P. Maurer
ENS Rennes

Leçon 121. Nombres premiers. Exemples et applications.

Devs :

- Loi de réciprocité quadratique
- Théorème des deux carrés

Références :

1. Gourdon, Algèbre
2. Caldero, H2G2
3. Perrin, Cours d'algèbre
4. Ulmer, Théorie des groupes
5. Gozard, Théorie de Galois
6. FGN, Oraux X-ENS Algèbre 1
7. Carrega, Théorie des corps
8. Plans de Owen et de 20-sided dice (c'est peut être dans le De Konick, Mercier : Introduction à la théorie des nombres, mais il est à 110 euros sur Amazon, et introuvable ailleurs)...

Dans ce qui suit, n désigne un entier naturel.

1 Arithmétique dans $\mathbb{Z}$

1.1 Nombres premiers entre eux, nombres premiers, et décomposition en facteurs premiers

Définition 1. *Soit $a_1,\ldots,a_n$ des entiers. Il existe un unique entier d tel que $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}=d\mathbb{Z}$. L'entier d est appelé le* pgcd *de $a_1,\ldots,a_n$ et on note $d=\mathrm{pgcd}(a_1,\ldots,a_n)$. L'entier d est le plus grand entier naturel qui divise tous les a_i. On note aussi $a\wedge b:=\mathrm{pgcd}(a,b)$ pour $a,b\in\mathbb{Z}$.*

Définition 2. *On dit que $a_1,\ldots,a_n$ sont premiers entre eux (dans leur ensemble) lorsque $\mathrm{pgcd}(a_1,\ldots,a_n)=1$. On dit qu'ils sont premiers entre eux deux à deux si pour tout $i\neq j\in[\![1,n]\!]$, on a $\mathrm{pgcd}(a_i,a_j)=1$.*

Proposition 3. *Pour $a,a_1,\ldots,a_n\in\mathbb{Z}$, on a $\mathrm{pgcd}(a a_1,\ldots,a a_n)=|a|\,\mathrm{pgcd}(a_1,\ldots,a_n)$.*

Théorème 4. *(Bézout). Des entiers $a_1,\ldots,a_n$ sont premiers entre eux dans leur ensemble si et seulement si il existe des entiers $u_1,\ldots,u_n$ tels que $a_1u_1+\cdots+a_nu_n=1$.*

Proposition 5. *(Algorithme d'Euclide).*

Soit a et b deux éléments non nuls d'un anneau euclidien A, soit $(r_i)_i$ la suite d'éléments définie par $r_0=a$, $r_1=b$, puis, pour $r\geq 2$, $r_i=\mathrm{rem}(r_{i-2},r_{i-1})$, où $\mathrm{rem}(x,y)$ désigne la fonction qui a (x,y) associe le reste dans la division de x par y dans A.

Alors la suite $(r_i)_i$ est finie : il existe un entier $n+1$ pour lequel $r_{n+1}=0$ et $\mathrm{pgcd}(a,b)=r_n$.

Définition 6. *On dit qu'un entier $p\geq 2$ est premier si ses seuls diviseurs sont p, $-p$, 1 et -1. On notera dans la suite $\mathbb{P}$ l'ensemble des nombres premiers.*

Théorème 7. *(Fondamental de l'arithmétique). Tout entier naturel $n\geq 2$ s'écrit de manière unique sous la forme*

$$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k},$$

où les p_i sont des nombres premiers distincts et les α_i des entiers naturels non nuls. On appelle cette égalité la décomposition de n en facteurs premiers.

Proposition 8. *Soit $p\in\mathbb{P}$ et $a_1,\ldots,a_n\in\mathbb{Z}$. Si p divise $a_1\cdots a_n$, alors p divise au moins l'un des a_i.*

Proposition 9. *L'ensemble des nombres premiers est infini.*

Proposition 10. *Soit $p\in\mathbb{P}$, et $1\leq k\leq p-1$ un entier. Alors p divise $\binom{k}{p}$.*

Théorème 11. *(Fermat). Soit $p\in\mathbb{P}$. Alors pour tout $a\in\mathbb{Z}$ $a^p\equiv a[p]$ et si $p\nmid a$, $a^{p-1}\equiv 1[p]$.*

Théorème 12. *(Wilson). Soit $p\geq 2$ un entier. Alors $p\in\mathbb{P}\Longleftrightarrow(p-1)!\equiv -1[p]$.*

Exemple 13. On pose $F_n=2^{2^n}+1$. Fermat avait conjecturé, à tort, que tous les nombres F_n étaient premiers. On montre en fait que F_5 ne l'est pas : les nombres F_n qui sont bel et bien premiers s'appellent nombres premiers de Fermat.

