Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Biológicas
Mestrado Profissional em Educação Matemática em Rede Nacional

Dissertação

A Equação de Pitágoras Módulo Primo

Denise Ramos da Silva

Ouro Preto
2021

UFOP

2021
Denise Ramos da Silva
DEMAT/UFOP

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

DENISE RAMOS DA SILVA

ORIENTADOR:
SÁVIO RIBAS

A EQUAÇÃO DE PITÁGORAS MÓDULO PRIMO

OURO PRETO - MG
FEVEREIRO - 2021

DENISE RAMOS DA SILVA

A EQUAÇÃO DE PITÁGORAS MÓDULO PRIMO

Dissertação de mestrado apresentada como parte dos requisitos para obtenção do título de Mestre pelo programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática do Instituto de Ciências Exatas e Biológicas da Universidade Federal de Ouro Preto.

Orientador: Sávio Ribas.

OURO PRETO - MG
FEVEREIRO - 2021

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

S586e Silva, Denise Ramos da .
A equação de Pitágoras módulo primo . [manuscrito] / Denise Ramos da Silva. - 2021.
25 f.

Orientador: Prof. Dr. Sávio Ribas.
Dissertação (Mestrado Profissional). Universidade Federal de Ouro Preto. Departamento de Matemática. Programa de Pós-Graduação em Matemática.
Área de Concentração: Matemática com Oferta Nacional.

1. Fermat, Teorema de. 2. Pitágoras, Teorema de. 3. Legendre, A. M. (Adrien Marie), 1752-1833 - Eléments de géométrie. 4. Equações. I. Ribas, Sávio. II. Universidade Federal de Ouro Preto. III. Título.

CDU 510:374

Bibliotecário(a) Responsável: Celina Brasil Luiz - CRB6-1589

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
PROGRAMA DE POS-GRADUACAO EM MATEMATICA EM REDE NACIONAL

FOLHA DE APROVAÇÃO

Denise Ramos Silva

A equação de Pitágoras módulo primo

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática Em Rede Nacional da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Mestre em em Matemática

Aprovada em 01 de fevereiro de 2021

Membros da banca

Prof. Dr. Sávio Ribas - Orientador(a) (Universidade Federal de Ouro Preto)
Prof. Dr. Lucas da Silva Reis - (Universidade Federal de Minas Gerais)
Prof. Dr. Edney Augusto Jesus de Oliveira - (Universidade Federal de Ouro Preto)

Sávio Ribas, orientador do trabalho, aprovou a versão final e autorizou seu depósito no Repositório Institucional da UFOP em 10/03/2021

Documento assinado eletronicamente por **Savio Ribas**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 10/03/2021, às 15:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0129869** e o código CRC **AFDB6B00**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.000900/2021-87 SEI nº 0129869

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: - www.ufop.br

Agradecimentos

À Deus, pela vida.
Ao meu marido Leandro Gaspar, que sempre esteve ao meu lado com muito amor, apoio e carinho em todos os momentos dessa dissertação.
À minha filha Maria Rita, que me faz ter forças para sempre lutar pelos meus sonhos.
Aos meus pais, que sempre me incentivaram e me apoiaram aos estudos.
À toda minha família e amigos, pelo incentivo constante, em especial à minha avó Dely.
Aos professores do PROFMAT-UFOP, em especial aos professores: Dr. Edney, Dr. Juliano.
Ao meu orientador professor Dr. Sávio Ribas, pela enorme ajuda, paciência e dedicação.

Resumo

As triplas de números inteiros positivos (x, y, z) que satisfazem a equação de Pitágoras

$$x^2 + y^2 = z^2$$

são chamadas de triplas pitagóricas. Por outro lado, para $n \geq 3$, a equação

$$x^n + y^n = z^n$$

é conhecida como equação de Fermat. Nessa dissertação, vamos descrever todas as triplas pitagóricas e mostrar que a equação de Fermat com $n = 4$ não tem solução. Contudo, o objetivo principal desse trabalho é calcular o número de soluções da equação de Pitágoras módulo um primo p, isto é,

$$x^2 + y^2 \equiv z^2 \pmod{p}.$$

Vamos provar que, embora tomando caminhos distintos para os casos $p = 2, p \equiv 1 \pmod 4$ e $p \equiv 3 \pmod 4$, o número de soluções é sempre p^2. O principal argumento usado é o símbolo de Legendre. Para isso, vamos obter diversas reduções que simplificam o problema. Vamos também discutir alguns problemas relacionados e mostrar como nossa solução pode ser generalizada.

Palavras-chave: Equação de Pitágoras, triplas pitagóricas, equação de Fermat, redução módulo primo, símbolo de Legendre, soma de caracteres.

Abstract

The triples of positive integers (x, y, z) that satisfy the Pythagoras' equation

$$x^2 + y^2 = z^2$$

are called Pythagorean triples. On the other hand, for $n \geq 3$, the equation

$$x^n + y^n = z^n$$

is known as Fermat's equation. In this master thesis, we will describe all Pythagorean triples and show that Fermat's equation with $n = 4$ has no solution. However, the main goal of this work is to calculate the number of solutions of Pythagoras' equation modulo a prime number p, that is

$$x^2 + y^2 \equiv z^2 \pmod{p}.$$

We will show that, although taking distinct ways for the cases $p = 2$, $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, the number of solutions is always p^2. The main argument used is the Legendre symbol. For this, we will obtain several reductions that simplify the problem. We will also discuss some related problems and show how our solution can be generalized.

Keywords: Pythagoras' equation, Pythagorean triples, Fermat's equation, reduction modulo prime, Legendre symbol, character sum.

Sumário

Capítulo 1

Introdução

O teorema de Pitágoras leva o nome do grego Pitágoras (570 a.C. – 495 a.C.), que foi um matemático e filósofo grego. A descoberta e a demonstração desse teorema é creditada à Pitágoras, embora na história encontramos relatos que os matemáticos egípcios e babilônios já o conheciam (ver, por exemplo, [6, Seção 1.1]).

O teorema de Pitágoras é uma relação matemática entre os comprimentos dos lados de um triângulo retângulo qualquer. Pode ser assim enunciado: Em qualquer triângulo retângulo, o quadrado do comprimento da hipotenusa é igual à soma dos quadrados dos comprimentos dos catetos.

Por definição, a hipotenusa é o lado oposto ao ângulo reto, consequentemente o maior lado, e os catetos são os outros dois lados que o formam. Com isso, podemos equacionar

$$x^2 + y^2 = z^2$$

em que z representa o comprimento da hipotenusa, e x e y representam os comprimentos dos catetos. Os números inteiros x, y, z que satisfazem a equação acima são chamados de triplas pitagóricas.

Um problema similar às triplas pitagóricas é o Último Teorema de Fermat. O Último Teorema de Fermat é um famoso problema matemático conjecturado pelo matemático francês Pierre de Fermat em 1637. Trata-se de um generalização do Teorema de Pitágoras para expoentes maiores que 2 e, em particular, uma generalização das triplas pitagóricas. De fato, Fermat substituiu o expoente 2 da fórmula de Pitágoras por um número natural $n \geq 3$ qualquer e considerou o caso onde x, y, z são números inteiros. O problema proposto por Fermat tem um enunciado simples: Não existem inteiros positivos x, y, z e $n > 2$ tais que $x^n + y^n = z^n$. Vários casos particulares foram obtidos ao longo dos anos (ver, por exemplo, Proposição 7.2 de [4] que prova o caso onde $n > 2$ é um primo tal que $2n + 1$ também é primo, nesse caso n é denominado primo de Sophie Germain. Contudo, a solução completa para esse problema só foi obtida

em 1995 por Andrew Wiles [7] com auxílio do seu estudante Richard Taylor, usando técnicas bastante avançadas de Teoria dos Números.

Nessa dissertação, vamos reduzir a equação de Pitágoras $x^2 + y^2 = z^2$ módulo um primo p e obter o número de soluções distintas para a congruência

$$x^2 + y^2 \equiv z^2 \pmod{p}$$

Vamos provar que, embora tomando caminhos distintos para os casos $p = 2$, $p \equiv 1 \pmod 4$ e $p \equiv 3 \pmod 4$, o número de soluções é sempre p^2. O principal argumento usado é o Símbolo de Legendre.

A ideia de reduzir equações módulo $m > 1$, onde m é um número inteiro, pode ajudar a solucioná-las. Por exemplo, a equação $x^2 + 3y = 8$ não tem solução inteira. De fato, se houvesse, deveríamos ter $x^2 \equiv 2 \pmod 3$, o que é um absurdo pois 2 não é resíduo quadrático módulo 3, ver Definição 3.1.1.

