Material Teórico - Módulo Aritmética dos Restos

O Pequeno Teorema de Fermat - Parte 2

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

18 de setembro de 2023

Neste material, continuaremos apresentando aplicações do Pequeno Teorema de Fermat.

Exemplo 1. *Encontre todos os números primos p tais que p divide $3^p + 2023$.*

Solução. Pelo Pequeno Teorema de Fermat, temos que $3^p \equiv 3 \pmod{p}$, logo, $p \mid (3^p - 3)$. Escrevendo $3^p + 2023 = 3^p - 3 + 2026$ temos que $p \mid (3^p + 2023)$ se, e somente se, $p \mid 2026$.

Agora, observe que $2026 = 2 \cdot 1013$. Além disso, utilizando os critérios de divisibilidade, podemos ver facilmente que 1013 não é divisível por 2, 3, 5, 7 e 11. Analisando a divisibilidade de 1013 pelos demais primos menores ou iguais a 31 — veja que $32^2 = 1024 > 1013$ — obtemos:

$$\begin{array}{r|l} 1013 & 13 \\ 103 & 77 \\ 12 & \end{array} \qquad \begin{array}{r|l} 1013 & 17 \\ 163 & 59 \\ 10 & \end{array} \qquad \begin{array}{r|l} 1013 & 19 \\ 63 & 53 \\ 6 & \end{array}$$

$$\begin{array}{r|l} 1013 & 23 \\ 93 & 44 \\ 1 & \end{array} \qquad \begin{array}{r|l} 1013 & 29 \\ 143 & 34 \\ 27 & \end{array} \qquad \begin{array}{r|l} 1013 & 31 \\ 83 & 32 \\ 21 & \end{array}$$

Assim, pelo crivo de Eratóstenes, concluímos que 1013 é primo.

Dessa forma, os números primos p tais que p divide $3^p + 2023$ (que coincidem com aqueles tais que $p \mid 2026 = 2 \cdot 1013$) são $p = 2$ e $p = 1013$. □

Exemplo 2. *Se p e q são primos distintos, prove que pq divide $p^{q-1} + q^{p-1} - 1$.*

Solução. Como p e q são primos distintos, temos $\text{mdc}\,(p,q) = 1$, logo, podemos aplicar o Pequeno Teorema de Fermat para obter $p^{q-1} \equiv 1 \pmod{q}$. Assim, q divide $p^{q-1} - 1$. Como q claramente divide q^{p-1}, pois $p > 1$, temos que q divide

$$p^{q-1} - 1 + q^{p-1} = p^{q-1} + q^{p-1} - 1.$$

Repetindo o argumento acima trocando q por p, obtemos que p também divide $p^{q-1} + q^{p-1} - 1$.

Então, como p e q dividem $p^{q-1} + q^{p-1} - 1$ e são primos entre si, concluímos que pq divide $p^{q-1} + q^{p-1} - 1$. □

Exemplo 3. *Encontre todos os inteiros positivos n tais que $n \mid (3^n - 2^n)$.*

Solução. É claro que $1 \mid (3^1 - 2^1)$. Então, suponhamos que $n > 1$ divide $3^n - 2^n$.

Consideremos p, o menor número primo que divide n. Assim, $p \mid (3^n - 2^n)$, ou seja, $3^n \equiv 2^n \pmod{p}$.

Note que $p > 3$, pois, se $p = 2$, obteríamos $2 \mid 3^n$ (o que é impossível) e, se $p = 3$, obteríamos $3 \mid 2^n$ (novamente uma contradição).

Sendo $p > 3$, o Pequeno Teorema de Fermat garante que

$$2^{p-1} \equiv 1 \pmod{p} \text{ e } 3^{p-1} \equiv 1 \pmod{p},$$

o que acarreta $3^{p-1} \equiv 2^{p-1} \pmod{p}$.

