# 110 NOMBRES PREMIERS, APPLICATIONS

## I Généralités

### 1) Définition [WAR]

déf : Un entier n est premier s'il admet dans $\mathbb{N}$ exactement 2 diviseurs : $(1, n)$

prop : Tout entier $n \geq 1$ admet au moins un diviseur premier.

Théorème : (Euclide) si on note $\mathcal{P}$ l'ensemble des nombres premiers. $\mathcal{P}$ est infini.

### 2) Théorème fondamental de l'arithmétique. [WAR]

Théorème : Tout entier $n \geq 2$ s'écrit de façon unique sous la forme $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ où $v_p(n)$ s'appelle la valuation p-adique de n.

$v_p(n) \in \mathbb{N}$ sont tous nuls sauf en nombre fini

$v_p(n) = \sup\{k \, ; \, p^k / n\}$

prop : i) $\exists (u,v) \in \mathbb{Z}^2$ tq $au + bv = a \wedge b$ (Bézout)

ii) si $a / bc$ et $a \wedge b = 1$ alors $a / c$ (Gauss)

Applications : * Théorème des 4 carrés
* Equation de Fermat $n = 2$ et 4
* Equation Diophantienne et Sophie Germain :

(DEV) Thm : soit $p$ un nombre premier de Sophie Germain (ie. nombre premier impair tq $q = 2p+1$ soit premier). Alors il n'existe pas de $(x,y,z) \in \mathbb{Z}^3$ tq $x^p + y^p + z^p = 0$ et $xyz \neq 0 [p]$.

### 3) Fonctions multiplicatives. [FRA] + [TEN] + [GOU]

déf : $f : \mathbb{N}^* \to \mathbb{N}$ est multiplicative si $m \wedge n = 1$
$\Rightarrow f(mn) = f(m) f(n)$.

* Indicatrice d'Euler.

déf : $\varphi(n) = \text{card}\{1 \leq k \leq n \, / \, k \wedge n = 1\} = \text{card}(\mathbb{Z}/n\mathbb{Z}^*)$.

Théorème (Euler) $n > 1$ $k \wedge n = 1$

on a $k^{\varphi(n)} \equiv 1 [n]$.

prop : si $n \geq 2$ s'écrit $n = p_1^{a_1} \dots p_k^{a_k}$ avec $p_i$ premiers

Alors $\varphi(n) = n \prod_{i=1}^{k} (1 - 1/p_i)$

En particulier si $p$ premier $\varphi(p) = p-1$

$\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow$ $n$ premier.

prop : $n = \sum_{d/n} \varphi(d)$

* fonction $\sigma$

déf : $\sigma : n \to \sigma(n) = \sum_{d/n} d$

déf : un nombre est parfait si $\sigma(n) = \sigma(2n)$

prop : des nombres parfaits pairs sont les $2^{p-1} M_p$ avec $M_p$ nombre de Mersenne premier.

* fonction de Möbius.

déf : $\mu : n \to \mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur carré} \\ -1 & \text{si } n \text{ possède } k \text{ facteurs premiers distincts} \end{cases}$

prop : i) $\varphi(n) = n \sum_{d/n} \frac{\mu(d)}{d}$

ii) $\sum_{d/n} \mu(d) = 0$ si $n > 1$.

Formule d'inversion : pour $f$ et $g$ arithmétiques on a :

$g(n) = \sum_{d/n} f(d) \Leftrightarrow f(n) = \sum_{d/n} g(d) \mu(n/d)$ $n \geq 1$

Application : Calcul de la probabilité que 2 entiers entre 1 et $n$ soient premiers entre eux.

## II Recherche des nombres premiers

### 1) Nombres de Fermat / de Mersenne. [WAR]

* nombres de Fermat.

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

ex : $37 = 6^2 + 1$, $101 = 10^2 + 1$.

déf : On appelle n-ième nombre de Fermat l'entier
$F_n = 2^{2^n} + 1$

Rq : des 5 premiers nombres de Fermat sont premiers mais $F_5$ non

* Nombres de Mersenne.

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

ex : $31 = 2^5 - 1$ ; $8191 = 2^{13} - 1$

contre ex : $2047 = 23 \times 89 = 2^{11} - 1$.

déf : On appelle nombre de Mersenne tout entier $M_p = 2^p - 1$ où p premier.

## 2) Tests [DEL] + [DEM]

* 1ers tests :

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

Crible d'Eratosthène : Soit n entier, on teste si $p / n$ pour tout p premier $\leq \sqrt{n}$

Rq : ces tests ne conviennent pas pour des grands nombres.

* Tests spécialisés dans la primalité des grands nombres

Test de Lucas-Lehmer : $2^p - 1 = M_p$ est un nombre premier ssi $2^p - 1 \mid S(p-1)$ avec
$S(1) = 4$ et $S(n+1) = S(n)^2 - 2$ $n > 1$

Théorème de Proth : si $N = k \cdot 2^n + 1$ avec $k < 2^n$ et s'il existe $a \in \mathbb{N}$ tq $a^{(N-1)/2} + 1 \equiv 0 [N]$ alors N est premier.

Test de Pepin : pour les $F_n = 2^{2^n} + 1$ :
$F_n$ premier ssi $F_n \mid 3^{(F_n - 1)/2} + 1$.

