1

121

Nombres premiers. Applications.

I- Généralités

1) Premières définitions

Def 1: Soit $p\in\mathbb{N}\setminus\{0,1\}$, p est dit premier si ses seuls diviseurs sont $1, -1, p$ et $-p$. On note $\mathcal{P}$ l'ensemble des nombres premiers.

Ex 2: 2, 3, 5, 7, 11, 13, 17, 19 sont les nombres premiers inférieurs à 20.

Rq 3: 1 n'est pas défini premier pour permettre l'unicité dans la décomposition en facteurs premiers.

Def 4: Soient $(a_1,\dots,a_n)\in\mathbb{N}^n$.
- Il existe un unique $d\in\mathbb{N}$ tel que $a_1\mathbb{Z}+\dots+a_n\mathbb{Z}=d\mathbb{Z}$. On le note $\mathrm{PGCD}(a_1,\dots,a_n)$. C'est le plus grand entier naturel divisant les $(a_i)_{1\le i\le n}$.
- Lorsque $\mathrm{PGCD}(a_1,\dots,a_n)=1$, $a_1,\dots,a_n$ sont dits premiers entre eux.

Lemme 5: (Euclide) Soit $(b,c)\in\mathbb{N}^2$, soit $p\in\mathcal{P}$. Si p divise bc (noté $p\mid bc$), alors $p\mid b$ ou $p\mid c$.

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

App 7: Soit $p\in\mathcal{P}$, soit $k\in[\![1,p-1]\!]$, alors $p\mid\binom{p}{k}$.

Ex 8: Soient $(x,y)\in\mathbb{Z}^2$, $p\in\mathcal{P}$. Alors $(x+y)^p\equiv x^p+y^p\,[p]$.

2) Décomposition

Thm 9: (thm fondamental de l'arithmétique). Tout $n\in\mathbb{Z}^*$ s'écrit de manière unique à l'ordre des coefficients près: $n=\varepsilon\prod_{p\in\mathcal{P}}p^{\alpha_p}$ où $(\alpha_p)\in\mathbb{N}^{\mathcal{P}}$ et $\varepsilon=\pm1$.

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

Prop 11: Soit $(n,m)\in(\mathbb{Z}^*)^2$ et $\varepsilon_n\prod_{p\in\mathcal{P}}p^{\alpha_p}$, $\varepsilon_m\prod_{p\in\mathcal{P}}p^{\beta_p}$ leur décomposition en facteurs premiers. Alors:

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

3) Fonctions arithmétiques

Def 12: Pour $n\in\mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers inférieurs à n qui sont premiers avec n. C'est l'indicatrice d'Euler.

Prop 13:
- Si $p\in\mathcal{P}$, $\alpha\in\mathbb{N}^*$, on a $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$.
- Si $(n,m)\in(\mathbb{N}^*)^2$, $\mathrm{PGCD}(n,m)=1$, alors $\varphi(nm)=\varphi(n)\varphi(m)$.

Prop 14: Pour $n\in\mathbb{N}\setminus\{0,1\}$, on a $n=\sum_{d\mid n}\varphi(d)$.

Def 15: On définit la fonction de Möbius $\mu:\mathbb{N}^*\to\{-1,0,1\}$:
- $\mu(1)=1$,
- $\mu(n)=0$ si il existe $p\in\mathcal{P}$, $p^2\mid n$,
- $\mu(\prod_{i=1}^{r}p_i)=(-1)^r$ si $(p_i)_{1\le i\le r}\in\mathcal{P}^r$, $p_i\neq p_j$ pour $1\le i<j\le r$.

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

Prop 17:
- Pour $n\in\mathbb{N}^*$, on a $0=\sum_{d\mid n}\mu(d)$.
- Soit $f:\mathbb{N}^*\to(A,+)$ où $(A,+)$ est un groupe abélien. On pose $g(n)=\sum_{d\mid n}f(d)$ pour $n\in\mathbb{N}^*$. On a la formule d'inversion de Möbius: $f(n)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)g(d)$.

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

App 19: Soit $n\in\mathbb{N}^*$. On définit le $n^{\text{ème}}$ polynôme cyclotomique par $\Phi_n(X)=\prod_{\mathrm{PGCD}(k,n)=1}(X-e^{2ik\pi/n})$.
- Le polynôme Φ_n est unitaire, de degré $\varphi(n)$, dans $\mathbb{Z}[X]$ et irréductible sur $\mathbb{Z}$.
- On a $X^n-1=\prod_{d\mid n}\Phi_d(X)$.
- On a $\Phi_n(X)=\prod_{d\mid n}(X^{n/d}-1)^{\mu(d)}$.

