Le grand théorème de Fermat

Henri Cohen

LE GRAND "THÉORÈME" DE FERMAT

HENRI COHEN

1. Les Triangles Pythagoriciens

Tout le monde connaît le théorème de Pythagore $a^2 + b^2 = c^2$, où a, b et c représentent les longueurs des trois côtés d'un triangle rectangle dont c est l'hypoténuse. Les mathématiciens grecs étaient obnubilés par la notion de *rationalité*, et il était naturel qu'ils s'intéressent aux cas où a, b et c sont des nombres rationnels. En fait, la découverte par l'école de Pythagore de l'irrationalité de $\sqrt{2}$, considéré comme l'hypoténuse d'un triangle rectangle dont les autres cotés sont de longueur 1, a provoqué une véritable révolution philosophique, un peu semblable à celle qu'a provoqué au 20e siècle le *théoreme d'incomplétude* de K. Gödel, affirmant (en gros) qu'une théorie mathématique suffisamment développée pour inclure la théorie des nombres entiers ne sera jamais "complète", c'est à dire qu'il restera toujours une infinité d'énoncés qui ne sont ni démontrables ni falsifiables.

Les triangles rectangles dont les trois côtés sont rationnels sont donc naturellement appelés pythagoriciens. Le plus célèbre est $(3, 4, 5)$ puisque $3^2 + 4^2 = 5^2$. Autre exemple: $(5, 12, 13)$.

Exercice 1. [D1]:

(1) montrer que tout triangle pythagoricien est de la forme $a = r(s^2 - t^2)$, $b = 2rst$, $c = r(s^2 + t^2)$, où r est un rationnel positif quelconque, et s et t sont deux entiers positifs premiers entre eux et de parité opposée avec $s > t$.

(2) Montrer que si a, b et c sont des entiers premiers entre eux deux à deux (ou dans leur ensemble, c'est la même chose) alors $r = 1$.

Exercice 2. [D3]:

(1) Le triangle $(3, 4, 5)$ est de surface $3.4/2 = 6$. Construire un triangle pythagoricien de surface 5 (on pourra utiliser l'exercice 1).

(2) Plus généralement, en utilisant l'exercice 1 et un petit programme, faire une table *d'entiers* inférieurs ou égaux à 100 qui sont la surface d'un triangle pythagoricien, et faire quelques remarques sur cette table.

Exercice 3 [D4] (extrait d'un problème de CAPES): On rappelle que l'anneau des entiers de Gauss $\mathbb{Z}[i] = \{A = a + bi,\ a,\ b \in \mathbb{Z}\}$ est un anneau possédant une division euclidienne naturelle, et des propriétés très semblables à celles de $\mathbb{Z}$, telle que l'existence d'un PGCD. En particulier ± 1 et $\pm i$ sont ses seuls éléments inversibles.

(1) Montrer que si $A^2 + B^2 = C^2$ avec A, B, et C dans $\mathbb{Z}[i]$ on a une formule analogue à celle de l'exercice 1.

(2) On considère un cube dans $\mathbb{R}^3$ dont tous les sommets sont à coordonnées entières, et on choisit les coordonnées de telle manière qu'un sommet soit

à l'origine. On appelle (x_i, y_i, z_i) $(i = 1, 2, 3)$ les coordonnées des trois sommets du cube reliés à l'origine. Montrer que la matrice

$$M = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix}$$

vérifie $M \cdot M^t = r \cdot I$, où M^t désigne la matrice transposée, r est un scalaire strictement positif, et I la matrice identité.

(3) On pose $A = x_1 + iy_1$, $B = x_2 + iy_2$, $C = i(x_3 + iy_3)$. Montrer que $M^t \cdot M = r \cdot I$ et en déduire que $A^2 + B^2 = C^2$.

(4) Déduire de la première question une paramétrisation complète des cubes à coordonnées entières.

Fermat s'est intéressé à ce type de sujet dans plusieurs directions différentes, et ce qui est tout à fait remarquable est que deux de ces directions l'ont mené à un même résultat. Le premier est le problème des *nombres congruents*, le second est le grand "théorème" de Fermat.

Avant de considérer ces problèmes, faisons un détour par la théorie des *courbes elliptiques*, dont on peut raisonnablement tracer l'origine dans les travaux de Fermat susmentionnés.

2. Les courbes elliptiques

La théorie des courbes elliptiques requièrerait plusieurs livres à elle seule. Il va donc être impossible de la résumer en une ou deux pages.

Commençons par une définition un peu bizarre mais essentiellement correcte:

Définition 2.1. *Une courbe elliptique définie sur un corps K est une courbe plane définie par une équation $f(x, y) = 0$ ayant les propriétés suivantes:*

(1) *C'est une cubique: en d'autres termes $f(x, y)$ est un polynôme dont le degré total en x et y est égal à 3:*

$$f(x, y) = a_1y^3 + a_2y^2x + a_3yx^2 + a_4x^3 + a_5y^2 + a_6yx + a_7x^2 + a_8y + a_9x + a_{10} .$$

(2) *Cette cubique, considérée comme une courbe* projective*, est* non singulière*. Ceci est presque équivalent au fait que les dérivées partielles de $f(x, y)$ par rapport à x et à y ne s'annulent pas simultanément quand $f(x, y) = 0$.*

(3) *Il existe un point (projectif) à coefficients dans le corps K sur la courbe.*

Ne vous inquiétez pas si vous ne connaissez pas la géométrie projective, nous n'en aurons pas vraiment besoin, mais sachez que c'est le cadre naturel dans lequel on étudie la géométrie algébrique, et en particulier les courbes.

Des raisonnements algébriques, mais basés sur des considérations géométriques, permettent de montrer qu'à un changement rationnel de coordonnées près, on peut se ramener à l'étude de cubiques de la forme

$$f(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) .$$

De plus, si le corps de base est de caractéristique différent de 2 et 3, on se ramène à la forme très simple $f(x, y) = y^2 - (x^3 + ax + b)$.

La première raison pour laquelle on s'intéresse aux courbes cubiques est banale: le degré 1 correspond aux droites, peu intéressantes, et le degré 2 aux *coniques*, étudiées en grand détail depuis l'antiquité grecque. Donc c'est le cas suivant dans

la hiérarchie des degrés. En fait, cette hiérarchie n'est pas mathématiquement intéressante: la notion de complexité d'une courbe est bien sûr liée à son degré, mais la bonne notion est la notion de *genre* que je ne peux définir ici: les droites et coniques sont de genre 0, les courbes elliptiques de genre 1.

