

Exercícios da Lista 6

1

7 (a) p ímpar

$$(p-1)! \equiv p-1 \pmod{1+2+\dots+(p-1)}$$

Pelo Teorema de Wilson $(p-1)! \equiv p-1 \pmod{p}$

$$1+2+\dots+p-1 = \frac{(p-1)(p-1+1)}{2} = p \frac{(p-1)}{2}$$

$$\underbrace{(p-1)! - (p-1)}_{p \mid} = (p-1) \underbrace{[(p-2)! - 1]}_{p \mid \text{ por (*)}} = 2 \underbrace{\left(\frac{p-1}{2}\right)}_{p \nmid} \underbrace{[(p-2)! - 1]}_{p \mid \text{ por (*)}}$$

$$(*) \text{ mdc}(p-1, p) = 1 \Rightarrow p \mid [(p-2)! - 1].$$

(b) p primo

Sabemos que $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$.

$$a^p + a(p-1)! \equiv a + a(p-1)! \pmod{p} \equiv a - a \pmod{p} \equiv 0 \pmod{p}$$

$\hookrightarrow$ Teo de Wilson.

12: Seja p um primo ímpar. Mostrar que $\binom{2p}{p} \equiv 2 \pmod{p}$.

$$\text{Seja } x = \binom{2p}{p} = \frac{2p(2p-1)\cdots 2p-(p-1)\cancel{p!}}{p!\cancel{p!}}.$$

$$\text{Logo } (p!)x = 2p(2p-1)\cdots(2p-(p-1))$$

$$\text{Assim } (p-1)!x = 2(2p-1)(2p-2)\cdots(2p-(p-1)) \equiv 2(-1)(-2)\cdots(-(p-1)) \pmod{p}$$

Assim, pelo T. de Wilson,

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

$$2(-1)^{p-1}(p-1)! \equiv -2 \pmod{p}$$

$$\text{Logo } x \equiv 2 \pmod{p}. \quad \square$$

$$14: \text{mdc}(n!+1, (n+1)!)$$

3

$$(n+1)! \mid (n!+1) \quad (n+1)! (n+1) (n!+1) - (n+1) \\ - (n+1)! - (n+1)(n+1)$$

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

Se $n+1 = p$ primo, então $n = p-1$ e $n!+1 \equiv 0 \pmod{(n+1)}$

Se $n+1$ é composto, sabemos que $n+1 \mid n!$. Logo

$$n!+1 \equiv 1 \pmod{n+1} \quad n! = (n+1)q + 1$$

$$\text{Assim } \text{mdc}(n!+1, (n+1)!) = \begin{cases} n+1 & \text{se } n+1 \text{ é primo} \\ 1 & \text{se } n+1 \text{ é composto} \end{cases}$$

(17) Mostrar que $\varphi(m^x) = m^{x-1} \varphi(m)$ para todos m, x inteiros positivos.

Suponha que $m = p^k$, p primo.

$$\begin{aligned} \varphi(m^x) &= \varphi(p^{kx}) = p^{kx-1} (p-1) = p^{kx-k+k-1} (p-1) \\ &= \underbrace{(p^k)^{x-1}}_m \underbrace{p^{k-1} (p-1)}_{\varphi(m)} \end{aligned}$$

Agora é só usar o TFA e escrever

$m = p_1^{x_1} \dots p_t^{x_t}$ e usar que φ é multiplicativa.

