ARITHMÉTIQUE

par

Christian Maire

ECOLE MATHÉMATIQUE AFRICAINE
RÉPUBLIQUE DU CONGO - BRAZZAVILLE
JUILLET 2025

Table des matières

Partie I. Nombres entiers	3
1. Divisibilité.....	3
1.1. Division euclidienne.....	3
1.2. Relation de Bézout et algorithme d'Euclide.....	4
1.3. Nombres premiers.....	7
1.4. Normes.....	9
1.5. Exercices.....	11
2. Congruences.....	12
2.1. L'ensemble $\mathbb{Z}/n\mathbb{Z}$	12
2.2. Congruences simultanées.....	13
2.3. $\mathbb{Z}/n\mathbb{Z}$ et ses lois.....	14
2.4. Le groupe multiplicatif.....	16
2.5. Exercices.....	17
Partie II. Corps finis	19
3. Sous-corps premiers.....	19
3.1. Anneau commutatif.....	19
3.2. Les corps $\mathbb{F}_p$ et $\mathbb{Q}$	19
4. Structure multiplicative.....	20
5. Logarithme discret.....	21
6. Polynômes.....	21
7. Le corps $\mathbb{F}_q$	22
7.1. Sur l'existence.....	22
7.2. Existence et unicité.....	23
7.3. Structure multiplicative.....	24
8. L'automorphisme de Frobenius.....	24
9. Polynômes primitifs.....	26
10. Exercices.....	26
Partie III. Un peu de cryptographie	28
11. Quelques chiffrements classiques.....	28
11.1. Chiffrement de Vigenère.....	28
11.2. Chiffrement de Hill.....	29
12. Le protocole de Diffie-Hellman.....	30
13. Le protocole RSA (Rivest-Shamir-Adelman).....	31
14. Exercices.....	32
Partie IV. Appendice	33
Rappels sur groupes.....	33
Ordre d'un élément.....	34
Groupes cycliques.....	34

Le théorème de Lagrange..... 35

PARTIE I

NOMBRES ENTIERS

On notera par

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ l'ensemble des entiers naturels,
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ l'ensemble des entiers (relatifs),
- $|a| = \max\{a, -a\}$ la valeur absolue du nombre réel a .

On rappelle que $(\mathbb{Z}, +, \cdot)$ est un anneau avec ± 1 comme éléments inversibles (voir la définition 3.1 de la section IV).

1. Divisibilité

1.1. Division euclidienne. —

Définition 1.1. — Soient $a, b \in \mathbb{Z}$. On dit que a divise b , ou que a est un diviseur de b , ou que b est un multiple de a , si $b = ac$ pour un certain $c \in \mathbb{Z}$. On note alors $a|b$.

Exemple 1.2. — 0 est le seul multiple de 0, et 0 est le multiple de tout entier.

Exemple 1.3. — Les entiers 1 et -1 divisent tout entier $a \in \mathbb{Z}$. En effet, $a = 1 \times a$ et $a = (-1) \times (-a)$.

Exemple 1.4. — L'entier a est dit pair quand 2 divise a . L'entier a est dit impair si il n'est pas pair.

Remarque 1.5. — Si $a|b$ alors $\pm a | \pm b$.

Remarque 1.6. — Soit un entier $b > 0$. Alors tout diviseur de b est compris entre $-b$ et b , par conséquent tout entier $b \neq 0$ a un nombre fini de diviseurs. Par contre tout entier est diviseur de l'entier $b = 0$. Enfin, $0|a$ si et seulement si, $a = 0$.

Enonçons quelques propriétés.

Proposition 1.7. — Soient trois entiers $a, b, c \in \mathbb{Z}$. On a les propriétés suivantes :

- (i) Si $a | b$ et $b | c$ alors $a | c$.
- (ii) Si $a | b$ alors $ac | bc$.
- (iii) Si $a | b$ et $a | c$ alors $a|(xb + yc)$ pour tout entier x, y .
- (iv) Si $a | b$ et $b | a$, alors $a = \pm b$.

Démonstration. — (i) Par hypothèse il existe $\alpha, \beta \in \mathbb{Z}$ tels que $b = \alpha a$ et $c = \beta b$. Ainsi $c = \alpha\beta a$ ce qui signifie que $a|c$.

(ii) Par hypothèse $b = \alpha a$ pour un certain $\alpha \in \mathbb{Z}$. Ainsi $bc = \alpha ac$, ce qui signifie que $ac|bc$.

(iii) On écrit $b = \alpha a$ et $c = \beta a$ avec $\alpha, \beta \in \mathbb{Z}$. Alors $xb + yc = a(x\alpha + y\beta)$, et ainsi $a|(xb + yc)$.

(iv) Par hypothèse il existe deux entiers $\alpha, \beta \in \mathbb{Z}$ tels que $b = \alpha a$ et $a = \beta b$. Par conséquent, $b = \alpha\beta b$ puis $b(1 - \alpha\beta) = 0$. Si $b = 0$, alors $a = 0$; sinon $b \neq 0$ et on en déduit que $\alpha\beta = 1$, puis que $\alpha = \pm 1$ (se rappeler que $\alpha, \beta \in \mathbb{Z}$). □

Le théorème suivant joue un rôle très important pour toute la suite.

Théorème 1.8 (Division euclidienne). — Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$. Il existe $q, r \in \mathbb{Z}$ tels que $b = aq + r$, avec $0 \leq r < |a|$. De plus, sous ces conditions, les éléments q et r sont uniques. On dit que l'entier r est le reste de la division de b par a et l'entier q est le quotient.

Démonstration. — *Existence.* On peut noter que le principe de la division euclidienne est immédiat si $a|b$ (avec $r = 0$ alors).

- Supposons $a, b \geq 0$. Soit q le plus petit entier naturel tel que $qa \leq b < (q+1)a$. On pose alors $r = b - qa < a$.

- Si $a < 0$ et $b > 0$. D'après le premier point, on effectue la division euclidienne de b par $-a$: il existe deux entiers q et r avec $0 \leq r < -a$ tels que $b = q(-a) + r$, c'est à dire tels que $b = -qa + r$; ici le quotient est $-q$ et le reste r est bien strictement plus petit que $|a|$.

- Si $a < 0$ et $b \leq 0$. On effectue la division euclidienne de $-b$ par $-a$: il existe deux entiers q et r avec $0 \leq r < -a$, tels que $-b = -qa + r$. On rappelle qu'ici $r = 0$ si et seulement si $\pm a \mid \pm b$ et donc en particulier si et seulement si $a \mid b$. Ainsi, d'après la remarque du début de la preuve, on peut supposer $r > 0$. Alors on écrit $-b = (-q-1)a + a + r$, ou encore $b = (q+1)a - a - r$. On note alors que $0 < -a - r < -a = |a|$.

- Si $a > 0$ et $b \leq 0$. D'après le point précédent, on effectue la division euclidienne de b par $-a$. Il existe deux entiers q et r avec $0 \leq r < -a$, tels que $-b = -qa + r$; ici le quotient est $-q$ et le reste r est bien strictement plus petit que $|a|$.

Unicité. Ecrivons $b = qa + r = q'a + r'$ avec $0 \leq r, r' < |a|$. On a alors $-|a| < a(q - q') = r' - r < |a|$: en d'autres termes l'entier $a(q - q')$ est un multiple de a compris strictement entre $-|a|$ et $|a|$, il est donc égal à 0. Comme a est non nul, on en déduit que $q = q'$, puis que $r = r'$. $\square$

On a alors

Corollaire 1.9. — *L'entier non nul a divise b si et seulement si le reste de la division euclidienne de b par a est nul.*

1.2. Relation de Bézout et algorithme d'Euclide. —

1.2.1. PGCD. —

Définition 1.10. — Soient a et b deux entiers non nuls. Le Plus Grand Commun Diviseur (PGCD) de a et de b est le plus grand entier d qui divise a et b . On le note $d = \text{pgcd}(a, b)$.

Le plus petit commun multiple (PPCM) à a et b est le plus petit entier m multiple de a et de b . On le note $\text{ppcm}(a, b)$.

Remarque 1.11. — On a $\text{pgcd}(\pm a, \pm b) = \text{pgcd}(a, b)$.

Remarque 1.12. — Il est possible d'étendre la définition du PGCD au cas où $b = 0$ par exemple. Ainsi, si $a \neq 0$, on a $\text{pgcd}(a, 0) = |a|$.

Exemple 1.13. — Les diviseurs positifs de 12 sont 1, 2, 3, 4, 6, 12 et ceux de 18 sont 1, 2, 3, 6, 9, 18. Ainsi, $\text{pgcd}(12, 18) = 6$.

Définition 1.14. — Deux entiers non nuls a et b sont dit premiers entre eux si $\text{pgcd}(a, b) = 1$. On dit aussi que a est premier à b (ou que b est premier à a).

1.2.2. *Relation de Bézout.* — Si $a_1, \dots, a_n$ désignent n entiers, on note par $a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$ le sous-ensemble de $\mathbb{Z}$ suivant :

$$a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = \{a_1x_1 + \dots + a_nx_n, x_1, \dots, x_n \in \mathbb{Z}\}.$$

Remarquons que $a\mathbb{Z}$ est exactement l'ensemble des multiples de a .

Proposition 1.15. — *Soient deux entiers a et b . Alors $b\mathbb{Z} \subset a\mathbb{Z}$ si et seulement si $a|b$.*

Démonstration. — En effet, si $b\mathbb{Z} \subset a\mathbb{Z}$ alors comme $b \in b\mathbb{Z}$, on a que $b \in a\mathbb{Z}$: l'élément b est un multiple de a ou encore $a|b$. La réciproque est immédiate : si $a|b$, il existe $c \in \mathbb{Z}$ tel que $b = ac$. Ainsi $b\mathbb{Z} = ac\mathbb{Z} \subset a\mathbb{Z}$. $\square$

On peut remarquer le lemme suivant

Lemme 1.16. — Soient $c, c' \in a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$. Alors $\alpha c + \beta c' \in a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$, pour tout $\alpha, \beta \in \mathbb{Z}$. En particulier, $(\alpha c + \beta c')\mathbb{Z} \subset a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$.

Démonstration. — C'est immédiat. □

On a alors une seconde proposition.

Proposition 1.17. — Soient a et b deux entiers. Alors $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$ pour un certain $m \in \mathbb{Z}$. De plus pour un tel entier m , il vient $m|a$ et $m|b$.

Démonstration. — Si $a = b = 0$, prendre $m = 0$. Sinon, soit $m > 0$ le plus petit entier *strictement* positif appartenant à $a\mathbb{Z} + b\mathbb{Z}$. Soit alors $n \in a\mathbb{Z} + b\mathbb{Z}$. Regardons la division euclidienne de n par m : il existe q, r dans $\mathbb{Z}$ avec $0 \leq r < m$, tels que $n = qm + r$. Ainsi, $r = n - qm \in a\mathbb{Z} + b\mathbb{Z}$ d'après le lemme 1.16. Par minimalité de m , on en déduit $r = 0$, et ainsi $n \in m\mathbb{Z}$. Nous venons de montrer que $a\mathbb{Z} + b\mathbb{Z} \subset m\mathbb{Z}$. Comme $m \in a\mathbb{Z} + b\mathbb{Z}$, l'inclusion inverse se déduit du lemme 1.16. Au final, on a bien $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$. Pour la seconde partie du lemme, on note que $a \in a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$: il existe $\alpha \in \mathbb{Z}$ tel que $a = m\alpha$, ce qui signifie que $m|a$. Idem pour b . □

Au passage, remarquons que par récurrence, on a la proposition suivante :

Proposition 1.18. — Soient n entiers $a_1, \dots, a_n$. Alors $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = m\mathbb{Z}$ pour un certain entier m .

On peut montrer le théorème suivant

Théorème 1.19. — Soient a, b deux entiers non nuls. Alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, où $d = \text{pgcd}(a, b)$.

Démonstration. — On sait que $d|a$ et que $d|b$, ainsi d'après la proposition 1.15, il vient $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$. De plus, d'après la proposition 1.17, il vient $a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}$ pour un certain entier $m > 0$; par la proposition 1.15, on a alors $d|m$: ainsi il existe $\alpha \in \mathbb{Z}$ tel que $m = \alpha d$. On peut remarquer que $\alpha \geq 1$ car positif non nul. Mais comme $m|a$ et $m|b$ (d'après la proposition 1.17), on en déduit que $m \leq d$ (par définition de d). Ainsi, de $\alpha d \leq d$, on obtient que $\alpha = 1$ puis que $m = d$. □

Corollaire 1.20. — Si a et b sont deux entiers non nuls et si m est tel que $m|a$ et $m|b$, alors $m|\text{pgcd}(a, b)$.

Démonstration. — Comme $m|a$ et $m|b$, alors $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset m\mathbb{Z}$, ce qui implique que $m|d$ d'après la proposition 1.15. □

Corollaire 1.21 (Relation de Bézout). — Soient a et b deux entiers non nuls. Soit $d = \text{pgcd}(a, b)$. Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$. En particulier, a et b sont premiers entre eux si et seulement si, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Démonstration. — La première partie se déduit immédiatement du théorème 1.19.

Il reste à montrer une partie de l'équivalence. Supposons l'existence d'une relation de Bézout de la forme $au + bv = 1$. Alors, $1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et donc $d = 1$. □

Corollaire 1.22 (Lemme de Gauss). — Soient a et b deux entiers premiers entre eux et soit $c \in \mathbb{Z}$. Si $a|bc$, alors $a|c$.

Démonstration. — Comme $\text{pgcd}(a, b) = 1$, on a la relation de Bézout $au + bv = 1$ pour deux entiers u et v . Alors $auc + bvc = c$. Comme $a|bc$ et $a|auc$, d'après la proposition 1.7 (iii) on en déduit que $a|c$. □

Corollaire 1.23. — Soient a et b deux entiers premiers entre eux divisant c . Alors $ab|c$.

Démonstration. — On écrit la relation de Bézout $au + bv = 1$ avec $u, v \in \mathbb{Z}$. Alors

$$c = c \times 1 = cau + cbv.$$

Comme $a|c$ et $b|c$, on écrit également $c = a\alpha$ et $c = b\beta$, avec $\alpha, \beta \in \mathbb{Z}$. Et ainsi on trouve

$$c = b\beta au + aabv = ab(u\beta + v\alpha),$$

ce qui signifie exactement que $ab|c$. □

Corollaire 1.24. — Soient trois entiers a, b, c tels que $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$. Alors $\text{pgcd}(a, bc) = 1$.

Démonstration. — On écrit les relations de Bézout $au + bv = 1$ et $au' + cv' = 1$ avec $u, u', v, v' \in \mathbb{Z}$, puis on les multiplie pour arriver à

$$a(auu' + cuv' + bu'v) + bcvv' = 1,$$

qui indique, d'après le corollaire 1.21, que $\text{pgcd}(a, bc) = 1$. □

Corollaire 1.25. — Soient a et b deux entiers non nuls. Alors l'équation diophantienne $ax + by = k$ a des solutions entières x et y si et seulement si, $\text{pgcd}(a, b)|k$.

Démonstration. — Soit $d = \text{pgcd}(a, b)$.

Supposons que x et y satisfont la relation $ax + by = k$. Alors $k \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et donc $k\mathbb{Z} \subset d\mathbb{Z}$. Par la proposition 1.15, on en déduit que $d|k$.

Réciproquement, supposons que $d|k$. Alors il existe $\alpha \in \mathbb{Z}$ tel que $k = d\alpha$. En utilisant la relation de Bézout, il vient $k = d\alpha = au\alpha + bv\alpha$, et ainsi le couple $(x, y) = (u\alpha, v\alpha)$ est solution de l'équation diophantienne considérée. □

1.2.3. *Algorithme d'Euclide.* — L'algorithme d'Euclide va reposer sur le lemme suivant

Lemme 1.26. — Soient a et b deux entiers non nuls. Si $b = aq + r$, alors $\text{pgcd}(a, b) = \text{pgcd}(a, r)$, avec la convention que $\text{pgcd}(a, 0) = |a|$.

Démonstration. — Il suffit alors de vérifier que l'ensemble des diviseurs communs à a et b coïncide avec l'ensemble des diviseurs communs à a et r . En effet, si $d|a$ et $d|b$ alors d'après la proposition 1.7 (iii), $d|(a - bq)$, c'est à dire que $d|r$. Par contre si $d|a$ et $d|r$, alors toujours suivant la proposition 1.7, $d|(bq + r)$ et donc $d|b$. □

Ce lemme indique que si l'on part de la division euclidienne de b par a , alors $\text{pgcd}(b, a) = \text{pgcd}(a, r)$ avec $r < |a|$: on a remplacé b par r qui est plus petit. On propose de continuer ce processus pour aboutir au calcul du PGCD de deux entiers (c'est l'algorithme d'Euclide).

