Université Paris Cité (Diderot Paris 7)

Cours d'arithmétique (M1), janvier-avril 2026

Feuille TD1 : Structures finies et arithmétique de $\mathbb{Z}$

Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 1. (Le groupe $(\mathbb{Z}/2^m\mathbb{Z})^\times$)

1. Lorsque $m = 1, 2$ vérifier que $(\mathbb{Z}/2^m\mathbb{Z})^\times$ est cyclique ; lorsque $m = 3$ vérifier que $(\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$
2. Montrer que 5 est un élément d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$. [Indication : on pourra montrer par récurrence la congruence
$$5^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}.$$
3. Montrer que -1 n'appartient pas au sous groupe engendré par 5.
4. Conclure que $(\mathbb{Z}/2^m\mathbb{Z})^\times = < 5 > \oplus < -1 >$.

Exercice 2.

1. Donner un générateur du groupe $(\mathbb{Z}/162\mathbb{Z})^\times$.
2. Donner un élément d'ordre maximal dans $(\mathbb{Z}/2592\mathbb{Z})^\times$.

Exercice 3. Pour quelles valeurs de n le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

Exercice 4. Soit p un nombre premier *impair* et $a \in \mathbb{Z}$.

1. Supposons que $a \mod p$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$, montrer que $a \mod p^2$ est un élément de $(\mathbb{Z}/p^2\mathbb{Z})^\times$ qui a pour ordre ou bien $p-1$ ou bien $p(p-1)$. Donner des exemples montrant que les deux cas peuvent se produire.
2. Supposons que $a \mod p^2$ engendre $(\mathbb{Z}/p^2\mathbb{Z})^\times$, montrer que $a \mod p^m$ est un générateur de $(\mathbb{Z}/p^m\mathbb{Z})^\times$ pour tout $m \geq 1$.
3. Peut-on donner des énoncés similaires lorsque $p = 2$?

Exercice 5. On définit un *nombre de Carmichael* comme un entier N qui n'est pas premier mais vérifie néanmoins l'analogue du petit théorème de Fermat :

$$\text{si} \quad \text{pgcd}\,(a, N) = 1, \quad \text{alors} \quad a^{N-1} \equiv 1 \mod N.$$

1. Montrer qu'un nombre de Carmichael est impair et sans facteur carré.
2. Un entier $N = p_1 \dots p_k$ est un nombre de Carmichael si et seulement si, pour tout i, on a $p_i - 1$ divise $N - 1$.
3. Montrer qu'il n'existe pas de nombre de Carmichael de la forme $N = pq$ avec p et q premiers distincts.
4. Supposons que $6m+1$, $12m+1$ et $18m+1$ soient premiers, montrer que leur produit est un nombre de Carmichael. [exemple : $N = 7.13.19$]

Exercice 6. Soit $M = 21560 = 2^3 \cdot 5 \cdot 7^2 \cdot 11$ et $N = 21576 = 2^3 \cdot 3 \cdot 29 \cdot 31$ et $G_1 = (\mathbb{Z}/M\mathbb{Z})^\times$ et $G_2 = (\mathbb{Z}/N\mathbb{Z})^\times$

1. Les deux groupes sont-ils isomorphes ? Ont-ils le même cardinal ?

2. Calculer l'exposant de ces groupes (i.e. le plus petit $m \geq 1$ tel que, si $\text{pgcd}\,(a, M) = 1$, alors $a^m \equiv 1 \mod M$)
3. Combien de solutions dans G_i l'équation $x^2 = 1$ a-t-elle ?
4. Combien de solutions dans G_i l'équation $x^2 = -1$ (resp. $x^2 = 13^2$) a-t-elle ?

Corps finis.

Exercice 7. Montrer que les anneaux $\mathbb{F}_3[X]/(X^2 + X + 2)$ et $\mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont isomorphes. Exhiber un isomorphisme explicite.

Exercice 8. Soit q une puissance d'un nombre premier.

1. Soit $f \in \mathbb{F}_q[X]$ un polynôme irréductible de degré $m \geq 1$. Montrer que f divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ si, et seulement si, $m|n$.
2. Pour $m \geq 1$, on note A_m l'ensemble des polynômes irréductibles unitaires dans $\mathbb{F}_q[X]$ de degré m. Montrer que l'ensemble A_m n'est pas vide et que :

$$\forall n \geq 1,\ X^{q^n} - X = \prod_{m|n} \prod_{f \in A_m} f.$$

Déduire que :