Existem outros tipos de redução, como por exemplo a redução da equação de Fermat ao expoente primo. Seja $n = pm$, onde p é um divisor primo de n. A equação de Fermat é equivalente a $(x^m)^p + (y^m)^p = (z^m)^p$. Assim, se mostrarmos que a equação de Fermat com expoente primo p, $x^p + y^p = z^p$, não tem solução inteira, então ela não terá solução para nenhum expoente múltiplo de p.

1.1 As triplas pitagóricas

As triplas de números inteiros positivos (x, y, z) que satisfazem a equação $x^2 + y^2 = z^2$ são denominadas triplas ou ternas pitagóricas, já que, pelo Teorema de Pitágoras, correspondem aos comprimentos dos lados de um triângulo retângulo de lados inteiros.
Notação: Escrevemos $a \mid b$ se a divide b, ou seja, se existe c inteiro tal que $b = ac$.

Na busca por ternas pitagóricas podemos nos restringir às triplas (x, y, z) em que $\mathrm{mdc}(x, y) = \mathrm{mdc}(x, z) = \mathrm{mdc}(y, z) = 1$, os quais denominamos triplas pitagóricas primitivas. De fato, se um primo p divide $mdc(x, y)$, então $p \mid x$ e $p \mid y$, logo $p \mid x^2+y^2 = z^2$, isto é, $p \mid z$. Logo, $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p})$ também é tripla pitagórica.

Em particular, x e y não podem ser ambos pares. Suponha que x é ímpar. Sabemos que todo natural n pode ser escrito como $2k$ ou $2k + 1$, com k inteiro. Assim, $n^2 = (2k)^2 = 4k^2 \equiv 0 \pmod 4$ ou $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$.

Vamos desenvolver o caso onde $\mathrm{mdc}(x, y) = 1$, para $\mathrm{mdc}(x, z) \neq 1$ e $\mathrm{mdc}(y, z) \neq 1$ é análogo.

Dessa forma, y não pode ser ímpar, pois caso contrário, teremos $z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$, o que é um absurdo, já que todos os quadrados perfeitos são con-

gruentes ou a 0 ou a $1 \pmod 4$.

Portanto, x é ímpar, y é par e z é ímpar. Por outro lado,

$$y^2 = z^2 - x^2 = (z+x)(z-x)$$

e

$$\mathrm{mdc}(z+x, z-x) = \mathrm{mdc}(z+x, z+x-(z-x)) = \mathrm{mdc}(z+x, 2x) = 2,$$

já que x é ímpar, z é ímpar e $z+x$ é par. Assim, $\mathrm{mdc}(\frac{z+x}{2}, \frac{z-x}{2}) = \frac{2}{2} = 1$, ou seja, $\left(\frac{z+x}{2}\right)$ e $\left(\frac{z-x}{2}\right)$ são coprimos.

Temos que

$$\frac{y^2}{4} = \frac{z^2 - x^2}{4} = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

Pelo Teorema Fundamental da Aritmética, cada um desses fatores deve ser o quadrado de um número natural. Dessa forma, existem m e n tais que $\frac{z+x}{2} = m^2$ e $\frac{z-x}{2} = n^2$. Assim,

$$\frac{y^2}{4} = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = m^2n^2 \Rightarrow y^2 = 4m^2n^2 \Rightarrow y = 2mn$$

com $\mathrm{mdc}(m, n) = 1$.

Escrevendo x e z em termos de m e n, temos:

$$z = \frac{z+x}{2} + \frac{z-x}{2} = m^2 + n^2 \Rightarrow z = m^2 + n^2,$$
$$x = \frac{z+x}{2} - \frac{z-x}{2} = m^2 - n^2 \Rightarrow x = m^2 - n^2.$$

Portanto, $x = m^2 - n^2$, $y = 2mn$ e $z = m^2 + n^2$. Acabamos de provar o seguinte:

Teorema 1.1.1. *Se (x, y, z) é uma tripla pitagórica então existem d, m, n naturais tais que $m > n$ e $(x, y, z) = ((m^2 - n^2)d, 2mnd, (m^2 + n^2)d)$ ou $(2dmn, (m^2 - n^2)d, (m^2 + n^2)d)$. No caso em que $d = 1$, $\mathrm{mdc}(m, n) = 1$ e m, n têm paridades distintas, obtemos as triplas pitagóricas primitivas.*

Exemplo 1.1.2. *Tomando $m = 11, n = 6, d = 1$, temos que $(x, y, z) = (85, 132, 157)$ é uma tripla pitagórica primitiva. Com isso, $(85d, 132d, 157d)$ é uma tripla pitagórica para todo $d \geq 1$.*

1.2 O caso $n = 4$ do Último Teorema de Fermat

Nesta seção vamos provar que o caso $n = 4$ da equação de Fermat não tem solução. Para isso, vamos utilizar uma técnica chamada Descida de Fermat, que consiste em su-

por que exista uma solução (a, b, c) com $c > 0$ mínimo (isso é possível pelo Princípio da Boa Ordenação), e encontrar outra solução ainda menor. Isso nos levará a um absurdo.

Para isso, consideremos que a equação $x^4 + y^4 = z^2$ possua solução inteira positiva não trivial (x, y, z), ou seja, com $x > 0, y > 0, x > 0$. Notemos que essa equação é mais geral que a equação $x^4 + y^4 = w^4$, uma vez que $z = w^2$ é um quadrado perfeito.

Dessa forma existe uma solução (a, b, c), com c mínimo. Sabemos que a e b são primos entre si, ou seja, $\text{mdc}(a, b) = 1$. De fato, se $d = \text{mdc}(a, b) > 1$ então $d \mid a$ e $d \mid b$. Daí, $d^4 \mid a^4$ e $d^4 \mid b^4$. Logo, $d^4 \mid a^4 + b^4 = c^2$ e então $d^2 \mid c$.

Assim, $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2}\right)$ seria uma solução para a equação com $\frac{c}{d^2} < c$, contradizendo a minimalidade de c já que $\frac{a}{d}$, $\frac{b}{d}$, $\frac{c}{d^2}$ são inteiros.

Como (a, b, c) é uma solução de $x^4 + y^4 = z^2$ então

$$a^4 + b^4 = c^2 = (a^2)^2 + (b^2)^2 = c^2.$$

Daí, (a^2, b^2, c) é uma tripla pitagórica primitiva. Assim, a^2 e b^2 tem paridades distintas e c é ímpar, de acordo com o que demonstramos na Seção 1.1. Logo,

$$a^2 = m^2 - n^2, \quad b^2 = 2mn, \quad c = m^2 + n^2$$

para certos inteiros positivos m e n.

Como $a^2 = m^2 - n^2$ temos $a^2 + n^2 = m^2$, então (a, n, m) é uma tripla pitagórica primitiva. Como $b^2 = 2mn$ então b^2 é par, logo a é ímpar, e então m é ímpar e n é par. Podemos observar que b^2 é um quadrado perfeito e $\text{mdc}(2n, m) = 1$, já que (a, n, m) é uma tripla pitagórica primitiva. Com isso $2n$ e m são quadrados perfeitos, ou seja, existem inteiros positivos u e v tais que $2n = 4u^2$ e $m = v^2$. Por outro lado, dado que $a^2 + n^2 = m^2$, então, pela Seção 1.1, existem i e j inteiros positivos, primos entre si, tais que

$$a = i^2 - j^2, \quad n = 2ij \quad \text{e} \quad m = i^2 + j^2.$$

Logo, $u^2 = \frac{n}{2} = ij$. Conclui-se que i e j são quadrados perfeitos. Dessa forma, existem r e s tais que $i = r^2$ e $j = s^2$. Já que, $m = i^2 + j^2$, $i = r^2$, $j = s^2$ e $m = v^2$, temos que

$$v^2 = m = i^2 + j^2 = (r^2)^2 + (s^2)^2 = r^4 + s^4.$$

Portanto, a tripla r, s, v é outra solução de $x^4 + y^4 = z^2$. Porém,

$$v \leq v^2 = m \leq m^2 < m^2 + n^2 = c,$$

com $v \neq 0$, já que $m \neq 0$. Absurdo, já que c é mínimo! Logo, $x^4 + y^4 = z^2$ não tem

solução inteira positiva.

Acabamos de provar o seguinte:

Teorema 1.2.1. *A equação $x^4 + y^4 = z^2$ não tem solução para x, y, z inteiros positivos.*

Como consequência, tomando z como um quadrado perfeito, segue que a equação de Fermat para $n = 4$ não tem solução inteira positiva.