Soient deux entiers non nuls a et b . Posons $a_1 = b$, $a_2 = a$ et considérons a_3 le reste de la division euclidienne de a_1 par a_2 . Alors d'après le lemme 1.26, $\text{pgcd}(b, a) = \text{pgcd}(a_1, a_2) = \text{pgcd}(a_2, a_3)$, avec $0 \leq a_3 < a_2 < |a|$. On continue le processus pour obtenir une suite $(a_n)_n$, où a_{n+2} est le reste de la division euclidienne de a_n par a_{n+1} et où $0 \leq a_{n+1} < \dots < |a|$. La suite d'entiers positifs $(a_n)_n$ est donc strictement décroissante et minorée par 0 : il existe n_0 tel que $a_{n_0} = 0$. Le lemme 1.30 indique alors que $\text{pgcd}(b, a) = \text{pgcd}(a_1, a_2) = \text{pgcd}(a_2, a_3) = \dots = \text{pgcd}(a_{n_0-1}, a_{n_0}) = a_{n_0-1}$. Ainsi le PGCD de a et b est le dernier entier non nul de la suite (a_n) .

Montrons alors comment l'algorithme d'Euclide donne aussi une relation de Bézout. Notons $d = \text{pgcd}(a, b) = a_{n_0-1}$. Alors par définition, $a_{n_0-3} = q_{n_0-2}a_{n_0-2} + d$ pour un certain entier q_{n_0-2} , ce qui donne la relation de Bézout $a_{n_0-3} - q_{n_0-2}a_{n_0-2} = d$, ici se rappeler que $\text{pgcd}(a_{n_0-3}, a_{n_0-2}) = d$. Toujours par définition, $a_{n_0-4} = q_{n_0-3}a_{n_0-3} + a_{n_0-2}$ pour un certain entier q_{n_0-3} et ainsi $a_{n_0-2} = a_{n_0-4} - q_{n_0-3}a_{n_0-3}$. On reporte dans l'égalité précédente pour arriver à

$$-a_{n_0-4}q_{n_0-2} + a_{n_0-3}(1 + q_{n_0-2}q_{n_0-2}) = d,$$

ce qui est exactement une relation de Bézout entre a_{n_0-4} et a_{n_0-3} . On continue ainsi ce processus pour arriver à une relation de Bézout entre a et b .

Exemple 1.27. — Prenons $b = 63$ et $a = 5$. La division euclidienne de 63 par 5 s'écrit

$$63 = 12 \times 5 + 3.$$

On effectue ensuite la division euclidienne de 5 par 3 pour arriver à

$$5 = 3 \times 1 + 2.$$

Puis ensuite la division euclidienne de 3 par 2

$$3 = 2 \times 1 + 1,$$

et enfin la division euclidienne de 2 par 1

$$2 = 2 \times 1 + 0.$$

Le dernier reste non nul est donc $d = 1$, c'est donc égal à $\text{pgcd}(63, 5)$.

On "remonte" maintenant les relations de Bézout en substituant les restes. On part de $1 = 3 - 2$ et on substitue le reste $r = 2$. Alors on obtient

$$1 = 3 - 2 = 3 - (5 - 3) = 3 \times 2 - 5$$

qui est une relation de Bézout entre 3 et 5. Puis on substitue le reste $r = 3$ pour obtenir

$$1 = 3 \times 2 - 5 = 2 \times (63 - 12 \times 5) - 5 = 2 \times 63 + 5(-2 \times 12 - 1) = 2 \times 63 - 25 \times 5.$$

On a donc ainsi obtenu la relation de Bézout suivante entre a et b :

$$2b - 25a = 1.$$

1.3. Nombres premiers. —

1.3.1. Factorisation. —

Définition 1.28. — Un entier $p > 1$ est un nombre premier si les seuls diviseurs positifs de p sont 1 et p .

Exemple 1.29. — Les entiers $2, 3, 5, 7, \dots$ sont des nombres premiers.

Commençons par donner le lemme d'Euclide.

Lemme 1.30. — Soient $a, b \in \mathbb{Z}$ et soit p un nombre premier. Si $p|ab$, alors $p|a$ ou $p|b$.

Démonstration. — Comme les seuls diviseurs positifs de p sont 1 et p , on a ou bien $\text{pgcd}(a, p) = 1$ ou bien $\text{pgcd}(a, p) = p$.

Si $\text{pgcd}(a, p) = 1$, alors d'après le lemme de Gauss 1.22, $p|b$.

Si $\text{pgcd}(a, p) = p$, alors $p|a$. □

Théorème 1.31 (fondamental de l'arithmétique). — Tout entier non nul n est, au signe près, le produit de nombres premiers uniquement déterminés à l'ordre près. Ou encore l'entier n s'écrit

$$n = \pm p_1^{n_1} \cdots p_k^{n_k},$$

où les p_i sont des nombres premiers deux à deux différents et où les n_i sont des entiers plus grand que 1. Les entiers n_i sont uniques.

Démonstration. — *Existence.* On montre la propriété par récurrence sur n . Si $n = 2$, c'est vrai (2 est un nombre premier). Supposons que tout nombre plus petit que n s'écrit comme produit de nombres premiers. Regardons $n + 1$. Alors si $n + 1$ est un nombre premier, la propriété est vraie à l'ordre $n + 1$. Si $n + 1$ n'est pas premier, il existe $a, b \geq 2 \in \mathbb{N}$ tels que $n + 1 = ab$; en particulier $a, b \leq n$. On leur applique l'hypothèse de récurrence, pour obtenir que finalement $n + 1$ s'écrit bien comme produit de nombres premiers..

Unicité. Là aussi, on raisonne par récurrence. C'est vrai pour $n = 2$ et l'on suppose que c'est vrai pour tout entier plus petit que n . On écrit alors $n + 1 = p_1^{n_1} \cdots p_k^{n_k} = q_1^{m_1} \cdots q_l^{m_l}$, où les p_i et q_j sont des

nombre premiers, deux à deux distincts pour les p_i (de même pour les q_j), $n_i, m_j \geq 1$. Par le lemme d'Euclide 1.30, le nombre premier p_1 divise l'un des nombres premiers q_i ; comme q_i est un nombre premier il vient $p_1 = q_i$; quitte à reprendre la numérotation on suppose que $p_1 = q_1$. On simplifie par p_1 pour arriver à l'égalité

$$\frac{n+1}{p_1} = p_1^{n_1-1} p_2^{n_2} \cdots p_k^{n_k} = q_1^{m_1-1} q_2^{m_2} \cdots q_l^{m_l}.$$

Comme $(n+1)/p_1 < n$, l'hypothèse de récurrence s'applique et l'on en déduit l'unicité souhaitée : on a $k = l$ et quitte à reprendre la numérotation, il vient $n_i = m_i$, pour $i = 1, \dots, k$. $\square$

Théorème 1.32. — *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

Démonstration. — Supposons l'ensemble $\mathbb{P}$ des nombres premiers fini. Notons par $\mathbb{P} = \{p_1, \dots, p_k\}$ cet ensemble. Posons alors $N = p_1 \times \cdots \times p_k$ l'entier égal au produit de ces nombres, et soit $n = N + 1$. Soit $p \in \{p_1, \dots, p_k\}$ un nombre premier divisant n . Il existe un entier b tel que $bp = n = N + 1 = p_1 \cdots p_k + 1$. On obtient alors $p(b - N/p) = 1$, où $N/p \in \mathbb{N}$ car p est l'un des p_i . On a donc obtenu que $p|1$, ce qui est absurde. $\square$

1.3.2. *Un résultat de divisibilité.* — Le théorème suivant est bien connu, il nous sera utile par la suite.

Théorème 1.33 (Petit théorème de Fermat). — *Soit p un nombre premier. Pour tout entier a , le nombre p divise $a^p - a$.*

Démonstration. — Montrons le par récurrence pour $a \geq 0$. C'est vrai pour $a = 0$. Regardons alors $(a+1)^p - (a+1)$. Par la formule du binôme de Newton, on a $p \mid ((a+1)^p - (a^p + 1))$. Par l'hypothèse de récurrence, $p \mid (a^p - a)$, ainsi par la proposition 1.7 (iii), $p \mid ((a+1)^p - (a^p + 1) + a^p - a)$, c'est à dire $p \mid ((a+1)^p - (a+1))$.

Ainsi la relation de divisibilité est vraie pour $a \geq 0$, ce qui implique facilement qu'elle est vraie pour tout $a \in \mathbb{Z}$. $\square$

1.3.3. *Pour aller un peu plus loin.* — Nous allons quantifier l'infinitude des nombres premiers.

Commençons par donner une autre preuve de l'infinitude de $\mathbb{P}$. Tout d'abord rappelons que la série $\sum_{n \geq 1} \frac{1}{n}$

diverge. Cela se voit en comparant cette série avec l'intégrale $\int_1^{+\infty} \frac{2}{t} dt$.

Supposons alors l'ensemble $\mathbb{P} = \{p_1, \dots, p_k\}$ fini. Pour $n \geq 2$, écrivons

$$n = \prod_{i=1}^k p_i^{a_i(n)}.$$

Soit $N \geq 2$. Alors pour $n \leq N$, il vient $2^{a_1(n) + \dots + a_k(n)} \leq N$, et par conséquent $a_i(n) \leq 2 \ln(N)$, $i = 1, \dots, k$. Ainsi

$$\begin{aligned} \sum_{n \geq 1} \frac{1}{n} &= \sum_{n \geq 1} \frac{1}{p_1^{a_1(n)} \cdots p_k^{a_k(n)}} \\ &\leq \left(\sum_{i=1}^{2 \ln(N)} \frac{1}{p_1^i} \right) \cdots \left(\sum_{i=1}^{2 \ln(N)} \frac{1}{p_k^i} \right) \\ &\leq \left(\sum_{i=1}^{2 \ln(N)} \frac{1}{2^i} \right)^k \leq \left(\frac{\pi^2}{6} \right)^k \end{aligned}$$

Au final, on obtient que la série $\sum_{n \geq 1} \frac{1}{n}$ converge, ce qui est en contradiction avec le point observé avant.

On peut compter les nombres premiers. Soit $X \geq 2$. Posons

$$\pi(X) := \#\{p \in \mathbb{P}, p \leq X\},$$

et soit p_n le n -ème premier.

Théorème 1.34 (Hadamard, de La Vallée Poussin, 1896). — Quand $X \rightarrow \infty$, il vient $\pi(X) \sim \frac{\ln(X)}{X}$.
Et pour n grand, $p_n \sim n \ln(n)$.

On en déduit alors le résultat suivant.

Corollaire 1.35. — La série $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge.

Démonstration. — Cette fois-ci on compare la série en question avec l'intégrale $\int_1^{+\infty} \frac{2}{t \ln(t)} dt$. □

1.4. Normes. —

1.4.1. Valuation p -adique. —

Définition 1.36. — Soit a un entier non nul et soit p un nombre premier. La valuation p -adique de a , notée $v_p(a)$, est le plus entier $n \geq 0$ tel que $p^n \mid a$. En d'autres termes, $a = p^{v_p(a)} n_0$, avec $\text{pgcd}(p, n_0) = 1$. Par convention, on pose $v_p(0) = \infty$.

On a les propriétés suivantes :

Proposition 1.37. — Soient a et b deux entiers et soit p un nombre premier. Il vient

- (i) $v_p(ab) = v_p(a) + v_p(b)$,
- (ii) $v_p(a + b) \geq \min(v_p(a), v_p(b))$ avec égalité si $v_p(a) \neq v_p(b)$.

Démonstration. — Ecrivons $a = p^{v_p(a)} a_0$ et $b = p^{v_p(b)} b_0$ avec p premier à a_0 et b_0 (ou encore $p \nmid a_0$ et $p \nmid b_0$; remarquons que par le lemme de Gauss 1.22 cela implique que $p \nmid a_0 b_0$).

(i) Alors $ab = p^{v_p(a) + v_p(b)} a_0 b_0$, et comme $p \nmid a_0 b_0$, il vient $v_p(ab) = v_p(a) + v_p(b)$.

(ii) Soit $m = \min(v_p(a), v_p(b))$; supposons que $m = v_p(a)$. Alors $a + b = p^m (a_0 + p^{v_p(b) - m} b_0)$, ce qui montre que $v_p(a + b) \geq m$. Si de plus $v_p(b) > m$, alors $p \mid (p^{v_p(b) - m} b_0)$. Mais comme $p \nmid a_0$, il vient que $p \nmid (a_0 + p^{v_p(b) - m} b_0)$ et ainsi $v_p(a + b) = m$. □

La connaissance de la factorisation d'un entier en produit de nombres premiers permet de donner la caractérisation du PGCD (et du PPCM).

Proposition 1.38. — Soient a et b deux entiers non nuls. On a $v_p(\text{pgcd}(a, b)) = \min(v_p(a), v_p(b))$ et $v_p(\text{ppcm}(a, b)) = \max(v_p(a), v_p(b))$.

Démonstration. — Immédiat. □

1.4.2. Normes p -adiques. — Ce paragraphe est consacré à l'étude des valeurs absolues sur l'ensemble des rationnels $\mathbb{Q}$.

Soit p un nombre premier. Commençons par étendre la valuation p -adique v_p à $\mathbb{Q}$.

Soit $x \in \mathbb{Q}$ un rationnel non nul. En utilisant le théorème de factorisation on peut écrire x sous la forme

$$x = p^n \frac{a}{b},$$

où $n \in \mathbb{Z}$ et où a et b sont des entiers premiers à p . On définit $v_p : \mathbb{Q}^\times \rightarrow \mathbb{Z}$ en posant $v_p(x) = n$.

Posons ensuite pour $x \neq 0$, $\|x\|_p := p^{-v_p(x)}$, et $\|0\|_p = 0$.

Proposition 1.39. — La fonction $x \mapsto \|x\|_p$ vérifie les propriétés suivantes :

- (i) $\|x\|_p \geq 0$, et $\|x\|_p = 0$ si, et seulement si, $x = 0$;
- (ii) Pour $x, y \in \mathbb{Q}$, $\|xy\|_p = \|x\|_p \|y\|_p$;
- (iii) Pour $x, y \in \mathbb{Q}$, $\|x + y\|_p \leq \max(\|x\|_p, \|y\|_p)$ avec égalité lorsque les quantités sont différentes.

Démonstration. — Cela se déduit de la proposition 1.37. □

Définition 1.40. — On dit que $\|\cdot\|_p$ est la valeur absolue p -adique (ou encore norme p -adique).

Remarque 1.41. — La norme p -adique induit une distance sur $\mathbb{Q}$. Le complété de $\mathbb{Q}$ avec $\|\cdot\|_p$ est le corps des nombres p -adiques et est noté $\mathbb{Q}_p$.

1.4.3. Valeurs absolues sur $\mathbb{Q}$. —

Définition 1.42. — On appelle valeur absolue sur $\mathbb{Q}$ une fonction

$$\|\cdot\| : \mathbb{K} \rightarrow \mathbb{R}$$

satisfaisant les trois propriétés suivantes :

- (i) $\|x\| \geq 0$ pour tout $x \in \mathbb{Q}$ et $\|x\| = 0$ si, et seulement si, $x = 0$;
- (ii) Pour $x, y \in \mathbb{Q}$ on a $\|xy\| = \|x\| \|y\|$;
- (iii) Pour $x, y \in \mathbb{Q}$ on a $\|x + y\| \leq \|x\| + \|y\|$.

Exemple 1.43. — La valeur absolue définie par $\|x\| = 1$ si $x \neq 0$ est dite triviale.

Donnons quelques propriétés élémentaires.

Proposition 1.44. — (i) On a $\|1\| = \|-1\| = 1$.

(ii) Pour tout $n \in \mathbb{N}$ on a $\|n\| \leq n$.

(iii) Pour tout $x \in \mathbb{Q}$, $\|-x\| = \|x\|$.

(iv) Pour $x \neq 0$, $\|x^{-1}\| = \|x\|^{-1}$.

(v) Pour $x, y \in \mathbb{Q}$ on a $|\|x\| - \|y\|| \leq \|x - y\|$.

Remarque 1.45. — On dispose déjà de la valeur absolue usuelle qu'on note ici $|\cdot|$. Cette norme est archimédienne.

Remarque 1.46. — Si p et ℓ sont deux nombres premiers distincts, les valeurs absolues $\|\cdot\|_p$ et $\|\cdot\|_\ell$ ne sont pas équivalentes. Les valeurs absolues p -adiques $\|\cdot\|_p$ ne sont pas archimédiennes.

Démonstration. — C'est immédiat. □

On peut légitimement se demander si $\mathbb{Q}$ a d'autres normes (à équivalence près).

Théorème 1.47 (Ostrowski, 1916). — Toute valeur absolue non triviale $\|\cdot\|$ sur $\mathbb{Q}$ est équivalente soit à la valeur absolue usuelle $|\cdot|$ soit à la valeur absolue p -adique $\|\cdot\|_p$, pour un certain nombre premier p .

