Material Teórico - Módulo Aritmética dos Restos

O Pequeno Teorema de Fermat - Parte 1

Tópicos Adicionais

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

18 de agosto de 2023

Iniciamos este material com o seguinte exemplo.

Exemplo 1. *Prove que* $8^{10} \equiv 1 \pmod{11}$.

Solução. Podemos mostrar que $8^{10} \equiv 1 \pmod{11}$ do seguinte modo:

$$\begin{aligned} 8^2 = 64 \equiv -2 \pmod{11} &\Longrightarrow \left(8^2\right)^5 \equiv (-2)^5 \pmod{11} \\ &\Longrightarrow 8^{10} \equiv -32 \equiv 1 \pmod{11}. \end{aligned}$$

Alternativamente, note que

$$\begin{aligned} 1 \cdot 8 &\equiv 8 \pmod{11} \\ 2 \cdot 8 = 16 &\equiv 5 \pmod{11} \\ 3 \cdot 8 = 24 &\equiv 2 \pmod{11} \\ 4 \cdot 8 = 32 &\equiv 10 \pmod{11} \\ 5 \cdot 8 = 40 &\equiv 7 \pmod{11} \\ 6 \cdot 8 = 48 &\equiv 4 \pmod{11} \\ 7 \cdot 8 = 56 &\equiv 1 \pmod{11} \\ 8 \cdot 8 = 64 &\equiv 9 \pmod{11} \\ 9 \cdot 8 = 72 &\equiv 6 \pmod{11} \\ 10 \cdot 8 = 80 &\equiv 3 \pmod{11} \end{aligned}$$

Multiplicando membro a membro as dez congruências acima, obtemos

$$10! \cdot 8^{10} \equiv 10! \pmod{11}.$$

Como $\text{mdc}(i,11) = 1$ para todo $i \in \{1,2,\ldots,10\}$, concluímos que $\text{mdc}(10!,11) = 1$. Logo,

$$10! \cdot 8^{10} \equiv 10! \pmod{11} \Longrightarrow 8^{10} \equiv 1 \pmod{11}.$$

Essa última prova de que $8^{10} \equiv 1 \pmod{11}$ evidencia a ideia da demonstração de um resultado mais geral, conhecido como o *Pequeno Teorema de Fermat*, apresentado a seguir. □

Teorema 2 (Pequeno Teorema de Fermat)**.** *Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então, $a^{p-1} \equiv 1 \pmod{p}$.*

Prova. Uma vez que $\{0,1,2,\ldots,p-1\}$ é um sistema completo de restos módulo p, existem inteiros $i_1,i_2,\ldots,i_{p-1} \in \{0,1,2,\ldots,p-1\}$ tais que

$$\begin{aligned} 1\cdot a &\equiv i_1 \,(\mathrm{mod}\, p),\\ 2\cdot a &\equiv i_2 \,(\mathrm{mod}\, p),\\ &\vdots\\ (p-1)\cdot a &\equiv i_{p-1} \,(\mathrm{mod}\, p). \end{aligned} \tag{1}$$

Afirmamos que $i_k \neq 0$, para todo $k \in \{1,2,\ldots,p-1\}$, e $i_k \neq i_l$, sempre que $i \neq l$.

Com efeito, se $i_k = 0$ para algum de tais k, teríamos $k\cdot a \equiv 0 \,(\mathrm{mod}\, p)$, ou seja, $p \mid k\cdot a$. Mas isso implicaria $p \mid k$ ou $p \mid a$, o que é um absurdo, pois p é primo (logo, $\mathrm{mdc}(k,p) = 1$) e, por hipótese, $p \nmid a$.

Além disso, supondo que $i_k = i_l$ para certos índices $k,l \in \{1,2,\ldots,p-1\}$, podemos supor, sem perda de generalidade, que $k \geq l$. Então,

$$\begin{aligned} &k\cdot a \equiv i_k = i_l \equiv l\cdot a \,(\mathrm{mod}\, p) \Longrightarrow\\ &\Longrightarrow (k-l)a \equiv 0 \,(\mathrm{mod}\, p)\\ &\Longrightarrow p \mid (k-l)a. \end{aligned}$$

Agora, como p é primo e $p \nmid a$, temos que $p \mid (k-l)$. Mas aí, como $0 \leq k-l < p$, a única forma de p dividir $k-l$ é termos $k-l = 0$, ou seja, $k = l$. Em resumo, mostramos que $i_k = i_l \Rightarrow k = l$, ou, o que é o mesmo, que $k \neq l \Longrightarrow i_k \neq i_l$.

