121 : Nombres premiers et applications

I - Généralités sur les nombres premiers

a) Définition et premières propriétés

[ROMS p.301 -303]

Déf. 1 : On dit qu'un entier p est premier s'il est supérieur ou égal à 2 et si ses seuls diviseurs positifs sont 1 et p. On note $\mathbb{P}$ l'ensemble des 1er.

Thm. 2 : (Euclide) $\forall n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.

Prop. 3 : Soit $p \in \mathbb{P}$. $\forall n \in \mathbb{N}^*$ soit $p \mid n$ soit $\text{pgcd}(p, n) = 1$

Prop. 4 : 2 nb 1er distincts sont premiers entre eux.

Prop. 5 : (Lemme d'Euclide) Soient $n_1, \dots, n_r \in \mathbb{N}^*$, $p \mid n_1 \dots n_r$ ssi p divise un des n_i.

Thm. 6 : $\mathbb{P}$ est infinie de nombre premier.

Exe. 7 : On appelle nombre de Fermat les $F_n = 2^{2^n} + 1$. Pour $n \in \{0, \dots, 4\}$ F_n est 1er. Pour $n \in \{5, \dots, 32\}$ F_n n'est pas 1er. Pour le reste on ne sait pas.

[CDFR p.52]

Appli. 8 : (Gauss Wantzel) Les polygônes constructibles sont ceux à 2^α côtés ou $2^\alpha p_1 \dots p_r$ où les p_i sont des nombres premiers de Fermat

[ROMS p.303 -304]

Thm. 9 : (Fondamental de l'arithmétique). Pour $n \geq 2$ entier, n se décompose en $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ où les p_i sont des nombres premiers tq $p_1 < \dots < p_r$.

Déf. 10 : On appelle valuation p-adique la quantité $v_p(n) = \max\{k \mid p^k \mid n\}$

Thm. 11 : Soient $n, m \geq 2$ des entiers et $n = \prod_{i=1}^{r} q_i^{\alpha_k}$, $m = \prod_{i=1}^{r} q_i^{\beta_k}$ leurs décompositions en facteurs premiers on a :

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

b) Fonctions remarquables

$n \in \mathbb{N}^*$, $n \geq 2$, $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ décomp en facteur 1ers

[DEAS p.29 -25]

Prop. 12 : Soit $s \in \mathbb{Z}$. Les ASSE :

(i) $\text{pgcd}(s, n) = 1$

(ii) $\bar{s}$ générateur de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$

(iii) $\bar{s} \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$

Déf. 13 : $\varphi(n)$ est le nombre d'entiers inférieurs à n et premiers à n.

Cor. 14 : $\varphi(n) = \left|\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times\right|$, $\varphi(p) = p - 1$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Prop. 15 : $\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

[ROMS p.291]

Thm. : $\forall a \in \mathbb{Z}$, tq $\text{pgcd}(a, n) = 1$ alors $a^{\varphi(n)} = 1 \ [n]$

Cor. : (Fermat) $p \in \mathbb{P}$, $\forall a \in \mathbb{Z}$ $a^p = a \ [p]$

[DEAS p.82]

Prop. 16 : $n = \sum_{d \mid n} \varphi(d)$

Déf. 17 : On appelle fonction de Möbius $\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n \text{ est sans facteur carrés} \\ 0 \text{ sinon} \end{cases}$

[ROMS p. 525 -532]

Thm. 18 : (Inversion de Möbius) Soient $u, v \in \mathbb{R}^{\mathbb{N}^*}$.

$\forall n \in \mathbb{N}^*$, $u(n) = \sum_{d \mid n} v(d)$ ssi $\forall n \in \mathbb{N}^*$ $v(n) = \sum_{d \mid n} \mu(d)\, u\left(\frac{n}{d}\right)$

Cor. 19 : $\forall n \in \mathbb{N}^*$, $\varphi(n) = \sum_{d \mid n} \mu(d) \cdot \frac{n}{d}$.

Déf. 20 : On appelle fonction zeta de Riemann $\zeta : s \mapsto \sum_{n=1}^{+\infty} \frac{1}{n^s}$

Prop. 21 : ζ est bien définie et continue sur $D = \{s \in \mathbb{C} \mid \text{Re}(s) > 1\}$

[ROMS p.306 -346]

Thm. 22 : Soit p_n le n-ème nombre premier, $\forall s \in D$

$$\zeta(s) = \prod_{k=1}^{\infty} \frac{1}{1 - \frac{1}{p_k^s}}$$

[GOUM p.305]

Cor. 23 : $\sum_{n=1}^{+\infty} \frac{1}{p_n}$ diverge.

c) Répartition des nombres premiers [ADMIS]

[ROMS p.310 -311]

