2 Calculs dans Z/nZ

Exercice 2.1. — Nombre de Carmichael. Soit $n = 561$.

1. Montrer que pour tout a premier avec n, on a $a^n = a \pmod n$.
2. Montrer que pour tout a, on a $a^n = a \pmod n$.

Solution 2.1. — On a $561 = 3 \cdot 11 \cdot 17$, produit de 3 nombres premiers. On montre que ce résultat est vrai modulo 3, 11 et 17. Dans $\mathbf{Z}/p\mathbf{Z}$, on a $a^{p-1} = 1$ si $a \neq 0$.

Donc pour $p = 3$, on a bien $a^2 \equiv 1 \pmod 3$ donc $a^{560} \equiv 1 \pmod 3$ si 3 ne divise pas a. Par conséquent $a^{561} \equiv a \pmod 3$, qui reste vrai même si $a \equiv 0 \pmod 3$. Pour $p = 11$, on a $a^{10} \equiv 1 \pmod{11}$ donc $a^{560} \equiv 1 \pmod{11}$ si $a \not\equiv 0 \pmod{11}$ et au final $a^{561} = a \pmod{11}$ pour tout a. De la même façon pour $p = 17$.

En fait on a utilisé le fait que $p-1$ divise $n-1$ dans le cas où p est un nombre premier divisant $n = p_1 \cdot p_2 \cdot p_3$. 561 est le plus petit entier ayant cette propriété, c'est un *nombre de Carmichaël*.

Exercice 2.2. — Soit $n = p_1 \cdots p_k$ un entier sans facteur carré et $k \geq 3$.

1. Que vaut $\varphi(n)$?
2. Montrer que tout $x \in (\mathbf{Z}/n\mathbf{Z})^*$ vérifie $x^{1/2\varphi(n)} = 1$. En déduire que $(\mathbf{Z}/n\mathbf{Z})^*$ n'est pas cyclique.
3. Montrer que pour tout x premier avec n, on a $x^{\varphi(n)} \equiv 1 \pmod n$.
4. Montrer que pour tout $\lambda \equiv 1 \pmod{\varphi(n)}$, et tout x premier avec n, on a $x^\lambda \equiv x \pmod n$.
5. Montrer que pour tout $x \in \mathbf{Z}$, on a $x^\lambda \equiv x \pmod n$.

Exercice 2.3. — Ordres
Pour chacun de ces groupes, écrire l'inverse et l'ordre des éléments : $(\mathbf{Z}/18\mathbf{Z}, +)$, $\mathbf{Z}/26\mathbf{Z}^*$, $\mathbf{Z}/31\mathbf{Z}^*$.

Solution 2.3. —

1. $\mathbf{Z}/18\mathbf{Z}$ est cyclique donc l'ordre de tout élément divise 18. On sait par ailleurs qu'il y a $\varphi(d)$ éléments d'ordre d, ce sont les $a\frac{n}{d}$ tels que $(a,d) = 1$ et $0 < a < d$. Une autre façon est d'utiliser le fait que $\operatorname{ord}(a) = \dfrac{18}{(a,18)}$. On obtient donc

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\operatorname{ord}(a)$	1	18	9	6	9	18	3	18	9	2	9	18	3	18	9	6	9	18

2. Les inversibles de $\mathbf{Z}/26\mathbf{Z}$ sont $\{1,3,5,7,9,11,15,17,19,21,23,25\}$. Il y en a $\varphi(26) = 12$. Donc l'ordre de tout élément divise 12. On sait que 1 est d'ordre 1, -1 d'ordre 2. Calculons l'ordre de 3. On a $3^2 = 9$, $3^4 = 81 = 3$ donc $3^3 = 1$ et $\operatorname{ord}(3) = \operatorname{ord}(3^2) = 3$. -3 est d'ordre 6 comme produit d'éléments d'ordre 2 et 3. On a ensuite $7^2 = 49 = -3$, donc 7 est d'ordre 12 car $7^6 = -1$ et $7^4 = 9$. $\mathbf{Z}/26\mathbf{Z}^*$ est cyclique engendré par 7 et $\operatorname{ord}(7^i) = \dfrac{12}{(i,12)}$. On a

i	0	1	2	3	4	5	6	7	8	9	10	11
7^i	1	7	23	5	9	11	25	19	3	21	17	15
$\operatorname{ord}(7^i)$	1	12	6	4	3	12	2	12	3	4	6	12

On aurait pu se douter que $\mathbf{Z}/26\mathbf{Z}^*$ était cyclique car il est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^* \times (\mathbf{Z}/13\mathbf{Z})^* \sim (\mathbf{Z}/13\mathbf{Z})^*$.

