Pequeno Teorema de Fermat

Seja p um primo e $a \in \mathbb{Z}$. Então $a^p \equiv a \pmod{p}$.

Em particular, se $p \nmid a$, então $a^{p-1} \equiv 1 \pmod{p}$.

PROVA (efetuada por Euler em 1730)

- Se $p = 2$, então $a^2 \equiv a \pmod{2}$ porque $a(a-1)$ é par.
- Seja $p > 2$. Para $a = 0$ e $a = 1$ a afirmação é verdadeira.

  Por hipótese de indução, suponhamos que, para certo $a \in \mathbb{N}_0$, $a^p \equiv a \pmod{p}$.
  Então,

$$
\begin{aligned}
(a+1)^p &\equiv a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1 \pmod{p} \\
&\equiv a^p + 1 \pmod{p} \qquad \text{(por hip. indução)} \\
&\equiv a + 1 \pmod{p}
\end{aligned}
$$

Logo $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{N}_0$.
Como $p-1$ é par, então $a^{p-1} = (-a)^{p-1}$ pelo que a afirmação é válida para todo o $a \in \mathbb{Z}$.

EXEMPLO 1

$2^{50} + 3^{50}$ é divisível por 13.

$$\begin{aligned} 2^{50} &= 2^{4\cdot 12+2} = (2^{12})^4 \cdot 2^2 \quad \text{logo} \\ 2^{50} &\equiv 2^2 \pmod{13} \end{aligned}$$

$$\begin{aligned} 3^{50} &= 3^{4\cdot 12+2} = (3^{12})^4 \cdot 3^2 \quad \text{logo} \\ 3^{50} &\equiv 3^2 \pmod{13} \end{aligned}$$

$$\begin{aligned} 2^{50} + 3^{50} &\equiv 2^2 + 3^2 \pmod{13} \\ &\equiv 0 \pmod{13} \end{aligned}$$

Será o recíproco do Teorema de Fermat válido?

i.e., se $a^{n-1} \equiv 1 \pmod{n}$ para todo o inteiro a tal que $\mathrm{m.d.c.}(a, n) = 1$, então n é primo?

Não, por exemplo, 561 é tal que:

- $561 = 3 \cdot 11 \cdot 17$
- $a^{560} \equiv 1 \pmod{561}$, para qualquer $a \in \mathbb{Z}$ tal que $\mathrm{m.d.c.}(a, 561) = 1$.

No entanto, se $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $\mathrm{m.d.c.}(a, n) = 1$ e $a^{n-1} \not\equiv 1 \pmod{n}$, então n não é primo.

Por exemplo, $2^{15} \pmod{15} = 8 \not\equiv 2 \pmod{15}$, logo 15 não é primo.

Definição

O número de elementos invertíveis módulo n num sistema completo de resíduos denota-se por $\phi(n)$.

A função $\begin{array}{rccc} \phi: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \phi(n) \end{array}$ chama-se função de Euler.

NOTA

$\phi(n)$ é igual ao número de inteiros positivos k tais que $k < n$ e $\mathrm{m.d.c.}(k, n) = 1$.

EXEMPLO 2

$$
\begin{aligned}
\phi(1) = \phi(2) &= 1 \\
\phi(3) &= 2 \\
\phi(4) &= 2 \\
\phi(5) &= 4 \\
\phi(6) &= 2 \\
\phi(7) &= 6 \\
\phi(8) &= 4
\end{aligned}
$$

Lema

Se p é primo, então $\phi(p) = (p-1)$, para $r \geq 1$.

NOTA

Se $n \in \mathbb{N}$ não é primo, então existe $p \in \mathbb{P}$ tal que $p > n$ e $p \mid n$. Logo $\phi(n) < (n-1)$.

Teorema

Seja $p \in \mathbb{N}$. Então,

$$p \text{ é primo se e só se } \phi(p) = (p-1).$$

Lema

Se p é primo, então $\phi(p^r) = p^{r-1}(p-1)$, para $r \geq 1$.

