

Leçon N° 12 1 : Nombres premiers - Applications

I) Etude des nombres premiers.

1) Présentation

Définition 1 : On dit qu'un entier naturel p est premier lorsqu'il est ≥ 2 et lorsque ses seuls diviseurs positifs sont 1 et p .

Notation 2 : On note $\mathcal{P}$ l'ensemble des nombres premiers.

Exemples 3 : 2, 3, 5, 7, 11, 13, 17 sont des nombres premiers.

Lemme 4 : (Euclidien). $\forall n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, n a au moins un diviseur premier.

Proposition 5 : Tout entier n supérieur ou égal à 2 qui se compose d'un ou de plusieurs nombres premiers p tel que $2 \leq p \leq \sqrt{n}$.

Exemple 6 : 229 est premier.

Lemme 7 : (Euclidien bis) Soit $(n_i)_{1 \leq i \leq r}$ une suite de $r \geq 2$ entiers naturels non nuls. Un nombre premier p divise le produit $a_1 \cdot \dots \cdot a_r$ si et seulement si il divise l'un des n_i .

Théorème 8 : (Fondamental de l'arithmétique). Soit $n \in \mathbb{N}$, $n \geq 2$. n se décompose de manière unique sous la forme $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_s^{\alpha_s}$ avec $p_i \in \mathbb{N}^*$, (p_i) premiers deux à deux distincts et $(\alpha_i) \in \mathbb{N}^*$, $p_1 < \dots < p_r$.

Exemple 9 : $564 = 3 \times 11 \times 17$

Proposition 10 : Soient $n \geq 2$, $m \geq 2$ deux entiers et $n = \prod_{i=1}^r p_i^{\alpha_i}$, $m = \prod_{j=1}^s q_j^{\beta_j}$ deux décompositions en facteurs premiers où les p_i sont des premiers deux à deux distincts et $\alpha_i, \beta_j \in \mathbb{N}$. Alors :
 $\text{P.C.D.}(n, m) = \prod_{i=1}^{\min(r, s)} p_i^{\min(\alpha_i, \beta_i)}$
 $\text{P.P.C.}(n, m) = \prod_{i=1}^{\max(r, s)} p_i^{\max(\alpha_i, \beta_i)}$

2) Répartition des nombres premiers

Théorème 11 : $\mathcal{P}$ est infini.

Application 12 : Le calcul d'Entierité permet de trouver tous les nombres premiers entre 2 et $n \in \mathbb{N}^*$, $n \geq 2$ finit.

Théorème 13 (Bertrand) (ADPIS) $\forall n \in \mathbb{N}^*$, il existe des nombres premiers compris entre n et $2n$.

Théorème 14 : (Hadamard et de la Vallée-Poussin) (ADPIS)

Notons $\pi : x \mapsto \text{Card}(\{p \in \mathcal{P} \mid p \leq x\})$ On a alors

$$\pi(x) \sim_{x \rightarrow \infty} \frac{x}{\ln(x)}$$

3) Tests de primalité

Définition 15 : On appelle fonction indicatrice d'Euler la fonction

$$\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$$

$$n \mapsto \# \{m \in [1, n] \mid \text{pgcd}(m, n) = 1\}$$

Théorème 16 : $\forall n \geq 2$, $\varphi(n) \in \mathbb{N}^*$.

$$1) n \in \mathcal{P}$$

$$1) \forall \alpha \in \mathbb{N}^*, \varphi(n^\alpha) = (n-1)n^{\alpha-1}$$

$$3) \varphi(n) = n-1$$

$$4) \forall m \in [1, n-1], \text{pgcd}(m, n) = 1, m+n=1$$

$$5) \frac{1}{n} \text{ est un corps}$$

$$6) \frac{1}{n} \text{ est entier}$$

Théorème 17 : (Euler) Soit $n \in \mathbb{Z}$, $\text{pgcd}(n, n) = 1$, alors $\varphi(n) \equiv 1 [n]$.

Théorème 18 : (Fermat (petit)) Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$, $p \nmid a \Rightarrow$

$$a^{p-1} \equiv 1 [p]$$

II) Théorie des corps fins

Soit K un corps fini.

Proposition 19 : La caractéristique de K est un nombre premier.

