

intro

Au milieu du XIX<sup>e</sup> siècle, commença la bataille pour la démonstration du « grand théorème de Fermat ». En effet, Fermat avait simplement pris la formule de Pythagore à savoir  $x^2 + y^2 = z^2$  et avait remplacé les carrés par des cubes ( $x^3 + y^3 = z^3$ ) avant de généraliser avec la formule suivante :  $x^n + y^n = z^n$ .

Par la suite Kummer a fait un pas vraiment notable grâce à ce qu'on appelle les lois de réciprocité entre nombres premiers, par exemple, si  $q$  est un nombre premier,  $q$  est un carré à un multiple de 5 près si et seulement si 5 est un carré à un multiple de  $q$  près. Ainsi  $q = 269 = 13^2 + 5 \times 20$  est un carré à un multiple de 5 près. Donc si on examine la suite  $5 + 269, 5 + 2 \times 269, 5 + 3 \times 269 \dots$  on tombera fatalement sur un carré. Ensuite au XIX<sup>e</sup> siècle, Gauss tenta une approche avec l'arithmétique avec des nombres de la forme  $x + z y$  avec  $x$  et  $y$  des entiers et  $z$  un nombre complexe tel que  $z^n = 1$ . Ceci lui permis de factoriser l'équation de Fermat  $z^n = x^n + y^n$  pour obtenir  $(x+y)(x+zy)\dots(x+z^{n-1}y)$ . Kummer pu ainsi démontrer le théorème de Fermat pour tous les exposants en dessous de 100 (à l'exception de 3 d'entre eux : 37, 59 et 67).

Enfin Dedekind et Kronecker qui ont travaillé sur l'arithmétique de nombres (algébriques) complexes a permis en particulier à Dedekind de compléter la théorie de Gauss et généraliser celle de Kummer. Par la suite, Riemann invente une nouvelle fonction pour étudier la répartition des nombres premiers qui aboutira à une hypothèse où la fonction (souvent nommée zêta) dans les complexes passe par la valeur 0 (ce qui est donc un réel pour une courbe représentative d'une fonction complexe). Puis plusieurs professeurs et élèves de Göttingen (une ville universitaire très célèbre en Allemagne (32.000 étudiants et 2.500 enseignants) et une université prestigieuse puisque 42 prix Nobel y ont enseigné ou étudié) ont travaillé sur des théorèmes relatifs aux nombres.

Ensuite, Hilbert développe très largement une nouvelle vision de l'arithmétique qui dépasse celle de Diophante et Fermat. Il simplifia aussi un grand nombre des travaux sur théorie algébrique des nombres déjà réalisés comme ceux de Kummer, Kronecker, Dirichlet et Dedekind.

L'arithmétique est devenue la théorie des nombres, limitées à l'étude des entiers naturels et relatifs et des nombres rationnels (sous forme de fractions) avec les opérateurs d'addition, de soustraction, de multiplication et de division. Et c'est ainsi, avec une grande implication de l'école allemande de mathématiques de la fin du XIX<sup>e</sup> siècle qu'est né la théorie algébrique des nombres utilisant l'algèbre en plus de la théorie des nombres pour mieux comprendre les nombres.

---

## 2<sup>e</sup> partie

La 8<sup>ème</sup> section de ses *Disquisitiones Arithmeticae* (vers une théorie des corps finis, trouvés dans les manuscrits de Gauss, éditée après sa mort dans ses œuvres complètes) est à l'origine de la plupart des recherches arithmétiques de la fin du XIX<sup>e</sup> siècle. A l'image des « entiers modulo  $p$  » (voir encadré), il y considère notamment des congruences modulo un polynôme irréductible : on dit que le polynôme  $q(x)$  est congru à  $r(x)$  modulo  $p(x)$  si  $p(x)$  divise la différence  $q(x) - r(x)$ , ce que les mathématiciens écrivent :

$$q(x) \equiv r(x) \pmod{p(x)} \Leftrightarrow p(x) \text{ divise } (q(x) - r(x)).$$

Par exemple 21 est congru à 46 modulo 5 car  $21 = 4 \cdot 5 + 1$  et  $46 = 9 \cdot 5 + 1$  le reste est donc dans les deux cas égale à 1.

Ceci l'amène à travailler sur des classes de polynômes à coefficients dans le corps  $\mathbb{Z}/p\mathbb{Z}$  où  $p$  est un nombre premier.

