121 Nombres premiers. Applications.

Soit $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ premier, $q = p^n$.
On note $\mathcal{P}$ l'ensemble des nombres premiers.

I] Arithmétique dans $\mathbb{Z}$

1] Nombres premiers et nombres premiers entre eux

Théorème 1 : (d'Euclide) Tout entier relatif $n \in \mathbb{Z} \setminus \{-1;0;1\}$ a au moins un diviseur premier.

Théorème 2 : L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Définition 3 : Soit $(a_i)_{i=1}^{r} \in \mathbb{Z}^r$. On dit que $a_1;\dots;a_r$ sont premiers entre eux dans leur ensemble si $PGCD(a_1;\dots;a_r) = 1$.
Pour $r=2$, on dit simplement que a_1 et a_2 sont premiers entre eux. On note $a_1 \wedge \dots \wedge a_r = 1$.

Théorème 4 : (de Gauss) Soit $a,b \in \mathbb{Z}^*$
Alors : $a \wedge b = 1$ ssi $\forall c \in \mathbb{Z}$, $a \mid bc \Rightarrow a \mid c$

Théorème 5 : (de Bézout) Soit $(a_i)_{i=1}^{r} \in \mathbb{Z}^*$.
Alors : $a_1 \wedge \dots \wedge a_r = 1$ ssi $\exists (u_i)_{i=1}^{r} \in \mathbb{Z}^r \setminus \sum_{i=1}^{r} u_i a_i = 1$

Corollaire 6 : (de Gauss) Soit $a,b,c \in \mathbb{Z}^*$
Alors : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$

2] Décomposition en facteurs premiers

Théorème 7 : (fondamental de l'arithmétique) Tout entier $n \geq 2$ se décompose de manière unique sous la forme : $n = q_1^{\alpha_1} \times \dots \times q_r^{\alpha_r}$ avec $2 \leq q_1 < \dots < q_r$ premiers et $(\alpha_k)_{k=1}^{r} \in \mathbb{N}^{*r}$

Application 8 : Pour $p > q \geq 2$ premiers, $\frac{\ln(p)}{\ln(q)}$ est irrationnel.

Application 9 : $\mathbb{Z}$ est un anneau factoriel.

Proposition 10 : Soit $n = \prod_{i=1}^{r} q_i^{\alpha_i}$ décomposé en facteurs premiers.
Alors : n a $\prod_{i=1}^{r} (\alpha_i + 1)$ diviseurs positifs de n

Théorème 11 : Soit $n = \prod_{k=1}^{r} q_k^{\alpha_k}$, $m = \prod_{k=1}^{r} q_k^{\beta_k} \geq 2$ leurs décompositions en facteurs premiers, $(\alpha_k), (\beta_k) \in \mathbb{N}$
Alors : $n \wedge m = \prod_{k=1}^{r} q_k^{\min(\alpha_k;\beta_k)}$ et $n \vee m = \prod_{k=1}^{r} q_k^{\max(\alpha_k;\beta_k)}$

Application 12 : Il y a une infinité de nombres premiers de la forme $6n-1$.

3] Fonctions remarquables et résolubilité d'équations

Définition 13 : On appelle valuation p-adique de n :
$v_p(n) = \max\{k \in \mathbb{N} \mid p^k \mid n\}$. On a : $n = \prod_{\substack{p \mid n \\ p \in \mathcal{P}}} p^{v_p(n)}$.

Proposition 14 : $p \mid n$ ssi $v_p(n) \neq 0$

Application 15 : On retrouve : $n \wedge m = \prod_{p \in \mathcal{P}} p^{\min(v_p(n);v_p(m))}$ et $n \vee m = \prod_{p \in \mathcal{P}} p^{\max(v_p(n);v_p(m))}$.

Définition 16 : On appelle fonction indicatrice d'Euler la fonction qui associe à tout entier $n \in \mathbb{N}$, $\varphi(n)$ le nombre d'entiers compris dans $[\![1;n]\!]$ premiers avec n.

Théorème 17 : (d'Euler) $\forall a \in \mathbb{Z}$, $a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$

Corollaire 18 : (petit théorème de Fermat) Soit $a \in \mathbb{Z}$ tel que $a \wedge p = 1$.
Alors : $a^{p-1} \equiv 1 [p]$

Théorème 19 : $\forall n \geq 2$, $n = \sum_{d \mid n} \varphi(d)$.