Thm. 24 : (Tchebychev) Pour $n \in \mathbb{N}^*$, $n \geq 3$ on a :

$$\ln(2) \frac{n}{\ln(n)} \leq \pi(n) \leq e \frac{n}{\ln(n)}, \text{ où } \pi(n) = |\mathbb{P} \cap \{1, \dots, n\}|$$

Thm. 25 : $\forall n \geq 2$, $\frac{1}{e} n \ln(n) \leq p_n \leq \frac{2}{\ln(2)} n \ln(n)$ où p_n est le n-ème nombre premier

[ROMS p.306]

Thm. 26 : (Hadamard, La Vallée-Poussin) $\pi(n) \underset{+\infty}{\sim} \frac{n}{\ln(n)}$

Thm. 27 : (Régraction de Legendre) $\lim_{n \to +\infty} \frac{\pi(n)}{n} = 0$

d) Tests de primalité

[ROMS p.302]

Thm. 28 : $\forall n \geq 2$ non premier a au moins un diviseur premier entre 2 et $\sqrt{n}$.

Appli 29 : Ce résultat nous donne un algorithme pour tester si un nombre est premier.

Rmq. 30 : Le crible d'Eratosthène nous permet de trouver une liste de nombres premiers.

Thm.31: Soit $n \geq 2$. Les ASSE :
(i) n est premier
(ii) $\forall \alpha \in \mathbb{N}^*, \varphi(n^\alpha) = (n-1)n^{\alpha-1}$
(iii) $\varphi(n) = n-1$
(iv) n est premier avec tous les entiers compris entre 1 et $n-1$
(v) $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps

[ROM] p.324

Thm.32: [ADM15] (Wilson) $n^{(\neq 2)}$ est premier ssi $(n-1)! \equiv -1 \ [n]$

Thm.33: (Test de primalité de Lehmer). n est premier ssi $\exists a \in \mathbb{Z}$ tq $a^{n-1} \equiv 1 \ [n]$ et pour tout diviseur d de $n-1$ tq $d \neq n-1$ $a^d \not\equiv 1 \ [n]$

[ROM] p.347 -348

Thm.34: (test de primalité de Lucas-Lehmer) $n \neq 2$ est premier ssi pour tout diviseur premier p de $n-1$, $\exists a \in \mathbb{N}$ tq $a^{n-1} \equiv 1 \ [n]$ et $a^{\frac{n-1}{p}} \not\equiv 1 \ [n]$

II - Application en théorie des corps

a) Corps finis

k un corps, $p \in \mathcal{P}$, $q = p^r$, $r \in \mathbb{N}^*$.

Prop.35: La caractéristique d'un corps est soit nulle soit un nombre premier.

Prop.36: Si k est fini alors la caractéristique de k est un nombre premier p et le sous corps premier de k est $\frac{\mathbb{Z}}{p\mathbb{Z}} := \mathbb{F}_p$

Prop.37: Si k est fini alors son cardinal est la puissance d'un nombre premier $p = \text{car}(k)$.

Prop.38: Si $\text{car}(k) = p$. $F : k \to k$, $x \mapsto x^p$ est appelé morphisme de Frobenius
Si k est fini c'est un automorphisme.
Si $k = \mathbb{F}_p$ c'est l'identité.

[PER] p.72 -76

Prop.39: $\exists!$ existe un corps à q éléments c'est $D_{\mathbb{F}_p}(X^q - X)$.

Rmq.40: Ce corps est unique à isomorphisme près.

Thm.41: $\mathbb{F}_q^\times$ est cyclique ! donc iso. à $\frac{\mathbb{Z}}{q-1\mathbb{Z}}$)

Thm.42: $\forall n \in \mathbb{N}^*$ $nI_n(p) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$ où $I_n(p)$ est le nombre de polynôme unitaire de degré irréductible dans $\mathbb{F}_p[X]$

[ROM] p.424 -425

Thm.43: Pour tout $P \in \mathbb{F}_p[X]$ unitaire irréductible $\mathbb{F}_q \simeq \frac{\mathbb{F}_p[X]}{(P)}$

b) Réduction modulo $p \in \mathcal{P}$

Thm.44: (Eisenstein) Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si
- $p \nmid a_n$
- $p \mid a_i \quad \forall i \in \{0, \dots, n-1\}$
- $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$. Si $\text{pgcd}(a_0, \dots, a_n) = 1$ alors P est irréductible dans $\mathbb{Z}[X]$.

[PER] p.76 -77

Thm.45: Soit $p \in \mathcal{P}$, $P \in \mathbb{Z}[X]$. En notant $\bar{P}$ sa réduction sur $\mathbb{F}_p$. Si $\deg(P) \neq 0$ dans $\mathbb{F}_p$ et $\bar{P}$ irréductible sur $\mathbb{F}_p$ alors P est irréductible sur $\mathbb{Q}[X]$.

