

Correction des exercices - Chapitre IV

Exercice 1

- 1) D'après le petit théorème de Fermat, on a $2^{12} \equiv 1 \pmod{13}$, d'où $2^{60} \equiv 1 \pmod{13}$. Par ailleurs, on a $2^5 \equiv 6 \pmod{13}$, d'où $2^{10} \equiv -3 \pmod{13}$, puis $2^{70} \equiv -3 \pmod{13}$. On a $3^3 \equiv 1 \pmod{13}$, d'où $3^{69} \equiv 1 \pmod{13}$, puis $3^{70} \equiv 3 \pmod{13}$, d'où le résultat.
- 2) On a $3 \equiv -4 \pmod{7}$. Puisque n est impair, on a donc $3^n \equiv -4^n \pmod{7}$.
- 3) D'après le petit théorème de Fermat, on a $2^{16} \equiv 1 \pmod{17}$, d'où l'assertion en élevant les deux membres de cette congruence au carré.
- 4) Si n est impair, on a $2^{n-1} \equiv 1 \pmod{3}$. Par suite, $2^n - 2 = 2(2^{n-1} - 1)$ est divisible par 6, i.e. il existe $k \in \mathbb{N}$ tel que $2^n = 6k + 2$. On a $2^6 \equiv 1 \pmod{7}$, d'où $2^{6k} \equiv 1 \pmod{7}$. On en déduit que l'on a

$$2^{2^n} + 3 = 2^{6k+2} + 3 \equiv 0 \pmod{7}.$$

Supposons $n \equiv 2 \pmod{6}$. Il existe $k \in \mathbb{N}$ tel que $n = 6k + 2$. On a $2^6 \equiv 1 \pmod{9}$, d'où $2^{6k} \equiv 1 \pmod{9}$. On a ainsi $2^{6k+2} \equiv 4 \pmod{18}$. D'après le petit théorème de Fermat, on a $2^{18} \equiv 1 \pmod{19}$, d'où $2^{2^{6k+2}} \equiv 2^4 \pmod{19}$, puis le résultat.

- 5) On a $1823 \equiv 5 \pmod{18}$. D'après le théorème d'Euler, on a $5^6 \equiv 1 \pmod{18}$. On a $242 \equiv 2 \pmod{6}$, d'où l'on déduit alors les congruences

$$1823^{242} \equiv 5^{242} \equiv 25 \equiv 7 \pmod{18}.$$

Ce procédé se justifie par le fait que 5 est inversible multiplicativement modulo 18.

- 6) Il s'agit de déterminer l'entier a compris entre 0 et 99 tel que $3^{1000} \equiv a \pmod{100}$. On a $\varphi(100) = 40$, où φ est la fonction indicatrice d'Euler. D'après le théorème d'Euler, on obtient $3^{40} \equiv 1 \pmod{100}$. Puisque $1000 = 40 \times 25$, on a donc $3^{1000} \equiv 1 \pmod{100}$, d'où $a = 1$ et le résultat.
- 7) On a $1800 = 2^3 \times 3^2 \times 5^2$. L'ordre cherché est donc $\varphi(1800) = 480$.

Exercice 2

- 1) Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est formé des éléments $\bar{a} = a + n\mathbb{Z}$ tels que a soit premier avec n . On obtient

$$(\mathbb{Z}/10\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} \quad \text{et} \quad (\mathbb{Z}/15\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}.$$

- 2) Le groupe $(\mathbb{Z}/10\mathbb{Z})^*$ est d'ordre 4. L'ordre de $\bar{3}$ dans $(\mathbb{Z}/10\mathbb{Z})^*$ est 4, donc ce groupe est cyclique. Dans $(\mathbb{Z}/15\mathbb{Z})^*$, on vérifie que $\bar{4}$, $\bar{11}$, $\bar{14}$ sont d'ordre 2 et que $\bar{2}$, $\bar{8}$, $\bar{7}$, $\bar{13}$ sont d'ordre 4. L'ordre maximum d'un élément de $(\mathbb{Z}/15\mathbb{Z})^*$ est 4, donc ce groupe n'est pas cyclique.
- 3) Le ppcm des ordres de $\bar{2}$ et $\bar{7}$ est 4. Ce n'est pas l'ordre de $\bar{14}$ qui vaut 2. Cela s'explique par le fait que le sous-groupe de $(\mathbb{Z}/15\mathbb{Z})^*$ engendré par $\bar{2}$ est $\{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}$, que celui engendré par $\bar{7}$ est $\{\bar{1}, \bar{7}, \bar{4}, \bar{13}\}$ et que l'intersection de ces deux sous-groupes n'est pas réduite à l'élément neutre.

