Aritmética dos Restos

Pequeno Teorema de Fermat

Tópicos Adicionais

Aritmética dos Restos
Pequeno Teorema de Fermat

1 Exercícios Introdutórios

Exercício 1. Encontre os restos da divisão de 2^{24} por a) 5 b) 7 c) 11 d) 17.

Exercício 2. Determine o resto de 2^{24} na divisão por 15. Dica: Perceba que $15 = 3 \cdot 5$ e aplique o Teorema de Fermat para cada um desses primos.

Exercício 3. Encontre os restos das divisões de:

a) $300^{3000} - 1$ por 1001

b) $7^{120} - 1$ por 143

Exercício 4. Seja p um primo ímpar maior que 5. Encontre o resto de $\underbrace{111\ldots11}_{p-1 \text{ uns}}$ na divisão por p.

Exercício 5. Prove que se n é ímpar, então

$$n^5 \equiv n \pmod{240}.$$

2 Exercícios de Fixação

Exercício 6. Prove que $20^{15} - 1$ é divisível por 11

Exercício 7. Prove que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é um inteiro para todo inteiro n.

Exercício 8. Mostre que $n^7 \equiv n \pmod{42}, \forall n \in \mathbb{N}$

Exercício 9. Prove que se p é primo, então

$$a^p \equiv b^p \pmod{p} \Rightarrow a^p \equiv b^p \pmod{p^2}$$

Exercício 10. Sejam p e q primos distintos. Mostre que

i) $(a+b)^p \equiv a^p + b^p \pmod{p}$

ii) $p^q + q^p \equiv p + q \pmod{pq}$

iii) $\left\lfloor \frac{p^q + p^q}{pq} \right\rfloor$ é par se $p, q \neq 2$.

Exercício 11. Mostre que se p é primo e $a^2 \equiv b^2 \pmod{p}$, então $a \equiv \pm b \pmod{p}$.

3 Exercícios de Aprofundamento e de Exames

Exercício 12. Encontre o número de inteiros $n > 1$ para os quais o número $a^{25} - a$ é divisível por n para cada inteiro a.

Exercício 13. Prove que para cada primo p, a diferença

$$111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99 - 123456789$$

(onde cada digito está escrito exatamente p vezes) é múltiplo de p.

Exercício 14. Dado um primo p, prove que existem infinitos naturais n tais que p divide $2^n - n$.

Exercício 15. Seja p um número primo da forma $4k + 3$. Mostre que

$$p \mid m^2 + n^2 \iff p \mid m \text{ e } p \mid n.$$

Exercício 16. Sejam p um número primo, a e n e inteiros positivos. Prove que se

$$2^p + 3^p = a^n,$$

então $n = 1$.

Exercício 17. Mostre que existem infinitos inteiros positivos n tais que $\frac{5^{n-2} - 1}{n}$ é inteiro

Respostas e Soluções.

1. Como 2 é relativamente primo com todos os divisores mencionados, podemos usar o Pequeno Teorema de Fermat em todos os itens, obtendo:

a)

$$\begin{aligned} 2^{5-1} &\equiv 1 \pmod 5 \\ (2^4)^6 &\equiv 1^6 \pmod 5 \\ 2^{24} &\equiv 1 \pmod 7 \end{aligned}$$

Portanto, o resto é 1.

b)

$$\begin{aligned} 2^{7-1} &\equiv 1 \pmod 7 \\ (2^6)^4 &\equiv 1^4 \pmod 7 \\ 2^{24} &\equiv 1 \pmod 7 \end{aligned}$$

Portanto, o resto é 1.

c)

$$\begin{aligned} 2^{11-1} &\equiv 1 \pmod{11} \\ (2^{10})^2 &\equiv 1^2 \pmod{11} \\ 2^{20} &\equiv 1 \pmod{11} \\ 2^{20} \cdot 2^4 &\equiv 2^4 \pmod{11} \\ 2^{24} &\equiv 5 \pmod{11} \end{aligned}$$

Portanto, o resto é 5.

d)

$$\begin{aligned} 2^4 &\equiv -1 \pmod{17} \\ (2^4)^6 &\equiv (-1)^6 \pmod{17} \\ 2^{24} &\equiv 1 \pmod{17} \end{aligned}$$

Portanto, o resto é 1.

