VIII Simpósio de Iniciação Científica 2025

"Do conhecimento acadêmico à transformação sustentável: inovação com validação científica"

NÚMEROS PRIMOS E TESTES DE PRIMALIDADE

Ruan Pablo Pereira de Almeida[1] (IC), Marcelo A. C. Nogueira (PQ)[2]

Palavras-chave: Congruências. Números primos. Testes de primalidade.

Introdução

Números primos são os inteiros positivos que possuem apenas dois divisores : 1 e o próprio número. O conjunto dos números primos possui diversas propriedades interessantes, que vão desde a infinitude dos números primos até a distribuição desses números no conjunto dos números naturais.

Também há muitas conjecturas envolvendo os números primos e que ainda não foram provadas. Dentre elas, destaca-se a conjectura de Goldbach. Essa conjectura afirma que todos os números pares maiores do que 4 podem ser escritos como a soma de dois números primos ímpares.

Vale destacar que os matemáticos, ao longo da história, tentaram encontrar fórmulas cujo resultado são apenas números primos, mas não obtiveram resultados muito satisfatórios.

São notórios também os diversos estudos e tentativas de encontro de resultados no que tange a progressões aritméticas formadas exclusivamente por números primos. O teorema de Green-Tao, por exemplo, afirma que o conjunto dos números primos possui progressões aritméticas de qualquer comprimento.

Nesse cenário, foi desenvolvida esta iniciação científica. O trabalho realizado tem como tema "números primos e testes de primalidade".

Os objetivos do trabalho são: estudar teoremas envolvendo o conjunto dos números primos, desde a infinitude desse conjunto e de alguns tipos de primos particulares, como os da forma $4n + 1$, $4n + 3$ e $6n + 5$; a distribuição dos números primos; progressões aritméticas envolvendo números primos; estimativas envolvendo números primos; a lei da reciprocidade quadrática; e testes de primalidade como: o teste de Lucas, o teste de Pépin, o teste de Miller-Rabin e o teste de primalidade AKS.

No que tange a justificativa, a importância de estudar números primos está relacionada com o desenvolvimento do raciocínio lógico e a construção de uma base de conhecimentos para o entendimento de Teoria dos Números e Álgebra. Além disso, os números primos possu[1]em diversas aplicações computacionais, principalmente criptografia, fator que justifica o estudo das propriedades envolvendo os números primos e dos testes de primalidade.

Metodologia

A metodologia consistiu em analisar e estudar os livros de Burton (2010) e Martinez (2011), estudando os conceitos e teoremas de capítulos envolvendo números primos destes livros.

Primeiramente, foi estudado o capítulo 3 do livro de Burton (2010). Nele, foi discutida a infinitude do conjunto dos números primos através do teorema de Euclides. Também foi estudada a conjectura de Goldbach, além de consequências que ocorrem se essa conjectura for verdadeira.

Ainda nesse capítulo, foram estudadas a infinitude de números das formas $4n + 1$, $4n + 3$ e 5, além de resultados envolvendo progressões aritméticas formadas exclusivamente por primos, como o teorema de Green-Tao.

Além disso, foi estudada parte do capítulo 2 de Martinez (2011), que envolve congruências de grau 2, incluindo resíduos quadráticos e o símbolo de Legendre, a fim de provar e estudar testes de primalidade.

O tópico final estudado são os testes de primalidade citados na introdução: teste de Lucas, o teste de Pépin, o teste de Miller-Rabin e o teste de Primalidade AKS, com algumas aplicações computacionais.

Resultados e discussão

Dentre os resultados do trabalho podemos citar alguns teoremas envolvendo o conjunto dos números primos.

O primeiro teorema estudado foi o teorema de Euclides, que valida a infinitude do conjunto dos

[1] Universidade Federal de Itajubá (UNIFEI)
[2] Universidade Federal de Itajubá (UNIFEI)

números primos.

Além disso, foram apresentadas no trabalho teoremas sobre a infinitude de primos de algumas formas, como $4n + 1$, $4n + 3$ e $6n + 5$, sendo feita a prova de que há infinitos primos das formas $4n + 3$ e $6n + 5$.

Ademais, há muitas conjecturas envolvendo números primos. Dentre elas, uma se destaca: a conjectura de Goldbach, que afirma que todo inteiro positivo par maior do que 4 pode ser escrito como a soma de dois inteiros primos ímpares.

