Leçon 121 : Nombres premiers. Applications

Développements :

Théorème de Chevalley-Warning, Théorème des deux carrés.

Bibliographie :

Rombaldi, Gourdon, Demazure,Perrin, Gozard, Calais, Combes, Escoffier.

Rapport du jury :

Le sujet de cette leçon est très vaste. Aussi les choix devront être clairement motivés. La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers est un résultat historique important qu'il faudrait citer. Sa démonstration n'est bien sûr pas exigible au niveau de l'agrégation. Quelques résultats sur les corps finis et leur géométrie sont les bienvenus, ainsi que des applications en cryptographie.

1 Arithmétique dans $\mathbb{Z}$.

1.1 Nombres premiers, premiers entre eux.

Définition 1 (Romb p301)**.** *Nombre premier.*

Notation : P l'ensemble des nombres premiers positifs.

Proposition 2 (Romb p301)**.** *Tout entier relatif $n \neq 0, 1, -1$ a au moins un diviseur premier.*

Proposition 3. *L'ensemble des nombres premiers est infini.*

Définition 4 (Gourdon 2009)**.** *a et b sont premiers entre eux si pgcd$(a, b) =$.*

Théorème 5 (Gourdon 2)**.** *Théorème de Gauss.*
+Si a et b sont premiers entre eux et a|c et b|c alors ab|c.

Théorème 6 (Romb p303)**.** *p premier divise $\prod n_k$ si et seulement si p divise l'un des n_k.*

Théorème 7 (Gourdon)**.** *Théorème de Bezout.*

Application 8 (Gourdon 2)**.** *p|pparmik pour $k \in \{1..p-1\}$. (Sert pour le Frobenius)*

Proposition 9 (Romb p302)**.** *Soit p un nombre premier. Soit p divise n soit p est premier avec n.*

Remarque 10 (Romb p302)**.** *Un test naïf pour savoir si n est premier revient à calculer la division euclidienne de n par d pour tout $1 \leq d \leq \sqrt{n}$.*

1.2 Décomposition en facteurs premiers

Théorème 11 (Romb p304)**.** *Théorème fondamental de l'arithmétique. Décomposition unique à l'ordre près.*

Application 12 (Romb p338)**.** *Si p et q premiersalors $\ln(p)/\ln(q)$ est irrationnel.*

Remarque 13 (Romb p304)**.** *$\mathbb{Z}$ est factoriel.*

Proposition 14 (Romb p305)**.** *Nombre de diviseurs d'un entier.*

Théorème 15 (Romb p305)**.** *Expression du pgcd et du ppcm avec cette forme.*

Application 16 (Gourdon 2 p12)**.** *[Romb p337] Il existe une infinité de nombres premiers de la forme $6k-1$. (On a besoin de la décomposition en facteurs premiers).*

1.3 Fonctions arithmétiques

Définition 17. *Une fonction arihtmétique est une fonction définie sur $\mathbb{N}^*$ et à valeurs dans $\mathbb{C}$.*

Exemple 18. *$d(n)$ le nombre de diviseurs positifs de n.*

Définition 19 (Demazure p55)**.** *$\phi(n)$ est le nombre d'entiers entre 0 et $n-1$ premiers avec n.*

Proposition 20 (Demazure p56)**.** *phi(p^r).*

Définition 21 (Romb p330)**.** *Fonction de Mobius.*

Définition 22 (Demazure p56)**.** *Fonction multiplicative.*

Proposition 23. *ϕ et μ sont multiplicative.*

Proposition 24 (Demazure p57)**.** *[Romb p282] Expression de $\phi(n)$ et $n = \sum_{d|n} \phi(d)$.*

Proposition 25 (Romb p332)**.** *Formule d'inversion de Mobius.*

Application 26. *Inversion de $\phi(n)$.*

Application 27 (Romb p332)**.** *Produit de deux séries absolument convergentes.*

1.4 Répartition des nombres premiers

Proposition 28 (Romb p302). *Crible d'Eratosthène.*

Théorème 29 (Gourdon p12). *[Romb] Théorème de Dirichlet faible. Si a et b sont premiers entre eux, il y a une infinité de nombres premiers de la forme $ak + b$.*

Théorème 30 (Romb p306). *[Admis]* $\pi(n) \sim \frac{n}{ln(n)}$.

