$S_9(3) = \{\bar{2}^2, \bar{2}^4, \bar{2}^6\}$ $\quad \{\bar{4}, \bar{7}, \bar{1}\}$

$\mathbb{Z}^\times_{3^3}$ $\quad \phi(3^3) = 3^2(3-1) = 18$

$\bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \overline{16}, \bar{2}^5 = \bar{5}, \bar{2}^6 = \overline{10}, \bar{2}^7 = \overline{20} = -\bar{7}$

$\bar{2}^8 = -\overline{14} = \overline{13}, \bar{2}^9 = -\overline{28} = -\bar{1}, \bar{2}^{10} = -\bar{2}, \bar{2}^{11} = -\bar{4}, \bar{2}^{12} = -\bar{8}, \bar{2}^{13} = -16$

$\bar{2}^{14} = -\bar{5}, \bar{2}^{15} = -\overline{10}, \bar{2}^{16} = -\overline{20} = \bar{7}, \bar{2}^{17} = \overline{14} \quad \bar{2}^{18} = 1$

$x^9 \equiv 1 \mod 27$

$2^{9\gamma} \equiv 1 \mod 27$

$\Updownarrow$

$9\gamma \equiv 0 \mod 18 \quad \phi(27)$

$\Downarrow$

$2 | \gamma$

$S = \{\bar{2}^2, \bar{2}^4, \bar{2}^6, \bar{2}^8, \bar{2}^{10}, \bar{2}^{12}, \bar{2}^{14}, \bar{2}^{16}, \bar{2}^{18}\}$

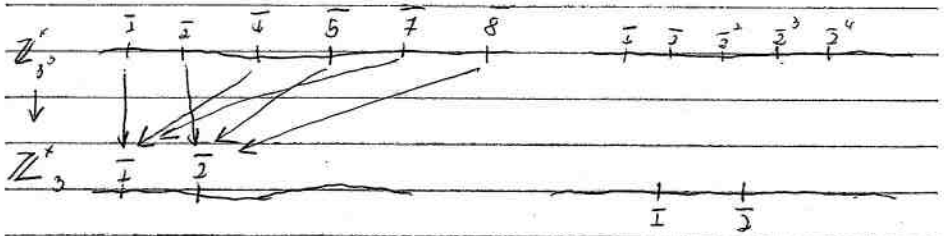
$\mathbb{Z}^\times_{7^2}$ $\quad \phi(7^2) = (7-1).7 = 42$

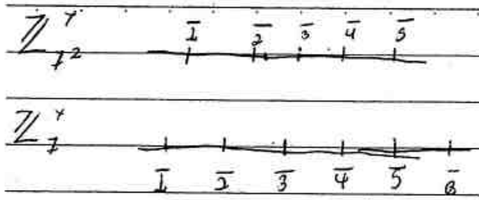
$\bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \overline{16}, \bar{2}^5 = \overline{32}, \bar{2}^6 = \overline{64} = \overline{15}, \bar{2}^7 = \overline{30}$

$\bar{2}^8 = \overline{60} = \overline{11}, \bar{2}^9 = \overline{22}, \bar{2}^{10} = \overline{44} = -\bar{5}, \bar{2}^{11} = -\overline{10}, \bar{2}^{12} = -\overline{20},$

$\bar{2}^{13} = \bar{9} \quad \bar{2}^{14} = \overline{18} \quad \bar{2}^{15} = \overline{36} \quad \bar{2}^{16} = \overline{23} \quad \bar{2}^{17} = \overline{46} = -3$

$2^{20} = -\overline{24} \quad 2^{21} = \bar{1}$



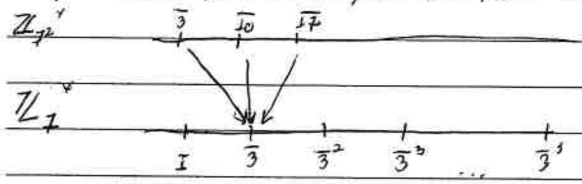


Para que exista um $\bar{g}$ em $\mathbb{Z}^\times_{p^e}$ t.q

$\mathbb{Z}^\times_{p^e} = \{\bar{1}, \bar{g}, \bar{g}^2, \bar{g}^3, \dots\}$

é necessário que $\mathbb{Z}^\times_p = \{\bar{1}, \bar{g}, \bar{g}^2, \dots, \bar{g}^{p-1}\}$

$\mathbb{Z}^\times_7 \quad \bar{3}, \bar{3}^2 = \bar{2}, \bar{3}^3 = \bar{6}, \bar{3}^4 = -\bar{3}, \bar{3}^5 = -\bar{2}, \bar{3}^6 = 1$



$\mathbb{Z}^\times_{7^2} \quad \bar{3}^k$

Desejo: $\bar{3}, \bar{3}^2, \dots, 3^k, \bar{3}^{k_0} = \bar{1}$

$k_0 = \phi(7^2) = 42$

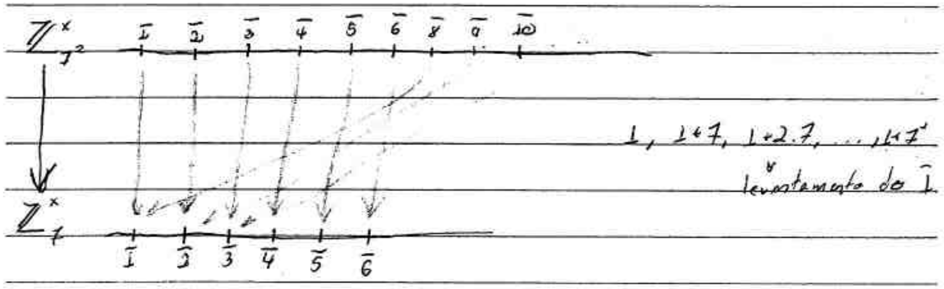
<u>Lema</u> Seja $\bar{a} \in \mathbb{Z}^\times_n$ e seja $k_0 = \min\{m \geq 1 : \bar{a}^m = \bar{1}\}$ então $k_0 | \phi(n)$ e, além disso, se $\bar{a}^a = \bar{1}$, então $k_0 | a$

Vimos
$$\mathbb{Z}^{\times}_{3^3} = \{1, 2, 2^2, \ldots, 2^{\phi(27)-1}\}$$

Def que $\mathbb{Z}^{\times}_n$ é cíclico se existir $g \in \mathbb{N}$ t.q.
$$\mathbb{Z}^{\times}_n = \{\bar{1}, \bar{g}, \bar{g}^2, \bar{g}^3, \ldots, \bar{g}^{\phi(n)-1}\}$$
e $\bar{g}$ é dito um gerador de $\mathbb{Z}^{\times}_n$

$\bar{2}$ é um gerador de $\mathbb{Z}^{\times}_{27}$

$\bar{2}$ NÃO é um gerador de $\mathbb{Z}^{\times}_{7^2}$



Se $\mathbb{Z}^{\times}_{7^2}$ for cíclico e gerado por $\bar{g}$
então $\mathbb{Z}^{\times}_7$ será cíclico e gerado por $\bar{g}$

$\mathbb{Z}^{\times}_7$ $\bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = 8 = \bar{1}$
$\{\bar{1}, \bar{2}, \bar{4}\} = \{2^s : s \geq 1\}$

$\bar{3}$ gera $\mathbb{Z}^{\times}_7$
$\bar{3}, \bar{3}^2 = 2, \bar{3}^3 = 6, \bar{3}^4 = 4, \bar{3}^5 = \bar{5}, \bar{3}^6 = \underline{1}$

Lema: Seja $\bar{a} \in \mathbb{Z}^{\times}_n$. Definindo
$h_0 \doteq \min\{m \geq 1 : a^m = \bar{1}\}$

Temos:

(1) $h_0 \mid \phi(n)$

(2) Se $\bar{a}^s = \bar{1}$ então $h_0 \mid s$

Dem

- $\phi(n) \in \{m \geq 1 : \bar{a}^m = \bar{1}\}$ pelo Teor Euler
  portanto h_0 está bem definido

$H \doteq \{\bar{1}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{h_0-1}\}$
H tem h_0 elementos

$\bar{b} \in \mathbb{Z}^{\times}_n$

$H.\bar{b} = \{\bar{1}.\bar{b}, \bar{a}.\bar{b}, \bar{a}^2.\bar{b}, \ldots, \bar{a}^{h_0-1}.\bar{b}\}$
transladados

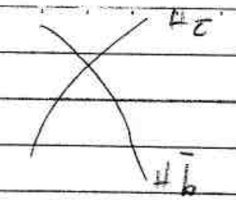
Quantos elementos tem $H\bar{b}$?
Se $\bar{a}^{\sigma}\bar{b} = \bar{a}^{i}\bar{b}$ então, como $b \in \mathbb{Z}^{\times}_n$ $\exists c \in \mathbb{Z}^{\times}_n$ $\bar{b}\bar{c} = \bar{1}$
$\bar{a}^{\sigma}.\bar{b}.\bar{c} = \bar{a}^{i}\bar{b}\bar{c}$
$\bar{a}^{J} = \bar{1}$

