121 : Nombres premiers. Applications.

Juliette Veuillez & Antoine Dequay

21 septembre 2022

Notes

— Prof : Lionel Fourquaux.

— Références :

  — Gourdon, *Algèbre & Analyse*,

  — Perrin,

  — Serre,

  — Isenmann,

  — Saux Picart-Rannou, *Cours de calcul formel, tome 2*,

  — Ulmer,

  — (X-ENS, *Analyse 1*).

— Références des développements :

  — X-ENS, *Algèbre 1* pour Dirichlet faible,

  — Isenmann pour le théorème des 2 carrés,

  — Saux Picart-Rannou pour les nombres de Mersenne.

1 Généralités

1.1 Premières définitions

Définition 1 *Nombre premier.* Un entier naturel $p \geq 2$ est un nombre premier si ses seuls diviseurs sont 1, -1, p et $-p$. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Exemple 2 Les nombres premiers inférieurs à 50 sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

Remarque 3 1 n'est pas définit premier, pour permettre l'unicité dans la décomposition en nombres premiers.

Définition 4 *PGCD.* Soient $a_1, \ldots, a_n$ des entiers.

- Il existe un unique entier naturel d tel que $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$. L'entier d est le PGCD $a_1, \ldots, a_n$, et est noté $d = \text{PGCD}(a_1, \ldots, a_n)$. C'est aussi le plus grand entier naturel divisant tous les $(a_i)_{1 \leq i \leq n}$.
- Lorsque $\text{PGCD}(a_1, \ldots, a_n) = 1$, on dit que les entiers $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble.

Lemme 5 (d'Euclide) Soient b et c deux entiers. Si un nombre premier p divise le produit bc, alors p divise b ou c.

Remarque 6 L'algorithme d'Euclide permet de calculer le PGCD de deux entiers.

Application 7 Soit $p \in \mathcal{P}$ et soit $k \in [\![1, p-1]\!]$. Alors $p \left| \binom{p}{k} \right.$.

Exemple 8 Soient $(x, y) \in \mathbb{Z}^2$ et $p \in \mathcal{P}$. Alors $(x+y)^p \equiv x^p + y^p \ (mod\ p)$.

1.2 Décomposition

Théorème 9 Théorème fondamental de l'arithmétique. Tout entier relatif $n \in \mathbb{Z}^*$ s'écrit de manière unique à l'ordre des facteurs près sous la forme :

$$n = \varepsilon \prod_{p \in \mathcal{P}} p^{\alpha_p},$$

où les α_p sont des entiers naturels et $\varepsilon = \pm 1$.

Remarque 10 Ce théorème affirme que $\mathbb{Z}$ est factoriel.

Proposition 11 Soient $n = \varepsilon_n \prod_{p \in \mathcal{P}} p^{\alpha_p}$ et $m = \varepsilon_m \prod_{p \in \mathcal{P}} p^{\beta_p}$ deux entiers naturels. Alors :

$$\text{PGCD}(n, m) = \prod_{p \in \mathcal{P}} p^{\gamma_p} \text{ où } \gamma_p = \min(\alpha_p, \beta_p) \text{ pour } p \in \mathcal{P}.$$

1.3 Fonctions arithmétiques

Définition 12 *Indicatrice d'*Euler. Si $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers inférieurs à n qui sont premiers avec n.

Proposition 13

— Si $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

— Si $(n,m) \in (\mathbb{N}^*)^2$ sont premiers entre eux, on a $\varphi(nm) = \varphi(n)\varphi(m)$.

Proposition 14 Pour tout $n \in \mathbb{N}\backslash\{0,1\}$, on a $n = \sum_{d|n} \varphi(d)$.

Définition 15 *Fonction de* Moëbius. On définit la fonction $\mu : \mathbb{N}^* \to \{0,1,-1\}$ par :

— $\mu(1) = 1$;

— $\mu(n) = 0$ si n contient un facteur carré ;

— $\mu\left(\prod_{i=1}^{r} p_i\right) = (-1)^r$ si $p_1, \dots, p_r$ sont des nombres premiers distincts.

