121 Nombres premiers. Applications.

G = Gourdon Algèbre
P = Perrin Cours d'algèbre
R-W : Ramis Warusfel Algèbre
DEM : Demazure Cours d'algèbre

I. GÉNÉRALITÉS SUR LES NOMBRES PREMIERS.

1. Définition et exemples.

G p9 **Def 1** = Soit $p \in \mathbb{N}$, $p \geq 2$. p est dit premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Ex 2 = 2, 3, 5, 7, 11, 13 ... mais $1 \notin \mathcal{P}$

p9 **Prop 3** = L'ensemble des nombres premiers est infini.

p8 **Thm 4** = Bezout. Soient $a, b \in \mathbb{Z}$. Alors $\mathrm{pgcd}(a,b) = 1$ ssi $\exists (u,v) \in \mathbb{Z}^2$ tq $au + bv = 1$.

p8 **Thm 5** = Gauss. Soient $a, b, c \in \mathbb{Z}$, si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

2. Décomposition en facteurs premiers.

p9 **Thm 6** = Thm fondamental de l'arithmétique :
Tout entier naturel $n \geq 2$ s'écrit de manière unique à l'ordre des facteurs près sous la forme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où les p_i sont des nombres premiers distincts et les α_i des entiers naturels non nuls. On appelle cette décomposition, la décomposition de n en facteurs premiers.

Ex 7 : $300 = 2^2 \times 3 \times 5^2$

p9 **Prop 8** = Si $p \in \mathcal{P}$, $a \in \mathbb{Z}$ alors $p \mid a$ ou $p \wedge a = 1$.

p9 **Cor 9** = Lemme d'Euclide :
Si $p \in \mathcal{P}$ et $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

besoin pr thm 6

App 10 = Soit $p \in \mathcal{P}$ et $1 \leq k \leq p-1$. alors $p \mid \binom{p}{k}$

Rq 11 = Cela mène à la définition d'anneau factoriel.
$\mathbb{Z}$ est factoriel

RW p282 **App 7 bis** = Produit Eulérien $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - 1/p^s}$

3. Répartition des nombres premiers. R-W p 275-276

Thm 12 : Dirichlet : Soient $a, b \in \mathbb{N}$ tq $a \wedge b = 1$ alors $\{an + b, n \in \mathbb{N}\}$ contient une infinité de nb premiers. (admis)

Def 13. On note $\pi(n) = \mathrm{card}\{p \in \mathcal{P},\ p \leq n\}$, pour $n \in \mathbb{N}$.

Thm 14 = Thm des nombres premiers : (admis)
$\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$

à voir avec la démo...

II CRITÈRES DE PRIMALITÉ.

1. Algorithmes élémentaires.

Algorithme 15 = Soit $n \in \mathbb{N}$ $n \geq 2$. On teste si $i \mid n$ pour $i \in [\![2, n-1]\!]$ DEM p66

Rq 16 = On peut se contenter de $i \leq \sqrt{n}$.

Algorithme 17 Ératosthène :
On veut trouver $\mathcal{P} \cap \{2, .., N\}$ pour un certain N.
On pose $\mathcal{P}_1 = \{2, .., N\}$, $\mathcal{P}_2 = \emptyset$ et on fait.
Tant que $\mathcal{P}_1 \neq \emptyset$ | $P_2 \leftarrow P_2 \cup \{\min \mathcal{P}_1\}$
| $P_1 \leftarrow P_1 \setminus (\min P_1)\mathbb{N}^*$.
Alors $\mathcal{P}_2 = \mathcal{P} \cap \{2, .., N\}$

2. Un test de primalité. DEM p67

G p9 **Thm 18** = Fermat = Soit $p \in \mathcal{P}$ alors $\forall a \in \mathbb{Z}$ $a^p \equiv a\ [p]$.
et $\forall a \in \mathbb{Z}$ $p \nmid a$ $a^{p-1} \equiv 1\ [p]$.

