Material Teórico - Módulo Aritmética dos Restos

O Teorema de Wilson

Tópicos Adicionais

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

20 de novembro de 2023

PORTAL DA MATEMÁTICA
OBMEP

Nas aulas anteriores deste módulo, apresentamos diversos resultados importantes envolvendo a relação de congruência de números inteiros. Em particular, na última sequência de materiais, provamos o Pequeno Teorema de Fermat e o Teorema de Euler, além de apresentar diversas aplicações desses dois resultados. Agora, apresentaremos outro importante resultado, conhecido como Teorema de Wilson, e algumas aplicações. Assim como nos teoremas citados anteriormente, iniciamos apresentando um exemplo que traz a ideia da prova do Teorema de Wilson.

Exemplo 1. *Mostre que* $12! \equiv -1 \pmod{13}$.

Solução. Uma vez que 13 é primo, temos $\text{mdc}\,(i,13) = 1$, para todo $i \in \{1,2,\ldots,12\}$. Desse modo, $\forall i \in \{1,2,\ldots,12\}$, existe $x_i \in \{1,2,\ldots,12\}$ tal que $ix_i \equiv 1 (\text{mod}\, 13)$, isto é, todos os números do conjunto $\{1,2,\ldots,12\}$ possuem inverso módulo 13 — perceba que 1 e 12 são os seus próprios inversos. De fato, temos as congruências abaixo.

$$\begin{aligned}
2 \cdot 7 &= 14 \equiv 1 \pmod{13} \\
3 \cdot 9 &= 27 \equiv 1 \pmod{13} \\
4 \cdot 10 &= 40 \equiv 1 \pmod{13} \\
5 \cdot 8 &= 40 \equiv 1 \pmod{13} \\
6 \cdot 11 &= 66 \equiv 1 \pmod{13}
\end{aligned}$$

Multiplicando membro a membro essas 5 congruências, obtemos

$$2 \cdot 3 \cdot \ldots \cdot 11 \equiv 1 \pmod{13}$$

ou, o que é o mesmo,

$$11! \equiv 1 \pmod{13}.$$

Multiplicando os dois membros da última congruência por 12, chegamos a $12 \cdot 11! \equiv 12 \pmod{13}$, logo,

$$12! \equiv -1 \pmod{13}.$$

□

Observação 2. *Na solução do exemplo 5, utilizamos apenas* 5 *das* 10 *congruências* $ix_i \equiv 1 \pmod{13}$, $i \in \{2,3,\ldots,11\}$ *para obter* $11! \equiv 1 \pmod{13}$. *Veja que as outras* 5 *congruências são cópias das* 5 *primeiras.*

$$\begin{aligned}
7 \cdot 2 &= 14 \equiv 1 \pmod{13} \\
8 \cdot 5 &= 40 \equiv 1 \pmod{13} \\
9 \cdot 3 &= 27 \equiv 1 \pmod{13} \\
10 \cdot 4 &= 40 \equiv 1 \pmod{13} \\
11 \cdot 6 &= 66 \equiv 1 \pmod{13}
\end{aligned}$$

Teorema 3 (Teorema de Wilson)**.** *Se* p *é um número primo, então* $(p-1)! \equiv -1 \pmod{p}$.

Prova. Como $(2-1)! = 1! \equiv -1 \pmod{2}$, podemos supor que p é um primo ímpar e seguir o raciocínio do exemplo 1.

Desse modo, temos $\text{mdc}(i,p) = 1$, para todo $i \in \{1,2,\ldots,p-1\}$, logo, $\forall i \in \{1,2,\ldots,p-1\}$, existe $x_i \in \{1,2,\ldots,p-1\}$ tal que $ix_i \equiv 1 \pmod{p}$.

