Proposição

Sejam G um grupo e $a \in G$. Se a tem ordem infinita, então todas as potências de a são distintas. Se a tem ordem finita n, então $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Além disso, $a^i = a^j$ se e só se $n \mid (i-j)$, isto é, i e j são congruentes módulo n.

Demonstração. Se a tem ordem infinita, então nenhuma potência não nula de a é a identidade. Como $a^i = a^j$ implica $a^{i-j} = e$, tem de se ter $i - j = 0$, o que prova a primeira parte do enunciado.
Suponhamos agora que $\operatorname{ord} a = n$ e vejamos que $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Os elementos deste conjunto são todos distintos, pois se $a^i = a^j$ com $0 \leq j < i \leq n-1$, então $a^{i-j} = e$. Mas isto contradiz o facto de n ser o mais pequeno inteiro positivo tal que a^n é a identidade.
Suponhamos agora que a^k é um elemento de $\langle a \rangle$. Pelo algoritmo da divisão, existem inteiros q e r tais que $k = qn + r$, com $0 \leq r < n$. Mas então, $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = ea^r = a^r$, logo $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$.
Seguidamente vamos provar que se $a^i = a^j$, então n divide $i - j$.

Começamos por observar que se $a^i = a^j$, então $a^{i-j} = e$ e aplicamos de novo o algoritmo de divisão. Existem inteiros q e r tais que $i - j = qn + r$, com $0 \leq r < n$. Então $e = a^{i-j} = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = ea^r = a^r$. Como n é o mais pequeno inteiro positivo tal que a^n é a identidade, temos de ter $r = 0$ e, portanto, $n \mid (i - j)$.
Reciprocamente, se $i - j = nq$, então $a^{i-j} = a^{nq} = e^q = e$, logo $a^i = a^j$. □

Como consequências imediatas temos:

Corolário

Para qualquer elemento a de um grupo tem-se: $\operatorname{ord} a = \operatorname{ord}\langle a\rangle$.

Corolário

Sejam G um grupo e a um elemento de ordem n em G. Se $a^k = e$, então n divide k.

Do teorema resulta ainda que, no caso finito, a multiplicação em $\langle a\rangle$ é essencialmente feita pela adição módulo n, isto é, se $(i + j) \pmod n = k$, então $a^i a^j = a^k$. Usando desde já terminologia a introduzir mais tarde, podemos dizer que, se $\operatorname{ord} a = n$, então $\langle a\rangle$ e $\mathbb{Z}_n$ são isomorfos.

Lema

Se $\operatorname{ord} a = n$, *então* $\operatorname{ord} a^d = n/d$ *para qualquer divisor* d *de* n.

Demonstração. Claro que $(a^d)^{n/d} = a^n = e$, logo $\operatorname{ord} a^d \leq n/d$. Por outro lado, resulta da definição de ordem de a que se i for um inteiro positivo menor que n/d, então $(a^d)^i \neq e$. □

Proposição

Seja a *um elemento de ordem* n *de um grupo e seja* k *um inteiro positivo. Então* $\langle a^k \rangle = \langle a^{\operatorname{mdc}(n,k)} \rangle$ *e* $\operatorname{ord} a^k = n/\operatorname{mdc}(n,k)$.

Demonstração. Seja $d = \operatorname{mdc}(n,k)$ e suponhamos que $k = dr$. Como $a^k = (a^d)^r$, tem-se que $\langle a^k \rangle \subseteq \langle a^d \rangle$. Sabemos que existem inteiros s e t tais que $d = ns + kt$. Logo,
$a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k \rangle$. Logo $\langle a^d \rangle \subseteq \langle a^k \rangle$, tendo-se, portanto, $\langle a^k \rangle = \langle a^{\operatorname{mdc}(n,k)} \rangle$.
A segunda parte resulta do lema anterior, com $d = \operatorname{mdc}(n,k)$. □

Seguidamente apresentamos uma consequência importante deste resultado.

Corolário

Suponhamos que $\operatorname{ord} a = n$. *Então* $\langle a^i \rangle = \langle a^j \rangle$ *se e só se* $\operatorname{mdc}(n, i) = \operatorname{mdc}(n, j)$.