Démonstration. — • Supposons qu'il existe $k \in \mathbb{N}$ tel que $\|k\| > 1$. Notons que pour tout entier n , $\|n\| \leq n$. Posons $\alpha := \frac{\ln \|k\|}{\ln k} > 0$, ou encore $\|k\| = k^\alpha$. Soit $m \in \mathbb{N}$. Écrivons le développement de m en base k :

$$m = \sum_{i=0}^r a_i k^i,$$

avec $a_i \in \{0, \dots, k-1\}$ et r tel que $m \geq k^r$. Comme $\|a_i\| \leq a_i \leq k-1$ et $\|k^i\| = \|k\|^i$, il vient

$$\|m\| \leq (k-1) \sum_{i=0}^r \|k\|^i \leq \frac{\|k\|(k-1)}{\|k\| - 1} \|k\|^r.$$

Ainsi $\|m\| \leq Ck^{\alpha r} \leq Cm^\alpha$, où $C = \frac{\|k\|(k-1)}{\|k\| - 1}$. De cette inégalité, on a pour tout entier $n \geq 1$: $\|m\|^n \leq Cm^{\alpha n}$; en prenant ensuite la racine n -ème et en faisant tendre n vers l'infini, on obtient $\|m\| \leq m^\alpha$ et ainsi

$$\frac{\ln \|m\|}{\ln m} \leq \frac{\ln \|k\|}{\ln k}.$$

Si m est tel que $\|m\| > 1$, par symétrie, on obtient l'égalité $\frac{\ln \|m\|}{\ln m} = \frac{\ln \|k\|}{\ln k}$. Sinon, il existe $s \geq 2$ tel que $\|k^s m\| > 1$. Alors

$$\frac{\ln \|k^s m\|}{\ln k^s m} = \frac{\ln \|k\|}{\ln k}$$

et alors en utilisant la multiplicativité de la norme, il vient également l'égalité $\frac{\ln \|m\|}{\ln m} = \frac{\ln \|k\|}{\ln k}$. Pour conclure, en utilisant la multiplicativité de la norme, on obtient que $\|\cdot\| = |\cdot|^\alpha$.

• Supposons maintenant que pour tout $n \in \mathbb{N}$, $\|n\| \leq 1$. Si $\|\cdot\|$ est non triviale, il existe $n \in \mathbb{N}$ tel que $\|n\| < 1$. Soit n_0 le plus petit entier vérifiant cette inégalité stricte. Alors n_0 est un nombre premier p . Prenons ensuite un nombre premier ℓ différent de p . Soit $n \gg 0$ et soit la relation de Bezout $1 = ap^n + b\ell^n$. Alors

$$1 = \|1\| \leq \|p\|^n + \|\ell\|^n.$$

Ainsi nécessairement $\|\ell\| = 1$! Par conséquent, $\|\cdot\|$ est équivalente à $\|\cdot\|_p$. □

Terminons enfin par la formule du produit.

Théorème 1.48. — Soit $x \in \mathbb{Q}^\times$. Alors

$$|x| \cdot \prod_{p \in \mathbb{P}} \|x\|_p = 1.$$

Remarque 1.49. — On pourra remarquer que le produit infini est en fait un produit fini.

1.5. Exercices. —

Exercice 1. — (i) Donner la liste complète des diviseurs de 20, 50 et 55.

(ii) En déduire $\text{pgcd}(20, 50)$, $\text{pgcd}(20, 55)$ et $\text{pgcd}(50, 55)$.

Exercice 2. — Déterminer $6\mathbb{Z} + 14\mathbb{Z}$, $6\mathbb{Z} + 21\mathbb{Z}$, $14\mathbb{Z} + 21\mathbb{Z}$ et $6\mathbb{Z} + 14\mathbb{Z} + 21\mathbb{Z}$.

Exercice 3. — Que vaut $\text{pgcd}(222, 344)$? Déterminer deux entiers $x, y \in \mathbb{Z}$ tels que $222x + 344y = 2$.

Exercice 4. — Résoudre les équations diophantiennes suivantes :

- $2018x + 203y = 1$.
- $2025x + 203y = 1$.

Exercice 5. — Trouver les entiers $a \in \mathbb{Z}$ tels que l'équation $4558x + 9546y = a$ possède une solution $x, y \in \mathbb{Z}$.

Exercice 6. — Résoudre l'équation diophantienne $4558x + 9546y = 2$.

Exercice 7. — Un nombre entier n est parfait s'il est égal à la somme de ses diviseurs stricts (c'est à dire à la somme des entiers d tels que $1 \leq d < n$ et $d \mid n$). Vérifier que 6, 28 et 496 sont parfaits.

Exercice 8. — Donner la liste des nombres premiers plus petits que 150.

Exercice 9. — Les nombres de la forme $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$, sont appelés nombres de Fermat.

1. Calculer F_0, F_1, F_2, F_3, F_4 .
2. Montrer que ces nombres sont des nombres premiers.
3. Vérifier que F_5 est divisible par 641.
4. Montrer que si $2^k + 1$ est un nombre premier alors k est une puissance de 2.

Exercice 10. — Les nombres de la forme $M_n = 2^n - 1$ sont appelés nombres de Mersenne.

1. Calculer $M_2, M_3, M_4, M_5, M_7, M_{11}$.
2. Factoriser ces nombres.
3. Montrer que si M_n est un nombre premier alors n est un nombre premier.
4. Montrer que si M_n est un nombre premier alors $2^{n-1}M_n$ est un nombre parfait.

2. Congruences

2.1. L'ensemble $\mathbb{Z}/n\mathbb{Z}$. — On fixe un entier $n \geq 0$.

Définition 2.1. — On dit que les entiers a et b sont congrus modulo n si $n \mid (a - b)$, ou encore s'il existe $\alpha \in \mathbb{Z}$ tel que $a = b + \alpha n$. On note $a \equiv b \pmod{n}$, ou encore $a \equiv b$ (modulo n), ou encore $a \equiv_n b$.

Remarque 2.2. — Pour $n = 0$, on a $a \equiv_n b$ si et seulement si, $a = b$.

Remarque 2.3. — Pour $n = 1$, on a $a \equiv_n 0$ pour tout entier a .

Proposition 2.4. — Soient $a, b, c \in \mathbb{Z}$. Alors

- (i) $a \equiv_n b$ si et seulement si, $a \equiv_n b$ (la relation "modulo" est symétrique),
- (ii) $a \equiv_n a$ (la relation "modulo" est réflexive),
- (iii) si $a \equiv_n b$ et $b \equiv_n c$, alors $a \equiv_n c$ (la relation "modulo" est transitive).

Démonstration. — (i) C'est immédiat : on a $a = b + \alpha n$, $\alpha \in \mathbb{Z}$, si et seulement si, $b = a - \alpha n$.

(ii) On a $a = a + 0 \times n$.

(iii) Si $a = b + \alpha n$ et $b = c + \beta n$ avec $\alpha, \beta \in \mathbb{Z}$, alors $a = c + n(\alpha + \beta)$. □

Remarque 2.5. — La relation "être congru à" est une relation d'équivalence sur $\mathbb{Z}$. Cette relation est appelée relation de congruence.

Définition 2.6. — Etant donné $a \in \mathbb{Z}$, on pose $[a]_n = \{x \in \mathbb{Z}, x \equiv_n a\}$. Le sous-ensemble $[a]_n$ de $\mathbb{Z}$ est appelé classe de congruence de a modulo n . On le note également $\bar{a}$ (lorsqu'il n'y a pas d'ambiguïté possible). L'ensemble des classes de congruence est noté $\mathbb{Z}/n\mathbb{Z}$. On parle aussi du quotient $\mathbb{Z}/n\mathbb{Z}$.

Remarque 2.7. — On a donc $[a]_n = a + n\mathbb{Z}$.

L'ensemble des classes $\mathbb{Z}/n\mathbb{Z}$ forme une partition de $\mathbb{Z}$: cela signifie que $\mathbb{Z}$ est réunion disjointe des classes d'équivalence. Par exemple, le lemme suivant illustre cette partition :

Lemme 2.8. — Soient deux entiers a et b tels que $[a]_n \cap [b]_n \neq \emptyset$. Alors $[a]_n = [b]_n$.

Démonstration. — Soit $z_0 \in [a]_n \cap [b]_n$. Alors $z_0 \equiv_n a$ et $z_0 \equiv_n b$. Il suffit de montrer une inclusion. Soit $z \in [a]_n$. Alors $z \equiv_n a$ et par transitivité, $z \equiv_n z_0$ puis $z \equiv_n b$, et ainsi $z \in [b]_n$. □

Précisons la partition de $\mathbb{Z}$ par $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.9. — Soit $n \geq 1$. On a $\mathbb{Z} = [0]_n \cup [1]_n \cup \dots \cup [n-1]_n$, et ces classes sont deux à deux disjointes. En particulier, $|\mathbb{Z}/n\mathbb{Z}| = n$.

Démonstration. — Soit $b \in \mathbb{Z}$. Effectuons la division euclidienne de b par n : il existe q et r , avec $0 \leq r < n$, tels que $b = nq + r$: ce qui signifie que $b \in [r]_n$ avec $r \in \{0, 1, \dots, n-1\}$. Il reste à montrer que ces classes d'équivalence sont disjointes. Soient donc $k, k' \in \{0, \dots, n-1\}$ tels que $[k]_n = [k']_n$. Alors n divise $k - k'$ avec $-n < k - k' < n$, et donc $k - k' = 0$. $\square$

Remarque 2.10. — Quand $n = 0$ il y a autant de classes que d'entiers.

Pour toute la suite, on suppose $n > 0$.

Soit donc $a \in \mathbb{Z}$. Alors il existe un unique entier $k \in \{0, \dots, n-1\}$ tel que $a \in [k]_n$. Comme $a \in [a]_n \cap [k]_n$ d'après la proposition 2.4 (ii), il vient $[a]_n = [k]_n$ d'après le lemme 2.8.

Définition 2.11. — Si $x \in [a]_n$, on dit que x est un représentant de la classe $[a]_n$. L'entier $k \in \{0, \dots, n-1\}$ tel que $k \in [a]_n$ est appelé représentant principal de la classe de a modulo n .

Exemple 2.12. — Soit $n = 131$ et $a = 2345$. Alors la division euclidienne de a par n s'écrit : $2345 = 17 \times 131 + 118$. Ainsi $[2345]_{131} = [118]_{131}$, et 118 est le représentant principal de la classe de 2345 modulo 131.

Proposition 2.13. — Soient $a, b, c, d \in \mathbb{Z}$.

- (i) Si $a \equiv_n b$ et $c \equiv_n d$, alors $a + c \equiv_n b + d$ et $ac \equiv_n bd$.
- (ii) Si $a \equiv_n b$, alors pour tout entier $r \geq 1$, il vient $a^r \equiv_n b^r$.
- (iii) Si a est premier à n , il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv_n 1$.
- (iv) Si c est premier à n et si $ac \equiv_n bc$ alors $a \equiv_n b$.

Démonstration. — (i) Si $n \mid (a - b)$ et $n \mid (c - d)$ alors $n \mid (a - b) + (c - d)$ d'après la proposition 1.7 (iii). Ecrivons ensuite $a = b + \alpha n$ puis $c = d + \beta n$ avec $\alpha, \beta \in \mathbb{Z}$. Alors $ac = bd + n(d\alpha + b\beta + n\alpha\beta)$, ce qui montre que $n \mid (ac - bd)$.

(ii) C'est une conséquence du point précédent : en prenant $c = a$ et $b = d$, on a $a^2 \equiv_n b^2$, etc.

(iii) Comme $\text{pgcd}(a, n) = 1$, on a la relation de Bézout $au + nv = 1$ pour deux entiers u, v . Ainsi, $n \mid (au - 1)$ et donc $au \equiv_n 1$. Prendre par exemple $a' = u$.

(iv) Comme c est premier à n , il existe $c' \in \mathbb{Z}$ tel que $cc' \equiv_n 1$. En utilisant (i), on obtient $acc' \equiv_n bcc'$, c'est à dire $a \equiv_n b$. $\square$

Remarque 2.14. — Attention la simplification (iv) de la proposition 2.13 n'a pas toujours lieu. En effet, prenons $n = 2$, $a = 1$ et $b = 2$. Alors $2a \equiv_2 2b$ mais $a \not\equiv_2 b$.

2.2. Congruences simultanées. — Dans ce paragraphe nous montrons

Théorème 2.15 (des restes chinois). — Soient deux entiers $m, n \geq 1$, avec $\text{pgcd}(m, n) = 1$. Soient $a, b \in \mathbb{Z}$. Alors le système suivant d'inconnue $x \in \mathbb{Z}$

$$(S) \begin{cases} x \equiv_m a \\ x \equiv_n b \end{cases}$$

admet une solution x_0 dans l'ensemble $\{0, \dots, mn-1\}$. De plus, les entiers de $[x_0]_{mn}$ sont exactement les solutions de (S).

Démonstration. — Nous allons deux preuves de l'existence d'une solution, la second preuve donne une façon explicite pour trouver une solution.

Première preuve. Soit l'application :

$$\begin{aligned} \theta : \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

L'application est bien définie : en effet, si $[a]_{mn} = [b]_{mn}$, alors $[a]_m = [b]_m$ et $[a]_n = [b]_n$. Par le corollaire 1.23, θ est injective : en effet si $[a]_{mn}$ et $[b]_{mn}$ sont tels que $[a]_m = [b]_m$ et $[a]_n = [b]_n$, alors n et m

divisent $a-b$ et donc mn divise $a-b$, c'est à dire $[a]_{mn} = [b]_{mn}$. Comme $|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z}| \cdot |\mathbb{Z}/n\mathbb{Z}|$, on en déduit que l'application θ est surjective, ce qui garantit donc l'existence d'une solution à (S).

Seconde preuve. Partons d'une relation de Bézout $mu + nv = 1$ avec $u, v \in \mathbb{Z}$. Ecrivons

$$(b - a) = 1 \times (b - a) = (mu + nv)(b - a),$$

ce qui donne

$$mu(b - a) + a = b - nv(b - a).$$

Posons alors $c = mu(b - a) + a$. Alors $c \in [a]_m$ et $c \in [b]_n$, et ainsi c est une solution de (S). Soit alors x_0 le représentant principal de la classe de congruence $[c]_{mn}$ de c modulo mn . On a $x_0 \equiv_{mn} c$ et $x_0 \equiv_{mn} c$, ce qui implique $x_0 \in [c]_m = [a]_m$ et $x_0 \in [c]_n = [b]_n$.

Soit y une autre solution de (S). Alors $y \equiv_m a \equiv_m x_0$ et $y \equiv_n b \equiv_n x_0$, par conséquent $m \mid (y - x_0)$ et $n \mid (y - x_0)$. Par le corollaire 1.23, on a $mn \mid (y - x_0)$ et ainsi $y \in [x_0]_{mn}$. La réciproque est immédiate. $\square$

Exemple 2.16. — On cherche à résoudre le système suivant $\begin{cases} x \equiv_5 3 \\ x \equiv_3 2 \end{cases}$. On part de la relation de Bézout $2 \times 5 - 3 \times 3 = 1$. Alors $x = 2 \times 5 \times (3 - 2) + 3 = 13$ est une solution particulière. Ainsi, les solutions du système étudié sont les entiers de $[13]_{15}$.

2.3. $\mathbb{Z}/n\mathbb{Z}$ et ses lois. — On se fixe un entier $n \geq 1$. L'objectif de ce paragraphe est de munir $\mathbb{Z}/n\mathbb{Z}$ de deux lois $+$ (addition) et $\cdot$ (multiplication) qui en font un *anneau commutatif* (voir la définition 3.1 de la section IV).

2.3.1. L'anneau $\mathbb{Z}/n\mathbb{Z}$. — Pour deux classes de congruences $[a]_n$ et $[b]_n$ de $\mathbb{Z}/n\mathbb{Z}$, on pose :

- $[a]_n + [b]_n = [a + b]_n$,
- $[a]_n \cdot [b]_n = [ab]_n$.

Remarquons immédiatement que ces lois sont bien définies. En effet, si a' est autre représentant de la classe $[a]_n$, il vient $a + b \equiv_n a' + b$ et $ab \equiv_n a'b$.

Théorème 2.17. — *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des lois $+$ et $\cdot$ est un anneau commutatif unitaire. De plus,*

- (i) *l'élément neutre pour l'addition est la classe $[0]_n$,*
- (ii) *l'opposé de $[a]_n$ est la classe $[-a]_n$,*
- (iii) *le neutre pour la multiplication est la classe $[1]_n$.*

Démonstration. — C'est une simple vérification. $\square$

Définition 2.18. — Lorsque $[a]_n$ admet un inverse (pour la multiplication), on le note $[a]_n^{-1}$ (il est bien unique!). On note par $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des classes $[a]_n$ inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Pour $k \in \mathbb{N}$, on pose $[a]_n^k = \overbrace{[a]_n \cdot [a]_n \cdots [a]_n}^k$ et $k[a]_n = \overbrace{[a]_n + [a]_n \cdots + [a]_n}^k$, puis $-k[a]_n = k[-a]_n$. Enonçons quelques propriétés de calcul.

Proposition 2.19. — *Soient $a, b \in \mathbb{Z}$, on a*

- (i) *pour $k \in \mathbb{Z}$, $k[a]_n = [ka]_n = [k]_n[a]_n$,*
- (ii) *pour $k \in \mathbb{N}$, $[a]_n^k = [a^k]_n$,*
- (iii) *pour $k \in \mathbb{Z}$ premier à n tel $k[a]_n = k[b]_n$, alors $[a]_n = [b]_n$.*

Démonstration. — (i) et (ii) sont immédiats.

(iii) est conséquence de la proposition 2.13 (iv). $\square$

Notons que l'inverse (pour la multiplication) n'existe pas toujours. En effet,

Proposition 2.20. — Soit $[a]_n \in \mathbb{Z}/n\mathbb{Z}$. Alors $[a]_n$ admet un inverse si et seulement si, $\text{pgcd}(a, n) = 1$. Si tel est le cas, alors pour tout $k \in \mathbb{N}$, il vient $([a]_n^{-1})^k = [a^k]_n^{-1}$.

