Autour de l'équation de Bachet

Daniel PERRIN

1 Nombres entiers, carrés et cubes

1.1 Carrés et cubes

Cet exposé tourne autour des nombres entiers, de leurs carrés et de leurs cubes. Il est clair que tous les entiers ne sont pas des carrés parfaits, par exemple 2 ou 3 n'en sont pas. Il nous sera utile ici d'avoir la liste des premiers carrés :

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400, ...$$

et celle des premiers cubes :

$$1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331, 1728, 2197, 2744, 3375, 4096, ...$$

1.2 Ramanujan

À propos de cubes, et notamment de 1728, je ne résiste pas au plaisir de vous raconter une histoire qui met en scène deux grands mathématiciens : Hardy et Ramanujan. Srinivasa Ramanujan était un jeune indien, de modeste origine, qui vivait en Inde au début du vingtième siècle (1887-1920). Il apprit les mathématiques en autodidacte à partir de deux livres élémentaires et se passionna notamment pour l'arithmétique, obtenant des résultats qu'il jugea assez intéressants pour les envoyer en 1913 au ponte des mathématiques britanniques[1] de l'époque : Godfrey-H. Hardy. Celui-ci, l'archétype du britannique de cette époque, considéra d'abord avec condescendance ce que lui envoyait ce jeune indien inconnu, mais il s'aperçut très vite qu'à côté de choses bien connues, il y avait des formules nouvelles, qui semblaient exactes et intéressantes, et que pourtant lui, Hardy, ne savait pas prouver. Bref, il se rendit compte qu'il avait affaire à un vrai génie et s'empressa de le faire venir en Angleterre où ils collaborèrent pendant six ans. Malheureusement, le climat de l'Angleterre ne valut rien à Ramanujan qui contracta la tuberculose et en mourut à 32 ans. Un jour qu'il lui rendait visite à l'hôpital, Hardy,

[1] Rappelons que l'Inde était alors une partie de l'Empire britannique.

qui ne savait pas bien quoi raconter et qui connaissait sa passion pour les nombres, lui dit :

– *Je suis venu en taxi, mais le numéro n'avait rien d'extraordinaire, c'était* 1729.

– *Détrompez-vous, répliqua Ramanujan, ce nombre est remarquable car c'est le plus petit entier qui s'écrit de deux manières différentes comme somme de deux cubes.*

Et, en effet, on a $1729 = 10^3 + 9^3 = 12^3 + 1^3$. Le lecteur vérifiera que le suivant est 4104.

1.3 La question

La question que nous allons poser ici consiste à trouver un cube x^3 et un carré y^2 qui diffèrent d'un entier d **donné** : $x^3 - y^2 = d$. Nous allons voir que ce problème a une longue histoire qui est d'ailleurs loin d'être terminée. Vous avez le droit de trouver cette question bien gratuite. S'il est vrai qu'autrefois ce genre de problèmes d'arithmétique n'avait que peu d'applications (Jacobi, au XIX-ième siècle, disait qu'on l'étudiait seulement *Pour l'honneur de l'esprit humain*), les choses ont bien changé depuis une trentaine d'années, notamment avec l'invention du code RSA qui sert en particulier dans la transmission de l'information (cela va des cartes bancaires aux secrets militaires), et qui utilise de manière essentielle les nombres premiers. Or les courbes elliptiques (et la courbe d'équation $y^2 = x^3 - d$ qui va nous intéresser en est une) sont très utilisées pour prouver que des nombres (très grands) sont premiers. Méfions-nous donc des conclusions hâtives.

2 Historique : les origines du problème posé

2.1 Bachet et les rationnels

L'équation à laquelle nous allons nous intéresser est donc l'équation en x et y : $x^3 = y^2 + d$ où d est un entier donné. Elle semble avoir été étudiée pour la première fois en 1621, dans le cas $d = 2$, par Bachet[2] qui, à partir de la solution évidente $x = 3, y = 5$, a donné une méthode géométrique pour construire d'autres solutions **rationnelles** (c'est-à-dire des fractions).

La méthode est très simple, mais fondamentale dans la théorie des courbes elliptiques. On suppose qu'on a une solution (a, b) de l'équation et on en cherche d'autres, (x, y). On peut faire un calcul très algébrique en posant $x = a + h$, $y = b + k$. En développant et en tenant compte de $a^3 = b^2 + d$, on

[2]Claude Gaspard Bachet de Méziriac, 1581-1638.

obtient $3a^2h + 3ah^2 + h^3 = 2bk + k^2$. Une idée pour trouver h et k consiste à imposer une relation supplémentaire entre ces inconnues et ici, on va imposer que les termes de degré 1 s'en aillent en posant $k = \dfrac{3a^2}{2b}\, h$. On constate alors que $h = 0$ est racine double de l'équation restante et qu'il y a une autre racine $h = \dfrac{9a^4 - 12ab^2}{4b^2}$, ce qui donne les nouvelles solutions :

$$x = \frac{9a^4 - 8ab^2}{4b^2} \quad y = \frac{8b^4 + 27a^6 - 36a^3b^2}{8b^3}.$$

On obtient ainsi de nouvelles solutions rationnelles, par exemple dans le cas de Bachet $\frac{129}{100}$, $\frac{383}{1000}$.

On peut comprendre cette méthode de manière géométrique. Elle consiste à partir du point (a, b) de la courbe d'équation $x^3 = y^2 + d$ et de tracer la tangente en ce point. Si on résout en y, en le supposant > 0, cette courbe s'écrit $y = f(x) = \sqrt{x^3 - d}$ et la tangente en (a, b) est $y - b = f'(a)(x - a)$. Comme on a $f'(x) = \dfrac{3x^2}{2\sqrt{x^3 - d}}$ on a $f'(a) = \dfrac{3a^2}{2b}$ et on retrouve le calcul précédent en posant $h = x - a$ et $k = y - b$.

Nous n'irons pas plus loin sur cet aspect du problème qui constitue une partie de l'immense théorie des courbes elliptiques. Il faut savoir qu'on ne connait pas exactement, à l'heure actuelle, l'ensemble des solutions rationnelles de l'équation $x^3 = y^2 + d$. On sait depuis Mordell qu'on peut les munir d'une structure de groupe abélien. Ce groupe contient un morceau fini, qui est connu, et un morceau de la forme $\mathbf{Z}^g$. Mais l'entier g ("le rang" de la courbe) est inconnu en général. Il y a bien une conjecture, due à Birch et Swinnerton-Dyer, qui le donne (voir [Hu] page 34), mais elle n'est pas prouvée. C'est même l'un des sept problèmes du millenium (et donc sa solution vaut un million de dollars).