Conclusão:
$|H\bar{b}| = |H| = h_0 \quad \forall\, \bar{b} \in \mathbb{Z}^{\times}_n$

$H\bar{a} = \{\bar{1}.\bar{a}, \bar{a}.\bar{a}, \ldots, \bar{a}^{h_0-1}.\bar{a}\}$
$= \{\bar{a}, \bar{a}^2, \ldots, \bar{a}^{h_0}\}$

$H\bar{a}^2 = H \qquad H\bar{a}^{J} = H \quad \forall_J$

tilibra



$\bar{f} \in H_{\bar{c}}$

$\bar{f} = \bar{a}^{s} \cdot \bar{c}$

$\bar{f} \in H_{\bar{b}}$

$\bar{f} = \bar{a}^{i} \cdot \bar{b}$

$H\bar{f} = H\bar{a}^{j} \cdot \bar{c} = H\bar{a}^{i} \cdot \bar{b}$

$\quad\ \ \ \ \ H\bar{c} \qquad\quad H\bar{b}$

$\phi(n) = h_0 \cdot (N^{\circ}$ de transladados distintos de $H)$

1) $\phi(n) = h_0 \cdot x \to h_0 \mid \phi(n)$

(2) Se $\bar{a}^{s} = \bar{1} \Rightarrow s \geq h_0$

$S = q \cdot h_0 + r$

$\bar{1} = \bar{a}^{s} = \bar{a}^{(q \cdot h_0 + r)} = \bar{a}^{q h_0} \cdot a^{r} = (\bar{a}^{h_0})^{q} \cdot a^{r}$

$\bar{1} = \bar{a}^{r}$ como $r < h_0 \Rightarrow r = 0$

<u>Def</u> Se $\bar{a} \in \mathbb{Z}_n^{\times}$

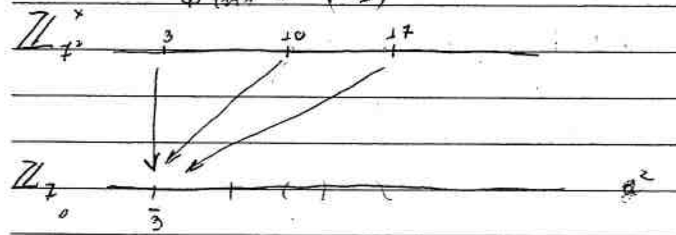
$h_0 = \min\{m \geq 1 : a^{m} = \bar{1}\}$

é chamado de a ordem de $\bar{a}$ em $\mathbb{Z}_n^{\times}$

$h_0 = ord_n(a)$

Como encontrar um gerador el $\mathbb{Z}_{7^2}^{\times}$?

$\phi(a) \neq (p-1)$



3 serve? $\Longleftrightarrow h_0 = ord_{49}(3) = \phi(49) = 42$

Em $\mathbb{Z}_n^{\times}$

$\bar{a}$ é gerador $\Longleftrightarrow ord_n(a) = \phi(n)$

Possibilidades para a ordem de $\bar{3}$ em $\mathbb{Z}49$

divisores de $\phi(49)$

" de 42

$\{\bar{1}, \bar{2}, \bar{3}, \bar{6}, \bar{7}, \overline{14}, \overline{21}, \overline{42}\}$

$\bar{3}$ também gera $\mathbb{Z}_7^{\times}$

$\Downarrow$

$\bar{3}^{h_0} = \bar{1} \mod 7$

Como $ord_7(3) = 6 \Rightarrow 6 \mid h_0$

Por contas $\bar{3}^{6} \equiv \bar{1} \mod 49$

<u>Teorema</u> Seja p um primo. Suponhamos que $\mathbb{Z}_p^{\times}$ seja cíclico gerado por $\bar{g}$. Então existe g_1 t.q. $g_1 \equiv g \mod p$ e $\mathbb{Z}_{p^2}^{\times}$ é cíclico gerado por $\bar{g}_1$

$\bar{g}$ serve? $\iff \mathrm{ord}_{p^2}(g) = \phi(p^2)$

Sei: (1) $\mathrm{ord}_{p^2}(g) \mid \phi(p^2) \Rightarrow \mathrm{ord}_{p^2}(g) \mid \phi(p-1)$

Sei: (2) $(p-1) \mid \mathrm{ord}_{p^2}(g)$

Possibilidade p/ $\mathrm{ordem}_{p^2}(g)$

- $p(p-1)$
- $(p-1)$

a^1, a^2, a^7

$a = 1, 2, 3, 4, \bmod p$

2

Se $\mathrm{ord}_{p^2}(g) = \phi(p^2)$ acabou!

Senão, $\mathrm{ord}_{p^2}(g) = (p-1)$

g_1 serve? $\mathrm{ord}_{p^2}(g_1) = \begin{cases} p(p-1) \\ (p-1) \end{cases}$

$$g_1^{p-1} = (g+p)^{p-1} = g^{p-1} + \binom{p-1}{1} g^{p-2} \cdot p + \dots + p^{p-1}$$

$$g_1^{p-1} = g^{p-1} + (p-1) \cdot p \cdot g^{p-2} + \dots + p^{p-1}$$

$$g_1^{p-1} = 1 + \underbrace{(p-1) \cdot p \cdot g^{p-2}}_{p^2 \nmid (p-1) \cdot p \cdot g^{p-2}} \bmod p^2$$

Portanto

Se $\mathrm{ord}_{p^2}(g) = p-1$

$$\mathrm{ord}_{p^2}(g+p) = p(p-1) = \phi(p^2)$$

Teorema Seja p um primo ímpar. Suponhamos que $\mathbb{Z}_p^{\times}$ seja cíclico gerado por $\bar{g}$. Então existe g_1 tal que $g_1 \equiv g \bmod p$ e $\bar{g}_1$ é gerador de $\mathbb{Z}_{p^3}^{\times}$

1º passo $\bar{g}$ serve? $\Rightarrow \mathrm{ord}_{p^3}(g) = \phi(p^3)$?

$\phi(p^3) = p^2(p-1)$

Sei: $\mathrm{ord}_{p^3}(g)$ divide $\phi(p^3)$

Sei: $(p-1)$ divide $\mathrm{ordem}_{p^3}(g)$ (Pois g gera $\mathbb{Z}_p^{\times}$)

Possibilidades

- $p^2(p-1)$
- $p(p-1)$
- $(p-1)$

Se $\mathrm{ord}_{p^3}(g) = p(p-1)$

Tomo $g_1 = g + p$

$$(g+p)^{p(p-1)} = g^{p(p-1)} + p(p-1)\, g^{p(p-1)-1} p + \binom{p(p-1)}{2} g^{p(p-1)-2} p^2 + \dots + p^{p(p-1)}$$

$$g_1^{p(p-1)} = g^{p(p-1)} + p^2(p-1)\, g^{p(p-1)-1} + \underline{\frac{p(p-1)(p(p-1)-1)}{2}} p^2 \cdot g^{p(p-1)-2}$$

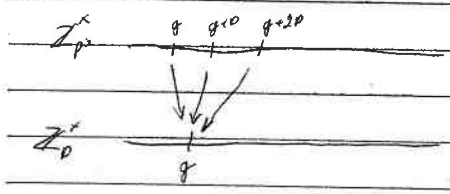
Se $\mathrm{ord}_{p^3}(g) = (p-1)$

Tomo $g_1 = g + p^2$

Teor. Seja p primo ímpar. Suponhamos que $\mathbb{Z}_p^\times$ seja cíclico com gerador g. Então existe g_1 t.q

(1) $g_1 \equiv g \mod p$ e $\mathbb{Z}_{p^3}^\times$ é cíclico gerado por g_1

Dem



Quero $g_1 = g + lp$ p/ algum l t.q

$ord_{p^3}(g_1) = \Phi(p^3) = p^2(p-1)$

$h_0 = \min\{m \geq 1 : g^m \equiv 1 \mod p^3\}$

$(ord_{p^3}(g_1))$

Sei: $h_0 \mid \Phi(p^3)$

Possibilidades

- $h_0 = \Phi(p^3) = p^2(p-1)$
- $h_0 = p(p-1)$
- $h_0 = (p-1)$

Se $h_0 = \Phi(p^3)$ então $\bar{g}$ gera $\mathbb{Z}_{p^3}^\times$

Se $h_0 = p(p-1) \rightsquigarrow \bar{g}$ não serve

Tome $g_1 = g + p$

$g_1^{p(p-1)} = (g+p)^{p(p-1)} = g^{p(p-1)} + p(p-1)g^{p(p-1)-1}p + p^3(p-1)(p(p-1)-1)g^{p(p-1)-2}$

