Etude de l'équation de Fermat pour les premiers réguliers

Philippe Caldero

10 avril 2021

Résumé : On expose ici les idées du problème de mathématiques générales de l'agrégation externe de 2019. Au programme : la belle utilisation de l'unicité de la décomposition en idéaux premiers dans les anneaux d'entiers de corps de nombres, au service d'un théorème préparatoire sur l'équation de Fermat $x^p + y^p + z^p = 0$ quand p est un nombre premier dit « régulier ».

1 Prérequis

Les prérequis demandés dans ce qui suit dépassent d'une tête ceux exigés par l'agrégation et ses standards.

Parmi les éléments bien connus des agrégatifs, on aura besoin des nombres premiers, qui constituent un ensemble infini, et l'indicatrice d'Euler qui calcule le nombre $\varphi(n)$ des entiers de 1 à n premiers avec n :

$$\varphi(n) = n \prod_{p \in \mathcal{P}_n} \left(1 - \frac{1}{p}\right),$$

où $\mathcal{P}_n$ désigne l'ensemble des nombres premiers qui divisent n. Chose sans doute moins classique, l'ensemble $\mathcal{P}_n$ voit son cardinal majoré par $\log_2(n)$, puisque, bien évidemment, $2^{|\mathcal{P}_n|} \leq n$. En séparant $\mathcal{P}_n$ en $p = 2$ (éventuellement) et $p \geq 3$, on en déduit une minoration grossière de $\varphi(n)$:

$$\varphi(n) \geq n \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3})^{|\mathcal{P}_n|} \geq \frac{n 2^{\log_2(n)}}{2 \times 3^{\log_2(n)}} = \frac{n^2}{2n^{\log_2(3)}} = \frac{n^{2-\log_2(3)}}{2},$$

ce qui implique que $\varphi(n)$ tend vers l'infini avec n.

On utilisera également avec bonheur le théorème de Kronecker qui stipule qu'un polynôme unitaire de $\mathbb{Z}[X]$ n'ayant que des racines complexes de norme inférieure à 1 ne peut avoir pour racines que 0 ou des racines de l'unité. Ce théorème est rarement ignoré des agrégatifs vu le nombre de fois qu'il a été choisi comme développement, voir [**?**].

A ce sujet, on rappelle aussi que pour tout entier naturel n le polynôme cyclotomique ϕ_n, c'est-à-dire le polynôme minimal sur $\mathbb{Q}$, d'une racine primitive n-ième de l'unité, est

irréductible. Il est dans $\mathbb{Z}[X]$, irréductible également sur $\mathbb{Z}$, et de degré $\varphi(n)$. On se servira surtout du cas où $n = p$ premier $\phi_p = X^{p-1} + \cdots + X + 1$.

Parmi les objets *borderline* du programme d'agrégation figure la théorie des corps, et donc des extensions de corps. Une fois passées les jolies applications du théorème de la base télescopique se dresse devant nous la théorie de Galois, que les étudiants préfèrent en général éviter, ayant suffisamment de soucis avec le reste du programme pour se consacrer à cette théorie splendide, certes, mais chronophage. On peut tout de même, sans trop s'impliquer, l'utiliser comme ligne directrice dans des cas particuliers bien connus. On commence par l'extension $\mathbb{R} \subset \mathbb{C}$, de degré 2, dont chacun sait qu'elle est gouvernée par l'automophisme bar, puisque $\overline{z} = z$ pour un z de $\mathbb{C}$ implique que z est dans le corps de base $\mathbb{R}$. Ce *théorème de descente* propre à la théorie de Galois se retrouve dans les extensions (finies) de corps finis, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, avec p premier, puisque l'on sait qu'un élément de $\mathbb{F}_{p^n}$ est dans $\mathbb{F}_p$ si et seulement s'il est stable par le morphisme $z \mapsto z^p$ de Frobenius.

