

# Le théorème de Fermat

## pour $p$ régulier, $p \nmid xyz$

Stéphane Vinatier

Le dernier théorème de Fermat a été démontré par WILES en 1994, après plus de trois siècles d'efforts des mathématiciens théoriciens des nombres. Il s'agit de montrer que si  $n$  est un entier supérieur ou égal à 3, l'équation :

$$x^n + y^n = z^n$$

n'a pas de solution entière ( $x \in \mathbb{Z}$ ,  $y \in \mathbb{Z}$  et  $z \in \mathbb{Z}$ ) non triviale ( $xyz \neq 0$ ). Ce résultat n'a pas de conséquences mathématiques notables ; cependant, les recherches qui ont finalement abouti à sa résolution ont été sources de progrès considérables dans plusieurs domaines des mathématiques.

FERMAT (1601-1665) était lui-même en mesure de démontrer son théorème pour quelques petites valeurs de  $n$ , mais il ne pouvait soupçonner l'existence d'une difficulté cruciale pour  $n > 19$  : l'*anneau* dans lequel se font les calculs n'est alors plus *principal*. A son époque, les notions de groupe et d'anneau sont inconnues, le concept d'anneau non principal est à fortiori complètement hors d'atteinte.

Une étape importante vers la résolution a été franchie lorsque le mathématicien allemand KUMMER a introduit en 1846 la notion d'*idéaux* dans le but de remédier (partiellement) à cette difficulté : la propriété d'*unique factorisation en produit d'irréductibles* n'est pas vraie pour les éléments de l'anneau quand celui-ci n'est pas principal, mais elle est vraie pour les idéaux des anneaux qui interviennent ici. Nous allons voir comment cette notion permet de démontrer le *premier cas* ( $p \nmid xyz$ ) du théorème de Fermat pour un nombre premier  $n = p$  *régulier* (nous verrons plus loin ce que cela signifie, c'est une hypothèse qui « adoucit » le fait que l'anneau ne soit pas principal).

## 1 Echauffement

L'équation de Fermat pour  $n = 2$  a des solutions non triviales : on se ramène à  $(x/z)^2 + (y/z)^2 = 1$ , donc à chercher les points du cercle trigonométrique à coordonnées rationnelles (c'est-à-dire dans  $\mathbb{Q}$ ). On paramétrise le cercle en utilisant  $\cos \theta = \frac{1-t^2}{1+t^2}$  et  $\sin \theta = \frac{2t}{1+t^2}$ , où  $t = \tan(\theta/2)$  ; les valeurs rationnelles de  $t$  fournissent les solutions.

Dès lors, montrer que l'équation de Fermat n'a pas de solution pour  $n \geq 3$  se ramène à montrer qu'elle n'en a pas pour  $n = 4$  et pour tout nombre premier impair  $p$ . En effet,

$$x^{ab} + y^{ab} = z^{ab} \Rightarrow (x^a)^b + (y^a)^b = (z^a)^b,$$

et tout entier supérieur à 3 est divisible par 4 ou par un premier impair. Enfin, on se ramène aisément à montrer qu'il n'y a pas de solutions  $(x, y, z)$  avec  $x, y$  et  $z$  premiers entre eux. FERMAT a traité le cas  $n = 4$  à l'aide du principe de la « descente infinie » dont il est l'inventeur. Nous fixons désormais un premier impair  $p$  et considérons l'équation :

$$x^p + y^p = z^p, \quad x, y, z \in \mathbb{Z} \text{ premiers entre eux.}$$

Le raisonnement dans le premier cas du théorème ( $p \nmid xyz$ ) est très simple pour  $p = 3$  :

**Exercice 1.1** *Montrer que  $3 \nmid x$  entraîne que  $x^3 \equiv \pm 1 \pmod{9}$ ; faire de même pour  $y^3$  et  $z^3$ , en déduire que  $x^3 + y^3 = z^3$  est impossible si  $3 \nmid xyz$ .*

La même méthode s'applique pour  $p = 5$  en considérant des congruences modulo 25. Par contre, ça ne marche plus pour  $7$  :  $1^7 + 30^7 \equiv 31^7 \pmod{49}$ , et on peut montrer qu'il y a des solutions modulo toutes les puissances de 7.

Le second cas du théorème pour  $p = 3$  ( $3 \mid xyz$ ) est une bonne introduction aux méthodes qui serviront dans le premier cas pour  $p \geq 5$  régulier. Nous commençons donc par celui-ci.

## 2 Le second cas pour $p = 3$

Ici  $p = 3$  et on suppose qu'il existe une solution  $(x, y, z)$  de l'équation de Fermat avec  $x, y, z \in \mathbb{Z}$  premiers entre eux et  $3 \mid xyz$ . En écrivant

$$x^3 + y^3 + (-z)^3 = 0,$$

on voit que, quitte à permuter  $x, y$  et  $z$ , on peut supposer que 3 divise  $z$ , si bien que 3 ne divise pas  $x$  et  $y$ .

On revient à l'équation sous la forme  $x^3 + y^3 = z^3$ ; puisqu'il est divisible par 3, l'idée « naturelle » est de factoriser le membre de gauche. Pour cela, on introduit une *racine cubique de l'unité*, que l'on note  $j$  : c'est l'une des solutions non réelles de l'équation  $X^3 = 1$ , donc une solution de  $X^2 + X + 1 = 0$ .