PROVA

No conjunto

$$\{1, 2, \cdots, p, p+1, \cdots 2p, \cdots, p^r\}$$

existem p^{r-1} múltiplos de p. Os restantes números são primos com p. Logo,

$$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1).$$

Proposição

Sejam m, $n \in \mathbb{Z}$ tais que $\mathrm{m.d.c.}(m, n) = 1$. Então $\phi(mn) = \phi(m)\phi(n)$, i.e., ϕ é multiplicativa.

EXEMPLO 3

$$\phi(6600) = \phi(11 \cdot 5^2 \cdot 3 \cdot 2^3) = 10 \cdot (5 \cdot 4) \cdot 2 \cdot (2^2 \cdot 1) = 1600.$$

EXEMPLO 4

Para ilustrar o raciocínio que justifica a proposição, considere-se o número 15 $(= 3 \cdot 5)$.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

Quais são os números primos com 3? Quais são os números primos com 5?
Notar que em cada coluna há um múltiplo de 3 e em cada linha há um múltiplo de 5. Nomeadamente, em cada coluna há $\phi(3)$ elementos primos com 3 e há $\phi(5)$ colunas em que os elementos são primos com 5.

Como um natural é primo com 15 se e só se é primo com 3 e com 5, então há $\phi(3)\phi(5)$ primos com 15.

Teorema de Euler

Sejam $a, m \in \mathbb{Z}$ tais que $\mathrm{m.d.c.}(a, m) = 1$. Então $a^{\phi(m)} \equiv 1 \pmod{m}$.

PROVA

Se $r_1, \ldots, r_{\phi(m)}$ são os elementos invertíveis módulo m num sistema completo de resíduos, então $ar_1, \ldots, ar_{\phi(m)}$ são invertíveis e incongruentes dois a dois módulo m.

$$a^{\phi(m)}(r_1 \cdots r_{\phi(m)}) = ar_1 \cdots ar_{\phi(m)} \equiv r_1 \cdots r_{\phi(m)} \pmod{m}.$$

Como $\mathrm{m.d.c.}(r_i, m) = 1$, então $\mathrm{m.d.c.}(r_1 \cdots r_{\phi(m)}, m) = 1$ e

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Aplicação no cálculo do inverso módulo m

Se $\mathrm{m.d.c.}(a, m) \neq 1$, então a não é invertível módulo m.

Se $\mathrm{m.d.c.}(a, m) = 1$, então $a^{\phi(m)} \equiv 1 \pmod{m}$, ou seja,

$$a \cdot a^{\phi(m)-1} \equiv 1 \pmod{m}.$$

Logo, o inverso de a módulo m é $a^{\phi(m)-1} \pmod{m}$.

Teorema de Wilson

Se p é primo, então $(p-1)! \equiv -1 \pmod{p}$.

PROVA

$$S = \{0, 1, 2, \ldots, p-1\}$$

é um sistema completo de resíduos módulo p. Como p é primo, os elementos de $S \setminus \{0\}$ são invertíveis módulo p, e

- 1 e $p-1$ são inversos módulo p de si próprios;
- os restantes elementos podem agrupar-se em pares de elementos distintos do tipo (a, a') em que a é inverso módulo p de a'.

Logo,

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot (p-1) &\equiv 1 \cdot (p-1) \pmod{p} \\ &\equiv (p-1) \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

EXEMPLO 5

Se $p = 7$, então

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \pmod{7}.$$

Proposição

Se n é um composto e $n > 1$, então

$$(n-1)! \equiv \begin{cases} 2 \bmod n & \text{se } n = 4 \\ 0 \bmod n & \text{se } n \neq 4 \end{cases}.$$

Teorema

Seja $p \in \mathbb{N}$. Então,

$$(p-1)! \equiv -1 \pmod{p} \text{ se e só se } p \text{ é primo.}$$