Jornal Eletrônico de Ensino e Pesquisa de Matemática
(1s.) **v. 2** 1 (2018): 81–89. ©JEEPEMA–ISSN-2594-6323.
www.dma.uem.br/kit/jeepema

Números Primos e Números de Mersenne

Doherty Andrade– FEITEP

RESUMO: Neste artigo faremos uma breve discussão sobre os números primos e sobre os números de Mersenne, origens e aplicações.

Palavras Chave: Números Primos. Primos de Mersenne.

Sumário

1. Introdução

Os números primos sempre despertaram a curiosidade dos matemáticos. Um número natural N é dito primo se os seus divisores positivos são apenas 1 e N. Ou seja, números inteiros que não se fatoram são chamados de primos. Acredita-se que Euclides tenha

sido o primeiro a demonstrar que existem infinitos números primos, há cerca de 2300 anos, na Proposição 20 do Livro IX dos seus *Os Elementos* há uma demonstração para esse resultado.

O argumento utilizado por Euclides é conhecido e admirado até hoje. A argumentação é bastante simples e vamos repeti-la aqui. Ele considerou que se existissem apenas os números primos $2, 3, 5, \ldots, p$, onde p seria o maior e último número primo, então o número

$$N = (2 \times 3 \times 5 \times \cdots \times p) + 1$$

não seria primo. Note que $N > p$. Assim, sendo N um número composto, N teria que ser divisível por algum dos primos listados acima: $2, 3, 5, \ldots, p$. Mas N não poderia ser divisível por 2, pois dividindo N por 2 sobraria resto igual a 1. O mesmo ocorre com os outros primos: dividindo N por qualquer outro primo, sobraria resto igual a 1. Assim, N seria divisível apenas por 1 e por ele mesmo. Ou seja, N seria um número primo, o que é um absurdo, pois $N > p$ e o maior primo é p. Logo, existem infinitos números primos.

Ao longo do tempo, muitas fórmulas foram propostas para gerar números primos arbitrariamente grandes: Fermat, por exemplo, conjecturou que todo número da forma $2^{2^n} + 1$ fosse primo, coube a Euler provar que isso não é verdade: $(2^{2^5} + 1)$ é número inteiro composto, divisível por 641. A maioria dos matemáticos acredita que não exista uma tal fórmula, sendo este um problema ainda sem resposta.

Existem, entretanto, algumas fórmulas que geram famílias interessantes de primos. A fórmula deste tipo que mais nos interessa aqui é $M_n = 2^n - 1$, os chamados números de Mersenne. Quando M_p é primo, dizemos que M_p é um primo de Mersenne. Parte da

razão pela qual números desta forma são interessantes é que apesar de M_p nem sempre ser primo é relativamente fácil testar computacionalmente para um dado expoente p, mesmo bastante grande, se M_p é primo ou composto. Por isso muitos dos números grandes primos conhecidos atualmente são primos de Mersenne.

Embora números da forma $M_n = 2^n - 1$ já fossem conhecidos por Euclides, deve-se a Mersenne (1588-1648) sua popularização. Mersenne durante sua vida no mosteiro mantinha correspondência com todos os nomes importantes no domínio do conhecimento. Por meio de correspondências Mersenne transmitia notícias relativas a avanços científicos em troca de mais informações para divulgação. Deste modo, divulgando questões e solicitando contribuições, estimulou o desenvolvimento científico. Depois da sua morte, foram encontradas cartas de 78 correspondentes espalhados pela Europa, entre os quais Fermat na França, Huygens na Holanda, Pell e Hobbes na Inglaterra e Galileu e Torricelli na Itália, entre outros. Mersenne foi um grande interessado no conceito de divisibilidade, em correspondências com Fermat questionava-o sobre a possível factoração de alguns números.

Muitos matemáticos antigos acreditavam que $2^p - 1$ seria primo para qualquer p primo considerado. Em 1536, Hudalrichus Regius apresentou a factorização de $2^{11} - 1 = 2047 = 23 \times 89$, demonstrando que a convicção era incorreta.

Um número de Mersenne M_n só tem chance de ser primo, se n for primo. De fato.

