121. Nombres premiers. Applications.

I - Arithmétique dans $\mathbb{Z}$

Def 1 : Un nombre $p \in \mathbb{Z} \setminus \{1\}$ est premier si ses seuls diviseurs positifs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers

Lemme 2 (Gauss) : soit $k, m, n \in \mathbb{Z}$ tels que $k \mid mn$ et $k \wedge m = 1$, alors $k \mid n$.

Lemme 3 (Euclide) : soit $p \in \mathcal{P}$ et $m, n \in \mathbb{Z}$ tels que $p \mid mn$, alors $p \mid m$ ou ...

Exemple 4 : $\forall k \in [\![1, p-1]\!], p \mid \binom{p}{k}$.

Thm 5 : L'anneau $\mathbb{Z}$ est euclidien, donc factoriel $\forall n \in \mathbb{Z}$ $\exists ! (p_1, \dots, p_n) \in \mathcal{P}^n$ distincts, $\exists (v_1, \dots, v_n) \in \mathbb{N}^*$ tels que $n = \pm p_1^{v_1} \cdots p_n^{v_n}$. Cette décomposition est unique à l'ordre des facteurs près. $v_i = v_{p_i}(n)$ est la valuation p_i-adique de n.

Ex 6 : $280 = 2 \times 2 \times 2 \times 5 \times 7 = 2^3 \times 5 \times 7$

App 7 : soit n et $m \in \mathbb{Z} \setminus \{0; \pm 1\}$, n divise m si et seulement si, pour tout p premier qui divise n, $v_p(n) \leq v_p(m)$

App 8 : soit $n = p_1^{v_{p_1}(n)} \cdots p_n^{v_{p_n}(n)}$ et $m = p_1^{v_{p_1}(m)} \cdots p_n^{v_{p_n}(m)}$, alors $n \wedge m = p_1^{\min(v_{p_1}(n), v_{p_1}(m))} \cdots p_n^{\min(v_{p_n}(n), v_{p_n}(m))}$

Ex 9 : $280 \wedge 308 = 28$.

II - Répartition des nombres premiers

Prop 10 (crible d'Eratosthène) : on peut chercher et représenter l'ensemble des nombres premiers entre 2 et n sous la forme d'un tableau, en éliminant, pour le plus petit premier p non-considéré, les entiers divisibles par p.

(cf annexe 1)

Prop 11 : l'ensemble $\mathcal{P}$ est infini.

Def 12 : soit ζ la fonction définie pour z tel que $\mathrm{Re}(z) > 1$ par $\zeta(z) = \sum_{n=0}^{+\infty} \frac{1}{n^z}$

Prop 13 : pour tout z tel que $\mathrm{Re}(z) > 1$, $\zeta(z) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^z}}$

App 14 : la série $\sum_{p \in \mathcal{P}} \frac{1}{p}$ diverge.

Thm 15 : (progression arithmétique) (admis) : soient m et n deux entiers premiers entre eux, il existe une infinité de nombres premiers congru à m modulo n.

Thm 16 : (des nombres premiers) (admis) : pour $x > 0$, on note $\pi(x) = \mathrm{Card}(\mathcal{P} \cap [0; x])$. On a $\pi(x) \sim \frac{x}{\ln(x)}$.

III - Corps finis

Prop 17 : soit $\mathbb{K}$ un corps fini, il existe un unique morphisme d'anneau φ de $\mathbb{Z}$ dans $\mathbb{K}$. De plus, il existe $p := \mathrm{car}(\mathbb{K})$ tel que $\mathrm{Ker}(\varphi) = p\mathbb{Z}$.

Thm 18 : soit $\mathbb{K}$ un corps fini, il existe un entier n tel que $\mathrm{card}(\mathbb{K}) = \mathrm{car}(\mathbb{K})^n$.

1) Le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Thm 19 (Bézout) : soit $(m, n) \in \mathbb{Z}^2$, alors $m \wedge n = 1$ si, et seulement si, $\exists (a, b) \in \mathbb{Z}^2$ tels que $am + bn = 1$.

App 20 : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ est un corps.