Démonstration. — Si $[a]_n$ admet un inverse cela signifie qu'il existe $b \in \mathbb{Z}$ tel que $[1]_n = [a]_n \cdot [b]_n = [ab]_n$, par conséquent que $n \mid (ab - 1)$, ce qui signifie exactement qu'il existe $u \in \mathbb{Z}$ tel que $nu + ab = 1$, c'est à dire que $\text{pgcd}(n, a) = 1$ d'après le corollaire 1.21.

Réciproquement, si $\text{pgcd}(n, a) = 1$, alors d'après la proposition 2.13 (iii), il existe $a' \in \mathbb{Z}$ tel que $[a]_n [a']_n = [1]_n$.

L'égalité sur les puissances est conséquence de la proposition 2.19 (ii). □

Définition 2.21. — La fonction (ou indicatrice) d'Euler φ est la fonction définie pour $n \geq 2$ par $\varphi(n) = |\{k, 0 < k < n - 1, \text{pgcd}(k, n) = 1\}|$. On a donc $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, où $(\mathbb{Z}/n\mathbb{Z})^\times$ est l'ensemble des classes inversibles.

Exemple 2.22. — Considérons l'ensemble de congruence $\mathbb{Z}/14\mathbb{Z}$. Comme $\text{pgcd}(3, 14) = 1$, la classe $[3]_{14}$ admet un inverse. Il s'obtient par la relation de Bézout entre 3 et 14. En effet de la relation $5 \times 3 - 1 \times 14 = 1$, on en déduit que $[5]_{14} [3]_{14} = [1]_{14}$ et ainsi $[3]_{14}^{-1} = [5]_{14}$.

Théorème 2.23. — Soit p un nombre premier. Alors

- (i) pour tout entier $a \in \mathbb{Z}$, il vient $[a]_p^p = [a]_p$,
- (ii) toute classe non nulle $[a]_p$, c'est à dire telle que $[a]_p \neq [0]_p$, admet un inverse $[a]_p^{-1}$, ou encore $\varphi(p) = p - 1$,
- (iii) pour toute classe non nulle $[a]_p$, il vient $[a]_p^{-1} = [a^{p-2}]_p$,
- (iv) les seules classes $[a]_p$ pour lesquelles $[a]_p = [a]_p^{-1}$ sont les classes $[1]_p$ et $[-1]_p = [p - 1]_p$,
- (v) si $[a]_p [b]_p = [0]_p$ alors, ou bien $[a]_p = [0]_p$, ou bien $[b]_p = [0]_p$.

Démonstration. — (i) : c'est une conséquence du petit théorème de Fermat 1.33.

(ii) et (iii) : Comme $p \mid (a^{p-1} - 1)$, d'après le lemme de Gauss 1.22, ou bien $p \mid a$ ou bien $p \mid (a^{p-1} - 1)$. Si $[a]_p$ est la classe non nulle, cela signifie exactement que p ne divise pas a et donc que $p \mid (a^{p-1} - 1)$, ce qui du point de vue des classes implique que $[a]_p^{p-1} = [1]_p$. En remarquant que $[a]_p^{p-1} = [a]_p [a]_p^{p-2} = [a^{p-2}]_p$, on a donc que $[a]_p$ est inversible d'inverse $[a^{p-2}]_p$.

(iv) : soit $[a]_p$ telle que $[a]_p = [a]_p^{-1}$, alors $[a]_p^2 = [1]_p$, ce qui signifie que $[a^2 - 1]_p = [0]_p$. Ainsi p divise $(a - 1)(a + 1)$, et donc par le lemme de Gauss 1.22, ou bien $p \mid (a - 1)$ ou bien $p \mid (a + 1)$.

(v) Ici $p \mid ab$ et comme p est premier, le résultat se déduit du lemme 1.30. □

Exemple 2.24. — Dans $\mathbb{Z}/11\mathbb{Z}$, on a

$$\begin{aligned} [5]_{11}^{-1} &= [5]_{11}^9 = [5]_{11}^{2^3} [5]_{11} = [5^2]_{11}^4 [5]_{11} \\ &= ([3]_{11}^2)^2 [5]_{11} = [81]_{11} [5]_{11} = [4]_{11} [5]_{11} \\ &= [9]_{11} \end{aligned}$$

Terminons avec le :

Théorème 2.25 (de Wilson). — Soit p un nombre premier. Alors $(p - 1)! \equiv_p -1$.

Démonstration. — D'après le théorème 2.23 (iv), toute classe $[k]_p$ avec $1 < k < p - 1$ a un inverse $[k']_p$ avec $1 < k' < p - 1$ et $k \neq k'$. Ainsi,

$$[2]_p \cdot [3]_p \cdots [p - 2]_p = [1]_p,$$

et ainsi

$$[1]_p \cdot [2]_p \cdots [p - 1]_p = [1]_p \cdot [p - 1]_p = [p - 1]_p = [-1]_p.$$

Par conséquent, p divise $(p - 1)! + 1$, ce qui est exactement le résultat recherché. □

2.4. Le groupe multiplicatif. — On se fixe un entier $n \geq 1$.

2.4.1. — Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$, noté $\mathbb{Z}/n\mathbb{Z}$, est engendré par $\bar{1}$: en effet $\bar{k} = k\bar{1}$. C'est un groupe cyclique d'ordre n .

Théorème 2.26. — Une classe $[k]_n$ engendre le groupe $\mathbb{Z}/n\mathbb{Z}$ si et seulement si, $\text{pgcd}(k, n) = 1$.

Démonstration. — Voir le théorème 14.11. □

On a alors le théorème suivant :

Théorème 2.27. — On a $n = \sum_{d|n} \varphi(d)$.

Démonstration. — Soit d un diviseur de n ; posons $n_0 = n/d$. Alors $[n_0]_n$ est d'ordre d et il engendre l'unique sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d (voir le théorème 14.10). Or, d'après le théorème 14.11, le groupe H contient exactement $\varphi(d)$ éléments d'ordre d . La somme porte donc sur les sous-groupes d'ordre $d | n$, et $\varphi(d)$ correspond aux éléments d'ordre $g \in G$ (et donc dans H) d'ordre exactement d . □

2.4.2. — Considérons maintenant le groupe multiplicatif.

Proposition 2.28. — L'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ muni de la loi $\cdot$ forme un groupe commutatif de cardinal $\varphi(n)$.

Démonstration. — C'est immédiat, voir la proposition 3.4. □

On a vu que lorsque $n = p$ est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1]_p, \dots, [p-1]_p\}$ et ainsi $\varphi(p) = p-1$. Pour le cas général, nous avons :

Théorème 2.29. — Soit $n = p_1^{n_1} \cdots p_k^{n_k}$, où les p_i sont des nombres premiers deux à deux distincts et où les entiers n_i sont tous plus grand que 1. Alors $\varphi(n) = (p_1 - 1)p_1^{n_1-1} \cdots (p_k - 1)p_k^{n_k-1}$.

Démonstration. — Commençons par le lemme suivant.

Lemme 2.30. — Soit $m, n \geq 2$ deux entiers premiers entre eux. Alors $\varphi(nm) = \varphi(n)\varphi(m)$.

Démonstration. — Nous avons vu dans la preuve du théorème 2.15 que l'application suivante :

$$\begin{aligned} \theta : \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

est bijective. Soit alors $[a]_{mn}$ inversible : cela signifie donc que $\text{pgcd}(a, mn) = 1$. L'image $\theta([a]_{mn})$ est un couple d'éléments $([a]_m, [a]_n)$ dans $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Ainsi, θ induit une application θ' nécessairement injective de $(\mathbb{Z}/mn)^\times$ vers $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n)^\times$. D'autre part on sait que θ est surjective. Donc pour $([b]_m, [c]_n) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n)^\times$, il existe $a \in \mathbb{Z}$ tel que $[a]_m = [b]_m$ et $[a]_n = [c]_n$. Alors $m | (a-b)$ et $n | (a-c)$. Par le lemme 1.26, il vient $\text{pgcd}(a, m) = \text{pgcd}(b, m) = 1$ et $\text{pgcd}(a, n) = \text{pgcd}(c, n) = 1$. Par conséquent, $\text{pgcd}(a, mn) = 1$ par le corollaire 1.24. Ainsi par la proposition 2.20, $[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^\times$. On vient de montrer que θ' est également une bijection. En considérant alors les cardinaux, on obtient le lemme. □

Nous avons besoin d'un second lemme

Lemme 2.31. — Soit p un nombre premier et soit $m \geq 1$. Alors $\varphi(p^m) = (p-1)p^{m-1}$.

Démonstration. — Cherchons le nombre N d'entiers a compris entre 1 et p^m et divisible par p . On aura alors $\varphi(p^k m) = p^m - N$. On écrit $a = pn_0$ avec $1 \leq n_0 < p^{m-1}$. Ainsi $N = p^{m-1}$. On a alors $\varphi(p^m) = p^m - p^{m-1} = (p-1)p^{m-1}$. □

Finissons la preuve du théorème 2.29 par récurrence sur k . Pour $k = 1$, c'est le cas où $n = p^m$ est la puissance d'un nombre premier p , et l'on a dans le lemme 2.31 que $|(\mathbb{Z}/p^m\mathbb{Z})^\times| = (p-1)p^{m-1}$. Partons alors de $n = p_1^{n_1} \cdots p_k^{n_k}$ et posons $n_0 = n/p_k^{n_k}$. Par hypothèse de récurrence, on suppose vrai le théorème pour n_0 . On a $\text{pgcd}(p_k^{n_k}, n_0) = 1$ et d'après le lemme 2.30, il vient $|(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/p_k^{n_k}\mathbb{Z})^\times| \times |(\mathbb{Z}/n_0\mathbb{Z})^\times|$, le résultat s'en déduit. $\square$

Avant d'énoncer le théorème d'Euler, effectuons l'observation suivante. Soit $n = p_1 \cdots p_k$, où les p_i sont des nombres premiers deux à deux distincts. Soit a premier à n . Alors a est premier à chaque p_i . Par le théorème 2.23, il vient $[a^{(p_i-1)}]_{p_i} = [1]_{p_i}$. Ainsi, $[a^{(p_1-1)\cdots(p_k-1)}]_{p_1} = [1]_{p_1}$ et, par conséquent, d'après le théorème 2.29 il vient $[a^{\varphi(n)}]_{p_1} = [1]_{p_1}$. Il en est de même pour chaque premier $p_i \mid n$. Ainsi, pour $i = 1, \dots, k$, on a $p_i \mid (a^{\varphi(n)} - 1)$. Comme les p_i sont deux à deux distincts, on en déduit, d'après le corollaire 1.23, que le produit $p_1 \cdots p_k$ divise $a^{\varphi(n)} - 1$, ce qui signifie que $[a^{\varphi(n)}]_n = [1]_n$.

Théorème 2.32 (Formule d'Euler). — Soit un entier a premier à $n \geq 2$. Alors $[a]_n^{\varphi(n)} = [1]_n$.

Démonstration. — La preuve est directe. On rappelle que $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe d'ordre $\varphi(n)$. Ainsi par le théorème de Lagrange (cf. corollaire 14.13 de l'Appendice §IV), on en déduit que tout élément $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ vérifie $[a]_n^{\varphi(n)} = [1]_n$. On conclut en notant que $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si, a est premier à n (cf. proposition 2.20). $\square$

Pour être complet terminons par le théorème suivant

Théorème 2.33. — L'application

$$\begin{aligned} \theta : \mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

est un isomorphisme d'anneaux.

Démonstration. — Par définition des lois sur les anneaux quotients $\mathbb{Z}/k\mathbb{Z}$, l'application θ est un morphisme d'anneaux, qui est un isomorphisme (vu dans la preuve du théorème 2.15). $\square$

2.5. Exercices. —

Exercice 11. — (i) Déterminer les représentants principaux des classes de congruence suivantes : $[223]_7, [354]_7, [1568]_7$.

(ii) Parmi ces classes, a-t-on deux classes identiques ?

Exercice 12. —

Trouver le plus petit entier positif x tel que $[x]_{89} = [60]_{89}$ et $[x]_{55} = [38]_{55}$.

Exercice 13. —

(i) Trouver les entiers $x \in \mathbb{Z}$ tels que $x \equiv 3 \pmod{7}$ et $x \equiv 5 \pmod{15}$.

(ii) Trouver les entiers $x \in \mathbb{Z}$ tels que $x \equiv 21 \pmod{37}$ et $x \equiv 130 \pmod{181}$.

(iii) Trouver le plus petit entier $x \in \mathbb{N}$ tels que $x \equiv 8 \pmod{14}$, $x \equiv 5 \pmod{23}$ et $x \equiv 13 \pmod{29}$.

Exercice 14. — Soit $n \in \mathbb{N}$.

(i) Montrer que n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

(ii) Montrer que n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

(iii) Sur le modèle des deux caractérisations précédentes, donner une condition nécessaire et suffisante pour que n soit divisible par 11.

Exercice 15. —

Soit le nombre entier $N = 27^{5n+a} - 26^{3n+b}$.

1. Déterminer les représentants principaux de $[27^5]_{31}$ et de $[26^3]_{31}$.
2. Calculer $[26^k]_{31}$ pour $k = 0, \dots, 6$.
3. Soit $a = 10$. Donner un entier $b > 0$ tel que 31 divise N .
4. Soit $a = 1$ et soit b quelconque. Montrer que le nombre N est premier à 31.

Exercice 16. —

Trouver l'ensemble des entiers n tel que 13 divise $n^2 + n + 1$.

Exercice 17. —

- (i) Quel est le reste de la division euclidienne de 13^{20} par 7 ?
- (ii) Quel est le reste de la division euclidienne de 2017^{2018} par 5 ? par 11 ? par 15 ?
- (iii) Soit $n \in \mathbb{N}$. Montrer que l'entier $5n^3 + n$ est divisible par 6.
- (iv) Soit $n \in \mathbb{N}$. Montrer que l'entier $3^{2n+1} + 2^{n+2}$ est divisible par 7.
- (v) Déterminer un entier $a \geq 0$ tel que, pour tout entier $n \in \mathbb{N}$, on ait : $3^{n+a} - 4^{4n+2} \equiv 0 \pmod{11}$.
- (vi) Déterminer un entier $a \geq 0$ tel que, pour tout entier $n \in \mathbb{N}$, on ait : $5^{n+1} - 7^{3n+a} \equiv 0 \pmod{13}$.

Exercice 18. — Déterminer les tables d'addition et de multiplication de $\mathbb{Z}/6\mathbb{Z}$ et de $\mathbb{Z}/7\mathbb{Z}$. Préciser l'inverse de chaque classe (lorsque celle-ci existe).

Exercice 19. —

- (i) Déterminer les inverses de $[11]_{23}$, $[35]_{13}$, $[13]_{35}$, et $[123]_{88}$.
- (ii) Trouver les entiers $x \in \mathbb{Z}$ vérifiant $35x \equiv 2 \pmod{13}$.
- (iii) Trouver les entiers $x \in \mathbb{Z}$ vérifiant $37x \equiv 2 \pmod{131}$.

Exercice 20. —

- (i) Déterminer les carrés de $\mathbb{Z}/29\mathbb{Z}$.
- (ii) Donner les entiers $x \in \mathbb{Z}$ tels que 29 divise $x^2 + x - 1$.
- (iii) Donner les entiers $x \in \mathbb{Z}$ tels que 29 divise $x^2 + x + 1$.

PARTIE II CORPS FINIS

3. Sous-corps premiers

3.1. Anneau commutatif. — Nous ne considérerons que des anneaux commutatifs.

Définition 3.1. — Un anneau A est un ensemble muni de deux lois $+$ (additive) et $\cdot$ (multiplicative) telles que

- (i) l'ensemble A muni de la loi $+$ forme un groupe (commutatif),
- (ii) la loi $\cdot$ est une loi interne associative et commutative munie d'un élément neutre, noté 1 , qui vérifie $g \cdot 1 = 1 \cdot g = g$ pour tout $g \in A$,
- (iii) la loi $\cdot$ est distributive par rapport à la loi $+$: $(g + g') \cdot g'' = g \cdot g'' + g' \cdot g''$ et $g \cdot (g' + g'') = g \cdot g' + g \cdot g''$.

Remarque 3.2. — Pour $x, y \in A$, on note par abus $xy = x \cdot y$.

Il est important de noter à ce niveau qu'un élément non nul de l'anneau A n'admet pas forcément d'inverse pour la seconde loi $\cdot$.

Définition 3.3. — Soit A un anneau. Un élément $a \in A$ est dit inversible s'il existe $b \in A$ tel que $ab = 1$. Dans ce cas, l'inverse de a est unique et on le note a^{-1} . L'ensemble des éléments inversibles de A est noté $A^\times$.

On a alors

Proposition 3.4. — L'ensemble $A^\times$ muni de la loi $\cdot$ forme un groupe (commutatif) de neutre 1 .

