121 Nombres premiers. Applications.

I - Généralités

1. Nombres premiers et premiers entre eux

Définition 1. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b (ou que b est un **multiple** de a), et on note $a \mid b$ s'il existe $n \in \mathbb{Z}$ tel que $b = an$. Dans le cas contraire, on note $a \nmid b$. [GOU21] p. 9

Théorème 2 (Division euclidienne dans $\mathbb{Z}$).

$$\forall (a, b) \in \mathbb{Z}^2, \exists ! (q, r) \in \mathbb{Z}^2 \text{ tel que } a = bq + r \text{ et } r \in [\![0, |b|]\!]$$

Définition 3. Soient $a_1, \dots, a_n \in \mathbb{Z}$. Par principalité de $\mathbb{Z}$, il existe un unique $d \in \mathbb{N}$ tel que

$$a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$$

Ainsi défini, d s'appelle le **pgcd** de $a_1, \dots, a_n$ et on note $d = \mathrm{pgcd}(a_1, \dots, a_n)$.

Remarque 4. Dans la définition précédente, d est le plus entier naturel divisant tous les a_i.

Définition 5. Soient $a_1, \dots, a_n \in \mathbb{Z}$. Lorsque $\mathrm{pgcd}(a_1, \dots, a_n) = 1$, on dit que $a_1, \dots, a_n$ sont **premiers entre eux** *dans leur ensemble*. Lorsque $\mathrm{pgcd}(a_i, a_j) = 1$ dès que $i \neq j$, on dit que $a_1, \dots, a_n$ sont **premiers entre eux** *deux à deux*.

Théorème 6 (Bézout). Soient $a_1, \dots, a_n \in \mathbb{Z}$.

$$\mathrm{pgcd}(a_1, \dots, a_n) = 1 \iff \exists u_1, \dots, u_n \in \mathbb{Z} \text{ tels que } \sum_{i=1}^{n} u_i a_i = 1$$

Théorème 7 (Gauss). Soient $a, b, c \in \mathbb{Z}$.

$$a \mid bc \text{ et } \mathrm{pgcd}(a, b) = 1 \implies a \mid c$$

Définition 8. On dit qu'un entier naturel p est **premier** s'il est supérieur ou égal à 2 et si ses seuls diviseurs positifs sont 1 et p. [ROM21] p. 304

Exemple 9. Les nombres de Fermat $F_n = 2^{2^n} + 1$ sont premiers pour $n \in [\![0,4]\!]$, mais pas pour $n \in [\![5,32]\!]$.

Théorème 10 (Euclide)**.** L'ensemble $\mathscr{P}$ des nombres premiers est infini.

Théorème 11 (Fondamental de l'arithmétique)**.** Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme :

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}$$

où les p_k sont des nombres premiers distincts et où les α_k sont des entiers naturels non nuls.

Proposition 12. (i) Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$, alors $\operatorname{pgcd}(n,m) = \prod_{i=1}^{k} p_i^{\inf(\alpha_i,\beta_i)}$. [GOU21] p. 11

(ii) Soient $p \in \mathscr{P}$ et $k \in [\![1, p-1]\!]$. Alors $p \mid \binom{p}{k}$.

Théorème 13 (Fermat)**.** Soient $p \in \mathscr{P}$ et $a \in \mathbb{Z}$. Alors :

(i) $a^p \equiv a \mod p$.

(ii) $p \nmid a \implies a^{p-1} \equiv 1 \mod p$.

2. Fonctions arithmétiques

Définition 14. On définit : [GOZ] p. 3

— L'**indicatrice d'Euler** φ est la fonction qui à un entier k, associe le nombre d'entiers compris entre 1 et n qui sont premiers avec k.

— La **fonction de Möbius**, notée μ, par

$$\mu : \begin{array}{ccl} \mathbb{Z} & \to & \mathbb{Z} \\ n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ avec } p_1, \dots, p_k \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases} \end{array}$$

Proposition 15. (i) $\forall m, n \in \mathbb{Z}$ premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.

(ii) Pour tout entier relatif a premier avec n, $a^{\varphi(n)} \equiv 1 \mod n$.

(iii) Pour tout entier naturel n, $\sum_{d \mid n} \varphi(d) = n$.

p. 89

Théorème 16 (Formule d'inversion de Möbius)**.** Soient f et g des fonctions de $\mathbb{N}^*$ dans $\mathbb{C}$ telles que $\forall n \in \mathbb{N}^*, f(n) = \sum_{d \mid n} g(d)$. Alors,

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

Corollaire 17.

$$\forall n \in \mathbb{N}^*, \varphi(n) = \sum_{d \mid n} d\mu\left(\frac{n}{d}\right)$$

3. Répartition des nombres premiers

Définition 18. L'ensemble des générateurs de μ_n, noté μ_n^*, est formé des **racines primitives n-ièmes de l'unité**. p. 67

Proposition 19. (i) $\mu_n^* = \{e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!], \text{pgcd}(k, m) = 1\}$.