Dans le texte qui suit, on aura besoin des extensions cyclotomiques de $\mathbb{Q}$: ce sont les extensions $\mathbb{Q} \subset \mathbb{Q}(\zeta)$, où ζ est une racine p-ième de l'unité, avec p premier. Nul besoin de théorie de Galois pour prouver facilement qu'il existe, pour tout $1 \leq k \leq p-1$, un automorphisme σ_k du corps $\mathbb{Q}(\zeta) = \mathbb{Q}[\zeta] \simeq \mathbb{Z}[X]/(\phi_p)$ tel que $P(\zeta)$, $P \in \mathbb{Z}[X]$, est envoyé sur $P(\zeta^k)$. L'ensemble de ces automorphismes constitue un groupe pour la loi $\circ$ isomorphe au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ et tout $z \in \mathbb{Q}(\zeta)$ est dans $\mathbb{Q}$ si et seulement s'il est stable par les σ_k (et donc, juste par un générateur puisqu'on sait que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique), voir [**?**, Exercice XIII-E.33].

On utilisera également la notion d'élément entier sur l'anneau $\mathbb{Z}$. Un élément de $\mathbb{C}$ est dit entier algébrique sur $\mathbb{Z}$, ou juste entier algébrique, s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. On peut montrer [1] que la somme et le produit de deux entiers algébriques est encore entier algébrique, voir [**?**], c'est-à-dire que l'ensemble des entiers algébriques de $\mathbb{C}$ forme un anneau. Comme $\mathbb{Z}$ est factoriel, on voit facilement à l'aide du lemme de Gauss que l'anneau des entiers algébriques de $\mathbb{Q}$ est $\mathbb{Z}$ lui-même.

Aux confins de ces résultats sur la théorie des corps et l'intégralité, on trouve que la trace $\mathrm{tr}(z) := \sum_{k=1}^{p-1} \sigma_k(z)$ et la norme $N(z) := \prod_{k=1}^{p-1} \sigma_k(z)$ d'un élément z d'une extension $\mathbb{Q}(\zeta)$ de $\mathbb{Q}$ sont des entiers. En effet, par théorème de descente, ce sont des éléments de $\mathbb{Q}$ et par intégralité, ils sont dans $\mathbb{Z}$.

On arrive maintenant à ce qui sort totalement du programme de l'agrégation, mais qui, toutefois, reste facile à admettre tant cela généralise des résultats bien ingurgités. Les "petites" équations diophantiennes comme on peut les voir, notamment dans [**?**], citons par exemple certaines équations de Mordell, de Fermat pour n petit, ou le "problème des canards", jouent sur la factorialité de certains anneaux quadratiques, comme $\mathbb{Z}[i]$, $\mathbb{Z}[j]$, $\mathbb{Z}[i\sqrt{2}]$. Or, les exemples d'anneaux factoriels dans ce monde-là sont plutôt rares. Pire : il est difficile dans ce contexte de plonger un anneau intègre dans un anneau factoriel raisonnable. En revanche, les anneaux d'entiers de corps de nombres vérifient une propriété très analogue à la factorialité : à condition de remplacer la notion de nombre, resp. nombre premier, par la notion d'idéaux, resp. d'idéaux premiers, et la divisibilité par l'inclusion, selon le principe *diviser, c'est contenir*, on obtient l'unicité de la décomposition d'un idéal en produit d'idéaux premiers (à permutation près). C'est même finalement un peu plus

1. Une méthode exotique utilise le résultant.

joli que la factorialité des nombres, puisqu'on n'a pas à gérer les unités !

Si ζ est une racine p-ième de l'unité, alors, comme on va le voir dans le théorème 3.1, $\mathbb{Z}[\zeta]$ est l'anneau des entiers de $\mathbb{Q}(\zeta)$. On dira que le nombre premier p est régulier [2] si tout idéal I de $\mathbb{Z}[\zeta]$ est principal si et seulement si I^p est principal. Si l'on sait que le groupe abélien des idéaux (pour le produit) quotienté par le sous-groupe des idéaux principaux, est un groupe fini $\mathrm{Cl}(\mathbb{Q}(\zeta))$ (appelé groupe des classes d'idéaux du corps de nombres), alors, on comprend que p régulier revient à dire que p ne divise pas $|\mathrm{Cl}(\mathbb{Q}(\zeta))|$.