Théorème 14. *(Gauss-Wantzel)*

Soit p un nombre premier impair, et $\alpha\in\mathbb{N}^*$. Alors l'angle $\widehat{\dfrac{2\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha=1$ et p est un nombre premier de Fermat, c'est-à-dire $p=1+2^{2^\beta}$ pour un certain $\beta\in\mathbb{N}$.

1.2 Fonctions arithmétiques

Définition 15. *(Indicatrice d'Euler)*

Pour $n\geq 1$, on définit la fonction indicatrice d'Euler par

$$\varphi\colon\begin{cases}\mathbb{N}^* & \rightarrow & \mathbb{N}^*\\ n & \mapsto & \mathrm{Card}(\{x\in[\![1,n]\!]\ :\ x\wedge n=1\})\end{cases}.$$

Proposition 16. *On a $\varphi(1)=1$. Si $n\geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z},+)$, et $\varphi(n)$ est l'ordre du groupe $((\mathbb{Z}/n\mathbb{Z})^\times,\times)$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 17. *Soit p un nombre premier, et $n\in\mathbb{N}^*$. On a $\varphi(p^n)=p^n-p^{n-1}$.*

Théorème 18. *(Euler). Soit $n\geq 2$ un entier, et a un entier relatif premier avec n. Alors $a^{\varphi(n)}\equiv 1[n]$.*

Théorème 19. *(des restes chinois). Soient $n,m\in\mathbb{N}$ avec $n,m\geq 2$ et $n\wedge m=1$. Alors les anneaux $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes.*

Corollaire 20. *Soit $n,m\in\mathbb{N}$ avec $n,m\geq 2$ et $n\wedge m=1$. Alors $\varphi(nm)=\varphi(n)\,\varphi(m)$.*

Corollaire 21. *Soit $n\geq 2$ un entier, décomposé en facteurs premiers sous la forme $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. Alors $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$.*

Proposition 22. *(formule de Gauss). Pour $n\in\mathbb{N}^*$, $n=\sum\limits_{d|n}\varphi(d)$.*

Définition 23. *On définit la fonction de Möbius $\mu\colon\mathbb{N}^*\rightarrow\{0,1,-1\}$ par $\mu(1)=1$, $\mu(n)=0$ si n contient un facteur carré, et $\mu(p_1\cdots p_r)=(-1)^r$ si $p_1,\ldots,p_r$ sont des nombres premiers distincts.*

Proposition 24. *Soit $n,m\in\mathbb{N}$ avec $n,m\geq 2$ et $n\wedge m=1$. Alors $\mu(nm)=\mu(n)\,\mu(m)$.*

Proposition 25. *(Formule d'inversion de Möbius). Soit $f\colon\mathbb{N}^*\rightarrow\mathbb{C}$ une application. On pose $g(n)=\sum_{d|n}f(d)$. Alors $f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)$.*

Application 26. On a $\varphi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)d$.

1.3 Recherche et répartition des nombres premiers

Proposition 27. *Soit $n\in\mathbb{N}^*$. Alors n est premier si et seulement si il n'admet aucun diviseur inférieur à $\sqrt{n}$.*

Proposition 28. *(Crible d'Eratosthène). On souhaite déterminer $[\![1,n]\!]\cap\mathbb{P}$ pour $n\geq 2$. On pose $\mathbb{P}_1=[\![2,n]\!]$ et $\mathbb{P}_2=\varnothing$. Tant que $P_1\neq\varnothing$, on fait $\mathbb{P}_2\leftarrow\mathbb{P}_2\cup\{\min\mathbb{P}_1\}$ et $\mathbb{P}_1\leftarrow\mathbb{P}_1\setminus(\min\mathbb{P}_1)\,\mathbb{N}^*$.*

Cet algorithme termine et lorsqu'il termine, l'ensemble $\mathbb{P}_2$ renvoyé correspond à $[\![1,n]\!]\cap\mathbb{P}$.

Définition 29. *On note $\pi(x)=\mathrm{Card}(\mathbb{P}\cap[\![0,x]\!])$.*

Proposition 30. *Pour tout $x\geq 2$, on a $\pi(x)\geq\ln(\ln(x))$.*

Théorème 31. *(Théorème des nombres premiers, admis). On a $\pi(x)\underset{x\rightarrow+\infty}{\sim}\frac{x}{\ln(x)}$.*

Théorème 32. *La série $\sum_{p\in\mathbb{P}}\frac{1}{p}$ diverge.*

Théorème 33. *(Kurschak). Pour $n\geq m\in\mathbb{N}$, on a $\sum_{i=m}^n\frac{1}{i}\in\mathbb{N}\Longleftrightarrow n=m=1$.*

2 Etude des corps finis

Dans ce qui suit, on se donne $p\in\mathbb{P}$ et on note $\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}$. On rappelle que $\mathbb{F}_p$ est un corps à p éléments.

