Leçon 121. Nombres premiers. Applications.

1. Généralité sur les nombres premiers

1.1. Les éléments premiers de l'anneau des entiers

1. Définition. Un nombre entier $n \in \mathbf{N}^*$ est *premier* s'il est supérieur à 2 et si ses seuls diviseurs positifs sont 1 et n.

2. Exemple. Les entiers 2, 3, 5 et 7 sont les quatre premiers nombres premiers.

3. Proposition. L'ensemble $\mathscr{P}$ des nombres premiers est infini.

4. Proposition. Tout entier différent de ± 1 et 0 admet un diviseur premier.

5. Proposition *(lemme d'Euclide).* Soient $n_1, \dots, n_r \in \mathbf{N}^*$ des entiers. Un nombre premier p divise le produit $n_1 \cdots n_r$ si et seulement s'il divise un des entiers n_k.

6. Théorème. Tout entier $n \geqslant 2$ s'écrit de manière unique sous la forme

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

pour des nombres premiers p_k avec $p_1 < \cdots < p_r$ et des entiers non nuls $\alpha_k \in \mathbf{N}^*$.

7. Exemple. On a $225 = 5^2 \times 7$ et $15 = 3 \times 5$.

8. Définition. Soit $n \in \mathbf{N}^*$ un entier. Il s'écrit sous la forme

$$n = \prod_{p \in \mathscr{P}} p^{v_p(n)}$$

pour une famille presque nulle d'entiers positifs $(v_p(n))_{p \in \mathscr{P}}$. Les quantités $v_p(n)$ sont les *valuations p-adiques* de l'entier n.

9. Théorème. Soient $a, b \in \mathbf{N}^*$ deux entiers. Alors les éléments

$$\prod_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))} \qquad \text{et} \qquad \prod_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$$

sont respectivement un PGCD et un PPCM des entiers a et b.

1.2. Des fonctions arithmétiques

10. Définition. La *fonction indicatrice d'Euler* est l'application

$$\varphi : \begin{vmatrix} \mathbf{N}^* \longrightarrow \mathbf{N}, \\ n \longmapsto |(\mathbf{Z}/n\mathbf{Z})^\times| = |\{k \in [\![1, n]\!] \mid k \wedge n = 1\}|. \end{vmatrix}$$

11. Théorème. Soient $n \geqslant 2$ un entier et $a \in \mathbf{N}$ un entier premier avec n. Alors

$$a^{\varphi(n)} \equiv 1 \mod n.$$

12. Proposition. Si l'entier p est premier, alors $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Par ailleurs, la fonction φ est *arithmétiquement multiplicative*, c'est-à-dire tout nombre $m, n \in \mathbf{N}^*$ premiers entre eux vérifie $\varphi(mn) = \varphi(m)\varphi(n)$. Enfin, elle vérifie

$$n = \sum_{d|n} \varphi(d).$$

13. Corollaire. Soit $n \in \mathbf{N}^*$ un entier qu'on écrit sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Alors

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}).$$

14. Définition. Pour un entier $n \in \mathbf{N}^*$ écrit sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, on pose

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \neq 1 \text{ et l'un des entiers } \alpha_i \text{ est } \geqslant 2, \\ (-1)^r & \text{sinon.} \end{cases}$$

L'application $\mu : \mathbf{N}^* \longrightarrow \{-1, 0, 1\}$ est la *fonction de Möbius*.

15. Proposition. La fonction μ est arithmétiquement multiplicative et vérifie

$$\forall n \geqslant 2, \qquad \sum_{d|n} \mu(d) = 1.$$

16. Théorème *(formule d'inversion de Möbius).* Soient G un groupe abélien additif et $f : \mathbf{N}^* \longrightarrow G$ une application. Pour tout entier $n \in \mathbf{N}^*$, on pose

$$g(n) = \sum_{d|n} f(n).$$

Alors pour tout entier $n \in \mathbf{N}^*$, on a

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, g(d).$$

17. Application. Pour tout entier $n \in \mathbf{N}^*$, on a

$$\varphi(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, d.$$

1.3. Recherche des nombres premiers, tests de primalité et non primalité

18. Proposition. Tout entier $n \geqslant 2$ qui n'est pas premier admet un diviseur premier entre les entiers 2 et $\lfloor \sqrt{n} \rfloor$.

19. Algorithme *(méthode naïve).* Pour savoir si un nombre $n \geqslant 2$ est premier, on teste s'il est divisible ou non par les entiers entre 2 et $\lfloor \sqrt{n} \rfloor$.