Demonstração. Pelo resultado anterior, basta provar que $\langle a^{\operatorname{mdc}(n,i)} \rangle = \langle a^{\operatorname{mdc}(n,j)} \rangle$ se e só se $\operatorname{mdc}(n, i) = \operatorname{mdc}(n, j)$. Ora $\langle a^{\operatorname{mdc}(n,i)} \rangle = \langle a^{\operatorname{mdc}(n,j)} \rangle$ implica $\operatorname{ord} a^{\operatorname{mdc}(n,i)} = \operatorname{ord} a^{\operatorname{mdc}(n,j)}$, logo, novamente pelo resultado anterior, $n/\operatorname{mdc}(n, i) = n/\operatorname{mdc}(n, j)$ e, portanto, $\operatorname{mdc}(n, i) = \operatorname{mdc}(n, j)$. O recíproco é óbvio. □

Com casos particulares importantes temos:

Corolário

1. *Seja* $G = \langle a \rangle$ *um grupo cíclico de ordem* n. *Então* $G = \langle a^k \rangle$ *se e só se* $\operatorname{mdc}(n, k) = 1$.
2. *Um inteiro* $k \in \mathbb{Z}_n$ *é um gerador de* $\mathbb{Z}_n$ *se e só se* $\operatorname{mdc}(n, k) = 1$.

Teorema

Todo o subgrupo de um grupo cíclico é cíclico. Além disso, se $\operatorname{ord} a = n$, *então a ordem de qualquer subgrupo de* $\langle a \rangle$ *é um divisor de n e, para qualquer divisor positivo k de n,* $\langle a \rangle$ *tem precisamente um subgrupo de ordem k, a saber,* $\langle a^{n/k} \rangle$.

Demonstração. Sejam $G = \langle a \rangle$ e $H \leq G$. Vamos mostrar que H é cíclico. Claro que se H consistir apenas da identidade é cíclico, pelo que vamos supor que $H \neq \{e\}$. Existe um elemento da forma a^t, com t positivo em H. (Note-se que os elementos de H são da forma a^s e sempre que a^s está em H, o mesmo acontece com a^{-s}.)
Seja m o mais pequeno inteiro positivo tal que $a^m \in H$. Claro que $\langle a^m \rangle \subseteq H$. Vejamos que também vale a inclusão recíproca. Seja então $b \in H$. Como $b \in G = \langle a \rangle$, existe k tal que $b = a^k$. Pelo algoritmo da divisão, existem inteiros q e r tais que $k = mq + r$, com $0 \leq r < m$. Então $a^k = a^{mq+r} = a^{mq} a^r$, logo $a^r = a^{-mq} a^k$. Como $a^k = b \in H$ e $a^{-mq} = (a^m)^{-q} \in H$, também se tem $a^r \in H$. Pela minimalidade de m, vem que $r = 0$ e isto prova a primeira parte do teorema.

Suponhamos agora que $\operatorname{ord} a = n$ e que $H \leq \langle a \rangle$. Já sabemos que $H = \langle a^m \rangle$, para algum m. Como $(a^m)^n = (a^n)^m = e$, sabemos que $\operatorname{ord} a^m$ é um divisor de n. Logo $\operatorname{ord} H = \operatorname{ord} a^m$ é um divisor de n.
Finalmente, suponhamos que k é um divisor positivo de n. Vejamos que $\langle a^{n/k} \rangle$ é o único subgrupo de $\langle a \rangle$ de ordem k. Sabemos que $\operatorname{ord} a^{n/k} = n/\operatorname{mdc}(n, n/k) = n/(n/k) = k$. Seja agora H um subgrupo de $\langle a \rangle$ de ordem k. Já mostrámos que $H = \langle a^m \rangle$, onde m é um divisor de n. Então $m = \operatorname{mdc}(m, n)$ e $k = \operatorname{ord} a^m = \operatorname{ord} a^{\operatorname{mdc}(m,n)} = n/\operatorname{mdc}(m, n) = n/m$. Logo $m = n/k$ e $H = \langle a^{n/k} \rangle$. □

Corolário

Seja n um inteiro positivo. Para cada divisor positivo k de n, o conjunto $\langle n/k \rangle$ é o único subgrupo de $\mathbb{Z}_n$ de ordem k. Além disso, estes são os únicos subgrupos de $\mathbb{Z}_n$