**Exercice 2.1** *Vérifier que  $x^3 + y^3 = (x + y)(x + jy)(x + j^2y)$ .*

On note que  $1 + j + j^2 = 0$ , si bien que  $j^2 = -1 - j$ ; comme  $j^3 = 1$ , toutes les puissances positives de  $j$  s'écrivent  $a + bj$  avec  $a \in \mathbb{Z}$  et  $b \in \mathbb{Z}$ .

## 2.1 L'anneau $\mathbb{Z}[j]$

On est ainsi amené à travailler avec des nombres qui se trouvent dans l'anneau :

$$\mathbb{Z}[j] = \{a + bj, a \in \mathbb{Z}, b \in \mathbb{Z}\} ,$$

qu'on peut voir comme un sous-anneau de  $\mathbb{C}$ , c'est-à-dire que l'addition et la multiplication s'y font de la manière habituelle. Cet anneau est *principal*, ce qui entraîne que tout élément s'écrit de manière unique produit d'une *unité* par des *irréductibles*.

**Définition 2.2** Un anneau  $A$  est dit *intègre* si, pour  $a, b \in A$ ,  $ab = 0$  entraîne  $a = 0$  ou  $b = 0$ . Si tel est le cas, un élément  $a \in A$  est une *unité* s'il admet un inverse  $b \in A$  :  $ab = 1$  ; un élément  $a \in A$  est *irréductible* si  $a = bc$  avec  $b \in A$  et  $c \in A$  entraîne  $b$  est une unité ou  $c$  est une unité.

L'ensemble des unités de  $A$  est noté  $A^\times$ .

**Exemple 2.3** L'anneau  $\mathbb{Z}$  est intègre. Ses unités sont 1 et  $-1$  ; ses irréductibles sont les nombres premiers (et leurs opposés). Tout nombre entier s'écrit de manière unique  $\pm 1$  multiplié par des nombres premiers positifs :  $1728 = 2^6 \times 3^3$ .

De même,  $\mathbb{Z}[j]$  est intègre, car c'est un sous-anneau de  $\mathbb{C}$ . En plus de  $\pm 1$ , il admet  $j$  et  $j^2$  (et leurs opposés) comme unités, puisque  $j \times j^2 = 1$ . Ce sont les seules :

$$\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\} .$$

Pour prouver cette assertion, on introduit l'application *norme* :

$$\begin{aligned} N: \mathbb{Z}[j] &\longrightarrow \mathbb{Z} \\ a + bj &\longmapsto (a + bj)(a + bj^2) \end{aligned}$$

On note que comme  $j$  et  $j^2$  sont conjugués pour la conjugaison complexe ( $\{j, j^2\} = \{e^{2i\pi/3}, e^{-2i\pi/3}\}$ ), la norme est égale au carré du module :

$$N(a + bj) = (a + bj)\overline{(a + bj)} = |a + bj|^2 .$$

**Exercice 2.4** *Etablir l'égalité :  $N(a + bj) = (a + b)^2 - 3ab$ . En déduire que  $N(a + bj) = 1$  si et seulement si  $a + bj \in \{\pm 1, \pm j, \pm j^2\}$ .*

L'assertion sur  $\mathbb{Z}[j]^\times$  découle maintenant de la proposition suivante.

**Proposition 2.5** *Soit  $u \in \mathbb{Z}[j]$ , alors  $u \in \mathbb{Z}[j]^\times$  si et seulement si  $N(u) = 1$ .*

*Preuve.* Supposons que  $u$  soit une unité, alors il existe  $v \in \mathbb{Z}[j]$  tel que  $uv = 1$ , d'où  $N(uv) = N(1)$ , c'est-à-dire  $N(u)N(v) = 1$ . Il s'ensuit que  $N(u) = \pm 1$ , puis  $N(u) = 1$  car la norme est positive.

Supposons que  $N(u) = 1$ , alors  $u\bar{u} = 1$ , donc  $u$  est une unité. ■

La norme donne aussi un critère pour repérer les irréductibles de  $\mathbb{Z}[j]$  : si  $N(s)$  est premier, alors  $s$  est irréductible (exercice). Ainsi,  $1 - j$  est irréductible :

$$N(1 - j) = (1 - j)(1 - j^2) = 3 .$$

Notons au passage qu'on obtient la décomposition de 3 en produit d'une unité par des irréductibles :

$$3 = (1 - j)(1 - j^2) = j^2(1 - j) \times j(1 - j^2) = -j^2(1 - j)^2 .$$

Par contre, la réciproque n'est pas vraie : 5 est irréductible dans  $\mathbb{Z}[j]$ , mais  $N(5) = 5 \times 5 = 25$  n'est pas premier.

## 2.2 La descente infinie

On note  $\lambda = 1 - j$  et, pour  $s \in \mathbb{Z}[j]$ , on note  $v_\lambda(s)$  l'exposant de  $\lambda$  dans la décomposition de  $s$  en produit d'une unité par des irréductibles. Par exemple :

$$v_\lambda(\lambda) = 1, \quad v_\lambda(1 - j^2) = 1, \quad v_\lambda(3) = 2, \quad v_\lambda(j) = 0 .$$

De plus,  $v_\lambda(z) \geq 2$  car 3 divise  $z$ .

