TP6 28 février 2025

Section 7.6

Exercice 1 : Soient $a, b, c, d, x, y \in \mathbb{Z}$. Montrer que

(b) $a \equiv c \pmod{n}$ et $b \equiv d \pmod{n} \Rightarrow ax + by \equiv cx + dy \pmod{n}$

Sol : (b) $a \equiv c \pmod{n} \Rightarrow a = k \cdot n + c$, pour $k \in \mathbb{Z}$

$$\Rightarrow ax = knx + cx$$

$b \equiv d \pmod{n} \Rightarrow b = ln + d$, pour $l \in \mathbb{Z}$

$$\Rightarrow by = lny + dy$$

Ainsi, $ax + by = knx + lny + cx + dy$

$$\Rightarrow ax + by \equiv cx + dy \pmod{n}$$

Exercice 4 : Soit p un nombre premier.

(a) Calculer $\phi(p^2)$, où ϕ est la fonction d'Euler.

(b) Le principe de la cryptographie à clé publique fonctionne pour un entier $n = p \cdot q$, où p et q sont deux grands nombres premiers distincts. Est-ce que le principe fonctionnerait aussi avec l'entier

$n=p^2$? Si oui, décrire les étapes à suivre.

Pourquoi alors ne l'utiliserait-on pas ?

<u>Sol</u> : (a) Rappel : $\phi(n)$ est le nombre d'entiers dans $\{1,2,\ldots,n-1\}$ qui sont relativement premiers avec n, pour $n>1$, et $\phi(1)=1$.

On a
$$\begin{aligned}\phi(p^2) &= \left|\{1\leq n\leq p^2-1 \mid (n,p^2)=1\}\right| \\ &= (p^2-1) - \left|\{1\leq n\leq p^2-1 \mid (n,p^2)\neq 1\}\right| \\ &= p^2-1-\left|\{p, p^2, \ldots, (p-1)p\}\right| \\ &= p^2-1-(p-1) \\ &= p^2-p \\ &= p(p-1)\end{aligned}$$

(b) Le système fonctionne de la même façon que dans le cas où on choisit p et q distincts. Par contre, pour briser le code, il suffit d'essayer de calculer $\sqrt{n}=\sqrt{p^2}$, qui est beaucoup plus facile que de trouver deux grands premiers distincts p et q

tels que $pq=n$.

Exercice 6 : Vous choisissez un entier premier p, tel que $p \equiv 2 \pmod 7$ et un entier premier q, tel que $q \equiv 3 \pmod 7$. Ceci vous permet de calculer $n=pq$. Le message d'Alain est un nombre m de $\{1, \dots, n-1\}$ tel que $(m,n)=1$. Pour envoyer son message, Alain calcule m^7 et divise ce nombre par n. Soit $a \in \{1, \dots, n-1\}$ le reste de la division de m^7 par n. Béatrice décode avec la clé de décryptage $d = \dfrac{3(p-1)(q-1)+1}{7}$.

Elle calcule a^d et le reste m_1 de la division de a^d par n. On affirme que ce reste est le message d'Alain.

(a) Vérifier que d est un entier

(b) Expliquer pourquoi a et m_1 ne peuvent s'annuler, c-à-d qu'on a $a, m_1 \in \{1, \dots, n-1\}$

(c) Montrer que $m_1 = m$.

Sol: (a) On a

$$d = \frac{3(p-1)(q-1)+1}{7}$$

$$= \frac{3(7\cdot k+2-1)(7\cdot \ell+3-1)+1}{7}, \text{ pour } k,\ell \in \mathbb{Z}$$

car $p \equiv 2 \pmod 7$
$q \equiv 3 \pmod 7$

$$= \frac{3(7k+1)(7\ell+2)+1}{7}$$

$$= \frac{3(49k\ell+14k+7\ell+2)+1}{7}$$

$$= \frac{3\cdot 49k\ell+3\cdot 14k+3\cdot 7\ell+6+1}{7}$$

$$= 3\cdot 7k\ell + 3\cdot 2k + 3\ell + 1 \in \mathbb{Z}$$

(b) Par définition, $m \in \{1, 2, \ldots, n-1\}$, et $(m,n) = 1$

$(m,n) = 1 \Rightarrow m \not\equiv 0 \pmod n$

$\overset{\text{Lemme}}{\Rightarrow} m^7 \not\equiv 0 \pmod n$

$\Rightarrow a \neq 0$, car a est le reste de la de m^7 par n

Par définition, $a \equiv m^7 \pmod n$, alors on a

$$a^d \equiv_n (m^7)^d \equiv_n m^{7d} \overset{\text{Lemme}}{\not\equiv} 0 \ (\text{mod } n)$$