2. Como $2^{3-1} \equiv 1 \pmod 3$ e $2^{5-1} \equiv 1 \pmod 5$, segue que

$$\begin{aligned} 2^{24} &= (2^2)^{12} \\ &\equiv 1^{12} \pmod 3 \\ 2^{24} &= (2^4)^6 \\ &\equiv 1^6 \pmod 5. \end{aligned}$$

Portanto, $2^{24} - 1$ é múltiplo de 3 e 5. Como $mdc(3,5) = 1$, segue que $15 \mid 2^{24} - 1$.

3.

a) Perceba que $1001 = 7 \cdot 11 \cdot 13$ e que $7-1$, $11-1$ e $13-1$ dividem 3000. Como 7, 11 e 13 são números primos, todos relativamente primos com 300, segue em virtude do Teorema de Fermat, que esses primos dividem $300^{3000} - 1$. Como esses primos são distintos, vale que $1001 = 7 \cdot 11 \cdot 13 \mid 3^{3000} - 1$.

b) Perceba que $143 = 11 \cdot 13$ e que $11-1$ e $13-1$ dividem 120. Como 11 e 13 são primos, ambos relativamente primos com 7, segue em virtude do Teorema de Fermat, que esses primos dividem $7^{120} - 1$. Como esses primos são distintos, vale que $11 \cdot 13 = 143$ divide $7^{120} - 1$.

4. Veja que:

$$\begin{aligned} \underbrace{111\ldots11}_{p-1 \text{ uns}} &= \frac{999\ldots99}{9} \\ &= \frac{10^{p-1}-1}{9} \end{aligned}$$

Pelo Teorema de Fermat, o numerador $10^{p-1} - 1$ é divisível por p, pois $mdc(5,p) = 1$. Além disso, usando que $p \neq 3$, segue que $\frac{10^{p-1}-1}{9}$ também é múltiplo de p.

5. Perceba que $240 = 2^4 \cdot 3 \cdot 5$. Daí, pelo Teorema de Fermat, seque que:

$$\begin{aligned} n^5 &\equiv n \pmod 5 \text{ e} \\ n^5 &\equiv n^3 n^2 \pmod 3 \\ &\equiv n \cdot n^2 \pmod 3 \\ &= n^3 \pmod 3 \\ &\equiv n \pmod 3 \end{aligned}$$

Como $mdc(3,5) = 1$, segue que $15 = 3 \cdot 5 \mid n^5 - n$. Como n é ímpar, podemos escrever $n = 2k+1$. Daí,

$$\begin{aligned} n^5 - n &= n(n^4 - 1) \\ &= n(n^2-1)(n^2+1) \\ &= n(4k(k+1)(n^2+1) \end{aligned}$$

Como $2 \mid k(k+1)$, segue que $8 \mid 4k(k+1)$. Além disso, como n^2+1 é par, podemos afirmar que

$$16 = 2 \cdot 8 \mid 4k(k+1)(n^2+1).$$

Portanto, como $mdc(16,15) = 1$, segue que

$$240 = 15 \cdot 16 \mid n^5 - n.$$

6. Como $11 - 1 = 10$ e $mdc(20,11) = 1$, segue em virtude do Teorema de Fermat que

$$\begin{aligned} 20^{15} &\equiv 9^{15} \pmod{11} \\ &\equiv (3^{10})^3 \pmod{11} \\ &\equiv 1^3 \pmod{11} \\ &= 1 \pmod{11} \end{aligned}$$

Portanto, $11 \mid 20^{15} - 1$.