Proposition 1.1 *Se $2^n - 1$ é primo, então n é primo.*

Demonstração: Se $n = ab$ com $a, b \geq 2$ então $1 < 2^a - 1 < 2^n - 1$ e $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$ e $2^n - 1$ é

composto. ∎

Esse resultado simplifica a busca por números primos de Mersenne: basta procurar por M_p primo, considerando apenas p primo. Mas isto não basta, pois pode ocorrer que p seja primo, mas M_p não, como já vimos.

Mesmo assim, algumas questões relacionadas aos números primos de Mersenne ainda não foram respondidas. Veja duas delas:

1. existem infinitos primos de Mersenne?
2. existem infinitos primos p para os quais M_p seja primo?

Não se sabe responder a essas perguntas, pois não se sabe demonstrar matematicamente.

Conjectura-se, no entanto, que existam infinitos primos p para os quais tem-se que M_p seja primo. Por isso há uma busca computacionalmente insana pelos números de Mersene que são primos. Você pode também participar da descoberta de novos números primos de Mersenne, basta aderir ao projeto GIMPS, *Great Internet Mersenne Prime Search*, acesse www.mersenne.org e deixe seu computador executar um algoritmo para encontrar novos números primos de Mersenne.

Divulgado recentemente (03/Jan/2018) pelo projeto GIMPS a descoberta de mais um número primo de Mersenne. Chamado simplesmente de

$$M_{77232917} = 2^{77232917} - 1,$$

é o maior número primo de Mersenne conhecido, ele tem mais de 23 milhões de dígitos, quase um milhão a mais de dígitos do que o recorde anteriormente alcançado em 2016. O progresso comutacio-

nal trouxe a possibilidade, e a facilidade, de testarmos conjecturas no campo da teoria dos números.

Os números primos são úteis em criptografia, em que são utilizados na criação de senhas (chaves) para proteger dados confidenciais. A busca por números primos cada vez maiores ou números primos de Mersenne cada vez maiores é só um exemplo nessa corrida. Sem esses números primos não seria possível efetuar compras seguras na internet. Atualmente, são usados números primos com algumas centenas de dígitos, mas à medida que os computadores forem se tornando mais rápidos, números primos maiores serão necessários. A corrida parece que não tem fim.

Essa corrida é altamente tecnológica e exige processadores cada vez mais velozes e confiáveis. Nesta corrida, os primos gêmeos (um par de primos p e q cuja diferença entre eles é 2, por exemplo, 5 e 7, 17 e 19) estão relacionados a um episódio importante na indústria dos computadores. Em 1993, o professor de matemática Thomas Nicely, tentando melhorar o cálculo da soma de Brun utilizando cinco computadores 486 e um Pentium, obteve resultados diferentes nas duas máquinas. O resultado obtido pelo computador 486 estava de acordo com os resultados já publicados. Mas os resultados obtidos com o Pentium não concordavam com os dados já publicados. Depois de várias verificações foi identificado o problema: o Pentium apresentava um erro 10^{10} vezes superior ao 486. O prof. Nicely comunicou o fato a Intel, fabricante do processador, que o ignorou. A notícia se espalhou pela internet e o bug foi confirmado por dezenas de pessoas até que a notícia chegou às TVs. Após a IBM anunciar que ia deixar de comercializar PCs com Pentium, a cotação das suas ações da Intel despencaram nas Bolsas de Valores. Algum tempo, a Intel lança no mercado o Pentium II e III sem bugs e reconquista a confiança do mercado.

O sistema de criptografia atualmente usado é o RSA. É um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto de Tecnologia de Massachusetts (MIT), Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman. É considerado um dos sistema mais seguros, já que resisitiu a todas as tentativas de quebrá-lo e fundamenta-se em teorias clássicas dos números. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, é uma das grandes inovações em criptografia de chave pública.

2. Números de Mersenne compostos

E quanto aos números de Mersenne compostos, são infinitos? Euler, mostrou o seguinte teorema:

Teorema 1 *Seja $k > 1$. Se $p = 4k + 3$ é primo, então $2p + 1$ é primo se, e somente se, $2^p \equiv 1 mod(2p + 1)$.*

Assim, se $p = 4k + 3$ e $2p + 1$ são primos, então o número de Mersenne $2^p - 1$ é composto. Logo, é razoável conjecturar que existem infinitos números de Mersenne compostos, pois existem infinitos pares primos $(p, 2p + 1)$.