$\Rightarrow n \nmid a^d$

$\Rightarrow m_1 \neq 0$, car m_1 est le reste de la division de a^d par n

(c) Par définition, m_1 est le reste de la division de a^d par n. On a

$$a^d = (m^7)^d = m^{7d} = m^{3(p-1)(q-1)+1} = \left(m^{(p-1)(q-1)}\right)^3 m$$
$$= \left(m^{\phi(n)}\right)^3 m$$
$$\equiv 1^3 \cdot m \ (\text{mod } n), \text{ par thm d'Euler}$$
$$\equiv m$$

Donc $m = m_1$.

Exercice 8: On utilise les 29 symboles de l'exercice 7. Voici comment on code un mot formé de tels symboles :

① • On remplace les symboles par leurs nombres associés

② • On multiplie par 3 le nombre associé à chaque symbole et on ajoute 4.

③ On réduit le résultat obtenu modulo 29

④ On trouve les symboles correspondant aux nombres obtenus. Ceci nous donne le mot codé.

(a) Coder le mot « MATHS »

(b) Expliquer pourquoi le code est inversible et comment on s'y prend pour décoder.

(c) Décoder le mot « CODE »

Sol: (a) ① M : 13 , A : 1, T : 20, H : 8 , S : 19

② $13 \cdot 3+4=43$, $1 \cdot 3+4=7$, $20 \cdot 3+4=64$, $8 \cdot 3+4=28$, $19 \cdot 3+4=61$

③ $43=29+\underline{14}$, $7=\underline{7}$, $64=29 \cdot 2+\underline{6}$, $28=\underline{28}$, $61=29 \cdot 2+\underline{3}$

④ N : 14, G : 7, F : 6, , : 28 , C : 3

Le mot « MATHS » devient « NGF,C »

(b) Le code est réversible car 29 est premier.

Comme 29 est premier, on a que $(x, 29)=1$ $\forall x \in \{1, 2, \ldots, 28\}$. On peut donc appliquer l'algorithme d'Euclide et le corollaire 7.6.

Par exemple, pour retrouver M (13) à partir de N (14), on veut résoudre l'équation modulaire

$x \cdot 3 + 4 \equiv 14 \pmod{29}$.

On a $x \cdot 3 + 4 \equiv 14 \pmod{29}$

$\Rightarrow x \cdot 3 \equiv 10 \pmod{29}$ (✯)

On applique l'algorithme d'Euclide pour trouver l'inverse modulo 29 de 3

$29 = 3 \cdot 9 + 2$	$2 = 29 - 3 \cdot 9$
$3 = 2 \cdot 1 + 1$	$1 = 3 - 2 \cdot 1$
$2 = 1 \cdot 2 + 0$	

$$\Rightarrow 1 = 3 - (29 - 3 \cdot 9) \cdot 1$$
$$= 3 - 29 + 3 \cdot 9$$
$$= 3 \cdot 10 - 29$$
$$\equiv 3 \cdot 10 \pmod{29}$$

$\Rightarrow$ L'inverse modulo 29 de 3 est 10.

On revient à l'équation (✯), on a

$x \cdot 3 \equiv 10 \pmod{29}$

$\Rightarrow x \equiv 100 \pmod{29}$

$\equiv 13 \pmod{29}$

On a bien retrouvé $\underset{(13)}{M}$ à partir de $\underset{(14)}{N}$.

