UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO DANIEL CARNEIRO DE CASTRO

OITO TESTES DE PRIMALIDADE

FORTALEZA
2018

FRANCISCO DANIEL CARNEIRO DE CASTRO

OITO TESTES DE PRIMALIDADE

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Valter Lopes Nunes

FORTALEZA

2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C351o Castro, Francisco Daniel Carneiro de.
Oito testes de primalidade / Francisco Daniel Carneiro de Castro. – 2018.
68 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, 1, Fortaleza, 2018.
Orientação: Prof. Dr. José Valter Lopes Nunes.

1. Testes de primalidade. 2. Números primos. 3. Teoria dos números. I. Título.

CDD

FRANCISCO DANIEL CARNEIRO DE CASTRO

OITO TESTES DE PRIMALIDADE

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovoda em: 23 / 07 / 2018.

BANCA EXAMINADORA

Prof. Dr. José Valter Lopes Nunes (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação, Ciências e Tecnologia do Ceará (IFCE)

Prof. Dr. José Othon Dantas Lopes
Universidade Federal do Ceará (UFC)

Dedico este trabalho a Deus, a ele seja dada toda honra e toda glória.

AGRADECIMENTOS

A Deus, por me conceder a vida, a saúde e tudo que necessitei até hoje.

À minha noiva Emanuela Moura de Melo, por seu apoio emocional e compreensão em momentos que estive ausente investindo tempo neste trabalho.

Ao Prof. Dr. José Valter Lopes Nunes, por sua orientação, disponibilidade e atenção.

Aos professores participantes da banca examinadora Prof. Dr. Ângelo Papa Neto e Prof. Dr. José Othon Dantas Lopes, pelo tempo, pelas valiosas colaborações e sugestões.

À minha família por se fazer presente em muitos momentos importantes de minha vida.

E aos meus colegas de turma, especialmente Edney Freitas Gregorio e Luiz Augustavo Almeida Feitoza pelas várias horas de estudos que partilhamos durante o curso.

"Não há ramo da Matemática, por mais abstrato que seja, que não possa um dia vir a ser aplicado aos fenômenos do mundo real" (LOBACHEVSKY).

RESUMO

Desde tempos remotos os números primos tem sido base de grandes problemas matemáticos, muitos desses problemas atravessaram séculos sem que alguém conseguisse resolve-los, é o caso da famosa conjectura de Goldbach que diz que todo número par maior do que 2 pode ser escrito como a soma de dois números primos, e da conjectura dos primos gêmeos que afirma que existem infinitos pares de primos gêmeos, estas afirmações ainda não foram demonstradas. Mas uma pergunta é inevitável quando o assunto é números primos: como reconhecê-los? Até hoje não se conhece nenhum método eficiente o suficiente para se demonstrar que um número qualquer é primo ou não, e isso influencia diretamente na dificuldade em se provar ou refutar conjecturas sobre números primos. Apesar de pouco eficientes, existem diversos teste para reconhecer se determinados números são primos, esses são conhecidos como testes de primalidade e muitos desses apresentam condições bastante específicas, sendo úteis apenas para tipos particulares de números. Neste trabalho serão apresentados alguns desses testes de primalidade com suas respectivas demonstrações e toda base teórica necessária para realiza-las. Serão apresentadas ainda aplicações desses testes na verificação da primalidade de alguns números.

Palavras-chave: Testes de primalidade. Números primos. Teoria dos números.

ABSTRACT

Since earliest times prime numbers have been the basis of great mathematical problems, many of theses problems have passed centuries without anyone being able to solve them, is the case of the famous Goldbach conjecture that says that any even number greater than 2 can be written as the sum of two prime numbers, and the conjecture of the twin cousins that states that there are infinite pairs of twin cousins, these statements have not yet been demonstrated. But a question is unavoidable when it comes to prime numbers: how to recognize them? To date, no efficient method has been known to prove that any number is prime or not, and this directly influences the difficulty in proving or refuting conjectures about prime numbers. Although not very efficient, there are several tests to recognize if certain numbers are prime, these are known as tests of primality and many of these present very specific conditions, being useful only for particular types of numbers. In this paper, some of these primality tests will be presented with their respective demonstrations and any theoretical basis necessary to carry them out. Applications of these tests will also be presented in the verification of the primality of some numbers.

Keywords: Primality tests. Prime numbers. Theory of numbers.

SUMÁRIO

1	**INTRODUÇÃO**	10
2	**BASE TEÓRICA**	13
2.1	**Princípio de indução finita e princípio da boa ordem**	13
2.2	**Divisão euclidiana**	16
2.3	**Teorema fundamental da aritmética**	20
2.4	**Congruência**	26
2.5	**O pequeno teorema de Fermat**	28
2.6	**Teorema de Wilson**	31
2.7	**Teorema de Euler**	36
2.8	**Critério de Euler**	38
2.9	**Lei de reciprocidade quadrática**	44
3	**TESTES DE PRIMALIDADE**	51
3.1	**Infinitude dos primos**	51
3.2	**Testes de primalidade básicos**	53
3.3	**Testes de primaridade baseados no teorema de Euler**	55
3.4	**Testes baseados na proposição de Pocklington**	60
3.5	**Teste de Pépin**	64
4	**CONCLUSÃO**	67
	REFERÊNCIAS	68

1 INTRODUÇÃO

O conjunto dos números naturais é o mais básico dentre os conjuntos numéricos, tanto é que lidamos com eles desde os primeiros anos de nossas vidas. É relativamente fácil compreender o conceito de número natural e historicamente, esses são os números mais antigos conhecido pelo homem. Dentre os números naturais podemos dar um destaque especial para um subconjunto em particular, os números primos.

Se um número natural maior do que 1 possui apenas dois divisores positivos, então este é um número primo, e se um número natural maior do que 1 não é primo, chamamos esse de composto. Esta simples definição deu origem a diversos problemas ao longo da história da matemática, mas não vem apenas daí a importância de tais números. A característica principal que tornam os números primos tão importantes para a matemática vem do fato desses estarem presentes na fatoração de todo número inteiro, com exceção apenas do 1. Euclides em sua principal obra, Os elementos, descreve que todo número natural pode ser escrito de maneira única, à menos que a ordem, como o produto de fatores primos, este teorema ficou conhecido como teorema fundamental da aritmética.

Conhecer os fatores primos de um número dado é um problema recorrente de aritmética e auxilia na resolução de situações ainda mais complexas, no entanto esta não é uma tarefa fácil. Ao tentarmos fatorar um número dado, corriqueiramente, após várias divisões descobrimos que esse é número primo ou que é um múltiplo de algum primo que não conhecíamos. Se houvesse um método eficiente para testar se um número é primo ou não, nos pouparia muitos desses cálculos. O problema é que tal método ainda não foi descoberto.

Desde tempos remotos matemáticos procuram por um método que possibilite de forma eficiente e prática afirma se um número qualquer é primo, ou até mesmo se determinados tipos de números são sempre primos. Pierre de Fermat (1601-1665) acreditava que os números da forma $2^{2^n} + 1$, com n sendo um número inteiro positivo, são todos primos (RIBENBOIM, 2015). Anos depois Leonhard Euler (1707-1783) provou que $2^{2^5} + 1$ é composto. Os números primos desta forma ficaram conhecidos como primos de Fermat e são bem mais raros do que ele imaginava. O maior primo de Fermat conhecido até hoje é $2^{2^4} + 1 = 65537$ e um dos maiores números de Fermat composto conhecido é $2^{2^{2478782}} + 1$ que tem por fator o número $3 \cdot 2^{2478785} + 1$ o qual possui 746190 algarismos (RIBENBOIM, 2012).

Marin Mersenne, um frade francês do século XVII, conjecturou algo muito parecido com o que Fermat acreditava. Ele afirmou sem apresentar prova ou argumento convincente que os números da forma $M(n) = 2^n - 1$, que são conhecidos atualmente como números de Mersenne, são primos quando n é igual a 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 ou 257, e são compostos para os demais números primos n menores do que 257

(COUTINHO, 2014).

Sobre a conjectura de Mersenne, Coutinho (2014) afirma:

> Como ocorria frequentemente na época, Mersenne não apresentou nenhuma justificativa para estes resultados. Em 1732 Euler afirmou que $M(41)$ e $M(47)$ seriam primos. Estes números não fazem parte da lista de Mersenne, só que, neste caso, quem estava errado era Euler! O primeiro erro da lista foi encontrado por Pervusin e Seelhof em 1886. Eles descobriram que $M(61)$ é primo. Outros erros foram encontrados em anos posteriores. Além de $M(61)$, a lista omite os primos $M(89)$ e $M(107)$; e inclui os compostos $M(67)$ e $M(257)$. (COUTINHO, 2014, p. 57)

Muitos problemas envolvendo números primos tornaram-se famosos no decorrer da história, dentre esses podemos citar o postulado de Goldbach, que afirma que todo número par maior do que 2 pode ser escrito como a soma de dois números primos, se existem infinitos primos gêmeos (números primos que diferem exatamente por duas unidades) e se existem infinitos primos de Fermat (EVES, 2002). Esses três problemas ainda encontram-se em aberto. Também podemos destacar três problemas complexos que já foram resolvidos, o postulado de Bertrand, que foi demonstrado por Tchebychev e que diz que entre n e $2n$ existe ao menos um número primo, para todo n natural maior do que 1, a existência de infinitos primos em qualquer progressão aritmética com o primeiro termo e a razão primos entre sí, demonstrado por Dirichlet, e o teorema dos números primos que dá uma estimativa da quantidade de primos menores do que n que "foi provado independentemente em 1896 pelo francês J. Hadamard e pelo belga C. J. de la Vallée Poussim". (EVES, 2002, p. 624).

Apesar de não serem eficiente o bastante, existem diversos testes para reconhecer se um número é primo, estes são conhecidos como testes de primalidade. Boa parte desses são úteis apenas para determinados tipos de números e envolvem condições bastante específicas. Atualmente os números primos são muito utilizados na computação, mais especificamente na área de criptografia de chave pública baseando-se na dificuldade de se fatorar números com fatores primos muito grandes utilizando os métodos atuais (COUTINHO, 2014). Pensando nesse assunto, estudaremos nos próximos capítulos alguns desses testes que apresentam menor complexidade tanto para aplicação como para compreensão.

Este trabalho tem por objetivo principal apresentar oito testes de primalidade. Dentre eles veremos dois básicos, o primeiro baseado no crivo de Eratóstenes e o outro que é propriamente a recíproca do teorema de Wilson. Os demais são úteis quando se quer verificar a primalidade de n quando é conhecida a fatoração de $n-1$, dos quais três destes são baseados essencialmente no teorema de Euler, outros dois se apoiam na proposição de Pockligton, e o ultimo é o clássico teste de Pépin, que dá uma condição necessária e suficiente para que um número de Fermat seja primo.

Realizaremos as demonstrações dos oito testes e apresentaremos toda a base teórica necessária: as definições, os teoremas e proposições com suas respectivas demonstrações. Apresentaremos ainda aplicações de cada teste em forma de exemplos, verificando se determinados números são primos, e a partir do teste de Pépin demonstraremos que o número de Fermat $2^{2^5} + 1 = 4294967297$ é composto.

2 BASE TEÓRICA

Neste capítulo veremos grande parte da base teórica necessária para demonstração de alguns dos testes de primalidade mais conhecidos. Trataremos de definições e teoremas muito importantes para na teoria dos números, dentre eles estão o teorema fundamental da aritmética, a definição de congruência modular, o pequeno teorema de Fermat, o critério de Euler para o símbolo de Legendre, a lei de reciprocidade quadrática e outros.

2.1 Princípio de indução finita e princípio da boa ordem

Começaremos a nossa teoria apresentando três postulados que serão de extrema importância para algumas das demonstrações dos teoremas presentes neste capítulo. Na verdade, é suficiente considerar apenas um deles como postulado como afirma Santos (2007), uma vez que, como veremos por demonstração eles são equivalentes.

Neste trabalho consideramos conhecido o conjunto dos números naturais, denotado por $\mathbb{N}$, e convencionamos de modo conveniente que o número 1 é o menor número natural. Definimos ainda o conjunto $I_n = \{x \in \mathbb{N} \,|\, x \leq n\}$ para facilitar um pouco a escrita.

Axioma 2.1 (Princípio da boa ordem)**.** *Todo conjunto não vazío de números naturais possui menor elemento.*

Axioma 2.2 (Primeiro princípio de indução finita)**.** *Se $X \subset \mathbb{N}$ é um conjunto com as propriedades:*

i : $1 \in X$;

ii : $n \in X \Rightarrow n + 1 \in X$,

então $X = \mathbb{N}$.

Axioma 2.3 (Segundo princípio de indução finita)**.** *Se $X \subset \mathbb{N}$ é um conjunto com as propriedades:*

i : $1 \in X$;

ii : $I_n \subset X \Rightarrow n + 1 \in X$,

então $X = \mathbb{N}$.

Demonstração (Axioma 2.1 $\Rightarrow$ Axioma 2.2). Suponhamos por absurdo que um conjunto $X \subset \mathbb{N}$ possui as duas propriedades descritas no axioma 2.2 e que $X \neq \mathbb{N}$. Isso implica que $\mathbb{N} \setminus X \neq \emptyset$, e pelo axioma 2.1 este conjunto deve ter um menor elemento r. Como $r \notin X$, temos que $r \neq 1$ e assim

$$(r-1) \in X \Rightarrow (r-1) + 1 \in X \Rightarrow r \in X,$$

absurdo, logo $X = \mathbb{N}$. □

Demonstração (Axioma 2.2 ⇒ Axioma 2.3). Consideremos $X \subset \mathbb{N}$ um conjunto com as duas propriedades descritas no axioma 2.3 e o conjunto $S = \{x \in \mathbb{N} \,|\, I_x \subset X\}$. Precisamos provar que $I_n \subset X, \forall n \in \mathbb{N}$, ou seja, que $S = N$, para isso usaremos o axioma 2.2.

De imediato temos que $1 \in S$, pois $1 \in X \Rightarrow I_1 \subset X$. Se $k \in S$, então

$$\begin{aligned} I_k \subset X &\Rightarrow k+1 \in X \\ &\Rightarrow I_{k+1} \subset X \\ &\Rightarrow k+1 \in S \\ &\Rightarrow S = \mathbb{N}. \end{aligned}$$

Para finalizarmos a demonstração, provaremos que $X = \mathbb{N}$ usando novamente o axioma 2.2. Por hipótese $1 \in X$. Se $k \in X$, como acabamos de demonstrar $I_k \subset X$, pois $S = N$, segue que também temos $k + 1 \in X$, e assim $X = \mathbb{N}$ como queríamos demonstrar. □

Demonstração (Axioma 2.3 ⇒ Axioma 2.1). Suponhamos que exista um conjunto não vazío $S \subset \mathbb{N}$, tal que S não possui menor elemento. Façamos $X = \mathbb{N} \setminus S$. Como 1 é o menor número natural, logo $1 \in X$, pois se $1 \in S$ este seria o menor elemento de S, que é absurdo. Observemos que se $I_k \subset X$, então $k + 1 \in X$, pois caso contrário $k + 1$ seria o menor elemento de S, assim, pelo axioma 2.3 temos que $X = \mathbb{N}$. Mas isso é um absurdo, uma vez que implica em $S = \emptyset$, concluímos então que S deve possuir menor elemento. □

Na prática os princípio de indução finita são utilizados principalmente para demonstrar que determinadas propriedades são válidas para todo número natural.

Dado uma propriedade $p(n)$ referente a números naturais, um modo bastante difundido no meio matemático de utilizar o primeiro princípio de indução finita é verificando se $p(1)$ é verdadeira, e em seguida se o fato de que $p(k)$ ser verdadeira implica em que $p(k+1)$ também seja, isso é suficiente para demonstrarmos que $p(n)$ é verdadeira para todo número natural n. Isso é justificado ao considerarmos $X = \{x \in \mathbb{N} \mid p(x) \text{ é verdadeira}\}$ como o conjunto que desejamos provar que é o próprio conjunto dos números naturais. Analogamente ocorre com o segundo princípio de indução finita.

Veremos a seguir três exemplos práticos de demonstração por indução finita. Esses exemplos serão úteis para a demonstração do teorema 3.1 que veremos no próximo capítulo.

Exemplo 2.1. Usando o primeiro princípio de indução sobre n provaremos que a desigualdade $2n \leq 2^n$ verifica-se para todo $n \in \mathbb{N}$.

De fato a desigualdade vale para $n = 1$, pois $2 \cdot 1 \leq 2^1$.

Suponhamos que a desigualdade é válida para o natural $n = k$, isto é, $2k \leq 2^k$,

segue que

$$\begin{aligned} & 2k \leq 2^k \\ \Rightarrow \quad & 2k+2 \leq 2^k + 2^k \\ \Rightarrow \quad & 2(k+1) \leq 2^{k+1}, \end{aligned}$$

logo a desigualdade inicial também é válida para $n = k+1$ e assim fica provado por indução finita que é válida para todo n natural.

Exemplo 2.2. Provaremos usando o primeiro princípio de indução sobre n que a desigualdade $1 + 2n^2 < 2^{2n}$ vale para todo $n \in \mathbb{N}$.

A desigualdade pode ser verificada facilmente para $n = 1$, pois

$$1 + 2 \cdot 1^2 = 3 < 4 = 2^{2 \cdot 1}.$$

Supondo que é válida para o inteiro positivo $n = k$, temos válidas as inequações

$$1 + 2k^2 < 2^{2k}, \tag{1}$$

$$1 + 2k < 2^{2k} \text{ e} \tag{2}$$

$$1 + 2k < 2 \cdot 2^{2k}. \tag{3}$$

Somando as inequações (1), (2) e (3) membro a membro obtemos

$$\begin{aligned} 1 + 2k^2 + 4k + 2 &< 4 \cdot 2^{2k} \\ 1 + 2(k^2 + 2k + 1) &< 2^2 \cdot 2^{2k} \\ 1 + 2(k+1)^2 &< 2^{2(k+1)}, \end{aligned}$$

ou seja, a desigualdade inicial também vale para $n = k+1$, logo, por indução finita concluímos que $1 + 2n^2 < 2^{2n}$ para todo n natural.

Exemplo 2.3. Provaremos que $1 + (n+3)n < 2^{n+3}$ para todo $n \in \mathbb{N}$. De fato é verdade para $n = 1$, pois $1 + (1+3) \cdot 1 = 5 < 2^{1+3} = 16$.

