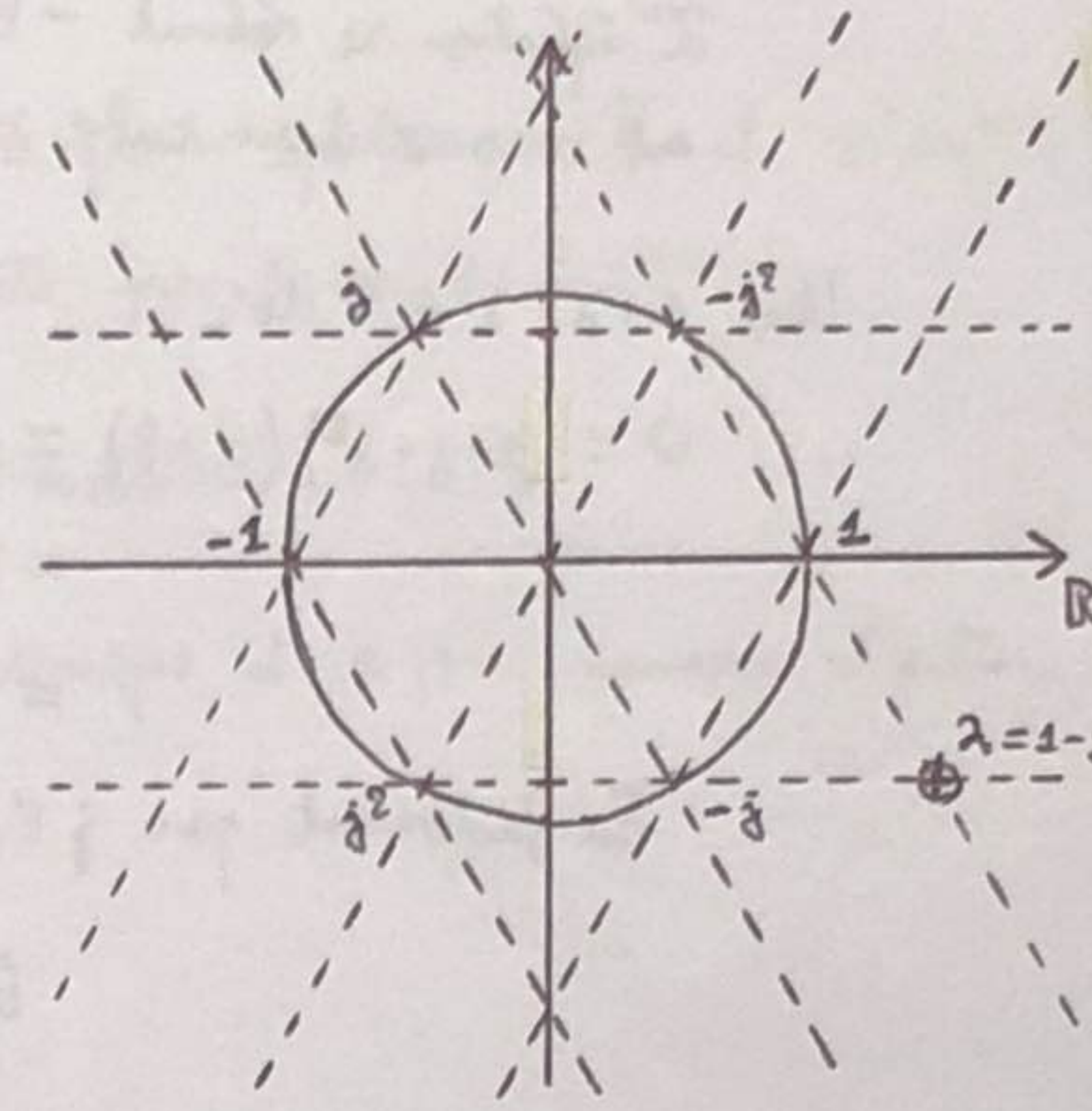
Leçons : 102, 122, 126.

Th de Fermat-Wiles, cas $n=3$

Énoncés :

- Lemme : Soit $\lambda = 1-j$ dans $\mathbb{Z}[j]$. λ est irréductible, et pour $\alpha \in \mathbb{Z}[j]$ tel que $\lambda \nmid \alpha$ on a $\alpha^3 \equiv \pm 1\ [\lambda^4]$.
- Th : L'équation $x^3+y^3=z^3$ n'admet aucune solution non triviale (cad tq $xyz \neq 0$) dans $\mathbb{Z}[j]$; en particulier dans $\mathbb{Z}$ non plus.

