Ficha 3

1.

a) $x = 17 \bmod 11 = 6$

$y = 13 \bmod 11 = 2$

$xy \bmod 11 = 12 \bmod 11 = 1$

$(x+y) \bmod 11 = 8 \bmod 11 = 8$

$(x-y) \bmod 11 = 4 \bmod 11 = 4$

b) $mdc(30030, 257) = 1$

30030	257	257	218	218	39	39	23	23	16
218	116	39	1	23	5	16	1	7	1

16	7	7	2	2	1
2	2	(1)	3	0	2

c) $17x + 101y = 1$ $\quad mdc(101, 17)$

$x_0 = 0 \quad y_0 = 1$

$x_1 = 1 \quad y_1 = 0$

101	17	17	16	16	1
16	5	1	1	0	16

3 quocientes

$x_2 = -5 \times 1 + 0 = -5$

$x_3 = -1 \times (-5) + 1 = 6$

$y_2 = -5 \times 0 + 1 = 1$

$y_3 = -1 \times 1 + 0 = -1$

$x = 6$ e $y = -1$

d) $172x + 190y = mdc(172, 190)$

- $mdc(190, 172)$:

190	172	172	18	18	10	10	8	8	2
18	1	10	9	8	1	(2)	1	0	4

$172x + 190y = 2$

- $x_0 = 0 \quad y_0 = 1$

$x_1 = 1 \quad y_1 = 0$

$x_2 = -1 \times 1 + 0 = -1$

$x_3 = -9 \times (-1) + 1 = 10$

$x_4 = -1 \times 10 - 1 = -11$

$x_5 = -1 \times (-11) + 10 = (21)$

$y_2 = -1 \times 0 + 1 = 1$

$y_3 = -9 \times 1 + 0 = -9$

$y_4 = -1 \times (-9) + 1 = 10$

$y_5 = -1 \times 10 - 9 = (-19)$

$x = 21, \; y = -19$

e) $1 = 7x \bmod 30$

$1 = 7x + 30k \Leftrightarrow 7x + 30k \equiv 1$

$mdc(30,7) = 1$ ✓

30 \ 7	7 \ 2	2 \ 1
2 4	(1) 3	0 2

⇒ Calcular o inverso multiplicativo de 7

$x_0 = 0 \quad y_0 = 1$

$x_1 = 1 \quad y_1 = 0$

$x_2 = -4 \times 1 + 0 = -4$

$x_3 = -3 \times (-4) + 1 = 13 \rightarrow x = 13$

f) $2^{1234} \bmod 789$, $mdc(789,2) = 1$

789 | 3
263 | 263
1 |

$789 = 3 \times 263$

$\phi(789) = (3-1)(263-1) = 2 \times 262 = 524$

$2^{1234} = (2^{524})^2 \times 2^{186}$

$2^{1234} \bmod 789 = \underbrace{(2^{524})^2}_{1} \times 2^{186} \bmod 789$

1 Pelo teorema de Euler

$= 2^{186} \bmod 789 = 2^{128} \times 2^{32} \times 2^{16} \times 2^8 \times 2^2 \bmod 789$

$= (\ldots) = 481 \bmod 789$

2. $\underset{b}{x} \bmod \underset{m}{7} = \underset{a}{3}$ $\quad x \bmod 15 = 5$

$\Leftrightarrow \begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 15 \end{cases} \Big\} x \equiv y \bmod (m * n)$

$3 + 7k \equiv 5 \bmod 15$

$7k \equiv 2 \bmod 15$

$k \equiv \frac{2}{7} \bmod 15$

⇒ Inverso multiplicativo

$mdc(7,15) = 1$ ✓

15	7	7	21
①	②	0	7

$7z \equiv 1 \bmod 15 \equiv 1 + 15k \Rightarrow 7z + 15k = 1$

$z_2 = -2 \times 1 + 0 = -2$

$z = -2 \bmod 15 = 13 \bmod 15$

$\frac{1}{7} = 13 \bmod 15$

$k \equiv 2 \times 13 \bmod 15 = 11 \bmod 15$

Então:

$y = 3 + 7k = 3 + 7 \times 11 = 80$

$x \equiv 80 \bmod (7 \times 15) \equiv 80 \bmod 105$

3.

Pela função de Euler sabemos que:

$$\begin{cases} n = p \cdot q \\ \phi(n) = (p-1)(q-1) \end{cases} \Leftrightarrow \begin{cases} p \cdot q = 221 \\ 192 = (p-1)(q-1) \end{cases}$$

$$\Leftrightarrow \begin{cases} \\ pq - p - q + 1 = 192 \end{cases} \Leftrightarrow \begin{cases} \\ 221 - p - q + 1 = 192 \end{cases} \Leftrightarrow \begin{cases} \\ p + q = 30 \end{cases}$$

$$\Leftrightarrow \begin{cases} (30 - q)q = 221 \\ p = 30 - q \end{cases} \Leftrightarrow \begin{cases} 30q - q^2 = 221 \\ \\ \end{cases} \Leftrightarrow \begin{cases} q = 13 \vee q = 17 \\ p = 17 \vee p = 13 \end{cases}$$