4) Répartition

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

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

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

Def 23: Si $s\in\mathbb{C}$, $\mathrm{Re}(s)>1$, on définit la fonction de Riemann: $\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s}$.

②

Prop 24: La fonction ζ se prolonge en une fonction méromorphe sur $\mathbb{C}\setminus\{1\}$ avec un pôle simple en 1.

Prop 25: Pour tout $s\in\mathbb{C}$, $Re(s)>1$: $\zeta(s)=\prod_{p\in\mathcal{P}}\frac{1}{1-p^{-s}}$.

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

Thm 27: (Thm des nombres premiers, admis) Soit $x>1$. On note $\pi(x)$ le nombre de nombres premiers inférieurs à x. Alors

$$\pi(x)\underset{x\to+\infty}{\sim}\frac{x}{\ln(x)}.$$

Rq 28: En fait, on peut montrer que $\pi(x)\sim\int_2^x\frac{dt}{\ln(t)}$, 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: (Golbach) Tout nombre entier pair supérieur à 3 peut s'écrire comme 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.

II- Application aux corps finis.

1) $\mathbb{Z}/p\mathbb{Z}$ et premières propriétés

Prop 31: Un élément $\alpha\in\mathbb{Z}/n\mathbb{Z}$, pour $n\in\mathbb{N}$, est inversible si et seulement si $PGCD(\alpha,n)=1$. Son inverse peut alors être calculé grace à la relation de Bézout.

Cor 32: Pour $n\in\mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n\in\mathcal{P}$.

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

Thm 34: (de Fermat). Soit $p\in\mathcal{P}$, alors:

$$\forall a\in\mathbb{Z},\ a^p\equiv a\,[p].$$

Thm 35: (de Wilson). Soit $p\in\mathbb{N}\setminus\{0,1\}$. Alors:

$$p\in\mathcal{P}\iff(p-1)!\equiv-1\,[p].$$

2) Polynômes irréductibles

Prop 36: (Critère d'Eisenstein) Soient $n\in\mathbb{N}^*$, $P(X)=\sum_{i=0}^n a_iX^i\in\mathbb{Z}[X]$ et $p\in\mathcal{P}$. Si:
- $p\nmid a_n$
- $\forall i\in[\![0,n-1]\!]$, $p|a_i$
- $p^2\nmid a_0$

Alors P est irréductible sur $\mathbb{Q}$. Il l'est sur $\mathbb{Z}$ si $PGCD(a_0,\dots,a_n)=1$.

Prop 37: Soient $(n,p)\in\mathbb{N}\times\mathcal{P}$ et $P(X)=\sum_{i=0}^n a_iX^i\in\mathbb{Z}[X]$. On note $\bar{P}$ sa réduction modulo p et on suppose $a_n\not\equiv0\,[p]$. Si $\bar{P}$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, alors P est irréductible sur $\mathbb{Q}$. Si de plus $PGCD(a_0,\dots,a_n)=1$, P est irréductible sur $\mathbb{Z}$.

C-ex 38: Le polynôme X^4+1 est irréductible sur $\mathbb{Z}$, mais réductible sur $\mathbb{Z}/p\mathbb{Z}$ pour tout $p\in\mathcal{P}$.

3) Carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Dans cette partie, $p\in\mathcal{P}$, $n\in\mathbb{N}^*$ et $q=p^n$.

Prop 39: On note $\mathbb{F}_q^2=\{x^2,x\in\mathbb{F}_q\}$ et $\mathbb{F}_q^{*2}=\{x^2,x\in\mathbb{F}_q^*\}$. On a:
- Pour $p=2$, $\mathbb{F}_q^2=\mathbb{F}_q$,
- Pour $p>2$, $\#\mathbb{F}_q^2=\frac{q+1}{2}$, $\#\mathbb{F}_q^{*2}=\frac{q-1}{2}$.

On suppose maintenant que $p>2$.

Def 40: Si $x\in\mathbb{F}_p$, on définit le symbole de Legendre:

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

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

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

Cor 43: On a: $-1\in\mathbb{F}_p^2\iff p=2$ ou $p\equiv1\,[4]$.

Thm 44: Pour $(\ell,p)\in(\mathcal{P}\setminus\{2\})^2$, $\ell\neq p$, on a la loi de réciprocité quadratique:

$$\left(\frac{\ell}{p}\right)=\left(\frac{p}{\ell}\right)(-1)^{(p-1)(\ell-1)/4}$$

Ex 45: On a:

$\left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)=-\left(\frac{7}{29}\right)=-\left(\frac{29}{7}\right)=-\left(\frac{1}{7}\right)=-1$, donc 29 n'est pas un carré modulo 43.