Se a inequação é válida para o natural $n = k$, então

$$\begin{aligned} & 1 + (k+3)k = 1 + 3k + k^2 < 2^{k+3} \\ \Rightarrow \quad & 1 + 3k + k^2 + 4 < 2^{k+3} + 2 \cdot 2^k \\ \Rightarrow \quad & 1 + 3k + k^2 + 4 + 2k < 2^{k+3} + 2 \cdot 2^k + 6 \cdot 2^k \\ \Rightarrow \quad & 1 + 5k + k^2 + 4 < 2^{k+3} + 2^{k+3} \\ \Rightarrow \quad & 1 + (k+4)(k+1) < 2^{k+4}, \end{aligned}$$

assim, a inequação é válida para $n = k+1$, e pelo axioma 2.2 é válida para todo $n \in \mathbb{N}$.

2.2 Divisão euclidiana

Antes de apresentar a divisão euclidiana vamos definir divisibilidade no conjunto dos números inteiros ($\mathbb{Z}$).

Definição 2.1. *Sejam $a, n \in \mathbb{Z}$. Dizemos que a divide n, representado pela notação $a \mid n$, se existe $b \in \mathbb{Z}$ tal que $n = a \cdot b$. Se para todo inteiro b temos $n \neq a \cdot b$, dizemos que a não divide n e denotamos por $a \nmid n$.*

Decorre diretamente da definição de divisibilidade as seguintes propriedades:

Proposição 2.1. *Para $n, a, b \in \mathbb{Z}$, temos:*

i. $1 \mid n$.
ii. $n \mid 0$.
iii. $n \mid n$.
iv. $a \mid n \Rightarrow ab \mid nb$.
v. $ab \mid nb, b \neq 0 \Rightarrow a \mid n$.
vi. $a \mid n, n \neq 0 \Rightarrow |a| \leq |n|$.
vii. $a \mid n, n \mid a \Rightarrow |a| = |n|$.
viii. $a \mid b, b \mid n \Rightarrow a \mid n$.

Demonstração. (i) Escrevemos $n = 1 \cdot n$ e da definição temos que $1 \mid n$. (ii) De modo análogo escrevendo $0 = n \cdot 0 \Rightarrow n \mid 0$. (iii) Também $n = n \cdot 1 \Rightarrow n \mid n$.

(iv) Como $a \mid n$, por definição existe c inteiro tal que $n = a \cdot c$. Multiplicando ambos os membros da igualdade por b obtemos

$$n \cdot b = (a \cdot c) \cdot b = c \cdot (a \cdot b) \Rightarrow ab \mid nb.$$

(v) Por definição deve existir c inteiro tal que

$$\begin{aligned} & nb = c \cdot (ab) = (ac) \cdot b \\ \Rightarrow \quad & nb - (ac) \cdot b = 0 \\ \Rightarrow \quad & (n - ac) \cdot b = 0. \end{aligned}$$

Como $b \neq 0$, segue que

$$n - ac = 0 \Rightarrow n = ac,$$

logo $a \mid n$.

(vi) Como $a \mid n$, temos $n = a \cdot c$ para algum inteiro c. Já que $n \neq 0$, então

$|a| > 0$ e $|c| > 0$, logo

$$\begin{aligned} |n| &= |a \cdot c| \\ &= |a| \cdot |c| \\ &\geq |a|. \end{aligned}$$

(vii) Se $a = 0$, então $n = 0 \cdot c = 0$, ou seja, $|a| = |n| = 0$. Se $a \neq 0$, então devem existir $c_1, c_2 \in \mathbb{Z}$ tais que $n = ac_1$ e $a = nc_2$. Multiplicando ambos os membros da primeira igualdade por c_2 obtemos

$$\begin{aligned} & n \cdot c_2 = (ac_1) \cdot c_2 = a \cdot (c_1 c_2) = a \\ \Rightarrow \quad & c_1 c_2 = 1 \\ \Rightarrow \quad & |c_1| \cdot |c_2| = 1, \end{aligned}$$

logo $|c_1| = |c_2| = 1$, e assim

$$\begin{aligned} & n = a \cdot c_1 \\ \Rightarrow \quad & |n| = |a| \cdot |c_1| \\ \Rightarrow \quad & |n| = |a|. \end{aligned}$$

(viii) Da hipótese devem existir inteiros c_1 e c_2 tais que $b = a \cdot c_1$ e $n = b \cdot c_2$, logo substituindo $b = a \cdot c_1$ na segunda igualdade obtemos

$$n = (a \cdot c_1) \cdot c_2 \Rightarrow n = a \cdot (c_1 \cdot c_2) \Rightarrow a \mid n.$$

□

Proposição 2.2. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid (b + c)$, então $a \mid b$ se, e somente se, $a \mid c$.*

Demonstração. Se $a \mid (b + c)$, logo existe $p \in \mathbb{Z}$ tal que $b + c = ap$. De mesmo modo, se $a \mid b$, então existe $q \in \mathbb{Z}$ tal que $b = aq$. Substituindo $b = aq$ na primeira igualdade obtemos

$$aq + c = ap \Rightarrow c = a(p - q),$$

ou seja, $a \mid c$. A outra parte da demonstração pode ser feita de modo totalmente análogo.

□

Proposição 2.3. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $a \mid c$, então*

$$a \mid (xb + yc), \forall x, y \in \mathbb{Z}.$$

Demonstração. Sejam $p, q \in \mathbb{Z}$ tais que $b = ap$ e $c = aq$. Segue que

$$xb + yc = x(ap) + y(aq) = a(xp + yq),$$

ou seja, $a \mid (xb + yc)$. □

Vejamos mais um exemplo de demonstração por indução finita. Usaremos também o resultado da proposição anterior. Este exemplo será importante na demonstração do teorema de Lagrange (teorema 2.20) que veremos mais a frente neste trabalho.

Exemplo 2.4. Dados $a, b \in \mathbb{Z}$ provaremos utilizando indução sobre n que

$$a - b \mid a^n - b^n, \forall n \in \mathbb{N}.$$

O resultado é válido trivialmente no caso $n = 1$, pois $a - b \mid a - b$ (item iii da proposição 2.1). Suponhamos que o resultado seja válido para o inteiro positivo $n = k$, isto é, $a - b \mid a^k - b^k$. Segue que

$$\begin{aligned} a^{k+1} - b^{k+1} &= a \cdot a^k - b \cdot b^k \\ &= a \cdot a^k - b \cdot a^k + b \cdot a^k - b \cdot b^k \\ &= a^k(a - b) + b(a^k - b^k). \end{aligned}$$

Como por hipótese de indução $a - b \mid a^k - b^k$ e por termos $a - b \mid a - b$, segue pela proposição 2.3 que

$$\begin{aligned} & a - b \mid a^k(a - b) + b(a^k - b^k) \\ \Rightarrow \quad & a - b \mid a^{k+1} - b^{k+1}. \end{aligned}$$

Assim, o resultado é válido para $n = k + 1$, e por indução concluímos que vale para todo $n \in \mathbb{N}$.

O próximo teorema é devido a Euclides e é conhecido como algoritmo de divisão. Na prática este teorema garante a existência e a unicidade de um quociente q e um resto r na divisão de dois inteiros quaisquer, que são elementos importantes para a resolução de diversos problemas básicos de aritmética, e por isso existem algoritmos muitos conhecidos que são vistos nas escolas durante o ensino fundamental usados para encontrar estes dois números quando são dados dois inteiros, sendo um deles diferente de zero.

Teorema 2.1 (Algoritmo de divisão)**.** *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, existem dois únicos inteiros q e r tais que $b = aq + r$, com $0 \leq r < |a|$.*

Demonstração. Primeiramente demonstraremos a existência de q e r. Se $a \mid b$, por definição existe $q \in \mathbb{Z}$ tal que $b = aq = aq + 0$, com $0 = r < |a|$. Se $a \nmid b$, então $\forall x \in \mathbb{Z}$

temos $b \neq ax$, logo $b - ax \neq 0$. Consideremos o conjunto

$$S = \{y \in \mathbb{N} |\ y = b - ax,\ \text{para } x \in \mathbb{Z}\}.$$

Como S é formado por inteiros positivos, pelo princípio da boa ordem (axioma 2.1) este conjunto possui um menor elemento r. Façamos $r = b - aq$, onde $q \in \mathbb{Z}$ e vamos mostrar que $r < |a|$.

Vejamos que $r \neq |a|$, pois

$$r = |a| \Rightarrow |a| = b - aq \Rightarrow b = a(q+1) \text{ ou } b = a(q-1)$$

que é absurdo uma vez que $a \nmid b$. Suponhamos então que $r > |a|$, logo $r = |a| + s$, para algum inteiro s tal que $0 < s < r$. Segue que

$$s = r - |a| = b - aq - |a| \Rightarrow s = b - a(q+1) \text{ ou } s = b - a(q-1),$$

ou seja, $s \in S$. Mas isso é absurdo, pois r é o menor elemento de S e $s < r$, assim $r < |a|$.

Agora demonstraremos a unicidade de q e r. Suponhamos que $b = aq_1 + r_1 = aq_2 + r_2$, com $q_1, q_2, r_1, r_2 \in \mathbb{Z}, 0 \leq r_1 < |a|$ e $0 \leq r_2 < |a|$. Sem perca de generalidade suponhamos que $r_1 \leq r_2$. Segue que

$$aq_1 + r_1 - (aq_2 + r_2) = 0 \Rightarrow a(q_1 - q_2) = r_2 - r_1 \Rightarrow a \mid r_2 - r_1.$$

Se $r_2 - r_1 \neq 0$, pelo item vi da proposição 2.1 teremos

$$|a| \leq |r_2 - r_1| = r_2 - r_1 \Rightarrow r_2 < r_2 - r_1 \Rightarrow r_1 + r_2 < r_2 \Rightarrow r_1 < 0,$$

absurdo, logo

$$r_2 - r_1 = 0 \Rightarrow r_2 = r_1, \text{ e}$$

$$a(q_1 - q_2) = 0 \Rightarrow q_1 - q_2 = 0 \Rightarrow q_1 = q_2$$

provando a unicidade de q e r. □

Exemplo 2.5. Provaremos que se a é um número inteiro ímpar, então $8 \mid a^2 - 1$. Notemos primeiramente que $a^2 - 1 = (a+1)(a-1)$. Pela divisão euclidiana (teorema 2.1) temos apenas 4 possibilidade para o resto da divisão de $a - 1$ por 4

$$a - 1 = 4k,\ \text{ou } a - 1 = 4k + 1,\ \text{ou } a - 1 = 4k + 2,\ \text{ou } a - 1 = 4k + 3,$$

para algum $k \in \mathbb{Z}$. Como a é ímpar temos que $a + 1$ e $a - 1$ são ambos pares, e daí

$$a - 1 \neq 4k + 1 \text{ e } a - 1 \neq 4k + 3,\ \forall k \in \mathbb{Z}.$$

Se $a-1=4k+2$ para algum inteiro k, então

$$\begin{aligned} a-1+2 &= 4k+2+2 \\ a+1 &= 4(k+1) \\ &\Rightarrow 4 \mid a+1. \end{aligned}$$

Assim, existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$\begin{aligned} & a+1=4k_1 \text{ e } a-1=2k_2 \\ \Rightarrow\ & (a+1)(a-1)=4k_1 \cdot 2k_2 \\ \Rightarrow\ & a^2-1=8k_1k_2 \\ \Rightarrow\ & 8 \mid a^2-1. \end{aligned}$$

Se $a-1=4k$ para algum inteiro k, como $a+1$ é par, então existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$\begin{aligned} & a-1=4k_1 \text{ e } a+1=2k_2 \\ \Rightarrow\ & (a-1)(a+1)=4k_1 \cdot 2k_2 \\ \Rightarrow\ & a^2-1=8k_1k_2 \\ \Rightarrow\ & 8 \mid a^2-1. \end{aligned}$$

2.3 Teorema fundamental da aritmética

Os números naturais em geral podem ser tratados como produtos de fatores primos, e além disto, para cada número existe uma única fatoração a menos que a ordem. Esta propriedade é de extrema importância para a teoria dos números e conhecida como o teorema fundamental da aritmética e devida a Euclides.

Temos por objetivo neste momento a demonstração deste teorema, e para isso apresentaremos uma série de propriedades e algumas definições, dentre elas, a definição de máximo divisor comum, que pode ser encontrada no livro VII de Os elementos de Euclides e que veremos a seguir.

Definição 2.2. *Sejam $a, b \in \mathbb{Z}$ não ambos nulos. Chamaremos de máximo divisor comum de a e b o maior inteiro d tal que $d \mid a$ e $d \mid b$. Denotaremos o máximo divisor de a e b por (a, b).*

Teorema 2.2. *Se $d=(a,b)$, então existem $x, y \in \mathbb{Z}$ tais que $d=ax+by$.*

Demonstração. Seja S o conjunto formado por todos os números naturais da forma $an+bm$, onde $n, m \in \mathbb{Z}$. Suponhamos sem perca de generalidade que $a \leq b$. É óbvio que $|b| \in S$, pois $b=a \cdot 0+b \cdot 1$ e $-b=a \cdot 0+b \cdot (-1)$, logo $S \neq \emptyset$ e pelo axioma 2.1 este

possui menor elemento $c = an_0 + bm_0$.

Suponhamos agora que $c \nmid a$, então devem existir $q, r \in \mathbb{Z}$ tais que $a = cq + r$ com $0 < r < c$. Assim $r = a - cq = a - (an_0 + bm_0)q = a(1 - n_0q) + b(-m_0q)$, portanto $r \in S$, que é absurdo uma vez que c é menor elemento de S. Logo $c \mid a$ e de modo análogo podemos mostrar facilmente que $c \mid b$. Isso nos garante que c é divisor comum de a e b.

Como $d \mid a$ e $d \mid b$, existem então $q_1, q_2 \in \mathbb{Z}$ tais que $a = dq_1$ e $b = dq_2$, que implica em

$$\begin{aligned} c &= an_0 + bm_0 \\ &= dq_1n_0 + dq_2m_0 \\ &= d(q_1n_0 + q_2m_0) \\ &\Rightarrow d \mid c. \end{aligned}$$

Assim, como c e d são inteiros positivos, segue pelo item vi da proposição 2.1 que $d \leq c$, mas como d é o maior divisor comum de a e b, então

$$d = c = an_0 + bm_0.$$

□

Notemos que na demonstração anterior, ao provarmos que $d = c$, estamos também provando que d é o menor número não negativo da forma $ax + by$ para todos $x, y \in \mathbb{Z}$, é o que nos diz o corolário a seguir.

Corolário 2.1. *Se $d = (a, b)$, então d é o menor número natural da forma $n = ax + by$, com $x, y \in \mathbb{Z}$*

Demonstração. A prova está inclusa na demonstração do teorema 2.2. □

Proposição 2.4. *Dados $k \in \mathbb{N}$ e $a, b \in \mathbb{Z}$ tem-se $(ka, kb) = k(a, b)$.*

Demonstração. Sejam $S_1 = \{x \in \mathbb{N} |\ x = an + bm, \text{ para } n, m \in \mathbb{Z}\}$ e $S_2 = \{x \in \mathbb{N} |\ x = (ka)n + (kb)m, \text{ com } n, m \in \mathbb{Z}\}$. Pelo corolário 2.1, (a, b) é o menor elemento de S_1, onde $(a, b) = an_0 + bm_0$ para algum $n_0, m_0 \in \mathbb{Z}$. Assim, $k(a, b) = kan_0 + kbm_0$ é o menor elemento de S_2, ou seja, $(ka, kb) = k(a, b)$. □

Proposição 2.5. *Dado $c \in \mathbb{N}$, se $c \mid a$ e $c \mid b$, então*

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

Demonstração. Se $c \mid a$ e $c \mid b$, então $\frac{a}{c}, \frac{b}{c} \in \mathbb{Z}$. Logo, da proposição 2.4 segue que

$$c\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{ca}{c}, \frac{cb}{c}\right) = (a, b) \Rightarrow \left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a, b)}{c}$$

□

Corolário 2.2. *Se $d = (a, b)$, então* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Demonstração. Da proposição anterior (proposição 2.5) temos que

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d} = \frac{d}{d} = 1$$

□

Teorema 2.3. *Seja $d = (a, b)$. Se c é divisor comum de a e b, então $c \mid d$.*

Demonstração. Pelo teorema 2.2 existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$. Se $c \mid a$ e $c \mid b$, então pela proposição 2.3

$$c \mid ax + by \Rightarrow c \mid d.$$

□

Teorema 2.4. $(a, b) = (a, b + an)\ \forall a, b \in \mathbb{Z}$.

Demonstração. Fazendo $d_1 = (a, b)$ e $d_2 = (a, b + an)$, existem $p, q \in \mathbb{Z}$ tais que $a = d_2 p$ e $b + an = d_2 q$. Segue que

$$\begin{aligned} b &= d_2 q - an \\ &= d_2 q - d_2 pn \\ &= d_2(q - pn) \\ &\Rightarrow d_2 \mid b. \end{aligned}$$

Como $d_2 \mid a$ e $d_2 \mid b$, pelo teorema 2.3 $d_2 \mid d_1$.

Provaremos agora que $d_1 \mid d_2$. Já que $d_1 \mid a$ e $d_1 \mid b$, pela proposição 2.3 $d_1 \mid b + an$, ou seja, d_1 é divisor comum de a e $b + an$, logo, novamente pelo teorema 2.3, $d_1 \mid d_2$. Por $d_1, d_2 \in \mathbb{N}$ concluímos pelo item vii da proposição 2.1 que $d_1 = d_2$. □

O teorema anterior é bem útil para se calcular o máximo divisor comum de dois inteiros quaisquer, e o mais interessante é que fazendo uso deste teorema não necessariamente precisamos conhecer os divisores destes dois números. Euclides usou este teorema para demonstrar de maneira construtiva a existência do máximo divisor comum, sobre este método Hefez (2014, p. 89) relata: "O método, chamado de *Algoritmo de Eu-*

clides, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios."

Uma demonstração desse teorema pode vista em SANTOS (2007, p. 8) e a demonstração dada por Euclides pode ser encontrada na tradução de Os elementos: (EUCLIDES, 2009, p. 271).