Le principe de la « descente infinie » est le suivant : à partir de notre solution  $(x, y, z)$  de l'équation de Fermat, on va construire une solution  $(x', y', z')$  de :

$$\begin{aligned} (x')^3 + (y')^3 &= u'(z')^3, \quad x', y', z' \in \mathbb{Z}[j] \text{ premiers entre eux,} \\ v_\lambda(x') &= v_\lambda(y') = 0, \quad v_\lambda(z') \geq 1, \end{aligned} \quad (1)$$

où  $u' \in \mathbb{Z}[j]^\times$  et

$$v_\lambda(z') = v_\lambda(z) - 1 .$$

Pour ce faire, on utilisera uniquement le fait que  $(x, y, z)$  est solution de :

$$\begin{aligned} x^3 + y^3 &= uz^3, \quad x, y, z \in \mathbb{Z}[j] \text{ premiers entre eux,} \\ v_\lambda(x) &= v_\lambda(y) = 0, \quad v_\lambda(z) \geq 1, \end{aligned} \quad (2)$$

avec  $u \in \mathbb{Z}[j]^\times$  (bien sûr,  $u = 1$ , mais on ne s'en servira pas).

A partir d'une solution au problème (2), on construit une solution au problème (1), qui satisfait les mêmes hypothèses et telle que  $v_\lambda(z') = v_\lambda(z) - 1$ . Ce procédé est récursif (rien n'empêche de l'itérer), et aboutit clairement à une contradiction : l'exposant de  $\lambda$  dans la troisième composante de la solution diminue de 1 à chaque étape, mais doit rester supérieur ou égal à 1... Il ne reste donc qu'à montrer que cette construction est possible pour achever la preuve du théorème de Fermat pour  $p = 3$ .

**Lemme 2.6** Pour tout  $s \in \mathbb{Z}[j]$ , on a  $s \equiv 0, 1$  ou  $-1 \pmod{\lambda}$  (c'est-à-dire  $s - 0, s - 1$  ou  $s + 1$  est divisible par  $\lambda$  dans  $\mathbb{Z}[j]$ ).

*Preuve.* Ecrivons  $s = a + bj$  avec  $a, b \in \mathbb{Z}$ , alors  $s = a + b + b(j - 1) = a + b - b\lambda$ , donc  $s \equiv a + b \pmod{\lambda}$ . Or  $a + b \in \mathbb{Z}$  donc  $a + b \equiv 0, 1$  ou  $-1 \pmod{3}$ , donc aussi  $\pmod{\lambda}$  puisque  $\lambda$  divise 3. ■

**Lemme 2.7** Si  $s \equiv \pm 1 \pmod{\lambda}$ , alors  $s^3 \equiv \pm 1 \pmod{\lambda^4}$ .

*Preuve.* On traite le cas  $s \equiv 1 \pmod{\lambda}$ , alors  $s - 1 = t\lambda$  pour un  $t \in \mathbb{Z}[j]$ , d'où

$$s^3 - 1 = (s-1)(s-j)(s-j^2) = (s-1)(s-1+1-j)(s-1+1-j^2) = t\lambda(t+1)\lambda(t-j^2)\lambda.$$

Comme  $t \equiv 0, 1$  ou  $-1 \pmod{\lambda}$  d'après le lemme qui précède et  $j^2 \equiv 1 \pmod{\lambda}$ , ceci entraîne  $s^3 \equiv 1 \pmod{\lambda^4}$ . L'autre cas est analogue. ■

On en déduit (exercice) :

$$v_\lambda(z) \geq 2.$$

Il s'ensuit que  $v_\lambda(z^3) \geq 6$ . On utilise alors la factorisation établie dans l'exercice 2.1 :

$$(x+y)(x+jy)(x+j^2y) = uz^3.$$

L'un des facteurs est forcément divisible par  $\lambda^2$ ; on peut supposer que c'est  $x+y$ , et on montre qu'alors  $v_\lambda(x+jy) = v_\lambda(x+j^2y) = 1$  :

$$x+jy = x+y+(j-1)y = x+y-y\lambda$$

et  $v_\lambda(y) = 0$ . On note  $t = v_\lambda(x+y) = 3v_\lambda(z) - 2$ . Comme  $\mathbb{Z}[j]$  est principal, la notion de pgcd existe comme dans  $\mathbb{Z}$ .

**Lemme 2.8** Le pgcd de  $x+y$  et  $x+jy$  est  $(x+y, x+jy) = \lambda$ .

*Preuve.* Supposons que  $r \in \mathbb{Z}[j]$  divise  $x+y$  et  $x+jy$ , alors  $r$  divise la différence  $\lambda y$  et  $r$  divise  $(x+y) - j^2(x+jy) = (1-j^2)x = -j^2\lambda x$ ; comme  $x$  et  $y$  sont premiers entre eux, ceci entraîne que  $r$  divise  $\lambda$ . Or on vient de voir que  $\lambda$  divise effectivement  $x+y$  et  $x+jy$ . ■

On montre de manière analogue que  $(x+y, x+j^2y) = (x+jy, x+j^2y) = \lambda$ . Il s'ensuit que

$$x+y = w_1 s_1^3 \lambda^t, \quad x+jy = w_2 s_2^3 \lambda, \quad x+j^2y = w_3 s_3^3 \lambda,$$

avec  $w_1, w_2, w_3 \in \mathbb{Z}[j]^\times$ ,  $s_1, s_2, s_3 \in \mathbb{Z}[j]$ ,  $v_\lambda(s_1) = v_\lambda(s_2) = v_\lambda(s_3) = 0$  et  $(s_1, s_2) = (s_2, s_3) = (s_3, s_1) = 1$ .