Voilà, ces quelques pages pourront intéresser ceux qui sont curieux de voir comment les idéaux ont remplacé les nombres de façon idéale et comment l'arithmétique s'est déployée autour de l'équation de Fermat, à tel point que l'on est en droit de se demander si on n'a pas tous été fermatés.

2 Les unités de $\mathbb{Z}[\zeta]$

2.1 Critère par la norme

Soit p un nombre premier impair. Comme ζ vérifie $X^p - 1 = 0$, c'est un entier algébrique et donc, $\mathbb{Z}[\zeta]$ est constitué d'entiers algébriques. On montrera plus tard qu'il s'agit exactement de l'anneau des entiers algébriques de $\mathbb{Q}(\zeta)$. En attendant, nous allons, comme il se doit dans les études d'anneaux, commencer par en étudier les unités, *i.e.* les inversibles.

Lemme 2.1. *Pour tout z de $\mathbb{Z}[\zeta]$, z est inversible dans $\mathbb{Z}[\zeta]$ si et seulement si $N(z) = \pm 1$.*

Démonstration. Comme z est dans $\mathbb{Z}[\zeta]$, il s'agit d'un entier algébrique et donc sa norme est dans $\mathbb{Z}$. S'il est inversible dans $\mathbb{Z}[\zeta]$, on peut écrire $zz' = 1$, avec $z' \in \mathbb{Z}[\zeta]$ et en prenant la norme qui est multiplicative, on voit que $N(z)N(z') = 1$, et donc, $N(z) = \pm 1$. Inversement, si $N(z) = \pm 1$, $z' := N(z) \prod_{\sigma \neq \mathrm{Id}} \sigma_k(z) \in \mathbb{Z}[\zeta]$ vérifie $zz' = N(z)N(z) = 1$.

2.2 Calculs de normes et traces

Il est temps de regarder de plus près les normes et traces d'éléments de $\mathbb{Z}[\zeta]$, nommément : ζ^k, $\lambda := 1 - \zeta$, $1 - \zeta^k$, $\lambda^k = (1 - \zeta)^k$. Voici un formulaire qui sera utile par la suite. On note N et tr respectivement la norme et la trace.

On a bien sur, $\mathrm{tr}(1) = p - 1$ et $N(1) = 1$, car 1 est stable par tous les σ_k, $1 \leq k \leq p - 1$.

$$N(\zeta^k) = 1,\ \mathrm{tr}(\zeta^k) = -1,\ 1 \leq k \leq p - 1.$$

On peut le faire par le calcul, mais cela provient surtout du fait que les conjugués de ζ, c'est-à-dire les ζ^k, $1 \leq k \leq p - 1$, sont les racines du polynôme unitaire irréductible $\phi_p = X^{p-1} + X^{p-2} + \cdots + 1$, donc la trace est la somme des racines et la norme est le produit des racines. On trouve bien $\mathrm{tr}(\zeta^k) = -1$ et $N(\zeta^k) = (-1)^{p-1} = 1$, d'après les relations coefficients racines.

$$N(1 - \zeta) = p,\ \mathrm{tr}(1 - \zeta) = p,\ N(1 + \zeta) = 1.$$

2. Notion introduite par Enrst Kummer en 1847.

Pour les normes, cela provient du fait que $1-\zeta$, resp. $1+\zeta$, est racine du polynôme de degré pair $\phi_p(1-X)$, resp. $\phi_p(X-1)$, dont l'évaluation en 0 est $\phi_p(1)=p$, resp. $\phi_p(-1)=1$. Pour la trace, on utilise juste sa linéarité.

