Nombres premiers. Applications.

121

Pour un entier n, $\mathrm{Div}(n)$ désigne l'ensemble des diviseurs positifs de n.

I - Résultats fondamentaux sur les nombres premiers

A - Notion de nombre premier, propriétés élémentaires

[R] 303 **Def 2** : On dit que $p \in \mathbb{N}$ est *premier* si $\mathrm{Div}(p) = \{1, p\}$
On dit que n est *composé* si $n \neq 0$ et si $\exists a \in \mathbb{N} \setminus \{1, n\} : a \mid n$.

$\mathcal{P}$ désignera l'ensemble des nombres premiers.

Lemme 3 (d'Euclide) : $\forall (a,b) \in \mathbb{N}^2, \forall p \in \mathcal{P}, \ p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$

[R] 303 **Lemme 5** : $\forall n \geq 2, \exists p \in \mathcal{P} : p \mid n$

[R] 304 **Prop 7** : Tout entier composé n admet un facteur premier entre 2 et $\sqrt{n}$.

[R] 306 **Thm 11** (fondamental de l'Arithmétique) :

$$\forall n \in \mathbb{N}^*, \ \exists ! (v_p(n))_{p \in \mathcal{P}} \in \mathbb{N}^{(\mathcal{P})} \ : \ n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Cette écriture est appelée "(la) décomposition en produit de facteurs premiers de n".

[R] 306 **Def 13** : Dans la décomposition en produit de facteurs premiers de n, l'entier $v_p(n)$ $(p \in \mathcal{P})$ est appelé valuation p-adique de n.

[R] 307 **Prop 17** : $\forall (a,b) \in (\mathbb{N}^*)^2, \quad a \mid b \Leftrightarrow \forall p \in \mathcal{P}, \ v_p(a) \leq v_p(b)$

[R] 319 **Prop 19** : $\forall (a,b) \in (\mathbb{N}^*)^2, \quad v_p(ab) = v_p(a) + v_p(b)$

[R] 307 **Prop 23** : $\forall (a,b) \in (\mathbb{N}^*)^2, \ \forall p \in \mathcal{P},$

$$v_p(a \vee b) = \max(v_p(a), v_p(b))$$
$$v_p(a \wedge b) = \min(v_p(a), v_p(b))$$

B - Répartition des nombres premiers

Thm 29 (Euclide) : Il existe une infinité de nombres premiers. [R] 305

Thm 31 (de la progression arithmétique, Dirichlet) [admis] : Pour tout $(a,b) \in (\mathbb{N}^*)^2$ tel que $a \wedge b = 1$, il existe une infinité de nombres premiers congrus à a modulo b.

Conj 37 (des nombres premiers jumeaux) : Il existe une infinité de nombres premiers p tels que $p+2$ est premier.

Prop 41 : Il existe des intervalles de longueur arbitrairement grande ne contenant aucun nombre premier.

Thm 43 (Bertrand) [admis] : Il existe toujours un nombre premier compris entre n importe quel entier naturel non nul et son double. [R] 325

Thm 47 (des nombres premiers) [admis] : $\#\mathcal{P} \cap [\![1, n]\!] \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$ [R] 308

II - Tests de primalité

Prop 53 (crible d'Ératosthène) : Le procédé suivant permet de trouver la liste croissante des nombres premiers : on part de la liste des entiers plus grands que 2. À chaque itération, on garde le plus petit nombre, et on supprime tous ses multiples.

Annexe : Crible d'Ératosthène : recherche de la liste des nombres premiers.

Prop 59 : n est premier si, et seulement si $\forall d \leq \lfloor \sqrt{n} \rfloor, \ d \nmid n$.
La complexité au pire de ce test est donc en $O(\sqrt{n})$.

Thm 61 (de Fermat) : Si p est premier, alors $\forall a \in \mathbb{N}, \ a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 \ [p]$

Rq 67[15] : On en déduit un test de non primalité.

[R] 329 Def 71[20] : Un nombre n composé satisfaisant le test du théorème de FERMAT est appelé *nombre de CARMICHAËL*.

[R] 329 Ex 73[21] : 561 est un nombre de Carmichaël.

[R] 330 Thm 79[24] (KORSELT) : n est un nombre de CARMICHAËL *si, et seulement si* pour tout diviseur premier p de n, $(p-1) \mid (n-1)$ et $p^2 \nmid n$.

[R] 326 Thm 83[23] (de WILSON) : n est premier $\iff (n-1)! \equiv -1 \ [n]$

C'est un test de primalité qui requiert $n-1$ multiplications dans $\mathbb{Z}/n\mathbb{Z}$.

