Plan détaillé [121] : Nbre 1er

I) Arithmétique dans $\mathbb{Z}$:

A) Premiers résultats :

(on suppose déf pgcd / ppcm acquis ?)

[GOU] p 9 - 11

THM 1 : $\mathbb{Z}$ euclidien $\rightsquigarrow$ div eucli

THM 2 : Bézout

THM 3 : Gauss

(démo : voir ROM fait chier GOU à faire aucune démo)

Déf 4 : nbre 1er

THM 5 : Thm fondam. de l'arithmétique

(⚠ ordre GOU on utilise Euclide pour THM 5)

Rem 6 : On a donc $\mathbb{Z}$ factoriel

Prop 7 : "autre" déf de pgcd / ppcm via la déc. en facteurs 1er

Prop 8 : p 1er, $p \mid a_1 \dots a_n \Rightarrow \exists i$ tq $p \mid a_i$

THM 9 : L'ensemble des nbres 1er est infini

Prop 10 : $n \geq 2$, $(\mathbb{Z}/n\mathbb{Z})$ corps $\Leftrightarrow$ n 1er

Cons 11 : $p \geq 2$, 1er, $\forall a \in \mathbb{Z}$ tq $p \nmid a$, $a^{p-1} \equiv 1\ [p]$; $\forall a \in \mathbb{Z}$, $a^p \equiv a\ [p]$. — Thm de Fermat

B) Fonctions particulières :

[GOU] p. 34

Déf 12 : indicatrice d'Euler

Prop 13 : p 1er $\Rightarrow \varphi(p) = p-1$, $\forall a \in \mathbb{Z}$ tq $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1\ [n]$

Rem 14 : on retrouve le thm de Fermat

Prop 15 : • $n = \prod p_i^{\alpha_i}$ $\quad \varphi(n) = \prod (p_i - 1) p_i^{\alpha_i - 1} = n \prod \left(1 - \frac{1}{p_i}\right)$

• $n \wedge m = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$

[ROM]

Prop 16 : $\forall n \geq 2$, $\sum_{d \mid n} \varphi(d) = n$

Cons 17 : Tt ss-grpe fini de $K^\times$ (où K corps) est cyclique

ex $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclique.

THM 18 : CNS cyclicité $(\mathbb{Z}/n\mathbb{Z})^\times$. — Dév 1

[ZÉM] ([PER] ou [ROM])

[ROM] p. 389

Déf 19 : fct μ Möbius

Lemme 20 : $\forall n \geq 1$, $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$

THM 21 : formule d'inv. de Möbius

Appli 22 : $\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}$. $\forall n \in \mathbb{N}^*$.

p. 339

[ROM] p. 401

Déf 23 : fct zeta $\zeta(\alpha) = \sum_{n=1}^{+\infty} 1/n^\alpha$

THM 24 : • le produit $\prod \frac{1}{1 - \frac{1}{p_n^\alpha}}$ est CV et vaut $\zeta(s)$

• $\lim_{\alpha \to 1^+} \zeta(\alpha) = +\infty$ on en déduit $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$

(si on a le tps ? enlever je pense)

C) Répartition des nombres premiers :

[GOU]

$\mathcal{P}$ = ens. des nbres 1er, $\mathcal{P}_n = \mathcal{P} \cap [1; n]$; $\pi(n) = \mathrm{card}(\mathcal{P}_n)$

[ROM] p 364 - p 372

THM 26 : (Inégalité de Tchebychev) : $\forall n \geq 3$, $\frac{\ln(2)\, n}{\ln(n)} \leq \pi(n) \leq e \frac{n}{\ln(n)}$

Cor 27 : $\forall n \geq 2$, $\frac{1}{e} n \ln(n) \leq p_n \leq \frac{2}{\ln(2)} n \ln(n)$

(↑ juste idées car super long)

THM 28 : (Raréfaction de Legendre) : $\frac{\pi(n)}{n} \xrightarrow[n \to +\infty]{} 0$

THM 29 [admis] (Hadamard-de la Vallée-Poussin) : $\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$

Prop 30 : $\alpha, \beta \in \mathbb{R}$, • $\sum \frac{1}{p_n^\alpha}$ CV ssi $\alpha > 1$

• $\sum \frac{1}{p_n^\alpha (\ln(p_n))^\beta}$ CV ssi $[\alpha > 1$ et $\beta \in \mathbb{R}]$ ou $[\alpha = 1, \beta > 0]$

(pas envie d'en mettre + mais on peut aller voir [FRA_AL1])

II) Application en théorie des corps et réduction mod p :

A) Corps finis : $p \in \mathcal{P}$

[ROM] p 415 - 421 + [PER] p 72 - 73

Déf 31 : caractéristique d'un anneau / corps (+ rem pr anneau intègre car$(A) = p \in \mathcal{P}$)

Déf 32 : ss-corps 1er k de K

Prop 33 : si car$(K) = 0$, $k \simeq \mathbb{Q}$, si car$(K) = p$, $k \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Déf-Prop 34 : morphisme de Frobenius

THM 35 : si K fini, $|K| = p^n$ où $p = \mathrm{car}(K)$ + les ss-corps de K sont les $\mathbb{F}_{p^d}$, $d \mid n \dots$

THM 36 : Existence et unicité d'un corps à p^n élém...