Se $h_0 = p-1$,

$g_1 = g + p^2$

$g_1^{p(p-1)} = (g+p^2)^{p(p-1)} + p(p-1)g_1^{p(p-1)} p^2 +$

$g_1 = g + l.p$

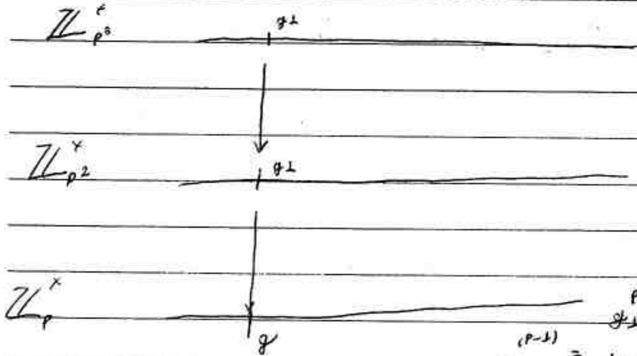
$g_1^{p(p-1)} = (g+pl)^{p(p-1)} = g^{p(p-1)} + p^2(p-1)l g^{p(p-1)-1} + A p^3$

Basta que $p \nmid l$

$g_1 = g + p$ serve

Teor: se g_1 é gerador de $\mathbb{Z}_{p^e}^\times$, g_1 é gerador de $\mathbb{Z}_{p^2}^\times$ $\forall e \geq 2$

(*) $e = 3$ seja g_1 um gerador de $\mathbb{Z}_{p^2}$



$g_1^{p(p-1)} \not\equiv 1 \mod p^2$ (pois é gerador)

$g_1^{p-1} \equiv 1 \mod p$ (P.T.F)

$g_1^{(p-1)} = 1 + b.p$ $\quad p \nmid b$

Teor $ord_{p^3}(g_1) = \Phi(p^3) = p^2(p-1) \Longleftrightarrow g_1^{p(p-1)} \not\equiv 1 \mod p^3$

$g_1^{p(p-1)} = (1+bp)^p = 1 + p.bp + \underbrace{\frac{p(p-1)}{2}.b^2p^2}_{\equiv 0 \mod p^3} + A.p^3$

$g_1^{p(p-1)} \equiv 1 + \underbrace{bp^2}_{\not\equiv 0} \mod p^3$

$g_1^{p(p-1)} \not\equiv 1 \mod p^3$

$e=4$ Tese: $ord_{p^4}(g_1) = \phi(p^4) = p^3(p-1) \iff g_1^{p^2(p-1)} \not\equiv 1 \mod p^4$

$\mathbb{Z}_{p^4}^\times$

$\mathbb{Z}_{p^3}^\times$ $g_1^{p(p-1)} \not\equiv 1 \mod p^3$ (pois g_1 é gerador)

$\mathbb{Z}_{p^2}^\times$ $g_1^{p(p-1)} \equiv 1 \mod p^2$ (Teor Euler)

$\mathbb{Z}_p^\times$ $g_1^{p(p-1)} = 1 + bp^2$ $\quad p \nmid b$

$$g_1^{p^2(p-1)} = (1+bp^2)^p = 1 + p.bp^2 + \frac{p.(p-1)}{2}.b^2.p^4 + \dots$$

$$\equiv 1 + \underbrace{bp^3}_{\not\equiv 0} \mod p^4 \not\equiv 1 \mod p^4$$

H.I. g_1 gera $\mathbb{Z}^\times_{p^{n-1}}$ Tese $ord_{p^n}(g_1) = \phi(p^n) = p^{n-1}(p-1)$

$\iff g_1^{p^{n-2}(p-1)} \not\equiv 1 \mod p^n$

$\mathbb{Z}^\times_{p^n}$ $\mid^{g_1}$

$\mathbb{Z}^\times_{p^{n-1}}$ $\mid^{g_1}$ $g_1^{p^{n-3}(p-1)} \not\equiv 1 \mod p^{n-1}$ (pe H.I, g_1 gera $\mathbb{Z}^\times_{p^{n-1}}$)

$\mathbb{Z}^\times_{p^{n-2}}$ $\mid^{g_1}$ $g_1^{p^{n-3}(p-1)} \equiv 1 \mod p^{n-2}$ (Teor Euler)

$g_1^{p^{n-3}(p-1)} = 1 + b.p^{n-2}$ e $p \nmid b$

$$g_1^{p^{n-2}(p-1)} = (1+b\,p^{n-2})^p = 1 + p.b.p^{n-2} + \frac{p(p-1)}{2}.b^2.p^{2n-4} + \dots$$

$$\equiv 1 + \underbrace{p^{n-1}}_{\not\equiv 0}.b \mod p^n \not\equiv 1 \mod p^n$$

<u>Questão</u> Será, que se p é primo $\mathbb{Z}_p^\times$ é cíclico

Teor [Lagrange] Seja p primo e $f(x) \in \mathbb{Z}[x]$

$f(x) = a_n x^n + \dots + a_1 x + a_0$ $\quad p \nmid a_n$

Então o número de classes de soluções de

$f(x) \equiv 0 \mod p$

é no máximo n

<u>OBS</u> $f(x) = x^2 - 1$ em $\mathbb{Z}_8$

$\bar{1}, \bar{7}, \bar{3}, \bar{5}$

<u>Dem</u> Indução no grau n

• $n=1$ $\quad f(x) = a_1 x + a_0$ $\quad p \nmid a_0$

$f(x) \equiv 0 \mod p \iff a_1 x \equiv -a_0 \mod p$

$p \nmid a_1 \rightsquigarrow a_1$ tem inversa $\exists!\, x$ dessa equação.

H.I suponhamos verdadeiro de grau $n-1$ p/ todo polinômio

Seja $f(x)$ de grau n. Por absurdo,

suponhamos $\bar{c}_0, \bar{c}_1, \dots, \bar{c}_n$ sejam $n+1$ classes distintas de ~~equação~~ soluções de

$f(x) \equiv 0 \mod p$

$f(x) - f(c_0) = a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \dots + a_1(x - c_0)$

$x^k - c^k = (x - c_0)(x^{k-1} + x^{k-2}c_0 + \dots + x\,c_0^{k-2} + c_0^{k-1})$

$f(x) - f(c_0) = (x - c_0)\, g(x)$ $\quad$ grau $g = n-1$

coef dominante de g é a_n

Substituindo x por c_j $\quad 1 \leq j \leq n$

$f(c_j) - f(c_0) = (c_j - c_0).\, g(c_j)$

$0 \equiv (c_j - c_0).\, g(c_j) \mod p$

$c_j \not\equiv c_0 \mod p \to g(c_j) \equiv 0 \mod p$

Teo Seja p primo ímpar e $d | (p-1)$
Então a equação
$$x^d \equiv 1 \mod p$$
possui exatamente d soluções distintas em $\mathbb{Z}_p$

Obs: Se $d = p-1$ $x^{p-1} \equiv 1 \mod p$ tem $p-1$ soluções pelo P.T.F
Se $d = 2$ $x^2 \equiv 1 \mod p$ só tem 2 soluções

Dem $d | (p-1)$ $p-1 = dk$
$x^{p-1} - 1 \equiv 0 \mod p$ tem $p-1$ soluções
$$x^{p-1} - 1 = x^{dk} - 1 = (x^d)^k - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1)$$
$$(x^d - 1)(x^{d(k-1)} + \dots + x^d + 1) \equiv 0 \mod p$$
se anula em $p-1$ classes
tem no máximo $d(k-1)$ raízes
no mínimo $\underbrace{p-1-(dk-d)}_{d}$ anulam $x^d - 1$

Por Lagrange $x^d - 1 \equiv 0 \mod p$ tem exatamente d raízes.

Teor Seja p um primo ímpar. E seja $d | p-1$
Então a equação $x^d \equiv 1 \mod p$
possui exatamente $\phi(d)$ classes de soluções de ordem d.

(Dentre das d soluções existem $\phi(d)$ tais que $x_0^d \equiv 1 \mod p$ e $ord_p(x_0) = d$

Corolário [Gauss] Seja p um primo ímpar, então a equação $x^{p-1} \equiv 1 \mod p$ possui ~~[illegible]~~ $\phi(p-1)$ soluções cuja ordem é $p-1$. Consequentemente $\mathbb{Z}_p^\times$ é cíclico

Corolário. Se p um primo ímpar e $e \geq 1$. Então $\mathbb{Z}_{p^e}^\times$ é cíclico e, se $e \geq 2$, um gerador de $\mathbb{Z}_{p^2}^\times$ gera $\mathbb{Z}_{p^e}^\times$

$$\mathbb{Z}_n^\times \xrightarrow{\sim} \mathbb{Z}_{p_1^{e_1}}^\times \times \dots \times \mathbb{Z}_{p_k^{e_k}}^\times$$

$$x^{n-1} \equiv 1 \mod n$$

Questão: quantas soluções tem a equação
$$x^q \equiv 1 \mod p^e$$

Teor: Seja p primo ímpar, $e \geq 1$ e $q \geq 1$. Então $x^q \equiv 1 \mod p^e$ possui exatamente $(q, \phi(p^e))$ soluções.

