

Aula 19.06.2020

Revisão 1

Ex.1 Resolve
$$\begin{cases} 2x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \\ 3x \equiv 4 \pmod{7} \end{cases}$$

Solução Inverso de 2 em $\mathbb{Z}_3$ é 2
3 em $\mathbb{Z}_4$ é 5, Assim

$$\begin{cases} 2x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \\ 3x \equiv 4 \pmod{7} \end{cases} \Rightarrow \begin{cases} 2 \cdot 2x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ 5 \cdot 3x \equiv 5 \cdot 4 \pmod{7} \end{cases}$$
$$\Rightarrow \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

Aplicando algoritmo de Gauss temos $N = 3 \cdot 5 \cdot 7 = 105$

$$N_1 = 5 \cdot 7 = 35, \quad N_1^{-1} = 2 \text{ em } \mathbb{Z}_3$$

$$N_2 = 3 \cdot 7 = 21, \quad N_2^{-1} = 1 \text{ em } \mathbb{Z}_5, \text{ Assim}$$

$$N_3 = 3 \cdot 5 = 15, \quad N_3^{-1} = 1 \text{ em } \mathbb{Z}_7$$

$$x = N_1 \cdot c_1 \cdot N_1^{-1} + N_2 \cdot c_2 \cdot N_2^{-1} + N_3 \cdot c_3 \cdot N_3^{-1}$$

$$= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 1 + 15 \cdot 6 \cdot 1 = 140 + 21 + 90 = 251$$

$$x = 251 \equiv 41 \pmod{105}$$

N

Assim $x \equiv 41 \pmod{105}$
é solução.

Ex. 2 [5 a) Lista 4]

(2)

Mostre que $\text{mdc}(a, 42) = 1 \Rightarrow 3 \cdot 7 \cdot 8 \mid a^6 - 1$

Solução:

Fato útil [pelo T. Chinês de Resto]

$$\text{Se } \begin{cases} x \equiv 1 \pmod{u} \\ x \equiv 1 \pmod{m} \end{cases} \Rightarrow x \equiv 1 \pmod{u \cdot m} //$$

Assim basta provar que

$$a^6 \equiv 1 \pmod{3} \checkmark [a^2 \equiv 1 \pmod{3} \Rightarrow a^6 \equiv 1 \pmod{3}]$$

$$a^6 \equiv 1 \pmod{7} \checkmark [\text{Segue do T. de Fermat, imediatamente}]$$

$$a^6 \equiv 1 \pmod{8} \checkmark$$

$$\text{Como } \text{mdc}(a, 42) = 1 \Rightarrow a \equiv 1 \pmod{2}.$$

$$\text{Assim } a \equiv \pm 1 \text{ ou } \pm 3 \pmod{8}, \text{ mas em todos estes casos } a^2 \equiv 1 \pmod{8}, \text{ portanto } a^6 \equiv 1 \pmod{8}$$

$$\text{Agora } (*) \Rightarrow a^6 \equiv 1 \pmod{3 \cdot 7 \cdot 8} //$$

Ex. 3 Encontre resto da div. de 13^{26} por 10.

Temos que $13 \equiv 3 \pmod{10}$, assim basta

encontrar resto da div. de 3^{26} por 10

Como $\text{mdc}(3, 10) = 1$, assim podemos aplicar o Teorema de Euler, temos que $\varphi(10) = 4$, assim $3^4 \equiv 1 \pmod{10}$

$$\Rightarrow 3^{26} = (3^4)^6 \cdot 3^2 \equiv 3^2 \pmod{10}$$

$$\Rightarrow 3^{26} \equiv 9 \pmod{10}.$$

Assim resto é 9.

Ex. 4 Encontre resto da divisão de 69^{903} por 31

Sol. Temos que $69 \equiv 7 \pmod{31}$.

Por outro lado 31 é primo, assim aplicando o T. de Fermat temos $7^{30} \equiv 1 \pmod{31}$.

$$\text{Assim } 7^{903} = (7^{30})^{30} \cdot 7^3 \equiv 7^3 \pmod{31}.$$

$$\text{Agora } 7^3 = 343 \equiv 2 \pmod{31}.$$

$$\Rightarrow \text{resto é } 2 //$$

Ex. 5. Resolva $\varphi(x) = 140$.

Sol. Suponha que $x = p_1^{d_1} \cdots p_k^{d_k}$, Assim $\varphi(x) = 140$, implique

$$p_1^{d_1-1} (p_1-1) \cdots p_k^{d_k-1} (p_k-1) = 2^2 \cdot 5 \cdot 7. \quad (1)$$

Primeiramente, se 2 não é fator primo

Assim, como $140 = 2^2 \cdot 5 \cdot 7$, n tem exatamente 2 fatores primos [pois $p_i - 1$ é par].

Neste caso $n = 3 \cdot 71 = 213$, e

$$\varphi(213) = (3-1) \cdot (71-1) = 2 \cdot 70 = 140 //$$

Agora, obviamente $2 \cdot 213$ é solução também, pois

$$\varphi(2 \cdot 213) = (2-1) \cdot (3-1) \cdot (71-1) = 140.$$

Suponha que 2^d é fator de n, com $d \geq 1$,

Assim $2^{d-1} \cdot \underbrace{p^{d-1} \cdot (p-1)}_{\text{par}} = 2^2 \cdot 5 \cdot 7$

e $d=2$, temos que $p=71$ de novo,

neste caso $n = 4 \cdot 71 = 284$. Assim

213, 284, 426 todas sol. possíveis.