Corolário 1.2.2. *A equação $x^4 + y^4 = z^4$ não tem solução para x, y, z inteiros positivos.*

Capítulo 2

Redução módulo primo

Nesse capítulo, vamos estudar os casos triviais da equação de Pitágoras módulo um primo p, a saber, o caso $p = 2$ e o caso onde z é múltiplo de p. Mas antes, vamos precisar de alguns resultados algébricos sobre as estruturas de anéis dos inteiros módulo n, corpos e grupos.

2.1 Congruências

Definição 2.1.1. *Sejam $a, b, n \in \mathbb{Z}$, com $n \geq 2$. Dizemos que a é congruente a b módulo n, e escrevemos*

$$a \equiv b \pmod{n},$$

se $n \mid a - b$, ou seja, se a e b deixam o mesmo resto na divisão de n. Por exemplo, temos que $17 \equiv 3 \pmod 7$ e $10 \equiv -5 \pmod 3$.

Proposição 2.1.2. *Seja $n \geq 2$ um inteiro. Para quaisquer $a, b, c, d \in \mathbb{Z}$, temos:*

1. *Reflexividade: $a \equiv a \pmod n$;*
2. *Simetria: Se $a \equiv b \pmod n$ então $b \equiv a \pmod n$;*
3. *Transitividade: Se $a \equiv b \pmod n$ e $b \equiv c \pmod n$ então $a \equiv c \pmod n$;*
4. *Compatibilidade com a soma e a diferença: Podemos somar e subtrair "membro a membro":*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{n} \\ a - c \equiv d - d \pmod{n}. \end{cases}$$

Em particular, se $a \equiv b \pmod n$ então $ka \equiv kb \pmod n$ para todo $k \in \mathbb{Z}$.

5. *Compatibilidade com o produto: Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Rightarrow ac \equiv bd \pmod{n}.$$

Em particular, se $a \equiv b \pmod{n}$ *então* $a^k \equiv b^k \pmod{n}$ *para todo* $k \in \mathbb{N}$.

6. *Cancelamento: Se* $\mathrm{mdc}(c, n) = 1$ *então* $ac \equiv bc \pmod{n} \iff a \equiv b \pmod{n}$.

Demonstração. Para o item 1., basta observar que $n \mid a - a = 0$. Em 2., se $n \mid a - b$ então $n \mid -(a - b) \iff n \mid b - a$. Em 3., se $n \mid a - b$ e $n \mid b - c$, então $n \mid (a - b) + (b - c) \iff n \mid a - c$. Em 4., se $n \mid a - b$ e $n \mid c - d$ então $n \mid (a - b) + (c - d) \iff n \mid (a + c) - (b + d)$ e $n \mid (a - b) - (c - d) \iff n \mid (a - c) - (b - d)$. Em 5., se $n \mid a - b$ e $n \mid c - d$ então $n \mid (a - b)c + (c - d)b \iff n \mid ac - bd$. Finalmente, como $\mathrm{mdc}(c, n) = 1$ temos que $n \mid ac - bc \iff n \mid (a - b)c$, logo $n \mid a - b$ uma vez que n e c não possuem fatores primos em comum o que prova 6.

□

2.2 O conjunto dos inteiros módulo n

A Proposição 2.1.2 determina que a relação $\equiv \pmod{n}$ ("ser congruente módulo n") tem um comportamento muito similar à relação de igualdade usual. Ambas relações, "ser congruente módulo n" e "ser igual", representam relações de equivalência em $\mathbb{Z}$. Em geral, uma relação $\sim$ sobre um conjunto A é dita relação de equivalência se possuir as seguintes propriedades:

1. Reflexiva: $x \sim x$ para todo $x \in A$;
2. Simétrica: $x \sim y \iff y \sim x$;
3. Transitiva: $x \sim y$ e $y \sim z \Rightarrow x \sim z$.

Exibir uma relação de equivalência em A é o mesmo que "dividir" (ou particionar) o conjunto A em subconjuntos não vazios A_λ, $\lambda \in \Lambda$ (conjunto de índices), dois a dois disjuntos, cuja união é A. Podemos definir uma relação de equivalência $\sim$ dizendo que $x \sim y$ se e somente se x e y pertencem a um mesmo A_λ. Reciprocamente, se $\sim$ é uma relação de equivalência, dado um elemento $x \in A$ podemos definir a classe de equivalência $\bar{x}$ de x como o conjunto de todos os elementos equivalentes a x:

$$\bar{x} = \{y \in A; y \sim x\}.$$

Vamos observar que, ou $\bar{x} \cap \bar{y} = \varnothing$ (no caso em que $x \nsim y$), ou $\bar{x} = \bar{y}$ (no caso em que $x \sim y$). Com isso, as distintas classes de equivalência $\bar{x}$ formam subconjuntos disjuntos de A. O conjunto $\{\bar{x} \mid x \in A\}$ das classes de equivalência de $\sim$ é chamado de quociente de A por $\sim$ e é denotado por $A/\sim$. Intuitivamente, tratamos os elementos equivalentes (isto é, elementos que pertencem à mesma classe de $A/\sim$) como elementos iguais. Aplicando-se esta construção geral ao caso de Congruências, o quociente de $\mathbb{Z}$ pela relação $\equiv \pmod{n}$ é chamado de anel de inteiros módulo n e será denotado por $\mathbb{Z}_n$. Pelos itens 1., 2. e 3. da Proposição 2.1.2, temos que a relação $\equiv \pmod{n}$ é uma relação de equivalência. Por exemplo, para $n = 2$, temos que $\mathbb{Z}_2$ possui apenas dois elementos, $\bar{0}$ (que equivale a todos os números pares) e $\bar{1}$ (que equivale a todos os números ímpares). Quando definimos a classe $\bar{a}$ de $\mathbb{Z}_n$, estamos tratando todos os inteiros que deixam resto a na divisão por n como equivalentes. Segue que:

$\bar{a} = \overline{a'} \iff a \equiv a' \pmod{n} \iff a$ e a' deixam o mesmo resto na divisão por n.

Pela divisão euclidiana, qualquer inteiro a é congruente a único inteiro a' com $0 \leq a' < n$, logo podemos reescrever:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}.$$

Os itens 4. e 5. da da Proposição 2.1.2 implicam que que as operações de soma, diferença e produto são compatíveis com relação de congruência. Em geral, definimos:

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} - \bar{b} = \overline{a-b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

e essa definição faz sentido pelos itens 4. e 5. da Proposição 2.1.2. Por exemplo, em $\mathbb{Z}_6$, temos as seguintes tabelas de soma e produto.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

2.3 O corpo $\mathbb{Z}_p$

Definição 2.3.1. *Um conjunto A munido de duas operações $(+, \cdot)$ é um anel se satisfaz as seguintes propriedades: para todos $a, b, c \in A$ temos:*

1. *Associatividade aditiva:* $(a+b)+c = a+(b+c)$;
2. *Comutatividade aditiva:* $a+b = b+a$;
3. *Existência de zero:* $a+0 = a$;
4. *Existência de simétrico aditivo:* $a+(-a) = 0$;
5. *Associatividade multiplicativa:* $(a\cdot b)\cdot c = a\cdot(b\cdot c)$;
6. *Existência de unidade:* $a\cdot 1 = a$;
7. *Distributividade:* $a\cdot(b+c) = a\cdot b + a\cdot c$.

Se, além disso, valer a propriedade da comutatividade multiplicativa, isto é, $a\cdot b = b\cdot a$ *para todos* $a, b \in A$*, dizemos que o anel é comutativo.*

Exemplo 2.3.2. *São exemplos de anéis comutativos: o conjunto dos inteiros* $\mathbb{Z}$*, munido da soma e produto usuais; o conjunto dos racionais* $\mathbb{Q}$*, munido da soma e produto usuais; o conjunto dos reais* $\mathbb{R}$*; e o conjunto dos complexos* $\mathbb{C}$*, também munidos com as operações usuais. Além disso, se* $m \geq 2$ *é um inteiro, então* $\mathbb{Z}_m$ *também é um anel.*

Portanto, $\mathbb{Z}_m$, com as operações de soma e produto vistos na Seção 2.1, é um anel, chamado anel das classes residuais módulo m, ou anel dos inteiros módulo m.

