teoria de números computacional

cláudia mendes araújo

2024/2025

lcc+lmat | uminho

números de Fermat

Os inteiros

$$F_n = 2^{2^n} + 1$$

são chamados números de Fermat.

Fermat conjecturou que estes inteiros são todos primos ($\approx$1640). De facto, os primeiros são primos, nomeadamente: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$.

No entanto, em 1742, Euler demonstrou que $F_5 = 2^{2^5} + 1$ é composto.

exemplo. O número de Fermat $F_5 = 2^{2^5} + 1$ é divisível por 641.

Podemos mostrar que $641 \mid F_5$ sem realizar explicitamente a divisão, utilizando algumas observações menos evidentes.

Note-se que

$$641 = 5 \times 2^7 + 1 = 2^4 + 5^4.$$

Assim,

$$\begin{aligned}
2^{2^5} + 1 &= 2^{32} + 1 \\
&= 2^4 \times 2^{28} + 1 \\
&= (641 - 5^4) \times 2^{28} + 1 \\
&= 641 \times 2^{28} - 5^4 \times (2^7)^4 + 1 \\
&= 641 \times 2^{28} - (5 \times 2^7)^4 + 1 \\
&= 641 \times 2^{28} - (641 - 1)^4 + 1 \\
&= 641(2^{28} - 641^3 + 4 \times 641^2 - 6 \times 641 + 4).
\end{aligned}$$

Deste modo, verifica-se que $641 \mid F_5$.

O seguinte resultado é útil na fatorização dos números de Fermat, pois impõe uma forte restrição sobre quais primos podem dividi-los.

Em particular, isso significa que os fatores primos de F_n crescem rapidamente, tornando a sua fatorização difícil para valores grandes de n.

teorema. Todo o divisor primo do número de Fermat $F_n = 2^{2^n} + 1$ é da forma $2^{n+2}k + 1$.

observação. A prova deste teorema baseia-se em teoria de grupos e na ordem de um elemento módulo p.

exemplo. Pelo teorema anterior, sabemos que todo o divisor primo de

$$F_3 = 2^{2^3} + 1 = 257$$

deve ser da forma $2^5 k + 1 = 32k + 1$.

Como não existem números primos dessa forma que sejam menores ou iguais a $\sqrt{257}$, podemos concluir que $F_3 = 257$ é primo.

exemplo. Ao fatorizar

$$F_6 = 2^{2^6} + 1,$$

sabemos, pelo teorema anterior, que todos os seus fatores primos são da forma $2^8 k + 1 = 256k + 1$.

Assim, basta realizar divisões de teste de F_6 por primos da forma $256k + 1$ que não excedam $\sqrt{F_6}$.

Após um cálculo considerável, encontramos um divisor primo com $k = 1071$: $274177 = 256 \times 1071 + 1$ divide F_6.

observação. Têm sido dedicados consideráveis esforços à fatorização dos números de Fermat, mas nenhum novo primo de Fermat foi encontrado além de $F4$.

Muitos matemáticos acreditam que não existem mais números de Fermat primos.

Até ao momento, são conhecidos 328 números de Fermat compostos, mas apenas sete foram totalmente fatorizados: F_5, F_6, F_7, F_8, F_9, $F10$ e F_{11}.

O número F_9, com 155 dígitos decimais, foi fatorizado em 1990 por Mark Manasse e Arjen Lenstra, utilizando o crivo do corpo dos números, com cálculos distribuídos por centenas de matemáticos e cientistas da computação, levando dois meses para ser concluído.

Já F_{11} foi parcialmente fatorizado por Richard Brent em 1989, usando o método das curvas elípticas, e totalmente fatorizado apenas em 1995.

Sabe-se que F_n é composto para $n = 20$ e $n = 24$, embora não se tenham encontrado fatores.

O maior índice para o qual se sabe que F_n é composto é $n = 18233954$.

O primeiro número de Fermat composto para o qual se encontrou um fator próprio com mais de 100000 dígitos foi F_{382447} em 1999.

O menor número de Fermat ainda não demonstrado como composto é F_{33}, caso realmente o seja.

Os números de Fermat são relevantes para a geração de números pseudoaleatórios, álgebra abstrata e teoria de números.

A 14 de janeiro de 2025 foi publicado que $99 \times 2^{5798449} + 1$ divide $F_{5798447}$ (sendo o terceiro maior número de Fermat composto conhecido).

Wilfrid Keller mantém um registo atual e detalhado de todos os fatores conhecidos de Fermat:

http://www.prothsearch.com/fermat.html

É possível provar que existe um número infinito de números primos utilizando os números de Fermat. Comecemos por demonstrar que quaisquer dois números de Fermat distintos são primos entre si. O seguinte lema será necessário.

lema. Seja $F_k = 2^{2^k} + 1$ o k-ésimo número de Fermat, onde k é um inteiro não negativo. Então, para todos os inteiros positivos n, temos:

$$F_0 F_1 F_2 \dots F_{n-1} = F_n - 2.$$

demonstração. A prova segue por indução. Para $n = 1$, a identidade escreve-se como:

$$F_0 = F_1 - 2.$$

Isto é obviamente verdadeiro, pois $F_0 = 3$ e $F_1 = 5$.

Seja $n \in \mathbb{N}$ tal que

$$F_0 F_1 F_2 \dots F_{n-1} = F_n - 2.$$

Sob esta hipótese, podemos facilmente demonstrar que a identidade também se verifica para $n+1$, pois:

$$\begin{aligned} F_0F_1F_2\ldots F_{n-1}F_n &= (F_0F_1F_2\ldots F_{n-1})F_n \\ &= (F_n - 2)F_n \\ &= (2^{2^n} + 1 - 2)(2^{2^n} + 1). \end{aligned}$$

Sabemos que

$$\begin{aligned} (2^{2^n} - 1)(2^{2^n} + 1) &= (2^{2^n})^2 - 1^2 \\ &= 2^{2^{n+1}} - 1 \\ &= F_{n+1} - 2, \end{aligned}$$

o que conclui a prova.

teorema. Sejam m e n inteiros não negativos distintos. Então, os números de Fermat F_m e F_n são primos entre si.

demonstração. Sem perda de generalidade, podemos assumir que $m < n$. Pelo lema anterior, sabemos que

$$F_0 F_1 F_2 \ldots F_m \ldots F_{n-1} = F_n - 2.$$

Seja d um divisor natural comum de F_m e F_n. Como $d \mid (F_0 F_1 F_2 \ldots F_m \ldots F_{n-1})$ e $d \mid F_n$, podemos afirmar que

$$d \mid (F_n - F_0 F_1 F_2 \ldots F_m \ldots F_{n-1}) = 2.$$

Consequentemente, $d = 1$ ou $d = 2$. Como F_m e F_n são ímpares, $d = 1$ e, portanto, $\mathrm{m.d.c.}(F_m, F_n) = 1$.

Usando os números de Fermat, apresentamos agora uma prova de que existe um número infinito de números primos. Primeiro, notamos que cada número de Fermat F_n tem um divisor primo p_n. Como $\mathrm{m.d.c.}(F_m, F_n) = 1$, sabemos que $p_m \neq p_n$ sempre que $m \neq n$. Assim, podemos concluir que existe um número infinito de números primos.