

- Cap 3: Seção 3.4

- Sistemas de Congruências Lineares:

$$(i) X \equiv 2 \pmod{3}$$

$$(ii) X \equiv 3 \pmod{5}$$

$$(iii) X \equiv 2 \pmod{7}$$

De (i), temos que $3 \mid x-2 \Rightarrow x-2 = 3y \Rightarrow x = 2 + 3y$. (1)

Agora, queremos que esses valores de x satisfaçam também (ii). Logo, devemos ter

$$2 + 3y \equiv 3 \pmod{5} \Leftrightarrow 3y \equiv 1 \pmod{5} \Leftrightarrow$$

$$y \equiv 2 \pmod{5} \Leftrightarrow 5 \mid y-2 \Leftrightarrow y = 2 + 5z$$
. (2)

Substituindo (2) em (1), vem que

$$x = 2 + 3(2 + 5z) = 8 + 15z$$
. (3)

são soluções de (i) e (ii).

Para que (3) seja sol. de (iii) devemos ter que

$$8 + 15z \equiv 2 \pmod{7} \Leftrightarrow 15z \equiv -6 \pmod{7} \Leftrightarrow$$

$$z \equiv -6 \pmod{7} \Leftrightarrow z = -6 + 7t$$
. (4)

Substituindo (4) em (3)

$$x = 3 + 15(-6 + 2t) = -82 + 105t$$

Logo, $x = -82 + 105t$ são soluções de (i), (ii) e (iii).



Vamos agora, tentar resolver um problema mais geral.

Considere o sistema:

$$(*) \begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases}$$

Para que o sistema tenha solução, será necessário que cada uma das congruências, considerada individualmente, admita solução. Logo, devemos ter que $d_i = \gcd(a_i, m_i) \mid b_i$, $1 \leq i \leq k$. (Prop. 3.3.1)

Nesse caso, cada uma das equações do sistema é equivalente a uma equação na forma $x \equiv c_i \pmod{n_i}$, onde $n_i = m_i/d_i$.

obs: Prop 3.3.9: Sejam a e m inteiros e b um múltiplo de $d = \gcd(a, m)$. Escrevendo $a = a_1 d$, $b = b_1 d$ e $m = n d$ e $d = ar + bs$ (Bezout), temos que a

congruência $ax \equiv b \pmod{m}$ é equivalente a
 $x \equiv rb_1 \pmod{n}$

Demonstração:

Queremos mostrar que o conjunto solução de
 $ax \equiv b \pmod{m}$ e de $x \equiv rb_1 \pmod{n}$ são iguais.

$$ax \equiv b \pmod{m} \Leftrightarrow a_1 d x \equiv b_1 d \pmod{nd} \Leftrightarrow$$

$$nd \mid a_1 d x - b_1 d \Leftrightarrow n \mid a_1 x - b_1 \Leftrightarrow a_1 x \equiv b_1 \pmod{n} \quad (*)$$

Observe que $d = ar + ms = a_1 dr + nds \Rightarrow$

$$1 = a_1 r + ns \Rightarrow a_1 r \equiv 1 \pmod{n}$$

$$\text{Logo, } a_1 x \equiv b_1 \pmod{n} \stackrel{(*)}{\Rightarrow} a_1 r x \equiv b_1 r \pmod{n} \Leftrightarrow$$

$$x \equiv b_1 r \pmod{n}$$

Observe que só precisamos mostrar que vale a
recíproca em (*). Como $ra_1 + ns = 1 \Rightarrow \gcd(r, n) = 1$,
logo, pelo prop. 3.2.4 vale a recíproca.



— " —
(Voltando ao nosso problema...)

Temos que o sistema original (*) é equivalente ao
seguinte sistema:

$$\begin{cases} X \equiv c_1 \pmod{n_1} \\ X \equiv c_2 \pmod{n_2} \\ \vdots \\ X \equiv c_k \pmod{n_k} \end{cases} \quad (**)$$

Para resolver o sistema acima, vamos recorrer ao Teorema Chinês do Resto.

