

101) No sistema RSA, suponha que um usuário tenha chave pública  $(53, 391)$ , ou seja, para enviar a uma mensagem  $m$  (inteiro positivo menor que  $\phi(391)$ ) a este usuário calcula-se  $c \equiv m^{53} \pmod{391}$  e enviar-se a mensagem criptografada  $c$ . Determine a chave privada desse usuário, ou seja, um expoente  $d$  tal que  $c^d \equiv m \pmod{391}$ .

Temos que  $391 = 17 \cdot 23$ , queremos  $d \neq \pm t.g.$

$$c^d \equiv m \equiv m^{53d} \pmod{391}.$$

Logo,  $53d \equiv 1 \pmod{\phi(391)}$ :

$$(17-1)(23-1) = 16 \cdot 22 = 352$$

Então, basta encontrar  $d \neq \pm t.g.$   $53d + 352k = 1$ . Como sabemos que esta igualdade tem solução, podemos aplicar o algoritmo de Euclides.

	6	1	1	1	3	1	
352	53	34	19	15	4	3	1
	34	19	15	4	3	1	

Portanto,  $b \in \mathbb{Z} \setminus \{-3\}$

$$= 4 - (15 - 3 \cdot 4)$$

$$= 4 \cdot 4 - 15$$

$$= 4 \cdot (19 - 15) - 15$$

$$= 4 \cdot 19 - 5 \cdot 15$$

$$= 4 \cdot 19 - 5 \cdot (34 - 19)$$

$$= 9 \cdot 19 - 5 \cdot 34$$

$$= 9 \cdot (53 - 34) - 5 \cdot 34$$

$$= 9 \cdot 53 - 14 \cdot 34$$

$$= 9 \cdot 53 - 14 \cdot (352 - 6 \cdot 53)$$

$$= 93 \cdot 53 - 14 \cdot 352$$

$$\begin{array}{r} 34 \\ \times 6 \\ \hline 84 \\ + 9 \\ \hline 83 \end{array}$$

Logo,  $d = 93 + 352k$ ,  $k \in \mathbb{Z}$  resolvem o problema

102 Determine todas as soluções inteiros do sistema

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

$$\Rightarrow \begin{cases} 9x \equiv 3 \pmod{4} \\ 4x \equiv 2 \pmod{3} \\ 8x \equiv 10 \pmod{7} \end{cases} \Rightarrow \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{7} \end{cases}$$

Pelo teorema chinês dos restos

$$\begin{cases} N = 4 \cdot 3 \cdot 7 = 84 \\ N_1 = 3 \cdot 7 = 21 \equiv 1 \equiv \bar{1} \pmod{4} \\ N_2 = 4 \cdot 7 = 28 \equiv 1 \equiv \bar{1} \pmod{3} \\ N_3 = 4 \cdot 3 = 12 \equiv 5 \equiv \bar{3} \pmod{7} \end{cases}$$

$$\begin{aligned} x &\equiv (21 \cdot 1 \cdot 3) + (28 \cdot 1 \cdot 2) + (12 \cdot 3 \cdot 3) \\ &\equiv 222 \\ &\equiv 59 \pmod{84}, \end{aligned}$$

103) Seja  $\Phi_{28}(x)$  o 28º polinomio ciclotomico. Calcule  $\Phi_{28}(2)$ .

Usando a fórmula, com p primo

$$\Phi_{p^k}(x) = \sum_{j=0}^{p-1} (-1)^j x^{2^{k-1}p^{k-1}j}$$

Onde,

$$\Phi_{28}(x) = \sum_{j=0}^6 (-1)^j x^{2^5 j}$$

$$= x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$$

~~Onde.~~  $\Phi_{28}(2) = 3247$

104) No algoritmo RSA, uma mensagem  $m$  é um inteiro tal que  $0 \leq m \leq 11 \cdot 47 = 517$  e a mensagem criptografada é  $c = m^{33} \pmod{517}$ . Qual o valor do expoente descriptografador  $d$ ? Em outras palavras, qual um possível valor de  $d$  tal que  $c^d \equiv m \pmod{517}$  para todo  $m$ ?

