Leçon 121 : Nombres premiers. Applications.

I Etude des nombres premiers

I.1 Arithmétique des entiers

Déf 1. 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. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Ex 2. Les nombres de Fermat sont les entiers de la forme $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$. Pour $n \in \{0, 1, 2, 3, 4\}$, F_n est premier. Mais F_5 n'est pas premier car $641 \mid F_5$.

Prop 3. Si p est un nombre premier, alors p est premier avec tous les entiers qu'il ne divise pas. En particulier, pour tout $k \in [\![1, p-1]\!]$, $k \wedge p = 1$.

Lemme 4 (lemme d'Euclide)**.** Soit p un nombre premier. Soient $a, b \in \mathbb{Z}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Thm 5. Pour tout entier relatif $n \in \mathbb{Z}\backslash\{-1, 0, 1\}$, n admet au moins un diviseur premier.

Thm 6. Tout entier $n \geq 2$ qui n'est pas premier a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Thm 7. Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ où les p_i sont des nombres premiers tels que $2 \leq p_1 < \dots < p_r$, et $\alpha_i \geq 1$.

I.2 Répartition des nombres premiers

Thm 8 (Euclide)**.** L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Déf 9. On définit pour tout $s > 1$ la fonction zeta de Riemann par $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$

Thm 10 (Produit Eulérien)**.** Pour tout $s > 1$, $\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p}}$

Déf 11. Pour tout $n \geq 1$, on note $\pi(n) = |\{1 \leq k \leq n : k \in \mathcal{P}\}|$ la fonction de comptage.

Thm 12 (Théorème des nombres premiers)**.** $\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$

I.3 Tests de primalités

[Odi23]

Prop 13. Si un entier n ne possède aucun diviseur premier p tel que $p^2 \leq |n|$, alors il est premier

Ex 14. 2,3,5,7 ne divisent pas 89, donc 89 est premier.

Algorithme 15 (Crible d'Eratosthène)**.** Cet algorithme permet d'obtenir la liste des nombres premiers inférieurs ou égaux à un nombre N fixé par avance :

- Choisir N.
- Ecrire la liste ordonnée des nombres entiers de 2 à N.
- Entourer le nombre 2, et barrer tous les multiples de 2.
- On prend ensuite le premier nombre de la liste non barré, et on l'entoure. On barre alors tous les multiples de ce nombre dans la liste.
- On recommence le procédé jusqu'à ce que tous les nombres soient ou barrés, ou entourés. Les nombres entourés sont alors les nombres premiers compris entre 2 et N.

Ex 16. Annexe ?

Thm 17 (Petit théorème de Fermat)**.** Soit $p \in \mathcal{P}$, alors pour $a \in \mathbb{Z}\backslash\{0\}$, $a^{p-1} \equiv 1 \pmod{p}$.

Algorithme 18 (Algorithme de Fermat)**.** Cet algorithme est un test de non primalité.

- Choisir N et a.
- Si $a^{N-1} \not\equiv 1 \pmod{N}$, alors N n'est pas premier.
- Sinon, on ne peut pas conclure.

C-ex 19. Pour tout entier non nul a, $a^{560} \equiv 1 \pmod{561}$, mais 561 n'est pas premier. On dit que c'est un nombre de Carmichael.

Prop 20. Pour tout entier non nul x et tout nombre premier $p \geq 2$, si $x^2 \equiv 1 \pmod{p}$, alors $x \equiv \pm 1 \pmod{p}$

Algorithme 21 (Test de Miller-Rabin)**.** Cet algorithme est un test de primalité probabiliste :

— Choisir N impair et un entier a.

— Factoriser N en $2^r \times k$, k impair.

— Résoudre $x_0 \equiv a^k \pmod N$.

— Si $x_0 = \pm 1$, on ne peut pas conclure. Sinon, poser $j = 1$.

— Si $j = r$, alors n n'est pas premier (par Fermat).

— Calculer $x_j \equiv (x_{j-1})^2 \pmod N$.

— Si $x_j = 1$, N n'est pas premier.