$$N(1-\zeta^k)=p,\ \mathrm{tr}(\lambda^k)=p,\ 1\leq k\leq p-1.$$

Comme $1-\zeta^k$ est conjugué à $1-\zeta$, la première formule découle de $N(1-\zeta)=p$. La dernière formule s'obtient en utilisant le binôme de Newton $(1-\zeta)^k=1-\binom{k}{1}\zeta+\binom{k}{2}\zeta^2+\cdots+(-1)^k\binom{k}{k}\zeta^k$, en prenant la trace, et en remarquant que

$$-1+\binom{k}{1}-\binom{k}{2}+\cdots-(-1)^k\binom{k}{k}=-(1-1)^k=0$$

2.3 Les racines de l'unité dans $\mathbb{Z}[\zeta]$

Proposition 2.2. *L'ensemble des racines de l'unité de $\mathbb{Z}[\zeta]$ forme un sous-groupe G du groupe multiplicatif $\mathbb{Z}[\zeta]^*$ des unités de $\mathbb{Z}[\zeta]$. Ce groupe est fini, cyclique, d'ordre $2p$, engendré par la racine primitive $2p$-ième de l'unité $(-\zeta)$.*

Démonstration. Comme -1 est d'ordre 2 et ζ est d'ordre p impair, $-\zeta$ est d'ordre $2p$; il s'agit bien d'une racine primitive $2p$-ième de l'unité. De plus, G est clairement un groupe et donc $2p$ divise l'ordre de G, à condition que celui-ci soit fini !

Montrons que ce groupe est fini. Soit $\omega\in G$, ω est une racine de l'unité d'ordre, disons, m. On a $\mathbb{Q}\subset\mathbb{Q}(\omega)\subset\mathbb{Q}(\zeta)$, et donc

$$\varphi(m)=[\mathbb{Q}(\omega):\mathbb{Q}]\text{ divise }[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(p)=p-1.$$

Ainsi, $\varphi(m)$ est borné par $p-1$ et donc m est borné (vu dans la section des prérequis) et G est inclus dans la réunion des racines m-ièmes de l'unité pour $1\leq m\leq p-1$; G est donc fini. Comme G est un sous-groupe fini d'un corps, on sait qu'il est cyclique engendré par ω d'ordre, disons, n et l'on sait d'après ce qui précède, que $2p$ divise n. On sait de plus, d'après ce qui précède, que $\varphi(n)$ divise $p-1=\varphi(2p)$. Montrons alors que $n=2p$, ce qui achèvera la preuve.

Ecrivons donc $n=2^kp^lm$ avec m premier avec $2p$, ce qui donne

$$\varphi(n)=\varphi(2^kp^l)\varphi(m)=(p-1)2^{k-1}p^{l-1}\varphi(m),$$

et donc $\varphi(n)$ ne peut diviser $p-1$ que si $k=l=1$ et $\varphi(m)=1$, c'est-à-dire $m=1$ compte tenu du fait que m est impair. Conclusion, $n=2p$.

2.4 L'idéal maximal (λ)

Proposition 2.3. *On rappelle que $\lambda=1-\zeta$. On a les assertions suivantes :*

(i) les idéaux (λ^{p-1}) et (p) de $\mathbb{Z}[\zeta]$ sont égaux,

(ii) $(\lambda)\cap\mathbb{Z}=p\mathbb{Z}$,

(iii) on a un isomorphisme d'anneaux $\mathbb{Z}[\zeta]/(\lambda)\simeq\mathbb{F}_p$,

(iv) l'idéal (λ) de $\mathbb{Z}[\zeta]$ est un idéal maximal (donc premier),

(v) tout élément de $\mathbb{Z}[\zeta]$ peut s'écrire sous la forme $a + \lambda\beta$, avec $0 \leq a \leq p-1$ et $\beta \in \mathbb{Z}[\zeta]$.