- 7) $(n-1)! \equiv -1 [n]$ (théorème de Wilson)
- 8) $(n-2)! \equiv 1 [n]$
- 9) $\forall a \in [1, n], (n-a)(a-1) \equiv (-1)^a [n]$
- 10) $n=2$ ou n impair et $\left(\frac{n-1}{2}\right)! \equiv (-1)^{\frac{n-1}{2}} [n]$
- 11) $\forall a \in [1, n-1] \left(\frac{n}{2}\right) \equiv 0 [n]$

Proposition 20: L'application $\sigma: x \mapsto x^2$ est un morphisme de corps appelé morphisme de Frobenius.

Lemme 21: Soit K un corps et $n \in \mathbb{N}$. On a $\sigma^n(x) = x^{2^n}$. Tout sous-corps de K est fixe par σ^n si et seulement si n est multiple de $\text{car}(K)$.
 Plus généralement, $\forall n \in \mathbb{N}, \exists ! \mathbb{F}_{2^n} \subseteq K$ et on a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Théorème 22: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.
 C'est le corps de définition de $\mathbb{F}_{2^n}$.

Théorème 23: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Corollaire 24: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Définition 25: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.
 C'est le corps de définition de $\mathbb{F}_{2^n}$.

Lemme 26: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Théorème 27: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

III) Fonctions de Frobenius

Définition 28: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.
 On définit la fonction de Frobenius par $f(x) = x^2$ si $x \in \mathbb{F}_2$ et $f(x) = x^2$ si $x \in \mathbb{F}_{2^n}$.

Théorème 29: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Lemme 30: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Alors $X^{2^n} - X = \prod_{\alpha \in \mathbb{F}_{2^n}} (X - \alpha)$

Théorème 31: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

IV) Applications en théorie des anneaux

1) Inductibilité des polynômes

Théorème 32: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Alors K est inductible dans $\mathbb{Q}[X]$ si et seulement si $K \cap \mathbb{Q} = \mathbb{Q}$.

Exemple 33: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Théorème 34: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Exemple 35: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

2) Théorème de la dérivée

Notations 36: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Théorème 37: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Lemme 38: Soit K un corps. On a $\sigma^n(x) = x^{2^n}$ si et seulement si $x \in \mathbb{F}_{2^n}$.

Alors

Lemme 40: $\mathcal{U}[\cdot]$ est croissante.

Lemma 41: $(p \in \Sigma) \Rightarrow (p \text{ max inductible dans } \mathcal{V}(\Gamma)) \Leftrightarrow p \in \mathcal{P}$

Exercise 42: Let $P \in \mathcal{P}$, (P, Σ) and $P = 1^{\mathbb{N}}$

II) Applications en chimie des groupes

Lemme 4.3. Soit $(G, \circ)$ est un groupe commutatif, $r \geq 2$ un entier et $a_1, \dots, a_r$ des éléments deux-à-deux distincts de G .
 1° Ordre multiples $ma_1, \dots, ma_r$, il existe dans G un élément d'ordre égal au ppcm de ces ordres.

Théorème 44: Tout sous groupe fini du groupe multiplicatif K^* ,
est isomorphe à un groupe cyclique.

Concussion 45: $\text{pin}(M) = \{ \lambda C(14), \lambda^5 = 1 \}$ est un sous groupe cyclotomique de M^Φ .

Lemme 46: Soit G un groupe fini avec $|G| = n = p^m q$, p et q premiers, $p \nmid q-1$ et soit H un sous groupe de G .

Supposons que C admette un p -Sylow S .

Neus 3906 19 259-1 714 1001 von p - 25900 de H.

théorème 67 (Sylvester) Soit G un groupe fini et soit $p \in \mathcal{P}$.

 $|G| = p^m q$ over $m \geq 0$ and $p \nmid q$.

Alors $\forall$ ϵ p-sup ϵ est sup p-sup ϵ sont

Condensin from *p*-Synthase

2) Le composé a) un p-Sulfone de C est un p-Sulfone de C et le composé b) un p-Sulfone de C est un p-Sulfone de C

En particulier, si S est un p -système de G , alors $S \trianglelefteq G$ car S est l'unique p -système de G .

3) $S_1 N p$ ist die nominale $S_1 p$ -Eigenschaft die G,
 von $S_1 N p \equiv T p$ zu $N p$ q.

Lemmas 48 n. 7.5, fin est engendré par les 3-éléments

Lemme 43: $n \geq 5$, les 3-cycles sont conjugués dans A_n

Lemme 50: Les doubles transposés sont conjugués dans B_1 .

Application 5.4: $V_n \geq 5$, $\mathcal{A}_n$ ex-samples