Teorema: Sejam $n_1, n_2, \dots, n_k$ inteiros, relativamente primos dois a dois (i.e., $\text{mdc}(n_i, n_j) = 1$, se $i \neq j$) e sejam $c_1, c_2, \dots, c_k$ inteiros arbitrários. Então, o sistema de congruências lineares

$$X \equiv c_1 \pmod{n_1}$$

$$X \equiv c_2 \pmod{n_2}$$

$$\vdots$$

$$X \equiv c_k \pmod{n_k}$$

admite uma solução, que é única módulo $n_1 \dots n_k$.

Demonstração:

Consideremos o número $n = n_1 \dots n_k$. Para cada índice i , definimos o número $N_i = \frac{n}{n_i}$. Como

N_i é o produto de todos os inteiros, $n_1, \dots, n_k$, omitindo n_i e eles são rel. primos, $\text{mdc}(N_i, n_i) = 1$. Assim,

pelo teorema de Bezout, existem $r_i, s_i \in \mathbb{Z}$ tais que

$$r_i N_i + s_i n_i = 1 \quad 1 \leq i \leq k \quad (1)$$

Mostremos então que o número

$$x_0 = c_1 r_1 N_1 + \dots + c_k r_k N_k$$

é uma solução do sistema.

De fato, observe que se $i \neq j$ então $N_j \equiv 0 \pmod{n_i}$,

pois n_i é um dos fatores de N_j , logo $c_j r_j N_j \equiv 0 \pmod{n_i}$, donde

$$x_0 = c_1 r_1 N_1 + \dots + c_k r_k N_k \equiv c_i r_i N_i \pmod{n_i}$$

Por (1), temos que $r_i N_i \equiv 1 \pmod{n_i}$. Portanto,

$$x_0 \equiv c_i \pmod{n_i}, \quad 1 \leq i \leq k.$$

Precisamos apenas mostrar que toda outra solução é congruente a x_0 módulo n .

Para tanto, seja x outra solução, temos que

$$x \equiv c_i \pmod{n_i}, \quad 1 \leq i \leq k. \text{ Como também } x_0 \equiv c_i \pmod{n_i},$$

pela transitividade da congruência, $x \equiv x_0 \pmod{n_i}$,

$1 \leq i \leq k$, i.e., $n_i \mid x - x_0$, para cada i , $1 \leq i \leq k$. Como

os n_i são rel. primos $n \mid x - x_0$. Logo $x \equiv x_0 \pmod{n}$

Observe que a demonstração nesse caso é importante não só por assegurar o resultado, mas ela nos dá um manual passo a passo de como encontrar uma solução para o sistema em questão.

→ Exemplo:

Considere o sistema

$$\left. \begin{array}{l} 6x \equiv 2 \pmod{4} \\ 2x \equiv 1 \pmod{3} \\ 4x \equiv 2 \pmod{7} \end{array} \right\} \quad (1)$$

Temos que

$$\begin{array}{lll} \text{mdc}(6, 4) = 2 & \Rightarrow & \begin{array}{c} r \\ \boxed{1} \end{array} \quad 6 + (-1) \cdot 4 = 2 \\ \text{mdc}(2, 3) = 1 & \Rightarrow & \begin{array}{c} \boxed{-1} \end{array} \quad 2 + (1) \cdot 3 = 1 \\ \text{mdc}(4, 7) = 1 & \Rightarrow & \begin{array}{c} \boxed{2} \end{array} \quad 4 + (-1) \cdot 7 = 1 \end{array}$$

Assim, o sistema (1) é equivalente a

$$(2) \quad \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv -1 \pmod{3} \\ x \equiv 4 \pmod{7} \end{cases}$$