Queremos  $c^d \equiv m^{33d} \equiv m \pmod{517}$ , logo  
 $33d \equiv 1 \pmod{\phi(517)}$   
 $(11-1)(47-1) = 460$

Então, basta encontrar  $d$  t.q.  $33d + 460k = 1, k \in \mathbb{Z}$ .  
 Como sabemos que esta igualdade tem solução (pelo teo. de Bézout), basta aplicarmos o algoritmo de euclides.

	13	1	15	2
460	33	31	2	1
	31	2	0	0
K	1	0	1	-1
d	0	1	-13	14
				-223

Portanto,  $33 \cdot (-223) + 460 \cdot 16 = 1$ , logo

$$d = 460 \times (460 - 223)$$

$$= 460 \times 237, x \in \mathbb{Z}$$

Assim, escolhendo  $x=0$ , temos que um valor possível de  $d$  é  $237$ .

(105) Prove que  $n^2$  é divisor de  $(n+1)^{2n}-1$  para todo  $n$  positivo.

Pelo teorema binomial:

$$(n+1)^{2n}-1 = \left( \sum_{k=0}^{2n} \binom{2n}{k} n^k \right) - 1 = \sum_{k=1}^n \binom{2n}{k} n^k$$

Para qualquer  $n \geq 2$  vale que  $n^2 | (n+1)^{2n}-1$ . E para  $n=1$ ,  $n^2=1 | (1+1)^2-1=1$ . Logo é válido para qualquer  $n$  positivo.

107) Sejam  $m$  e  $n$  primos em comum, e seja  $P(x)$  um polinômio com coeficientes inteiros. Prove que se  $P(x)$  tem raízes em  $\mathbb{Z}_m$  e  $\mathbb{Z}_n$ , então também tem alguma raiz em  $\mathbb{Z}_{mn}$ .

E temos que  $P(r_m) \equiv 0 \pmod{m}$  e  $P(r_n) \equiv 0 \pmod{n}$  com  $r_m \in \{1, 2, \dots, m\}$  e  $r_n \in \{1, 2, \dots, n\}$ . Queremos mostrar que existe  $r_{mn}$  tal que  $P(r_{mn}) \equiv 0 \pmod{m \cdot n}$ . Pelo teorema Chines dos restos, existe uma única solução a módulo  $m \cdot n$  para o sistema

$$x \equiv r_m \equiv 0 \pmod{m}$$

$$x \equiv r_n \equiv 0 \pmod{n}$$

Pelo teorema Chines dos restos existe uma solução a módulo  $m \cdot n$  tal que  $x \equiv r_m, r_n \pmod{m \cdot n}$  (rende  $r_{mn}$  a solução). Agora vamos mostrar que  $r_{mn}$  é uma raiz de  $P(x)$  a módulo  $m \cdot n$ .

$$P(r_{mn}) \equiv P(r_m) \equiv 0 \pmod{m}$$

$$P(r_{mn}) \equiv P(r_n) \equiv 0 \pmod{n}$$

Pelo Teorema Chines dos restos  $P(r_{mn}) \equiv 0 \pmod{mn}$ . Então  $r_{mn}$  é raiz em  $\mathbb{Z}_{mn}$ .

108) Fatore  $x^4+x^2+1$  como produto de polinômios com coeficientes inteiros.

Note que,  $(x^4+x^2+1)(x-1)(x+1) = x^6-1$ , por outro lado

$$x^6-1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$$

$$= (x^4+x^2+1)(x-1)(x+1)$$

$$\text{Dai}, x^4+x^2+1 = \Phi_3(x)\Phi_6(x) = (x^2-x+1)(x^2+x+1)$$

III) Um inteiro positivo  $n$  é chamado "número de Carmichael" se  $a^n \equiv a \pmod{n}$ , para todo inteiro positivo  $a$ , mas  $a$  não é primo.

