121 – Nombres premiers. Applications.

Références : Gourdon Algèbre, Perrin, Rombaldi, X-ENS Algèbre 1

1 Arithmétique dans $\mathbb{Z}$

1.1 Division et nombres premiers entre eux

Définition 1. Soient a et b deux entiers relatifs. On dit que a divise b si il existe k $\in \mathbb{Z}$ tel que b=ak.

Définition 2. Soient $(a_1, a_2, ..., a_n)$ des entiers. Comme n$\mathbb{Z}$ est un idéal de l'anneau principal $(\mathbb{Z}, +)$, on peut définir le pgcd et le ppcm de la manière suivante :

- Il existe un unique entier d=pgcd$(a_1, a_2, ..., a_n)$ tel que $a_1\mathbb{Z}+a_2\mathbb{Z}+...+a_n\mathbb{Z} = d\mathbb{Z}$. d est aussi le plus grand entier qui divise tout les a_i.
- Il existe un unique entier m=ppcm$(a_1, a_2, ..., a_n)$ tel que $a_1\mathbb{Z} \bigcap a_2\mathbb{Z} \bigcap ... \bigcap a_n\mathbb{Z} = m\mathbb{Z}$. m est aussi le plus petit entier non-nul qui est multiple de tout les a_i.

Si pgcd$(a_1, a_2, ..., a_n)$=1, on dit que $(a_1, a_2, ..., a_n)$ sont premiers entre-eux.

Théorème 3 (Théorème de Bézout). *Soient $(a_1, a_2, ..., a_n)$ des nombres premiers entre eux. Alors il existe des entiers $(u_1, ..., u_n)$ tel que $1 = u_1a_1 + ... + u_na_n$*

Théorème 4 (Lemme de Gauss). *Si c divise ab et si a et b sont premiers entre eux, alors c divise b.*

Application 5. *Si p est premier, alors pour tout j compris entre 1 et p-1, p divise $\binom{j}{p}$.*

Proposition 6. *Si a est premier avec $(a_1, a_2, ..., a_n)$, alors a est premier avec le produit $(a_1a_2...a_n)$*

Proposition 7. *Soient $(a_1, a_2, ..., a_n)$ premiers entre eux deux à deux et b un entier. Le produit $a_1a_2, ...a_n$ divise b ssi a_i divise b pour tout i.*

1.2 Nombres premiers et premières applications

Définition 8. Un entier naturel p plus grand que 2 est dit premier si ses seuls diviseurs sont lui-même, 1 (et leurs opposés). Exemple : 3,5,7,13

Théorème 9. *Comme $\mathbb{Z}$ est un anneau factoriel, tout entier n> 1 dans $\mathbb{Z}$ s'écrit $n = \pm p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ avec $(p_1, p_2, ..., p_k)$ des nombres premiers, $(\alpha_1, \alpha_2, ..., \alpha_k)$ des entiers naturels non-nuls (α_i est appelé valuation p_i adique dans n.)*

Théorème 10. *Expression des pgcd (et ppcm) avec les valuations p-adiques.*

Corollaire 11. $a \vee b \; a \wedge b = |ab|$

Proposition 12.
- *Si p premier ne divise pas a, alors p et a sont premiers entre eux.*
- *Si p divise une produit $a_1a_2, ...a_n$, alors il divise au moins l'un des a_i.*

Théorème 13. *Il y a une infinité de nombres premiers.*

Théorème 14. *Répartition des nombres premiers (admis) : Le nombre d'entiers premiers inférieur ou égal à n est équivalent, quand n tend vers ∞, à $\frac{n}{ln(n)}$*

2 Lien avec les structures algébriques classiques

2.1 Lien avec la théorie des groupes

Proposition 15. *Si G est cyclique d'ordre n, tel que G =< g >, alors ses générateurs sont les g^k avec k premier avec n.*

Corollaire 16. *Un groupe de cardinal p premier est cyclique, engendré par n'importe lequel de ses éléments.*

Définition 17. Définition d'un p-groupe et des p-sylows.