Os argumentos acima mostraram que os $p-1$ números i_1, i_2, …, i_{p-1} são elementos dois a dois distintos do conjunto (de $p-1$ elementos) $\{1,2,\ldots,p-1\}$. Então,

$$\{i_1,i_2,\ldots,i_{p-1}\} = \{1,2,\ldots,p-1\}.$$

e, argumentando como no exemplo 1, isto é, multiplicando membro a membro as $p-1$ congruências em (1), obtemos

$$(p-1)!\, a^{p-1} \equiv (p-1)! \,(\mathrm{mod}\, p).$$

Também como antes, o fato de p ser primo garante que

$$\text{mdc}(k,p) = 1,\ \forall 1 \leq k \leq p-1 \Longrightarrow \text{mdc}((p-1)!, p) = 1.$$

Então, podemos cancelar $(p-1)!$ na última congruência acima, obtendo

$$a^{p-1} \equiv 1 \,(\text{mod}\, p).$$

□

Corolário 3. *Sejam p um número primo e a um inteiro. Então $a^p \equiv a \,(\text{mod}\, p)$.*

Prova. Se $p \nmid a$, então, pelo Pequeno Teorema de Fermat, temos que $a^{p-1} \equiv 1 \,(\text{mod}\, p)$. Por outro lado,

$$\begin{aligned} a^{p-1} \equiv 1 \,(\text{mod}\, p) &\Longrightarrow a \cdot a^{p-1} \equiv a \cdot 1 \,(\text{mod}\, p) \\ &\Longrightarrow a^p \equiv a \,(\text{mod}\, p). \end{aligned}$$

Por outro lado, se $p \mid a$, então também temos que $p \mid a^p$, logo, $p \mid (a^p - a)$. Mas isso é o mesmo que dizer que $a^p \equiv a \,(\text{mod}\, p)$. □

Corolário 4. *Sejam p um número primo e a e b inteiros. Então, $(a+b)^p \equiv a^p + b^p \,(\text{mod}\, p)$.*

Prova. Utilizando repetidas vezes o corolário 3, obtemos

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

As duas últimas congruências acima garantem que

$$a^p + b^p \equiv a + b \,(\text{mod}\, p).$$

Comparando essa última congruência com a primeira acima, concluímos que

$$(a+b)^p \equiv a + b \equiv a^p + b^p \,(\text{mod}\, p),$$

□

Vejamos alguns exemplos de aplicação do Pequeno Teorema de Fermat, começando pelo cálculo de restos.

Exemplo 5. *Encontre o resto na divisão de* 3^{2023} *por* 13.

Solução. Como mdc(3,13) = 1, podemos utilizar o Pequeno Teorema de Fermat para obter

$$3^{12} \equiv 1 \,(\mathrm{mod}\, 13).$$

Para passar de 3^{12} para 3^{2023}, dividimos 2023 por 12, obtendo

$$\begin{array}{r|l} 2\,0\,2\,3 & 1\,2 \\ \cline{2-2} 8\,2 & 1\,6\,8 \\ 1\,0\,3 & \\ 7 & \end{array}$$

Então, $2023 = 12 \cdot 168 + 7$, de modo que

$$\begin{aligned} 3^{12} \equiv 1 \,(\mathrm{mod}\, 13) &\Longrightarrow \left(3^{12}\right)^{168} \equiv 1^{168} \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{12 \cdot 168} \equiv 1 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{12 \cdot 168} \cdot 3^7 \equiv 1 \cdot 3^7 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{12 \cdot 168 + 7} \equiv 3^7 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{2023} \equiv 3^7 \,(\mathrm{mod}\, 13). \end{aligned}$$

