Leçon 121 : Nombres premiers. Applications.

Rombaldi
Gourdon
Garet - K. (dev 1)
Ulmer (dev. 2)

I - Généralités sur les nombres premiers

1. Définition et premières propriétés

Définition 1.1 Un entier naturel p est dit premier s'il admet exactement deux diviseurs positifs : 1 et p.

Notation 1.2 On notera $\mathcal{P}$ l'ensemble des nombres premiers.

Exemples 1.3
2, 3, 5, 7 sont des nombres premiers tandis que 1, 4, 6 ne le sont pas

Théorème 1.4 Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admet un diviseur premier.

Proposition 1.5 Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$. Alors, soit p divise n, soit p et n sont premiers entre eux.

Proposition 1.6 (Lemme d'Euclide) Soient $(n_k)_{1 \leq k \leq r}$ une famille de $r \geq 2$ entiers naturels non nuls. Soit $p \in \mathcal{P}$ tel que $p \mid \prod_{k=1}^{r} n_k$ alors il existe $k \in [\![1, r]\!]$ tel que $p \mid n_k$.

Théorème 1.7 (fondamental de l'arithmétique) 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 $p_1, \dots, p_r \in \mathcal{P}$ et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$.

Remarque 1.8 Cette décomposition permet de donner explicitement le ppcm et le pgcd de deux nombres entiers naturels non nuls.

Proposition 1.9 Soient $p \in \mathcal{P}$ et $k \in [\![1, p-1]\!]$. Alors p divise $\binom{p}{k}$.

Théorème 1.10 (de Wilson) Un entier $p \geq 2$ est un nombre premier si et seulement si $(p-1)! \equiv -1 \mod p$.

2. Répartition des nombres premiers

Théorème 1.11 L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Conséquence 1.12 On a $\mathcal{P} = (p_k)_{k \geq 1}$, de sorte que si $k_1 < k_2$, $p_{k_1} < p_{k_2}$.

Proposition 1.13 En notant pour tout $s > 1$, $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$, on obtient que pour tout $s > 1$, $\frac{1}{\zeta(s)} = \prod_{k=1}^{+\infty} \left(1 - \frac{1}{p_k^s}\right)$.

Proposition 1.14 On a : $\sum_{k=1}^{+\infty} -\log\left(1 - \frac{1}{p_k}\right) = +\infty$ et $\sum_{k=1}^{+\infty} \frac{1}{p_k} = +\infty$.

développement 1

Théorème 1.15 (de Tchebychev) - admis En notant $\pi(n)$ le nombre de nombres premiers inférieurs ou égaux à n, on obtient pour $n \geq 3$, $\ln 2 \frac{n}{\ln n} \leq \pi(n) \leq e \frac{n}{\ln n}$.

Corollaire 1.16 Pour tout $n \geq 2$, $\frac{1}{e} n \ln(n) \leq p_n \leq \frac{2}{\ln 2} n \ln(n)$.

Théorème 1.17 (de Bertrand) - admis Pour tout entier $n \in \mathbb{N}^*$, il existe des nombres premiers compris entre n et $2n$.

3. Fonctions en arithmétique

Définition 1.18 On appelle fonction indicatrice d'Euler la fonction φ qui associe à tout $n \in \mathbb{N}^*$, le nombre d'entiers compris entre 1 et n qui sont premiers avec n.

Proposition 1.19 Un entier naturel $p \in \mathbb{N}^*$ est premier si et seulement si $\varphi(p) = p - 1$.

Conséquence 1.20 Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \mathbb{N}^*$ alors $\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{\alpha_i}$.

Définition 1.21 On appelle fonction de Möbius la fonction μ qui associe à tout $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \mathbb{N}^*$, 1 si $n = 1$, $(-1)^r$ si n est sans facteur carré et 0 sinon.

Proposition 1.22 La fonction μ est multiplicative.

Théorème 1.23 (Formule d'inversion de Möbius) Soit $f : \mathbb{N}^* \longrightarrow \mathbb{R}$. On définit $g : n \in \mathbb{N}^* \longmapsto \sum_{d|n} f(d)$. Alors, $f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$ pour tout $n \in \mathbb{N}^*$.

Application 1.24 Calcul du nombre de polynômes irréductibles et unitaires de $\mathbb{F}_q$.

II - Lien avec la théorie des corps et des groupes

1. Les corps finis

Proposition 2.1 Soit $n \in \mathbb{N}^*$. Alors les assertions suivantes sont équivalentes :

(i) n est un nombre premier

(ii) $\mathbb{Z}_n$ est intègre

(iii) $\mathbb{Z}_n$ est un corps

Théorème 2.2 (de Fermat) Soit $p \in \mathcal{P}$. Alors pour tout $k \in \mathbb{Z}$, $k^p \equiv k \mod p$ et si p ne divise pas k alors $k^{p-1} \equiv 1 \mod p$.

Proposition 2.3 Soit A un anneau intègre, alors soit $\operatorname{car} A = 0$, soit $\operatorname{car} A = p \in \mathcal{P}$.

Conséquence 2.4 Tout corps fini est de cardinal p^n avec $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$.

2. Les groupes

Définition 2.5 On appelle p-groupe un groupe fini dont l'ordre est une puissance de p, avec $p \in \mathcal{P}$.

Proposition 2.6 Soit $p \in \mathcal{P}$. Alors pour tout p-groupe G, le centre $Z(G)$ est non trivial.

Proposition 2.7 Un groupe d'ordre p^2, avec $p \in \mathcal{P}$, est abélien.

III - La primalité en pratique

1. Tests de primalité

Proposition 3.1 Tout entier $n \geqslant 2$ qui ne soit pas premier, admet au moins un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.

Conséquence 3.2 Cette proposition nous donne un premier algorithme relativement simple pour tester si $n \geqslant 2$ est premier, on effectue la division de n par tous les entiers $k \in [\![2, \lfloor \sqrt{n} \rfloor]\!]$. Si l'un des restes est nul, $n \notin \mathcal{P}$.

On peut améliorer légèrement cet algorithme, en remarquant si 2 ne divise pas n alors il est inutile de tester la divisibilité par des entiers pairs.

Proposition 3.3 (Crible d'Eratosthène) Pour obtenir la liste des nombres premiers inférieure à $\sqrt{n}$, on met en place l'algorithme suivant :

1) On se donne la liste de tous les entiers entre 2 et $\sqrt{n}$

2) On garde 2 et on supprime les autres multiples de 2 de la liste

3) Le premier entier strictement supérieur à 2 (encore dans la liste) est 3, on le garde et on supprime les autres multiples de 3

4) On continue ainsi de suite

2. Somme de deux carrés de Fermat

Définition 3.4 On définit $\sum_2 = \{ n \in \mathbb{N} \mid \exists\, a, b \in \mathbb{N},\ a^2 + b^2 = n \}$.

Théorème 3.5 Soit $p \in \mathcal{P}$. Alors $p \in \sum_2$ si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

Théorème 3.6 Un nombre entier $n = p_1^{\alpha_1} \dots p_r^{\alpha_r} \in \sum_2$ si et seulement si pour tout $i \in [\![1, r]\!]$ tel que $p_i \equiv 3\ [4]$, on a α_i est un nombre pair.

développement 2