2.2 Fermat et les entiers

Sur cette même équation, Fermat[3], lui, se pose le problème d'en trouver les solutions **entières**. Il y a évidemment la solution $x = 3$, $y = 2$, mais Fermat va plus loin :

"Peut-on trouver en nombres entiers un carré autre que 25 qui, augmenté de 2, fasse un cube ? À la première vue cela paraît d'une recherche difficile ; en fractions une infinité de nombres se déduisent de la méthode de Bachet ; mais la doctrine des nombres entiers, qui est assurément très belle et très

[3]Pierre de Fermat, 1601-1665.

subtile, n'a été cultivée ni par Bachet, ni par aucun autre dans les écrits venus jusqu'à moi."

Dans une lettre de 1657 à son correspondant anglais Sir Kenelm Digby, il revient sur ce problème et sur le cas $d = 4$. Là encore vous ne manquerez pas d'en trouver une solution. Mais, écoutez Fermat :

"Je lui avais écrit (à Frénicle) *qu'il n'y a qu'un nombre carré entier qui, joint au binaire, fasse un cube, et que ledit carré est 25, auquel, si vous ajoutez 2, il se fait 27, qui est un cube. Il a peine à croire cette proposition négative, et la trouve trop hardie et trop générale. Mais, pour augmenter son étonnement, je dis que, si l'on cherche un carré qui, ajouté à 4 fasse un cube, il ne s'en trouvera jamais que deux en nombres entiers, savoir 4 et 121, car 4 ajouté à 4 fait 8 qui est un cube et 121 ajouté à 4 fait 125 qui est aussi un cube ; mais, après cela, toute l'infinité des nombres n'en saurait fournir un troisième qui ait la propriété."*

Aviez-vous bien vu les deux solutions ? Même si c'est le cas, vous concevrez aisément qu'il n'est pas évident de montrer qu'il n'y en a pas d'autres.

Comme c'est habituel chez Fermat, il n'y a pas vraiment de traces de la solution de ce problème dans ses œuvres, de sorte qu'il est difficile de dire comment il pouvait démontrer les faits annoncés ci-dessus. En revanche on imagine assez bien comment ses successeurs (Euler, Gauss, Kümmer) pouvaient aborder ce problème et plus généralement celui de l'équation $x^3 = y^2 + d$ et c'est ce que je vais tenter d'expliquer ci-dessous.

3 Quelques principes pour aborder le problème

3.1 Identifier le champ : l'arithmétique

Le problème général de Bachet-Fermat est donc de trouver les solutions de l'équation **diophantienne** $x^3 = y^2 + d$ où d est un entier. Quelques précisions sur ce problème. Dire que l'équation est diophantienne (en référence au mathématicien grec Diophante[4], le premier à s'être posé ce genre de questions) signifie qu'on en cherche des solutions qui soient des **entiers**, *a priori* de signe quelconque. On fait donc de l'arithmétique (on dit parfois, plus pompeusement, de la théorie des nombres). Chercher les solutions signifie deux choses, qui vont parfois se traiter séparément : trouver **des** solutions, puis (et comme le fait remarquer Fermat c'est cela le plus difficile) être sûr qu'on les a trouvées **toutes**[5]. Précisons aussi que d peut être un entier positif ou

[4]On pense qu'il vivait au III-ième siècle, mais sans aucune certitude.

[5]On peut montrer que cette équation n'a qu'un nombre fini de solutions entières, mais ce n'est pas du tout évident.

négatif, les deux cas étant également intéressants mais assez différents.

Ce qui suit est à prendre comme une promenade dans le merveilleux pays de l'arithmétique. Nous y rencontrerons d'autres problèmes, mais nous ne résoudrons pas complètement – tant s'en faut – le problème de Bachet-Fermat. Mon objectif est plutôt de vous montrer que, pour faire des mathématiques, quelques idées simples peuvent suffire, mais, à condition de faire preuve de beaucoup d'obstination pour essayer de faire fonctionner ces idées, même quand elles n'ont pas l'air de s'appliquer. Pour des indications historiques, voir [W].

3.2 Une recette en arithmétique : fac-to-ri-ser

La plupart du temps, lorsqu'on est confronté à un problème d'arithmétique, on n'a de cesse d'écrire les expressions sous forme de produits. Il y a plusieurs raisons à cela qui tournent toutes autour de la notion de divisibilité : lorsqu'on cherche un nombre entier x et qu'on a réussi à écrire $a = xy$ avec pour a un entier connu, le nombre x n'est peut-être pas complètement déterminé, mais, comme il divise a, il ne peut prendre qu'un nombre fini de valeurs (et si x est connu, y aussi). On voit qu'en arithmétique, contrairement à ce qui se passe habituellement en algèbre, on peut trouver des solutions même si on n'a pas autant d'équations que d'inconnues. Bien sûr, ce que je viens de dire vaut aussi pour l'équation $a = x + y$ (au moins si l'on reste dans les entiers positifs), mais il y a nettement plus de solutions car tout x compris entre 0 et a convient. Le cas multiplicatif est donc bien plus intéressant. Cela explique l'importance de la divisibilité, notamment de la notion de nombre premier, car si a est premier, x ne peut valoir que 1 ou a. Plus généralement c'est grâce à la décomposition de a en produit de facteurs premiers qu'on peut déterminer ses diviseurs, on verra ci-dessous un exemple de cette procédure.

3.3 Un exemple

Pour illustrer ce qui précède, examinons un exemple qui ressemble au nôtre, mais qui est beaucoup plus élémentaire. On considère l'équation diophantienne en x et y : $x^2 = y^2 + d$, avec d connu (et disons $d > 0$). Là, il est facile de factoriser l'équation, il suffit de passer le y^2 dans le premier membre et on obtient $x^2 - y^2 = (x + y)(x - y) = d$. Pour trouver x et y, on note que $x - y$ est un **diviseur** de d et que, si $x - y$ est connu, $x + y$ est déterminé aussi (car c'est $d/(x - y)$). Si on est capable d'énumérer les diviseurs de d on aura donc $x + y$ et $x - y$, et on en déduira x et y en résolvant un système de deux équations à deux inconnues. Le mieux pour comprendre le processus est de regarder quelques exemples.

Prenons $d = 3$. Ce nombre étant premier, il n'a que deux diviseurs : 1 et 3. Comme $x-y$ est plus petit que $x+y$ c'est qu'on a nécessairement $x-y = 1$ et $x + y = 3$, ce qui donne $x = 2$ et $y = 1$.

Avec $d = 2$ en revanche on se casse les dents. En effet, le même raisonnement donne $x - y = 1$ et $x + y = 2$ qui donne $x = 3/2$ et $y = 1/2$: c'est raté car x et y doivent être des entiers.