⊛ Lemme.



- $N(\lambda) = 1+1+1 = 3$: si $\lambda = \alpha\beta$ alors $3 = N(\alpha)N(\beta)$ dans $\mathbb{Z}$: l'un (disons $N(\alpha)$) est ± 1, et donc $\alpha \in \mathbb{Z}[j]^\times$.
  λ est bien irréductible.
- Soit $\alpha \in \mathbb{Z}[j]$: mq $\alpha \equiv 0\ [\lambda]$ ou $\alpha \equiv \pm 1\ [\lambda]$.
  On écrit $\alpha = a + jb$ avec $a, b \in \mathbb{Z}$: $\alpha \equiv a+b\ [\lambda]$.
  Mais $\lambda^2 = 1-2j+j^2 = -3j$ est associé à 3 :
  $a+b$ est congru à 0 ou ± 1 modulo 3, donc modulo λ^2, donc aussi modulo λ.
- Soit $\alpha \in \mathbb{Z}[j]$ tq $\lambda \nmid \alpha$: mq $\alpha^3 \equiv \pm 1\ [\lambda^4]$.
  Par ce qui précède $\alpha \equiv \pm 1\ [\lambda]$: quitte à prendre l'opposé on suppose $\alpha \equiv 1\ [\lambda]$ et on écrit $\alpha = 1+\beta\lambda$, $\beta \in \mathbb{Z}[j]$. On a $\alpha^3 - 1 = (\alpha-1)(\alpha-j)(\alpha-j^2) = \beta\lambda(\beta\lambda+1-j)(\beta\lambda+1-j^2) = \lambda^3 \cdot \beta(\beta+1)(\beta-j^2)$.
  $0, 1, -j^2$ sont deux à deux non congrus modulo λ, donc $\beta, \beta+1, \beta-j^2$ aussi. D'après ce qui précède l'un est multiple de λ, et alors $\lambda^4 \mid \alpha^3-1$. On a $\alpha^3 \equiv \pm 1\ [\lambda^4]$. □

⊛ Th.

- On suppose que l'on a $\alpha^3+\beta^3+\gamma^3 = 0$ dans $\mathbb{Z}[j]$ avec $\alpha\beta\gamma \neq 0$.
  - ↳ On se ramène à $\alpha\wedge\beta = \beta\wedge\gamma = \gamma\wedge\alpha = 1$.
    Quitte à diviser par $(\alpha\wedge\beta\wedge\gamma)^3$ on peut supposer que $\alpha\wedge\beta\wedge\gamma = 1$. Si alors $\delta \mid \alpha$ et $\delta \mid \beta$, par l'équation $\delta^3 \mid \gamma^3$ et $\delta \mid \gamma$; alors $\delta \mid 1$: $\alpha\wedge\beta = 1$. De même pour les deux autres.
  - ↳ Mq λ divise α, β ou γ.
    On suppose le contraire : d'après le lemme, $\pm 1 \pm 1 \pm 1 \equiv 0\ [\lambda^4]$, cad $\pm 1 \equiv 0\ [\lambda^4]$ ou $\pm 3 \equiv 0\ [\lambda^4]$.
    Mais d'une part $\lambda \nmid 1$, et d'autre part $\lambda^2 = -3j$ donc $\lambda^4 \nmid 3$. Contradiction.
    Donc α, β ou γ est multiple de λ : quitte à les permuter on peut supposer que c'est γ.
    L'équation se réécrit alors $\alpha^3+\beta^3+\lambda^{3n}\gamma'^3 = 0$ pour un certain $n \geq 1$ et avec $\lambda \nmid \gamma'$.
- On mq l'équation $\alpha^3+\beta^3+\varepsilon\lambda^{3n}\gamma^3 = 0$ en $\alpha,\beta,\gamma \in \mathbb{Z}[j]$ et $\varepsilon \in \mathbb{Z}[j]^\times$ tq $\begin{cases} \alpha\wedge\beta = \beta\wedge\gamma = \gamma\wedge\alpha = 1 \\ \lambda \nmid \alpha\beta\gamma \end{cases}$ n'a pas de solutions pour $n \geq 1$. Par l'absurde supposons qu'il en existe : soit $n \geq 1$ minimal tel que ce soit le cas. On va mq $n \geq 2$ et qu'il en existe encore pour $n-1$ ("descente infinie"), d'où une contradiction.
  - ↳ Mq $n \geq 2$.
    D'après le lemme, $\varepsilon\lambda^{3n}\gamma^3 \equiv \pm 1 \pm 1\ [\lambda^4]$. Si c'est ± 2, $\lambda^3 \mid 2$: absurde. Donc c'est 0 :
    $\lambda^4 \mid \varepsilon\lambda^{3n}\gamma^3$, cad $4 \leq 3n$: donc $n \geq 2$.

