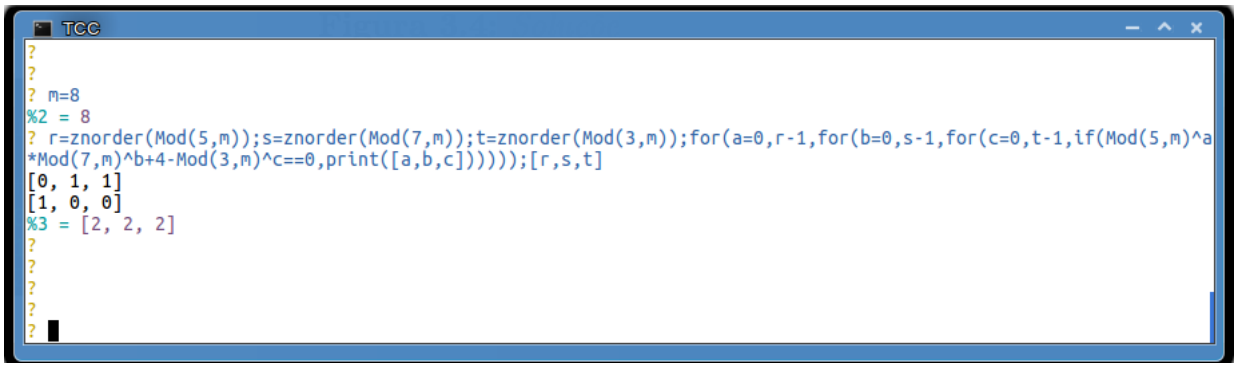



*O comando 3.6 determina a ordem de* $3$, $5$ *e* $7$ *relativa a* $m$ *e as soluções para a equação* $5^a7^b+4-3^c$ *módulo* $m$ *com seus expoentes variando no intervalo de* $0$ *até* $r-1$, $s-1$ *e* $t-1$, *onde* $r$, $s$ *e* $t$ *são as ordens de* $3$, $5$ *e* $7$, *respectivamente. Por exemplo, se fizermos* $m=8$, *obteremos a saída conforme a figura 3.4.*

*Na figura 3.4,* $\{[0,1,1],[1,0,0]\}$ *são os valores de* $[a,b,c]$ *que são soluções para a equação* $5^a7^b+4\equiv 3^c \pmod 8$ *e os valores* $[2,2,2]$ *são as ordens de* $3$, $5$ *e* $7$, *respectivamente. No Apêndice B, temos as soluções para outros módulos.*

*Devemos, nesta altura, escolher um valor para* $m$ *em que* $3$, $5$ *e* $7$ *tem ordem relativamente pequenas, é claro, que isso não é uma tarefa fácil.*

**Figura 3.4:** *Soluções e Ordens módulo* 8.




*Para essa tarefa, faremos o seguinte procedimento, escolheremos uma ordem* $x$ *e depois determinaremos todos os módulos onde "*$a$*" tem ordem dividindo* $k$*, tais módulos serão pela Proposição 2.8.4 também divisores de* $a^k - 1$*, ou seja, dado* $k$ *e* $ord_m(a)|k \implies m|a^k - 1$*.*

*Por exemplo, tomando* $k$ *igual a* 12*, e aplicando o comando "*`factor(3^{12}-1)`*" no Pari/GP, obtemos os divisores de* $3^{12} - 1$ *que são:*

$$D = \{2^4,\ 5,\ 7,\ 13,\ 73\},$$

*ou seja,* $3^{12} \equiv 1 \pmod{m}$ *com* $m \in D$*.*

*Queremos todos os valores de* $m$ *inteiro tais que* $3^x \equiv 1 \pmod{m}$ *onde* $x = ord_m(3)|k = 12$*.*

*Faremos primeiro a eliminação de outras soluções e determinaremos a paridade de* $a$*,* $b$ *e* $c$*.*

*Note que para* $c = 0$*, obtemos:*

$$\begin{aligned} (5^a)(7^b)+4 &= 1 \iff \\ (5^a)(7^b) &= -3 \end{aligned}$$

*logo não há soluções, pois* $-3$ *não é uma potência de* 5 *vezes uma potência de* 7*.*

*Agora relativo a módulo* 3 *temos que, como* $3^c$ *é divisível por* 3*, isso significa que*

$$\begin{aligned} (5^a)(7^b)+4 = 3^c &\equiv 0 \pmod 3 \iff \\ (5^a)(7^b) &\equiv -4 \pmod 3 \iff \\ (5^a)(7^b) &\equiv -1 \pmod 3 \end{aligned}$$

*Agora como* $7 \equiv 1 \pmod{3}$*, então* $7^b \equiv 1 \pmod 3$ *para todo* $b \in \mathbb{N}$ *e, como* $5 \equiv -1 \pmod 3$ *então,* $5^a \equiv (-1)^a \pmod 3$ *daí pelo, item (f) da Propriedade 2.7.1, resulta*

$$(5^a)(7^b) \equiv (-1)^a \equiv -1 \pmod 3$$

*a partir do qual podemos concluir que* $a$ *é um número ímpar, pois se* $a$ *fosse par teríamos* $(-1)^a = 1 \not\equiv -1 \pmod 3$*.*

*Agora, reduzindo módulo* $8$*:*

$$(5^a)(7^b)+4 \equiv 3^c \pmod 8.$$

*Como,* $5^2 \equiv 1 \pmod 8$*, isso significa que* $5^{2k+1} \equiv 5 \pmod 8$*, para todo* $k \in \mathbb{N}$*, logo* $5^a \equiv 5 \pmod 8$*. Temos também que,* $3^2 \equiv 1 \pmod 8$ *donde* $3^{2k} \equiv 1 \pmod 8$ *e* $3^{2k+1} \equiv 3 \pmod 8$*, para todo* $k \in \mathbb{N}$*, portanto* $3^c \equiv 1$ *ou* $3 \pmod 8$*, se* $c$ *for par ou ímpar, respectivamente.*

*De* $7 \equiv -1 \pmod 8$ *obtemos que* $7^b \equiv (-1)^b \pmod 8$ *e, então*

$$(5^{a+1})(7^b) \equiv (5^2)(-1)^b \equiv (-1)^b \equiv 5(3^c-4) \pmod 8$$

*logo,*

$$(-1)^b \equiv \begin{cases} 1 \pmod 8, \text{ se } c \text{ for par} \\ \qquad ou \\ 3 \pmod 8, \text{ se } c \text{ for ímpar} \end{cases}$$