Démonstration. Montrons (i). Pour cela, on pose $\omega_k := \frac{1-\zeta^k}{1-\zeta}$, $1 \leq k \leq p-1$, qui est bien dans $\mathbb{Z}[\zeta]$ par la formule de la série géométrique. On a $N(\omega_k) = \frac{N(1-\zeta^k)}{N(1-\zeta)} = 1$, et donc ω_k est un inversible de $\mathbb{Z}[\zeta]$ par le lemme 2.1. On en déduit que $\prod_{k=1}^{p-1} \omega_k$ est également inversible, or il vaut

$$\prod_{k=1}^{p-1} \omega_k = \frac{\prod_{k=1}^{p-1}(1-\zeta^k)}{\lambda^{p-1}} = \frac{N(1-\zeta)}{\lambda^{p-1}} = \frac{p}{\lambda^{p-1}}.$$

Montrons l'assertion (ii). Comme (λ) est un idéal de $\mathbb{Z}[\zeta]$ ne contenant pas 1, puisque $N(\lambda) > 1$, $(\lambda) \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ ne contenant pas 1. Or, il contient p, puisque $(p) = (\lambda^{p-1}) \subset (\lambda)$, par (i). L'assertion résulte du fait que $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$ car p est premier.

Pour l'assertion (iii), considérons le morphisme $\psi : \mathbb{Z}[X] \to \mathbb{Z}[\zeta]/(\lambda)$ qui envoie P sur la classe $P(\zeta) + (\lambda)$. Ce morphisme est clairement surjectif et nous allons montrer que son noyau est donné par $\mathrm{Ker}(\psi) = \{P \in \mathbb{Z}[X],\ P(1) \in p\mathbb{Z}\}$.

Pour l'inclusion directe, soit P dans $\mathrm{Ker}(\psi)$, alors $P(\zeta) = \lambda Q(\zeta)$, avec $\deg(Q) < \deg(\phi_p) = p-1$. Par la formule de Taylor polynomiale

$$P(1) = P(\zeta + \lambda) = P(\zeta) + \lambda P'(\zeta) + \cdots + \frac{1}{p!}\lambda^p P^{(p)}(\zeta) \in (\lambda).$$

On a donc bien $P(1) \in (\lambda) \cap \mathbb{Z} = p\mathbb{Z}$ par (ii).

Pour l'inclusion inverse, on suppose $P(1) \in p\mathbb{Z}$, et donc $P(1) \in (\lambda^{p-1}) \subset (\lambda)$. Encore une fois, on applique la formule de Taylor polynomiale pour trouver

$$P(\zeta) = P(1-\lambda) = P(1) - \lambda P'(1) + \cdots - \frac{1}{p!}\lambda^p P^{(p)}(1) \in (\lambda),$$

et ainsi, $P \in \mathrm{Ker}(\psi)$. D'où l'égalité.

Or, $\{P \in \mathbb{Z}[X],\ P(1) \in p\mathbb{Z}\}$ est exactement le noyau du morphisme surjectif $\psi' : \mathbb{Z}[X] \to \mathbb{F}_p$ qui envoie P sur $P(1)$ modulo p. Il en résulte que

$$\mathbb{Z}[\zeta]/(\lambda) \simeq \mathbb{Z}[X]/\mathrm{Ker}\psi = \mathbb{Z}[X]/\mathrm{Ker}(\psi') \simeq \mathbb{F}_p.$$

L'idéal (λ) est donc maximal, donc premier, puisque le quotient est un corps. D'où (iv).

Encore une fois, comme 1 n'est pas dans (λ), sa classe $\overline{1}$ est non nulle, et comme le groupe additif $\mathbb{Z}[\zeta]$ est d'ordre premier p, $\overline{1}$ est d'ordre p. Donc, tous les $\overline{a}$, $0 \leq a \leq p-1$, sont des classes deux à deux distinctes qui constituent l'ensemble $\mathbb{Z}[\zeta]/(\lambda)$, ce qui prouve (v).