Definição 2.3.3. *Um anel comutativo K munido das operações* $(+,\cdot)$ *é um corpo se todo elemento não nulo tem inverso multiplicativo, isto é, para todo* $a \in K$ *com* $a \neq 0$*, existe* $b \in K$ *tal que* $a\cdot b = 1$*.*

Exemplo 2.3.4. *São exemplos de corpos com as operações de soma e produto usuais:* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$*.*

Teorema 2.3.5 (Bézout)**.** *Sejam* $a, b \in \mathbb{Z}$*. Então existem* $x, y \in \mathbb{Z}$ *com*

$$ax + by = \mathrm{mdc}(a, b).$$

Demonstração. Se $a = b = 0$, tomamos $x = y = 0$. Suponha então que ou $a \neq 0$ ou $b \neq 0$. Defina $I(a,b) = \{ax+by; x, y \in \mathbb{Z}\}$, isto é, $I(a,b)$ é o conjunto das combinações lineares de a e b com coeficientes em $\mathbb{Z}$. Notemos que $I(a,b)$ contém os inteiros $\{a, -a, b, -b\}$ e pelo menos um desses números é positivo. Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a,b)$. Vamos mostrar que d divide todos os elementos de $I(a,b)$. De fato, se $m = ax+by \in I(a,b)$ então, pela divisão euclidiana, existem $q, r \in \mathbb{Z}$ com $m = dq+r$ e $0 \leq r < d$. Temos $r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a,b)$. Pela minimalidade de d, devemos ter $r = 0$, logo $d \mid m$.

Dessa forma, como $a, b \in I(a, b)$ temos $d \mid a$ e $d \mid b$, logo $d \mid mdc(a, b)$. Além disso, se $c \mid a$ e $c \mid b$ então $c \mid ax_0 + by_0 = d$. Tomando $c = mdc(a, b)$ temos que $mdc(a, b) \mid d$. Logo, $d = \text{mdc}(a, b)$ e existem x, y inteiros tais que $ax + by = d$. □

Proposição 2.3.6. *Seja n um inteiro positivo. Então $\mathbb{Z}_n$ é corpo se somente se n é primo.*

Demonstração. ($\Rightarrow$) Suponha que $\mathbb{Z}_m$ é corpo e, por absurdo, suponha que m é composto, digamos $m = m_1 \cdot m_2$ com $1 < m_1, m_2 < m$. Dessa forma, $m_1 \not\equiv 0 \pmod{m}$, logo m_1 possui inverso multiplicativo módulo m. Assim, existe x inteiro tal que $m_1 x \equiv 1 \pmod{m}$. Isso implica que existe y inteiro tal que $m_1 x - my = 1$. Mas, m_1 divide o lado esquerdo da igualdade e não divide o lado direito, o que é um absurdo. Logo, m é primo.

($\Leftarrow$) Suponha que m é primo. Pelo Exemplo 2.3.2, $\mathbb{Z}_m$ é um anel. Vamos mostrar que todo elemento não nulo de $\mathbb{Z}_m$ possui inverso, e isso implica que $\mathbb{Z}_m$ é corpo. Seja $a \not\equiv 0 \pmod{m}$. Como m é primo, temos que $\text{mdc}(a, m) = 1$. Pelo Teorema de Bézout 2.3.5, existem $x, y \in \mathbb{Z}$ tais que $ax + my = 1$, logo $ax \equiv 1 \pmod{m}$, ou seja, x é o inverso de a módulo m. □

Teorema 2.3.7. *Seja K um corpo e seja $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ um polinômio com coeficientes em K na variável x. Se $n \geq 1$ e $a_n \neq 0$ (ou seja, $f(x)$ tem grau n) então $f(x)$ tem no máximo n raízes em K.*

Demonstração. Vamos proceder por indução. Se $f(x)$ não tem raízes então não há o que fazer. Suponha agora que $\alpha \in K$ é raiz. Temos que $f(x) = (x - \alpha)g(x)$, onde $g(x)$ tem grau $n - 1$, coeficientes em K e no máximo $n - 1$ raízes por hipótese. Logo, $f(x)$ tem no máximo n raízes. □

2.4 Grupos

Nessa seção, vamos definir grupos e exibir suas principais propriedades.

Definição 2.4.1. *Seja G um conjunto munido de uma operação $*$. Dizemos que $(G, *)$ é um grupo se satisfaz as seguintes propriedades, onde $a, b, c \in G$.*

1. *G é fechado para sua operação: $a * b \in G$,*
2. *Se $a, b, c \in G$ então $(a * b) * c = a * (b * c)$ (isto é, a operação é associativa),*
3. *Existência do elemento neutro e: $e * a = a * e = a$ (e também é chamado de identidade do grupo),*
4. *Existência do inverso: para todo $a \in G$ existe $b \in G$ tal que $a * b = e$ (b é o inverso de a).*

Quando não restar dúvidas sobre a operação do grupo $(G, *)$, diremos apenas que G é um grupo. Se $a * b = b * a$ para todo $a, b \in G$ então dizemos que G é comutativo ou abeliano.

Se a operação $*$ for uma soma, diremos que o grupo é aditivo e $e = 0$ nesse caso. Se a operação $*$ for um produto, diremos que o grupo é multiplicativo e $e = 1$ nesse caso.

Definição 2.4.2. *Seja $n \geq 2$ um inteiro. Um elemento $a \in \mathbb{Z}_n$ é inversível se existe $b \in \mathbb{Z}_n$ tal que $a \cdot b = 1$. O conjunto $\mathbb{Z}_n^*$ é o conjunto dos elementos inversíveis de $\mathbb{Z}_n$, isto é,*

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n;\ \textit{existe } x \in \mathbb{Z}_n \textit{ tal que } a \cdot x \equiv 1 \pmod{n}\}.$$

Observemos que $ax \equiv 1 \pmod{n}$ é equivalente a $ax + ny = 1$ para algum y inteiro. Pelo Teorema de Bézout 2.3.5, $a \in \mathbb{Z}_n^*$ se, e somente se, $\mathrm{mdc}(a, n) = 1$.

Exemplo 2.4.3. *São exemplos de grupos aditivos: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$. São exemplos de grupos multiplicativos: o conjunto dos racionais positivos $\mathbb{Q}_+^*$, conjunto dos reais positivos $\mathbb{R}_+^*$, o conjunto dos elementos inversíveis módulo n, $\mathbb{Z}_n^*$. Outro exemplo de grupo com uma operação diferente da soma e da multiplicação é o grupo das funções bijetivas munido da operação composição.*

Definição 2.4.4. *Seja G um grupo. A ordem de G, denotada por $|G|$, é a cardinalidade de G. Além disso, G é um grupo finito se $|G| < \infty$; nesse caso, $|G|$ é o número de elementos de G.*

Definição 2.4.5. *Sejam G um grupo finito e $g \in G$. A ordem de g, $ord(g)$, é definida como o menor inteiro positivo n tal que $\underbrace{g * g * g * \cdots * g}_{n \text{ vezes}} = e$.*

Notação: Se G é aditivo então $ng = \underbrace{g + \cdots + g}_{n \text{ vezes}}$. Se G é multiplicativo então $g^n = \underbrace{g \ldots g}_{n \text{ vezes}}$.

Observe que, pelo Princípio da Casa dos Pombos, se G é finito então $ord(g) \leq |G|$ para todo $g \in G$. De fato, considere os $|G|$ elementos: $g, 2g, 3g, \ldots, |G|g$. Se todas essas somas forem distintas então para algum $n \leq |G|$ teremos $ng = e$. Caso contrário, existem $1 \leq i < j \leq |G|$ tais que $ig = jg \Rightarrow (j - i)g = e$. Logo $ord(g) \leq j - i \leq |G|$, teremos $ord(g) \leq |G|$.

Vamos agora relembrar os teoremas de Euler-Fermat e o pequeno teorema de Fermat.

Teorema 2.4.6 (Teorema de Euler-Fermat [1, Teorema 10.5])**.** *Se $a \in \mathbb{Z}_n^*$ então $a^{\varphi(n)} \equiv 1 \pmod{n}$, onde $\varphi(n)$ é função de Euler definida por $\varphi(n) = \#\{1 \leq a \leq n; \mathrm{mdc}(a, n) = 1\}$.*

Corolário 2.4.7 (Pequeno Teorema de Fermat [1, Corolário 10.6])**.** *Se p é primo e $a \not\equiv 0 \pmod{p}$ então $a^{p-1} \equiv 1 \pmod{p}$.*

Definição 2.4.8. *Sejam a e n inteiros positivos primos entre si. Definimos a ordem de a módulo n como o menor inteiro positivo t tal que $a^t \equiv 1 \pmod{n}$, e escrevemos $t = ord_n(a)$.*

Lema 2.4.9. *Sejam m, n inteiros positivos com $n \geq 2$. Se $a^m \equiv 1 \pmod{n}$ então $ord_n(a)$ divide m.*

Demonstração. Se $a \equiv 1 \pmod{n}$ então $ord_n(a) = 1$, que divide m. Senão, seja $a \not\equiv 1 \pmod{n}$ e $t = ord_n(a) > 1$. Pela divisão euclidiana, $m = t \cdot q + r$, onde $0 \leq r < t$. Queremos mostrar que $r = 0$. Se $r \neq 0$ então $1 \equiv a^m = (a^t)^q \cdot a^r = 1^q \cdot a^r \Rightarrow a^r \equiv 1 \pmod{p}$, o que contradiz a minimalidade de t. □

Pelo Teorema 2.4.6 (Euler-Fermat) e pelo Lema 2.4.9, se a e n são primos entre si então $ord_n(a)$ é um divisor de φ.