---

### 3) Des polynômes aux nombres idéaux.

S'intéressant au grand théorème de Fermat, Kummer cherche à factoriser en  $p$  facteurs premiers l'expression  $x^n + y^n$  où  $p$  est premier. Il introduit pour cela les racines  $p$ -ièmes de l'unité. En effet, tout comme 1 a deux racines carrées, 1 et  $-1$ , il y a trois racines cubiques, une réelle : 1 et deux dans le corps  $\mathbb{C}$  des « complexes » :  $j$  et  $j^2$  dont  $j = \frac{-1+i\sqrt{3}}{2} = e^{\frac{i2\pi}{3}}$  et  $j^2 = \frac{-1-i\sqrt{3}}{2} = e^{-\frac{i2\pi}{3}}$ . (On notera aussi les relations des racines cubiques  $1+j+j^2=0$ ).  $p$  racines  $p$ -ièmes s'écriront alors  $\alpha_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$  où  $i$  est le nombre imaginaire  $\sqrt{-1}$ , car : si l'on prend  $\lambda \in \mathbb{C}$  et que l'on appelle racine  $p$ -ièmes de  $\lambda$  tout  $z$  tel que  $z^p = \lambda$  (avec  $p \neq 0$ )

$$\lambda = r(\cos \alpha + i \sin \alpha)$$

$$z = \rho (\cos \theta + i \sin \theta)$$

d'après la formule  $z^p = \lambda$  on obtient alors :

$$\rho^p (\cos p\theta + i \sin p\theta) = r(\cos \alpha + i \sin \alpha)$$

$$\text{D'où } \rho^p = r \text{ et où } r \text{ et } \rho \in \mathbb{R}^+$$

$$\text{Soit } \rho = \sqrt[p]{r} = r^{1/p}$$

$$\text{Et } p\theta = \alpha + 2k\pi$$

$$\text{D'où } \theta = \frac{\alpha}{p} + \frac{2k\pi}{p} \text{ avec } \forall k \in [0, 1, \dots, p-1]$$

Les racines sont toutes des puissances de l'une d'entre elles,  $\alpha$ , et s'écriront :

$$1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{p-1}$$

De tels nombres  $\alpha$  sont appelés « racines primitives de l'unité » c'est-à-dire des racines de l'équation  $Z^n = 1$  avec  $n$  entier. Si  $p$  est premier, toute racine  $p$ -ième sauf 1 est racine primitive.

Kummer, comme l'avait fait Lagrange avant lui, obtient la relation suivante :

$$x^n + y^n = (x+y)(x + \alpha y) \dots (x + \alpha^{p-1} y).$$

Il étudie alors ce qu'il nomme les entiers complexes, de la forme :

$a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + \dots + a_{p-1} \alpha^{p-1}$ , par analogie avec les entiers complexes de Gauss s'écrivant  $a + bi$  (les  $a_k$  sont entiers). Sa démonstration du théorème de Fermat repose sur une hypothèse avancée : sur les *entiers complexes*, la décomposition en facteurs premiers est unique.

Cauchy réfutera la preuve : l'hypothèse est fausse, en prenant le contre-exemple  $p = 23$ .

En effet, la démonstration de Kummer s'avéra valable pour les nombres premiers dits réguliers, (nombres impairs et qui ne divisent pas le nombre de classes du corps cyclotomique

$\mathbb{Q}(e^{\frac{2i\pi}{p}})$ ). Kummer trouve ainsi les premiers nombres premiers irréguliers à savoir 37, 59, 67 et 101. Par la suite il développe sa théorie des nombres idéaux, basée sur le théorème fondamental de l'arithmétique qui dit que tout nombre entier peut être factorisé de façon unique. On obtient ainsi une structure algébrique comprise dans un anneau. Par exemple la structure  $4k+1$  (formant un anneau) si on prend l'exemple de 441

$$441 = 21 \times 21$$

$4 \times 110 + 1 = (4 \times 20 + 1)(4 \times 20 + 1)$  est une décomposition possible mais pas unique car on peut aussi avoir :  $441 = 9 \times 49$

$$4 \times 110 + 1 = (4 \times 2 + 1)(4 \times 12 + 1).$$

Cependant, si on prend la structure  $4k+3$  alors la décomposition de 441 devient unique :

$$441 = 3^2 \times 7^2$$

$$441 = (4 \times 0 + 3)^2 (4 \times 1 + 1)^2.$$

Kummer parvient ainsi à palier le problème de non unicité, il ajouta ces nombres idéaux aux précédents. La factorisation devenait unique, les lois de l'arithmétique classique (addition, soustraction, multiplication, division, puissance et racine) redevenaient valables. Par ailleurs, la théorie de Kummer restait liée aux racines de l'unité et ne permettait pas de visée générale de certains problèmes de divisibilité. Elle inspira cependant d'autres de ses collègues.

sources

<http://villemin.gerard.free.fr/Wwwgvm/Type/Ideaux.htm>

<http://fr.wikipedia.org>

Le cours de J. GUALINO chapitre 2 Nombres Complexes