

Primos que nos protegem

Roberto Lobo 11 de agosto de 2014

Os números primos são conhecidos de todos que estudaram na escola fundamental por serem divisíveis apenas por eles próprios e por um, sendo usados para obter, por exemplo, o máximo divisor comum de dois números inteiros. Não se dá muita importância a eles nessa fase dos estudos. No entanto, os números primos formam um mundo fascinante.

Como os números inteiros são a base de toda a aritmética e os números primos são a base dos números inteiros, pois todo número inteiro é um produto de números primos, eles são as unidades mínimas da matemática (como os átomos são para a matéria) que tudo descrevem. A partir deles se constrói a própria matemática. Os inteiros não primos seriam as moléculas formadas pela combinação de primos.

Todo número inteiro pode ser decomposto de uma única forma, em um produto de primos. Os primos são em número infinito e a soma de seus inversos também é infinita. Há também números primos chamados de gêmeos, distando um do outro pela diferença mínima de dois inteiros, como 5 e 7, 41 e 43 etc. Não se sabe ainda se há um número infinito desses gêmeos.

Os números primos se distribuem ao longo da sequência dos números inteiros sem uma regra fixa, mas eles vão rareando quanto mais longe se sobe na escala dos números inteiros. Entretanto, há sempre um número primo entre um número inteiro e seu dobro. É possível estimar quantos números primos existem entre o número 2 (que é o primeiro número primo) e N (um inteiro qualquer) com crescente precisão (quanto maior for N mais nos aproximamos do valor real de quantos números primos existem entre 2 e N).

Acredita-se, mas ainda não se sabe provar, que todo o número par pode ser escrito como a soma de dois primos (chamada “Conjetura Forte de Goldbach”, proposta por ele em 1742). Tente provar isso ou achar um contra exemplo e ficará famoso.

Se a conjetura for verdadeira, então seria simples provar que todo o número ímpar maior que 5 poderia ser escrito como a soma de três primos (a “Conjetura fraca de Goldbach”). Mesmo sem provar a conjetura forte, 270 anos depois do desafio de Goldbach (2012), um matemático peruano chamado Harald Helfgott, da École Normale Supérieure de Paris, demonstrou (ao que tudo indica) que a conjetura fraca é verdadeira. Como se vê, os números primos são ainda objeto de muitas pesquisas contemporâneas.

Apesar da aparente simplicidade desses números, há resultados e teoremas de enorme complexidade e importância sobre os números primos. A pesquisa para encontrar primos cada vez maiores vem ocupando matemáticos há muitos séculos, mas se intensificou tremendamente nas últimas décadas. Utilizando a capacidade de cálculo dos computadores e as redes de comunicação.

A razão dessa intensificação está, como poucos podem imaginar, em uma questão essencialmente prática e cotidiana: a necessidade cada vez maior de segurança no uso dos cartões de crédito cuja decodificação se baseia em teoremas existentes sobre os números primos e, para ser efetiva, o tamanho desses números precisa ser descomunal, por exemplo, números comprovadamente primos formados por mais de 150 algarismos.

Não sabemos nem transformar esse número gigante em palavras (zilhões?), mas graças a ele e aos teoremas dos primos criativamente reunidos por um cientista de computação e dois matemáticos (Rivest, Adleman e Shamir), todos do MIT, é possível fazer códigos praticamente indecifráveis. Códigos que são rotineiramente utilizados para assegurar o sigilo de nossos cartões de crédito. O sistema que eles criaram é chamado RSA, as iniciais de seus sobrenomes.

Esse é mais um exemplo de como a ciência básica é fundamental na criação e aplicação de novas tecnologias. Quem gostar de desafios e da elegância da matemática, terá uma grande diversão ao dedicar um pouco de seu tempo para compreender as belas propriedades dos átomos da matemática.