Agora, veja que $p - 1$ não pode possuir um fator primo em comum com n, pois se isso acontecesse, esse fator primo seria menor do que $p - 1$, logo, menor do que p, e dividiria n, contrariando o fato de p ser o menor primo que divide n. Portanto, $\text{mdc}\,(n, p-1) = 1$, e a relação de Bézout garante a existência de a e b inteiros positivos tais que

$$an = b(p-1) + 1.$$

Juntando todas as informações que obtivemos acima e aplicando o Pequeno Teorema de Fermat, temos que

$$\begin{aligned} 3^n \equiv 2^n \pmod{p} &\implies (3^n)^a \equiv (2^n)^a \pmod{p} \\ &\implies 3^{an} \equiv 2^{an} \pmod{p} \\ &\implies 3^{b(p-1)+1} \equiv 2^{b(p-1)+1} \pmod{p} \\ &\implies (3^{p-1})^b \cdot 3 \equiv (2^{p-1})^b \cdot 2 \pmod{p} \\ &\implies 1^b \cdot 3 \equiv 1^b \cdot 2 \pmod{p} \\ &\implies 3 \equiv 2 \pmod{p}. \end{aligned}$$

Assim, $p \mid (3-2)$, de modo que $p = 1$, o que é um absurdo (pois p é primo). Portanto, não existe inteiro $n > 1$ tal que n divida $3^n - 2^n$. □

Exemplo 4 (Romênia). *Sejam p e q primos, com $q \neq 5$. Se q divide $2^p + 3^p$, então $q > p$.*

Solução. É claro que $q \neq 2$ e $q \neq 3$; por exemplo, se $q \mid (2^p + 3^p)$ e $q = 3$, então $3 \mid (2^p + 3^p)$, o que implicaria $3 \mid 2^p$, um absurdo.

Como $q \neq 5$ por hipótese, temos $q > 5$. Assim, podemos assumir $p > 5$, pois se $p \leq 5$, obtemos imediatamente $p \leq 5 < q$.

Suponhamos, por contradição, que $q \leq p$. Desse modo, obtemos $q - 1 < p$ e, daí, $\text{mdc}\,(q-1,p) = 1$. Utilizando novamente a relação de Bézout, garantimos a existência de r e s inteiros positivos tais que

$$pr = (q-1)s + 1.$$

Ademais, como q é ímpar, temos $(q-1)s+1$ ímpar, logo, r é ímpar.

Utilizando a hipótese de que $q \mid (2^p + 3^p)$, obtemos $2^p \equiv -3^p \pmod q$. Mas aí,

$$\begin{aligned} 2^p \equiv -3^p \pmod q &\implies (2^p)^r \equiv (-3^p)^r \pmod q \\ &\implies 2^{pr} \equiv -3^{pr} \pmod q \\ &\implies 2^{(q-1)s+1} \equiv -3^{(q-1)s+1} \pmod q \\ &\implies (2^{q-1})^s \cdot 2 \equiv -(3^{q-1})^s \cdot 3 \pmod q \\ &\implies 1^s \cdot 2 \equiv -1^s \cdot 3 \pmod q \\ &\implies 2 \equiv -3 \pmod q, \end{aligned}$$

em que aplicamos o Pequeno Teorema de Fermat na penúltima implicação acima.

Por fim, a última congruência acima implica $q \mid 5$, o que é um absurdo. Logo, não podemos ter $q \leq p$, de sorte que devemos ter $q > p$. □

Exemplo 5 (Estados Unidos). *Seja p um número primo dado. Prove que existem infinitos números inteiros positivos n tais que $p \mid (2^n - n)$.*

Solução. Uma vez que, para todo n inteiro positivo par, temos que $2 \mid (2^n - n)$, podemos supor que $p > 2$.

