9 Leçon 121 : Nombres premiers. Applications.

I. Généralités sur les nombres premiers

1. Définition et propriétés [ROM]

Nombre premier, théorème d'Euclide, lemme d'Euclide, théorème fondamental de l'arithmétique, valuation p-adique, prop, lien avec le PGCD et PPCM

2. Répartition des nombres premiers [ROM] [GOU]

Infinité des nombres premiers, théorème de Dirichlet faible, théorème de Dirichlet fort, théorème des nombres premiers

3. Critères de primalité [ROM]

Test avec $\sqrt{n}$, crible d'Erathostène, théorème de Wilson

II. Applications

1. Théorie des groupes [ROM] [ULM]

$(\mathbb{Z}/n\mathbb{Z})^\times$, indicatrice d'Euler, prop, théorème d'Euler, théorème de Fermat, p-groupe, formule des classes pour un p-groupe, classification des groupes d'ordre p^2, théorème de Cauchy

2. Corps finis [PER] [GOZ]

Sous-corps premier, caractéristique, morphisme de Frobenius, DEV 1 : existence et unicité des corps finis, $\mathbb{F}_q^*$ est cyclique

3. Irréductibilité de polynômes [GOZ] [PER]

Contenu, prop sur les polynômes irréductibles, DEV 2 : critère d'Eisenstein, réduction modulo p, $\mathbb{U}_n^*$, polynômes cyclotomiques

Présentation :

- L'idée de départ est de trouver une « décomposition atomique » des nombres entiers. Ces « atomes » sont les nombres premiers.
- Il existe encore beaucoup de problèmes non-résolus sur les nombres premiers : il n'y a par exemple aucune formule explicite pour tous les atteindre.
- Les nombres premiers sont par exemple utilisés afin des chiffrer des messages, ils sont à la base du chiffrement RSA. Cette méthode repose sur le fait qu'il est très difficile (à l'heure actuelle) de décomposer un très grand nombre en produit de deux nombres premiers.
- Pour trouver le PGCD ou le PPCM de deux nombres, on peut se ramener à étudier leur décomposition en facteurs premiers.
- Les polynômes cyclotomiques ont leur place dans cette leçon, tout d'abord car le critère d'Eisenstein permet de montrer que les Φ_p avec p premier sont irréductibles sur $\mathbb{Q}$, et ensuite car on se sert à de nombreuses reprises des nombres premiers dans la preuve de leur irréductibilité.

Développements :

- Existence et unicité des corps finis
  - Théorie de Galois, Gozard, p85
  - Algèbre Tome 4, Szpirglas, p85
- Critère d'Eisenstein

- Théorie de Galois, Gozard, p10
- Cours d'algèbre, Perrin, p51 et 76

Références :

- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [GOU] Algèbre-Probabilités, Gourdon
- [ULM] Théorie des Groupes, Ulmer
- [PER] Cours d'algèbre, Perrin
- [GOZ] Théorie de Galois, Gozard

Leçon 121 : Nombres premiers. Applications

I Généralités sur les nombres premiers

1) Définition et propriétés [ROM]

ROM 303 **Déf 1 :** On dit que $p \in \mathbb{N}$ 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.

∅ **Exemple 2 :** 2, 3, 5, 7, 11, 13 sont les premiers nombres premiers.

ROM 303 **Théorème 3 (d'Euclide) :** Tout élément $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admet au moins un diviseur premier.

Lemme 4 : Soit $p \in \mathcal{P}$. Pour tout $n \in \mathbb{N}^*$, on a soit p qui divise n, soit p qui est premier avec n.

Lemme 5 : Deux nombres premiers distincts sont premiers entre eux.

Prop 6 : Soit $n \in \mathbb{N}^*$. On a : $(p \mid n^\alpha) \Leftrightarrow (p \mid n)$

Théorème 7 (fondamental de l'arithmétique) : Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme : $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$ où les q_k sont des nombres premiers tel que $2 \leq q_1 < q_2 < \dots < q_r$ et $\alpha_k \in \mathbb{N}^*$

Déf 8 : Soit $p \in \mathcal{P}$ et $n \geq 2$. On note $v_p(n)$ l'exposant de p dans la décomposition de n. On dit que $v_p(n)$ est la valuation p-adique de n.

Remarque 9 : On a donc : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

Lemme 10 : Soit $n = \prod_{k=1}^{\hat{r}} q_k^{\alpha_k}$ et $m = \prod_{k=1}^{\hat{r}} q_k^{\beta_k}$ leur décomposition en facteurs premiers.