On rappelle que  $1+j+j^2=0$ ; il s'ensuit que  $(x+y)+j(x+jy)+j^2(x+j^2y)=0$ , d'où l'on déduit :

$$w_1(s_1 \lambda^{v_\lambda(z)-1})^3 + j w_2 s_2^3 + j^2 w_3 s_3^3 = 0,$$

soit

$$(x')^3 + \varepsilon(y')^3 = u'(z')^3,$$

avec  $x' = s_2$ ,  $y' = s_3$  et  $z' = s_1 \lambda^{v_\lambda(z)-1}$ ,  $\varepsilon = j\omega_3\omega_2^{-1} \in \mathbb{Z}[j]^\times$  et  $u' = -j^2\omega_1\omega_2^{-1} \in \mathbb{Z}[j]^\times$ . On vérifie aisément les propriétés requises pour  $x'$ ,  $y'$  et  $z'$ . Il ne reste donc qu'à voir que  $\varepsilon = \pm 1$ , ce qui se fait en réduisant modulo  $\lambda^3$  :

$$\pm 1 \pm \varepsilon \equiv 0 \pmod{\lambda^3} ,$$

ce qui est impossible pour  $\varepsilon \in \{\pm j, \pm j^2\}$ . Ceci termine la preuve du théorème de Fermat pour  $n = 3$  (la première preuve écrite remonte à EULER, 1707-1783 et se présente un peu différemment de celle donnée ci-dessus).

### 3 Le premier cas pour $p$ régulier supérieur à 5

On fixe un nombre premier  $p \geq 5$  et on suppose que  $(x, y, z)$  est solution de :

$$x^p + y^p = z^p , \quad x, y, z \in \mathbb{Z} \text{ premiers entre eux, } p \nmid xyz .$$

Ecrivons à nouveau l'équation sous la forme  $x^p + y^p + (-z)^p = 0$  : on ne peut pas avoir  $x \equiv y \equiv -z \pmod{p}$ , sinon  $-3z^p \equiv 0 \pmod{p}$ , ce qui est impossible puisque  $p \geq 5$  et  $p \nmid xyz$ . Quitte à permuter  $x$ ,  $y$  et  $z$ , on peut donc supposer  $x \not\equiv y \pmod{p}$ .

Pour factoriser le membre de gauche, on introduit cette fois-ci une racine primitive  $p$ -ième de l'unité  $\zeta$ , c'est-à-dire une racine du polynôme  $X^p - 1$  distincte de 1, c'est-à-dire encore une racine du  $p$ -ième *polynôme cyclotomique* :

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1 .$$

**Exercice 3.1** Vérifier que les racines de  $X^p - 1$  sont les  $\zeta^k$  pour  $0 \leq k \leq p-1$ . En déduire les factorisations :

$$\begin{aligned} x^p + y^p &= (x + y)(x + \zeta y)(x + \zeta^2 y) \dots (x + \zeta^{p-1} y) , \\ p &= (1 - \zeta)(1 - \zeta^2) \dots (1 - \zeta^{p-1}) . \end{aligned}$$

On travaille donc dans  $\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}, a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}\}$  (noter que  $\zeta^{p-1} = -1 - \zeta - \dots - \zeta^{p-2}$ ). Cet anneau n'est principal que pour  $p$  inférieur à 19. Pour le cas général, on doit donc s'intéresser à ses idéaux.

#### 3.1 Les idéaux d'un anneau

Un anneau  $A$  est un ensemble muni d'une loi  $+$  pour laquelle il est un groupe (élément neutre noté 0, opposé de  $a$  noté  $-a$ ), et d'une loi  $\times$  associative (pour laquelle il contient un élément neutre noté 1) qui se comporte bien par rapport à l'addition (distributivité). Les éléments de  $A$  qui ont un symétrique pour la multiplication (inverse) sont ses *unités*.

**Définition 3.2** Un *idéal* de  $A$  est un sous-groupe (additif) de  $A$  qui est stable par multiplication par n'importe quel élément de  $A$ . Un idéal  $I$  de  $A$  est dit *principal* s'il existe  $s \in A$  tel que  $I = sA = \{sa, a \in A\}$ . L'anneau  $A$  est *principal* s'il est intègre et si tous ses idéaux sont principaux.

**Exemple 3.3** L'ensemble des entiers multiples de 6,  $6\mathbb{Z}$ , est un idéal principal de  $\mathbb{Z}$ , qui est un anneau principal. Cela découle du fait qu'il est *euclidien* (on peut y faire des divisions euclidiennes).

L'anneau  $\mathbb{Z}[X]$  n'est pas principal, car l'idéal  $(2, X)$  (engendré par 2 et par  $X$ ) ne l'est pas. En particulier, 2 et  $X$  n'ont pas de pgcd.

Soient  $I$  et  $J$  des idéaux de  $A$ , on construit deux nouveaux idéaux :

$$I + J = \{a + b, a \in I, b \in J\}, \quad IJ = \{a_1 b_1 + \dots + a_n b_n, a_i \in I, b_i \in J\} .$$

**Exercice 3.4** Montrer que  $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$  et  $2\mathbb{Z}3\mathbb{Z} = 6\mathbb{Z}$ . Que valent la somme et le produit de  $10\mathbb{Z}$  et  $15\mathbb{Z}$  ?

On vérifie immédiatement que la multiplication est distributive sur l'addition :

$$I(J + J') = IJ + IJ' .$$

La similarité avec l'addition et la multiplication des nombres vont nous permettre d'utiliser très facilement les opérations sur les idéaux. Pour continuer l'analogie, on dira que  $I$  divise  $J$  s'il existe un idéal  $J'$  tel que  $J = IJ'$  (et donc  $J \subset I$ ). Et on s'interrogera sur la possibilité de décomposer un idéal en produit d'idéaux premiers, dès qu'on aura défini ceux-ci.

