Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Números Primos: Propriedades, Aplicações e Avanços

Ricardo Minoru Morimoto

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Carina Alves

2014

512.7 Morimoto, Ricardo Minoru
M857n Números Primos: Propriedades, Aplicações e Avanços/ Ricardo Minoru Morimoto- Rio Claro: [s.n.], 2014.
63 f. : il., figs., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
Orientadora: Carina Alves

1. Teoria dos Números. 2. Números Primos. 3. Pequeno Teorema de Fermat. 4. Testes de Primalidade. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Ricardo Minoru Morimoto

Números Primos: Propriedades, Aplicações e Avanços

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Eliris Cristina Rizziolli
Departamento de Matemática - UNESP - Rio Claro

Profa. Dra. Grasiele Cristiane Jorge
Instituto de Ciência e Tecnologia - UNIFESP - São José Dos Campos

Rio Claro, 10 de Março de 2014

Agradecimentos

Agradeço primeiramente aos meu pais, que me prestaram apoio incondicional ao longo de todos os anos de estudo, e à minha irmã, que me mostrou que devemos fazer aquilo que gostamos, mesmo que isso signifique recomeçar do zero. E também à minha namorada, que sempre me encorajou a seguir em frente, mesmo nos momentos difíceis.

Não poderia esquecer também dos meus colegas de turma, e principalmente dos amigos Luís, Pedro, Roberto e Ronaldo companheiros em todos os momentos de nossa jornada.

Aos idealizadores do programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), que nos deram essa incrível oportunidade de crescimento, tanto pessoal quanto profissional. Aos funcionário da UNESP - Rio Claro, cujo excelente trabalho nos garantiu um ambiente propício para o estudo, à Profa. Suzinei Marconato, que desde o princípio acreditou no sucesso do programa e dos alunos.

Por fim, agradeço à minha orientadora, Profa. Dra. Carina Alves, que pacientemente acompanhou o progresso do meu trabalho, e dedicou seu tempo à correção do meu trabalho e à minha orientação.

Arquimedes será lembrado enquanto Ésquilo foi esquecido, porque os idiomas morrem mas as ideias matemáticas permanecem. "Imortalidade" pode ser uma ideia tola, mas provavelmente um matemático tem a melhor chance que pode existir de obtê-la.

Godfrey Harold Hardy (1877-1947)

Resumo

O foco deste trabalho está nos números primos, sobre os quais apresentamos algumas propriedades, primos especiais, avanços recentes e alguns testes de primalidade que detectam se um número é primo ou composto.

Palavras-chave: Teoria dos Números, Números Primos, Pequeno Teorema de Fermat, Testes de Primalidade.

Abstract

Prime numbers have been studied for millennia and still hide many mysteries. The focus of this work is on prime numbers. We present some properties, special primes, recent advances and some primality tests that detect if a number is prime or composite.

Keywords: Number Theory, Prime Numbers, Fermat's Little Theorem, Primality Tests.

Sumário

Referências **62**

Introdução

Desde a antiguidade o homem vem se utilizando da matemática para resolver problemas. Sejam eles de natureza prática, como o cálculo de áreas para a agricultura e transações comerciais, ou de natureza teórica, como é o caso da busca pela resposta do que é conhecido como o último teorema de Pierre Fermat: "Não existem inteiros positivos x, y, z, n, onde $n > 2$, de modo que $x^n + y^n = z^n$" [6].

Os primeiros a enxergar a matemática como algo maior do que uma ferramenta para contagem e cálculos simples foram os filósofos e matemáticos gregos. Sendo os principais nomes, que surgem como os grandes idealizadores da sistematização e abstração da matemática, Tales de Mileto e Pitágoras. Tamanha foi a importância de Tales e Pitágoras para o desenvolvimento da ciência, que até hoje suas descobertas são ensinadas aos jovens nas escolas.

A partir dos trabalhos dos pensadores gregos surgiu a Teoria dos Números, o ramo da matemática que se dedica ao estudo das propriedades dos números inteiros, e que será estudada nesta dissertação. O foco em específico estará sobre os números primos, base da Teoria dos Números, e que vem ganhando grande importância na área da computação, especialmente para a proteção à informação.

Este trabalho foi dividido em quatro partes, um capítulo inicial sobre Teoria dos Números, onde veremos as propriedades básicas dos conjuntos dos números naturais e inteiros, e a definição de números primos e algumas de suas propriedades. No segundo capítulo estudaremos alguns números especiais, como é o caso dos primos gêmeos, primos de Mersenne e os pseudoprimos, e também alguns dos testes que nos permitem verificar se um determinado número é primo ou não. Já o terceiro capítulo é dedicado à exposição de avanços que ocorreram recentemente, inclusive com relação a problemas que permaneceram por algumas centenas de anos sem solução. E, por fim, o capítulo quatro é dedicado a atividades que envolvem números primos, e que ficam como sugestão para serem utilizadas em sala de aula.

1 Teoria dos Números

Para que possamos compreender como funcionam os testes de primalidade que serão apresentados no Capítulo 2, devemos primeiro estar familiarizados com a base da Teoria dos Números. Neste capítulo serão apresentados tópicos que são imprescindíveis para o estudo dos números primos, caso da *divisibilidade*, do *máximo divisor comum* e, principalmente, das *congruências*.

1.1 Números Naturais

Nesta seção apresentamos alguns resultados sobre os números naturais, como suas operações, axioma de indução e princípio da boa ordem, divisibilidade, máximo divisor comum e mínimo múltiplo comum.

Os números naturais podem ser desenvolvidos admitindo somente algumas de suas propriedades mais simples. Estas simples propriedades conhecidas como Axiomas de Peano, em homenagem ao matemático italiano que, em 1899, inaugurou este processo, podem ser anunciadas como segue.

Axiomas de Peano:

P_1) $0 \in \mathbb{N}$

P_2) Para qualquer $n \in \mathbb{N}$ existe um único $n* \in \mathbb{N}$ denominado o *sucessor de* n.

P_3) para cada $n \in \mathbb{N}$ temos $n* \neq 0$.

P_4) Se $m, n \in \mathbb{N}$ e $m* = n*$, então $m = n$.

P_5) Qualquer subconjunto $K \subset \mathbb{N}$ que satisfaça (a) e (b) é igual a $\mathbb{N}$.

(a) $1 \in K$

(b) $k* \in K$ sempre que $k \in K$

O axioma P_5 é chamado de axioma de indução, e é utilizado quando queremos demonstrar que uma propriedade é válida para todos os números Naturais.

Teorema 1.1 (Princípio da Boa Ordem)**.** *[16]*

Todo subconjunto não vazio de $\mathbb{N}$ *possui um elemento mínimo.*

1.1.1 Operações em $\mathbb{N}$

Assumimos familiaridade com os conjuntos $\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\}$ e $\mathbb{N}^* = \{1, 2, 3, 4, \cdots\}$. Abordaremos as propriedades das operações nos números Naturais, que são mais relevantes para o estudo dos números primos.

O conjunto $\mathbb{N}$ conta com duas operações básicas, a adição$(+)$ e a multiplicação$(\cdot)$, as quais tem as seguintes propriedades:

i) Ambas as operações são bem definidas.

$\forall\ m, n, m', n' \in \mathbb{N}$, se $m = m'$ e $n = n'$, então $m + n = m' + n'$ e $m \cdot n = m' \cdot n'$.

ii) Ambas as operações são associativas.

$\forall\ m, n, s \in \mathbb{N}$, temos $(m + n) + s = m + (n + s)$ e $(m \cdot n) \cdot s = m \cdot (n \cdot s)$.

iii) Ambas as operações são comutativas.

$\forall\ m, n \in \mathbb{N}$, temos $m + n = n + m$ e $m \cdot m = n \cdot m$.

iv) Ambas as operações contam com um elemento neutro.

$\forall\ m \in \mathbb{N}$, valem $m + 0 = m$ e $m \cdot 1 = m$.

v) A multiplicação é distributiva em relação à adição.

$\forall\ m, n, s \in \mathbb{N}$, temos $m \cdot (n + s) = m \cdot n + m \cdot s$.

vi) $\mathbb{N}$ é um domínio de integridade, ou seja, não tem divisores de 0.

$\forall\ m, n \in \mathbb{N}$, se $m \cdot n = 0$ então $m = 0$ ou $n = 0$.

vii) Vale a tricotomia, ou seja, dados $m, n \in \mathbb{N}$ vale uma, e apenas uma, das afirmações abaixo:

- $m = n$
- $\exists\ s \in \mathbb{N}^*$; $n = m + s$, ou seja, m é *menor do que* n e denotamos $m < n$.
- $\exists\ s \in \mathbb{N}^*$; $m = n + s$, ou seja, m é *maior do que* n e denotamos $m > n$.

Definição 1.1. *[7]*

Uma relação R sobre um conjunto A não vazio é dita uma relação de equivalência sobre A se, e somente se, R satisfaz as propriedades reflexiva, simétrica e transitiva. Ou seja, valem

i) se $x \in A$, então $x\ R\ x$;

ii) se $x, y \in A$ e $x\ R\ y$, então $y\ R\ x$;

iii) se $x, y, z \in A$ e $x\ R\ y$ e $y\ R\ z$, então $x\ R\ z$.

Definição 1.2. *[7]*

Uma relação R sobre um conjunto A não vazio é dita uma relação de ordem sobre A se, e somente se, R satisfaz as propriedades reflexiva, anti-simétrica e transitiva. Ou seja, valem

i) se $x \in A$, então $x\ R\ x$;

ii) se $x, y \in A$ e $x\ R\ y$, então $x = y$;

iii) se $x, y, z \in A$ e $x\ R\ y$ e $y\ R\ z$, então $x\ R\ z$.

Uma vez conhecidas as propriedades de $\mathbb{N}$, podemos demonstrar as seguintes proposições, conforme [7]:

Proposição 1.1. $\forall\ m \in \mathbb{N}$, *temos que* $m \cdot 0 = 0$.

Demonstração. Utilizando a propriedade v), temos:

$$m \cdot 0 = m \cdot (0 + 0) = m \cdot 0 + m \cdot 0.$$

Caso tivéssemos $m \cdot 0 = n > 0$, teríamos $m \cdot 0 = m \cdot 0 + n \Rightarrow m \cdot 0 > m \cdot 0$, o que é absurdo.

□

Proposição 1.2. *A adição preserva a relação de igualdade e nela vale a lei do cancelamento. Ou seja,* $\forall\ m, n, s \in \mathbb{N}$, $m = n \iff m + s = n + s$.

Demonstração. Como a adição é bem definida, a implicação $m = n \Rightarrow m + s = n + s$ já está comprovada.

Supondo então que vale a igualdade $m + s = n + s$, nos baseamos na tricotomia e devemos analisar cada uma das possíveis relações entre m e n.

i) Se $m < n$, temos $n = m + r$ para algum $r \in \mathbb{N}^*$. Assim sendo, temos $m + s = n + s = (m + r) + s = (m + s) + r$, que é absurdo.

ii) Se $m > n$, temos $m = n + r$ para algum $r \in \mathbb{N}^*$. Assim sendo, temos $n + s = m + s = (n + r) + s = (n + s) + r$, que é absurdo.

iii) $m = n$ deve ser verdadeira, já que as outras duas possibilidades da tricotomia se mostraram falsas.

□

Proposição 1.3. *A relação menor do que ($<$) é transitiva. Ou seja, para todo* $m, n, s \in \mathbb{N}$, *se* $m < n$ *e* $n < s$, *então* $m < s$.

Demonstração. Sejam $m, n, s \in \mathbb{N}$, com $m < n$ e $n < s$, pela propriedade vii) temos $n = m + r$ e $s = n + s$, com $r, s \in \mathbb{N}^*$. Logo $s = n + s = (m + r) + s = m + (r + s) \Rightarrow m < 0$.

□

Proposição 1.4. *A adição preserva a relação menor do que e nela vale a lei do cancelamento. Ou seja,* $\forall\ m, n, s \in \mathbb{N}$, $m < n \iff m + s < n + s$.

Demonstração. Primeiramente, vamos supor que $m < n$. Neste caso, deve existir $r \in \mathbb{N}^*$, tal que $n = m+r$. Segue que $n+s = s+n = s+(m + r) = (s + m)+r = (m + s)+r$, ou seja, $m + s < n + s$.

Supondo agora que $m+s < n+s$, vamos novamente analisar cada um dos possíveis casos da tricotomia:

i) Se $m = n$, pela Proposição 1.2, teríamos $m + o = n + o$, o que é absurdo.

ii) Se $n < m$, teríamos $n + s < m + s$, como acabamos de demonstrar.

iii) Como as outras duas possibilidades se mostraram falsas, $m < n$ deve ser verdadeiro.

□

Proposição 1.5. *A multiplicação preserva a relação de menor do que e nela vale a lei do cancelamento. Ou seja,* $\forall\ m, n \in \mathbb{N}$ *e* $\forall\ s \in \mathbb{N}^*$, $m < n \iff m \cdot s < n \cdot s$.

Demonstração. Primeiramente vamos supor que $m < n$. Neste caso, deve existir $r \in \mathbb{N}^*$, tal que $n = m+r$. Segue que $n \cdot s = s \cdot n = s \cdot (m + r) = s \cdot m + s \cdot r = m \cdot s + s \cdot r$, ou seja, $m \cdot s < n \cdot s$.

Supondo agora que $m \cdot s < n \cdot s$, vamos novamente analisar cada um dos possíveis casos da tricotomia:

i) Se $m = n$, pela Proposição 2.2, teríamos $m \cdot s = n \cdot s$, o que é absurdo.

ii) Se $n < m$, teríamos $n \cdot s < m \cdot s$, como acabamos de demonstrar.

iii) Como as outras duas possibilidades se mostraram falsas, $m < n$ deve ser verdadeiro.

□

Proposição 1.6. *A multiplicação preserva a relação de igualdade e nela vale a lei do cancelamento. Ou seja,* $\forall\ m, n \in \mathbb{N}$, $\forall s \in \mathbb{N}^*$, $m = n \iff m \cdot s = n \cdot s$.

Demonstração. Como a multiplicação é bem definida, a implicação $m = n \Rightarrow m \cdot s = n \cdot s$ já está comprovada.

Supondo então que vale a igualdade $m \cdot s = n \cdot s$, vamos novamente analisar cada um dos possíveis casos da tricotomia:

i) Se $m < n$, pela Proposição anterior teríamos $m \cdot s < n \cdot s$, que é absurdo.

ii) Se $n < m$, teríamos um caso análogo ao $m < n$, outro absurdo.

iii) Como as outras duas possibilidades se mostraram falsas, $m = n$ deve ser verdadeiro.

□

Além das relações *menor do que* e *maior do que*, há ainda as relações *menor ou igual* e *maior ou igual*, que são denotadas, respectivamente, por $\leq$ e $\geq$.

Podemos notar que a relação $<$ não é uma relação de ordem, pois ela não é reflexiva. Mas a partir dela podemos criar uma outra relação que é reflexiva, como definido a seguir.

Dizemos que m é menor ou igual a n, ou n é maior ou igual a m se $m < n$ ou $m = n$, e denotamos por $m \leq n$.

De maneira análoga à relação $<$, temos que $m \leq n$ se, e somente se, existir $r \in \mathbb{N}$ tal que $n = m + r$. E podemos verificar se $\leq$ satisfaz as três propriedades que caracterizam uma relação de ordem.

i) $\forall\ m$, $m \leq m$. (Reflexiva)

ii) $\forall m, n$, $m \leq n$ e $n \leq m \Rightarrow a = b$. (Anti-simétrica)

iii) $\forall m, n, s$, $m \leq n$ e $n \leq s \Rightarrow m \leq s$. (Transitiva)

Com os elementos do conjunto dos números Naturais é possível realizar uma terceira operação, a subtração, mas ao contrário da adição e da multiplicação nem sempre o resultado de uma subtração pertence aos Naturais . Sendo assim, dizemos que o conjunto $\mathbb{N}$ é fechado apenas para a adição e a multiplicação, mas não para a subtração.

Podemos definir a subtração da seguinte maneira:

Definição 1.3. *[7] Dados $m, n, r \in \mathbb{N}$ com $n = m + r$, definimos a subtração n menos m como*

$$n - m = r \iff m + r = n$$

Podemos notar que a definição exige que a igualdade $n = m + r$ seja satisfeita, mas essa é a definição de $m < n$, logo não existe a subtração $m - n$ caso $m \geq n$.

Proposição 1.7. *[7] Dados $m, n, s \in \mathbb{N}$ com $m \leq n$, vale a propriedade distributiva:*

$$s \cdot (n - m) = s \cdot n - s \cdot m.$$

Demonstração. Sabemos que se $n \geq m$, então vale $s \cdot n \geq s \cdot m$, ou seja, $s \cdot n - s \cdot m \in \mathbb{N}$.

Partimos de $n = m + r$, com $r \in \mathbb{N}$, que é verdade pois $m \leq n$. Se multiplicarmos ambos os lados por s, obtemos $s \cdot n = s \cdot (m + r) \Rightarrow s \cdot n = s \cdot m + s \cdot r$, que pode ser reescrito como $s \cdot r = s \cdot n - s \cdot m$.