*o que implica que* $b$ *é par, pois se* $b$ *fosse ímpar teríamos* $(-1)^b = -1 \not\equiv 1 \pmod 8$ *caso* $c$ *fosse par ou* $(-1)^b = -1 \not\equiv 3 \pmod 8$*, caso* $c$ *fosse ímpar. Em particular, temos que* $c$ *é par.*

*Utilizaremos nesse momento potências de* $3$ *ou* $5$ *com expoentes superiores as soluções consideradas. Supondo* $a \geqslant 2$*, então* $5^2 \mid 5^a$ *faremos uma análise da equação 3.30 em relação a módulo* $25$*, assim:*

$$\begin{aligned}(5^a)(7^b)+4 \equiv 3^c \pmod{25} &\iff \\ 4 \equiv 3^c \pmod{25}&\end{aligned}$$

*Fazendo no Pari/GP o comando* `znorder(Mod(3,25))`*, obtemos que* $3$ *tem ordem* $20$*, então como* $\phi(25) = ord_{25}(3)$ *temos que* $3$ *é uma raiz primitiva módulo* $25$ *e o conjunto*

$$S^3_{(\text{mod } 25)} = \{3,\ 3^2, \cdots,\ 3^{20}\}$$

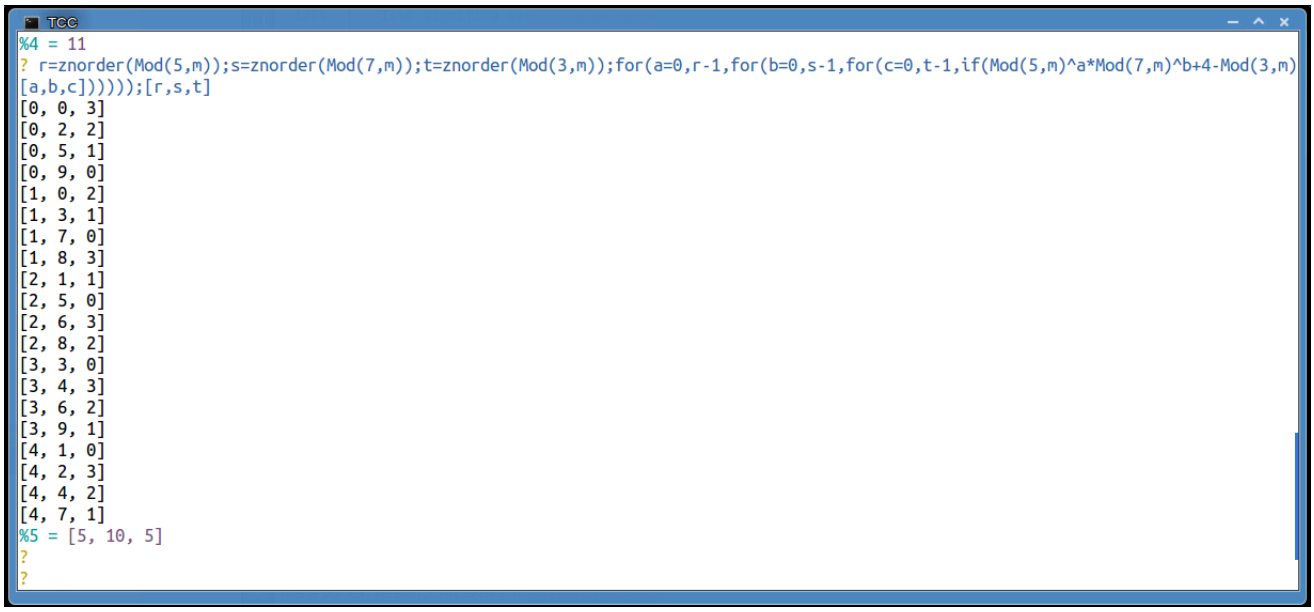
*é um sistema reduzido de resíduos módulo* $25$*, e como* $3^6 \equiv 4 \pmod{25}$ *por transitividade obtemos* $3^c \equiv 3^6 \pmod{25}$ *e pelo Teorema 2.8.2 isso significa que* $c \equiv 6 \pmod{20}$*. Note também, que sendo* $c = 20k+6 = 5(4k+1)+1$*, temos que,* $c \equiv 1 \pmod 5$*. Fazendo no Pari/GP* $m = 11$*, encontramos, conforme a figura 3.5, as soluções para equações relativas a esse módulo.*

*Na saída do comando da figura 3.5 para* $a \geqslant 2$ *e* $c \equiv 1 \pmod 5$ *obtemos os seguintes resultados:* $[a,b,c] \in \{[2,1,1],\ [3,9,1],\ [4,7,1]\}$ *o que mostra que* $b$ *é ímpar, o que é uma contradição pois já havíamos mostrado que* $b$ *é par. Daremos uma justificativa para isto, porém é claro, já estamos sabendo que* $11$ *é um módulo ideal.*

*Como* $ord_{11}(3) = 5$ *o conjunto*

$$\{1, 3,\ 3^2, \cdots, 3^{10}\}$$

**Figura 3.5:** *Soluções para módulo* 11.




*é formado por elementos incongruentes módulo* 11. *De* $3^5 \equiv 1 \pmod{11}$ *temos para todo* $q \in \mathbb{N}$, $3^{5q+1} \equiv 3 \pmod{11}$, *logo* $3^c \equiv 3 \pmod{11}$ *e, portanto*

$$(5^a)(7^b)+4 = 3^c \equiv 3 \pmod{11} \iff$$
$$(5^a)(7^b) \equiv -1 \pmod{11}$$

