Leçon 110 : NOMBRES PREMIERS . APPLICATIONS.

I - Généralités

1) Définitions et premiers résultats d'arithmétique [WAR]

Déf : Un entier $p \geq 2$ est dit premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p. Sinon il est dit composé. On note $\mathcal{P}$ l'ensemble des nb premiers

Application : Tout groupe d'ordre p premier, est cyclique.

Déf : Deux entiers a et b sont premiers entre eux si leur pgcd est 1.

Théorème de Bézout : $a, b \in \mathbb{Z}$ sont premiers entre eux ssi il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$

Théorème de Gauss : $a, b, c \in \mathbb{Z}$, si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

Applications :
- si p est premier, $p \mid \binom{p}{k}$ pour tout $k \in \{1, \dots, p-1\}$ et $(a+b)^p \equiv a^p + b^p \ [p]$.
- équations diophantiennes $ax + by = c$

Prop : Tout entier $n \geq 2$ possède un diviseur premier.

Th : Il existe une infinité de nombres premiers.

Ex : Il existe une infinité de nombres premiers de la forme $6n-1$ ou $4n-1$

2) Factorisation et décomposition en facteurs premiers [WAR]

a) Théorème fondamental de l'arithmétique

Théorème : Tout entier $n \geq 2$ s'écrit de manière unique, à l'ordre près, sous la forme $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec $p_i \in \mathcal{P}$ distincts et $\alpha_i \in \mathbb{N}^*$.

Applications :
- Calcul du pgcd et du ppcm de $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{k} p_i^{\beta_i}$ avec $p_i \in \mathcal{P}$ distincts et $\alpha_i, \beta_i \in \mathbb{N}$:
  $\text{pgcd}(a,b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$ et $\text{ppcm}(a,b) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$
- Si $x, y \in G$ groupe abélien, alors G contient un élément d'ordre $\text{ppcm}(\text{ord}(x), \text{ord}(y))$.

Application aux équations diophantiennes : [SAIT]
- $x^2 + y^2 = z^2$ et $x^4 + y^4 = z^4$ (équations de Fermat)
- $x^2 = yz$ dans $\mathbb{N}$
- $x^2 - ny^2 = \pm 1$ (équation de Pell)

b) Fonction de Möbius [X-ENS]

Déf : La fonction $\mu : \mathbb{N}^* \to \mathbb{N}$ de Möbius est définie par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ possède un facteur carré} \\ (-1)^k & \text{si } n = \prod_{i=1}^{k} p_i \ , p_i \in \mathcal{P} \text{ distincts} \end{cases}$$

Prop : μ est multiplicative : si $n \wedge m = 1$, $\mu(nm) = \mu(n)\mu(m)$

Prop : $S(n) = \sum_{d \mid n} \mu(d) = 0$ si $n > 1$ et $S(1) = 1$

Application : La probabilité pour que deux entiers de $[\![1, n]\!]$ soient premiers entre eux est $x_n = \frac{1}{n^2} \sum_{d \mid n} \mu(d) E\left(\frac{n}{d}\right)^2$ et tend vers $\frac{6}{\pi^2}$ lorsque $n \to +\infty$. DVPT

3) Deux familles particulières [WAR]

a) Nombres de Fermat

Théorème : Tout nombre premier de la forme $a^m + 1$ avec $a, m > 1$ est de la forme $a^{2^n} + 1$ avec a pair.

Déf : $F_n = 2^{2^n} + 1$ est le n-ième nombre de Fermat.

Rq : F_0, F_1, F_2 sont premiers mais pas $F_5 = 641 \times 6700417$

Application : Construction à la règle et au compas de polygônes réguliers. [EX]

b) Nombres de Mersenne

Théorème : Tout nombre premier de la forme $a^m - 1$ avec $a, m > 1$ est de la forme $2^p - 1$ avec p premier.