Démonstration. — Il nous suffit de vérifier que si $x, y \in A^\times$, alors $xy \in A^\times$, ce qui est immédiat : en effet, xy est inversible d'inverse $x^{-1}y^{-1}$. □

Définition 3.5. — Lorsque pour un anneau A , tout élément g non nul (ou encore $g \neq 0$) admet un inverse alors on dit que A est un corps. Ou encore, A est un corps si $A^\times = A - \{0\}$.

3.2. Les corps $\mathbb{F}_p$ et $\mathbb{Q}$. —

Théorème 3.6. — 1) Soit p un nombre premier. Alors, l'anneau $\mathbb{Z}/p\mathbb{Z}$ muni des lois $+$ et $\cdot$ est un corps. On le note $\mathbb{F}_p$. C'est l'unique corps à p éléments (à isomorphisme près).

2) Soit $\mathbb{K}$ un corps. Alors $\mathbb{K}$ est un espace vectoriel ou bien sur (un corps isomorphe à) $\mathbb{F}_p$, ou bien sur (un corps isomorphe à) $\mathbb{Q}$.

3) Soit $\mathbb{K}$ un corps fini. Il existe un nombre premier p et un entier $d \geq 1$ tel que $|\mathbb{K}| = p^d$. Plus précisément $\mathbb{K}$ est un $\mathbb{F}_p$ -espace vectoriel de dimension d sur $\mathbb{F}_p$.

Démonstration. — 1) : La première partie est conséquence du théorème 2.23.

On va répondre à la seconde partie de 1), 2) et 3) en même temps.

Soit e le neutre multiplicatif de $\mathbb{K}$. Alors $\mathbb{Z}e \subset \mathbb{K}$. En fait, de cette inclusion on construit une application $\psi : \mathbb{Z} \rightarrow \mathbb{K}$ définie par $\psi(k) = ke$. Cette application est un morphisme d'anneaux, c'est à dire que ψ respecte les lois de $\mathbb{Z}$ et de $\mathbb{K}$: $\psi(k + k') = \psi(k) + \psi(k')$, $\psi(1) = e$ et $\psi(kk') = \psi(k)\psi(k')$.

On cherche à déterminer le noyau $\ker(\psi)$ de ψ .

— Si ψ est injectif, cela signifie que $\mathbb{K}$ contient un sous-anneau isomorphe à $\mathbb{Z}$, et comme $\mathbb{K}$ est un corps, il contient un sous-corps isomorphe à $\mathbb{Q}$: en particulier c'est un espace vectoriel sur $\mathbb{Q}$.

— Si ψ n'est pas injectif, son noyau $\ker(\psi)$ est l'ensemble des entiers k tels que $ke = 0$; il n'est pas réduit à $\{0\}$. Soit $m \geq 1$ le plus entier non nul tel que $me = 0$. En utilisant la division euclidienne, on vérifie

que $\ker(\psi) = m\mathbb{Z}$. Soit alors l'application injective ψ_m définie par

$$\begin{aligned}\psi_m : \mathbb{Z}/m\mathbb{Z} &\rightarrow \mathbb{K} \\ [k]_m &\mapsto ke\end{aligned}$$

Comme $\mathbb{K}$ est un corps, nécessairement m est un nombre premier p (en effet si $ne \cdot n'e = 0$ alors ou bien $ne = 0$ ou bien $n'e = 0$). Notons par $\mathbb{F} := \psi(\mathbb{F}_p)$: c'est un sous-corps de $\mathbb{K}$, isomorphe à $\mathbb{F}_p$, et les compatibilités des lois font que $\mathbb{K}$ est un $\mathbb{F}$ -espace vectoriel. Appelons d la dimension de $\mathbb{K}$ sur $\mathbb{F}$ (éventuellement infinie). Alors quand $\mathbb{K}$ est fini, $|\mathbb{K}| = |\mathbb{F}|^d$ et donc $|\mathbb{K}| = p^d$, ce qui entraîne $m = p$. En particulier $d = 1$ quand $|\mathbb{K}| = p$, puis $\mathbb{K} = \mathbb{F} = \psi_p(\mathbb{F}_p)$. $\square$

Remarque 3.7. — Lorsque $\mathbb{K}$ contient $\mathbb{Q}$, on dit qu'il est de caractéristique nulle (ou zéro), lorsqu'il contient $\mathbb{F}_p$, on dit qu'il est de caractéristique p .

Remarque 3.8. — Tout élément de $\mathbb{F}_p$ est racine du polynôme $X^p - X$. Ou encore, $x^p = x$. C'est une conséquence du petit théorème de Fermat.

Le théorème 3.6 amène la définition suivante.

Définition 3.9. — Les corps $\mathbb{Q}$ et $\mathbb{F}_p$, $p \in \mathbb{P}$, sont dits sous-corps premiers.

Pour toute la suite, on se fixe un nombre premier p , et pour un entier k , on notera par $\bar{k}$ (voire k) la classe $[k]_p$.

4. Structure multiplicative

Nous venons de voir que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, est l'unique corps à p éléments (à isomorphisme près).

Théorème 4.1. — Soit le corps fini $\mathbb{F}_p$. Alors $\mathbb{F}_p^\times$ est un groupe cyclique d'ordre $p - 1$.

Démonstration. — (Nous donnerons une autre preuve plus loin, voir théorème 7.9.) On a déjà vu que $\mathbb{F}_p^\times$ est un groupe (commutatif) d'ordre $p - 1$. Soit $\bar{x} \in \mathbb{F}_p^\times$, et soit d son ordre : on rappelle que c'est le plus petit entier $d > 0$ tel que $\bar{x}^d = \bar{1}$. D'après le corollaire 14.13 de la section IV, l'entier d divise $p - 1$. Il vient alors que $\bar{x}$ est racine du polynôme $X^d - \bar{1}$. Ainsi, si l'on note par E_d l'ensemble des éléments de $\mathbb{F}_p^\times$ d'ordre d et par F_d les éléments de $\mathbb{F}_p$ racines de $X^d - \bar{1}$, on a $E_d \subset F_d$. Or le polynôme $X^d - \bar{1}$ a au plus d racines dans $\mathbb{F}_p$ (d'après le corollaire 6.6 à venir). Comme le sous-groupe $\langle \bar{x} \rangle$ de $\mathbb{F}_p^\times$ engendré par $\bar{x}$, de cardinal d (voir la proposition 14.8 de la section IV), est contenu dans F_d , on en déduit que $F_d = \langle \bar{x} \rangle$. Et ainsi, $E_d \subset \langle \bar{x} \rangle$, et est donc cyclique. Un élément $\bar{x}^k$ est d'ordre d si et seulement si $\text{pgcd}(k, d) = 1$ (d'après le théorème 14.11). Par conséquent $|E_d| = \varphi(d)$ quand E_d n'est pas vide. En conclusion, pour $d \mid (p - 1)$, il vient $|E_d| \leq \varphi(d)$. On a alors

$$p - 1 = |\mathbb{F}_p^\times| = \sum_{d \mid (p-1)} |E_d| \leq \sum_{d \mid (p-1)} \varphi(d) = p - 1,$$

la dernière égalité résultant du théorème 2.27. Ceci implique alors que pour tout $d \mid (p - 1)$, $|E_d| = \varphi(d)$, et en particulier que E_{p-1} est non-vide : il existe dans $\mathbb{F}_p^\times$ un élément a d'ordre $p - 1$. Et ainsi $\mathbb{F}_p^\times = \langle a \rangle$. $\square$

Définition 4.2. — Un élément a de $\mathbb{F}_p^\times$ d'ordre $p - 1$ s'appelle une racine primitive de l'unité ; c'est aussi un générateur du groupe $\mathbb{F}_p^\times$.

Remarque 4.3. — Le corps $\mathbb{F}_p^\times$ contient donc $\varphi(p - 1)$ racines primitives de l'unité.

5. Logarithme discret

Étant donné $\mathbb{F}_p$, nous venons donc de voir qu'il existe $a \in \mathbb{F}_p$, tel que $\mathbb{F}_p = \langle a \rangle \cup \{0\}$. Plus précisément, pour $x \neq 0$, il existe *un unique* $k_x \in \{0, \dots, p-2\}$ tel que $x = a^{k_x}$.
On en arrive à la définition du logarithme discret.

Définition 5.1. — Soit a un générateur $\mathbb{F}_p^\times$. Soit $k_a \in \{0, \dots, p-2\}$ tel $x = a^{k_x}$. L'entier k_x est par définition le logarithme de x (en base a) : on note alors $k = \log_a(x)$.

Remarque 5.2. — On a en particulier, $\log_a(a) = 1$ et $\log_a(\bar{1}) = 0$.

Remarque 5.3. — D'après le théorème 14.11, l'élément x est une racine primitive de l'unité si et seulement si, $\text{pgcd}(p-1, \log_a(x)) = 1$.

Exemple 5.4. — Dans $\mathbb{F}_5^\times$, la classe $\bar{2}$ est d'ordre 4. Ainsi, $\log_{\bar{2}}(\bar{1}) = 0$, $\log_{\bar{2}}(\bar{2}) = 1$, $\log_{\bar{2}}(\bar{3}) = \log_{\bar{2}}(\bar{8}) = 3$ et $\log_{\bar{2}}(\bar{4}) = 2$.

Proposition 5.5. — Soit a un générateur de $\mathbb{F}_p^\times$. Alors pour tout $x, y \in \mathbb{F}_p^\times$, il vient

$$\log_a(xy) \equiv \log_a(x) + \log_a(y) \pmod{p-1}.$$

Démonstration. — On écrit $x = a^k$ et $y = a^{k'}$ avec $0 \leq k, k' \leq p-2$. Si l'on note par r le reste de la division euclidienne de $k + k'$ par $p-1$, il vient $xy = a^{k+k'} = a^r$. Ainsi, $\log_a(x) + \log_a(y) = r \equiv_{p-1} k + k' = \log_a(x) + \log_a(y)$. □

Remarquons enfin le corollaire suivant :

Corollaire 5.6. — Pour $x \in \mathbb{F}_p^\times$, on a

$$\log a(x^{-1}) \equiv -\log_a(x) \pmod{p-1}.$$

Démonstration. — C'est une conséquence de la proposition 5.5 associée au fait que $\log_a(1) = 0$. □

6. Polynômes

On se fixe le corps fini $\mathbb{F}_p$, et on considère $\mathbb{F}_p[X]$ l'ensemble des polynômes à coefficient dans $\mathbb{F}_p$. On munit $\mathbb{F}_p[X]$ des deux lois $+$, $\cdot$, issues de celles de $\mathbb{F}_p$.

Proposition 6.1. — $(\mathbb{F}_p[X], +, \cdot)$ est un anneau (commutatif) intègre. Le groupe $\mathbb{F}_p^\times$ est exactement le groupe des inversibles de $\mathbb{F}_p[X]$.

Démonstration. — C'est immédiat. □

On définit alors le degré $\deg(P)$ d'un polynôme non nul $P = a_n X + \dots + a_0$ comme le plus grand indice i tel que $a_i \neq 0$. On pose également $\deg(0) = -\infty$. Comme pour $\mathbb{Z}$, on peut définir la notion de divisibilité et munir $\mathbb{F}_p[X]$ d'une division euclidienne

Théorème 6.2. — Soient $Q, P \in \mathbb{F}_p[X]$ avec $P \neq 0$. Alors il existe $R, S \in \mathbb{F}_p[X]$ tels que $Q = PS + R$ et $0 \leq \deg(R) < \deg(P)$. De plus, sous ces conditions les polynômes R et S sont uniques.

Démonstration. — Commençons par montrer l'existence.

Si $Q = 0$, prendre $R = S = 0$.

Pour le cas général, c'est un algorithme qui ramène à la situation suivante.

– Si $m < n$, prendre $S = 0$, et $R = Q$.

Sinon, Ecrivons $P = a_n X^n + a_{n-1} X^{n-1} + \dots$, avec $a_n \neq 0$, puis $Q = b_m X^m + b_{m-1} X^{m-1} + \dots$, $m \geq 0$, $b_m \neq 0$.

– Soit $k := m - n \geq 0$. Posons $Q_1 := Q - b_m a_k^{-1} X^k P$: c'est un polynôme de degré m_1 strictement plus petit que m . Si $m_1 < n$, prendre $S = b_m a_k^{-1} X^k$ et $R = Q_1$.

Sinon, on écrit $Q_1 = m_1 X^{m_1} + \dots$, avec $m_1 \neq 0$ et $m_1 < m$. Si $m_1 < n$, on pose alors $Q_2 := Q_1 - b_{m_1} a_n^{-1} X^{n-m_1} P$. C'est un polynôme de degré $m_2 < m_1$. Observons l'égalité

$$Q_2 = Q_1 - b_{m_1} a_n^{-1} P = Q - b_m a_k^{-1} X^{m-n} P - b_{m_1} a_k^{-1} X^{m_1-n} P = Q - a_k^{-1} P (b_m X^{m-n} + b_{m_1} X^{m_1-n}).$$

– Si $m_2 < n$, prendre $S = a_k^{-1} (b_m X^{m-n} + b_{m_1} X^{m_1-n})$ et $R = Q_2$.

– Sinon, on continue le processus qui aboutira à un polynôme Q_i avec $\deg(Q_i) < n$. Cet algorithme nécessite au plus k étapes.

Pour l'unicité, on écrit $Q = PS + R = PS_1 + R_1$, avec $\deg(R_i) < \deg(P)$. Ce qui implique $P(S - S_1) = R_1 - R$. Or $\deg(R_1 - R) < n$, ce qui implique $R = R_1$ car $P \neq 0$, puis $S = S_1$, là aussi car $P \neq 0$ et $\mathbb{F}_p[X]$ est intègre. $\square$

Cette division euclidienne est une propriété extrêmement riche : en effet comme pour $\mathbb{Z}$ (ou $\mathbb{R}[X]$), on a la notion de PGCD, d'éléments premiers entre eux, de polynômes irréductibles (l'équivalent des nombres premiers), d'algorithme d'Euclide, du théorème fondamental de factorisation (l'équivalent du théorème 1.31), du théorème des restes chinois, etc. Nous avons également les relations de Bézout (et les corollaires de la section 1.2). Typiquement

Corollaire 6.3 (Relation de Bézout). — Soient P et Q deux polynômes non nuls de $\mathbb{F}_p[X]$. Alors P et Q sont premiers entre eux si et seulement si, il existe $U, V \in \mathbb{F}_p[X]$ tels que $UP + VQ = 1$.

Exemple 6.4. — Dans $\mathbb{F}_2$, soient $Q = X^5 + X^4 + 1$ et $P = X^3 + X$.

Alors $Q = (X^2 + X + 1)P + X^2 + X + 1$ et la relation de Bézout est

$$(X^2 + X + 1)Q + (X^4 + X^3 + X^2 + X + 1)P = 1.$$

Donnons également une autre conséquence de la division euclidienne.

Corollaire 6.5. — Soit $P \in \mathbb{F}_p[X]$ non nul. Posons $r = \deg(P)$. Supposons qu'il existe $a \in \mathbb{F}_p$ tel que $P(a) = 0$. Alors il existe un polynôme Q de degré $r - 1$ tel que $P = (X - a)Q$.

Démonstration. — Grâce à la division euclidienne, on écrit $P = (X - a)Q + b$, avec $b \in \mathbb{F}_p$. Comme $P(a) = 0$, on en déduit que $b = 0$. $\square$

On a alors

Corollaire 6.6. — Soit $P \in \mathbb{F}_p[X]$ non nul de degré r . Alors P a au plus r racines. Plus précisément, il existe $a_1, \dots, a_k \in \mathbb{F}_p$ tel que $P = (X - a_1)^{n_1} \dots (X - a_k)^{n_k} Q$, avec $a_i \neq a_j$ pour $i \neq j$, avec $n_1 + \dots + n_k \leq r$ et avec $Q \in \mathbb{F}_p[X]$ sans racine. De plus, si $P(b) = 0$ alors nécessairement $b = a_i$ pour un certain $i \in \{1, \dots, k\}$.

Démonstration. — La factorisation s'obtient à partir du corollaire 6.5. Alors pour $b \in \mathbb{F}_p$ tel que $P(b) = 0$, il vient $(b - a_1)^{n_1} \dots (b - a_k)^{n_k} Q(b)$ et comme $\mathbb{F}_p$ est un corps, on a nécessairement l'un des $b - a_i$ qui est nul (car $Q(b) \neq 0$ par hypothèse). $\square$

Remarque 6.7. — Le corps $\mathbb{F}_p$ peut aussi être vu comme l'ensemble des racines de $X^p - X$: en effet nous avons déjà vu que tout élément de $\mathbb{F}_p$ est racine de $X^p - X$, et le corollaire 6.6 montre que $X^p - X$ a au plus p racines dans $\mathbb{F}_p$.

7. Le corps $\mathbb{F}_q$

7.1. Sur l'existence. — Nous venons de montrer qu'un corps fini est de cardinal p^d pour un certain nombre premier p . Montrons comment construire de tel corps finis.

La démarche va être identique à celle qui permet de construire le corps $\mathbb{F}_p$ mais cette fois-ci en partant de $\mathbb{F}_p[X]$. On commence par définir une relation de congruence sur $\mathbb{F}_p[X]$ de la façon suivante :

Définition 7.1. — Soit $P \in \mathbb{F}_p[X]$ et soient $A, B \in \mathbb{F}_p[X]$. On dit que A est congru à B modulo P , si P divise $A - B$. Ou encore le reste de la division euclidienne de $A - B$ par P est le polynôme nul. On note alors $A \equiv_P B$, ou encore $A \equiv B (P)$, ou encore $A \equiv B \pmod{P}$.

