Leçon 121 : Nombres premiers. Applications

1 Généralités[GOU21]

1.1 Nombres premiers et premiers entre eux

Définition 1. On dit qu'un entier $p \in \mathbb{N}$ est premier lorsque $p \geqslant 2$ et ses seuls diviseurs sont 1 et p. L'ensemble des nombres premiers est noté $\mathcal{P}$.
Un entier est dit composé si $n \neq 0$ et il existe $a \in \mathbb{N}\backslash\{1, n\}$ tel que $a|n$.

Théorème 2. *Tout entier relatif $n \in \mathbb{Z}\backslash\{-1, 0, 1\}$ possède au moins un diviseur premier.*

Théorème 3. *Tout entier $n \geqslant 2$ qui est composé, possède au moins un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$.*

Définition 4. Deux entiers $a, b \in \mathbb{N}$ sont dits premiers premiers entre eux lorsque $\text{pgcd}(a, b) = 1$.

Théorème 5. *(Bézout) Soient $a, b \in \mathbb{Z}$, a et b sont premier entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Lemme 6. *Soit p premier, pour tout entier $n \in \mathbb{N}^*$ alors soit $p|n$, soit ils sont premiers entre eux.*

Lemme 7. *Deux nombres premiers distincts sont premiers entre eux.*

Lemme 8. *(Gauss) Soient $a, b, c \in \mathbb{Z}$, si $a|bc$ et a est premier avec b alors $a|c$.*

Théorème 9. *(Euclide) Si p premier divise un produit $ab \in \mathbb{N}$ alors ou bien $p|a$ ou bien $p|b$.*

Théorème 10. *(Fondamental de l'arithmétique) Pour tout entier $n \in \mathbb{N}^*$ il existe une unique suite $(v_p(n))_{p\in\mathcal{P}}$ telle que $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$. Cette écriture est appelée décomposition en produit de facteurs premiers de n.*

Définition 11. Dans la décomposition en facteurs premiers de n, l'entier $v_p(n)$ est appelé valuations p-adique de n.

Proposition 12. *Soit $n, m \in \mathbb{N}$ on a $n|m \iff \forall p \in \mathcal{P}, v_p(n) \leqslant v_p(m)$.*

Théorème 13. *Soient $n, m \geqslant 2$ des entiers, alors $pgcd(n, m) = \prod_{p\in\mathcal{P}} p^{\min(v_p(n),v_p(m))}$ et $ppcm(n, m) = \prod_{p\in\mathcal{P}} p^{\max(v_p(n),v_p(m))}$*

Proposition 14. *Soit p premier, pour tout $k \in [\![1, p-1]\!]$, le coefficient binomial $\binom{n}{k}$ est divisible par p. Ainsi pour tout $a, b \in \mathbb{Z}$ on a $(a+b)^p \equiv a^p + b^p [p]$.*

Proposition 15. *Soit $n \geqslant 2$ un entier, alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Théorème 16. *(Fermat) Soit $p \in \mathcal{P}$, alors pour tout $a \in \mathbb{Z}$ on a $a^p \equiv a[p]$. Si de plus $p \nmid a$ alors $a^{p-1} \equiv 1[p]$*

1.2 Répartition des nombres premiers

Remarque 17. (Crible d'Ératosthène) Ce procédé permet de compter le nombre d'entier premier jusqu'à un certain $n \in \mathbb{N}$, il consiste à écrire la liste des entiers et consiste en rayer les multiples des nombres précédents à partir de 2. Les nombres non rayés restants seront premiers.

Théorème 18. *(Wilson) Un entier $p \in \mathbb{N}$ est premier si et seulement si $(p-1)! \equiv -1[p]$.*

Exemple 19. Un nombre premier de la forme $2^p - 1$ avec $p \in \mathcal{P}$ est appelé nombre de Mersenne.

Proposition 20. *(Test de Lucas) Soit (Y_n) la suite définie par $Y_0 = 2$ et $Y_{n+1} = 2Y_n^2 - 1$. Si $n \geqslant 3$, alors $2^n - 1$ est premier si et seulement $(2^n - 1)|Y_{n-2}$.*

Exemple 21. Les nombres de Fermat sont les entiers de la forme $F_n = 2^{2^n} + 1$ avec $n \in \mathbb{N}$, ils sont premiers pour $n \in \{0, 1, 2, 3, 4\}$ mais pas pour n entre 5 et 32.