Application 31 (Romb p312). $\sum_{p \in P} \frac{1}{p}$ *diverge.*

Application 32. *Exercices 11.10 , 11 et 12 Romb p345.*

2 Liens avec les orps finis

2.1 Anneau $\mathbb{Z}/n\mathbb{Z}$ et cryptographie

Proposition 33 (Gourdon 2 p9). $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si n est premier.*

Théorème 34 (Gourdon 2). *Théorème de Wilson.*

Théorème 35 (Gourdon p9). *[Demazure p62][Romb p281] Théorème de Fermat. Si a et n sont premiers entre eux alors* $a^{\phi(n)} = 1$ *modulo n. Cas particulier avec* $n = p$.

Proposition 36 (Demazure p66). *Test de primalité de Fermat. S'il existe a tel que* a^{n-1} *n'est pas congru à* 1 *modulo n avec* $a \in \{2, ..n-1\}$, *alors n n'est pas premier. Témoins de Fermat.*

Remarque 37 (Demazure p67). *Il existe des nombres premiers sans témoins de Fermat.*

Exemple 38 (Romb p328). *561*

Définition 39 (Romb p328). *Nombre de Carmichael.*

Théorème 40 (Demazure p68). *Critère de Miller Rabin*

Proposition 41 (Demazure). *Algorithme RSA.*

2.2 La primalité dans les corps finis

Définition 42 (Romb p415). *Caractéristique d'un corps.*

Proposition 43 (Romb p415). *La caractéristique est nulle ou un nombre premier.*

Définition 44 (Romb p416). *Sous-corps premier.*

Proposition 45. *Les seuls anneaux* $\mathbb{Z}/n\mathbb{Z}$ *qui sont des corps sont les* $F_p = \mathbb{Z}/p\mathbb{Z}$ *avec p premier.*

Proposition 46 (Perrin p72). *Si K est fini,* $car(K) = p > 0$. *Le sous-corps premier de K est* $\mathbb{Z}/p\mathbb{Z}$.

Proposition 47 (Romb p417). *Si K est un corps fini, il est de cardinal* p^n *où p est un nombre premier (la caractéristique). K est muni d'une structure de* F_p *ev de dimension finie n donc isomorphe à* F_p^n *en tant qu'ev. (K est une* F_p*-algèbre de dimension finie en tant que* F_p*-ev.).*

Remarque 48. *Il n'existe pas de corps de cardinal* 105.

Théorème 49 (Perrin p73). *Soit p premier et* $n \in \mathbb{N}^*$. *Il existe un corps de card* p^n. *Ce corps est unique à isomorphisme de* F_p*-algèbres près, on le note* F_{p^n}.

Remarque 50. *L'ensemble des éléments de* F_{p^n} *est solution de* $X^{p^n} - X = 0$. *Ce polynôme est scindé à racines simples sur* F_{p^n}.

Application 51 (Perrin p74). $F_{p^n}^*$ *possède un élément d'ordre* $p^n - 1$. *Il est donc cyclique.*

Application 52. *Théorème de Chevalley Warning et EGZ.*

Proposition 53 (Romb p417). *Tout sous-corps de* F_{p^n} *est de cardinal* p^d *où* $d|n$. *Pour tout diviseur d de n ; il existe un unique sous-corps de* F_{p^n} *de cardinal* p^d, *à savoir* $\{x \in F_{p^n}, x^{p^d} = x$.

Définition 54 (Romb p416). *Morphisme de Frobenius sur un corps de caractétistique p.*

Proposition 55. *Le morphisme de Frobenius est un automorphisme de* F_{p^n} *dont l'ensemble des points fixes est* F_p.

Théorème 56 (Romb p426). *Le groupe des automorphismes de* F_{p^n} *est cyclique d'ordre n engendré par l'automorphisme de Frobenius.*

2.3 Carrés dans F_q

Définition 57 (Perrin p74). F_q^2, F_q^{*2}.

Exemple 58. *Avec* $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$.

Proposition 59 (Perrin p74). *Pour* $p = 2$, $F_q^2 = F_q$.
Sinon, cardinaux.

Proposition 60 (Perrin p75). $x \in F_q^{*2} sietseulementsix^{(p-1)/2} = 1$.