Comme dans $\mathbb{Z}$, la relation "modulo à" est une relation d'équivalence : symétrique, réflexive et transitive. On considère alors les classes d'équivalence

$$[A]_P = \{B \in \mathbb{F}_p[X], A \equiv_P B\}.$$

La classe $[A]_P$ est aussi notée $\overline{A}$.

Définition 7.2. — On note par $\mathbb{F}_p[X]/(P)$ l'ensemble des classes d'équivalences modulo P ; on parle aussi du quotient $\mathbb{F}_p[X]/(P)$.

Les classes de $\mathbb{F}_p[X]/(P)$ forment alors une partition de $\mathbb{F}_p[X]$.

Remarque 7.3. — Lorsque $P = 0$, il y a autant de classes que de polynômes.

Soit $P \in \mathbb{F}_p[X]$ non nul de degré d . Alors, comme pour $\mathbb{Z}$, on montre que toute classe d'équivalence contient un *unique* polynôme A de degré plus petit que d . Et ainsi on a $|\mathbb{F}_p[X]/(P)| = p^d$. Les deux théorèmes importants 2.17 et 2.23 deviennent ici :

Théorème 7.4. — Soit le corps fini $\mathbb{F}_p$ et soit $P \in \mathbb{F}_p[X]$ de degré d . Alors le quotient $\mathbb{F}_p[X]/(P)$, muni des deux lois $+$ et $\cdot$ induite de $\mathbb{F}_p$, est un anneau fini de cardinal p^d , où $d = \deg(P)$. Si de plus P est un polynôme irréductible alors le quotient $\mathbb{F}_p[X]/(P)$ est un corps fini de cardinal p^d .

Posons $\alpha = \overline{X} \in \mathbb{F}_p[X]/(P)$. Chaque classe de $\mathbb{F}_p[X]/(P)$ contient un unique polynôme A de degré plus petit que d ; écrivons $A = a_0 + a_1X + \dots + a_dX^d$. Alors il vient $\overline{Q} = a_0 + a_1X + \dots + a_dX^d = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{d-1}\alpha^{d-1}$ (ici on a posé $a_0\overline{1} = a_0$). Ainsi, nous venons de montrer que tout élément $\beta \in \mathbb{F}_p[X]/(P)$ s'écrit de façon unique

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{d-1}\alpha^{d-1},$$

avec $\alpha_i \in \mathbb{F}_p$. On écrit alors $\mathbb{F}_p[X]/(P) := \mathbb{F}_p(\alpha)$.

En conclusion, $\mathbb{F}_p(\alpha)$ est un espace vectoriel de dimension d sur $\mathbb{F}_p$ de base $\{\overline{1}, \alpha, \dots, \alpha^{d-1}\}$, muni d'une multiplication avec la relation $P(\alpha) = 0$.

Comme pour $\mathbb{Z}$, on peut se poser la question de l'existence d'une infinité de polynômes $P \in \mathbb{F}_p[X]$ irréductibles.

Proposition 7.5. — Soit $n \geq 1$. Il existe une infinité de polynôme $P \in \mathbb{F}_p[X]$ (unitaires) irréductibles et de degré plus grand que n .

Démonstration. — La preuve est identique à celle pour $\mathbb{Z}$, cf théorème 1.32. Quant à l'assertion sur le degré, cela provient tout simplement du fait que l'ensemble des polynômes de $\mathbb{F}_p[X]$ de degré plus petit que n est fini : il est de cardinal plus petit que p^n . □

Conclusion : on sait construire des corps finis $\mathbb{F}$ de cardinalité p^d , avec $d \rightarrow \infty$. Nous allons montrer que c'est la seule méthode pour construire un corps fini de cardinal p^d , d quelconque.

7.2. Existence et unicité. — Commençons par donner le résultat suivant.

Théorème 7.6. — Soit $\mathbb{F}$ un corps fini à $q := p^d$ éléments. Alors pour tout $x \in \mathbb{F}$, il vient $x^q - x = 0$. Ou encore, les éléments de $\mathbb{F}$ sont exactement les racines du polynôme $P = X^q - X$ (dans $\mathbb{F}$).

Démonstration. — En effet, $\mathbb{F}^\times$ est un groupe d'ordre $q - 1$. Par le théorème de Lagrange 14.13, pour tout $x \in \mathbb{F}^\times$, $x^{q-1} = 1$, ou encore $x^q = x$. Comme $0^q = 0$, on en déduit que tout élément de $\mathbb{F}$ est racine de $X^q - X$. On conclut avec le corollaire 6.6 qui indique que $X^q - X \in \mathbb{F}[X]$ a au plus q racines dans $\mathbb{F}$. $\square$

Nous avons vu qu'un corps fini à p éléments est unique à isomorphisme près. En fait, le théorème 7.6 permet de montrer le théorème suivant (que l'on admet)

Théorème 7.7. — Soit un nombre premier p et soit $d \geq 1$. Il existe un unique corps fini de cardinal p^d (à isomorphisme près). On le note $\mathbb{F}_{p^d}$.

7.3. Structure multiplicative. — Commençons par rappeler un résultat assez général.

Lemme 7.8. — Soit un corps $\mathbb{F}$. Alors tout sous-groupe fini de $\mathbb{F}^\times$ est cyclique. En particulier $\mathbb{F}^\times$ est cyclique pour tout corps fini $\mathbb{F}$.

Démonstration. — Soit un sous-groupe fini G de $(\mathbb{F}^\times, \cdot)$. C'est un groupe abélien fini. Par le théorème de structure des groupes abéliens finis, il existe des entiers $a_1 \mid \cdots \mid a_n$ tels que $G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$. En particulier, tout élément x de G vérifie $x^{a_n} = 1$ et est donc racine de $X^{a_n} - 1$. Or dans un corps $\mathbb{F}$, un polynôme Q non nul a au plus $\deg(Q)$ racines (utiliser la division euclidienne dans $\mathbb{F}[X]$) et donc nécessairement $G \simeq \mathbb{Z}/a_n\mathbb{Z}$. $\square$

On a alors le théorème suivant.

Théorème 7.9. — Soit un corps fini $\mathbb{K}$ de cardinal p^d . Alors il existe $a \in \mathbb{K}$ tel que $\mathbb{K}^\times = \langle a \rangle$.

Démonstration. — Le résultat se déduit du lemme 7.8. $\square$

Remarque 7.10. — Ainsi ce théorème montre que comme pour $\mathbb{F}_p$, il est possible de définir le logarithme discret dans $\mathbb{F}_q$.

Exemple 7.11. — Soit le corps fini $\mathbb{F}_2$. Le polynôme $P = X^2 + X + \bar{1} \in \mathbb{F}_2[X]$ n'a pas de racine sur $\mathbb{F}_2$, il est irréductible. Ainsi le quotient $\mathbb{K} := \mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps fini à 4 éléments. Tout élément de $\mathbb{K}$ s'écrit de façon unique $a_0 + b\alpha$, où α est la classe de X (modulo P) et où $a_i \in \mathbb{F}_2 = \{\bar{0}, \bar{1}\}$. On écrit alors $\mathbb{K} = \mathbb{F}_2(\alpha)$. L'élément α vérifie donc la relation $\alpha^2 + \alpha + \bar{1} = \bar{0}$. Effectuons quelques calculs dans le corps $\mathbb{K}$. Soit $\beta = \alpha + 1$. Alors $\beta^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + \bar{1}$. Mais ici $2\alpha = \bar{0}$ et ainsi $\beta^2 = \alpha^2 + \bar{1} = -(\alpha + \bar{1}) + \bar{1} = \alpha$, car $-\bar{1} = \bar{1}$. Puis $\beta^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + \bar{1} + \alpha = \bar{1}$, ce qui illustre le théorème 7.9.

8. L'automorphisme de Frobenius

Soit $q = p^d$ une puissance du nombre premier p , et soit $\mathbb{F}_q$ le corps fini à q éléments.

Soit φ l'application

$$\begin{aligned} \varphi : \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ x &\mapsto x^p. \end{aligned}$$

Observons que $\varphi(x) = x$ pour tout $x \in \mathbb{F}_p$.

Posons $\varphi_d := \overbrace{\varphi \circ \varphi \cdots \circ \varphi}^d$.

Proposition 8.1. — Soit $q = p^d$.

- 1) L'application φ est un automorphisme (de corps) de $\mathbb{F}_q$.
- 2) On a $\varphi_d = \text{id}$. Ou encore φ_d agit trivialement sur $\mathbb{F}_q$.

Démonstration. — Observons que pour $x, y \in \mathbb{F}_q$, il vient $(x + y)^p = x^p + y^p$: cela provient du fait que $\mathbb{F}_q$ est de caractéristique p . De ceci, on montre facilement que φ est un automorphisme de corps. Soit $x \in \mathbb{F}_q$. Observons que $\varphi(\varphi(x)) = x^{p^2}$, par conséquent $\varphi_d(x) = x^q = x$, ceci par le théorème 7.6. $\square$

Définition 8.2. — L'application φ est appelée automorphisme de Frobenius. Pour tout $d \geq 1$, c'est un automorphisme du corps fini $\mathbb{F}_{p^d}$ qui agit trivialement sur $\mathbb{F}_p$.

Théorème 8.3. — On a $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{d'}}$ si et seulement si, $d \mid d'$.

Démonstration. — • Supposons que $d' = nd$. Nous avons le lemme suivant

Lemme 8.4. — Soit $\mathbb{F}$ un corps. Soient $m > 0$ et $n \geq 1$ deux entiers. Dans $\mathbb{F}[X]$, le polynôme $X^{m^n-1} - 1$ divise $X^{m^{n-1}} - 1$.

Démonstration. — On raisonne par induction sur n . Vrai pour $n = 1$. Soit $n > 1$. Effectuons le début de la division euclidienne de $X^{m^n-1} - 1$ par $X^{m^{n-1}} - 1$:

$$X^{m^n-1} - 1 = X^{m^n-m} (X^{m^{n-1}} - 1) + X^{m^n-m} - 1$$

On divise ensuite $X^{m^n-m} - 1$ par $X^{m^{n-1}} - 1$

$$X^{m^n-m} - 1 = X^{m^n-2m+1} (X^{m^{n-1}} - 1) + X^{m^n-2m+1} - 1$$

puis

$$X^{m^n-2m+1} - 1 = X^{m^n-3m+2} (X^{m^{n-1}} - 1) + X^{m^n-3m+2} - 1$$

et après k étapes

$$X^{m^n-km+(k-1)} - 1 = X^{m^n-(k+1)m+k} (X^{m^{n-1}} - 1) + X^{m^n-(k+1)m+k} - 1.$$

Pour $k = m^{n-1} - 1$, on obtient

$$X^{m^n-m(m^{n-1}-1)+(m^{n-1}-2)} - 1 = X^{m^{n-1}-1} (X^{m^{n-1}} - 1) + X^{m^{n-1}-1} - 1.$$

Or par hypothèse de récurrence, $X^m - 1$ divise $X^{m^{n-1}-1} - 1$, ce qui implique, en remontant, que $X^m - 1$ divise $X^{m^n-1} - 1$. $\square$

Ainsi comme $\mathbb{F}_{p^{nd}}$ contient toutes les racines de $X^{p^{dn}} - X$, d'après le lemme 8.4 appliqué avec $m = p^d$, il contient les p^d racines de $X^{p^d} - X$. Or l'ensemble des racines de $X^{p^d} - X$ forme un corps à p^d éléments : en effet, si x et y sont deux racines de $X^{p^d} - X$, alors xy et $x + y$ sont aussi racines de $X^{p^d} - X$. Par unicité, c'est le corps $\mathbb{F}_{p^d}$, et ainsi $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{nd}}$.

• Supposons maintenant que $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{d'}}$. Alors $\varphi_{d'}$ agit par l'identité sur $\mathbb{F}_{p^{d'}}$, donc agit par l'identité sur $\mathbb{F}_{p^d}$. Or φ restreint à $\mathbb{F}_{p^d}$ est d'ordre d , par conséquent, $d \mid d'$. $\square$

Exemple 8.5. — Le corps $\mathbb{F}_{2^{12}}$ a pour sous-corps le treillis suivant :

$$\begin{array}{ccccc} \mathbb{F}_8 & \xrightarrow{2} & \mathbb{F}_{64} & \xrightarrow{2} & \mathbb{F}_{4096} \\ 3 \downarrow & & 3 \downarrow & & 3 \downarrow \\ \mathbb{F}_2 & \xrightarrow{2} & \mathbb{F}_4 & \xrightarrow{2} & \mathbb{F}_{16} \end{array}$$

Pour aller plus loin...

Théorème 8.6. — Soient $\mathbb{F} = \mathbb{F}_{p^d}$ un corps fini et $\mathbb{K}/\mathbb{F}$ une extension de degré n . Alors $\mathbb{K}/\mathbb{F}$ est galoisienne et le groupe de Galois $\text{Gal}(\mathbb{K}/\mathbb{F})$ est engendré par le Frobenius φ_d . En particulier $\text{Gal}(\mathbb{K}/\mathbb{F})$ est cyclique d'ordre n .

9. Polynômes primitifs

Soit $\mathbb{F}_q$ le corps fini à $q = p^d$ éléments. Le groupe $\mathbb{F}_p^\times$ est engendré par un élément ε . En particulier, $\mathbb{F} = \mathbb{F}_p(\varepsilon)$. L'élément ε est donc de degré d sur $\mathbb{F}_p$ et $(\varepsilon, \mathbb{F}_p)$ est de degré d .

Définition 9.1. — Un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré d dont une racine est d'ordre $p^d - 1$ dans $\mathbb{F}_q^\times$, est appelé polynôme primitif de degré d .

Remarque 9.2. — Observons que si une racine ε d'un polynôme irréductible $P \in \mathbb{F}_q[X]$ est d'ordre k , alors toute racine de P est d'ordre k . En particulier, si P est primitif de degré d , alors toutes les racines de P sont d'ordre $p^d - 1$ dans $\mathbb{F}_q^\times$.

Exemple 9.3. — Sur $\mathbb{F}_3[X]$, le polynôme $P = X^2 + 1$ est irréductible (il n'a pas de racine dans $\mathbb{F}_3$), mais n'est pas primitif. En effet si θ est une racine de P dans $\overline{\mathbb{F}}$, alors $\theta^2 = -1$, $\theta^4 = 1$ et donc θ est d'ordre 4. Or ici $\mathbb{F}_3(\theta) = \mathbb{F}_9$ et $\mathbb{F}_9^\times$ est cyclique d'ordre 8.

Par contre le polynôme $P = X^2 - X - 1$ est primitif (sur $\mathbb{F}_3$). Si α est une racine de P , alors $\alpha^2 = \alpha + 1$ et $\alpha^4 = -1$. L'ordre de α divise 8, il est donc égal à 8. Ainsi $\mathbb{F}_9^\times = \langle \alpha \rangle$.

Proposition 9.4. — Le nombre de polynômes primitifs de degré d sur $\mathbb{F}_p$ est exactement $\varphi(p^d - 1)/d$, où φ est la fonction d'Euler.

Démonstration. — Posons $q = p^d$. Soit ε un générateur de $\mathbb{F}_q^\times$. L'élément ε est d'ordre $p^d - 1$ et, ε^i est également d'ordre $p^d - 1$ si et seulement si $\text{pgcd}(i, p^d - 1) = 1$. Il y a donc $\varphi(p^d - 1)$ éléments de $\mathbb{F}^\times$ qui engendrent $\mathbb{F}^\times$ soit au total $\varphi(p^d - 1)/d$ polynômes primitifs. $\square$

10. Exercices

Exercice 21. — Soit le corps fini $\mathbb{F}_{19}$.

- (i) Donner les ordres possibles d'un élément de $\mathbb{F}_{19}^\times$.
- (ii) Quel est l'ordre de $\bar{3}$?
- (iii) Pour chaque ordre possible, donner un élément de $\mathbb{F}_{19}^\times$ qui a l'ordre en question.

Exercice 22. — Vérifier que 107 est un nombre premier. Soit alors le corps $\mathbb{F}_{107}$. Quels sont les ordres de $\bar{2}$ et de $\bar{3}$?

Exercice 23. — Montrer que $\bar{2}$ est une racine primitive de l'unité de $\mathbb{F}_{13}$. Donner alors la table des logarithmes en base $\bar{2}$ des éléments de $\mathbb{F}_{13}^\times$.

Exercice 24. — Montrer que $\bar{7}$ est une racine primitive de l'unité de $\mathbb{F}_{11}$. Donner alors la table des logarithmes en base $\bar{7}$ des éléments de $\mathbb{F}_{11}^\times$.

Exercice 25. — Soit le corps $\mathbb{F}_{29}$.

- (i) Montrer que $\bar{2}$ est une racine primitive de l'unité.
- (ii) Calculer $\log_{\bar{2}}(\bar{3})$.
- (iii) En déduire $\log_{\bar{2}}(\bar{6})$ puis $\log_{\bar{2}}(\bar{5})$.