Mais la deuxième raison pour laquelle on s'intéresse aux cubiques planes est beaucoup plus importante: on peut définir dessus de manière naturelle une *loi de composition interne*. En effet, si P_1 et P_2 sont sur la cubique, la droite passant par P_1 et P_2 (ou la tangente à la courbe si $P_2 = P_1$) coupe la courbe en trois points, et on connaît deux d'entre eux, P_1 et P_2, donc le troisième point d'intersection P_3 a des coordonnées qui s'expriment facilement et rationnellement en fonction de celles de P_1 et P_2.

Il en résulte que si l'on connaît ne serait-ce qu'un seul point sur la courbe, en utilisant ce processus appelé naturellement sécante (quand $P_2 \neq P_1$) et tangente (quand $P_2 = P_1$), on peut la plupart du temps construire une *infinité* de points sur la courbe à coordonnées dans le même corps K, par exemple rationnelles si $K = \mathbb{Q}$.

Et ceci est bien entendu vrai pour toute équation qui peut se ramener à une équation cubique.

Pour terminer cette très brève introduction aux courbes elliptiques, notons que la loi de composition interne que l'on utilise n'est pas tout à fait la loi qui à (P_1, P_2) associe P_3 comme ci-dessus, mais son "symétrique" par rapport à un point origine: dans le cas d'une équation $f(x, y) = y^2 - (x^3 + ax + b)$, c'est le point obtenu de P_3 en changeant y en $-y$.

Remarque: le mot "elliptique" provient du calcul de la longueur d'un arc *d'ellipse*, qui s'effectue à l'aide de *fonctions elliptiques* qui paramétrisent naturellement une courbe elliptique, comme les fonctions trigonométriques paramétrisent naturellement un cercle. Ces fonctions elliptiques interviennent dans beaucoup de calculs d'intégrales, outre la rectification d'une ellipse, également dans le calcul de la période d'un pendule, etc...

3. Le problème des nombres congruents

Disons tout de suite que c'est le dernier problème de l'antiquité grecque (plus précisément de Diophante d'Alexandrie) qui n'est toujours pas complètement résolu (mais presque, voir plus loin).

Définition 3.1. *On dit qu'un entier n est un nombre* congruent *si c'est la surface d'un triangle pythagoricien, c'est-à-dire d'un triangle rectangle dont les trois côtés sont rationnels.*

Si vous avez fait l'exercice 2, vous voyez que 5 et 6 sont des nombres congruents, et vous avez même peut-être construit une petite table de tels nombres inférieurs à 100.

Le résultat facile suivant est fondamental:

Proposition 3.2. *Un nombre entier positif n est congruent si et seulement si il existe un point (x, y) à coordonnées rationnelles non nulles sur la courbe elliptique $f(x, y) = 0$ avec $f(x, y) = y^2 - x(x^2 - n^2)$. Plus précisément si (a, b, c) est un triangle pythagoricien de surface n, les quatre points $(a(a + \varepsilon c)/2, a^2(a + \varepsilon c/2))$ et $(b(b + \varepsilon c)/2, b^2(b + \varepsilon c)/2)$ avec $\varepsilon = \pm 1$ sont de tels points. Réciproquement, un tel point (x, y) fournit un triangle pythagoricien de surface n avec $a = |y/x|$, $b = 2n|x/y|$, $c = (x^2 + n^2)/|y|$.*

Exercice 4. [**D1**]: démontrer cette proposition.

Exercice 5. [**D3**]: en utilisant la loi de composition interne sur les courbes elliptiques décrite ci-dessus, montrer que si n est un nombre congruent il existe une *infinité* de triangles pythagoriciens de surface n (bien entendu on considère deux triangles comme distincts s'ils n'ont pas les mêmes côtés).

Si vous avez construit une petite table comme ci-dessus, vous voyez qu'il y a des entiers inférieurs à 100 dont la nature (congruent ou non) n'a pas été déterminée: ceci ne veut bien sûr pas dire qu'ils ne sont pas congruents: il est possible qu'en poussant les calculs plus loin vous puissiez en trouver d'autre. En d'autres termes, montrer qu'un nombre n'est *pas* congruent est à priori beaucoup plus difficile (à postériori ce n'est pas tout à fait vrai: le nombre 157 est congruent, mais je vous défie de le montrer sans tricher). Le résultat profond (lire "difficile") de Fermat sur ce sujet est le suivant:

Théorème 3.3. *Le nombre* 1 *n'est pas un nombre congruent.*

D'après la proposition ci-dessus, ceci est donc équivalent à dire que si x et y sont des nombres rationnels tels que $y^2 = x^3 - x$, alors $y = 0$, et donc $x = 0$ ou $x = \pm 1$.

Fermat a démontré ce théorème en utilisant sa "méthode de descente infinie" qu'il a inventée, et qui est extrêmement utile. En gros, il montre que si (x, y) est une solution (avec $y \neq 0$), on peut en construire une "plus petite".

Exercice 6. [**D7**] Essayer de reconstruire la démonstration de Fermat, sans tricher. Si vous y arrivez sans aide ni livre, contactez moi, je connais peu de personnes capables de le faire. Mais ce n'est pas impossible: voir le problème 8 comme exemple de la méthode de descente.

Le *problème des nombres congruents* consiste à déterminer quels nombres sont congruents, ou du moins de donner un critère simple. Ce problème date donc essentiellement du III-ième siècle de notre ère.

Après de nombreux calculs sur ordinateur, qui ont augmenté notre liste de nombres congruents mais pas vraiment fait progresser le problème, le premier pas fondamental a été fait en 1970 grâce à l'utilisation d'une des conjectures les plus importantes de la théorie des nombres, la conjecture BSD du nom de ses inventeurs, Birch et Swinnerton-Dyer. Ceci permet pour chaque entier n de déterminer rapidement mais conjecturalement s'il est congruent ou non, puis d'essayer d'en déduire une "vraie" démonstration. Au moins, il n'y a plus d'incertitude, même si la démonstration peut manquer.

