Nombres premiers. Applications.

(I) Arithmétique élémentaire dans $\mathbb{Z}$.

1) Nombre premier.

Déf 1 : Soit $p \in \mathbb{N}$. On dit que p est un nb premier s'il admet exactement deux diviseurs positifs. On note $\mathbb{P}$ l'ensemble des nombres premiers.

Exple 2 : Crible d'Eratosthène : $2, 3, 5, 7, 11, \dots, 2017, \dots \in \mathbb{P}$.

Exple 3 : On appelle nombre de Fermat tout nombre 1er de la forme $F_k = 2^{2^k} + 1$.

Exple 4 : On appelle nombre de Sophie Germain tout nombre 1er impair p tel que $q = 2p+1 \in \mathbb{P}$.

Prop 5 : Tout entier $n \geq 2$ possède au moins un facteur premier.

Déf 6 : On note $\pi(n) = |\{p \in \mathbb{P},\ p \leq n\}|$ la fonction de compte des nombres premiers, et p_n le $n^{ième}$ nombre premier, de sorte que $\forall n \in \mathbb{N},\ \pi(p_n) = n$.

Th 7 : L'ensemble des nombres premiers $\mathbb{P}$ est infini. En d'autres termes, $\lim_{n \to \infty} \pi(n) = +\infty$.

Lemme d'Euclide : $\forall a, b \in \mathbb{Z}, \forall p \in \mathbb{P}$, si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

2) Nombres premiers entre eux.

Déf 9 : Soient $a, b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux s'ils n'ont pas d'autres diviseurs communs que 1 et -1. On note alors $\text{pgcd}(a,b) = a \wedge b = 1$.

Th de Bézout : $\forall a, b \in \mathbb{Z}, \exists u, v \in \mathbb{Z}$ tq $au + bv = \text{pgcd}(a,b)$.
En particulier, $a \wedge b = 1 \iff \exists u, v \in \mathbb{Z}$ tq $au + bv = 1$.

Lemme de Gauss : $\forall a, b, c \in \mathbb{Z}$, si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

Th fondamental de l'arithmétique : Tout entier $n \geq 2$ s'écrit, de manière unique à l'ordre près des facteurs, sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $p_1, \dots, p_r \in \mathbb{P}$ deux à deux distincts, $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$.

Exple 14 : $2016 = 2^5 . 3^2 . 7$.

3) Réduction modulaire

Th 15 : Soit $n \in \mathbb{N}^*$. $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff n \in \mathbb{P}$. On note alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Petit théorème de Fermat : Soit $p \in \mathbb{P}$. $\forall a \in \mathbb{Z}$, $a^p \equiv a \ [p]$.

DV ① **Appli 17 : Théorème de Sophie Germain :** Soit p un nb 1er de Sophie Germain, alors il n'existe pas de solutions $(x, y, z) \in \mathbb{Z}^3$ à l'équation $x^p + y^p + z^p = 0$ telle que $xyz \not\equiv 0 [p]$.

Th de Wilson : Un entier $p \geq 2$ est un nombre premier ssi $(p-1)! \equiv -1 \ [p]$.

Chiffrement RSA : Soient p, q deux nombres 1ers distincts. On pose $n = pq$.
Soient $c, d \in \mathbb{N}$ tq $cd \equiv 1 \ [(p-1)(q-1)]$. Alors $\forall t \in \mathbb{Z}$, $t^{cd} \equiv t \ [n]$.

4) Irréductibilité de polynômes

Critère d'Eisenstein : Soit $P(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$
Si $\exists p \in \mathbb{P}$, $\forall k \in [\![0, n-1]\!]$, $p \mid a_k$, $p \nmid a_n$, $p^2 \nmid a_0$, alors P est irréductible ds $\mathbb{Q}[X]$.
Si de plus, $c(P) = 1$, alors P est irréductible dans $\mathbb{Z}[X]$.