Definição 2.3. *Dizemos que a e b são primos entre si quando $(a, b) = 1$.*

Teorema 2.5. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração. Se $(a, b) = 1$, então pelo teorema 2.2 devem existir $n, m \in \mathbb{Z}$ tais que $an + bm = 1$. Multiplicando ambos os membros desta equação por c obtemos

$$n(ac) + m(bc) = c.$$

Se $a \mid bc$, logo existe $q \in \mathbb{Z}$ tal que $bc = aq$, assim

$$\begin{aligned} & n(ac) + m(bc) = c \\ \Rightarrow \quad & n(ac) + m(aq) = c \\ \Rightarrow \quad & a(nc + mq) = c \\ \Rightarrow \quad & a \mid c. \end{aligned}$$

□

O teorema a seguir é essencialmente uma versão mais específica do teorema 2.4 e será exposto para utilização mais didática em algumas demonstrações.

Teorema 2.6. *Sejam $a, b \in \mathbb{Z}$. Se $a = bq + r$ com q e r inteiros, então $(a, b) = (b, r)$*

Exemplo 2.6. Vamos calcular o máximo divisor comum de 2431 e 988. Aplicando sucessivas vezes o teorema 2.6 obtemos

$$\begin{aligned} (2431, 988) &= (2 \cdot 988 + 455, 988) \\ &= (988, 455) \\ &= (2 \cdot 455 + 78, 455) \\ &= (455, 78) \\ &= (5 \cdot 78 + 65, 78) \\ &= (78, 65) \\ &= (1 \cdot 65 + 13, 65) \\ &= (65, 13) \\ &= (5 \cdot 13 + 0, 13) \\ &= (13, 0) \\ &= 13. \end{aligned}$$

Demonstração. Inicialmente escrevemos $r = a - bq$. Observamos que $(a, b) = (b, a)$, e pelo teorema 2.4

$$(b, a) = (b, a - bq) = (b, r).$$

Logo $(a, b) = (b, r)$. □

Definição 2.4. *Dizemos que um número inteiro $p > 1$ é primo se este possui apenas dois divisores positivos, 1 e p. Se $n > 1$ não é primo, então dizemos que n é composto. Denotaremos o conjunto dos números primos por $\mathbb{P}$.*

Proposição 2.6. *Dados $p \in \mathbb{P}$ e $a, b \in \mathbb{Z}$, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \mid a$ não há nada o que se demonstrar. Suponhamos então que $p \nmid a$, logo $(p, a) = 1$ e pelo teorama 2.5 concluimos que $p \mid b$. □

Corolário 2.3. *Dados $p \in \mathbb{P}$ e $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, se $p \mid a_1 a_2 \cdots a_r$, então $p \mid a_i$ para algum $i \in \{1, 2, \ldots, r\}$.*

Demonstração. Se $p \mid a_r$ a demonstração esta feita. Suponhamos então que $p \nmid a_r$, logo pela proposição anterior (proposição 2.6) $p \mid a_1 a_2 \cdots a_{r-1}$. Se $p \mid a_{r-1}$ novamente a demonstração estaria finalizada. Supondo que $p \nmid a_{r-1}$, teremos novamente pela proposição 2.6 que $p \mid a_1 a_2 \cdots a_{r-2}$. Continuando o mesmo processo, por estarmos considerando um conjunto finito de inteiros, em algum momento este processo deve acabar, ou seja, um dos números $a_1, a_2, \ldots, a_r$ é divisível por p. □

Com o que foi apresentado até aqui, podemos agora demonstrar o teorema fundamental da aritmética de Euclides. Este é composto por duas partes: a existência, e a unicidade da fatoração de um inteiro positivo em em um produto de primos. Em uma tradução da obra Os elementos a existência da fatoração é enunciada assim: "Todo número ou é primo ou é medido por algum número primo."(EUCLIDES, 2009, p. 292). Podemos interpretar a palavra "medido" fazendo o papel do termo "divisível" usado na linguagem moderna.

Teorema 2.7 (Teorema fundamental da aritmética)**.** *Dado $n \in \mathbb{N}$, existe uma única maneira (a menos da ordem) de representá-lo como o produto de fatores primos.*

Demonstração. O teorema é válido de forma trivial para todo $n \in \mathbb{P}$. Provaremos então para n composto e faremos primeiramente a demonstração da existência da fatoração.

Seja $q_1 > 1$ o menor divisor de n, de fato este é primo, pois se $q \mid q_1$ e $1 \leq q < q_1$, então $q \mid n$, logo $q = 1$. Como n é composto temos $n = q_1 n_1$, para algum $n_1 > 1$. Se $n_1 \in \mathbb{P}$, então a fatoração existe. Se n_1 é composto tomamos $q_2 > 1$ o seu menor divisor, e como já vimos, este também é primo. Logo $n_1 = q_2 n_2$ com $n_2 > 1$.

Repetimos o processo e obtemos $n_1 > n_2 > \ldots > n_r$, e como estes números são todos inteiros maiores do que 1, então o processo deve finalizar com $n_r = q_r$ primo, logo $n = q_1 q_2 \ldots q_r$, onde não necessariamente temos primos $q_1, q_2, \ldots, q_r$ distintos, assim,

em geral podemos escrever

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, \text{com } p_i \in \mathbb{P} \text{ para } i = 1, \dots, k.$$

Agora mostraremos a unicidade da fatoração usando o segundo princípio de indução finita (axioma 2.3). Seja

$$S = \{x \in \mathbb{N} \mid x = 1 \text{ ou } x \text{ possui fatoração única em potências de primos}\}.$$

Obviamente que $1 \in S$.

Suponhamos que $I_k \subset S$. Se $k+1 \in \mathbb{P}$, então $I_{k+1} \subset S$ e a demonstração estará concluída. Se $k+1$ é composto, supomos que hajam duas fatorações

$$k+1 = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

onde $p_i, q_j \in \mathbb{P}$ para $i = 1, \dots, r$ e $j = 1, \dots, s$. Como $p \mid q_1 q_2 \dots q_s$ pelo corolário 2.3 p_1 divide algum q_j, sem perca de generalidade digamos que $p_1 \mid q_1$, logo $p_1 = q_1$. Assim

$$\frac{k+1}{p_1} = p_2 \dots p_r = q_2 \dots q_s$$

tem fatoração única pois $\dfrac{k+1}{p_1} < k+1 \Rightarrow \dfrac{k+1}{p_1} \in S$. Segue que $r = s$ e as duas fatorações $p_1 p_2 \dots p_r$ e $q_1 q_2 \dots q_s$ são iguais a menos da ordem, ou seja,

$$k+1 \in S \Rightarrow I_{k+1} \subset S \Rightarrow S = \mathbb{N}.$$

□

O teorema a seguir será usado juntamente com o teorema fundamental da aritmética, que acabamos de provar, na demonstração do teste 1 que veremos no próximo capítulo deste trabalho.

Teorema 2.8. *Se n é um número natural composto, então existe um primo $p \leq \sqrt{n}$ tal que $p \mid n$.*

Demonstração. Como n é um número natural composto, então existem $n_1, n_2 \in \mathbb{N}$ tais que $n = n_1 n_2$ onde

$$1 < n_1 \leq n_2 < n.$$

Suponhamos por absurdo que $n_1 > \sqrt{n}$, logo

$$n = n_1 n_2 > \sqrt{n} \cdot \sqrt{n} = n,$$

absurdo, assim $n_1 \leq \sqrt{n}$.

Pelo teorema fundamental da aritmética (teorema 2.7), n_1 pode ser escrito como o produto de fatores primos, assim, tomando p primo tal que $p \mid n_1$, teremos pelos itens vi e viii da proposição 2.1 que $p \leq n_1 \leq \sqrt{n}$ onde $p \mid n$. □

2.4 Congruência

A seguir veremos a definição de congruência módulo um inteiro n e algumas das propriedades básicas decorrente desta. Elas serão necessárias para demonstrarmos alguns dos próximos teoremas presentes neste trabalho, como por exemplo o pequeno teorema de Fermat e os teoremas de Wilson e de Euler.

Os resultados que veremos são devidos a Carl Friedrich Gauss (1777-1855) e foram apresentados em seu trabalho *Disquisitiones Arithmeticae* (Investigações de Aritmética) publicado em 1801. Sobre esse trabalho Santos (2007) fala: "Várias ideias de grande importância, que serviram de base para o desenvolvimento da teoria dos números, aparecem neste trabalho."(SANTOS, 2007, p. 32).

Definição 2.5. *Dados $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, dizemos que a é congruente a b módulo n se $n \mid a - b$. Representamos isto por*

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

Se $n \nmid a - b$, então dizemos que a é incongruente a b módulo n e denotamos por

$$a \not\equiv b \pmod{n}.$$

Exemplo 2.7. Como $45 = 3 \cdot 13 + 6$, logo $13 \mid 45 - 6$ e assim, $45 \equiv 6 \pmod{13}$.

Proposição 2.7. *$a \equiv b \pmod{n}$ se, e somente se, existe $q \in \mathbb{Z}$ tal que*

$$a = b + qn.$$

Demonstração. Considerando a definição temos as seguintes equivalências

$$\begin{aligned} a \equiv b \pmod{n} &\Leftrightarrow n \mid a - b \\ &\Leftrightarrow \exists\, q \in \mathbb{Z} \text{ tal que } a - b = qn \\ &\Leftrightarrow \exists\, q \in \mathbb{Z} \text{ tal que } a = b + qn. \end{aligned}$$

□

Proposição 2.8. *Seja m um divisor positivo de $n \in \mathbb{N}$. Se $a \equiv b \pmod{n}$, então*

$$a \equiv b \pmod{m}.$$

Demonstração. Se $a \equiv b \pmod{n}$, então $n \mid a - b$. Como $m \mid n$ temos pelo item viii da proposição 2.1 que $m \mid a - b$, logo $a \equiv b \pmod{m}$. □

Proposição 2.9. *Dados $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$, são verdadeiras as sentenças:*

i: $a \equiv a \pmod{n}$*;*

ii: $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$*;*

iii: $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Demonstração. (i) Como $n \mid 0$, logo $n \mid a - a$ e consequentemente $a \equiv a \pmod{n}$. (ii) Se $a \equiv b \pmod{n}$, da proposição 2.7 existe $q \in \mathbb{Z}$ tal que

$$a = b + qn \Rightarrow b = a + (-q)n,$$

assim, também pela proposição 2.7 temos que $b \equiv a \pmod{n}$. (iii) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $n \mid (a - b)$ e $n \mid (b - c)$. Usando a proposição 2.3 obtemos

$$n \mid (a - b) + (b - c) \Rightarrow n \mid a - c.$$

Logo $a \equiv c \pmod{n}$. □

Teorema 2.9. *Dados $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $a \equiv b \pmod{n}$, então:*

i: $a + c \equiv b + c \pmod{n}$*;*

ii: $ac \equiv bc \pmod{n}$.

Demonstração. (i) Como $a \equiv b \pmod{n}$, temos que

$$n \mid (a - b) \Rightarrow n \mid (a + c) - (b + c) \Rightarrow a + c \equiv b + c \pmod{n}.$$

(ii) Como $a \equiv b \pmod{n}$, segue que

$$n \mid (a - b) \Rightarrow n \mid (a - b) \cdot c \Rightarrow n \mid ac - bc \Rightarrow ac \equiv bc \pmod{n}.$$

□

Teorema 2.10. *Dados $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$, com $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:*

i: $a + c \equiv b + d \pmod{n}$*;*

ii: $ac \equiv bd \pmod{n}$.

Demonstração. (i) Como $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $a - b = k_1 n$ e $c - d = k_2 n$. Somando as duas últimas equações membro a membro

obtemos

$$\begin{aligned} & (a+c)-(b+d) = (k_1+k_2)n \\ \Rightarrow \quad & n \mid (a+c)-(b+d) \\ \Rightarrow \quad & a+c \equiv b+d \pmod{n}. \end{aligned}$$

(ii) Sejam $a = b + k_1 n$ e $c + k_2 n = d$ para $k_1, k_2 \in \mathbb{Z}$. Multiplicando membro a membro as duas últimas equações obtemos

$$\begin{aligned} & ac + ak_2 n = bd + dk_1 n \\ \Rightarrow \quad & ac - bd = (dk_1 - ak_2)n \\ \Rightarrow \quad & n \mid ac - bd \\ \Rightarrow \quad & ac \equiv bd \pmod{n}. \end{aligned}$$

□

2.5 O pequeno teorema de Fermat

As propriedades que seguem serão utilizadas na demonstração do pequeno teorema de Fermat. Usaremos também a definição de sistema completo de resíduos módulo n (definição 2.6).

Teorema 2.11. *Sejam $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$. Se $ac \equiv bc \pmod{n}$ e $d = (c, n)$, então*

$$a \equiv b \pmod{n/d}.$$

Demonstração. Da hipótese obtemos $ac - bc = c(a-b) = kn$ para algum $k \in \mathbb{Z}$. Segue que

$$c(a-b) = kn \Rightarrow \frac{c}{d} \cdot (a-b) = k \cdot \frac{n}{d},$$

logo $\frac{n}{d} \mid \frac{c}{d} \cdot (a-b)$ uma vez que $\frac{n}{d}, \frac{c}{d} \in \mathbb{Z}$. Do corolário 2.2 temos que $\left(\frac{n}{d}, \frac{c}{d}\right) = 1$, assim, pelo teorema 2.5

$$\frac{n}{d} \mid a-b \Rightarrow a \equiv b \pmod{n/d}.$$

□

Corolário 2.4. *Sejam $a, b, c \in \mathbb{Z}$ e $p \in \mathbb{P}$. Se $ac \equiv bc \pmod{p}$ e $p \nmid c$, então temos que $a \equiv b \pmod{p}$.*

Demonstração. Nas condições da hipótese temos que $(p, c) = 1$. Aplicando o teorema anterior (teorema 2.11) terminamos a demonstração. □

Definição 2.6. *Dado um número n natural, chamamos de sistema completo de resíduos módulo n todo conjunto com n elementos dois a dois incongruentes módulo n.*

Teorema 2.12. *Seja* $S = \{s_1, s_2, \ldots, s_n\}$ *um sistema completo de resíduos módulo n. Dado* $m \in \mathbb{N}$*, existe um único* $s_i \in S$ *tal que* $s_i \equiv m \pmod{n}$.

Demonstração. Pelo teorema 2.1 podemos escrever

$$\begin{aligned} s_1 - m &= q_1 n + r_1, \\ s_2 - m &= q_2 n + r_2, \\ &\vdots \\ s_n - m &= q_n n + r_n, \end{aligned}$$

com $0 \leq r_i < n$ para $i = 1, 2, \ldots, n$.

Suponhamos que $r_k = r_j$ para algum $k \neq j$, segue que

$$s_k - m - q_k n = s_j - m - q_j n \Rightarrow s_k - s_j = q_k n - q_j n = (q_k - q_j)n,$$

assim

$$n \mid s_k - s_j \Rightarrow s_k \equiv s_j \pmod{n},$$

absurdo, pois os elementos de S são incongruentes dois a dois. Logo $r_1, r_2, \ldots, r_n$ são inteiros positivos distintos e menores que n e assim, algum r_t dentre eles deve ser igual a zero, ou seja,

$$s_t - m = q_t n \Rightarrow n \mid s_t - m \Rightarrow s_t \equiv m \pmod{n}.$$

□

O próximo teorema trata-se do pequeno teorema de Fermat, e é na verdade um caso particular do teorema de Euler (teorema 2.18).

Sabe-se que "esse teorema [...] foi apenas enunciado por Fermat numa carta de 18 de outubro de 1640 a Frénicle de Bessy. A primeira demonstração publicada desse teorema data de 1736 e é devida a Euler."(EVES, 2002, p. 391).

Teorema 2.13 (Pequeno teorema de Fermat)**.** *Sejam* $p \in \mathbb{P}$ *e* $a \in \mathbb{Z}$*. Se* $p \nmid a$*, então* $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração. Consideremos o conjunto

$$S = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

Se $p \nmid a$, então $(p, a) = 1$. Suponhamos que p seja divisor de algum elemento de S, digamos $p \mid ia$, logo pelo teorema 2.5 teríamos $p \mid i$, absurdo, ou seja, nenhum elemento de S é congruente a zero módulo p.

Do corolário 2.4, temos que

$$\begin{aligned} & 1 \leq j \leq k \leq p-1,\, aj \equiv ak \pmod{p} \\ \Rightarrow\ & j \equiv k \pmod{p} \\ \Rightarrow\ & p \mid j-k \\ \Rightarrow\ & j-k=0 \\ \Rightarrow\ & j=k. \end{aligned}$$

Concluímos que os elementos de S são incongruentes dois a dois, e assim, cada elemento desse conjunto é congruente a apenas um dos números $1, 2, \ldots, p-1$. Multiplicando essas $p-1$ congruências membro a membro obtemos

$$\begin{aligned} a \cdot 2a \cdot 3a \cdots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p}. \end{aligned}$$

Como $((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ de ambos os membros da última congruência (usando o corolário 2.4) e obtermos $a^{p-1} \equiv 1 \pmod{p}$. □

Corolário 2.5. *Se $p \in \mathbb{P}$ e $a \in \mathbb{Z}$ com $a \geq 0$, então $a^p \equiv a \pmod{p}$.*

Demonstração. Se $p \nmid a$, então $(a, p) = 1$, e pelo teorema anterior temos

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

Multiplicando ambos os membros da congruência por a obtemos

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

Suponhamos agora que $p \mid a$, logo $a \equiv 0 \pmod{p}$. Aplicando o item ii do teorema 2.10 $p-1$ vezes obtemos

$$\begin{aligned} a \cdot a \cdots a &\equiv 0 \cdot 0 \cdots 0 \pmod{p} \\ a^p &\equiv 0 \pmod{p}, \end{aligned}$$

assim,

$$a^p \equiv 0 \equiv a \pmod{p}.$$

□

2.6 Teorema de Wilson

O teorema a seguir apresenta a condição necessária e suficiente para a existência de soluções no conjunto dos números inteiros para uma equação da forma

$$ax + by = c$$

dados os inteiros a, b e c, isto é, a existência de $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = c$. Essas equações são conhecidas como equações diofantinas lineares em homenagem ao matemático Diofanto (300 d.C.) de Alexandria (HEFEZ, 2014). O teorema ainda apresenta uma maneira de gerar outras soluções quando se é conhecido uma solução particular.