$$\forall n \geq 1,\ q^n = \sum_{m|n} m|A_m|.$$

3. On prend $q = 2$.
   (a) Montrer que $\prod_{f \in P_4} f = \frac{X^{16}-X}{X^4-X} \in \mathbb{F}_2[X]$.
   (b) Expliciter tous les éléments de A_4.
   (c) Calculer $|A_6|$.
4. On revient au cas général où q est une puissance d'un nombre premier. On définit la fonction $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par $\mu(1) = 1$, $\mu(p_1...p_r) = (-1)^r$ si $p_1, ..., p_r$ sont des nombres premiers deux à deux distincts et $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier.
   (a) Soient f et g deux fonctions de $\mathbb{N}$ dans $\mathbb{C}$ telles que :

$$\forall n \in \mathbb{N}, g(n) = \sum_{d|n} f(d).$$

Montrer la formule d'inversion de Möbius :

$$\forall n \in \mathbb{N}, f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right).$$

   (b) A l'aide des questions 2 et 4(a), calculer $|A_m|$ pour chaque m.

Exercice 9. Soit p un nombre premier différent de 2 et 3. On considère le polynôme $\phi_3 = X^2 + X + 1 \in \mathbb{F}_p[X]$.

1. Montrer que ϕ_3 admet une racine dans $\mathbb{F}_p$ si, et seulement si, $p \equiv 1 \mod 3$.
2. Soit L un corps de décomposition de ϕ_3 sur $\mathbb{F}_p$. Soit ζ une racine de ϕ_3 dans L. On poset $\beta := 2\zeta + 1$. Montrer que $\beta^2 = -3$.
3. Montrer que -3 est un carré dans $\mathbb{F}_p$ si, et seulement si, $p \equiv 1 \mod 3$.

Exercice 10. Soit p un nombre premier différent de 5. Soit L un corps de décomposition du polynôme $\phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$.

1. Soitt ζ une racine de ϕ_5 dans L. Montrer que $L = \mathbb{F}_p(\zeta)$.
2. Montrer que $[L : \mathbb{F}_p]$ est 1 si $p \equiv 1 \mod 5$, 2 si $p \equiv -1 \mod 5$, 4 si $p \equiv \pm 2 \mod 5$.
3. Soit $\beta := \zeta + \zeta^{-1}$. Montrer que $(2\beta + 1)^2 = 5$.
4. Utiliser les questions précédentes pour montrer que 5 est un carré dans $\mathbb{F}_p$ si, et seulement si, $p \equiv \pm 1 \mod 5$.

Exercice 11. *(Théorème de Chevalley-Warning)* Soit $P \in \mathbb{F}_q[X_1, ..., X_n]$ homogène de degré d avec $0 < d < n$. Soit $V = \{(x_1, ..., x_n) \in \mathbb{F}_q^n : P(x_1, ..., x_n) = 0\}$.

1. Soient $Q = 1 - P^{q-1} \in \mathbb{F}_q[X]$ et $S = \sum_{x \in \mathbb{F}_q^n} Q(x)$. Montrer que $S = |V|$ dans $\mathbb{F}_q$.
2. Montrer que $S = 0$.
3. Déduire de ce qui précède que P admet un zéro non trivial dans $\mathbb{F}_q^n$.
4. Par contre, il existe un polynôme $P \in \mathbb{F}_q[X_1, ..., X_n]$ homogène de degré n dont l'unique zéro dans $\mathbb{F}_q^n$ est $(0, ..., 0)$. Pouvez-vous exhiber un tel polynôme ? Vous pourrez vous aider de la fonction norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Exercice 12. Soient $P_1, \ldots, P_r \in \mathbb{F}_q[X_1, ..., X_n]$ des polynômes homogène de degrés respectifs $d_1, \ldots, d_r > 0$ avec $d_1 + \cdots + d_r < n$. Montrer que le système $P_1(x_1, \ldots, x_n) = \cdots = P_r(x_1, \ldots, x_n) = 0$ admet une solution non nulle dans $\mathbb{F}_q^n$. On pourra s'inspirer de l'exercice précédent.

Résidus quadratiques.

Exercice 13. Déterminer si 2024 est un carré modulo 2953. On remarquera que 2953 est premier.

Exercice 14. Soit p un nombre premier impair. Soit C le nombre de carrés modulo p appartenant à l'intervalle $\{1, \ldots, \frac{p-1}{2}\}$, et soit N celui des non carrés.

1. Montrer que, si $p \equiv 1 \mod 4$, alors $C = \frac{p-1}{4}$.
2. Montrer que $C = N$ si, et seulement si, $p \equiv 1 \mod 4$.