↳ On factorise l'équation en $-\varepsilon\lambda^{3m}\gamma^3 = (\alpha+\beta)(\alpha+j\beta)(\alpha+j^2\beta)$. $3m \geq 3$ donc au moins l'un des trois facteurs est multiple de λ^2. Les différences entre les facteurs sont $\beta - j\beta = \lambda\beta$, $j\beta - j^2\beta = j\lambda\beta$, $j^2\beta - \beta = j^2\lambda\beta$: elles sont associées à $\lambda\beta$ donc multiples de λ mais pas de λ^2. Le facteur multiple de λ^2 est donc unique, et les deux autres sont multiples de λ mais pas de λ^2. Quitte à multiplier β par une unité on peut supposer que le multiple de λ^2 est $\alpha+\beta$; on écrit alors, avec $\lambda \nmid \eta_1\eta_2\eta_3$: $\begin{cases} \alpha+\beta = \lambda^{3m-2}\eta_1 \\ \alpha+j\beta = \lambda\eta_2 \\ \alpha+j^2\beta = \lambda\eta_3 \end{cases}$.

Mq $\eta_1 \wedge \eta_2 = \eta_2 \wedge \eta_3 = \eta_3 \wedge \eta_1 = 1$. Par exemple soit $\delta \in \mathbb{Z}[j]$ tq $\delta | \eta_2$ et $\delta | \eta_3$.
D'une part $\lambda(\eta_2 - \eta_3) = j\beta - j^2\beta = j\lambda\beta$ donc $\eta_2 - \eta_3 = j\beta$ et $\delta | \beta$; d'autre part $\lambda(j^2\eta_2 - j\eta_3) = j^2(\alpha+j\beta) - j(\alpha+j^2\beta) = (j^2-j)\alpha + (j^3-j^3)\beta = -j\lambda\alpha$ donc $j^2\eta_2 - j\eta_3 = -j\alpha$ et $\delta | \alpha$. $\alpha\wedge\beta = 1$ donc $\delta | 1$: $\eta_2 \wedge \eta_3 = 1$. Pour les deux autres : pareil.

L'équation se réécrit $-\varepsilon\gamma^3 = \eta_1\eta_2\eta_3$. D'après ce que l'on vient de montrer, chaque η_i est associé à un cube : on écrit $\eta_i = \varepsilon_i\theta_i^3$ avec $\varepsilon_i \in \mathbb{Z}[j]^\times$ et $\theta_i \in \mathbb{Z}[j]$.

↳ $1+j+j^2 = 0$ donc :

$$\begin{aligned} 0 = (1+j+j^2)(\alpha+\beta) &= \alpha+\beta+j\alpha+j\beta+j^2\alpha+j^2\beta \\ &= (\alpha+\beta) + j(\alpha+j\beta) + j^2(\alpha+j^2\beta) \\ &= \lambda^{3m-2}\varepsilon_1\theta_1^3 + j\lambda\varepsilon_2\theta_2^3 + j^2\lambda\varepsilon_3\theta_3^3. \end{aligned}$$

En factorisant par $j\varepsilon_2\lambda$ on obtient, en posant $\varepsilon' = j\varepsilon_3\varepsilon_2^{-1}$ et $\varepsilon'' = \varepsilon_1(j\varepsilon_2)^{-1}$:

$$\theta_2^3 + \varepsilon'\theta_3^3 + \varepsilon''\lambda^{3(m-1)}\theta_1^3 = 0.$$

On a presque une solution pour $m-1$, il faudrait remplacer ε' par 1. Puisque $3(m-1) \geq 3$, cette égalité implique $\theta_2^3 + \varepsilon'\theta_3^3 \equiv 0\ [\lambda^3]$. Or d'après le lemme, $\theta_2^3, \theta_3^3 \equiv \pm 1\ [\lambda^3]$ (c'est vrai pour 4 donc pour 3). Alors $\pm 1 \pm \varepsilon' \equiv 0\ [\lambda^3]$. Si $\varepsilon' \in \{\pm j, \pm j^2\}$ on obtient $\pm 1 \pm j$ ou $\pm 1 \pm j^2$, qui sont (facile) associés à $\lambda = 1-j$. Puisque $\lambda^3 \nmid \lambda$, on a plutôt $\varepsilon' = \pm 1$. Si $\varepsilon' = 1$: on a une solution. Sinon : on en a une aussi en remplaçant θ_3 par son opposé. Ceci conclut. □

Complément : Propriétés de l'anneau $\mathbb{Z}[j]$, où $j = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$.