Teorema 2.14. *Sejam $a, b, c \in \mathbb{Z}$ e $d = (a, b)$. São válidas as afirmações*

i: Existem $x, y \in \mathbb{Z}$ tais que $ax + by = c$ se, e somente se, $d \mid c$.

ii: Se $x = x_0$ e $y = y_0$ é uma solução particular de $ax + by = c$, então as soluções desta equação são da forma

$$x = x_0 + \frac{bt}{d}$$
$$y = y_0 - \frac{at}{d}$$

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

Demonstração. (i) Como $d \mid a$ e $d \mid b$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = dk_1$ e $b = dk_2$, logo, se $ax + by = c$ temos que

$$\begin{aligned} ax + by &= dk_1x + dk_2y \\ &= d(k_1x + k_2y) \\ &= c \\ &\Rightarrow \; d \mid c. \end{aligned}$$

Por outro lado, se $d \mid c$, então $c = dk$ para algum k inteiro. Pelo teorema 2.2 existem $n, m \in \mathbb{Z}$ tais que $an + bm = d$. Multiplicando ambos os membros desta última igualdade por k obtemos

$$ank + bmk = dk = c,$$

e para $x = nk$ e $y = mk$ teremos $ax + by = c$.

(ii) Se $x = x_0$ e $y = y_0$ é uma solução particular de $ax + by = c$, então

$$\begin{aligned} a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{at}{d}\right) &= ax_0 + \frac{abt}{d} + by_0 - \frac{abt}{d} \\ &= ax_0 + by_0 \\ &= c, \end{aligned}$$

ou seja,

$$x = x_0 + \frac{bt}{d}$$
$$y = y_0 - \frac{at}{d}$$

é solução de $ax + by = c$.

Provaremos agora que toda solução da equação é desta forma. Suponhamos que $x = x_1$ e $y = y_1$ seja uma solução da equação, isto é,

$$ax_1 + by_1 = c. \tag{4}$$

Subtraindo membro a membro esta última equação por $ax_0 + by_0 = c$ teremos

$$\begin{aligned} & ax_1 + by_1 - ax_0 - by_0 = c - c \\ \Rightarrow \quad & a(x_1 - x_0) + b(y_1 - y_0) = 0, \end{aligned}$$

logo

$$\begin{aligned} & a(x_1 - x_0) = b(y_0 - y_1) \\ \Rightarrow \quad & \frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1). \end{aligned}$$

Assim $\frac{b}{d} \mid \frac{a}{d}(x_1 - x_0)$, e como $\left(\frac{b}{d}, \frac{a}{d}\right) = 1$ (corolário 2.2), pelo teorema 2.5 temos que $\frac{b}{d} \mid x_1 - x_0$, isto é, existe $t \in \mathbb{Z}$ tal que

$$x_1 - x_0 = \frac{bt}{d} \Rightarrow x_1 = x_0 + \frac{bt}{d}.$$

Finalizamos a demonstração substituindo $x_1 = x_0 + \frac{bt}{d}$ em (4) para obtermos

$$\begin{aligned} a\left(x_0 + \frac{bt}{d}\right) + by_1 &= ax_0 + by_0 \\ \frac{abt}{d} + by_1 &= by_0 \\ \frac{at}{d} + y_1 &= y_0 \\ y_1 &= y_0 - \frac{at}{d}. \end{aligned}$$

□

Exemplo 2.8. Mostraremos usando o teorema 2.14 que dados $a, b, c \in \mathbb{Z}$, temos que

$$(ab, c) = 1 \Leftrightarrow (a, c) = (b, c) = 1.$$

Se $(ab, c) = 1$, então existe $x_0, y_0 \in \mathbb{Z}$ tais que $abx_0 + cy_0 = 1$ (teorema 2.2). notemos que $x = bx_0$ e $y = y_0$ é solução de $ax + cy = 1$, logo pelo teorema 2.14

$$(a, c) \mid 1 \Rightarrow (a, c) = 1.$$

Analogamente, $x = ax_0$ e $y = y_0$ é solução de $bx + cy = 1$, assim $(b, c) = 1$.

Para provarmos a recíproca, consideremos $(a, c) = (b, c) = 1$. Logo, segue pelo teorema 2.2 que existem $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ tais que

$$\begin{aligned} ax_1 + cy_1 &= 1 \\ bx_2 + cy_2 &= 1. \end{aligned}$$

Multiplicando membro a membro estas duas equações obtemos

$$\begin{aligned} & ax_1bx_2 + ax_1cy_2 + cy_1bx_2 + c^2y_1y_2 = 1 \\ \Rightarrow \quad & ab(x_1x_2) + c(ax_1y_2 + by_1x_2 + cy_1y_2) = 1, \end{aligned}$$

assim, novamente pelo teorema 2.14 temos que

$$(ab, c) \mid 1 \Rightarrow (ab, c) = 1,$$

finalizando nossa demonstração.

O teorema a seguir apresenta uma condição necessária para que uma congruência do tipo

$$ax \equiv b \pmod{n}, \text{ com } a, b \in \mathbb{Z} \text{ e } n \in \mathbb{N}$$

possua solução no conjunto dos números inteiros, isto é, que exista x_0 inteiro tal que $ax_0 \equiv b \pmod{n}$.

Tais congruências são conhecidas como congruências lineares, e como veremos na demonstração do próximo teorema, elas se relacionam diretamente com a resolução de equações diofantinas lineares.

Teorema 2.15. *Sejam $a, b, \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = (a, n)$. Se $d \nmid b$, então não há solução para a congruência $ax \equiv b \pmod{n}$, e se $d \mid b$, então há exatamente d soluções incongruentes módulo n.*

Demonstração. Pela proposição 2.7 $ax \equiv b \pmod{n}$ se, e somente se, existe y inteiro tal que $ax = b + yn$, que equivale a $ax - ny = b$. Do item i do teorema 2.14, se $d \nmid b$, então

não existem $x, y \in \mathbb{Z}$ tais que $ax - ny = b$, logo não existe solução para a congruência $ax \equiv b \pmod{n}$.

Se $d \mid b$, pelo item ii do teorema 2.14, as soluções de $ax - ny = b$ são da forma

$$x = x_0 - \frac{nt}{d}$$
$$y = y_0 - \frac{at}{d}$$

para todo $t \in \mathbb{Z}$, onde $x = x_0$ e $y = y_0$ é uma solução pasticular. Logo, pela proposição 2.7 temos que $x = x_0 - \dfrac{nt}{d}$ é solução da congruência $ax \equiv b \pmod{n}$ para todo t inteiro.

Para finalizarmos a demonstração, verificaremos sobre quais condições duas soluções são incongruentes módulo n. Se

$$x_1 = x_0 - \frac{nt_1}{d} \quad \text{e} \quad x_2 = x_0 - \frac{nt_2}{d}$$

são congruentes módulo n, então

$$\begin{aligned} x_0 - \frac{nt_1}{d} &\equiv x_0 - \frac{nt_2}{d} \pmod{n} \Rightarrow \\ \frac{nt_1}{d} &\equiv \frac{nt_2}{d} \pmod{n}. \end{aligned}$$

Como $\dfrac{n}{d} \mid n$, temos que $\left(\dfrac{n}{d}, n\right) = \dfrac{n}{d}$, logo pelo teorema 2.11

$$\begin{aligned} \frac{nt_1}{d} \cdot \frac{d}{n} &\equiv \frac{nt_2}{d} \cdot \frac{d}{n} \pmod{n \cdot \frac{d}{n}} \\ t_1 &\equiv t_2 \pmod{d}. \end{aligned}$$

Assim, avaliando a contrapositiva, se $t_1 \not\equiv t_2 \pmod{d}$, então $x_1 \not\equiv x_2 \pmod{n}$, ou seja, há exatamente d soluções incongruentes módulo n para a congruência $ax \equiv b \pmod{n}$. □

Definição 2.7. *Uma solução x_0 da congruência $ax \equiv b \pmod{n}$ é dita única módulo n se para toda solução x_1 desta congruência tivermos $x_1 \equiv x_0 \pmod{n}$.*

É fácil concluirmos usando o teorema 2.15 que uma solução de $ax \equiv b \pmod{n}$ é única módulo n se, e somente se, $(a, n) = 1$.

Definição 2.8. *Uma solução $x = \overline{a}$ da congruência $ax \equiv 1 \pmod{n}$ é chamada inverso de a módulo n.*

Proposição 2.10. *Dados p primo e a inteiro, a é seu próprio inverso módulo p se, e somente se, $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$.*

Demonstração. Se $a \cdot a \equiv 1 \pmod{p}$, então $p \mid a^2 - 1$, logo $p \mid (a-1)(a+1)$. Como p é primo, pela proposição 2.6 temos que $p \mid a - 1$ ou $p \mid a + 1$, ou seja,

$$a \equiv 1 \pmod{p} \quad \text{ou} \quad a \equiv -1 \pmod{p}.$$

Para demonstrarmos a recíproca verificamos que se temos $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$, então $p \mid a-1$ ou $p \mid a+1$, logo

$$p \mid (a-1)(a+1) \Rightarrow p \mid a^2 - 1 \Rightarrow a^2 \equiv 1 \pmod{p}.$$

□

O teorema a seguir foi publicado pela primeira vez em 1770 na Inglaterra nas *Meditationes algebraicae* de Edward Waring (1734-1793). Este teorema leva o nome de seu amigo e discípulo John Wilson (1741-1793) e foi demonstrado pela primeira vez por Joseph Louis Lagrange (1736-1813) no mesmo ano de sua publicação (BOYER; MERZBACH, 2012).

Este teorema será importante para o teste 2 que veremos no próximo capítulo.

Teorema 2.16 (Teorema de Wilson)**.** *Se $p \in \mathbb{P}$, então $(p-1)! \equiv -1 \pmod{p}$.*

Demonstração. No caso em que $p = 2$, temos $(2-1)! = 1 \equiv -1 \pmod{2}$ e assim o teorema é válido nesta situação.

Provaremos agora para p ímpar, neste caso, se a pertence ao conjunto

$$S = \{1, 2, \ldots, p-1\},$$

então $(a, p) = 1$ e pelo teorema 2.15 a congruência $ax \equiv 1 \pmod{p}$ tem solução única módulo p. Da proposição 2.10, dentre os elementos de S, apenas 1 e $p-1$ são seus próprios inversos módulo p, logo podemos obter $\dfrac{p-3}{2}$ congruências da forma

$$a \cdot \overline{a} \equiv 1 \pmod{p}$$

agrupando os números $2, 3, \ldots, p-2$ com seus respectivos inversos módulo p. Multiplicando todas essa congruências membro a membro obtemos

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

e multiplicando ambos os membros desta congruência por $p-1$ teremos

$$\begin{aligned} (p-1)! &\equiv (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$

□

2.7 Teorema de Euler

Para apresentarmos o teorema de Euler precisamos definir primeiramente a uma função que ficou conhecida historicamente como função φ de Euler. Esta função associa a cada natural n o total $\varphi(n)$ de números naturais menores que n que são primos com n.

Definição 2.9. *Definimos a função φ de Euler como*

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

onde $\varphi(1) = 1$ e para $n > 1$, $\varphi(n)$ é igual ao número de naturais menores que n que são primos com n.

De imediato podemos observar que p é um número primo se, e somente se, todos os $p - 1$ números naturais menores que p são primos com ele, ou seja,

$$p \text{ é primo} \Leftrightarrow \varphi(p) = p - 1.$$

Para demonstração do teorema de Euler precisamos definir ainda o que é um sistema reduzido de resíduos módulo n. Como o próprio nome sugere, trata-se de um subconjunto em particular de um sistema completo de resíduos módulo n (definição 2.6).

Definição 2.10. *Chamamos de sistema reduzido de resíduos módulo n um conjunto formado por $\varphi(n)$ inteiros primos com n e incongruentes dois a dois módulo n.*

Teorema 2.17. *Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que $(a, n) = 1$. Se $r_1, r_2, \ldots, r_{\varphi(n)}$ é um sistema reduzido de resíduos módulo n, então $ar_1, ar_2, \ldots, ar_{\varphi(n)}$ também é um sistema reduzido de resíduos módulo n.*

Demonstração. Devemos mostrar que $ar_i \not\equiv ar_j \pmod{n}$ se $i \neq j$ e que $(ar_i, n) = 1$ para todo $i = 1, 2, \ldots, \varphi(n)$.

Como $(a, n) = 1$, do teorema 2.11 segue que

$$\begin{aligned} & ar_i \equiv ar_j \pmod{n} \\ \Rightarrow \quad & r_i \equiv r_j \pmod{n} \\ \Rightarrow \quad & i = j, \end{aligned}$$

logo pela contrapositiva, para $i \neq j$ temos $ar_i \not\equiv ar_j \pmod{n}$.

Para segunda parte da demonstração utilizaremos o resultado do exemplo 2.8, isto é, para $i = 1, 2, \ldots, \varphi(n)$ temos

$$(a, n) = (r_i, n) = 1 \Rightarrow (ar_i, n) = 1.$$

□

O próximo teorema é conhecido como teorema de Euler em homenagem a Leonhard Euler (1707-1783). Este teorema será de extrema importância para a demonstração de alguns dos testes de primalidades presentes no próximo capítulo.

Teorema 2.18 (Teorema de Euler)**.** *Se* $(a, n) = 1$ *com* $n \in \mathbb{N}$*, então*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Demonstração. Consideremos o conjunto $S_1 = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$ um sistema reduzido de resíduos módulo n. Se $(a, n) = 1$, pelo teorema 2.17 o conjunto $S_2 = \{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ também é um sistema reduzido de resíduos módulo n. Logo, cada elemento de S_1 é congruente módulo n a um único elemento de S_2, assim, podemos multiplicar membro a membro estas $\varphi(n)$ congruências para obtermos

$$\begin{aligned} & ar_1 ar_2 \cdots ar_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n} \\ \Rightarrow \quad & a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n}. \end{aligned}$$

Como $(r_1, n) = (r_2, n) = \ldots = (r_{\varphi(n)}, n) = 1$, podemos concluir pelo exemplo 2.8 que

$$(r_1 r_2 \cdots r_{\varphi(n)}, n) = 1.$$

Logo, segue do teorema 2.11 que

$$\begin{aligned} & a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \equiv r_1 r_2 \cdots r_{\varphi(n)} \pmod{n} \\ \Rightarrow \quad & a^{\varphi(n)} \equiv 1 \pmod{n}. \end{aligned}$$

□

A próxima definição juntamente com a proposição que a sucede será usada em algumas demonstrações dos testes de primalidades que veremos no próximo capítulo.

Definição 2.11. *Dados* $a, n \in \mathbb{Z}$ *com* $(a, n) = 1$ *e* $n > 1$*, chamamos de ordem de* a *com respeito a* n *o menor número natural* i *tal que* $a^i \equiv 1 \pmod{n}$*. Usamos a notação* $ord_n(a)$ *para representar a ordem de* a *com respeito a* n*.*

Proposição 2.11. *Dados* $a, n \in \mathbb{Z}$ *com* $(a, n) = 1$ *e* $n > 1$*, então*

$$a^m \equiv 1 \pmod{n} \Leftrightarrow ord_n(a) \mid m.$$

Demonstração. Suponhamos que $a^m \equiv 1 \pmod{n}$. Pela divisão euclidiana (teorema 2.1) devem existir $q, r \in \mathbb{Z}$, com $0 \leq r < \mathrm{ord}_n(a)$ tais que $m = \mathrm{ord}_n(a) \cdot q + r$. Suponhamos

que $r \neq 0$, logo

$$\begin{aligned} & a^{\mathrm{ord}_n(a)\cdot q+r} \equiv 1 \pmod{n} \\ \Rightarrow \quad & \left(a^{\mathrm{ord}_n(a)}\right)^q \cdot a^r \equiv 1 \pmod{n}. \end{aligned}$$

Como $a^{\mathrm{ord}_n(a)} \equiv 1 \pmod{n}$ temos que

$$\begin{aligned} a^{\mathrm{ord}_n(a)} &\equiv 1 \pmod{n} \\ \left(a^{\mathrm{ord}_n(a)}\right)^q &\equiv 1 \pmod{n} \\ \left(a^{\mathrm{ord}_n(a)}\right)^q \cdot a^r &\equiv a^r \pmod{n} \\ 1 &\equiv a^r \pmod{n}, \end{aligned}$$

absurdo pois $r < \mathrm{ord}_n(a)$ e $i = \mathrm{ord}_n(a)$ é o menor natural tal que $a^i \equiv 1 \pmod{n}$, assim, $r = 0$ e consequentemente $\mathrm{ord}_n(a) \mid m$.

Para demonstrarmos a recíproca suponhamos que $\mathrm{ord}_n(a) \mid m$. Logo existe $q \in \mathbb{Z}$ tal que $m = \mathrm{ord}_n(a) \cdot q$, assim

$$\begin{aligned} a^m &\equiv a^{\mathrm{ord}_n(a)\cdot q} \pmod{n} \\ &\equiv \left(a^{\mathrm{ord}_n(a)}\right)^q \pmod{n} \\ &\equiv 1^q \pmod{n} \\ &\equiv 1 \pmod{n}. \end{aligned}$$

□

2.8 Critério de Euler

Neste momento temos por objetivo demonstrar o critério de Euler para o símbolo de Legendre. Este símbolo está associado diretamente a existência de soluções no conjunto dos inteiros para congruências do tipo $x^2 \equiv a \pmod{p}$ com a inteiro e p um primo ímpar.

As propriedades e definições que veremos a seguir são necessárias para a demonstração do critério de Euler, que por sua vez é pré-requisito para a demonstração do teste de Pepín que veremos no final do próximo capítulo.

Teorema 2.19. *Dados $p \in \mathbb{P}$ e $a \in \mathbb{Z}$ tais que $p \neq 2$ e $p \nmid a$, temos que a congruência*

$$x^2 \equiv a \pmod{p}$$

não tem solução ou tem exatamente duas soluções incongruentes módulo p.

Demonstração. Se x_0 é uma solução desta congruência, então

$$(x_0)^2 = (-x_0)^2 \equiv a \pmod{p},$$

que equivale a dizermos que $-x_0$ também é solução da congruência.

