121 Nombres premiers. Applications.

Refs : [Gou1] Gourdon Algèbre. [FGN1] Francinou X-ens Algèbre 1. [Perr] Perrin Algèbre. [Serre] Serre Cours d'Arithmétique. [Ulm] Ulmer. Théorie des groupes. [Dem] Demazure. Cours d'algèbre.

Devts :
26 Dirichlet faible
43 Réciprocité quadratique
45 Deux carrés.

Cadre, on note $\mathbb{P}$ l'ensemble des nombres premiers positifs. Par défaut p désigne un élément de $\mathbb{P}$.

I. Généralités sur les nombres premiers.

1) Définition, nombres premiers entre eux

[Gou1] 7,8,9

Def 1 : Un nombre $p \in \mathbb{Z}$ est dit premier si il admet exactement quatre diviseurs : $\{\pm 1, \pm p\}$.

Ex 2 : 2 est premier, 1 n'est pas premier, 0 non plus.

Théo 3 : Tout entier naturel $n \geq 2$ s'écrit de manière unique (à réordonnement des facteurs près) comme un produit
$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$
où $p_i \in \mathbb{P}$, $\alpha_i \in \mathbb{N}^*$ et les p_i sont distincts deux à deux.
On appelle cette décomposition la décomposition de n en produit de facteurs premiers.

Ex 4 : $60 = 2^2 \times 3 \times 5$

Prop 5 : L'ensemble $\mathbb{P}$ est infini.

Prop 6 : Si p divise un produit d'entiers alors p divise au moins un des facteurs de ce produit.

Ex 7 Ceci est faux si p n'est pas premier : $6 \mid 12 = 3 \times 4$ sans diviser aucun des facteurs.

Def 8 : Soient $n_1 \dots n_k$ des entiers, ils sont dits premiers entre eux dans leur ensemble si $\mathrm{pgcd}(n_1 \dots n_k) = 1$ et premiers entre eux deux à deux si $\mathrm{pgcd}(n_i, n_j) = 1$ $\forall i, j \in [\![1, k]\!]$.

Théo 9 : Des entiers $n_1, \dots, n_k$ sont premiers entre eux dans leur ensemble si et seulement si il existe $u_1 \dots u_k \in \mathbb{Z}$ tels que
$$\sum_{i=1}^{k} u_i n_i = 1$$

Rq 10 Dans le cas $k=2$, l'algorithme d'Euclide permet un calcul pratique d'un couple (u_1, u_2).
Les $u_1 \dots u_k$ ne sont pas uniques a priori.

[Gou1] 8,9

Théo 11 Soient $a, b, c \in \mathbb{Z}$ avec $a \mid bc$, si a et b sont premiers entre eux. Alors a divise c.

Appli 12 $\sqrt{2}$ n'est pas rationnel. Plus généralement, pour $n \in \mathbb{N}$ $\sqrt{n}$ est entier ou irrationnel.

Appli 13 Soit $k \in [\![1, p-1]\!]$, alors p divise $\binom{p}{k}$.

Prop 14 Deux entiers sont premiers entre eux si et seulement si leurs diviseurs premiers forment des ensembles disjoints.

2) Fonctions arithmétiques

[FGN1] 150

Def 15 On appelle fonction arithmétique toute application $f : \mathbb{N}^* \to \mathbb{C}$. Une telle application sera dite totalement multiplicative (resp multiplicative) si $f(nm) = f(n)f(m)$ $\forall n, m \in \mathbb{N}$ (resp $\forall n, m \in \mathbb{N}$ premiers entre eux).

[Gou1] 31,32

Def 16 : Soit $n \in \mathbb{N}$, $n > 1$, on appelle indicatrice d'Euler de n le nombre $\varphi(n) = \#(\{k \in [\![0, n-1]\!] \mid k \wedge n = 1\})$
(c'est aussi le cardinal des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$).

Prop 17 La fonction φ est multiplicative (avec la convention $\varphi(1) = 1$)

Prop 18 : Pour $\alpha \geq 1$, on a $\varphi(p^\alpha) = p^\alpha - p^{\alpha - 1}$, ce qui permet de calculer φ sur tout entier.

Ex 19 : $\varphi(60) = \varphi(2^2)\varphi(3)\varphi(5) = 2 \times 2 \times 4 = 16$.