4. $C = 5859$

$p = 101, q = 113$

$d \times 7467 \equiv 1 \bmod (100 \times 112)$

$\Leftrightarrow 7467 \times d \bmod 11200 = 1$ (b, n, a)

$\Leftrightarrow 7467\, d \equiv 1 \bmod 11200$

$\Leftrightarrow d = \frac{1}{7467} \bmod 11200$

$\gcd(11200, 7467) = 1$ ✓

$11200 \,/\, 7467$
$3733 \;\; 1$

$7467 \,/\, 3733$
$1 \;\; 2$

$3733 \,/\, 1$
$0 \;\; 3733$

$7467x \equiv 1 \bmod 11200 \Leftrightarrow 7467x = 1 + 11200k$

$\Leftrightarrow 7467x + 11200k = 1$

$x_2 = -1 \times 1 + 0 = -1$

$x_3 = -2 \times (-1) + 1 = 3$

$34\,327881 \,/\, 11413$

$d \equiv 1 \times 3 \bmod 11200 = 3$

$m = 5859^3 \bmod 11413 \equiv 5859^2 \times 5859 \bmod 11413$

$\equiv 8990 \times 5859 \bmod 11413$

$\equiv 1415 \bmod 11413$

$m = 1415$

5.
a) $n = 55 = p \cdot q = 5 \times 11$

$de \equiv 1 \bmod 40 \Leftrightarrow 3d \equiv 1 \bmod 40 \Leftrightarrow d \equiv \frac{1}{3} \bmod 40$

$mdc(40, 3) = 1$ ✓

40	3		3	1
1	13		0	3

$3d \equiv 1 + 40k \Leftrightarrow 3d + 40k \equiv 1$

$x_2 = -13 \times 1 + 0 = (-13)$ → Inverso multip de 3

$d \equiv -13 \times 1 \bmod 40 \equiv \underline{\underline{27}} \bmod 40$

Logo $d = 27$

b) $mdc(m, 55) = 1 \qquad \phi(55) = 4 \times 10 = 40$

$m^{\phi(55)} = 1 \bmod 55 \Leftrightarrow m^{40} = 1 \bmod 55$

$c = m^e \bmod 55$

$c^d \bmod n \equiv (m^e)^d \bmod n \equiv m^{3 \times 27} \bmod n \equiv m^{81} \bmod n$

$\equiv \underbrace{(m^{40})^2}_{1} \times m \bmod n \equiv m \bmod n$

$\Downarrow$

$m = e^d \bmod 55$

6. $m = 5575$

a) $\pi(7500) = \frac{7500}{\ln 7500} \simeq 841$ (arredondado para cima)

b) • Usar $\pi(n)$ e teorema de Fermat

$\pi(4000) \simeq 482$

Entre 4000 e 7500 há aprox. 359 nº primos

Ex: $p = 4099, q = 7193$

P.T.F

$2^{4098} \bmod 4099 \equiv 2^{4096} \times 2^2 \bmod 4099$ (...) Logo $p = 4099$ provavelmente é primo

c) $n = 4099 \times 7193 = 29484107$

$\phi(n) = 4098 \times 7192 = 29472816$

d) Primo maior que 100 $\Rightarrow$ 101

$mdc(e, \phi(n)) = 1$

$mdc(101, 29472816) = 1$? ✓✓

$29472816 \mid 101$

291810

$101 \mid 67$

$5 \quad 16$

$6 \mid 5 \quad 5 \mid 1$

$1 \quad 1 \quad 0 \quad 5$

e) $de \equiv 1 \bmod 29472816$

$101d \equiv 1 \bmod 29472816$

$d \equiv \frac{1}{101} \bmod 29472816$

$mdc(5575$

$mdc(29472816, 101) = 1$ ✓

$101d + 29472816k = 1$

$x_2 = -291810 \times 1 + 0 = -291810$

$x_3 = -16 \times (-291810) + 1 = 4668961$

$x_4 = -1 \times 4668961 + (-291810) = -4960771$

$d \equiv -4960771 \bmod 29472816 \equiv 24512045$

f) $c = (5575)^{101} \bmod 29484107$

$m = 5575^{64} \times 5575^{32} \times 5575^{4} \times 5575 \bmod 29484107$

$= 3123925 \times 13407110 \times 27642385 \times 5575 \bmod 29484107$

$= 9935116$

$20 \quad 55 \quad 1 \quad 5$

- 5575
- $5575^2 = 1596518$
- $5575^4 = 27642385$
- $5575^8 = 18237467$
- $5575^{16} = 3807279$
- $5575^{32} = 13407110$
- $5575^{64} = 3123925$

g) $m = (9935116)^{24512045} \mod 29484107$

$= 5575$

7. Pelo enunciado sabemos que:

$e^2 = 1 + k\phi(n)$

$c_1 = m^e \mod n$

$c_2 = (c_1)^e \mod n = (m^e)^e \mod n = m^{e^2} \mod n$

$= m^{1+k\phi(n)} \mod n = m \times m^{k\phi(n)} \mod n$

$= m \times (m^{\phi(n)})^k \mod n = m \mod n = m$

(Teorema Euler)

Mensagem Original

OU

Como

$e^2 = 1 \mod \phi(n)$ e $de = 1 \mod \phi(n)$

Então encriptar duas vezes equivale a termos a mensagem original