2.5 Expression des unités de $\mathbb{Z}[\zeta]$

Proposition 2.4. *Tout élément inversible de $\mathbb{Z}[\zeta]$ peut s'écrire sous la forme $u = \zeta^r \varepsilon$ avec $r \in \mathbb{N}$ et ε un réel inversible de $\mathbb{Z}[\zeta]$.*

Démonstration. Soit u inversible dans $\mathbb{Z}[\zeta]$, avec $uu' = 1$, ce qui implique $\sigma_k(u)\sigma_k(u') = 1$ pour tout k, et donc tous les conjugués $u_k := \sigma_k(u)$ sont également inversibles. De plus, si P est un polynôme de $\mathbb{Z}[X]$ tel que $u = P(\zeta)$, il vient que $u_k = \sigma_k(u) = P(\zeta^k)$, et en particulier en prenant le conjugué complexe, on obtient

$$\overline{u_k} = \overline{\sigma_k(u)} = P(\overline{\zeta}^k) = P(\zeta^{p-k}) = u_{p-k}.$$

Soit donc $v_k = \sigma_k\left(\frac{u}{\overline{u}}\right) = \frac{u_k}{u_{p-k}}$. Les v_k sont des complexes conjugués de module 1 dans $\mathbb{Z}[\zeta]$. Il en résulte que le polynôme $P = \prod_{k=1}^{p}(X - v_k)$ est unitaire, à coefficients dans $\mathbb{Z}[\zeta]$, stables par les σ_k, donc dans $\mathbb{Z}$ (voir prérequis). Comme P n'a que des racines de module 1, le théorème de Kronecker assure que ses racines sont des racines de l'unité. Par la proposition 2.2, les v_k sont des racines $2p$-ièmes de l'unité. En particulier, $\frac{u}{\overline{u}} = e\zeta^m$, avec $e = \pm 1$.

Par la proposition 2.3, $u = a + \lambda Q(\zeta)$, pour $1 \leq a \leq p-1$, et pour un polynôme $Q \in \mathbb{Z}[X]$. De plus, a est non nul car $N(u)$ est inversible et $N(\lambda)$ ne l'est pas. Donc, $\overline{u} = a + \overline{\lambda}Q(\overline{\zeta}) = a - \zeta^{-1}\lambda Q(\overline{\zeta})$. Comme $\zeta = 1 - \lambda$, on en déduit que $\zeta^m = 1$ modulo (λ),

$$u = e\zeta^m \overline{u} = ea \mod (\lambda).$$

Par identification $ea = a$ et donc $e = 1$ car a est non nul.

On en déduit que $\frac{u}{\overline{u}} = \zeta^m$. Soit a et b deux entiers tels que la relation de Bezout $2a + bp = 1$ est vérifiée (rendu possible car p est impair), alors $\zeta^m = \zeta^{m(2a+bp)} = \zeta^{2am}$. Posons donc $\varepsilon = \zeta^{-am}u$. Il vient alors

$$\overline{\varepsilon} = \zeta^{am}\overline{u} = \zeta^{am}\zeta^{-m}u = \zeta^{am}\zeta^{-2am}u = \varepsilon.$$

Il résulte que ε est réel, et il suffit de poser $r = am$ pour conclure la proposition.

3 L'anneau des entiers de $\mathbb{Q}(\zeta)$

Théorème 3.1. *L'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$.*

Démonstration. On a déjà vu que tout élément de $\mathbb{Z}[\zeta]$ est un entier algébrique. Il reste à montrer la réciproque. Soit donc θ dans $\mathbb{Q}(\zeta)$, supposons θ entier algébrique et écrivons-le sous la forme $\theta = \sum_{k=0}^{p-2} a_k\zeta^k$, avec $a_k \in \mathbb{Q}$. Le but est donc de montrer que les a_k sont entiers.

Posons pour tout k de 0 à $p-2$, $b_k := \mathrm{tr}(\theta\zeta^{-k} - \theta\zeta)$. On trouve

$$b_k = \mathrm{tr}\left(\sum_{s=0}^{p-2} a_s\zeta^{s-k} - a_s\zeta^{s+1}\right) = a_k(p-1) - \sum_{s\neq k} a_s - \sum_{s=0}^{p-2}(-a_s) = (p-1)a_k + a_k = pa_k.$$

Comme b_k est la trace d'un entier algébrique, b_k est un entier. Il reste à montrer que p divise tous les b_k.