3. $\mathbf{Z}/31\mathbf{Z}^*$ est cyclique car 31 est premier. Trouvons un élément d'ordre 30. On a $2^5 \equiv 1 \pmod{31}$ donc 2 est d'ordre 5. On a $3^2 = 9$, $3^4 = 19 = -12$, donc $3^3 = -2^2$ est d'ordre 10. L'ordre de 3 est donc un multiple de 10. Mais $3^9 = -2^8 = -8$ donc $3^{10} = 25$. On déduit que 3 est d'ordre 30.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
3^i	1	3	9	27	19	26	16	17	20	29	25	13	8	24	10
$\mathrm{ord}(3^i)$	1	30	15	10	15	6	5	30	15	10	3	30	5	30	15
i	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
3^i	30	28	22	4	12	5	15	14	11	2	6	18	23	7	21
$\mathrm{ord}(3^i)$	2	15	30	5	30	3	10	15	30	5	6	15	10	15	30

Exercice 2.4. — Soit G un groupe commutatif. Montrer que si a est d'ordre n et b est d'ordre m avec $(n,m) = 1$, alors ab est d'ordre nm. Montrer que si G n'est plus commutatif ce résultat ne subsiste pas.

Solution 2.4. — On a $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = 1$, donc $\mathrm{ord}(ab) | nm$. Sinon, en posant $a^d = b^{-d} = c$, l'ordre de c divise l'ordre de a et l'ordre de b donc $c = 1$. Mais alors n et m divisent d donc, d'après le lemme de Gauss, nm divise d si $(ab)^d = 1$.

Par exemple, dans le groupe $\mathcal{S}_3$. Le produit de $\tau = (12)$ et du cycle $c = (123)$ donne le 3 cycle (123) d'ordre 3.

Par exemple dans $M_2(\mathbf{Q})$, le produit de la symétrie $S = \begin{pmatrix} a & 1-a \\ 1+a & -a \end{pmatrix}$ et de la matrice compagnon de Φ_2 : $M = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, d'ordre 3 vaut $SM = \begin{pmatrix} 1-a & -1 \\ -1+a & -1 \end{pmatrix}$ dont la trace vaut $-a$. Lorsque $|a| > 2$, cette matrice ne peut être d'ordre fini.

Exercice 2.5. —

1. Soit G un groupe d'ordre N. Montrer que g est d'ordre N si et seulement si pour tout diviseur premier p de N, on a $g^{N/p} \neq 1$.
2. Calculer la complexité du test : g est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$, supposant que l'on sait factoriser $p-1$.
3. Quel est la probabilité que g soit un générateur ? Trouver une estimation du temps moyen nécessaire à trouver un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$.
4. Trouver un générateur des groupes $(\mathbf{Z}/p\mathbf{Z})^*$, pour p premier de 11 à 41. On pourra commencer par 2, puis 3 et utiliser également l'exercice 2.4.

Solution 2.5. —

1. Si g est un générateur alors N est le plus petit entier positif, tel que $g^k = 1$. En particulier $g^{N/p} \neq 1$. Si g est d'ordre d strictement inférieur à N, alors il existe un diviseur premier p à N/d (donc un diviseur de N), c'est-à-dire, $d \mid N/p$ et $g^{N/p} = 1$.
2. Soit $N = p-1$ que l'on a factorisé. Si p_i est un diviseur premier de N, on calcule g^{N/p_i} en $O(\log N/p_i)$ opérations dans $\mathbf{F}_p$, soit en un temps $O((\log N)^3/\log p_i)$. Auparavant on aura calculé N/p_i en base 2 en $O((\log N/p_i)^2)$ opérations binaires. Au total on teste si g est primitif en $O((\log N)^4)$ opérations.
3. (a) $p = 11$. On voit que $2^5 = -1$ et $2^2 = 4$ donc 2 est d'ordre 10 (d'après 1).
   (b) $p = 13$. On voit que $2^4 = 3$ et $2^6 = -1$ donc 2 est d'ordre 12 (d'après 1).
   (c) $p = 17$. On voit que $2^2 = 4$, $2^4 = -1$ donc 2 est d'ordre 8. Essayons 3. $3^2 = 9$, $3^4 = 81 = -2^2$ est donc d'ordre 4 et 3 est d'ordre 16.
   (d) $p = 19$. On voit que $2^4 = -3$, $2^8 = 9$, $2^9 = -1$. Donc 2 est d'ordre 18 (d'après la première question).
   (e) $p = 23$. On voit que $2^5 = 9$, $2^{10} = 12$, donc $2^{11} = 1$. 2 est d'ordre 11 donc $-2 = 17$ est d'ordre 22 (d'après 2.4).