Test 19 = n n'est pas premier (on dit qu'il est composé) ssi il existe $a \in [\![1, n]\!]$ tq $a^{n-1} \not\equiv 1\ [n]$.
On appelle un tel a, si $a \wedge n = 1$ un témoin de Fermat.

Def 20 = n est un nombre de Carmichael si $n \notin \mathcal{P}$, $a^{n-1} \equiv 1\ [n]$ pour tout $a \wedge n = 1$ et $a^n \equiv a\ [n]$ pour tout a.

Ex 21 = 561 est un nombre de Carmichael, c'est le plus petit.

III CORPS FINIS.

1. Anneaux $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler.

G p9 **Prop 22** = Soit $n \geq 2$. $\mathbb{Z}/_n\mathbb{Z}$ est un corps ssi n est premier.
On note $\mathbb{Z}/_p\mathbb{Z} = \mathbb{F}_p$ où $p \in \mathcal{P}$.

Méthode = Soit $\bar{x} \in (\mathbb{Z}/_p\mathbb{Z})^\times$, par Bezout $ap + bx = 1 \Rightarrow \bar{x}^{-1} = \bar{b}$

Ex 23 = $\overline{36}^{-1} = \overline{17}$ dans $(\mathbb{Z}/47\mathbb{Z})^\times$.

G p9 **Thm 24** Wilson = $p \geq 2$ est premier ssi $(p-1)! \equiv -1\ [p]$.

G p31 **Def 25** = Soit $n \geq 2$. On appelle indicatrice d'Euler
$\varphi(n) = \#(\mathbb{Z}/_n\mathbb{Z})^*$

Prop 26 = $\varphi(n) = \#\{k \in [\![1, n]\!],\ k \wedge n = 1\}$.

Thm 27 Euler = Si $n \geq 2$. Si $k \wedge n = 1$ alors $k^{\varphi(n)} \equiv 1\ [n]$.

Rq 28 = Ce résultat généralise le théorème de Fermat.

on peut rajouter fonctions arithmétiq

Gp31

Prop 29 : Si $n \wedge m = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$ csqce du lemme chinois

Prop 30 = Soit $p \in \mathcal{P}$, $\alpha \in \mathbb{N}$ $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Prop 31 = pour $n \geq 2$ on a $n = \sum_{d \mid n} \varphi(d)$ + Dirichlet faible (DVLPT)

2. Théorie élémentaire des corps finis - Perrin p72

Def 32 = Soit k un corps et $\psi : \mathbb{Z} \to k$, $n \mapsto n \cdot 1_k$ morphisme. Le nombre p générateur de l'idéal $\ker\psi$ est appelé la caractéristique de k. On a $p = 0$ ou $p \in \mathcal{P}$. On le note $car(k)$.

Rq 33 = Ici k est fini d'où $Car(k) \in \mathcal{P}$.

Prop 34 = Soit k un corps fini tq $car(k) = p$. Alors $|k| = p^n$, $n \in \mathbb{N}$

Prop 35 = Soit k un corps fini, $car(k) = p$. alors $F = k \to k$, $x \mapsto x^p$ est un automorphisme, appelé morphisme de Frobenius.

Rq 36 = Si $k = \mathbb{F}_p$, $F = id_{\mathbb{F}_p}$.

Thm 37 = Soit $p \in \mathcal{P}$, soit $n \in \mathbb{N}^*$. On pose $q = p^n$

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

Thm 38 = Le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique (donc isomorphe à $\mathbb{Z}/_{(q-1)}\mathbb{Z}$).

3. Carrés dans $\mathbb{F}_q$ ($q = p^n$). Perrin p74

Def 39 : $x \in \mathbb{F}_q$ est un carré ssi il existe $a \in \mathbb{F}_q^\times$ tq $x = a^2$

On note $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q, \exists a \in \mathbb{F}_q \ x = a^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$

Prop 40 = pour $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

- pour $p > 2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$

Prop 41 = Si $p > 2$, $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Cor 42 = si $p > 2$, $q = p^n$, $n \in \mathbb{N}^*$.