Definição 2.4.10. *Seja G um grupo. Dizemos que G é cíclico se existe $g \in G$ tal que $\{ng; n \in \mathbb{Z}\} = G$. Nesse caso, dizemos que g é um gerador de G e escrevemos $G = \langle g \rangle$.*

Exemplo 2.4.11. *Nesse exemplo, vamos entender melhor a definição de grupo cíclico e gerador.*

- $(\mathbb{Z}, +) = \langle 1 \rangle$, *pois* $\pm(1 + 1 + \cdots + 1)$ *gera todos os inteiros.*
- $(\mathbb{Z}_n, +) = \langle a \rangle$, *onde* $\text{mdc}(a, n) = 1$, *pois se* $0 \leq m \leq n - 1$ *então a congruência* $\underbrace{a + a + \cdots + a}_{x \text{ vezes}} = xa \equiv m \pmod{n}$ *tem uma única solução módulo* n, *a saber,* $x \equiv ma^{-1} \pmod{n}$.
- $(\mathbb{Z}_6^*, \cdot) = \langle 5 \rangle$, *pois* $5^2 \equiv 1 \pmod{6}$ *e* $\mathbb{Z}_6^* = \{1, 5\}$.
- $(\mathbb{Z}_7^*, \cdot) = \langle 3 \rangle = \langle 5 \rangle$, *pois* $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, $3^2 \equiv 2 \pmod{7}, 3^3 \equiv 6 \pmod{7}, 3^4 \equiv 4 \pmod{7}, 3^5 \equiv 5 \pmod{7}, 3^6 \equiv 1 \pmod{7}$, *e além disso* $5^2 \equiv 4 \pmod{7}, 5^3 \equiv 6 \pmod{7}, 5^4 \equiv 2 \pmod{7}, 5^5 \equiv 3 \pmod{7}, 5^6 \equiv 1 \pmod{7}$.
- $(\mathbb{R}, +)$ *não é cíclico, pois se* $\mathbb{R}$ *fosse gerado por* y, *teríamos* $y \neq 0, \langle y \rangle = \{0\}$, *o que seria absurdo, logo não conseguiríamos obter o número real* $\frac{y}{2}$. *De fato, se* $\frac{y}{2} = ny$, *onde* $n \in \mathbb{Z}$, *então* $n = \frac{1}{2}$, *absurdo.*

Teorema 2.4.12. *Se p é primo então $(\mathbb{Z}_p^*, \cdot)$ é cíclico.*

Demonstração. Seja $p - 1 = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ a fatoração de $p - 1$ em primos. Como $\mathbb{Z}_p$ é corpo, o polinômio $x^{(p-1)/p_i} - 1$ tem no máximo $(p-1)/p_i$ raízes em $\mathbb{Z}_p$ pelo Teorema 2.3.7. Como 0 não é raiz, temos que as raízes estão em $\mathbb{Z}_p^*$. Escolhemos a_i que não é raiz $x^{(p-1)/p_i} - 1$. Defina $b_i \equiv a_i^{p_i^{\alpha_i}} \pmod{p}$. Como $b_i^{p_i^{\alpha_i}} \equiv a_i^{p-1} \equiv 1 \pmod{p}$ (pelo Pequeno Teorema de Fermat), a ordem de b_i é p_i^{ℓ} com $1 \leq \ell \leq \alpha_i$ (pelo Lema 2.4.9). Mas $1 \equiv b_i^{p_i^{\ell}} \equiv a_i^{(p-1)/p_i^{\alpha_i - \ell}} \pmod{p}$ vale apenas se $\ell = \alpha_i$, pois $a_i^{(p-1)/p_i} \not\equiv 1 \pmod{p}$. Seja $t \mid p - 1$ com $t < p - 1$ então t divide $(p-1)/p_i$ para algum $1 \leq i \leq m$. Se $b \equiv b_1 \dots b_m \pmod{p}$ então temos:

$$b^{(p-1)/p_i} \equiv b_1^{(p-1)/p_i} \cdots b_i^{(p-1)/p_i} \cdots b_m^{(p-1)/p_i} \equiv 1 \cdots b_i^{(p-1)/p_i} \cdots 1 \equiv b_i^{(p-1)/p_i} \not\equiv 1 \pmod{p},$$

o que é um absurdo. Logo, $t = p-1$ e $\mathbb{Z}_p^* = \langle b \rangle$. □

2.5 Casos triviais da equação de Pitágoras em $\mathbb{Z}_p$

Nessa seção, vamos estudar alguns casos particulares da Equação de Pitágoras, a saber, os casos $p = 2$ e $p \mid z$.

(i) Caso $p = 2$. Temos então que $x, y, z \in \mathbb{Z}_2$. Pelo Pequeno Teorema de Fermat, $a^2 \equiv a \pmod 2$, logo a equação $x^2+y^2 \equiv z^2 \pmod p$ equivale a $x+y \equiv z \pmod 2$. Dessa forma, temos 4 soluções: $(0,0,0)$, $(1,0,1)$, $(0,1,1)$ e $(1,1,0)$.

A partir de agora, vamos considerar p primo ímpar.

(ii) Caso $p \mid z$. A equação $x^2 + y^2 \equiv z^2 \pmod p$ equivale a $x^2 + y^2 \equiv 0 \pmod p$.

Se $p \mid x$ então $p \mid y$, logo temos a solução trivial módulo p: $(0,0,0)$.

Se $p \nmid x$ então $p \nmid y$, logo y é inversível módulo p. Com isso, multiplicando por y^{-2}, a equação de Pitágoras equivale a

$$(xy^{-1})^2 + 1 \equiv 0 \pmod p \iff (xy^{-1})^2 \equiv -1 \pmod p.$$

Com isso, basta encontrar o número de soluções de $a^2 \equiv -1 \pmod p$. Isso será feito na Seção 3.1. Veremos que o número de soluções para $a^2 \equiv -1 \pmod p$ é 0 ou 2, a depender do resto da divisão de p por 4. Quando tiver duas soluções para a, basta voltar para a mudança de variáveis: $xy^{-1} \equiv a \pmod p$. Fixado $y \not\equiv 0 \pmod p$, existe único $x \equiv ay \pmod p$. Logo, o número de soluções não triviais para $x^2 + y^2 \equiv 0 \pmod p$ é 0 ou $2(p-1)$.

A partir de agora, vamos supor que $p \nmid z$.

Estamos supondo $p > 2$ primo e $p \nmid z$. Assim, z é inversível módulo p. Multiplicando pelo seu inverno, temos que a equação de Pitágoras equivale a

$$(xz^{-1})^2 + (xz^{-1})^2 \equiv 1 \pmod p \iff \tilde{x}^2 + \tilde{y}^2 \equiv 1 \pmod p, \tag{2.1}$$

onde fizemos a mudança de variáveis $\tilde{x} = xz^{-1}$ e $\tilde{y} = yz^{-1}$.

No próximo capítulo, vamos estudar a equação de Pitágoras excluíndo os casos triviais feitos acima.

Capítulo 3

A equação de Pitágoras em $\mathbb{Z}_p$

Os casos $p = 2$ e $p \mid z$ já foram tratados no capítulo anterior. Assim, nesse capítulo, por equação de Pitágoras vamos considerar a Equação (2.1), ou seja,

$$x^2 + y^2 \equiv 1 \pmod{p},$$

onde p é primo ímpar. Nosso objetivo é encontrar o número de soluções dessa equação. Para isso, vamos precisar do Símbolo de Legendre.

3.1 Símbolo de Legendre

Definição 3.1.1. *Seja $a \in \mathbb{Z}_p^*$. Dizemos que a é resíduo quadrático módulo p se a equação $x^2 \equiv a \pmod{p}$ tem solução $x \in \mathbb{Z}_p$. Caso contrário, dizemos que a não é resíduo quadrático módulo p.*

Definição 3.1.2. *Sejam $a, p \in \mathbb{Z}$ com p primo. Definimos o Símbolo de Legendre por*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \mid a, \\ 1 & \text{se } a \text{ é resíduo quadrático módulo } p, \\ -1 & \text{se } a \text{ não é resíduo quadrático módulo } p. \end{cases}$$

Proposição 3.1.3. *Seja p um primo e a um inteiro. São válidos:*

(i) *Se $a \equiv b \pmod{p}$ tem-se que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) *Se p é primo ímpar então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

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

(iv) *Se* $p \nmid a$ *então* $\left(\frac{a^2}{p}\right) = 1$. *Em particular,* $\left(\frac{1}{p}\right) = 1$.