Mas se substituirmos r por $n - m$, temos:

$$s \cdot (n - m) = s \cdot n - s \cdot m.$$

□

1.1.2 Divisibilidade

Definição 1.4. *[7]*

Sejam $m, n \in \mathbb{N}$, dizemos que m divide n, e denota-se $m \mid n$, quando houver $q \in \mathbb{N}$ tal que $n = m \cdot q$. Chamaremos m e q de divisores ou fatores de n e diremos que n é múltiplo de m e q.

Caso não exista q tal que $n = m \cdot q$, diremos que m não divide n e denotaremos por $m \nmid n$.

Proposição 1.8. *[7] $\forall\ m, n \in \mathbb{N}^*$ e $o \in \mathbb{N}$, são verdadeiras as afirmações a seguir:*

i) $m \mid m$, $1 \mid m$ e $m \mid 0$.

ii) Se $m \mid n$ e $n \mid o$, segue que $m \mid o$.

Demonstração.

i) Como visto anteriormente, $m = m \cdot 1$, $\forall\ m \in \mathbb{N}$, logo $m \mid m$ e $1 \mid m$.

   Da mesma forma $m \cdot 0 = 0$, $\forall\ m \in \mathbb{N}$, logo $m \mid 0$.

ii) Se $m \mid n$ e $n \mid o$, temos $n = m \cdot q$ e $o = n \cdot r$, com $q, r \in \mathbb{N}$. Se substituirmos n por $m \cdot q$ na segunda igualdade, teremos $o = (m \cdot q) \cdot r = m \cdot (q \cdot r)$, portanto $m \mid o$.

□

Proposição 1.9. *[7]*

Dados $l, m, n, o \in \mathbb{N}$, com $l \neq 0$ e $n \neq 0$, temos que $l \mid m$ e $n \mid o \Rightarrow l \cdot n \mid m \cdot o$.

Demonstração. Se $l \mid m$ e $n \mid o$, então devem existir $q, r \in \mathbb{N}$ tais que $m = l \cdot q$ e $o = n \cdot r$. Temos então $m \cdot o = (l \cdot q) \cdot (n \cdot r) = (l \cdot n) \cdot (q \cdot r)$, ou seja, $l \cdot n \mid m \cdot o$.

□

Um caso particular especialmente importante dessa Proposição ocorre quando $o = n$. Assim temos $l \mid m \Rightarrow l \cdot n \mid m \cdot n$, $\forall\ n \in \mathbb{N}^*$.

Proposição 1.10. *[7]*

Dados $m, n, o \in \mathbb{N}$, com $m \neq 0$, que satisfaçam $m \mid (n+o)$. Então $m \mid n \iff m \mid o$.

Demonstração. $m \mid (n + o)$ implica na existência de um q tal que $n + o = m \cdot q$, da mesma forma $m \mid n$ implica na existência de um r tal que $n = m \cdot r$. Se substituirmos n na primeira igualdade, temos $m \cdot r + o = m \cdot q \Rightarrow m \cdot r < m \cdot q$, o que implica em $r < q$. Podemos concluir que $o = m \cdot q - m \cdot r = m \cdot (q - r)$, o que equivale a $m \mid o$.

A demonstração da volta é análoga, logo não será mostrada aqui.

□

Proposição 1.11. *[7] Dados $m, n, o \in \mathbb{N}$, com $m \neq 0$ e $n \geq o$, tais que $m \mid (n - o)$. temos que $m \mid n \iff m \mid o$.*

Demonstração. $m \mid (n - o)$ implica na existência de um q tal que $n - o = m \cdot q$, da mesma forma $m \mid n$ implica na existência de um r tal que $n = m \cdot r$. Se substituirmos n na primeira igualdade, temos $m \cdot r - o = m \cdot q \Rightarrow m \cdot r = m \cdot q + o \Rightarrow m \cdot q < m \cdot r$, o que implica em $q < r$. Podemos concluir que $o = m \cdot r - m \cdot q = m \cdot (r - q)$, o que equivale a $m \mid o$.

A demonstração da volta é análoga, logo não será mostrada aqui.

□

Proposição 1.12. *[7] Dados $m, n, o, a, b \in \mathbb{N}$, com $m \neq 0$, tais que $m \mid n$ e $m \mid o$, então $m \mid (an + bo)$. E caso tenhamos $an \geq bo$, então $m \mid (an - bo)$.*

Demonstração. $m \mid n$ e $m \mid o$ implica na existência de $q, r \in \mathbb{N}$ tais que $n = m \cdot q$ e $o = m \cdot r$. Temos então $a \cdot m \pm b \cdot o = a \cdot (m \cdot q) \pm b \cdot (m \cdot r) = m \cdot (a \cdot q \pm b \cdot r)$, portanto $m \mid (a \cdot q \pm b \cdot r)$.

□

Proposição 1.13. *[7] Sejam $m, n \in \mathbb{N}^*$, se $m \mid n$ então $m \leq n$.*

Demonstração. $m \mid n$ implica na existência de $q \in \mathbb{N}^*$, tal que $n = m \cdot q$. Como $q \geq 1$, temos $m \leq m \cdot q = n$.

□

Divisão Euclidiana

No livro VII da sua obra "Os elementos" Euclides enuncia o que conhecemos como "algoritmo de divisão Euclidiana", sem no entanto demonstrá-lo. Veremos a seguir uma possível demonstração.

Teorema 1.2. *[7]*

Sejam $m, n \in \mathbb{N}$, com $0 < m < n$. Existem, e são únicos, $q, r \in \mathbb{N}$ tais que $n = m \cdot q + r$, com $r < m$.

Demonstração. Tomemos m, n satisfazendo as condições do teorema, e criemos o conjunto $A = \{n, n-m, n-2m, n-3m, \cdots\}$.

Pelo Princípio da Boa Ordem, existe um menor elemento no conjunto A, digamos que seja $n - m \cdot q = r$. Precisamos provar que $r < m$.

Caso $m \mid n$, então $r = 0 < m$. Caso contrário, então $r \neq m$, e aí bastaria provar que r não pode ser maior do que m.

Se $r > m$ fosse verdadeiro, teríamos $r = m + a$ para algum $a \in \mathbb{N}^*$, mas como $r = n - q \cdot m$, resulta que $r = m + a = n - q \cdot m \Rightarrow a = n - (q+1) \cdot m \in A$, e $a < r$, o que contradiz o fato de r ser o menor elemento de A.

Temos, pela tricotomia, que $r < m$, e temos $n = m \cdot q + r$, com $r < m$.

Para provar a unicidade, supomos que exista um segundo par r' e $q' \in \mathbb{N}$, que satisfaça $n = m \cdot q' + r'$, com $r' < m$ e $r < r'$. Como $r' \in A$, temos que $r' \geq r + m \Rightarrow r' > m$, o que é absurdo, logo devemos ter $r = r'$.

Por fim, temos $n - m \cdot q = n - m \cdot q' \Rightarrow m \cdot q = m \cdot q' \Rightarrow q = q'$.

□

Corolário 1.1. *[7]*

Dados $m, n \in \mathbb{N}$, com $1 < m \leq n$, existe $a \in \mathbb{N}$ tal que $m \cdot a \leq n < m \cdot (a+1)$.

Demonstração. Pelo algoritmo da divisão Euclidiana, devem existir $q, r \in \mathbb{N}$ tais que $n = m \cdot q + r$, com $r < m$. Basta tomarmos então, $a = q$, assim teremos $m \cdot a \leq n$, uma vez que $r \geq 0$, e como $m > r$, teremos $m \cdot (a+1) = m \cdot a + m > m \cdot a + r = n$.

□

1.1.3 Máximo Divisor Comum

Dados dois números naturais m e n, chamamos de *divisor comum* qualquer $a \in \mathbb{N}$ tal que $a \mid m$ e $a \mid n$. Dentre os divisores comuns de um par qualquer de números, existe um que apresenta algumas características especiais.

Definição 1.5. *Sejam $m, n, d \in \mathbb{N}$, com m e n não simultaneamente nulos, tais que as seguintes condições são satisfeitas:*

i) d é divisor comum de m e n.

ii) todo divisor comum de m e n divide d.

Damos a d o nome de máximo divisor comum de m e n ou, simplesmente, mdc e denotamos por $d = mdc(m, n)$.

E a partir do conceito de *mdc* podemos definir um outro conceito muito importante, e que será utilizado na demonstração de algumas propriedades do *mdc*.

Definição 1.6. *Dizemos que dois números $m, n \in \mathbb{N}$ são primos entre si quando $mdc(m, n) = 1$.*

Exemplo 1.1. $mdc(21, 143) = 1$, logo 21 e 143 são primos entre si, mesmo sendo eles, isoladamente, números não primos, como veremos na seção 1.3.

As seguintes propriedades, com $m, n \in \mathbb{N}$, são fáceis de serem verificadas:

i) $mdc(m, n) = mdc(n, m)$

ii) $mdc(0, m) = m$

iii) $mdc(1, m) = 1$

iv) $mdc(m, m) = m$

Uma outra propriedade muito mais importante do *mdc* já era conhecida por Euclides.

Lema 1.1. *[7] Dados $m, n, a \in \mathbb{N}$, com $m < m \cdot a < n$, $mdc(m, n) = mdc(m, n - m \cdot a)$.*

Demonstração. Seja $d = mdc(m, n - m \cdot a)$, temos que $d \mid m \Rightarrow d \mid m \cdot a$ e $d \mid n - m \cdot a$, em particular, $d \mid (n - m \cdot a + m \cdot a) = n$, portanto d é um divisor de n também.

Se supormos que exista um número c que seja divisor comum de a e b, temos que $c \mid n - m \cdot a$, e como $d = mdc(m, n - m \cdot a)$, temos que $c \mid d$, portanto $d = mdc(m, n)$. □

Esse lema foi utilizado por Euclides para criar o que conhecemos como *algoritmo de Euclides* para encontrar o *mdc* de dois números quaisquer, que veremos a seguir.

Algoritmo de Euclides

Dados $m, n \in \mathbb{N}$, supomos, sem perda de generalidade, que $m \leq n$. Se $m = 1$ ou $m = n$, ou ainda $m \mid n$, sabemos que $mdc(m, n) = m$. Suponhamos, então, que $1 < m < n$ e que $m \nmid n$. Pela divisão Euclidiana temos $n = m \cdot q_1 + r_1$, com $r_1 < m$.

Disso, temos dois possíveis resultados:

i) $r_1 \mid m$, e pelo lema 1.3 $r_1 = mdc(m, r_1) = mdc(a, n - q_1 \cdot m) = mdc(m, n)$ e encerra-se o algoritmo.

ii) $r_1 \nmid m$, e então efetuamos a divisão de m por r_1, donde temos $m = r_1 \cdot q_2 + r_2$, com $r_2 < r_1$.

De onde podemos ter novamente dois resultados diferentes:

i') $r_1 \mid r_2$, e, novamente pelo lema 1.3, $r_2 = mdc(r_1, r_2) = mdc(r_1, m - q_2 \cdot r_1) = mdc(r_1, m) = mdc(n - q_1 \cdot m, m) = mdc(n, m) = mdc(m, n)$, e encerra-se o algoritmo.

ii') $r_2 \nmid r_1$, e efetuamos a divisão de r_1 por r_2, donde temos $r_1 = r_2 \cdot q_3 + r_3$, com $r_3 < r_2$.

Pelo princípio da boa ordem sabemos que a sequência $a > r_1 > r_2 > \cdots$ deve ter um menor elemento, portanto teremos $r_l \mid r_{l-1}$, o que implica que $mdc(m, n) = r_l$.

O algoritmo pode ser realizado de uma maneira prática se, após efetuarmos a divisão $n = m \cdot q_1 + r_1$, completarmos o diagrama a seguir.

	q_1	
n	m	
r_1		

Em seguida efetuamos a divisão $m = r_1 \cdot q_2 + r_2$ e anotamos no diagrama os resultados:

	q_1	q_2	
n	m	r_1	
r_1	r_2		

Esse procedimento se repete até encontrarmos o $mdc(m, n)$.

	q_1	q_2	$\cdots$	q_{l-1}	q_l	q_{l+1}
n	m	r_1	$\cdots$	r_{l-2}	r_{l-1}	$r_l = mdc(m, n)$
r_1	r_2	r_3	$\cdots$	r_l		

Exemplo 1.2. Utilizemos o algoritmo de Euclides para encontrar $mdc(724, 168)$.

$724 = 168 \cdot 4 + 52$, $r_1 = 52$

$168 = 52 \cdot 3 + 12$, $r_2 = 12$

$52 = 12 \cdot 4 + 4$, $r_3 = 4$

Como $4 \mid 12$, temos que $mdc(724, 168) = 4$.

Exemplo 1.3. Calculemos agora $mdc(935, 182)$.

$935 = 182 \cdot 5 + 25$, $r_1 = 25$

$182 = 25 \cdot 7 + 7$, $r_2 = 7$

$25 = 7 \cdot 3 + 2$, $r_3 = 2$

$7 = 2 \cdot 3 + 1$

Como chegamos a um resto 1, concluímos que $mdc(935, 182) = 1$.

Propriedades do MDC

Para demonstrar algumas propriedades do mdc utilizaremos o conjunto auxiliar J definido a seguir.

Definição 1.7. *Sejam $m, n \in \mathbb{N}^*$, temos:*

$$J(m,n) = \{x \in \mathbb{N}^* \mid \exists\ a, b \in \mathbb{N}, x = am - bn\}.$$

É fácil notar que $J(n,m) = \{y \in \mathbb{N}^* \mid \exists\ a, b \in \mathbb{N}, y = bn - am\}$.

Lema 1.2. *[7]* $J(m,n) = J(n,m) \neq \emptyset$.

Demonstração. Se tomarmos um $c \in J(m,n)$, teremos $c = a \cdot m - b \cdot n$ para algum par $a, b \in \mathbb{N}$. Pela Propriedade Arquimediana, existem $\delta, \epsilon \in \mathbb{N}$ tais que $\delta \cdot m > b$ e $\epsilon \cdot n > a$. Sendo $\sigma = max\{\delta, \epsilon\}$, temos $\sigma \cdot m > b$ e $\sigma \cdot n > a$, o que resulta em

$$c = a \cdot m - b \cdot n = a \cdot m - b \cdot n + (\sigma \cdot m \cdot n) - (\sigma \cdot m \cdot n)$$

$$= n \cdot (\sigma \cdot m - b) - m \cdot (\sigma \cdot n - a) \in J(n,m).$$

A demonstração da volta é completamente análoga, e portanto será omitida.

Uma vez provado que $J(m,n) = J(n,m)$, basta provarmos que $J(m,n) \neq \emptyset$. Para isso basta tomarmos $a = n+1$ e $b = m$, assim teremos $a \cdot m - b \cdot n = (n+1) \cdot m - m \cdot n = m \cdot n + m - m \cdot n = m \Rightarrow m \in J(a,b) \Rightarrow J(a,b) \neq \emptyset$.

□

O próximo teorema mostra a existência do máximo divisor comum para todo $m, n \in \mathbb{N}$

Teorema 1.3. *[7] Dados $m, n \in \mathbb{N}^*$ e d o menor elemento de $J(m,n)$, temos que:*

i) $d = mdc(m,n)$.

ii) $J(m,n)$ *é composto pelos múltiplos de* d.

Demonstração. i) Tomemos s divisor comum qualquer de m e n. Como $s \mid m$ e $s \mid n$, temos que $s \mid am - bn$, ou seja, s divide qualquer elemento de $J(m,n)$ e , em particular, $s \mid d$.

Falta provar que d é divisor comum de todos os elementos de $J(m,n)$. Suponhamos o contrário, existe $c \in J(m,n)$, tal que $d \nmid c$. Neste caso, teríamos $c = dq + r$ para algum par $q, r \in \mathbb{N}$ e com $1 < r < d$.

Como $c \in J(m,n)$, temos $c = am - bn$ e $d = xm - yn$ para alguns $a, b, x, y \in \mathbb{N}$, o que resulta em

$$(am - bn) = (xm - yn)q + r$$

$$r = (am - bn) - (xm - yn)q$$

$$r = m(a - xq) - n(b - yq)$$

O que significa que $r \in J(m,n)$, mas isso é absurdo, pois $r < d$ e d é o menor elemento de $J(m,n)$.

ii) É fácil notar que $\forall\ s \in \mathbb{N}, sd \in J(m,n)$, pois $sd = s(xm - yn) = (sx)m - (sy)n \in J(m,n)$. Ou seja, temos $\{sd : s \in \mathbb{N}\} \subset J(m,n)$.

Por outro lado, como d divide todos os elementos de $J(m,n)$, temos que $J(m,n) \subset \{sd : s \in \mathbb{N}\}$.