App 21 : on peut appliquer l'algorithme d'Euclide étendu à a et p pour trouver l'inverse de a dans $\mathbb{F}_p$.

Thm 22 (Fermat) : soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$, alors $a^p = a$ dans $\mathbb{F}_p$.

App 23 (Wilson) : $p \in \mathcal{P} \iff (p-1)! \equiv -1$ dans $\mathbb{Z}/p\mathbb{Z}$.

Thm 24 : $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique.

Thm 25 (racine primitive) : soit $n \in \mathbb{N}^*$, alors n est premier si, et seulement si, il existe un élément d'ordre $n-1$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.

2) Polynômes irréductibles

Prop 26 : soit P un polynôme de degré n irréductible dans $\mathbb{F}_p[X]$. Alors $\mathbb{F}_p[X]/\langle P\rangle$ est un corps fini à p^n éléments.

Ex 27 : $\mathbb{F}_{16} = \mathbb{F}_2/\langle X^4+X^3+X^2+X+1\rangle$

Prop 28 : soit $P \in \mathbb{Z}[X]$ non-constant, et $p \in \mathcal{P}$ tel que p ne divise pas le coefficient dominant de P. Alors si P est irréductible dans $\mathbb{F}_p[X]$, P est irréductible dans $\mathbb{Q}[X]$.

C-ex 29 : X^4+1 est irréductible dans $\mathbb{Q}[X]$ mais réductible dans tout les $\mathbb{F}_p$.

Prop 30 : soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et $p \in \mathcal{P}$ tel que p ne divise pas a_n, p divise a_i pour $i<n$ et p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{Q}[X]$.

Ex 31 : $3X^3+4X^2+6X+14$ est irréductible dans $\mathbb{Q}[X]$.

3) Carrés dans $\mathbb{F}_p$.

Prop 32 : pour $p \in \mathcal{P}\setminus\{2\}$, l'application $\varphi : \left|\begin{array}{l} \mathbb{F}_p^* \to \{\pm 1\} \\ x \mapsto x^{\frac{p-1}{2}} \end{array}\right.$ est un morphisme de groupes.

Prop 33 : pour $p \in \mathcal{P}\setminus\{2\}$, l'ensemble $\mathbb{F}_p^2$ des carrés de $\mathbb{F}_p$ est de cardinal $\frac{p+1}{2}$.

Def 34 : soit $p \in \mathcal{P}\setminus\{2\}$, et $a \in \mathbb{F}_p$, on définit le symbole de Legendre

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré non-nul} \\ -1 & \text{si } a \text{ n'est pas un carré} \\ 0 & \text{si } a = 0 \end{cases}$$

App 35 : soit $p \in \mathcal{P}\setminus\{2\}$ et $a \in \mathbb{F}_p$, l'équation $x^2=a$ possède $1+\left(\frac{a}{p}\right)$ solution dans $\mathbb{F}_p$.

Thm 36 (loi de réciprocité quadratique) : soit $p, q \in \mathcal{P}\setminus\{2\}$, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$

IV - Application à la théorie des groupes

Def 37 : un p-groupe est un groupe fini d'ordre p^n avec $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$.

Thm 38 (Cauchy) : soit G un groupe fini de cardinal divisible par $p \in \mathcal{P}$. Alors G possède un élément d'ordre p.

Thm 39 : le centre d'un p-groupe n'est pas trivial. En particulier, un p-groupe n'est pas simple.

App 40 : si $p \in \mathcal{P}$, un groupe d'ordre p^2 est abélien.

Def 41 : soit G un groupe fini de cardinal $p^n m$ avec $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ et $p \wedge m = 1$. Un p-Sylow de G est un sous-groupe de G, d'ordre p^n. On note $Syl_p(G)$ l'ensemble des p-Sylow de G et $n_p(G)$ son cardinal.

Thm 42 (Sylow) : soit G un groupe de cardinal $p^n m$ avec $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ et $p \wedge m = 1$. On a

1) Tout p-sous-groupe de G est inclus dans un p-Sylow.

2) Les p-Sylows de G sont conjugués. En particulier, si il existe un unique p-Sylow, il est distingué.

3) $n_p(G) \equiv 1\ [p]$ et $n_p(G) \mid m$.