Dem p primo ímpar $\rightsquigarrow \mathbb{Z}_{p^e}^\times$ é cíclico gerado por um certo g.

$$\mathbb{Z}_{p^e}^\times \{ \bar{1}, \bar{g}, \bar{g}^2, \dots, \bar{g}^{\phi(p^e)-1} \}$$

$$\bar{x}^q \equiv 1 \mod p^e \longleftrightarrow (\bar{g}^\gamma)^q = \bar{1} \longleftrightarrow \bar{g}^{q\gamma} = \bar{1}$$
$$q \cdot \gamma \equiv 0 \mod \phi(p^e)$$

tilibra

/ /

Corol Seja $n = p_1^{a_1} \cdots p_k^{e_k}$ ímpar. Então o nº de soluções da eq.

$$x^q \equiv 1 \mod n$$

é $\prod_{i=1}^{k} (q, \phi(p_i^{e_i}))$

Corol Se $n = p_1^{a_1} \cdots p_k^{e_k}$ é ímpar, o nº de soluções da equação

$$x^{n-1} \equiv 1 \mod n$$

é $\prod_{j=1}^{k} (n-1, \phi(p_j^{e_j})) = \prod_{j=1}^{k} (n-1, p_j - 1)$

Ex $n = 3^3 \cdot 5^2 \cdot 7^3 = 231.525$

Encontre todas as soluções da equação

$$x^{231\,524} \equiv 1 \mod 231\,525$$

$(231\,524, 2)(231\,524, 4)(231\,524, 6) = 16$
$\quad \overset{\shortparallel}{2} \qquad \overset{\shortparallel}{4} \qquad \overset{\shortparallel}{2}$

$\mathbb{Z}_n \longrightarrow \mathbb{Z}_{3^3} \times \mathbb{Z}_{5^2} \times \mathbb{Z}_{7^3}$

$<2>$

/ /

$x^{231\,524} \equiv 1 \mod 3^3 \cdot 5^2 \cdot 7^3$

$x^{231\,524} \equiv 1 \mod 3^3$
$x^{231\,524} \equiv 1 \mod 5^2 \qquad t_0 \mid \phi(n)$
$x^{231\,524} \equiv 1 \mod 7^3$

$\phi(5) = 4 \qquad \phi(7) = 6 \qquad \phi(3) = 2$
$g(5) = 2 \qquad g(7) = 3 \qquad g(3) = 2$
$\downarrow \qquad \downarrow$
$g(5^2) = 2 \qquad g(7^2) = 3$
2 4 8 16, 3 9 27 32 42 43 31

$g(3^2) = 3$
2 4

$(2^{\gamma})^{231\,524} \equiv 1 \mod 3^3$
$(2^{\gamma})^{231\,524} \equiv 1 \mod 5^2$
$(2^{\gamma})^{231\,524} \equiv 1 \mod 7^3$
$(18)\ 231\,524 \cdot \gamma \equiv 0 \mod \phi(3^3)(=18) \div 2$
$(20)\ 231\,524 \cdot \gamma \equiv 0 \mod \phi(5^2)(=20) \div 2$
$(294)\ 231\,524\ \gamma \equiv 0 \mod \phi(7^3)(=294) \div 2$
$115\,762\ \gamma \equiv 0 \mod 9$
$115\,762\ \gamma \equiv 0 \mod 10 \div 2$
$115\,762\ \gamma \equiv 0 \mod 147 (= 7^2 \cdot 3)$
$9 \mid \gamma \qquad S = \{9, 18\}$
$57\,881 \cdot \gamma \equiv 0 \mod 5 \to 5 \mid \gamma \qquad S = (5, 10, 15, 20)$
$115\,762 - 4 = 11\,572 \to 1\,157 - 4 = 1\,153 \to 115 - 6 = 109 \ldots$
$147 \mid \gamma \qquad S = \{147, 294\}$

tilibra

Encontre todas as soluções
$x^{242} \equiv 1 \mod 5^4 \cdot 7^3$

$q = 242 = 11^2 \cdot 2$

$x^{242} \equiv 1 \mod n \Leftrightarrow \begin{cases} x^{242} \equiv 1 \mod 5^4 \\ x^{242} \equiv 1 \mod 7^3 \end{cases}$

$\mathbb{Z}_n^\times \xrightarrow[\cong]{\varphi} \mathbb{Z}_{5^4}^\times \times \mathbb{Z}_{7^3}^\times$

$\bar{x} \longmapsto (\bar{x}, \bar{x})$

$S_n(242) \xrightarrow[\cong]{\varphi} S_{5^4}(242) \times S_{7^3}(242)$

nº de soluções de $x^{242} \equiv 1 \mod 5^4 7^3 = \left(\begin{matrix} \text{nº de sol} \\ x^{242} \equiv 1 \mod 5^4 \end{matrix}\right) \times \left(\begin{matrix} \text{nº de sol} \\ x^{242} \equiv 1 \mod 7^3 \end{matrix}\right)$

$(q, \phi(5^4))$ $\quad (q, \phi(7^3))$

$(2 \cdot 11^2, 5^3 \cdot 4) = 2$ $\quad (2 \cdot 11^2, 7^2 \cdot 6) = 2$

nº de soluções = 4

Resolução em $\mathbb{Z}_{5^4}^\times$
$x^{242} \equiv 1 \mod 5^4$

• gerador do $\mathbb{Z}_5^\times$

$ord_5(2) = 4$ $\quad$ 2 gera $\mathbb{Z}_5$

• Gerador de $\mathbb{Z}_{5^2}^\times$. 2 serve?

$ord_{5^2}(2) \begin{cases} 5 \cdot 4 = \phi(5^2) \\ 4 \end{cases}$

Basta verificar se $2^4 \equiv 1 \mod 25$
$2^4 \equiv 16 \not\equiv 1 \mod 5^2$

$ord_{5^2}(2) = \phi(5^2)$

2 é gerador de $\mathbb{Z}_{5^2}^\times$

2 é gerador de $\mathbb{Z}_{5^4}^\times$

$x_0^{242} \equiv 1 \mod 5^4$ $\quad x_0 = 2^{\gamma}$

$(2^{\gamma})^{242} \equiv 1 \mod 5^4$

$\Updownarrow$

$\phi(5^4)$ divide $\gamma \cdot 2 \cdot 11^2$

$\gamma \cdot 2 \cdot 11^2 \equiv 0 \mod 5^3 \cdot 4$

$\Updownarrow$

$11^2 \cdot \gamma \equiv 0 \mod 5^3 \cdot 2$

$\Updownarrow$

$\gamma = 5^3 \cdot 2 \cdot k$

$\gamma = 5^3 \cdot 2$ $\quad \gamma = 4 \cdot 5^3$

$x_0 = 2^{4 \cdot 5^3} = \bar{1}$ $\quad x_0 = 2^{2 \cdot 5^3} = -\bar{1}$

$S_{5^4}(242) = \{\bar{1}, -\bar{1}\}$

$\mathbb{Z}_{7^3}^\times$, $x^{242} \equiv 1 \mod 7^3$

• Gerador de $\mathbb{Z}_7^\times = 3$ (Sabemos que 3 é gerador)

• $\mathbb{Z}_{7^2}^\times$, 3 é gerador

$ord_{7^2}(3) = \begin{cases} \phi(7^2) \\ 6 \end{cases}$ $\quad 3^6 \equiv ? \mod 7^2$

$3^{4+2} = (3^2)^2 \cdot 3^2 = 32 \cdot 9 \equiv -6$

$3^4 \equiv 81 \mod 7^2$ $\quad 3^4 = 32$ $\quad$ 3 gera $\mathbb{Z}_{7^2}^\times$

3 gera $\mathbb{Z}_{7^3}^\times$

$x_0^{242} \equiv 1 \mod 7^3$ $\quad x_0 = 3^{\gamma}$

$(3^{\gamma})^{242} \equiv 1 \mod 7^3 \Rightarrow 7^2 \cdot 6 \mid \gamma \cdot 2 \cdot 11^2$

$2 \cdot 11^2 \cdot \gamma \equiv 0 \mod 7^2 \cdot 6$

$11^2 \cdot \gamma \equiv 0 \mod 7^2 \cdot 3$ $\quad S_{7^3}^\times \{\bar{1}, -\bar{1}\}$

$\gamma = 7^2 \cdot 3$ $\quad \gamma = 7^2 \cdot 6$

$x_0 = 3^{3 \cdot 7^2} = \bar{1}$ $\quad x_0 = 3^{7^2 \cdot 3} = -\bar{1}$

$S_{5^4}(242) \times S_{7^3}(242) = \{(\bar{1},\bar{1}),(\bar{1},-\bar{1}),(-\bar{1},\bar{1}),(-\bar{1},-\bar{1})\}$