Essayons maintenant avec un nombre plus grand, par exemple $d = 105$. Il s'agit de déterminer les diviseurs de 105. Il y a une méthode générale pour cela qui consiste à décomposer 105 en produit de facteurs premiers. Rappelons le théorème essentiel à ce sujet :

3.1 Théorème. *Tout nombre entier > 0 s'écrit de manière unique (à l'ordre près des facteurs) comme produit de nombres premiers.*

Dans notre cas, on a $105 = 3 \times 5 \times 7$. Cela permet d'énumérer les diviseurs en prenant parmi les facteurs premiers de 105 ceux qui sont produits de zéro facteur (1), d'un facteur ($3, 5$ ou 7), de deux facteurs ($3 \times 5 = 15$, $3 \times 7 = 21$ et $5 \times 7 = 35$), et enfin de trois (105). Comme $x - y$ doit être plus petit que son compagnon $x+y$, cela donne les solutions $x-y = 1, 3, 5, 7$, qui vont avec $x + y = 105, 35, 21, 15$ et on trouve pour (x, y) les solutions $(53, 52)$, $(19, 16)$, $(13, 8)$ et $(11, 4)$, dont on vérifie qu'elles satisfont bien $x^2 - y^2 = 105$. De plus, le raisonnement montre que les solutions sont toutes obtenues ainsi.

Avec ces indications, vous n'aurez pas de peine à résoudre complètement le problème de trouver les solutions de $x^2 = y^2 + d$.

3.4 Le lemme d'Euclide

C'est un résultat très simple, que nous reverrons plus loin et qui est, en fait, équivalent à l'assertion d'unicité du théorème précédent :

3.2 Lemme. *Si un nombre premier p divise un produit ab, il divise a ou b.*

Démonstration. On écrit $ab = pq$ et on décompose a, b, q en produits de facteurs premiers. On obtient deux décompositions du produit ab. Comme ce sont les mêmes, c'est que p intervient soit dans la décomposition de a soit dans celle de b.

4 L'équation de Bachet, un cas où la factorisation est facile : le cas où $-d$ est un carré

Pour appliquer notre idée-clé qui consiste à factoriser, commençons par un cas où d est < 0, cas qui nous éloigne un peu de Fermat. Si on pose

$d = -k$, l'équation est de la forme $x^3 = y^2 - k$ et il y a un cas où le membre de droite se factorise sans peine, c'est lorsque k est un carré parfait. Par exemple, si k est égal à 1, l'équation s'écrit $x^3 = y^2 - 1 = (y-1)(y+1)$. Dans le premier membre on a un cube, dans le second le produit de deux entiers. Bien entendu, comme le produit de deux cubes en est un : $\alpha^3\beta^3 = (\alpha\beta)^3$, si les deux nombres du second membre sont des cubes, celui du premier aussi. La réciproque est – presque – vraie (et ce sera l'un des résultats-clés de notre recherche) :

4.1 Lemme. *Soient x, a, b des entiers > 0. On suppose qu'on a $x^3 = ab$ et que a et b sont premiers entre eux. Alors a et b sont des cubes (d'entiers).*

Démonstration. On écrit les décompositions en produit de facteurs premiers (distincts) de a, b, x :

$$a = p_1^{\alpha_1} \cdots p_l^{\alpha_l}, \quad b = q_1^{\beta_1} \cdots q_m^{\beta_m} \quad x = r_1^{\gamma_1} \cdots r_n^{\gamma_n}$$

où les p_i, q_j, r_k sont des nombres premiers, les p_i étant distincts et de même pour les q_j et les r_k et les exposants $\alpha_i, \beta_j, \gamma_k$ étant dans $\mathbf{N}^*$. On a

$$x^3 = r_1^{3\gamma_1} \cdots r_n^{3\gamma_n} = p_1^{\alpha_1} \cdots p_l^{\alpha_l}\, q_1^{\beta_1} \cdots q_m^{\beta_m}.$$

Comme a et b sont premiers entre eux, les p_i et les q_j sont distincts. Par unicité de la décomposition en produit de facteurs premiers de x^3, cela montre que chaque p_i (par exemple), est égal à un r_k et que son exposant est alors $3\gamma_k$, ce qui montre que a est un cube et de même pour b.

Revenons alors à notre équation. Il y a deux cas de figure.

• Si y est pair, alors $y-1$ et $y+1$ sont premiers entre eux. En effet, sinon, ils auraient un diviseur commun $p \neq 1$ qui diviserait aussi leur différence $(y+1) - (y-1) = 2$. On aurait donc nécessairement $p = 2$, ce qui est absurde.

En vertu de 4.1, $y-1$ et $y+1$ sont donc des cubes : $y-1 = a^3$, $y+1 = b^3$, mais on voit aussitôt que c'est impossible car la différence entre deux cubes consécutifs est soit égale à 1 (dans le cas de 0 et 1), soit toujours plus grande que 2 (le calcul est immédiat : $(a+1)^3 - a^3 = 3a^2 + 3a + 1 \geq 7$ si $a \geq 1$).

• Si y est impair on montre (mais ce n'est pas trivial du tout[6]) que la seule solution de l'équation est alors $x = 2$, $y = 3$.

[6]Cela résulte du fait que l'équation $x^3 + dy^3 = 1$ admet au plus une solution en entiers non nuls (théorème de Delaunay-Nagell).

5 L'équation de Bachet : le cas $d > 0$, trouver des solutions

5.1 Les imaginaires

Lorsque d est négatif mais pas un carré parfait, $d = -k$, il n'est pas évident de factoriser $y^2 - k$. En tous cas, ce n'est pas possible en restant dans les entiers, mais on peut au moins factoriser dans $\mathbf{R}$:

$$y^2 - k = (y + \sqrt{k})(y - \sqrt{k}).$$

Cela peut d'ailleurs mener, dans certains cas, à une solution du problème.

La difficulté est pire encore dans le cas $d > 0$ car, cette fois, il n'y a plus moyen de factoriser le second membre de $x^3 = y^2 + d$ car, même dans $\mathbf{R}$, $-d$, qui est négatif, n'est plus un carré. Plus moyen ? Vous qui êtes instruits, vous savez bien qu'il suffit pour le faire de travailler avec des nombres complexes, mais imaginez quel plongeon dans l'inconnu cela pouvait constituer pour les anciens, même au XVIII-ième siècle. Bien entendu, pour nous ce n'est plus que la routine et on a la factorisation $x^3 = y^2 + d = y^2 - (-d) = (y + i\sqrt{d})(y - i\sqrt{d})$.