(i) Si $a, b \in \mathbb{Z}$, $N(a+jb) = a^2 - ab + b^2$.
(ii) $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\} = \mathbb{U}_6$.
(iii) $\mathbb{Z}[j]$ est euclidien pour N.

Preuve. (i) : $N(a+jb) = N\left((a - b/2) + i\sqrt{3}\, b/2\right) = (a-b/2)^2 + 3(b/2)^2 = a^2 - ab + b^2/4 + 3b^2/4 = a^2 - ab + b^2$.
(ii) : Soit $a+jb \in \mathbb{Z}[j]^\times$, cad tq $N(a+jb) = 1$, cad tq $(2a-b)^2 + 3b^2 = 4$. Si $b = 0$ on obtient $(2a)^2 = 4$ cad $a = \pm 1$, donc ± 1. Sinon on a forcément $b^2 = 1$. Si $b = 1$ on obtient $(2a-1)^2 + 3 = 4$ cad $2a-1 = \pm 1$, cad $a \in \{0, 1\}$, donc j ou $-j^2$. Si $b = -1$ on obtient $(2a+1)^2 + 3 = 4$ cad $2a+1 = \pm 1$, cad $a \in \{-1, 0\}$, donc j^2 ou $-j$. Réciproquement $\pm 1, \pm j, \pm j^2$ sont de norme 1.

(iii) : Il suffit de mq $\forall \xi \in \mathbb{Q}(j), \exists \gamma \in \mathbb{Z}[j], N(\xi - \gamma) < 1$. En effet si $\alpha, \beta \in \mathbb{Z}[j]$ avec $\beta \neq 0$ on pourra prendre $\gamma \in \mathbb{Z}[j]$ tq $N(\frac{\alpha}{\beta} - \gamma) < 1$ et donc $N(\alpha - \gamma\beta) < N(\beta)$: le quotient γ et le reste $\rho = \alpha - \gamma\beta$ conviendront.
Soit donc $\xi \in \mathbb{Q}(j)$: on écrit $\xi = x + jy$, $x, y \in \mathbb{Q}$. Soient a l'entier le plus proche de x, b l'entier le plus proche de y : $|x-a|$ et $|y-b|$ sont $\leq 1/2$. Alors : $N(\xi - (a+jb)) = N((x-a) + j(y-b)) = (x-a)^2 - (x-a)(y-b) + (y-b)^2$ $\leq 1/4 + 1/4 + 1/4 < 1$: $\gamma = a + jb$ convient. $\square$

Réf : • Hardy, Wright – An introduction to the theory of numbers : p 248.
• Hindry – Arithmetics : p 84 (réf alternative).
• Ireland, Rosen – A classical introduction to modern number theory : p 284 (réf alternative).

↳ C'est le cas $n = 3$ du th de Fermat – Wiles : pour $n \geq 3$, la grande équation de Fermat $x^n + y^n = z^n$ n'a aucune solution non triviale dans $\mathbb{Z}$. Le th général n'a été prouvé qu'en 1994.

↳ La clé ici est la factorialité de $\mathbb{Z}[j]$ (cq du fait qu'il est euclidien).

↳ Si ζ est une racine de l'unité, $\mathbb{Q}(\zeta)$ est appelé corps cyclotomique et a pour anneau d'entiers $\mathbb{Z}[\zeta]$. Celui-ci n'est en général pas factoriel.

↳ Ne pas inclure le lemme dans le DV : trop long.

↳ Mettre dans le plan le complément et le lemme.

↳ Ici pour la norme on suppose que l'on est parti de la définition générale comme déterminant et que l'on a donc (corps quadratique imaginaire) $N = |\cdot|^2$. On peut aussi partir de cette égalité comme définition. On a en particulier directement que N est multiplicative et que si $\alpha \in \mathbb{Z}[j]$, $\alpha \in \mathbb{Z}[j]^\times$ ssi $N(\alpha) = 1$ (mettre dans le plan également).

↳ DV très technique : attention !