(ii) $|\mu_n^*| = \varphi(n)$, où φ désigne l'indicatrice d'Euler.

Définition 20. On appelle **n-ième polynôme cyclotomique** le polynôme

$$\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$$

Théorème 21. (i) $X^n - 1 = \prod_{d \mid n} \Phi_d$.

(ii) $\Phi_n \in \mathbb{Z}[X]$.

(iii) Φ_n est irréductible sur $\mathbb{Q}$.

Corollaire 22. Le polynôme minimal sur $\mathbb{Q}$ de tout élément ξ de μ_n^* est Φ_n. En particulier,

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(m)$$

[DEV] **Théorème 23** (Dirichlet faible)**.** Pour tout entier n, il existe une infinité de nombres premiers congrus à 1 modulo n. [GOU21] p. 99

Remarque 24. La version forte de ce théorème est que, pour tout entiers naturels a, b non nuls, il existe une infinité de nombres premiers de la forme $ak + b$, $k \in \mathbb{N}$.

p. 16

Théorème 25 (des nombres premiers)**.** Si $x > 0$, on note $\pi(x)$ le nombre de nombres premiers inférieurs à x. Alors,

$$\pi(x) \sim \frac{x}{\ln(x)}$$

II - Théorie des corps

1. Corps finis

[GOZ] p. 3

Proposition 26. Les conditions suivantes sont équivalentes :

(i) n est un nombre premier.

(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.

(iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Notation 27. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

p. 7

Définition 28. Soit A un anneau. L'application

$$f_A : \begin{array}{ccc} \mathbb{Z} & \to & A \\ n & \mapsto & \underbrace{1 + \dots + 1}_{n \text{ fois}} \end{array}$$

On note $\text{car}(A)$ l'unique $n \in \mathbb{N}$ tel que $\text{Ker}(f_A) = n\mathbb{Z}$: c'est la **caractéristique** de A.

Proposition 29. (i) Soit A un anneau intègre. Alors, $\text{car}(A) = 0$ ou p avec p premier.

(ii) Soit A un anneau fini. Alors, $\text{car}(A) \neq 0$ et $\text{car}(A) \mid |A|$.

(iii) Un anneau et un quelconque de ses sous-anneaux ont la même caractéristique.

Remarque 30. — Le Point (i) est en particulier vrai pour un corps.

— Si $\text{car}(A) = 0$, A est infini.

p. 81

Proposition 31. Soit $\mathbb{K}$ un corps fini.

(i) $\text{car}(\mathbb{K})$ est un nombre premier p.

(ii) Le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{F}_p$.

(iii) $|\mathbb{K}| = p^n$ pour $n \geq 2$.

Proposition 32. Soit $\mathbb{K}$ un corps de caractéristique p. L'application

$$\mathrm{Frob} : \begin{array}{ccc} \mathbb{K} & \rightarrow & \mathbb{K} \\ x & \mapsto & x^p \end{array}$$

est un morphisme de corps.

(i) Si $\mathbb{K}$ est fini, c'est un automorphisme.

(ii) Si $\mathbb{K} = \mathbb{F}_p$, c'est l'identité.

Théorème 33. Soient $p \in \mathscr{P}$ et $n \in \mathbb{N}^*$. On pose $q = p^n$. Alors :

(i) Il existe un corps $\mathbb{K}$ à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

(ii) $\mathbb{K}$ est unique à isomorphisme près : on le note $\mathbb{F}_q$.

Corollaire 34 (Théorème de Wilson)**.** Soit $n \geq 2$ un entier. Alors,

$$n \text{ est premier} \iff (n-1)! + 1 \equiv 0 \mod n$$

Théorème 35. $\mathbb{F}_q^*$ est cyclique, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$. [PER] p. 74

Remarque 36. En fait, tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Théorème 37 (Wedderburn)**.** Tout corps fini est commutatif. [GOU21] p. 100

2. Carrés dans les corps finis

Soit $q = p^n$ avec p premier et $n \geq 2$. [GOZ] p. 93

Proposition 38. On note $\mathbb{F}_q^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Alors $\mathbb{F}_q^{*2}$ est un sous-groupe de $\mathbb{F}_q^*$.

Proposition 39. (i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$, donc $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.

(ii) Si $p > 2$, alors :

- $\mathbb{F}_q^{*2}$ est le noyau de l'endomorphisme de $\mathbb{F}_q^*$ défini par $x \mapsto x^{\frac{q-1}{2}}$.
- $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.
- $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
- $(-1) \in \mathbb{F}_q^{*2} \iff q \equiv 1 \mod 4$.

Notation 40. Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de a modulo p. On a ainsi $\left(\frac{a}{p}\right) = \pm 1$ avec $\left(\frac{a}{p}\right) = 1$ si et seulement si $a \in \mathbb{F}_p^2$. [I-P] p. 203

Application 41 (Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où u est vu comme une permutation des éléments de V.