En vérité, ce n'est pas vraiment dans le corps des complexes que nous allons travailler mais dans le sous-ensemble $\mathbf{Z}[i\sqrt{d}]$ des éléments de la forme $a + ib\sqrt{d}$ avec a, b entiers puisque c'est là que la factorisation a lieu. Cet ensemble est ce qu'on appelle un **anneau**. Cela signifie qu'on sait ajouter, soustraire et multiplier ses éléments (mais pas les diviser, en général). Par exemple, on a $(x + iy\sqrt{d})(x' + iy'\sqrt{d}) = xx' - dyy' + i(xy' + x'y)\sqrt{d}$. Un anneau c'est le lieu par excellence où l'on peut parler de divisibilité en toute généralité comme nous le verrons ci-dessous.

On a vu ci-dessus (cf. Lemme 4.1) que, dans $\mathbf{Z}$, si un cube est produit de deux nombres premiers entre eux, alors les nombres sont des cubes. Admettons que cela reste vrai dans l'anneau $\mathbf{Z}[i\sqrt{d}]$. Si on a $x^3 = y^2 + d = (y + i\sqrt{d})(y - i\sqrt{d})$, cela voudrait dire que les nombres $z = y + i\sqrt{d}$ et $\overline{z} = y - i\sqrt{d}$ (son conjugué) sont des cubes dans cet anneau, disons, pour le premier, le cube de $w = a + ib\sqrt{d}$. Faisons le calcul sans crainte. Cela donne :

$$y + i\sqrt{d} = a^3 + 3a^2bi\sqrt{d} - 3ab^2d - ib^3d\sqrt{d}.$$

Si l'on sépare les quantités réelles et imaginaires, cela nous mène à deux équations : $y = a^3 - 3ab^2d$ et $1 = 3a^2b - b^3d$, qui sont des équations dans $\mathbf{Z}$.

On regarde la deuxième équation. On est dans les entiers et on voit que b doit diviser 1. Ah, mais 1, c'est encore pire qu'un nombre premier, il n'a

pas de diviseurs autres que lui-même et son opposé. On a donc $b = \pm 1$, d'où $d = 3a^2 \pm 1$ (ce qui nous donne donc une condition nécessaire sur d pour avoir des solutions) et on obtient $y = a^3 - 3ad$ et $x = a^2 + d$ (car $x^3 = z\overline{z}$ est le cube de $w\overline{w} = a^2 + d$). Vite, on vérifie ! Si l'on en croit ce calcul, on doit avoir, si $d = 3a^2 \pm 1$:

$$(a^2 + d)^3 = (a^3 - 3ad)^2 + d,$$

on constate, avec ravissement, que c'est vrai !

5.2 Des solutions !

On notera que, même si l'on émet des doutes sur l'existence des imaginaires, ce qui était encore le cas au XVIII-ième siècle, cela n'a plus d'importance. En effet le dernier calcul effectué ci-dessus est parfaitement valable et il nous fournit des solutions de l'équation lorsque d est de la forme $3a^2 \pm 1$, disons $d = 3a^2 + \epsilon$ avec $\epsilon = \pm 1$. Quand un phénomène de ce genre lui arrive, le mathématicien ne peut s'empêcher de penser qu'il y a sans doute une bonne raison qui justifie son calcul : c'est trop beau pour être faux ! Mais il faut parfois beaucoup d'efforts pour justifier une intuition fulgurante, nous le reverrons plus loin.

Revenons à notre équation : pour $d = 2$, $\epsilon = -1$, $a = 1$, on trouve $y = 1 - 6 = -5$ et $x = 3$: au signe près, c'est la solution évidente, celle annoncée par Fermat. Avec $d = 4$, $\epsilon = 1$, $a = 1$, on trouve $y = -11$ et $x = 5$, mais pas l'autre solution $y = 2$ et $x = 2$!

Moins évident, on a les solutions suivantes :

1) $\epsilon = 1, d = 3a^2 + 1$

a	0	1	2	3	4	5
d	1	4	13	28	49	76
x	1	5	17	37	65	101
y	0	11	70	225	524	1015

2) $\epsilon = -1, d = 3a^2 - 1$

a	1	2	3	4	5
d	2	11	26	47	74
x	3	15	35	63	99
y	5	58	207	500	985

On a donc, pour $d = 74$ par exemple, la solution $99^3 = 985^2 + 74$.

6 Le cas $d < 0$, suite, toutes les solutions ?

6.1 Position du problème

La question qui se pose maintenant, et qui est beaucoup plus difficile, est de savoir si on a trouvé ainsi toutes les solutions. Cela n'est pas toujours vrai puisque, pour $d = 4$, on a vu que l'une des solutions (d'ailleurs la plus évidente, $x = y = 2$) nous a échappé.

Rappelons le raisonnement ébauché ci-dessus pour montrer que les solutions sont de la forme annoncée : si on a une solution x, y de l'équation $x^3 = y^2 + d$ et si on pose $z = y + i\sqrt{d}$, de sorte que l'on a $x^3 = z\overline{z}$ dans $\mathbf{Z}[i\sqrt{d}]$, alors z est un cube de $\mathbf{Z}[i\sqrt{d}]$.

Ce qu'on espère c'est une preuve analogue à celle de 4.1. Il y a deux difficultés. D'abord, même sur $\mathbf{Z}$, cette preuve requiert le fait que z et $\overline{z}$ soient premiers entre eux. On voit bien que, pour $d = 4$, c'est cela qui cloche. En effet, les nombres $z = 2 + 2i$ et $\overline{z} = 2 - 2i$ ne sont pas premiers entre eux car ils ont le facteur 2 en commun. Pour avoir cette condition nous devrons donc faire des hypothèses supplémentaires.

Ensuite, il y a un point beaucoup plus fondamental. On a vu que, dans $\mathbf{Z}$, la preuve de 4.1 repose sur l'existence et surtout l'unicité de la décomposition d'un nombre en produit de facteurs premiers et que cette propriété est essentiellement équivalente au lemme d'Euclide. La question est donc de savoir si l'anneau $\mathbf{Z}[i\sqrt{d}]$ vérifie cette propriété (on dit alors qu'il est **factoriel**). Dans un premier temps, nous allons supposer que cette condition est réalisée comme l'ont fait les premiers mathématiciens à s'être confrontés à ce type de problème, puis nous discuterons plus sérieusement cette condition. Mais avant, il est bon de fixer précisément quelques points.