Définition 20 : Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ décomposé en facteurs premiers.
On appelle fonction de Möbius : $\mu : \begin{array}{l} \mathbb{N}^* \to \{-1;0;1\} \\ n \mapsto \begin{cases} 1 & \text{si } n=1 \\ (-1)^r & \text{si } n = \prod_{i=1}^{r} p_i \\ 0 & \text{sinon} \end{cases} \end{array}$

Lemme 21 : $\forall n \in \mathbb{N}^*$, $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{sinon} \end{cases}$

Théorème 22 : (d'inversion de Möbius)
$\left(n \in \mathbb{N}^*, u(n) = \sum_{d \mid n} v(d)\right)$ ssi $\left(n \in \mathbb{N}^*, v(n) = \sum_{d \mid n} \mu(d) u\left(\frac{n}{d}\right)\right)$

Théorème 23 : (de Sophie Germain) Soit p premier impair, $q = 2p+1$ premier
Alors : $\nexists (x;y;z) \in \mathbb{Z} \setminus \begin{cases} xyz \not\equiv 0 [p] \\ x^p + y^p + z^p = 0 \end{cases}$

II] Application à la théorie des corps

1] Construction de corps finis

XIII.4 [Rom]

Définition 24 : On note $\mathcal{U}_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$.

Théorème 25 : $\forall P \in \mathcal{U}_n(p)$, $\mathbb{F}_p[X]/\langle P \rangle$ est une $\mathbb{F}_p$-algèbre de dimension n de base $(\overline{X}^k)_{k=0}^{n-1}$. C'est un corps fini de cardinal p^n.

Exemples 26 : (1) $\forall \lambda \in \mathbb{F}_p$, $X-\lambda \in \mathcal{U}_1(p)$ et $\mathbb{F}_p[X]/\langle X-\lambda \rangle$ est isomorphe à $\mathbb{F}_p$.
(2) Les polynômes $X^2+\lambda X+\mu$ sont dans $\mathcal{U}_2(p)$ ssi ils n'ont pas de racines. Dans ce cas, il définissent des corps $\mathbb{F}_p[X]/\langle X^2+\lambda X+\mu \rangle$ à p^2 éléments.

Lemme 27 : Tout diviseur irréductible de $X^{p^n}-X$ dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, pour tout $d|n$, tout polynôme $P \in \mathcal{U}_d(p)$ divise $X^{p^n}-X$.

Théorème 28 : $X^{p^n}-X$ est sans facteur carré dans $\mathbb{F}_p[X]$ et :
$$X^{p^n}-X = \prod_{d|n} \prod_{P \in \mathcal{U}_d(p)} P$$

[Isen]

Proposition 29 : L'application $S : \begin{array}{l} \mathbb{F}_q[X] \to \mathbb{F}_q[X] \\ Q \mapsto Q^q \end{array}$ est un $\mathbb{F}_q$-endomorphisme de $\mathbb{F}_q[X]$.

Lemme 30 : Soit $\mathbb{L}$ extension de $\mathbb{F}_q$ et $x \in \mathbb{L}$.
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$.

Théorème 31 : Soit $P \in \mathbb{F}_q[X]$ sans facteur carré, $P = \prod_{i=1}^{r} P_i$ sa décomposition en irréductibles sur $\mathbb{F}_q[X]$.
Alors : (1) Si $r=1$, alors P est irréductible
(2) Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $PGCD(P ; V-a)$ est facteur non-trivial de P.

2] Critères d'irréductibilité de polynômes

III.3 [Per]

Théorème 32 : (critère d'Eisenstein) Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et p premier tel que $p \nmid a_n$, $\forall i \in [\![0 ; n-1]\!]$, $p | a_i$ et $p^2 \nmid a_0$.
Alors : P est irréductible dans $\mathbb{Q}[X]$
si de plus, $c(P) = 1$, alors P est irréductible dans $\mathbb{Z}[X]$.

Exemple 33 : Si p premier, alors $X^{p-1}+\dots+X+1$ est irréductible dans $\mathbb{Z}[X]$.

Théorème 34 : (critère d'irréductibilité modulo p) Soit p premier, $P = \sum_{i}^{n} a_i X^i \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction modulo p telle que $\overline{a_n} \neq 0$.
Alors : si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible sur $\mathbb{Q}$.

Exemple 35 : $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

3] Résidus quadratiques et symbole de Legendre.

XIII.5

Théorème 36 : (1) Il y a $\frac{p+1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p$.
(2) Les carrés de $\mathbb{F}_p^*$ sont les racines de $X^{\frac{p-1}{2}}-1$ et les non-carrés sont les racines de $X^{\frac{p-1}{2}}+1$.

Corollaire 37 : -1 est carré dans $\mathbb{F}_p^*$ ssi $p \equiv 1 [4]$.