Agora provaremos que $x_0 \not\equiv -x_0 \pmod{p}$, para isto notemos primeiramente que $p \mid x_0^2 - a$. Como $p \nmid a$ temos que $p \nmid x_0^2 \Rightarrow p \nmid x_0$, logo, se fosse $x_0 \equiv -x_0 \pmod{p}$ teríamos

$$\begin{aligned} & 2x_0 \equiv 0 \pmod{p} \\ \Rightarrow \quad & p \mid 2x_0, \end{aligned}$$

que é absurdo uma vez que implicaria pelo teorema 2.5 que $p \mid x_0$, pois $(p, 2) = 1$. Assim, $x_0 \not\equiv -x_0 \pmod{p}$.

Para finalizarmos a demonstração precisamos provar que

$$x_1^2 \equiv a \pmod{p} \Rightarrow x_1 \equiv x_0 \pmod{p} \text{ ou } x_1 \equiv -x_0 \pmod{p}.$$

Consideremos $x = x_1$ uma solução da congruência $x^2 \equiv a \pmod{p}$. Segue que

$$\begin{aligned} & x_1^2 \equiv a \pmod{p} \\ \Rightarrow \quad & x_1^2 \equiv x_0^2 \pmod{p} \\ \Rightarrow \quad & x_1^2 - x_0^2 \equiv 0 \pmod{p} \\ \Rightarrow \quad & (x_1 + x_0)(x_1 - x_0) \equiv 0 \pmod{p}, \end{aligned}$$

logo

$$\begin{aligned} & p \mid (x_1 + x_0)(x_1 - x_0) \\ \Rightarrow \quad & p \mid (x_1 + x_0) \text{ ou } p \mid (x_1 - x_0) \\ \Rightarrow \quad & x_1 \equiv -x_0 \pmod{p} \text{ ou } x_1 \equiv x_0 \pmod{p} \end{aligned}$$

como queriamos demonstrar. □

O próximo teorema foi demonstrado pela primeira vez por Lagrange.

> Embora não usasse a linguagem das congruências, Lagrange demonstrou, em 1768, o equivalente do enunciado que para um módulo primo p, a congruência $f(x) \equiv 0$ não pode ter mais que n soluções distintas, onde n é o grau (exceto no caso trivial em que todos os coeficientes de $f(x)$ são divisíveis por p). (BOYER; MERZBACH 2012, p. 321).

Vejamos tal teorema e uma demonstração deste.

Teorema 2.20 (Lagrange)**.** *Sejam $a_n \in \mathbb{Z}$ e p um número primo tal que $(a_n, p) = 1$.*

Considerando

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$$

com $n \geq 1$ *e* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$*, temos que a congruência* $f(x) \equiv 0 \pmod{p}$ *tem no máximo* n *soluções incongruentes módulo* p*.*

Demonstração. Faremos a demonstração usando indução sobre n. No caso em que $n = 1$ temos que

$$\begin{aligned} & a_0 + a_1x \equiv 0 \pmod{p} \\ \Leftrightarrow \quad & a_1x \equiv -a_0 \pmod{p}. \end{aligned}$$

Como $(a_1, p) = 1$, pelo teorema 2.15 a congruência $a_1x \equiv -a_0 \pmod{p}$ tem exatamente uma solução incongruente módulo p, pois $(a_1, p) \mid -a_0$, provando que o resultado é válido para $n = 1$.

Suponhamos que o resultado seja válido para o inteiro $n = k \geq 1$ e suponhamos por absurdo que a congruência

$$f(x) = a_0 + a_1x + \ldots + a_kx^k + a_{k+1}x^{k+1} \equiv 0 \pmod{p} \tag{5}$$

possua $k + 2$ soluções incongruentes módulo p, onde $a_0, a_1, \ldots, a_{k+1} \in \mathbb{Z}$ e $(a_{k+1}, p) = 1$. Consideremos $x_1, x_2, \ldots, x_{k+2}$ soluções incongruentes módulo p da congruência (5). Usando o resultado do exemplo 2.4 temos que $x - x_1 \mid x^i - x_1^i$ para $i = 1, 2, \ldots, k + 1$, assim

$$\begin{aligned} f(x) - f(x_1) &= a_1(x - x_1) + \cdots + a_k(x^k - x_1^k) + a_{k+1}(x^{k+1} - x_1^{k+1}) \\ &= (x - x_1)g(x) \end{aligned}$$

onde

$$g(x) = b_0 + b_1x + \cdots + b_{k-1}x^{k-1} + a_{k+1}x^k$$

com $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Z}$.

Como $f(x_j) \equiv f(x_1) \equiv 0 \pmod{p}$ para $j = 1, 2, \ldots, k + 2$ podemos obter

$$f(x_j) - f(x_1) = (x_j - x_1)g(x_j) \equiv 0 \pmod{p},$$

logo, para $j \neq 1$ temos que

$$(x_j - x_1)g(x_j) \equiv 0 \pmod{p} \Rightarrow p \mid (x_j - x_1)g(x_j),$$

e como $p \nmid x_j - x_1$, pois $x_j \not\equiv x_1 \pmod{p}$ segue pela proposição 2.6 que

$$p \mid g(x_j) \Rightarrow g(x_j) \equiv 0 \pmod{p}.$$

Assim, a congruência $g(x) \equiv 0 \pmod{p}$ tem pelo menos $k+1$ soluções (pois $x_2, x_3, \ldots, x_{k+2}$ são soluções), que é absurdo contra a hipótese de indução.

Concluímos então que a congruência (5) tem no máximo $k+1$ soluções provando que o resultado é válido para $n = k+1$. Isso finaliza a demonstração. □

Definição 2.12. *Sejam a e n inteiros primos entre si com $n > 0$. Nestas condições dizemos que a é um resíduo quadrático módulo n se houver solução para a congruência*

$$x^2 \equiv a \pmod{n}.$$

Se não houver solução para esta congruência, então dizemos que a não é resíduo quadrático módulo n.

Teorema 2.21. *Se p é um primo ímpar, então o conjunto $S = \{1, 2, \ldots, p-1\}$ possui exatamente $(p-1)/2$ resíduos quadráticos módulo p.*

Demonstração. Provaremos inicialmente que os números

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

são incongruentes dois a dois módulo p.

Consideremos $x_1 \neq x_2$ tais que

$$1 \leq x_1 < x_2 \leq \frac{p-1}{2}$$

e suponhamos por absurdo que $x_2^2 \equiv x_1^2 \pmod{p}$. Logo

$$\begin{aligned} & p \mid x_2^2 - x_1^2 \\ \Rightarrow \quad & p \mid (x_2 + x_1)(x_2 - x_1). \end{aligned}$$

Como $1 < x_2 + x_1 < p$, então $p \nmid x_2 + x_1$, assim, pela proposição 2.6 segue que

$$p \mid x_2 - x_1 \Rightarrow x_2 \equiv x_1 \pmod{p},$$

absurdo, pois x_1 e x_2 são números positivos distintos menores que p, isto nos garante que os números

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

são incongruentes dois a dois módulo p e consequentemente cada um deles é um resíduo

quadrático módulo p distinto.

Para finalizarmos a demonstração provaremos que cada um dos números

$$\left(\frac{p-1}{2}+1\right)^2, \left(\frac{p-1}{2}+2\right)^2, \ldots, (p-1)^2$$

é congruente a um dos números

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2,$$

mais precisamente provaremos que $(p-k)^2 \equiv k^2 \pmod{p}$ para $k = 1, 2, \ldots, (p-1)/2$. De fato, temos que

$$\begin{aligned} & p \mid p(p-2k) \\ \Rightarrow\ & p \mid ((p-k)+k)((p-k)-k) \\ \Rightarrow\ & p \mid (p-k)^2 - k^2 \\ \Rightarrow\ & (p-k)^2 \equiv k^2 \pmod{p}. \end{aligned}$$

Portanto, no conjunto S há exatamente $(p-1)/2$ resíduos quadráticos módulo p. □

Definiremos agora e o símbolo de Legendre. Trata-se de uma simplificação de notação baseado na solubilidade de uma congruência na forma $x^2 \equiv a \pmod{p}$, onde p é um primo ímpar e a um inteiro não divisível por p, ou como vimos na definição 2.12, se a é ou não um resíduo quadrático módulo p. O nome foi dado em homenagem a Adrien Marie Legendre (1752-1833) o qual foi o primeiro a utilizar tal notação (BOYER; MERZBACH, 2012).

Definição 2.13. *Dados $p, a \in \mathbb{Z}$ onde p é um primo ímpar e $p \nmid a$ definimos o Símbolo de Legendre, denotado por $\left(\frac{a}{p}\right)$, como*

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

Teorema 2.22 (Critério de Euler)**.** *Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $p \nmid a$, então*

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

Demonstração. Por definição, há apenas duas possibilidades para $\left(\frac{a}{p}\right)$, igual a 1 ou igual a -1.

Se $\left(\frac{a}{p}\right) = 1$, então existe solução para a congruência $x^2 \equiv a \pmod{p}$. Consi-

deremos $x = x_0$ uma destas soluções. Logo

$$x_0^2 \equiv a \pmod{p} \Leftrightarrow p \mid x_0^2 - a.$$

Como $p \nmid a$, então

$$p \nmid x_0^2 \Rightarrow p \nmid x_0 \Rightarrow (x_0, p) = 1.$$

Assim, pelo teorema de Euler (teorema 2.18)

$$x_0^{\varphi(p)} = x_0^{p-1} \equiv 1 \pmod{p}$$

e consequentemente

$$\begin{aligned} \left(\frac{a}{p}\right) = 1 &\equiv x_0^{p-1} \pmod{p} \\ &\equiv (x_0^2)^{(p-1)/2} \pmod{p} \\ &\equiv a^{(p-1)/2} \pmod{p}. \end{aligned}$$

Agora provaremos o caso em que $\left(\frac{a}{p}\right) = -1$. Pelo teorema 2.20 a congruência $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ possui no máximo $(p-1)/2$ soluções incongruentes módulo p. Como já vimos, $a_k^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ para todo resíduo quadrático a_k, e pelo teorema 2.21 há apenas $(p-1)/2$ resíduos quadráticos módulo p. Logo as soluções da congruência $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ são apenas os resíduos quadráticos módulo p, isto é, se a não é um resíduo quadrático módulo p temos que

$$\left(\frac{a}{p}\right) = -1 \Rightarrow a^{(p-1)/2} - 1 \not\equiv 0 \pmod{p} \Rightarrow a^{(p-1)/2} \not\equiv 1 \pmod{p}.$$

Para finalizarmos a demonstração, notemos que

$$a^{p-1} - 1 = (a^{(p-1)/2} - 1)(a^{(p-1)} + 1),$$

segue pelo teorema de Euler (teorema 2.18) que

$$\begin{aligned} & a^{p-1} \equiv 1 \pmod{p} \\ \Leftrightarrow\ & p \mid a^{p-1} - 1 \\ \Leftrightarrow\ & p \mid (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \\ \Rightarrow\ & p \mid a^{(p-1)/2} - 1 \text{ ou } p \mid a^{(p-1)/2} + 1. \end{aligned}$$

Como $a^{(p-1)/2} \not\equiv 1 \pmod{p} \Rightarrow p \nmid a^{(p-1)/2} - 1$, então temos que

$$\begin{aligned} & p \mid a^{(p-1)/2} + 1 \\ \Rightarrow \quad & -1 = \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \end{aligned}$$

□

2.9 Lei de reciprocidade quadrática

Para demonstrarmos a lei de reciprocidade quadrática usaremos o resultado do teorema 2.23, que por sua vez se baseia no lema a seguir.

Lema 2.1. *Sejam p um primo ímpar e $a \in \mathbb{Z}$ tais que $p \nmid a$. Consideremos as congruências*

$$\begin{aligned} a &\equiv r_1 \pmod{p} \\ 2a &\equiv r_2 \pmod{p} \\ &\vdots \\ \left(\frac{p-1}{2}\right) a &\equiv r_{(p-1)/2} \pmod{p} \end{aligned}$$

onde $0 \leq r_i < p$ para todo $i = 1, 2, \ldots, (p-1)/2$. Se s é o número de resíduos dentre $r_1, r_2, \ldots, r_{(p-1)/2}$ que são maiores que $p/2$, então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Demonstração. Sejam $a_1, a_2, \ldots, a_r$ os resíduos dentre $r_1, r_2, \ldots, r_{(p-1)/2}$ que são menores que $p/2$ e $b_1, b_2, \ldots, b_s$ os que são maiores que $p/2$. Multiplicando todas as $(p-1)/2$ congruências membro a membro temos

$$\begin{aligned} a \cdot 2a \cdots \frac{p-1}{2} a &\equiv r_1 r_2 \cdots r_{(p-1)/2} \pmod{p} \\ &\equiv a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s \pmod{p}, \end{aligned}$$

logo

$$a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s \pmod{p}. \tag{6}$$

Notemos que os números $(p - b_1), (p - b_2), \ldots, (p - b_s)$ são todos menores do que $p/2$.

Provaremos agora que os números $a_1, a_2, \ldots, a_r, (p - b_1), (p - b_2), \ldots, (p - b_s)$ são, a menos da ordem, os números $1, 2, \ldots, (p-1)/2$, e para isso basta provar que eles

são incongruentes dois a dois módulo p. Se $a_i \equiv a_j \pmod{p}$, então teríamos

$$\begin{aligned} & p \mid a_i - a_j \\ \Rightarrow \quad & p \mid k_1 a - k_2 a \\ \Rightarrow \quad & p \mid (k_1 - k_2)a \\ \Rightarrow \quad & p \mid k_1 - k_2 \end{aligned}$$

para algum $k_1, k_2 \in \{1, 2, \ldots, (p-1)/2\}$, logo a única possibilidade é que $k_1 = k_2 \Rightarrow i = j$. Se $(p-b_i) \equiv (p-b_j) \pmod{p}$, então podemos mostra de forma análoga a situação anterior que $i = j$, pois

$$\begin{aligned} & p - b_i \equiv p - b_j \pmod{p} \\ \Rightarrow \quad & -b_i \equiv -b_j \pmod{p} \\ \Rightarrow \quad & b_i \equiv b_j \pmod{p}. \end{aligned}$$

Vejamos ainda que, supondo que existam i e j tais que $a_i \equiv p - b_j \pmod{p}$, então

$$\begin{aligned} a_i \equiv -b_j \pmod{p} \quad \Rightarrow \quad & p \mid a_i + b_j \\ \Rightarrow \quad & p \mid k_1 a + k_2 a \\ \Rightarrow \quad & p \mid (k_1 + k_2)a \\ \Rightarrow \quad & p \mid k_1 + k_2 \end{aligned}$$

para algum $k_1, k_2 \in \{1, 2, \ldots, (p-1)/2\}$, que é absurdo, pois o mínimo que a soma de dois destes números pode dá é 2 e o máximo é $p - 1$, enquanto nenhum número neste intervalo é múltiplo de p.

Assim, como nós queríamos demonstrar, os números $a_1, a_2, \ldots, a_r, (p-b_1), (p-b_2), \ldots, (p-b_s)$ são, a menos da ordem, os números $1, 2, \ldots, (p-1)/2$. Segue que

$$\begin{aligned} 1 \cdot 2 \cdots \frac{(p-1)}{2} = \left(\frac{p-1}{2}\right)! \quad \equiv \quad & a_1 a_2 \cdots a_r (p-b_1)(p-b_2)\cdots(p-b_s) \pmod{p} \\ \equiv \quad & a_1 a_2 \cdots a_r (-b_1)(-b_2)\cdots(-b_s) \pmod{p} \\ \equiv \quad & (-1)^s a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s \pmod{p}. \end{aligned}$$

Comparando a congruência (6) com esta última obtemos

$$\begin{aligned} & \left(\frac{p-1}{2}\right)! \equiv (-1)^s a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod{p} \\ \Rightarrow \quad & 1 \equiv (-1)^s a^{(p-1)/2} \pmod{p}, \end{aligned} \tag{7}$$

pois $(((p-1)/2)!, p) = 1$. Multiplicando ambos os membros da congruência (7) por $(-1)^s$

teremos

$$\begin{aligned}(-1)^s &\equiv (-1)^{2s}a^{(p-1)/2} \pmod{p} \\ &\equiv a^{(p-1)/2} \pmod{p},\end{aligned}$$

e pelo critério de Euler (teorema 2.22) segue que

$$\begin{aligned}\left(\frac{a}{p}\right) &\equiv a^{(p-1)/2} \pmod{p} \\ &\equiv (-1)^s \pmod{p} \\ &\Rightarrow p \mid \left(\frac{a}{p}\right) - (-1)^s.\end{aligned}$$

Para finalizarmos, notemos que $\left(\frac{a}{p}\right) - (-1)^s = \pm 2$ ou $\left(\frac{a}{p}\right) - (-1)^s = 0$. Como $p \nmid 2$, pois é ímpar, concluímos que

$$\left(\frac{a}{p}\right) - (-1)^s = 0 \Rightarrow \left(\frac{a}{p}\right) = (-1)^s.$$

□

Teorema 2.23. *Sejam p e a inteiros ímpares tais que $p \in \mathbb{P}$ e $p \nmid a$, então*

$$\left(\frac{a}{p}\right) = (-1)^M$$

onde

$$M = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{a}{p} \right\rfloor.$$

Demonstração. Nas mesmas notações do lema 2.1 é suficiente mostrarmos que s e M tem a mesma paridade, isto é, s e M são ambos ímpares ou ambos pares.