Note que (2) está nas condições do teorema chinês do Resto. Assim,

Considerando $n = 2 \cdot 3 \cdot 7 = 42$, $N_1 = \frac{42}{2} = 21$,

$N_2 = \frac{42}{3} = 14$ e $N_3 = \frac{42}{7} = 6$. Escrevemos então

$$\text{mdc}(N_1, n_1) = \text{mdc}(21, 2) = 1 \cdot 21 + (-10) \cdot 2 \Rightarrow r_1 = 1$$

$$\text{mdc}(N_2, n_2) = \text{mdc}(14, 3) = (-1) \cdot 14 + (5) \cdot 3 \Rightarrow r_2 = -1$$

$$\text{mdc}(N_3, n_3) = \text{mdc}(6, 7) = (-1) \cdot 6 + (1) \cdot 7 \Rightarrow r_3 = -1$$

Daí,

$$x_0 = 1 \cdot 1 \cdot 21 + (-1) \cdot (-1) \cdot 14 + 4 \cdot (-1) \cdot 6 = 11$$

Logo, toda outra sol. do sistema é congruente a x_0 ,

$$x \equiv x_0 \pmod{n} \Leftrightarrow n \mid x - x_0 \Leftrightarrow x = x_0 + n \cdot t, t \in \mathbb{Z}.$$



↳ Os teoremas de Fermat, Euler e Wilson

- Teorema de Fermat:

Seja p um primo e a um inteiro tal que $p \nmid a$. Então, $a^{p-1} \equiv 1 \pmod{p}$

Demonstração:

Consideremos o conjunto de inteiros:

$$\{a, 2a, 3a, \dots, (p-1)a\} \quad (1)$$

Dados dois elementos quaisquer desse conjunto, eles não são congruentes entre si, caso ocorresse,

$$xa \equiv ya \pmod{p} \Leftrightarrow x \equiv y \pmod{p}, \text{ pois}$$

$\text{mdc}(a, p) = 1$ logo como $1 \leq x, y \leq p-1$ e $x \neq y$, teremos

uma contradição, pois os elementos de

$$\{1, \dots, (p-1)\} \quad (2)$$

não são congruentes entre si, módulo p .

Além disso, nenhum dos elementos de (1) é congruente a 0 módulo p , já que se $p \mid xa$, $x \in \{1, \dots, (p-1)\}$, como $\text{mdc}(p, a) = 1$, pelo teo. de Euclides $p \mid x$, contradição.

Logo, como $\{1, \dots, (p-1)\}$ é um sistema completo de Resíduos módulo p , todo elemento de $\{a, \dots, (p-1)a\}$, deve ser congruente a um único elemento de $\{1, \dots, (p-1)\}$. Com isso, temos $(p-1)$ congruências.

$$a \equiv x_1 \pmod{p}$$

⋮

$$(p-1)a \equiv x_{p-1} \pmod{p}$$

onde $x_1, \dots, x_{p-1}$ são os inteiros $1, \dots, (p-1)$, eventualmente em uma outra ordem

Multiplicando ordenadamente essas congruências, temos

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

ou seja,

$$(p-1)! a^{p-1} \equiv (p-1)! \pmod{p} \quad (*)$$

Como $\text{mdc}((p-1)!, p) = 1$, de (*) segue que,

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



→ Corolário: Seja p um primo e a um inteiro arbitrário. Então $a^p \equiv a \pmod{p}$.

Demonstração:

Se $p \nmid a$, pelo teo. de Fermat,

$$a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$$

Se $p \mid a \Rightarrow p \mid a^p$. Logo $p \mid a^p - a \Rightarrow$

$$a^p \equiv a \pmod{p}$$



↳ Exemplo:

Dados a e b inteiros arbitrários e p um primo tem-se

$$\text{que } (a+b)^p \equiv a^p + b^p \pmod{p}$$

Assim, veja que

$$(a+b)^P = \sum_{i=0}^P \binom{P}{i} a^{P-i} b^i$$

e, para $1 \leq i \leq P-1$, temos que

$$\binom{P}{i} a^{P-i} b^i = \left(\frac{P!}{(P-i)! \cdot i!} \right) a^{P-i} b^i =$$

$$P \left(\frac{(P-1)!}{(P-i)! \cdot i!} \right) a^{P-i} b^i \equiv 0 \pmod{P}.$$

Dai, segue que $(a+b)^P \equiv a^P + b^P \equiv a + b \pmod{P}$.