Alors : $(m \mid n) \Leftrightarrow (\forall k \in [\![1; r]\!], \alpha_k \leq \beta_k)$

Théorème 11 : On reprend les notations précédentes. ROM 307

Alors : $\text{pgcd}(n, m) = \prod_{k=1}^{\hat{r}} q_k^{\min(\alpha_k, \beta_k)}$

et $\text{ppcm}(n, m) = \prod_{k=1}^{\hat{r}} q_k^{\max(\alpha_k, \beta_k)}$

2) Répartition des nombres premiers [ROM] [GOU]

Théorème 12 : Il existe une infinité de nombres premiers. ROM 305

Théorème 13 (de Dirichlet faible) : Soit $n \geq 2$. Il existe une infinité de nombres premiers p vérifiant $p \equiv 1 [n]$ GOU 99

Théorème 14 (de Dirichlet) : Soit $a, b \in \mathbb{N}^*$ premiers entre eux. Alors il existe une infinité de nombres premiers p tel que $p \equiv b [a]$

Théorème 15 (des nombres premiers) : Soit $\mathcal{P}_n = \mathcal{P} \cap [\![1; n]\!]$ ROM 309

On note $\pi(n) = \text{card}(\mathcal{P}_n)$. Alors on a :

$$\pi(n) \underset{n \to \infty}{\sim} \frac{n}{\ln(n)}.$$

3) Critères de primalité [ROM]

Théorème 16 : Soit $n \geq 2$ qui est non premier. Alors n admet au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$. ROM 304

Méthode 17 : Le théorème nous donne une méthode pour savoir si n est premier ou non, il suffit de regarder la division euclidienne de n par tous les entiers $d \leq \sqrt{n}$.

Méthode 18 : Le crible d'Eratosthène donne une méthode pour obtenir la liste des nombres premiers. Le principe est : on se donne la liste $[\![1$

de tous les entiers entre 2 et $\sqrt{n}$. On garde 2 et on supprime tous les multiples de 2. On garde alors le premier entier strictement plus grand que 2 et on supprime tous ses multiples. On continue ainsi et on s'arrête quand on obtient un nombre premier strictement plus grand que $\sqrt{n}$.
On a obtenu tous les nombres premiers inférieurs à $\sqrt{n}$.

Prop 19 : Soit $n \geq 2$. On a équivalence entre :
1) n est premier 2) $\mathbb{Z}/n\mathbb{Z}$ est un corps
3) $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Rom 326 **Théorème 20 (de Wilson)** : On a équivalence entre :
$(n \in \mathcal{P}) \Leftrightarrow (n-1)! \equiv -1 \ [n]$

II Applications

1) Théorie des groupes [ROM][ULM]

Rom 282 **Déf 21** : Soit $n \geq 2$. On pose $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Déf 22 : On appelle fonction indicatrice d'Euler la fonction qui à $n \in \mathbb{N}^*$ associe $\ell(n)$ le nombre d'entiers compris entre 1 et n premiers avec n.

Prop 23 : $\ell(n)$ est égal au nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, ou encore au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Prop 24 : Si $p \in \mathcal{P}$, $\ell(p) = p-1$

Prop 25 : Si $p \in \mathcal{P}$ et $d \in \mathbb{N}^*$, $\ell(p^d) = (p-1)p^{d-1}$

Rom 288 **Prop 26** : Si $m \wedge n = 1$, alors $\ell(m.n) = \ell(m).\ell(n)$

Théorème 27 : Soit $n = \prod_{i=1}^{\omega} p_i^{d_i}$ sa décomposition en facteurs premiers.
Alors : $\ell(n) = \prod_{i=1}^{\omega} p_i^{d_i-1}(p_i-1) = n \prod_{i=1}^{\omega}\left(1-\frac{1}{p_i}\right)$

Rom 283 **Théorème 28 (d'Euler)** : Soit $a \wedge n = 1$. Alors : $a^{\ell(n)} \equiv 1 \ [n]$

Théorème 29 (de Fermat) : Soit $p \in \mathcal{P}$. Soit $a \wedge p = 1$.
Alors $a^{p-1} \equiv 1 \ [p]$.
Pour tout $a \in \mathbb{Z}$, $a^p \equiv a \ [p]$

Soit G un groupe agissant sur un ensemble fini X.

ULM 69 **Déf 30** : Soit $p \in \mathcal{P}$. Un p-groupe est un groupe G dont l'ordre est une puissance de p.

Prop 31 : Soit $X^G = \{x \in X ; g.x = x \ \forall g \in G\}$.
Soit G un p-groupe. Alors : $|X^G| \equiv |X| \ [p]$.