Vamos considerar as $(p-1)/2$ congruências

$$\begin{aligned}a &\equiv r_1 \pmod{p} \\ 2a &\equiv r_2 \pmod{p} \\ &\vdots \\ \left(\frac{p-1}{2}\right)a &\equiv r_{(p-1)/2} \pmod{p}\end{aligned}$$

onde $0 \leq r_i < p$ para todo $i = 1, 2, \ldots, (p-1)/2$. Dessas congruências, realizando a

divisão euclidiana (teorema 2.1), podemos obter as igualdades a seguir

$$\begin{aligned} a &= p\left\lfloor \frac{a}{p} \right\rfloor + r_1 \\ 2a &= p\left\lfloor \frac{2a}{p} \right\rfloor + r_2 \\ &\vdots \\ \frac{p-1}{2}\cdot a &= p\left\lfloor \frac{p-1}{2}\cdot\frac{a}{p} \right\rfloor + r_{(p-1)/2}. \end{aligned}$$

Somando membro a membro estas igualdades obtemos

$$\begin{aligned} \left(1+2+\ldots+\frac{p-1}{2}\right)a &= pM + r_1 + r_2 + \ldots r_{(p-1)/2} \\ \Rightarrow pM + r_1 + r_2 + \ldots r_{(p-1)/2} &= a\cdot\frac{(1+(p-1)/2)}{2}\cdot\frac{p-1}{2} \\ &= a\cdot\left(\frac{p+1}{4}\right)\cdot\left(\frac{p-1}{2}\right) \\ &= a\cdot\frac{p^2-1}{8}. \end{aligned}$$

Assim como nas notações vistas na demonstração do lema 2.1, façamos $a_1, a_2, \ldots, a_r$, os números dentre $r_1, r_2, \ldots, r_{(p-1)/2}$ que são menores do que $p/2$ e $b_1, b_2, \ldots, b_s$ os que são maiores que $p/2$, logo

$$pM + \sum_{i=1}^{r} a_i + \sum_{i=1}^{s} b_i = a\cdot\frac{p^2-1}{8}. \tag{8}$$

Na demonstração do lema 2.1 vimos ainda que os números $a_1, a_2, \ldots, a_r, p-b_1, p-b_2, \ldots, p-b_s$ são, a menos da ordem os números $1, 2, \ldots, (p-1)/2$, assim

$$\begin{aligned} & a_1 + a_2 + \cdots + a_r + ps - (b_1 + b_2 + \cdots + b_s) = 1 + 2 + \cdots + \frac{p-1}{2} \\ \Rightarrow\quad & ps + \sum_{i=1}^{r} a_i - \sum_{i=1}^{s} b_i = \frac{p^2-1}{8}. \end{aligned} \tag{9}$$

Subtraindo membro a membro a equação (9) da equação (8) teremos

$$p(M-s) + 2\sum_{i=1}^{s} b_i = \frac{p^2-1}{8}\cdot(a-1).$$

Como $8 \mid p^2-1$ (ver exemplo 2.5) e $a-1$ é par, então existem $k_1, k_2 \in \mathbb{Z}$ tais

que

$$\begin{aligned} & p(M-s)+2\sum_{i=1}^{s} b_i = k_1 \cdot 2k_2 \\ \Rightarrow \quad & p(M-s) = 2 \cdot \left(2k_1k_2 - \sum i = 1^s\right) \\ \Rightarrow \quad & 2 \mid p(M-s). \end{aligned}$$

Como $2 \nmid p$, pela proposição 2.6, $2 \mid M-s \Rightarrow M-s$ é par, ou seja, M e s são ambos ímpares ou ambos pares como queríamos demonstrar. □

Finalizamos este capítulo apresentando o teorema que ficou conhecido historicamente como lei de reciprocidade quadrática. Este teorema foi inicialmente enunciado por Euler e redescoberto posteriormente por Legendre, mas nenhum dos dois apresentou uma demonstração.

Este teorema foi demonstrado pela primeira vez em 1801 por Gauss, o qual apresentou duas demonstrações em sua *Disquisitiones Arithmeticae*. Gauss chamou a lei de reciprocidade quadrática de *theorema aureum*, ou a joia da aritmética (BOYER; MERZBACH, 2012).

A demonstração que veremos agora foi adaptada de Santos (2007) e foi dada originalmente por Ferdinand Eisenstein (1823-1852). Apenas na demonstração deste teorema usaremos a notação (x, y) para representar o ponto sobre um plano cartesiano de coordenadas ortogonais de abcissa x e ordenada y, ao invés de representar o máximo divisor comum entre x e y.

Teorema 2.24 (Lei de reciprocidade quadrática)**.** *Sejam p e q primos ímpares e distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Demonstração. Consideremos um sistema de coordenadas cartesianas ortogonais com a unidade definida. Sobre este sistema consideramos um retângulo com vértices nos pontos de coordenadas $A = (0,0), B = (0, q/2), C = (p/2, q/2)$ e $D = (p/2, 0)$ como na figura 1.

Um ponto de coordenadas inteiras (x, y) é interior ao retângulo $ABCD$ se $0 < x < p/2, 0 < y < q/2$ e $x, y \in \mathbb{Z}$, isto é, se $x = 1, 2, \ldots, (p-1)/2$ e $y = 1, 2, \ldots, (q-1)/2$, logo o total desses pontos é

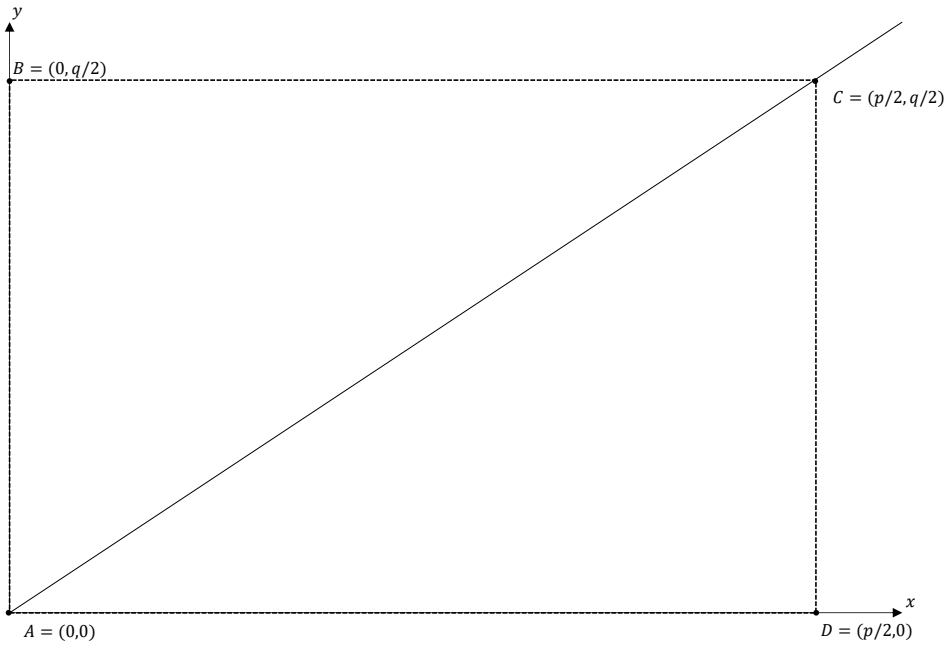
$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Consideremos agora a reta que passa pelos pontos A e C, esta tem por equação

$$\overleftrightarrow{AC} : y = \frac{q}{p}x.$$

Notemos que se um ponto de coordenadas inteira (x_0, y_0) pertence a reta $\overleftrightarrow{AC}$, então $py_0 = qx_0 \Rightarrow p \mid qx_0$ e $q \mid py_0$, e pela proposição 2.6 temos que $p \mid x_0$ e $q \mid y_0$, absurdo pois

Figura 1 – Demonstração de Eisenstein da lei de reciprocidade quadrática



Fonte: Adaptada de Santos (2007, p. 107).

$0 < x_0 < p/2$ e $0 < y_0 < q/2$, logo nenhum ponto de coordenadas inteiras que esteja no interior do retângulo $ABCD$ pertence a reta $\overleftrightarrow{AC}$.

Observemos que, dado uma reta paralela ao eixo x de equação $y = k$, esta é intersectada pela reta $\overleftrightarrow{AC}$ no ponto de coordenadas $(kp/q, k)$. Logo, $\left\lfloor \dfrac{kp}{q} \right\rfloor$ é o número de pontos de coordenadas inteiras que são interiores ao triângulo ABC e que estão sobre a reta de equação $y = k$, para $k = 1, 2, \ldots, (q-1)/2$. Assim, o total N de pontos de coordenadas inteiras que são interiores ao triângulo ABC é

$$N = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{q-1}{2} \cdot \frac{p}{q} \right\rfloor.$$

De modo análogo, dado uma reta paralela ao eixo y de equação $x = k$, a interseção desta com a reta $\overleftrightarrow{AC}$ é o ponto de coordenadas $(k, kq/p)$. Assim, como na situação anterior podemos provar que o total M de pontos de coordenadas inteiras interiores ao triângulo ACD é

$$M = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2} \cdot \frac{q}{p} \right\rfloor.$$

Concluímos que o números de pontos interiores ao retângulo $ABCD$ de coordenadas inteiras é

$$N + M = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Pelo teorema 2.23 temos que

$$\left(\frac{p}{q}\right) = (-1)^N \text{ e}$$
$$\left(\frac{q}{p}\right) = (-1)^M,$$

logo

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^N \cdot (-1)^M \\ &= (-1)^{N+M} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\end{aligned}$$

□

3 TESTES DE PRIMALIDADE

Desde Euclides sabe-se que todo número inteiro maior do que 1 ou é primo ou é o produto de números primos, tal afirmação é suficiente para observamos a importância desses números para a aritmética. Uma questão relacionado diretamente com números primos é a de testa a primalidade de números. Tal tarefa não é fácil, e não se conhece ainda um método totalmente eficiente para testar se um número qualquer é primo ou não.

Neste capítulo veremos oito testes de primalidades distintos e suas respectivas demonstrações. Boa parte desses testes, como veremos, são úteis para testar tipos específicos de números, como por exemplo números de Fermat, que definiremos a seguir.

Definição 3.1. *Chamamos de número de Fermat um número da forma* $F_n = 2^{2^n} + 1$*, onde* $n \in \mathbb{N} \cup \{0\}$*.*

3.1 Infinitude dos primos

Um aspecto relevante sobre números primos é a existência de uma infinidade deles. Testar a primalidade de números seria uma tarefa mais fácil se existisse apenas uma quantidade finita de números primos, uma vez que seria suficiente, dependo obviamente dessa quantidade de primos, criar uma lista com todos os primos e consulta-la sempre que houvesse a necessidade de reconhecer se determinado número é primo ou não.

Hoje já se conhecem diversas demonstrações da existência de uma infinidade de números primos. Historicamente, a primeira demonstração foi dada pelo próprio Euclides e baseia-se, assim como muitas das demais demonstrações, no teorema fundamental da aritmética. Veremos a seguir três demonstrações distintas da infinitude dos primos que utilizam ideias diferentes mas se assemelham por usarem direta ou indiretamente esse teorema.

Teorema 3.1. *O conjunto* $\mathbb{P}$ *é infinito.*

Demonstração de Euclides. Suponhamos que $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ seja finito, com p_n sendo o maior número primo. Consideremos o número

$$p = p_1 p_2 \ldots p_n + 1.$$

Observamos que p não é composto, pois não pode ser escrito como produto de fatores primos uma vez que nenhum elemento de $\mathbb{P}$ divide p, que é absurdo pelo teorema 2.7, pois $p > p_n$ também não é primo. Logo, existem infinitos números primos. □

A Próxima demonstração foi dada por Christian Goldbach (1690-1764) em uma carta enviada por ele a Euler em 1730 (RIBENBOIM, 2012). Essa demonstração consiste essencialmente em provar que um determinado conjunto infinito de números tem seus elementos dois à dois primos entre sí, pois assim podemos tomar um fator primo

distinto para cada elemento desse conjunto.

Demonstração de Goldbach. Seja $F_0, F_1, \ldots, F_n, \ldots$ a sequência dos números de Fermat. Provaremos por indução finita sobre n que a relação

$$F_0F_1 \ldots F_{n-1} = F_n - 2$$

é válida para todo n natural. De fato a relação é válida para $n = 1$, pois $F_0 = 2^{2^0} + 1 = 3 = 2^{2^1} + 1 - 2 = F_1 - 2$.

Suponhamos que a relação é válida para $n = k$, segue que

$$\begin{aligned} F_0F_1 \ldots F_k &= (F_0F_1 \ldots F_{k-1})F_k \\ &= (F_k - 2)F_k \\ &= (2^{2^k} - 1)(2^{2^k} + 1) \\ &= (2^{2^k})^2 - 1 \\ &= 2^{2^{k+1}} + 1 - 2 \\ &= F_{k+1} - 2. \end{aligned}$$

Logo a relação é válida para $k + 1$ e pelo axioma 2.2 concluímos que também vale para todo $n \in \mathbb{N}$.

Pela relação que acabamos de demonstrar temos que $F_n - F_0F_1 \ldots F_{n-1} = 2$. Segue pelo teorema 2.14 que se $0 < m < n$, então $(F_n, F_m) \mid 2$. Como $2 \nmid F_n$, pois os números de Fermat são todos ímpares, então temos que $(F_n, F_m) = 1$, ou seja, os números de Fermat são primos entre si dois a dois.

Assim, concluímos que existem infinitos números primos, uma vez que podemos tomar um fator primo distinto de cada número de Fermat. □

A próxima demonstração é devida a Axel Thue (1863-1952) e consiste em encontrar uma função crescente $f : \mathbb{N} \to \mathbb{N}$ tal que a quantidade de primos menores que $f(m)$ seja maior que m, deste modo, podemos tomar m tão grande quanto se queira escolhendo $f(m)$ suficientemente grande.

Demonstração de Thue. Dado $m \in \mathbb{N}$ podemos tomar $q \in \mathbb{N}$ tal que $1+qm < 2^q$ (podemos verificar a existência de q pelo exemplo 2.3). Fazendo $n = qm$ segue que

$$\begin{aligned} & 1 + n < 2^q \\ \Rightarrow \quad & (1 + n)^m < 2^{qm} \\ \Rightarrow \quad & (1 + n)^m < 2^n. \end{aligned}$$

Denotemos por $p_1 < p_2 < \ldots < p_r$ todos os números primos menores que 2^n. Uma vez

que qualquer número natural $k \leq 2^n$ pode ser escrito de forma única como

$$k = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

onde $0 \leq a_1 \leq n$ e $0 \leq a_i < n$, para $i = 2, \ldots, r$, logo o total de possibilidades para k não é maior do que $(n+1)n^{r-1}$, ou seja, $2^n \leq (n+1)n^{r-1}$.

Suponhamos por absurdo que $r \leq m$, assim teríamos que

$$2^n \leq (n+1)n^{r-1} < (n+1)^r \leq (n+1)^m < 2^n,$$

que é absurdo, logo $r > m$.

Elevando ambos os membros da desigualdade $1 + 2m^2 < 2^{2m}$, que nós vimos no exemplo 2.2, a m obtemos

$$(1 + 2m^2)^m < 2^{2m^2} = 4^{m^2},$$

logo a quantidade r de primos menores do que 4^{m^2} é maior que m. Como m pode ser escolhido tão grande quanto se queira, concluímos que existem infinitos números primos. □

3.2 Testes de primalidade básicos

Veremos a seguir dois testes de primalidade que podem ser aplicados em qualquer número natural e que apresentam enunciados simples e de fácil compreensão. No entanto, ambos se mostram pouco eficientes a medida que queremos testar a primalidade de números cada vez maiores.

O nosso primeiro teste é uma versão moderna do crivo de Eratóstenes, e talvez seja a forma mais conhecida e mais antiga de reconhecer se determinado número é primo ou não. Este teste baseia-se essencialmente na existência da fatoração de um número em fatores primos vista no teorema 2.7 do capítulo anterior.

Estima-se que Eratóstenes nasceu por volta de 280 a.C na cidade de Cirene, na costa sul do mar Mediterrâneo, foi bibliotecário-chefe da Universidade de Alexandria e por volta de 194 a.C ficou quase cego, o que levou a suicidar-se após voluntariamente ter deixado de se alimentar (EVES, 2002).

> Eratóstenes foi singularmente talentoso em todos os ramos do conhecimento de seu tempo. Distinguiu-se como matemático, astrônomo, geógrafo, historiador, filósofo, poeta e atleta. Consta que alunos da Universidade de Alexandria costumavam chamá-lo de *Pentathlus*, o que significa campeão em cinco esportes atléticos. (EVES, 2002, p. 197).

Teste 1 (Crivo de Eratóstenes)**.** *Sejam $n \in \mathbb{N}$ e $p_1 < p_2 < \ldots < p_r$ todos os primos menores ou iguais que $\sqrt{n}$, então n é primo se, e somente se, $p_i \nmid n$ para $i = 1, 2, \ldots, r$.*

Demonstração. Se n é primo, então nenhum primo menor que ele pode ser seu divisor, logo

$$p_1 < p_2 < \ldots < p_r \leq \sqrt{n} < n \Rightarrow p_i \nmid n, \text{ para } i = 1, 2, \ldots, r.$$

Para demonstrarmos a recíproca basta observarmos que se $p_i \nmid n$ para $i = 1, 2, \ldots, r$, pelo teorema 2.8, n não pode ser composto, pois caso contrário haveria um primo $p \leq \sqrt{n}$ tal que $p \mid n$. Logo, n é primo. □

Exemplo 3.1. Vamos verificar que 41 é primo utilizando o teste 1 e pra isso notemos primeiramente que

$$\begin{aligned} & \sqrt{36} < \sqrt{41} < \sqrt{49} \\ \Rightarrow \quad & 6 < \sqrt{41} < 7. \end{aligned}$$

Logo os primos menores que $\sqrt{41}$ são $2, 3$ e 5. Realizando divisão euclidiana podemos escrever

$$\begin{aligned} 41 &= 20 \cdot 2 + 1, \\ 41 &= 13 \cdot 3 + 2 \text{ e} \\ 41 &= 8 \cdot 5 + 1, \end{aligned}$$

ou seja, $2 \nmid 41$, $3 \nmid 41$ e $5 \nmid 41$. Assim concluímos pelo teste 1 que 41 é primo.

O teste 1 é muito prático, mas exige o conhecimento de todos o números primos menores que $\sqrt{n}$ para testar a primalidade de n, tarefa que pode se tornar muito difícil a medida que avançamos na sequencia dos números.

O próximo teste, juntamente com o teorema de Wilson (teorema 2.16) exprime, assím como no teste 1, uma condição necessária e suficiente para que um inteiro n qualquer seja primo.

