Leçon 121 : Nombres premiers. Applications

Références : Rombaldi, Gourdon, Perrin, Berhuy, Caldero [H2G1]

I - Arithmétique dans $\mathbb{Z}$

1) Premiers résultats
2) Fonctions particulières
3) Répartition des nombres premiers
4) Tests de primalité

II - Application en théorie des corps

1) Corps finis
2) Carrés dans $\mathbb{F}_q$
3) Polynômes irréductibles et cyclotomie

III - Autres applications

1) Théorie des groupes
2) L'anneau $\mathbb{Z}[i]$ et le problème des deux carrés

DEV 1 : Théorème de Kronecker

DEV 2 : Loi de réciprocité quadratique

Leçon 121 : Nombres premiers. Applications.

I - Arithmétique dans $\mathbb{Z}$

1) Premiers résultats [PER] [GOU] [ROT]

[ARI] **DEF 1** : Soit A un anneau commutatif unitaire intègre. On dit que A est euclidien lorsqu'il existe $\delta : A\setminus\{0\} \to \mathbb{N}$ telle que $\forall a, b \in A\setminus\{0\}$, il existe $q, r \in A$ avec $a = bq + r$ et $r = 0$ ou $\delta(r) < \delta(b)$. δ est appelé stathme euclidien.

EX 2 : $\mathbb{Z}$ est euclidien pour $\delta(n) = |n|$.

[GOU] **PROP 3** : Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) de $\mathbb{Z}\times\mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$.

THM 4 (Bézout) : Des entiers $a_1, \dots, a_n$ sont premiers entre eux si et seulement si il existe $u_1, \dots, u_n$ dans $\mathbb{Z}$ tels que $a_1u_1 + \dots + a_nu_n = 1$.

THM 5 (Gauss) : Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

DEF 6 : Soit $p \in \mathbb{N}$, $p \geq 2$. On dit que p est premier lorsque p possède exactement deux diviseurs positifs : 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

THM 7 (Euclide) : Soit $n \in \mathbb{Z}\setminus\{-1, 0, 1\}$. Alors n a au moins un diviseur premier.

THM 8 : Tout entier $n \geq 2$ composé a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

LEMME 9 : Soit p un nombre premier. Pour tout $n \in \mathbb{N}^*$, on a soit $p \mid n$ soit $p \wedge n = 1$.

LEMME 10 : Deux nombres premiers distincts sont premiers entre eux.

LEMME 11 : Soit $(n_k)_{k\in[\![1,r]\!]} \in \mathbb{N}^{*r}$, $r \geq 2$. Si $p \mid \prod_{k=1}^{r} n_k$, alors p divise l'un des n_k au moins.

THM 12 : L'ensemble $\mathcal{P}$ des nombres premiers est infini.

THM 13 : (fondamental de l'arithmétique) Tout entier $n \geq 2$ se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où les p_k sont premiers tels que $2 \leq p_1 < \dots < p_r$ et les $\alpha_k \in \mathbb{N}^*$.

DEF 14 : Le nombre $v_p(n) = \max\{\alpha \in \mathbb{N} / p^\alpha \mid n\}$ est appelé valuation p-adique de n.

EX : Nombres de Fermat

LEMME 15 : Soient $n, m \geq 2$, $n = \prod_{k=1}^{r} p_k^{\alpha_k}$, $m = \prod_{k=1}^{r} p_k^{\beta_k}$.
$n \mid m \iff \forall k \in [\![1; r]\!]$, $\alpha_k \leq \beta_k$.

THM 16 : Soient $n \geq 2$, $m \geq 2$, $n = \prod_{k=1}^{r} p_k^{\alpha_k}$, $m = \prod_{k=1}^{r} p_k^{\beta_k}$.
On a : $\mathrm{PGCD}(n, m) = \prod_{k=1}^{r} p_k^{\min(\alpha_k, \beta_k)}$ et $\mathrm{PPCM}(n, m) = \prod_{k=1}^{r} p_k^{\max(\alpha_k, \beta_k)}$

2) Fonctions particulières [ROT] [FRA 1]

DEF 17 : On définit la fonction indicatrice d'Euler par :
$\forall n \in \mathbb{N}$, $n \geq 2$, $\varphi(n) = \#\{k \in [\![1; n]\!] / k \wedge n = 1\}$.

PROP 18 : On a que $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

THM 19 : Pour tout $a \in \mathbb{Z}$, $a \wedge n = 1$, on a $a^{\varphi(n)} \equiv 1 \bmod n$.