III - Applications des nombres premiers

A - Fonctions spéciales

[R] 283 Def 89[21] : L'*indicatrice d'EULER* est :

$$\varphi : n \in \mathbb{N}^* \longmapsto \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{k \in [\![1,n]\!] \mid k \wedge n = 1\}$$

[R] 288 Prop 97[25] : ▸ $\forall (a,b) \in (\mathbb{N}^*)^2$, $a \wedge b = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$

▸ $\forall p \in \mathcal{P}$, $\forall \alpha \geq 1$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

[R] 288 Cor 101[26] : $\forall n \in \mathbb{N}^*$, $\varphi(n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \geq 1}} p^{v_p(n)-1}(p-1) = n \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \geq 1}} \left(1 - \frac{1}{p}\right)$

Def 103[28] : La *fonction ζ de RIEMANN* est définie par :

$$\zeta : \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 1\} \longrightarrow \mathbb{C}$$
$$s \longmapsto \sum_{n=0}^{+\infty} \frac{1}{n^s}$$

[KG] 461 Prop 107[29] : $\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$ (cette écriture est appelée "*produit eulérien*")

[KG] 461 [R] 343 Thm 109[29] : $\sum_{p \in \mathcal{P}} \frac{1}{p} = +\infty$

[R] 331 Def 113[30] : La *fonction de MOËBIUS* est définie par :

$$\mu : n \in \mathbb{N}^* \longmapsto \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \text{ si } n = p_1 \cdots p_r \text{ avec } p_1, \dots, p_r \text{ distincts} \\ 0 \text{ sinon} \end{cases}.$$

[R] 334 Thm 127[31] (CESÀRO) [admis] : La probabilité de choisir au hasard $r \geq 2$ entiers entre 1 et n qui sont premiers entre eux vaut $\frac{1}{\zeta(r)}$.

B - Algorithme de chiffrement RSA

[G] 54 Thm 131[39] (d'EULER) : $\forall (a,n) \in (\mathbb{N}^*)^2$, $a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \ [n]$

De la complexité des tests de primalité découle la grande difficulté de la recherche de la décomposition en produit de facteurs premiers d'un entier donné. Ce principe est à la base de la sécurité de l'algorithme de chiffrement RSA, détaillé ci-dessous.

Alice veut envoyer à Bob un message représenté par un nombre entier m, en toute sécurité.

- Bob choisit en secret deux nombres premiers distincts p et q et calcule leur produit $n = pq$.
- Il choisit ensuite un entier $c < \varphi(n) = (p-1)(q-1)$ premier à $\varphi(n)$.
- Il trouve ensuite un entier d tel que $cd \equiv 1 \ [\varphi(n)]$
- La clé publique de Bob est (n,c), qu'il donne à Alice, et sa clé privée est (n,d), qu'il garde secrète.
- Alice envoie à Bob le message $m^c \bmod n$
- Pour décoder le message, Bob calcule $(m^c)^d \equiv m \ [n]$.

C- Corps finis

[R] 415 **Def 137**[33] : La caractéristique d'un anneau A est l'unique générateur positif du noyau du morphisme $\varphi : \mathbb{Z} \to A$, $n \mapsto n 1_A$.

[R] 415 **Lemme 139**[34] : La caractéristique d'un corps est nulle ou première.

Ex 149[35] : $\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p.

[R] 421 **Thm 151**[36] : Il existe un corps fini de cardinal q si, et seulement si q est une puissance d'un nombre premier. Le cas échéant, un tel corps est unique à isomorphisme près, et on note $\mathbb{F}_q$ le corps fini à q éléments. Par ailleurs, $p = \mathrm{car}(\mathbb{F}_q)$ est un nombre premier, et q est une puissance de p.

D- Le théorème des deux carrés de Fermat

[P] 75 **Lemme 157**[37] : -1 est un carré dans $\mathbb{F}_p$ si, et seulement si $p \equiv 1\ [4]$

[P] 56 **Thm 163**[38] (des deux carrés de FERMAT) : Soit $E = \{n \in \mathbb{N}^* \mid \exists (a,b) \in \mathbb{N}^2 : n = a^2 + b^2\}$.

$n \in E \iff \forall p \in \mathcal{P},\ p \equiv 3\ [4] \Rightarrow v_p(n)$ pair **DEV 1**

E- En théorie des groupes

[R] 22 **Def 167**[43] : Un p-groupe est un groupe de cardinal une puissance de p.

[R] 22 **Prop 173**[40] : Si un p-groupe G agit sur un ensemble fini X, alors $\#X \equiv \#X^G\ [p]$ où X^G est l'ensemble des éléments de X fixes par l'action de G.

[R] 23 **Cor 179**[41] : Le centre d'un p-groupe n'est pas trivial.

[U] 85 **Def 181**[42] : Soit G un groupe fini de cardinal $p^\alpha m$, $m \wedge p = 1$. Un p-Sylow de G est un sous-p-groupe de G de cardinal p^α.

[U] 87 **Thm 191**[43] (de Sylow) [admis] : Soit G un groupe fini.

1. G admet un p-Sylow. On note n_p son nombre de p-Sylow.
2. G agit transitivement par conjugaison sur l'ensemble de ses p-Sylow.
3. $n_p \equiv 1\ [p]$

Prop 193[44] : Si $p \geq 3$, alors pour tout $\alpha \geq 1$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique **DEV 2** [R] 282

Prop 197[45] : Tout groupe d'ordre p^2 est abélien. [R] 23

RÉFÉRENCES :

[R] : Mathématiques pour l'agrégation - Algèbre et géométrie (Jean-Étienne Rombaldi) [3e édition]

[P] : Cours d'algèbre (Daniel Perrin)

[U] : Théorie des groupes (Félix Ulmer)

[KG] : De l'intégration aux probabilités (Olivier Garet, Aline Kurtzmann) [2e édition augmentée]

Crible d'Ératosthène