Teste 2 (Recíproca do teorema de Wilson)**.** *Se* $(n-1)! \equiv -1 \pmod{n}$*, então* n *é primo.*

Demonstração. Suponhamos que $(n-1)! \equiv -1 \pmod{n}$, e que n seja composto, então existem $n_1, n_2 \in \mathbb{N}$ tais que $n = n_1 n_2$, com

$$1 < n_1 \leq n_2 < n.$$

Logo, $n_1 \mid n$ e como $n \mid (n-1)! + 1$ temos pelo item viii da proposição 2.1 que $n_1 \mid (n-1)! + 1$. Notemos também que $n_1 \mid (n-1)!$, pois $n_1 < n$, assim, segue pela proposição 2.3 que

$$\begin{aligned} & n_1 \mid (n-1)! + 1 - (n-1)! \\ \Rightarrow \quad & n_1 \mid 1, \end{aligned}$$

absurdo, pois $1 < n_1$, e daí n é primo. □

Exemplo 3.2. Para provarmos que 11 é primo usaremos o teste 2, para isso devemos mostrar que $10! \equiv -1 \pmod{11}$. Considerando as congruências

$$\begin{aligned}
&10 \cdot 1 = 11 - 1 \equiv -1 \pmod{11},\\
&9 \cdot 5 = 45 = 4 \cdot 11 + 1 \equiv 1 \pmod{11},\\
&8 \cdot 7 = 56 = 5 \cdot 11 + 1 \equiv 1 \pmod{11},\\
&6 \cdot 2 = 12 = 11 + 1 \equiv 1 \pmod{11} \text{ e}\\
&4 \cdot 3 = 12 = 11 + 1 \equiv 1 \pmod{11}
\end{aligned}$$

podemos utilizar o item ii do teorema 2.10 para obtermos

$$\begin{aligned}
10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 &\equiv (-1) \cdot 1^4 \pmod{11}\\
10! &\equiv -1 \pmod{11}
\end{aligned}$$

como queríamos demonstrar.

É interessante observarmos que, teoricamente necessitamos apenas realizar a divisão de $(n-1)!$ por n para a partir do resto garantirmos se n é primo ou não usando o teste 2, no entanto, calcular $(n-1)!$ pode ser mais difícil que testar a primalidade de n usando o crivo de Eratóstenes. Mas, não está descartada a possibilidade de um dia alguém inventar um método rápido de se calcular o resto da divisão de $(n-1)!$ por n (MARTINEZ; *et al.*, 2015).

3.3 Testes de primaridade baseados no teorema de Euler

Os testes que veremos a seguir são baseados no teorema de Euler (teorema 2.18) e foram adaptados, com suas respectivas demonstrações, de Ribenboim (2012).

O primeiro deles foi dado por Anatole Lucas (1842-1891) em 1876.

Teste 3. *Seja $n \in \mathbb{N}$, com $n > 1$. Se existe um inteiro $a > 1$ tal que:*

i: $a^{n-1} \equiv 1 \pmod{n}$,

ii: $a^m \not\equiv 1 \pmod{n}$ *para todo natural* $m < n-1$,

então n é primo.

Demonstração. Das hipóteses i e ii podemos concluir que $\mathrm{ord}_n(a) = n-1$ (ver definição 2.11). Se $a^{n-1} \equiv 1 \pmod{n}$, então pela proposição 2.7 existe q inteiro tal que $a(a^{n-2}) - nq = 1$, logo pelo teorema 2.14, $(a,n) \mid 1 \Rightarrow (a,n) = 1$. Segue da proposição 2.11 e do teorema de Euler (teorema 2.18) que

$$\mathrm{ord}_n(a) \mid \varphi(n) \Rightarrow (n-1) \mid \varphi(n).$$

Como $\varphi(n) \leq n-1$, então $\varphi(n) = n-1$, assim n é primo. □

Exemplo 3.3. Utilizando o teste 3 provaremos que $n = 5$ é primo. Primeiramente vejamos que $2^{n-1} = 2^4 = 16 = 3 \cdot 5 + 1 \equiv 1 \pmod 5$. Consideremos também as congruências

$$\begin{aligned} 2^3 = 8 = 1 \cdot 5 + 3 \equiv 3 \not\equiv 1 \pmod 5, \\ 2^2 = 4 \equiv 4 \not\equiv 1 \pmod 5 \text{ e} \\ 2^1 = 2 \equiv 2 \not\equiv 1 \pmod 5, \end{aligned}$$

logo pelo teste 3, $n = 5$ é primo.

Como pudemos observar no exemplo anterior, o teste 3 exige o cálculo de $n-1$ congruências e ainda assím encontrar um $a > 1$ conveniente. Provavelmente seria mais prático dividir n por todos os números naturais menores que n para testar a sua primalidade.

O próximo teste foi dado em 1891 também por Lucas e é uma evolução do teste anterior. Ao invés de calcularmos $n-1$ congruências como no teste anterior, com o teste 4 precisaremos calcular apenas m congruências, onde m é o número de divisores positivos de $n-1$.

Teste 4. *Seja $n \in \mathbb{N}$, com $n > 1$. Se existe um inteiro $a > 1$ tal que:*

i: $a^{n-1} \equiv 1 \pmod n$,

ii: $a^d \not\equiv 1 \pmod n$ *para todo divisor d de $n-1$ tal que $0 < d < n-1$,*

então n é primo.

Demonstração. Se $a^{n-1} \equiv 1 \pmod n$, então existe q inteiro tal que $a(a^{n-2}) - nq = 1$, e pelo teorema 2.14 temos que $(a, n) \mid 1 \Rightarrow (a, n) = 1$. Logo, temos pela proposição 2.11 que $\text{ord}_n(a) \mid n-1$, e se $a^d \not\equiv 1 \pmod n$ para todo divisor d de $n-1$ com $0 < d < n-1$ podemos concluir que $\text{ord}_n(a) = n-1$.

Como $(a, n) = 1$, segue do teorema de Euler (teorema 2.18) que

$$a^{\varphi(n)} \equiv 1 \pmod n,$$

assim, pela proposição 2.11 temos que $\text{ord}_n(a) \mid \varphi(n) \Rightarrow n-1 \mid \varphi(n)$, e como $\varphi(n) \leq n-1$ podemos concluir pelo item vi da proposição 2.1 que $\varphi(n) = n-1$, isto é, n é primo. □

Exemplo 3.4. Provemos que $n = 257$ é primo. Como $n - 1 = 256 = 2^8$, então seus divisores positivos são todos potências de 2, isto é, os divisores positivos de $n-1$ são os

números $1, 2, 4, 8, 16, 32, 64, 128$ e 256. Nas notações do testes 4, façamos $a = 3$, logo

$$
\begin{aligned}
&3^1 \equiv 3 \pmod{257},\\
&3^2 \equiv 9 \pmod{257},\\
&3^4 \equiv 81 \pmod{257},\\
&3^8 = 6561 \equiv 136 \pmod{257},\\
&3^{16} = 3^8 \cdot 3^8 \equiv 136 \cdot 136 \equiv 18496 \equiv -8 \pmod{257},\\
&3^{32} = 3^{16} \cdot 3^{16} \equiv (-8) \cdot (-8) \equiv 64 \pmod{257},\\
&3^{64} = 3^{32} \cdot 3^{32} \equiv 64 \cdot 64 \equiv 4096 \equiv -16 \pmod{257},\\
&3^{128} = 3^{64} \cdot 3^{64} \equiv (-16) \cdot (-16) \equiv 256 \equiv -1 \pmod{257},\\
&3^{256} \equiv (-1) \cdot (-1) \equiv 1 \pmod{257}.
\end{aligned}
$$

Assim, pelo teste 4, $n = 257$ é primo.

O teste anterior pode ser útil quando $n-1$ possui poucos divisores e desejamos testar a primalidade de n. Vejamos mais um exemplo.

Exemplo 3.5. Vamos provar que $n = 20759$ é primo, para isso notemos que $n - 1 = 97 \cdot 107 \cdot 2$. Como $97, 107$ e 2 são primos, então os divisores positivos de $n - 1$ são $1, 2, 97, 107, 2 \cdot 97, 2 \cdot 107, 97 \cdot 107$ e $97 \cdot 107 \cdot 2$.

Nas notações do teste 4 façamos $a = 7$. Segue que

$$
\begin{aligned}
&7^1 \equiv 7 \pmod{20759}, && (10)\\
&7^2 \equiv 49 \pmod{20759}, && (11)\\
&7^{10} = 282475249 \equiv 7536 \pmod{20759},\\
&7^6 = 117649 \equiv -6905 \pmod{20759}\\
\Rightarrow\ &7^{16} = 7^{10} \cdot 7^6 \equiv -52036080 \equiv 6733 \pmod{20759}\\
\Rightarrow\ &7^{32} \equiv 45333289 \equiv -4367 \pmod{20759}\\
\Rightarrow\ &7^{64} \equiv 19070689 \equiv -6832 \pmod{20759}\\
\Rightarrow\ &7^{96} = 7^{64} \cdot 7^{32} \equiv 29835344 \equiv 4661 \pmod{20759}\\
\Rightarrow\ &7^{97} = 7^{96} \cdot 7 \equiv 32627 \equiv -8891 \pmod{20759} && (12)\\
\Rightarrow\ &(7^{97})^2 \equiv 79049881 \equiv -391 \pmod{20759}, && (13)\\
&7^{107} = 7^{97} \cdot 7^{10} \equiv -67002576 \equiv 7476 \pmod{20759} && (14)\\
\Rightarrow\ &(7^{107})^2 \equiv 55890576 \equiv 7348 \pmod{20759} && (15)\\
\Rightarrow\ &(7^{107})^4 \equiv 53993104 \equiv -1055 \pmod{20759}\\
\Rightarrow\ &(7^{107})^8 \equiv 1113025 \equiv -7961 \pmod{20759}\\
\Rightarrow\ &(7^{107})^{16} \equiv 63377521 \equiv 294 \pmod{20759}\\
\Rightarrow\ &(7^{107})^{32} \equiv 86436 \equiv 3400 \pmod{20759}
\end{aligned}
$$

$$\Rightarrow \quad (7^{107})^{64} \equiv 11560000 \equiv -2763 \pmod{20759}$$
$$\Rightarrow \quad (7^{107})^{96} = (7^{107})^{64} \cdot (7^{107})^{32} \equiv -9394200 \equiv 9627 \pmod{20759}$$
$$\Rightarrow \quad (7^{107})^{97} = (7^{107})^{96} \cdot 7^{107} \equiv 71971452 \equiv -1 \pmod{20759}. \tag{16}$$
$$\Rightarrow \quad ((7^{107})^{97})^2 \equiv (-1)^2 \equiv 1 \pmod{20759}. \tag{17}$$

Das congruência (10), (11), (12), (13), (14), (15), (16) e (17) podemos concluir pelo teste 4 que $n = 20759$ é primo.

O próximo teste data de 1967 e foi dado por Brillhart e Selfridge. Este foi baseado no teste anterior dado por Lucas.

Teste 5. *Seja $n \in \mathbb{N}$ com $n \neq 1$. Se para cada fator primo p de $n-1$ existe um inteiro $a_p > 1$ tal que:*
i: $a_p^{n-1} \equiv 1 \pmod{n}$,
ii: $a_p^{(n-1)/p} \not\equiv 1 \pmod{n}$,
então n é primo.

Demonstração. Como $\varphi(n) \leq n-1$, será suficiente mostrarmos que $(n-1) \mid \varphi(n)$, pois consequentemente teremos $\varphi(n) = n-1$. Suponhamos que $(n-1) \nmid \varphi(n)$, logo existe p primo tal que $p^r \mid n-1$ e $p^r \nmid \varphi(n)$, para algum $r \in \mathbb{N}$.

Seja $a_p \in \mathbb{N}$ com $a_p > 1$ tal que $a_p^{n-1} \equiv 1 \pmod{n}$ e $a_p^{(n-1)/p} \not\equiv 1 \pmod{n}$. Notemos que se $a_p^{n-1} \equiv 1 \pmod{n}$, então pela proposição 2.7 existe q inteiro tal que $a_p(a_p^{n-2}) - nq = 1$, logo pelo teorema 2.14 $(a_p, n) \mid 1 \Rightarrow (a_p, n) = 1$. Assim, pela proposição 2.11 temos que $\mathrm{ord}_n(a_p) \mid n-1$ e $\mathrm{ord}_n(a_p) \nmid (n-1)/p$, isto garante a existência de $q \in \mathbb{N}$ tal que $n-1 = q \cdot \mathrm{ord}_n(a_p)$. Segue que

$$\begin{aligned} & p^r \mid q \cdot \mathrm{ord}_n(a_p) \\ \Rightarrow \quad & p^{r-1} \mid \frac{q \cdot \mathrm{ord}_n(a_p)}{p}. \end{aligned} \tag{18}$$

Como

$$\mathrm{ord}_n(a_p) \nmid \frac{q \cdot \mathrm{ord}_n(a_p)}{p}$$

temos que $p \nmid q$, pois q/p não é inteiro, e consequentemente $p^r \nmid q$. De (18) obtemos que

$$p^r \mid \mathrm{ord}_n(a_p).$$

Segue do teorema de Euler (teorema 2.18) e da proposição 2.11 que

$$a_p^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow \mathrm{ord}_n(a_p) \mid \varphi(n) \Rightarrow p^r \mid \varphi(n),$$

o que contraria a hipótese de que $p^r \nmid \varphi(n)$, assim concluímos que toda potência de primo que divide $n-1$ também divide $\varphi(n)$, ou seja, $(n-1) \mid \varphi(n)$ como queriamos demonstrar. □

Exemplo 3.6. Testaremos a primalidade de $n = 17$ usando o testes 5. Notemos que $n-1 = 16 = 2^4$, logo $n-1$ tem apenas um fator primo, que é 2. Nas notações do teste 5 façamos $a_2 = 5$. Segue que

$$\begin{aligned} & 5^2 = 25 = 1 \cdot 17 + 8 \equiv 8 \pmod{17} \\ \Rightarrow \quad & 5^4 = 5^2 \cdot 5^2 \equiv 8 \cdot 8 \equiv 64 \equiv -4 \pmod{17} \\ \Rightarrow \quad & 5^8 = 5^4 \cdot 5^4 \equiv (-4) \cdot (-4) \equiv 16 \equiv -1 \pmod{17} \\ \Rightarrow \quad & 5^{16} = 5^8 \cdot 5^8 \equiv (-1) \cdot (-1) \equiv 1 \pmod{17}, \end{aligned}$$

assim

$$\begin{aligned} & 5^8 = 5^{\frac{16}{2}} = 5^{\frac{17-1}{2}} \not\equiv 1 \pmod{17} \text{ e} \\ & 5^{16} \equiv 1 \pmod{17}. \end{aligned}$$

Pelo teste 5 podemos concluir que $n = 17$ é primo.

O teste anterior é útil para testar a primalidade de números de Fermat, vamos ver um exemplo.

Exemplo 3.7. Provemos que F_4 é primo. Vejamos que $F_4 = 2^{2^4} + 1 = 65537$, logo o único fator primo de $F_4 - 1$ é $p = 2$. Fazendo $a_2 = 3$ segue que

$$\begin{aligned} & 3^{2^3} \equiv 6561 \pmod{65537} \\ \Rightarrow \quad & 3^{2^4} \equiv 3^{2^3} \cdot 3^{2^3} \equiv 6561 \cdot 6561 \equiv 43046721 \equiv -11088 \pmod{65537} \\ \Rightarrow \quad & 3^{2^5} \equiv 3^{2^4} \cdot 3^{2^4} \equiv (-11088) \cdot (-11088) \equiv 122943744 \equiv -3668 \pmod{65537} \\ \Rightarrow \quad & 3^{2^6} \equiv 3^{2^5} \cdot 3^{2^5} \equiv (-3668) \cdot (-3668) \equiv 13454224 \equiv 19139 \pmod{65537} \\ \Rightarrow \quad & 3^{2^7} \equiv 3^{2^6} \cdot 3^{2^6} \equiv 19139 \cdot 19139 \equiv 366301321 \equiv 15028 \pmod{65537} \\ \Rightarrow \quad & 3^{2^8} \equiv 3^{2^7} \cdot 3^{2^7} \equiv 15028 \cdot 15028 \equiv 225840784 \equiv 282 \pmod{65537} \\ \Rightarrow \quad & 3^{2^9} \equiv 3^{2^8} \cdot 3^{2^8} \equiv 282 \cdot 282 \equiv 79524 \equiv 13987 \pmod{65537} \\ \Rightarrow \quad & 3^{2^{10}} \equiv 3^{2^9} \cdot 3^{2^9} \equiv 13987 \cdot 13987 \equiv 195636169 \equiv 8224 \pmod{65537} \\ \Rightarrow \quad & 3^{2^{11}} \equiv 3^{2^{10}} \cdot 3^{2^{10}} \equiv 8224 \cdot 8224 \equiv 67634176 \equiv -8 \pmod{65537} \\ \Rightarrow \quad & 3^{2^{13}} \equiv 3^{2^{12}} \cdot 3^{2^{12}} \equiv (-8)^2 \cdot (-8)^2 \equiv 4096 \pmod{65537} \\ \Rightarrow \quad & 3^{2^{14}} \equiv 3^{2^{13}} \cdot 3^{2^{13}} \equiv 4096 \cdot 4096 \equiv 16777216 \equiv -256 \pmod{65537} \\ \Rightarrow \quad & 3^{2^{15}} \equiv 3^{2^{14}} \cdot 3^{2^{14}} \equiv (-256) \cdot (-256) \equiv -1 \pmod{65537} \\ \Rightarrow \quad & 3^{\frac{F_4-1}{2}} = 3^{\frac{2^{16}}{2}} = 3^{2^{15}} \equiv -1 \pmod{F_4} \\ \Rightarrow \quad & 3^{F_4-1} \equiv 1 \pmod{F_4}. \end{aligned}$$

Assim, pelas duas últimas congruências concluímos pelo teste 5 que F_4 é primo.

3.4 Testes baseados na proposição de Pocklington

Os dois últimos testes que vimos necessitam do conhecimento da fatoração de $n-1$ para podermos testar a primalidade de n, isso faz com que estes testes sejam eficientes apenas para tipos de números muito específicos. A seguir, veremos dois testes que exigem apenas um conhecimento parcial da fatoração de $n-1$, tais testes baseiam-se fundamentalmente na próxima proposição, que foi demonstrada por Pocklington em 1914.

Proposição 3.1 (Proposição de Pocklington)**.** *Dado $n \in \mathbb{N}$ com $n-1 = p^r R$, onde p é primo, $r \geq 1$ e $p \nmid R$. Se existe um inteiro $a > 1$ tal que:*

i: $a^{n-1} \equiv 1 \pmod{n}$,

ii: $(a^{(n-1)/p} - 1, n) = 1$,

então os fatores primos de n são da forma $mp^r + 1$, para algum $m \in \mathbb{N}$.