Além disso, observe que, se $i,j \in \{1,2,\ldots,p-1\}$, então

$$\begin{aligned}
x_i \equiv x_j \pmod{p} &\Longrightarrow ix_i \equiv ix_j \pmod{p} \\
&\Longrightarrow 1 \equiv ix_j \pmod{p} \\
&\Longrightarrow j \cdot 1 \equiv jix_j \pmod{p} \\
&\Longrightarrow j \equiv ijx_j \pmod{p} \\
&\Longrightarrow j \equiv i \cdot 1 \pmod{p} \\
&\Longrightarrow j \equiv i \pmod{p} \\
&\Longrightarrow j = i.
\end{aligned}$$

Portanto, excluindo-se 1 e $p-1$, que têm inversos módulo p iguais a eles próprios, podemos agrupar os $p-3$ números $2,3,\ldots,p-2$ em $\frac{p-3}{2}$ pares do tipo $\{a,b\}$, tais que em cada par um elemento é o inverso do outro.

Multiplicando membro a membro as $\frac{p-3}{2}$ congruências $ab \equiv 1 \pmod{p}$ e reordenando os fatores do primeiro membro, obtemos

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}.$$

Multiplicando ambos os membros da última congruência por $p-1$, chegamos a

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

□

Vale também a recíproca do Teorema de Wilson.

Teorema 4. *Se n é um inteiro positivo tal que $(n-1)! \equiv -1 \pmod{n}$, então n é primo.*

Prova. Se n não for primo, existe um primo p tal que p divide n. Assim p divide $(n-1)!$ — pois p é um dos fatores do produto $(n-1)\cdot(n-2)\cdot\ldots\cdot 2\cdot 1$.

Por outro lado, por hipótese, temos que $(n-1)! \equiv -1 \pmod{n}$, o que implica n divide $(n-1)!+1$. Como p divide n, temos então que p também deve dividir $(n-1)!+1$.

Desse modo, o primo p divide a diferença $(n-1)!+1-(n-1)!=1$, o que é uma contradição. Logo, n é primo. □

Exemplo 5. *Encontre o resto da divisão do produto $14\cdot 15\cdot\ldots\cdot 26$ por 13.*

Solução. Inicialmente, note que

$$\begin{aligned} 14 &\equiv 1 \pmod{13} \\ 15 &\equiv 2 \pmod{13} \\ &\vdots \\ 26 &\equiv 12 \pmod{13} \end{aligned}$$

Logo,

$$14\cdot 15\cdot\ldots\cdot 26 \equiv 1\cdot 2\cdot\ldots\cdot 12 \equiv 12! \pmod{13}.$$

Pelo Teorema de Wilson, temos que $12! \equiv -1 \equiv 12 \pmod{13}$, logo, o resto da divisão de $14\cdot 15\cdot\ldots\cdot 26$ por 13 é 12. □

Exemplo 6. *Mostre que se p é um primo ímpar, então*

(a) $1^2\cdot 3^2\cdot 5^2\cdot\ldots\cdot(p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

(*b*) $2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

Solução. Vamos provar apenas o item (a), pois (b) é inteiramente análogo. Pelo Teorema de Wilson, temos que $(p-1)! \equiv -1 \pmod{p}$, ou seja,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdot 5 \cdot 6 \cdot \ldots \cdot (p-2)(p-1) \equiv -1 \pmod{p}.$$

Mas

$$\begin{aligned} 2 &\equiv -(p-2) \pmod{p} \\ 4 &\equiv -(p-4) \pmod{p} \\ 6 &\equiv -(p-6) \pmod{p} \\ &\vdots \\ p-1 &\equiv -1 \pmod{p}. \end{aligned}$$

Assim, substituindo 2,4,6, $\ldots$,$p-1$ respectivamente por $-(p-2)$, $-(p-4)$, $-(p-6)$, $\ldots$, -1 na congruência anterior — observe que são $\frac{p-1}{2}$ substituições ao todo — obtemos

$$(-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-1)^2 \equiv -1 \pmod{p}.$$

Multiplicando ambos os lados da última congruência por $(-1)^{\frac{p-1}{2}}$, obtemos

$$(-1)^{p-1} \cdot 1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \pmod{p},$$

ou seja,

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

□

Exemplo 7 (Estônia). *Mostre que não é possível dividir um conjunto formado por* 18 *inteiros consecutivos em dois conjuntos disjuntos tais que os produtos dos elementos nos dois conjuntos sejam iguais.*

Solução. Seja $A = \{n,n+1,n+2,\ldots,n+17\}$ um conjunto formado por 18 inteiros consecutivos. Suponha que existam B e C subconjuntos de A tais que $A = B \cup C$, $B \cap C = \emptyset$ e o produto dos elementos de B seja igual ao produto dos elementos de C.