(a) Prove que se  $n$  é um produto de números primos distintos e  $p-1$  divide  $n-1$  para todo fator primo  $p$  de  $n$ , então  $n$  é um número de Carmichael.

(b) Prove que, se  $n$  é um número de Carmichael, então  $n$  não é divisível por  $p^2$ , para qualquer  $p$  primo.

(c) Prove que, se  $n$  é número de Carmichael, então  $p-1$  divide  $n-1$ , para todo  $p$  divisor de  $n$ .

Seja  $n = p_1 p_2 \dots p_k$  ( $k \geq 2$ ),  $p_i$  primo e  $\forall i, j \quad p_i \neq p_j$ .  
suponha  $\forall p_i \quad \text{t.g. } p_i \mid m, p_i - 1 \mid m - 1$

(i)  $p_i \nmid a$

$$\forall a, \text{ord}_n(a) \in D(\varphi(n)), \text{ como } \varphi(n) = \prod_{i=1}^k (p_i - 1) \Rightarrow$$

$$p_i - 1 \mid m - 1, \forall i$$

$$\text{ord}_{p_i}(a) \mid \varphi(p_i) = p_i - 1$$

$$\begin{cases} a^{n-1} \equiv 1 \pmod{p_i} & \text{T.C.R.} \\ a^{n-1} \equiv 1 \pmod{p_j} \Leftrightarrow a^{n-1} \equiv 1 \pmod{\prod_{i=1}^m p_i} \\ a^{n-1} \equiv 1 \pmod{p_k} \end{cases} \Leftrightarrow a^n \equiv a \pmod{n}$$

(ii)  $\forall i, p_i \mid a$

$$0 \equiv a \equiv a^n \pmod{n}$$

(iii)  $\exists i \quad \text{t.g. } p_i \mid a \Leftrightarrow a \equiv 0 \pmod{p_i}$

$$\begin{cases} a^{n-1} \equiv 1 \pmod{p_i} & \text{T.C.R.} \\ a^{n-1} \equiv 0 \pmod{p_i} \Leftrightarrow \\ a^{n-1} \equiv 1 \pmod{p_k} \end{cases} \Leftrightarrow \begin{cases} a^{n-1} \equiv 1 \pmod{\prod_{i=1}^k p_i} \\ a^{n-1} \equiv 0 \pmod{p_i} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} a^n \equiv a \pmod{\prod_{\substack{j=1 \\ j \neq i}}^k p_j} & \text{T.C.R.} \\ a^n \equiv 0 \equiv a \pmod{p_i} \end{cases} \Leftrightarrow a^n \equiv a \pmod{m}$$

(b) Seja  $m$  de Carmichael (\*). Suponha por absurdo que  $\exists p$  t.g.  $p^2 \mid m$ . (i). Temos de (\*)  $p^n \equiv p \pmod{p^2}$ , i.e.  $m \mid p^n - p$ . (ii). E também que  $p^2 \mid p^n$ , de (\*),  $n \geq 2$  (iii). Logo,  $p^2 \mid p^n - p$  (de (i) e (ii)), com (iii)  $p^2 \mid p$ , absurdo. Portanto,  $m$  não é divisível por  $p^2$ .

(c) Suponhamos que  $m$  é um número de Carmichael(\*)

$$\varphi(n) = \prod_{i=1}^k (p_i - 1)$$

Seja  $a$  o gerador de  $(\mathbb{Z}/p_3\mathbb{Z})^*$

$(\mathbb{Z}/p_3\mathbb{Z})^*$  é cíclico, se primo  $\Rightarrow$  Existe um elemento

de ordem  $p-1$  em  $(\mathbb{Z}/p_3\mathbb{Z})^*$

Tomos de (\*) que  $a^n \equiv a \pmod{m} \Leftrightarrow a^{n-1} \equiv 1 \pmod{m}$ , logo  $\text{ord}_m(a) \mid n-1$ , como  $\text{ord}_{p_3}(a) = p_3 - 1$ , temos que  $p_3 - 1 \mid n-1$ .

