

MAT2450 Ch 7.

1.6 Soient $a \equiv c \pmod n$, $b \equiv d \pmod n$.

Montrons $ax + by \equiv cx + dy \pmod n$.

Supposons $a = k_a n + r_a$; $c = k_c n + r_c$; $b = k_b n + r_b$; $d = k_d n + r_d$

$k_a, k_b, k_c, k_d \in \mathbb{Z}$, $r_a, r_b \in \{0, 1, 2, \dots, n\}$

Alors

$$\begin{aligned} x \underbrace{(k_a n + r_a)}_a + y \underbrace{(k_b n + r_b)}_b &= x r_a + y r_b + n(k_a \cdot x + k_b \cdot y) \\ &\equiv x r_a + y r_b + n(k_c x + k_d y) \pmod n \\ &= x(k_c n + r_c) + y(k_d n + r_d) \pmod n \\ &= xc + yd \pmod n \quad \text{c.q.f.d.} \blacksquare \end{aligned}$$

$$7.6.4.a) \Phi(p^2) = p^2 - p.$$

$$\Phi(n) = |\{x < n : (x, n) = 1\}| \rightarrow \Phi(p) = p - 1.$$

Pour p^2 , on donne l'intuition avec $5^2 = 25$

1 2 3 4 ~~5~~ 6 7 8 9 ~~10~~ 11 12 13 14 ~~15~~ 16 17 18 19 ~~20~~ 21 22 23 24 ~~25~~

b) Le chiffrement marche de façon pareille,
mais il faudra trouver $e \in \{3, 4, \dots, n-1\}$

$$\text{tq } (e, \Phi(p^2)) = 1.$$

Ensuite, si un adversaire sait qu'on a utilisé p^2 au lieu de $pq : p \neq q$, leur espace de recherche pour trouver nos paramètres de chiffrement sera beaucoup plus petit.

$$7.6.6a) d = \frac{3(p-1)(q-1)+1}{7} ; \quad \begin{array}{l} p \equiv 2 \pmod{7} \\ q \equiv 3 \pmod{7} \end{array} \rightarrow \begin{array}{l} p-1 \equiv 1 \pmod{7} \\ q-1 \equiv 2 \pmod{7} \end{array}$$

$$\Rightarrow 3 \cdot (p-1) \cdot (q-1) \equiv 3 \cdot 1 \cdot 2 \pmod{7} \equiv 6 \pmod{7}$$

$$\Rightarrow 7 \text{ divise } (3 \cdot (p-1)(q-1) + 1).$$

b) Pour que a^d s'annule mod n , il faut qu'il soit un multiple de $n=pq$, càd de pq .

Mais cela nécessite aussi que m soit un multiple de p et q comme ils sont premiers.

Ce n'est pas possible car $m < n = pq$.

$$c) a^d \equiv m^{7d} \equiv m^{(3(p-1)(q-1)+1)} \equiv (m^{\phi(pq)})^3 \cdot m \equiv m \pmod{pq}.$$

7.6.8. a) $\overset{14}{N} \overset{7}{G} \overset{6}{F}, \overset{28}{C}$

N.B. En programmation, on écrit la fonction $f_n: \mathbb{R} \rightarrow [0, n) \quad x \mapsto x \bmod n$ comme " $x \% n$ "

b) Il y a toujours une bijection entre les lettres encodées et pas encodées, comme $(29, 3) = 1$.

On peut trouver 3^{-1} dans le groupe $\mathbb{F}_{29}^*$:

$$3^{29-1} \equiv 10^{\overset{\text{(trouvé par ordi)}}{3}} \bmod 29.$$

Alors au lieu de $y = (3x + 4) \% 29$

on fera $x = (y - 4) \cdot 10 \% 29$.

c) $\overset{19}{S} \overset{23}{W} \overset{0}{\square} \overset{10}{J}$.

$$7.6.9. \quad R_q : 10 \equiv 1 \pmod{9} \rightarrow 10^k \equiv 1 \pmod{9} \forall k.$$

$$M_q \quad F(nm) = F(F(n)F(m)).$$

$$\text{Soit } s(x) : \mathbb{N} \rightarrow \mathbb{N} \quad \text{t.q.} \quad \begin{array}{l} \text{Si } x = \sum_{k=0}^N a_k \cdot 10^k \\ \text{alors } s(x) = \sum_{k=0}^N a_k \end{array} \rightarrow F(x) \equiv s(x) \pmod{9}.$$

$$10^k \equiv 1 \pmod{9} \Rightarrow x \equiv s(x) \pmod{9}.$$

$$\text{Alors } s(nm) \equiv nm \equiv s(n)s(m) \equiv s(\underbrace{s(n)s(m)}) \pmod{9}.$$

$$\Rightarrow F(nm) = F(n).$$

C) Clairement, non. La condition est nécessaire mais pas suffisante.

7.6.11

On cherche $d : de \equiv 1 \pmod{\phi(n)}$ où $e=47$

$$\text{et } \phi(n) = (p-1)(q-1) = 22 \cdot 36 = 792$$

$\rightarrow d=457$ ^{$\rightarrow$ (trouvé par ord.)}
marche.

7.6.12.

a) On commence par remarquer

$$10 \equiv -1 \pmod{11} \rightarrow 10^k \equiv (-1)^k \pmod{11}$$

$$\Rightarrow \sum_{k=0}^{N-1} 10^k a_k \equiv \sum_{k=0}^{N-1} (-1)^k a_k \pmod{11}. \quad \text{c.q.f.d.}$$

b) $100 \equiv -1 \pmod{101} \rightarrow 10^{2k} \equiv (-1)^k \pmod{101}$
 $\rightarrow 10 \cdot 10^{2k} = 10^{2k+1} \equiv 10(-1)^k \pmod{101}.$

Supposons N est pair et $a_{N+1} = 0$, en définissant $a_N = 0$
si nécessaire.

$$\sum_{k=0}^{N/2} (10^{2k} a_{2k} + 10^{2k+1} a_{2k+1}) \equiv \sum_{k=0}^{N/2} (-1)^k (a_{2k} + 10 a_{2k+1}) \pmod{101}$$

c.q.f.d.