*assim temos que, como* $ord_{11}(5) = 5$, *o conjunto*

$$\{1,\ 5,\ 5^2,\ 5^3,\ 5^4\}$$

*é formado por elementos incongruentes módulo* 11 *e sendo* $a$ *ímpar devemos ter*

$$5^a \equiv 5 \pmod{11}$$
$$5^a \equiv 5^3 \equiv 4 \pmod{11}$$

*Por outro lado, como* $\phi(11) = ord_{11}(7) = 10$ *temos que* 7 *é raiz primitiva módulo* 11 *e, o conjunto*

$$S^7_{(\text{mod } 11)} = \{7,\ 7^2.\cdots,7^10\}$$

*é um sistema reduzido de resíduos módulo* 11. *Como* $b$ *é par, então*

$$7^b \equiv 7^2 \equiv 5 \pmod{11} \tag{3.31}$$
$$7^b \equiv 7^4 \equiv 3 \pmod{11} \tag{3.32}$$
$$7^b \equiv 7^6 \equiv 4 \pmod{11} \tag{3.33}$$
$$7^b \equiv 7^8 \equiv 9 \pmod{11} \tag{3.34}$$
$$7^b \equiv 7^{10} \equiv 1 \pmod{11} \tag{3.35}$$

*Pela Propriedade 2.7.1, multiplicando as equivalências 3.31, 3.32, 3.33, 3.34 e 3.35 com* $5^a \equiv 5 \pmod{11}$ *ou* $5^a \equiv 4 \pmod{11}$ *verificamos que em nenhum caso teremos*

$$(5^a)(7^b) \equiv -1 \pmod{11}. \tag{3.36}$$

*Portanto a equação 3.30 não possui solução módulo* $11$ *para* $a \geqslant 2$.

*Verificamos, assim, que para esse primeiro caso em que* $a \geqslant 2$*, não há soluções. Resta verificar se para os caos* $a = 0$ *e* $a = 1$ *se há soluções ou não. Na primeira situação temos, para* $a = 0$*:*

$$7^b + 4 = 3^c \tag{3.37}$$

*Neste caso a equação só tem duas bases* $7$ *e* $3$*. Podemos fazer algumas simulações no Pari/GP aplicando o comando 3.7 para saber algumas informações sobre a equação 3.37.*

| Equação | Comando no pari/GP |
|---|---|
| $7^b + 4 = 3^c$ | `s=znorder(Mod(7,m));t=znorder(Mod(3,m));for(b=0,s-1,for(c=0,t-1, if(Mod(7,m)^b+4-Mod(3,m)^c==0,print([b,c])));[s,t]` |

**Tabela 3.7:** *Comando para* $7^b + 4 = 3^c$ *módulo* $m$.

*Aplicando o comando 3.7, note que o módulo* $8$ *nos dá que* $ord_8(7) = ord_8(3) = 2$*. Como* $7 \equiv -1 \pmod{8}$*, então* $7^b \equiv (-1)^b \pmod{8}$*, daí*

$$(-1)^b \equiv 3^c - 4 \pmod{8}.$$

*Consideremos dois casos:*

- *Se* $c$ *for par, então como* $3^2 \equiv 1 \pmod{8} \Longrightarrow 3^{2k} \equiv 1 \pmod{8}$*, para todo* $k \in \mathbb{N}$*, logo*

$$(-1)^b \equiv 3^c - 4 \pmod{8} \Longleftrightarrow$$
$$(-1)^b \equiv 1 - 4 = -3 \pmod{8}$$

  *Donde concluímos que tanto para* $b$ *par ou* $b$ *ímpar* $(-1)^b \not\equiv -3 \pmod{8}$ *e, portanto não podemos ter* $c$ *par.*

- *Se* $c$ *for ímpar, teremos* $3^2 \equiv 1 \pmod{8} \Longrightarrow 3^{2k+1} \equiv 3 \pmod{8}$*, para todo* $k \in \mathbb{N}$*, logo*

$$(-1)^b \equiv 3^c - 4 \pmod{8} \Longleftrightarrow$$
$$(-1)^b \equiv -1 = 3 - 4 \pmod{8}$$

  *daí para* $b$ *par* $(-1)^b = 1 \not\equiv -1 \pmod{8}$ *e para* $b$ *ímpar* $(-1)^b = -1 \equiv -1 \pmod{8}$.

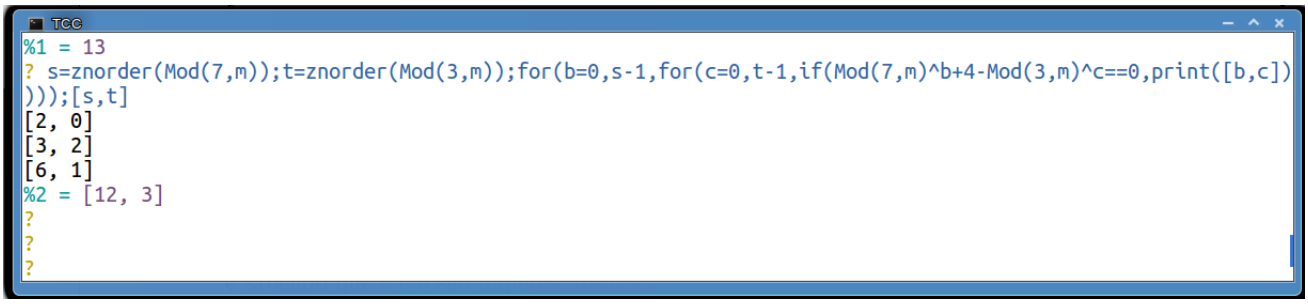
*Portanto* $c$ *e* $b$ *devem ser ambos ímpares.*

Por outro lado, olhando para equação módulo $13$, ou seja,

$$7^b + 4 \equiv 3^c \pmod{13}$$

e sabendo que $c$ e $b$ são ímpares, resulta que $b$ é divisível por $3$. Esse fato também poderia ser comprovado fazendo $m = 13$ e aplicando o comando conforme a figura 3.6. Agora, como $ord_{19}(7) =$

**Figura 3.6:** *Soluções para módulo* $13$.




$3$, o conjunto

$$\{7^0,\ 7,\ 7^2\}$$

é formado por elementos incongruentes módulo $19$. Como $b$ é ímpar e múltiplo de $3$, temos

$$\begin{aligned} 3^c = 7^b + 4 \equiv 7^3 + 4 \equiv 1 + 4 \pmod{19} \iff \\ 3^c \equiv 5 \pmod{19} \end{aligned}$$

como $ord_{19}(3) = 18$[3], temos que $3$ é raiz primitiva módulo $19$ e, o conjunto

$$S^3_{(\text{mod } 19)} = \{3,\ 3^2, \cdots, 3^{18}\}$$

forma um sistema completo de resíduos módulo $19$. Note que $3^4 \equiv 5 \pmod{19}$ e por transitividade

$$3^c \equiv 3^4 \pmod{19}$$

e pelo Teorema 2.8.2 obtemos que $c \equiv 4 \pmod{18}$, logo $c$ é par, contradição. Portanto não existe solução para equação $7^b + 4 = 3^c$.