2.1 Définitions et propriétés

Proposition 34. *Soit K un corps, et $\varphi\colon\mathbb{Z}\rightarrow K$ l'homomorphisme d'anneau défini par $\varphi(n)=n\cdot 1=1+\cdots+1$. L'ensemble $\mathrm{Ker}\,\varphi$ est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ et comme $\mathbb{Z}/p\mathbb{Z}\simeq\mathrm{Im}(\varphi)\subset K$ est intègre, $p\mathbb{Z}$ est un idéal premier. Il y a donc deux cas : p est nul ou p est premier.*

Définition 35. *On appelle caractéristique de K l'entier p tel que $\mathrm{Ker}\,\varphi=p\mathbb{Z}$, et on le note $\mathrm{car}(K)$. On a donc $\mathrm{car}(K)=0$ ou $\mathrm{car}(K)\in\mathbb{P}$.*

Proposition 36. *Si $\mathrm{car}(K)=p>0$, alors pour tout $x\in K$, on a $px=0$.*

Exemple 37. Les corps de caractéristique nulle sont infinis.

Exemple 38. Si K est fini, alors $\mathrm{car}(K)=p>0$, et $\mathbb{F}_p\subset K$. Le théorème de la base téléscopique donne alors $|K|=q=p^n$ pour un certain $n\geq 1$.

Proposition 39. *Soit K un corps de caractéristique $p>0$. L'application $F\colon K\rightarrow K$ définie par $x\mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme, et si $K=\mathbb{F}_p$, c'est l'identité.*

Théorème 40. *Soit $n\in\mathbb{N}^*$. On pose $q=p^n$. Alors il existe un corps K à q éléments, c'est le corps de décomposition du polynôme X^q-X sur $\mathbb{F}_p$. En particulier, K est unique à isomorphisme près.*

Théorème 41. *(Wedderburn). Tout corps fini est commutatif.*

2.2 Carrés dans $\mathbb{F}_p$

Notation 42. *On pose* $\mathbb{F}_q^2 := \{y \in \mathbb{F}_q\ :\ \exists x \in \mathbb{F}_q,\ y = x^2\}$, *et* $\mathbb{F}_q^{*2} := \mathbb{F}_q^* \cap \mathbb{F}_q^2$.

Proposition 43. *Si* $p = 2$, *on a* $\mathbb{F}_q^2 = \mathbb{F}_q$. *Si* $p > 2$, *on a* $|\mathbb{F}_q^2| = \frac{q+1}{2}$ *et* $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Proposition 44. *On suppose* $p > 2$ *et on se donne* $a \in \mathbb{F}_q^*$. *Alors*

$$a^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^* \end{cases}.$$

Définition 45. *On définit le symbole de Legendre pour* $p > 2$ *et* $a \in \mathbb{F}_p$ *par*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^*, \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^*, \\ 0 & \text{si } a = 0. \end{cases}$$

Remarque 46. D'après ce qui précède, pour $a \neq 0$ on a donc $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. En particulier, le symbole de Legendre est multiplicatif, au sens où $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proposition 47. *Soit* p *un nombre premier impair et* a *un élément de* $\mathbb{F}_p^*$. *On a*

$$|\{x \in \mathbb{F}_p\ :\ ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Développement 1 :

Théorème 48. *(Loi de réciprocité quadratique)*
Soit p *et* q *deux nombres premiers impairs distincts. Alors on a*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Exemple 49. Calcul du symbol de Legendre :
$\left(\frac{23}{59}\right) = (-1)^{11.29} \left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = \cdots = \left(\frac{2}{3}\right) = -1.$

Lemme 50. *Pour tout nombre premier* p *impair,* 8 *divise* $p^2 - 1$.

Proposition 51. *Pour tout nombre premier* p *impair, on a* $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

2.3 Réduction modulo p et résolution de problèmes arithmétiques

Théorème 52. *(Critère d'Eisenstein)*

Soit $P = \sum_{i=1}^{n} a_i X^i \in \mathbb{Z}[X]$, *avec* $n \geq 1$. *On suppose qu'il existe* $p \in \mathbb{P}$ *tel que :*

- p *divise* a_i *pour tout* $i \in [\![0, n-1]\!]$.
- p *ne divise pas* a_n.
- p^2 *ne divise pas* a_0.