Application 18. *Soit G un p-groupe (p premier plus grand que 2) qui opère sur un ensemble finie X. alors en notant $X^G = \{x \in X \mid G.x = \{x\}\}$, on a $\#(X^G) \equiv \#(X) \; [mod\ p]$*

Application 19. *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à 1.*

Théorème 20 (théorèmes de Sylow). *Soit G un groupe d'ordre $n = p^am$ avec p qui ne divise pas m. Alors :*
- *il existe un sous-groupe de G d'ordre p^a*
- *Les p-Sylows de G sont tous conjugués*
- *On note N_p le nombre de p-Sylows, il vérifie $N_p|m$ et $N_p \equiv 1 \pmod p$*

Application 21. *Soit G un groupe fini d'ordre $n = p^am$ avec p qui ne divise pas m. Si G possède un unique p-sylow, alors celui-ci est distingué dans G*

Application 22. *Un groupe d'ordre 63 n'est pas simple.*

2.2 Anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et conséquences arithmétiques

Proposition 23. *Soit G un groupe cyclique d'ordre n, alors il est isomorphe à* $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$

Définition 24. Soit A un anneau, l'application

$$\begin{aligned} \phi : \quad & \mathbb{Z} \to A \\ & n \mapsto n.1_A \end{aligned} \tag{1}$$

est un morphisme d'anneau. Il existe un entier n tel que $\ker(\phi) = n\mathbb{Z}$. Cet entier n s'appelle caractéristique de l'anneau A.

Proposition 25. *La caractéristique d'un anneau unitaire intègre est 0 ou un nombre premier.*

Application 26. *p est premier* $\iff$ $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *est intègre* $\iff$ $\frac{\mathbb{Z}}{p\mathbb{Z}}$ *est un corps.*

Théorème 27 (Théorème des restes chinois). *Théorème des restes chinois version* $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Définition 28. On définit la fonction indicatrice d'Euler : $\varphi(n) = \text{Card}(\{k \in [1,n], \ | \ k \wedge n = 1\})$

Remarque 29. $\varphi(n)$ est aussi égal au nombre de générateur d'un groupe cyclique d'ordre n, où encore à $\text{Card}((\frac{\mathbb{Z}}{n\mathbb{Z}})^\times)$

Définition 30. $((\frac{\mathbb{Z}}{n\mathbb{Z}})^\times,\times)$ est un groupe à $\phi(n)$ éléments, où ϕ est la fonction indicatrice d'Euler. $\phi(n)$ est aussi égal au nombre de générateur d'un groupe cyclique d'ordre n.

Proposition 31. *Si p est premier et n un entier naturel,* $\phi(p^n) = p^{n-1}(p-1)$

Théorème 32 (Théorème chinois). — $(n_1, ...n_r)$ *sont premiers entre eux deux à deux, ssi* $\mathbb{Z}/(n1...n_r)\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$. *On donne l'isomorphisme correspondant et son inverse !.*

Application 33. *Multiplicativité de la fonction d'Euler.*

Théorème 34 (Euler et petit théorème de Fermat). — *Soit k un entier premier avec n un entier non-nul. Alors* $k^{\phi(n)} \equiv 1 \ [mod\ n]$

— *Soit p un nombre premier et n un entier non-nul. Pour tout* $a \in \mathbb{Z}$, $a^p \equiv a \ [mod\ p]$ *et* $a^{p-1} \equiv 1 \ [mod\ p]$ *si* $pgcd(p,a) = 1$

Application 35. *Chiffrement RSA.*

Théorème 36 (Wilson). *Théorème de Wilson. Soit p> 1, p est premier ssi* $(p-1)! \equiv= -1 \ [mod\ p]$

Proposition 37. *Si p est premier plus grand que 2. Le groupe* $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times$ *est cyclique d'ordre p-1.*

Théorème 38. *Si p est premier plus grand que 2 et* $\alpha > 2$, *alors le groupe* $(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}})^\times$ *est cyclique d'ordre* $p^{\alpha-1}(p-1)$

2.3 Résultats sur les corps finis

— La caractéristique d'un corps fini est nécéssairement un nombre premier.
— Pour p premier, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps à p éléments, noté $\mathbb{F}_p$

Définition 39. On introduit l'application

$$\begin{aligned} F : \quad & \mathbb{F}_| \to \mathbb{F}_p \\ & x \mapsto x^p \end{aligned} \tag{2}$$

. Il s'agit d'un morphisme de corps, appelé morphisme de Frobenius.