→ Teorema de Euler (1747) - generalização do Teorema de Fermat

obs: Se n não é primo, $\text{mdc}((n-1)!, n) \neq 1$.

De fato, considere que $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Temos que

$(n-1)! = (n-1) \cdot (n-2) \cdots 2 \cdot 1$. Veja que $p_i < n$, $1 \leq i \leq k$.

Logo $p_i \in \{1, \dots, n-1\}$. Portanto $p_i \mid (n-1)!$, para $1 \leq i \leq k$. Logo, $\text{mdc}(n, (n-1)!) \neq 1$.



A prova de Euler é uma modificação da prova de Fermat.

Dado n , considere o conjunto de números entre 1 e $(n-1)$ que são relativamente primos com n . Vamos denotar esse conjunto por A

$$A = \{x_1, \dots, x_t\}$$

isto é, cada x_i é tal que

$$1 \leq x_i \leq n-1 \text{ e } \text{mdc}(x_i, n) = 1$$

Agora, dada outra número a tal que $\text{mdc}(a, n) = 1$, consideremos o conjunto de números

$$B = \{x_1 a, \dots, x_t a\}$$

Como $x_i a$ é relativamente primo com n , o resto de $x_i a$ por n deve ser um dos elementos de A . De fato, note que pelo algoritmo da divisão,

$$x_i a = nq + x, \quad 0 \leq x < n \quad \text{Veja que } A \subseteq \{0, 1, \dots, n-1\}.$$

Considere que $x \notin A$ então, $\text{mdc}(x, n) = d \neq 1$. Então

$d|x$ e $d|n \Rightarrow d|x + nq = x_i a$. Portanto, $\text{mdc}(x_i a, n) \geq d$.
contradição.

Agora, como $x_i a \equiv x_j a \pmod{n} \Leftrightarrow x_i \equiv x_j \pmod{n}$ e
não podemos ter $x_i \equiv x_j \pmod{n}$, devemos ter que os

os elementos de B são congruentes a elementos de A de modo biunívoco, i.e., cada elemento de A é congruente a um único elemento de B .

Desse modo, segue que

$$x_1 a \equiv x_{i_1} \pmod{n}$$

$$x_2 a \equiv x_{i_2} \pmod{n}$$

$\vdots$

$$x_t a \equiv x_{i_t} \pmod{n}$$

em que os elementos de $x_{i_1}, \dots, x_{i_t}$ são os elementos de A , eventualmente em outra ordem. Com isso, prosseguimos analogamente ao teorema de Fermat e,

$$(x_1 \dots x_t) a^t \equiv (x_{i_1} \dots x_{i_t}) \pmod{n}$$

Como $\text{mdc}(x_i, n) = 1 \Rightarrow \text{mdc}(x_1 \dots x_t, n) = 1$. Assim,

$$(x_1 \dots x_t) a^t \equiv (x_1 \dots x_t) \pmod{n} \Rightarrow a^t \equiv 1 \pmod{n}$$

Assim, provamos a generalização do teorema de Fermat proposto por Euler. Mas antes de enunciarmos o resultado, considere a seguinte definição:

Definição: Para cada inteiro $n \geq 1$, indicaremos por $\phi(n)$ o número de inteiros positivos, menores ou iguais a n , que são relativamente primos com n . A função assim definida, chama-se função ϕ de Euler.

Observe que no nosso estudo feito a pouco, $t = \phi(n)$. Assim, provamos:

Teorema (de Euler): Sejam a e n inteiros com $n \geq 1$, tais que $\text{mdc}(a, n) = 1$. Então

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

Note que $\phi(p) = p-1$, com p primo, assim o Teorema de Fermat é um caso particular do Teorema de Euler.

Lema: Seja $p > 0$ um inteiro primo. Consideremos o conjunto $C = \{1, 2, \dots, p-1\}$. Para cada elemento $a \in C$ existe um número $b \in C$ tal que $ab \equiv 1 \pmod{p}$.