$x_1 \equiv 1 \mod 5^4$ $\quad x_1 = \bar{1}$

$x_1 \equiv 1 \mod 7^3$

$x_2 \equiv 1 \mod 5^4$

$x_2 \equiv -1 \mod 7^3$

$x_3 \equiv -1 \mod 5^4$, $5^4 a \equiv 2 \mod 7^3$

$x_3 \equiv 1 \mod 7^3$

$x_4 \equiv -1 \mod 5^4$ $\quad x_4 = -\bar{1}$

$x_4 \equiv -1 \mod 7^3$

$x_2 = 1 + 5^4 a$

$1 + 5^4 \cdot a \equiv -1 \mod 7^3$

$5^4 \cdot a \equiv -2 \mod 7^3$

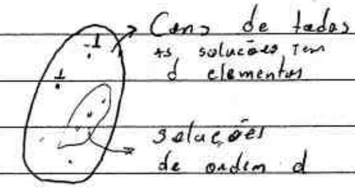
Preciso inverter 5^4

Thq

Teorema Se p é um primo ímpar e $d \mid (p-1)$. Então existem exatamente $\phi(d)$ classes de soluções da equação

$$x^d \equiv 1 \mod p$$

de ordem d



$\sum_{j \mid d} \phi(j) = d$

Dem Suponhamos, por absurdo, o teorema falso.
Seja d_0 o primeiro divisor de $p-1$ p/ o qual o teorema falha

$2, \dots, d, \dots, d_0$

não falha $\qquad$ primeiro problemático

Para todo divisor divisor $1 \leq d < d_0$ o teorema vale e para d_0 o número de soluções de ordem d_0 Não é $\phi(d_0)$

$x^{d_0} \equiv 1 \mod$

O nº de soluções de $x^{d_0} \equiv 1 \mod p$ de ordem exatamente d_0 é

$$d_0 - \sum_{\substack{j \mid d_0 \\ j < d_0}} \phi(j) = d_0 - \Big(\sum_{j \mid d_0} \phi(j) - \phi(d_0)\Big)$$

Álgebra - 16/06 (2ª)

· geradores p/ $\mathbb{Z}^\times_{5^2}$. $\bar{2}$ serve? $\text{ord}_{5^2}(\bar{2}) \begin{cases} 5 \times 4 = \phi(5^2) \\ \text{ou} \\ 4 \quad (p-1) \end{cases}$

Basta que $\bar{2}^4$ seja $\equiv 1$ ou não
mas $\bar{2}^4 = 16 \not\equiv 1 \mod 5^2$

$\Downarrow$

2 é gerador de $\mathbb{Z}^\times_{5^2}$

$\Downarrow$ (graças ao teorema)

2 é gerador de $\mathbb{Z}^\times_{5^4}$

$\left.\begin{array}{l} x_0^{242} \equiv 1 \mod 5^4 \\ x_0 = 2^\gamma \end{array}\right\} 2^{\gamma \cdot 2 \cdot 11^2} \equiv 1 \mod 5^4$

$\phi(5^4)$ divide $\gamma 2 . 11^2$

$\gamma 2 . 11^2 \equiv 0 \mod (5^3 . 4) \Leftrightarrow 11^2 \gamma \equiv 0 \mod (5^3 . 2)$

$\Leftrightarrow 2 . 5^3 \mid \gamma \rightarrow \gamma = \begin{cases} 2 . 5^3 \\ 4 . 5^3 \end{cases}$

$x_0 = 2^{4.5^3} = \bar{1}$ (pois 4.5^3 é $\phi(5^4)$)

$x_0 = 2^{2.5^3} = -\bar{1}$ (pois ele ao quadrado é $\bar{1}$ e não pode ser $\bar{1}$ pois 2 é gerador)

$S_{5^4}(242) = \{\bar{1}, -\bar{1}\}$.

Agora em $\mathbb{Z}^\times_{7^3}$, $x^{242} \equiv 1 \mod 7^3$.

· gerador de $\mathbb{Z}^\times_7$. sabemos que $\bar{3}$ é gerador

· geradores de $\mathbb{Z}^\times_{7^2}$. $\text{ord}_{7^2}(3) \begin{cases} 7 . 6 \\ 6 \end{cases}$ $\quad \bar{3}^6 \equiv ? \mod 7^2$

$3^6 = 3^{4+2} = 3^2 . 3^2 \equiv 32 . 9 \equiv \ldots$

3	3	$\mod 7^2$
3^2	9	7^2
3^{2^2}	$81 = 32$	7^2
3^{2^3}		

$\Downarrow$

$\bar{3}$ gera $\mathbb{Z}^\times_{7^2}$

$\Downarrow$

$\bar{3}$ gera $\mathbb{Z}^\times_{7^3}$

$x_0^{242} \equiv 1 \mod 7^3 \rightsquigarrow x_0 = 3^\gamma$ e $3^{\gamma 2 . 11^2} \equiv 1 \mod 7^3$

$\rightarrow 2 . 11^2 . \gamma \equiv 0 \mod (7^2 . 6)$

$11^2 \gamma \equiv 0 \mod (7^2 . 3) \rightarrow 3 . 7^2 \mid \gamma$

$\rightarrow \gamma = \begin{cases} 3 . 7^2 \\ 6 . 7^2 \end{cases}$ $\quad \bar{3}^{6.7^2} \equiv \bar{1}$ (teo Euler).
$\bar{3}^{3.7^2} = -\bar{1}$

$S_{7^3}(242) = \{\bar{1}, -\bar{1}\}$.

$S_{5^4}(242) \times S_{7^3}(242) = \{(\bar{1}, \bar{1}), (\bar{1}, -\bar{1}), (-\bar{1}, \bar{1}), (-\bar{1}, -\bar{1})\}$

$x_1 \equiv 1 \mod 5^4$ $x_1 \equiv 1 \mod 7^3$	$x_2 \equiv 1 \mod 5^4$ $x_2 \equiv -1 \mod 7^3$	$x_3 \equiv -1 \mod 5^4$ $x_3 \equiv 1 \mod 7^3$	$x_4 \equiv -1 \mod 5^4$ $x_4 \equiv -1 \mod 7^3$

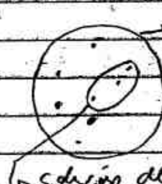
$x_1 \equiv 1$	$x_2 = 1 + 5^4 k$
	$1 + 5^4 k \equiv -1 \mod 7^3$
	$5^4 k \equiv -2 \mod 7^3$
	// Preciso inverter 5^4
	// $(5^4, 7^3) = 1$
	// {Bézout
	// $a 5^4 + b 7^3 = 1$ (reduzindo
	// módulo 7^3, sobra $a 5^4$, onde
	// $\bar{a}$ é a inversa de 5^4
			$x_4 \equiv -1$

[Teorema]

Seja p um primo ímpar e $d \mid (p-1)$. Então existem exatamente $\phi(d)$ classes de soluções da equação

$x^d \equiv 1 \mod p$

de ordem d



// Questão:
$\sum_{g \mid d} \phi(g) = ?$

Álgebra + 14/06 (4)

___/___/___

Corolário [Gauss]

Seja p um primo ímpar então a equação $x^{p-1} \equiv 1 \mod p$ possui $\phi(p-1)$ soluções cuja ordem é $p-1$. Consequentemente, $\mathbb{Z}_p^*$ é cíclico.

Corolário: Seja p primo ímpar e $e \geq 1$. Então $\mathbb{Z}_{p^e}^*$ é cíclico e, se $e \geq 2$, um gerador de $\mathbb{Z}_{p^2}^*$ gera $\mathbb{Z}_{p^e}^*$.

Questão: Quantas soluções tem a eq.

$$x^q \equiv 1 \mod p^e ?$$

[Teorema]

Seja p primo ímpar, $e \geq 1$ e $q \geq 1$. Então $x^q \equiv 1 \mod p^e$ possui exatamente $(q, \phi(p^e))$ soluções $(q, \phi(p^e)) = \text{mdc}$.

Dem.:

p primo ímpar $\Rightarrow \mathbb{Z}_{p^e}^*$ é cíclico gerado por g.

$\mathbb{Z}_{p^e}^* = \{\bar{1}, \bar{g}, \bar{g}^2, \ldots, \bar{g}^{\phi(p^e)-1}\}$.