Exer. 6

Sejam p, q primos distintos impares, tais que $(p-1) | (q-1)$ e $\text{mdc}(a, pq) = 1$. Mostre que $a^{q-1} \equiv 1 \pmod{pq}$.

Solução

$\text{mdc}(a, pq) = 1$ implique que

$$\text{mdc}(a, p) = 1$$

$$\text{mdc}(a, q) = 1$$

Assim, pelo T. de Fermat,

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{e} \quad \{a^{q-1} \equiv 1 \pmod{q}\} \quad \textcircled{1}$$

Mas $(p-1) \mid (q-1)$, ou seja $(q-1) = (p-1) \cdot t$ $\textcircled{2}$

$$\text{Assim } a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^{(q-1)} \equiv 1 \pmod{p}$$

$$\textcircled{1}, \textcircled{2} \Rightarrow a^{(q-1)} \equiv 1 \pmod{pq}, \text{ pois } p, q \text{ s\~ao distintas.} //$$

Ex. 7 Sejam a inteiro, $n > 0$ com
 $\text{mdc}(a, n) = 1 = \text{mdc}(a-1, n).$

Mostre que

$$1 + a + \dots + a^{\varphi(n)-1} \equiv 0 \pmod{n}$$

Solu\~ao Temos $a^{\varphi(n)} \equiv 1 \pmod{n}$ [pois $\text{mdc}(a, n) = 1$]

$$\text{Assim } a^{\varphi(n)} - 1 \equiv 0 \pmod{n}, //$$

$$(a-1)(1+a+a^2+\dots+a^{\varphi(n)-1}) \equiv 0 \pmod{n}$$

Como $\text{mdc}(a-1, n) = 1$, assim

$$1 + a + a^2 + \dots + a^{\varphi(n)-1} \equiv 0 \pmod{n} //$$

Ex. 8 [12 b) Lista 4].

6

Mostre que $a^{37} \equiv a \pmod{1729}$

Solução. Note que $1729 = 7 \cdot 13 \cdot 19$.

Agora aplicando o T. de Fermat, temos

$$a^{37} = (a^7)^5 \cdot a^2 \equiv a^5 \cdot a^2 = a^7 \equiv a \pmod{7}$$

$$a^{37} = (a^{13})^2 \cdot a^{11} \equiv a^2 \cdot a^{11} = a^{13} \equiv a \pmod{13}$$

$$a^{37} = a^{19} \cdot a^{18} \equiv a \cdot a^{18} = a^{19} \equiv a \pmod{19}$$

Assim $a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19}$.

Ex. 9 Mostre que 2017 divide $2016^{2017} + 2016! \cdot 2016$

Solução. Observe que 2017 é um primo.

Assim, aplicando T. de Fermat e Wilson, temos

$$2016^{2017} \equiv 2016 \pmod{2017}$$

$$2016! \cdot 2016 \equiv -2016 \pmod{2017}$$

$$\Rightarrow 2016^{2017} + 2016! \cdot 2016 \equiv 0 \pmod{2017}$$

ou seja 2017 divide $2016^{2017} + 2016! \cdot 2016$ //

Ex.10. Encontre o resto da divisão de $85!$ por 89 .

Sol. 89 é primo, assim $88! \equiv -1 \pmod{89}$ pelo T. de Wilson. Assim

$$-1 \equiv 85! \cdot 86 \cdot 87 \cdot 88 \pmod{89}$$

$$-1 \equiv 85! \cdot (-3) \cdot (-2) \cdot (-1) \pmod{89}$$

$$\Rightarrow 85! \cdot 6 \equiv 1 \pmod{89}.$$

Fácil ver que $6 \cdot 15 \equiv 1 \pmod{89}$, ou seja 15 é inverso multiplicativo de 6 , Assim

$$85! \cdot 6 \cdot 15 \equiv 85! \equiv 15 \pmod{89}$$

Assim o resto é 15 //

Ex.11. Suponha que $p > 3$ um primo.

Mostre que $(p-3)! \equiv -\frac{p+1}{2} \pmod{p}$.

Sol. Pelo T. de Wilson, temos que

$$(p-1)! \equiv -1 \pmod{p}, \text{ assim}$$

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

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

$$\text{Mas } -2 \cdot \left(-\frac{p+1}{2}\right) = p+1 \equiv 1 \pmod{p}$$

$$\Rightarrow (p-3)! \equiv -\frac{p+1}{2} \pmod{p} //$$

Ex. 12 [20 da lista 4].

8

8. Mostre que

a) $\varphi(4n) = 2\varphi(2n)$

b) $\varphi(4n+2) = \varphi(2n+1)$

Solução a) Suponha que $n = 2^k \cdot u$, com $\text{mdc}(2, u) = 1$.

Assim

$$\varphi(4 \cdot n) = \varphi(2^{k+2} \cdot u) = \varphi(2^{k+2}) \cdot \varphi(u) = 2^{k+1} \cdot \varphi(u)$$

" " "

$$2 \varphi(2n) = 2 \cdot \varphi(2^{k+1} \cdot u) = 2 \cdot 2^k \cdot \varphi(u) = 2^{k+1} \cdot \varphi(u)$$

$$b) \quad \varphi(4n+2) = \varphi(2 \cdot (2n+1)) = \varphi(2) \cdot \varphi(2n+1) = \varphi(2n+1)$$

" 1

$$\text{mdc}(2, 2n+1) = 1.$$