Números Primos e Testes de Primalidade

Douglas Vinícius Gonçalves Araújo

Orientadora: Lúcia De Fátima De Medeiros Brandão Dias

Departamento Acadêmico de Matemática e Estatística, Universidade Federal de Rondônia, Ji-Paraná, Brasil — 2020

Objetivos

1. Estudar algumas definições e teoremas relacionados a Teoria dos números;
2. Provar teoremas e proposições relacionados ao números inteiros;
3. Apresentar alguns testes de primalidade determinísticos e probabilísticos;
4. Compreender e demonstrar os conceitos relacionados aos testes de primalidade.

1. Números Primos e Fatoração

Os números primos desempenham um papel fundamental no estudo dos inteiros e nas técnicas de criptografia. Os gregos foram os primeiros a perceber que qualquer número natural pode ser gerado pela multiplicação de números primos, também chamados de blocos de construção.

Definição 1: Um número inteiro $n > 1$ possuindo somente dois divisores positivos n e 1 é chamado *primo*.

Teorema Fundamental da Aritmética: Todo inteiro positivo $n > 1$ pode ser decomposto de meneira única, a menos da ordem dos fatores, como um produto de primos.

Teorema de Euclides: Existe uma infinidade de números primos.

2. Pequeno Teorema de Fermat

O problema de fatorar números compostos grandes é algo difícil até mesmo para computadores atuais. Razão pela qual os testes de primalidade são essenciais para verificar a primalidade de um número. Todos os testes eficientes conhecidos até o momento, sejam determinístico ou probabilístico, baseiam-se no pequeno teorema de Fermat.

Definição : Sejam $a, b, n \in \mathbb{Z}$. Dizemos que a é congruente a b módulo n, escrevemos $a \equiv b \pmod{n}$ se $n \mid a - b$, ou seja, existe um $k \in \mathbb{Z}$ tal que $a = b + nk$. .

Exemplo 2: Temos que $7 \equiv 2 \pmod{5}$. Caso contrário, denotamos por $a \not\equiv b \pmod{n}$ e chamamos de *incongruente*.

Pequeno Teorema de Fermat: Seja p um número primo e a um número inteiro qualquer, então $p \mid a^p - a$.

3. Pseudoprimos

Definição 3: Um número composto n é dito *pseudoprimo* na base $b > 1$ se $b^{n-1} \equiv 1 \pmod{n}$. .

Exemplo: O número $341 = 11 \cdot 31$ é pseudoprimo na base 2, pois $2^{340} \equiv 1 \pmod{341}$. A existência de pseudoprimos atesta que recíproca do Teorema de Fermat II não é verdadeira. Mas pseudoprimos são raros. Por exemplo, há apenas 245 pseudoprimos na base 2 entre 1 e 1 milhão. Podemos aumentar ainda mais a eficiência do teste de Fermat (contra-positiva do Teorema de Fermat II) aplicando-o para várias bases. Observe que no caso de 341, temos $3^{340} \not\equiv 1 \pmod{341}$, portanto 3 é testemunha de que 341 é composto, pela contra-positiva do Teorema de Fermat II.

Definição : Um inteiro positivo composto n é número de Carmichael se satisfaz a congruência $b^{n-1} \equiv 1 \pmod{n}$ para todo os inteiros b, $1 < b < n - 1$.

4. Testes de Primalidade

Um teste de primalidade é qualquer algoritmo que determina se um inteiro é primo ou composto. Um teste determinístico é o que determina com toda certeza se o inteiro dado é primo ou composto. Segundo (ANDRADE, 2017 P.41) "Os testes probabilísticos são aqueles que retornam uma resposta com um percentual de confiabilidade e utilizam números gerados aleatoriamente para a sua execução." Esses tipos de teste podem indicar, com certa probabilidade, que um inteiro é primo. São apresentados dois testes determinísticos: Divisão sucessiva e teste de Lucas. E um teste probabilístico: teste de Miller.

Divisão Sucessiva: Seja n um número natural composto, então n tem um divisor primo p tal que $p \leq \sqrt{n}$.

Exemplo: Vamos determinar se 127 é primo. Como $\sqrt{127}$ é um pouco maior que 11, basta testar a divisibilidade de 127 pelos primos 2, 3, 5, 7 e 11. Como 127 não é divisível por nenhum destes númerosm, então é primo.

