Soluções: Congruência

Prof. Giuliano Boava

1. Dizer que $n+1$ divide n^3-1 é equivalente a dizer que $n^3-1 \equiv 0 \bmod(n+1)$. Assim, vamos estudar a congruência de n^3-1 módulo $n+1$. Note que

$$\begin{aligned} n^3-1 &\equiv n^3-1-n^2(n+1) && \bmod(n+1) \\ &\equiv -n^2-1 && \bmod(n+1) \\ &\equiv -n^2-1+n(n+1) && \bmod(n+1) \\ &\equiv n-1 && \bmod(n+1) \\ &\equiv n-1-(n+1) && \bmod(n+1) \\ &\equiv -2 && \bmod(n+1). \end{aligned}$$

   Isso diz que $n^3-1 \equiv 0 \bmod(n+1)$ se, e somente se, $-2 \equiv 0 \bmod(n+1)$, isto é, $n+1$ divide -2. Como os divisores de -2 são -1, 1, -2 e 2, então os valores de n para os quais $n+1$ divide -2 são $n_1=-2$, $n_2=0$, $n_3=-3$ e $n_4=1$.

2. Pelo teorema de Euler-Fermat, $p^{q-1} \equiv 1 \bmod(q)$ e $q^{p-1} \equiv 1 \bmod(p)$ (o teorema se aplica pois p e q são primos distintos e, portanto, $\varphi(p)=p-1$, $\varphi(q)=q-1$ e $\text{mdc}(p,q)=1$). Como $p^{q-1} \equiv 0 \bmod(p)$ e $q^{p-1} \equiv 0 \bmod(q)$, então $p^{q-1}+q^{p-1} \equiv 1 \bmod(p)$ e $p^{q-1}+q^{p-1} \equiv 1 \bmod(q)$. Isso diz que $p^{q-1}+q^{p-1}-1$ é múltiplo de p e de q. Como p e q são primos distintos, então $p^{q-1}+q^{p-1}-1$ é múltiplo de pq, o que mostra que $p^{q-1}+q^{p-1} \equiv 1 \bmod(pq)$.

3. Todo número da forma $n = 20000\ldots011$ se escreve como $n = 2\cdot 10^k+11$, para algum $k>2$. Nosso objetivo é mostrar que existem infinitos valores de k para os quais $2\cdot 10^k+11 \equiv 0 \bmod(2011)$. Para isso, observe que

$$2\cdot 10^k+11 \equiv 0 \mod(2011) \iff 2\cdot 10^k+11 \equiv 2011 \mod(2011) \iff$$

$$2\cdot 10^k \equiv 2000 \mod(2011) \iff 2000\cdot 10^{k-3} \equiv 2000 \mod(2011).$$

   Como 2000 e 2011 são primos entre si, então podemos "cortar" o 2000 da congruência acima. Assim,

$$2000\cdot 10^{k-3} \equiv 2000 \mod(2011) \iff 10^{k-3} \equiv 1 \mod(2011).$$

   Visto que 10 e 2011 são primos entre si, então $10^{\varphi(2011)} \equiv 1 \bmod(2011)$ e, com isso, $10^{\varphi(2011)t} \equiv 1 \bmod(2011)$ para qualquer t natural. Fazendo $k-3=\varphi(2011)t$, vemos que para qualquer k da forma $\varphi(2011)t+3$ tem-se que $n=2\cdot 10^k+11$ é múltiplo de 2011.

4. O problema é equivalente a mostrar que não existe x tal que $x^3 \equiv 2 \bmod(37)$. Suponha, por contradição, que exista x tal que $x^3 \equiv 2 \bmod(37)$. Note que x não é múltiplo de 37 pois, neste caso, $x^3 \equiv 0 \bmod(37)$. Elevando ambos os lados a 12, obtemos $x^{36} \equiv 2^{12} \bmod(37)$. Fazendo as contas, observamos que

$$2^{12} \equiv 2^2\cdot(2^5)^2 \equiv 4\cdot(32)^2 \equiv 4\cdot(-5)^2 \equiv 4\cdot 25 \equiv 100 \equiv 26 \mod(37).$$

   Por outro lado, segue do teorema de Euler-Fermat que $x^{36} \equiv 1 \bmod(37)$, uma contradição! Logo, não existe x inteiro tal que $x^3 \equiv 2 \bmod(37)$.

5. Encontrar os 3 últimos dígitos de um número n na notação decimal é equivalente a estudar a congruência de n módulo 1000. Primeiramente, note que $1000 = 2^3\cdot 5^3$ e, portanto,

$\varphi(1000) = 1000 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 400$. Sabendo que 3 e 1000 são primos entre si, segue do teorema de Euler-Fermat que $3^{400} \equiv 1 \bmod(1000)$. Assim,

$$3^{2012} \equiv (3^{400})^5 \cdot 3^{12} \equiv 3^{12} \mod(1000)$$

e isso mostra que basta encontrar os últimos 3 dígitos de 3^{12}. Para finalizar,

$$3^{2012} \equiv 3^{12} \equiv (3^6)^2 \equiv (729)^2 \equiv (-271)^2 \equiv 73441 \equiv 441 \mod(1000),$$

ou seja, os últimos 3 dígitos são 441.