(f) $p = 29$. On voit que $2^4 \neq 1$ et $2^5 = 3$, donc $2^{15} = -2$, donc $2^{14} = -1$. 2 est d'ordre 28 (d'après 1).

(g) $p = 31$. On voit que $2^5 = 1$. Donc 2 est d'ordre 5. On a $3^3 = -4$. Donc $3^{15} = -1$ et $3^6 = 16$ et $3^9 = -1$, soit $3^{10} \neq 1$. 3 est d'ordre 30 (d'après 1).

(h) $p = 37$. On voit que $2^5 = -5$ donc $2^{10} = 25$ et $2^6 = -10 = 27 = 3^3$ et $2^{12} = -11$. Mais alors $2^{18} = 110 = -1$. 2 est d'ordre 36 (d'après 1).

(i) $p = 41$. On voit que $2^5 = -3^2$. $2^{10} = 81 = -1$ donc $2^{20} = 1$. D'ailleurs 2 est d'ordre 20. Donc $3^4 = -1$ et 3 est d'ordre 8. Mais alors $2^4 = 16$ est d'ordre 5 et donc $3 \cdot 16 = 7$ est d'ordre 40, (d'après 2.4).

Exercice 2.6. — Soit $p = 31$ et $q = 37$ et $n = p \cdot q$.

1. Calculer $\varphi(n)$.
2. Bob choisit l'algorithme RSA pour recevoir des messages (modulo n) et publie la clé publique $(n, e = 11)$.
   (a) Montrer que $x^{ed} = x$ pour tout $x \in \mathbf{Z}/n\mathbf{Z}$ si et seulement si $ed \equiv 1 \pmod{180}$.
   (b) Trouver d tel que $ed \equiv 1 \pmod{180}$.

Solution 2.6. —

1. On a $\varphi(n) = 30 \cdot 36 = 1080$.
2. (a) $x^{ed} = x$ si et seulement si $x^{ed} = x \pmod{p}$ et $x^{ed} = x \pmod{q}$, pour tout x. Mais dans le corps $\mathbf{Z}/p\mathbf{Z}$, $x^m = x$ si $x = 0$ ou si x est d'ordre $p-1$ si $(p-1)$ divise m. Dans $\mathbf{Z}/q\mathbf{Z}$, $x^m = x$ pour rout x si $(q-1)$ divise $m-1$. La condition est donc que le ppcm de $(p-1)$ et de $(q-1)$ divise m. Ce ppcm vaut 180.
   (b) On effectue l'algorithme d'Euclide entre 11 et 180. On obtient : On a $180 = 1 \times 180 + 0 \times 11$, $11 = 0 \times 180 + 1 \times 11$, puis $4 = 1 \times 180 - 16 \times 11$, $-1 = -3 \times 180 + 49 \times 11$, On trouve donc, $(-49) \times 11 \equiv 1 \pmod{180}$ et $d = 180 - 49 = 131$ convient.

Exercice 2.7. — Afin de communiquer en utilisant le protocole RSA, Alice choisit (et publie) la clé publique $(e, n) = (37, 65)$.

1. Déterminer la clé secrète.
2. Déterminer toutes les clés de déchiffrement $(r, \varphi(n))$ avec $0 < r < \varphi(n)$.
3. Alice réalise avoir fait un très mauvais choix. Pourquoi ?

Solution 2.7. —

1. On a $\varphi(n) = 4.12 = 48$. De la relation de Bézout $13.37 - 10.48 = 1$, on tire que la clé secrète est 13 .
2. Une clé de déchiffrement est un entier r tel que $x^{er} = x$ pour tout $x \in \mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$. Il est équivalent de dire que $er \equiv 1 \pmod{()(p-1, q-1)}$. Ici, $37r \equiv 1 (\bmod 12)$, ou $r \equiv 1 (\bmod 12)$, ou $r \in \{1, 13, 25, 37\}$.
3. En fait $d = 37 \equiv 1 (\bmod 12)$. Les messages ne sont pas chiffrés du tout !