121 NOMBRE PREMIERS. APPLICATIONS.

On désigne par $\mathcal{P}$ l'ensemble des nombres premiers.

I. Généralités et arithmétique dans $\mathbb{Z}$ [Rom17, Ch11, p301]

I. A. Nombres premiers et premiers entre eux

Définition 1. [entier premier]
$p \in \mathbb{N}$ est dit premier (et on note $p \in \mathcal{P}$) si p a exactement deux diviseurs positifs 1 et $|p|$.

Remarque 2. $(\mathbb{Z}, +, \times)$ est euclidien donc principal, ses idéaux sont les $(n\mathbb{Z})_{n\in\mathbb{N}}$. Dire que $p \in \mathcal{P}$ c'est dire que $p\mathbb{Z}$ est un idéal maximal.

Exemple 3. Les premiers nombres premiers sont $2, 3, 5, 7, 9, 11, 13, 17, \ldots$. Mais $6 = 2 \times 3$ n'est pas premier.

Définition 4. [entiers premiers entre eux, dans leur ensemble]
Deux entiers a et b sont dits premiers entre eux si le plus grand diviseur entier de a et b est 1.
Des entiers $(a_i)_{i\in I}$ sont dits premiers dans leur ensemble si le plus grand diviseur entier de chacun des $(a_i)_{i\in I}$ est 1.

Exemple 5. Si $p \in \mathcal{P}$ et $a \in \mathbb{N}$, p et a sont premiers entre eux si et seulement si $p \nmid a$.
$\{6, 10, 15\}$ sont premiers dans leur ensemble bien que $\{6, 10\}$, $\{6, 15\}$ et $\{10, 15\}$ ne soient pas premiers entre eux.

Application 6. Deux groupes de cardinaux premiers entre eux sont d'intersection triviale.

Lemme 7. [lemme d'Euclide] *Tout entier $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admet un diviseur premier.*

Théorème 8. [décomposition en produit de facteurs premiers]
Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ où $r \in \mathbb{N}^*$, $p_1 < p_2 < \cdots < p_r \in \mathcal{P}$ et $(\alpha_i)_{1\leq i\leq r} \in (\mathbb{N}^*)^r$.

Exemple 9. $1663200 = 2^5 \times 3^3 \times 5^2 \times 7 \times 11$.

I. B. Arithmétique [Rom17, Ch8, p231]

Définition 10. [PGCD, PPCM] On définit le PGCD (resp. PPCM) d'une famille d'éléments comme le plus grand diviseur (resp. le plus petit multiple) commun à chacun de ses éléments.

Application 11. $\mathrm{PGCD}(10, 30) = 10, \mathrm{PGCD}(2, 15) = 1, \mathrm{PPCM}(2, 3, 5, 7) = 210$.

Application 12. Calcul des PGCD et PPCM d'une famille d'éléments en fonction de leur décomposition en produit de facteurs premiers. On pourra introduire les valuations p-adique.

Théorème 13. [identité de Bézout]
Soit $r \geq 2$ et $(a_1, \ldots, a_r)$ des entiers relatifs. Si $\delta = \mathrm{PGCD}((a_i)_{1\leq i\leq r})$, alors il existe des entiers relatifs $u_1, \ldots, u_r$ tels que $\sum_{i=1}^r u_i a_i = \delta$.
Les $(a_i)_{1\leq i\leq r}$ sont premiers entre eux si et seulement si il existe des entiers relatifs $u_1, \ldots, u_r$ tels que $\sum_{i=1}^r u_i a_i = 1$.

Lemme 14. [lemme de Gauss] *Soient $a, b, c \in \mathbb{Z}$.*
(i) Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.
(ii) Si $a \mid bc$ et $b \wedge c = 1$, alors $a \mid b$ et $a \mid c$.

Application 15. Pour $p \in \mathcal{P}$ et $k \in [\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$.

I. C. Répartition des nombres premiers

Théorème 16. *$\mathcal{P}$ est de cardinal infini.*

Application 17. Le crible d'Ératosthène permet de trouver tous les nombres premiers compris entre 2 et un entier $n > 2$ fixé.