Finalmente verificaremos que $a = 1$ é a única solução para a e equação $5^a 7^b + 4 = 3^c$.

Seja $a = 1$ então, temos $5 \cdot 7^b + 4 = 3^c$, se $b = 0$:

$$5^a 7^b + 4 = 5 + 4 = 9 = 3^c \implies c = 2.$$

Agora verificaremos que não existem soluções para $b > 0$. Como feito anteriormente começaremos utilizando alguma das potências que ainda constam na equação como estamos interessados em $b$ examinaremos em relação ao módulo $7$. Supondo por absurdo $b > 0$, então $7 \mid 7^b$.

$$\begin{aligned} 5 \cdot 7^b + 4 &\equiv 3^c \pmod{7} \\ 4 &\equiv 3^c \pmod{7},. \end{aligned}$$

[3] Esse fato pode ser facilmente verificado rodando o comando znorder(Mod(3,19)).

Como $\phi(7) = ord_7(3) = 6$ 3 é raiz primitiva e sendo $3^4 \equiv 4 \pmod 7$, resulta pelo Teorema 2.8.2 que $c \equiv 4 \pmod 6$. Agora se examinarmos os fatores de $3^6 - 1$, podemos utilizar o comando *factor* no Pari/GP e teremos os seguintes fatores $2,\ 7$ e $13$, conforme a figura 3.7.

**Figura 3.7:** *Fatoração de* $3^6 - 1$.


Escolhendo como módulo o fator $13$ , ou seja, $5 \cdot 7^b + 4 \equiv 3^c \pmod{13}$. Como $c \equiv 4 \pmod 6$ e sabendo que $3^3 \equiv 1 \pmod{13}$ donde obtemos que

$$3^{6k} \equiv 1 \pmod{13} \Longrightarrow$$
$$3^{6k}3^4 = 3^{3k+4} \equiv 3^4 \equiv 3 \pmod{13},$$

para todo $k \in \mathbb{N}$, ou seja,

$$3^c \equiv 3 \pmod{13} \tag{3.38}$$

Por outro lado, como $\phi(13) = ord_{13}(7) = 12$ temos que 7 é raiz primitiva módulo $13$. Como

$$\begin{aligned} 5 \cdot 7^b + 4 &\equiv 3^c \pmod{13} \Longleftrightarrow \\ 5 \cdot 7^b + 4 &\equiv 3 \pmod{13} \Longleftrightarrow \\ 5 \cdot 7^b &\equiv -1 \pmod{13} \Longleftrightarrow \\ 5 \cdot 7^b &\equiv 25 \pmod{13} \Longleftrightarrow \\ 7^b &\equiv 5 \pmod{13} \Longleftrightarrow \\ 7^b &\equiv 7^3 \pmod{13} \end{aligned}$$

e pelo **Teorema 2.8.2** obtemos $b \equiv 3 \pmod{12}$.

Sabendo que $7^3 \equiv 1 \pmod{19}$, daí

$$\begin{aligned} 7^{12q+3} &\equiv 7^3 \pmod{19} \Longleftrightarrow \\ 7^{12q+3} &\equiv 1 \pmod{19}, \forall\ q \in \mathbb{N}, \end{aligned}$$

desse fato obtemos

$$\begin{aligned} 5 \cdot 7^b + 4 &\equiv 5 \cdot 1 + 4 = 9 \pmod{19} \Longleftrightarrow \\ 3^2 &\equiv 3^c \pmod{19} \end{aligned} \tag{3.39}$$

Agora, como $ord_{19}(3) = 18$ e pelo Teorema 2.8.2 temos $c \equiv 2 \pmod{18}$ o que é absurdo, pois já tínhamos $c \equiv 4 \pmod{6}$.

Isso, portanto, mostra que não podemos ter $b > 0$, sendo então $b = 0$ a única solução possível e, que implica, como já mostramos que $c = 2$ e $a = 1$.

# 4 Conclusões

A complexidade de abordagem nas soluções de problemas que envolvem equações diofantinas podem ser superadas, a apresentação de forma contextualizadas, conforme feito na seção 2.10 ou, quando no caso dos problemas mais teóricos mas feito de forma a estarem inseridos em uma contextualização teórica, como nos Problemas 3.3.1 e 3.3.3. A teoria de Números mostrou sua importância a medida que durante a exploração dos problemas foram surgindo situações que exigiram novas posturas.

O ensino significativo tem como objetivo oportunizar ao aluno uma nova e diferente maneira de ver os conteúdos, através do contato e estímulo, desta forma, uma alternativa ao modelo didático tradicional.

Deve-se também lembrar que o objetivo da abordagem desses tipos de problemas é significar o algoritmo, pela valorização dos conteúdos procedimentos, em articulação com o desenvolvimento de conhecimentos.

Alguns teoremas e proposições dessa teoria foram essenciais, por exemplo: Proposição 2.8.4, Teorema 2.8.2, Corolário 2.8.3, Teorema 2.8.3 e Corolário 2.8.4 que nos permitiu reduzir o conjunto solução dos problemas. Além disso, presenciamos diversas aplicações do Pari/GP que se mostrou uma importante ferramente de auxilio para compreender de forma construtiva e intuitiva o melhor modo de testar e comparar soluções nos tipos de problemas considerados. Destaca-se, portanto, o grande potencial do Pari/GP na exploração através de levantamentos de informações sobre vários aspectos de contorno dos problemas considerados.

O aluno no papel de pesquisador, ou seja, quando ele busca e testa informações, tem a seu favor que todos os procedimentos por ele testados são frutos de uma experimentação e este pode ser relembrado em outras ocasiões e possibilitar compreender e rememorar o algoritmo.