Le deuxième (et dernier) pas fondamental a été effectué en 1982 par Tunnell, qui a finalement donné un critère très simple pour déterminer si un nombre est congruent ou non, vérifiable en quelques microsecondes sur ordinateur. Malheureusement, la véracité de son critère dépend d'une forme très faible de la conjecture BSD, et c'est pourquoi on dit que le problème est "presque", mais pas complètement, résolu.

4. Le problème (grand "théorème") de Fermat

Fermat s'est aussi posé le problème de généraliser les triangles pythagoriciens à des puissances plus élevées que 2: plus précisément, puisqu'il existe des entiers a, b et c tels que $a^2 + b^2 = c^2$ (et même une infinité), serait-il possible qu'il existe des entiers (non nuls) tels que $a^3 + b^3 = c^3$, ou plus généralement $a^n + b^n = c^n$ pour $n \geq 3$? Il est bien connu que Fermat a écrit ceci dans la marge du livre d'arithmétique de Diophante d'Alexandrie, avec une remarque disant en substance

qu'il avait une démonstration merveilleuse de ce fait mais que la marge était trop étroite, etc...: il est désormais universellement admis que Fermat n'avait pas une telle démonstration. En fait, il a écrit ceci quand il était relativement jeune, cette annotation a été trouvée après sa mort, et il est probable qu'il n'a jamais imaginé que quiconque la lise, et qu'il aurait probablement lui-même dit qu'il s'était laissé emballer.

Mais revenons à la question de Fermat: il y a un raisonnement très simple qui permet de se convaincre que la réponse à sa question est probablement négative: considérons l'ensemble des entiers de la forme $a^n+b^n-c^n$ qui sont en valeur absolue plus petit que X. Très en gros, ceci implique que a^n, b^n et c^n sont plus petits que X, donc a, b et c plus petits que $X^{1/n}$. Il y a donc approximativement $X^{3/n}$ triplets (a, b, c) possibles, donc au plus $X^{3/n}$ valeurs de $a^n + b^n - c^n$, parmi les nombres plus petits que X en valeur absolue. On voit donc qu'il y a une distinction très marquée entre trois ensembles de valeurs de n:

(1) Si $n = 1$ ou $n = 2$, $X^{3/n}$ est beaucoup plus grand que $2X$, donc il y a une très forte chance que l'on obtienne 0 parmi toutes ces valeurs.
(2) Si $n = 3$, $X^{3/n} = X$, et il y a alors une chance raisonnable que l'on obtienne 0.
(3) Si $n \geq 4$, $X^{3/n} \leq X^{3/4}$ est négligeable par rapport à X, et donc il y a très peu de chance d'obtenir 0.

Bien que ce raisonnement soit très approximatif, il est en fait qualitativement correct. Et d'ailleurs, je suggère de faire l'exercice suivant:

Exercice 7. **[D3]**: En utilisant le même "raisonnement" que ci-dessus, "montrer" ce qui suit. On considère l'équation plus générale $a^p + b^q = c^r$ avec p, q et r entiers plus grands où égaux à 2. On pose $\chi = 1/p + 1/q + 1/r$ (ce qui est l'équivalent de $3/n$ ci-dessus).

(1) Si $\chi > 1$, il y a de très fortes chances que l'équation soit soluble, si $\chi = 1$ il y a une chance raisonnable, si $\chi < 1$ il y a très peu de chance.
(2) On suppose par exemple que $p \leq q \leq r$. Montrer (cette fois-ci rigoureusement) que $\chi > 1$ équivaut soit à $p = q = 2$ et $r \geq 2$ quelconque, soit à $p = 2$, $q = 3$, et $r = 3$, 4, ou 5, puis montrer que $\chi = 1$ équivaut à $(p, q, r) = (2, 3, 6)$, $(2, 4, 4)$ ou $(3, 3, 3)$.
(3) Montrer enfin (rigoureusement) que si $\chi < 1$ alors $\chi \leq 41/42$.

Tout ceci est bien joli, mais ne résoud pas vraiment la question de Fermat. Nous dirons que le "theorème" de Fermat est vrai pour n s'il n'existe pas d'entiers non nuls a, b et c tels que $a^n + b^n = c^n$.

Le premier résultat qu'il a obtenu, à nouveau en utilisant sa *méthode de descente infinie*, est que son équation est effectivement impossible pour $n = 4$. Plus précisément:

Théorème 4.1. *(Fermat). Si a, b et c sont non nuls on ne peut pas avoir $a^4+b^4 = c^2$. A fortiori, le théorème de Fermat est vrai pour $n = 4$.*

Problème 8. **[D6]** Le but de ce problème est de démontrer le théorème ci-dessus par la méthode de descente infinie de Fermat. On suppose donc que $a^4 + b^4 = c^2$ avec a, b et c entiers strictement positifs, et on suppose que c a été choisi le plus petit possible.

(1) Montrer que a, b et c sont premiers entre eux deux à deux, que c est impair en regardant modulo 4, et que a est impair et b est pair en échangeant a et b si nécessaire.
(2) En utilisant l'exercice 1, il existe donc s et t positifs premiers entre eux de parité opposée tels que $a^2 = s^2 - t^2$ et $b^2 = 2st$. Montrer que s est pair et t impair, et en déduire qu'il existe u et v positifs premiers entre eux de parité opposée tels que $a = u^2 - v^2$, $s = u^2 + v^2$ et $t = 2uv$.
(3) De l'équation $(b/2)^2 = uv(u^2+v^2)$ en déduire que $u = u_1^2$, $v = v_1^2$, $u^2+v^2 = w^2$, donc que $u_1^4 + v_1^4 = w^2$, ce qui est la même équation qu'au début.
(4) Montrer que $w < c$ et en déduire une contradiction.

Le résultat le plus difficile que Fermat a (probablement) réussi à démontrer est le suivant:

Théorème 4.2. *(Fermat, Euler). Le théorème de Fermat est vrai pour $n = 3$.*

Exercice 9. **[D2]**. On suppose que a, b et c sont des entiers tels que $a^3+b^3 = c^3$.
(1) Montrer en raisonnant modulo 9 que l'un des trois entiers est divisible par 3.
(2) En partant de $1^3 + 2^3 = 9$ et en raisonnant par récurrence sur $k \geq 2$, montrer qu'il existe $a \equiv 1 \pmod 3$ tel que $a^3 + 2^3 \equiv 0 \pmod{3^k}$.