Appli 21 : Soit $p \in \mathbb{P}$, le polynôme cyclotomique $\Phi_p(X) = X^{p-1} + \dots + X + 1$ est irréductible ds $\mathbb{Z}[X]$

Th 22 : Soit $P(X) = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction modulo $p \in \mathbb{P}$.
Si $\overline{a_n} \neq \overline{0}$, alors si $\overline{P}$ est irréductible sur $\mathbb{F}_p[X]$, on a P irréductible sur $\mathbb{Q}[X]$.

II Théorie des nombres

1) Fonctions arithmétiques

Déf 23 : On définit la fonction indicatrice d'Euler par : $\forall n \in \mathbb{N}^*, \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{k \in [\![1,n]\!] : k \wedge n = 1\}|$

Prop 24 : Soient $m, n \in \mathbb{Z}$, $m \wedge n = 1$ alors $\varphi(mn) = 1$ et soient $p \in \mathbb{P}$, $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Prop 25 : Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \mathbb{N}^*$, alors $\varphi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$

Appli 26 : Soit $p \in \mathbb{P}$, alors le groupe $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^*$ est cyclique.

Th de Wantzel : $z \in \mathbb{C}$ est constructible $\Leftrightarrow$ z est dans une tour d'extensions quadratiques de $\mathbb{Q}$.

DVI 2 **Th de Gauss-Wantzel :** Soit $n \geq 2$. Le n-gône est constructible (à la règle et au compas) ssi $n = 2^\alpha \cdot p_1 \cdots p_r$ avec $\alpha \in \mathbb{N}$, $p_1, \dots, p_r$ nombres 1^{ers} de Fermat distincts

Déf 29 : On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \{-1; 0; 1\}$,
$$n \mapsto \begin{cases} (-1)^r & \text{si } n = p_1 \cdots p_r \\ 0 & \text{si } \exists p \in \mathbb{P},\ p^2 \mid n \end{cases}$$

Prop 30 : Si $m \wedge n = 1$, alors $\mu(mn) = \mu(m) \cdot \mu(n)$.

Déf 31 : Soient $u, v \in \mathbb{R}^{\mathbb{N}^*}$. On définit leur pdt de convolution arithmétique par : $\forall n \in \mathbb{N}^*, (u*v)(n) = \sum_{d \mid n} u(d) \cdot v\left(\frac{n}{d}\right)$

Th 32 : $(\mathbb{R}^{\mathbb{N}^*}, +, *)$ est un anneau commutatif unitaire, d'élément neutre $\delta_1 : n \mapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$
De plus, $\mu * 1 = \delta_1$. En d'autres termes : $\forall n \in \mathbb{N}^*, v(n) = \sum_{d \mid n} u(d) \Leftrightarrow \forall n \in \mathbb{N}^*, u(n) = \sum_{d \mid n} v(d)\mu\left(\frac{n}{d}\right)$

DVI 3 **Appli 33 :** Soit $n \in \mathbb{N}^*$. On note r_n la probabilité que 2 entiers de $[\![1,n]\!]$ soient 1^{ers} entre eux.
alors $\forall n \in \mathbb{N}^*, r_n = \frac{1}{n^2} \cdot \sum_{d=1}^{n} \mu(d) \cdot \left\lfloor \frac{n}{d} \right\rfloor^2$. En particulier, $\lim_{n \to \infty} r_n = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$.

2) La fonction ζ de Riemann.

Déf 34 : On définit $\forall s \in \Omega_1 = \{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$ la fonction ζ de Riemann par : $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Th 35 : La fonction ζ se prolonge en une fonction holomorphe sur $\mathbb{C} \setminus \{1\}$, admettant un pôle simple en 1.

DVI 4 **Produit eulérien :** La série $\sum_{n \geq 1} \frac{1}{p_n}$ diverge. D'autre part, $\forall s \in \Omega_1$, $\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$.

Corollaire 37 : La fonction ζ ne s'annule pas sur la droite $\mathrm{Re}(s) = 1$.