Def.46: On appelle n-ème polynôme cyclotomique la quantité
$\Phi_n(X) = \prod_{\zeta \in U_n^*} (X - \zeta)$ où U_n^* est l'ensemble des racines n-ème primitives de l'unité
Une application de la réduction modulo p est ce résultat :

[PER] p.73 -82

Thm.47: $\forall n \in \mathbb{N}$, Φ_n est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

III - Application en théorie des groupes

a) Nombres premiers et groupes

G un groupe

Thm.48: Soit $p \in \mathcal{P}$, et G d'ordre p, alors G est cyclique ($G \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$)

Thm.49: (Cauchy) G un groupe fini et $p \in \mathcal{P}$. Si $p \mid |G|$ alors G a au moins un élément d'ordre p.

[PER] p.15

Def.50: Soit $p \in \mathcal{P}$. On appelle p-groupe un groupe fini dont l'ordre est une puissance de p.

Prop.51: Soit G un p-groupe non trivial. Alors son centre $Z(G) = \{z \in G \mid \forall g \in G \ zg = gz\}$ est non trivial.

[PER] p.A -18

b) Théorèmes de Sylow

G d'ordre fini n et $p \in \mathcal{P}$.
On note $|G| = p^m q$ où $p \nmid q$ et $m \in \mathbb{N}$.

Def.52: Un p-Sylow de G est un sous groupe de G d'ordre p^m.

Thm. 53 [CADHISS] (Sylow) On a :
- $\exists P$ associé 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. Tous les p-Sylow de G sont conjugués. En particulier, soit S un p-Sylow de G, on a que S est distingué dans G ssi S est l'unique p-Sylow de G.
- En notant n_p le nombre de p-Sylow alors $n_p = 1 [p]$ et $n_p | q$.

[CBER] p.311 -313

Exe. 54: Tout groupe d'ordre 63 est simple

c) Automorphismes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ $n \in \mathbb{N}$, $n \geq 2$.

Prop. 55: $\mathrm{Aut}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$

Prop. 56: $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \simeq \prod_{i=1}^{r} \left(\frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}\right)^\times$ où $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ décomp. en facteurs

Lemme 57: Soit $k \in \mathbb{N}^*$, $p \in \mathcal{P} \setminus p \neq 2$. On a :
$(1+p)^{p^k} = 1 + \lambda p^{k+1}$ où $\mathrm{pgcd}(\lambda, p) = 1$

Thm. 58: Soit $p \in \mathcal{P}$, $p \neq 2$ et $\alpha \in \mathbb{N}^*$ alors :

$$\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{\varphi(p^\alpha)\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p^{\alpha-1}(p-1)\mathbb{Z}}$$

Thm. 59: Soit $\alpha \geq 3$ alors $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ n'est pas cyclique

[CBER] p.25 -27 DEV1

Lemme 60: Soit G un groupe fini. $a, b \in G$ d'ordres p et q.
Si $ab = ba$ et $\mathrm{pgcd}(p,q) = 1$ alors ab est d'ordre pq

III. L'anneau des entiers de Gauss et les nombres premiers

On note $\Sigma := \{n \in \mathbb{N} \mid n = a^2 + b^2,\ a, b \in \mathbb{N}\}$

Def. 61: On appelle anneau des entiers de Gauss l'ensemble $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, c'est un anneau intègre.
On définit $N : \mathbb{Z}[i] \to \mathbb{N}$
$a + ib \mapsto a^2 + b^2 \ (= (a+ib)(a-ib))$

Prop. 62: $\forall z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$

Prop. 63: $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $z \in \mathbb{Z}[i]^\times$ ssi $N(z) = 1$

Prop. 64: Σ est stable par produit.

Prop. 65: $(\mathbb{Z}[i], N)$ est euclidien.

Lemme 66: -1 est un carré de $\mathbb{F}_p$ ssi $p = 2$ ou $p = 1 [4]$

Lemme 67: $p \in \Sigma$ ssi p n'est pas irr. dans $\mathbb{Z}[i]$

Thm. 68: $p \in \mathcal{P}$. $p \in \Sigma$ ssi $p = 2$ ou $p = 1 [4]$

Thm. 69: $n \in \mathbb{N}^*$ tq $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.
$n \in \Sigma$ ssi $v_p(n)$ est pair pour $p = 3 [4]$

DEV1A [CPER] p.56 -58 DEV2B

Thm. 70: Les irréductibles de $\mathbb{Z}[i]$ sont (à inversibles près) :
- $p \in \mathcal{P}$ tq $p = 3 [4]$
- $z \in \mathbb{Z}[i]$ tq $N(z) \in \mathcal{P}$

Références :
[ROU] : Rombaldi, algèbre et géo ...
[CAR] : Caregha, Theorie ...
[PER] : Perrin, cours d'algèbre
[BER] : Berhuy, algèbre le grand combat