Ce dernier résultat montre qu'on ne peut pas démontrer Fermat pour $n = 3$ en se servant uniquement de congruences.

Problème 10. **[D8]**. Montrer le théorème de Fermat pour $n = 3$, c'est-à-dire le théorème ci-dessus.

Même commentaire que pour l'exercice 6: contactez moi si vous arrivez à le faire sans tricher. Toutefois, ce qui suit pourra vous aider.

Nous avons vu que le problème des nombres congruents peut se reformuler comme un problème sur l'existence de points à coordonnées rationnelles sur une courbe elliptique. C'est également le cas ici pour $n = 3$, et ce n'est pas étonnant puisque c'est une cubique. Mais le fait est général. On a la proposition facile suivante:

Proposition 4.3. *Soit n un entier impair, et a, b, c des entiers. Si $ax^n+by^n = cz^n$ avec $x \neq 0$, alors le point (X, Y) est sur la courbe $Y^2 - (X^n + a^2(bc)^{n-1}/4) = 0$, avec*

$$X = bcyz/x^2 \quad et \quad Y = (bc)^{(n-1)/2}(by^n + cz^n)/(2x^n) \; .$$

Exercice 11. **[D1]**: démontrer cette proposition.

On voit donc que le problème de Fermat pour $n = 3$ se ramène à montrer qu'il n'existe pas de point à coordonnées rationnelles sur la courbe elliptique $Y^2 - (X^3 + 1/4) = 0$, ce qui comme je l'ai mentionné n'est pas très facile.

Par contre, on peut utiliser cette proposition d'une manière positive, et c'est ce qu'a fait Fermat en posant le défi suivant à ses collègues anglais:

Exercice 12. **[D3]**: Trouver trois entiers strictement positifs x, y, et z tels que $x^3 + y^3 = 9z^3$ autres que $(x, y) = (1, 2)$ et $(2, 1)$.

Indication: grâce à la proposition, on se ramène à une courbe elliptique de forme simple, puis on utilise la loi de composition interne (qu'on peut d'ailleurs utiliser directement sur la cubique $X^3 + Y^3 - 9 = 0$ si on préfère). On trouve ainsi un certain nombre de (x, y, z) avec certaines coordonnées négatives, mais en persévérant on en trouve avec toutes les coordonnées positives.

5. Les premières avancées: la théorie algébrique des nombres

Fermat a donc (probablement) résolu son problème pour $n = 3$ et $n = 4$. Il est immédiat de voir qu'il suffit donc de considérer son problème pour $n = p \geq 5$ un nombre premier.

Diverses avancées ont été faites au 18-ième siècle et au début du 19-ième, mais la véritable percée est venu avec les travaux de Kummer au milieu du 19-ième.

Depuis Gauss (et même avant), il est apparu qu'il était nécessaire d'agrandir l'anneau des entiers naturels $\mathbb{Z}$ en un anneau plus grand, qu'on appelle un anneau *d'entiers algébriques*, l'exemple de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss étant le plus simple.

Dans le cas du problème de Fermat, on pose $\zeta = \zeta_p = e^{2\pi i/p}$ une racine p-ième de 1 différente de 1, et on considère l'anneau

$$A_p = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}\} ,$$

où les a_i sont dans $\mathbb{Z}$.

Exercice 13. [**D1**]: En utilisant le fait que ζ est racine d'un polynôme de degré $p-1$ que l'on explicitera, montrer que A_p est effectivement un anneau commutatif unitaire.

En fait, les premiers mathématiciens à considérer ce type d'anneau ont eu de la chance: tout d'abord le polynôme de degré $p-1$ ci-dessus se trouve être *irréductible*, ou de manière équivalente ζ n'est pas racine d'un polynôme de degré plus petit à coefficients rationnels.

Exercice 14. [**D4**]: démontrer ceci en considérant le polynôme satisfait par $\zeta - 1$.

Mais surtout, cet anneau est "maximal" en un sens que je ne peux pas définir ici. Mais je donne un contre-exemple: puisque ζ_3 est égal à $(-1+\sqrt{-3})/2$, à la place de l'anneau $A_3 = \{a_0+a_1\zeta_3\}$ on pourrait considérer le sous-anneau $A_3' = \{b_0+b_1\sqrt{-3}\}$. Et justement, comme c'est un sous-anneau il n'est pas "maximal" donc ne convient pas.

Bref, l'anneau A_p se trouve heureusement être le bon.

Associés à un anneau comme celui-ci, il y a deux *groupes abéliens* qui sont absolument fondamentaux.

• Le premier est le groupe des *unités*: ce sont les éléments $\alpha \in A_p$ dont l'inverse $1/\alpha$ est aussi dans A_p. Les exemples les plus simples sont: le groupe des unités de $\mathbb{Z}$, qui est le groupe à 2 éléments $\{\pm 1\}$, le groupe des unités de l'anneau des entiers de Gauss $\mathbb{Z}[i]$, qui est le groupe à 4 éléments $\{\pm 1,\ \pm i\}$, le groupe des unités de l'anneau A_3 considéré ci-dessus, qui est le groupe à 6 éléments $\{\pm 1,\ \pm\zeta_3,\ \pm\zeta_3^2\}$.

Ces exemples donneraient à penser que le groupe des unités est toujours fini: ceci est en fait totalement faux: parmi les anneaux A_p pour $p \geq 3$ premier il n'y a que A_3 dont le groupe des unités est fini. On montre que la dimension (en un sens convenable) du groupe des unités de A_p est égale à $(p-3)/2$, donc égale à 0 seulement pour $p = 3$.

Je donne un exemple d'unité qui n'est pas une racine de l'unité pour $p = 5$: on remarque que si $\zeta = \zeta_5$ est une racine primitive 5-ième de l'unité, on a l'identité

$$1 + \zeta = \frac{1-\zeta^2}{1-\zeta} = \frac{1-\zeta^2}{1-\zeta^6} = \frac{1}{1+\zeta^2+\zeta^4} .$$

On a bien entendu $u = 1 + \zeta \in A_5$, et puisque $1/u = 1 + \zeta^2 + \zeta^4$, on a aussi $1/u \in A_5$, donc u est une unité de A_5 (qui ne peut pas être une racine de l'unité puisque son module n'est pas égal à 1).

Exercice 15 [D1] Soit A un anneau commutatif unitaire. Montrer que $\alpha A = \beta A$ si et seulement si $\beta = \alpha u$ pour une unité $u \in A$.