Etant donné un idéal  $I$  de  $A$ , on considère la relation binaire sur  $A$  :  $a \mathcal{R} b$  si  $a - b \in I$ . C'est une relation d'équivalence, et on note  $A/I$  l'ensemble des classes :

$$A/I = \{a + I, a \in A\} .$$

$A/I$  est naturellement un anneau pour les lois induites par celles de  $A$ .

**Définition 3.5** Un idéal  $I$  est dit *premier* si  $A/I$  est intègre (il est dit *maximal* si  $A/I$  est un corps).

**Exemple 3.6**  $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$ ;  $6\mathbb{Z}$  n'est pas un idéal premier de  $\mathbb{Z}$  :  $\bar{2} \times \bar{3} = \bar{0}$ , bien que  $\bar{2} \neq \bar{0}$  et  $\bar{3} \neq \bar{0}$ . Les idéaux premiers de  $\mathbb{Z}$  sont les  $(p) = p\mathbb{Z}$ , où  $p$  est un nombre premier. De même,  $(\lambda) = \lambda\mathbb{Z}[j]$  est un idéal premier de  $\mathbb{Z}[j]$ .

### 3.2 L'anneau $\mathbb{Z}[\zeta]$

Pour  $p \geq 23$ ,  $\mathbb{Z}[\zeta]$  n'est plus principal, c'est-à-dire que certains de ses idéaux ne sont pas engendrés par un seul élément (on peut montrer cependant que tout idéal de  $\mathbb{Z}[\zeta]$  s'écrit  $(a, b) = a\mathbb{Z}[\zeta] + b\mathbb{Z}[\zeta]$  avec  $a, b \in \mathbb{Z}[\zeta]$ ). Cela entraîne qu'il n'y a pas unique décomposition en produit d'irréductibles pour ses éléments. Par contre :

**Proposition 3.7** *Tout idéal non nul de  $\mathbb{Z}[\zeta]$  admet une unique décomposition en produit d'idéaux premiers.*

Cette propriété provient du fait que  $\mathbb{Z}[\zeta]$  n'est pas "n'importe quel" anneau : c'est l'anneau d'entiers du corps de nombres  $\mathbb{Q}(\zeta)$ , qu'on peut voir comme le plus petit sous-corps de  $\mathbb{C}$  contenant  $\mathbb{Q}$  et  $\zeta$ , ou encore comme le quotient :

$$\mathbb{Q}[X]/(\Phi_p) ,$$

où  $(\Phi_p)$  désigne l'idéal principal engendré par  $\Phi_p(X)$  dans l'anneau  $\mathbb{Q}[X]$ .  $\mathbb{Q}(\zeta)$  est aussi un  $\mathbb{Q}$ -espace vectoriel de dimension  $p - 1$ , de base  $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$ . Tous les éléments de  $\mathbb{Q}(\zeta)$  sont racines d'un polynôme à coefficients dans  $\mathbb{Q}$  de degré divisant  $p - 1$ . L'anneau d'entiers de  $\mathbb{Q}(\zeta)$  est, par définition, l'ensemble de ses éléments qui sont racines d'un polynôme *unitaire* (de coefficient dominant 1) à coefficients dans  $\mathbb{Z}$ .

**Exemple 3.8** Les  $\zeta^k$ ,  $1 \leq k \leq p - 1$ , sont solutions de  $X^{p-1} + \dots + X + 1 = 0$ .

Les  $\zeta^k$ ,  $1 \leq k \leq p - 1$ , fournissent aussi des exemples d'unités de  $\mathbb{Z}[\zeta]$ . De plus, ils permettent d'en construire d'autres :

**Exercice 3.9** *Montrer que, si  $k$  et  $l$  sont des entiers premiers à  $p$ , alors*

$$\frac{\zeta^k - 1}{\zeta^l - 1} \in \mathbb{Z}[\zeta]^\times$$

(on pourra faire intervenir un entier  $m$  tel que  $k \equiv lm \pmod{p}$ ).

Contrairement à  $\mathbb{Z}[j]$ ,  $\mathbb{Z}[\zeta]$  contient une infinité d'unités, ce qui complique un peu les choses. KUMMER a montré qu'elles sont toutes de la même forme, qui fait intervenir une unité *réelle*, c'est-à-dire une unité invariante par conjugaison complexe (comme  $\mathbb{Z}[\zeta] \subset \mathbb{C}$ , on peut considérer le conjugué complexe  $\bar{s}$  de  $s \in \mathbb{Z}[\zeta]$ ). Son résultat s'énonce :

**Proposition 3.10** *Tout  $u \in \mathbb{Z}[\zeta]^\times$  s'écrit  $u = \zeta^r \varepsilon$ , avec  $r \in \mathbb{Z}$  et  $\varepsilon \in \mathbb{Z}[\zeta]^\times$  tel que  $\bar{\varepsilon} = \varepsilon$ .*