Exercice 3

- 1) Supposons $n > m$. On a

$$F_n = (2^{2^m})^{2^{n-m}} + 1 = (F_m - 1)^{2^{n-m}} + 1 \equiv 2 \pmod{F_m}.$$

Par suite, tout diviseur commun de F_m et F_n divise 2, d'où l'assertion vu que F_m et F_n sont impairs.

- 2) C'est une conséquence de la première question et du fait que chaque nombre de Fermat est divisible par un nombre premier.
- 3) Posons $k = 2^n - 1$. On a

$$\frac{F_n - 1}{2} = 2^k \quad \text{et} \quad k \geq n.$$

Il en résulte que l'on a

$$2^{\frac{F_n - 1}{2}} = 2^{2^k} = (F_n - 1)^{2^{k-n}} \equiv (-1)^{2^{k-n}} \pmod{F_n}.$$

Par hypothèse, on a $n \geq 2$. Cela implique $k > n$ et le résultat.

- 4) On a

$$2^{2^n} \equiv -1 \pmod{p} \quad \text{et} \quad 2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Par suite, l'ordre de 2 modulo p , qui divise 2^{n+1} , est 2^{n+1} . D'après le théorème de Lagrange, 2^{n+1} divise donc $p - 1$.

Exercice 4 (Cipolla, 1904)

- 1) L'entier $(a^2)^p - 1$ est divisible par $a^2 - 1$, donc n est un entier. Par ailleurs, on a

$$n = \left(\frac{a^p - 1}{a - 1} \right) \left(\frac{a^p + 1}{a + 1} \right).$$

Ainsi n est le produit de deux entiers au moins égaux à 2, donc n est composé.

- 2) On a l'égalité

$$n - 1 = \frac{a^{2p} - a^2}{a^2 - 1}.$$

D'après le petit théorème de Fermat, on a $a^{2p} \equiv a^2 \pmod{p}$. Puisque p ne divise pas $a^2 - 1$, il en résulte que p divise $n - 1$. Vu l'égalité

$$n = (a^2)^{p-1} + \cdots + a^2 + 1,$$

$n - 1$ est la somme d'un nombre pair de termes de même parité (p est impair). Par suite, $n - 1$ est pair et $2p$ divise $n - 1$. Puisque l'on a $a^{2p} \equiv 1 \pmod{n}$, on en déduit que $a^{n-1} \equiv 1 \pmod{n}$, d'où le résultat.

Exercice 5

- 1) Posons $N = a^n - 1$ et notons d l'ordre de a modulo N . On a $a^n \equiv 1 \pmod{N}$, donc d divise n . Par ailleurs, on a $a^d \equiv 1 \pmod{N}$ i.e. $a^n - 1$ divise $a^d - 1$. En particulier, on a $n \leq d$, d'où $n = d$.
- 2) L'entier a est premier avec N . On a donc $a^{\varphi(N)} \equiv 1 \pmod{N}$ (théorème d'Euler). D'après la question précédente, cela entraîne que n divise $\varphi(N)$.

Exercice 6

Il s'agit de vérifier que 429 et 700 sont premiers entre eux et de trouver deux entiers u et v tels que $429u + 700v = 1$. L'algorithme d'Euclide fournit le tableau suivant :

	1	1	1	1	2	1	1	22	
700	429	271	158	113	45	23	22	1	0
1	0	1	-1	2	-3	8	-11	19	
0	1	-1	2	-3	5	-13	18	-31	

On en déduit que $u = -31$ et $v = 19$ conviennent, de sorte que l'inverse multiplicatif de 429 modulo 700 est -31 . Autrement dit, on a $\overline{429}^{-1} = \overline{669}$.

Exercice 7

Les entiers 31 et 53 sont premiers entre eux. Conformément à la démonstration du théorème 4.3, et à la remarque 4.3, on commence par expliciter deux entiers u et v tels que $53u + 31v = 1$. En effectuant l'algorithme d'Euclide, on trouve le tableau suivant :

	1	1	2	2	4	
53	31	22	9	4	1	0
1	0	1	-1	3	-7	
0	1	-1	2	-5	12	

On en déduit que les entiers $u = -7$ et $v = 12$ conviennent, par suite

$$c = 53u + 2(31v) = 373$$

satisfait la condition de l'énoncé. L'ensemble cherché est donc

$$\{373 + 1643k \mid k \in \mathbb{Z}\}.$$

Exercice 8

Un entier est multiple de 2, 3, 4, 5 et 6 si et seulement si il est multiple du ppcm de ces entiers i.e. de 60. Il s'agit donc de déterminer le plus petit entier naturel n vérifiant les congruences

$$n \equiv 0 \pmod{7} \quad \text{et} \quad n \equiv 1 \pmod{60}.$$

En utilisant l'algorithme d'Euclide, on obtient l'égalité $-17 \times 7 + 2 \times 60 = 1$. L'ensemble des entiers vérifiant ces congruences sont donc ceux de la forme $-119 + 420k$ où $k \in \mathbb{Z}$. L'entier cherché est ainsi 301.