• Le deuxième groupe abélien associé à A_p est le *groupe de classes d'idéaux*, qui est un peu plus délicat à définir. J'y reviendrai, mais notons dès à présent les deux propriétés suivantes: c'est un groupe abélien fini, et d'autre part il "mesure" l'écart qu'a l'anneau à posséder la propriété (comme $\mathbb{Z}$) d'avoir unicité de la factorisation en premiers.

Voyons tout de suite comment sont utilisés les nombres algébriques, ici les anneaux A_p. Considérons d'abord l'exposant 3: on *factorise* le polynôme x^3+y^3 dans l'anneau $A_3 = \{a + b\zeta\}$ avec $\zeta = \zeta_3$, et on écrit donc

$$x^3 + y^3 = (x + y)(x + \zeta y)(x + \zeta^2 y) = z^3 \ .$$

Plus généralement, si p est un nombre premier impair et $\zeta = \zeta_p$, on peut écrire

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

Nous avons donc un produit d'éléments de A_p égal à une puissance p-ième. Si ces éléments sont "premiers entre eux", ce qui a un sens quand A_p possède la propriété de factorisation unique, cela implique que chaque facteur est un une puissance p-ième, mais attention, à multiplication par une unité près: regardez déjà dans $\mathbb{Z}$: si $xy = z^2$ et x et y sont premiers entre eux, on en déduit que x et y sont des carrés à une unité près, donc ici soit $x = u^2$ et $y = v^2$, soit $x = -u^2$ et $y = -v^2$.

Pour le problème de Fermat, il est évident que l'on peut supposer x et y entiers premiers entre eux (sinon on divise toute l'équation par le PGCD à la puissance p). Remarquant que $x + y - (x + \zeta y) = (1 - \zeta)y$ et $x + \zeta y - \zeta(x + y) = (1 - \zeta)x$, il en résulte que le PGCD de $x + y$ et $x + \zeta y$ est un diviseur de $1 - \zeta$. Il est facile de montrer que $1 - \zeta$ est un élément premier qui divise p, et on en déduit donc que le PGCD est égal soit à 1 soit à $1 - \zeta$, et qu'il ne peut être égal à $1 - \zeta$ que si p divise z.

Notons dès à présent que cette différence est fondamentale et fait que l'on distingue deux **cas** du problème de Fermat: le **premier cas** est quand on suppose que aucun de x, y, ou z n'est divisible par p, le **deuxième cas** quand l'un deux est divisible par p.

Revenant à notre étude, on en déduit donc que, dans le premier cas tout au moins, on a $x + y = u\alpha^p$ et $x + \zeta y = v\beta^p$, où α et β sont dans A_p, et u et v sont des unités de A_p (ceci est bien entendu aussi vrai pour les $x+\zeta^k y$ pour $k \geq 2$, mais c'est en fait une conséquence du cas $k = 1$).

A partir de là, des considérations assez techniques mais pas trop difficiles (une page) permettent de montrer que l'équation de Fermat est effectivement impossible dans le premier cas. Des considérations similaires mais beaucoup plus techniques (5 pages) montrent qu'elle est également impossible dans le deuxième cas.

Ceci est une victoire majeure sur ce problème: en particulier, les *unités*, qui posent un véritable problème en général, sont ici apprivoisées.

Bien entendu, rappelons nous que pour faire tout ce travail nous avons fait l'hypothèse fondamentale de l'existence et unicité à unité près d'un PGCD. D'ailleurs

il est facile de démontrer pour les anneaux $A = A_p$ (et c'est également vrai en beaucoup plus grande généralité) que les propriétés suivantes sont équivalentes:

(1) Il existe un PGCD unique à unité près.
(2) On a la propriété de factorisation unique en éléments premiers à unité près (on dit que l'anneau est *factoriel*).
(3) Tout idéal est principal, c'est-à-dire de la forme αA pour un élément $\alpha \in A$ (on dit que l'anneau est *principal*).

Malheureusement, on peut montrer que ces propriétés sont vraies pour A_p si et seulement si $p \leq 19$. On a donc démontré (moyennant les détails techniques que je ne vous ai pas donnés) Fermat pour $p = 3$, 5, 7, 11, 13, 17 et 19, ce qui est bien mais loin d'être suffisant.

L'idée d'utiliser les éléments de A_p (les nombres algébriques) dans l'étude du théorème de Fermat nécessite déjà l'étude des anneaux de ce type, donc est le début de la *théorie algébrique des nombres*. Mais la véritable révolution est venue des travaux de Kummer et successeurs avec la notion *d'idéal* (Kummer utilisait une notion légèrement différente).

Rappelons qu'un idéal I d'un anneau (commutatif) A est un sous-groupe additif stable par multiplication par les éléments de A ($x \in A$ et $y \in I$ impliquent $xy \in I$). Les idéaux les plus simples sont les idéaux *principaux*, ensemble des multiples αA d'un même élément $\alpha \in A$, car ce sont "presque" eux-mêmes des éléments.

Le produit de deux idéaux se définit aisément: si I et J sont deux idéaux IJ est l'ensemble des *combinaisons linéaires* de produits d'un élément de I par un élément de J (l'ensemble des produits lui-même n'est pas un sous-groupe additif).

On définit aussi de manière naturelle la notion d'idéal *premier*, et le résultat (facile) qui justifie complètement l'introduction de cette notion d'idéal est le suivant (attention: ici et dans la suite, pour les anneaux A_p, mais pas en général):

Proposition 5.1. *Tout idéal non nul de A_p est un produit de puissances d'idéaux premiers de manière unique (à permutation près des facteurs bien sûr).*

En d'autres termes, on a bien la propriété voulue (unicité de la décomposition en premiers) pour faire marcher la démonstration de Fermat, mais *au niveau des idéaux*. (Notez que la proposition ci-dessus est facile à démontrer, après une légère introduction à la théorie algébrique des nombres.)

Justement, revenons à la démonstration de Fermat: soit $I_k = (x+\zeta^k y)A_p$ l'idéal principal engendré par $x + \zeta^k y$, et appelons $J = zA_p$ l'idéal principal engendré par z. La factorisation en éléments vue ci-dessus donne maintenant la factorisation en idéaux $I_0 I_1 I_2 \cdots I_{p-1} = J^p$. Grâce à la proposition ci-dessus, sans aucune restriction sur p on en déduit que chaque I_k est aussi une puissance p-ième, donc $I_k = (x + \zeta^k y)A_p = U_k^p$ pour un certain idéal U_k.