Prop 32 : Le centre d'un p-groupe est non-trivial.

Prop 33 : Tout groupe d'ordre p^2 est abélien.

IP 106 **Théorème 34** : Soit G un groupe d'ordre p^2. Alors :
$G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Prop 35 : Soit $p \in \mathcal{P}$. Tout groupe d'ordre p est cyclique.

ULM 69 **Théorème 36 (de Cauchy)** : Soit G un groupe dont l'ordre est divisible par $p \in \mathcal{P}$. Alors G admet un élément d'ordre p.

2) Corps finis [PER] [GOZ]

Soit K et L des corps.

PER 72 **Déf 37** : On appelle sous-corps premier de K le plus petit sous-corps de K.

Déf 38 : Soit $f : \mathbb{Z} \to K$ le morphisme d'anneaux tel que $f(n) = n.1_K$. Alors $\ker(f)$ est de la forme $p\mathbb{Z}$ avec $p = 0$ ou $p \in \mathcal{P}$. Le nombre p est appelé la caractéristique de K, noté $\mathrm{car}(K)$

Remarque 39 : Si K est fini, $\mathrm{car}(K) = p > 0$. Le sous-corps premier de K est $\mathbb{Z}/p\mathbb{Z}$, noté $\mathbb{F}_p$. On a que $q = |K| = p^n$: le cardinal d'un corps fini est une puissance de sa caractéristique.

Prop 40 : Soit $\mathrm{car}(K) = p > 0$. L'application $F : K \to K$ tel que $F(x) = x^p$ est un morphisme de corps appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme. Si $K = \mathbb{F}_p$, c'est l'identité.

Théorème 41 : Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, Soit $q = p^n$. Alors il existe un corps fini à q éléments. Il s'agit du corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$. Il est unique à $\mathbb{F}_p$-isomorphisme près. On le note $\mathbb{F}_q$. DEV 1

Corollaire 42 : Le produit des éléments de $\mathbb{F}_q^*$ vaut -1. GOZ 96 PER 74

Théorème 43 : Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Théorème 44 : Soit $q = p^n$. Alors $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$. DEV 1 GOZ 97

Corollaire 45 : Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

3) Irréductibilité de polynômes [GOZ][PER]

Déf 46 : Soit $P \in \mathbb{Z}[X]$. On appelle contenu de P, noté $c(P)$, le PGCD de ses coefficients. On dit que P est primitif si $c(P) = 1$. GOZ 10

Lemme 47 : Soit $P, Q \in \mathbb{Z}[X]$ non nuls. Alors : $c(PQ) = c(P)\,c(Q)$

Théorème 48 : Soit $P \in A[X]$ avec $\deg(P) \geq 1$. Alors P est irréductible dans $A[X]$ ssi il est primitif et irréductible dans $\mathbb{Q}[X]$.

Théorème 49 (critère d'Eisenstein) : Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ avec $\deg(P) \geq 1$
Soit $p \in \mathcal{P}$. On suppose que :
1) $p \nmid a_n$ 2) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$ 3) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$. DEV 2

Application 50 : Pour $n \geq 1$, il existe des polynômes irréductibles de degré n dans $\mathbb{Q}[X]$.

Application 51 : Le polynôme $\Phi_p(X) = X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}[X]$. GOZ 11 PER

Théorème 52 (réduction modulo p) : Soit $p \in \mathcal{P}$. Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et $\bar{P}$ sa réduction dans $\mathbb{F}_p[X]$. On suppose que $\bar{a_n} \neq \bar{0}$ dans $\mathbb{F}_p$. Si $\bar{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 53 : Soit $P(X) = X^3 + 462X^2 + 2433X - 67691$
Alors P est irréductible sur $\mathbb{Z}$.

Déf 54 : Soit $U_n = \{z \in \mathbb{C} ; z^n = 1\}$. Soit U_n^* l'ensemble des racines primitives n-ièmes de l'unité, c'est à dire appartenant à U_n et d'ordre n. GOZ 67

Déf 55 : Soit $n \in \mathbb{N}^*$. On appelle n-ième polynôme cyclotomique le polynôme : $\Phi_n(X) = \prod_{\xi \in U_n^*} (X - \xi)$
C'est un polynôme unitaire de degré $\varphi(n)$

Prop 56 : $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Prop 57 : $\forall n \in \mathbb{N}^*$, $\Phi_n(X) \in \mathbb{Z}[X]$

Théorème 58 : $\forall n \in \mathbb{N}^*$, $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.