20. Algorithme *(crible d'Ératosthène).* On veut dresser la liste des nombres premiers jusqu'à un entier $N \geqslant 2$. Pour cela, si un entier $n \in [\![2, N]\!]$ est encore dans la liste, on teste s'il est premier ou non :

- s'il est premier, on passe au suivant dans la liste ;
- sinon on le retire ainsi que tous ses multiples.

21. Proposition. Soient $p \geqslant 2$ un entier et $a \in [\![1, p-1]\!]$ un entier. Si le nombre p est premier, alors $a^{p-1} \equiv 1 \mod p$.

22. Remarque. La contraposée de cette proposition fournit un test de non-primalité : pour tout entier $n \geqslant 2$, s'il existe un entier $a \in [\![1, p-1]\!]$ tel que $a^{n-1} \not\equiv 1 \mod n$, alors l'entier n n'est pas premier.

23. Remarque. Le problème de la factorisation d'un grand entier est difficile.

24. Application *(système RSA).* Soient p et q deux nombres premiers distincts. On pose $n \coloneqq pq$. Soit $e \in \mathbf{Z}$ un entier premier avec $\varphi(n) = (p-1)(q-1)$. Soit $d \in \mathbf{Z}$ un inverse de e modulo $\varphi(n)$. Alors $m^{cd} \equiv m \mod n$ pour tout entier $m \in \mathbf{Z}$

1.4. Répartition des nombres premiers

25. Théorème *(Dirichlet faible).* Pour tout entier $n \in \mathbf{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo n.
26. Théorème *(Dirichlet fort, admis).* Pour tous entiers $a, b \in \mathbf{N}^*$ premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo b.
27. Théorème *(des nombres premiers).* Pour un entier $x \geqslant 1$, on note $\pi(x) \geqslant 2$ le nombre de nombres premiers $\leqslant x$. Lorsque $x \longrightarrow +\infty$, on a

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

2. Théorie des corps finis

2.1. Caractéristique et sous-corps premiers

28. Proposition. Soit $n \in \mathbf{N}^*$ un entier non nul. Alors les propositions suivantes sont équivalentes :
- l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps ;
- l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre ;
- l'entier n est premier.

Pour un nombre premier p, on note $\mathbf{F}_p \coloneqq \mathbf{Z}/p\mathbf{Z}$ ce corps fini.
29. Proposition. La caractéristique d'un corps est soit nulle soit un nombre premier. En particulier, la caractéristique d'un corps fini est un nombre premier.
30. Contre-exemple. La réciproque du dernier point est fausse : le corps $\mathbf{F}_p(t)$ est infini et de caractéristique p.
31. Corollaire. Soit K un corps de caractéristique $p \geqslant 0$.
- Si $p = 0$, alors il existe un morphisme de corps $\mathbf{Q} \longrightarrow K$;
- Si $p > 0$, alors il existe un morphisme de corps $\mathbf{F}_p \longrightarrow K$.

32. Corollaire. Un corps fini est de cardinal p^n pour un entier $n \in \mathbf{N}^*$.
33. Exemple. Soit K un corps fini de caractéristique $p > 0$. Alors l'application

$$\mathrm{Frob}_K : \left| \begin{array}{l} K \longrightarrow K, \\ x \longmapsto x^p \end{array} \right.$$

est un automorphisme de corps.
34. Théorème *(Germain).* Soit $p \geqslant 3$ un nombre premier tel que le nombre $q \coloneqq 2p+1$ soit premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbf{Z}^3$ tel que

$$xyz \not\equiv 0 \mod p \qquad \text{et} \qquad x^p + y^p + z^p = 0.$$

2.2. Construction des corps finis

35. Théorème. Soient p un nombre premier et $n \in \mathbf{N}^*$ un entier non nul. Alors il existe un unique corps de cardinal $q \coloneqq p^n$ à isomorphisme près et il s'agit du corps de décomposition du polynôme $X^q - X$ sur $\mathbf{F}_p$. On le note $\mathbf{F}_q$.
36. Exemple. Attention, le corps $\mathbf{F}_q$ ne correspond pas à l'anneau $\mathbf{Z}/q\mathbf{Z}$.
37. Exemple. Le corps $\mathbf{F}_4$ s'obtient comme le quotient $\mathbf{F}_2[X]/\langle X^2 + X + 1\rangle$.
38. Théorème. Le groupe $\mathbf{F}_q^\times$ est isomorphe au groupe cyclique $\mathbf{Z}/(q-1)\mathbf{Z}$.
39. Théorème. Soient $m, n \in \mathbf{N}^*$ deux entiers non nuls. Alors il existe un morphisme de corps $\mathbf{F}_{p^m} \longrightarrow \mathbf{F}_{p^n}$ si et seulement si $m \mid n$.