□

Corolário 1.2. *[7] Para todo $m, n, l \in \mathbb{N}^*$, temos que $mdc(lm, ln) = l \cdot mdc(m,n)$.*

Demonstração. Como $(lm)a - (ln)b = l(am - bn)$, temos $J(lm, ln) = l \cdot J(m,n)$, e, em particular, $min\ J(lm, ln) = min\ l \cdot J(m,n)$. Então, pelo teorema anterior, concluímos que $mdc(lm, ln) = l \cdot mdc(m,n)$.

□

Corolário 1.3. *[7] Dados $m,\ n \in\ N$, temos $mdc\left(\dfrac{m}{mdc(m,n)}, \dfrac{n}{mdc(m,n)}\right) = 1$.*

Demonstração. Pelo Corolário anterior, temos

$$mdc(m,n) \cdot mdc\left(\frac{m}{mdc(m,n)}, \frac{n}{mdc(m,n)}\right)$$

$$= mdc\left(mdc(m,n)\frac{m}{mdc(m,n)}, mdc(m,n)\frac{n}{mdc(m,n)}\right) = mdc(m,n).$$

Portanto $mdc\left(\dfrac{m}{mdc(m,n)}, \dfrac{n}{mdc(m,n)}\right) = 1$.

□

Proposição 1.14. *[7] Dados $m, n \in \mathbb{N}$, a e b são primos entre si se, e somente se, existirem $x, y \in \mathbb{N}$ tais que $xm - yn = 1$.*

Demonstração. Como m e n são primos entre si, temos $mdc(m,n) = 1$. E pelo teorema anterior existem $a, b \in \mathbb{N}$ tais que $am - bn = mdc(m,n) = 1$.

Por outro lado, se existirem a, b tais que $am - bn = 1$, e $d = mdc(m,n)$, teremos que $d \mid (am - bn) \Rightarrow d \mid 1 \Rightarrow d = 1$.

□

Conhecendo o conceito de números primos entre si e a Proposição anterior, podemos enunciar um lema muito útil demonstrado por Euclides.

Lema 1.3 (Lema de Euclides)**.** *Sejam $a, b, c \in \mathbb{N}$, tais que $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração. Sejam $d, x, y \in \mathbb{N}$ tais que $ad = bc$ e $ax - by = 1$. Temos

$$c = c \cdot 1 = c(ax - by) = cax - cby = cax - ady = a(cx - dy).$$

Isso implica que $a \mid c$.

□

E a partir do lema 1.3 podemos provar o seguinte Corolário e a próxima Proposição:

Corolário 1.4. *[7] Dados $m \in \mathbb{N}$, e $n, o \in \mathbb{N}^*$, temos que $n \mid m$ e $o \mid m \iff \left(\frac{no}{mdc(n,o)}\right) \mid m$.*

Demonstração. Se $n \mid m$ e $o \mid m$, devemos ter $a, b \in \mathbb{N}$ tais que $m = an = bo$, e, consequentemente, $a\frac{n}{mdc(n,o)} = b\frac{o}{mdc(n,o)}$.

Mas como $mdc\left(\frac{n}{mdc(n,o)}, \frac{o}{mdc(n,o)}\right) = 1$, temos que $\frac{n}{mdc(n,o)} \mid a$, que implica que $o\frac{n}{mdc(n,o)} \mid om \Rightarrow \frac{no}{mdc(n,o)} \mid m$.

□

Proposição 1.15. *[1] Seja $a \in \mathbb{N}$. Então $\forall\ m, n \in \mathbb{N}$ temos que $a \mid mn \Rightarrow a \mid m$ ou $a \mid n$.*

Demonstração. Vamos supor que $a \mid mn$ e $a \nmid m$. Como $a \nmid m$, temos que $mdc(m, a) = 1$, e pelo lema 1.3 $a \mid n$.

□

1.1.4 Mínimo Múltiplo Comum

Dados dois números naturais m e n, chamamos de *múltiplo comum* qualquer $a \in \mathbb{N}$ tal que $m \mid a$ e $n \mid a$. Cada par de números naturais apresenta infinitos múltiplos comuns, mas um deles em particular possui algumas características especiais.

Definição 1.8. *Chamamos o menor número natural que é divisível tanto por m quanto por n de mínimo múltiplo comum entre m e n , e denotamos por $mmc(m, n)$.*

Proposição 1.16. *[7]*

Dados $m, n \in \mathbb{N}$, existe $mmc(m, n)$ e $mdc(m, n) \cdot mmc(m, n) = mn$.

Demonstração. Seja $a = \frac{mn}{mdc(m,n)}$, então temos $a = m \cdot \frac{n}{mdc(m,n)} = n \cdot \frac{m}{mdc(m,n)}$, ou seja, $m \mid a$ e $n \mid a$.

Seja c um múltiplo comum de m e n, teremos $c = k_1 m = k_2 n$, com $k_1, k_2 \in N$. Podemos então dividir ambos os lados da igualdade anterior por $mdc(m, n)$, chegando em

$$k_1 \cdot \frac{m}{mdc(m,n)} = k_2 \cdot \frac{n}{mdc(m,n)}.$$

Sabemos, pelo Corolário 1.3, que $mdc\left(\frac{m}{mdc(m,n)}, \frac{n}{mdc(m,n)}\right) = 1$, e pelo lema 1.3 temos que $\frac{m}{mdc(m,n)} \mid k_2$, o que implica que $a \mid k_2 n = c$, e portanto $a \mid c$.

□

Temos então uma forma simples de encontrar o *mmc* de dois números, bastando conhecer o seu *mdc* e o resultado da multiplicação dos dois números dos quais se deseja encontrar o *mmc*.

Corolário 1.5. *[7] Sejam $m, n \in N$, primos entre si, temos que $mmc(m, n) = mn$.*

Demonstração. Pela Proposição anterior, temos que $mdc(m, n) \cdot mmc(m, n) = mn$. Mas m, n primos entre si implica que $mdc(m, n) = 1$, logo $mmc(m, n) = mn$.

□

1.2 Congruências

O conceito de congruência e aritmética modular foi introduzido pela primeira vez por Carl Friedrich Gauss, matemático alemão, em seu trabalho *Disquisitiones Arihmeticae* de 1801. A ideia de Gauss foi de trabalhar aritmética com os restos da divisão Euclidiana por um número previamente fixado. Esse tipo de abordagem foi importante para o desenvolvimento da Teoria dos Números, e até mesmo a notação original de Gauss acabou persistindo até a matemática atual.

Para definir as congruências devemos primeiro conhecer o conjunto dos números inteiros, que é definido usando a noção de relação de equivalência, e a relação $\sim$, como veremos a seguir.

Dados dois pares (a, b) e c, d quaisquer em $\mathbb{N} \times \mathbb{N}$, definimos $\sim$ como

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

Verifiquemos então se $\sim$ satisfaz as propriedades necessárias para ser uma relação de equivalência.

- $\forall\ (a, b) \in \mathbb{N} \times \mathbb{N}$, $a + b = b + a \Rightarrow (a, b) \sim (a, b)$. (*Reflexiva*)
- $(a, b) \sim (c, d) \Rightarrow a + d = b + c \Rightarrow c + b = d + a \Rightarrow (c, d) \sim (a, b)$. (*Simétrica*)
- Se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, temos $a + d = b + c$ e $c + f = d + e$, donde obtemos $a + d + f = b + c + f$ e $c + f + b = e + d + b$, resultando em $a + d + f = e + d + b \Rightarrow a + f = e + b \Rightarrow (a, b) \sim (e, f)$. (*Transitiva*)

Sendo $\sim$ uma relação de equivalência, podemos criar as classes de equivalência $\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} : (x, y) \sim (a, b)\}$. E definimos o conjunto dos números inteiros $\mathbb{Z}$ como

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim = \{\overline{(a, b)} : (a, b \in \mathbb{N} \times \mathbb{N}).$$

Sejam $m, n \in \mathbb{Z}$. Definimos o conjunto

$$I(m, n) = \{xm + yn; x, y \in Z\}.$$

Note que m e n não são simultaneamente nulos, logo $I(m, n) \cap \mathbb{N} \neq \emptyset$. De fato, temos que $m^2 + n^2 = m \cdot m + n \cdot n \in I(m, n) \cap \mathbb{N}$.

Teorema 1.4. *Sejam $m, n \in \mathbb{Z}$ não ambos nulos. Se $d = min\ I(m,n) \cap \mathbb{N}$, então*

i) d é o mdc de a e b;

ii) $I(m,n) = d\mathbb{Z} = \{ld; l \in \mathbb{Z}\}$.

Definição 1.9. *[16] Dizemos que dois números inteiros a e b são congruentes módulo m, com $m > 0$, quando $m \mid (a-b)$, e denotamos $a \equiv b\ (mod\ m)$. Caso $m \nmid (a-b)$, dizemos que a e b são incongruentes, e denotamos $a \not\equiv b\ (mod\ m)$.*

Exemplo 1.4. $5 \mid (17-2)$, logo $17 \equiv 2\ (mod\ 5)$.

Exemplo 1.5. $13 \nmid (172-27)$, logo $172 \not\equiv 27\ (mod\ 13)$.

Proposição 1.17. *[16] Para $a, b \in \mathbb{Z}$, vale $a \equiv b\ (mod\ n)$ se, e somente se, existir $l \in \mathbb{Z}$ tal que $a = b + lm$.*

Demonstração. $a \equiv b\ (mod\ m) \Rightarrow m \mid (a-b)$, logo deve existir l tal que $(a-b) = lm \Rightarrow a = b + lm$.

Por outro lado, se existe l tal que $a = b + lm$, temos $lm = a - b \Rightarrow m \mid (a-b)$, ou seja, $a \equiv b\ (mod\ m)$.

□

Proposição 1.18. *[16] Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 0$, valem as seguintes propriedades:*

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

ii) (Simétrica) $a \equiv b\ (mod\ m) \Rightarrow b \equiv a\ (mod\ m)$.

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

Demonstração. i) $\forall\ m \in \mathbb{N}^*$, temos que $m \mid 0 = (a-a)$, logo $a \equiv a\ (mod\ m)$.

ii) $a \equiv b\ (mod\ m) \Rightarrow a - b = lm$, para algum $l \in \mathbb{Z}$. Multiplicando esta igualdade por -1, temos $b - a = (-l)m$, portanto $b \equiv a\ (nod\ m)$.

iii) $a \equiv b\ (mod\ m) \Rightarrow a = b + l_1 m$, para algum $l_1 \in \mathbb{Z}$, e $b \equiv c\ (mod\ m) \Rightarrow b = c + l_2 m$, para algum $l_2 \in \mathbb{Z}$. Então

$$\begin{aligned} a + b &= b + l_1 m + c + l_2 m \\ \Rightarrow a + b - b - c &= l_1 m + l_2 m \\ \Rightarrow a - c &= (l_1 l_2) m \\ \Rightarrow a &= c + (l_1 l_2) m \\ \Rightarrow a &\equiv c\ (mod\ n). \end{aligned}$$

□

Concluímos portanto que a relação de congruência é uma relação de equivalência.

Teorema 1.5. *[16] Sejam $a, b, c, m \in \mathbb{Z}$, satisfazendo $a \equiv b \ (mod\ n)$, valem:*

i) $a + c \equiv b + c \ (mod\ m)$.

ii) $a - c \equiv b - c \ (mod\ m)$.

iii) $ac \equiv bc \ (mod\ m)$.

Demonstração. i) $a \equiv b \ (mod\ m) \Rightarrow a - b = lm$, para algum $l \in \mathbb{Z}$, mas como $a-b = a-b+0 = a-b+(c-c) = a-b+c-c = a+c-b-c = (a+c)-(b+c)$, temos que $(a + c) - (b + c) = lm \Rightarrow a + c \equiv b + c \ (mod\ m)$.

ii) A demonstração é análoga à do item i).

iii) Por hipótese temos que $a - b = lm$, para algum $l \in \mathbb{Z}$. Então $c(a - b) = clm \Rightarrow ca - cb = (cl)m \Rightarrow ac \equiv bc \ (mod\ m)$.

□

Teorema 1.6. *[16] Sejam $a, b, c, m \in \mathbb{Z}$, satisfazendo $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, valem:*

i) $a + c \equiv b + d \ (mod\ m)$.

ii) $a - c \equiv b - d \ (mod\ m)$.

iii) $ac \equiv bd \ (mod\ m)$.

Demonstração. i) $a \equiv b \ (mod\ m) \Rightarrow a - b = km$ e $c \equiv d \ (mod\ m) \Rightarrow c - d = lm$ para algum par $k, l \in \mathbb{Z}$, logo $(a - b) + (c - d) = km + lm \Rightarrow (a + c) - (b + d) = (k + l)m \Rightarrow a + c \equiv b + d \ (mod\ m)$

ii) A demonstração é análoga à do item i).

iii) Por hipótese temos que $a - b = km$ e $c - d = lm$ para algum par $k, l \in \mathbb{Z}$. Temos então que $c(a - b) = ckm \Rightarrow ac - bc = ckm$ e $b(c - d) = blm \Rightarrow bc - bd = blm$, e

$$(ac - bc) + (bc - bd) = ckm + blm$$

$$\Rightarrow ac - bc + bc - bd = ckm + blm$$

$$\Rightarrow ac - bd = m(ck + bl)$$

$$\Rightarrow ac \equiv bd \ (mod\ m).$$

□

Teorema 1.7. *[16] Sejam $a, b, c, m \in \mathbb{Z}$, com $ac \equiv bc \ (mod\ m)$, temos que $a \equiv b \ (mod\ m/d)$, sendo $d = mdc(|\ c\ |, |\ m\ |)$.*

Demonstração. $ac \equiv bc \ (mod\ m) \Rightarrow ac - bc = c(a-b) = lm$ para algum $l \in \mathbb{Z}$, e se dividirmos cada lado da igualdade por d, temos $\frac{c}{d}(a-b) = l\frac{m}{d} \Rightarrow \frac{m}{d} \mid \frac{c}{d}(a-b)$, mas como $mdc\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, segue que $\frac{m}{d} \mid (a-b) \Rightarrow a \equiv b \ (mod\ m/d)$.

□

Proposição 1.19. *[16] Sejam $a, b, m, n \in \mathbb{Z}$, com $n > 0$ e $a \equiv b \ (mod\ m)$, temos $a^n \equiv b^n \ (mod\ m)$.*

Demonstração. De $a \equiv b \ (mod\ m)$, segue que $m \mid (a-b)$, e temos a identidade $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$, de onde podemos concluir que $m \mid a^n - b^n \Rightarrow a^n \equiv b^n \ (mod\ m)$.

□

1.3 Números Primos

O número $p > 1$ é um número **primo** se seus únicos divisores são ± 1 e $\pm p$. Qualquer número $n > 1$ tem pelo menos um divisor primo. Se n é primo, então esse divisor primo é o próprio n. De fato, se n não é primo, seja $a > 1$ seu menor divisor, $n = ab$, onde $1 < a \leqslant b$. Se a não fosse primo, então $a = a_1 a_2$ com $1 < a_1 \leq a_2 < a$ e $a_1 | n$ contradizendo a minimalidade de a.

Exemplo 1.6. Os menores números primos são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29...

Um número $n > 1$ que não é primo é chamado **composto**. Se n é um número composto, então ele tem um divisor primo menor que $\sqrt{n}$. De fato, como acima, $n = ab$, onde $1 < a \leq b$ e a é o menor divisor de n. Logo $n \geqslant a^2$, e portanto $a \leqslant \sqrt{n}$. Essa ideia pertence ao matemático da Grécia Antiga Eratóstenes (250a.C.).

Exemplo 1.7. Os menores números compostos são: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18...

Teorema 1.8 (Teorema Fundamental da Aritmética)**.** *[1]*

i) Para todo $n \geq 2$, com $n \in \mathbb{N}$, temos que n pode ser escrito como

$$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$$

onde os p_i, $1 \leq i \leq k$, são todos primos.

ii) Se $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_m$, com p_i, $1 \leq i \leq k$ e q_j, $1 \leq j \leq m$ primos, e se $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ e $q_1 \leq q_2 \leq q_3 \leq ... \leq q_m$, então $k = m$ e $p_1 = q_1$, $p_2 = q_2$, ... , $p_k = q_k$.

Demonstração.

i) Se $n = p$ é um número primo, a afirmação é claramente verdadeira. Suponhamos então que n seja composto, e que a afirmação seja verdadeira para todo m, $1 < m < n$.

Tomando $D = \{d \in \mathbb{N} : 1 < d \mid n\}$, temos $D \neq \emptyset$, pois $n \mid n$, logo $n \in D$. Pelo princípio da boa ordem existe $p_1 \in D$ minimal. Temos que p_1 deve ser primo, pois caso contrário teríamos $p_1 = a \cdot b$, e como $p_1 \mid n$, seguiria que $a \mid p$ e $b \mid p$, e $a \mid n$ e $b \mid n$, o que contraria a minimalidade de p_1.

