121 Nombres premiers. Applications.

On désigne par $\mathbb{P}$ l'ensemble des nombres premiers.

I Généralités et arithmétique dans $\mathbb{Z}$.

A Nombres premiers (et premiers entre eux.) Rem

Définition 1 : On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si ses seuls diviseurs positifs sont 1 et p.

Remarque 2 : $(\mathbb{Z}, +, \times)$ est euclidien donc principal, ses idéaux sont les $(n\mathbb{Z})_{n\in\mathbb{N}}$. Dire que $p\in\mathbb{P}$ c'est dire que $p\mathbb{Z}$ est un idéal maximal.

Exemple 3 : Les premiers nombres premiers sont 2, 3, 5, 7, 11... mais 6 par exemple n'est pas premier car $6 = 2\times 3$

Théorème 4 : (Euclide) Tout entier relatif $n\in\mathbb{Z}\setminus\{-1,0,1\}$ a au moins un diviseur premier.

Définition 5 : Soit A un anneau. On dit que A est factoriel s'il vérifie :
i) A est intègre
ii) $\forall a\in A\setminus\{0\}$, $a = u p_1 \dots p_r$ avec $u\in A^\times$ et $p_1, \dots, p_r$ irréductibles.
iii) Cette décomposition est unique à permutation près et à des inversibles près : si $a = u p_1 \dots p_r = v q_1 \dots q_s$ alors $r = s$ et il existe $\sigma\in S_r$ tel que p_i et $q_{\sigma(i)}$ sont associés.

Théorème 6 : Si A est euclidien, alors A est factoriel.

Exemple 7 : $\mathbb{Z}$ muni de l'application $v(n) = |n|$ est euclidien.

Corollaire 8 : $\mathbb{Z}$ est un anneau factoriel.

B Arithmétique Romb

Définition 8 : On définit le pgcd (resp ppcm) d'une famille d'éléments comme le plus grand diviseur (resp le plus petit multiple) commun à chacun de ses éléments.

Exemple 9 : $\mathrm{pgcd}(3,6) = 3$ $\mathrm{pgcd}(2,3,6) = 1$ $\mathrm{ppcm}(2,3) = 6$.

Lemme 10 (Gauss) : Deux éléments non nuls a, b de $\mathbb{Z}$ sont premiers entre eux si et seulement si pour tout $c\in\mathbb{Z}$, $a \mid bc \Rightarrow a \mid c$.

Application 11 : Pour $p\in\mathbb{P}$ et $k\in[\![1, p-1]\!]$, on a $p \mid \binom{p}{k}$

Théorème 12 (Bézout) :
Soit $n\geq 2$ et $a_1, \dots, a_n$ des entiers relatifs. Si $\mathrm{pgcd}(a_i) \overset{\Delta}{=} d$ alors il existe des entiers relatifs $u_1, \dots, u_n$ tels que $\sum u_i a_i = d$.
Les (a_i) sont premiers entre eux si et seulement si il existe $u_1, \dots, u_n$ des entiers relatifs tels que $\sum u_i a_i = 1$.

C Répartition des nombres premiers. Rem (cours et exo)

Théorème 13 (Euclide) : L'ensemble $\mathbb{P}$ est infini.

Définition 14 : Soit $n\in\mathbb{N}^*$, on note $\mathbb{P}_n = \mathbb{P}\cap[\![1, n]\!]$ et $\pi(n) = |\mathbb{P}_n|$.

Remarque 15 : $\lim\limits_{n\to+\infty} (\pi(n)) = +\infty$

Théorème 16 (admis) : $\pi(n) \underset{+\infty}{\sim} \dfrac{n}{\ln n}$

Corollaire 17 (minoration de Legendre) : $\lim\limits_{n\to+\infty} \dfrac{\pi(n)}{n} = 0$

Proposition 18 : Soit $n\geq 2$, alors il existe n entiers consécutifs non premiers

Exemple 19 : $n_k = (n+1)! + k$ pour $k\in[\![2, n+1]\!]$.

Lemme 20 : En notant p_n le $n$ième nombre premier, on a $2^{n-1} \leq p_n \leq 2^{2^{n-1}}$ et $p_n \sim n\ln n$ et si $n\geq 2$ alors $\pi(n) > \ln(\ln(n))$.

Théorème 21 : $\sum\limits_{n=1}^{+\infty} \dfrac{1}{p_n} = +\infty$

II Tests de primalité Rem

On considère $n\geq 2$

Théorème 22 : Si n n'est pas premier alors n admet un diviseur premier p tel que $2\leq p\leq\sqrt{n}$.