Como  $p_i$  arbitrários, concluimos que  $\forall p$  divisor primo de  $m$ ,  $\Rightarrow p-1 \mid n-1$ .

112) De quantas maneiras podemos pintar um tabuleiro  $n \times n$ , sendo que cada casinha pode ter uma de  $K$  cores, para

(a)  $n$  par;

(b)  $n$  ímpar;

Duas pinturas são consideradas iguais quando uma pode ser obtida através de uma rotação.

(a)

$$\text{Total: } \underbrace{K \cdot K \cdots K}_{n^2} = K^{n^2}$$

Simetria em  $180^\circ$ : determinado por metade dos quadrados  $\Rightarrow K^{\frac{n^2}{2}}$

Simetria em  $90^\circ$ : determine por  $\frac{1}{4}$  dos quadrados  
 $\Rightarrow \cancel{K^{\frac{n^2}{2}}} K^{\frac{n^2}{4}}$

Simetria em  $270^\circ$ : determine por  $\frac{1}{4}$  dos quadrados  
 $\Rightarrow K^{\frac{n^2}{4}}$

Pelo lema de Burnside:

$$\frac{K^{n^2} + K^{\frac{n^2}{2}} + 2 \cdot K^{\frac{n^2}{4}}}{4}$$

(b) Total:  $K \cdot K \cdots K = K^{n^2}$

Simetria em  $180^\circ$ : determinado por  $(\text{quadrados} - 1)/2 +$   
 $\Rightarrow K^{\left(\frac{(n^2-1)}{2}\right) \frac{n!}{2}}$

Simetria em  $90^\circ$  e  $270^\circ$ : determinado por  
 $(quadrantes -1)/4 + 1 \Rightarrow K^{\frac{(m^2-1)}{4}+1}$

Pelo teorema de Burnside:

$$\frac{K^{m^2} + K^{\frac{(m^2-1)}{4}+1} + 2K}{4}$$

113) A cada 43 anos o cometa  $\alpha$  retorna à terra, e a cada 47 anos um outro cometa,  $\beta$ , retorna à terra. Sabe-se que o cometa  $\alpha$  foi visto na terra em 1871 e que o cometa  $\beta$  foi visto em 1530. Qual foi o último ano em que ambos os cometas poderiam ser vistos juntos? E qual será o próximo?

Queremos que  $1871 + 43x = 1530 + 47y \Rightarrow 47y - 43x = 341$ . Como  $(47, 43) = 1$  a equação possui soluções inteiros. Utilizando o algoritmo de Euclides temos que

$$\begin{array}{c|ccccc} & 1 & 10 & 1 \\ \hline 47 & | & 43 & | & 4 & | & 3 \\ & 4 & 3 & 1 & & & \end{array} \Rightarrow \left. \begin{array}{l} 47 = 43 \cdot 1 + 4 \\ 43 = 4 \cdot 10 + 3 \\ 4 = 3 \cdot 1 + 1 \end{array} \right\} \begin{array}{l} 4 = 47 - 43 \\ 3 = 4 - 1 \\ 1 = 43 - 42 \end{array}$$

$$\Rightarrow 43 = 10(47 - 43) + (47 - 43) - 1 \quad \left. \begin{array}{l} 11 \cdot 47 - 12 \cdot 43 = 1 \\ 11 \cdot 47 - 11 \cdot 43 - 1 \end{array} \right\} \quad (1)$$

Multiplicando (1) por 341 obtemos  $47 \cdot 3751 - 43 \cdot 4092 = 341$ . A solução geral é dada por  $x = 3751 + 43\alpha$  e  $y = 4092 + 47\alpha$ , com  $\alpha \in \mathbb{Z}$  e  $x, y \in \mathbb{Z}^+$ . Temos então que

$$1871 + 43(4092 + 47\alpha) = 1871 + 43 \cdot 4092 + 2021\alpha = \beta$$

e daí

$$\beta \equiv 1871 + 43 \cdot 50 \equiv 2000 \pmod{2021}$$

Portanto, a última vez em que eles foram vistos juntos foi em 2000, e a próxima será em  $2000 + 2021 = 4021$ .