> [...] é preciso tornar os alunos pessoas capazes de enfrentar situações e contextos variáveis, que exijam deles a aprendizagem de novos conhecimentos e habilidades. Por isso, os alunos que hoje aprenderem a aprender estarão, previsivelmente, em melhores condições de adaptar-se às mudanças culturais, tecnológicas e profissionais que nos aguardam na virada do milênio (POZO, 1998, p. 9)

Em geral nas soluções utilizando congruências trabalhadas no Capítulo 3 tivemos sempre considerar implicitamente a conjectura de Skolem pois dado a equação $a^x - b^y = c$ nas incógnitas $x$,$y \in \mathbb{N}$ sempre era necessário encontrar um módulo $m$ inteiro maior do que ou igual a $2$ para o qual

a congruência $a^x - b^y \equiv c \pmod{m}$ não tivesse solução. Nos casos considerados aqui se verificou sempre existência de tais módulo. No problema 3.3.1 foi necessário calcular as soluções módulo $m$ para os $17$ primeiros números naturais primos com $3$ e $5$, no Problema 3.3 foram calculados as soluções módulo $m$ para os $11$ primeiros números naturais primos com $3$ e $2$, e finalmente no Problema 3.3.3 foram calculados os módulos para todas os divisores de $3^{12} - 1$, as soluções para este caso estão na Tabela B.1 do Apêndice B.

Percebe-se a importância da teoria dos números e das equações diofantinas lineares e exponenciais que poderiam estar no currículo do Ensino Médio, sabendo que a base necessária para trabalhá-lo já está presente neste nível de ensino. Esperamos portanto que este trabalho sirva como fonte de informação para o professor o que o ajude na tarefa da formação de alunos capazes de selecionar as informações e de realizar pesquisas.

# 5 Referências Bibliográficas


ANDREESCU, Titu; GELCA, R. **Mathematical Olympiad Challenges**. New York: Birkhauser, 2000.

ANDREESCU, Titu; ANDRICA, Dorin; CUCUREZEANO, Ion. **An Introduction to Diophantine Equations**. New York: Birkhauser, 2010.

BATUT, C. **User's Guide to PARI-GP** . Université Bordeaux, Laboratoire A2X. 1997. Disponível em: <http://math.mit.edu/ brubaker/PARI/PARIusers.pdf>. Acesso em: 01 mai. 2013.

BRASIL. Secretaria de Educação Média e Tecnológica. **PCN+ Ensino Médio: Orientações Educacionais complementares aos Parâmetros Curriculares Nacionais. Ciências da Natureza, Matemática e suas tecnologias**. Brasília: MEC/SEF, 2002.

BURTON, David M.. **Elementary Number Theory**. Boston. 1980.

BOYER, C.B., **História da Matemática**. 9. ed. São Paulo: Editora Edgard Blucher, 1991.

CERVO, Amado L.; BERVIAN, Pedro A.; SILVA, Roberto da. **Metodologia científica**. 6. ed. São Paulo: Pearson, 2009.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro, IMPA/SBM, 1997.

D'AMORE, Bruno. **Epistemologia e didática da Matemática**. São Paulo: Escrituras, 2005.

ECHEVERRÍA, M. P. P.; POZO, J. I. **Aprender a Resolver Problemas e Resolver Problemas para Aprender**. In: POZO, J. I. (org). **A Solução de problemas: Aprender a resolver, resolver para aprender**. Porto Alegre: ArtMed, 1998.

HEFEZ, Abramo. **Elementos de Aritmética**. Rio de Janeiro: SBM, 2011. (Coleção Textos Universitários).

HAJDU, Lajos. **A Hasse-type principle for exponential diophantine equations and its applications**. 23 slides: color. Budapest, 2013. Disponível em:< http://www.renyi.hu/conferences/erdos100/slides/hajdu.pdf >. Acesso em: 10 jul. 2013.

HAJDU, Lajos. **A Hasse-type principle for exponential diophantine equations and its applications**. Conferência. Budapest, 2013. Disponível em:< http://www.renyi.hu/conferences/erdos100/erdos100abs.pdf >. Acesso em: 10 jul. 2013.

HALMOS, Paul R.. **Teoria Ingênua dos Conjuntos**. Rio de Janeiro: Ciência Moderna, 2001. (Coleção Clássicos da Matemática).

LANDAU, Edmund. **Teoria elementar dos números**. Rio de Janeiro: Ciência Moderna, 2002. (Coleção Clássicos da Matemática).

LA ROQUE, G., PITOMBEIRA, J. B. **Uma Equação Diofantina e suas Resoluções**. In Revista do Professor de Matemática v. 19, p. 39-47, 1991.

LOZANSKY, Edward; ROUSSEAU, Cecil. **Winning Solutions**. New York: Springer, 1996.

LIMA, Elon Lages. **Matemática e Ensino**. Rio de Janeiro: SBM, 2002. (Coleção do Professor de Matemática).

MACHADO, N. J..**Educação: competência e qualidade**. São Paulo: Escrituras, 2009

MAYER, Rudolf. **Teoria dos Números**. UNB, 2005. Disponível em:<http://www.mat.unb.br/maierr /tnotas.pdf >. Acesso em: 03 jun. 2013.

MOREIRA, Carlos Gustavo T. de A.. **Introdução à Teoria dos Números(com ênfase em Aproximações Diofantinas)**. IMPA, 2005. Disponível em:< http://www.impa.br/˜gugu>. Acesso em: 12 jun. 2012.

NETO, Antonio Caminha Muniz. **Equações Diofantinas**. Revista Eureka!, vii, 2000. Disponível em:<http://www.obm.org.br/export/sites/default/revista_eureka/docs/ artigos/diofantinas.pdf>. Acesso em: 10 fev. 2014.

NIVEN, Ivan; ZUCKERMAN, H. S. **An Introduction to the Theory of Numbers**. New York: Wiley, 1960.

PATRÍCIO, Pedro. **Teoria de Números Computaciona visto pelos olhos do Pari/GP**. UMINHO, 2009. Disponível em:<http://w3.math.uminho.pt/ pedro/Aulas0708/TNC/notasTNC.pdf>. Acesso em: 10 fev. 2012.

PILLAI, Subbayya S.**On** $a^x - b^y = 1$. Indian Math. Soc. 1936.

PÓLYA, George. **A Arte de Resolver Problemas**. Rio de Janeiro: Editora Interciência, 2006

POZO, J. I. Introdução. In: POZO, J. I. (org).**A Solução de problemas: Aprender a resolver, resolver para aprender**. Porto Alegre: ArtMed, 1998.

SANTOS, José Plinio O.**Introdução à Teoria dos Números**. 1. ed. Rio de Janeiro: IMPA, 2007.