(18) Mostrar que $\varphi(n) \mid n \iff n$ é da forma $1, 2^k, 2^k 3^l$

$$\begin{aligned} n = 1 & \quad \varphi(n) = 1 \\ n = 2^k & \quad \varphi(n) = 2^{k-1} \mid 2^k = n \end{aligned}$$

$$n = 2^k 3^l \Rightarrow \varphi(n) = 2^{k-1} (3-1) 3^{l-1} = 2^k 3^{l-1} \mid n.$$

6

$$(\Rightarrow) \quad n = 2^{k_1} 3^{k_2} p_3^{k_3} \dots p_s^{k_s} \quad p_i \text{ primo}, p_i > 3$$

$$\varphi(n) = 2^{k_1-1} 3^{k_2-1} p_3^{k_3-1} \dots p_s^{k_s-1} (p_3-1) \dots (p_s-1)$$

$$\varphi(n) \mid n \Rightarrow \frac{n}{\varphi(n)} = \frac{3 p_3 \dots p_s}{(p_3-1) \dots (p_s-1)} \Rightarrow$$

$$\underbrace{(p_3-1) \dots (p_s-1)}_{\text{par}} \mid \underbrace{3 p_3 \dots p_s}_{\text{ímpar}} \quad \text{impossível}$$

Logo não pode haver primos maiores do que 3 na decomposição de n . Assim $n = 2^k 3^l$, Agora $k=0$ e $l>0 \Rightarrow l=1$, pois se $l>1$

$$\varphi(3^l) = 2 \cdot 3^{l-1} \nmid 3^l.$$

①⑨ $n = 3, 4, 6 \quad \varphi(n) = 2$ primo.

Suponha agora que $\varphi(n) = p$, primo.

$$n = 2^{k_1} 3^{k_2} p_2^{k_3} \dots p_s^{k_s}$$

Se $p > 3$ é tq $p | n$ então

$p-1 | \varphi(n)$. Mas $p-1 > 2$ e $p-1$ é par.

$$\text{Logo } (p-1) = 2 \cdot \underbrace{\left(\frac{p-1}{2}\right)}_{>1}$$

Logo não há primos maiores do que 3 na decomposição de n .

Assim $n = 2^k 3^l$.

Temos que ter $l = 0$ ou $l = 1$, pois se $l > 2 \Rightarrow 6 | \varphi(n)$ e 6 não é primo. Também, $k \leq 2$, pois se $k > 2$, $4 | \varphi(n)$

Assim $n = 2^k 3^l$, $l \leq 1$, $k \leq 2$

$l = 1$ e $k = 0$, OK $n = 3$ e $\varphi(n) = 2$

$l = 1$ e $k = 1$, OK $n = 6$ e $\varphi(n) = 2$

$l = 1$ e $k = 2$ não pode pois $n = 2 \cdot 3$ e $\varphi(n) = 4$ —

$l = 0$ e $k = 2$ OK $n = 4$ e $\varphi(n) = 2$

$l = 0$ e $k = 1$ $n = 2$ $\varphi(n)$ não é primo.

2.2) Mostrar que se $m > 0$

$$\sum_{d|m} \varphi(d) = m.$$

(Fórmula de Gauss)

Seja $I = \{1, 2, \dots, m\}$

Seja d tal que $d|m$ e seja $I_d = \{x \in I \mid \text{mdc}(x, m) = d\}$.

Se $d \neq d' \Rightarrow I_d \cap I_{d'} = \emptyset$. (É claro)

Se $x \in I$, $\exists d$ com $d|m$ tal que $\text{mdc}(x, m) = d \Rightarrow x \in I_d$.

Logo $I = \bigsqcup_{d|m} I_d$ e como eles são 2 a 2 disjuntos,

$$|I| = \sum_{d|m} |I_d|.$$

Se $x \in I_d \Rightarrow \text{mdc}\left(\frac{x}{d}, \frac{m}{d}\right) = 1 \iff x = kd, \text{mdc}\left(k, \frac{m}{d}\right) = 1$.
Além disso, $1 \leq k \leq \frac{m}{d}$. Assim $|I_d| = \varphi\left(\frac{m}{d}\right)$.

Agora, $d \mid m \Leftrightarrow \frac{m}{d} \mid m$

$$m = |I| = \sum_{d \mid m} |I_d| = \sum_{d \mid m} \varphi\left(\frac{m}{d}\right) = \sum_{\frac{m}{d} \mid m} \varphi\left(\frac{m}{d}\right) = \sum_{d \mid m} \varphi(d).$$