THM 20 : Pour tout $n \geq 2$, on a $n = \sum_{d \mid n} \varphi(d)$

PROP 21 : Si $p \in \mathcal{P}$, $\varphi(p) = p - 1$.

PROP 22 : Si n, m sont premiers entre eux, on a alors : $\varphi(mn) = \varphi(n)\varphi(m)$

THM 23 : Soit $n \geq 2$, $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Alors $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

DEF 24 : On définit la fonction de Möbius par :
$\mu : n \in \mathbb{N}^* \mapsto \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \text{ contient un facteur carré} \\ (-1)^r \text{ si } n = p_1 \cdots p_r, \ p_i \text{ premiers 2 à 2 distincts} \end{cases}$

PROP 25 : On a : $\forall n \geq 2$, $\sum_{d \mid n} \mu(d) = 0$.

PROP 26 : (Inversion de Möbius) Soit $f : \mathbb{N}^* \to \mathbb{R}$ et $g : n \in \mathbb{N}^* \mapsto \sum_{d \mid n} f(d)$. Alors $f(n) = \sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right)$.

3) Répartition des nombres premiers [PER] [ROM]

THM 27 : (progression arithmétique de Dirichlet) : [ADMIS]
Soient $a, n \in \mathbb{N}^*$ tels que $a \wedge n = 1$. Il existe une infinité de nombres premiers p vérifiant $p \equiv a \bmod n$.

CONJ 28 : (Nombres premiers jumeaux) Il existe une infinité de $p \in \mathcal{P}$ tel que $p + 2 \in \mathcal{P}$.

THM 29 : (Bertrand) Pour tout $n \in \mathbb{N}^*$, il existe des nombres premiers compris entre n et $2n$. [ADMIS]

THM 30 : Soit $\pi(n)$ le nombre de nombres premiers entre 1 et n.
Alors $\pi(n) \underset{+\infty}{\sim} \frac{n}{\ln(n)}$ [ADMIS]

4) Tests de primalité [ROM]

REM 31 : Pour trouver les nombres premiers entre 1 et n, on dessine le crible d'Ératosthène (voir ANNEXE)

THM 32 (Wilson) : Soit $n \geq 2$. $n \in \mathbb{P} \Leftrightarrow (n-1)! \equiv -1 \bmod n$

THM 33 : (Fermat) : Soit $p \geq 2$ premier. Alors :
$\forall a \in \mathbb{Z}$, $a^p \equiv a \bmod p$.

REM 34 : La contraposée du théorème de Fermat constitue un test de primalité.

DEF 35 : On appelle nombre de Carmichael tout entier $n \geq 3$ non premier tel que $a^{n-1} \equiv 1 \bmod n$ pour tout a premier avec n.

EX 36 : 561 est un nombre de Carmichael DEV 1

LEMME 37 : Un nombre de Carmichael est impair

LEMME 38 : Un nombre de Carmichael est sans facteur carré.

THM 39 : (Korselt) Soit $n \geq 3$ un entier. LASSE :
1) Il existe un entier $r \geq 3$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et pour tout $j \in [\![1; r]\!]$, $p_j - 1 \mid n-1$.
2) n est non premier et pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x^n = x$.
3) n est un nombre de Carmichael.

II - Application en théorie des corps

1) Corps finis [PER]

THM 40 : (Wedderburn) Tout corps fini est commutatif

DEF 41 : Soit K un corps. On appelle sous-corps premier le plus petit sous-corps de K.

DEF 42 : Soit $\varphi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1$. $\ker(\varphi)$ est un idéal de $\mathbb{Z}$ donc $\ker(\varphi) = p\mathbb{Z}$. Si $p = 0$, le sous-corps premier est isomorphe à $\mathbb{Q}$. Si $p \neq 0$, c'est un nombre premier et le sous-corps premier est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. L'entier p s'appelle la caractéristique de K.

PROP 43 : Soit K un corps fini. Alors $\text{car}(K) = p > 0$ un nombre premier donc K est un $\mathbb{F}_p$-espace vectoriel donc $\#K = p^n$ où $n = [K : \mathbb{F}_p]$.

THM 44 : Soit p premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.
- Il existe un corps à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
- En particulier, K est unique à isomorphisme près.

EX 45 : $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+1)$ + morphisme de Frobenius !

2) Carrés dans $\mathbb{F}_q$ [PER]

DEF 46 : On note $\mathbb{F}_q^2 = \{x^2 / x \in \mathbb{F}_q\}$; $(\mathbb{F}_q^*)^2 = \{x^2 / x \in \mathbb{F}_q^*\}$.

