[R]
[P]

121 : Nombres premiers. Applications

I- Généralités sur les nombres premiers

1) Définitions et propriétés [R] 303 - 307

- def
- Th Euclide
- Lemme d'Euclide
- infinité
- Th Fondamental de l'arithmétique
- Valuation p-adique
- Lien pgcd ppcm

2) Critère de primalité [R] 304 326

- test $\sqrt{n}$
- crible d'ératosthène
- Th Wilson

II- Arithmétique et applications

1) Généralités [R] 282-283 325 292 [Per] 21

- $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow$ n premier $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ intègre
- $(\mathbb{Z}/n\mathbb{Z})^\times$
- indicatrice d'Euler
- prop de l'indicatrice
- $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclique
- Th Euler
- Th Fermat
- Th Chinois

2) Les nombres de Carmichaël [R] 329

- def
- Th Korselt
- ex 561

3) Polynômes cyclotomiques et répartition des nombres premiers. [R] 285 [R] 308

- $\mathbb{U}_n$ et $\mathbb{U}_n^*$
- def polynôme cyclotomique
- $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$
- p premier $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$
- $\Phi_n(X) \in \mathbb{Z}[X]$

DEV1

- Th Dirichlet faible [FGN] 136
- Th des nb premiers (Admis)

III - Autres applications

1) Nombres premiers dans $\mathbb{Z}[i]$ [Per] 56-57

- def $\mathbb{Z}[i]$
- def $\leq$
- Th des 2 carrés
- irréductibles de $\mathbb{Z}[i]$

2) Irréductibilité des polynômes [Per] 76-77

- Eisenstein
- Réduction modulo p
- exemples

121: Nombres premiers. Applications

I- Généralités sur les nombres premiers

1) Définitions et propriétés

[R] 303 **Définition 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 de tous les nombres premiers

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

304 **Lemme 3** Soit $p \in \mathcal{P}$. Pour tout $n \in \mathbb{N}^*$, on a soit p divise n, soit p est premier avec n.

Lemme 4: Deux nombres premiers distincts sont premiers entre eux.

305 **Lemme 5** (Euclide) Soit $(n_k)_{1 \leq k \leq r}$ suite de $r \geq 2$ entiers naturels non nuls. Un nombre premier p divise $\prod_{k=1}^{r} n_k$ si, et seulement si, il divise l'un des n_k

Théorème 6 (Euclide) L'ensemble $\mathcal{P}$ des nombres premiers est infini.

306 **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 tels que $2 \leq q_1 < \dots < q_r$ et les $\alpha_k \in \mathbb{N}^*$.

Définition 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 $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$

Théorème 10: Soit $n, m \in \mathbb{N}^* \setminus \{1\}$ et $n = \prod_{k=1}^{r} q_k^{\alpha_k}$, $m = \prod_{k=1}^{r} q_k^{\beta_k}$ 307 leurs décomposition en facteurs premiers. ($\alpha_k, \beta_k \in \mathbb{N}$)
On a alors : $n \wedge m = \prod_{k=1}^{r} q_k^{\min(\alpha_k, \beta_k)}$ et $n \vee m = \prod_{k=1}^{r} q_k^{\max(\alpha_k, \beta_k)}$

2) Critères de primalité

Théorème 11: Tout entier n supérieur ou égal à 2 non premier a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$. 304

Méthode 12: Le théorème nous donne un algorithme 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 13 (Crible d'Eratosthène) On cherche les nombres premiers inférieurs ou égaux à $n \in \mathbb{N}$.
- On fait la liste des nombres entiers entre 2 et $\sqrt{n}$.
- On garde 2 et on supprime tous les multiples de 2.
- On garde le premier entier strictement plus grand que 2 et on supprime ses multiples de la liste.
- On continue de la même façon 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 $\sqrt{n}$. (voir annexe)

326 **Théorème 14 :** (de Wilson) On a l'équivalence entre :

$n \in \mathbb{P} \iff (n-1)! \equiv -1 \ [n]$

II - Arithmétique et applications

1) Généralités

Proposition 15 : Soit $n \geq 2$ On a les équivalences :

1) n est premier
2) $\mathbb{Z}/n\mathbb{Z}$ est un corps
3) $\mathbb{Z}/n\mathbb{Z}$ est intègre

282 **Définition 16 :** Soit $n \geq 2$. On pose $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$

Définition 17 : On appelle fonction indicatrice d'Euler la fonction qui à $n \in \mathbb{N}^*$ associe $\varphi(n)$ le nombre d'entiers compris entre 1 et n premiers avec n.

Proposition 18 : $\varphi(n)$ est égal au nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, et aussi au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

325 **Proposition 19 :**
- Si $p \in \mathbb{P}$, $\varphi(p) = p-1$
- $\forall p \in \mathbb{P}, \forall \alpha \in \mathbb{N}^*$ $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$
- $\forall m, n \in \mathbb{N}^*$, si $m \wedge n = 1$ $\varphi(mn) = \varphi(m)\varphi(n)$
- Soit $n = \prod_{i=2}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers Alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$

- $\forall n \in \mathbb{N}^*$, $n = \sum_{d \mid n} \varphi(d)$

252 **Théorème 20 :** Pour $p \geq 3$ premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique

DEV 1 b)

Théorème 21 : (Euler) 283
Pour tout $a \in \mathbb{Z}$ premier avec n, on a $a^{\varphi(n)} \equiv 1 \ [n]$.