6.2 Un peu d'algèbre

6.2.1 Des définitions

Donnons quelques définitions :

6.1 Définition. *Soit A un anneau.*
1) Si a, b sont deux éléments de A, on dit que a **divise** *b s'il existe $c \in A$ tel que $b = ac$.*
2) Un élément a de A est dit **inversible** *s'il existe $b \in A$ avec $ab = 1$. On note A^* l'ensemble des éléments inversibles de A.*
3) Un élément non inversible $a \in A$ est dit **irréductible** *si les seuls diviseurs de a sont les inversibles et les éléments associés[7] à a.*

[7] C'est-à-dire les éléments de la forme au avec u inversible.

4) Deux éléments a, b sont dits **premiers entre eux** *s'ils n'ont pas de diviseurs communs autres que les inversibles.*

6.2 *Remarques.*
1) Les inversibles sont les éléments triviaux relativement à la relation de divisibilité : ils divisent tout le monde. Dans $\mathbf{Z}$ ce sont 1 et -1. Pour le cas de $\mathbf{Z}[i\sqrt{d}]$, voir ci-dessous.
2) Si p est irréductible il en est de même des up avec u inversibles (les "associés" de p).

6.2.2 Exemples : le cas des anneaux $\mathbf{Z}[i\sqrt{d}]$

Introduisons un outil essentiel pour l'étude de ces anneaux : la norme.

6.3 Définition. *Soit $z = a + ib\sqrt{d}$ un élément de $\mathbf{Z}[i\sqrt{d}]$. On définit son conjugué $\overline{z} = a - ib\sqrt{d}$ et sa norme $N(z) = z\overline{z} = a^2 + db^2$.*

La proposition suivante est évidente, mais fondamentale.

6.4 Proposition.
1) La conjugaison est un automorphisme : on a $\overline{z+w} = \overline{z} + \overline{w}$ et $\overline{zw} = \overline{z}\,\overline{w}$.
2) La norme de $z \in \mathbf{Z}[i\sqrt{d}]$ est un entier ≥ 0, elle est nulle si et seulement si z est nul. La norme est multiplicative : $N(zw) = N(z)N(w)$.

Une première application de la norme est la détermination des inversibles :

6.5 Proposition. *Les éléments inversibles de $\mathbf{Z}[i\sqrt{d}]$ sont les éléments de norme 1. Il y a seulement ± 1, sauf dans le cas $d = 1$ où il y a aussi $\pm i$.*

Démonstration. Dire que $z = a + ib\sqrt{d}$ est inversible c'est dire qu'il existe w tel que $zw = 1$. On a donc $N(z)N(w) = 1$ et comme les normes sont des entiers naturels on a $N(z) = 1$, la réciproque étant évidente avec $\overline{z}$. On a donc $a^2 + db^2 = 1$. Si d est ≥ 2 cela impose $b = 0$ et $a = \pm 1$. Dans le cas $d = 1$ on a aussi les solutions $a = 0$, $b = \pm 1$.

La norme permet aussi, dans certains cas, de conclure à l'irréductibilité :

6.6 Proposition. *Soit $t \in \mathbf{Z}[i\sqrt{d}]$.*
1) Si $N(t)$ est un nombre premier ou si $N(t)$ n'est pas produit de deux normes distinctes de 1, t est irréductible dans $\mathbf{Z}[i\sqrt{d}]$.
2) Un nombre premier $p \in \mathbf{Z}$ est réductible dans $\mathbf{Z}[i\sqrt{d}]$ si et seulement si c'est une norme.

Démonstration. 1) Si t est réductible il s'écrit $t = zw$ avec $z, w \in \mathbf{Z}[i\sqrt{d}]$, non inversibles. On a donc $N(t) = N(z)N(w)$ et $N(z)$ et $N(w)$ sont des normes > 1. Le point 2) en résulte car on a $N(p) = p^2$.

6.7 *Exemple.* Dans $\mathbf{Z}[i\sqrt{5}]$ le nombre 41 est réductible car on a $41 = 6^2+5 = (6+i\sqrt{5})(6-i\sqrt{5})$ et ces facteurs sont irréductibles. En revanche, 3 et 7 ne sont pas des normes, donc sont irréductibles, de même que le nombre $4+i\sqrt{5}$, dont la norme est $21 = 3 \times 7$.

6.8 *Remarque.* Quitte à multiplier par -1, on peut toujours supposer qu'un élément irréductible a une partie réelle positive ou nulle et, si elle est nulle, que sa partie imaginaire est positive[8]. On parlera d'élément irréductible **normalisé**.

6.3 Anneaux factoriels

Pour des détails, voir par exemple [P].

Soit A un anneau. On suppose qu'on a choisi un système P d'éléments irréductibles normalisés de telle sorte que tout irréductible q s'écrive de manière unique sous la forme $q = up$ avec $p \in P$ et $u \in A^*$. (C'est le cas avec le choix opéré ci-dessus dans $\mathbf{Z}[i\sqrt{d}]$ et on peut toujours faire cela.)

6.9 Définition. *L'anneau A est dit* **factoriel** *s'il vérifie les deux conditions suivantes :*
1) Tout élément a non nul de A s'écrit sous la forme $a = up_1 \cdots p_r$ où u est inversible et où les p_i sont dans P.
2) Cette écriture est unique à l'ordre près.

6.10 *Remarques.*
1) La condition 2) signifie que si l'on a deux décompositions de a : $a = up_1 \cdots p_r = vq_1 \cdots q_r$ alors on a $r = s$, $u = v$ et les q_j sont égaux aux p_i à permutation près.
2) Bien entendu, l'anneau $\mathbf{Z}$ est factoriel.

Dans tous les anneaux usuels, la condition d'existence est réalisée. C'est le cas en particulier pour les anneaux $\mathbf{Z}[i\sqrt{d}]$:

6.11 Proposition. *L'anneau $\mathbf{Z}[i\sqrt{d}]$ vérifie la condition d'existence de décomposition en irréductibles.*

Démonstration. On raisonne par l'absurde. Supposons qu'il existe un élément t qui ne s'écrive pas sous la forme annoncée et choisissons un tel élément de norme minimale (c'est possible car $N(t)$ est un entier naturel). Cet entier est > 1 (si c'est 0, on a $t = 0$, si c'est 1, t est inversible). Comme t n'est pas irréductible il s'écrit $t = zw$ avec z et w non inversibles. On a alors

[8] Dans le cas $d = 1$, quitte à multiplier par ± 1 ou $\pm i$, on peut supposer à la fois que la partie réelle et la partie imaginaire sont positives ou nulles.

$N(t) = N(z)N(w)$, et comme z et w sont non inversibles, leurs normes sont > 1, donc aussi inférieures à $N(t)$. Mais alors, l'hypothèse de minimalité montre que z et w admettent des décompositions en irréductibles et donc t aussi.