(v) *Se* a *é ímpar então* $\left(\frac{a}{2}\right) = 1$.

(vi) *Se* p *é ímpar então* $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$.

Demonstração. *(i)* Suponhamos que $a \equiv b \pmod p$. Nesse caso, a congruência quadrática $X^2 \equiv a \pmod p$ tem solução, se somente se, a congruência quadrática $X^2 \equiv b \pmod p$ tem solução, o que equivale a dizer que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) Se $a \equiv 0 \pmod p$ então não há o que provar. Suponhamos $a \not\equiv 0 \pmod p$. Pelo Pequeno Teorema de Fermat, temos que $a^{p-1} \equiv 1 \pmod p$. Daí, segue que p divide $a^{(p-1)/2} + 1$ ou $a^{(p-1)/2} - 1$, ou seja,

$$a^{(p-1)/2} \equiv \pm 1 \pmod p.$$

Vamos mostrar que $a^{(p-1)/2} \equiv 1 \pmod p$ se e somente se a é um resíduo quadrático módulo p. Se a é um quadrado módulo p, digamos $a \equiv b^2 \pmod p$, então

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod p.$$

Dessa forma, os resíduos quadráticos são raízes do polinômio $f(x) = x^{(p-1)/2} - 1$ em $\mathbb{Z}_p$. Como $\mathbb{Z}_p$ é corpo, esse polinômio tem no máximo $(p-1)/2$ raízes. Mas, de fato, os números $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ são raízes de $f(x)$ pois são quadrados. Resta mostrar todos esses números são diferentes módulo p. Suponha que $r, s \in \{1, 2, \ldots, (p-1)/2\}$ e $r^2 \equiv s^2 \pmod p$. Isso equivale a $r \equiv \pm s \pmod p$. Mas $0 < r + s \leq p - 1$, logo $r \equiv -s \pmod p$ não tem solução. Isso significa que $r \equiv s \pmod p$. Logo, $a^{(p-1)/2} \equiv 1 \pmod p$ se e somente se a é um quadrado módulo p.

(iii) Observamos que, do item *(ii), nós temos que* $\left(\frac{a \cdot b}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$.

(iv) *Do item (ii), segue que* $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2 = (\pm 1)^2 = 1$.

(v) *Do item (i),* $\left(\frac{a}{2}\right) = \left(\frac{1}{2}\right) = 1$.

(vi) *Pelo item (ii),* $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p$, *mas ambos os termos são iguais a* 1 *ou* -1, *logo vale a igualdade.*

□

Corolário 3.1.4. *Seja p um primo ímpar. Então -1 é resíduo quadrático módulo p se e somente se $p \equiv 1 \pmod 4$.*

Demonstração. Observe que, se p é ímpar, então, pelo item (ii) da Proposição 3.1.3, -1 é resíduo quadrático módulo p se e somente se $(p-1)/2$ é par, ou seja, existe k inteiro tal que $(p-1)/2 = 2k$, o que equivale a $p = 4k+1$. □

Corolário 3.1.5. *A equação $a^2 \equiv -1 \pmod p$ tem 0 soluções se $p \equiv 3 \pmod 4$ e tem 2 soluções se $p \equiv 1 \pmod 4$.*

Demonstração. Se $p \equiv 3 \pmod 4$ então o corolário anterior nos garante que $a^2 \equiv -1 \pmod p$ não tem solução. Se $p \equiv 1 \pmod 4$ então temos pelo menos uma solução. Como $\mathbb{Z}_p$ é corpo, o polinômio x^2+1, de grau 2, tem no máximo duas raízes em $\mathbb{Z}_p$. Se a é solução então $-a$ também é solução, pois $(-a)^2 \equiv a^2 \equiv -1 \pmod p$. Além disso, $a \not\equiv -a \pmod p$, pois caso contrário teríamos que $p \mid 2a$, e como p é ímpar devemos ter $p \mid a$, o que é um absurdo. □

Observação 3.1.6. *Fixado um primo p, notemos que o Símbolo de Legendre é uma função totalmente multiplicativa pela Proposição 3.1.3 (iii). Restrito a $\mathbb{Z}_p^*$, temos que o símbolo toma os valores -1 e 1, e o conjunto $\{-1, 1\}$ com a operação de produto forma um grupo cíclico gerado por -1, ou seja, o conjunto dos símbolos de Legendre módulo p forma um grupo cíclico de ordem 2.*

Agora, vamos enunciar um importante teorema que permite, juntamente com a Proposição 3.1.3, encontrar o valor do símbolo de Legendre $\left(\frac{a}{p}\right)$ para todo a inteiro, onde p é primo. A demonstração pode ser encontrada em [1, Teorema 12.29].

Teorema 3.1.7 (Lei da Reciprocidade Quadrática)**.** *Sejam p, q primos ímpares. São válidos:*

(a) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$;

(b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

A seguir, temos uma aplicação do Teorema anterior.

Exemplo 3.1.8. *Vamos verificar que a equação $X^2 - 41Y = 2020$ não tem solução. Para isso, vamos calcular $\left(\frac{2020}{41}\right)$. Note inicialmente que 41 é um número primo e que*

$$2020 \equiv 11 \pmod{41}.$$

Logo, pela Proposição 3.1.3(i), temos que

$$\left(\frac{2020}{41}\right) = \left(\frac{11}{41}\right).$$

Como 11 *é primo, pela Lei da Reciprocidade Quadrática, temos que*

$$\left(\frac{11}{41}\right)\left(\frac{41}{11}\right) = (-1)^{5\cdot 20} = 1.$$

Como $41 \equiv 8 \pmod{11}$ *segue que,*

$$\left(\frac{11}{41}\right) = \left(\frac{41}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{2^2}{11}\right)\left(\frac{2}{11}\right) = 1 \cdot (-1)^{120/8} = (-1)^{15} = -1.$$

Com isso, provamos que 2020 *não é resíduo quadrático módulo* 41*. Como consequência imediata, temos que a equação diofantina*

$$X^2 - 41Y = 2020$$

não possui soluções inteiras.

3.2 A equação $x^2 \equiv a \pmod{p}$

Vimos, através do Corolário 3.1.5, que a equação $x^2 \equiv -1 \pmod{p}$ possui 0 soluções se $p \equiv 3 \pmod{4}$ e 2 soluções se $p \equiv 1 \pmod{4}$.

Agora, mais geralmente, vamos estudar a equação $x^2 \equiv a \pmod{p}$. Seja $N(x^2 = a)$ o número de soluções da congruência $x^2 \equiv a \pmod{p}$. Notemos que

$$N(x^2 = a) = 1 + \left(\frac{a}{p}\right), \tag{3.1}$$

pois a congruência $x^2 \equiv a \pmod{p}$ tem 0 ou 2 soluções quando $\left(\frac{a}{p}\right) = -1$ ou $\left(\frac{a}{p}\right) = 1$, respectivamente. De fato, quando $\left(\frac{a}{p}\right) = 1$, argumentamos da mesma forma que no Corolário 3.1.5 para mostrar que existem duas soluções.