Observe que nenhum dos conjuntos B e C possui um múltiplo de 19. Realmente, se um deles possuísse um desses múltiplos, o outro também deveria possuir, uma vez que estamos assumindo que os produtos dos elementos dos dois conjuntos são iguais. Contudo, em um conjunto formado por 18 números consecutivos há, no máximo, um múltiplo de 19.

Assim, cada um dos elementos de A é congruente, módulo 19, a um dos elementos do conjunto $\{1,2,3,\ldots,18\}$.

Agora, seja $r > 0$ o resto da divisão do produto dos elementos de B por 19 — observe que esse resto é igual ao resto da divisão do produto dos elementos de C por 19, pois os produtos são iguais. Então,

$$\begin{aligned} r^2 &\equiv n(n+1)(n+2)\ldots(n+17) \pmod{19} \\ &\equiv 1 \cdot 2 \cdot 3 \cdot \ldots 18 \pmod{19} \\ &\equiv 18! \pmod{19}. \end{aligned}$$

Mas, pelo Teorema de Wilson, temos que $18! \equiv -1 \pmod{19}$. Daí, seguiria que $r^2 \equiv -1 \pmod{19}$.

Entretanto, veja que

$$\begin{aligned} r^2 \equiv -1 \pmod{19} &\Longrightarrow \left(r^2\right)^9 \equiv (-1)^9 \pmod{19} \\ &\Longrightarrow r^{18} \equiv -1 \pmod{19}. \end{aligned}$$

Por outro lado, como $19 \nmid r$, o Pequeno Teorema de Fermat nos dá $r^{18} \equiv 1 \pmod{19}$, o que é uma contradição. □

Encerramos este material, discorrendo um pouco sobre os conceitos de *ordem* e *raiz primitiva*, módulo n. Os resultados aqui apresentados serão utilizados para demonstrar uma generalização do Teorema de Wilson, que será apresentada no próximo material.

Sejam a e n inteiros tais que $n > 1$ e $\text{mdc}\,(a,n) = 1$. O Teorema de Euler garante que $a^{\phi(n)} \equiv 1 \pmod{n}$. Portanto,

podemos definir a **ordem de a módulo n**, a qual denotaremos por $\mathrm{ord}_n(a)$, como o menor inteiro positivo pertencente ao conjunto

$$\{k \in \mathbb{Z} | a^k \equiv 1 \pmod{n}\}.$$

Esse conjunto não é vazio, justamente porque $\phi(n)$ é um de seus elementos. Em particular,

$$\mathrm{ord}_n(a) \leq \phi(n).$$

Quando não houver perigo de confusão, a ordem de a módulo n será denotada simplesmente por $\mathrm{ord}(a)$. Temos o seguinte resultado fundamental.

Proposição 8. *Sejam a, $n > 1$ inteiros relativamente primos, $d = \mathrm{ord}_n(a)$ e h um inteiro positivo qualquer. Então $a^h \equiv 1 \pmod{n}$ se, e somente se, $d \mid h$. Em particular, $d \mid \phi(n)$.*

Prova. Se $d \mid h$, então existe q inteiro positivo tal que $h = qd$. Logo, uma vez que $d = \mathrm{ord}_n(a)$, temos

$$\begin{aligned} a^d \equiv 1 \pmod{n} &\Longrightarrow \left(a^d\right)^q \equiv 1^q \pmod{n} \\ &\Longrightarrow a^{qd} \equiv 1 \pmod{n} \\ &\Longrightarrow a^h \equiv 1 \pmod{n}. \end{aligned}$$