Sendo então p_1 o menor divisor de n, temos $n = p_1 \cdot m$, com $1 < m < n$. Mas como a afirmação é verdadeira para todo m nessas condições, temos $m = p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_k$. Por fim, chegamos a

$$n = p_1 \cdot m = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_k.$$

ii) Suponha $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot ... \cdot q_s$ com $p_1, p_2, p_3, p_4, ...$, $p_r, q_1, q_2, q_3, q_4, ..., q_s$ primos e $p_1 \leq p_2 \leq ... \leq p_r$, bem como $q_1 \leq q_2 \leq ... \leq q_s$.

Como $p_1 \mid n$, temos $p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot ... \cdot q_s$, e se aplicarmos a Proposição anterior várias vezes, concluímos que p_1 deve dividir algum dos fatores de $q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot ... \cdot q_s$. Ou seja, existe m, com $1 \leq m < s$ tal que $p_1 \mid q_m$. Como p_1 e q_m são primos. temos $p_1 = q_m \geq q_1$. Da mesma forma, $q_1 \mid p_l$ para algum l, $1 \leq l \leq r$ e $q_1 = p_l \geq p_1$. Podemos renomear os primos de forma a obter $p_1 = q_1$, e assim teremos

$$p_2 \cdot p_3 \cdot ... \cdot p_r = q_2 \cdot q_3 \cdot ... \cdot q_s.$$

Por indução, podemos concluir que $r - 1 = s - 1 \rightarrow r = s$ e $p_i = q_i$, $\forall\ 1 \leq i \leq r$, o que confirma a afirmação.

□

1.3.1 Distribuição dos Números Primos

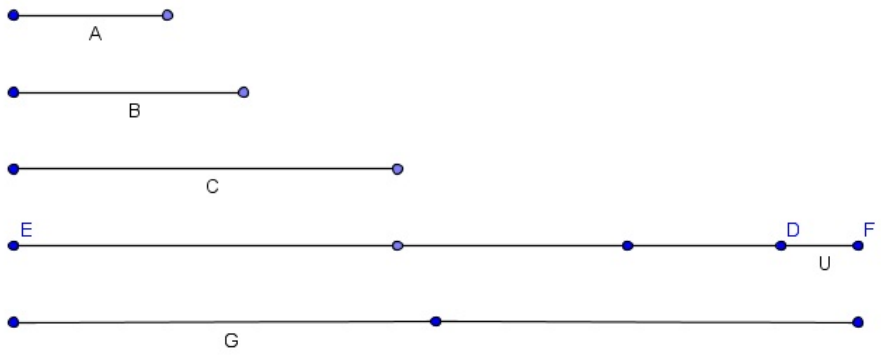
Uma vez definidos o que eram os números primos, surgiu uma importante questão acerca deles. Os gregos viam os números primos como "tijolos", a partir dos quais seria possível construir todos os outros números, mas até determinado momento não se sabia se havia uma quantidade limitada desses "tijolos", ou se eles eram infinitos.

Tal questão foi esclarecida por Euclides, com a demonstração da Proposição 20 do livro IX dos "Elementos". Além de Euclides, vários outros matemáticos propuseram demonstrações para esse problema, incluindo-se nessa lista grandes nomes, como Euler e Goldbach.

A seguir veremos a Proposição de Euclides e sua demonstração traduzida do livro "Os Elementos" de Euclides por Bicudo, I. [5]. Apresentaremos também uma demonstração alternativa da infinitude dos primos.

Proposição 1.20. *[5] Os números primos são mais numerosos do que toda quantidade que tenha sido proposta de números primos.*

Demonstração. Sejam os números primos que tenham sido propostos A, B, C; digo que os números primos são mais numerosos do que os A, B, C.



Fique, pois, tomado o menor medido pelos A, B, C e seja o DE, e fique acrescida a unidade DF ao DE. Então, o EF ou é primo ou não. Primeiramente, suponha que EF seja primo; portanto, os números primos A, B, C, EF achados são mais numerosos do que os A, B, C.

Mas, então, caso não seja primo o EF; portanto, é medido por algum número primo. Seja medido pelo primo G; digo que o G não é o mesmo que algum dos A, B, C. Pois, se possível, seja. Mas os A, B, C medem o DE; portanto, o G também medirá o DE. E também mede o EF; e o G, sendo um número, medirá a unidade DF restante; o que é absurdo. Portanto, o G não é o mesmo que algum dos A, B, C. E foi suposto primo. Portanto, os números primos achados A, B, C, G são mais numerosos do que a quantidade qua tenha sido proposta dos A, B, C; o que era preciso provar.

□

A demonstração de Euclides se baseia mais em elementos geométricos, do que na álgebra, mas pode ser reescrita da seguinte maneira:

Demonstração. Suponhamos que haja uma quantidade n finita de números primos, chamados $p_1, p_2, p_3, ..., p_n$, e tomemos o número $P = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$. Pelo teorema fundamental da aritmética, P deve ser divisível por algum $p_i \in \{p_1, p_2, p_3, ..., p_n\}$, mas como $p \mid a+b \Rightarrow p \mid a$ e $p \mid b$, temos que $p_i \mid P = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1 \Rightarrow p_i \mid p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n$ e $p_i \mid 1$, o que é um absurdo, pois p_i é primo.

Sendo assim, ou P é primo, ou existe algum outro número primo, além dos n inicialmente conhecidos, e que divide P.

□

Uma outra demonstração completamente nova foi dada por Leonhart Euler, nessa demonstração ele relaciona os números primos com a função $\zeta(s)$, $s \in \mathbb{C}$, criada por

ele, mas que posteriormente viria a ser conhecida como a *função zeta de Riemann*:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Uma vez respondida essa questão, as novas perguntas que surgiram foram sobre a frequência, organização e distribuição dos primos. A ideia inicial para descobrir como eles se organizavam foi de criar tabelas com todos os números primos até um certo valor e tentar encontrar alguma lógica.

De posse das tabelas de primos, as primeiras tentativas foram no sentido de se estudar as progressões aritméticas e descobrir se era possível utilizá-las como uma forma fácil de encontrar primos. Sendo que algumas progressões bem triviais contém uma quantidade infinita de primos, como é o caso em que temos o termo inicial $a_1 = 1$ e a razão $r = 2$, $\{1, \mathbf{3}, \mathbf{5}, \mathbf{7}, 9, \mathbf{11}, \mathbf{13}, 15, \mathbf{17}, \mathbf{19}, 21...\}$, onde os números primos estão em negrito.

É fácil notar que a progressão descrita acima é composta por todos os números naturais ímpares, o que claramente nos daria todos os primos, à exceção do número 2. Além desta, é possível provar, utilizando resíduos quadráticos, que as seguintes progressões também nos fornecerão infinitos primos:

- $a_1 = 1$ e $r = 3$: $\{1, 4, \mathbf{7}, 10, \mathbf{13}, 16, \mathbf{19}, 22, 25, 28, \mathbf{31}, ...\}$
- $a_1 = 1$ e $r = 4$: $\{1, \mathbf{5}, 9, \mathbf{13}, \mathbf{17}, 21, 25, \mathbf{29}, 33, \mathbf{37}, \mathbf{41}, ...\}$
- $a_1 = 1$ e $r = 6$: $\{1, \mathbf{7}, \mathbf{13}, \mathbf{19}, 25, \mathbf{31}, \mathbf{37}, \mathbf{43}, 49, 55, \mathbf{61}, ...\}$
- $a_1 = 3, 5$ ou 7 e $r = 8$: $\{\mathbf{3}, \mathbf{11}, \mathbf{19}, 27, 35, \mathbf{43}, 51, \mathbf{59}, \mathbf{67}, 75, \mathbf{83}, ...\}$
- $a_1 = 5, 7$ ou 11 e $r = 12$: $\{\mathbf{5}, \mathbf{17}, \mathbf{29}, \mathbf{41}, \mathbf{53}, 65, 77, \mathbf{89}, \mathbf{101}, \mathbf{113}, 125, ...\}$

Assim como é possível encontrar progressões que contenham infinitos primos, existem progressões que são compostas exclusivamente por números compostos. Como é o caso das progressões com $a_1 = 4$ e $r = 2$, que é composta por todos o números naturais pares maiores do que 2. Da mesma forma, se tomarmos a_1 composto e r não primo com relação a a_1, teremos outras progressões formadas apenas por números compostos.

O fato de a_1 e r serem primos entre si está diretamente ligado à existência ou não de números primos na progressão. Isso foi comprovado pelo matemático belga Johann Dirichlet em 1837, no seguinte teorema:

Teorema 1.9. *[15] Se $r \geq 2$ e $a_1 \neq 0$ são inteiros primos entre si, então a progressão aritmética*

$$a_1, a_1 + r, a_1 + 2r, a_1 + 3r, ...$$

contém uma infinidade de números primos.

A demonstração do teorema de Dirichlet para números primos em progressões aritméticas pode ser encontrada em Landau [10].

Infelizmente o teorema de Dirichlet sobre progressões aritméticas não dá pistas sobre quais termos da progressão serão primos ou não. Porém é possível provar que podemos ter um intervalo entre dois números primos tão grande quanto se queira.

Proposição 1.21. *[1]* $\forall\ n \in \mathbb{N}$ *existe* $k_n \in \mathbb{N}$ *tal que*

$$k_n + 1, k_n + 2, k_n + 3, ..., k_n + n$$

são compostos.

Demonstração. Dado $n \in \mathbb{N}$, basta tomarmos $k_n = (n+1)!+1$. Desta forma garantimos que k_n é divisível por 2, 3, 4, ... , n, ou seja

$$2 \mid (n+1)! + 2 = k_n + 1,$$

$$3 \mid (n+1)! + 3 = k_n + 2,$$

$$\vdots$$

$$n \mid (n+1)! + n = k_n + (n-1),$$

$$(n+1) \mid (n+1)! + (n+1) = k_n + n,$$

e todos estes números são compostos.

□

Exemplo 1.8. Suponha que se queira criar um intervalo com pelo menos 1000 números compostos consecutivos. Para tanto basta tomarmos o número 1001!, que é claramente composto, e à partir dele montamos a sequência $1001!+2, 1001!+3, 1001!+4, ..., 1001!+1001$. É fácil notar que $1001! + 2$ é divisível por 2, $1001! + 3$ é divisível por 3, e assim sucessivamente até $1001! + 1001$, que é divisível por 1001, totalizando 1000 números consecutivos que são compostos.

Essa forma de encontrar um número arbitrário de naturais compostos consecutivos é simples, mas geralmente nos leva a números cuja ordem de grandeza é bastante alta, e nada garante que não haja uma outra sequência de números compostos que seja tão extensa quanto essa e mais próxima do 0.

Proposição 1.22. *[1] Para todo* $n \in \mathbb{N}$*, vale que*

$$p_n \leq 2^{2^{n-1}},$$

onde p_n *representa o n-ésimo número primo.*

Demonstração. Provemos a Proposição por indução em n.

Para $n = 1$, temos $2 = p_1 \leq 2^{2^{1-1}} = 2^1 = 2$, que é claramente verdadeira.

Vamos supor agora que as seguintes afirmações são verdadeiras:

$$p_1 \leq 2^{2^0}$$

$$p_2 \leq 2^{2^1}$$

$$p_3 \leq 2^{2^2}$$

$$\vdots$$

$$p_n \leq 2^{2^{n-1}}.$$

Se $q = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$ é primo, então $q > p_n$. Em todo caso, $p_{n+1} \leq q$.

Temos então

$$p_{n+1} \leq p_1 \cdot p_2 \cdot ... \cdot p_n + 1 \leq 2^{1+2+2^2+...+2^{n-1}} = 2^{2^n-1} + 2^{2^n-1} = 2^{2^n}.$$

□

1.3.2 A Função π dos Números Primos

Outra forma de se trabalhar com primos foi utilizando a função $\pi(x)$, que é definida da seguinte maneira:

Definição 1.10. *Seja x um número real, definimos $\pi(x)$ como sendo a quantidade de números primos p tais que $0 < p \leq x$.*

Exemplo 1.9. $\pi(0) = \pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$.

De forma geral, se organizarmos os primos de forma crescente, $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, ... , teremos que $\pi(x) = n$ se $p_n \leq x < p_{n+1}$.

A função $\pi(x)$ foi estudada por vários matemáticos famosos antes que uma aproximação razoável para ela fosse encontrada e devidamente demonstrada. Um dos primeiros matemáticos a se dedicar ao estudo de $\pi(x)$ foi o matemático suíço Leonhard Euler, que demonstrou que os primos são menos frequentes do que os quadrados de números inteiros, como podemos ver na demonstração da Proposição que segue.

Proposição 1.23. *[15] A soma dos inversos dos números primos é divergente, isto é, $\sum_p (1/p) = \infty$.*

Demonstração. Seja $N \in \mathbb{N}$ arbitrário, todo número $n \in \mathbb{Z}$, $n < N$ é o produto, que se obtém de modo único, de potências de primos $p \leq n$, com $p \leq n$. Para cada primo p, temos

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}.$$

Então

$$\sum_{n=1}^{N}\frac{1}{n} \leq \prod_{p\leq N}(\sum_{k=0}^{\infty}\frac{1}{p^k}) = \prod_{p\leq N}\frac{1}{1-\frac{1}{p}}.$$

Mas,

$$ln\prod_{p\leq N}\frac{1}{1-\frac{1}{p}} = -\sum_{p\leq N} ln(1-\frac{1}{p})$$

e, para cada número primo p,

$$-ln(1-\frac{1}{p}) = \sum_{m=1}^{\infty}\frac{1}{mp^m} \leq \frac{1}{p}+\frac{1}{p^2}(\sum_{h=0}^{\infty}\frac{1}{p^h})$$

$$= \frac{1}{p}+\frac{1}{p^2}\times\frac{1}{1-\frac{1}{p}} = \frac{1}{p}+\frac{1}{p(p-1)}$$

$$< \frac{1}{p}+\frac{1}{(p-1)^2}.$$

Então

$$ln\sum_{n=1}^{N}\frac{1}{n} \leq ln\prod_{p\leq N}\frac{1}{1-\frac{1}{p}} \leq \sum_{p\leq N}\frac{1}{p}+\sum_{p\leq N}\frac{1}{(p-1)^2}$$

$$\leq \sum_{p}\frac{1}{p}+\sum_{n=1}^{\infty}\frac{1}{n^2}.$$

Uma vez que a série harmônica $\sum_{n=1}^{\infty}\frac{1}{n}$ é divergente, a série $\sum_{n=1}^{\infty}\frac{1}{n^2}$ é convergente, e como N é arbitrário, temos que $ln\sum_{n=1}^{N}\frac{1}{n}$ é divergente, portanto a série $\sum_{p}\frac{1}{p}$ com p primo é divergente.

□

Como os recíprocos dos números primos produz uma série divergente, isto é

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\cdots \longrightarrow \infty$$

Segue que o conjunto dos números primos é grande. Além disso, como a série $\sum\frac{1}{n^2}$ é convergente, os quadrados são mais frequentes que os primos.

Outro famoso matemático que estudou a função $\pi(x)$ foi o francês Adrien-Marie Legendre que propôs em 1808 a aproximação

$$\pi(x) \sim \frac{x}{ln\ x - A(x)}$$

sendo que a notação $f(x) \sim g(x)$ significa que $f(x)$ é assintoticamente igual a $g(x)$ e $lim_{x\to\infty}A(x) = -1,08366$.

Mas antes de Legendre, outros dois grandes matemáticos haviam encontrado uma mesma aproximação para $\pi(x)$. O suíço Leonhard Euler e Gauss propuseram, em 1762 e 1791, respectivamente, que $\pi(x) \sim \frac{x}{ln\ x}$.

Futuramente, o matemático russo Pafnuty Chebyshev (grafia de Martinez [11] e Landau[10]), também escrito Tschebycheff (*grafia de Ribenboim* [15]), conseguiu demonstrar que tanto a aproximação dos alemães, quanto a aproximação de Legendre não poderiam chegar a um erro de ordem menor do que $\frac{x}{ln^2\ x}$.

Anos mais tarde, Gauss iria encontrar uma nova aproximação. Ele propôs que $\pi(x)$ era assintoticamente igual a $Li(x) = \int_2^x \frac{dt}{ln\ t}$, mas como $Li(x) \sim \frac{x}{ln\ x}$ bastava provar a sua aproximação anterior.

A demonstração, no entanto, seria conhecida apenas um século depois. Em 1896 os matemáticos franceses Charles-Jean de La Vallée Poussin e Jacques Hadamard a encontraram de maneira independente, mas o mérito da descoberta não pode ser atribuído somente a eles, Riemann trouxe novas ideias e ferramentas entre as descobertas de Gauss e as demonstrações dos matemáticos franceses, sem as quais a demonstração não teria sido possível. Para maiores detalhes sobre essa demonstração e a de Chebyshev, consultar o livro de W. Narkiewicz [12].

Após a demonstração o resultado passou a ser conhecido como Teorema dos Números Primos.

Teorema 1.10 (Teorema dos Números Primos)**.** $lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{ln\ x}\right)} = 1.$

O que o teorema nos diz é que, quanto maior for x, a quantidade de primos menores do que x estará 2 vezes mais próxima do valor de $\frac{x}{ln\ x}$.