— Si $x_j = -1$, on ne peut pas conclure. Sinon, poser $j \leftarrow j+1$ et revenir à l'étape 5.

Prop 22. Cet algorithme se finit, et la probabilité que N ne soit pas premier est inférieure à 0.25. Si l'on répète k fois l'algorithme, et qu'il n'est jamais concluant, la probabilité que N soit premier est de $1 - 0.25^k$.

II Réduction modulo p

II.1 Etude de $\mathbb{Z}/p\mathbb{Z}$

Déf 23. On appelle indicatrice d'Euler la fonction définie pour tout $n \geq 1$ par $\varphi(0) = 0$, et $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Thm 24. Soit $n \geq 2$. n est un nombre premier, si et seulement si, $(\mathbb{Z}/n\mathbb{Z})$ est un corps. Si p est premier, on notera parfois $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Cor 25. Pour tout nombre premier p, $\varphi(p) = p-1$. Plus généralement, pour tout $\alpha \geq 1$, $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Thm 26 (Théorème chinois)**.** Pour tout $n_1, \dots, n_r$ premiers deux à deux entre eux, si l'on note $n = n_1 \dots n_r$, alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$.

Cor 27. Soit $n \in \mathbb{N}^*$ dont la décomposition en facteurs premiers est $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Alors $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$. Entre autre, $\varphi(n) = \prod_{i=1}^{r} (p_i - 1)p_i^{\alpha_i - 1} = n \prod_{p|n,\ p\in\mathcal{P}} (1 - \frac{1}{p_i})$

Thm 28. Pour tout p premier impair, et pour tout $\alpha \geq 1$, $((\mathbb{Z}/p^\alpha\mathbb{Z})^\times, \cdot)$ est un groupe cyclique d'ordre $(p-1)p^{\alpha-1}$.

II.2 Irréductibilité dans $\mathbb{Z}[X]$

[Odi23] Soit $P \in \mathbb{Z}[X]$.

Prop 29. S'il existe $p \in \mathcal{P}$ tel que p ne divise pas le coefficient dominant de p, et que $P \mod p$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible.

Ex 30. $P(X) = X^7 + 2X^5 + 1$ est irréductible modulo 3 dans $\mathbb{F}_3[X]$, et donc P est irréductible dans $\mathbb{Z}[X]$.

Prop 31. Si P n'a pas de racines rationnelles, qu'il existe p premier ne divisant pas le terme dominant de P, et tel que $P \mod p$ est produit de deux facteurs irréductibles dans $\mathbb{F}_p[X]$, dont un de degré 1, alors P est irréductible.

Ex 32. En raisonnant modulo 5, $P(X) = X^9 + X^4 + X^3 + 5X^2 + 11$ est irréductible dans $\mathbb{Z}[X]$.

Thm 33 (Eisenstein)**.** Soit p un nombre premier et $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ non constant. Alors si $p \nmid a_n$, pour tout $i \in [\![0, n-1]\!]$, $p \mid a_i$ et $p^2 \nmid a_0$, alors f est irréductible dans $\mathbb{Q}[X]$. Si de plus f est primitif, alors f est irréductible dans $\mathbb{Z}[X]$.

App 34. Soit Φ_p le p-ième polynôme cyclotomique. Alors $\Phi_p = 1 + X + \dots + X^{p-1}$, et il est irréductible dans $\mathbb{Z}[X]$.

Thm 35. Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$, et donc dans $\mathbb{Q}[X]$.

C-ex 36. Pour tout nombre premier p, $\Phi_4 \mod p$ n'est pas irréductible dans $\mathbb{F}_p[X]$.

Cor 37. Soit ζ une racine primitive n-ième de l'unité. Alors $\mathbb{Q}(\zeta)$ est une extension de $\mathbb{Q}$, et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

App 38 (Théorème de Dirichlet faible)**.** Si $n \geq 2$, $\mathcal{P}_{n,1} := \{p \text{ premiers } : p \equiv 1[n]\}$ est infini.