$\bar{x}_0^q = \bar{1} \Leftrightarrow (\bar{g}^\gamma)^q = \bar{1} \Leftrightarrow \bar{g}^{q\gamma} = \bar{1}$

$\Leftrightarrow q\gamma \equiv 0 \mod \phi(p^e)$

Corolário: Seja $n = p_1^{e_1} \cdots p_k^{e_k}$ ímpar. Então o nº de soluções da equação

$$x^q \equiv 1 \mod n \quad \text{é} \quad \prod_{j=1}^{k} (q, \phi(p_j^{e_j}))$$

Corolário: Se $n = p_1^{e_1} \cdots p_k^{e_k}$ é ímpar o nº de sol. da eq.

$$x^{n-1} \equiv 1 \mod n \quad \text{é} \quad \prod_{j=1}^{k} (n-1, \phi(p_j^{e_j})) = \prod_{j=1}^{k} (n-1, p_j - 1)$$

// pois $\left((p_1^{e_1} \cdots p_k^{e_k}) - 1,\ p_j^{e_j - 1}(p_j - 1)\right)$

DATAPEL

___/___/___

Exercício: $n = 3^? \cdot 5^2 \cdot 7^3 = 231525$ Encontre todas as soluções de

$$x^{231524} \equiv 1 \mod 231525.$$

16/06/11

Exemplo: Encontre todas as soluções da eq.

$$x^{242} \equiv 1 \mod (5^4 \cdot 7^3)$$

$q = 242 = 2 \cdot 11^2$

$$x^{242} \equiv 1 \mod n \Leftrightarrow \begin{cases} x^{242} \equiv 1 \mod 5^4 \\ x^{242} \equiv 1 \mod 7^3 \end{cases}$$

$$\mathbb{Z}_n^* \xrightarrow[\simeq]{\phi} \mathbb{Z}_{5^4}^* \times \mathbb{Z}_{7^3}^*$$

$$\bar{x} \longmapsto (\bar{x}, \bar{x})$$

$$S_n(242) \xrightarrow[\simeq]{\phi} S_{5^4}(242) \times S_{7^3}(242)$$

$$\begin{pmatrix} \text{Nº de elementos de sols de} \\ x^{242} \equiv 1 \mod n \end{pmatrix} = \underbrace{\begin{pmatrix} \text{Nº sols} \\ x^{242} \equiv 1 \mod 5^4 \end{pmatrix}}_{(q,\, \phi(5^4))} \times \underbrace{\begin{pmatrix} \text{Nº sols} \\ x^{242} \equiv 1 \mod (7^3) \end{pmatrix}}_{(q,\, \phi(7^3))}$$

$(2 \times 11^2, 5^3(4)) = 2$

$(2 \cdot 11^2, 7^2(6)) = 2$

Resoluções em $\mathbb{Z}_{5^4}^*$

$x^{242} \equiv 1 \mod 5^4$ // as sols. são -1 e 1. E se não soubesse?

- achar gerador de $\mathbb{Z}_5^*$

Tentar o $\bar{2}$. $\bar{2}$, $\bar{2}^2 = \bar{4} = (\overline{-1})$, $2^3 = \overline{-2}$, $\bar{2}^4 = -\bar{4} = \bar{1}$

$\text{ord}_5(2) = 4 \leadsto \bar{2}$ gera $\mathbb{Z}_5^*$

DATAPEL

Se mostrarmos que $\sum_{j|d_0} \phi(j) = d_0$

Temos,

$$d_0 - \left(\sum_{j|d_0} \phi(j) - \phi(d_0)\right) = d_0$$ e isso é um absurdo

Leminha $d_0 \geq 1$ então

$$\sum_{j|d_0} \phi(j) = d_0$$

$$\varphi(n) = \sum_{j|n} \phi(j) \qquad \varphi(nm) = m.n = \varphi(n).\varphi(m)$$

$$\varphi(p^e) = \sum_{j|p^e} \phi(j) = \phi(1) + \phi(p) + \phi(p^2) + \dots + \phi(p^e)$$

$$1 + p - 1 + p(p-1) + \dots + p^{e-1}(p-1) = p^e$$

- Se $(m,n) = 1 \Rightarrow \varphi(m.n) = \varphi(m).\varphi(n)$

$$\varphi(m)\,\varphi(n) = \left(\sum_{j_1|m} \phi(j_1)\right).\left(\sum_{j_2|n} \phi(j_2)\right)$$

$$= \sum_{j_1|m} \sum_{j_2|n} \phi(j_1).\phi(j_2)$$

$$= \sum_{j_1|m} \sum_{j_2|n} \phi(j_1.j_2) = \sum_{u|mn} \phi(u) = \varphi(m.n)$$

$(j_1, j_2) \in Div(m) \times Div(n) \xrightarrow{\sim} Divis(mn)$

$(j_1, j_2) \longrightarrow j_1 j_2$

Teo [Miller-Rabin] Se n é um nº composto ímpar, então n passa no teste de Miller no máximo para $(n-1)/4$ bases $1 \leq b \leq (n-1)$

$n - 1 = 2^s.t \qquad s \geq 1, \; t$ ímpar

- n passa no Miller na base b se (1) $b^t \equiv 1 \mod n$

(2) $b^{2^j t} \equiv -1 \mod n \; (0 \leq j \leq s-1)$

Se n passa no Miller na base b

Se (1) $\Rightarrow b^t \equiv 1 \mod n$

$(b^t)^{2^s} \equiv 1^{2^s} \equiv 1 \mod n$ i.e. $b^{n-1} \equiv 1 \mod n$

Se (2) $\Rightarrow b^{2^j t} \equiv -1 \mod n$

$(b^{2^j t})^{2^{s-j}} \equiv (-1)^{2^{s-j}} \equiv 1 \mod n$ i.e. $b^{n-1} \equiv 1 \mod n$

Se n é composto e passa no Miller na base b (i.e. n é pseudoprimo forte)

$\Downarrow$

n é pseudoprimo na base b

As bases b's para as quais n passa no teste de Miller são todas soluções da eq

$$x^{n-1} \equiv 1 \mod n$$

Já sei o número de soluções desta equação

$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$

#

$$\# Sols = \prod_{j=1}^{k} \left(n-1, \phi(p_j^{e_j})\right)$$

$$= \prod_{j=1}^{k} \left(n-1, p_j^{e_j - 1}.(p_j - 1)\right) = \prod_{j=1}^{k} (n-1, p_j - 1)$$

1º Caso $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, $e_k \geq 2$ p/ certo $1 \leq k \leq r$

Vou estimar o nº de soluções da eq

$$x^{n-1} \equiv 1 \mod n$$

$$\# Sols = \prod_{j=1}^{r} (n-1, p_j - 1) \leq \prod_{j=1}^{r} (p_j - 1) \leq \prod_{j=1}^{r} p_j (p_k - 1) \quad j \neq k$$

$$\frac{(p_k - 1)}{p_k^{e_k}} = \frac{p_k}{p_k^{e_k}} - \frac{1}{p_k^{e_k}} = \frac{1}{p_k^{e_k - 1}} - \frac{1}{p_k^{e_k}} = \frac{1}{p_k^{e_k-1}}\left(1 - \frac{1}{p_k}\right) \leq$$

$e_k \geq 2$, $p_j \geq 3 \ \forall j$

$$\leq \frac{1}{p_k}\left(1 - \frac{1}{p_k}\right) \leq \frac{1}{3}\left(1 - \frac{1}{3}\right) = \frac{2}{9}$$

$$\frac{1}{x}\left(1 - \frac{1}{x}\right) = \frac{1}{x} - \frac{1}{x^2} = f(x)$$

$$f'(x) = -\frac{1}{x^2} + \frac{2}{x^3} < 0 \iff \frac{2}{x^3} < \frac{1}{x^2} \iff 2 < x$$

$$(p_k - 1) \leq \frac{2}{9} p_k^{e_k}$$

$$\# Sols \leq \prod_{\substack{j=1 \\ j \neq k}}^{r} p_j \cdot \frac{2}{9} \cdot p_k^{e_k} \leq \prod_{\substack{j=1 \\ j \neq k}}^{r} p_j^{e_j} \cdot \frac{2}{9} p_k^{e_k} = \frac{2n}{9}$$

$$\frac{x-1}{4} \geq \frac{2x}{9} \qquad 9x - 9 \geq 8x \qquad x \geq 9$$

$n \geq 9$ $\quad \# Sols \leq \frac{n-1}{4}$

~~Mesmo~~

Obs: Se n é um número de Carmichael, então n é pseudo primo em todas as bases b $(b, n) = 1$

$\# Sols$ da eq $x^{n-1} \equiv 1$ mod n é $= \phi(n)$

$$\prod_{j=1}^{r} (n-1, p_j - 1) = \phi(n) = \phi(p_1^{e_1}) \dots \phi(p_r^{e_r}) = p_1^{e_1}(p_1 - 1) \dots p_r^{e_r - 1}(p_r - 1)$$

$e_j = 1 \ \forall j$. Todo nº de Carmichael é da forma do tipo $n = p_1 \cdot p_2 \dots p_r$ $\quad p_i \neq p_j$