Observação 3.2.1. *Caso quiséssemos resolver a equação* $x^n \equiv a \pmod{p}$*, nós definiríamos uma função totalmente multiplicativa similar ao símbolo de Legendre. Isso é o que chamamos de caracter (ou caráter) módulo* p *de ordem* n*. Por exemplo, o símbolo de Legendre é um caracter módulo* p *de ordem* 2*. Nesse sentido, a Equação (3.1) viraria uma soma de caracteres com* n *termos. Para saber mais sobre soma de caracteres, veja [2].*

Corolário 3.2.2. *Se p é primo ímpar então existem $\frac{p-1}{2}$ resíduos quadráticos módulo p e $\frac{p-1}{2}$ não-resíduos quadráticos módulo p.*

Demonstração. Fixamos $1 \leq x \leq p-1$. Temos que x^2 é congruente a algum valor a módulo p. Com isso, o número de possibilidades para x é

$$p - 1 = 2\# \left\{ 1 \leq a \leq p-1; \left(\frac{a}{p}\right) = 1 \right\},$$

ou seja, cada par de elementos de $\mathbb{Z}_p^*$ da forma $\{x, p-x\}$ é associado a um elemento x^2 módulo p, que é um resíduo quadrático, logo o número de resíduos quadráticos é $\frac{p-1}{2}$ e o número de não-resíduos quadráticos é $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$. □

Uma prova alternativa para o corolário anterior pode ser dada sabendo que existe um não-resíduo quadrático módulo p como a seguir:

Sejam $S = \sum_{a \in \mathbb{Z}_p^*} \left(\frac{a}{p}\right)$ e $b \in \mathbb{Z}_p^*$ um não-resíduo quadrático módulo p. Temos:

$$-S = \left(\frac{b}{p}\right) S = \sum_{a \in \mathbb{Z}_p^*} \left(\frac{ab}{p}\right) = \sum_{c \in \mathbb{Z}_p^*} \left(\frac{c}{p}\right) = S \Longrightarrow S = 0$$

$$\Longrightarrow \# \left\{ a \in \mathbb{Z}_p^*; \left(\frac{a}{p}\right) = 1 \right\} - \# \left\{ a \in \mathbb{Z}_p^*; \left(\frac{a}{p}\right) = -1 \right\} = 0,$$

donde segue o resultado.

3.3 A equação $x^2 + y^2 \equiv 1 \pmod{p}$

Da mesma forma que na seção anterior, seja $N(x^2 + y^2 = 1)$ o número de soluções da congruência $x^2 + y^2 \equiv 1 \pmod{p}$. Notemos que:

$$\begin{aligned}
N(x^2 + y^2 = 1) &= \sum_{k \in \mathbb{Z}_p} N(x^2 = k) N(y^2 = 1 - k) \\
&= \sum_{k \in \mathbb{Z}_p} \left[1 + \left(\frac{k}{p}\right)\right] \left[1 + \left(\frac{1-k}{p}\right)\right] \\
&= \sum_{k \in \mathbb{Z}_p} \left[1 + \left(\frac{k}{p}\right) + \left(\frac{1-k}{p}\right) + \left(\frac{k(1-k)}{p}\right)\right] \\
&= \sum_{k \in \mathbb{Z}_p} 1 + \sum_{k \in \mathbb{Z}_p} \left(\frac{k}{p}\right) + \sum_{k \in \mathbb{Z}_p} \left(\frac{1-k}{p}\right) + \sum_{k \in \mathbb{Z}_p} \left(\frac{k(1-k)}{p}\right)
\end{aligned}$$

$$
\begin{aligned}
&= p + 0 + 0 + \sum_{k \in \mathbb{Z}_p^*} \left(\frac{(k^2(k^{-1}-1)}{p} \right) \\
&= p + \sum_{k \in \mathbb{Z}_p^*} \left(\frac{(k^{-1}-1)}{p} \right) \\
&= p + \sum_{m \in \mathbb{Z}_p} \left(\frac{m}{p} \right) - \left(\frac{-1}{p} \right) \\
&= p + 0 - \left(\frac{-1}{p} \right) \\
&= p - (-1)^{(p-1)/2},
\end{aligned}
$$

onde na 5ª linha das equações anteriores usamos o Corolário 3.2.2 em que o número de resíduos quadráticos e de não-resíduos quadráticos é igual a $\frac{p-1}{2}$ e na 7ª linha usamos que k^{-1} só não gera o elemento 0 módulo p, ou seja, $k^{-1} - 1$ só não gera o elemento -1 módulo p. Em particular, provamos o seguinte teorema, que é o principal resultado dessa dissertação.

Teorema 3.3.1. *A equação* $x^2 + y^2 \equiv 1 \pmod{p}$ *tem* $p - 1$ *soluções se* $p \equiv 1 \pmod{4}$, *e tem* $p + 1$ *soluções se* $p \equiv 3 \pmod{4}$.

Como corolário imediato, podemos juntar o teorema anterior com a Seção 2.5.

Corolário 3.3.2. *O número de soluções da equação de Pitágoras* $x^2 + y^2 \equiv z^2 \pmod{p}$ *é* p^2.

Demonstração. Vamos dividir em casos:

1. Se $p = 2$, já vimos da Subseção 2.5(i) que o número de soluções é $4 = 2^2$.

2. Se $p \equiv 1 \pmod{4}$, então temos $1 + 2(p-1) = 2p - 1$ soluções triviais. Para as soluções não triviais, fixado $z \in \mathbb{Z}_p^*$, temos $p - 1$ soluções. Logo, o número total de soluções é $1 + 2(p-1) + (p-1)(p-1) = p^2$.

3. Se $p \equiv 3 \pmod{4}$, de maneira análoga ao que fizemos no caso anterior, concluímos que o número de soluções é $1 + 0 + (p+1)(p-1) = p^2$.

□

Para valores de p muito pequenos, a equação $x^2 + y^2 \equiv 1 \pmod{p}$ pode ser facilmente resolvida testando todos os valores.

Exemplo 3.3.3. *Resolver a equação* $x^2 + y^2 \equiv 1 \pmod{p}$ *para* $p \in \{3, 5, 7\}$.

a) Para $p = 3$, *testamos todos os* 9 *pares* $(x, y) = (0,0)$, $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(1,2)$, $(2,0)$, $(2,1)$, $(2,2)$ *e encontramos como soluções* $(x, y) = (0,1)$, $(0,2)$, $(1,0)$ *e* $(2,0)$.

b) Para $p = 5$*, testamos todos os* 25 *pares* $(x, y) = (0, 0)$*,* $(0, 1)$*,* $\ldots$*,* $(0, 4)$*,* $(1, 0)$*,* $(1, 1)$*,* $\ldots$*,* $(1, 4)$*,* $(2, 0)$*,* $\ldots$*,* $(2, 4)$*,* $(3, 0)$*,* $\ldots$*,* $(3, 4)$*,* $(4, 0)$*,* $\ldots$*,* $(4, 4)$ *e encontramos como soluções* $(x, y) = (0, 1)$*,* $(0, 4)$*,* $(1, 0)$ *e* $(4, 0)$*.*

c) Para $p = 7$*, testamos todos os* 49 *pares* $(x, y) \in \mathbb{Z}_7^2$ *e encontramos como soluções* $(0, 1)$*,* $(0, 6)$*,* $(1, 0)$*,* $(6, 0)$*,* $(2, 2)$*,* $(2, 5)$*,* $(5, 2)$ *e* $(5, 5)$*.*

O método que usamos pode ser generalizado para outros tipos de equações diagonais quadráticas com mais termos. Por exemplo:

Teorema 3.3.4. *A equação* $x^2 + y^2 + z^2 \equiv 1 \pmod{p}$ *tem* $p^2 + p$ *soluções se* $p \equiv 1 \pmod{4}$*, e tem* $p^2 - p$ *soluções se* $p \equiv 3 \pmod{4}$*.*

Demonstração. Seja N o número de soluções da congruência $x^2 + y^2 + z^2 \equiv 1 \pmod{p}$. Temos