1.3.3 Polinômios e Primos

Uma pergunta que é pertinente no estudo dos primos é se existe alguma função polinomial, com domínio em $\mathbb{N}$, e cuja imagem seja composta apenas por números primos. A resposta para esta pergunta é não, e isso pode ser comprovado pela seguinte Proposição.

Proposição 1.24. *[1] Seja* $f(n) = a_g n^g + a_{g-1}s^{g-1} + ... + a_1 n + a_0$ *uma expressão polinomial com coeficientes* $a_0, a_1, ..., a_g \in \mathbb{Z}$ *e* $a_g > 0, g \geq 1$*. Então a sequência* $(f(n))_{n\in\mathbb{N}}$ *assume infinitos valores naturais* ***compostos****.*

Demonstração. Como $a_g > 0$, teremos $f(n) > 0$ para todo $n > n_0$, para algum número n_0. Caso $f(n)$ seja formada apenas por números compostos, está provada a afirmação. Caso contrário, podemos assumir que existe n_1 tal que $f(n_1) = p$ é primo, e $f(n) > 0, \forall\ n \geq n_1$.

Para todo $r \in \mathbb{N}$, temos $f(n_1 + rp) = a_g(n_1 + rp)^g + ... + a_1(n_1 + rp) + a_0 = a_g n_1^g + ... + a_1 n_1 + a_0 + c_r p = p(1 + c_r)$, onde $c_r \in \mathbb{N}$ é a constante apropriada.

Sendo assim, provamos que $f(n_1+rp) = p(1+c_r)$ é composto, e como $c_r = a_g p^g r^g \pm ...$ assume infinitos valores naturais distintos, $f(n)$ também assumirá infinitos valores compostos.

□

Exemplo 1.10. Uma função que a princípio parece ser formada apenas por primos é a $f(x) = x^2 + x + 41$. Isso se deve ao fato de que ela fornece somente números primos para todo $1 \leq x \leq 39$, mas tem $f(40) = 1681 = 41^2$ e $f(41) = 1763 = 41 \cdot 43$.

x	$f(x)$	x	$f(x)$	x	$f(x)$	x	$f(x)$
1	43	11	173	21	503	31	1033
2	47	12	197	22	547	32	1097
3	53	13	223	23	593	33	1163
4	61	14	251	24	641	34	1231
5	71	15	281	25	691	35	1301
6	83	16	313	26	743	36	1373
7	97	17	347	27	797	37	1447
8	113	18	383	28	853	38	1523
9	131	19	421	29	911	39	1601
10	151	20	461	30	971		

1.4 Pequeno Teorema de Fermat

Os números primos possuem muitas propriedades. Uma delas foi encontrada por Pierre de Fermat, chamada de Pequeno Teorema de Fermat.

Antes de enunciarmos e demonstrarmos este teorema, apresentamos primeiramente um lema, necessário para a sua demonstração.

Lema 1.4. *[3] Seja p um número primo e a e b inteiros. Então,*

$$(a+b)^p \equiv a^p + b^p \,(mod\, p).$$

Demonstração. O lema é demonstrado utilizando a notação do binômio de Newton, no caso

$$(a+b)^p \equiv a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i.$$

Para provar a veracidade do lema, basta mostrar que

$$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i \equiv 0 \,(mod\, p).$$

Ao expandirmos o número binomial, temos

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{i!}.$$

Como não sabemos se a e b são múltiplos de p, nos resta tentar concluir que $\binom{p}{i}$ o seja, e isso pode ser feito ao lembrarmos que $\binom{p}{i}$ é inteiro.

O fato de que $\binom{p}{i}$ é inteiro implica no fato de que todos os fatores de $i!$ são cancelados com fatores do numerador da fração. Mas como $1 \leq i \leq p-1$ e p é primo, concluímos que nenhum dos fatores do denominador da fração cancela o fator p. Portanto $\binom{p}{i}$ é múltiplo de p.

□

Demonstrado o lema, podemos demonstrar o teorema por indução em n para os casos em que n é natural e depois estendermos a validade para todos os inteiros.

Teorema 1.11 (Pequeno teorema de Fermat)**.** *[3] Seja p um número primo e a um número inteiro, então*

$$a^p \equiv a \,(mod\, p).$$

Demonstração. Inicialmente suponha que $n^p \equiv n \,(mod\, p)$.

Para $n = 1$, temos $1^p \equiv 1 \,(mod\, p)$, que é obviamente verdadeira.

Assumimos então que $n^p \equiv n \,(mod\, p)$ é verdadeira, e utilizando o lema que acabamos de demonstrar, temos

$$(n+1)^p \equiv n^p + 1^p \equiv n + 1 \,(mod\, p).$$

Caso tomemos n negativo, temos $-n$ positivo, logo vale

$$(-n)^p \equiv -n \,(mod\, p).$$

Aqui devemos considerar os dois casos possíveis de paridade de p. Ou p é par, especificamente o número 2, pois é o único primo par, ou p é ímpar.

Quando tivermos $p = 2$, teremos $(-n)^2 \equiv -n \,(mod\, 2)$, ou seja,

$$n^2 \equiv -n \,(mod\, 2).$$

Se estivermos tomando um n par, teremos $n^2 \equiv 0 \,(mod\, 2)$ e $-n \equiv 0 \,(mod\, 2)$, logo $n^2 \equiv -n \,(mod\, 2)$. E caso tenhamos escolhido n ímpar, teremos $n^2 \equiv 1 (mod\, 2)$ e $-n \equiv 1 \,(mod\, 2)$, satisfazendo também $n^2 \equiv -n \,(mod\, 2)$.

Já no caso em que p é ímpar, teremos

$$(-n)^p \equiv -n^p \equiv -n \,(mod\, p).$$

Mas como estamos trabalhando com congruências, podemos multiplicar ambos os lados da nossa congruência por (-1), obtendo $n^p \equiv n \,(mod\, p)$.

□

O pequeno teorema de Fermat tem uma forma alternativa de ser enunciado, como podemos ver a seguir.

Teorema 1.12. *[3] Seja p primo e a um inteiro não divisível por p. Então* $a^{p-1} \equiv 1\,(mod\,p)$.

Muitos algoritmos e testes de primalidade se basearam neste teorema para aumentar sua eficiência.

2 Números Especiais e Testes de Primalidade

O grande objetivo das pesquisas envolvendo números primos atualmente é encontrar algum algoritmo que seja ao mesmo tempo determinístico, ou seja, que consiga dizer com certeza se o número testado é primo ou não, e tenha um tempo de execução razoável mesmo quando o número é extremamente grande, da ordem de mais de uma dezena de milhões de dígitos.

Mesmo com a ajuda de computadores de alto desempenho, o tempo necessário para realizar os cálculos envolvidos nos testes determinísticos que conhecemos é absurdamente alto. Os maiores números primos confirmados por esse tipo de teste levaram alguns anos para serem testados, e isso utilizando simultaneamente vários computadores capazes de realizar bilhões de operações por segundos.

Neste capítulo abordaremos alguns testes de primalidade. Eles possuem uma grande importância na Teoria dos Números e também muitas aplicações, associadas principalmente à criptografia.

2.1 Números Especiais

2.1.1 Primos Gêmeos

Damos o nome de **primos gêmeos** ao par de números primos que diferem de apenas 2 unidades. Devido à grande quantidade de pares de primos gêmeos conhecidos, conjectura-se que eles sejam infinitos, mas a demonstração para isso ainda não foi alcançada, apesar de alguns avanços terem sido feitos recentemente, como veremos mais à frente, no Capítulo 3.

A seguir temos um tabela com os 30 menores pares de primos gêmeos conhecidos.

O maior par de números primos gêmeos conhecido é o par $3756801695685 \cdot 2^{666669} \pm 1$ [2].

Primos	gêmeos	Primos	gêmeos
3	5	227	229
5	7	239	241
11	13	269	271
17	19	281	283
29	31	311	313
41	43	347	349
59	61	419	421
71	73	431	433
101	103	461	463
107	109	521	523
137	139	569	571
149	151	599	601
179	181	617	619
191	193	641	643
197	199	659	661

Tabela 2.1: Primos Gêmeos

2.1.2 Pseudoprimos

Pelo que vimos no pequeno teorema de Fermat, caso tomemos um número n primo, a congruência $a^n \equiv a(mod\, n)$ deve ser verdadeira para todo inteiro a, com $1 < a < n-1$. Mas nada é dito no teorema sobre a primalidade de n caso a congruência seja verdadeira para um ou alguns inteiros a e falsa para outros. O matemático alemão Gottfried Leibniz acreditava que bastava a congruência ser verdadeira para um elemento a para provar que n é primo, mas o mesmo pode ser desmentido com o exemplo abaixo.

Exemplo 2.1. Tomando $a = 2$ e $n = 341$, temos $2^{341} \equiv 2\ (mod\ 341)$, mas $341 = 11 \cdot 31$.

Devido à crença de Leibniz, os inteiros n que satisfazem $a^n \equiv a(mod\, n)$ para apenas alguns valores de a são chamados de **pseudoprimos**. E apesar de não acertar sempre, o teste de Leibniz tem sua utilidade se o usarmos com bases menores e mais fáceis de serem trabalhadas, sendo conclusivo nos casos em que a congruência se mostra falsa.

2.1.3 Números de Carmichael

Sabemos pelo pequeno teorema de Fermat que a congruência $a^n \equiv a(mod\, n)$ deve ser verdadeira para todo inteiro a, com $1 < a < n-1$, caso n seja primo, mas nada é dito sobre a possibilidade de termos um número composto que também satisfaça essas condições.

O primeiro matemático a se dedicar ao estudo de tais números foi o americano Robert D. Carmichael, que teve seu artigo "On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1(mod\, P)$" publicado em 1912, e nele dá alguns exemplos desses números. Por esse motivo os números compostos que satisfazem a congruência acima são chamados de números de Carmichael.

Antes mesmo de Carmichael publicar seu artigo, o alemão Arwin Korselt já havia descoberto que todo número que viria a se chamar de Carmichael deveria obedecer a duas condições, o que ficou conhecido como o teorema de Korselt.

Teorema 2.1 (Teorema de Korselt)**.** *[3] Um número inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as condições:*

1. *p^2 não divide n;*
2. *$(p-1)$ divide $(n-1)$.*

Demonstração. Para começar, vamos supor que temos um inteiro positivo composto ímpar n que satisfaz as condições do teorema. Seja p um fator primo de n, mostremos que, para qualquer $b \in \mathbb{Z}$, temos

$$b^n \equiv b(mod\, p).$$

Se b for divisível por p, a congruência é evidentemente verdadeira, pois ambos os lados seriam congruentes a 0. Caso contrário, podemos usar o Teorema 1.10, que diz que $b^{p-1} \equiv 1(mod\, p)$, bastando fazer uma pequena substituição na congruência acima.

Pela condição 2, temos que $(p-1)$ divide $(n-1)$, ou seja, $(n-1) = (p-1) \cdot q$ para algum q inteiro positivo. Sendo assim, temos $n = (n-1) + 1 = (p-1) \cdot q + 1$. Então

$$b^n \equiv (b^{p-1})^q \cdot b \equiv b(mod\, p).$$

Dessa forma, concluímos que se p é um fator primo de n, então $b^n \equiv b(mod\, p)$ para qualquer inteiro b.

Tomando agora a condição 1, temos $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$, com $p_1 < p_2 < ... < p_k$ primos distintos. Vimos com Teorema 1.10 que $b^n - b$ é divisível por cada um desses p_i, $1 \leq i \leq k$, o que implica em $b^n - b$ ser divisível por $p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k = n$, ou seja, $b^n \equiv b(mod\, n)$. Mas como isso vale para todo b, temos que n é um número de Carmichael.

Façamos agora o caminho inverso, suponhamos que n seja um número de Carmicheal, e provemos que as condições 1 e 2 são válidas. Para isso provaremos primeiro a contrapositiva da condição 1, ou seja, que se houver um primo p divisor de n, tal que p^2 divide n, então n não pode ser um número de Carmichael.

Suponhamos então que tanto o primo p quanto p^2 dividam n. Para que n não seja de Carmichael é suficiente mostrar um inteiro b tal que $b^n \equiv b(mod\, n)$ seja falsa. Para tanto, tomamos $b = p$, e temos então

$$p^n - p = p(p^{n-1} - 1).$$

Como p não divide $p^{n-1}-1$, temos que p^2 não divide $p^n - p$. Mas como p^2 divide n, resulta que n não pode dividir $p^n - p$, ou seja, n não é número de Carmichael.

A demonstração de que se n é número de Carmichael então a condição 2 é verdadeira depende de alguns resultados que não serão aqui demonstrados, para maiores detalhes consultar [3].

□

Exemplo 2.2. Vamos mostrar que o número $n = 561$ é um número de Carmichael. Para isso deveríamos testar a congruência $a^{561} \equiv a \ (mod\ 561)$ para todo $1 < a < n-1$, mas é fácil calcular que $561 = 3{\cdot}11{\cdot}17$, portanto basta mostrarmos que $b^{561}-b$ é divisível por 3, 11 e 17, o que é equivalente e mostrar aqui $561 \mid (b^{561}-b) \iff b^{561} \equiv b \ (mod\ 561)$.

Para os casos em que tomamos b múltiplo de 3, 11 ou 17 não há o que provar, mostremos então o que acontece quando b não for múltiplo de cada um dos fatores de 561.

Caso $3 \nmid b$, teremos $b^2 \equiv 1 \ (mod\ 3) \Rightarrow b^{561} \equiv (b^2)^{280} \cdot b \equiv b \ (mod\ 3)$.

Se $11 \nmid b$, podemos utilizar o Teorema 1.10 para chegar à congruência $b^{10} \equiv 1 \ (mod\ 11)$, que nos leva a $b^{561} \equiv (b^{10})^{56} \cdot b \equiv b \ (mod\ 11)$.

E por fim, caso $17 \nmid b$, temos, novamente utilizando o pequeno teorema de Fermat, $b^{16} \equiv 1 \ (mod 17)$, que resulta em $b^{561} \equiv (b^{16})^{35} \cdot b \equiv b \ (mod\ 17)$.

A seguir temos uma tabela com os vinte menores números de Carmichael, com seus respectivos fatores.

2.1.4 Primos de Mersenne

Marin Mersenne foi um padre e filósofo francês que viveu do final do século XVI até meados do século XVII. Mersenne tinha grande interesse pelas ciências, em particular pela matemática, tanto que se comunicava por correspondências com muitos cientistas contemporâneos, dentre eles grandes mentes como Pierre de Fermat, René Descartes, Blaise Pascal, Evangelista Torricelli e Galileu Galilei.

Mersenne servia como uma espécie de difusor de informações em sua época, cruzando informações sobre as descobertas de seus correspondentes e espalhando-as.

Uma das descobertas atribuídas a Mersenne é a de que se um número da forma $2^p - 1$ for primo, então p é primo. Devido a essa descoberta, todo número $M_n = 2^n - 1$ com n primo é chamado de número de Mersenne. Mas a recíproca da descoberta de Mersenne, no entanto, não se mostra verdadeira. Se tomarmos $n = 11$, temos $2^{11} - 1 = 2047 = 23 \cdot 89$.

No ano de 1644, Mersenne publicou um trabalho chamado *Cogitata physico-mathematica*, em que ele afirma que os números M_i são primos para $i = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257. Posteriormente comprovou-se que ele se enganara com relação aos números M_{67} e M_{257}, e ainda não incluiu em sua lista os primos M_{61}, M_{89} e M_{107}.

Nº de Carmichael	Fatoração
561	$3 \cdot 11 \cdot 17$
1105	$5 \cdot 13 \cdot 17$
1729	$7 \cdot 13 \cdot 19$
2465	$5 \cdot 17 \cdot 29$
2821	$7 \cdot 13 \cdot 31$
6601	$7 \cdot 23 \cdot 41$
8911	$7 \cdot 19 \cdot 67$
10585	$5 \cdot 29 \cdot 73$
15841	$7 \cdot 31 \cdot 73$
29341	$13 \cdot 37 \cdot 61$
41041	$7 \cdot 11 \cdot 13 \cdot 41$
46657	$13 \cdot 37 \cdot 97$
52633	$7 \cdot 73 \cdot 103$
62745	$3 \cdot 5 \cdot 47 \cdot 89$
63973	$7 \cdot 13 \cdot 19 \cdot 37$
75361	$11 \cdot 17 \cdot 31$
101101	$7 \cdot 11 \cdot 13 \cdot 101$
115921	$13 \cdot 37 \cdot 241$
126217	$7 \cdot 13 \cdot 19 \cdot 73$
162401	$17 \cdot 41 \cdot 233$

Tabela 2.2: Números de Carmichael e suas fatorações

Até o presente momento, o maior primo de Mersenne encontrado é o $2^{57.885.161} - 1$, 48º primo de Mersenne, descoberto em janeiro de 2013, que possui 17.425.170 dígitos no sistema decimal, e atualmente o maior número primo conhecido. O resultado foi publicado no site do grupo conhecido como GIMPS (Great Internet Mersenne Prime Search), responsável também pela descoberta, no ano de 2009, do 47º primo de Mersenne, $2^{43.112.609} - 1$, que possui no sistema decimal 12.978.189 dígitos.