App 39 (DEV 1)**.** Soit p un nombre premier de Fermat, alors $\zeta := e^{\frac{2i\pi}{p}}$ est constructible à la règle et au compas.

Cor 40 (Gauss-Wantzel)**.** Soit $n \in \mathbb{N}^*$, le polygone régulier à n côtés est constructible si et seulement si soit $n = 2^m$ où $m \geq 2$, soit $n = 2^m p_1 \dots p_r$ où $m \in \mathbb{N}$, $r \geq 1$ et les p_i sont des nombres premiers de Fermat distincts.

Ex 41. — Le polygone régulier à 17 côtés est constructible à la règle et au compas.

— Le polygone régulier à 19 côtés n'est pas constructible à la règle et au compas.

III Théorie des groupes

[Per96] [Ulm21] Soit p un nombre premier. Soit G un groupe fini.

Notation 42. On note $X^G := \{x \in E : G \cdot x = \{x\}\}$ l'ensemble des éléments de X dont l'orbite est réduite à un point.

Déf 43. On dit que G est un p-groupe si $|G| = p^\alpha$, où $\alpha \in \mathbb{N}^*$.

Prop 44. Soit G un p-groupe agissant sur un ensemble fini X. Alors $|X| \equiv |X^G| \pmod p$.

Cor 45. Le centre d'un p-groupe distinct de $\{e\}$ n'est pas réduit à $\{e\}$.

Thm 46 (Théorème de Cauchy)**.** Soit G un groupe fini d'ordre $n \geq 2$. Si $p \mid n$, alors il existe un élément d'ordre p.

Déf 47. Si G est fini, de cardinal $n := p^\alpha m$, où $p \nmid m$. On appelle p-sous-groupe de Sylow de G un sous-groupe de G de cardinal p^α.

Rq 48. Dire que S est un p-sous-groupe de Sylow de G revient à dire que S est un p-groupe tel que $[G : S]$ est premier à p.

Ex 49. Soient $\mathbb{F}_p$ le corps fini à p éléments et $n \in \mathbb{N}^*$. Alors l'ensemble des matrices triangulaires supérieurs strictes est un p-sous-groupe de Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 50. Si G est fini, d'ordre $|G| = n = p^\alpha m$, $p \nmid m$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H

Thm 51 (Premier théorème de Sylow)**.** Si G est fini, et $p \mid |G|$, alors G contient au moins un p-sous-groupe de Sylow.

Ex 52. Un groupe G d'ordre 36 possède au moins un 3-Sylow S. Celui-ci est de cardinal 9 et d'indice 4 dans G.

Cor 53. Si $|G| = p^\alpha m$, $p \nmid m$, G contient des sous-groupes d'ordre p^i, pour $0 \leq i \leq \alpha$.

Thm 54 (Deuxième théorème de Sylow)**.** Si $|G| = p^\alpha m$, $p \nmid m$, alors si l'on note n_p le nombre de p-Sylow de G :

1. Si $H \leq G$ est un p-groupe, il existe un p-Sylow S de G contenant H.
2. Les p-Sylow sont tous conjugués.
3. $n_p \equiv 1 \pmod p$. Entre autre, $n_p \mid m$.

Cor 55. Si S est un p-Sylow de G, alors S est distingué dans G, si et seulement si, il est l'unique p-Sylow de G.

App 56. Un groupe d'ordre 200 n'est pas simple.

App 57. Un groupe d'ordre 77 est toujours cyclique.

App 58. Tout groupe d'ordre 85 est isomorphe à $\mathbb{Z}/85\mathbb{Z}$.

IV Corps finis

Soit p premier, $n \in \mathbb{N}^*$ et $q = p^n$.

IV.1 Construction des corps finis

[Odi23]

Thm 59 (Existence et "unicité" d'un corps fini)**.**
1. Le corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$ de $X^q - X$ est un corps fini de cardinal q.
2. Si $\mathbb{K}$ et $\mathbb{K}'$ sont deux corps finis de cardinal q, alors ils sont $\mathbb{Z}/p\mathbb{Z}$–isomorphes.