Demonstração:

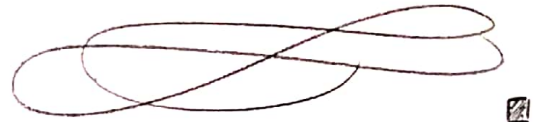
Considere $a \in \mathbb{C}$, note que $\text{mdc}(a, p) = 1$. Agora pelo Teorema de Bézout, existem $r, s \in \mathbb{Z}$ tais que

$$ar + ps = 1$$

Daí, $ar \equiv 1 \pmod{p}$. Como $\{1, \dots, (p-1)\}$ é um sistema completo de resíduos módulo p , existe $b \in \mathbb{C}$ tal que

$$r \equiv b \pmod{p} \text{ logo}$$

$$ab \equiv ar \equiv 1 \pmod{p}$$



Lemma: Seja p um inteiro primo. Os únicos elementos do conjunto $C = \{1, 2, \dots, (p-1)\}$ que verificam a equação $x^2 \equiv 1 \pmod{p}$ são 1 e $p-1$.

Demonstração:

Se $a \in \mathbb{C}$ é tal que $a^2 \equiv 1 \pmod{p}$, temos que $p \mid a^2 - 1$, i.e., $p \mid (a+1)(a-1)$.

Como p é primo, $p \mid a+1$ ou $p \mid a-1$.

No primeiro caso, como $1 \leq a \leq p-1$, temos que

$$2 \leq a+1 \leq p. \quad (1)$$

$$\text{Como } p \mid a+1 \Rightarrow a+1 \geq p. \quad (2)$$

Por (1) e (2), segue que $p = a+1 \Rightarrow a = p-1$

Analogamente se $p \mid a-1$ então como

$$1 \leq a \leq p-1 \Rightarrow 0 \leq a-1 \leq p-2 \quad (3)$$

Como $p \mid a-1 \Rightarrow a-1 \geq p \quad (4)$. De (3) e (4),

devemos ter que $a-1=0 \Rightarrow a=1$.



Teorema de Wilson:

Seja p um inteiro primo. Então:

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

Demonstração:

Se $p=2$, então $(2-1)! + 1 = 2 \equiv 0 \pmod{2}$. Se

$p=3$, $2! + 1 = 3 \equiv 0 \pmod{3}$. Considere $p > 3$.

Pelo lema 1 (ou lema 3.5.9 - pág 131), podemos agrupar os elementos $2, 3, \dots, (p-2)$, de dois em dois de forma a obter um valor congruente a 1. (Note que "ignoramos" 1 e $p-1$, pois pelo lema 2, $i^2 \equiv 1 \pmod{p}$ e $(p-1)^2 \equiv 1 \pmod{p}$). Assim,

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

Veja que $p-1 \equiv -1 \pmod{p}$. Daí, usando (1),

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

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

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



→ Lsta 6 (Solução)

Ex 1 (ex 2 - pág 133)

Demonstração:

(i) Como $\text{mdc}(a, p) = 1 \Rightarrow p \nmid a$. Assim, pelo Teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$. Daí,

$$a(a^{p-2} \cdot b) = a^{p-1} b \equiv 1 \cdot b \pmod{p}$$

(ii)(a) Vamos resolver $2x \equiv 1 \pmod{31}$. Observe que

$\text{mdc}(2, 31) = 1$. Daí, $2^{30} \equiv 1 \pmod{31}$. Assim,

$$2x \equiv 1 \pmod{31} \Leftrightarrow 2^{30} x \equiv 2^{29} \pmod{31} \Leftrightarrow$$

$$x \equiv 2^{29} \pmod{31}. \text{ Portanto, } x = 2^{29} + 31t, t \in \mathbb{Z}$$

são soluções de $2x \equiv 1 \pmod{31}$.