Pela descoberta do 47º primo de Mersenne, o GIMPS recebeu um prêmio de 100 mil dólares, que havia sido oferecido pela Electronic Frontier Foundation aos descobridores do primeiro número primo com mais de 10 milhões de dígitos.

A seguir temos uma tabela contendo os primos p menores que 1 milhão e que geram os 33 primeiros primos de Mersenne.

Nº do Primo de Mersenne	p	Nº do Primo de Mersenne	p	Nº do Primo de Mersenne	p
1º	2	12º	127	23º	11213
2º	3	13º	521	24º	19937
3º	5	14º	607	25º	21701
4º	7	15º	1279	26º	23209
5º	13	16º	2203	27º	44497
6º	17	17º	2281	28º	86243
7º	19	18º	3217	29º	110503
8º	31	19º	4253	30º	132049
9º	61	20º	4423	31º	216097
10º	89	21º	9689	32º	756839
11º	107	22º	9941	33º	859433

Tabela 2.3: Primos de Mersenne

2.1.5 Números de Fermat

Em uma de suas cartas a Mersenne, Fermat disse que acreditava que todos os números da forma $F_n = 2^{2^n} + 1$ eram primos. A afirmação de Fermat se baseava no fato de que F_n é primo para $n = 1, 2, 3$ e 4. O que Fermat ignorou, ou muito provavelmente não teve condições de checar, é que o próximo número dessa forma não é primo.

$$F_5 = 4294967297 = 641 \cdot 6700417$$

A fatoração de F_5, no entanto, só foi realizada quando Euler provou que os fatores dos números F_n que não são primos são da forma

$$k \cdot 2^{n+2} + 1.$$

Atualmente os únicos números de Fermat primos conhecidos são:

F_0	3
F_1	5
F_2	17
F_3	257
F_4	65537

Tabela 2.4: Primos de Fermat

Sabe-se que os outros números de Fermat até o F_{24} são compostos, sendo que os

números de F_5 a F_{11} foram completamente fatorados, e do restante conhecemos apenas alguns fatores, ou nenhum, como é o caso do F_{20} e do F_{24}.

Vemos na tabela abaixo alguns dos fatores conhecidos dos números de Fermat até o F_{23}:

Nº de Fermat	Fatores conhecidos
F_5	$641, 6700417$
F_6	$274177, 67280421310721$
F_7	$59649589127497217, 5704689200685129054721$
F_8	1238926361552897
F_9	$2424833, 7455602825647884208337395736200454918783366342657$
F_{10}	$45592577, 6487031809,$ $4659775785220018543264560743076778192897$
F_{11}	$319489, 974849, 167988556341760475137,$ 3560841906445833920513
F_{12}	$114689, 26017793, 63766529, 190274191361, 1256132134125569,$ $5686306475353569551690334109408678048393607420608184 33$
F_{13}	$2710954639361, 2663848877152141313, 3603109844542291969,$ $319546020820551643220672513$
F_{14}	$1169280858730743698290359938345963713403867034233733 13$
F_{15}	$1214251009, 2327042503868417,$ $168768817029516972383024127016961$
F_{16}	$825753601, 188981757975021318420037633$
F_{17}	31065037602817
F_{18}	$13631489, 81274690703860512587777$
F_{19}	$70525124609, 646730219521,$ $3759005551413375428652444608049 9713$
F_{21}	4485296422913
F_{22}	$646587059945918510090557748685045 77$
F_{23}	167772161

Tabela 2.5: Números de Fermat compostos e fatores conhecidos

2.1.6 Primos de Sophie Germain

Sophie Germain foi uma matemática francesa, nascida em 1776, que publicou seus trabalhos sob o pseudônimo masculino de M. Leblanc, pois acreditava que o trabalho de uma mulher não seria levado a sério pela, predominantemente masculina, sociedade matemática. Mesmo tendo seu acesso à École Polytechnique negado por ser mulher,

ela estudou matemática utilizando notas de aula de professores e chegou a ganhar um prêmio da Academia de Ciência da França em 1816, por um trabalho sobre elasticidade. Em seus estudos sobre Teoria dos Números, Germain deu atenção especial a alguns primos que satisfaziam uma determinada condição, a esses números foi dado o nome de **primo de Sophie Germain**, como vemos a seguir.

Definição 2.1. *[15] p é um primo de Sophie Germain se $2p + 1$ é também número primo.*

A grande contribuição de Germain para a Teoria dos Números foi a demonstração do teorema a seguir:

Teorema 2.2. *[15] Se p é um primo de Sophie Germain, então não existem inteiros x, y e z, diferentes de zero e não múltiplos de p, tais que $x^p + y^p = z^p$.*

O Teorema 2.2 trata de casos particulares do Teorema de Fermat, citado na introdução deste trabalho.

Além da demonstração desse teorema, ela também provou que a equação de Fermat é falsa para todos os números primos menores que 100.

A seguir veremos uma tabela com os 20 primeiros primos de Sophie Germain.

nº do Primo de Germain	Primo de Sophie Germain
2	113
3	131
5	173
11	179
23	191
29	233
41	239
53	251
83	281
89	293

Tabela 2.6: Primos de Sophie Germain

2.2 Crivo de Eratóstenes

O algoritmo mais antigo para encontrar números primos foi criado pelo curador da biblioteca de Alexandria, Eratóstenes, que nasceu por volta de 276 a.C..

O crivo de Eratóstenes consiste em se escolher um número n e montar uma lista com todos os números ímpares m, tais que $1 < m \leq n$. Os números pares não são listados pois sabemos que seriam todos múltiplos de 2, logo compostos. Em seguida devemos tomar o menor valor da lista e riscar todos os seus múltiplos maiores do que ele mesmo. Feito isso, tomamos o próximo número que não foi riscado e riscamos todos os seus múltiplos maiores do que este. E assim sucessivamente, até que tenhamos utilizado todos os valores menores ou iguais a $\sqrt{n}$. Os números que não foram riscados antes disso são todos os primos p com $2 < p \leq n$.

O ponto de parada em $\sqrt{n}$ se deve ao fato de que se o número $m < n$ for composto, então ele terá fatores primos menores do que $\sqrt{m}$, mas como $m < n$, temos $\sqrt{m} < \sqrt{n}$. Logo, ao eliminarmos os múltiplos dos números menores do que $\sqrt{n}$, certamente teremos eliminado todos os números compostos entre $\sqrt{n}$ e n, sobrando apenas os números primos.

Este teste é bastante útil se buscamos todos os primos até um determinado valor, mas se torna muito complicado de realizar quando o valor n é muito grande.

Exemplo 2.3. Vamos utilizar o crivo de Eratóstenes para encontrar todos os primos até 100.

Listando os ímpares de 3 a 99, temos:

	3	5	7	9
11	13	15	17	19
21	23	25	27	29
31	33	35	37	39
41	43	45	47	49
51	53	55	57	59
61	63	65	67	69
71	73	75	77	79
81	83	85	87	89
91	93	95	97	99

Ao eliminarmos os múltiplos de 3, ficamos com:

	3	5	7	~~9~~
11	13	~~15~~	17	19
~~21~~	23	25	~~27~~	29
31	~~33~~	35	37	~~39~~
41	43	~~45~~	47	49
~~51~~	53	55	~~57~~	59
61	~~63~~	65	67	~~69~~
71	73	~~75~~	77	79
~~81~~	83	85	~~87~~	89
91	~~93~~	95	97	~~99~~

E assim fazemos com os múltiplos de 5 e 7 resultando em:

	3	5	7	~~9~~
11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29
31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	~~49~~
~~51~~	53	~~55~~	~~57~~	59
61	~~63~~	~~65~~	67	~~69~~
71	73	~~75~~	~~77~~	79
~~81~~	83	~~85~~	~~87~~	89
~~91~~	~~93~~	~~95~~	97	~~99~~

Como o próximo primo seria 11, que é maior que $\sqrt{100} = 10$, encerramos o processo aqui e podemos afirmar que todos os primos até 100 são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.

2.3 Método das Divisões Sucessivas

Utilizando-nos da ideia de que se um número n for composto, ele deve ter fatores primos menores ou iguais a $\sqrt{n}$, podemos tentar provar a primalidade de n pela força bruta, ou seja, tentando dividir n por todos os primos menores ou iguais a $\sqrt{n}$. Caso n não seja divisível por nenhum desses primos, então ele é certamente um número primo.

Este método é chamado de método das divisões sucessivas, e ele se aproveita da habilidade do crivo de Eratóstenes de localizar todos os primos menores do que um determinado número para sabermos por quais primos devemos dividir o nosso candidato a número primo.

Mas diferentemente do crivo de Eratóstenes, o método das divisões sucessivas nos responde apenas se o número n escolhido é ou não um primo, nada dizendo sobre os números menores do que n.

Este teste é bastante útil caso n tenha algum fator primo relativamente pequeno e o próprio n não seja demasiadamente grande. Caso contrário, a busca pelos fatores primos de n se torna muito trabalhosa, como podemos ver pelo exemplo abaixo.

Exemplo 2.4. Verificar se os números 10658417 e 5963 são primos.

Rapidamente podemos verificar que o número 10658417 não é divisível por 2, 3 e 5. Devemos então tentar dividi-lo pelo próximo número primo, que seria o 7.

Realizando essa divisão encontramos o resultado 1522631, ou seja, 10658417 é um número composto.

Já o número 5963, apesar de ser muito menor do que 10658417 se mostra bastante difícil de ser testado por esse método, uma vez que teríamos que dividi-lo pelos primos menores do que $\sqrt{5963} \simeq 77,22$. E como $5963 = 67 \cdot 89$, encontraríamos resultados

negativos até o 61. Ou seja, teríamos que dividir 5963 por 19 números primos distintos para chegarmos à conclusão de que 5963 é um número composto.

Um aspecto interessante deste teste é que ele é facilmente programável como um algoritmo a ser processado por um computador, o que nos permite trabalhar com números ainda maiores. Se tomarmos um número $n > 1$ arbitrário, podemos utilizar o seguinte algoritmo:

1. Seja $d = 2$.
2. Se $d > \sqrt{n}$, então n é primo. Caso contrário, realizar o passo 3.
3. Se d divide n, então n é composto. Caso contrário, realizar o passo 4.
4. Incrementar d em uma unidade e retornar ao passo 2.

Claramente esse algoritmo não está otimizado, pois caso tomemos n primo, ele realizará a divisão de n por todo d, $2 \leq d \leq \sqrt{n}$, para então chegar à conclusão de que n é primo, o que resultaria em aproximadamente $\sqrt{n}$ divisões. Mas destas $\sqrt{n}$ divisões aproximadamente metade seria realizada desnecessariamente, que seriam todos os casos em que d é par e $d \neq 2$

Para termos uma ideia do tempo desperdiçado vejamos os exemplos abaixo.

Exemplo 2.5. Suponhamos que o tamanho do nosso n seja da ordem de 10^{100} dígitos. Neste caso, o algoritmo acima realizaria até $\sqrt{n} = 10^{50}$ divisões. Mas se pensarmos que um computador realiza menos de 10^{10} operações por segundo, e que um ano tem aproximadamente $3 \cdot 10^7$ segundos, teríamos menos de 10^{18} operações por anos, o que resultaria em um tempo de espera maior que 10^{32} anos para chegar à resposta caso n seja primo.

Exemplo 2.6. Caso utilizássemos um algoritmo otimizado, que apenas realizasse as divisões nos casos em que d fosse primo, teríamos até $\pi(\sqrt{n}) = \pi(10^{50}) \simeq \dfrac{10^{50}}{ln\ 10^{50}} > 10^{47}$ operações. Ou seja, mesmo com o novo algoritmo ainda seriam necessários mais de 10^{29} anos para executá-lo, caso n fosse primo.

Como podemos ver, o teste pode ser muito simples ou muito complicado para encontrar os números compostos. Quando testamos um número primo a situação se complica ainda mais, pois neste caso certamente teremos que testar todos os primos menores ou iguais a $\sqrt{n}$, o que torna este teste impraticável para encontrar primos muito grandes.

2.4 Fatoração de Fermat

Fermat criou um algoritmo que nos permite encontrar fatores de um número, principalmente se tivermos $n = ab$, com a e b são relativamente próximos e n ímpar.

Proposição 2.1. *[1] Seja $n \in \mathbb{N}$ ímpar. Existe uma correspondência biunívoca entre os pares (x, y), com $0 \leq y < x \leq n = x^2 - y^2$, e (r, s), com $1 \leq s \leq r \leq n = rs$.*

Demonstração. Sendo $n = x^2 - y^2$, podemos tomar $r = x + y$ e $s = x - y$, de forma que $n = x^2 - y^2 = (x + y) \cdot (x - y) = rs$.

Por outro lado, como n é ímpar, e $n = rs$, tanto r quanto s devem ser ímpares também, o que implica que $\frac{r \pm s}{2}$ é inteiro. Se tomarmos $x = \frac{r+s}{2}$ e $y = \frac{r-s}{2}$, teremos $0 \leq y < x \leq n$, e $x^2 - y^2 = \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2 = \frac{(r^2 + 2rs + s^2) - (r^2 - 2rs + s^2)}{4} = \frac{4rs}{4} = rs = n$.

□

Da Proposição anterior decorrem duas consequências que são importantes para a próxima técnica de fatoração:

Seja $n \in \mathbb{N}$ ímpar.

i) Para cada decomposição distinta de n, $n = rs$, existe uma decomposição como diferença de quadrados, $n = x^2 - y^2$.

ii) n é primo $\iff n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$ é a única decomposição possível de n como diferença de quadrados.

Exemplo 2.7. Seja $n = 35 = 35 \cdot 1 = 7 \cdot 5$, n pode ser escrito como $n = 6^2 - 1^2 = 18^2 - 17^2$.

Exemplo 2.8. Seja $n = 47 = 47 \cdot 1$, n pode ser escrito como $n = 24^2 - 23^2$.

Exemplo 2.9. Seja $n = 25 = 25 \cdot 1 = 5 \cdot 5$, n pode ser escrito como $n = 13^2 - 12^2 = 5^2 - 0^2$.

O algoritmo consiste em supormos que $n = x^2 - y^2$, o que pode ser feito pois n é ímpar e todo número ímpar pode ser escrito como a diferença de dois quadrados. Como $x^2 - y^2 = (x + y)(x - y)$, temos $a = (x - y)$ e $b = (x + y)$.

Devemos então procurar $[\sqrt{n}]$, a parte inteira de $\sqrt{n}$. Caso $\sqrt{n}$ seja inteiro, sabemos que ele é um dos fatores de n. Caso contrário, acrescentamos uma unidade a $[\sqrt{n}]$ e dizemos que $[\sqrt{n}] + 1 = x$ é um candidato a fator de n.

Para sabermos se esse x é mesmo um fator de n, temos que calcular $y = \sqrt{x^2 - n}$, caso y seja inteiro, calculamos a e b a partir desses x e y. Caso contrário, devemos

acrescentar outra unidade ao nosso candidato a fator de n e repetir o processo até que encontremos y inteiro ou $x = \dfrac{n+1}{2}$.

Se o processo se estender até termos $x = \dfrac{n+1}{2}$, então sabemos que n é primo.

Exemplo 2.10. Tentemos achar fatores para o número 1242699.

$\sqrt{1242699} \simeq 1114,76$, logo devemos testar candidatos maiores do que 1114.

Organizando os resultados em uma tabela, temos:

candidato a x	$\sqrt{x^2 - n}$
1115	22,93
1116	52,50
1117	70,63
1118	85

Temos então $x = 1118$ e $y = 85$, logo $a = (x - y) = (1118 - 85) = 1033$ e $b = (x + y) = (1118 + 85) = 1203$. Portanto $1242699 = 1033 \cdot 1203$.

2.5 Teste de Primalidade de Fermat

O Pequeno Teorema de Fermat, que originou o Teste de primalidade de Fermat, oferece um teste simples e eficiente para ignorar números não primos.

Teste de primalidade de Fermat: O teste consiste em tomarmos um número a qualquer e calcularmos a^{n-1} $(mod\ n)$, onde n é o número cuja primalidade desejamos atestar.

Feito o cálculo, temos dois possíveis resultados:

i) Caso $a^{n-1} \equiv 1\ (mod\ n)$, dizemos que n provavelmente é primo, podendo o teste ser repetido para valores diferentes de a, afim de obter uma probabilidade melhor de que n seja primo.

ii) Caso $a^{n-1} \not\equiv 1\ (mod\ n)$, confirmamos que n é composto, e encerramos o teste.

O Teste de Primalidade de Fermat se mostra bastante eficiente para n grande, mas possui uma limitação. Existem números que independentemente do valor de a que for escolhido, irão sempre retornar primos, apesar dos números serem compostos. Estes números são os números de Carmichael, apresentados anteriormente, e eles são suficientes para que o teste de primalidade de Fermat não seja tão utilizado quanto o teste de Miller- Rabin, que apresentaremos mais adiante.