$$
\begin{aligned}
N &= \sum_{a,b\in\mathbb{Z}_p} N(x^2 = a)N(y^2 = b)N(z^2 = 1 - a - b) \\
&= \sum_{a,b\in\mathbb{Z}_p} \left[1 + \left(\frac{a}{p}\right)\right]\left[1 + \left(\frac{b}{p}\right)\right]\left[1 + \left(\frac{1-a-b}{p}\right)\right] \\
&= \sum_{a,b\in\mathbb{Z}_p} \left[1 + \left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \left(\frac{1-a-b}{p}\right) + \left(\frac{ab}{p}\right) + \left(\frac{a(1-a-b)}{p}\right) + \right. \\
&\quad \left. + \left(\frac{b(1-a-b)}{p}\right) + \left(\frac{ab(1-a-b)}{p}\right)\right] \\
&= p^2 + 0 + 0 + 0 + \sum_{a,b\in\mathbb{Z}_p} \left(\frac{ab}{p}\right) + \sum_{a,b\in\mathbb{Z}_p} \left(\frac{a(1-a-b)}{p}\right) + \sum_{a,b\in\mathbb{Z}_p} \left(\frac{b(1-a-b)}{p}\right) \\
&\quad + \sum_{a,b\in\mathbb{Z}_p} \left(\frac{ab(1-a-b)}{p}\right) \\
&= p^2 + \sum_{a\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{Z}_p} \left(\frac{b}{p}\right) + \sum_{a\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{Z}_p} \left(\frac{1-a-b}{p}\right) + \sum_{b\in\mathbb{Z}} \left(\frac{b}{p}\right) \sum_{a\in\mathbb{Z}_p} \left(\frac{1-a-b}{p}\right) \\
&\quad + \sum_{a\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{Z}} \left(\frac{b(1-a-b)}{p}\right) \\
&= p^2 + 0 + 0 + 0 + \sum_{a\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{Z}_p^*} \left(\frac{b^{-1} - ab^{-1} - 1}{p}\right) \\
&= p^2 + \sum_{a\in\mathbb{Z}_p} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{Z}_p^*} \left(\frac{b^{-1}(1-a) - 1}{p}\right) \\
&= p^2 + \sum_{a\in\mathbb{Z}_p^*} \left(\frac{a}{p}\right) \sum_{b\in\mathbb{Z}_p^*} \left(\frac{b^{-1}(1-a) - 1}{p}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= p^2 + \sum_{\substack{a\in\mathbb{Z}_p^* \\ a\not\equiv 1 \pmod p}} \left(\frac{a}{p}\right) \sum_{\substack{b\in\mathbb{Z}_p^* \\ [b^{-1}(1-a)]\not\equiv 0 \pmod p}} \left(\frac{b^{-1}(1-a)-1}{p}\right) + \sum_{\substack{b\in\mathbb{Z}_p^* \\ a\equiv 1 \pmod p}} \left(\frac{-1}{p}\right) \\
&= p^2 + \sum_{\substack{a\in\mathbb{Z}_p^*, \\ a\not\equiv 1 \pmod p}} \left(\frac{a}{p}\right) \left[\sum_{c\in\mathbb{Z}_p} \left(\frac{c}{p}\right) - \left(\frac{-1}{p}\right)\right] + (p-1)(-1)^{\frac{p-1}{2}} \\
&= p^2 + \sum_{\substack{a\in\mathbb{Z}_p^* \\ a\not\equiv 1 \pmod p}} \left(\frac{a}{p}\right) \cdot (-1)^{\frac{p+1}{2}} + (p-1)(-1)^{\frac{p-1}{2}} \\
&= p^2 + (-1)^{\frac{p+1}{2}} \cdot \left[\sum_{a\in\mathbb{Z}_p^*} \left(\frac{a}{p}\right) - \left(\frac{1}{p}\right)\right] + (p-1)(-1)^{\frac{p-1}{2}} \\
&= p^2 + (-1)^{\frac{p-1}{2}} + p\cdot(-1)^{\frac{p-1}{2}} - (-1)^{\frac{p-1}{2}} \\
&= p^2 + p\cdot(-1)^{\frac{p-1}{2}} \\
&= \begin{cases} p^2+p & \text{se } p \equiv 1 \pmod 4, \\ p^2-p & \text{se } p \equiv 3 \pmod 4. \end{cases}
\end{aligned}
$$

□

Observação 3.3.5. *Pela Observações 3.1.6 e 3.2.1, usando os caracteres módulo p de ordem n, pelo mesmo argumento do Teorema 3.3.1, podemos estudar o número de soluções da equação de Fermat módulo primo:*

$$x^n + y^n \equiv z^n \pmod p.$$

Ainda mais geralmente, podemos com esse argumento estudar o número de soluções de qualquer equação diagonal

$$a_1 x_1^{n_1} + \ldots a_k x_k^{n_k} \equiv b \pmod p,$$

onde podemos supor sem perda de generalidade que n_i divide $p-1$ para todo $1 \leq i \leq k$. De fato, para mostrar que podemos fazer essa suposição, precisamos da seguinte proposição.

Proposição 3.3.6. *Se p é um primo ímpar e a é um inteiro tal que $p \nmid a$, então $x^n \equiv a \pmod p$ tem solução se e somente se $a^{(\frac{p-1}{d})} \equiv 1 \pmod p$, onde $d = mdc(n, p-1)$.*

Demonstração. Seja ζ um gerador de $\mathbb{Z}_p^*$, isto é, $\mathbb{Z}_p^* = \langle\zeta\rangle$ (que existe pelo Teorema 2.4.12). Temos $x \not\equiv 0 \pmod p$. Sejam y e b inteiros tais que $x \equiv \zeta^y \pmod p$ e $a \equiv \zeta^b \pmod p$, de forma que $\zeta^{ny} \equiv \zeta^b \pmod p$. Isso é equivalente a $\zeta^{ny-b} \equiv 1 \pmod p$, ou seja, $ny \equiv b \pmod{p-1}$. Essa última congruência tem solução se e somente se $d = \text{mdc}(n, p-1)$ divide b. Se $d \mid b$ então temos que $a^{\frac{(p-1)}{d}} \equiv \zeta^{\frac{b(p-1)}{d}} \equiv 1 \pmod p$. Por outro lado, se $a^{\frac{(p-1)}{d}} \equiv 1 \pmod p$ então $\zeta^{\frac{b(p-1)}{d}} \equiv 1 \pmod p$, o que implica que $p-1$ divide $\frac{b(p-1)}{d}$, ou seja, $d \mid b$. □

Capítulo 4

Conclusões

Utilizando o símbolo de Legendre e suas propriedades, vimos que se p é primo então a equação $x^2 + y^2 \equiv z^2 \pmod{p}$ tem p^2 soluções, independente da forma de p, isto é, se $p = 2$, se $p \equiv 1 \pmod{4}$ ou se $p \equiv 3 \pmod{4}$. Além disso, vimos que o argumento utilizado é diretamente generalizado para equações de grau 2 com mais termos:

$$x_1^2 + x_2^2 + \cdots + x_k^2 \equiv 1 \pmod{p}.$$

Além disso, podemos generalizar para equações com outros coeficientes, como por exemplo:

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_kx_k^2 \equiv 1 \pmod{p}.$$

Para equações de graus maiores, vamos depender dos chamados caracteres módulo p, que são funções totalmente multiplicativas que se anulam apenas nos múltiplos de p. O símbolo de Legendre é um exemplo de caracter módulo p de ordem 2, por isso pudemos estudar as equações módulo p de grau 2. O caso mais geral de equação diagonal é o seguinte:

$$a_1x_1^{n_1} + a_2x_2^{n_2} + \cdots + a_kx_k^{n_k} \equiv 1 \pmod{p}.$$

que foi estudado por diversos autores (ver, por exemplo, [5, Seção 7.3]). Pela Proposição 3.3.6, podemos supor que n_i divide $p-1$ para todo i (no caso onde $n_i = 2$ para todo i temos que se p é ímpar então 2 divide $p-1$ trivialmente; isso explica a divisão entre os casos $p = 2$ e $p > 2$ que fizemos). Para resolver a equação diagonal na sua forma mais geral, vamos precisar dos caracteres módulo p de ordem n_i. Ainda mais geralmente, podemos pensar em equações (como as citadas anteriormente) sobre corpos finitos. Um corpo finito é um corpo que possui uma quantidade finita de elementos (por exemplo, $\mathbb{Z}_p$ é um corpo finito com p elementos). Sobre um corpo finito K, vale

a cota de Hasse-Weil (ver, por exemplo, [5] ou [3, Teorema 5.38]), que afirma que em uma equação $F = 0$ que possui N soluções temos

$$|N - (q + 1)| \leq 2g\sqrt{q},$$

em que $q = |K|$ e g é o gênero da equação (uma constante que depende da forma da equação). Isso explica, por exemplo, porque a equação $x^2 + y^2 \equiv 1 \pmod{p}$ tem aproximadamente p soluções. Um caso interessante de equação diagonal a ser pesquisado é a equação de Fermat sobre um corpo finito qualquer (ou, em particular, sobre $\mathbb{Z}_p$):

$$x^n + y^n = z^n, \quad n \mid p - 1.$$

Pela cota de Hasse-Weil, podemos ver que essa equação terá muitas soluções, ao contrário da equação sobre os inteiros, visto o que diz o Último Teorema de Fermat.

Referências Bibliográficas

[1] HEFEZ, A.; *Aritmética.* 2ª ed. Coleção PROFMAT, SBM, 2016.

[2] IRELAND, K., ROSEN, M.; *A Classical Introduction to Modern Number Theory.* 2ª ed., Springer-Verlag, 1990.

[3] LIDL, R., NIEDERREITER, H.; *Finite fields.* 2ª ed., Cambridge University Press, 1997.

[4] MARTINEZ, F. B.; et al. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.* Rio de Janeiro: IMPA, 2010.

[5] MULLEN, G.L., PANARIO, D.; *Handbook of finite fields.* Taylor & Francis, 2013.

[6] WAGNER, E.; *Teorema de Pitágoras e Áreas.* PIC-OBMEP. Rio de Janeiro: IMPA, 2015.

[7] WILES, A.; *Modular elliptic curves and Fermat's Last Theorem.* Annals of Mathematics 141 (3), 1995, 443-551.