Vale destacar que por séculos os matemáticos tentaram encontrar fórmulas cujos resultados são apenas números primos. Acreditava-se que o polinômio de Euler, dado por $f(n) = n^2 + n + 41$ assumia apenas valores primos para $n > 0$ e n inteiro. Porém, Euler mostrou que essa afirmação é falsa para $n = 40$ e $n = 41$.

No que tange a progressões aritméticas formadas apenas por números primos, há prova para a proposição que afirma que não existe uma progressão aritmética $a, a + b, a + 2b, a + 3b, \ldots$ com apenas números primos. Contudo, teoremas mostram que pode-se encontrar infinitos números primos em determinadas condições ligadas a progressões aritméticas. Nesse contexto, destaca-se o teorema de Dirichlet, que afirma que se a e b são inteiros positivos relativamente primos, então a progressão aritmética $a, a + b, a + 2b, \ldots$ contém infinitos números primos.

Ainda na questão do conjunto dos números primos e progressões aritméticas, destaca-se o teorema de Green-Tao, um resultado recente que afirma que existem progressões aritméticas de qualquer comprimento formadas apenas por números primos.

Além dos números primos, foi estudado o símbolo de Legendre, em que, dado p um número primo ímpar e $mdc(a, p) = 1$, é definido como 1 se a é um resíduo quadrático módulo p e -1 se a não é um resíduo quadrático módulo p

Os principais testes de primalidade foram estudados serão descritos a seguir.

Teste de Lucas: seja $N > 1$ um número natural. Se, para cada fator primo p de $N - 1$, existe um inteiro a tal que $a^{N-1} \equiv 1 \pmod N$ e $a^{(N-1)/p} \not\equiv 1 \pmod N$, então N é primo.

Teste de Pocklington: seja d um divisor positivo de $N - 1$, $d > \sqrt{N}$. Supondo que exista um inteiro a que satisfaça $a^{N-1} \equiv 1 \pmod N$ e $mdc(a^{(N-1/q)} - 1, N) = 1$ para cada primo q dividindo d então N é primo.

Teste de Pépin: seja $F_n = 2^{2^n} + 1$ o n-ésimo número de Fermat, com n um inteiro positivo. Então, F_n é um primo se, e somente se, $3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$. Este critério fornece uma caracterização simples para a primalidade de números de Fermat.

Teste de Miller-Rabin: é um dos testes de primalidade mais utilizados na prática, principalmente em criptografia. Ele é um teste probabilístico baseado em propriedades da aritmética modular. A ideia central é que, se n é um número ímpar, podemos escrever $n - 1 = 2^s d$, com d ímpar, e verificar condições sobre as potências de uma base a escolhida aleatoriamente. Mais precisamente, escolhe-se um inteiro a com $1 < a < n - 1$. Calcula-se $a^d \pmod n$. Se esse valor é 1 ou -1, n passa no teste para essa base. Caso contrário, elevamos sucessivamente ao quadrado: $a^{2^r d} \pmod n$, para $0 \leq r < s$. Se algum desses valores é congruente $a - 1$ módulo n, o número n também passa no teste para essa base. Caso contrário, n é composto.

Se n passar no teste para várias bases diferentes, a probabilidade de ser composto cai drasticamente. De fato, se n é composto, pelo menos 75% das escolhas de a irão detectar essa composição. Isso torna o teste de Miller-Rabin extremamente confiável para aplicações práticas.

Teste AKS (Agrawal–Kayal–Saxena): foi apresentado em 2002 e revolucionou a teoria dos testes de primalidade, pois foi o primeiro algoritmo a provar, de forma determinística e em tempo polinomial, se um número é primo ou não.

A ideia central do teste está ligada à verificação da congruência $(X + a)^n \equiv X^n + a \pmod n$, para determinados parâmetros r e a, sendo r o menor inteiro tal que $ord_r(n) > (\log n)^2$, onde $ord_r(n)$ é a ordem multiplicativa de n módulo r. Se esta congruência for satisfeita em condições apropriadas, conclui-se que n é primo.

O teste AKS é importante porque resolve uma questão fundamental em teoria da complexidade: saber se existe um algoritmo polinomial determinístico para a primalidade. Apesar de sua relevância teórica, ele não é

usado na prática, pois algoritmos probabilísticos como o de Miller-Rabin são muito mais rápidos.