Proposition 22. *Il existe une infinité de nombres premiers de la forme* $6k - 1$ *avec* $k \in \mathbb{N}^*$.

Théorème 23. *(Dirichlet) Soient* $a, b \in \mathbb{N}$ *premiers entre eux, alors il existe une infinité de nombres premiers de la forme* $ak + b$ *avec* $k \in \mathbb{N}^*$.

2 Théorie des corps

Définition 24. Soit $\varphi : \mathbb{Z} \to \mathbb{K}\ ;\ n \mapsto 1 + \cdots + 1$ morphisme d'anneau. Son noyau est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec p premier ou $p = 0$. Ce nombre est appelé caractéristique de $\mathbb{K}$ noté $car(\mathbb{K})$

Proposition 25. *Soit* $\mathbb{K}$ *un corps de caractéristique* $p > 0$. *L'application* $F : \mathbb{K} \to \mathbb{K}\ ;\ x \mapsto x^p$ *est un morphisme de corps appelé morphisme de Frobenius.*

Théorème 26. *Soit* p *premier et* $n \in \mathbb{N}^*$, *on pose* $q = p^n$. *Il existe un corps* $\mathbb{K}$ *à* q *éléments, unique à isomorphisme près noté* $\mathbb{F}_q = D_{\mathbb{F}_p}(X^q - X)$.

Théorème 27. *Le groupe multiplicatif* $\mathbb{F}_q^*$ *est cyclique d'ordre* $q - 1$.

3 Applications

3.1 Irréductibilité des polynômes

Soit A anneau factoriel et $\mathbb{K}$ son corps des fractions.

Définition 28. Pour $P \in A[X]$ on définit son contenu $c(P)$ comme le pgcd de ses coefficients.

Proposition 29. *Pour* $P, Q \in A[X]\backslash\{0\}$ *on a* $c(PQ) = c(P)c(Q)$

Proposition 30. *Soit* $P \in A[X]$ *non constant, si* P *est réductible dans* $\mathbb{K}[X]$, *alors il existe* $Q, R \in A[X]$ *non constants tels que* $P = QR$.

Proposition 31. *Soient* $P, Q \in \mathbb{K}[X]$ *unitaires non constants tels que* $PQ \in A[X]$ *alors* $P, Q \in A[X]$.

Théorème 32. *(Critère d'Eisenstein) Soit* $P(X) = a_n X^n + \cdots + a_0 \in A[X]$ *et* $p \in A$ *irréductible. Si on a les conditions suivantes :*

1. $p \nmid a_n$,
2. $p \mid a_i$ *pour* $i \in \{0, \ldots, n-1\}$,
3. $p^2 \nmid a_0$

Alors P *est irréductible dans* $\mathbb{K}[X]$ *(donc si* $pgcd(a_i) = 1$ *il l'est dans* $A[X]$*).*

Exemple 33. Pour p premier dans $\mathbb{N}$, $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}$.
Pour tout $n \in \mathbb{N}^*$ le polynôme $X^n - 2$ est irréductible sur $\mathbb{Z}$.

Remarque 34. Le deuxième exemple nous donne l'existence d'extensions de $\mathbb{Q}$ de n'importe quel degré puis l'existence des nombres transcendants sur $\mathbb{R}$.

Théorème 35. *(Réduction) Soient* A *un anneau factoriel et* $\mathbb{K}$ *son corps des fractions,* I *idéal premier de* A *et* $B = A/I$ *intègre de corps des fractions Ł. Soit* $P(X) = a_n X^n + \cdots + a_0 \in A[X]$ *et* $\overline{P}$ *sa réduction modulo* I. *On suppose que* $\overline{a_n} \neq 0$ *dans* B. *Si* $\overline{P}$ *est irréductible sur* B *ou Ałors* P *est irréductible sur* $\mathbb{K}$.