Demonstração. Seja q um fator primo de n, será suficiente provarmos que $p^r \mid q-1$. Se existe $a > 1$ tal que $a^{n-1} \equiv 1 \pmod{n}$, temos que $a(a^{n-2}) - nk = 1$ para algum k inteiro. Pelo teorema 2.14 podemos obter

$$(a, n) \mid 1 \Rightarrow (a, n) = 1 \Rightarrow (a, q) = 1,$$

logo, pelo teorema de Euler (teorema 2.18) $a^{\varphi(q)} = a^{q-1} \equiv 1 \pmod{q}$, e pela proposição 2.11 temos que $\mathrm{ord}_q(a) \mid q-1$.

Da proposição 2.8 podemos obter ainda

$$\begin{aligned} & a^{n-1} \equiv 1 \pmod{n} \\ \Rightarrow\ & a^{n-1} \equiv 1 \pmod{q} \\ \Rightarrow\ & \mathrm{ord}_q(a) \mid n-1 \\ \Rightarrow\ & \mathrm{ord}_q(a) \mid p^r R. \end{aligned}$$

Se $(a^{(n-1)/p} - 1, n) = 1$, suponhamos por absurdo que $\mathrm{ord}_q(a) \mid (n-1)/p$, segue pela proposição 2.11 que

$$\begin{aligned} a^{(n-1)/p} \equiv 1 \pmod{q} \ \Rightarrow\ & q \mid a^{(n-1)/q} - 1 \\ \Rightarrow\ & q \mid \left(a^{(n-1)/p} - 1, q\right) \\ \Rightarrow\ & q \mid \left(a^{(n-1)/p} - 1, n\right) \\ \Rightarrow\ & q \mid 1, \end{aligned}$$

absurdo, pois q é primo, assim $\text{ord}_q(a) \nmid p^{r-1}R$, e como $\text{ord}_q(a) \mid p^r R$ temos que

$$\begin{aligned} & p \cdot \text{ord}_q(a) \nmid p^r R \\ \Rightarrow \quad & p \nmid \frac{p^r R}{\text{ord}_q(a)} \\ \Rightarrow \quad & p^r \mid \text{ord}_q(a) \\ \Rightarrow \quad & p^r \mid q-1 \end{aligned}$$

como queriamos demonstrar. □

O próximo teste é conhecido como critério de Proth, data de 1878 e pode ser demonstrado utilizando a proposição anterior. A demonstração que veremos aqui foi adaptada de Ribenboim (2012).

Teste 6 (Critério de Proth)**.** *Seja $n-1 = 2^r R$, com R ímpar e menor do que 2^r. Se existe um inteiro $a > 1$ tal que $a^{(n-1)/2} \equiv -1 \pmod{n}$, então n é primo.*

Demonstração. Se $a^{(n-1)/2} \equiv -1 \pmod{n}$, então

$$\begin{aligned} & \left(a^{(n-1)/2}\right)^2 \equiv (-1)^2 \pmod{n} \\ \Rightarrow \quad & a^{n-1} \equiv 1 \pmod{n}. \end{aligned}$$

Também temos que existe $k \in \mathbb{Z}$ tal que

$$\begin{aligned} & nk = a^{(n-1)/2} + 1 \\ \Rightarrow \quad & nk - (a^{(n-1)/2} - 1) = 2, \end{aligned}$$

logo, pelo teorema 2.14, $(a^{(n-1)/2} - 1, n) \mid 2$, isto é,

$$(a^{(n-1)/2} - 1, n) = 1 \text{ ou } (a^{(n-1)/2} - 1, n) = 2.$$

Como $n = 2^r R + 1$ é ímpar, só é possível que seja $(a^{(n-1)/2} - 1, n) = 1$.

Podemos então usar a proposição de Pocklington (proposição 3.1), que nos diz que os fatores primos de n são da forma $q = m2^r + 1 > 2^r$. Segue que

$$n = 2^r R + 1 < 2^r \cdot 2^r = 2^{2r}.$$

Logo $\sqrt{n} < 2^r < q$, e pelo teorema 2.8 concluímos que n é primo. □

Exemplo 3.8. Demonstraremos que $n = 97$ é primo. Inicialmente temos que $n - 1 = 96 = 32 \cdot 3 = 2^5 \cdot 3$. Como $2^5 > 3$, pelo teste anterior (teste 6) basta encontrarmos $a > 1$

tal que $a^{\frac{n-1}{2}} = a^{\frac{96}{2}} \equiv a^{48} \equiv -1 \pmod{97}$. Fazendo $a = 7$, segue que

$$\begin{aligned}
& 7^2 \equiv 49 \pmod{97} \\
\Rightarrow\ & 7^4 = 49 \cdot 49 = 2401 = 25 \cdot 97 - 24 \equiv -24 \pmod{97} \\
\Rightarrow\ & 7^8 = 7^4 \cdot 7^4 \equiv (-24) \cdot (-24) \equiv 576 \equiv 6 \cdot 97 - 6 \equiv -6 \pmod{97} \\
\Rightarrow\ & 7^{24} = 7^8 \cdot 7^8 \cdot 7^8 \equiv (-6) \cdot (-6) \cdot (-6) \equiv -216 \equiv -2 \cdot 97 - 22 \equiv -22 \pmod{97} \\
\Rightarrow\ & 7^{48} = 7^{24} \cdot 7^{24} \equiv (-22) \cdot (-22) \equiv 484 \equiv 5 \cdot 97 - 1 \equiv -1 \pmod{97},
\end{aligned}$$

como queríamos demonstrar.

O testes anterior pode ser útil para testar a primalidade de números da forma $n = k \cdot 2^m + 1$, onde k é um inteiro ímpar. Vejamos mais um exemplo.

Exemplo 3.9. Usando o teste 6 provaremos que $n = 12289$ é primo. Notemos que $n - 1 = 3 \cdot 2^{12}$ e façamos $a = 11$, logo

$$\begin{aligned}
& 11^6 = 1771561 \equiv 1945 \pmod{12289}, \\
& 11^4 = 14641 \equiv 2352 \pmod{12289} \\
\Rightarrow\ & 11^{10} = 11^6 \cdot 11^4 \equiv 4574640 \equiv 3132 \pmod{12289} \\
\Rightarrow\ & 11^{2^4} = 11^{10} \cdot 11^6 \equiv 6091740 \equiv -3604 \pmod{12289} \\
\Rightarrow\ & 11^{2^5} \equiv 12988816 \equiv -657 \pmod{12289} \\
\Rightarrow\ & 11^{2^6} \equiv 431649 \equiv 1534 \pmod{12289} \\
\Rightarrow\ & 11^{2^7} \equiv 2353156 \equiv 5957 \pmod{12289} \\
\Rightarrow\ & 11^{2^8} \equiv 35485849 \equiv 7506 \pmod{12289} \\
\Rightarrow\ & 11^{2^9} \equiv 56340036 \equiv 7260 \pmod{12289} \\
\Rightarrow\ & 11^{2^{10}} \equiv 52707600 \equiv 79 \pmod{12289} \\
\Rightarrow\ & 11^{2^{11}} \equiv 6241 \pmod{12289} \\
\Rightarrow\ & 11^{2 \cdot 2^{11}} \equiv 38950081 \equiv 6240 \pmod{12289} \\
\Rightarrow\ & 11^{3 \cdot 2^{11}} = 11^{2 \cdot 2^{11}} \cdot 11^{2^{11}} \equiv 38943840 \equiv -1 \pmod{12289}.
\end{aligned}$$

Como $11^{(n-1)/2} = 11^{3 \cdot 2^{11}} \equiv -1 \pmod{12289}$, fica provado que $n = 12289$ é primo.

O próximo teste também é uma aplicação direta da proposição de Pocklington. A demonstração que veremos foi adaptada de Martinez *et al.* (2015).

Teste 7. *Dado $n \in \mathbb{N}$ com $n - 1 = FR$, com $F > R > 0$ e $(F, R) = 1$. Se existe um inteiro $a_k > 1$ para cada fator primo p_k de F tal que:*

i: $a_k^{n-1} \equiv 1 \pmod{n}$,

ii: $(a_k^{(n-1)/p_k} - 1, n) = 1$,

então n é primo.

Demonstração. Seja $F = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$. Como $(F, R) = 1$, temos que

$$p_i \nmid \frac{FR}{p_i^{\alpha_i}} \text{ , para } i = 1, 2, \ldots, r.$$

Se para cada fator primo p_k de F existe um inteiro a_k tal que $(a_k^{(n-1)/p_k} - 1, n) = 1$, então pela proposição de Pocklington (proposição 3.1) os fatores primos de n são da forma

$$m \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} + 1 = mF + 1, \text{ para algum } m \in \mathbb{Z}.$$

Como $F > R > 0$, segue que

$$\begin{aligned} & n - 1 = FR \\ \Rightarrow \quad & n - 1 \leq F(F-1) = F^2 - F \\ \Rightarrow \quad & n < F^2 \\ \Rightarrow \quad & \sqrt{n} < F. \end{aligned}$$

Assim, se q é um fator primo de n, então deve existe um inteiro m tal que

$$\begin{aligned} & q = mF + 1 \\ \Rightarrow \quad & q > m\sqrt{n} + 1 \\ \Rightarrow \quad & q > \sqrt{n}, \end{aligned}$$

e pelo teorema 2.8 n não pode ser composto, ou seja, n é primo. □

Exemplo 3.10. Testaremos a primalidade de $n = 19$, para isso notemos que $n - 1 = 18 = 3^2 \cdot 2$. Nas notações do teste 7 façamos $F = 3^2 > R = 2$. Como F é uma potência de 3, então este tem apenas $p_1 = 3$ como fator primo, façamos então $a_1 = 2$. Logo

$$\begin{aligned} 2^{\frac{19-1}{3}} - 1 &= 2^6 - 1 \\ &= 63. \end{aligned}$$

Assim, aplicando sucessivamente o teorema 2.4 obtemos

$$\begin{aligned} (63, 19) &= (3 \cdot 19 + 6, 19) \\ &= (19, 6) \\ &= (3 \cdot 6 + 1, 6) \\ &= (6, 1) = 1 \\ &\Rightarrow (63, 19) = 1. \end{aligned} \tag{19}$$

Como 2 é primo e $2 \nmid 19$, então $(2, 19) = 1$, assim, pelo teorema de Euler (teorema 2.18)

$$2^{18} \equiv 1 \pmod{19}. \tag{20}$$

De (19) e (20) podemos concluir pelo teste 7 que $n = 19$ é primo.

O principal problema do teste anterior está em calcular o máximo divisor comum entre $a_k^{(n-1)} - 1$ e n, pois $a_k^{(n-1)} - 1$ pode facilmente ser um número muito grande, tal problema não está presente no teste 6, o que torna este mais viável nos casos em que podemos aplica-lo. Sobre o critério de Proth, Martinez *et al.* (2015) afirma:

> Muitos dentre os maiores primos conhecidos estão nas condições do teorema de Proth [...]. Isto se deve ao fato de primos desta forma serem mais frequentes (mais frequentes do que, por exemplo, primos de Mersenne) e que sua primalidade é facilmente demonstrada usando este resultado. (MARTINEZ; *et al.*, 2015, p 339).

3.5 Teste de Pépin

O último teste que veremos foi dado por Pépin em 1877 e exprime uma condição necessária e suficiente para que um número de Fermat (ver definição 3.1) seja primo. Usando este teste Lucas mostrou que F_6, um número com 20 algarismos, é composto. A demonstração que veremos foi adaptada de Martinez *et al.* (2015).

Teste 8 (Teste de Pépin)**.** *Um número de Fermat F_n com $n > 0$ é primo se, e somente se,* $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

Demonstração. Se F_n com $n > 0$ é primo, como $F_n > 3$, segue que $F_n \nmid 3$ e pelo critério de Euler (teorema 2.22)

$$\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}} \pmod{F_n}. \tag{21}$$

Usando a lei de reciprocidade quadrática (teorema 2.24) obtemos

$$\left(\frac{3}{F_n}\right)\left(\frac{F_n}{3}\right) = (-1)^{\frac{F_n-1}{2}\cdot\frac{3-1}{2}}$$

$$\Rightarrow \left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) \cdot (-1)^{2^{2^n}-1} = \left(\frac{F_n}{3}\right). \tag{22}$$

Como vimos na demonstração da infinitude dos primos feita por Goldbach, os números de Fermat são dois à dois primos entre sí, logo $3 \nmid F_n$ para $n > 0$, pois $3 \mid F_0$, assim pelo critério de Euler

$$\left(\frac{F_n}{3}\right) \equiv F_n^{\frac{3-1}{2}} \equiv F_n \pmod{3}.$$

Segue da última congruência que se $\left(\frac{F_n}{3}\right) = 1$, então $3 \mid F_n - 1 \Rightarrow 3 \mid 2^{2^n}$ que é absurdo, logo $\left(\frac{F_n}{3}\right) = -1$, assim, de (21) e (22) temos que

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Por outro lado, se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, então

$$\begin{aligned} & 3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n} \\ \Rightarrow \quad & 3^{\frac{F_n-1}{2}\cdot 2} \equiv (-1)^2 \pmod{F_n} \\ \Rightarrow \quad & 3^{F_n-1} \equiv 1 \pmod{F_n} \end{aligned}$$

e como 2 é o único fator primo de $F_n - 1$, pelo teste 5 concluímos que F_n é primo. □

Exemplo 3.11. Provaremos usando o teste de Pepín que $F_5 = 2^{2^5} + 1 = 4294967297$ não é primo, para isso vejamos as implicações a seguir

$$\begin{aligned} & 3^{2^5} \equiv 3793201458 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^6} \equiv 1461798105 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^7} \equiv 852385491 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^8} \equiv 54249794 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^9} \equiv 1194573931 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{10}} \equiv 2171923848 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{11}} \equiv 3995994998 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{12}} \equiv 2840704206 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{13}} \equiv 1980848889 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{14}} \equiv 2331116839 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{15}} \equiv 2121054614 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{16}} \equiv 2259349256 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{17}} \equiv 1861782498 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{18}} \equiv 1513400831 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{19}} \equiv 2897320357 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{20}} \equiv 367100590 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{21}} \equiv 2192730157 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{22}} \equiv 2050943431 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{23}} \equiv 2206192234 \pmod{F_5} \\ \Rightarrow \quad & 3^{2^{24}} \equiv 2861695674 \pmod{F_5} \end{aligned}$$

$$
\begin{aligned}
&\Rightarrow \quad 3^{2^{25}} \equiv 2995335231 \pmod{F_5} \\
&\Rightarrow \quad 3^{2^{26}} \equiv 3422723814 \pmod{F_5} \\
&\Rightarrow \quad 3^{2^{27}} \equiv 3416557920 \pmod{F_5} \\
&\Rightarrow \quad 3^{2^{28}} \equiv 3938027619 \pmod{F_5} \\
&\Rightarrow \quad 3^{2^{29}} \equiv 2357699199 \pmod{F_5} \\
&\Rightarrow \quad 3^{2^{30}} \equiv 1676826986 \pmod{F_5} \\
&\Rightarrow \quad 3^{2^{31}} \equiv 10324303 \pmod{F_5}.
\end{aligned}
$$

Logo, $3^{(F_n-1)/2} = 3^{2^{31}} \not\equiv -1 \pmod{F_5}$, e pelo teste 8, F_5 não é primo.

4 CONCLUSÃO

Identificar se um número é primo ou não, no geral é uma tarefa muito difícil, principalmente quando estamos lidando com números grandes. Tal tarefa vem sendo estudada por muitos matemáticos no decorrer da história, e os testes que vimos neste trabalho refletem os avanços obtidos por alguns deles.

Cada um dos oito testes que vimos apresentam defeitos e qualidades, por exemplo, os testes 1 e 2 podem ser usados em qualquer número e ambos apresentam uma condição necessária e suficiente para que tal número seja primo, no entanto, o teste 1 exige o conhecimento de todos os primos menores que a raiz quadrada do número testado, isso se torna cada vez mais difícil a medida que avançamos na sequência dos números, e o teste 2 apesar de precisarmos calcular apenas uma congruência, esta envolve um número gigantesco. Os demais testes que vimos, com exceção apenas do teste 8, apresentam apenas condições suficientes para testar a primalidade de um número, ao passo que temos que encontrar um segundo número conveniente para suporte, e encontrar tal número envolve um pouco de sorte, se é que ele existe.

É bastante engenhoso testar a primalidade de um número conhecendo a decomposição do seu antecessor, esta ideia está presente nos testes 4, 5, 6, 7 e 8. Como pudemos ver nas demonstrações desses testes, tal ideia foi sustentada principalmente pelo teorema de Euler (teorema 2.18). Sugerimos ao leitor interessado, uma leitura de RIBENBOIM (2012) e de MARTINEZ *et al.* (2015) para conferir alguns testes de primalidades baseados no conhecimento da decomposição do sucessor do número que se deseja testar, tais testes são baseados principalmente em sucessões de Lucas, e um desses, inclusive, apresenta uma condição necessária e suficiente para que um número de Mersenne seja primo.

Optamos em escolher os oito testes por estes possuírem demonstrações curtas e condições práticas de aplicação se comparados com os demais testes encontrados durante a pesquisa. Os testes baseados em sucessões de Lucas, por exemplo, apresentam demonstrações muito longas, condições de aplicações extremamente específicas e ainda necessitam de uma base teórica maior.

Podemos destacar a utilidade de dois testes em particular vistos neste trabalho. O teste de Pépin, como vimos, facilita a verificação da primalidade de números de Fermat ao apresentar uma condição necessária e suficiente. Já o critério de Proth apresenta uma condição de razoável aplicação em números da forma $n = k \cdot 2^m + 1$, com k ímpar, que são menos raros que os números de Fermat.

REFERÊNCIAS

BOYER, Carl B.; MERZBACH, UTA C. **História da matemática:** tradução de Helena Castro. São Paulo: Blucher, 2012.

COUTINHO, S. C. **Número inteiros e criptografia RSA**. Rio de Janeiro: IMPA, 2014.

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

EVES, Howard. **Introdução à história da matemática:** tradução de Hygino H. Domingues. 3 ed. Campinas: Editora da UNICAMP, 2002.

HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2014.

MARTINEZ, Fabio Brochero; et al. **Teoria dos números:** um passeio com primos e outros números familiares pelo mundo inteiro. 4 ed. Rio de Janeiro: IMPA, 2015.

RIBENBOIM, Paulo. **Números primos:** Velhos mistérios e novos recordes. 1 ed. Rio de Janeiro: IMPA, 2012.

RIBENBOIM, Paulo. **Números primos, amigos que causam problemas**. Rio de Janeiro: SBM, 2015.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 2007.