Corollaire 23 : Le théorème précédent donne un premier algorithme pour savoir si un entier $n \geq 2$ est premier. On effectue successivement la division euclidienne de n par tous les entiers $d \leq \sqrt{n}$: si l'une de ces divisions donne un reste nul, n est composé. Sinon il est premier.

Application 24 : Crible d'Eratosthène
Soit n la partie entière de $\sqrt{n}$, on se donne la liste $[\![2, n]\!]$, on garde 2 et on supprime les multiples de 2 de cette liste, pareil pour 3 et pour tous les autres nombres premiers $p \leq \sqrt{n}$.

Théorème 25 : (Euler) Soit $a \in \mathbb{Z}$ premier avec n, alors $a^{\varphi(n)} \equiv 1 \ [n]$

Théorème 26 (petit théorème de Fermat) : Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tels que $p \nmid a$, alors $a^{p-1} \equiv 1 \ [p]$

Développement (Sophie Germain) Soit p premier impair tel que $q = 2p+1$ soit premier. Alors $\exists (x,y,z) \in \mathbb{Z}^3$ tel que $q \nmid xyz$ et $x^p + y^p + z^p = 0$.

Théorème 27 (Wilson) : $n \in \mathcal{P} \iff (n-1)! \equiv -1 \ [n]$

Théorème 28 : $n \in \mathcal{P} \iff \forall \alpha \in \mathbb{N}^*, \varphi(n^\alpha) = (n-1) n^{\alpha-1} \iff \varphi(n) = n-1$.

III Applications en algèbre

A Théorie de Sylow

Soit G un groupe fini d'ordre n et $p \in \mathcal{P}$ diviseur de n. On notera $n = p^\alpha m$, $p \nmid m$

Définition 29 : Si G est un groupe de cardinal $n = p^\alpha m$, $p \nmid m$, on appelle p-sous groupe de Sylow de G un sous groupe de cardinal p^α.

Remarque 30 : Dire que P est un p-sous groupe de Sylow de G signifie :
i) P est un p-groupe
ii) $[G : P]$ est premier à p.

Exemple 31 : Soit $G = GL_n(\mathbb{Z}_p)$, alors $|G| = (p^n - 1) \cdots (p^n - p^{n-1}) = m p^{\frac{n(n-1)}{2}}$ avec $m \wedge p = 1$, et le sous groupe des matrices triangulaires supérieures de diagonale unitaire est un p-sous groupe de Sylow de G.

Lemme 32 : Soit $H < G$, S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Théorème 33 (Sylow 1) Soit G un groupe fini et p un diviseur (premier) de $|G|$, alors G contient au moins un p-sous groupe de Sylow.

Corollaire 34 : G contient des sous groupes d'ordre p^i pour tout $i \leq \alpha$.

Théorème 36 (Sylow 2)
i) Si H est un sous groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$.
ii) Les p-Sylow sont tous conjugués (et donc leur nombre k divise m).
iii) On a $k \equiv 1 \ [p]$ (donc $k \mid m$)

Corollaire 37 : Si S est un p-Sylow de G on a :
$S \lhd G \iff S$ est l'unique p-Sylow de $G \iff k = 1$.

Application 38 : un groupe d'ordre 63 n'est pas simple.

B Propriétés des corps finis Rom

Définition 39 : Soit A un anneau commutatif unitaire. Il existe un unique entier positif appelé caractéristique de A, noté $\text{car}(A)$, tel que le sous anneau premier de A est isomorphe à $\mathbb{Z}/\text{car}A\,\mathbb{Z}$

Proposition 40 : Soit K un corps fini, alors $\text{car}(K) \in \mathcal{P}$.

Définition 41 : Pour tout $n \in \mathbb{N}^*$ on note $\mathcal{U}_n(p)$ l'ensemble de tous les polynômes unitaires irréductibles de degré n dans $\mathbb{Z}_p[X]$ et $I_n(p)$ le cardinal de $\mathcal{U}_n(p)$.

Proposition 42 : Pour tout $P \in \mathcal{U}_n(p)$, le quotient $\mathbb{Z}_p[X]/(P)$ est une $\mathbb{Z}_p$-algèbre de dimension n et de base $(\bar{X}^k)_{0 \leq k \leq n-1}$ et c'est un corps fini de cardinal p^n.

Exemple 43 : $\forall \lambda \in \mathbb{Z}_p$, $X - \lambda \in \mathcal{U}_1(p)$ donc $I_1(p) = p$ et tous ces corps $\mathbb{F}_p[X]/(X-\lambda)$ sont isomorphes à $\mathbb{Z}_p$
Comme $P = X^2 + \lambda X + \mu$ est irréductible si et seulement si non racines, $I_2(p) = \frac{p(p-1)}{2}$

Lemme 44 : En notant $P_n = X^{p^n} - X \in \mathbb{Z}_p[X]$, tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, pour tout diviseur d de n, tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.