Proposition 16 Si $(n,m) \in (\mathbb{N}^*)^2$ sont premiers entre eux, on a $\mu(nm) = \mu(n)\mu(m)$.

Proposition 17

— Pour tout $n \in \mathbb{N}^*$, on a $\sum_{d|n} \mu(d) = 0$.

— Soit $f : \mathbb{N}^* \to A$ où A est un groupe abélien noté additivement. On pose $g(n) = \sum_{d|n} f(d)$ pour $n \in \mathbb{N}^*$. On a alors la *formule d'inversion de* Moëbius :

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Corollaire 18 Pour $n \in \mathbb{N}^*$, on a $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$.

Application 19 *Polynômes cyclotomiques.*

Soit $n \in \mathbb{N}^*$. On définit le $n^{\text{ème}}$ polynôme cyclotomique par $\phi_n(X) = \prod_{\text{PGCD}(k,n)=1} (X - e^{2ik\pi/n})$.

— Le polynôme ϕ_n est unitaire, de degré $\varphi(n)$, dans $\mathbb{Z}[X]$ et irréductible sur $\mathbb{Z}$.

— On a $X^n - 1 = \prod_{d|n} \phi_d(X)$.

— On a $\phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}$.

1.4 Répartition

Proposition 20 L'ensemble $\mathcal{P}$ est infini.

Théorème 21 (Dirichlet faible). Pour tout $n \in \mathbb{N}^*$, il existe un infinité de nombres premiers congrus à 1 modulo n.

[DEV Juliette].

Théorème 22 (Dirichlet fort, admis). Pour tout $n \in \mathbb{N}^*$ et $k \in [\![1, n-1]\!]$, il existe une infinité de nombres premiers congrus à k modulo n.

Définition 23 *Fonction ζ de* Riemann. Si $s \in \mathbb{C}$ est tel que $Re(s) > 1$, on définit $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$.

Proposition 24 La fonction ζ se prolonge en une fonction méromorphe sur tout le plan complexe, avec un unique pôle en 1.

Proposition 25 Si $k \in \mathbb{N}^*$, on note p_k le $k^{\text{ème}}$ nombre premier. On a alors, pour tout $s \in \mathbb{C}$ tel que $Re(s) > 1$: $\zeta(s) = \prod_{k=0}^{+\infty} \frac{1}{1 - p_k^{-s}}$.

Application 26 La série $\sum_{p \in \mathcal{P}} \frac{1}{p}$ diverge.

Théorème 27 (Théorème des nombres premiers, admis). Soit $x > 1$. On note $\pi(x)$ le nombre de nombres premiers inférieurs à x. Alors on a l'équivalent $\pi(x) \underset{x \to +\infty}{\sim} \frac{x}{\ln(x)}$.

Remarque 28 En fait, on peut même montrer que $\pi(x) \sim \int_2^x \frac{\mathrm{dx}}{\ln(x)}$, c'est à dire que la proportion de nombres premiers au voisinage de $x > 1$ est de l'ordre de $\frac{1}{\ln(x)}$.

Conjecture 29 (de Goldbach). Tout nombre entier pair supérieur à 3 peut s'écrire comme la somme de deux nombres premiers.

Conjecture 30 Un couple $(n, n+2)$ est dit couple de nombres premiers jumeaux si $(n, n+2) \in \mathcal{P}^2$.

Il existe une infinité de nombres premiers jumeaux.

2 Application aux corps finis

2.1 $\mathbb{Z}/p\mathbb{Z}$ et premières propriétés

Proposition 31 Un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si il est premier avec n. Dans ce cas, son inverse peut être calculée grâce à la relation de Bézout les reliant.