(b) $6x \equiv 5 \pmod{11}$. Observe que $\text{mdc}(6, 11) = 1 \Rightarrow$

$11 \nmid 6$. Daí, pelo teorema de Fermat,

$$6^{10} \equiv 1 \pmod{11}. \text{ Com efeito,}$$

$$6x \equiv 5 \pmod{11} \Leftrightarrow 6^9 6x \equiv 6^9 5 \pmod{11} \stackrel{(*)}{\Leftrightarrow}$$

$$x \equiv 6^9 5 \pmod{11}$$

Logo $x = 6^9 \cdot 5 + 11t, t \in \mathbb{Z}$.

Veja que $\text{m.d.c.}(6^9, 11) = 1$, pois $6^9 = (2 \cdot 3)^9 = 2^9 \cdot 3^9$.

(c) $3x \equiv 17 \pmod{29}$

Analogos aos anteriores.



Ex 2 (ex 4 - pag 133)

Demonstração:

Observe que $1, \dots, p-1$ são menores do que p . Assim,

$p \nmid 1, \dots, p \nmid p-1$. Logo, pelo teorema de Fermat,

$$1^{p-1} \equiv 1 \pmod{p}, \dots, (p-1)^{p-1} \equiv 1 \pmod{p}, \text{ donde,}$$

$1^p \equiv 1, \dots, (p-1)^p \equiv (p-1) \pmod{p}$ (Isso também segue do corolário 3.5.4). Daí,

$$1^p + \dots + (p-1)^p \equiv 1 + 2 + \dots + (p-1) = \frac{p(p-1)}{2} \equiv 0 \pmod{p},$$

pois $1 + \dots + (p-1)$ é uma soma de p.a.



Ex 3 (ex 5 - pág 133)

Demonstração:

- (i) Observe que $(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}$,
 $\forall x \in \mathbb{Z}$.

Ex 4 (ex 9 - pág 134)

Demonstração:

- (i) Queremos provar que $a^{37} \equiv a \pmod{1729}$. ^{primeiro}

Primeiro, veja que $1729 = 7 \cdot 13 \cdot 19$. Assim, lembre que se mostrarmos que $7 \mid a^{37} - a$, $13 \mid a^{37} - a$ e $19 \mid a^{37} - a$ então $1729 \mid a^{37} - a$. Na linguagem de congruências isso equivale a:

(1) $a^{37} \equiv a \pmod{7}$

De fato, $a^{37} = a^{35+2} = (a^7)^5 \cdot a^2$. Pelo corolário do Teo. de Fermat, $a^7 \equiv a \pmod{7}$. Assim,

$(a^7)^5 \cdot a \equiv a^5 \cdot a^2 = a^7 \pmod{7}$. Daí, novamente por esse cor.,

$$a^{37} \equiv a^7 \equiv a \pmod{7}.$$

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

Veja que $a^{37} = a^{2 \cdot 13 + 1} = (a^{13})^2 \cdot a$. Daí, usando a corolário do Teo de Fermat,

$$a^{37} = (a^{13})^2 \cdot a \equiv a^2 \cdot a = a^3 \pmod{13}. \text{ Novamente}$$

Pelo cor., $a^{37} \equiv a^3 \equiv a \pmod{13}$

(3) $a^{37} \equiv a \pmod{19}$

Temos que,

$$a^{37} = a^{19 + 18} = a^{19} \cdot a^{18}. \text{ Pelo cor. do Teo. de Fermat,}$$

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

Daí, $a^{37} \equiv a \pmod{19}$.

(ix) Vamos provar que $a^{79} \equiv a \pmod{158}$.

obs: Aproveitando a deixa, devemos mostrar que 79 é primo (assim como deveríamos fazer no item

(i) - reveja se consegue). No caso de 79, já discutimos em monitoria, que para um número ser primo ele não deve ter divisor menor ou igual a sua raiz quadrada. Assim, veja que

$\sqrt{79} < \sqrt{100} = 10$ e nenhum número entre 1 e 10 divide 79. Logo, ele é primo

Repare que $158 = 2 \cdot 79$. Daí, como no item anterior, se mostrarmos que $2 \mid a^{79} - a$ e $79 \mid a^{79} - a$ então $158 \mid a^{79} - a$. Então:

(1) $2 \mid a^{79} - a$. Vamos usar o cor. do Teo. de Fermat:

$$\text{Temos que } a^{79} = a^{78} \cdot a = (a^2)^{39} \cdot a \equiv a^{39} \cdot a = a^{40} \pmod{2}.$$

Tente mostrar que $a^{40} \equiv a \pmod{2}$. Daí,

$$a^{79} \equiv a \pmod{2}$$

(2) $79 \mid a^{79} - a$

Segue direto do corolário do teorema de Fermat.



