Aula 12.05.2020

Lembrete

(a) Teorema de Fermat

Sejam p - primo, a - inteiro com $p \nmid a$.

Assim: $\boxed{a^{p-1} \equiv 1 \pmod{p}}$

Corolario:

p - primo
a - arbitrario
$\Rightarrow \boxed{a^p \equiv a \pmod{p}}$

(b) Teorema de Euler

Sejam a, n dois inteiros, $n > 0$,
e $\text{mdc}(a,n) = 1$, assim

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}},$$

onde $\varphi(n)$ é função de Euler, dada por

$$\varphi(n) = \#\{1 \leq a \leq n \mid \text{mdc}(a,n) = 1\}.$$

Exemplo. a) Sejam $a = 31$, $n = 20$. $\text{mdc}(a,n) = 1$

e $\{\textcircled{1}, 2, \textcircled{3}, 4, \textcircled{5}, 6, \textcircled{7}, 8, 9, 10, \textcircled{11}, 12, \textcircled{13}, 14, 15, 16, \textcircled{17}, 18, \textcircled{19}, 20\}$ $\Rightarrow \boxed{31^8 \equiv 1 \pmod{20}}$

$\text{mdc}(\cancel{8}, 20) = 1$, $\varphi(n) = 8$

b) $a = 2$, $n = 9$. $mdc(a, n) = 1$.

$\varphi(9) = 6 \Rightarrow 2^6 = 2^{\varphi(9)} = 64 \equiv 1 \pmod 9$.

c) Busca o resto de divisão de 5^{100} por 7.

Pelo Teorema de Fermat

$5^6 \equiv 1 \pmod 7$

$\Rightarrow (5^6)^{16} \equiv 1 \pmod 7$, ou seja $5^{96} \equiv 1 \pmod 7$

$5^2 \equiv 4 \pmod 7$, assim $5^4 \equiv 16 \equiv 2 \pmod 7$

$\Rightarrow 5^{100} \equiv 2 \pmod 7$ //

Teorema de Wilson

Teorema (Wilson)

Se p é um primo, assim

| p divide $(p-1)! + 1$ //

Exemplos:

a) $p = 2$, $(p-1)! + 1 = 1! + 1 = 2 = 2 \cdot 1$

b) $p = 3$, $(p-1)! + 1 = 2! + 1 = 3 = 3 \cdot 1$

c) $p = 5$, $(p-1)! + 1 = 4! + 1 = 25 = 5 \cdot 5$

d) $p = 7$, $(p-1)! + 1 = 6! + 1 = 721 = 7 \cdot 103$ //

Para provar o resultado, primeiramente vamos provar os seguintes lemas.

Lema. Seja p um primo. Para todo a em

$$C = \{1, 2, \ldots, p-1\}$$

existe único inverso modular do a em C ou seja único $b \in C$, tal que $\boxed{a \cdot b \equiv 1 \pmod{p}}$

Prova $\mathrm{mdc}(a, p) = 1$, Logo $a \cdot x \equiv 1 \pmod{p}$ tem solução. $t \in \mathbb{Z}$. Pelo Alg. da divisão

$$t = q \cdot p + b, \text{ com } 0 \leq b \leq p-1,$$

mas $b \neq 0$, pois caso contrario $at \equiv 0 \pmod{p}$

assim $b \in C$ □.

Exemplo 1) $p = 5$, assim $C = \{1, 2, 3, 4\}$ e

$1 \cdot 1 \equiv 1 \pmod{5}$, $2 \cdot 3 \equiv 1 \pmod{5}$

$3 \cdot 2 \equiv 1 \pmod{5}$, $4 \cdot 4 \equiv 1 \pmod{5}$.

2) $p = 11$, assim $C = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

$1 \cdot 1 \equiv 1 \pmod{11}$, $2 \cdot 6 \equiv 1 \pmod{11}$, $3 \cdot 4 \equiv 1 \pmod{11}$

$8 \cdot 7 \equiv 1 \pmod{11}$, $5 \cdot 9 \equiv 1 \pmod{11}$, $10 \cdot 10 \equiv 1 \pmod{11}$.

Obs. $x = 1, 4$ são únicos tais que $x^2 \equiv 1 \pmod 5$.

$x = 1, 10$ — // — // — // — $x^2 \equiv 1 \pmod{11}$.

Lema Seja p - primo, $x \in \{1, \dots, p-1\}$. Assim:

$$x^2 \equiv 1 \pmod p \iff \begin{array}{l} x = 1, \text{ ou} \\ x = p-1. \end{array}$$

Prova [$\Leftarrow$]. Se $\begin{array}{l} x = 1 \\ x = p-1 \end{array} \Rightarrow$ $\begin{array}{l} x^2 \equiv 1 \pmod p \\ x^2 = p^2 - 2p + 1 \equiv 1 \pmod p. \end{array}$

[$\Rightarrow$] Se $x^2 \equiv 1 \pmod p \Rightarrow p \mid x^2 - 1 \Rightarrow p \mid (x-1)(x+1)$

Como $1 \leq x \leq p-1$ assim

$p \mid x-1$ ou $p \mid x+1$

$\Downarrow$ $\Downarrow$

$x = 1$ $x = p-1$ $\square$

Teorema (Wilson) Seja p um primo, assim

$p \mid (p-1)! + 1$ ou seja $(p-1)! \equiv -1 \pmod p$.