2.6 Teste de Primalidade de Euler

Seja n um primo ímpar, todo número inteiro pode ter, no máximo, duas raízes quadradas $mod\ n$. E em particular, as raízes quadradas de 1 $mod\ n$ são ± 1 .

Se $a \not\equiv 0\ (mod\ n)$, $a^{(n-1)/2}$ é uma raiz quadrada de $a^{(n-1)} \equiv 1\ (mod\ n)$, então $a^{(n-1)/2} \equiv \pm 1\ (mod\ n)$.

Se $a^{(n-1)/2} \not\equiv \pm 1\ (mod\ n)$ para algum a, com $a \not\equiv 0\ (mod\ n)$, então n é composto.

Teste de primalidade de Euler: Escolhido um a qualquer, com $a \not\equiv 0\ (mod\ n)$, calculamos $a^{(n-1)/2}\ (mod\ n)$. Temos então os possíveis resultados:

i) Caso $a^{(n-1)/2} \equiv \pm 1\ (mod\ n)$, dizemos que n provavelmente é primo, podendo o teste ser repetido para valores diferentes de a. Se n for suficientemente grande, e escolhido ao acaso, a probabilidade de que ele seja primo é muito próxima de 1.

ii) Caso $a^{(n-1)/2} \not\equiv \pm 1\ (mod\ n)$, confirmamos que n é composto, e encerramos o teste.

O teste de Euler é mais confiável do que o teste de Fermat, pois nos casos em que n for um inteiro composto ímpar, mas não potência de um primo, teremos quatro raízes quadradas para 1 $mod\ n$.

Sendo assim, podemos ter $a^{(n-1)/2} \equiv m\ (mod\ n)$, onde $m \neq \pm 1$ é uma raiz quadrada de 1. Então $a^{n-1} \equiv 1\ (mod\ n)$. Neste caso, o teste de Fermat retornaria que n provavelmente é primo, enquanto que o teste de Euler retornaria a resposta correta, que n é composto.

Mesmo sendo mais preciso do que o teste de primalidade de Fermat, o teste de Euler ainda não é completamente confiável, pois existem números que são pseudoprimos para alguma base no teste de Euler, como veremos no exemplo a seguir.

Exemplo 2.11. Tomemos os números $341 = 11 \cdot 31$ e $561 = 3 \cdot 187$, e façamos o teste de Fermat para as bases 2 e 5, respectivamente.

$2^{340} \equiv 1\ (mod\ 341)$ e $5^{560} \equiv 1\ (mod\ 561)$.

O teste de Fermat retornaria primo para ambos os números.

Já utilizando o teste de Euler, temos:

$2^{170} \equiv 1\ (mod\ 341)$ e $5^{280} \equiv 67\ (mod\ 561)$.

Já o teste de Euler acertaria a resposta para o número 341, dizendo que o mesmo é composto, mas erraria ao concluir que 561 é primo.

Apesar da existência de pseudoprimos de Euler, o teste ainda se mostra muito mais eficiente do que o teste de Fermat, pois a quantidade de pseudoprimos de Euler seria aproximadamente a metade do número de pseudoprimos de Fermat.

Se tomarmos os números de Carmichael menores do que 10000, veremos que o teste de Euler retorna a resposta correta em cinco dos sete casos, como veremos na tabela a seguir.

n	$\varphi(n)$	qtde. de a tais que $a^{n-1} \equiv 1(mod\ n)$	qtde. de a tais que $a^{(n-1)/2} \equiv \pm 1\ (mod\ n)$
561	320	320	160
1105	768	768	384
1729	1296	1296	1296
2465	1792	1792	1792
2881	2160	2160	1080
6601	5280	5280	2640
8911	7128	7128	1782

Onde $\varphi(n) = \#\{x \in \mathbb{N} \mid x \leq n \text{ e } mdc(x,n) = 1\}$ e é conhecida como função totiente ou função de Euler.

O teste de Euler falha para os números 1729 e 2465, resultando em $a^{(n-1)/2} \equiv \pm 1\ (mod\ n)$ para todo a tal que $mdc(a,n) = 1$. O números que apresentam tal característica são chamamos de pseudoprimos absolutos de Euler, em analogia aos números de Carmichael, que são também conhecidos como pseudoprimos absolutos de Fermat.

Esses números não podem ser comprovados compostos utilizando o teste de Euler, a menos que se tenha $mdc(a,n) \neq 1$ para algum a escolhido, o que pode ser difícil de acontecer caso n não tenha fatores primos pequenos.

2.7 Teste de Primalidade de Miller-Rabin

O teste de Miller-Rabin, assim como os dois testes anteriores, é baseado numa congruência. Neste caso, partimos da congruência utilizada no teste de Fermat, $a^{(n-1)} \equiv \pm 1\ (mod\ n)$, mas substitui-se $(n-1)$ por $2^s \cdot m$, com m ímpar e $s \geq 1$.

O primeiro passo do teste consiste em calcularmos $a^m\ (mod\ n)$. Caso encontremos $a^m \equiv \pm 1\ (mod\ n)$, dizemos que n provavelmente é primo e encerramos o teste.

Caso contrário, verificamos se $s \neq 1$. Se isso for verdade calculamos $a^{2m}\ (mod\ n)$, que pode ter três possíveis resultados:

i) Se $a^{2m} \equiv 1\ (mod\ n)$, confirmamos que n é composto e encerramos o teste.

ii) Se $a^{2m} \equiv -1\ (mod\ n)$, dizemos que n provavelmente é primo e encerramos o teste.

iii) Se $a^{2m} \not\equiv \pm 1\ (mod\ n)$, verificamos se $s \neq 2$, e se isso for verdade calculamos $a^{2^2 m}\ (mod\ n)$.

O teste continuará dessa forma até que uma dessas duas situações aconteça:

- Algum dos resultados das congruências posteriores é igual a ± 1, sendo n composto se igual a -1 e provavelmente primo se igual a 1.
- O teste se estende até $a^{2^{s-1}m}$, sem chegar a conclusão alguma, o encerramos e declaramos n como sendo composto.

Exemplo 2.12. Vamos aplicar o teste de Miller-Rabin no pseudoprimo absoluto de Euler 1729, e usaremos $a = 671$.

Como $1729 - 1 = 1728 = 2^6 \cdot 27$, temos $s = 6$ e $m = 27$.

Como $671^{27} \equiv 1084\ (mod\ 1729)$, continuamos o teste calculando $671^{2 \cdot 27} \equiv 1065\ (mod\ 1729)$.

Por fim calculamos $671^{2^2 \cdot 27} \equiv 1\ (mod\ 1729)$, o que nos faz concluir que 1729 é um número composto.

Exemplo 2.13. Testemos agora $n = 972133929835994161$, um outro número de Carmichael, mas bem mais extenso do que o anterior, utilizando $a = 2$.

$972133929835994161 - 1 = 2^4 \cdot 60758370614749635$, logo $s = 4$ e $m = 60758370614749635$.

$2^{60758370614749635} \equiv 338214802923303483\ (mod\ n)$
$2^{2 \cdot 60758370614749635} \equiv 332176174063516118\ (mod\ n)$
$2^{2^2 \cdot 60758370614749635} \equiv 779803551049098051\ (mod\ n)$
$2^{2^3 \cdot 60758370614749635} \equiv 1\ (mod\ n)$
Concluímos, portanto, que 972133929835994161 é composto.

Exemplo 2.14. Vamos utilizar o teste de Miller-Rabin com um número composto, mas não de Carmichael, $n = 2857191047211793$, e $a = 1003$.

$2857191047211793 - 1 = 2^4 \cdot 178574440450737$, logo $s = 4$ e $m = 178574440450737$.

$1003^{178574440450737} \equiv 1135781085623492\ (mod\ n)$
$1003^{2 \cdot 178574440450737} \equiv 84313648747407\ (mod\ n)$
$1003^{2^2 \cdot 178574440450737} \equiv 2321094267189023\ (mod\ n)$
$1003^{2^3 \cdot 178574440450737} \equiv 978857874792606\ (mod\ n)$
Como chegamos a $a^{2^{s-1}} \cdot m$, concluímos que n é composto.

Exemplo 2.15. Testemos então um número primo, $n = 104513$, e $a = 3$.

$n - 1 = 2^6 \cdot 1633$, logo $s = 4$ e $m = 1066$

$3^{1066} \equiv 88958\ (mod\ n)$
$3^{2 \cdot 1066} \equiv 10430\ (mod\ n)$
$3^{2^2 \cdot 1066} \equiv 91380\ (mod\ n)$
$3^{2^3 \cdot 1066} \equiv 29239\ (mod\ n)$

$3^{2^4 \cdot 1066} \equiv 2781 \ (mod\ n)$

$3^{2^5 \cdot 1066} \equiv -1 \ (mod\ n)$

O teste nos indica que n provavelmente é primo, havendo ainda a possibilidade de repetirmos o teste para outros valores de a afim de aumentar a confiabilidade do resultado.

Assim como os teste anteriores, o teste de Miller-Rabin não é infalível, havendo casos em que um número composto é declarado provavelmente primo.

Quando isso acontece chamamos o número n testado de pseudoprimo forte, e há, comparativamente, menos pseudoprimos fortes do que pseudoprimos de Euler e números de Carmichael. Diferentemente do que acontece com esses testes, não há pseudoprimos absolutos para o teste de Miller-Rabin.

Se tomarmos um número composto ímpar n qualquer, existem no máximo $\varphi(n)/4$ inteiros a, com $mdc(a, n) = 1$ e $1 \leq a < n$, tais que o teste de Miller-Rabin afirma que n é primo, mas na prática a quantidade de pseudoprimos fortes é muito menor do que $\varphi(n)/4$ para valores grandes de n.

Dentre os diversos testes de primalidade existentes, o teste de Miller-Rabin é um dos mais utilizados.

2.8 Teste de Primalidade de Lucas-Lehmer

Este teste foi criado por Fançois Edouard Lucas e aperfeiçoado por Derrick Henry Lehmer, e apesar de ser determinístico e não depender de conjecturas sua utilização acaba sendo limitada a casos específicos, pois para se testar um número n devemos conhecer os fatores do número $n - 1$. Por esse motivo acaba se mostrando mais eficaz para testar números como os de Mersenne.

A sequência $S_0, S_1, S_2, \cdots$, onde $S_0 = 4$ e $S_{n+1} = S_n^2 - 2$, é de extrema importância para o teste de Lucas-Lehmer, pois ele afirma que um número de Mersenne $M(p)$ será primo se, e somente se, $S_{p-2} \equiv 0 \ (mod\ M(p))$.

Exemplo 2.16. Utilizemos o teste de Lucas-Lehmer para testar a primalidade de $M(7) = 2^7 - 1 = 127$.

Sabemos que $M(7)$ será primo se $S_5 \equiv 0 \ (mod\ 127)$ for verdadeiro, então nos aproveitamos da forma como foi definida a sequência S_n e das propriedades das congruências para efetuar esse cálculo.

$S_1 = 4^2 - 2 = 14 \equiv 14 \ (mod\ 127)$

$S_2 = S_1^2 - 2 \Rightarrow S_2 \equiv 14^2 - 2 \equiv 67 \ (mod\ 127)$

$S_3 = S_2^2 - 2 \Rightarrow S_3 \equiv 67^2 - 2 \equiv 42 \ (mod\ 127)$

$S_4 = S_3^2 - 2 \Rightarrow S_4 \equiv 42^2 - 2 \equiv 111 \ (mod\ 127)$

$S_5 = S_4^2 - 2 \Rightarrow S_5 \equiv 111^2 - 2 \equiv 0 \ (mod\ 127)$

Concluímos então que o número de Mersenne $M(7)$ é primo.

Exemplo 2.17. Testemos agora a primalidade de $M(11) = 2^{11} - 1 = 2047$.

Sabemos que $M(11)$ será primo se $S_9 \equiv 0 \ (mod\ 2047)$ for verdadeiro, então temos:

$S_1 = 4^2 - 2 = 14 \equiv 14 \ (mod\ 2047)$

$S_2 = S_1^2 - 2 \Rightarrow S_2 \equiv 14^2 - 2 \equiv 194 \ (mod\ 2047)$

$S_3 = S_2^2 - 2 \Rightarrow S_3 \equiv 194^2 - 2 \equiv 788 \ (mod\ 2047)$

$S_4 = S_3^2 - 2 \Rightarrow S_4 \equiv 788^2 - 2 \equiv 701 \ (mod\ 2047)$

$S_5 = S_4^2 - 2 \Rightarrow S_5 \equiv 701^2 - 2 \equiv 119 \ (mod\ 2047)$

$S_6 = S_4^2 - 2 \Rightarrow S_6 \equiv 119^2 - 2 \equiv 1877 \ (mod\ 2047)$

$S_7 = S_4^2 - 2 \Rightarrow S_7 \equiv 1877^2 - 2 \equiv 240 \ (mod\ 2047)$

$S_8 = S_4^2 - 2 \Rightarrow S_8 \equiv 240^2 - 2 \equiv 282 \ (mod\ 2047)$

$S_9 = S_4^2 - 2 \Rightarrow S_9 \equiv 282^2 - 2 \equiv 1736 \ (mod\ 2047)$

Concluímos então que o número de Mersenne $M(11)$ é composto.

2.9 Teste de Primalidade AKS

O teste criado pelos indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena no ano de 2002, no artigo chamado "*PRIMES is in P*" foi um marco na história dos testes de primalidade, pois se tratava do primeiro teste que conseguia ser, simultaneamente, determinístico, ter um tempo de execução polinomial e não depender de conjectura. O teste se baseia em uma variação do pequeno teorema de Fermat:

$$(x - a)^n \equiv (x^n - a) \ (mod\ n).$$

Mas ao invés de testar a primalidade de n utilizando a equivalência acima, que tem um tempo de execução exponencial, o teste AKS se utiliza da equivalência

$$(x - a)^n \equiv (x^n - a) \, (mod\ (x^r - 1, n)),$$

onde $(mod\ (x^r - 1, n))$ simboliza que devemos efetuar a congruência $(mod\ x^r - 1)$ e, em seguida, tomar o resultado e efetuar uma nova congruência $(mod\ n)$. A resolução dessa equivalência tem tempo de execução polinomial.

O teste em si consiste no seguinte algoritmo:

1. Se $n = a^b$ para qualquer a inteiro e $b > 1$, então retorne COMPOSTO.
2. Encontre o menor r no qual $o_r(n) > log^2\ n$.
3. Se $1 < mdc(a, n) < n$ para algum $a < r$, então retorne COMPOSTO.
4. Se $n \leq r$, então retorne PRIMO.
5. Para $a = 1$ até $\left\lfloor \sqrt{\varphi(r)} log\ n \right\rfloor$ faça: se $(x-a)^n \not\equiv (x^n - a) \ (mod\ (x^r - 1, n))$ então retorne COMPOSTO.

6. Retorne PRIMO.

Exemplo 2.18. Vamos utilizar o teste de primalidade AKS com o número $n = 7$, e tomaremos $a = 2$ e $r = 3$.

Substituindo esses valores em $(x - a)^n \equiv (x^n - a)\ (mod\ (x^r - 1, n))$, temos:

$$(x - 2)^7 \equiv (x^7 - 2)\ (mod\ (x^3 - 1, 7)).$$

Calculamos primeiro $(x^7 - 2)\ (mod\ x^3 - 1)$, o que resulta em $x - 2$, e em seguida calculamos $(x - 2)\ (mod\ 7)$, que resulta em $x + 5$.

Resta então verificar o outro lado da congruência: $(x^7 - 2)\ (mod\ x^{3-1})$ é igual a $-588x^2 + 169x + 418$, e $-588x^2 + 169x + 418(mod\ 7)$ resulta em $x + 5$ também.

Como $(x - 2)^7 \equiv (x^7 - 2)\ (mod\ (x^3 - 1, 7))$ se mostrou verdadeira, e temos um r primo e que não divide n, temos $n^a \equiv 1\ (mod\ r) \Rightarrow 7^2 \equiv 1\ (mod\ 3)$, que é verdadeira, portanto 7 é primo.

Exemplo 2.19. Utilizemos então o teste AKS para testar o número $n = 4$, e tomemos $a = 2$ e $r = 3$ novamente.

Assim como no exemplo anterior substituímos n, a e r na congruência $(x - a)^n \equiv (x^n - a)\ (mod\ (x^r - 1, n))$, chegando a $(x - 2)^4 \equiv (x^4 - 2)\ (mod\ (x^3 - 1, 4))$.

Calculamos então $(x - 2)^4\ (mod\ x^3 - 1)$, que resulta em $x - 2$, e $x - 2\ (mod\ 4)$ que é igual a $x - 2$.

Em seguida calculamos $(x^4 - 1)\ (mod\ x^3 - 1)$ que é igual a $24x^2 - 31x + 16$, e $24x^2 - 31x + 16\ (mod\ 4)$ que é igual a $-3x$.

Como $(x - 2)^4 \not\equiv (x^4 - 2)\ (mod\ (x^3 - 1, 4))$, concluímos que 4 é composto.