Teste de Miller: Seja um inteiro ímpar $n > 0$ e $1 < b < n - 1$, $b \in \mathbb{N}$. Então, $n - 1$ é par e fatorando-o, obtemos $n - 1 = 2^k q$, $k \geq 1$ e q ímpar. Calcule as potências $b^q, b^{2q}, ..., b^{2^{k-1}q}, b^{2^k q} = b^{n-1}$. Se n for primo, então pelo menos um dessas potências tem que ser congruente $a - 1$ módulo n ou $b^q \equiv 1 \pmod{n}$. Se nada disso acontencer, então n é composto

Exemplo: Seja $n = 104513$. Temos que $n - 1 = 104513 = 2^6 \cdot 1633$, então $k = 6$ e $q = 1633$. Tomando $b = 3$ vamos analisar as congruências: $3^1 633 \equiv 1 \pmod{104513}$
$3^{2 \cdot 1633} \equiv 88958^2 \equiv 10430 \pmod{104513}$
$3^{2^2 \cdot 1633} \equiv 10430^2 \equiv 91380 \pmod{104513}$
$3^{2^3 \cdot 1633} \equiv 91380^2 \equiv 29239 \pmod{104513}$
$3^{2^4 \cdot 1633} \equiv 29239^2 \equiv 2781 \pmod{104513}$
$3^{2^5 \cdot 1633} \equiv 2781^2 \equiv -1 \pmod{104513}$
Portanto, conclui-se que n é provavelmente primo.

Teste de Lucas: Seja n um inteiro positivo ímpar e b um inteiro tal que $2 \leq b \leq n - 1$. Se $b^{n-1} \equiv 1 \pmod{n}$ e $b^{(n-1)/p} \equiv 1 \pmod{n}$, para cada fator primo p de $n-1$, então n é primo.

Exemplo: Testar que 7 é primo. Temos que $n = 7$ e $2 \leq b \leq 6$. $n-1 = 6 = 2 \cdot 3$. Para a base $b = 2$, 1º argumento: $2^6 \equiv 1 \pmod{7} \iff 7 \mid (2^6 - 1) \implies 7 \mid 63 = 9$, 1º argumento válido. 2º argumento e $q = 2$: $2^{6/2} \not\equiv 1 \pmod{7} \iff 7 \mid (2^3 - 1) \implies 7 \mid 7 = 1$, 2º argumento inválido. Agora para base $b = 3$: 1º argumento: $3^6 \equiv 1 \pmod{7} \iff 7 \mid (3^6 - 1) \implies 7 \mid 728 = 104$, 1º argumento válido. 2º argumento e $q = 2$: $3^{6/2} \not\equiv 1 \pmod{7} \iff 7 \mid (3^3 - 1) \implies 7 \nmid 26$, 2º argumento válido. Para $q = 3$, $3^{6/3} \not\equiv 1 \pmod{7} \iff 7 \mid (3^2 - 1) \implies 7 \nmid 8$, também válido. Logo, 7 é primo.

5.Considerações Finais

Este trabalho apresentou um estudo sobre as propriedades dos números inteiros, resultados básicos sobre números primos e a descreveu alguns testes de primalidade. Testes de primalidades são essenciais para determinar números primos e estes números são primordiais para a segurança da criptografia R.S.A., cuja implementação necessita ter à disposição um estoque de números primos grandes.

Referências

Andrade, R. P. **Testes de primalidade: uma análise matemática dos algoritmos determinísticos e probabilísticos**. Dissertação mestrado profissional de matemática-PROFMAT. Universidade Federal do Ceará-UFC. 2017.

Coutinho, S. C. **Números Inteiros e Criptografia RSA**. Coleção Matemática e Aplicações, Rio de Janeiro: IMPA, 2013.

Martinez F. E. B., Moreira C. G. , Saldanha N. C., Tengan E. **Teoria dos Números** - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

Ribenboim, P. **Números Primos**: Velhos mistérios e novos recordes. 1 ed. Coleção Matemática Universitária, IMPA, 2012.

Santos, J. P. de Oliveira. **Introdução à Teoria dos Números.**. Coleção Matemática Universitária, IMPA, 1998.