Notons tout d'abord que l'on peut écrire

$$p\theta = \sum_{k=0}^{p-2} b_k \zeta^k = \sum_{k=0}^{p-2} b_k (1-\lambda)^k = \sum_{k=0}^{p-2} c_k \lambda^k,$$

où $(c_k)_k$ est défini en fonction de $(b_k)_k$ selon l'automorphisme de $\mathbb{Z}[X]$ qui envoie P sur $P(1-X)$ (et donc, $(c_k)_k$ est une suite à valeurs dans $\mathbb{Z}$) ; comme il envoie bijectivement $p\mathbb{Z}[X]$ sur $p\mathbb{Z}[X]$, montrer que p divise tous les b_k revient à montrer qu'il divise tous les c_k.

En prenant la trace dans l'égalité $p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$, on obtient $p\,\mathrm{tr}(\theta) = (p-1)c_0 + p\sum_{k=1}^{p-2} c_k$, ce qui prouve que p divise c_0 puisque $\mathrm{tr}(\theta)$ est un entier. Soit $c_0 = pc_0'$.

Ecrivons maintenant l'égalité $p\theta = pc_0' + \sum_{k=1}^{p-2} c_k \lambda^k$, puis, en écrivant $p \in (\lambda^{p-1})$ par la proposition 2.3 (i), on considère l'égalité précédente modulo (λ^2), afin d'obtenir $\lambda c_1 = \lambda^2 \beta$, avec $\beta \in \mathbb{Z}[\zeta]$. Il en résulte que c_0 est divisible par λ et donc $c_0 \in (\lambda) \cap \mathbb{Z} = p\mathbb{Z}$. On montre ensuite par récurrence que tous les c_k sont dans $p\mathbb{Z}$ et on achève ainsi la preuve.

4 p-régulier et l'équation de Fermat

Théorème 4.1. *Soit $p > 3$ un nombre premier régulier, x, y, z trois entiers deux à deux premiers entre eux tels que $x^p + y^p + z^p = 0$, alors p divise xyz.*

Démonstration. On suppose par l'absurde [3] que x, y, z trois entiers deux à deux premiers entre eux tels que $x^p + y^p + z^p = 0$, et p ne divisant pas xyz.

On fixe $0 \leq k < l \leq p-1$, et on va montrer dans un premier temps que les idéaux $(x + \zeta^k y)$ et $(x + \zeta^l y)$ sont premiers entre eux. Par l'absurde, soit J un idéal premier les contenant tous les deux. Alors, en soustrayant, on obtient $x + \zeta^k y - x - \zeta^l y \in J$ et donc, $y(\zeta^k - \zeta^l) \in J$. En rappelant la preuve de la proposition 2.3 (i), on a $1 - \zeta^{l-k} = \lambda\beta$, avec β inversible, il vient que $\lambda y \zeta^k \beta \in J$ et donc, $\lambda y \in J$.

Si par l'absurde, y est dans J, alors $x \in J$, et donc $z^p \in J$, et $z \in J$ puisque J est un idéal premier. Donc, x, y, z sont tous trois dans $J \cap \mathbb{Z}$ qui est un idéal (strict : ni nul, forcément, ni $\mathbb{Z}$ sinon J contiendrait 1) de $\mathbb{Z}$, donc, de la forme $n\mathbb{Z}$. Ceci contredit le fait que les trois entiers sont premiers entre eux.

Donc, $y \notin J$, ce qui implique $\lambda \in J$ puisque J est premier. On a donc $(\lambda) \subset J$, et on obtient l'égalité des deux idéaux, par maximalité de (λ). Or,

$$x + y = x + \zeta^k y + (1 - \zeta^k) y = (x + \zeta^k y) + \lambda\gamma y \in J = (\lambda)$$

Résultat des courses : $x + y \in (\lambda) \cap \mathbb{Z} = p\mathbb{Z}$.

Réduisons l'égalité $x^p + y^p + z^p = 0$ modulo p, ce qui donne à l'aide du Frobenius $x + y + z = 0$ et donc $z = 0$. Donc p divise z, absurde par hypothèse.