Resta, agora, calcular $3^7 \,(\mathrm{mod}\, 13)$. Mas $3^3 = 27 \equiv 1 \,(\mathrm{mod}\, 13)$, logo,

$$3^7 = 3^3 \cdot 3^3 \cdot 3 \equiv 1 \cdot 1 \cdot 3 \equiv 3 \,(\mathrm{mod}\, 13).$$

Daí, concluímos que

$$3^{2023} \equiv 3^7 \equiv 3 \,(\mathrm{mod}\, 13),$$

isto é, o resto da divisão de 3^{2023} por 13 é igual a 3. □

Observação 6. *O exemplo anterior poderia ter sido mais facilmente resolvido se tivéssemos partido da congruência* $3^3 \equiv 1 \,(\mathrm{mod}\, 13)$ *e de*

$$\begin{array}{r|l} 2\,0\,2\,3 & 3 \\ \cline{2-2} 2\,2 & 6\,7\,4 \\ 1\,3 & \\ 1 & \end{array}$$

De fato, como $2023 = 3 \cdot 674 + 1$*, teríamos obtido*

$$\begin{aligned} 3^3 \equiv 1 \,(\mathrm{mod}\, 13) &\Longrightarrow \left(3^3\right)^{674} \equiv 1^{674} \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{3\cdot 674} \equiv 1 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{3\cdot 674} \cdot 3 \equiv 1 \cdot 3 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{3\cdot 674+1} \equiv 3 \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 3^{2023} \equiv 3 \,(\mathrm{mod}\, 13). \end{aligned}$$

Note, contudo, que isso não desmerece o Pequeno Teorema de Fermat, pois a virtude dele é não precisarmos nos preocupar em encontrar, caso a caso, expoentes $k \geq 1$ *tais que* $a^k \equiv 1 \,(\mathrm{mod}\, p)$ *quando* p *é primo e* $\mathrm{mdc}(a,p) = 1$*. O teorema garante que* $p-1$ *sempre funciona!*

Exemplo 7. *Utilizando o Pequeno Teorema de Fermat, encontre:*

(*a*) *O resto na divisão de* 2^{1000} *por* 101*.*

(*b*) *O resto na divisão de* 4^{102} *por* 101*.*

Solução.
(a) Inicialmente, note que 101 é primo e mdc(2,101) = 1. Portanto, podemos utilizar o Pequeno Teorema de Fermat para obter $2^{100} \equiv 1 \,(\mathrm{mod}\, 101)$. A partir daí,

$$\begin{aligned} 2^{100} \equiv 1 \,(\mathrm{mod}\, 101) &\Longrightarrow \left(2^{100}\right)^{10} \equiv 1^{10} \,(\mathrm{mod}\, 101) \\ &\Longrightarrow 2^{1000} \equiv 1 \,(\mathrm{mod}\, 101). \end{aligned}$$

Assim, o resto na divisão de 2^{1000} por 101 é 1.

(b) Utilizando mais uma vez o Pequeno Teorema de Fermat, obtemos $4^{100} \equiv 1 \,(\mathrm{mod}\, 101)$. Agora, argumentando como em

(a), temos que

$$4^{100} \equiv 1 \pmod{101} \Longrightarrow 4^2 \cdot 4^{100} \equiv 4^2 \cdot 1 \pmod{101}$$
$$\Longrightarrow 4^{102} \equiv 16 \pmod{101}.$$

Portanto, o resto na divisão de 4^{102} por 101 é 16. □

Exemplo 8. *Encontre o resto da divisão de* 8^{900} *por* 29*.*

Solução. Temos que 29 é primo e $29 \nmid 8$, logo, mdc(8,29) = 1; portanto, pelo Pequeno Teorema de Fermat, obtemos $8^{28} \equiv 1 \pmod{29}$.