Théorème 45 : Le polynôme $P_m(X) = X^{p^m} - X$ est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en facteurs irréductibles :
$$X^{p^m} - X = \prod_{d \mid m} \prod_{P \in \mathcal{U}_d(p)} P$$

Théorème 46 : A isomorphisme près, il existe un unique corps à p^m éléments c'est le corps $\mathbb{F}_{p^m} = \mathbb{F}_p[X]/(P)$ où $P \in \mathcal{U}_m(p)$.

Exemple 47 : $\mathbb{F}_1 = \mathbb{Z}_2$, $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+1)$.

C Critères d'irréductibilité des polynômes. Pcc

Définition 48 : On définit pour $P \in A[X]$, $P \neq 0$, le contenu de P noté $c(P)$: si $P(X) = a_n X^n + \dots + a_0$ on pose $c(P) = \text{pgcd}(a_0, \dots, a_n)$, l'élément $c(P)$ est défini modulo A^*. Si $c(P) = 1$, on dit que P est primitif.

Lemme 49 (Gauss) : On a $c(PQ) = c(P)c(Q)$ modulo $A^\times$.

Proposition 50 : Les polynômes $P(X) \in A[X]$ irréductibles dans $A[X]$ sont :
i) les constantes $p \in A$, irréductibles dans A.
ii) les polynômes $P(X)$, de degré ≥ 1 primitif et irréductibles dans $\text{Frac}(A)[X]$

Développement (critère d'Eisenstein)
Soit A un anneau factoriel et soit $K = \text{Frac}(A)$. Soit $P(X) = a_n X^n + \dots + a_0$ avec $a_i \in A$. Soit $p \in A$ un élément irréductible. On suppose :
i) $p \nmid a_n$ ii) $\forall i \in [\![0, n-1]\!]$ $p \mid a_i$ iii) $p^2 \nmid a_0$
Alors P est irréductible dans $K[X]$ (et donc dans $A[X]$ si $c(P) = 1$).

Application 51 : Soit p un nombre premier et $\Phi(X) = X^{p-1} + \dots + X + 1$. Alors Φ est irréductible dans $\mathbb{Q}[X]$ (et donc sur $\mathbb{Z}[X]$ puisque $c(\Phi) = 1$).

D Résidus quadratique et symbole de Legendre. Pcc Callero

Définition 52 : Soit $p \in \mathcal{P}$ on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_q\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$

Proposition 53 : pour $p = 2$ on a $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon $|\mathbb{F}_p^2| = \frac{p+1}{2}$

Proposition 54 (caractérisation des carrés)
On suppose $p > 2$. Alors on a : $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$

Exemple 55 : Dans $\mathbb{Z}_7$, 2 est un carré mais pas 7.

Corollaire 56 : Soit $p \in \mathcal{P}$, $p > 2$. On pose $q = p^n$ $m \in \mathbb{N}^*$. Alors, -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 [4]$.

Application 57 : Il existe une infinité de nombres premiers de la forme $4m+1$.

Définition 58 : On dit que le non multiple de $p \in \mathcal{P}$ impair est un résidu quadratique modulo p si il est un carré dans $\mathbb{F}_p^*$. Pour $a \in \mathbb{F}_p^*$, le symbole de Legendre est l'entier $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon} \end{cases}$

Proposition 59 : i) pour tout $a \in \mathbb{F}_p^*$ on a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) [p]$.
ii) L'application : $\mathbb{F}_p^* \to \{-1, 1\}$, $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1, 1\}$.

Corollaire 60 : Si $m = \pm \prod_i p_i^{\alpha_i}$ alors $\left(\frac{m}{p}\right) = (\pm 1) \prod_i \left(\frac{p_i}{p}\right)^{\alpha_i}$

Proposition 61 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Théorème 62 (Loi de réciprocité quadratique) Soit p et q deux nombres premiers impairs distincts, alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Exemple 63 : $\left(\frac{-1}{83}\right) = 1$ donc -1 est un résidu quadratique modulo 83.

$\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383.

$\left(\frac{2}{5}\right) = -1$ donc 2 n'est pas un résidu quadratique modulo 5.

Références

X G Algèbre

Rombaldi : Mathématiques pour l'agrégation

D. Perrin Cours d'Algèbre

Oraux X ENS algèbre 1 2007 Francinou

Eventuellement remplacer III. A Sylow

par III. A Equations diophantiennes.

Mettre alors Sophie Germain dans cette partie.

N2H2G tome I Caldero.