3. Mettez les compteurs à zéro, ce n'est que le début qu'une longue suite d'absurdités. Welcome in Absurdland !

Il résulte que les idéaux $(x+\zeta^k y)$ et $(x+\zeta^l y)$ sont premiers entre eux[4]. Comme le produit des idéaux est égal à :

$$\prod_{k=0}^{p-1}(x+\zeta^k y) = (\prod_{k=0}^{p-1}(x+\zeta^k y)) = (x^p+y^p) = (z^p) = (z)^p,$$

et comme les idéaux du membre de gauche sont deux à deux premiers entre eux, il vient, en décomposant tous les idéaux en idéaux premiers, que les idéaux du membre de gauche sont tous les puissances p-ièmes d'idéaux. En particulier, il existe un idéal I tel que $(x+\zeta y) = I^p$.

Comme p est régulier, le fait que I^p soit principal implique que I est principal, disons $I = (\alpha)$, avec $\alpha \in \mathbb{Z}[\zeta]$. Ceci implique $(x+\zeta y) = (\alpha^p)$, et donc que $x+\zeta y$ et α^p sont égaux modulo un inversible. Par la proposition 2.4, on peut trouver un réel ε inversible de $\mathbb{Z}[\zeta]$ et un entier r tels que $x+\zeta y = \zeta^r \varepsilon \alpha^p$.

Il reste encore un dernier coup de collier pour atteindre une dernière absurdité.

Posons $\alpha = \sum_{k=0}^{p-2} a_k \zeta^k$, avec $a_k \in \mathbb{Z}$. Dans $\mathbb{Z}[\zeta]/(p)$, on a $\overline{\alpha}^p = \left(\sum_{k=0}^{p-2} a_k \overline{\zeta}^k\right)^p = \sum_{k=0}^{p-2} a_k^p \overline{\zeta}^{kp} = \sum_{k=0}^{p-2} a_k^p =: a$, avec $a \in \mathbb{Z}$. On en déduit que modulo (p)

$$x + y\zeta - x\zeta^{2r} - y\zeta^{2r-1} = \zeta^r \varepsilon \alpha^p - \zeta^r \varepsilon \overline{\alpha}^p = \zeta^r \varepsilon (a-a) = 0.$$

On voit que $r = 0$ est impossible, sinon, on aurait $y(1-\zeta^2) = p\beta$, avec $\beta \in \mathbb{Z}[\zeta]$. En prenant la norme, on aurait que p^{p-1} divise $y^{p-1}p$, donc p divise y contrairement aux hypothèses. De même $r \neq 1$.

Si $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ sont deux à deux distincts, ils sont $\mathbb{Z}$-libres, donc x et y seraient multiples de p, contrairement à l'hypothèse. On en déduit que modulo p, $r = 0$ ou 1, mais ceci est impossible, la seule possibilité qu'il reste est $2r = 1$ modulo p.

Conclusion, $x + y\zeta - x\zeta - y$ est dans l'idéal (p), ce qui peut s'écrire $\lambda(x-y) \in (p)$. En utilisant une dernière fois la norme, il vient que p^{p-1} divise $N(\lambda)(x-y)^{p-1} = p(x-y)^{p-1}$.

Ainsi, $x = y$ modulo p et de même on montrerait que $y = z$ modulo p. L'équation de Fermat donne alors $3z^p = 0$ modulo p et, comme $p > 3$, z est un multiple de p, ce qui achève la preuve dans une absurdité finale.

Remarque 4.2. Quels sont les p réguliers au fait ? Tout d'abord, le premier nombre premier irrégulier est 37, et la liste se prolonge avec 59, 67, etc... Plus généralement, on montre qu'un nombre premier p est régulier s'il ne divise pas les numérateurs des nombres de Bernoulli B_2, B_4,..., B_{p-3}. Si l'on en croit Wikipedia, on ne sait toujours pas si l'ensemble des nombres premiers réguliers est infini.

4. J'en vois qui suivent plus là !