Note, agora, que $900 = 28 \cdot 32 + 4$. Assim,

$$\begin{aligned} 8^{28} \equiv 1 \pmod{29} &\Longrightarrow \left(8^{28}\right)^{32} \equiv 1^{32} \pmod{29} \\ &\Longrightarrow 8^{28\cdot 32} \equiv 1 \pmod{29} \\ &\Longrightarrow 8^{28\cdot 32} \cdot 8^4 \equiv 1 \cdot 8^4 \pmod{29} \\ &\Longrightarrow 8^{28\cdot 32+4} \equiv 8^4 \pmod{29} \\ &\Longrightarrow 8^{900} \equiv 8^4 \pmod{29}. \end{aligned}$$

Por fim, veja que

$$\begin{aligned} 8^2 = 64 \equiv 6 \pmod{29} &\Longrightarrow \left(8^2\right)^2 \equiv 6^2 \pmod{29} \\ &\Longrightarrow 8^4 \equiv 36 \equiv 7 \pmod{29}. \end{aligned}$$

Dessa forma,

$$8^{900} \equiv 8^4 \equiv 7 \pmod{29},$$

de sorte que 8^{900} deixa resto 7 na divisão por 29. □

Os próximos exemplos mostram usos um pouco mais *sofisticados* do Pequeno Teorema de Fermat.

Exemplo 9. *Mostre que todo primo diferente de* 2 *e* 5 *tem um múltiplo formado apenas por algarismos* 1*.*

Solução. Sendo p um primo diferente de 2 e de 5, é claro que mdc(10,p) = 1. Daí, podemos utilizar o Pequeno teorema de Fermat para obter

$$10^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

Então, $10^{p-1} - 1$ é um múltiplo de p, com

$$10^{p-1} - 1 = \underbrace{999\ldots99}_{p-1 \text{ algarismos}}\ .$$

Escrevendo

$$10^{p-1} - 1 = 9 \cdot \underbrace{111\ldots11}_{:=N},$$

concluímos que $p \mid 9N$. Consideremos, agora, dois casos:

(i) Se $p \neq 3$, então mdc(p,9) = 1, logo $p \mid 9N$ implica $p \mid N$. Dessa forma, N é múltiplo de p formado apenas por algarismos 1.

(ii) Se $p = 3$, não é necessário usar o Pequeno Teorema de Fermat: o número 111 é múltiplo de p formado apenas por algarismos 1. □

Exemplo 10. *Encontre um múltiplo de* 221 *formado apenas por algarismos* 1*.*

Solução. Comecemos encontrando um múltiplo de 221 formado apenas por algarismos 9. Para tanto, observamos que qualquer número formado apenas por algarismos 9 é do tipo $10^n - 1$, logo, vamos procurar uma potência de 10 que seja congruente a 1 módulo 221.

Veja que $221 = 13 \cdot 17$, com mdc(10,13) = 1, mdc(10,17) = 1. Assim, podemos utilizar o Pequeno Teorema de Fermat para obter as congruências

$$10^{12} \equiv 1 \,(\mathrm{mod}\, 13) \quad \text{e} \quad 10^{16} \equiv 1 \,(\mathrm{mod}\, 17).$$

A partir delas, tomaremos $n = 12 \cdot 16 = 192$, uma vez que

$$\begin{aligned} 10^{12} \equiv 1 \,(\mathrm{mod}\, 13) &\Longrightarrow \left(10^{12}\right)^{16} \equiv 1^{10} \,(\mathrm{mod}\, 13) \\ &\Longrightarrow 10^{192} \equiv 1 \,(\mathrm{mod}\, 13) \end{aligned}$$

e

$$10^{16} \equiv 1 \pmod{17} \Longrightarrow \left(10^{16}\right)^{12} \equiv 1^{12} \pmod{17}$$
$$\Longrightarrow 10^{192} \equiv 1 \pmod{17}.$$

Então, 13,17 | $(10^{192} - 1)$ e, como são primos entre si, concluímos que $13 \cdot 17 \mid \left(10^{192} - 1\right)$, ou seja, 221 | $\left(10^{192} - 1\right)$.