Sendo $p > 2$, temos $\text{mdc}\,(2,p) = 1$, logo, o Pequeno Teorema de Fermat garante que $2^{p-1} \equiv 1 \pmod p$. Agora,

para todo κ inteiro positivo, considere $q = p - 1 + \kappa p$. Assim, temos

$$\begin{aligned} 2^{p-1} \equiv 1 \,(\mathrm{mod}\, p) &\Longrightarrow \left(2^{p-1}\right)^q \equiv 1^q \,(\mathrm{mod}\, p) \\ &\Longrightarrow 2^{(p-1)q} \equiv 1 \,(\mathrm{mod}\, p) \\ &\Longrightarrow 2^{pq-q} \equiv 1 \,(\mathrm{mod}\, p). \end{aligned}$$

Por outro lado, como $q \equiv -1 \,(\mathrm{mod}\, p)$, temos que

$$pq - q \equiv -q \equiv 1 \,(\mathrm{mod}\, p).$$

Então, juntando essa congruência com a anterior, obtemos

$$2^{pq-q} \equiv 1 \equiv pq - p \,(\mathrm{mod}\, p),$$

de sorte que

$$p \mid \left(2^{pq-q} - (pq - q)\right).$$

Assim, para $n = pq - q = p(p - 1 + \kappa p)$, com $\kappa \in \mathbb{N}$, temos que $p \mid (2^n - n)$. □

Exemplo 6 (Olimpíada Balcânica). *Prove que a equação $y^2 = x^5 - 4$ não possui soluções inteiras.*

Solução. Suponha que exista um par de inteiros (x,y) tal que $y^2 - x^5 + 4 = 0$. Analisando a equação módulo 11, temos que, se $x \equiv 0 \,(\mathrm{mod}\, 11)$, então

$$\begin{aligned} x \equiv 0 \,(\mathrm{mod}\, 11) &\Longrightarrow x^5 \equiv 0 \,(\mathrm{mod}\, 11) \\ &\Longrightarrow y^2 - x^5 + 4 \equiv y^2 + 4 \,(\mathrm{mod}\, 11) \\ &\Longrightarrow 0 \equiv y^2 + 4 \,(\mathrm{mod}\, 11) \\ &\Longrightarrow y^2 \equiv -4 \equiv 7 \,(\mathrm{mod}\, 11). \end{aligned}$$

Por outro lado, temos as seguintes alternativas para os restos da divisão de um quadrado perfeito por 11:

$$\begin{aligned} y \equiv \pm 0 \,(\mathrm{mod}\, 11) &\Longrightarrow y^2 \equiv 0 \,(\mathrm{mod}\, 11); \\ y \equiv \pm 1 \,(\mathrm{mod}\, 11) &\Longrightarrow y^2 \equiv 1 \,(\mathrm{mod}\, 11); \\ y \equiv \pm 2 \,(\mathrm{mod}\, 11) &\Longrightarrow y^2 \equiv 4 \,(\mathrm{mod}\, 11); \\ y \equiv \pm 3 \,(\mathrm{mod}\, 11) &\Longrightarrow y^2 \equiv 9 \,(\mathrm{mod}\, 11); \end{aligned}$$

$$y \equiv \pm 4 \pmod{11} \Longrightarrow y^2 \equiv 16 \equiv 5 \pmod{11};$$
$$y \equiv \pm 5 \pmod{11} \Longrightarrow y^2 \equiv 25 \equiv 3 \pmod{11};$$
$$y \equiv 6 \pmod{11} \Longrightarrow y^2 \equiv 36 \equiv 3 \pmod{11}.$$

Desse modo, não existe y inteiro tal que $y^2 \equiv 7 \pmod{11}$. Logo, $x \not\equiv 0 \pmod{11}$. Assim, mdc $(x,11) = 1$ e podemos aplicar o pequeno teorema de Fermat para obter $x^{10} \equiv 1 \pmod{11}$. Mas aí,

$$\begin{aligned} x^{10} \equiv 1 \pmod{11} &\Longrightarrow 11 \mid \left(x^{10} - 1\right) \\ &\Longrightarrow 11 \mid \left(x^5 + 1\right)\left(x^5 - 1\right) \\ &\Longrightarrow 11 \mid \left(x^5 + 1\right) \text{ ou } 11 \mid \left(x^5 - 1\right), \end{aligned}$$

pois 11 é primo.