3. Réduction modulo p

Le résultat suivant justifie que l'on s'intéresse aux polynômes irréductibles en théorie des corps.

Théorème 42. Soit $P \in \mathbb{K}[X]$ un polynôme irréductible sur un corps $\mathbb{K}$. [GOZ] p. 57

- Il existe un corps de rupture de P.
- Si $\mathbb{L} = \mathbb{K}[\alpha]$ et $\mathbb{L}' = \mathbb{K}[\beta]$ sont deux corps de rupture de P, alors il existe un unique $\mathbb{K}$-isomorphisme $\varphi : \mathbb{L} \to \mathbb{L}'$ tel que $\varphi(\alpha) = \beta$.
- $\mathbb{K}[X]/(P)$ est un corps de rupture de P.

Lemme 43 (Gauss)**.** p. 10
(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est égal à 1).
(ii) $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[DEV] **Théorème 44** (Critère d'Eisenstein)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose qu'il existe p premier tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.
(ii) $p \nmid a_n$.
(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 45. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$. [PER] p. 67

[GOZ] p. 12

Théorème 46 (Critère d'irréductibilité modulo p)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré $n \geq 1$. Soit p un premier. On suppose $p \nmid a_n$.

Si $\overline{P}$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 47. Le polynôme $X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$.

III - Autres applications en algèbre

1. Entiers sommes de deux carrés

Notation 48. On note

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ a+ib & \mapsto & a^2+b^2 \end{array}$$

et Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P] p. 137

Remarque 49. $n \in \Sigma \iff \exists z \in \mathbb{Z}[i]$ tel que $N(z) = n$.

Théorème 50 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

2. En théorie des groupes

Soit G un groupe fini opérant sur un ensemble fini X.

[ROM21] p. 22

Définition 51. On dit que G est un p**-groupe** s'il est d'ordre une puissance d'un nombre premier p.

Théorème 52 (Formule des classes)**.** Soit Ω un système de représentants des orbites de l'action de G sur X. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \mathrm{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(\omega)|}$$

Corollaire 53. Soit p un nombre premier. Si G est un p-groupe opérant sur X, alors,

$$|X^G| \equiv |X| \mod p$$

où X^G désigne l'ensemble des points fixes de X sous l'action de G.

Corollaire 54. On note $G \cdot h_1, \dots, G \cdot h_r$ les classes de conjugaison de G. Alors,

$$\begin{aligned} |G| &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} |G \cdot h_i| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |G \cdot h_i| = 2}}^{r} \frac{|G|}{|\operatorname{Stab}_G(h_i)|} \end{aligned}$$

Corollaire 55. Soit p un nombre premier. Le centre d'un p-groupe non trivial est non trivial.

Corollaire 56. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 57 (Théorème de Cauchy)**.** On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G. Alors il existe un élément d'ordre p dans G.

Application 58 (Premier théorème de Sylow)**.** On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α. **[GOU21]** p. 44

3. RSA

Définition 59. Afin de chiffrer un **message** (tout entier découpé en séquence d'entiers de taille bornée) en utilisant RSA, on doit a besoin de deux clés : **[ULM18]** p. 62

— Une **clé privée**, qui est un couple de nombres premiers (p, q).

— La **clé publique** correspondante, qui est le couple (n, e) où $n = pq$ et e est l'inverse de d modulo $\phi(n)$ où d désigne un nombre premier à $\phi(n)$.

Nous conserverons ces notations pour la suite.

Théorème 60 (Chiffrement RSA)**.** Soit $m = (m_i)_{i \in [\![1,r]\!]}$ un message où pour tout i, $m_i < n$.

(i) Possédant la clé publique, on peut *chiffrer* ce message en un message m' :

$$m' = (m_i^e)_{i \in [\![1,r]\!]}$$

(ii) Possédant la clé privée, on peut *déchiffrer* le message m' pour reconstituer m :

$$\forall i \in [\![1, r]\!], (m_i^e)^d \equiv d \mod n$$

Remarque 61.
- L'intérêt vient pour des premiers p et q très grands : il devient alors très compliqué de factoriser n et d'obtenir la clé privée.
- Les inverses peuvent se calculer à l'aide de l'algorithme de Bézout.

Bibliographie

Les maths en tête [GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités.* 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Théorie de Galois [GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1.* 2e éd. Ellipses, 1er avr. 2009.
https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html.

L'oral à l'agrégation de mathématiques [I-P]

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements.* 2e éd. Ellipses, 26 mars 2024.
https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html.

Cours d'algèbre [PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation.* Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

Mathématiques pour l'agrégation [ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie.* 2e éd. De Boeck Supérieur, 20 avr. 2021.
https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie.

Anneaux, corps, résultants [ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation.* Ellipses, 28 août 2018.
https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html.