Théorème 22 : (Fermat)
Soit $p \in \mathbb{N}^*$ premier. Soit $a \in \mathbb{Z}$. Alors $a^p \equiv a \ [p]$
Si $a \wedge p = 1$ alors $a^{p-1} \equiv 1 \ [p]$

Théorème 23 : (Théorème Chinois) [Per] 21
Si p et q sont des entiers premiers entre eux, on a

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

2) Les nombres de Carmichaël

Définition 24 : On appelle nombre de Carmichaël tout entier $n \geq 3$ non premier tel que $a^{n-1} \equiv 1 \ [n]$ pour tout entier a premier avec n. [R] 329

Exemple 25 : $n = 561$ est un nombre de Carmichaël.

Théorème 26 : (Korselt).
Pour $n \geq 3$, n est un nombre de Carmichaël si et seulement si il existe $r \geq 3$ et des nombres premiers $(p_i)_{1 \leq i \leq r}$ tels que $n = \prod_{i=1}^{r} p_i$ et pour tout indice $i \in \{1, \dots, r\}$ $p_i - 1$ divise $n - 1$.

DEV 1 a)

3) Polynômes cyclotomiques et répartition des nombres premiers

[R] 285

$\forall n \in \mathbb{N}^*$, on note $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ racines n-ièmes de l'unité et μ_n^* les racines primitives n-ième de l'unité.

Définition 27 : Pour $n \in \mathbb{N}^*$, on appelle polynôme cyclotomique le polynôme $\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$.

Théorème 28 : $\forall n \in \mathbb{N}^*$, on a $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Proposition 29 : Si $p \in \mathbb{N}^*$ est premier, alors $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 30 : Soit $n \in \mathbb{N}^*$. On a $\Phi_n(X) \in \mathbb{Z}[X]$.

[FGN] p136 **Théorème 31 :** (Dirichlet faible)
Pour tout $n \in \mathbb{N}$, il existe une infinité de nombres premiers congru à 1 modulo n.

[R] p 308 **Théorème 32 :** (des nombres premiers) Admis
$\forall n \in \mathbb{N}^*$, on note $\pi(n) = \mathrm{Card}(\mathcal{P})$. On a donc

$$\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)} \quad \mathcal{P} \leq n$$

III – Autres applications.

1) Nombres premiers dans $\mathbb{Z}[i]$.

[Per] 56 57 **Définition 33 :** On définit l'anneau des entiers de Gauss

$$\mathbb{Z}[i] := \{ a+ib \in \mathbb{C},\ a, b \in \mathbb{Z} \}$$

On lui attribue la norme $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$

$$z = a+ib \longmapsto z\bar{z} = a^2 + b^2.$$

Définition 34 : On note Σ l'ensemble

$$\Sigma = \{ n \in \mathbb{N} \text{ tel que } \exists (a,b) \in \mathbb{N}^2 \text{ tel que } n = a^2 + b^2 \}$$

Théorème 35 : Soit p un nombre premier, on a :

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1 \ [4].$$ **DEV 2**

Théorème 36 : Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :

1) Les entiers premiers $p \in \mathbb{N}$ avec $p \equiv 3 \ [4]$
2) Les entiers de Gauss $a+ib$ dont la norme a^2+b^2 est un nombre premier.

2) Irréductibilité des polynômes.

Théorème 37 : (Critère d'Eisenstein)
Soit $P(X) = a_n X^n + \dots + a_0$ avec $a_i \in \mathbb{Z}$. Soit $p \in \mathbb{N}^*$ premier. 76.
Supposons : 1) $p \nmid a_n$
2) $\forall i = 0, \dots, n-1$, $p \mid a_i$
3) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$ et si $\mathrm{pgcd}(a_i) = 1$, P est irréductible dans $\mathbb{Z}[X]$.

Théorème 38 : (Réduction)
Soit $P(X) = a_n X^n + \dots + a_0$ un polynôme de $\mathbb{Z}[X]$ et $\bar{P}$ sa réduction dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier. On suppose $\bar{a}_n \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$. Alors, si $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}$, le polynôme P est irréductible dans $\mathbb{Q}[X]$.

Exemple 39 : • $3X^4 + 10X^2 + 5$ est irréductible dans $\mathbb{Z}[X]$
• $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$.

Référencer :
- ROMBALDI – Mathématiques pour l'agrégation – Algèbre et géométrie
- PERRIN – Cours d'Algèbre.

→ premiers nb remarquables étudié pas de diviseurs autre que 1 et lui même

121 : Nombres premiers applications

PQ étudier les nb premier ?

→ Th Fondamentale de l'arithmétique $n = \prod_{p \in P} p_i^{\alpha_i}$

→ utile en cryptographie

→ Pb non résolu : pas de formule explicite pour trouver tous les nb premiers

particularités
→ infinité
→ Tt entiers n admet un diviseur premier

Critères ?

→ test (cible eratosthène, wilson...)

Utilités ?

En arithmétique

$\mathbb{Z}/p\mathbb{Z}$ corps ssi p premier

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

Th Fermat $a \wedge p = 1$ $a^{p-1} \equiv 1 [p]$

↳ CN pas suffisante de primalité

Dev 1

ex Nb de Carmichaël "Faux premier" vérifiant fermat

Th de Korselt

Extension d'anneaux

$\mathbb{Z}[i]$

Th des 2 carrés

Dev 2

→ irréductibles de $\mathbb{Z}[i]$

Polynomes

Eisenstein + réduction modulo p

étude des polynômes cyclotomiques pour une répartition + fine des nb premiers

Dirichlet faible
infinité de nb premier congru à 1 mod n.