Thm 46 : Soit $n \in \mathbb{N}^*$. Alors n est somme de deux carrés si et seulement si $v_p(n)$ est pair pour tout $p \in \mathcal{P}$ tel que $p \equiv 3\ [4]$. DEV

III – p-groupes et théorème de Sylow

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

Def 47 : Un p-groupe est un groupe dont le cardinal est une puissance de p.

Ex 48 : Le groupe Q_8 des quaternions et le groupe diédral D_4 sont des 2-groupes d'ordre 8.

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

Def 50 : Soit G un groupe fini, $n = \#G$, $p \mid n$. 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.

Ex 51 : Si $n \in \mathbb{N}^*$, $G = GL_n(\mathbb{F}_p)$ est un groupe fini d'ordre $\#G = m\,p^{\frac{n(n-1)}{2}}$ avec $p \nmid m$. L'ensemble des matrices triangulaires supérieures strictes est un p-sous-groupe de Sylow de G.

Thm 52 : (de Sylow) Soit G un groupe de cardinal $p^\alpha m$, $p \nmid m$.
1) Soit H un sous-groupe de G qui est un p-groupe. Alors il existe un p-Sylow S de G tel que $H \subset S$.
2) Les p-Sylow sont tous conjugués.
3) Si on note k_p le nombre de p-Sylow de G, on a :
$$k_p \mid m \text{ et } k_p \equiv 1\ [p].$$

Cor 53 : Soit G un groupe et S un p-Sylow de G. On a :
$$S \lhd G \iff S \text{ est l'unique } p\text{-Sylow de } G \iff k_p = 1.$$

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

IV – Les nombres premiers en pratique.

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

annexe

```
def Eratosthène(L):
    t = [True]*L
    t[1] = False
    i = 2
    while i*i <= L:
        if t[i]:
            for j in range(i*i, L, i):
                t[j] = False
        i += 1
    return t
```

Def 56 : Soit $n \in \mathbb{N}$, n est dit de Carmichaël si $n \notin \mathcal{P}$ et :
$$\forall a \in \mathbb{N},\ PGCD(a,n) = 1 \Rightarrow a^{n-1} \equiv 1\ [n].$$

Ex 57 : Le nombre 561 est le plus petit nombre de Carmichaël.

Thm 58 : (Critère de Korselt) Soit $n \in \mathbb{N}$ et $\prod_{i=1}^{u} p_i^{d_i}$ sa décomposition en facteurs premiers. Alors n est de Carmichaël si et seulement si : $\forall i \in [\![0,u]\!]$ $p_i - 1 \mid n-1$ et $d_i = 1$.

Prop 59 : Soit $n \in \mathbb{N}$. Si $2^n + 1 \in \mathcal{P}$, alors n est une puissance de 2.

Def 60 : Pour $n \in \mathbb{N}$, on définit le $n^{\text{ème}}$ nombre de Fermat :
$$F_n := 2^{2^n} + 1.$$

Ex 61 : On a $F_2 = 17 \in \mathcal{P}$, mais $F_5 \notin \mathcal{P}$.

Test 62 : Pour $n \in \mathbb{N}$, on a le test de Pépin :
$$F_n \in \mathcal{P} \iff 3^{(F_n - 1)/2} \equiv -1\ [F_n].$$

Def 63 : Pour $q \in \mathbb{N}$, on définit le $q^{\text{ème}}$ nombre de Mersenne
$$M_q := 2^q - 1.$$

Prop 64 : Si $q \in \mathbb{N}$, $q \notin \mathcal{P}$, alors $M_q \notin \mathcal{P}$.

Thm 65 : Pour $q \in \mathcal{P} \setminus \{2\}$, on a :
$$M_q \in \mathcal{P} \iff (2+\sqrt{3})^{2^{q-1}} \equiv -1\ [M_q].$$
DEV

Ex 66 : $M_3 = 2^3 - 1 = 7 \in \mathcal{P}$, mais $M_{11} = 2047 = 23 \times 89$ (c'est le plus petit nombre de Mersenne non-premier)

Test 67 : On a le test de Lehmer-Lucas : Pour $q \in \mathcal{P} \setminus \{2\}$, on définit $(L_n) \in (\mathbb{Z}/M_q\mathbb{Z})^{\mathbb{N}}$ par :
$$\begin{cases} L_{n+1} = L_n^2 - 2\ [M_q] \text{ si } n \in \mathbb{N} \\ L_0 = 4 \end{cases}$$
On a alors : $M_q \in \mathcal{P} \iff L_{q-2} \equiv 0\ [M_q]$.

55) Crible d'Eratosthène pour L=100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100