Reciprocamente, suponha que $a^h \equiv 1 \pmod{n}$. Pelo algoritmo da divisão, existem q e r inteiros tais que

$$h = qd + r,\ 0 \leq r < d.$$

Note que $q \geq 0$, pois, caso contrário, teríamos $h = qd + r \leq -d + 0 < 0$. Daí, temos que

$$\begin{aligned} a^h \equiv 1 \pmod{n} &\Longrightarrow a^{qd+r} \equiv 1 \pmod{n} \\ &\Longrightarrow a^{qd} \cdot a^r \equiv 1 \pmod{n} \\ &\Longrightarrow \left(a^d\right)^q \cdot a^r \equiv 1 \pmod{n} \\ &\Longrightarrow 1^q \cdot a^r \equiv 1 \pmod{n} \\ &\Longrightarrow a^r \equiv 1 \pmod{n}. \end{aligned}$$

Como d é o menor inteiro positivo que satisfaz $a^d \equiv 1 \pmod{n}$, concluímos que $0 < r < d$ não pode acontecer. Logo, $r = 0$, o que implica $d \mid h$.

Por fim, conforme já lembramos, o teorema de Euler afirma que, se a e n são relativamente primos, então $a^{\phi(n)} \equiv 1 \pmod{n}$. Então, pela primeira parte, temos que $d \mid \phi(n)$. □

Quando $\text{ord}_n(a) = \phi(n)$ dizemos que a é uma **raiz primitiva** módulo n. Por exemplo, quando $n = 10$, temos que $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$. Assim, a ordem, módulo 10, de qualquer inteiro a relativamente primo com 10 é 1, 2 ou 4, pois $\text{ord}_{10}(a) \mid \phi(10)$ e $\phi(10) = 4$. Vamos calcular a ordem de 3 módulo 10:

$$3^1 \equiv 3 \pmod{10};$$
$$3^2 \equiv 9 \pmod{10};$$
$$3^3 = 27 \equiv 7 \pmod{10};$$
$$3^4 = 81 \equiv 1 \pmod{10}.$$

Dessa forma, $\text{ord}\,10(3) = 4$, donde concluímos que 3 é uma raiz primitiva módulo 10.

Note, ainda, que o conjunto $\{3^1,3^2,3^3,3^4\}$ é um sistema reduzido de resíduos, módulo 10. Isso acontece sempre que a for uma raiz primitiva módulo n, como afirma a próxima proposição.

Proposição 9. *Sejam a e $n > 1$ inteiros relativamente primos. Se a é uma raiz primitiva módulo n, então o conjunto $\{1,a,a^2,\ldots,a^{\phi(n)-1}\}$ é um sistema reduzido de resíduos, módulo n.*

Prova. Como $\{1,a,a^2,\ldots,a^{\phi(n)-1}\}$ possui $\phi(n)$ elementos, é suficiente provar que $a^i \not\equiv a^j \pmod{n}$, sempre que i e j forem elementos distintos do conjunto $\{0,1,\ldots,\phi(n)-1\}$.

Suponha que existam $i < j$ elementos desse conjunto tais que $a^i \equiv a^j \pmod{n}$. Então

$$\begin{aligned} a^j \equiv a^i \pmod{n} &\Longrightarrow a^{j-i+i} \equiv a^i \pmod{n} \\ &\Longrightarrow a^{j-i} \cdot a^i \equiv a^i \pmod{n} \\ &\Longrightarrow a^{j-i} \equiv 1 \pmod{n}. \end{aligned}$$

(Na última implicação, utilizamos o fato de que $\text{mdc}\,(a,m) = 1$, logo, $\text{mdc}\,\left(a^i,m\right) = 1$, para cancelar a^i.)

Desse modo, $0 < j - i < \phi(n) = \text{ord}_n(a)$, o que contradiz a minimalidade de $\text{ord}_n(a)$. □

Dicas para o Professor

Sugerimos que sejam utilizadas três 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. É interessante apresentar outro problema como o exemplo 1, para que os alunos entendam a ideia da prova do Teorema de Wilson. No exemplo 7, o r^2 aparece quando multiplicamos o produto dos elementos de B pelo produto dos elementos de C. Daí, do lado direito da congruência, aparecem todos os elementos do conjunto A, que é igual à reunião de B e C.

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.

2. J. P. O. Santos *Introdução à Teoria dos Números.* IMPA, 2000.