Le problème est qu'en passant aux idéaux on a gagné ceci, tout à fait remarquable, mais on a aussi perdu puisque un idéal n'est pas un élément, sauf s'il est principal auquel cas il est "presque" un élément.

Pour résoudre ce problème, on introduit une relation d'équivalence entre idéaux, toujours supposés non nuls dans la suite:

Définition 5.2. *On dit que deux idéaux non nuls I et J sont équivalents si on peut passer de l'un à l'autre par multiplication par des idéaux principaux: $I \sim J$ si et seulement si il existe α et $\beta \in A$ non nuls tels que $\beta I = \alpha J$.*

Le quotient $Cl(A)$ de l'ensemble des idéaux non nuls par cette relation d'équivalence est donc à nouveau un ensemble muni de la multiplication. On montre très facilement la proposition suivante:

Proposition 5.3. *$Cl(A)$ est un groupe abélien, appelé le* groupe de classes d'idéaux *(ou simplement le groupe de classes) de A.*

L'élément neutre de $Cl(A)$ est bien entendu la classe d'équivalence de tous les idéaux principaux de A.

Mais le résultat le plus important et un peu plus difficile est le théorème suivant:

Théorème 5.4. *Le groupe abélien $Cl(A)$ est un groupe* fini *dont le cardinal, noté $h(A)$, est bien entendu appelé le* nombre de classes *de A.*

Ce théorème est important pour la raison suivante: vous devez savoir (c'est un résultat facile mais crucial de théorie des groupes) que si H est un groupe fini de cardinal h et d'élément neutre e, alors pour tout $x \in H$ on a $x^h = e$:

Exercice 16 [D2].

(1) Démontrer le résultat ci-dessus.
(2) En appliquant ceci au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, en déduire que si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} \equiv 1 \pmod{p}$ (en d'autres termes $a^{p-1} - 1$ est divisible par p): ceci est le "petit" théorème de Fermat.

Dans notre contexte, on en déduit donc le corollaire suivant:

Corollaire 5.5. *Pour tout idéal I de A_p l'idéal $I^{h(A_p)}$ est un idéal principal.*

Puisque $(x + \zeta^k y)A_p = U_k^p$, l'idéal U_k^p est principal. D'après ce corollaire, il en va de même de U_k^h ($h = h(A_p)$). Or puisque p est un nombre premier, si p ne divise pas h il est premier avec h, donc d'après l'identité de Bezout il existe des entiers a et b tels que $ah + bp = 1$, donc $U_k = (U_k^h)^a (U_k^p)^b$. Or U_k^h est principal d'après le corollaire, et $U_k^p = (x + \zeta^k y)A_p$ est principal par construction. Il en résulte donc que U_k lui-même est principal!

C'est la clé de la démonstration: on a eu besoin des idéaux, mais maintenant on a presque fini d'en être débarrassé: puisque U_k est principal nous pouvons écrire $U_k = \alpha_k A_p$ pour un élément $\alpha_k \in A_p$. On a donc $(x + \zeta^k y)A_p = U_k^p = \alpha_k^p A_p$, et donc d'après l'exercice 15, $x + \zeta^k y = u_k \alpha_k^p$ pour une certaine unité u_k. Ceci est exactement la conclusion à laquelle nous étions parvenus en supposant que l'anneau A_p était factoriel, et on en déduit donc le théorème de Fermat pour l'exposant p.

Mais **attention**, tout ceci a été possible parce qu'on a supposé que p ne divise pas le nombre de classes $h = h(A_p)$. Or ceci n'est pas toujours vrai. Malgré tout, voyons ce qu'on peut dire.

Définition 5.6. *On dit qu'un nombre premier p est* régulier *s'il ne divise pas $h(A_p)$.*

Le théorème de Fermat est donc vrai pour tous les nombres premiers réguliers. Il existe un critère très facile pour tester si un nombre premier est régulier ou pas, et à l'aide de ce critère on montre que les seuls nombres premiers *irréguliers* inférieurs à 100 sont 37, 59 et 67. On a donc fait un progrès remarquable puisqu'on a démontré Fermat pour tous les nombres premiers réguliers, donc par exemple pour tous les nombres premiers inférieurs à 100 à l'exception des trois ci-dessus.

Notez au passage qu'il est facile de prouver qu'il existe une infinité de nombres premiers irréguliers, mais que, paradoxalement, on ne sait pas prouver qu'il existe une infinité de nombres premiers réguliers, bien qu'expérimentalement il y en ait une proportion de $e^{-1/2} \approx 0.607...$ parmi les nombres premiers.

Les travaux de Kummer, suivis de ses successeurs tels que Dirichlet, Dedekind, Kronecker, et d'autres ont véritablement créé cette branche de la théorie des nombres appelée la théorie algébrique des nombres, qui a de nombreuses et importantes applications pour bien d'autres problèmes que celui de Fermat.

6. Avancées ultérieures utilisant la théorie algébrique des nombres

La théorie algébrique des nombres était loin d'avoir dit son dernier mot. Les avancées suivantes sont dues à l'utilisation d'un nouvel outil appelé les *lois de réciprocité* supérieures. Je décris brièvement la plus simple et la plus célèbre des lois de réciprocité, due à Legendre et Gauss, la loi de réciprocité quadratique, parfois considérée comme le théorème le plus élégant de toutes les mathématiques. On peut l'énoncer de la manière suivante.

Définition 6.1. *Soit p un nombre premier et a un entier non divisible par p. On dit que a est un* résidu quadratique *modulo p si il existe x tel que $x^2 - a$ soit divisible par p (on écrit $x^2 \equiv a \pmod{p}$, x^2 est congru à a modulo p).*

Théorème 6.2. *Soient p et q deux nombres premiers impairs distincts.*

1. *Si p ou q est congru à 1 modulo 4, alors p est un résidu quadratique modulo q si et seulement si q est un résidu quadratique modulo p.*
2. *Si p et q sont tous deux congrus à 3 modulo 4, alors p est un résidu quadratique modulo q si et seulement si q n'est* pas *un résidu quadratique modulo p.*

Bien que relativement élémentaire, ce beau résultat possède litéralement des centaines de démonstrations plus ou moins différentes.