7. Primeiramente, note que

$$\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15}.$$

Como $mdc(3,5) = 1$, basta mostrarmos que o numerador é

mútiplo de 3 e 5. Pelo teorema de Fermat:

$$\begin{aligned} 3n^5+5n^3+7n &\equiv 5n^3+7n \pmod 3 \\ &\equiv 5n+7n \pmod 3 \\ &\equiv 12n \pmod 3 \\ &\equiv 0 \pmod 3 \\ 3n^5+5n^3+7n &\equiv 3n^5+7n \pmod 5 \\ &\equiv 3n+7n \pmod 5 \\ &\equiv 10n \pmod 5 \\ &\equiv 0 \pmod 5. \end{aligned}$$

8. Pelo Teorema de Fermat,

$$\begin{aligned} n^7 &\equiv n \pmod 7 \\ n^7 &\equiv (n^3)^2 \cdot n \pmod 3 \\ &\equiv n^2 \cdot n \pmod 3 \\ &\equiv n^3 \pmod 3 \\ &\equiv n \pmod 3 \\ n^7 &\equiv (n^2)^3 \cdot n \pmod 2 \\ &\equiv n^3 \cdot n \pmod 2 \\ &\equiv (n^2)^2 \pmod 2 \\ &\equiv n^2 \pmod 2 \\ &\equiv n \pmod 2. \end{aligned}$$

Como $2, 3$ e 7 são primos entre si, $n^7 \equiv n \pmod{2\cdot 3\cdot 7 = 42}$.

9. Pelo teorema de Fermat, $a \equiv a^p \equiv b^p \equiv b \pmod p$. Assim,

$$\begin{aligned} a^{p-1}+a^{p-2}b+\ldots+ab^{p-2}+b^{p-1} &\equiv \\ a^{p-1}+a^{p-1}+\ldots+a^{p-1} &\equiv \\ &\equiv pa^{p-1} \\ &\equiv 0 \pmod p \end{aligned}$$

Como $a-b \equiv 0 \pmod p$, temos:

$$\begin{aligned} a^p-b^p &= (a-b)(a^{p-1}+a^{p-2}b+\ldots+ab^{p-2}+b^{p-1}) \\ &\equiv 0 \pmod{p^2} \end{aligned}$$

10.

i) Pelo Teorema de Fermat:

$$\begin{aligned} (a+b)^p &\equiv a+b \\ &\equiv a^p+b^p \pmod p. \end{aligned}$$

ii) Pelo Teorema de Fermat,

$$\begin{aligned} p^q+q^p &\equiv 0+q \\ &\equiv p+q \pmod p \\ p^q+q^p &\equiv p+0 \\ &\equiv p+q \pmod q \end{aligned}$$

11. Como $p \mid (a^2-b^2) = (a-b)(a+b)$, seque que $\mid a-b$ ou $p \mid a+b$.

12. (Extraído da Olimpíada Búlgara) Se n satisfaz o enunciado, $p^2(p$ primo) não pode dividi-lo, pois $p^{25}-p$ não é divisível por p^2. Assim, n é múltiplo de primos diferentes. Os fatores primos de n são fatores de $2^{25}-2 = 2\cdot 3^2\cdot 5\cdot 7\cdot 13\cdot 17\cdot 241$. Entretanto, n não é divisível por 17 e 241, pois $3^{25} \equiv -3 \pmod{17}$ e $3^{25} \equiv 32 \pmod{241}$. Podemos usar o teorema de Fermat para mostrar que $a^{25} \equiv a \pmod p$ para $p \in \{2,3,5,7,13\}$. Portanto, n deve ser igual a um dos divisores de $2\cdot 3\cdot 5\cdot 7\cdot 13$ diferente de 1. A quantidade de tais divisores é $2^5-1 = 31$.