$-1 \in \mathbb{F}_q^2 \iff q \equiv 1 [4]$.

App 43 = il existe une infinité de nombres premiers de la forme $4m+1$.

App 44 = Théorème des deux carrés.

Soit $p \in \mathcal{P}$. p est somme de deux carrés ssi $p = 2$ ou $p \equiv 1 [4]$. DVLPT

Def 45 = Soit $p \in \mathcal{P}$, $p \geq 3$. Soit $x \in \mathbb{N}$. Symbole de Legendre : ~~Combes p268~~ ou R-W p129-130 ou Gourdon p46

On appelle symbole de Legendre :

$$\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } p \mid a \\ 1 \text{ si } a \in \mathbb{F}_q^2 \\ -1 \text{ si } a \notin \mathbb{F}_q^2 \end{cases}$$

Prop 46 = Formule d'Euler = Soit $x \in \mathbb{F}_p^\times$ alors $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ ~~DVLPT~~

Thm 47 = Loi de réciprocité quadratique.

Soit $q \in \mathcal{P}$ $q \neq p$ $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Ex 48 = $\left(\frac{3}{17}\right) = -1$: 3 n'est pas un carré dans $\mathbb{F}_{17}$.

IV APPLICATIONS

Irréductibilité de polynômes

1. Réduction des polynômes modulo p. Perrin p76-77

Thm 49 = Critère d'Eisenstein. Si $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe $p \in \mathcal{P}$ tq

- $p \nmid a_n$
- $p \mid a_i$ pour $i \in [\![0, n-1]\!]$
- $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$. Si en plus, P est primitif, il est irréductible dans $\mathbb{Z}[X]$.

App 50 = Soit $p \in \mathcal{P}$, $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}[X]$.

Thm 51 = Critère de réduction. Si $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$, $\overline{P} = P \bmod p$ où $p \in \mathcal{P}$. Si $\overline{a_n} \neq 0$ dans $\mathbb{F}_p$. Alors si $\overline{P}$ est irréductible sur $\mathbb{F}_p[X]$, P est irréductible sur $\mathbb{Q}[X]$ et si en plus P est primitif alors il est irréductible sur $\mathbb{Z}[X]$.

Ex 52 = $P = X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}[X]$. ($p = 2$).

Rq 53 = La réciproque est fausse : $X^4 + 1$ est irréductible sur $\mathbb{Z}$ (donc sur $\mathbb{Q}$) mais est réductible sur $\mathbb{F}_p$, pour tout nombre premier p.

2- Cryptographie = chiffrement RSA - Gourdon p34

Bob et Alice veulent échanger des messages sans que d'autres puissent les lire. Alice choisit un nombre $n = pq$ où $p, q \in \mathcal{P}$ $p \neq q$

On a $\varphi(n) = (p-1)(q-1)$ Elle prend $d \in \mathbb{N}$ tq $d \wedge \varphi(n) = 1$.

et c l'inverse de d modulo $\varphi(n)$. (calculable grâce à l'algorithme de Bézout). Elle publie la clé publique (n, c) mais garde secret d. Bob qui désire lui envoyer une séquence de nombres m_i lui envoie m_i^c mod n.

Alice calcule alors $m_i^{cd} \equiv m_i\ [n]$.

Rq : Les nombres premiers p et q doivent être choisis grands pour rendre impossible la factorisation : de l'ordre de 100 chiffres

L'application $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $\bar{t} \longmapsto \bar{t}^c$ est la fonction de chiffrement

et $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $\bar{t} \longmapsto \bar{t}^d$ la fonction de déchiffrement.

La sécurité de ce système repose sur le fait que connaissant la clé publique, il est très difficile de déterminer d. En fait, tout le monde peut chiffrer mais seuls ceux connaissant la clé secrète d peuvent déchiffrer.

↑ à mettre en fin de III 1).

④ = Théorie des groupes = p-groupes + thm de Sylow

IV. Théorie des groupes
1- p-groupes
2- thm de Sylow

Calais.

↑ à voir...