Leçon n° 121 : Nombres premiers. Applications.

I/ Généralités sur les nombres premiers.

A/ Nombres premiers. [ROM]

Définition 1 : Nombre premier et ensemble $\mathcal{P}$.

Exemple 2 : 2, 3, 5, 7, 11 sont premiers mais pas $6 = 2 \times 3$.

Lemme 3 : Lemme d'Euclide : tout $x \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admet un diviseur premier.

Théorème 4 : Décomposition en facteurs premiers.

Application 5 : $\mathbb{Z}$ est principal et ses idéaux maximaux sont les $p\mathbb{Z}$ avec $p \in \mathcal{P}$.

Application 6 : Calcul de pgcd et ppcm.

Exemple 7 : $18 = 2 \times 3^2$.

B/ Répartition des nombres premiers. [ROM]

Théorème 8 : $\mathcal{P}$ est de cardinal infini.

Proposition 9 : Crible d'Ératosthène.

Théorème 10 : [Culturel] Théorème de Bertrand.

Théorème 11 : [Culturel] Théorème de De La Vallée-Poussin.

II/ Tests de primalité et cryptographie RSA. [ROM] [G]

Théorème 12 : Euler.

Théorème 13 : Fermat.

Remarque 14 : Réciproque fausse, nombres de Carmichaël.

Application 15 : Test de primalité de Fermat.

Application 16 : Cryptographie RSA.

Théorème 17 : Théorème de Wilson

III/ Applications en algèbre.

A/ En théorie des groupes. [PER]

Définition 18 : p-sous-groupe de Sylow.

Théorème 19 : Théorème de Sylow 1 : Existence des p-Sylows.

Théorème 20 : Théorème de Sylow 2 : Dénombrement des p-Sylows et ils sont tous conjugués.

Corollaire 21 : Un p-Sylow est unique ssi il est distingué.

Application 22 : Un sous-groupe d'ordre 63 n'est pas simple. Les groupes d'ordre pq avec p et q premiers distincts ne sont pas simples.

B/ En théorie des corps. [PER] [ROM]

Proposition 23 : Caractéristique et $\mathbb{F}_p$ sous-corps premier des $\mathbb{K}$ de caractéristique p.

Corollaire 24 : Les corps finis sont de cardinalité une puissance d'un nombre premier.

Théorème 25 : Existence et unicité des corps finis.

Exemple 26 : Construction explicite de $\mathbb{F}_4$.

Définition 27 : Morphisme de Frobenius.

Proposition 28 : C'est un automorphisme.

Théorème 29 : L'ensemble des $\mathbb{F}_p$-isomorphismes de $\mathbb{F}_q$ est cyclique engendré par le Frobenius.

Proposition 30 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n!H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

C/ Étude des carrés dans $\mathbb{F}_p$. [PER] [ROM]

Proposition 31 : Nombres de carrés dans $\mathbb{F}_p$.

Proposition 32 : Caractérisation des carrés : x est un carré $\iff x^{\frac{p-1}{2}} = 1$ et x est un non carré $\iff x^{\frac{p-1}{2}} = -1$.

Application 33 : Algorithme pour trouver des carrés dans $\mathbb{F}_p$: tirer au hasard un élément de $x \in \mathbb{Z}/p\mathbb{Z}$ et calculer $x^{\frac{p-1}{2}}$ pour tester s'il s'agit d'un carré ou non.

Corollaire 34 : -1 est un carré mod $p \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.

Développement 1

Application 35 : Théorème des deux carrés.

Définition 36 : Symbole de Legendre.

Théorème 37 : C'est un morphisme.

Lemme 38 : Réduction des formes quadratiques sur $\mathbb{F}_p$.

Développement 2

Théorème 39 : Loi de réciprocité quadratique.

Proposition 40 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Application 41 : On peut calculer tous les symboles de Legendre, exemple de calcul d'un d'entre eux.

D/ Irréductibles de $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ et réduction mod p. [PER]

Proposition 42 : Eisenstein dans $\mathbb{Z}[X]$.

Application 43 : Il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$ (considérer les $X^n - p$ avec p premier) et $\overline{\mathbb{Q}}$ est donc de dimension infinie en tant que $\mathbb{Q}$-espace vectoriel.

Proposition 44 : Irréductibles et réduction mod p.

Définition 45 : Polynôme cyclotomique Φ_n.

Proposition 46 : $\Phi_n \in \mathbb{Z}[X]$ unitaire.

Théorème 47 : Il sont irréductibles dans $\mathbb{Z}[X]$ et donc dans $\mathbb{Q}[X]$ car unitaires.

Corollaire 48 : $[\mathbb{Q}(e^{\frac{2i\pi}{n}}) : \mathbb{Q}] = \varphi(n)$.

Références :

— [PER] Perrin p. 18, p. 72 et p. 76
— [ROM] Rombaldi Algèbre 2nd éd. p. 303 et p. 426
— [G] Gourdon Algèbre p. 34-37