PROP 47 : Pour $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Pour $p > 2$, on a :
$\#\mathbb{F}_q^2 = \frac{q+1}{2}$ et $\#(\mathbb{F}_q^*)^2 = \frac{q-1}{2}$.

PROP 48 : On suppose $p > 2$. Alors : $x \in (\mathbb{F}_q^*)^2 \Leftrightarrow x^{\frac{q-1}{2}} = 1$

COR 49 : Si $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \bmod 4$.

EX 50 : 2 est un carré dans $\mathbb{F}_7$ mais pas 3.

APPLI 51 : Il existe une infinité de nombres premiers de la forme $4n+1$. (*)

3) Polynômes irréductibles et cyclotomie [PER]

THM 52 : (Eisenstein) Soit A factoriel et $K = \text{Frac}(A)$ son corps des fractions. Soit $P(X) = a_n X^n + \cdots + a_0 \in A[X]$ soit $p \in A$ irréductible. On suppose :
- $p \nmid a_n$
- $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$ et $p^2 \nmid a_0$.

Alors P est irréductible dans $K[X]$.

REM 53 : On utilise ce critère le plus souvent avec $A = \mathbb{Z}$ et p un nombre premier

THM 54 : Soit $P \in \mathbb{Z}[X]$ tel qu'il existe $p \in \mathbb{P}$ tel que $\overline{P} \in \mathbb{F}_p[X]$ soit irréductible. Alors, P est irréductible dans $\mathbb{Z}[X]$.

EX 55 : $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$.

DEF 56 : Pour $\mathbb{K}$ un corps, on note $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \mid \zeta^n = 1\}$ et μ_n^* l'ensemble des générateurs de $\mu_n(\mathbb{K})$. Le n-ième polynôme cyclotomique est $\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$

PROP 57 : On a $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

PROP 58 : $\forall n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}$.

III – Autres applications

1) En théorie des groupes [BERHUY]

Soit G un groupe fini

DEF 59 : On dit que G est un p-groupe si $\#G$ est une puissance d'un nombre premier p.

THM 60 : (Equation aux classes) : Si G agit sur un ensemble X on note $X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$. Alors :

$$\#X \equiv \#X^G \bmod p.$$

COR 61 : Si G est un p-groupe, alors son centre $Z(G)$ n'est pas réduit au neutre.

DEF 62 : Soit $\#G = p^m q$, $p \nmid q$, $m \geq 0$, p premier. On appelle p-Sylow de G un sous-groupe de cardinal p^m.

THM 63 : (Sylow) : Il existe des p-Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow

- Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow sont conjugués. Si S est un p-Sylow de G, alors $S \lhd G \Leftrightarrow S$ est unique.
- Si n_p est le nombre de p-Sylow de G, alors $n_p \equiv 1 \bmod p$ et $n_p \mid m$.

EX 64 : Un groupe d'ordre 63 n'est pas simple.

THM 65 : (Cauchy) Si $p \mid \#G$, G possède au moins un élément d'ordre p.

2) L'anneau $\mathbb{Z}[i]$ et le problème des deux carrés [PER]

DEF 66 : Soit $\Sigma = \{n \in \mathbb{N} / n = a^2 + b^2, a, b \in \mathbb{N}\}$. Le problème est déterminer Σ.

PROP 67 : Si $n \equiv 3 \bmod 4$, $n \notin \Sigma$.

PROP 68 : $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$, $\mathbb{Z}[i]^* = \{-1; 1\}$ et $\mathbb{Z}[i]$ est euclidien

LEMME 69 : Σ est stable par multiplication et si p est un nombre premier, $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \bmod 4$.

THM 70 : Soit $n \in \mathbb{N}^*$, $n \neq 1$, $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$

$n \in \Sigma \Leftrightarrow v_p(n)$ est pair pour $p \equiv 3 \bmod 4$.

(*) OUBLI :

[CAL] Histoires Hédonistes ... 1

DEF 71 : Pour p premier impair, $a \in \mathbb{F}_p$, on définit le symbole de Legendre de a par :

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 \text{ si } a = 0 \end{cases}$$

DEF 2

PROP 72 : Soit p premier et $a \in \mathbb{F}_p^*$. On a :

$$\#\{x \in \mathbb{F}_p \mid ax^2 = 1\} = 1 + \left(\frac{a}{p}\right).$$

THM 73 : (Loi de réciprocité quadratique) Soient p, q les nombres premiers impairs distincts. Alors :

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