Théorème 40 (Existence et unicité des corps finis). — *Soit F un corps finis, alors il existe p premier et* $n \in \mathbb{N}$ *tel que* $|F| = p^n = q$

— *Soit p premier et* $n \in \mathbb{N}$. *Alors le corps de décomposition de* $X^q - X$ *dans* $\mathbb{F}_p$ *est un corps finis à q éléments.*

— *Il est unique à isomorphisme près*

Corollaire 41. *Soit F un corps à* p^n *éléments. Soit A un sous-corps de F. A est un sous-corps de F de cardinal h ssi il existe d qui divise n tel que* $h = p^d$

Proposition 42. *Eventuellement compter le nombre de carrés dans* $\mathbb{F}_p$ *? Puis symbole de Legendre vers la réciprocité quadratique.*

3 Applications aux polynômes dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$

3.1 Des critères d'irréductibilités

Proposition 43. *Soit p premier.*
— *Soit A et B dans* $\mathbb{Z}[X]$, *alors* $(A + B)^p = \bar{A}^p + \bar{B}^p$ *dans* $\mathbb{F}_p[X]$.
— *Si A est dans* $\mathbb{Z}[X]$ *et* $B = A^p$, *alors on à l'égalité dans* $\mathbb{F}_p[X]$ *:* $\bar{B}(X) = \bar{A}(X^p)$

Définition 44. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. On appelle contenu de P l'entier c(p)=pgcd$(a_0, ..., a_n)$.

Proposition 45. — $c(PQ) = c(P)c(Q)$ *pour deux polynômes de* $\mathbb{Z}[X]$

- *Soit* P *un polynôme de* $\mathbb{Z}[X]$*, de degré* > 1*.* P *est irreductible dans* $\mathbb{Z}[X]$ *ssi* P *est de contenu 1 et* P *est irreductible dans* $\mathbb{Q}[X]$
- *Si* P,Q *sont deux polynômes unitaires de* $\mathbb{Q}[X]$ *tel que le produit* PQ *soit dans* $\mathbb{Z}[X]$*, alors* P *et* Q *sont dans* $\mathbb{Z}[X]$

Théorème 46 (Critère d'irreductibilité d'Eisenstein). *Soit* $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ *et* p *un nombre premier. On suppose que* $p|a_i \forall i \in \{0, ..., n-1\}$*,* p *ne divise pas* a_n *et* p^2 *ne divise pas* a_0*. Alors* P *est un polynôme irreductible de* $\mathbb{Z}[X]$

Exemple 47. $P_n(X) = X^n - p$ est un polynôme irreductible de $\mathbb{Q}[X]$ de degré n.

Théorème 48 (Réduction modulo p). *Réduction modulo* p*. Soit* $P = \sum_{i=0}^{n} a_k X^k$ *non constant dans* $\mathbb{Z}[X]$*,* p *premier,* $\bar{P} = \sum_{i=0}^{n} \bar{a_k} X^k$*. Si* p *ne divise pas* a_n *et* $\bar{P}$ *est irreductible dans* $\mathbb{F}_p[X]$*, alors* P *est irreductible dans* $\mathbb{Q}[X]$

Application 49. *Le polynôme* $X^3 + 462X^2 + 2433X - 67691$ *est irreductible sur* $\mathbb{Z}[X]$ *(et donc sur* $\mathbb{Q}[X]$*.*

3.2 Les polynômes cyclotomiques

Définition 50. On définit le nème polynôme cyclotomique Φ_n tout en introduisant les racines nèmes primitives de l'unité. Le degré de Φ_n est $\varphi(n)$

Théorème 51. *On a* $X^n - 1 = \Pi_{d|n} \Phi_d(X)$ *et* $\Phi_n(X)$ *est unitaire dans* $\mathbb{Z}[X]$

Application 52 (Progression arithmétique de Dirichlet)**.** *Soit* a, n *tel que* $a \wedge n = 1$*. Alors il existe une infinité de nombres premiers tel que* $p \equiv a \pmod{n}$

Théorème 53. *Pour tout entier naturel n plus grand que 1,* Φ_n *est irreductible dans* $\mathbb{Q}[X]$*, donc dans* $\mathbb{Q}[X]$

Application 54. *Degré de l'extension cyclotomique. Soit* ω *une racine nème première de l'unité, on a* $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$