SHOREY, Tarlok. N.; TIJDEMAN, Robert. **Exponential Diophantine Equations**. Cambridge University Press, Cambridge, 1986.

STEIN, Wlliam. **Introdution to Computing and PARI**. Harward University, 2001. Disponívelem: <http://modular.math.washington.edu/edu/124/lectures/lecture3/lecture3.ps>. Acesso em:10 jul. 2013.

SKOLEM, Thoralf. **A method for the solution of the exponential equation** $A_1^{x_1} \cdots A_m^{x_m} - B_1^{y_1} \cdots B_n^{y_n} = C$. Norwegian, Norks Mat. Tidsskr, 1945.

SKOLEM, Thoralf. **Anwendung exponentieller Kongruenzen zum Beweis der Unlosbarkeit gewesser diophantisher Gleichungen**. Avh. Norske Vid. Akad. Oslo, 1937.

WALDSCHMIDT, Michel. **Perfect powers: Pillai's works and their developments**. 2009. Disponível em:<http://www.math.jussieu.fr/ miw/articles/pdf/PerfectPowers.pdf>. Acesso em:10 jun. 2013.

# *APÊNDICE A – Soluções*

A solução apresentada a seguir é uma tradução, com poucas modificações, da resolução encontrada em ANDREEESCU(2000, p. 86).

" Encontrar todas as soluções inteiras não negativas da equação $7^y 5^x + 4 = 3^z$."

**Solução A.0.4.** *Ou $x$ ou $y$ é diferente de zero, e olhando para a igualdade módulo $5$ ou módulo $7$, concluímos que $z$ deve ser no primeiro caso, da forma $4k+2$ e, no segundo caso da forma de $6k+4$. Seja $z = 2Z_1$ e reescrevendo a equação como $5^x 7^y = (3^{Z_1} - 2)(3^{Z_1} + 2)$. Os dois fatores são divisíveis apenas por potências de $5$ e $7$, e desde que sua diferença é $4$, eles devem ser relativamente primos. Assim, teremos $3^{Z_1} + 2 = 5^x$ e $3^{Z_1} - 2 = 7^y$ ou $3^{Z_1} + 2 = 7^y$ e $3^{Z_1} - 2 = 5^x$.*

*No primeiro caso, supondo $y \geq 1$, subtraindo-se as duas igualdades obtemos $5^x - 7^y = 4$. Olhando para os resíduos módulo $7$, podemos concluir que $x$ é da forma $6k+2$, portando par. Mas, então, como $x = 2x_1$, temos $7^y = (5^{x_1} - 2)(5^{x_1} + 2)$. Isso é impossível, pois a diferença entre os dois fatores é $4$, e assim eles não podem ser ambos potências de $7$. Daqui resulta que $y = 0$, e, consequentemente, $x = 1$, $z = 2$.*

*No segundo caso, mais uma vez, subtraindo as igualdades encontramos $7^y - 5^x = 4$. Olhando modulo $5$, concluímos que $y$ deve ser par e, usamos o mesmo argumento feito acima, mutatis mutandis, para mostrar que não existem soluções neste caso.*

# *APÊNDICE B – Tabelas*

Na Tabela B.1 encontra-se a saída do Comando 3.6 para as soluções, e suas respectivas ordens, módulo $m$ da equação $5^a 7^b - 3^c = 4$, com $m \in \{2,\ 4,\ 8,\ 16,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31\}$.