Proposition 18. *Il existe des segments de longueur arbitraire sans nombre premier.*

Théorème 19. *(admis) Notons $\Pi(n) = \mathrm{card}(\mathcal{P} \cap [\![1, n]\!])$. Alors $\Pi(n)/n \sim \frac{1}{\ln(n)}$.*

II. Tests de primalité [Rom17, §10.2/11.5-6, p280–282/324–329] [Gou09, §1.4, p34–37]

Théorème 20. [théorème d'Euler] *Soit $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1 \mod n$.*

Théorème 21. [petit théorème de Fermat]
Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tels que $p \nmid a$. Alors $a^{p-1} \equiv 1 \mod p$.

Remarque 22. La réciproque est fausse ! Par exemple avec 561. En revanche, pour tout $a \in \mathbb{Z}$, on a $a^p \equiv 1 \mod p$.

Définition 23. [Nombre de Carmichaël]
Un entier $n > 1$ non premier est de Carmichaël si $\forall a \in \mathbb{Z}, a \wedge n = 1 \implies a^{n-1} \equiv 1 \mod n$.

Proposition 24. *Un nombre de* Carmichaël *est impair et sans facteur carré.*

Application 25. [Algorithme RSA]
Alice veut envoyer un message privé à Bob.
- Bob choisit deux entiers premiers distincts $p, q \in \mathcal{P}$ et pose $n = pq$, puis il choisit ensuite $d, e \in \mathbb{Z}$ tels que $de \equiv 1 \mod \varphi(n)$ (on a $\varphi(n) = (p-1)(q-1)$ et il suffit de trouver d premier à $\varphi(n)$ et son inverse).
- Bob diffuse la clé publique (n, d) à tout le monde et converse la clé secrète (n, e).
- Pour envoyer son message $m \mod n$, Alice envoie le message chiffré $M \equiv m^d \mod n$.
- Bob déchiffre le message $m = M^e \mod n$ d'après le théorème d'Euler.

Le succès de cet algorithme réside dans la difficulté de factorisation d'un entier.

Théorème 26. [Théorème de Wilson] *Si $n \geq 2$, on a $n \in \mathcal{P} \iff (n-1)! \equiv -1 \mod n$.*

III. Applications en algèbre

III. A. Théorie de Sylow

[Per96, §1.5, p18–20]

Soit G un groupe fini d'ordre n, et $p \in \mathcal{P}$ diviseur de n. On notera $n = p^a m$ où $p \nmid m$.

Définition 27. [p-groupe, p-sous-groupe de Sylow]
Si n est une puissance de p ($m = 1$), on dit que G est un p-groupe.
Plus généralement, on appelle p-sous-groupe de Sylow (ou p-Sylow) un sous-groupe de G de cardinal p^a.

Corollaire 28. [Équation aux classes]
Si $|G| < +\infty$, choisissons pour chaque orbite O un représentant x_O. Alors on a :

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} \frac{|G|}{|\mathrm{Stab}(x_O)|}$$

Application 29. Le centre d'un p-groupe non trivial est non trivial.

Théorème 30. [Théorème de Sylow 1] *Il existe au moins un p-Sylow dans G.*

Corollaire 31. *Il existe au moins un sous-groupe de G d'ordre p^i pour tout $i \in [\![1, a]\!]$.*

Théorème 32. [Théorème de Sylow 2]
(i) si $H < G$ est un p-groupe, alors il existe un p-Sylow S tel que $H < S$,
(ii) les p-Sylow sont tous conjugués,
(iii) notons Σ le nombre de p-Sylow de G. Alors $\Sigma \mid m$ et $\Sigma \equiv 1 \mod p$.

Corollaire 33. *Soit S un p-Sylow de G. Alors $S \lhd G \iff S$ est l'unique p-Sylow de G.*

Application 34. Tout groupe d'ordre 63 ou 255 n'est pas simple.

III. B. Propriétés des corps finis

[Per96, §3.2, p72–76] [Rom17, Ch13, p415]

Pour $p \in \mathcal{P}$, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition 35. Soit A un anneau commutatif unitaire. Il existe un unique entier positif, appelé caractéristique de A, noté $\mathrm{car}(A)$, tel que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\mathrm{car}(A)\mathbb{Z}$.

