Dois Mais Dois

Computadores, segredos e os números primos

Por Luiz Barco

Você sabe fatorar um número? Seguramente, a pergunta o levará a recordar o primeiro curso de álgebra e a decomposição em fatores primos, o que não é propriamente uma novidade. Novidade interessante é que um verdadeiro exército de homens bem preparados busca hoje, com o auxílio de uma rede de computadores espalhados pelo planeta, fatorar números, enormes, com mais de 100 dígitos, que por sua vez são produto de fatores igualmente grandes. Com base na fatoração de números gigantescos que permitem quebrar códigos criptográficos, Ronald L. Rivest, Adi Shamir e Leonard Adelman, pesquisadores do Instituto de Tecnologia de Massachusetts, nos Estados Unidos, criaram o sistema *RSA* - sigla resultante da junção da primeira letra do sobrenome de cada um deles.

O sistema consiste em escolher dois números primos grandes que depois de multiplicados geram um produto. A mensagem, então, é convertida em uma seqüência de números por algum método convencional e a seguir é codificada por uma operação baseada no número gerado. Essa mensagem só poderá ser decodificada por uma segunda operação matemática com base nos números primos originais. Mas, se alguém conseguir fatorar o número gerado, a mensagem poderá ser decifrada. Para que isso não ocorra, é imprescindível escolher números primos suficientemente grandes, assegurando- se que o número gerado não poderá ser fatorado. Em' 1977, Rivest calculou que um código de 125 dígitos - o produto de dois números primos de aproximadamente 63 dígitos - seria seguro, pois levaria cerca de 40 quatrilhões de anos para ser quebrado pelos mais rápidos computadores. Ele não imaginava que hoje, doze anos de- pois, isso pode ser feito em um ano.

Por isso, a segurança de tais sistemas vive sendo abalada e eles têm de ser substituídos em caráter de urgência,: Para se ter uma idéia do método responsável por tal proeza, vamos tomar como exemplo o número 6, um número composto que pode ser quebrado em dois fatores primos, 2 e 3, cujo produto recompõe o 6. Usamos o termo fatorar para indicar a idéia de achar os dois números primos cujo produto resulta num número código, o 6 nesse caso.

Enquanto os pesquisadores de Massachusetts desenvolviam seu sistema, Carl Pomerance, pesquisador da Universidade da Geórgia, Estados Unidos, projetou um método que chamarei de "peneira quadrática" para descobrir fatores primos. Trata-se de encontrar dois números cujos quadrados divididos pelo número código deixam o mesmo resto. Por exemplo, para o 15 encontramos 8 e 2, cujos quadrados (64 e 4) na divisão por 15, deixam o mesmo resto (4). Mas atenção: só valem resultados inteiros, e, corno 4 não é divisível por 15, o quociente é zero. Assim, zero multiplicado por 15 dá zero e para 4 o resto é 4.

Uma vez encontrados os dois números - 8 e 2 -.- na base do acerto e erro, efetuamos a subtração 8 ─ 2 = 6, cujo resultado - 6 - vamos subtrair de 15 tantas vezes quanto possível, sem produzir números negativos. O resultado será 3, um dos fatores primos de 15. Dois outros pesquisadores, Mark S. Manasse, da *Digit Equipment Corporation* (*DEC*). em Paio Alto, e Argen K. Lenstra, da Universidade de Chicago, completaram o método da "peneira quadrática" - vagaroso para fatorar números pequenos mas muito mais eficiente que qualquer outro para números grandes. Além disso, o método tem a vantagem de permitir que vários computadores diferentes compartilhem a tarefa de achar fatores. Por exemplo, um computador no *DEC* controla as tarefas de fatorar um número (código) de 100 dígitos, enquanto outros centros de computação nos Estados Unidos. Holanda e Austrália compartilham o resto dos cálculos. Assim, já no vigésimo sexto dia do projeto, Lenstra e Manasse, trabalhando em rede com mais de 400 computadores velozes, quebraram todos os recordes anteriores ao encontrar os dois grandes fatores primos para um número (código) de mais de 100 dígitos. Foi a coroação de um dos mais ambiciosos projetos de computação já feitos até aqui.

Luiz Barco é professor da Escola de Comunicações e Artes da Universidade de São Paulo