2.10 Outros Testes

Além dos teste já citados nas seções anteriores deste capítulo há mais alguns dignos de nota, mas cuja fundamentação teórica foge do escopo deste texto. É o caso dos testes APR e com curvas elípticas.

Teste APR[15] - Em 1983, o teste APR foi publicado no artigo "*On Distinguishing Prime Numbers from Composite Numbers.*", e seu nome vem das iniciais dos sobrenomes dos autores do artigo: Leonard M. Adleman, Carl Pomerance e Robert S. Rumely.

O teste tem como vantagem o fato de não ser necessário conhecer a fatoração do antecessor ou sucessor do número n a ser testado, e o seu tempo de execução é quase polinomial. Além disso, o teste foi aperfeiçoado algumas vezes: por Henri Cohen e Hendrik W. Lenstra em 1984 e 1987, e também por Wieb Bosma e Marc-Paul van der Hulst em 1990.

Teste com curvas elípticas[15] - Arthur O. L. Atkin foi o homem responsável pela criação do algoritmo de teste de primalidade com curvas elípticas no ano de 1986, baseado nas ideias de Shafi Goldwasser e Joe Kilian. Ao longo do teste há alguns

resultados que podem ser verificados individualmente para comprovarmos se o teste foi feito corretamente, tornando desnecessária a repetição de todos os cálculos.

Em 1993 Atkin e François Morain publicaram um trabalho chamado "*Elliptic Curves and Primality Proving*", em que eles aperfeiçoam o método original de Atkin.

Além da criação dos primeiros algoritmos utilizando curvas elípticas, Atkin também foi co-autor, justamente com Daniel J. Bernstein, do chamado *Crivo de Atkin*, uma versão melhorada do crivo de Eratóstenes.

Primalidade de Números Grandes

A Teoria dos Números foi, por muito tempo, descrita pelos seus estudiosos como a mais pura das ciências, pelo simples fato de que ela não apresentava usos práticos imediatos, seu estudo apenas levava ao conhecimento mais profundo de como os números se comportam.

Com a evolução da tecnologia, no entanto, um dos ramos da Teoria dos Números passou a ser o centro das atenções de muitos matemáticos. A crescente necessidade de se proteger dados sigilosos, trocar informações confidenciais, ou mesmo preservar a privacidade das pessoas, nos levou à criação de novos métodos de criptografia. Sendo que estes devem ser cada vez mais elaborados, pois, junto com a necessidade de proteger dados, evoluem também os computadores, que tornam métodos menos rebuscados de criptografia obsoletos devido à sua capacidade computacional elevada.

Atualmente, os melhores métodos de criptografia dependem da utilização de um par de números primos extremamente grandes, que garantiriam que o código é praticamente inquebrável, a menos que se saiba quais foram os primos utilizados.

3 Avanços Recentes e uma Questão a ser Resolvida

Neste Capítulo apresentaremos três avanços recentes e os esforços em busca de uma função que consiga contar a quantidade de números primos até um determinado valor.

3.1 Avanços Recentes

No ano de 2013 foram anunciadas três descobertas de suma importância para a Teoria dos Números, duas delas envolvendo grandes avanços em direção à resposta de duas das maiores questões não resolvidas até hoje, a conjectura de Goldbach e a conjectura dos primos gêmeos, e a terceira foi a descoberta de um primo com mais de 17 milhões de dígitos em sua representação decimal.

3.1.1 Conjectura dos Números Primos Gêmeos

O avanço com relação à conjectura dos números primos gêmeos veio de uma fonte totalmente inesperada. Um matemático sino-americano, professor da Universidade de New Hampshire, mas desconhecido entre os especialistas no ramo da Teoria dos Números, submeteu um artigo à revista *Annals of Mathematics* no dia 17 de janeiro de 2013, alegando ter dado um importante passo em direção à solução da conjectura.

Ao contrário do que acontece com a maioria dos trabalhos em que se alega ter sido encontrada a solução de problemas famosos, o trabalho de Yitang Zhang parecia ser impecável, mostrando completo domínio sobre o assunto. Sendo assim, o artigo de Zhang foi analisado e aprovado para publicação em apenas três semanas, e ele logo foi convidado a fazer uma apresentação do seu trabalho na Universidade de Harvard, que foi marcada para o dia 13 de maio.

Diante de um auditório lotado, Zhang mostrou seu trabalho, ele não havia chegado a demonstrar a conjectura dos números primos gêmeos, mas conseguira provar que existe uma quantidade infinita de primos que diferem de, no máximo, 70 milhões.

O mais surpreendente de tudo é que ele não havia desenvolvido um método totalmente novo para chegar a tal resultado, e sim insistido em métodos que já haviam sido

testados, mas com mais persistência do que seus predecessores.

3.1.2 Conjectura de Goldbach

"*Parece... que todo número maior do que 2 é a soma de três números primos.*"

Esta foi a afirmação que o matemático prussiano Christin Goldbach fez em uma carta destinada a Euler, e datada de 7 de junho de 1742 e à qual Euler respondeu:

"*... todo inteiro par a é uma soma de dois primos. Eu tenho isso como certamente um teorema, embora não possa prová-lo.*"

Assim surgiu um dos maiores mistérios da Teoria dos Números, a conjectura de Goldbach, que já foi testada e verificada verdadeira para todo $n \leq 4 \cdot 10^{18}$, mas para a qual ainda não existe solução definitiva.

Exemplo 3.1. $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, $12 = 5 + 7$, $14 = 7 + 7$, $16 = 5 + 11, \cdots, 200 = 3 + 197 = 7 + 193 = 19 + 181 = 37 + 163 = 43 + 157 = 61 + 139 = 73 + 127 = 97 + 103$, $202 = 5 + 197$, $204 = 5 + 199 = 7 + 197$, $206 = 7 + 199, ...$

Para Goldbach o número 1 era considerado primo, logo não haveria problemas para provar sua afirmação para os números 3, 4 e 5. A exclusão do número 1 como número primo acabou fazendo com que a conjectura passasse a ser conhecida em duas versões, uma forte e uma fraca.

A versão fraca diz: *Todo inteiro ímpar maior do que 5 pode ser escrito como a soma de 3 primos.* Enquanto que a versão forte diz: *Todo número par maior do que 2 pode ser escrito como a soma de dois primos.*

Essa diferenciação acontece pois uma vez provada a versão forte, a fraca resultaria como um corolário, enquanto que o contrário não é verdade.

A partir do ano de 2006, o matemático peruano Harald Andrés Helgoff, que atualmente trabalha na École Normale Supérieure, em Paris, passou a se dedicar ao estudo da versão fraca da conjectura. O foco de Helgoff foi em tentar reduzir o número C, limite para o qual todo número n tal que $n > C$ satisfaz a conjectura.

Desde a década de 1930 já sabia que o número C era da ordem de $10^{6846168}$, sendo que até 2002 esse número já havia sido melhorado para 10^{1346}. Mas Helgoff foi além, conseguindo chegar à marca de 10^{30}, ponto em que os computadores seriam capazes de fazer o resto do trabalho e testar os números que ainda faltavam.

O trabalho final do peruano, *Major Arcs for Goldbach's theorem*, composto por 133 páginas, foi postado no servidor *Arxiv*, no mesmo dia em que Yitang Zhang fazia sua apresentação em Harvard, e apesar de ainda não ter sido completamente analisado, os especialistas em Teoria dos Números estavam otimistas. Posteriormente o trabalho foi revisado, e passou a ter apenas 79 páginas [8], e que serviu de base para um outro trabalho, *The ternary Goldbach conjecture is true* [9].

3.1.3 Descoberta do 48º Primo de Mersenne

Como mencionado na Subseção 2.1.4, em 2013, mais especificamente no mês de janeiro, foi descoberto o 48º primo de Mersenne. O número $2^{57.885.161} - 1$ não só é o maior primo conhecido, como também supera o antigo detentor deste recorde em quase quatro milhões e meio de dígitos no sistema decimal.

O grupo que mantém o site GIMPS foi responsável pela descoberta dos 10 maiores números primos conhecidos, isso se deve em grande parte ao fato de que existem testes de primalidade que foram criados especificamente para testar se números de Mersenne são primos.

3.2 A Música dos Números Primos

A maior promessa de avanço em direção ao aperfeiçoamento da função que supostamente consegue contar a quantidade de números primos até um determinado valor se baseia em uma conjectura que resiste às tentativas de solução por mais de 150 anos.

Para entendermos essa conjectura precisamos primeiro retomar uma função que já foi citada na subseção (1.3.1) deste trabalho, a zeta de Riemann. Euler já sabia que sua função zeta poderia ser reescrita como

$$\zeta(s) = \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \cdots\right)\cdots\left(1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \cdots\right)\cdots$$

onde p seriam todos os números primos, mas a grande ideia de Riemann foi a de testar a função zeta com os números complexos, criados recentemente por Gauss.

A conjectura proposta por Riemann diz que todos os zeros não triviais da função zeta têm parte real igual a $\frac{1}{2}$, e é hoje conhecida como *hipótese de Riemann*. A princípio essa afirmação parece não ter relação alguma com os números primos, mas uma outra descoberta de Riemann foi de uma função $R(x)$, que estima a quantidade de primos menores que x, sendo ainda melhor que a integral logarítmica de Gauss, e que poderia ser melhorada até a perfeição caso conhecêssemos todos os zeros da função zeta.

Riemann descobriu que, quando calculada em seus zeros, a função zeta gera ondas senoidais semelhantes a notas musicais, e que a sua função $R(x)$ se torna cada vez mais próxima de $\pi(x)$ conforme somamos mais e mais as senoides geradas pelos zeros.

Uma vez que se prove a hipótese de Riemann, a tarefa de encontrar todos os zeros da função zeta se torna um pouco mais fácil, gerando assim um avanço significativo em direção à função $\pi(x)$.

4 Propostas de Abordagens em Sala de Aula

Os números primos, pela diversidade de propriedades e problemas nos quais aparecem, constituem um rico tema a ser explorado no Ensino de Matemática.

Neste Capítulo apresentamos algumas propostas de atividades para ensinar e explorar as propriedades dos números primos no Ensino de Matemática. Salienta-se que são apenas sugestões e cabe ao professor de Matemática fazer as devidas adaptações.

4.1 Atividade: Caça aos Primos

Para essa atividade devemos dividir os alunos em dois ou três grupos, que deverão, alternadamente, escolher números dentre os presentes num quadro, como o mostrado abaixo:

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

Após cada escolha, o número é riscado e não pode ser escolhido novamente. O grupo que escolheu o número deve calcular seus divisores, somá-los e o resultado será o número de pontos feito pelo time naquela rodada, devendo ser anotado em uma folha. Quando todos os números do quadro já tiverem sido escolhidos, os grupos calculam a soma de seus pontos e o time vencedor será aquele que obtiver menos pontos.

Ao término do jogo iniciamos uma discussão com os alunos, buscando saber quais estratégias eles adotaram para as escolhas durante o jogo. Espera-se que eles notem que as escolhas mais vantajosas são os números primos, e que é possível facilitar a

busca pelos primos se eles eliminaram as colunas pares e a que contém os números terminados em 5.

O objetivo da atividade é de despertar a curiosidade dos alunos, apresentando números com diferentes quantidades de divisores, e fazendo-os refletir sobre o motivo para que isso ocorra.

4.2 Atividade: Cálculo Mental

Para essa atividade devemos providenciar três dados comuns de seis faces, além de um quadro, como o mostrado abaixo:

0	1	2	3	4	5	6	7
27	28	29	30	31	32	33	8
26	54	55	60	64	66	34	9
25	50	120	125	144	72	35	10
24	48	108	180	150	75	36	11
23	45	100	96	90	80	37	12
22	44	42	41	40	39	38	13
21	20	19	18	17	16	15	14

Um representante de cada grupo deverá tirar par ou ímpar para decidir quem começará lançando os dados. Feito isso, o grupo vencedor deverá lançar os três dados, e em seguida montar uma expressão matemática utilizando os resultados dos três dados e quaisquer operações básicas que eles quiserem.

Por exemplo, se os números sorteados nos dados forem 1, 2 e 5, poderia ser formada a expressão $(5 + 2) \cdot 1$, ou então $2 \cdot 5 - 1$.

Uma vez montada a expressão, calcula-se seu resultado e a casa correspondente a ele é riscada do quadro. O grupo receberá tantos pontos quanto for o número de casas previamente riscadas e que forem adjacentes ao número recém formado, seja horizontal ou verticalmente.

Uma vez que um determinado número for riscado do quadro, ele não poderá ser formado novamente, mesmo que seja usada uma expressão diferente da que fora usada anteriormente. E caso não seja possível chegar a algum resultado válido, a equipe deverá rolar os dados novamente. Quando todas as casas do quadro tiverem sido preenchidas o jogo acaba.

O objetivo desta atividade é estimular o raciocínio dos alunos, fazendo com que eles pensem em diferentes expressões para formar os números que ainda não foram preenchidos no quadro. E espera-se que os alunos notem que o uso da multiplicação é

imprescindível para que se complete o quadro, colocando-os em uma situação em que eles vão, intuitivamente, recorrer à divisão, mais especificamente à busca pelos divisores dos números restantes, a fim de conseguir encontrar as expressões corretas.

4.3 Atividade: Vídeo

O vídeo realizado pela BBC Open University, Grã-Bretanha, 2007, conta a história dos números primos e uma proposta é exibi-lo em sala de aula. Este vídeo pode ser encontrado no youtube, no link:

`http://www.youtube.com/watch?v=f_ybfr0zz-4`

É interessante que, antes da exibição do vídeo, o professor pergunte aos alunos onde encontramos os números. Podemos encontrá-los em nosso cotidiano e na natureza? Qual a importância de conhecermos a história dos números, as principais descobertas que os envolvem e a sua utilidade?

Toda a história dos números primos pode ser constatada no vídeo, que será o ponto de partida para a introdução do tema e servirá para ilustrar as aulas e suscitar questionamentos. O professor deve exibir os vídeos em partes, combinando-os com o planejamento das aulas, os interesses dos alunos, a utilização de jogos e situações reais.

Para maiores detalhes consultar o endereço:

`http://portal.mec.gov.br/seed/arquivos/pdf/tvescola/grades/destaques_out_nov_08.pdf`

Referências

[1] BURTON, D. M. *Elementary number theory*. Revised Printing. Boston: Allyn and Bacon, Inc., 1980.

[2] CALDWELL, C. K. *The largest known primes*: A summary, 1994. Disponível em: <http://primes.utm.edu/largest.html>. Acesso em: 7 jan. 2014.

[3] COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2 ed. Rio de Janeiro: IMPA, 2005. (Coleção Matemática e Aplicações).

[4] DOMINGUES, Hygino H. *Fundamentos de aritmética*. São Paulo: Atual Editora, 1991.

[5] EUCLIDES *Os elementos*: tradução e introdução de Irineu Bicudo. São Paulo: Editora UNESP, 2009.

[6] EVES, H. *Introdução à história da matemática*. 1 ed. Campinas: Editora Unicamp, 2004.

[7] HEFEZ, A. *Elementos de aritmética*. 2 ed. Rio de Janeiro: SBM, 2011. (Coleção Textos Universitários).

[8] HELFGOTT, H. A. *Major arcs for Goldbach's theorem*, 2013. Disponível em: <http://arxiv.org/abs/1305.2897>. Acesso em 9 jan. 2014.

[9] HELFGOTT, H. A. *The ternary Goldbach conjecture is true*, 2013. Disponível em: <http://arxiv.org/abs/1312.7748>. Acesso em 9 jan. 2014.

[10] LANDAU, E. *Elementary number theory*. Nova Iorque: Chelsea Publishing Company, 1958.

[11] MARTINEZ, F. B.; Moreira, C. G.; Saldanha, N. e Tengan, E. *Teoria dos números*: Um passeio com primos e outros números familiares pelo mundo inteiro. 2 ed. Rio de Janeiro: IMPA, 2011.

[12] NARKIEWICZ, W. *The development of prime number theory*: From Euclid to Hardy and Littlewood. Berlim: Springer-Verlag, 2000.

[13] OGILVY, C. S. and Anderson, J. T. *Excursions in number theory*. Nova Iorque: Dover, 1988.

[14] POLYMATH: Bounded gaps between primes, 2013. Disponível em: <http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes>. Acesso em: 7 jan. 2014.

[15] RIBENBOIM, P. *Números primos*: Velhos mistérios e novos recordes. Rio de Janeiro: IMPA, 2012.

[16] SANTOS, J. P. O. *Introdução à teoria dos números*. 3 ed. Rio de Janeiro: IMPA, 2012. (Coleção Matemática Universitária).

[17] SAUTOY, M. *A música dos números primos*: A história de um problema não resolvido na matemática. Tradução: Diego Alfaro. Rio de Janeiro: Zahar, 2008.

[18] WOLTMAN, G. *Great internet Mersenne prime search*, 1996. Disponível em: <http://www.mersenne.org>. Acesso em: 7 jan. 2014.