(c) Pour C : 3

$x \cdot 3 + 4 \equiv 3 \pmod{29}$

$\Rightarrow x \cdot 3 \equiv 28 \pmod{29}$

$\Rightarrow x \equiv 280 \pmod{29}$

$\equiv 19 \pmod{29}$

On change $\underset{(3)}{C}$ pour $\underset{(19)}{S}$

Pour O : 15

$x \cdot 3 + 4 \equiv 15 \pmod{29}$

$\Rightarrow x \cdot 3 \equiv 11 \pmod{29}$

$\Rightarrow x \equiv 110 \pmod{29}$

$\equiv 23 \pmod{29}$

On change $\underset{(15)}{O}$ pour $\underset{(23)}{W}$

Pour D : 4

$$x \cdot 3 + 4 \equiv 4 \pmod{29}$$

$$\Rightarrow x \cdot 3 \equiv 0 \pmod{29}$$

$$\Rightarrow x \equiv 0 \pmod{29}$$

On change $\underset{(4)}{D}$ pour $\underset{(0)}{\square}$

Pour E : 5

$$x \cdot 3 + 4 \equiv 5 \pmod{29}$$

$$\Rightarrow x \cdot 3 \equiv 1 \pmod{29}$$

$$\Rightarrow x \equiv 10 \pmod{29}$$

On change $\underset{(5)}{E}$ pour $\underset{(10)}{J}$

En décodant «CODE», on obtient «SW□J»

<u>Exercice 9</u> : On multiplie deux nombres m et n. Soit $N = mn$. On veut vérifier le résultat obtenu. Pour cela, on utilise la notation décimale d'un nombre $M \in \mathbb{N}$: $M = a_p \ldots a_0$, où $a_i \in \{0, 1, 2, \ldots, 9\}$. On a

$$M = \sum_{i=0}^{p} a_i 10^i$$

Au nombre M, on associe le nombre $F(M) \in \{0, 1, \ldots, 8\}$, où $F(M)$ est le reste de la division de

$\sum_{i=0}^{p} a_i$ par 9. Exemple : $F(2857)=4$.

On calcule $F(m)$, $F(n)$ et $r=F(m)F(n)$. On calcule ensuite $F(r)$.

(a) Montrer que, s'il n'y a pas d'erreur de calcul dans la *multiplication*, c-à-d si $N=mn$, alors on doit avoir $F(N)=F(r)$.

(b) Donner un exemple simple

(c) Que peut-on dire si $F(N)=F(r)$? Peut-on dire qu'il n'y a pas eu d'erreur dans la multiplication $N=mn$?

Sol : (a) Supposons que $N=mn$.

$$\begin{aligned} \text{On a } M &= \sum_{i=0}^{p} a_i 10^i \\ &\equiv \sum_{i=0}^{p} a_i \pmod 9 \\ &\equiv F(M) \pmod 9 \end{aligned}$$

Ainsi, la fonction F prend un nombre M entré et redonne M modulo 9, donc le reste de la division de M par 9.

On obtient

$$F(N) \equiv N \pmod 9$$
$$\equiv nm \pmod 9$$
$$\equiv F(n)F(m) \pmod 9$$
$$\equiv r \pmod 9$$
$$\equiv F(r) \pmod 9$$

Comme $F(N) \equiv F(r) \pmod 9$ et $F(N), F(r) \in \{0, 1, \ldots, 8\}$,

$F(N) = F(r)$.

(b) $n = 28, m = 5$

$\Rightarrow N = 28 \cdot 5 = 140$

$\Rightarrow F(N) = 5$

$F(n) = 1$, $F(m) = 5 \Rightarrow r = 5 \Rightarrow F(r) = 5$

$\Rightarrow F(N) = 5 = F(r)$

(c) Supposons qu'on fait une erreur de calcul et qu'on obtient $28 \cdot 5 = 131 = N$

On a $F(131) = 5$, $F(28) = 1$, $F(5) = 5 \Rightarrow r = 5 \Rightarrow F(r) = 5$

On a donc $F(N) = F(r)$, mais $28 \cdot 5 \neq 131$.

On sait seulement qu'on est à plus ou moins un multiple de 9 près.

Exercice 11: On se donne un code RSA avec clé $n = 23 \cdot 37 = 851$ et clé de cryptage $e = 47$. Trouver la clé de décryptage d qui satisfait à

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

Sol: On a $\phi(n) = \phi(851) = \phi(23 \cdot 37) = (23-1)(37-1)$

$$= 792$$

$\hookrightarrow (47, 792) = 1$

On cherche donc l'inverse modulo 792 de $e = 47$. On applique l'algorithme d'Euclide.

