121

Nombres premiers. Applications

$\mathcal{P}$ désigne l'ensemble des nombres premiers

I. Généralités sur les nombres premiers

1) Définitions et premières propriétés [Rom]

Définition 1 : Un entier naturel p est premier s'il admet exactement 2 diviseurs, 1 et p.

Exemple 2 : 2, 3, 5, 7 et 11 sont les premiers nombres premiers

Théorème 3 (Euclide) : Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.

Définition 4 : Un entier naturel $n \geq 2$ non premier, ie qui s'écrit $n = pq$ avec p premier et $q \geq 2$ est dit composé

Théorème 5 (Euclide) : L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Théorème 6 : Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ où les p_i sont des nombres premiers tels que $2 \leq p_1 < p_2 < \cdots < p_r$ et les α_i sont des entiers naturels non nuls.

Exemple 7 : $1120 = 2^5 \times 5 \times 7$.

Définition 8 : Soient $n \geq 2$ un entier naturel et p un nombre premier, on appelle valuation p-adique de n, noté $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. $v_p(n) = 0$ si p ne figure pas dans la décomposition.

2) Répartition des nombres premiers [Rom]

Notation 9 : Pour tout $n \in \mathbb{N}^*$, on note $\mathcal{P}_n = \mathcal{P} \cap [1, n]$ et $\pi(n) = \mathrm{Card}(\mathcal{P}_n)$

Théorème 10 (des nombres premiers) (admis) : $\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$.

Application 11 : On note, pour tout $n \in \mathbb{N}^*$ p_n le n-ième nombre premier. $\sum \frac{1}{p_n}$ est une série divergente. Il n'existe pas de mesure de probabilité $\mathbb{P}$ sur $(\mathbb{N}^*, \mathcal{P}(\mathbb{N}^*))$ telle que

$$\forall n \in \mathbb{N}^*, \ \mathbb{P}(\text{multiples de } n) = \frac{1}{n}$$

Théorème 12 (raréfaction de Legendre) $\lim_{n \to +\infty} \frac{\pi(n)}{n} = 0$.

DEV1

Théorème 13 (Progression arithmétique de Dirichlet, faible) Pour tout entier $n \geq 1$, il existe une infinité de nombres premiers de la forme $\lambda n + 1$, $\lambda \in \mathbb{N}^*$

3) Tests de primalité [Rom] [Gou]

Théorème 14 : Tout entier naturel $n \geq 2$ qui est composé a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Corollaire 15 : $n \in \mathbb{N}^*$ est premier si et seulement si il n'admet pas de diviseur premier dans $[\![2, \sqrt{n}]\!]$.

Théorème 16 (Wilson) : Soit n un entier supérieur ou égal à 2. n est premier si et seulement si $(n-1)! \equiv -1 \ [n]$

Théorème 17 (Fermat) : Soit $p \geq 2$ un nombre premier. Alors

$$\forall a \in \mathbb{Z}, \ a^p \equiv a \ [p].$$

$$\forall a \in \mathbb{Z}, \ p \nmid a, \ a^{p-1} \equiv 1 \ [p].$$

Remarque 18 : La réciproque du théorème de Fermat est fausse.

Exemple 19 : $561 = 3 \times 11 \times 17$ et $\forall a \in \mathbb{Z}$, $a^{560} \equiv 1 \ [561]$.

Définition 20 : On appelle nombre de Carmichael tout entier $n \geq 3$ non premier tel que pour tout entier a premier avec n, $a^{n-1} \equiv 1 \ [n]$.

II. Arithmétique dans $\mathbb{Z}$

1) Nombres premiers entre eux [Gou] [Rom]

Définition 21 : Soient $a_1, \dots, a_n$ des entiers. Il existe un unique entier naturel d tel que $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$. Ainsi défini, d s'appelle le pgcd de $a_1, \dots, a_n$ et on note $d = \mathrm{pgcd}(a_1, \dots, a_n)$. d est aussi le plus grand diviseur commun à tous les a_i. Lorsque $\mathrm{pgcd}(a_1, \dots, a_n) = 1$, on dit que les entiers $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble. Lorsque $\mathrm{pgcd}(a_i, a_j) = 1$ dès que $i \neq j$, les entiers a_i sont premiers entre eux deux à deux.

Remarque 22 : Si les a_i sont deux à deux premiers entre eux, alors ils sont premiers dans leur ensemble. La réciproque est fausse

Exemple 23 : 3, 10 et 15 sont premiers dans leur ensemble mais $\mathrm{pgcd}(10, 15) = 5 \neq 1$.

Définition 24 : Soient $a_1, \dots, a_n$ des entiers. Il existe un unique entier naturel m tel que $a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = m\mathbb{Z}$. Ainsi défini, m s'appelle le ppcm de $a_1, \dots, a_n$ et on note $m = \text{ppcm}(a_1, \dots, a_n)$. m est aussi le plus petit entier naturel non nul multiple de tous les a_i.

Notation 25 : On note également $n \vee m$ le ppcm de n et m et $n \wedge m$ le pgcd de n et m.