En revanche l'unicité n'est pas toujours vraie. Précisément on a le résultat suivant que le lecteur prouvera sans peine :

6.12 Lemme. *On suppose que A vérifie la condition 1). Alors la condition 2) équivaut au "lemme d'Euclide" : si un élément irréductible p divise un produit ab il divise a ou b (c'est seulement dans ce cas qu'on dit qu'il est* **premier***).*

6.4 Le théorème crucial, version 1

Maintenant que ces choses sont dites, on peut prouver un théorème. La justification des hypothèses apparaîtra au cours de la démonstration.

6.13 Théorème. (Théorème crucial) *On suppose que d est un entier sans facteur carré et congru à 1 ou 2 modulo 4 et que l'anneau $\mathbf{Z}[i\sqrt{d}]$ est factoriel. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$. Alors les nombres z et $\overline{z}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$ et sont des cubes de $\mathbf{Z}[i\sqrt{d}]$.*

Démonstration. Une première remarque c'est que x est impair. En effet, s'il est pair, on a $x^3 \equiv 0 \pmod 4$. Mais alors on a $d \equiv -y^2 \pmod 4$ et c'est impossible car $-y^2$ vaut 0 ou -1 modulo 4.

On note ensuite que x et y sont premiers avec d. En effet, si p est un nombre premier qui divise y et d il divise x et inversement, mais alors p^2 divise d, ce qui est absurde car d n'a pas de facteur carré.

Soit alors $t \in \mathbf{Z}[i\sqrt{d}]$ un facteur commun de z et $\overline{z}$, que l'on peut supposer irréductible. Comme t divise $z\overline{z} = x^3$ il divise x d'après le lemme d'Euclide. Par ailleurs, t divise aussi $z + \overline{z}$ et $z - \overline{z}$ i.e., $2y$ et $2i\sqrt{d}$ donc, *a fortiori*, $2d$. Il divise donc à la fois x et $2d$. Mais on a vu que x et $2d$ sont premiers entre eux et en écrivant la relation de Bézout dans $\mathbf{Z}$: $1 = ax + b(2d)$, on voit que cela implique que t est inversible dans $\mathbf{Z}[i\sqrt{d}]$ ce qui est absurde.

Pour finir de montrer le théorème, le raisonnement est identique à celui produit pour prouver 4.1. On décompose z et $\overline{z}$ en produits d'irréductibles (normalisés) dans $\mathbf{Z}[i\sqrt{d}]$:

$$z = up_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad \overline{z} = vq_1^{\beta_1} \cdots q_s^{\beta_s}$$

où les p_i (resp. les q_j) sont des irréductibles distincts et u, v des inversibles. De plus, comme z et $\overline{z}$ sont premiers entre eux, les p_i et les q_j sont distincts.

Décomposons aussi $x = w\pi_1^{\gamma_1} \cdots \pi_n^{\gamma_n}$. On a alors

$$x^3 = w^3\pi_1^{3\gamma_1} \cdots \pi_n^{3\gamma_n} = uvp_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}.$$

Mais, **en vertu de l'unicité de la décomposition**, ceci montre que chaque p_i est égal à un π_k. De plus, comme p_i est différent des autres p_j et des q_j, l'exposant α_i de p_i est égal à celui de π_k c'est-à-dire à $3\gamma_k$. Comme les inversibles sont tous des cubes[9], u est un cube et on en déduit que z est un cube dans $\mathbf{Z}[i\sqrt{d}]$.

6.14 Corollaire. *Sous les hypothèses de 6.13 on a les résultats suivants :*
1) Si d n'est pas de la forme $3a^2 \pm 1$ l'équation de Bachet $x^3 = y^2 + d$ n'a pas de solutions dans $\mathbf{Z}$.
2) Si $d = 3a^2 \pm 1$, les solutions positives de l'équation de Bachet sont

$$x = a^2 + d, \qquad y = a(3d - a^2).$$

Démonstration. Avec les notations précédentes, on a $z = w^3$ avec $w = a + ib\sqrt{d}$, avec $a, b \in \mathbf{Z}$ et les solutions de l'équation sont bien celles annoncées.

6.5 Discussion

Il reste à savoir si l'anneau $\mathbf{Z}[i\sqrt{d}]$ est bien factoriel. C'est une chose que les anciens (par exemple Euler, ou Kümmer) ont cru un moment. Hélas, c'est très, très faux :

6.15 Proposition. *Soit d un entier > 0. L'anneau $\mathbf{Z}[i\sqrt{d}]$ est factoriel si et seulement si on a $d = 1$ ou 2.*

Démonstration. Si $d = 1$ ou 2 on montre que l'anneau est euclidien (c'est-à-dire qu'il admet une division euclidienne) et cela implique qu'il est factoriel.

Pour $d > 2$ on note que le nombre entier 2 reste irréductible dans $\mathbf{Z}[i\sqrt{d}]$. En effet, sinon, 2 serait une norme, donc de la forme $a^2 + db^2$. Comme d est > 2 cela impose $b = 0$. Il reste $a^2 = 2$ et c'est impossible avec $a \in \mathbf{Z}$ (et même $a \in \mathbf{Q}$). Il suffit de montrer que 2 ne vérifie pas le lemme d'Euclide. Pour cela on note que 2 divise $d^2 + d = d(d + 1)$. Mais, dans $\mathbf{Z}[i\sqrt{d}]$, on a $d^2 + d = (d + i\sqrt{d})(d - i\sqrt{d})$. Si le lemme d'Euclide était vrai, d devrait diviser l'un des deux et on devrait donc avoir, par exemple, $d + i\sqrt{d} = 2(a + ib\sqrt{d})$ avec $a, b \in \mathbf{Z}$. En identifiant les parties imaginaires on a $1 = 2b$, ce qui est absurde.

[9] Même dans le cas $d = 1$.

6.16 *Exemple.* Par exemple, dans $\mathbf{Z}[i\sqrt{5}]$ on a deux décompositions du nombre 21 en 3×7 et $(4+i\sqrt{5})(4-i\sqrt{5})$, avec des nombres tous irréductibles.

On voit que, hormis dans le cas $d = 2$ de Fermat[10] (mais c'est déjà quelque chose), il n'y a pas d'espoir que notre preuve soit correcte.

6.6 Une remarque pour les gens très, très instruits

Ce paragraphe peut être omis en première lecture, il vise juste à préciser une question qui est apparue lors de l'exposé oral.