Notation 60. On notera $\mathbb{F}_q$ le corps fini de cardinal q, unique à $\mathbb{Z}/p\mathbb{Z}$–isomorphe près.

Rq 61. $\mathbb{F}_q = \mathbb{F}_p(\alpha_1, \ldots, \alpha_q) = \{\alpha_1, \ldots, \alpha_q\}$ où $\alpha_1, \ldots, \alpha_q$ sont les racines de $X^q - X \in \mathbb{F}_p[X]$

Ex 62. $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$ où α est une racine de $X^4 - X \in \mathbb{F}_2[X]$ différente de 0 et 1.

Thm 63. Soit α un générateur de $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p(\alpha)$

Thm 64. Il existe au moins un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n, et on a alors que $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$.

Ex 65. X^2+X+1 est irréductible sur $\mathbb{F}_2$, et il vient que $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$. Soit α une racine de X^2+X+1, alors $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{a+b\alpha : a,b \in \mathbb{F}_2\} = \{0,1,\alpha,1+\alpha\}$.

IV.2 Carrés dans un corps fini

Soient $q = p^n$ où $p \in \mathcal{P}$, $n \in \mathbb{N}^*$.

Déf 66. On note $\mathbb{F}_q^{[2]} = \{x^2 : x \in \mathbb{F}_q\}$ l'ensemble des carrés de $\mathbb{F}_q$.

Thm 67. i) Si $\mathrm{car}(\mathbb{F}_q) = 2$, alors $\mathbb{F}_q^{*[2]} = \mathbb{F}_q^*$.

ii) Si $\mathrm{car}(\mathbb{F}_q) \neq 2$:

(a) $\left|\mathbb{F}_q^{*[2]}\right| = \dfrac{q-1}{2}$ et pour tout $\alpha \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*[2]}$, $\mathbb{F}_q^* = \mathbb{F}_q^{*[2]} \bigsqcup \alpha\mathbb{F}_q^{*[2]}$

(b) $x \in \mathbb{F}_q^{*[2]}$ si et seulement si $x^{\frac{q-1}{2}} = 1$

(c) $-1 \in \mathbb{F}_q^{[2]}$ si et seulement si $q \equiv 1[4]$

On suppose p impair.

Déf 68 (Symbole de Legendre)**.** Pour tout $a \in \mathbb{Z}$ non divisible par p, on pose :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } \overline{a} \in \mathbb{F}_p^{*[2]} \\ -1 \text{ sinon} \end{cases}$$

Ex 69. $\left(\dfrac{1}{p}\right) = 1$, $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ et $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Prop 70 (Critère d'Euler)**.** Si $a \in \mathbb{Z}$ non divisible par p, alors $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$

Rq 71. Si $a \equiv b[p]$, alors $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$. On peut alors voir le symbole de Legendre comme une application définie sur $\mathbb{F}_p^*$.

Prop 72. $\begin{cases} \mathbb{F}_p^* & \longrightarrow & \{-1,1\} \\ x & \longmapsto & \left(\dfrac{x}{p}\right) \end{cases}$ est un morphisme de groupe.

Lemme 73. Soient $A, B \in M_n(\mathbb{F}_q)$ inversibles symétriques. Alors A et B sont congruentes si et seulement si $\delta(A) = \delta(B)$, où $\delta(A)$ est la classe de $\det A$ dans $\mathbb{F}_q^*/\mathbb{F}_q^{*[2]}$.

(DEV 2 - Loi de réciprocité quadratique) Soient p, q deux nombres premiers impairs distincts. Alors :

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

Ex 74. $\left(\dfrac{-30}{53}\right) = -1$

Bibliographie

[Odi23] Alain Ninet Odile Fleury Loic Foissy. *Algèbre et calcul formel*. 2eme edition. ellipses, 2023.

[Per96] Daniel Perrin. *Cours d'algèbre*. ellipses, 1996.

[Ulm21] Felix Ulmer. *Théorie des groupes*. 2021.