Il n'y a bien entendu pas de raison de se limiter aux résidus *quadratiques*, et on peut plus généralement considérer les congruences $x^\ell \equiv a \pmod{p}$ pour de plus grands exposants ℓ. Ceci a conduit à des recherches extrêmement fécondes, d'abord par Gauss lui-même ($\ell = 3$ et $\ell = 4$), puis par Eisenstein (ℓ premier quelconque) pour culminer en 1920 par la *loi de réciprocité d'Artin*, qui est l'un des théorèmes fondamentaux de ce qui est probablement le sommet de la théorie algébrique des nombres classique, la *théorie du corps de classes*.

En utilisant de manière relativement élémentaire la loi d'Eisenstein, on a pu au début du 20-ième siècle faire des avancées majeures sur le *premier cas* du théorème de Fermat (celui où on suppose que p ne divise aucune des variables). Le premier et le plus célèbre de ces résultats est dû à Wieferich:

Théorème 6.3. *Si 2^{p-1} n'est pas congru à 1 modulo p^2, alors le premier cas du théorème de Fermat est vrai.*

Rappelons que d'après le "petit" théorème de Fermat (exercice 16) 2^{p-1} est toujours congru à 1 modulo p, mais on demande ici que $2^{p-1} - 1$ soit divisible par p^2, pas seulement par p.

On ne connaît que deux nombres premiers p tels que $2^{p-1} \equiv 1 \pmod{p^2}$, à savoir $p = 1093$ et 3511, et donc le premier cas est démontré pour beaucoup plus de nombres premiers qu'avant. Notez toutefois que des considérations probabilistes

semblent indiquer qu'il existe une infinité de p tels que $2^{p-1} \equiv 1 \pmod{p^2}$, mais qu'ils sont extrêmement rares.

Le théorème de Wieferich a été généralisé par plusieurs auteurs (permettant au passage de traiter les deux cas exceptionnels 1093 et 3511), et ces méthodes permettent par exemple de démontrer le premier cas pour $p < 10^{18}$.

Les avancées sur le deuxième cas ont été beaucoup plus minces. Les seuls résultats notables en utilisant la théorie algébrique des nombres ont été obtenus en utilisant le *critère de Vandiver*: nous avons vu que si p ne divise pas le nombre de classes $h(A_p)$ alors le théorème de Fermat est vrai. En fait, on peut montrer un résultat beaucoup plus fort: au lieu de considérer A_p, on considère le sous-anneau défini dans l'exercice suivant.

Exercice 17 [D2]. De la même manière que l'on a défini A_p comme l'ensemble des combinaisons linéaires à coefficients entiers des puissances de $\zeta = \zeta_p$, on définit A_p^+ comme étant l'ensemble des combinaisons linéaires à coefficients entiers des puissances de $\zeta + 1/\zeta$. Montrer que A_p^+ est un anneau, et qu'en fait A_p^+ est égal à l'ensemble des éléments de A_p qui sont *réels*.

Le théorème un peu plus difficile mais encore classique est le suivant:

Théorème 6.4. *Si p ne divise pas le nombre de classes $h(A_p^+)$ alors le théorème de Fermat est vrai pour p.*

Remarques.

(1) Ce théorème est strictement plus fort que le théorème utilisant $h(A_p)$ car on peut montrer que $h(A_p^+)$ divise $h(A_p)$.
(2) De fait, il est tellement fort qu'on ne connaît *aucun* p qui divise $h(A_p^+)$, bien que des raisonnements probabilistes semblent indiquer qu'il devrait y en avoir une infinité, mais en proportion infime.
(3) Pire, si on trouvait un p divisant $h(A_p^+)$, on ne connaîtrait à priori aucune méthode pour démontrer le deuxième cas du théorème de Fermat en utilisant la théorie algébrique des nombres.

7. L'attaque finale: le théorème de Taylor–Wiles

La résolution finale du problème de Fermat est venue d'une direction un peu inattendue, à savoir par l'utilisation des courbes elliptiques mais dans un contexte beaucoup plus profond et totalement différent de celui vu ci-dessus. De fait, cette nouvelle attaque permet d'obtenir des résultats profonds sur toute équation du type $A + B = C$, où A, B et C sont des nombres divisibles par des grandes puissances d'entiers (Fermat étant le cas particulier $A = x^n$, $B = y^n$ et $C = z^n$). Considérons le polynôme du troisième degré $P(X) = X(X - A)(X + B)$. Son discriminant D est par définition le carré du produit des différences de ses racines (si vous ne savez pas ça, dans ce cas particulier vous pouvez retrouver la formule à partir de celle du discriminant de $X^3 + pX + q$, égal à $-(4p^3 + 27q^2)$). Donc ici $D = (A \cdot (-B) \cdot (A + B))^2 = A^2B^2C^2$ puisque $C = A + B$.

On considère alors la courbe elliptique d'équation $f(X, Y) = 0$ avec

$$f(X, Y) = Y^2 - P(X) = Y^2 - X(X - A)(X + B) .$$

Cette courbe possède un autre invariant, qu'on appelle le *conducteur* N, et qui, à des petits facteurs près que je ne peux pas préciser ici, est égal au produit des

nombres premiers divisant le discriminant, mais à la puissance 1. Dans le cas de Fermat, on a $D = (xyz)^{2n}$, donc N divise xyz.

L'idée de considérer cette courbe est due à Y. Hellegouarch. Mais l'idée d'en déduire une contradiction est due à G. Frey, donc on appelle ces courbes les *courbes de Hellegouarch–Frey*, ou plus simplement les courbes de Frey. La contradiction devrait provenir du fait que le discriminant ne devrait pas être tellement plus grand que le conducteur (en fait une conjecture due à L. Szpiro dit qu'il ne devrait pas être beaucoup plus grand que sa puissance 6-ième).

En fait, on a besoin d'une propriété légèrement différente que je décrirai très en gros ci-dessous qu'on appelle la *modularité*. J.-P. Serre, probablement l'un des meilleurs mathématiciens mondiaux, a montré que si l'on acceptait certaines conjectures techniques en plus de la modularité, ceci entrainerait Fermat.

Le premier pas décisif a été franchi par K. Ribet, qui a montré dans un article très profond et fondamental que la modularité seule suffisait pour montrer Fermat.