Exercice 26. — Soit le corps $\mathbb{F}_{101}$. On admet que $\bar{2}$ est racine primitive de l'unité.

- (i) Déterminer un représentant principal de $\bar{2}^{50}$.
(ii) En déduire $\log_2(\overline{10})$, $\log_2(\overline{20})$ puis $\log_2(\overline{40})$.

Exercice 27. — 1. Donner quelques solutions de l'équation diophantienne $5X^2 - Y^2 = 1$, c'est à dire avec $X, Y \in \mathbb{Z}$.
2. Montrer que l'équation diophantienne $5X^2 - Y^2 = 3$ n'a pas de solution dans $\mathbb{Z}$.

Exercice 28. — Résoudre dans $\mathbb{F}_{11}$ le système
$$\begin{cases} -x + 2y = \bar{2} \\ 3x + 4y = \bar{1} \end{cases}.$$

Exercice 29. — Déterminer les polynômes irréductibles (unitaires) de $\mathbb{F}_2[X]$ de degré 1, de degré 2, de degré 3, degré 4 et de degré 5.

Exercice 30. — Déterminer les polynômes irréductibles de degré 2 de $\mathbb{F}_3$ puis de $\mathbb{F}_5$.

Exercice 31. — Soit ℓ un nombre premier. Déterminer le nombre de polynômes irréductibles de degré ℓ sur $\mathbb{F}_p$.

Exercice 32. — Dans $\mathbb{F}_2[X]$, factoriser les polynômes $P = X^4 + X^2 + X + \bar{1}$ et $Q = X^4 + X^3 + X + \bar{1}$.

Exercice 33. — Dans $\mathbb{F}_5[X]$, factoriser les polynômes $P = X^3 + X^2 + X + \bar{1}$ puis $Q = X^3 + X^2 + X + \bar{2}$.

Exercice 34. — Donner les tables d'addition et de multiplication du corps $\mathbb{F}_4$. Déterminer l'ordre de chaque élément de $\mathbb{F}_4^\times$.

Exercice 35. — Expliquer comment construire le corps à 1024 éléments.

Exercice 36. — Soit le corps fini $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, avec α vérifiant l'équation $\alpha^2 + 1 = 0$. Vérifier que le corps $\mathbb{F}_9$ contient les racines de tous les polynômes irréductibles de degré 2 de $\mathbb{F}_3[X]$.

Exercice 37. — Donner les tables d'addition et de multiplication du corps $\mathbb{F}_9$. Déterminer l'ordre de chaque élément non nul de $\mathbb{F}_9$. Parmi les polynômes irréductibles de degré 2 sur $\mathbb{F}_3$, trouver les polynômes primitifs (c'est à dire ceux dont une racine engendre $\mathbb{F}_9^\times$).

Exercice 38. — Reprendre l'exercice précédent avec $\mathbb{F}_8$.

Exercice 39. — Soit le corps fini $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$, avec α vérifiant l'équation $\alpha^4 + \alpha + 1 = 0$. Exprimer les éléments α^{-1} et $(\alpha^5 + \alpha)^{-1}$.

Exercice 40. — Soit $\mathbb{F}_q$ le corps à q éléments. On suppose q impair.

- (i) Montrer que tout élément de $\mathbb{F}_q$ est somme de deux carrés.
(ii) Montrer que -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \pmod{4}$.

Exercice 41. — A quelle condition sur le paramètre $\lambda \in \mathbb{F}_{13}$ la matrice $A = \begin{pmatrix} \bar{1} & \bar{3} \\ \bar{\lambda} & \bar{4} \end{pmatrix}$ est-elle inversible ?

Exercice 42. — Dans $\mathbb{F}_7$, inverser la matrice $B = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}$.

Exercice 43. — Dans $\mathbb{F}_2$, inverser la matrice $C = \begin{pmatrix} \bar{1} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \\ \bar{1} & \bar{1} & \bar{1} \end{pmatrix}$.

Exercice 44. — Sur $\mathbb{F}_p$, soit la matrice $A = \begin{pmatrix} \bar{1} & \bar{2} & \bar{1} \\ \bar{1} & \bar{0} & -\bar{1} \\ \bar{0} & \bar{1} & -\bar{1} \end{pmatrix}$.

(i) Calculer le polynôme caractéristique de A .

(ii) Etudier la diagonalisation de la matrice A pour $p = 2$, pour $p = 3$, pour $p = 5$ et pour $p = 13$.

Exercice 45. — Montrer qu'une matrice carrée A à coefficient dans $\mathbb{F}_p$ est diagonalisable si et seulement si, $A^p = A$.

PARTIE III UN PEU DE CRYPTOGRAPHIE

Le but de cette section est de donner quelques protocoles cryptographiques pour illustrer les sections précédentes.

Nous commencerons par donner deux protocoles symétriques (le chiffrement de Vigenère, et le chiffrement de Hill), puis un protocole d'échange de clefs (Diffie-Hellman), et enfin le protocole asymétrique RSA.

Expliquons le principe général. Deux personnes, que l'on nomme traditionnellement Alice et Bob, veulent échanger un message qu'ils souhaitent garder confidentiel. Ils vont donc procéder à un chiffrement de celui-ci. Il apparaît alors au moins trois types de principes.

— *Protocole symétrique.* Alice et Bob disposent d'une clef de chiffrement et d'une clef de déchiffrement, que eux seuls possèdent (enfin, c'est ce qu'ils espèrent...). Grâce à ces clefs, Alice peut envoyer un message chiffré à Bob, et Bob peut le déchiffrer ; et vice et versa. Et ainsi, les deux personnes sont en mesure de s'envoyer des messages : les échanges peuvent aller dans les deux sens.

— *Protocole d'échange de clefs.* Pour le protocole précédent, on voit aisément une première question : si Alice et Bob ne se rencontrent pas, comment partager un système de clefs avec une certaine sécurité ?

— *Protocole asymétrique.* Alice rend publique une clef permettant à toute personne de lui envoyer un message chiffré. Alice déchiffre à l'aide d'une clef privée tout message chiffré par cette clef publique. Cet échange ne va que dans un sens : de Bob vers Alice.

D'autres exigences peuvent apparaître comme l'authentification, la non-répudiation et l'authenticité. Nous ne les aborderons pas.

11. Quelques chiffrements classiques

11.1. Chiffrement de Vigenère. — C'est un principe de chiffrement par substitution. On commence par numéroter les lettres de l'alphabet : la lettre A est numérotée 0, la lettre B numérotée 1, ..., la lettre Z numérotée 25. Cette numérotation permet de voir l'alphabet dans l'ensemble $\{0, 2, \dots, 25\}$... que l'on peut voir dans $\mathbb{Z}/26\mathbb{Z}$.

On choisit ensuite la clef de chiffrement : c'est un mot (que l'on traduit dans $\mathbb{Z}/26\mathbb{Z}$).

Expliquons maintenant le principe de ce chiffrement à partir d'un exemple. Typiquement prenons comme clef le mot EXEMPLE, et le texte à chiffrer VOICI UN EXEMPLE. L'opération va alors être la suivante : on commence par écrire le texte à chiffrer, puis en dessous en écrit le mot clef autant de fois que nécessaire pour "couvrir" le texte.

V	O	I	C	I	U	N	E	X	E	M	P	L	E
E	X	E	M	P	L	E	X	E	M	P	L	E	E

Le chiffrement va consister à faire la somme "lettre par lettre", modulo 26. Par exemple, la première colonne voit la somme de V avec E, c'est à dire de 21 et de 4, soit 25, qui correspond à la lettre Z. Pour la seconde colonne, c'est la somme de O avec X, c'est à dire de 14 et 23, soit 37 modulo 26, c'est à dire 11, qui correspond à la lettre L.

V	O	I	C	I	U	N	E	X	E	M	P	L	E
E	X	E	M	P	L	E	X	E	M	P	L	E	E
Z	L	M	O	X	F	R	I	U	I	Y	E	W	I

Le texte chiffré est donc ZLMOX FRIUI YEWI. Le déchiffrement va consister à faire la même opération avec le mot "inverse". La clef de chiffrement EXEMPLE consiste à translater les lettres successivement rencontrées par : 4, 23, 4, 12, 15, 11, 4. Pour le déchiffrement il faut donc translater par $-4, -23, -4, -12, -15, -11, -4$, ce qui modulo 26 correspond à 22, 3, 22, 14, 11, 15, 22, soit le mot WDWOLPW.

Observons qu'avec le chiffrement de Vegenère une même lettre peut être chiffrée différemment. Ce chiffrement est protégé contre une attaque à partir de l'analyse classique des fréquences d'apparition des lettres.

Pour terminer, notons qu'il est possible d'agrandir l'alphabet en introduisant le caractère blanc, la virgule, le point, etc.

11.2. Chiffrement de Hill. —

11.2.1. Le chiffrement affine. — C'est une extension du chiffrement par transformation affine. Commençons par rappeler celui-ci. Comme précédemment on part de l'alphabet vu dans $\mathbb{Z}/26\mathbb{Z}$. Soient ensuite $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ et $b \in \mathbb{Z}/26\mathbb{Z}$. On rappelle que $a \in (\mathbb{Z}/26\mathbb{Z})^\times$ si et seulement si a est premier à 26. On considère alors l'application affine φ sur $\mathbb{Z}/26\mathbb{Z}$ définie par

$$\varphi(x) = ax + b.$$

Comme $a \in (\mathbb{Z}/26\mathbb{Z})^\times$, l'application φ est inversible d'inverse $\varphi'(y) = a^{-1}y - a^{-1}b$, où ici a^{-1} est l'inverse de a dans $\mathbb{Z}/26\mathbb{Z}$. L'application φ est la clef de chiffrement, et φ' la clef de déchiffrement.

Partons du texte à chiffrer VOICI UN EXEMPLE. Alors V est chiffrée par $\varphi(21)$, O par $\varphi(14)$, etc. Typiquement prenons $a = \bar{3}$ et $b = \bar{5}$. Il vient alors $\varphi(21) = 16$, et V est chiffrée par Q, puis $\varphi(14) = 21$, et donc O est chiffrée par V, etc. Après quelques calculs on trouve le message chiffré QVDLD NSPRH HFXR.

La relation de Bézout $9 \times 3 - 26 = 1$ montre que $(\bar{3})^{-1} = \bar{9}$, et ainsi la clef de déchiffrement est la fonction $\varphi'(y) = \bar{9}y - \bar{1}$. Le message de départ s'obtient en "appliquant" φ' au message QVDLD NSPRH HFXR.

Lorsque $a = 1$, la fonction φ correspond à une translation, c'est le principe de chiffrement de César.

11.2.2. — Le chiffrement de Hill va consister à une généralisation du chiffrement affine. On se donne un entier $n \geq 1$, puis une matrice carrée A , de taille $n \times n$, à coefficients dans $\mathbb{Z}/26\mathbb{Z}$. Le déterminant de la matrice A se calcule comme pour le cas où les coefficients sont réels ; en particulier A est inversible dès lors que $\det(A) \in (\mathbb{Z}/26\mathbb{Z})^\times$; dans ce cas, il existe une matrice B à coefficients dans $\mathbb{Z}/26\mathbb{Z}$ telle que $AB = BA = I_n$, où I_n est la matrice identité (la classe $\bar{1}$ sur la diagonale et la classe $\bar{0}$ ailleurs).

On suppose A inversible. La matrice A est la clef de chiffrement.

On va appliquer des transformations sur le texte à chiffrer sur des paquets de n lettres via la matrice A .

Voyons ce principe sur l'exemple initial. Soit le texte à chiffrer VOICI UN EXEMPLE.

Prenons $n = 2$, et soit la matrice $A = \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{1} \end{pmatrix}$ à coefficients dans $\mathbb{Z}/26\mathbb{Z}$. La matrice A a pour déterminant $-\bar{1}$, la matrice A est inversible.

Prenons le premier paquet de 2 lettres du texte à chiffrer VO. On lui associe le vecteur de coordonnées $\begin{pmatrix} \bar{21} \\ \bar{14} \end{pmatrix}$. Alors, le couple VO est chiffré par le vecteur

$$A \begin{pmatrix} \bar{21} \\ \bar{14} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{3} \\ \bar{1} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{21} \\ \bar{14} \end{pmatrix} = \begin{pmatrix} \bar{6} \\ \bar{9} \end{pmatrix};$$

le vecteur $\begin{pmatrix} \bar{6} \\ \bar{9} \end{pmatrix}$ correspond au couple de lettres GJ. Ainsi VO est chiffré en GJ.

Il vient ainsi les transformations suivantes :

$$\begin{aligned} VO &\longrightarrow \begin{pmatrix} \bar{21} \\ \bar{14} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{6} \\ \bar{9} \end{pmatrix} \longrightarrow GJ; & IC &\longrightarrow \begin{pmatrix} \bar{8} \\ \bar{2} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{22} \\ \bar{10} \end{pmatrix} \longrightarrow WK; \\ IU &\longrightarrow \begin{pmatrix} \bar{8} \\ \bar{0} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{24} \\ \bar{2} \end{pmatrix} \longrightarrow YC; & NE &\longrightarrow \begin{pmatrix} \bar{21} \\ \bar{14} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{10} \\ \bar{25} \end{pmatrix} \longrightarrow KZ; \\ XE &\longrightarrow \begin{pmatrix} \bar{0} \\ \bar{5} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{10} \\ \bar{22} \end{pmatrix} \longrightarrow KW; & MP &\longrightarrow \begin{pmatrix} \bar{24} \\ \bar{5} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{10} \\ \bar{8} \end{pmatrix} \longrightarrow KS; \\ & & LE &\longrightarrow \begin{pmatrix} \bar{13} \\ \bar{16} \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \bar{24} \\ \bar{10} \end{pmatrix} \longrightarrow YK. \end{aligned}$$

Le texte chiffré est GJWKY CKZKW KSYK.

La clef de déchiffrement est la matrice inverse de A : pour le déchiffrement, on procède comme pour le chiffrement mais avec la matrice A^{-1} .

Pour l'exemple suivi, on a $A^{-1} = \begin{pmatrix} -\bar{1} & \bar{3} \\ \bar{1} & -\bar{2} \end{pmatrix}$.

12. Le protocole de Diffie-Hellman

La question ici est la suivante : comment Alice et Bob peuvent partager une clef secrète ?

Nous allons donner le protocole de Diffie-Hellman (datant de 1976).

Soit p un nombre premier et soit $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre assez grand. On sait que l'ordre d'un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ divise $p - 1$, et qu'il existe des éléments d'ordre $p - 1$.

Le nombre premier p et l'élément g peuvent être rendus publics.

Alice choisit alors un entier n , et Bob en entier m . Alice et Bob gardent bien pour eux ces entiers.

Alice calcule g^n ; Bob calcule g^m ; ces calculs se font dans $\mathbb{Z}/p\mathbb{Z}$. Notons par g_n la classe de g^n et par g_m la classe de g^m .

Alice envoie alors g_n à Bob, et Bob envoie g_m à Alice. Ensuite, Alice calcule $(g_m)^n$ et Bob calcule $(g_n)^m$. La clef partagée est alors le résultat obtenu, car en effet on a :

$$(g_m)^n = (g^m)^n = g^{mn} = g^{nm} = (g^n)^m = (g_n)^m.$$

Observons que si une tiers personne intercepte les messages envoyés, c'est à dire g_n et g_m , il lui faut connaître n ou m pour avoir la clef. En d'autres termes, la question est la suivante : sachant g et g_m est-il facile de déterminer m ? C'est la problématique du logarithme discret... et c'est quelque chose qu'on ne sait pas résoudre "efficacement".

Bien entendu dans la pratique le nombre premier p doit être très grand ainsi que les entiers m et n . Le calcul g^m est un calcul modulo p , qui par une approche naive nécessite m opérations (dans $\mathbb{Z}/p\mathbb{Z}$). Mais on peut optimiser celui-ci. Donnons ici le principe de l'*exponentiation rapide*. Ecrivons m en base 2 :

$$m = a_0 + 2a_1 + 4a_2 + 8a_3 + \dots + 2^k a_k,$$

où $a_i \in \{0, 1\}$; cela nécessite au plus k opérations (divisions et soustractions). Observons alors que $m \geq 2^k$ et donc $k \leq \log m / \log 2$. Alors

$$g^m = g^{a_0} (g^2)^{a_1} (g^4)^{a_2} \dots (g^{2^k})^{a_k}.$$

Etant donnés les g^{2^i} , $i = 1, \dots, k$, il faut au plus k opérations pour avoir g^m . Mais comme $g^{2^{i+1}} = (g^{2^i})^2$, on voit que k opérations suffisent pour avoir la famille g^{2^i} , $i = 0, \dots, k$. Ainsi au total il faut donc de l'ordre de $k = \log m$ opérations pour avoir g^m .

Prenons un exemple. Soit le nombre premier $p = 2459$. Alors $p - 1 = 2458 = 2 \times 1229$; ici 1229 est un nombre premier. Observons alors que tout élément non nul de $\mathbb{Z}/2459\mathbb{Z}$ est d'ordre 1, 2, 1229 ou 2458 dans $(\mathbb{Z}/2459\mathbb{Z})^\times$.