Rem 37 : Une autre manière de voir les corps finis : corps de rupture ex de $\mathbb{F}_4$ ou $\mathbb{F}_9$...

(THM 38 : Wedderburn) ← vrm là ?

|121| Suite :

II) B) Carrés de $\mathbb{F}_q$: p 1er impair, $n \in \mathbb{N}^*$, $q = p^n$

Notations 39 : $\mathbb{F}_q^{\,2}$, $\mathbb{F}_q^{*2}$

THM 40 : • $\frac{q-1}{2}$ carrés et non carrés dans $\mathbb{F}_q^*$

• -1 carré de $\mathbb{F}_q^* \Leftrightarrow q \equiv 1 [4]$

Déf 41 : symbole de Legendre

Lemme 42 : $\#\{x \in \mathbb{F}_p \mid ax^2 = 1\} = \left(\frac{a}{p}\right) + 1$, $a \in \mathbb{F}_p^*$

THM 43 : • $\forall a \in \mathbb{F}_p^*$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ dans $\mathbb{F}_p$

$\left(\frac{\cdot}{p}\right)$ est l'unique morphisme de grpe non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$

[ROM] p 428 – 431

THM 44 : Loi de réciprocité quadratique (Dév 2) [CAL]

+ Thm Frob-Zolotarev + exemples ← aller voir dans [GOZ]

C) Application à la réduction des polynômes mod p :

THM 45 : Critère d'Eisenstein (dans $\mathbb{Z}, \mathbb{Q}$)

THM 46 : réduct° mod p

Ex 47 : 2 / 3 exs.

Déf 48 : polyn. cyclot.

Prop 49 : $X^n - 1 = \prod_{d|n} \Phi_d$, $\Phi_d \in \mathbb{Z}[X]$, $\forall n$

Ex 50 : 2 / 3 exs

THM 51 : Φ_n irréd. sur $\mathbb{Q}$ et sur $\mathbb{Z}$

Rem 52 : La preuve nécessite la réd mod p C3 ...

[PER] p. 76 – 83

III) D'autres applications :

A) Théorie des groupes :

[ROM]

Prop 53 : Un grpe de card 1er est cyclique

Prop 54 : Un grpe commutatif d'ordre pq où p, q 1er $\neq$, est cyclique (9)

Déf 55 : p-groupe

THM 56 : Le centre d'un p-grpe est non trivial (10)

Applis 57 : Tt ss-grpe d'ordre p^2 est commutatif (11)

THM 58 : Cauchy

Rem 59 : On peut prouver la prop 54 avec Cauchy aussi.

B) Nombres premiers dans $\mathbb{Z}[i]$:

[PER] p. 56 – 58

Déf-Prop 60 : $\mathbb{Z}[i]$ anneau intègre

+ N : $a+ib \mapsto a^2+b^2$ multiplicative

Prop 61 : • $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

• $\mathbb{Z}[i]$ euclidien pour le stathme N

Déf 62 : $\Sigma := \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N},\ a^2+b^2 = n\}$ ← stable par multiplicat°

THM 63 : $p \in \mathbb{N}$ 1er, $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 [4]$ (Dév 2 ?)

Lemme 62' : ——, $p \in \Sigma \Leftrightarrow p$ réductible dans $\mathbb{Z}[i]$

THM 64 : $n \geq 2$, $n \in \Sigma \Leftrightarrow v_p(n)$ pair, $\forall p \equiv 3 [4]$ 1er.

Applis 65 : irréd de $\mathbb{Z}[i]$ sont ...

C) Quelques tests de primalité : → [GOU] + [ROM] ?

[ROM] p. 324 et 347 348

Lemme 65' : $n \geq 2$, n 1er $\Leftrightarrow \varphi(n) = n-1$.

Prop 66 : (Thm de Wilson) : n premier $\Leftrightarrow (n-1)! \equiv -1 [n]$

Prop 67 : (Test de Lehmer). $n \geq 3$, n 1er $\Leftrightarrow \exists a \in \mathbb{Z}$ tq $a^{n-1} \equiv 1 [n]$ et $\forall d | n-1$, $d \neq n-1$, $a^d \not\equiv 1 [n]$

$[\exists a \in (\mathbb{Z}/n\mathbb{Z})$ d'ordre $n-1]$

Prop 68 : Test de Lucas-Lehmer : $n \geq 3$

n 1er $\Leftrightarrow \forall p | n-1, \exists a \in \mathbb{Z}$ tq $\begin{cases} a^{n-1} \equiv 1 [n] \\ a^{\frac{n-1}{p}} \not\equiv 1 [n] \end{cases}$ (12)

[GOU] p...

Appli 69 : Chiffrement RSA : voir blabla exo [GOU] (13)

Références : • [GOU] (Alg)

• [ROM]

• [PER]

Dév : [CAL] + ([ZEM])

ou

[PER]