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

Théorème 53. *Soit* $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, *et* $\bar{P}$ *sa réduction sur* $\mathbb{F}_p$, *c'est-à-dire* $\bar{P} = \sum_{i=0}^{n} \bar{a_i} X^i$. *Si* $\bar{P}$ *est irréductible sur* $\mathbb{F}_p$, *alors* P *est irréductible sur* $\mathbb{Q}$.

Exemple 54. $X^3 + X + 1$ est irréductible sur $\mathbb{Z}$.

Remarque 55. La réciproque est fausse, par exemple en prenant $P = X^4 + 1$.

Théorème 56. *Pour* $n \geq 1$, *le* $n^{\text{ème}}$ *polynôme cyclotomique* $\Phi_n(X) = \prod_{\substack{\zeta^n = 1 \\ \forall k < n, \zeta^k \neq 1}} X - \zeta$.

Alors Φ_n *est de degré* $\varphi(n)$, *vérifie* $X^n - 1 = \prod_{d|n} \Phi_d$, *est à coefficients dans* $\mathbb{Z}$ *et irréductible sur* $\mathbb{Z}$.

Définition 57. *On note* $\mathbb{Z}[i] := \{a + ib\ :\ a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$ *l'anneau des entiers de Gauss. On définit sur* $\mathbb{Z}[i]$ *l'application* $N: \mathbb{Z}[i] \to \mathbb{N}$, $a + ib \mapsto a^2 + b^2$. *Pour* $z \in \mathbb{Z}[i]$, $N(z)$ *est appelé la norme de l'entier de Gauss* z. *On remarque que* N *est multiplicative :* $\forall z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.

On note $\Sigma := \{n \in \mathbb{Z}\ :\ \exists a, b \in \mathbb{Z} \quad n = a^2 + b^2\}$ *l'ensemble des entiers qui s'écrivent comme somme de deux carrés.*

Proposition 58. $\mathbb{Z}[i]$ *est euclidien pour l'application* N, *donc principal.*

Développement 2 :

Théorème 59. *(Des deux carrés). Soit* p *un nombre premier impair. Alors* $p \in \Sigma \iff p \equiv 1[4]$.

3 Etude des p-groupes

3.1 Résultats sur les p-groupes

Définition 60. *Soit* p *un nombre premier. On appelle* p*-groupe un groupe fini d'ordre une puissance de* p.

Définition 61. *On appelle ensemble des points fixes de X sous G l'ensemble :*

$$X^G = \{x \in X \,:\, \forall g \in G \quad g.x = x\}$$

Proposition 62. *On suppose que G est un p-groupe et que X est fini. Alors on a :*

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

Corollaire 63. *Le centre d'un p-groupe distinct de $\{1\}$ n'est pas réduit à $\{1\}$.*

Corollaire 64. *Soit p un nombre premier. Alors tout groupe fini G de cardinal p^2 est abélien, et plus précisément isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou bien à $\mathbb{Z}/p^2\mathbb{Z}$.*

Exemple 65. Le corollaire devient faux pour les groupes d'ordre p^k avec $k \geq 3$. On peut donner en exemple le sous-groupe $T_3(\mathbb{F}_p)$ de $\mathrm{GL}_3(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures avec des 1 sur la diagonale, ou encore le groupe des quaternions, défini par : $\mathbb{H}_8 := \{1, -1, i, -i, j, -j, k, -k\}$ où $(-1)^2 = 1$, $-1 \times a = a \times -1 = -a$ pour tout $a \in \mathbb{H}_8$ et $i^2 = j^2 = k^2 = ijk = -1$.

Théorème 66. *(Cauchy)*

Soit G un groupe fini et p un diviseur premier de l'ordre de G. Alors G comprend au moins un élémnt d'ordre p.

3.2 Théorèmes de Sylow

Définition 67. *Soit G un groupe de cardinal $n = p^\alpha m$ avec p premier avec $p \nmid n$. On appelle p-Sylow de G tout sous-groupe de cardinal p^α.*

Exemple 68. Soit $n = p^\alpha m$ avec $p \nmid m$. Alors $\mathbb{Z}/n\mathbb{Z}$ a un unique p-Sylow donné par $\langle m \rangle$.

L'ensemble $T_n(\mathbb{F}_p)$ des matrices triangulaires supérieures de taille n avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Théorème 69. *(Sylow)* [DEV 1]

Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. Alors :

1. *G possède au moins un p-Sylow.*
2. *Les p-Sylow sont tous conjugués entre eux.*
3. *En notant k le nombre de p-Sylow, on a $k \equiv 1 \pmod p$ et k divise m.*

Exemple 70. Tout groupe d'ordre 15 est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exemple 71. Il n'existe pas de groupe simple d'ordre 63 et 255.