Prenons $g = \bar{2}$ (la classe de 2 dans $\mathbb{Z}/2459\mathbb{Z}$). Cherchons l'ordre de g . Pour cela calculons g^{1229} en utilisant l'exponentiation rapide. Ecrivons 1229 en base 2 :

$$1229 = 1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^{10}.$$

On trouve alors

$$g^{1229} = g \cdot g^{2^2} \cdot g^{2^3} \cdot g^{2^6} \cdot g^{2^7} \cdot g^{2^{10}}.$$

Ecrivons le calcul des g^{2^k} pour $0 \leq k \leq 10$:

k	0	1	2	3	4	5	6	7	8	9	10
g^{2^k}	$\bar{2}$	$\bar{4}$	$\bar{16}$	$\bar{256}$	$\bar{1602}$	$\bar{1667}$	$\bar{219}$	$\bar{1240}$	$\bar{725}$	$\bar{1858}$	$\bar{2187}$

Alors,

$$g^{1229} = \bar{2} \cdot \bar{16} \cdot \bar{256} \cdot \bar{219} \cdot \bar{1240} \cdot \bar{2187} = \bar{-1},$$

et ainsi $(\mathbb{Z}/2459\mathbb{Z})^\times = \langle \bar{2} \rangle$: en d'autres termes $\bar{2}$ est d'ordre maximal dans $(\mathbb{Z}/2459\mathbb{Z})^\times$.

Les données $p = 2459$ et $g := \bar{2} = 2 \pmod{2459}$ peuvent être publiques.

Supposons que Alice choisisse le nombre $n = 1300$. Comme $n = 2^2 + 2^4 + 2^8 + 2^{10}$, il vient

$$g_n = g^n = g^{2^2} g^{2^4} g^{2^8} g^{2^{10}} = \bar{16} \cdot \bar{1602} \cdot \bar{725} \cdot \bar{2187} = \bar{1476}.$$

Quant à Bob, supposons qu'il choisisse le nombre $m = 123$. Comme $m = 1 + 2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7$, il vient

$$g_m = g^m = g g^{2^3} g^{2^4} g^{2^5} g^{2^6} g^{2^7} = \bar{1883}.$$

Ainsi Alice envoie à Bob la classe $\bar{1476}$ et Bob envoie à Alice la classe $\bar{1883}$. Toujours avec l'exponentiation rapide, Alice calcule $\bar{1883}^{1300}$ et Bob calcule $\bar{1476}^{123}$: la clef partagée par Alice et Bob est le résultat de ces deux calculs, à savoir $\bar{42}$.

13. Le protocole RSA (Rivest-Shamir-Adelman)

C'est un protocole asymétrique datant de 1978.

Alice va générer une clef publique qui permettra à toute personne (ici Bob) de lui envoyer un message chiffré, qu'elle pourra déchiffrer avec sa clef privée. Le protocole ici va dans un sens unique : seul Bob peut envoyer un message à Alice (le protocole ne permet pas à Alice d'envoyer un message à Bob).

Alice commence par choisir deux nombres premiers p et q (dans la pratique ces nombres premiers sont très grands). Alice effectue ensuite les opérations suivantes :

- (i) elle calcule $n = pq$,
- (ii) elle calcule $\varphi(n) = (p-1)(q-1)$,

(iii) elle choisit un entier e premier à $\varphi(n)$, et elle calcule l'inverse d de e modulo $\varphi(n)$, ou encore $[d]_{\varphi(n)} = [e]_{\varphi(n)}^{-1}$.

Notons que (i) et (ii) sont de simples multiplications. Pour (iii), il faut déterminer une relation de Bézout entre e et $\varphi(n)$, cela se fait via l'algorithme d'Euclide, c'est une opération très rapide.

Alice rend public le couple (n, e) : c'est la *clef publique*. Par contre, elle conserve secrètement l'entier d : c'est la *clef privée*. Un message sera un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Bob souhaite envoyer le message $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ à Alice : le message a peut être vu comme un entier plus petit que n et premier à n .

Bob calcule $a^e \in \mathbb{Z}/n\mathbb{Z}$; notons par b le résultat. Bob envoie alors b à Alice.

Alice reçoit b puis calcule $b^d \in \mathbb{Z}/n\mathbb{Z}$... et retrouve a .

En effet, comme $[d]_{\varphi(n)} = [e]_{\varphi(n)}^{-1}$, cela signifie qu'il existe un entier k tel que

$$de = 1 + k\varphi(n).$$

Il vient alors

$$b^d = (a^e)^d = a^{ed} = a^{1+k\varphi(n)}.$$

Par le théorème d'Euler 2.29, on a que $a^{\varphi(n)} = [1]_n$. Ainsi

$$b^d = a \cdot (a^{\varphi(n)})^k = a \cdot [1]_n^k = a.$$

Ici la sûreté du protocole réside sur le fait que, sachant (n, e) , il est difficile de déterminer $[e]_{\varphi(n)}^{-1}$. En effet, la réelle difficulté est de déterminer $\varphi(n)$ sachant n : pour cela il faut factoriser n ... ce qui est considéré comme un problème difficile.

Prenons un exemple.

Soient $p = 29$ et $q = 31$; posons $n = 29 \times 31 = 899$. On a alors $\varphi(899) = 28 \times 30 = 840$.

Prenons $e = 37$. On a la relation de Bézout

$$840 \times 10 - 227 \times 37 = 1,$$

prouvant que 37 est bien premier à 840 et que

$$[37]_{840}^{-1} = [-227]_{840} = [613]_{840}.$$

La clef publique ici est le couple $(899, 37)$ et la clef privée est l'entier 613.

Bob souhaite envoyer un entier a premier à 899 (l'algorithme d'Euclide détermine rapidement si a est bien premier à 899). Par exemple Bob souhaite envoyer $a = 121$. Il calcule alors $([121]_{899})^{37}$ par l'exponentiation rapide ; détaillons ce calcul. Établissons tout d'abord les puissances successives de $\overline{121}$ (dans $\mathbb{Z}/899\mathbb{Z}$) :

$$\overline{121}^2 = \overline{257}, \overline{121}^{2^2} = \overline{257}^2 = \overline{422}, \overline{121}^{2^3} = \overline{422}^2 = \overline{82}, \overline{121}^{2^4} = \overline{82}^2 = \overline{431}, \overline{121}^{2^5} = \overline{567}.$$

De $37 = 1 + 2^2 + 2^5$, il vient

$$\overline{121}^{37} = \overline{121} \cdot \overline{121}^{2^2} \cdot \overline{121}^{2^5} = \overline{121} \cdot \overline{422} \cdot \overline{567} = \overline{758}.$$

Ainsi Bob envoie $\overline{758}$ à Alice.

Alice calcule ensuite $([\overline{758}]_{899})^{613}$ qui est bien égal à $[121]_{899}$.

14. Exercices

Exercice 46. — On numérote les lettres de l'alphabet de 1 à 26. Le blanc, symbolisé par $\bullet$, est numéroté 0. Les éléments de cette numérotation peuvent être vus dans $\mathbb{Z}/27\mathbb{Z}$.

Pour le protocole de Hill (dans $\mathbb{Z}/27\mathbb{Z}$) avec la clef $A = \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{3} & \overline{4} \end{pmatrix}$, on reçoit le message chiffré RYCX SLTF. Déchiffrer ce message.

Exercice 47. — Soit le nombre premier $p = 47$.

- (i) Quels sont les ordres possibles des éléments de $(\mathbb{Z}/47\mathbb{Z})^\times$?
- (ii) Déterminer l'ordre de $\bar{2} \in (\mathbb{Z}/47\mathbb{Z})^\times$.
- (iii) Déterminer l'ordre de $\bar{5} \in (\mathbb{Z}/47\mathbb{Z})^\times$.
- (iii) Alice et Bob souhaitent partager une clef via le protocole de Diffie-Hellman à partir du nombre premier $p = 47$ et de $\bar{5} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Alice choisit le nombre $m = 15$ et Bob le nombre $n = 24$.
 - (a) Quelle classe va envoyer Alice ?
 - (b) Quelle classe va envoyer Bob ?
 - (c) Quelle est la clef produite ?

Exercice 48. — Soit le nombre $n = 2021 = 43 \times 47$.

- (i) Soit $e = 59$. Donner une relation de Bézout entre $\varphi(n)$ et e .
- (ii) Avec la clef publique $(2021, 59)$, Bob envoie à Alice la classe $[1969]_{2021}$. Quel est le message que Bob souhaite partager avec Alice via le protocole RSA ?

PARTIE IV APPENDICE

Rappels sur groupes

Commençons par la notion de groupe.

Définition 14.1. — Un groupe (abélien ou commutatif) G est un ensemble muni d'une loi interne + telle que

- (i) pour tout $g, g' \in G$, $g + g' = g' + g \in G$ (commutativité),
- (ii) pour tout $g, g', g'' \in G$, $g + (g' + g'') = (g + g') + g''$ (associativité),
- (iii) il existe un élément neutre, noté 0 , c'est dire tel que $g + 0 = g$, pour tout $g \in G$,
- (iv) pour tout $g \in G$, il existe un élément opposé dans G , noté $-g$, tel que $g + (-g) = 0$.

Si G est fini, son cardinal $|G|$ est appelé l'ordre de G . Un sous-groupe H de G est un sous-ensemble de G qui muni de la loi induite + forme également un groupe.

Remarque 14.2. — Ici, on a fait le choix d'utiliser une loi additive +. Pour une loi multiplicative $\cdot$, on note par 1 l'élément neutre.

Proposition 14.3. — L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la loi + (issue de l'addition dans $\mathbb{Z}$) forme un groupe : pour $[a]_n$ et $[b]_n$ de $\mathbb{Z}/n\mathbb{Z}$, on pose : $[a]_n + [b]_n = [a + b]_n$.

Remarquons immédiatement que cette loi est bien définie. En effet, si a' est autre représentant de la classe $[a]_n$, il vient $a + b \equiv_n a' + b$.

Démonstration. — La proposition 14.3 est immédiate. Notons simplement que le neutre est la classe $[0]_n$ et que l'opposé de $[a]_n$ est la classe $[-a]_n$. □

Ordre d'un élément. — Soit G un groupe. Pour $k \in \mathbb{N}$ et $g \in G$, on pose $kg = \overbrace{g + \cdots + g}^k$ puis $-kg = k(-g)$. Considérons le sous-ensemble $\langle g \rangle = \mathbb{Z}g$ de G constitué des éléments kg , avec $k \in \mathbb{Z}$. Il est alors immédiat de voir que $\langle g \rangle$ muni de la loi $+$ est également un groupe : c'est le sous-groupe de G engendré par g . En fait,

Lemme 14.4. — Soit G un groupe fini et soit $g \in G$. Alors $\mathbb{N}g = \mathbb{Z}g$.

Démonstration. — En effet, comme G est fini, il existe deux entiers $m, k \in \mathbb{N}$, $m \neq k$, tels que $mg = kg$, ce qui implique $\lambda g = 0$ avec $\lambda \in \mathbb{N}_{>0}$. Par conséquent, $-g = (\lambda - 1)g$, avec $\lambda \in \mathbb{N}$. $\square$

Définition 14.5. — Soit G un groupe fini. L'ordre de g est par définition le plus petit entier $k > 0$ tel que $kg = 0$. On le note $\text{ord}(g)$.

Remarque 14.6. — L'élément neutre est d'ordre 1.

On a le résultat suivant bien utile

Proposition 14.7. — Soit G un groupe et soit $g \in G$. Alors si g est d'ordre k et que $mg = 0$, on a $k \mid m$.

Démonstration. — Soit m tel que $mg = 0$. Effectuons la division euclidienne de m par k : il existe deux entiers q et $0 \leq r < k$ tel que $m = qk + r$. Alors $rg = mg - qkg = 0$. Par minimalité de k , on en déduit que $r = 0$. $\square$

Proposition 14.8. — Soit G un groupe fini. Alors l'ordre de g est aussi égal à l'ordre du sous-groupe $\langle g \rangle$. Ou encore, $\text{ord}(g) = |\langle g \rangle|$.

Démonstration. — Soit r l'ordre de g . D'après le lemme 14.4, $\langle g \rangle = \{0, g, \dots, (r-1)g\}$ et ainsi $|\langle g \rangle| \leq r$. Supposons que $|\langle g \rangle| < r$: il existe deux entiers $0 \leq k < m \leq r-1$ tels que $(m-k)g = 0$. Or $0 < m-k < r$, ce qui contredit la minimalité de r . $\square$

Groupes cycliques. — Introduisons la notion de groupe cyclique.

Définition 14.9. — Un groupe G est dit cyclique s'il est engendré par un élément g ; ou encore si $G = \langle g \rangle$. On dit que g est un générateur de G .

On a alors

Théorème 14.10. — Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n . Alors

- (i) tout sous-groupe H de G est cyclique,
- (ii) pour tout $d \geq 1$ diviseur de n , il existe un unique sous-groupe cyclique H de G d'ordre d .

Démonstration. — (i) Si $H = \langle 0 \rangle$, c'est immédiat ! Soit donc $a > 0$ le plus petit entier tel que $ag \in H$. Alors $\langle ag \rangle \subset H$. Soit $g' \in H$. Comme G est cyclique et fini engendré par g , il existe un entier $b \geq 0$ tel que $g' = bg$. Effectuons alors la division euclidienne de b par a : il existe deux entiers q et $0 \leq r < a-1$ tel que $b = qa + r$ ce qui implique que $rg = g' - qag \in H$. Par minimalité de a , on en déduit que $r = 0$ et donc que $g' = qag \in \langle ag \rangle$.

(ii) Soit d un diviseur de n . Posons $n_0 = n/d$. Alors n_0g est d'ordre d et ainsi $\langle n_0g \rangle$ est un sous-groupe d'ordre d (si l'ordre de n_0g était strictement plus petit que d cela impliquerait que l'ordre de g serait strictement plus petit que n). Montrons qu'un tel sous-groupe est unique. Soit H un sous-groupe de G d'ordre $d \mid n$. Nous avons vu dans (i) que $H = \langle ag \rangle$ pour un certain entier a . Mais comme ag doit être d'ordre d , cela signifie que $dag = 0$ et donc que da est un multiple de n (d'après la proposition 14.7) : il existe un entier λ tel que $da = \lambda n$ et ainsi $a = \lambda n_0$, ce qui implique que $H = \langle \lambda n_0g \rangle \subset \langle n_0g \rangle$. En comparant les ordres, on en déduit que $H = \langle n_0g \rangle$. $\square$

Enfin on termine par le résultat suivant

Théorème 14.11. — Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n . Soit $k \in \mathbb{Z}$. Alors kg est un générateur de G si et seulement si, $\text{pgcd}(k, n) = 1$. En particulier, G a exactement $\varphi(n)$ générateurs.

Démonstration. — Supposons $\text{pgcd}(k, n) = 1$. Alors il existe $u, v \in \mathbb{Z}$ tel que $ku + nv = 1$, ce qui signifie que

$$g = (ku + nv)g = kug + vng = u(kg).$$

Or pour tout élément h de G , il existe un entier m tel que $h = mg$, et ainsi $h = mu(kg)$, ce qui signifie que kg est bien un générateur de G .

Réciproquement. Supposons qu'il existe un nombre premier $p \mid \text{pgcd}(k, n)$. Posons $n_0 = n/p$ et $k_0 = k/p$. Alors

$$n_0(kg) = n_0pk_0g = nk_0g = k_0(ng) = 0.$$

Par conséquent, kg est d'ordre $n_0 < n$ et ainsi kg n'engendre pas G . $\square$

Le théorème de Lagrange. — On a le théorème suivant sur le lien entre l'ordre d'un groupe et celui d'un de ses sous-groupes.

Théorème 14.12. — Soit H un sous-groupe d'un groupe fini G . Alors $|H|$ divise $|G|$.

Démonstration. — On définit sur G une relation d'équivalence $\sim$ par : $g \sim g'$ si et seulement si, il existe $h \in H$ tel que $g = g'h$ (on utilise la notation multiplicative, le groupe G n'est pas forcément commutatif). Comme H est un groupe, il est immédiat de voir que c'est bien une relation d'équivalence. Une classe est de la forme gH . Comme G est fini, le nombre de classes est fini ; notons le k . L'ensemble de ces classes forment une partition de G : le groupe G peut s'écrire comme une réunion disjointe d'un nombre fini k de classes. Or chaque classe est de cardinal $|H|$, et ainsi $|G| = k|H|$. $\square$

On en déduit alors immédiatement le corollaire suivant.

Corollaire 14.13 (Théorème de Lagrange). — Soit G un groupe fini et soit $g \in G$. Alors l'ordre de g divise $|G|$. En particulier $|G|g = 0$.

Démonstration. — On pose $H = \langle g \rangle$. Alors d'après la proposition 14.8, $\text{ord}(g) = |H|$, et ainsi $\text{ord}(g) \mid |G|$ par le théorème 14.12, ce qui implique facilement $|G|g = 0$. $\square$

17 juillet 2025

CHRISTIAN MAIRE, Université Marie et Louis Pasteur, Institut FEMTO-ST, 15B chemin des Montboucons, 25000 Besançon
E-mail : christian.maire@univ-fcomte.fr • Url : <http://members.femto-st.fr/christian-maire/fr>