En vérité, l'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est pas toujours le bon anneau à considérer dans la situation qui nous occupe. En effet, une condition minimale pour qu'on puisse y faire de la divisibilité, c'est qu'il soit **intégralement clos**. Dans notre cas cela signifie que les seuls éléments de $\mathbf{Q}(i\sqrt{d})$ (c'est-à-dire de la forme $a + ib\sqrt{d}$ avec cette fois a et b rationnels) qui vérifient une équation de la forme $z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0$, avec les a_i dans $\mathbf{Z}[i\sqrt{d}]$ sont les éléments de $\mathbf{Z}[i\sqrt{d}]$ et eux seuls. On montre facilement qu'un anneau factoriel est intégralement clos. Or, lorsqu'on a $d \equiv 3 \pmod 4$, l'anneau $\mathbf{Z}[i\sqrt{d}]$ n'est pas intégralement clos car l'élément $\alpha_d = \dfrac{1 + i\sqrt{d}}{2}$ vérifie l'équation $X^2 - X + \dfrac{d+1}{4} = 0$. Le bon anneau à considérer est alors $\mathbf{Z}[\alpha_d]$ qui, lui, est intégralement clos. Pour ces anneaux, le résultat (pas du tout évident) est le suivant :

6.17 Théorème. *Soit d un entier congru à 3 modulo 4. L'anneau $\mathbf{Z}[\alpha_d]$ est factoriel si et seulement si d est égal à 3, 7, 11, 19, 43, 67 ou 163.*

7 Le cas $d > 0$, suite : il ne faut pas jeter le bébé avec l'eau du bain

7.1 L'analyse de Kümmer : les nombres idéaux

Cette difficulté (que l'on peut considérer comme la première difficulté fondamentale de la théorie algébrique des nombres) a été repérée (sous une forme voisine) par Lagrange dès la fin du XVIII-ième siècle, mais au début du XIX-ième siècle d'illustres mathématiciens tombent encore dans le panneau. C'est le cas, semble-t-il, de Kümmer lui-même à qui Dirichlet aurait signalé son erreur. Pour sortir de cette impasse Kümmer a inventé, vers 1840, les

[10] Le cas $d = 4$ peut aussi être traité de manière analogue en travaillant dans $\mathbf{Z}[i]$.

"nombres idéaux". Pour tenter d'expliquer l'idée de Kümmer partons de la difficulté rencontrée ci-dessus en considérant par exemple dans $\mathbf{Z}[i\sqrt{5}]$ les deux décompositions du nombre 21 :

$$21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5}). \tag{1}$$

Une hypothèse plausible consiste à imaginer que Kümmer a interprété l'égalité (1) comme l'analogue de la décomposition dans $\mathbf{Z}$:

$$14 \times 15 = 10 \times 21. \tag{2}$$

Dans ce dernier cas la non unicité de la décomposition vient, bien entendu, du fait que les nombres ne sont pas irréductibles et (2) s'écrit simplement

$$(2 \times 7) \times (5 \times 3) = (2 \times 5) \times (7 \times 3). \tag{3}$$

Si on désigne par (a, b) le pgcd de a et b dans $\mathbf{N}$, on peut encore écrire (3) sous la forme suivante :

$$(14, 10)(14, 21)(15, 10)(15, 21) = (14, 10)(15, 10)(14, 21)(15, 21), \tag{4}$$

et on a les relations $14 = (14, 10)(14, 21)$, etc.

Revenons à l'égalité (1). Dans cette décomposition, les divers facteurs : 3, 7, $4 + i\sqrt{5}$ et $4 - i\sqrt{5}$ n'ont pas de diviseur commun dans $\mathbf{Z}[i\sqrt{d}]$, puisqu'ils sont irréductibles. Toutefois, certains sont "plus premiers entre eux" que les autres : 3 et 7 d'une part, $4 + i\sqrt{5}$ et $4 - i\sqrt{5}$ d'autre part ont une propriété supplémentaire : ils vérifient une relation de Bézout dans $\mathbf{Z}[i\sqrt{d}]$ (on pourrait dire qu'ils sont fortement premiers entre eux, mais on dit plutôt qu'ils sont **étrangers**). C'est clair pour 3 et 7 (c'est le théorème de Bézout dans $\mathbf{Z}$) et pour les autres c'est un calcul facile (exercice). Par exemple, on a :

$$(4 + i\sqrt{5})(-4 + 3i\sqrt{5}) + 8(4 - i\sqrt{5}) = 1.$$

(On peut aussi conclure en notant que la somme et le produit de ces deux nombres valant respectivement 8 et 21, on va pouvoir trouver 1 avec la formule $1 = 8 \times 8 - 3 \times 21$.) En revanche, si 3 et $4 + i\sqrt{5}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$, on vérifie facilement qu'ils ne sont pas étrangers (exercice), et de même pour les autres couples. Ce que Kümmer imagine alors c'est qu'en dépit des apparences (ou de l'évidence) on doit pouvoir raffiner les deux décompositions du nombre 21 comme dans le cas de l'égalité (2) et il introduit pour cela, de manière formelle dans un premier temps, des pgcd pour 3 et $4 + i\sqrt{5}$ (et les autres), de telle sorte que (1) s'écrive alors sous la forme analogue à (4) :

$$(3, 4 + i\sqrt{5})(3, 4 - i\sqrt{5})(7, 4 + i\sqrt{5})(7, 4 - i\sqrt{5})$$

$$= (3, 4 + i\sqrt{5})(7, 4 + i\sqrt{5})(3, 4 - i\sqrt{5})(7, 4 - i\sqrt{5}),$$

avec les relations partielles du type :

$$3 = (3, 4 + i\sqrt{5})(3, 4 - i\sqrt{5}). \tag{5}$$

Ainsi, Kümmer postule l'existence d'un "pgcd" formel de 3 et $4 + i\sqrt{5}$, noté $(3, 4 + i\sqrt{5})$, ou encore, comme il le dit, d'un facteur commun "idéal" à ces deux nombres. L'idée est séduisante, mais, bien entendu, il faut ensuite donner une base solide à cette théorie des nombres idéaux et préciser les règles de calcul auxquelles ils sont soumis. C'est le travail entrepris par Kümmer dans les années 1840-1850 et poursuivi par Kronecker et Dedekind jusqu'en 1880.

Voici ce que Kümmer dit à ce sujet dans une lettre à Liouville datée de 1847 (cf. [K]) : *"quant à la propriété qu'un nombre complexe ne peut être décomposé en facteurs premiers que d'une seule manière, je puis vous assurer qu'elle n'a pas lieu généralement tant qu'il s'agit des nombres de la forme : $a + ib\sqrt{d}$ mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes que j'ai nommé nombre complexe idéal."*.