2º Caso n é livre de quadrados

$n = p_1 \cdot p_2 \cdots p_r \qquad p_i \neq p_j \quad r \geq 2$

$n - 1 = 2^s t \qquad s \geq 1$, t ímpar

$p_j - 1 = 2^{s_j} \cdot t_j \qquad s_j \geq 1$, t_j ímpar

n passa no Miller na base b

$b^t \equiv 1 \mod n$ ou $b^{2^r t} \equiv -1 \mod n$ p/ certo $r_j \leq s - 1$

b é solução de $x^t \equiv 1 \mod n$

b é sol de $x^{2^r t} \equiv -1 \mod n$

$$x^t \equiv 1 \mod n \leftrightarrow x^t \equiv 1 \mod p_j \ \forall j$$

$$\# Sols = \prod_{j=1}^{r} (t, p_j - 1) = \prod_{j=1}^{r} (t, 2^{s_j} t_j) = \prod_{j=1}^{r} (t, t_j)$$

$$T_j = (t, t_j) \quad 1 \leq j \leq r$$

Teor O nº de soluções da equação $x^{2^j t} \equiv -1 \mod p_i$ é $2^j T_i$ se $j < S_i$ e é 0 se $j \geq S_i$

Dem $\mathbb{Z}_{p_i}^{*}$ é cíclico gerado por $\bar{g}$

Se $x_0^{2^j t} \equiv -1 \mod p_i \rightsquigarrow x_0 = \bar{g}^{\delta}$

$\bar{g}^{\delta \cdot 2^j t} = (\bar{-1}) = \bar{g}^{\left(\frac{p-1}{2}\right)}$

$\left[\bar{g}^{\left(\frac{p-1}{2}\right)}\right]^2 = \bar{g}^{p-1} \equiv \bar{1}$

$\bar{g}^{(p-1)/2} = \bar{1}$ ou $\bar{g}^{(p-1)/2} = -1$

como g é gerador $\text{ord}_p(g) = p_i - 1 \Rightarrow \bar{g}^{\left(\frac{p-1}{2}\right)} = -\bar{1}$

$\bar{g}^{2^j t \delta} = \bar{g}^{\left(\frac{p-1}{2}\right)}$

$\bar{g}^{2^j t \cdot \delta + \frac{p-1}{2}} = \bar{g}^{p-1} = \bar{1}$

$2^j t \cdot \delta + (p_i - 1)/2 = 0 \mod 2^{s_i} t_i$

$2^j t \cdot \delta + (2^{s_i - 1} \cdot t_i) \equiv 0 \mod 2^{s_i} t_i$

$2^j \cdot t\, \delta \equiv -(2^{s_i - 1} \cdot t_i) \mod 2^{s_i} t_i$

$AX \equiv B \mod m$
$(A, M) = d$ se $d \nmid B$ Não tem soluções
se $d \mid B$, tem d soluções

$(2^j t, 2^{s_i} t_i) = 2^{\min(j, s_i)} \cdot (t, t_i) = 2^{\min(j, s_i)} \cdot T_i$

Se $2^{\min(j, s_i)} T_i \nmid 2^{s_i - 1} t_i$ $\nexists$ sol

se $j \geq S_i$ $\nexists$ Sol

Se $j \leq S_i - 1$ $\exists$ o nº de soluções é $2^j \cdot T_i$

Resumo

$\#$ Sols de $x^t \equiv 1 \mod n = T_1 \cdot T_2 \cdot T_3 \ldots T_r$

$\#$ Sols de $x^{2^j t} \equiv -1 \mod p_i = \begin{cases} 2^j T_i & 0 \leq j \leq s_i - 1 \\ & j \geq S_i \end{cases}$

Coloquem

$x^{2^j t} \equiv -1 \mod n \longleftrightarrow x^{2^j t} \equiv -1 \mod p_i\ \forall i$

$\#\text{Sols} = \prod_{i=1}^{r} \#\text{Sol} \neq 0$
$\Downarrow$
só se $0 \leq j \leq \min\{s_i\} - 1$

Vou ordenar $S_1 \leq S_2 \leq S_3 \leq \ldots \leq S_r$

$\#\text{Sols} = (2^j T_1)(2^j T_2) \ldots (2^j T_r)$

$x^{2^j t} \equiv -1 \mod n$ desde que $0 \leq j \leq S_1 - 1$

Então se n passa no Miller numa base b, b está entre as

$T_1 \cdot T_2 \ldots T_r + \sum_{j=0}^{S_1 - 1} 2^{jr} T_1 \cdot T_2 \ldots T_r$

$T_1 \cdot T_2 \ldots T_r \times \left(1 + \sum_{j=0}^{S_1 - 1} 2^{jr}\right) = T_1 \ldots T_r \left(1 + \frac{2^{S_1 r} - 1}{2^r - 1}\right)$

Vou provar que $T_1 \cdot T_2 \ldots T_r \left(1 + \frac{2^{S_1 r} - 1}{2^r - 1}\right) \leq \frac{\phi(n)}{4} \leq \frac{n-1}{4}$

$$T_1 . T_2 \dots T_r \left(1 + \frac{2^{s_i r} - 1}{2^r - 1}\right) \overset{?}{\leq} \frac{(p_1-1)(p_2-1)\dots(p_r-1)}{4} = \frac{2^{s_1} t_1 . 2^{s_2} t_2 \dots 2^{s_r} t_r}{4}$$

$$T_1 . T_2 \dots T_r \left(1 + \frac{2^{s_i r} - 1}{2^r - 1}\right) \leq \frac{2^{s_1 + s_2 + \dots + s_r} . t_1 . t_2 \dots t_r}{4}$$

Como $T_i \leq t_i$, basta provar que

$$1 + \frac{2^{s_i r} - 1}{2^r - 1} < \frac{2^{s_1 + s_2 + \dots + s_r}}{4}$$

Vou provar que $\dfrac{\left(1 + \dfrac{2^{s_i r} - 1}{2^r - 1}\right)}{2^{s_1 + s_2 + s_r}}$

Como $2^{s_1 + s_2 + \dots + s_n} \geq 2^{r s_1}$

$$\frac{1}{2^{s_1 + s_2 + \dots + s_n}} \leq \frac{1}{2^{r s_1}}$$

$$\frac{\left(1 + \dfrac{2^{s_i r} - 1}{2^r - 1}\right)}{2^{s_1 + s_2 + \dots + s_n}} \leq \frac{\left(1 + \dfrac{2^{s_1 r} - 1}{2^r - 1}\right)}{2^{s_1 r}} = \frac{1}{2^{s_1 r}} + \frac{2^{s_1 r}}{(2^r - 1) 2^{s_1 r}} - \frac{1}{2^{s_1 r}(2^r - 1)}$$

$$< \frac{1}{2^r - 1} + \frac{2^r - 2}{2^{s_1 r}(2^r - 1)} \leq \frac{1}{2^r - 1} + \frac{1}{2^{s_1 r}} \leq \frac{1}{2^{(r-1)}} \leq \frac{1}{4}$$

$\hookrightarrow r \geq 3$

Teor $n =$ inteiro composto ímpar

Então n passa no teste de Miller no máximo $\frac{n-1}{4}$ bobes b's $1 \leq b \leq n-1$

passar no Miller na base b $\begin{cases} b^t \equiv 1 \mod n \\ \text{ou} \\ b^{2^j t} \equiv -1 \mod n \text{ para algum } j \quad 0 \leq j \leq s-1 \end{cases}$

$n - 1 = 2^s . t$; $s \geq 1$; t ímpar

Se n passa no Miller na base $b \Rightarrow b^{n-1} \equiv 1 \mod n$

caso 1:

$n = p_1^{e_1} \dots p_h^{e_h} \dots p_r^{e_r}$ $e_h \geq 2$

$$x^{n-1} \equiv 1 \mod n \Leftrightarrow x^{n-1} \equiv 1 \mod p_i^{e_i} \ \forall i$$

\# Sols de $x^{n-1} \equiv 1 \mod n = \prod_{j=1}^{r} (n-1, \phi(p_j^{e_j})) = \prod_{j=1}^{r} (n-1, p_j - 1)$

$\leq \frac{2n}{9}$ $\qquad n \geq 9 \Rightarrow \frac{2}{9} n \leq \frac{n-1}{4}$

caso 2:

$n = p_1^{e_1} \dots p_2^{e_2} \dots p_r^{e_r}$, $p_1 \neq p_2$ $r \geq 2$

n passa no Miller na base b $\to x^t \equiv 1 \mod n$

$\hookrightarrow x^{2^j t} \equiv -1 \mod n$ certo $0 \leq j \leq s-1$

Obs: Se $x_0^{t} \equiv 1 \ (n) \rightsquigarrow (x_0^{t})^{2^j} \equiv 1^{2^j} \equiv 1 \ (n)$

Se $x_0^{2^j t} \equiv -1 \ (n) \rightsquigarrow x_0^{t} \not\equiv -1 \ (n)$

$\rightsquigarrow x^t \equiv 1 \ (n) \Leftrightarrow x^t \equiv 1 \ (p_i) \ \forall i$

$\# Sols \ x^t \equiv 1 \ (n) = \prod_{j=1}^{r} (t, \phi(p_j)) = \prod_{j=1}^{r} (t, p_j - 1)$