Pour le prouver, on a besoin de considérer d'autres transformations de  $\mathbb{Z}[\zeta]$  dans lui-même que la conjugaison complexe. En fait, comme  $\zeta$  est de module 1, on a  $\bar{\zeta} = \zeta^{-1} = \zeta^{p-1}$ , donc  $\bar{\zeta}$  est une autre racine du polynôme  $\Phi_p$ . Définissons l'application  $\sigma$  de  $\mathbb{Z}[\zeta]$  dans lui-même par :

$$\sigma(\zeta) = \zeta^2 ,$$

en imposant que  $\sigma$  soit invariante sur les éléments de  $\mathbb{Z}$ , additive et multiplicative, ce qui entraîne :

$$\sigma(a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}) = a_0 + a_1\sigma(\zeta) + \dots + a_{p-2}\sigma(\zeta)^{p-2} ,$$



où les  $a_i \in \mathbb{Z}$ . On peut composer  $\sigma$  avec elle-même pour obtenir d'autres transformations. Ainsi,  $\sigma^2(\zeta) = \sigma \circ \sigma(\zeta) = \sigma(\zeta^2) = \sigma(\zeta)^2 = \zeta^4$  et, en itérant la manœuvre,  $\sigma^k(\zeta) = \zeta^{2^k}$ . Comme 2 engendre le groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^\times$ , les  $2^k$  pour  $1 \leq k \leq p-1$  prennent modulo  $p$  toutes les valeurs de 1 à  $p-1$ , si bien que :

$$\{\zeta, \sigma(\zeta), \sigma^2(\zeta), \dots, \sigma^{p-2}(\zeta)\} = \{\zeta^k, 1 \leq k \leq p-1\} , \quad (3)$$

En particulier, comme  $2^{p-1} \equiv 1 \pmod{p}$  (petit théorème de Fermat),  $\sigma^{p-1}$  est l'application identité. Les nombres de l'ensemble ci-dessus sont appelés les *conjugués* de  $\zeta$ , car ils sont tous racines du même polynôme irréductible à coefficients dans  $\mathbb{Q}$ .

On est en mesure de prouver la proposition 3.10.

*Preuve.* Posons  $\alpha = u/\bar{u}$ , alors  $\alpha \in \mathbb{Z}[\zeta]$  car  $\bar{u}$  est une unité, et

$$\sigma^k(\alpha) = \sigma^k(u)/\sigma^k(\bar{u}) = \sigma^k(u)/\overline{\sigma^k(u)} ,$$

donc tous les conjugués  $\sigma^k(\alpha)$ ,  $0 \leq k \leq p-2$ , sont de module 1. Il en va bien sûr de même pour les conjugués de  $\alpha^n$  pour tout  $n \in \mathbb{N}$ .

Or, en tant qu'élément de  $\mathbb{Z}[\zeta]$ ,  $\alpha^n$  est racine d'un polynôme de  $\mathbb{Z}[X]$ , dont les coefficients sont des *fonctions symétriques* des  $\sigma^k(\alpha^n)$ . Ceci permet de borner les coefficients de tous les polynômes unitaires (de degrés divisant  $p-1$ ) qui annulent les  $\alpha^n$ ; comme ces coefficients sont entiers, ils ne peuvent prendre qu'un nombre fini de valeurs. Il n'y a donc qu'un nombre fini de polynômes dont les  $\alpha^n$  peuvent être les racines, ce qui entraîne que l'ensemble  $\{\alpha^n, n \in \mathbb{N}\}$  est fini, et donc  $\alpha^N = 1$  pour un certain  $N \in \mathbb{N}$ .

Les seules *racines de l'unité* dans  $\mathbb{Z}[\zeta]$  sont de la forme  $\pm\zeta^l$ , donc  $u/\bar{u} = \pm\zeta^l$ . On montre assez facilement qu'en fait  $u/\bar{u} = \zeta^l$ ; il ne reste qu'à choisir  $r \in \mathbb{Z}$  tel que  $2r \equiv l \pmod{p}$ , et à poser  $\varepsilon = \zeta^{-r}u$ , qui vérifie bien  $\bar{\varepsilon} = \varepsilon$ . ■

On s'intéresse maintenant aux idéaux premiers de  $\mathbb{Z}[\zeta]$ , en particulier à l'un d'eux. On a besoin de définir l'application *norme* :

$$\begin{aligned} \mathbf{N}: \mathbb{Z}[\zeta] &\longrightarrow \mathbb{Z} \\ s &\longmapsto \mathbf{N}(s) = s\sigma(s)\sigma^2(s)\dots\sigma^{p-2}(s) , \end{aligned}$$

qui est multiplicative car les  $\sigma^k$  le sont.

Les  $\sigma^k$  sont aussi additifs, si bien que  $\sigma^k(1-\zeta) = \sigma^k(1) - \sigma^k(\zeta) = 1 - \sigma^k(\zeta)$ , d'où, en utilisant l'égalité (3) et l'exercice 3.1 :

$$\mathbf{N}(1-\zeta) = (1-\zeta)(1-\sigma(\zeta))\dots(1-\sigma^{p-2}(\zeta)) = (1-\zeta)(1-\zeta^2)\dots(1-\zeta^{p-1}) = p .$$

**Lemme 3.11**  $(1-\zeta)$  est un idéal premier de  $\mathbb{Z}[\zeta]$ .

*Preuve.* Montrons que  $\mathbb{Z}[\zeta]/(1-\zeta)$  est intègre : soient  $a, b \in \mathbb{Z}[\zeta]$  tels que  $ab \in (1-\zeta)$ , c'est-à-dire  $ab = (1-\zeta)c$  pour un  $c \in \mathbb{Z}[\zeta]$ . Alors  $\mathbf{N}(a)\mathbf{N}(b) = p\mathbf{N}(c)$ , donc  $p|\mathbf{N}(a)$  ou  $p|\mathbf{N}(b)$  (car  $p$  est premier). Dans le premier cas, on obtient que l'idéal

