

Leçon 121 : Nombres premiers. Applications.

[Dem] : *Cours d'algèbre*, Michel Demazure

[Gou] : *Algèbre et probabilité*, Xavier Gourdon

[Goz] : *Théorie de galois*, Ivan Gozard

[Gra-Gra] : *Algèbre et Arithmétique fondamentales*, Georges Gras, Marie-Nicole Gras

[Hau] : *Les contre-exemples en mathématiques*, Bertrand Hauchecorne

[Per] : *Cours d'algèbre*, Daniel Perrin

[Rom] : *Mathématiques pour l'agrégation*, Jean-Étienne Rombaldi

[Sau-Ran] : *Cours de calcul formel. Corps finis, systèmes polynomiaux, applications*, Phillipe Saux Picart, Eric Rannou

[Szp] : *Mathématiques Algèbre L3*, Aviva Szpirglas

[Ulm] : *Théorie des groupes*, Félix Ulmer

I Partie A - Arithmétique de base [Rom]

■ Déf 1 (nombre premier) :

■ Prop 2 (Infinité) :

■ Thm 3 (Euclide, Gauss) :

■ Thm 4 (Théorème fondamental) :

■ Déf 5 (Valuation p-adique) :

■ Prop 6 (pgcd et ppcm) :

II Partie B - Applications aux groupes

II.1 $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler [Rom] [Szp] [Per]

■ Déf 7 (Indicatrice d'Euler) :

■ Ex 8 ($\varphi(p)$) :

App 9 (Euler / Fermat) :

■ Thm 10 (Générateurs de $\mathbb{Z}/n\mathbb{Z}$) :

■ Ex 11 : Donner des exemples triviaux.

■ Prop 12 (Corps et $\mathbb{Z}/n\mathbb{Z}$) :

■ Thm 13 (Restes chinois) :

■ Contre-Ex 14 : Groupe de Klein.

App 15 ($\varphi(n)$) :

■ Dév 16 (Critère de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$) :

II.2 p-groupes [Ulm] [Szp]

■ Déf 17 (p-groupe) :

■ Ex 18 (p-Sylow) :

■ Thm 19 (Équation aux classes) :

App 20 (Centre d'un p-groupe) :

App 21 (Structure des groupes d'ordre p^2) :

App 22 (Lemme de Cauchy) :

III Partie C - Applications aux polynômes

III.1 Critères généraux [Goz] [Per]

■ Thm 23 (Eisenstein) :

App 24 (Irréductibilité Φ_p) :

■ Prop 25 (Polynômes réductibles modulo p) :

■ Ex 26 :

■ Contre-Ex 27 : Voir [Hau] et [Per] (Φ_8).

■ Thm 28 (Réduction modulo p) :

■ Ex 29 : Voir [Goz].

III.2 Polynômes cyclotomiques [Goz]

■ Déf 30 (Corps cyclotomique) :

■ Déf 31 (Polynôme cyclotomique) :

■ **Ex 32 :** $\Phi_{1,\mathbb{Q}}(X) = X - 1$, $\Phi_{2,\mathbb{Q}}(X) = X + 1$, $\Phi_{3,\mathbb{Q}}(X) = X^2 + X + 1$, $\Phi_{4,\mathbb{Q}}(X) = X^2 + 1$

■ **Prop 33 :** $X^m - 1 = \prod_{d|m} \Phi_{d,\mathbb{Q}}(X)$.

■ **Thm 34 :** $\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ et est irréductible dans $\mathbb{Q}[X]$.

App 35 : Le polynôme minimal de toute racine primitive n -ième est $\Phi_{n,\mathbb{Q}}(X)$, et $[\mathbb{Q}(\mathbb{U}_n) : \mathbb{Q}] = \varphi(n)$.

IV Partie D - Applications en théorie des corps

IV.1 Trucs habituels

■ **Déf 36 (Caractéristique) :**

■ **Prop 37 (Caractéristique d'un corps fini) :**

■ **Déf 38 (Corps premier, sous-corps premier) :**

■ **Prop 39 (Cardinal d'un corps fini) :**

■ **Ex 40 :** Exemples de corps qui ne peuvent exister.

■ **Prop 41 (Frobenius) :**

App 42 : Racine p -ième.

■ **Thm 43 (Existence des corps finis) :**

■ **Ex 44 :** $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_9$ [**Annexe : Table de $\mathbb{F}_4$**].

IV.2 Carré dans $\mathbb{F}_p$ [Goz] [Per]

■ **Déf 45 (Symbole de Legendre, résidu quadratique) :**

■ **Ex 46 :** Résidus quadratiques dans $\mathbb{F}_7$.

■ **Thm 47 (Réciprocité quadratique) :**

App 48 (Calcul du symbole de Legendre) : Voir [Goz].

V Partie E - Comment trouver des nombres premiers ?

V.1 Tests de primalité [Rom] [Dem] [Gra-Gra][Sau-Ran]

■ **Thm 49 :** Encadrement par la racine.

■ **Prop 50 (Crible d'Eratosthène) :**

■ **Déf 51 (Nombre de Carmichael) :**

■ **Ex 52 :**

■ **Prop 53 (Test de Fermat) :**

■ **Thm 54 (Rabin) :**

■ **Prop 55 (Test de Rabin-Miller) :**

■ **Déf 56 (Nombre de Mersenne) :**

■  **Dév 57 (Lucas-Lehmer 1) :**

■  **Dév 58 (Lucas-Lehmer 2) :**

V.2 Répartitions des nombres premiers [Rom] [Gou]

■ **Thm 59 (Dirichlet faible) :**

■ **Thm 60 (Dirichlet) :**

■ **Déf 61 (π) :**

■ **Thm 62 (Répartition des nombres premiers) :**