Corollaire 32 L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Théorème 33 Si $n \in \mathbb{N}^*$, on a $\#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$.

Théorème 34 (de Fermat). Soit $p \geq 2$ un nombre premier. Alors :

$$\forall a \in \mathbb{Z}, a^p \equiv a \ (mod\ p).$$

Application 35 (de Wilson). Un entier $p \geq 2$ est un nombre premier si et seulement si $(p-1)! \equiv -1 \ (mod\ p)$.

2.2 Polynômes irréductibles

Proposition 36 Critère d'Eisenstein. Soit $n \in \mathbb{N}^*$ et $P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. On suppose :

— $p \nmid a_n$;
— $\forall i \in [\![0, n-1]\!], p | a_i$;
— $p^2 \nmid a_0$.

Alors P est irréductible sur $\mathbb{Q}$. Il est aussi irréductible sur $\mathbb{Z}$ si l'on a $\text{PGCD}(a_i) = 1$.

Proposition 37 Critère d'irréductibilité modulo p. Soit $n \in \mathbb{N}$, $p \in \mathcal{P}$ et $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de $\mathbb{Z}[X]$. On note $\overline{P}$ sa réduction modulo p et on suppose $a_n \not\equiv 0 \ (mod\ p)$. Si $\overline{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$, et sur $\mathbb{Z}$ si $\text{PGCD}(a_i) = 1$.

Contre-exemple 38 Le polynômes $X^4 + 1$ est irréductible sur $\mathbb{Z}$, mais est réductible sur $\mathbb{F}_p$ pour tout nombre premier p.

2.3 Carrés dans $\mathbb{F}_p$

Dans cette partie, on se donne $p \in \mathcal{P}$.

Proposition 39 On note $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{*2} = \{x^2, x \in \mathbb{F}_q^*\}$. Alors on a :
— pour $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$;
— pour $p > 2$, $|\mathbb{F}_q^2| = \dfrac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \dfrac{q-1}{2}$

Á partir de maintenant, on suppose $p > 2$.

Définition 40 *Symbole de* Legendre. Si $x \in \mathbb{F}_p$, on définit le symbole de Legendre $\left(\dfrac{x}{p}\right)$ par :

$$\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } x \notin \mathbb{F}_p^*, \\ 1 \text{ si } x \in \mathbb{F}_p^{*2}, \\ -1 \text{ si } x \notin \mathbb{F}_p^{*2}. \end{cases}$$

Proposition 41 Soit $x \in \mathbb{F}_p$. On a $\left(\dfrac{x}{p}\right) = x^{\frac{p-1}{2}}$.

Proposition 42 On a les formules suivantes :
— Si $x, y \in \mathbb{F}_p$, on a $\left(\dfrac{xy}{p}\right) = \left(\dfrac{x}{p}\right)\left(\dfrac{y}{p}\right)$;
— $\left(\dfrac{1}{p}\right) = 1$;
— $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;
— $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Corollaire 43 -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \ (mod\ 4)$ ou $p = 2$.

Théorème 44 Loi de réciprocité quadratique. Soient $l, p > 2$ deux nombres premiers distincts. On a :

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\frac{(p-1)(l-1)}{4}}.$$

Exemple 45 On a :

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

On a donc montré que 29 n'est pas un carré modulo 43.

Théorème 46 Soit $n \in \mathbb{N}^*$. Alors n est somme de 2 carrés si et seulement si $v_p(n)$ est pair pour tout $p \in \mathcal{P}$ tel que $p \equiv 3 \ (mod\ 4)$.

[DEV Commun].

3 p-groupes et théorème de Sylow

Dans cette partie, on se donne $p \in \mathcal{P}$.

Définition 47 *p-groupe.* Un p-groupe est un groupe dont le cardinal est une puissance de p.

Exemple 48 Le groupe des quaternions $\mathcal{Q}_8$ et le groupe diédral D_4 sont des 2-groupes d'ordre 8.