Ex 5 (ex 11 - pág 139).

Demonstração:

Temos que $\text{mdc}(m, n) = 1$. Queremos provar que

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

Pelo teorema de Euler seguem:

$$m^{\phi(n)} \equiv 1 \pmod{n} \quad (1)$$

$$n^{\phi(m)} \equiv 1 \pmod{m} \quad (2)$$

De (1), vem que $n \mid m^{\phi(n)} - 1$ e de (2),

$m \mid n^{\phi(m)} - 1$. Assim,

$$mn \mid (m^{\phi(n)} - 1)(n^{\phi(m)} - 1) \quad (*)$$

Veja que $(m^{\phi(n)} - 1)(n^{\phi(m)} - 1) =$

$$= m^{\phi(n)} \cdot n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1 =$$

$$m^{\phi(n)} \cdot n^{\phi(m)} - (m^{\phi(n)} + n^{\phi(m)}) + 1.$$

Observe que, $\phi(n), \phi(m) \geq 1$ (Por que?). Logo,

$$mn \mid m^{\phi(n)} \cdot n^{\phi(m)} \Leftrightarrow m^{\phi(n)} \cdot n^{\phi(m)} \equiv 0 \pmod{mn}.$$

Por fim, de (*),

$$\underbrace{m^{\phi(n)} \cdot n^{\phi(m)}}_{\equiv 0 \pmod{mn}} - (m^{\phi(n)} + n^{\phi(m)}) + 1 \equiv 0 \pmod{mn} \Rightarrow$$

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$



→ Ex 6 (ex 13 - pag 133)

Demonstração:

(i) $a = 15!$ e $b = 17$ (primo)

Queremos que $15! = 17q + r$, $0 \leq r < 17$, na linguagem de congruências, esse fato é equivalente à

$$15! \equiv r \pmod{17} \quad (1).$$

Observe que, pelo Teorema de Wilson,

$$(17-1)! \equiv -1 \pmod{17} \Rightarrow 16! \equiv -1 \pmod{17} \Rightarrow$$

$$16 \cdot 15! \equiv -1 \pmod{17}. \text{ Note que } 16 \equiv -1 \pmod{17},$$

então,

$$16 \cdot 15! \equiv -1 \pmod{17} \Rightarrow -1 \cdot 15! \equiv -1 \pmod{17} \Rightarrow$$

$$15! \equiv 1 \pmod{17}$$

Portanto, $r = 1$.

(ix) $a = 2(26!)$, $b = 29$ (primo)

Queremos que $2 \cdot (26!) = 29q + r$, $0 \leq r < 29$. Usando congruências, devemos ter que

$$2 \cdot (26!) \equiv r \pmod{29}$$

Pelo teorema de Wilson, devemos ter que

$$(29-1)! \equiv -1 \pmod{29} \Rightarrow 28! \equiv -1 \pmod{29} \Rightarrow$$

$$28 \cdot 27 \cdot 26! \equiv -1 \pmod{29}.$$

Observe que $28 \equiv -1 \pmod{29}$ e $27 \equiv -2 \pmod{29}$,

Logo.

$$28 \cdot 27 \cdot 26! \equiv -1 \pmod{29} \Rightarrow$$

$$2 \cdot (26!) \equiv -1 \pmod{29} \Rightarrow 2(26!) \equiv 28 \pmod{29}$$

Portanto, $r = 28$.



Ex 7 (ex 14 - pág 134)

Demonstração:

obs

Pelo lema 3.5.9, considerando $p = 23$ (primo),

temos que para cada $a \in C = \{1, \dots, 22\}$, existe

$b \in C$ tal que $ab \equiv 1 \pmod{23}$.