$p_j - 1 = 2^{s_j} t_j \qquad s_j \geq 1 \qquad t_j$ ímpar

$\prod_{j=1}^{r} (t, 2^{s_j} t_j) = \prod_{j=1}^{r} (t, t_j) = \prod_{j=1}^{r} T_j$

$T_j \doteq (t, t_j)$

$x^{2^j t} \equiv -1 \mod n \Leftrightarrow x^{2^j t} \equiv -1 \ p_i \ \forall i$

$\# Sols \ x^{2^j t} \equiv -1 \ (p_i) = \begin{cases} 2^j T_i & se \ 0 \leq j \leq s_i - 1 \\ 0 & se \ j \geq s_i \end{cases}$

$\# \ x^{2^j t} \equiv -1 = \prod_{j=1}^{r}$ ~~...~~

$= \prod (2^j T_1)(2^j T_2) \dots (2^j T_r)$ se $0 \leq j \leq \min(s_1, \dots, s_r) - 1$

Posso supor: $S_1 \leq S_2 \leq S_r$

$\# Sols \ x^{2^j t} \equiv -1 \ (n) = T_1 T_2 \dots T_r 2^{rj}$

O número de bases b's nas quais n pode passar no Miller é no máximo,

$T_1 \cdot T_2 \dots T_r + \sum_{j=0}^{s_1-1} 2^{jr} (T_1 \cdot T_2 \dots T_r)$

$T_1 \cdot T_2 \dots T_r \left(1 + \sum_{j=0}^{s_1-1} 2^{jr}\right) = T_1 \dots T_r \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right)$

Tese $T_1 \dots T_r \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right) \leq \frac{(p_1 - 1)(p_2 - 2) \dots (p_r - 1)}{4} = \frac{2^{s_1} t_1 \cdot 2^{s_2} t_2 \dots 2^{s_r} t_r}{4} =$

$= 2^{s_1 + s_2 + \dots + s_r} \cdot t_1 \cdot t_2 \dots t_r$

Como $T_i = (t, t_i)$ então $T_i \mid t_i$ em particular, $T_i \leq t_i$

Basta provar que

$\left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right) \leq \frac{2^{s_1 + s_2 + \dots + s_r}}{4}$ ou seja

$\frac{\left(1 + \frac{2^{s_1 r} - 1}{2^r - 1}\right)}{2^{s_1 + s_2 + \dots + s_r}} \leq \frac{1}{4}$

$\frac{\left(1 + \frac{2^{s_1 r} - 1}{2^r - 1}\right)}{2^{s_1 + s_2 + \dots + s_r}} \leq \frac{\left(1 + \frac{2^{s_1 r} - 1}{2^r - 1}\right)}{2^{rs_1}} =$

$= \frac{1}{2^{rs_1}} + \frac{1}{\cancel{2^{s_1 r}}(2^r - 1)} - \frac{1}{2^{s_1 r}(2^r - 1)} = \frac{2^r - 2}{2^{rs_1}(2^r - 1)} + \frac{1}{2^r - 1}$

$= \frac{2^r - 2}{2^{s_1 r}(2^r - 1)} + \frac{1}{2^r - 1} \underset{s_1 \geq 1}{\leq} \frac{2^r - 2}{2^r (2^r - 1)} + \frac{1}{2^r - 1} \overset{?}{\leq} \frac{1}{2^{r-1}}$

é equivalente a provar que

$\frac{2^{r-1}}{2^r - 1} + \frac{2^{r-1}(2^r - 2)}{2^r (2^r - 1)} \overset{?}{\leq} 1$

$\frac{2^{r-1}}{2^r - 1} \left(1 + \frac{(2^r - 2)}{2^r}\right) \overset{?}{\leq} 1$

$$\frac{2^{r-1}}{2^r-1}\left(1+1-\frac{2}{2^{r-1}}\right) \overset{?}{\leq} 1$$

$$\frac{2^r}{2^r-1}-\frac{2}{2^r-1} = 1 \leq 1 \checkmark$$

Conclusão,

se $r \geq 3$ $\quad \frac{1}{2^{r-1}} \leq \frac{1}{4}$

Sub caso do caso $r=2$

$n = p_1 . p_2 \qquad p_1-1 = 2^{s_1} t_1 \qquad p_2-1 = 2^{s_2} t_2$

$n-1 = 2^{s} . t$

$s_1 \leq s_2$

Tese : $T_1 . T_2 \left(1+\frac{2^{s_1}-1}{3}\right) \leq \frac{t_1 . t_2 \, 2^{s_1+s_2}}{4}$

Basta provar

$$\frac{\left(1+\frac{2^{2s_1}-1}{3}\right)}{2^{s_1+s_2}} \leq \frac{1}{4}$$

$$\frac{\left(1+\frac{2^{2s_1}-1}{3}\right)}{2^{2s_1} . 2^{s_2-s_1}} = \frac{\frac{1}{2^{2s_1}}+\frac{1}{3}-\frac{1}{2^{2s_1}.3}}{2^{s_2-s_1}} = \frac{\frac{1}{3}+\frac{1}{2^{2s_1}}\left(1-\frac{1}{3}\right)}{2^{s_2-s_1}}$$

$s_2 - s_1 \geq 0 \qquad \frac{\frac{1}{3}+\frac{1}{2^{2s_1}} . \frac{2}{3}}{2^{s_2-s_1}} =$

sub sub caso , $s_2 - s_1 > 0$

$$\frac{\frac{1}{3}+\frac{1}{2^{2s_1}}\left(\frac{2}{3}\right)}{2^{s_2-s_1}} \leq \frac{\frac{1}{3}+\frac{1}{2^{2s_1}}\left(\frac{2}{3}\right)}{2} \checkmark$$

$$\leq \frac{\frac{1}{3}+\frac{1}{2^2}\left(\frac{2}{3}\right)}{2} = \frac{1}{6}+\frac{1}{12} = \frac{1}{4}$$

$s_1 \geq 1$

sub sub caso $\quad s_2 = s_1$

$n = p_1 . p_2 \qquad p_1 - 1 = 2^{s_1} t_1 \; , \; p_2 - 1 = 2^{s_1} t_2$

$p_1 \neq p_2$

tese : $\frac{T_1 . T_2 \left(1+\frac{2^{2s_1}-1}{3}\right)}{1} \leq \frac{2^{s_1 . 2} \, t_1 . t_2}{4}$

$T_1 \leq t_1$ basta que $1+\frac{2^{2s_1}-1}{3} \leq \frac{2^{2s_1}}{4}$ é

$$2^{2s_1}\left(\frac{1}{3}-\frac{1}{4}\right) \leq \frac{1}{3} - 1 \quad \text{Absurdo}$$

Rascunho Vou saber $T_1 = t_1$

$T_1 = (t, t_1) = t_1 \quad \leadsto \quad t_1 \mid t$

$(n-1, p-1) = (2^s t, 2^{s_1} t_1) = 2^{\min\{s, s_1\}} . t_1$

$2^s t = n-1 = p_1 p_2 - 1 = (2^{s_1} t_1 + 1)(2^{s_1} t_2 + 1) - 1$

$2^{st} = 2^{2s_1} t_1 t_2 + 2^{s_1} t_1 + 2^{s_1} t_2$

/ /

$2^s f = 2^{s_1}\underbrace{(2^{s_1} t_1 t_2 + t_1 + t_2)}_{par} \rightsquigarrow \boxed{s > s_1}$

$(n-1, p_1 - 1) = 2^{s_1} t_1 = p_1 - 1$

$(p_1 - 1) \mid (n-1) \rightsquigarrow n \equiv 1 \mod p_1 - 1$

$p_1 . p_2 \equiv 1 \mod p_1 - 1$

$p_2 \equiv 1 \mod p_1 - 1$

$p_2 = 1 + k(p_1 - 1)$ se $k = 1$ $p_1 = p_2$, absurdo

$\therefore k \geq 2 \rightsquigarrow p_2 > p_1$

min $p_2 = 2p_1 - 1$

Se $T_1 = t_1$

$p_2 > p_1$

se $p_2 < p_1 \Rightarrow T_1 \neq t_1 \rightsquigarrow T_1 \leq \frac{t_1}{3}$

Tese:

$T_1 . T_2 \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{t_1}{3} t_2 \left(\frac{2^{2s_1} - 1}{3} + 1\right) \leq \frac{\phi(n)}{4}$

$\frac{t_1}{3} . t_2 \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{t_1 . t_2\, 2^{2s_1}}{3\, \cancel{2}} = \frac{\phi(n)}{6} < \frac{\phi(n)}{4} \leq \frac{n-1}{4}$

$\frac{\left(1 + \frac{2^{2s_1} - 1}{3}\right)}{2^{2s_1}} = \frac{1}{2^{2s_1}} + \frac{1}{3} - \frac{1}{2^{2s_1} . 3} = \frac{1}{3} + \frac{1}{2^{s_1}}\left(\frac{2}{3}\right) \overset{s_1 \geq 1}{\leq} \frac{1}{3} + \frac{1}{6}$

$= \frac{1}{2}$