Agora, procedemos como no exemplo anterior: a última divisibilidade acima é o mesmo que dizer que 221 divide o número $9 \cdot \underbrace{111\ldots11}_{192\,\text{algarismos}}$. Mas, como mdc(221,9) = 1, segue que 221 divide $\underbrace{111\ldots11}_{192\,\text{algarismos}}$. □

Observação 11. *Os argumentos dos dois exemplos anteriores podem ser generalizados para mostrar que, se p_1, p_2, ..., p_k forem primos dois a dois distintos e todos diferentes de* 2 *e de* 5*, então o número $p_1 p_2 \ldots p_k$ tem um múltiplo formado apenas por algarismos* 1*. Tente fazer isso!*

Mais geralmente, é verdadeiro que todo natural n primo com 10 *(e não só os n primos) tem um múltiplo formado apenas por algarismos* 1*. A demonstração do caso geral usa o Princípio da Casa dos Pombos e pode ser vista no exemplo* 10 *do material teórico "Princípio da Casa dos Pombos", no módulo "Métodos Sofisticados de Contagem", do segundo ano do Ensino Médio.*

Mesmo nos casos discutidos acima, a demonstração utilizando o Princípio da Casa dos Pombos é mais simples que a utilizando o Pequeno Teorema de Fermat. Entretanto, ela não diz exatamente quantos algarismos o múltiplo terá; ela apenas garante que esse múltiplo existe!

Exemplo 12. *Prove que não existe inteiro m tal que* 103 | $\left(m^3 - 2\right)$.

Solução. Inicialmente, note que 103 é primo. Por outro lado, se existisse um inteiro m tal que 103 | $\left(m^3 - 2\right)$, teríamos $m^3 \equiv 2 \pmod{103}$; em particular, $103 \nmid m$ (pois, do contrário, teríamos $m^3 \equiv 0 \pmod{103}$).

Contudo, notando que $103 - 1 = 3 \cdot 34$ (e "com um olho" no Pequeno Teorema de Fermat), temos que

$$\begin{aligned} m^3 \equiv 2 \pmod{103} &\Longrightarrow \left(m^3\right)^{34} \equiv 2^{34} \pmod{103} \\ &\Longrightarrow m^{102} \equiv 2^{34} \pmod{103}. \end{aligned}$$

Agora, calculemos $2^{34} \pmod{103}$:

$$\begin{aligned} 2^7 = 128 \equiv 25 \pmod{103} &\Longrightarrow \left(2^7\right)^2 \equiv 25^2 = 625 \pmod{103} \\ &\Longrightarrow 2^{14} \equiv 625 \equiv 7 \pmod{103} \\ &\Longrightarrow \left(2^{14}\right)^2 \equiv 7^2 = 49 \pmod{103} \\ &\Longrightarrow 2^{28} \equiv 49 \pmod{103} \\ &\Longrightarrow 2 \cdot 2^{28} \equiv 2 \cdot 49 \pmod{103} \\ &\Longrightarrow 2^{29} \equiv 98 \equiv -5 \pmod{103} \\ &\Longrightarrow 2^5 \cdot 2^{29} \equiv 2^5 \cdot (-5) \pmod{103} \\ &\Longrightarrow 2^{34} \equiv -160 \equiv -57 \pmod{103} \\ &\Longrightarrow 2^{34} \equiv 46 \pmod{103}. \end{aligned}$$

Juntando essa congruência com a anterior, obtemos que

$$m^{102} \equiv 46 \pmod{103}.$$

Agora, como $103 \nmid m$, o Pequeno Teorema de Fermat garante que $m^{102} \equiv 1 \pmod{103}$, o que contradiz a penúltima congruência acima. A contradição, evidentemente, vem de termos assumido a existência de um inteiro m tal que $103 \mid (m^3 - 2)$. □

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores apresentem outros exemplos como o exemplo 1 antes de apresentar a demonstração do Pequeno Teorema

de Fermat, pois isso facilitará a compreensão da ideia da demonstração do teorema. Além disso, como fica claro na observação 6, certos problemas podem ser facilmente resolvidos apenas aplicando as propriedades de congruências, sem utilizar o teorema 2. Entretanto, o teorema facilita a resolução de outros problemas. Nesse sentido, remetemos o leitor interessado às referências listadas a seguir.

Sugestões de Leitura Complementar

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

2. D. Fomin, S. Genkin e I. Itenberg. *Círculos Matemáticos: A Experiência Russa*. Rio de Janeiro, IMPA 2012.

3. J. P. O. Santos. *Introdução à Teoria dos Números*. Rio de Janeiro, IMPA, 2000.