2.3. Les carrés dans les corps finis

40. Définition. Soient p un nombre premier impair. Pour tout élément $a \in \mathbf{F}_p$, son *symbole de Legendre* est l'entier

$$\left(\frac{a}{p}\right) \coloneqq a^{(p-1)/2} = \begin{cases} 1 & \text{si } a \in \mathbf{F}_p^{\times 2}, \\ -1 & \text{si } a \in \mathbf{F}_p^\times \setminus \mathbf{F}_p^{\times 2}, \\ 0 & \text{si } a = 0. \end{cases}$$

41. Exemple. En reprenant l'exemple précédent, on a $(\frac{2}{7}) = 1$ et $(\frac{-1}{7}) = (\frac{3}{7}) = -1$.
42. Proposition. Pour tout élément $a \in \mathbf{F}_p^\times$, on a

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

43. Proposition. Pour tout nombre premier impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{et} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Autrement dit,
- l'entier -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$;
- l'entier 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$;

44. Théorème. L'application

$$a \in \mathbf{F}_p^\times \longmapsto \left(\frac{a}{p}\right) \in \{\pm 1\}$$

est un morphisme de groupes.
45. Théorème *(loi de réciprocité quadratique).* Soient p et q deux nombres premiers impairs. Alors

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

46. Exemple. Avec les quatre derniers points, on trouve

$$\left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$

Ainsi l'entier 14 n'est pas un carré modulo 23.

3. Théorie des p-groupes

3.1. Les p-groupes

47. Définition. Soit p un nombre premier. Un *p-groupe* est un groupe fini dont le cardinal est une puissance de l'entier p.
48. Exemple. Le groupe diédral $\mathbf{D}_4$ d'ordre 4 est un 2-groupe.
49. Lemme. Soit G un p-groupe agissant sur un ensemble fini X. On note $X^G \subset X$ l'ensemble des points fixes sous cette action. Alors

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

50. Théorème *(Cauchy).* Tout groupe fini d'ordre divisible par un nombre premier p admet un élément d'ordre p.
51. Proposition. Le centre d'un p-groupe non trivial est non trivial.

D1 — D2

3.2. Les théorèmes de Sylow

52. Définition. Soient G un groupe fini de cardinal n et p un diviseur premier de l'entier n. On note $n = p^\alpha m$ avec $p \nmid m$. Un *p-sous-groupe de Sylow* de G est un sous-groupe de cardinal p^α.

53. Exemple. Un p-sous-groupe de Sylow du groupe $\mathrm{GL}_n(\mathbf{F}_p)$ est le groupe des matrices triangulaires supérieures dont les coefficients de la diagonale valent 1.

54. Théorème *(Sylow)*. Soient G un groupe fini et p un diviseur de son ordre. Alors le groupe G contient au moins un p-sous-groupe de Sylow.

55. Théorème *(Sylow)*. Soient G un groupe fini de cardinal n et p un diviseur premier de l'entier n. On note $n = p^\alpha m$ avec $p \nmid m$. Alors

- pour tout sous-groupe $H \subset G$, il existe un p-sous-groupe de Sylow $S \subset G$ tel que $H \subset S$;
- les p-sous-groupes de Sylow sont conjugués ;
- le nombre de p-sous-groupes de Sylow vérifie $k \equiv 1 \mod p$ et $k \mid |G|$

56. Corollaire. Soit S un p-sous-groupe de Sylow de G. Alors il est distingué si et seulement s'il est l'unique p-sous-groupe de Sylow de G.

57. Application. Un groupe d'ordre 63 n'est pas simple.

[1] Éric Amar et Étienne Matheron. *Analyse complexe*. 2e édition. Cassini, 2020.
[2] Josette Calais. *Éléments de théorie des groupes*. 3e édition. Presses Universitaires de France, 1998.
[3] Serge Francinou, Hervé Gianella et Serge Nicolas. *Algèbre 1*. Cassini, 2001.
[4] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.
[5] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2e édition. De Boeck Supérieur, 2021.
[6] Felix Ulmer. *Théorie des groupes*. 2e édition. Ellipses, 2021.