Proposition 36. *Si $\mathbb{K}$ est un corps fini, sa caractéristique est un nombre premier $p \in \mathcal{P}$ et son sous-corps premier est isomorphe à $\mathbb{F}_p$.*

Corollaire 37. *Si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectorieloù $p = \mathrm{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$. De plus, tout sous-corps de $\mathbb{K}$ est de cardinal p^d pour un $d \mid n$ et réciproquement pour tout $d \mid n$ il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d.*

Théorème 38. *Il existe un corps fini à $q = p^n$ éléments pour tout $p \in \mathcal{P}, n \in \mathbb{N}^*$. Il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ ou de tout autre polynôme irréductible de $\mathbb{F}_p$. Ce corps est unique à isomorphisme près. On le note $\mathbb{F}_q$*

Exemple 39. $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments de caractéristique 2.

Corollaire 40. *Tout corps de rupture d'un polynôme P irréductible sur $\mathbb{F}_p[X]$ est un corps de décomposition de P sur $\mathbb{F}_p$.*

Définition 41. [Morphisme de Frobenius]
$\mathrm{Frob} : \mathbb{F}_q \longrightarrow \mathbb{F}_q, x \longmapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Proposition 42. *Frob est un automorphisme et les sous-corps de $\mathbb{F}_q$ sont exactement les ensembles des points fixes de Frob^d pour $d \mid n$.*

Théorème 43. *Frob est cyclique d'ordre n et on a $\mathrm{Aut}(\mathbb{F}_q) = \langle \mathrm{Frob} \rangle$.*

III. C. Résidus quadratiques modulo p

[Rom17, §13.6-7, p429–435] [Per96, §3.2, p72–76]

Soit $p \in \mathcal{P}$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \left\{x^2 \mid x \in \mathbb{F}_p\right\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 44. *Si $p = 2$, alors $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon, on a $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$.*

Application 45. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

On suppose dans la suite p impair.

Lemme 46. *On a $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.*

Exemple 47. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 48. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 49. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Exemple 50. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

Proposition 51. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Remarque 52. Le nombre de solutions de $x^2 = a$ pour $a \in \mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Théorème 53. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 54. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n :

Exemple 55. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

III. D. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p

[Per96, §3.3-3.4, p76–85]

Proposition 56. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Proposition 57. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^r a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si $p \nmid a_r$, $\forall i < r, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 58. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 59. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^r a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 60. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Définition 61. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Proposition 62. $\Phi_n \in \mathbb{Z}[X]$.

Théorème 63. [Irréductibilité de Φ_n] *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

SPEECH

Les nombres premiers apparaissent naturellement dans de nombreux domaines mathématiques. C'est pourquoi ils ont été étudié très tôt dans l'histoire des mathématiques.
La première partie contient les définitions de bases et la formulation équivalente en terme d'idéaux. Le premier résultat important est la décomposition en facteurs premiers. Notons aussi le lemme de GAUSS qui est fondamental en arithmétique. La répartition des nombres premiers est un problème très étudié, de nombreux résultats sont connus, nous en rappelons quelques uns.
Dans une deuxième partie, on s'intéresse aux applications des nombres premiers en arithmétique avec notamment les théorèmes de FERMAT et de WILSON. Cela mène aujourd'hui aux algorithmes de cryptographie qui s'appuient sur les nombres premiers.
Ensuite, on regarde les applications en algèbre, que ce soit en théorie des groupes avec les p-SYLOW, mais aussi en théorie des corps avec la notion de caractéristique, la cardinal d'un corps de caractéristique p … Le morphisme de FROBENIUS caractérise les sous-corps de $\mathbb{F}_q$. On regarde ensuite les carrés dans un corps fini via la loi de réciprocité quadratique (en développement). Citons enfin des critères d'irréductibilité de polynômes sur des anneaux comme $\mathbb{Z}[X]$ (critère d'EISENSTEIN) mais aussi l'irréductibilité des polynômes cyclotomiques (en développement) dont la preuve s'appuie sur les nombres premiers.

BIBLIOGRAPHIE

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.