Prop 20 : Pour $n \geq 2$, on a $n = \sum_{d \mid n} \varphi(d)$.

[Perr] 89,92

Def 21 : On définit $\mu : \mathbb{N}^* \to \{0, \pm 1\}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n contient un facteur carré. $\mu(p_1 \dots p_r) = (-1)^r$ si $p_1 \dots p_r$ sont des nombres premiers distincts. On appelle μ la fonction de Möbius.

Prop 22 : La fonction de Möbius est multiplicative. Pour $n > 1$, on a $0 = \sum_{d \mid n} \mu(d)$.

Théo 23 (Inversion de Möbius) Soit f une fonction arithmétique, on pose $g(n) = \sum_{d \mid n} f(d)$. On a $\forall n \in \mathbb{N}^*$, $f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$.
En particulier $\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$.

Appli 24 : Pour $n \in \mathbb{N}^*$, on a
$$\Phi_n(X) = \prod_{d \mid n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}$$
(en particulier Φ_n est à coefficients dans $\mathbb{Z}$)

3) Répartition des nombres premiers.

[FGN1] 158 159

Lemme 25 Soit $m\in\mathbb{N}$, $a\in\mathbb{Z}$, $p\in\mathbb{P}$ tel que $p\mid\Phi_m(a)$ et $p\nmid\Phi_d(a)$ pour $d\mid m$ et $d<m$. Alors p est congru à 1 modulo m.

Théo 26 (Dirichlet faible) Il existe, pour tout n dans $\mathbb{N}^*$, une infinité de nombres premiers congrus à 1 modulo n. DVP

Ce dernier résultat peut être largement renforcé :

Théo 27 (Dirichlet) Soient a, b premiers entre eux. Il existe une infinité de nombres premiers congrus à a modulo b.

Théo 28 (des nombres premiers) On pose $\pi(n)=\#(\mathbb{P}\cap[\![1,n]\!])$. On a, quand n tend vers $+\infty$ que $\pi(n)\sim\frac{n}{\ln n}$.

Rq 29 : Ce résultat peut être raffiné grâce à la connaissance des zéros de la fonction ζ de Riemann.

[Serre] 115

Prop 30 (Produit Eulérien) $\forall s\in\mathbb{C}/Re(s)>1$ $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\in\mathbb{P}}\frac{1}{1-\frac{1}{p^s}}$

II. Corps finis.

1) Anneaux $\mathbb{Z}/n\mathbb{Z}$.

[Cou1] 9,31

Prop-déf 31 Soit $m\in\mathbb{N}^*$, l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier, on note $\mathbb{F}_n$ le corps ainsi obtenu.

Théo 32 (Fermat). Soit $p\in\mathbb{P}$. Alors

$\forall a\in\mathbb{Z},\ a^p\equiv a[p]$ $\quad\forall a\in\mathbb{Z}/a\wedge p=1,\ a^{p-1}\equiv 1[p]$

[FGN1] 167

Appl 33 (Sophie Germain) Soit $p\in\mathbb{P}$ impair avec $2p+1\in\mathbb{P}$. Alors $\forall(x,y,z)\in\mathbb{Z}^3$ tel que $x^p+y^p+z^p=0$, on a $xyz\equiv 0[p]$.

2) Théorie élémentaire des corps finis

[Perr] 72

Déf 34 : Soit k un corps, $\Psi:\mathbb{Z}\to k$ l'unique morphisme d'anneaux non trivial. On appelle caractéristique de k le générateur positif de $\ker\Psi$ comme idéal de $\mathbb{Z}$. On note car(k) cet entier.

Prop 35 : La caractéristique est soit nulle (auquel cas k est infini) soit un nombre premier. Fixons p la caractéristique de k, fini.

Prop 36 : k contient un sous corps isomorphe à $\mathbb{F}_p$. Son cardinal est donc une puissance de p (il est muni naturellement d'une structure de $\mathbb{F}_p$-ev de dimension finie).

[Perr] 73-74

Prop 37 : L'application $F_p: k\to k$ envoyant x sur x^p est un morphisme de corps dit morphisme de Frobenius. Il s'agit d'un automorphisme si k est fini, et de l'identité si $k=\mathbb{F}_p$.

Théo 34 : Soit $p\in\mathbb{P}$ et $n\geq 1$, on pose $q=p^n$. Il existe un unique (à isomorphisme près) corps de cardinal q. Défini comme corps de décomposition du polynôme X^q-X sur $\mathbb{F}_p$. On note ce corps $\mathbb{F}_q$.