Proposition 49 Tout groupe d'ordre p^2 est abélien.

Définition 50 *p-sous-groupe de Sylow.* Soit G un groupe fini de cardinal $n \in \mathbb{N}^*$ divisible par p. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-sous-groupe de Sylow de G un sous-groupe de G d'ordre p^α

Exemple 51 Si $n \in \mathbb{N}^*$, le groupe $G = Gl_n(\mathbb{F}_p)$ est un groupe fini de cardinal $|G| = mp^{\frac{n(n-1)}{2}}$ avec $p \nmid m$. L'ensemble des matrices triangulaires supérieures strictes est un p-sous-groupe de Sylow de G.

Théorème 52 (Théorèmes de Sylow) Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$.

1. Soit H est un sous-groupe de G qui est un p-groupe. Il existe un p-Sylow S, avec $H \subset S$.
2. Les p-Sylow sont tous conjugués.
3. Si on note k_p le nombre de p-Sylows de G, on a $k_p | m$ et $k_p \equiv 1 \ (mod\ p)$.

Corollaire 53 Soit G un groupe. Si S est un p-Sylow de G, on a les équivalences :

$$S \triangleleft G \iff S \text{ est l'unique } p\text{-Sylow de } G \iff k_p = 1.$$

Application 54 Un groupe d'ordre 63 n'est pas simple.

4 Les nombres premiers en pratique

Proposition 55 On donne l'algorithme du crible d'Eratosthène, qui, pour un $L \in \mathbb{N}$ donné, permet d'énumérer tous les premiers plus petits que L : Dessin

```
1 def Eratosthene(L):
2     t = [True]*L
3     t[1] = False
4     i = 2
```

```
    while i*i <= L:
        if t[i]:
            for j in range(i*i, L, i):
                t[j] = False
        i += 1
    return t
```

Définition 56 *Nombre de* Carmichaël. Un entier n est dit de Carmichaël s'il n'est pas premier et si, pour tout $b \in \mathbb{N}$ premier avec n, $b^{n-1} \equiv 1 \ (mod\ n)$.

Exemple 57 Le nombre 561 est le plus petit entier de Carmichaël.

Théorème 58 (Critère de Korselt). Soit $n \in \mathbb{N}$ et $\prod_{k=0}^{u} p_i^{\alpha_i}$, $u > 0$ sa décomposition en facteurs premiers. Alors n est un entier de Carmichaël si et seulement si pour tout $i \in [\![0, u]\!]$, $p_i - 1 | n - 1$ et $\alpha_i = 1$.

Proposition 59 Si un nombre $2^n + 1$ est premier pour un certain $n \in \mathbb{N}$, alors n est une puissance de 2.

Définition 60 *Nombre de* Fermat. Pour $n \in \mathbb{N}$, on appelle $n^{\text{ème}}$ nombre de Fermat le nombre :

$$F_n := 2^{2^n} + 1.$$

Exemple 61 $F_2 = 17$ est premier, mais Euler a prouvé que F_5 n'est pas premier.

Test 62 On a le test de Pépin : pour $n \in \mathbb{N}$, on a l'équivalence :

$$F_n \in \mathcal{P} \iff 3^{(F_n-1)/2} \equiv -1 \ (mod\ F_n).$$

Définition 63 *Nombre de* Mersenne. Pour $q \in \mathbb{N}$, on appelle $q^{\text{ème}}$ nombre de Mersenne le nombre :

$$M_q := 2^q - 1.$$

Remarque 64 Si $q \in \mathbb{N}$ n'est pas premier, M_q n'est pas premier.

Théorème 65 Pour tout nombre premier impair q, on a :

$$M_q \in \mathcal{P} \iff \left(2 + \sqrt{3}\right)^{2^{q-1}} \equiv -1 \ (mod\ M_q).$$

[DEV Antoine].