3) Distribution asymptotique des nombres premiers

Déf 38 : On définit la fonction θ de Tchebychev par : $\forall x \in \mathbb{R}^+, \theta(x) = \sum_{p_n \leq x} \ln(p_n)$.

Prop 39 : $\forall s \in \Omega_1$, $\psi(s) := \sum_{n=1}^{\infty} \frac{\ln(p_n)}{p_n^s} = s \int_1^{\infty} \frac{\theta(x)}{x^{s+1}} dx$.

Lemme de Newman : Soit $f \in \mathbb{L}^\infty([0, \infty[)$ de transformée de Laplace $F : z \mapsto \int_0^\infty e^{-tz} f(t)\, dt$
Si F se prolonge en une fonction holomorphe sur un voisinage de $\overline{\Omega_0}$, alors $\int_0^\infty f(t)\, dt = F(0)$

Th 41 : Lorsque x tend vers $+\infty$, on a $\theta(x) \underset{+\infty}{\sim} x$.

Théorème des nombres premiers : on a : $\theta(n) \underset{+\infty}{\sim} n \Leftrightarrow \pi(n) \underset{+\infty}{\sim} \frac{n}{\ln(n)} \Leftrightarrow p_n \underset{+\infty}{\sim} n \ln(n)$.

4) Nombres premiers dans les progressions arithmétiques

Soit $D \in \mathbb{N}$, $D \geq 2$. On note $G = (\mathbb{Z}/D\mathbb{Z})^\times$.

Déf 43 : On appelle caractère de Dirichlet modulo D tout morphisme de groupes $\chi : G \to \mathbb{C}^*$. On a $\chi \in \hat{G}$.

Prop 44 : On peut étendre χ en une fonction sur $\mathbb{Z}$, D-périodique, strictement multiplicative.

Déf 45 : On définit la somme de la série de Dirichlet par : $\forall s \in \Omega_1$, $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$

Th de Landeau : Soit $L(a, s)$ une série de Dirichlet à coefficients positifs.
Alors σ_{abs} n'a aucun voisinage de c sur lequel $L(a,s)$ admet un prolongement analytique.

DVPT 5 **Th 47 :** Si $\chi = 1_D$ est le caractère trivial, $s \mapsto L(1_D, s)$ admet un pôle simple en $s = 1$, de résidu $\varphi(D)$.
Si $\chi \neq 1_D$, on peut prolonger $L(\chi, s)$ sur Ω_0, et alors $L(\chi, 1) \neq 0$.

Th de la progression arithmétique : Soient $D, b \in \mathbb{N}$, $D \geq 2$, $D \wedge b = 1$,
alors il existe une infinité de nombres premiers de la forme $p = Dn + b$, $n \in \mathbb{N}$.

III Nombres premiers en théorie des groupes.

1) p-groupes, $p \in \mathbb{P}$

Prop 48 : Tout groupe d'ordre p est cyclique, isomorphe à $\mathbb{Z}/p\mathbb{Z}$. De plus, c'est un gpe simple.

Déf 49 : Soit $p \in \mathbb{P}$, on appelle p-groupe tout groupe d'ordre p^α avec $\alpha \in \mathbb{N}^*$.

Exple 50 : $V_4 = (\mathbb{Z}/2\mathbb{Z})^2$ et $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ sont des 2-groupes

DV 6 **Prop 51 :** Le centre d'un p-groupe est non trivial, plus précisément, $|Z(G)| \geqslant p$.

Coro 52 : Tout groupe d'ordre p^2 est abélien. Ainsi, il est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

2) Sous-groupes de Sylow

Soit G un groupe fini de cardinal $|G| = n = p^\alpha \cdot m$ avec $p \in \mathbb{P}$, $p \nmid m$.

Déf 53 : On appelle p-Sylow de G tout sous groupe de cardinal p^α.

DVPT 7 **Exple 54 :** $S = \{A = (a_{i,j}) \in M_n(\mathbb{F}_p) : \forall i,\ a_{i,i} = 1$ et $\forall i > j,\ a_{i,j} = 0\}$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 55 : Soit $H < G$ et S p-Sylow de G, alors $\exists a \in G : aSa^{-1} \cap H$ soit un p-Sylow de H.