Théorème 26 : Soient $n \geq 2$ et $m \geq 2$ deux entiers, $n = \prod_{k=1}^{r} q_k^{\alpha_k}$ et $m = \prod_{k=1}^{r} q_k^{\beta_k}$ leurs décompositions en facteurs premiers. Alors $n \wedge m = \prod_{k=1}^{r} q_k^{\min(\alpha_k, \beta_k)}$ et $n \vee m = \prod_{k=1}^{r} q_k^{\max(\alpha_k, \beta_k)}$

(certains α_k ~~et~~ β_k sont éventuellement nuls)

Théorème 27 (Bezout) : Des entiers $a_1, \dots, a_n$ sont premiers entre eux si, et seulement si il existe des entiers $u_1, \dots, u_n$ tels que $a_1 u_1 + \dots + a_n u_n = 1$.

Théorème 28 (Chinois) : Soient $a_1, \dots, a_n$ des entiers naturels distincts de 0 et 1. et $a = a_1 \dots a_n$. Les entiers $a_1, \dots, a_n$ sont deux à deux premiers entre eux si, et seulement si les anneaux $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$ sont isomorphes

Application 29 Le système d'équations

$$\begin{cases} k \equiv 2 \ [4] \\ k \equiv 3 \ [5] \\ k \equiv 1 \ [9] \end{cases}$$

a pour ensemble de solutions $S = \{118 + 180q, q \in \mathbb{Z}\}$.

Théorème 30 (Gauss) : Soient a, b et c trois entiers. Si a divise bc et si $a \wedge b = 1$ alors a divise c

2) Fonctions arithmétiques [Goz] [Per]

Définition 31 : On appelle fonction arithmétique toute fonction $f : \mathbb{N}^* \to \mathbb{C}$ telle que pour tout $(n,m) \in (\mathbb{N}^*)^2$, si $n \wedge m = 1$, $f(mn) = f(m) f(n)$.

Définition 32 : Pour tout $n \in \mathbb{N}^*$, on note $G_n = \{k \in [\![1,n]\!], k \wedge n = 1\}$. On définit l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ par

$$\forall n \in \mathbb{N}^*, \ \varphi(n) = \text{Card}(G_n)$$

Proposition 33 : φ est une fonction arithmétique

Proposition 34 : $\varphi(1) = 1$, si $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$

Proposition 35 : Soit p un nombre premier. $\varphi(p^n) = p^n - p^{n-1}$

Théorème 36 (Euler) : Soient $n \geq 2$ un entier naturel et $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1 \ [n]$

Proposition 37 : Soit $n \geq 2$ un entier naturel et soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Alors $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

Proposition 38 (Formule de Gauss). Pour $n \in \mathbb{N}^*$, $n = \sum_{d \mid n} \varphi(d)$.

Définition 39 : On définit la fonction de Möbius par

$$\mu : \mathbb{N}^* \to \{0, 1, -1\}$$
$$n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ contient un facteur carré} \\ (-1)^r & \text{si } n \text{ contient } r \text{ facteurs premiers deux à deux distincts} \end{cases}$$

Proposition 40 : μ est une fonction arithmétique

Proposition 41 : Soient G un groupe abélien noté additivement $f : \mathbb{N}^* \to G$. On pose $g(n) = \sum_{d \mid n} f(d)$. Alors $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$

Corollaire 42 : $\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$.

III. Applications

1) Corps finis [Per]

Théorème 43 : Soit $n \geq 2$ un entier. Les propositions suivantes sont équivalentes :

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

Notation 44 : On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier

Proposition-définition 45 : Soit $\mathbb{K}$ un corps. Soit $\varphi : \mathbb{Z} \to \mathbb{K}$ le morphisme défini par $\varphi(n) = n.1$. Le noyau est de la forme $p\mathbb{Z}$ avec $p = 0$ ou p premier

L'entier p est appelé la caractéristique de $\mathbb{K}$.

Proposition 46 : Le cardinal d'un corps fini est une puissance d'un nombre premier.

Théorème 47 : Soient p un nombre premier et $n \in \mathbb{N}^*$. On pose $q = p^n$.

1) Il existe un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.
2) $\mathbb{K}$ est unique à isomorphisme près. On le note $\mathbb{F}_q$.

2) Irréductibilité de polynômes [FGN]

Définition 48 : Soit $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$. On appelle contenu de P, noté $c(P)$ l'entier $\mathrm{pgcd}(a_0, \dots, a_n)$.

Proposition 49 : Pour tout $(P, Q) \in \mathbb{Z}[X]^2$, $c(PQ) = c(P)c(Q)$.

DEV 2

Lemme 50 : Soit $A \in \mathbb{Z}[X]$. Si A n'est pas irréductible dans $\mathbb{Q}[X]$, il existe $B, C \in \mathbb{Z}[X]$ tels que $A = BC$ avec $\deg B < \deg A$ et $\deg C < \deg A$.

Théorème 51 (Critère d'Eisenstein) Soit $A = a_n X^n + \dots + a_1 X + a_0$ dans $\mathbb{Z}[X]$. Soit p un nombre premier. On suppose que

1) p ne divise pas a_n
2) p divise $a_0, \dots, a_{n-1}$
3) p^2 ne divise pas a_0

Alors A est irréductible dans $\mathbb{Q}[X]$.

Application 52 : Si p est un nombre premier, $\phi_p(X) = 1 + X + \dots + X^{p-1}$ est irréductible

Ajouter s'il y a du temps le symbole de Legendre

Références

[FGN] Oraux X-ENS, Algèbre 1, FGN
[Gou] Algèbre, Gourdon
[Goz] Théorie de Galois, Gozard
[Per] Cours d'Algèbre, Perrin
[Rom] Algèbre et géométrie, Rombaldi