Exemple 66 $M_3 = 2^3 - 1 = 7$ est premier, mais pas $M_{11} = 2047 = 23 \times 89$ (c'est le plus petit contre-exemple à la non-primalité des nombres de Mersenne).

Test 67 On a le test de Lehmer-Lucas : pour $q \in \mathcal{P}$, $q \neq 2$, on définit la suite de Lucas $(L_n)_{n\in\mathbb{N}} \in (\mathbb{Z}/M_q\mathbb{Z})$ par :

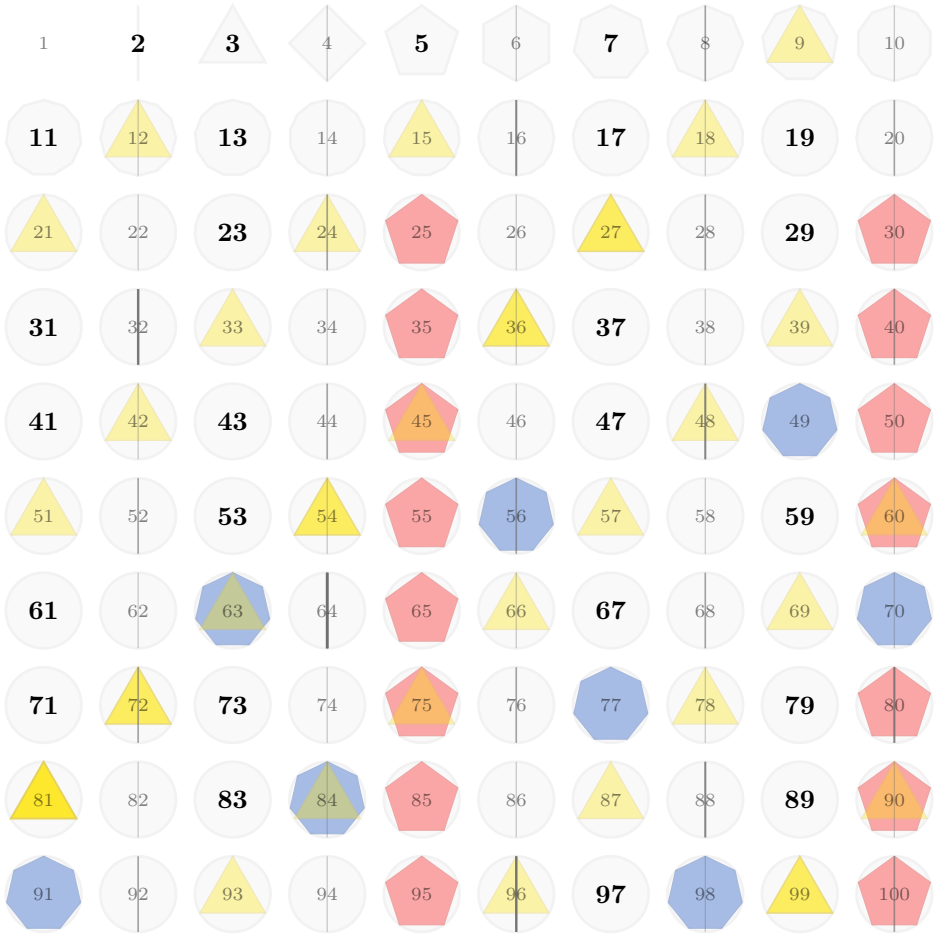
$$\begin{cases} L_{n+1} \equiv L_n^2 - 2 \ (mod\ M_q) \text{ si } n \in \mathbb{N}, \\ L_0 = 4. \end{cases}$$

On a alors l'équivalence :

$$M_q \in \mathcal{P} \iff L_{q-2} \equiv 0 \ (mod\ M_q).$$

Annexe

Proposition 55



Juste pour la beauté de Tikz, voici une autre version du crible, où l'on ne commence pas à barrer à i^2 mais à $2i$ (version absente du vrai plan...) :