Exercice 9

Le raisonnement utilisé dans la question 6 de l'exercice 1 ne s'applique pas directement, car 2 n'est pas premier avec 100. On a $2^{1000} \equiv 0 \pmod{4}$. L'idée est alors de déterminer la congruence de 2^{1000} modulo 25 et d'utiliser le théorème chinois. On a $2^{20} \equiv 1 \pmod{25}$ (th. d'Euler), d'où $2^{1000} \equiv 1 \pmod{25}$. Il en résulte que l'on a $2^{1000} \equiv -24 \equiv 76 \pmod{100}$, d'où le résultat.

Exercice 10

Il existe des entiers u et v tels que l'on ait

$$3u \equiv 1 \pmod{2^t} \quad \text{et} \quad 2v \equiv 1 \pmod{d}.$$

Parce que 2^t et d sont premiers entre eux, il existe $x \in \mathbb{Z}$ tel que l'on ait (th. chinois)

$$x \equiv -u \pmod{2^t} \quad \text{et} \quad x \equiv -v \pmod{d}.$$

On en déduit que 2^t divise $3x + 1$ et que d divise $2x + 1$. L'entier $(2x + 1)(3x + 1)$ est donc divisible par m .

Exercice 11

On a la congruence

$$2^{2p} \equiv 1 \pmod{q}.$$

Soit d l'ordre multiplicatif de 2 modulo q (q est impair). Il divise $2p$, donc d vaut 1, 2 , p ou $2p$. On a $d \neq 1$. Par ailleurs, on a $d \neq 2$ car $q \neq 3$. Si $d = p$, on obtient $2^p \equiv 1 \pmod{q}$, ce qui d'après l'hypothèse faite implique $q = 2$, d'où une contradiction. On a donc $d = 2p$. On a $2^{q-1} \equiv 1 \pmod{q}$, donc d divise $q - 1$, i.e. on a $q \equiv 1 \pmod{2p}$.

Exercice 12

Soit d l'ordre de $\bar{2}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Par hypothèse, on a $2^n \equiv 1 \pmod{p}$. Puisque p est impair, on a $2^{p-1} \equiv 1 \pmod{p}$. Ainsi, d divise n et $p-1$. D'après le caractère minimal de p , on en déduit que $d = 1$, ce qui conduit à $2 \equiv 1 \pmod{p}$, d'où une contradiction et le résultat.

Exercice 13

Parce que n est impair, on a $2^{\varphi(n)} \equiv 1 \pmod{n}$ (th. d'Euler). Par ailleurs, on a l'inégalité $\varphi(n) \leq n$, donc $\varphi(n)$ divise $n!$. On en déduit que $2^{\varphi(n)} - 1$ divise $2^{n!} - 1$: si a et b sont des entiers naturels tels que a divise b , alors $2^a - 1$ divise $2^b - 1$. Cela entraîne l'assertion.

Exercice 14

- 1.1) Soit a un élément de B . Pour tout $i = 1, \dots, r$, on a $a^2 \equiv 1 \pmod{p_i^{n_i}}$, ce qui entraîne $a^2 \equiv 1 \pmod{n}$ i.e. a est dans A . Inversement, soit a un élément de A . Le pgcd des entiers $a-1$ et $a+1$ est 1 ou 2. Puisque n est impair, pour tout $i = 1, \dots, r$, l'entier $p_i^{n_i}$ divise donc $a-1$ ou $a+1$. Par suite, a est dans B , d'où $A = B$.
- 1.2) D'après le théorème chinois, pour tout système de signes $(\varepsilon_1, \dots, \varepsilon_r)$, il existe $a \in \mathbb{Z}$, unique modulo $n\mathbb{Z}$, vérifiant les congruences

$$a \equiv \varepsilon_i \pmod{p_i^{n_i}} \quad \text{pour } i = 1, \dots, r.$$

Il y a 2^r tels systèmes de signes. L'ensemble des classes modulo $n\mathbb{Z}$ des éléments de B est donc de cardinal 2^r . Puisque l'on a $A = B$, on obtient $|S| = 2^r$.