* Tests probabilistes

Théorème de Fermat : si p premier et si $p \nmid a$ $(a \in \mathbb{Z})$ alors $a^{p-1} \equiv 1 [p]$

⚠ Réciproque fausse : nombres de Carmichaël.

Les nombres de Carmichaël sont des entiers n non premiers tq pour $a \wedge n = 1$ on a $a^{n-1} \equiv 1 [n]$.

Test de Fermat : On prend a au hasard entre 2 et n-1, si $a^{n-1} \not\equiv 1 [n]$ n n'est pas premier sinon on ne peut pas conclure à cause des nombres de Carmichaël.

Test de Rabin-Miller : (pour améliorer Fermat).
si on trouve $a^{n-1} \equiv 1 [n]$ on poursuit en calculant $a^{\frac{n-1}{2}} [n]$, $a^{\frac{n-1}{4}} [n]$, ....
On s'arrête à un temps fixé et on attribue une probabilité sur la primalité de n.

# III Répartition des nombres premiers [FGI] + [TEN] + [DEL]

déf : Pour tout $x > 0$, on note $\pi(x)$ le nombre de nombres premiers dans $[0, x]$

prop : il existe des plages de nombres aussi grandes que l'on veut sans nombre premier.

Théorème : (raréfaction des nombres premiers) $\frac{\pi(n)}{n} \xrightarrow[n \to +\infty]{} 0$.

Théorème de Dirichlet : $n \in \mathbb{N}^*$ il existe une infinité de nombres premiers $\equiv 1 [n]$. (version faible [DEV])

Postulat de Bertrand : pour tout $n \geq 4$ il existe $p_0$ vérifiant $n < p < 2n - 2$.

Application : si $\sqrt{n!}$ est entier alors $n = 0$ ou $1$.

prop : (Inégalité de Tchebychev) : [RMS 118]
$$0{,}92129 \frac{x}{\ln x} + O\left(\frac{x}{\ln x}\right) \leq \pi(x) \leq 1{,}10556 \frac{x}{\ln x} + O\left(\frac{x}{\ln x}\right)$$

prop : $\pi(x) = O\left(\frac{x}{\ln x}\right)$ [RMS 118]

déf : pour $Re(s) > 1$ on définit $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ la fonction zêta de Riemann

prop : • $\forall s$ $Re(s) > 1$ on a
$\zeta(s) = \prod (1 - 1/p^s)^{-1}$ : Identité d'Euler )

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

Application: Théorème des nombres premiers:

$$\pi(x) \sim \frac{x}{\ln x}.$$

# IV Cryptographie

## 1) Algorithme de Diffe-Hellman. [GRA].

2 individus Breizhman et Super-Breizh se mettent d'accord sur un premier $p$ et $g$ un générateur de $\mathbb{F}_p^*$

1) Breizhman choisit aléatoirement $a \in [2, p-2]$.
il calcule $x = g^a [p]$ $x$ est la clé publique
$a$ est la clé privée.

2) Super-Breizh choisit aléatoirement $b \in [2, p-2]$.
il calcule $y = g^b [p]$ $y$ est la clé publique
$b$ est la clé privée.

3) Breizhman calcule $k = y^a [p]$
Super-Breizh calcule $k = x^b [p]$.
$(g^a)^b = (g^b)^a = g^{ab}$

Cet algorithme permet à Breizhman et Super-Breizh d'établir une clé commune $[p]$ : $k$ sans que personne ne soit capable de la connaître.

## 2) Méthode RSA [GOU].

Théorème du RSA Soient $p$ et $q$ 2 nombres premiers.
On pose $n = pq$. On a alors $\varphi(n) = (p-1)(q-1)$.
Si $e$ est un entier premier avec $\varphi(n)$ alors il existe $d$ tq $ed \equiv 1 [(p-1)(q-1)]$
On a alors $\forall a \in \mathbb{N}$ $a^{ed} \equiv a [n]$.

Protocole du RSA : • Bertrand choisit $p$ et $q$ tq. $p$ et $q$ calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$.
Il choisit $d$ et calcule $e$ tq $ed \equiv 1 [\varphi(n)]$.
• Bertrand rend publics $n$ et $e$ mais garde secret $\varphi(n)$ et $d$.
• Annabelle veut écrire un message codé par Bertrand $A \leq n$ et calcule $B = A^e [n]$ puis envoie $B$ à Bertrand.
• Bertrand veut décoder le message, il choisit $B^d [n]$ ce qui donne $A$ à Bertrand car $B^d \equiv A^{ed} [n]$ et $ed = 1 + k\varphi(n)$ donc $A^{ed} \equiv 1 [n]$ par Euler.

Rq: C'est le système de cryptage le plus utilisé
ex: Banque

Références: • Debaye "Merveilleux nombres premiers" [DEL]
• Wagschal "Arithmétique" [WAR]
• Tenenbaum "Les nombres premiers" [TEN]
• Gourdon Algèbre [GOU]
• Francinou "Oraux X-ENS" [FRA]
• Grandall, Pomerance "Prime Numbers" [GRA]
• Francinou, Gianella Algèbre 1 [FG 1]
• Demazure "Cours d'algèbre" [DEM].
• [RMS 118].

- Complexité
- Détailler Miller - Rabin