114) a) Determine todas as raízes primitivas módulo 14.

b) Determine todas as raízes primitivas módulo 49.

c) Determine as ordens de 3, 27 e 81 módulo 98.

a)  $\phi(14) = (2-1)(7-1) = 6 \quad D_6 = \{1, 2, 3, 6\}$

	13	5	9	11	13
2	9	11	11	9	1
3	13	13	1	1	-
6	1	1	1	1	1

✓ ✓ X X X

As raízes primitivas são  $\{3, 5\}$

b)  $\phi(49) = 42$ , repetindo a mesma tabela do item anterior temos as raízes primitivas são:

$$\{3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47\}.$$

c) 3: Como 3 é raiz primitiva de 49,  $\phi(98) = 42$   
 $\text{ord}_{98}(3) = 42$

27: Note que  $27 = 3^3$ , dai

$$\text{ord}_{98}(3^3) = 42/3 = 14$$

$$81: 81 = 3^4 \Rightarrow (3^4)^d \equiv 1 \pmod{98}$$

$$\Leftrightarrow 4d = 42k \Rightarrow d = 21, k=2$$

$$\Rightarrow \text{ord}_{98}(81) = 21,$$

115 Determine todos os inteiros positivos  $x$  para os quais  $2^x - 2^{2021}$  é múltiplo de 101.

Reveremos que  $2^x - 2^{2021} = 101k$ , para  $k \in \mathbb{N}$ ; ou seja

$$2^x - 2^{2021} \equiv 0 \pmod{101}$$

$$2^x \equiv 2^{2021} \pmod{101}$$

$$2^x \equiv 2^{100 \cdot 20 + 21} \pmod{101}$$

Como 101 é primo pelo Teorema de Fermat  $2^{100} \equiv 1 \pmod{101}$  daí

$$2^x \equiv (2^{100})^{20} \cdot 2^{21} \equiv 2^{21} \pmod{101}$$

Como  $2^{100k+21} \equiv 2^{21} \pmod{101}$ , a solução geral é dada por  $x = 100k + 21$ ,  $k \in \mathbb{N}$ .

116 Dado  $p$  primo ímpar, determine todos os inteiros  $k$  para os quais  $S_k = \sum_{j=1}^{p-1} j^k$  é múltiplo de  $p$ .

~~Suponha~~ Suponha que para algum  $x$ , tal que  $0 < x < p-1$ , temos  $\Rightarrow x^k \not\equiv 1 \pmod{p}$ . Então

$$x^k \cdot S_k \equiv \sum_{j=1}^{p-1} (xj)^k \pmod{p}$$

Dado que  $\{1, 2, \dots, p-1\} \pmod{p} = \{xj \mid j=1, \dots, p-1\} \pmod{p}$  ou seja, o conjunto ~~de restos~~ não iguais.

Portanto,  $x^k S_k \equiv S_k \pmod{p}$ . Só que como assumimos que  $x^k \not\equiv 1 \pmod{p}$ , concluimos que  $S_k \equiv 0 \pmod{p}$ .

A partir disso todo, retiramos a informação que para  $S_k$  ser múltiplo de  $p$ , só precisamos que  $x^k \not\equiv 1 \pmod{p}$ , para todo ~~retiramos a informação que para~~ ~~seja~~ ~~multiplo de p, só precisamos~~ todo  $0 < x < p-1$ . Como  $p$  é primo,  $\text{ord}_p(k) = p-1$ , ou seja, a resposta para  $k$  é todos inteiros, exceto os múltiplos de  $p-1$ .