Primos de Mersenne são interessantes também por causa de números perfeitos. Dado $n \in \mathbb{N}^*$, definimos

$$\sigma(n) = \sum_{d|n} d,$$

a soma dos divisores (positivos) de n. Um inteiro positivo n é dito perfeito se $\sigma(n) = 2n$. Como exemplo, apresentamos os primeiros números perfeitos: $6 = 1 + 2 + 3 + 6$, $28 = 1 + 2 + 4 + 7 + 14 + 28$, 496 e 8128.

A última proposição do nono livro dos Elementos de Euclides, sua mais famosa obra, Euclides não só define número perfeito, como enuncia e demonstra um método para calculá-los, método conhecido por fórmula dos números perfeitos euclidianos.

Proposition 2.1 *Se M_p é um primo de Mersenne, então $2^{p-1}M_p$ é um número perfeito.*

Além disso, todo número perfeito par é da forma $2^{p-1}M_p$ para algum primo p, sendo M_p um primo de Mersenne.

Entre outros resultados da teoria dos números, Euler demonstrou o recíproco do teorema de Euclides: que todos os números perfeitos pares são da forma $(2^{k-1}-1)(2^k-1)$.

Teorema 2 *Se n é um número perfeito par, então $n = (2^{k-1}-1)(2^k-1)$, com 2^k-1 número primo.*

3. Alguns problemas clássicos

Iniciamos com a conjectura de Goldbach. Ela afirma que se n é um natural maior do que ou igual a 4, então n pode ser escrito como soma de dois números primos. Por exemplo, 6=3+3 e 8=3+5.

O matemático peruano Harald Helfgott, tornou-se 2m 2015 o primeiro latino-americano e também o cientista mais jovem a ganhar o Prêmio de Pesquisa Humboldt, concedido pela Fundação Alexander von Humboldt, da Alemanha. Ele recebeu o prêmio por ter respondido uma pergunta que vinha desafiando matemáticos por quase trezentos anos: é verdade que todo número ímpar maior do que cinco pode ser expresso como uma soma de três números primos? Essa é a conjecutra fraca de Goldbach.

Em 1742, o matemático prussiano Christian Goldbach enviou uma carta a seu colega suíço Leonhard Euler na qual propunha que todo número par maior do que dois podia ser expresso como a soma de dois números primos. Ainda não foi possível encontrar uma demonstração para esse conjectura. Desde Goldbach e Euler essa conjectura espera por uma demonstração ou refutação.

Tomás Oliveira e Silva, Siegfried Herzog e Silvio Pardi, verificaram em 2014 que até o número 4×10^{18} a conjectura se mantém. Veja o artigo em: Mathematics of Computation 83, 2033- 2060 (2014). *Empirical verification of the even Goldbach conjecture, and computation of prime gaps up to* 4×10^{18}.

Outra questão em aberto é a conjectura dos números primos gêmeos diz que existem infinitos números primos gêmeos Ao leitor interessado nos assuntos tratados aqui recomendamos o livro [4] que contém fatos históricos e as demonstrações.

4. Conclusão

Os números naturais, início e origem dos corpos numéricos, apesar de sua simplicidade, escondem muitos mistérios: muitas perguntas permanecem ainda sem respostas. Vimos aqui uma pequena parte dos estudos avançados sobre a teoria dos números primos e suas aplicações: criar senhas invioláveis, testar processadores e arrebanhar uma legião de estudiosos para decifrar seus segredos. Aceita o convite?

Referências

1. P. Ribenboim, The new book of prime number records, 3rd edition, Springer-Verlag, New York, NY, 1995. pp. xxiv+541, ISBN 0-387-94457-5.

2. Nielsen, Pace P., "Odd perfect numbers have at least nine distinct prime factors,"Math. Comp., 76:260 (2007) 2109–2126.

3. McKee, Maggie (14 de maio de 2013). «First proof that infinitely many prime numbers come in pairs». Nature. ISSN 0028-0836.

4. H.M. Edwards, Riemann zeta function. Academic Press, 1974 88