Então, concluímos que $x^5 \equiv 1 \pmod{11}$ ou $x^5 \equiv -1 \pmod{11}$. Portanto,

$$0 = y^2 - x^5 + 4 \equiv y^2 - 1 + 4 = y^2 + 3 \pmod{11}$$

ou

$$0 = y^2 - x^5 + 4 \equiv y^2 - (-1) + 4 = y^2 + 5 \pmod{11},$$

de sorte que $y^2 \equiv -3 \equiv 8 \pmod{11}$ ou $y^2 \equiv -5 \equiv 6 \pmod{11}$. Entretanto, já vimos acima que nenhum quadrado perfeito deixa resto 6 ou 8 quando dividido por 11.

Concluímos, assim, que a equação $y^2 = x^5 - 4$ não possui soluções inteiras. □

Exemplo 7 (IMO). *Encontre os números inteiros que são relativamente primos com todos os números da sequência*

$$a_n = 2^n + 3^n + 6^n - 1.$$

Solução. Veja que $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$, logo, $2 \mid a_2$ e $3 \mid a_2$. No que segue, mostraremos que para qualquer número primo $p \geq 5$, vale $p \mid a_{p-2}$. Desse modo, o único inteiro relativamente primo com todos os termos da sequência é 1.

Para o que falta, sendo $p \geq 5$ primo, temos, graças ao Pequeno Teorema de Fermat, que $2^{p-1} \equiv 1 \pmod{p}$, $3^{p-1} \equiv 1 \pmod{p}$ e $6^{p-1} \equiv 1 \pmod{p}$.

Por outro lado, como $\text{mdc}\,(2,p) = 1$, existem a e r inteiros tais que $2a + pr = 1$, o que implica $2a \equiv 1 \pmod{p}$. Analogamente, como $\text{mdc}\,(3,p) = 1$ e $\text{mdc}\,(6,p) = 1$, garantimos a existência de b e c inteiros tais que $3b \equiv 1 \pmod{p}$ e $6c \equiv 1 \pmod{p}$. Logo,

$$\begin{aligned} 2^{p-1} \equiv 1 \pmod{p} &\implies 2^{p-2} \cdot 2 \equiv 1 \pmod{p} \\ &\implies 2^{p-2} \cdot 2a \equiv a \pmod{p} \\ &\implies 2^{p-2} \cdot 1 \equiv a \pmod{p} \\ &\implies 2^{p-2} \equiv a \pmod{p}. \end{aligned}$$

De modo inteiramente análogo, obtemos $3^{p-2} \equiv b \pmod{p}$ e $6^{p-2} \equiv c \pmod{p}$.

Agora, veja que, também módulo p,

$$\begin{aligned} 6(a+b+c) &= 6a + 6b + 6c \\ &= 3 \cdot 2a + 2 \cdot 3b + 6c \\ &\equiv 3 \cdot 1 + 2 \cdot 1 + 1 \\ &\equiv 3 + 2 + 1 \\ &= 6. \end{aligned}$$

Assim, como $\text{mdc}\,(6,p) = 1$, podemos cancelar o 6 na congruência $6(a+b+c) \equiv 6 \pmod{p}$ para obter $a + b + c \equiv 1 \pmod{p}$. Portanto, somando as congruências $2^{p-2} \equiv a \pmod{p}$, $3^{p-2} \equiv b \pmod{p}$ e $6^{p-2} \equiv c \pmod{p}$, obtemos

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv a + b + c \equiv 1 \pmod{p},$$

logo,

$$a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Concluímos, assim, que $p \mid a_{p-2}$, conforme precisávamos mostrar. □

Dicas para o Professor

Sugerimos que sejam utilizadas quatro sessões de 50min para expor o conteúdo deste material. Recomendamos fortemente que os alunos tentem encontrar soluções para os problemas apresentados neste material utilizando meios próprios. Se, depois de certo tempo, os alunos não conseguirem apresentar uma solução para determinado problema, dê dicas antes de apresentar a solução completa.

Alguns dos exemplos aqui discutidos aparecem na referência [1]. Remetemos o leitor a ela para outros exemplos interessantes.

Sugestões de Leitura Complementar

1 A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*, terceira edição. Rio de Janeiro, SBM, 2022.