ACEPIPE MATEMÁTICO

O poder dos restos

Quando números gigantes obedecem a pequenos ciclos

Há uma curiosa maneira de fazer com que números imensos se tornem pequenos: ignorar quase tudo o que sabemos sobre eles.

Imagine um relógio marcando 9 horas. Oito horas depois, seus ponteiros indicarão 5 horas. A aritmética usual nos informa que $9 + 8 = 17$, mas o relógio parece discordar: para ele, 17 e 5 representam a mesma posição.

Em linguagem matemática, escrevemos

$$17 \equiv 5 \pmod{12}.$$

Essa notação expressa que 17 e 5 deixam o mesmo resto na divisão por 12. Mais precisamente, dois inteiros a e b são **congruentes módulo** m, com $m \geq 2$, quando sua diferença é divisível por m:

$$\boxed{a \equiv b \pmod{m} \iff m \mid (a - b).}$$

A ideia é simples: em vez de distinguir todos os inteiros, agrupamos aqueles que possuem o mesmo resto.

Entretanto, essa aparente simplificação esconde uma propriedade extraordinária.

Um número que não precisamos conhecer

Considere o número

$$N = 7^{7^7}.$$

Seria possível determinar seus dois últimos algarismos sem calcular o próprio número?

O expoente 7^7 já ultrapassa oitocentos mil. Calcular N diretamente seria uma tarefa descomunal. Mas a pergunta não exige conhecer todos os seus algarismos. Exige apenas determinar seu resto na divisão por 100.

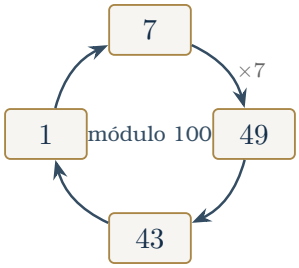
Comecemos observando que

$$\begin{aligned} 7^1 &\equiv 7 \pmod{100}, \\ 7^2 &\equiv 49 \pmod{100}, \\ 7^3 &\equiv 43 \pmod{100}, \\ 7^4 &\equiv 1 \pmod{100}. \end{aligned}$$

A última congruência revela algo decisivo: multiplicar uma potência de 7 por 7^4 não altera seu resto módulo 100.

Assim, os restos das potências de 7 repetem-se em ciclos de quatro termos:

7, 49, 43, 1, 7, 49, 43, 1,...



Ciclo dos restos das potências de 7 na divisão por 100.

Basta, portanto, determinar o resto do expoente 7^7 na divisão por 4.

Como

$$7 \equiv -1 \pmod 4,$$

temos

$$7^7 \equiv (-1)^7 \equiv -1 \equiv 3 \pmod 4.$$

Consequentemente, existe um inteiro k tal que $7^7 = 4k + 3$. Logo,

$$\begin{aligned} 7^{7^7} &= 7^{4k+3} \\ &= (7^4)^k \cdot 7^3 \\ &\equiv 1^k \cdot 343 \pmod{100} \\ &\equiv 43 \pmod{100}. \end{aligned}$$

Portanto,

> **Os dois últimos algarismos de 7^{7^7} são 43.**

O infinito que se repete

O resultado é surpreendente: um número com centenas de milhares de algarismos termina exatamente como o modesto número 343.

Não há coincidência. A explicação está na periodicidade das potências quando observadas módulo um inteiro.

Nesse contexto, números de grandezas completamente distintas podem pertencer à mesma classe de congruência. O que importa deixa de ser o seu tamanho e passa a ser sua posição em um ciclo.

É como substituir a reta dos inteiros por um relógio: podemos avançar indefinidamente e, ainda assim, retornar à posição de partida.

A aritmética modular nos ensina, portanto, uma lição que ultrapassa o próprio cálculo:

> *A grandeza de um número nem sempre determina a dificuldade de compreendê-lo. Às vezes, a estrutura que procuramos está justamente naquilo que resta.*

Professor Yuri Politano · *Politano Aprova*