13. Uma boa maneira de associar os números do problema com o teorema de Fermat é perceber que:

$$\underbrace{111\ldots11}_{p\ uns} = \frac{10^p-1}{9}.$$

Assim, podemos escrever o número $S = 111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99$ como:

$$\begin{aligned} S &= \frac{10^p-1}{9}\cdot 10^{8p} + 2\cdot\frac{10^p-1}{9}\cdot 10^{7p}+\ldots \\ &+ 9\cdot\frac{10^p-1}{9} \\ 9S &= (10^p-1)\cdot 10^{8p}+2\cdot(10^p-1)\cdot 10^{7p}+\ldots \\ &+ 9\cdot(10^p-1) \end{aligned}$$

Para $p=2$ ou $p=3$, o resultado do enunciado segue dos critérios de divisibilidade por 2 e 3. Podemos então nos concentrar no caso $p>3$. Nesse caso, é suficiente mostrarmos que $9(S-123456789)$ é divisível por p pois $mdc(p,9)=1$. Pelo Teorema de Fermat:

$$\begin{aligned} 9S &= (10^p-1)\cdot 10^{8p}+2\cdot(10^p-1)\cdot 10^{7p}+\ldots \\ &+ 9\cdot(10^p-1) \\ &\equiv (10-1)\cdot 10^8+2\cdot(10-1)\cdot 10^7+\ldots \\ &+ 9\cdot(10-1) \pmod p \\ &\equiv 9\cdot 123456789 \pmod p. \end{aligned}$$

14. Se $p=2$, n pode ser qualquer número par. Suponha que $p>2$. Considere $(p-1)^{2k}$, pelo teorema de Fermat temos

$$\begin{aligned} 2^{(p-1)^{2k}} &\equiv (2^{p-1})^{(p-1)^{2k-1}} \\ &\equiv 1^{(p-1)^{2k-1}} \\ &= 1 \\ &\equiv (p-1)^{2k} \pmod p. \end{aligned}$$

Assim, para qualquer k, $n=(p-1)^{2k}$ satisfaz o problema.

15. Façamos inicialmente a primeira implicação. Se $p \nmid m$, então $m^{p-1} \equiv 1 \pmod p$, e daí temos as equivalências

módulo p

$$\begin{aligned} & n^2 \equiv -m^2 \\ \Rightarrow \quad & (nm^{p-2})^2 \equiv -(m^{p-1})^2 \\ & \equiv -1 \\ \Rightarrow \quad & (nm^{p-2})^{p-1} \equiv (-1)^{\frac{p-1}{2}} \\ & \equiv (-1)^{2k+1} \\ & \equiv -1, \end{aligned}$$

o que contraria o Teorema de Fermat. Assim, $p \mid m$ e $p \mid n$.

16. Se $p = 2$, claramente $a = 13$ e $n = 1$. Se $p > 2$, p é ímpar e $5 \mid 2^p + 3^p$. Consequentemente 5 divide a. Se fosse $n > 1$, $25 \mid a^n$ e teríamos:

$$\begin{aligned} 0 &\equiv \frac{a^n}{5} \\ &\equiv \frac{2^p + 3^p}{5} \\ &= 2^{p-1} - 2^{p-2} \cdot 3 + \ldots + 2 \cdot -3^{p-2} + 3^{p-1} \\ &\equiv 2^{p-1} + 2^{p-1} + \ldots + 2^{p-1} \\ &\equiv p2^{p-1} \pmod 5 \end{aligned}$$

A única possíbilidade é termos $p = 5$. Entretanto, $2^5 + 3^5$ não é uma potência perfeita não trivial. Logo, $n = 1$.

17. (Extraído da OBM 2008) Para qualquer primo p, com $p > 5$, o número $n = 2p$ é solução. Para verificar isso, note que $5^{n-2} - 1$ é par e que, graças ao Teorema de Fermat,

$$\begin{aligned} 5^{n-2} &\equiv 5^{2p-2} \pmod p \\ &\equiv (5^{p-1})^2 \pmod p \\ &\equiv 1^2 \pmod p \\ &\equiv 1 \pmod p \end{aligned}$$

Daí, como p e 2 dividem $5^{n-2} - 1$ e $mdc(2, p) = 1$, segue que $n = 2p \mid 5^{n-2} - 1$.

Produzido por Arquimedes Curso de Ensino
contato@cursoarquimedes.com