Déf : Les nombres $2^p - 1$ avec p premier sont les nombres de Mersenne

Rq : $M_5 = 31$ et $M_7 = 127$ sont premiers mais pas $M_{11} = 23 \times 89$

II - Arithmétique modulaire

1) L'anneau $\mathbb{Z}/n\mathbb{Z}$ [DEL]

Prop: • $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier
• $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

Application: Critère d'Eisenstein

Déf: L'indicatrice d'Euler $\varphi : \mathbb{N}^* \to \mathbb{N}$ est définie par
$\varphi(n) = \text{Card}\{1 \leq k \leq n \mid k \wedge n = 1\}$

Prop: $\varphi(n) = \text{Card}\left(\mathbb{Z}/n\mathbb{Z}^\times\right)$

Prop: φ est multiplicative et pour p premier, $\alpha \geq 1$ $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Théorème d'Euler: Soit $n \in \mathbb{N}^*$, pour tout a premier à n, on a
$$a^{\varphi(n)} \equiv 1 \ [n]$$
En particulier, si n est premier, on obtient le petit théorème de Fermat.

2) Application en cryptographie, la méthode RSA [DEL]

Théorème: Soient p, q premiers et $n = pq$. Si e est premier avec $\varphi(n) = (p-1)(q-1)$, alors il existe $d > 0$ tel que $ed \equiv 1 \ [\varphi(n)]$.
On a alors, pour tout entier a, $a^{ed} \equiv a \ [n]$

Principe du RSA:
- Le destinataire construit (p, q, e, d) et calcule $n = pq$
- Il rend publics n et e
- L'expéditeur transforme son message en un nombre entier $A \leq n$.
- Il calcule $B = A^e \ [n]$ puis envoie B.
- Le destinataire, pour décoder B calcule $B^d \ [n]$ ce qui lui redonne A.

Rq:
- Conjecture : il est "difficile" de factoriser de grands nombres donc de trouver p et q à partir de n.
- C'est le système de cryptage le plus utilisé.

3) Résidues quadratiques modulo p [SER]

Déf: n est un résidu quadratique modulo m s'il existe a tel que $n \equiv a^2 \ [m]$

Déf: Symbole de Legendre, p premier, $n \in \mathbb{Z}$
$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n \\ 1 & \text{si } p \nmid n \text{ et } n \text{ est un résidu quadratique modulo } p \\ -1 & \text{sinon} \end{cases}$$

Identité d'Euler: p premier impair, $n \in \mathbb{Z}$
$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \ [p]$$

Ex: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \ [4] \\ -1 & \text{si } p \equiv -1 \ [4] \end{cases}$

Multiplicativité de $\left(\frac{n}{p}\right)$: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Application: Théorème des deux carrés

Déf: Soient p, q premiers distincts, Ω une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$ et $\xi \in \Omega$ une racine primitive q-ième de l'unité. On définit la "somme de Gauss" $y = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{x}{q}\right) \xi^x$

Lemme: $y^2 = (-1)^{\frac{q-1}{2}} q$, $y^{p-1} = \left(\frac{p}{q}\right)$

Loi de réciprocité quadratique: p, q premiers impairs distincts
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

DVPT

III - Recherche de nombres premiers

1) Tests de primalité [WAR] et [DET]

- **Le crible d'Eratostène:**

Théorème: Le plus petit diviseur strictement supérieur à 1 d'un nombre composé est un nombre premier inférieur à $\sqrt{n}$.

Principe: On construit un tableau des entiers $\leq n$ puis on barre successivement tous les multiples stricts des nombres premiers $\leq \sqrt{n}$.
On a alors n est premier ssi il n'est pas barré.

- **Théorème de Wilson:** p est premier ssi $(p-1)! \equiv -1 \ [p]$

- **Critère de Lucas**: Soit $n>1$ impair tel que l'on connaisse tous les facteurs premiers de $n-1$. Alors n est premier ssi il existe a tel que $a^{n-1}\equiv 1[n]$ et $a^{\frac{n-1}{q}}\not\equiv 1[n]$ pour tout diviseur q premier de $n-1$.

- **Amélioration de Pocklington**: Soit $n=ab+1>1$ avec $0<a\leqslant b+1$. Si pour tout diviseur premier p de b il existe x tel que $x^{n-1}\equiv 1[n]$ et $pgcd\left(x^{\frac{n-1}{p}}-1, n\right)=1$ Alors n est premier.