Ex 35 Il n'y a pas de corps de cardinal 60.

Rq 36 : On n'a pas $(\mathbb{F}_q,+)\simeq\mathbb{Z}/q\mathbb{Z}$, mais $(\mathbb{F}_q,+)\simeq(\mathbb{Z}/p\mathbb{Z})^n$.

Théo 38 : Tout sous groupe fini de $(k^*,\times)$ où k est un corps quelconque, est cyclique. En particulier, $\mathbb{Z}/(q-1)\mathbb{Z}\simeq\mathbb{F}_q^*$.

3) Carrés dans $\mathbb{F}_q$.

On fixe $p\in\mathbb{P}$ et $q=p^n$ pour un $n\geq 1$.

[Perr] 74-75

Déf 39 On pose $\mathbb{F}_q^2:=\{x\in\mathbb{F}_q\mid\exists y\in\mathbb{F}_q,\ y^2=x\}$ et $\mathbb{F}_q^{*2}=\mathbb{F}_q^*\cap\mathbb{F}_q^2$.

Prop 40 Si $p=2$, on a $\mathbb{F}_q^2=\mathbb{F}_q$. Si $p>2$, on a $x\in\mathbb{F}_q^{*2}\Leftrightarrow x^{\frac{q-1}{2}}=1$. Plus précisément, $\mathbb{F}_q^{*2}$ s'écrit comme le noyau du morphisme $\mathbb{F}_q^*\to\mathbb{F}_q^*$ envoyant x sur $x^{\frac{q-1}{2}}$.

On a alors $|\mathbb{F}_q^{*2}|=\frac{q-1}{2}$ et $|\mathbb{F}_q^2|=\frac{q+1}{2}$.

[Serre] 16-18

On fixe pour cette sous partie $p\geq 3$.

Déf 41 : Soit $x\in\mathbb{F}_p$. On appelle symbole de Legendre de x, noté $\left(\frac{x}{p}\right)$, l'entier

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

Cette définition s'étend naturellement à $x\in\mathbb{Z}$ par $\left(\frac{x}{p}\right):=\left(\frac{\bar{x}}{p}\right)$.

+ multiplicativité

Prop 42 : On a les formules

$\left(\frac{1}{p}\right)=1$ $\quad\left(\frac{-1}{p}\right)=(-1)^{\varepsilon(p)}$ $\quad\left(\frac{2}{p}\right)=(-1)^{\omega(p)}$ (preuve 2e forme du Serre).

avec $\varepsilon(p)=\frac{p-1}{2}[2]$ $\quad\omega(p)=\frac{p^2-1}{8}[2]$.

Théo 43 (Réciprocité quadratique) Soient p et q deux nombres premiers distincts. Alors $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$. DVP

Rq 44 : Les deux résultats précédents permettent de calculer $\left(\frac{p}{q}\right)$ pour $p,q\in\mathbb{P}$:

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

L'équation $x^2+43y=29$ n'a pas de solutions.

DVP

[Perr] 57 Appli 45 (Deux carrés). $p \in \mathbb{P}$ est somme de deux carrés si et seulement si $p=2$ ou $p \equiv 1[4]$.

4) Application à la réduction des polynômes modulo p.

[Perr] 76.77. Théo 46 (Critère d'Eisenstein) Soit $P(X)=\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Et $p \in \mathbb{P}$ tel que $p \nmid a_n$, p divise a_i pour $i<n$ et $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Q}[X]$. C'est donc dans $\mathbb{Z}[X]$ si $\mathrm{pgcd}(a_1 ... a_n)=1$).

Théo 47 Soit $P(X)=\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $\bar{P}$ sa réduction sur $\mathbb{F}_p$, avec $a_n \not\equiv 0[p]$. Alors si $\bar{P}$ est irréductible sur $\mathbb{F}_p$, P est irréductible sur $\mathbb{Q}$.

Ex 48 : Attention, P peut être réductible sur $\mathbb{Z}$ si son contenu est non trivial.

Ex 49 : $P(X)=X^3+462X^2+2433X-67691$. $\bar{P}=X^3+X+1$ sur $\mathbb{F}_2$, irréductible.

Rq 50. La réciproque est fausse : X^4+1 est irréductible sur $\mathbb{Q}$, mais jamais sur $\mathbb{F}_p$.