Théorème 61 (Romb p428). *1. Nombre de carrés et de non carrés.*

2. *Les carrés de F_q^* sont les racines de $X^{(q-1)/2}-1$ et les non carrés sont les racines de $X^{(q-1)/2}+1$.*

Corollaire 62 (Romb p428). 1. *-1 est un carré dans F_q^* si et seulement si q est congru à 1 modulo 4.*
2. *Le produit de deux carrés ou de deux non carrés est un carré. Le produit d'un carré et d'un non carré est un non carré.*
3. *Pour tout $a,b \in F_q^*$ et tout $c \in F_q$, il existe $x,y \in F_q$ tels que $c = ax^2+by^2$.*

Application 63 (Perrin p76). *Il existe une infinité de nombres premiers de la forme $4m+1$.*

Application 64. *Le théorème des deux carrés.*

Définition 65 (Romb p429). *[Gozard p155] Symbole de Legendre.*

Proposition 66. *Le symbole de Legendre est une fonction multiplicative.*

Proposition 67. $(\frac{x}{p}) = x^{\frac{p-1}{2}}$.

Exemple 68 (Gozard p155). $(\frac{-1}{p}), (\frac{2}{p})$

Théorème 69. *Loi de réciprocité quadratique.*

Remarque 70. *La loi de réciprocité quadratique, les symboles pour -1 et 2 et la division euclidienne, permettent de calculer les symboles de Legendre.*

Exemple 71 (Gozard p156). $(\frac{23}{59} = -1$.

Corollaire 72. *L'équation $x^2+59y = 23$ n'a pas de solutions.*

2.4 Irréductibilité des polynômes

Proposition 73 (Perrin p77). *[Escoffier] Soit $P \in \mathbb{Z}[X]$ et p un nombre premier ne divisant pas le coefficient dominant de P. Si $\overline{P}$ est irréductible dans $F_p[X]$ alors P est irréductible dans $\mathbb{Z}[X]$.*

Contre exemple 74 (Perrin p78). *X^4+1 est irréductible sur $\mathbb{Z}$ mais est réductible sur F_p pour tout premier p.*

Théorème 75 (Perrin p76). *Critère d'Eisenstein.*

Exemple 76 (Perrin p77). *$X^{p-1}+..+X+1$ est irréductible sur $\mathbb{Z}$.*

Proposition 77. *Polynômes cyclotomiques.*

Théorème 78 (Romb). *Théorème de Dirichlet version faible.*

3 Nombres premiers en théorie des groupes

3.1 Résultats sur les p-groupes

Définition 79 (Romb p23). *p-groupe.*

Exemple 80. *$\mathbb{Z}/125\mathbb{Z}$ est un 5-groupe. D_4 est un 2-groupe.*

Proposition 81. *Un groupe d'ordre p premier est cyclique.*

Théorème 82 (Combes p45). *L'ordre est une puissance de p si et seulement si l'ordre de tout élément est une puissance de p. [Combes p 45]*

Théorème 83 (Romb p24). *Pour tout nombre premier p, le centre d'un p-groupe n'est pas trivial.*

Corollaire 84 (Romb p24). *Tout groupe d'ordre p^2 est abélien.*

Théorème 85. *Théorème de Cauchy. Si G est un groupe de cardinal et p premier divise n alors G admet un élément d'ordre p.*

3.2 Utilisation des p-Sylow pour trouver des sous-groupes distingués

Définition 86 (Calais p236). *p-sous-groupe de Sylow de G.*

Proposition 87 (Romb). *$card(GL_n(F_q)$.*

Proposition 88 (Romb). *Les matrices triangulaires d'éléments diagonaux égaux à 1 est un p-Sylow de $GL_n(F_q)$.*

Théorème 89 (Combes). *Théorème de Sylow*

Proposition 90 (Calais p238). *Un groupe fini G a un unique p-sous-groupe de Sylow si et seulement si S est distingué dans G.*

Application 91 (Calais p240). *Si G est un groupe fini d'ordre pq où p et q sont premiers distincts alors G n'est pas simple.*

Application 92. *Si G est un groupe fini d'ordre pq où $p<q$ sont premiers distincts et q non congru à 1 modulo p alors G est cyclique.*