2) Tests pour les nombres de Fermat et de Mersenne [DET]

- **Test de Pépin**: $F_n=2^{2^n}+1$ est premier ssi $F_n \mid 3^{(F_n-1)/2}+1$

- **Test de Lucas-Lehmer**: $M_p=2^p-1$ est premier ssi $2^p-1 \mid S(p-1)$ où $S(1)=4$ et $S(n+1)=S(n)^2-2$, $n\geqslant 1$

3) Critères de non primalité [DET]

- **Test de Fermat**: S'il existe $a\in\{2,\dots,n-1\}$ tel que $a^{n-1}\not\equiv 1[n]$, alors n est composé. a est appelé témoin de Fermat.

Rq: La réciproque est fausse. Il existe des nombres composés tels que $a^{n-1}\equiv 1[n]$ pour tout a. On les appelle nombres de Carmichael

Th: n est un nombre de Carmichael ssi il n'est divisible par aucun carré et si pour chaque diviseur premier p de n, $p-1 \mid n-1$.

- **Critère de Miller-Rabin**: $n>1$ impair, $n-1=2^s t$ avec t impair. S'il existe $a\in\{2,\dots,n-1\}$ tel que $a^t\not\equiv 1[n]$ et $a^{2^i t}\not\equiv -1[n]$ pour $i\in\{0,\dots,s-1\}$, alors n est composé. a est appelé témoin de Miller.

Prop: Si n est composé, au moins 3/4 des $a\in\{2,\dots,n-1\}$ sont des témoins de Miller pour n.

Rq:
- C'est une amélioration du test de Fermat
- 561 est un nombre de Carmichael mais 2 est un témoin de Miller pour 561 ($560=2^4\cdot 35$ et $2^{2^4\cdot 35}\equiv 67[561]$)

IV - Répartition des nombres premiers

1) Théorème des nombres premiers [Z.-Q.]

Notation: $\pi(x)=Card(\mathcal{P}\cap[0,x])$

Théorème de raréfaction de Legendre: $\frac{\pi(x)}{x}\underset{x\to+\infty}{\to}0$

Déf: Fonction ζ de Riemann:
pour $s\in\mathbb{C}$ tel que $Re(s)>1$, $\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s}$
C'est une fonction holomorphe sur $\Omega_1=\{s\in\mathbb{C} \mid Re(s)>1\}$

Prop: pour $s\in\Omega_1$, $\zeta(s)=\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p^s}\right)^{-1}$

Prop: La fonction ζ se prolonge en une fonction méromorphe sur $\{s\in\mathbb{C} \mid Re(s)>c\}$ avec un pôle simple en 1.

Conséquence: $\sum_{p\in\mathcal{P}}\frac{1}{p}$ diverge

Déf: Pour $x\geqslant 2$, on définit $\Phi(x)=\sum_{\substack{p\in\mathcal{P}\\ p\leqslant x}}\ln(p)$

Prop: $\Phi(x)\underset{x\to+\infty}{\sim}x$

Corollaire (théorème des nombres premiers): $\pi(x)\underset{x\to+\infty}{\sim}\frac{x}{\ln x}$.

2) Théorème de la progression arithmétique [TEN]+[SER]

Théorème de Dirichlet: Soit $n\in\mathbb{N}^*$ et a premier à n. Alors il existe une infinité de nombres premiers p tels que $p\equiv a[n]$.

Notation: On note $\pi(x;a,n)$ le nombre de nombres premiers p inférieurs ou égaux à x, congrus à a modulo n.

Théorème: $\pi(x;a,n)\underset{x\to+\infty}{\sim}\frac{x}{\varphi(n)\ln x}$

Références:

[WAR] Arithmétique. Warusfel, Attali, Callet.
[DEL] Merveilleux nombres premiers. Delahaye.
[TEN] Les nombres premiers. Tenenbaum.
[DEM] Cours d'algèbre. Demazure.
[SAM] Théorie algébrique des nombres. Samuel
[Z-Q] Analyse pour l'agrégation. Zuily Queffelec
[X-ENS] Oraux X-ENS. Algèbre 1.
[EX] Exercices pour l'agrégation. Algèbre 1. Francinou Gianella.
[SER] Cours d'arithmétique. Serre

Ce dont on peut parler:
- applications en théorie des groupes
- généralisation aux idéaux premiers
- formes quadratiques, écriture de nombres premiers sous la forme $p = ax^2 + bxy + cy^2$ (Delevoets, formes quadratiques et groupes classiques)

Autres développements possibles:
- Equation de Fermat pour $n=2$ et $n=4$
- Théorème des deux carrés