| ***Módulo*** $m$ | **Saída do Pari/GP** | |
|---|---|---|
| | ***Resultados das Potências*** [a,b,c] | **Ordem** |
| **2** | [0, 0, 0] | [1, 1, 1] |
| **4** | [0, 0, 0], [0, 1, 1] | [1, 2, 2] |
| **8** | [0, 1, 1],[1, 0, 0] | [2, 2, 2] |
| **16** | [0, 1, 3],[1, 0, 2],[2, 1, 1],[3, 0, 0] | [4, 2, 4] |
| **11** | [0, 0, 3],[0, 2, 2], [0, 5, 1], [0, 9, 0],[1, 0, 2],[1, 3, 1],[1, 7, 0], [1, 8, 3],[2, 1, 1],[2, 5, 0],[2, 6, 3], [2, 8, 2],[3, 3, 0],[3, 4, 3],[3, 6, 2], [3, 9, 1],[4, 1, 0],[4, 2, 3],[4, 4, 2], [4, 7, 1] | [5, 10, 5] |
| **13** | [0, 2, 0] ,[0, 3, 2], [0, 6, 1],[1, 0, 2],[1, 3, 1],[1, 11, 0],[2, 0, 1],[2, 8, 0], [2, 9, 2],[3, 5, 0],[3, 6, 2],[3, 9, 1] | [4, 12, 3] |
| **17** | [0, 0, 5], [0, 1, 7],[0, 2, 14],[0, 3, 11],[0, 4, 10],[0, 5, 6],[0, 6, 4],[0, 7, 8], [0, 8, 1],[0, 9, 9],[0, 10, 15],[0, 11, 0],[0, 13, 3],[0, 14, 13],[0, 15, 2],[1, 0, 2], [1, 1, 5],[1, 2, 7],[1, 3, 14],[1, 4, 11],[1, 5, 10],[1, 6, 6],[1, 7, 4],[1, 8, 8], [1, 9, 1],[1, 10, 9],[1, 11, 15],[1, 12, 0],[1, 14, 3],[1, 15, 13],[2, 0, 13],[2, 1, 2], [2, 2, 5],[2, 3, 7],[2, 4, 14],[2, 5, 11],[2, 6, 10],[2, 7, 6],[2, 8, 4],[2, 9, 8], [2, 10, 1],[2, 11, 9],[2, 12, 15],[2, 13, 0],[2, 15, 3],[3, 0, 3],[3, 1, 13],[3, 2, 2], [3, 3, 5],[3, 4, 7],[3, 5, 14],[3, 6, 11],[3, 7, 10],[3, 8, 6],[3, 9, 4],[3, 10, 8], [3, 11, 1],[3, 12, 9],[3, 13, 15],[3, 14, 0],[4, 1, 3],[4, 2, 13],[4, 3, 2],[4, 4, 5], [4, 5, 7],[4, 6, 14],[4, 7, 11],[4, 8, 10],[4, 9, 6],[4, 10, 4],[4, 11, 8],[4, 12, 1], [4, 13, 9],[4, 14, 15],[4, 15, 0],[5, 0, 0],[5, 2, 3],[5, 3, 13],[5, 4, 2],[5, 5, 5] [5, 6, 7],[5, 7, 14],[5, 8, 11],[5, 9, 10],[5, 10, 6],[5, 11, 4],[5, 12, 8],[5, 13, 1], [5, 14, 9],[5, 15, 15],[6, 0, 15],[6, 1, 0],[6, 3, 3],[6, 4, 13],[6, 5, 2],[6, 6, 5], [6, 7, 7],[6, 8, 14],[6, 9, 11],[6, 10, 10],[6, 11, 6],[6, 12, 4],[6, 13, 8],[6, 14, 1], [6, 15, 9],[7, 0, 9],[7, 1, 15],[7, 2, 0],[7, 4, 3],[7, 5, 13],[7, 6, 2],[7, 7, 5], [7, 8, 7],[7, 9, 14],[7, 10, 11],[7, 11, 10],[7, 12, 6],[7, 13, 4],[7, 14, 8],[7, 15, 1], [8, 0, 1],[8, 1, 9],[8, 2, 15],[8, 3, 0],[8, 5, 3],[8, 6, 13],[8, 7, 2],[8, 8, 5],[8, 9, 7], [8, 10, 14],[8, 11, 11],[8, 12, 10],[8, 13, 6],[8, 14, 4],[8, 15, 8],[9, 0, 8],[9, 1, 1], [9, 2, 9],[9, 3, 15],[9, 4, 0],[9, 6, 3],[9, 7, 13],[9, 8, 2],[9, 9, 5],[9, 10, 7],[9, 11, 14], [9, 12, 11],[9, 13, 10],[9, 14, 6],[9, 15, 4],[10, 0, 4],[10, 1, 8],[10, 2, 1],[10, 3, 9],[10, 4, 15], [10, 5, 0],[10, 7, 3],[10, 8, 13],[10, 9, 2],[10, 10, 5],[10, 11, 7],[10, 12, 14],[10, 13, 11],[10, 14, 10], [10, 15, 6],[11, 0, 6],[11, 1, 4],[11, 2, 8],[11, 3, 1],[11, 4, 9],[11, 5, 15],[11, 6, 0],[11, 8, 3], [11, 9, 13],[11, 10, 2],[11, 11, 5],[11, 12, 7],[11, 13, 14],[11, 14, 11],[11, 15, 10],[12, 0, 10], [12, 1, 6],[12, 2, 4],[12, 3, 8],[12, 4, 1],[12, 5, 9],[12, 6, 15],[12, 7, 0],[12, 9, 3],[12, 10, 13] | [16, 16, 16] |
| **17** | [12, 11, 2],[12, 12, 5],[12, 13, 7],[12, 14, 14],[12, 15, 11],[13, 0, 11],[13, 1, 10],[13, 2, 6], [13, 3, 4],[13, 4, 8],[13, 5, 1],[13, 6, 9],[13, 7, 15],[13, 8, 0],[13, 10, 3],[13, 11, 13],[13, 12, 2], [13, 13, 5],[13, 14, 7],[13, 15, 14],[14, 0, 14],[14, 1, 11],[14, 2, 10],[14, 3, 6],[14, 4, 4],[14, 5, 8], [14, 6, 1],[14, 7, 9],[14, 8, 15],[14, 9, 0],[14, 11, 3],[14, 12, 13],[14, 13, 2],[14, 14, 5],[14, 15, 7], [15, 0, 7],[15, 1, 14],[15, 2, 11],[15, 3, 10],[15, 4, 6],[15, 5, 4],[15, 6, 8],[15, 7, 1],[15, 8, 9], [15, 9, 15],[15, 10, 0],[15, 12, 3],[15, 13, 13],[15, 14, 2],[15, 15, 5] | [16, 16, 16] |
| **19** | [0, 0, 4],[0, 1, 12],[0, 2, 5],[1, 0, 2],[1, 1, 0],[1, 2, 7],[2, 0, 11],[2, 1, 3],[2, 2, 17], [3, 0, 5],[3, 1, 4],[3, 2, 12],[4, 0, 7],[4, 1, 2],[4, 2, 0],[5, 0, 17],[5, 1, 11],[5, 2, 3], [6, 0, 12],[6, 1, 5],[6, 2, 4],[7, 0, 0],[7, 1, 7],[7, 2, 2],[8, 0, 3],[8, 1, 17],[8, 2, 11] | [9, 3, 18] |