On cherche à montrer que, si $p \equiv 3 \mod 8$ et $p \neq 3$, alors $C \equiv N \mod 3$. Pour ce faire, on introduit :

$$\alpha = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a, \quad \beta = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) a, \quad \gamma = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

1. Montrer que $\alpha = \left[1 - \left(\frac{-1}{p}\right)\right] \beta + p \left(\frac{-1}{p}\right) \gamma$.
2. Montrer que $\alpha = \left(\frac{2}{p}\right) \left[2 \left(1 - \left(\frac{-1}{p}\right)\right) \beta + p \left(\frac{-1}{p}\right) \gamma\right]$.
3. En déduire que, si $p \equiv 3 \mod 8$, alors $p\gamma = 3\beta$.
4. Conclure.

Exercice 15. Soient $\alpha, \beta \in \mathbb{F}_p^\times$. On cherche à calculer le nombre S de solutions de l'équation $\alpha x^2 + \beta y^2 = 1$ dans $\mathbb{F}_p^2$.

1. Soit $a \in \mathbb{F}_p$. Montrer que le nombre de solutions de l'équation $x^2 = a$ dans $\mathbb{F}_p$ est $N_a := 1 + \left(\frac{a}{p}\right)$.

2. En déduire que :
$$S = \sum_{\substack{a,b\in\mathbb{F}_p \\ \alpha a+\beta b=1}} N_a N_b,$$
puis que $S = p + \left(\frac{\beta}{p}\right) J$, avec :
$$J := \sum_{a\in\mathbb{F}_p} \left(\frac{a(1-\alpha a)}{p}\right).$$

3. Montrer que :
$$J = \sum_{a\in\mathbb{F}_p^\times} \left(\frac{a^{-1}-\alpha}{p}\right),$$
puis que $S = p - \left(\frac{-\alpha\beta}{p}\right)$.

Exercice 16. Pour cet exercice on commencera par réviser la preuve par Euclide de l'existence d'une infinité de nombres premiers. On demande de montrer qu'il existe ...

1. une infinité de nombres premiers congrus à $+1$ modulo 3 (resp. congrus à -1 modulo 3)
2. une infinité de nombres premiers congrus à $+1$ modulo 4 (resp. congrus à -1 modulo 4)
3. une infinité de nombres premiers congrus à -1 modulo 5 (resp. congrus à -1 modulo 8)

[Indication : Euclide introduit $N := p_1 \dots p_k + 1$, on pourra introduire $N = a(p_1 \dots p_k)^m + b$, pour a, b, m idoines.]

Arithmétique de $\mathbb{Z}$.

Exercice 17.

1. Soit $r \geq 2$. Soit a_1, ..., a_k, des entiers (dans $\mathbb{Z}$) premiers entre eux deux à deux. On suppose que $a_1 \dots a_k = b^r$. Montrer que chaque a_i s'écrit $\pm b_i^r$ avec $b_i \in \mathbb{Z}$.
2. Trouver toutes les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation :
$$4x^2 = y^3 + 1.$$

Exercice 18. On se propose de décrire l'ensemble des solutions $(x, y, z) \in \mathbb{Z}^3$ de l'équation
$$x^2 + y^2 = z^2. \tag{1}$$

1. Soit $d = \text{pgcd}\,(x, y)$, montrer que d divise z ; en remplaçant (x, y, z) par $(x/d, y/d, z/d)$ on peut donc se ramener à supposer x, y, z premiers entre deux à deux.
2. Montrer que z est impair et, quitte à échanger x et y, on a x impair et y pair.
3. En utilisant $y^2 = (z-x)(z+x)$ et l'exercice précédent, en déduire l'existence d'entiers a, b tels que $z + x = 2a^2$ et $z - x = 2b^2$
4. Conclure que, à permutation près de x et y, l'ensemble des solutions de (1) s'écrit
$$S = \{(d(a^2 - b^2), 2dab, d(a^2 + b^2)) \mid \text{avec } d \geq 1 \text{ et } \text{pgcd}\,(a, b) = 1\}.$$

Exercice 19. On commence dans cet exercice l'étude de l'équation de Pell-Fermat, pour un entier $d \geq 1$ fixé, on cherche les paires $(x, y) \in \mathbb{Z}^2$ telles que :
$$x^2 - dy^2 = +1. \tag{2}$$

1. Si $d = e^2$ est un carré, montrer que les seules solutions entières sont $(x, y) = (\pm 1, 0)$.
2. Montrer que l'opération $(x_1, y_1) * (x_2, y_2) := (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)$ définit une loi de groupe sur l'ensemble des solutions de (2).
3. Vérifier que si $x^2 - dy^2 = -1$ alors $(x^2 + dy^2, 2xy)$ est une solution de (2).
4. Déduire de la question 2 que, s'il existe une solution (x_1, y_1) non triviale (i.e. avec $y_1 \neq 0$), alors il existe une infinité de solutions.
5. On considère le cas $d = 2$, vérifier que $(x_1, y_1) = (3, 2)$ est une solution. On note (x_n, y_n) la suite obtenue par induction $(x_n, y_n) = (x_{n-1}, y_{n-1}) * (x_1, y_1)$; on note $(x_0, y_0) = (1, 0)$; est-il vrai que l'ensemble des solutions s'écrit

$$S = \{(\pm x_n, \pm y_n) \mid \text{pour } n \geq 0\} \, ?$$

Exercice 20. On se propose de montrer que l'ensemble des solutions $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ de l'équation suivante (3) est vide.