App 43 : soit $p, q \in \mathcal{P}$, un groupe d'ordre pq n'est pas simple.

App 44 : un groupe d'ordre 60 est isomorphe à $\mathfrak{A}_5$.

App 45 : un groupe d'ordre 33 est cyclique.

DVP 1

V - Cryptographie et nombres premiers

1) La méthode RSA

Prop 46 : Alice a un message chiffré M pour Bob, dont il faut sécuriser le contenu. Pour cela :

1) Bob choisit deux grands premiers p et q ainsi qu'un nombre e premier avec $(p-1)(q-1)$.
2) Il calcule $n = pq$ et d, l'inverse de e dans $\mathbb{Z}/_{(p-1)(q-1)\mathbb{Z}}$
3) Il rend publique uniquement n et e.
4) Alice décompose son message M en $A_1 \cdots A_n$ avec $A_i < n$
5) Elle envoie successivement à Bob les A_i^e modulo n.
6) Bob calcule $(A_i^e)^d = A_i$ modulo n.

Rem 47 : l'efficacité de ce système de transmission provient de la difficulté de trouver la décomposition en nombre premier d'un entier donné n.

2) Conséquences du théorème de Fermat

Thm 48 : Soit n un entier tel qu'il existe a tel que $a^n \not\equiv a$ modulo n, Alors n n'est pas premier. Un tel a premier avec n est appelé témoin de Fermat pour n

Prop 49 : Il existe des nombres non-premiers, dits de Carmichael, sans témoins de Fermat.

Ex 50 : $561 = 3 \times 11 \times 17$ est un nombre de Carmichael.

Thm 51 : Soit $n \in \mathbb{N}$ tel que $n-1 = 2^\eta t$ avec t impair. Si il existe $a \in \mathbb{N}$ tel que $a^t \not\equiv 1$ modulo n et $\forall i \in [\![0, \eta-1]\!]$ $a^{2^i t} \not\equiv -1$ modulo n, alors n n'est pas premier. Un tel a premier avec n est appelé témoin de Miller pour n

Ex 52 : 2 est un témoin de Miller pour 561, donc 561 n'est pas premier

Prop 53 : si n n'est pas premier, au moins trois quarts des entiers de 2 à $n-1$ sont des témoins de Miller.

App 54 (Test de Miller-Rabin) : pour déterminer si n est premier, on choisit aléatoirement un entier a entre 2 et $n-1$. Soit a est un témoin de Miller, soit on recommence. Après k itérations de ce test, le nombre n est premier avec probabilité $1-\left(\frac{1}{4}\right)^k$.

3) Famille de nombres premiers

Def 55 : un nombre de Fermat est un entier de la forme $2^{2^k}+1$. $Fer_k = 2^{2^k}+1$

Thm 56 : Fer_k est premier si, et seulement si, $3^{2^{2^k-1}} \equiv -1\ [Fer_k]$

Ex 57 : les seuls nombres premiers de Fermat connus sont les 5 premiers : 3, 5, 17, 257 et 65537.

App 58 (Gauss-Wantzel) : le polygone régulier à n côtés est constructible à la règle et au compas si n est le produit d'une puissance de 2 et nombres premiers de Fermat distincts.

Ex 59 : le 83-gone n'est pas constructible à la règle et au compas.

Def 60 : un nombre de Mersenne est un entier de la forme $M_p = 2^p - 1$ avec $p \in \mathcal{P}$.

Thm 61 : pour $p \in \mathcal{P} \setminus \{2\}$, M_p est premier si, et seulement si, $(2+\sqrt{3})^{2^{p-1}} = -1$ dans un corps contenant $\mathbb{Z}/_{M_p\mathbb{Z}}$ où 3 est un carré.

App 62 : on définit une suite dans $\mathbb{Z}/_{M_p\mathbb{Z}}$ par $L_0 = 4$ et $L_{n+1} = L_n^2 - 2$. Alors M_p est premier si, et seulement si, $L_{p-2} = 0$.

DVP 2

Annexe 1 : Grille de Poincaré

		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	101	102	103	104	~~105~~	106	107	108	109