III Théorie des groupes.

1) Notions de p-groupes. Fixons $p \in \mathbb{P}$

[Ulm] Def 51 : Un groupe fini est appelé p groupe si son ordre est une puissance non triviale de p.

Ex 52 : $(\mathbb{Z}/2\mathbb{Z})^3$ et Q_8 sont des 2-groupes.

Prop 53 : Le centre d'un p groupe est non trivial.

Cor 54 : Tout groupe d'ordre p ou p^2 est abélien.

Cor 55 Tout p-groupe est résoluble.

2) Théorèmes de Sylow. On fixe G groupe d'ordre mp^{α} $\alpha \geq 1$, $p \nmid m$.

[Perr] 18. Def 52 On appelle p-sous groupe de Sylow de G (ou p-Sylow) tout sous groupe de G d'ordre p^{α}. On note $Syl_p(G)$ l'ensemble des p-Sylow de G.

Théo 53 (Sylow) On a $Syl_p(G) \neq \emptyset$. Pour $S \in Syl_p(G)$ et $H \leq G$ un p-groupe, il existe $a \in G$ tel que $H \leq aSa^{-1}$. Et $|Syl_p(G)| \mid m$ et $|Syl_p(G)| \equiv 1[p]$.

Cor 54 : Si $|Syl_p(G)|=1$, alors G n'est pas simple (c'est équivalent à $S \trianglelefteq G$ pour $S \in Syl_p(G)$).

Appl 55 : Un groupe d'ordre 63 n'est pas simple. Un groupe d'ordre 15 est cyclique.

IV Primalité en pratique.

1) Test de primalité. Algorithmes élémentaires.

Algo 56 : $n \in \mathbb{N}^*$ est premier si et seulement si il n'admet aucun diviseur inférieur à $\sqrt{n}$ (belle réduction, mais impraticable pour n grand).

Algo 56 (Eratosthène) Pour N fixé on veut trouver $[\![1,N]\!] \cap \mathbb{P}$. On pose $P_1=[\![2,N]\!]$ et $P_2=\emptyset$.

Tant que $P_1 \neq \emptyset$ faire $P_2 \leftarrow P_2 \cup \{\min P_1\}$; $P_1 \leftarrow P_1 \setminus (\min P_1)\mathbb{N}^*$; Fin

P_2 est alors le résultat voulu.

Cet algorithme a l'avantage de donner tous les nombres premiers inférieurs à N contrairement au premier.

Prop 57 : (Critère de Lehmer) Soit $n>1$ impair. Alors n est premier si et seulement si $\exists a \in \mathbb{N} \mid a^{n-1} \equiv 1[n]$ et ($\forall q$ facteur premier de $n-1$). $a^{\frac{n-1}{q}} \not\equiv 1[n]$)

Ex 58 : $n=7$ et $a=3$.

2) Une application en cryptographie : Le chiffrement RSA

[Gou] 34.35 Etant donnés $p, q \in \mathbb{P}$ distincts et $n=pq$, c et d deux entiers tels que $cd \equiv 1[\varphi(n)]$. Alors pour $t \in \mathbb{Z}$, on a $t^{cd} \equiv t[n]$. L'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ donnée par $t \mapsto t^c$ est la fonction de chiffrement, et $T \mapsto T^d$ celle de déchiffrement. Le couple (n,c) forme une "clef publique", permettant à tous le chiffrement d'un message, que seule la connaissance de d permet de décoder. La fiabilité de ce système repose sur la difficulté à trouver p, q (donc $\varphi(n)$) pour n grands (plusieurs centaines de décimales).

3) Deux classes de nombres remarquables.

[Dema] 75-77. Nombres de Fermat On pose $F_n=2^{2^n}+1$. Les nombres F_n ne sont pas tous premiers : F_5 est le plus petit non premier.

Lemme 59 (Pépin) F_n est premier si et seulement si $3^{2^{2^n-1}} \equiv 1[F_n]$.

Rq 60 Critère encore valable pour 5 ou 7 au lieu de 3.

Nombres de Mersenne :

Entier de la forme 2^n-1. Comme $2^a-1 \mid 2^{ab}-1$, 2^n-1 est premier entraîne n premier. Mais la réciproque est fausse : $2^{11}-1=2047=23 \times 89$ n'est pas premier.