Cette conjecture de modularité a été faite par plusieurs éminents mathématiciens, et s'appelait la conjecture de Taniyama–Shimura–Weil du nom des principaux mathématiciens qui ont contribué, mais il y a eu une polémique sur qui a fait quoi. Peu importe.

Il a fallu attendre 1995 pour que A. Wiles annonce enfin la démonstration d'une partie de la conjecture de modularité, partie suffisante pour entraîner Fermat. Ceci a bien entendu fait grand bruit, y compris dans la presse, puisque c'était la résolution d'un problème célèbre vieux de 4 siècles.

Mais patatras, peu après on s'est aperçu, Wiles le premier, qu'il y avait une faille dans sa démonstration. Il s'est alors attelé de manière acharnée (vu l'importance) avec l'aide d'un de ses collègues R. Taylor à réparer cette faille. En fait, il n'y est pas arrivé, et pour cause, la méthode utilisée ne peut effectivement pas marcher. Mais heureusement, en utilisant une autre méthode pour l'étape finale (tout en gardant globalement l'approche initiale de Wiles) ils ont réussi à trouver une démonstration légèrement différente, qui est parfaitement correcte et publiée. Le problème de Fermat est donc devenu le théorème de Taylor–Wiles.

Pour être complet, Wiles n'avait pas complètement démontré la modularité, mais seulement la partie dont il avait besoin pour Fermat. Le théorème complet de modularité n'a été démontré que plusieurs années plus tard par Breuil-Conrad-Diamond-Taylor, en utilisant des outils similaires à ceux de Wiles, mais encore plus sophistiqués.

Avant de passer à la conclusion, je vais essayer de donner un aperçu de ce qu'est la "modularité".

Soit E une courbe elliptique donnée par exemple par une équation $f(x, y) = 0$ avec $f(x, y) = y^2 - (x^3 + ax + b)$ et a et b dans $\mathbb{Z}$. Pour chaque nombre premier p on peut compter le nombre de solutions N_p de la congruence modulo p $f(x, y) \equiv 0 \pmod{p}$. A partir de tous ces nombres, on crée grâce à une recette universelle (c'est-à dire valable pour tout système d'équations, pas seulement celle d'une courbe elliptique) une fonction d'une variable *complexe* $L(s)$. Bien que pour des raisons historiques l'école Polytechnique empêche les taupins d'apprendre la théorie des fonctions de variable complexe, cette théorie n'est pas difficile et est probablement la plus importante de toute l'analyse. Mais nous n'en avons pas besoin pour comprendre la suite: pour simplifier, considérons que $L(s)$ est une

fonction de variable réelle. Pour de simples raisons de convergence, sa construction ne permet de la définir que pour $s > 3/2$.

Pensez à une fonction très analogue, la série de Riemann $\zeta(s) = \sum_{n\geq 1} 1/n^s$: vous savez fort bien que cette série converge si et seulement si $s > 1$.

Prenons un point où $L(s)$ converge, disons $s = 2$. On peut considérer la série de Taylor de $L(s)$ autour de $s = 2$, en d'autres termes

$$L(s) = \sum_{k\geq 0} \frac{L^{(k)}(2)}{k!}(s-2)^k \ .$$

Le théorème de modularité affirme entre autres choses (mais c'est le plus difficile) que le *rayon de convergence* de cette série entière en $s-2$ est infini (en introduisant des critères pour la convergence d'une série entière vous pouvez si vous le désirez traduire ça en bornes supérieures pour les coefficients $L^{(k)}(2)$).

Exercice 18. **[D6]**. On pose $\zeta(s) = \sum_{n\geq 1} 1/n^s$, et on rappelle que cette série converge absolument pour $s > 1$.

(1) Montrer que le développement en série de Taylor de la fonction $\zeta(s) - 1/(s-1)$ au voisinage de $s = 2$ est

$$\zeta(s) = \sum_{k\geq 0} (-1)^k \frac{c_k}{k!}(s-2)^k \quad \text{avec} \quad c_k = \sum_{n\geq 1} \frac{\log(n)^k}{n^2} - k! \ .$$

(2) (Difficile) Donner une borne supérieure pour c_k qui permette de montrer que le rayon de convergence de la série de Taylor ci-dessus est infini.

.

8. Conclusion

La morale qu'il faut tirer de cette longue histoire est la suivante: le problème de Fermat et le problème des nombres congruents sont très élégants, mais n'ont que peu d'interêt en eux-mêmes, en ce qu'ils n'ont essentiellement pas d'application dans le reste de la théorie des nombres ou ailleurs. Leur importance provient des nombreuses théories qui ont été inventées spécifiquement pour résoudre ces problèmes, et qui eux ont des conséquences cruciales aussi bien en théorie des nombres, que dans d'autres branches des mathématiques:

- Tout d'abord la théorie des courbes elliptiques, qui apparaît dans la résolution du problème de Fermat pour l'exposant 3 et dans le problème des nombres congruents, et qui a conduit Fermat à inventer sa méthode de *descente infinie*, qu'on appelle maintenant la 2-descente (et la 3-descente, etc..., qui sont ultérieures).
- Ensuite la théorie algébrique des nombres, initiée par Gauss, et prolongée ensuite par de nombreux mathématiciens, en particulier par Kummer. Cette vaste théorie a des applications innombrables en dehors du théorème de Fermat, et a culminé dans les années 1920 par l'invention de la *théorie du corps de classes*.
- Enfin et de manière étonnante, les courbes elliptiques réapparaissent aussi dans la résolution finale du problème de Fermat à travers la propriété beaucoup plus profonde de *modularité*, et donc également la théorie des *formes modulaires*.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math. **138**, Springer-Verlag (1993), Fourth corrected printing (2000).

[2] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag, 2000.

[3] H. Cohen, *Number Theory, vol. I: Tools and Diophantine Equations*, Graduate Texts in Math. **239**, Springer-Verlag, 2007.

[4] H. Cohen, *Number Theory, vol. II: analytic and modern tools*, Graduate Texts in Math. **240**, Springer-Verlag, 2007.

Université de Bordeaux, Institut de Mathématiques, U.M.R. 5251 du C.N.R.S., 351 Cours de la Libération, 33405 TALENCE Cedex, FRANCE

E-mail address: Henri.Cohen@math.u-bordeaux.fr