Prova Conforme Lema 1 e Lema 2 agrupamos os elementos

$$2, 3, \dots, (p-3), (p-2)$$

em grupos a, a' com $a \neq a'$ e

$a\, a' \equiv 1 \pmod p$

Consequentemente fazendo o produto de tais congruencias temos:

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

Por outro lado

$$p-1 \equiv -1 \pmod{p}$$

$$\Rightarrow \quad (p-1)! \equiv -1 \pmod{p} \quad \square$$

Exemplo: Observe que 2017 é primo e mostre que $2015^{2016} + 2016!$ é um multiplo de 2017.

Solução. Pelo T. Ferma $\Rightarrow$ $2015^{2016} \equiv 1 \pmod{2017}$

Pelo T. Wilson $\Rightarrow$ $(2016)! \equiv -1 \pmod{2017}$

Assim $2015^{2016} + 2016! \equiv 0 \pmod{2017}$ //

Exemplo 2 Encontre o resto da divisão de $10!$ por 13.

Solução Pelo T. Wilson $12! \equiv -1 \pmod{13}$

Observe: $11 \equiv -2 \pmod{13}$, $12 \equiv -1 \pmod{13}$

$$\Rightarrow \quad 10! \cdot 11 \cdot 12 = 10!(-2) \cdot (-1) \equiv (-1) \pmod{13}$$

$$\Rightarrow \quad 2 \cdot 10! \equiv -1 \pmod{13}.$$

O inverso modular de 2 modulo 13 é 7, pois $2 \cdot 7 \equiv 1 \pmod{13}$, assim

$$\underbrace{2 \cdot 7}_{\parallel 1} \cdot 10! \equiv -7 \pmod{13}$$

$$\Rightarrow 10! \equiv -7 \equiv 6 \pmod{13}.$$

Assim o resto é 6 //

Como calcular $\varphi(n)$?

$\varphi(n) = \#\{1 \leq a \leq n$ tais que $mdc(a,n)=1\}$.

Seja $n = p^\alpha$, com p um primo $\alpha \geq 1$.

Escrevendo todos inteiros entre 1 e p^α, temos:

$1, 2, \ldots, \cancel{p}, p+1, \ldots, \cancel{2p}, \ldots \cancel{3p}, \ldots, \ldots \cancel{p \cdot p^{\alpha-1}}$

elementos vermelhos são multiplos de p assim $mdc(\cancel{\ }, p^\alpha) \neq 1$. Como cancelamos exatamente $p^{\alpha-1}$, assim

$$\boxed{\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}} \quad (1)$$

para todos os primos.

Exemplo $p=2$, $\alpha=3$, $\varphi(2^3) = \varphi(8) = 2^3 - 2^2 = 4$

pois $\{\underline{1}, \cancel{2}, \underline{3}, \cancel{4}, \underline{5}, \cancel{6}, \underline{7}, \cancel{8}\}$

Na aula que vem vamos mostrar que (2) $\boxed{\varphi(m\,n) = \varphi(m)\cdot\varphi(n)}$ se $mdc(m,n)=1$.

Assim para calcular $\varphi(n)$ para

$n = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot \dots \cdot p_k^{\alpha_k}$, com $p_1,\dots,p_k$ primos distintos, temos

$$\left[\varphi(n) = \varphi\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\dots\cdot p_k^{\alpha_k}\right) \overset{(2)}{=}\right.$$

$$= \varphi\left(p_1^{\alpha_1}\right)\cdot\varphi\left(p_2^{\alpha_2}\right)\cdot\dots\cdot\varphi\left(p_k^{\alpha_k}\right) \overset{(1)}{=}$$

$$\left.= \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\cdot\left(p_2^{\alpha_2-\alpha_2}\right)\cdot\dots\cdot\varphi\left(p_k^{\alpha_k} - p_k^{\alpha_k-1}\right)\right]$$

Exemplos

- $\varphi(10) = \varphi(2\cdot 5) = \varphi(2)\cdot\varphi(5)$
  $= (2-1)\cdot(5-1) = 4$ //
- $\varphi(90) = \varphi(2\cdot 5\cdot 3^2) = \varphi(2)\cdot\varphi(5)\cdot\varphi(3^2)$
  $= (2-1)\cdot(5-1)\cdot(3^2-3) = 24$ //
- $\varphi(300) = \varphi(2^2\cdot 3\cdot 5^2) = \varphi(2^2)\cdot\varphi(3)\cdot\varphi(5^2)$
  $= (2^2-2)\cdot(3-1)\cdot(5^2-5) = 80$ //

Exemplo Encontre 3 últimos dígitos de 2017^{2001}.

Solução 3 últimos dígitos de q.q. inteiro é seu resto da divisão por 1000.

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3)$$
$$= (2^3 - 2^2) \cdot (5^3 - 5^2) = 800$$

Assim, pelo T. de Euler $2017^{800} \equiv 1 \pmod{1000}$

Assim $2017^{2000} \equiv 1 \pmod{1000}$

$\Rightarrow 2017^{2000} \equiv 2017 \pmod{1000}$

$\Rightarrow$ 3 últimos dígitos são 017 //

Exercício [pr casa]

a) Encontre 2 últimos dígitos de 3^{999} e 5^{2011}.

b) Encontre o resto da divisão de 15^{175} por 11.

c) " " " " " de 67! por 71

d) " " " " " de 53! por 61.