$(1 - \zeta)^{p-1}$  divise le produit d'idéaux  $(a)(\sigma(a)) \dots (\sigma^{p-2}(a))$ , donc  $(1 - \zeta) | (\sigma^k(a))$  pour un certain  $k$ , puis  $(\sigma^{p-1-k}(1 - \zeta)) | (a)$ , si bien que

$$a \in (\sigma^{p-1-k}(1 - \zeta)) = (1 - \zeta^{p-1-k}) = (1 - \zeta)$$

et  $a$  vaut 0 dans  $\mathbb{Z}[\zeta]/(1 - \zeta)$ . Le deuxième cas se traite de façon analogue. ■

**Exercice 3.12** (a) Montrer que  $(1 - \zeta) \cap \mathbb{Z} = p\mathbb{Z}$ .

(b) Montrer que la décomposition de  $(p) = p\mathbb{Z}[\zeta]$  en produit d'idéaux premiers est :  
 $(p) = (1 - \zeta)^{p-1}$ .

Avant d'en venir à la preuve du théorème, il reste à expliquer l'hypothèse  $p$  **régulier** : elle signifie que si  $I$  est un idéal de  $\mathbb{Z}[\zeta]$  tel que  $I^p$  soit principal, alors  $I$  est principal.

### 3.3 La contradiction

Récapitulons nos hypothèses :  $p$  est un premier régulier supérieur à 5,  $x$ ,  $y$  et  $z$  sont des entiers premiers entre eux 2 à 2 avec  $p \nmid xyz$  et  $x \not\equiv y \pmod{p}$ , qui satisfont :

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \dots (x + \zeta^{p-1} y) = z^p .$$

Considérons ceci comme une égalité entre idéaux de  $\mathbb{Z}[\zeta]$  :

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \dots (x + \zeta^{p-1} y) = (z)^p .$$

**Lemme 3.13** Les idéaux  $(x + \zeta^k y)$ ,  $0 \leq k \leq p - 1$ , sont premiers entre eux deux à deux.

*Preuve.* Soit  $\wp$  un idéal premier de  $\mathbb{Z}[\zeta]$  qui divise les idéaux  $(x + \zeta^k y)$  et  $(x + \zeta^l y)$ , avec  $k \neq l$ , alors  $\wp$  divise la somme des deux idéaux. En particulier  $\wp$  divise l'idéal engendré par  $(x + \zeta^k y) - (x + \zeta^l y)$ , c'est-à-dire  $\wp$  divise  $((\zeta^k - \zeta^l)y) = ((1 - \zeta)y)$ ; de même  $\wp$  divise l'idéal engendré par  $\zeta^l(x + \zeta^k y) - \zeta^k(x + \zeta^l y)$ , c'est-à-dire  $\wp$  divise  $((1 - \zeta)x)$ . Comme  $x$  et  $y$  sont premiers entre eux, il s'ensuit que  $\wp = (1 - \zeta)$ . On a donc  $x + y \equiv x + \zeta^k y \equiv 0 \pmod{1 - \zeta}$ , puis  $x + y \in (1 - \zeta) \cap \mathbb{Z} = p\mathbb{Z}$ ; alors  $z^p = x^p + y^p \equiv x + y \equiv 0 \pmod{p}$ , donc  $p | z$ , ce qui est contredit l'hypothèse. ■

En utilisant l'unique décomposition des idéaux en produits d'idéaux premiers, il s'ensuit que les  $(x + \zeta^k y)$ ,  $0 \leq k \leq p - 1$ , sont tous des puissances  $p$ -ièmes :

$$(x + \zeta^k y) = A_k^p ,$$

où les  $A_k$  sont des idéaux de  $\mathbb{Z}[\zeta]$  premiers entre eux 2 à 2. De plus, comme  $A_k^p$  est principal et  $p$  est régulier, chaque  $A_k$  est principal :  $A_k = (\alpha_k)$ , avec  $\alpha_k \in \mathbb{Z}[\zeta]$ , si bien que :

$$x + \zeta^k y = u_k \alpha_k^p , \text{ avec } u_k \in \mathbb{Z}[\zeta]^\times , \text{ pour tout } 0 \leq k \leq p - 1 .$$

A l'aide de la proposition 3.10, on a  $u_1 = \zeta^r \varepsilon$  avec  $r \in \mathbb{Z}$  et  $\varepsilon \in \mathbb{Z}[\zeta]^\times$  tel que  $\bar{\varepsilon} = \varepsilon$ .  
Ecrivons  $\alpha_1 = n_0 + n_1 \zeta + \cdots + n_{p-2} \zeta^{p-2}$  avec les  $n_i \in \mathbb{Z}$ , alors

$$\alpha_1^p \equiv n_0^p + (n_1 \zeta)^p + \cdots + (n_{p-2} \zeta^{p-2})^p \equiv n_0^p + n_1^p + \cdots + n_{p-2}^p \pmod{p} ,$$

c'est-à-dire  $\alpha_1^p \equiv a \pmod{p}$  pour un certain  $a \in \mathbb{Z}$ . On obtient ( $k = 1$ ) :

$$x + \zeta y = \zeta^r \varepsilon \alpha_1^p \equiv \zeta^r \varepsilon a \pmod{p} ,$$

d'où l'on tire  $x + \zeta^{-1} y = \overline{x + \zeta y} = \zeta^{-r} \overline{\varepsilon} \overline{\alpha_1^p} \equiv \zeta^{-r} \varepsilon a \pmod{p}$ , car  $\bar{a} = a$  et  $\bar{p} = p$ . On a donc  $\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1} y) \pmod{p}$ , ce qui donne :