Agora usando o lema 3.5.10, sabemos que os únicos elementos de C que satisfazem $x^2 \equiv 1 \pmod{23}$

são 1 e 22. Logo, podemos reunir os elementos

2, ..., 21 em pares tais que o produto seja con-

gruo a 1.

└───

Temos que

$$1) \quad 2x \equiv 1 \pmod{23} \Leftrightarrow \underbrace{12 \cdot 2}_2 x \equiv 12 \pmod{23} \Leftrightarrow$$

$x \equiv 12 \pmod{23}$. Logo, 2 e 12 estão associados.

$$2) 3X \equiv 1 \pmod{23} \Leftrightarrow \underbrace{8 \cdot 3}_{24} X \equiv 8 \pmod{23} \Leftrightarrow$$

$$X \equiv 8 \pmod{23} \quad \text{Assim, } 3 \text{ e } 8 \text{ est\u00e3o associados.}$$

$$3) 4X \equiv 1 \pmod{23} \Leftrightarrow \underbrace{6 \cdot 4}_{24} X \equiv 6 \pmod{23} \Leftrightarrow$$

$$X \equiv 6 \pmod{23}. \quad \text{Logo, } 4 \text{ e } 6 \text{ est\u00e3o associados.}$$

$$4) 5X \equiv 1 \pmod{23} \Leftrightarrow 25X \equiv 5 \pmod{23} \Leftrightarrow$$

$$2X \equiv 5 \pmod{23} \Leftrightarrow 2 \cdot 12X \equiv 60 \pmod{23} \Leftrightarrow$$

$$X \equiv 60 \pmod{23} \Leftrightarrow X \equiv 14 \pmod{23}. \quad \text{Logo, } 5 \text{ e } 14 \text{ est\u00e3o associados.}$$

$$5) 7X \equiv 1 \pmod{23} \Leftrightarrow 3 \cdot 7X \equiv 3 \pmod{23} \Leftrightarrow$$

$$21X \equiv 3 \pmod{23} \Leftrightarrow -2X \equiv 3 \pmod{23} \Leftrightarrow$$

$$2X \equiv -3 \pmod{23} \Leftrightarrow 2X \equiv 20 \pmod{23} \Leftrightarrow$$

$$X \equiv 20 \cdot 12 \pmod{23} \Leftrightarrow X \equiv 240 \pmod{23} \Leftrightarrow$$

$$X \equiv 10 \pmod{23}. \quad \text{Logo, } 7 \text{ e } 10 \text{ est\u00e3o associados.}$$

Da\u00ed, em diante voc\u00eas terminam.



Ex 8 (ex 15 - p\u00e1g 134)

Demonstra\u00e7\u00e3o:

Queremos provar que $18! \equiv -1 \pmod{437}$, ou ainda,

(25)

$437 \mid 18! + 1$. Repare que $437 = 19 \cdot 23$. Daí,

vamos mostrar que:

1) $19 \mid 18! + 1$

2) $23 \mid 18! + 1$

Pois $\text{m.d.c.}(19, 23) = 1$.

1) Pelo Teorema de Wilson, como 19 é primo,

$$18! + 1 \equiv 0 \pmod{19} \Rightarrow 19 \mid 18! + 1.$$

2) Novamente, pelo teorema de Wilson, para

o primo 23,

$$22! \equiv -1 \pmod{23} \Rightarrow 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23}$$

$$\text{(Como } 22 \equiv -1 \pmod{23}, 21 \equiv -2 \pmod{23},$$

$$20 \equiv -3 \pmod{23} \text{ e } 19 \equiv -4 \pmod{23}, \text{ temos que}$$

$$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \equiv -1 \pmod{23} \Leftrightarrow$$

$$\underbrace{2 \cdot 3 \cdot 4 \cdot (18!)}_{24 \equiv 1 \pmod{23}} \equiv -1 \pmod{23} \Leftrightarrow 18! \equiv -1 \pmod{23}.$$

Logo, $23 \mid 18! + 1$.