$792 = 47 \cdot 16 + 40$	$40 = 792 - 47 \cdot 16$
$47 = 40 \cdot 1 + 7$	$7 = 47 - 40 \cdot 1$
$40 = 7 \cdot 5 + 5$	$5 = 40 - 7 \cdot 5$
$7 = 5 \cdot 1 + 2$	$2 = 7 - 5 \cdot 1$
$5 = 2 \cdot 2 + 1$	$1 = 5 - 2 \cdot 2$
$2 = 1 \cdot 2 + 0$	

$$\Rightarrow 1 = 5 - (7 - 5 \cdot 1) \cdot 2$$

$$= 5 - 7 \cdot 2 + 5 \cdot 2$$

$$= 5 \cdot 3 - 7 \cdot 2$$

$$= (40 - 7 \cdot 5) \cdot 3 - 7 \cdot 2$$

$$= 40 \cdot 3 - 7 \cdot 15 - 7 \cdot 2$$

$$= 40 \cdot 3 - 7 \cdot 17$$

$$= 40 \cdot 3 - (47 - 40 \cdot 1) \cdot 17$$

$$= 40 \cdot 3 - 47 \cdot 17 + 40 \cdot 17$$

$$= 40 \cdot 20 - 47 \cdot 17$$

$$= (792 - 47 \cdot 16) \cdot 20 - 47 \cdot 17$$

$$= 792 \cdot 20 - 47 \cdot 16 \cdot 20 - 47 \cdot 17$$

$$= 792 \cdot 13 - 47 \cdot 337$$

$$= 792 \cdot 13 - 337 \cdot 47$$

$$\equiv -337 \pmod{792}$$

$$\equiv 455$$

$$\Rightarrow d = 455$$

Exercice 12: On se donne un nombre entier de N chiffres.

Soit $a_{N-1} \cdots a_1 a_0$ sa représentation décimale, c-à-d

$$N = a_{N-1} 10^{N-1} + a_{N-2} 10^{N-2} + \dots + a_1 10 + a_0$$

(a) Montrer que N est divisible par 11 si et seulement si $a_0 - a_1 + a_2 - a_3 + \dots + (-1)^{N-2} a_{N-2} + (-1)^{N-1} a_{N-1} \equiv 0 \pmod{11}$

(b) Montrer que N est divisible par 101 si et seulement si $(a_0 + 10a_1) + (a_2 + 10a_3) - (a_4 + 10a_5) + \dots \equiv 0 \pmod{101}$

Sol: (a) On a que $N \equiv 0 \pmod{11}$

$$\Leftrightarrow a_{N-1} 10^{N-1} + a_{N-2} 10^{N-2} + \dots + a_1 10 + a_0 \equiv 0 \pmod{11}$$

$$\Leftrightarrow a_{N-1} (-1)^{N-1} + a_{N-2} (-1)^{N-2} + \dots + a_1 \cdot 10 + a_0 \equiv 0 \pmod{11}$$

Remarque: $10^i \equiv (-1)^i \pmod{11}$, car

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

$$\Rightarrow 10^2 \equiv (-1)^1 (-1)^1 \equiv (-1)^2 \pmod{11}$$

$$\vdots$$

$$\Rightarrow 10^i \equiv (-1)^{i-1} (-1)^1 \equiv (-1)^i \pmod{11}$$

(b) On a $10^2 \equiv 100 \equiv -1 \pmod{101}$

$$\Rightarrow 10^4 \equiv (-1)^2 \pmod{101}$$

$$\vdots$$

$$\Rightarrow 10^{2i} \equiv (-1)^i \pmod{101}$$

On a $N \equiv 0 \pmod{101}$

$$\Leftrightarrow a_0 + a_1 10^1 + a_2 10^2 + a_3 10^3 + a_4 10^4 + a_5 10^5 + \dots \equiv 0 \pmod{101}$$

$$\Leftrightarrow (a_0 + a_1 10) + 10^2(a_2 + 10a_3) + 10^4(a_4 + 10a_5) + \quad \equiv 0 \pmod{101}$$

$$\Leftrightarrow (a_0 + a_1 10) - (a_2 + 10a_3) + (a_4 + 10a_5) + \dots \equiv 0 \pmod{101}$$

$$\Leftrightarrow -(a_0 + a_1 10) + (a_2 + 10a_3) - (a_4 + 10a_5) + \dots \equiv 0 \pmod{101}$$