(1.17) Seja  $n$  um inteiro positivo e  $a$  um inteiro qualquer. Prove que se um primo  $p$  divide  $\Phi_n(a)$ , então

1.  $p$  divide  $n$ , ou

2.  $p \equiv 1 \pmod{n}$

$$\Phi_n(a) = \frac{a^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(a)}, \quad p \mid \Phi_n(a) \mid a^n - 1 \Rightarrow p \mid a^n - 1 \text{ e } p \nmid a$$

Tomemos  $K = \text{ord}_p(a)$ .

$$p \mid a^n - 1 \Rightarrow a^n \equiv 1 \pmod{p} \Rightarrow K \mid n \Rightarrow K = n \text{ ou } K \in D_n$$

Se  $K = n$

$$\begin{aligned} p \text{ é primo e } p \nmid a &\Rightarrow p \nmid a^{p-1} \Rightarrow p \nmid a^{p-1} - 1 \pmod{p} \Rightarrow \\ &\Rightarrow p \nmid p-1 \Rightarrow p \equiv 1 \pmod{n} \leftarrow \text{Caso (2).} \end{aligned}$$

Se  $K < n$

$$a^K - 1 \equiv 0 \equiv \prod_{d|K} \Phi_d(a) \pmod{p}$$

$\Rightarrow \exists d$  divisor de  $K$  tal que  $p \mid \Phi_d(a)$

$$\Rightarrow d \mid K \mid n \Rightarrow d \mid n$$

Portanto, pode-se concluir que  $p \mid n$ . <sup>d</sup> Caso (1)

(116) Seja  $p$  um primo ímpar, e seja,  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  uma função tal que, para todos os inteiros  $m, n$ .

• (i)  $f(m \cdot n) = f(m) \cdot f(n)$

• (ii) se  $m \equiv n \pmod{p}$

(a) Prove que a imagem de  $f$  está contida no conjunto  $\{-1, 0, 1\}$ .

(b) Determine todos os possíveis funções  $f$ .

Seja  $m$  inicialmente  $m \in \mathbb{Z}$ .

$$f(m) = f(m \cdot 1) = f(m) \cdot f(1)$$

ou  $f(1) = 1$ , ou  $f(1) = 0$ , como o segundo caso tornaria o problema trivial, suponha  $f(1) = 1$ . Vamos dividir em 2 casos  $m \equiv m \pmod{p}$  t.g.  $(m, p) = 1$  e  $(m, p) \neq 1$ .

• Para  $(m, p) = 1$ , vale o teorema de Fermat ou seja  $m^{p-1} \equiv 1 \pmod{p}$  e pela propriedade (ii)

$$f(m^{p-1}) = f(1) = 1$$

Como  $f(m \cdot m) = f(m)^2$ , então  $f(m^{p-1}) = f(m)^{p-1} = 1$ , ou seja  $f(m) = \pm 1$ .

• Para  $m = kp$ ,  $k \in \mathbb{Z}$

$$f(m) = f(k) \cdot f(p) \stackrel{(ii)}{=} f(0)$$

E como  $f(p) = f(0)$  (também por (ii)), temos que para  $k \in \mathbb{Z}$

$$f(k) \cdot f(0) = f(0)$$

sendo  $f(k) = \pm 1$  então  $f(0) = 0$ , caso  $f(k) = 0$ , então  $f(m) = 0 \Leftrightarrow f(0) = 0$ .

(6)  $\mathbb{R} \neq \mathbb{S}$  pode ser t.g.

- $f(m) = 0, \forall m$

- $f(m) = 1, \forall m$

- ~~$\Rightarrow f(m) =$~~   $f(m) = \begin{cases} 1, & \text{se } m = 1 \\ 0, & \text{se } m \neq 1 \end{cases}$

$$\begin{cases} 0, & \text{se } m \neq 1 \\ \pm 1, & \text{se } m = 1 \end{cases} \quad (\text{otherwise})$$