Théorèmes de Sylow : (1) G contient au moins un p-Sylow

(2) Tout les p-Sylow de G sont conjugués

(3) Soit n_p le nb de p-Sylow de G alors $\begin{cases} n_p \mid m \\ n_p \equiv 1 \ [p] \end{cases}$

Corollaire 57 : Soit S un p-Sylow de G. $S \lhd G \iff S$ est l'unique p-Sylow de G.

Appli 58 : Soient $p < q \in \mathbb{P}$. Un groupe d'ordre $p^2 q$ n'est jamais simple

DV 8 **Appli 59 :** Soient $p < q \in \mathbb{P}$ et G un groupe d'ordre pq.

- Si $q \not\equiv 1 \ [p]$ alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$;
- Si $q \equiv 1 \ [p]$ alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou bien $G \simeq \mathbb{Z}/q\mathbb{Z} \times_\alpha \mathbb{Z}/p\mathbb{Z}$ avec $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

IV Etude des corps finis.

1) Construction des corps finis

Déf 60 : Soit $\mathbb{K}$ un corps et $\varphi : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{K} \\ n & \mapsto & n.1_\mathbb{K} \end{array}$ morphisme d'anneaux.

Le nombre p générateur de $\mathrm{Ker}(\varphi)$ est appelé caractéristique de $\mathbb{K}$. De plus, $p \in \mathbb{P} \cup \{0\}$.

Prop 61 : Soit $\mathbb{K}$ un corps de cardinal fini ; $\exists p \in \mathbb{P}$ tq $\mathrm{Caract}(\mathbb{K}) = p$, alors $|\mathbb{K}| = p^n = q$ avec $n \in \mathbb{N}^*$.

Prop 62 : Soit $\mathbb{K}$ un corps fini de caractéristique $p \in \mathbb{P}$.

alors $F : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{array}$ est un morphisme appelé automorphisme de Frobenius.

Th 63 : Soit $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$. On pose $q = p^n$.

(1) Il existe un corps $\mathbb{K}$ à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$

(2) $\mathbb{K}$ est unique à isomorphisme près. On le note $\mathbb{F}_q$.

2) Carrés dans $\mathbb{F}_p$.

Déf 64 : On note $\mathbb{F}_p^2 = \{x \in \mathbb{F}_p, \exists y \in \mathbb{F}_p$ tq $x = y^2\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Prop 65 : On a $\mathbb{F}_2^2 = \mathbb{F}_2$ et pour $p \geqslant 3$, $|\mathbb{F}_p^{*2}| = \dfrac{p-1}{2}$ donc $|\mathbb{F}_p^2| = \dfrac{p+1}{2}$.

Déf 66 : Soit $p \in \mathbb{P}$, $p \geqslant 3$. On définit le symbole de Legendre : $\mathbb{F}_p^* \to \{-1 ; 1\}$.

Prop 67 : $\left(\frac{\cdot}{p}\right)$ est un morphisme de groupes et $\forall x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$. $\quad x \mapsto \begin{cases} 1 & \text{si } x \in \mathbb{F}_p^{*2} \\ -1 & \text{sinon} \end{cases}$

DV 9 **Appli 68 :** **Th des 2 carrés de Fermat :** p est somme de 2 carrés $\iff p = 2$ ou $p \equiv 1 \ [4]$.

Ainsi, $n \in \mathbb{N}, n \geqslant 2$ est somme de 2 carrés $\iff \forall p \in \mathbb{P}, p \mid n$ tq $p \equiv 3 \ [4]$, on a $v_p(n)$ est pair

DV 10 **Loi de Réciprocité quadratique :** Soient $p \neq q \in \mathbb{P}$, impairs, alors $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

Exple 70 : $\left(\frac{3}{2017}\right) = -1$: 3 n'est pas un carré dans $\mathbb{F}_{2017}$.