| | | |
|---|---|---|
| **23** | [0, 3, 7],[0, 4, 5],[0, 6, 10],[0, 7, 2],[0, 8, 6],[0, 11, 1],[0, 13, 0], [0, 14, 8],[0, 15, 9],[0, 20, 4],[1, 0, 2],[1, 1, 6],[1, 4, 1],[1, 6, 0],[1, 7, 8], [1, 8, 9],[1, 13, 4],[1, 18, 7],[1, 19, 5],[1, 21, 10],[2, 0, 8],[2, 1, 9],[2, 6, 4], [2, 11, 7],[2, 12, 5],[2, 14, 10],[2, 15, 2],[2, 16, 6],[2, 19, 1],[2, 21, 0],[3, 4, 7], [3, 5, 5],[3, 7, 10],[3, 8, 2],[3, 9, 6],[3, 12, 1],[3, 14, 0],[3, 15, 8],[3, 16, 9], [3, 21, 4],[4, 0, 10],[4, 1, 2],[4, 2, 6],[4, 5, 1],[4, 7, 0],[4, 8, 8],[4, 9, 9], [4, 14, 4],[4, 19, 7],[4, 20, 5],[5, 0, 0],[5, 1, 8],[5, 2, 9],[5, 7, 4],[5, 12, 7], [5, 13, 5],[5, 15, 10],[5, 16, 2],[5, 17, 6],[5, 20, 1],[6, 0, 4], [6, 5, 7],[6, 6, 5],[6, 8, 10],[6, 9, 2],[6, 10, 6],[6, 13, 1],[6, 15, 0],[6, 16, 8], [6, 17, 9],[7, 1, 10],[7, 2, 2],[7, 3, 6],[7, 6, 1],[7, 8, 0],[7, 9, 8],[7, 10, 9], [7, 15, 4],[7, 20, 7],[7, 21, 5],[8, 1, 0],[8, 2, 8],[8, 3, 9],[8, 8, 4],[8, 13, 7], [8, 14, 5],[8, 16, 10],[8, 17, 2],[8, 18, 6],[8, 21, 1],[9, 1, 4],[9, 6, 7],[9, 7, 5], [9, 9, 10],[9, 10, 2],[9, 11, 6],[9, 14, 1],[9, 16, 0],[9, 17, 8],[9, 18, 9],[10, 0, 5], [10, 2, 10],[10, 3, 2],[10, 4, 6],[10, 7, 1],[10, 9, 0],[10, 10, 8],[10, 11, 9],[10, 16, 4], [10, 21, 7],[11, 0, 1],[11, 2, 0],[11, 3, 8],[11, 4, 9],[11, 9, 4],[11, 14, 7],[11, 15, 5], [11, 17, 10],[11, 18, 2],[11, 19, 6],[12, 2, 4],[12, 7, 7],[12, 8, 5],[12, 10, 10],[12, 11, 2], [12, 12, 6],[12, 15, 1],[12, 17, 0],[12, 18, 8],[12, 19, 9],[13, 0, 7],[13, 1, 5],[13, 3, 10], [13, 4, 2],[13, 5, 6],[13, 8, 1],[13, 10, 0],[13, 11, 8],[13, 12, 9],[13, 17, 4],[14, 1, 1], [14, 3, 0],[14, 4, 8],[14, 5, 9],[14, 10, 4],[14, 15, 7],[14, 16, 5],[14, 18, 10],[14, 19, 2], [14, 20, 6],[15, 3, 4],[15, 8, 7],[15, 9, 5],[15, 11, 10],[15, 12, 2],[15, 13, 6],[15, 16, 1], [15, 18, 0],[15, 19, 8],[15, 20, 9],[16, 1, 7],[16, 2, 5],[16, 4, 10],[16, 5, 2],[16, 6, 6], [16, 9, 1],[16, 11, 0],[16, 12, 8],[16, 13, 9],[16, 18, 4],[17, 2, 1],[17, 4, 0],[17, 5, 8], [17, 6, 9],[17, 11, 4],[17, 16, 7],[17, 17, 5],[17, 19, 10],[17, 20, 2],[17, 21, 6],[18, 4, 4], [18, 9, 7],[18, 10, 5],[18, 12, 10],[18, 13, 2],[18, 14, 6],[18, 17, 1],[18, 19, 0],[18, 20, 8], [18, 21, 9],[19, 2, 7],[19, 3, 5],[19, 5, 10],19, 6, 2],[19, 7, 6],[19, 10, 1],[19, 12, 0], [19, 13, 8],[19, 14, 9],[19, 19, 4],[20, 0, 6],[20, 3, 1],[20, 5, 0],[20, 6, 8],[20, 7, 9], [20, 12, 4],[20, 17, 7],[20, 18, 5],[20, 20, 10],[20, 21, 2],[21, 0, 9],[21, 5, 4],[21, 10, 7], [21, 11, 5],[21, 13, 10],[21, 14, 2],[21, 15, 6],[21, 18, 1],[21, 20, 0],[21, 21, 8] | [22, 22, 11] |
| **29** | [0, 0, 10],[0, 1, 5],[0, 2, 24],[0, 3, 14], [0, 4, 3],[0, 5, 16],[1, 0, 2],[1, 1, 27],[1, 2, 21],[1, 3, 23],[1, 4, 1],[1, 5, 15], [1, 6, 26],[2, 1, 10],[2, 2, 5],[2, 3, 24],[2, 4, 14],[2, 5, 3],[2, 6, 16],[3, 0, 26], [3, 1, 2],[3, 2, 27],[3, 3, 21],[3, 4, 23],[3, 5, 1],[3, 6, 15],[4, 0, 16],[4, 2, 10], [4, 3, 5],[4, 4, 24],[4, 5, 14],[4, 6, 3],[5, 0, 15],[5, 1, 26],[5, 2, 2],[5, 3, 27], [5, 4, 21],[5, 5, 23],[5, 6, 1],[6, 0, 3],[6, 1, 16],[6, 3, 10],[6, 4, 5],[6, 5, 24], [6, 6, 14],[7, 0, 1],[7, 1, 15],[7, 2, 26],[7, 3, 2],[7, 4, 27],[7, 5, 21],[7, 6, 23], [8, 0, 14],[8, 1, 3],[8, 2, 16],[8, 4, 10],[8, 5, 5],[8, 6, 24],[9, 0, 23],[9, 1, 1] [9, 2, 15],[9, 3, 26],[9, 4, 2],[9, 5, 27],[9, 6, 21],[10, 0, 24],[10, 1, 14],[10, 2, 3], [10, 3, 16],[10, 5, 10],[10, 6, 5],[11, 0, 21],[11, 1, 23],[11, 2, 1],[11, 3, 15],[11, 4, 26], [11, 5, 2],[11, 6, 27],[12, 0, 5],[12, 1, 24],[12, 2, 14],[12, 3, 3],[12, 4, 16],[12, 6, 10], [13, 0, 27],[13, 1, 21],[13, 2, 23],[13, 3, 1],[13, 4, 15],[13, 5, 26],[13, 6, 2] | [14, 7, 28] |
| **31** | [0, 0, 20],[0, 1, 23], [0, 2, 17],[0, 3, 25],[0, 4, 26],[0, 5, 2], [0, 6, 12],[0, 7, 0],[0, 8, 22],[0, 9, 19], [0, 10, 9],[0, 11, 13],[0, 12, 8],[0, 13, 27], [0, 14, 11],[1, 0, 2],[1, 1, 12],[1, 2, 0], [1, 3, 22],[1, 4, 19],[1, 5, 9],[1, 6, 13], [1, 7, 8],[1, 8, 27],[1, 9, 11],[1, 10, 20], [1, 11, 23],[1, 12, 17],[1, 13, 25],[1, 14, 26], [2, 0, 9],[2, 1, 13],[2, 2, 8],[2, 3, 27], [2, 4, 11],[2, 5, 20],[2, 6, 23],[2, 7, 17], [2, 8, 25],[2, 9, 26],[2, 10, 2],[2, 11, 12], [2, 12, 0],[2, 13, 22],[2, 14, 19] | [3, 15, 30] |

**Tabela B.1:** *Soluções módulo $m$ para $5^a 7^b - 3^c = 4$.*