O procedimento do AKS pode ser resumido em etapas: verificar se n é uma potência perfeita, escolher um parâmetro r adequado, e depois verificar a congruência acima para valores de a menores que $\sqrt{\varphi(r)}\, log\, n$. Caso n passe em todos os testes, é garantidamente primo.

Como exemplo de aplicação de um teste de primalidade, pode-se verificar a primalidade do número $N = 97$ usando o teste de Pocklington. Temos que $N - 1 = 996 = 12.83$. Tome $d = 83 > \sqrt{997}$ e $a = 2$ como base. Note que $2^{996} \equiv 1\,(mod\, 997)$ e $mdc(2^{996/83} - 1, 997) = mdc(2^{12} - 1, 997) = mdc(4095, 997) = 1$. Logo, pelo teste de Pocklington, 997 é primo.

A aplicação desses testes é fundamental, visto que, na era digital, a importância dos números primos aumentou significativamente, principalmente devido à criptografia. Sistemas criptográficos modernos, como RSA, dependem da dificuldade de fatorar números grandes em seus fatores primos. A segurança desses sistemas baseia-se no fato de que, mesmo que multiplicar dois grandes primos seja fácil, fatorar o produto é computacionalmente difícil.

Testes de primalidade rápidos e confiáveis permitem gerar chaves criptográficas seguras. O teste de Miller-Rabin, probabilístico, é amplamente utilizado devido à sua eficiência, permitindo verificar rapidamente a primalidade de números com centenas ou milhares de dígitos. Já o teste AKS, determinístico, embora mais lento, comprova que a primalidade pode ser decidida em tempo polinomial.

Além da criptografia, testes de primalidade são aplicados em outras áreas, como geração de números pseudoaleatórios, algoritmos de hashing, e protocolos de autenticação. Eles também são úteis em matemática pura, como na busca por primos gigantes e na pesquisa em teoria dos números.

A confiabilidade dos testes probabilísticos pode ser aumentada repetindo-os com diferentes bases, reduzindo a chance de erro. Esse aspecto é crucial em ambientes onde a segurança é prioritária, como transações financeiras e comunicação segura.

O desenvolvimento de algoritmos eficientes para testes de primalidade também estimula a pesquisa em complexidade computacional. Compreender quais problemas podem ser resolvidos em tempo polinomial versus probabilístico é essencial para a ciência da computação teórica.

Em suma, os testes de primalidade não apenas respondem a uma questão matemática clássica, mas também sustentam a infraestrutura da segurança digital moderna. Sem eles, a criptografia pública, que protege dados, senhas e transações na internet, seria impraticável.

Portanto, estudar e aprimorar testes de primalidade continua sendo uma área de extrema relevância. Desde a geração de chaves seguras até a proteção de informações sensíveis, esses testes garantem que o mundo digital funcione de maneira confiável e segura.

A importância desses testes reflete a intersecção entre teoria e prática. Eles demonstram como conceitos matemáticos abstratos podem ter impacto direto em tecnologia, segurança e comunicação global.

Conclusões

Neste trabalho foram estudados alguns tópicos não-elementares de Teoria dos Números. Nota-se que há resultados que já foram demonstrados como a infinitude dos números primos (Teorema de Euclides) ou a existência de progressões aritméticas formadas apenas por primos de qualquer comprimento (Teorema de Green-Tao). Porém, algumas conjecturas ainda não foram provadas, como a conjectura de Goldbach.

Além disso, menciona-se que no trabalho foram estudados a noção de reciprocidade quadrática e resultados envolvendo estimativas para números primos.

A parte principal do trabalho foi aplicar a terminologia e resultados da teoria dos números para estudar testes de primalidade. Os principais testes estudados foram os testes de Lucas, Pocklington, Pépin, e noções básicas envolvendo o teste AKS e o teste de Miller-Rabin.

Por fim, conclui-se que, em resumo, os testes de primalidade são essenciais para a criptografia moderna, a proteção de dados e o avanço da matemática aplicada. A pesquisa contínua nessa área promete aumentar a eficiência, confiabilidade e segurança em diversas aplicações tecnológicas.

Agradecimentos

Agradeço a Universidade Federal de Itajubá, ao meu orientador Marcelo Nogueira e ao CNPq pela bolsa concedida.

Referências

BURTON, David M. **Elementary Number Theory**. 7. ed. New York: McGraw-Hill, 2010.

MARTINEZ, Fábio Brochero *et al.* **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. 2. ed. Rio de Janeiro: SBM, 2011.