Exemplo

Indica-se aseguir a lista dos subgrupos de $\mathbb{Z}_{12}$.

$$\begin{array}{rcll} \langle 11\rangle = \langle 7\rangle = \langle 5\rangle = \langle 1\rangle & = & \{0,1,2,\ldots,11\} & (k=12) \\ \langle 10\rangle = \langle 2\rangle & = & \{0,2,4,6,8,10\} & (k=6) \\ \langle 9\rangle = \langle 3\rangle & = & \{0,3,6,9\} & (k=4) \\ \langle 8\rangle = \langle 4\rangle & = & \{0,4,8\} & (k=3) \\ \langle 6\rangle & = & \{0,6\} & (k=2) \\ \langle 0\rangle & = & \{0\} & (k=1) \end{array}$$

Resolução de exercícios

Exercício

Considere os inteiros $a = 849$ e $b = 198$. Determine o máximo divisor comum d de a e b e exprima-o como combinação linear desses dois números, isto é, determine inteiros x e y tais que $d = xa + yb$.

Resolução.

$$\begin{aligned} 849 &= 4 \times 198 + 57 \\ 198 &= 3 \times 57 + 27 \\ 57 &= 2 \times 27 + 3 \\ 27 &= 9 \times 3 + 0 \end{aligned}$$

Resulta que $\mathrm{mdc}(849, 198) = 3$.

$$\begin{aligned} 3 = \mathrm{mdc}(849, 198) &= 57 - 2 \times 27 \\ &= 57 - 2 \times (198 - 3 \times 57) \\ &= -2 \times 198 + 7 \times 57 \\ &= -2 \times 198 + 7 \times (849 - 4 \times 198) \\ &= 7 \times 849 - 30 \times 198 \end{aligned}$$

Assim, $x = 7$ e $y = -30$ é uma solução.

Exercício

Determine o resto da divisão de 537^{1000} por 35.

Resolução. Tem-se $537 = 15 \times 35 + 12$, pelo que $537 \equiv 12 \pmod{35}$.
Resulta que $537^{1000} \equiv 12^{1000} \pmod{35}$.
Como 12 e 35 são primos entre si, vamos poder usar o Teorema de Euler na resolução do exercício. Tem-se $\varphi(35) = \varphi(5)\varphi(7) = 4 \times 6 = 24$.
Pelo Teorema de Euler tem-se $12^{24} \equiv 1 \pmod{35}$. Logo,
$537^{1000} \equiv 12^{1000} \equiv (12^{24})^{41} \cdot 12^{16} \equiv 12^{16} \pmod{35}$.
Agora,
$12^2 \equiv 4 \pmod{35}$
$12^4 \equiv 16 \pmod{35}$
$12^8 \equiv 16^2 = 256 \equiv 11 \pmod{35}$
$12^{16} = (12^8)^2 \equiv 11^2 \equiv 16 \pmod{35}$.
Resulta então que $537^{1000} \equiv 12^{1000} \equiv 12^{16} \equiv 16 \pmod{35}$, logo o resto pedido é 16. □

Exercício

Determine o resto da divisão de 537^{1018} por 33.

Resolução. Tem-se $537 = 16 \times 33 + 9$, pelo que $537 \equiv 9 \pmod{33}$.
Resulta que $537^{1018} \equiv 9^{1018} = 3^{2036} \pmod{33}$.
9 e 33 não são primos entre si, pelo que o Teorema de Euler não vai poder ser usado na resolução deste exercício.
Tem-se:
$3^4 = 81 \equiv 15 \pmod{33}$
$3^6 \equiv 15 * 3^2 \equiv 3 \pmod{33}$.
Então,
$3^{2036} = (3^6)^{339} \times 3^2 \equiv 3^{339} \times 3^2 = 3^{441} \equiv (3^6)^{56} \times 3^5 \equiv 3^{61} = (3^6)^{10} \times 3 \equiv 3^{11} \equiv 3^5 \times 3 \equiv 3 \pmod{33}$.
Resulta então que $537^{1018} \equiv 9^{1018} = 3^{2036} \equiv 3 \pmod{33}$, logo a resposta é: 3. □