$$2y^2 = x^4 - 17. \tag{3}$$

[Indication pour l'exercice : penser à utiliser la *loi de réciprocité quadratique* !]

1. Montrer qu'une solution rationnelle de (3) s'écrit $(x, y) = (A/D, B/D^2)$ avec A, B D entiers vérifiant $\text{pgcd}\,(A, D) = \text{pgcd}\,(B, D) = 1$ et l'équation :

$$2B^2 = A^4 - 17D^4. \tag{4}$$

2. Montrer que si q premier divise B alors q est un carré modulo 17. [Indication : on distinguera $q = 2$ ou q impair et dans ce dernier cas on montrera d'abord que 17 est un carré modulo q.]
3. En déduire que B est un carré modulo 17 et que 2 est un bicarré modulo 17.
4. On note $\mathcal{C}_4 := \{a^4 \mid a \in \mathbb{F}_{17}^*\}$. Montrer que $\mathcal{C}_4 := \{a \in \mathbb{F}_{17}^* \mid a^4 = 1\}$ et conclure que $2 \notin \mathcal{C}_4$.
5. En déduire que l'équation $2y^2 = x^4 - 17$ ne possède aucune solution rationnelle.

Exercice 21. Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ une solution de l'équation suivante :

$$x^2 = y^3 + 7. \tag{5}$$

1. Montrer que y est impair.
2. Montrer que $y^3 + 8$ admet un facteur premier congru à 3 modulo 4.
3. Aboutir à une contradiction.

Algorithmes, primalité et factorisation.

Exercice 22. Afin de communiquer en toute sécurité, Sacha Ketchum et Pikachu chiffrent leurs messages à l'aide du système RSA. Ils choisissent de travailler dans $(\mathbb{Z}/N\mathbb{Z})^\times$, avec $N = 55$.

1. Calculer $\varphi(N)$.
2. Sacha choisit comme clé publique 3 et Pikachu 7. Quelles sont leurs clés privées ?
3. Sacha souhaite envoyer le message $M = 2 \in \mathbb{Z}/55\mathbb{Z}$ de manière chiffrée. Que doit-il envoyer à Pikachu ?
4. Sacha reçoit le message $M' = 21 \in \mathbb{Z}/55\mathbb{Z}$ de la part de Pikachu. Pouvez-vous l'aider à déchiffrer ce message ?

Exercice 23. Sacha Ketchum tente de communiquer de manière sécurisée avec Pikachu et Salamèche à l'aide du système RSA. Il a malheureusement la mauvaise idée d'utiliser le même modulo $N = pq$ (où p et q sont deux grands nombres premiers distincts) pour communiquer avec ses deux compagnons. On note c_K, c_P et c_S les clés publiques de Sacha Ketchum, Pikachu et Salamèche respectivement. On note d_K, d_P et d_S leurs clés privées. De manière imprudente, Sacha envoie un même message m à Pikachu et à Salamèche.

1. Sous leurs formes chiffrées, quels sont les messages m_P et m_S que Sacha a envoyés à Pikachu et Salamèche ?
2. On suppose que $c_P \wedge c_S = 1$. Miaouss intercepte les messages chiffrés envoyés par Sacha. Vérifiez qu'il peut retrouver le message initial m par la procédure suivante :
   (i) Calculer l'inverse b_P de c_P modulo c_S.
   (ii) Calculer $b_S := \frac{b_P c_P - 1}{c_S}$.
   (iii) Trouver m en calculant $m_P^{c_K b_P} m_S^{-c_K b_S}$ modulo N.

Exercice 24. On choisit $N_1 = 7$, $N_2 = 21$ et $N_3 = 561$.

1. Vérifer que N_1 est un nombre premier à l'aide du test de Solovay-Strassen.
2. Vérifier que N_2 n'est pas premier à l'aide du test de Fermat.
3. Montrer que N_3 n'est pas premier à l'aide du test de Rabin-Miller. Auriez-vous pu faire de même avec le test de Fermat ?

Exercice 25. Un nombre de Fermat est un nombre de forme $F_n = 2^{2^n} + 1$. Montrer que F_n est premier si, et seulement si, $3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$.