- 2.1) Si $n = 2$, on a $S = \{\bar{1}\}$ et si $n = 4$, on a $S = \{\bar{1}, \bar{3}\}$.
- 2.2) Considérons un entier a tel que $a^2 \equiv 1 \pmod{2^t}$. Le pgcd de $a-1$ et $a+1$ est 2. Il en résulte que $a+1$ ou bien $a-1$ est divisible par 2^{t-1} . Autrement dit, on a $a \equiv \pm 1 \pmod{2^{t-1}}$. Supposons $a \not\equiv \pm 1 \pmod{2^t}$. Dans ce cas, il existe $u \in \mathbb{Z}$ impair tel que $a = \pm 1 + u2^{t-1}$, ce qui conduit à la congruence $a \equiv \pm 1 + 2^{t-1} \pmod{2^t}$, d'où le résultat annoncé.
- 3) Posons $n = 2^t d$, où d est impair. D'après le théorème chinois les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2^t\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ sont isomorphes. Le cardinal de S est donc le nombre de couples de l'anneau produit $\mathbb{Z}/2^t\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ dont le carré vaut 1. Compte tenu de ce qui précède, si r est le nombre de facteurs premiers de d , on a donc

$$|S| = \begin{cases} 2^r & \text{si } t = 0 \text{ ou } t = 1 \\ 2^{r+1} & \text{si } t = 2 \\ 2^{r+2} & \text{si } t \geq 3. \end{cases}$$

- 4) Supposons $n = 128 = 2^7$. D'après la deuxième question, on a

$$S = \{\bar{1}, \bar{63}, \bar{65}, \bar{127}\}.$$

Supposons $n = 735 = 3 \times 5 \times 7^2$. L'équation $x^2 = 1$ possède huit solutions dans l'anneau $\mathbb{Z}/735\mathbb{Z}$. Pour les trouver, il faut résoudre les huit systèmes de trois congruences (question 1)

$$x \equiv \pm 1 \pmod{3}, \quad x \equiv \pm 1 \pmod{5}, \quad x \equiv \pm 1 \pmod{49}.$$

En réalité, il suffit d'en résoudre quatre par un choix convenable de systèmes de signes, les autres solutions étant les opposées des précédentes. Il suffit donc d'examiner les triplets de signes $(1, 1, 1)$, $(1, -1, -1)$, $(1, 1, -1)$ et $(1, -1, 1)$. Indiquons dans ce qui suit des solutions particulières de ces systèmes, obtenues en utilisant l'algorithme d'Euclide.

Pour le triplet $(1, 1, 1)$, on a directement $x = 1$.

Pour le triplet $(1, -1, -1)$, on résout le système

$$x \equiv 1 \pmod{3} \quad \text{et} \quad x \equiv -1 \pmod{245}.$$

On a la relation de Bézout $82 \times 3 - 245 = 1$, d'où $x = 244$.

Pour le triplet $(1, 1, -1)$, on résout le système

$$x \equiv 1 \pmod{15} \quad \text{et} \quad x \equiv -1 \pmod{49}.$$

On a $-13 \times 15 + 4 \times 49 = 1$, d'où $x = 13 \times 15 + 4 \times 49 = 391$.

Pour le triplet $(1, -1, 1)$, on résout le système

$$x \equiv 1 \pmod{147} \quad \text{et} \quad x \equiv -1 \pmod{5}.$$

On a $-2 \times 147 + 59 \times 5 = 1$, d'où $x = 59 \times 5 + 2 \times 147 = 589$.

Il en résulte que l'on a

$$S = \{\overline{1}, \overline{146}, \overline{244}, \overline{344}, \overline{391}, \overline{491}, \overline{589}, \overline{734}\}.$$

Exercice 15 (Algorithme RSA)

- 1) On a $n = 5 \times 7$ et $\varphi(n) = 24$. Par ailleurs, on a $1 = 5 \times 5 - 24$, donc 5 est son propre inverse modulo 24. Dans ce cas, la clé secrète est donc $(5, 24)$.

On a $n = 5 \times 53$ et $\varphi(n) = 208$. Il s'agit de déterminer l'inverse de 139 modulo 208.

En utilisant l'algorithme d'Euclide, on obtient la relation

$$1 = 3 \times 139 - 2 \times 208.$$

La clé secrète est donc $(3, 208)$.

On a $n = 59 \times 61$, d'où $\varphi(n) = 3480$. On a l'égalité

$$4 \times 3480 - 449 \times 31 = 1,$$

donc l'inverse de 31 modulo 3480 est 3031. La clé secrète est ainsi $(3031, 3480)$.

2) On a $\varphi(n) = (p-1)(q-1)$ i.e. on a

$$(1) \quad 3e = 2\varphi(n) + 1,$$

donc e est premier avec $\varphi(n)$ et 3 est l'inverse de e modulo $\varphi(n)$.

3) On a $n = 11 \times 17$ et $\varphi(n) = 160$. On vérifie que l'égalité (1) est satisfaite. Par suite, l'inverse de 107 modulo 160 est 3. Le message secret m que Bob souhaite envoyer à Alice est donc

$$m = 9^3 \bmod. 187 = 168 \bmod. 187.$$
