

Leçon 121 : Nombres premiers. Applications.

Matei Lefebvre

2025/2026

1 L'ensemble des nombres premiers.

1.1 Généralités.

[Gou21], I.1.2 et [Rom21], XI.1-2

~ 14 items.

théorème de Bézout | théorème de Gauss | définition nombre premier | exemple (tableau en annexe) |
théorème fondamental de l'arithmétique | exemple | définition valuation p -adique | exemple : valuation
du pgcd | $p \nmid n \Leftrightarrow p \wedge n = 1$ | un premier est premier | $p \mid \binom{n}{k}$ | $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow p \in \mathcal{P}$ | définition
indicatrice d'Euler | formule explicite de $\varphi(n)$

1.2 Répartition des nombres premiers.

[Rom21], XI.3-4 et [Per96], III.4

~ 8 items.

$|\mathcal{P}| = +\infty$ | théorème Dirichlet faible (Perrin, exos) | théorème de la progression arithmétique de
Dirichlet (admis) | théorème de Bertrand (admis) | définition de π fonction de répartition des nombres
premiers | remarque : $\pi(x) \xrightarrow{x \rightarrow +\infty} +\infty$ | $\pi(x) \sim \frac{x}{\ln(x)}$ (admis) | corollaire : $\frac{\pi(x)}{x} \rightarrow 0$

1.3 Tests de primalité.

[Rom21], XI.5-6, [Dem09], II.3.6-7 et [App24], XIX.4

~ 6 items.

Théorème de Wilson (Rombaldi XI.5) | : critère de Fermat, témoins de Fermat | exemple avec
 $F_5 = 2^{2^5} + 1 = 2^{32} + 1$ | critère de Miller-Rabin, témoins de Miller | nombre de témoins de Miller
(Demazure II.3.6-7) : | test probabiliste de primalité (Appel)

2 Exemples d'applications.

2.1 Théorème des deux carrés.

[Per96], II.6

~ 7 items.

définition Σ | exemples | définition $\mathbb{Z}[i]$, norme | Σ stable par multiplication | inversibles de $\mathbb{Z}[i]$ |
DEV 1 : théorème des deux carrés

Dbon

Théorème. 1. Soit $p \in \mathcal{P}$. Alors, p est somme de deux carrés $\Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$
 $\Leftrightarrow p = 2$ ou $p \equiv 1[4]$.

2. Soit $n = \prod_{p \in \mathcal{P}} p^{vp(n)} \geq 2$. Alors, n est somme de deux carrés si et seulement si $\forall p \equiv 3[4], vp(n) \in 2\mathbb{N}$.

3. Les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près, les $p \in \mathcal{P}$ avec $p \equiv 3[4]$ et les $z \in \mathbb{Z}[i]$ avec $N(z) \in \mathcal{P}$.

[Per96], II.6

2.2 Théorie des groupes finis.

[Per96], I.5 et [Ber20], XI.1

~ 5 items.

définition p -Sylow | $|X| \equiv |X^G| [p]$ | centre d'un p -groupe | théorèmes de Sylow | applications des théorèmes de Sylow (on peut en chercher quelques unes dans les exos du Berhuy)

2.3 Arithmétique des polynômes.

[Ber20], XIX.2-3

~ 5 items.

critère d'irréductibilité modulo p | exemple | critère d'Eisenstein | exemple : Φ_p | (factorialité et irréductibles de $\mathbb{Z}[X]$)

2.4 Polygones constructibles.

[Goz09], VI.1 et [Car01], II.1

~ 3 items.

Φ_n irréductible sur $\mathbb{Q}$ | DEV bonus : polygones constructibles | exemple : construction du pentagone

D1

Théorème. 1. Soit $n \geq 3$ et $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors, $e^{\frac{2i\pi}{n}}$ est constructible si et seulement si les $e^{\frac{2i\pi}{p_j^{\alpha_j}}}$ sont constructibles ;

2. $\forall \alpha \in \mathbb{N}, e^{\frac{2i\pi}{2^\alpha}}$ est constructible ;

3. Soient $p \geq 3$ un nombre premier et $\alpha \in \mathbb{N}^*$. Alors, $e^{\frac{2i\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat (i.e. de la forme $p = 2^m + 1$).

[Car01], IV.2 et X.4.1

3 Corps finis.

3.1 Généralités.

[Per96], III.2

~ 5 items.

caractéristique, sous-corps premier | cardinal d'un corps fini | morphisme de Frobenius | existence et unicité d'un corps fini | exemple : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$

3.2 Loi de réciprocité quadratique.

[Goz09], VII.7 et XII.2

~ 8 items.

carrés dans $\mathbb{F}_p$ pour $p = 2$ et $p > 2$ | carrés = noyau de $x \mapsto x^{\frac{p-1}{2}}$ | -1 est un carré ssi $p \equiv 1[4]$ | définition symbole de Legendre | $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ | définition sommes de Gauss | DEV 2 : réciprocité quadratique | exemple en annexe (Gozard XII.2)

D2

Proposition. On a $s(a) = \left(\frac{a}{p}\right) s(1) \forall a \in \mathbb{F}_p^*$ et $s(1)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p \in \mathbb{K}$.

Théorème (Loi de réciprocité quadratique et deuxième loi complémentaire). .

1. $\left(\frac{p}{p'}\right) \left(\frac{p'}{p}\right) = (-1)^{\frac{(p-1)(p'-1)}{4}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

[Goz09], XII.2 et [Zav13], II.6

Remarque : besoin de définir les sommes de Gauss.

Références

- [Per96] D. PERRIN. *Cours d'algèbre (Agrégation)*. ELLIPSES, 1996. ISBN : 9782729855529.
- [Car01] J.C. CARREGA. *Théorie des corps : La règle et le compas*. HERMANN, 2001. ISBN : 9782705614492.
- [Dem09] M. DEMAZURE. *Cours d'algèbre*. CASSINI, 2009. ISBN : 9782842251277.
- [Goz09] I. GOZARD. *Théorie de Galois : Niveau L3-M1*. ELLIPSES, 2009. ISBN : 9782729842772.
- [Zav13] M. ZAVIDOVIQUE. *Un max de math*. CALVAGE&MOUNET, 2013. ISBN : 9782916352299.
- [Ber20] G. BERHUY. *Algèbre : le grand combat*. CALVAGE&MOUNET, 2020. ISBN : 9782916352831.
- [Gou21] X. GOURDON. *Les Maths en tête - Algèbre et probabilités - 3e édition*. ELLIPSES, 2021. ISBN : 9782340059597.
- [Rom21] J.E. ROMBALDI. *Mathématiques pour l'agrégation - Algèbre et géométrie*. DEBOECK, 2021. ISBN : 9782807332201.

[App24] W. APPEL. *Mathématiques pour l'agrégation externe. Probabilités*. DEBOECK, 2024. ISBN : 9782807361669.