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \pmod{p} , \quad (4)$$

donc  $x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y = ps$  pour un  $s \in \mathbb{Z}[\zeta]$ . Les éléments de  $\mathbb{Z}[\zeta]$  ont une unique écriture de la forme  $m_0 + m_1 \zeta + \cdots + m_{p-2} \zeta^{p-2}$  avec les  $m_i \in \mathbb{Z}$ , donc, si les nombres  $1, \zeta, \zeta^{2r}$  et  $\zeta^{2r-1}$  sont distincts, on voit que  $p$  doit diviser  $x$  et  $y$ . Puisque ceci contredit nos hypothèses (et que  $1 \neq \zeta, \zeta^{2r} \neq \zeta^{2r-1}$ ), on est forcément dans l'un des trois cas suivants :

- (i)  $1 = \zeta^{2r}$  : (4) devient  $\zeta y - \zeta^{-1} y \equiv 0 \pmod{p}$ , ce qui entraîne (comme ci-dessus)  $p|y$  : impossible.
- (ii)  $1 = \zeta^{2r-1}$  (ce qui équivaut à  $\zeta = \zeta^{2r}$ ) : (4) devient  $(x - y) - \zeta(x - y) \equiv 0 \pmod{p}$ , ce qui entraîne  $p|x - y$  : impossible.
- (iii)  $\zeta = \zeta^{2r-1}$  : (4) devient  $x - \zeta^2 x \equiv 0 \pmod{p}$ , ce qui entraîne  $p|x$  : impossible.

Les trois cas étant impossibles, on arrive à une contradiction. L'équation de Fermat pour  $p \geq 5$  premier régulier n'a donc pas de solution entière  $(x, y, z)$  avec  $p \nmid xyz$ . Ce résultat est dû à KUMMER (1847), qui a aussi donné une preuve dans le deuxième cas du théorème (toujours pour  $p$  régulier), utilisant le principe de la descente infinie.

## 4 Quelques questions ouvertes

Le théorème de Fermat était donc résolu par KUMMER pour  $p$  régulier ; il a de plus trouvé un critère permettant de dire si un nombre premier est régulier. On définit les nombres de Bernouilli  $B_n$  par la formule :

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!} .$$

Les  $B_n$  sont des nombres rationnels et ont une grande importance en arithmétique. En particulier, KUMMER a établi qu'un premier  $p$  est irrégulier si et seulement si  $p$  divise le numérateur d'un  $B_n$  pour  $2 \leq n \leq p - 3$ . Ceci permet de prouver qu'il y a une infinité de nombres premiers  $p$  irréguliers (c'est-à-dire tels que  $\mathbb{Z}[\zeta]$  contienne

un idéal  $I$  non principal avec  $I^p$  principal), les plus petits étant 37, 59, 67, 101... Par contre, on ne sait toujours pas s'il existe une infinité de nombres premiers *réguliers*, ce que l'on conjecture (des calculs et des arguments probabilistes font penser qu'environ 61% des premiers sont réguliers).

Dans le même ordre d'idées, la conjecture de VANDIVER (milieu XX<sup>e</sup> siècle) prédit que si  $I$  est un idéal de l'anneau  $\mathbb{Z}[\zeta + \zeta^{-1}]$  tel que  $I^p$  soit principal, alors  $I$  est principal (l'anneau  $\mathbb{Z}[\zeta + \zeta^{-1}]$  est le sous-anneau *totalelement réel* de  $\mathbb{Z}[\zeta]$ ). Cette question a motivé de nombreuses recherches.

Un problème plus ancien résiste toujours ; il a été posé par GAUSS (1777-1855), il s'agit de savoir s'il existe une infinité de *corps de nombres* (des sous-corps de  $\mathbb{C}$  de dimension finie comme  $\mathbb{Q}$ -espaces vectoriels) dont l'*anneau d'entiers* (ensemble des éléments qui sont racines d'un polynôme à coefficients dans  $\mathbb{Z}$ , de coefficient dominant 1) soit principal. On pense généralement que c'est le cas (et même qu'il en existe une infinité parmi les corps de nombres de dimension 2 sur  $\mathbb{Q}$ ).

Enfin, les développements spectaculaires du 20<sup>e</sup> siècle dans l'étude des courbes elliptiques, qui ont permis la résolution par WILES du second cas du théorème de Fermat, ont aussi ouvert de nombreuses questions, mais cela sort du cadre de cet exposé.

## Références

- [1] Hellegouarch Y., *Invitation aux mathématiques de Fermat-Wiles*, Enseignement des mathématiques, Masson, Paris (1997).

Un panorama mathématique et historique de toutes les techniques inventées et développées pour démontrer le théorème de Fermat, particulièrement autour de l'usage des courbes elliptiques, dont l'auteur a été l'un des précurseurs.

- [2] Samuel P., *Théorie algébrique des nombres*, 2<sup>e</sup> édition, Hermann, Paris (1971).

Une exposition claire des outils algébriques pour la théorie des nombres : corps de nombres, anneaux d'entiers, idéaux,...

- [3] Washington L.C., *Introduction to cyclotomic fields*, 2nd edition, Graduate texts in maths. **83**, Springer-Verlag, New York (1997).

Ouvrage présentant les résultats à la pointe de la recherche dans l'approche « cyclotomique » (nombres de Bernoulli, conjecture de Vandiver,...) ; la preuve du premier cas du théorème pour  $p$  régulier est tirée de son premier chapitre (le plus accessible).