Exemple 36. Si $A = \mathbb{Z}$ et $I = (p)$ avec p premier alors $B = \mathbb{F}_p$ est un corps. Par exemple $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ en réduisant modulo 2 dans $\mathbb{F}_2$.

Lemme 37. *Le polynôme* $X^p - X - 1$ *est irréductible sur* $\mathbb{F}_p$.

Théorème 38. *Soit* $P \in \mathbb{K}[X]$ *de degré* $n \in \mathbb{N}^*$, *alors* P *irréductible si et seulement si* P *n'a pas de racines dans les extensions de* $\mathbb{K}$ *de degré inférieur ou égal à* $n/2$.

Exemple 39. $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Définition 40. Une racine n-ième primitive de l'unité de $\mathbb{K}$ est un élément $\zeta \in \mathbb{K}$ tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour tout $d < n$. C'est un générateur de $\mu_n(\mathbb{K})$ de sorte qu'il y ait $\varphi(n)$ racines primitives de l'unité, leur ensemble est noté $\mu_n^*(\mathbb{K})$.

Définition 41. Le n-ième polynôme cyclotomique de $\mathbb{K}$ est $\Phi_n(X) \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$.

Remarque 42. Si $\zeta \in \mu_n^*(\mathbb{K})$ alors les ζ^d avec $pgcd(d,n) = 1$.
Le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 43. *On a* $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Proposition 44. *Dans* $\mathbb{Q}$ *on a* $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 45. *Le polynôme cyclotomique* $\Phi_n(X)$ *est irréductible sur* $\mathbb{Z}$ *donc sur* $\mathbb{Q}$.

3.2 $\mathbb{Z}[i]$ et théorème des 2 carrés[PER96]

Définition 46. On appelle anneau des entiers de Gauss l'anneau $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ muni de l'addition et multiplication usuelle.

Proposition 47. *L'anneau* $\mathbb{Z}[i]$ *est intègre et ses inversibles sont* $\mathbb{Z}[i]^* = \{-1, 1, -i, i\}$.

Proposition 48. *On pose* $\Sigma = \{n \in \mathbb{N} | n = a^2 + b^2, a, b \in \mathbb{N}\}$. *Cet ensemble est stable par multiplication*

Proposition 49. *L'anneau* $\mathbb{Z}[i]$ *est euclidien donc principal, pour le stathme* $N : a + ib \mapsto a^2 + b^2$.

Proposition 50. *On a* $p \in \Sigma \iff p$ *réductible dans* $\mathbb{Z}[i] \iff p = 2$ *ou* $p \equiv 1[4]$.

Applications 51. Il existe une infinité de nombre premier de la forme $4m + 1$.

Théorème 52. *Les irréductibles de* $\mathbb{Z}[i]$ *sont, à inversible près :*

1. *Les entiers premiers* $p \in \mathbb{N}$ *avec* $p \equiv 3[4]$,
2. *Les entiers de Gauss* $a + ib$ *tels que* $a^2 + b^2 \in \mathcal{P}$.

Dev 1 : Théorème des 2 carrés 50 et 52
Dev 2 : Eisenstein 29, 30, 31 et 32
Dev 3 : Polynômes cyclotomiques irréductibles 44 et 45

Références

[GOU21] Xavier GOURDON : Les maths en tête. Algèbre et probabilités. Ellipses, 2021.

[PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

[TAU07] Patrice TAUVEL : Corps commutatifs et théorie de Galois : cours et exercices. Calvage et Mounet, 2007.

RAPPORT DU JURY :
Le sujet de cette leçon est très vaste. Elle doit donc être abordée en faisant des choix qui devront être clairement motivés. On attend une étude purement interne à l'arithmétique des entiers, avec des applications dans différents domaines : théorie des corps finis, théorie des groupes, arithmétique des polynômes, cryptographie, etc. On peut définir certaines fonctions importantes en arithmétique, les relier aux nombres premiers et illustrer leurs utilisations. Il est recommandé de s'intéresser aux aspects algorithmiques du sujet (tests de primalité). 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 doit être évoquée : certains résultats sont accessibles dans le cadre du programme du concours, d'autres peuvent être admis et cités pour leur importance culturelle.