XIII.6 [Rom]

Définition 38 : On dit que $k \in \mathbb{N}$ tel que $p \nmid k$ est un résidu quadratique modulo p si $\overline{k}$ est un carré dans $\mathbb{F}_p^*$.
Pour tout $a \in \mathbb{F}_p^*$, on appelle symbole de Legendre l'entier :
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon.} \end{cases}$$

Théorème 39 : L'application $\begin{array}{l} \mathbb{F}_p^* \to \{\pm 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array}$ est l'unique morphisme de groupes non-trivial de $\mathbb{F}_p^*$ sur $\{\pm 1\}$.

XIII.7

Théorème 40 : (loi de réciprocité quadratique) Soit $p \neq q$ premiers.
Alors : $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$

[Isen]

Définition 41 : Soit E un $\mathbb{F}_p$-espace vectoriel, H hyperplan de E, G son supplémentaire i.e. $E = H \oplus G$. La dilatation de base H, direction G, rapport $\lambda \in \mathbb{K}^*$ tel que : $\forall h, u \in H \times G$, $f(h+u) = h + \lambda u$.

[Isom]

Théorème 42: Soit $p\geq 3$, V un $\mathbb{F}_p$-espace vectoriel.
Alors: les dilatations engendrent $GL(V)$.

Lemme 43: Soit $\mathbb{K}$ corps fini.
Alors: $\exists a\in\mathbb{K}^* \setminus \mathbb{K}^*=\langle a\rangle$.

Théorème 44: (de Frobénius - Zolotarev) Soit p premier impair, V un espace vectoriel de dimension n.
Alors: $\forall u\in GL(V)$, $\varepsilon(u)=\left(\frac{\det(u)}{p}\right)$

III/ Recherche de nombres premiers

1/ Répartition des nombres premiers

XI.3

Notation 45: On note $\mathcal{P}_n=\mathcal{P}\cap[\![1;n]\!]$ et $\pi(n)=\mathrm{card}(\mathcal{P}_n)$.

Rappel 46: $\mathcal{P}$ est infini.

Théorème 47: (admis) $\pi(n)\underset{+\infty}{\sim}\frac{n}{\ln(n)}$

Corollaire 48: (théorème de raréfaction de Legendre) $\lim\limits_{n\to+\infty}\frac{\pi(n)}{n}=0$

XI.2.exos

Proposition 49: $\forall n\geq 2$, il existe n entiers consécutifs non-premiers
ie. il existe des plages d'entiers aussi grandes que l'on veut sans nombres premiers.

Exemple 50: $[\![(n+1)!+2\ ;\ (n+1)!+(n+1)]\!]$ est un segment d'entiers non-premiers.

[Rom]

Proposition 51: $2n-1\leq p_n\leq 2^{2^{n-1}}$ avec p_n le n-ième nombre premier

Corollaire 52: $\pi(n)>\ln(\ln(n))$

Proposition 53: $\sum\limits_{n=1}^{+\infty}\frac{1}{p_n}=+\infty$

2/ Tests de primalité

XI.1

Théorème 54: Tout entier $n\geq 2$ non-premier a au moins un diviseur premier p tel que $2\leq p\leq\sqrt{n}$.

[Rom]

Remarque 55: On peut vérifier si un entier n est premier en testant s'il est divisible par un entier $d\leq\sqrt{n}$.

XI.1

[Rom]

Proposition 56: (crible d'Eratosthène) Principe:
(i) On se donne la liste $[\![2;m]\!]$ avec $m=\lceil\sqrt{n}\rceil$
(ii) On garde 2 et on supprime tous les multiples de 2 de la liste
(iii) Le premier entier >2 est 3 et comme il ne possède pas de diviseur stricte, il est premier. On le garde et on supprime tous les multiples de 3 de la liste.
(iv) On continue comme ça jusqu'à dépasser $\sqrt{n}$.

XI.5

Théorème 57: Soit $n\geq 2$.
Alors: n est premier ssi $\forall \alpha\in\mathbb{N}^*$, $\varphi(n^\alpha)=(n-1)n^{\alpha-1}$
ssi $\varphi(n)=n-1$
ssi $(n-1)!\equiv -1[n]$ (théorème de Wilson)

Remarque 58: Ces caractérisations fournissent des tests de primalité ~~mais sont souvent~~ coûteux pour la machine.

Rappel 59: (petit théorème de Fermat) Soit p premier.
Alors: $a^{p-1}\equiv 1[p]$, $\forall a\in\mathbb{Z}$, $a\wedge p=1$

Remarque 60: La réciproque de ce résultat fournit un critère de non-primalité. Ainsi, il est moins coûteux de vérifier la non-primalité d'un entier avant de sortir l'artillerie lourde des tests de primalité.

Références :

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi

[FGN Al1] Exercices de mathématiques oraux X-ENS Algèbre 1 - Francinou

[Isen] L'oral à l'agrégation de mathématiques - Isenmann

[Per] Cours d'algèbre - Perrin