Dans un article de 1851 il développe un étonnant parallèle avec la chimie :

"Qu'il me soit permis de signaler ici en peu de mots l'analogie de cette théorie de la composition des nombres idéaux avec les principes fondamentaux de la chimie. La composition des nombres complexes peut être envisagée comme l'analogue de la composition chimique ; les facteurs premiers correspondent aux éléments (...). Les nombres complexes idéaux sont comparables aux radicaux hypothétiques qui n'existent pas par eux-mêmes, mais seulement dans les combinaisons ; le fluor, en particulier, comme élément qu'on ne sait pas représenter isolément, peut être comparé à un facteur premier idéal. (...) Toutes ces analogies qu'on pourra poursuivre et augmenter à volonté, ne proviennent pas d'un jeu d'esprit oisif, mais elles sont bien fondées en ce que les mêmes idées fondamentales de la composition et de la décomposition des éléments règnent aussi bien dans la chimie des matières naturelles que dans celle des nombres complexes."

7.2 Formalisation : encore un peu d'algèbre

Il s'agit de donner un sens aux nombres idéaux de Kümmer afin d'interpréter notamment la relation (5). Ce n'est pas si facile, car il faut pour cela changer de cadre : les idéaux ne sont pas des nombres, mais des ensembles de nombres. L'idée est de regarder des ensembles de nombres tels que ceux qui apparaissent dans Bézout : l'ensemble des nombres $\lambda a + \mu b$ pour $\lambda, \mu \in A$. En

fait, on dégage les propriétés d'un tel ensemble de nombres en introduisant la notion suivante :

7.1 Définition. *Si A est un anneau on appelle* **idéal** *de A une partie I qui vérifie les deux propriétés suivantes :*
1) Si $x, y \in I$, alors $x + y \in I$.
2) Si $x \in I$ et $a \in A$, $ax \in I$.

7.2 *Exemple.* L'exemple le plus simple d'idéal, celui qui constitue le point de départ de la théorie, est l'idéal **principal** (a) engendré par $a \in A$, c'est l'ensemble des multiples de a. En fait, dans ce cas, on n'est pas encore vraiment sorti des nombres, puisque cet idéal est déterminé par un nombre (et qu'il le détermine, aux inversibles près). Les idéaux principaux sont liés à la divisibilité par la relation évidente :

$$(*) \qquad a \text{ divise } b \Longleftrightarrow (b) \subset (a).$$

On notera que, dans le passage des éléments aux idéaux, l'ordre est renversé.

Tout le jeu consiste maintenant à étendre aux idéaux un certain nombre de notions qui valent pour les éléments de A, en essayant de calquer les définitions. La première définition découle de $(*)$:

7.3 Définition. *Si I et J sont des idéaux quelconques on dit que I* **divise** *J si on a $J \subset I$.*

Il s'agit ensuite de définir le "plus grand commun diviseur" de deux idéaux. Comme le *pgcd* c'est, pour les éléments, le plus grand des plus petits, sur les idéaux ce sera le plus petit des plus grands :

7.4 Définition. *Si I, J sont deux idéaux, leur pgcd est l'idéal somme $I + J$, ensemble des $x + y$ pour $x \in I$ et $y \in J$.*

Dans le cas où I et J sont principaux, $I = (a)$, $J = (b)$, on obtient l'idéal (a, b) engendré par a et b, ensemble des nombres de la forme $\lambda a + \mu b$ pour $\lambda, \mu \in A$. **Attention**, cet idéal n'est pas principal en général (autrement dit, on n'a pas de relation de Bézout). Plus généralement, on appelle **idéal engendré** par des éléments $a_1, \ldots, a_n$ l'ensemble des combinaisons linéaires $\lambda_1 a_1 + \cdots + \lambda_n a_n$ avec $\lambda_i \in A$ et on le note $(a_1, \ldots, a_n)$.

7.5 *Remarque.* Dans le cas de $\mathbf{Z}[i\sqrt{d}]$, le fameux facteur commun "idéal" à 3 et $4 + i\sqrt{5}$ de Kümmer, noté $(3, 4 + i\sqrt{5})$ n'est autre que l'idéal (non principal) engendré à la fois par 3 et $4 + i\sqrt{5}$, et cet idéal est exactement la somme des deux autres, ce qui correspond bien au pgcd.

Dans la foulée, on peut dire ce que sont deux idéaux étrangers, ce sont ceux qui n'ont comme seul diviseur commun que l'idéal trivial $(1) = A$:

7.6 Définition. *Les idéaux I et J sont dits* **étrangers** *si le seul idéal qui les contient est l'idéal unité $(1) = A$, c'est-à-dire si on a $I + J = A$.*

Dans le cas de deux éléments, la condition $(a, b) = 1$ n'est autre que la relation de Bézout.

Il reste à définir le produit de deux idéaux. C'est simplement l'idéal engendré par les produits :

7.7 Définition. *Le* **produit** *des idéaux $I = (a_1, \cdots, a_n)$ et $J = (b_1, \cdots, b_m)$ est l'idéal IJ engendré par tous les produits $a_i b_j$ (on vérifie que cette définition ne dépend pas du choix des générateurs). Il est contenu dans I et J.*

Nous sommes maintenant en mesure de prouver que la relation (5) est vraie si on la pense en termes d'idéaux. Cela résulte du lemme suivant :

7.8 Lemme. *Soient A un anneau intègre et $a, u, v \in A$. On suppose que a divise uv et que u et v sont étrangers, c'est-à-dire qu'on a, en termes d'idéaux, $(u, v) = (1)$. Alors on a la formule, sur les idéaux : $(a) = (a, u)(a, v)$.*

Démonstration. Le produit des idéaux est l'idéal $I = (a^2, av, au, uv)$. Comme uv est multiple de a il est clair que I est inclus dans (a). Réciproquement, on a une relation de Bézout $\lambda u + \mu v = 1$ qui donne, en multipliant par a, $\lambda ua + \mu va = a$, ce qui montre que a est dans I.

Ce lemme donne les deux décompositions

$$(3) = (3, 4 + i\sqrt{5})(3, 4 - i\sqrt{5}), \qquad (7) = (7, 4 + i\sqrt{5})(7, 4 - i\sqrt{5})$$

d'où la décomposition de (21) en produit de quatre idéaux. Il donne aussi les décompositions $(4 + i\sqrt{5}) = (3, 4 + i\sqrt{5})(7, 4 + i\sqrt{5})$ et $(4 - i\sqrt{5}) = (3, 4 - i\sqrt{5})(7, 4 - i\sqrt{5})$ et ces diverses décompositions expliquent la non unicité de la décomposition du nombre 21 comme la formule (4) explique la formule (2).

7.3 Les anneaux de Dedekind

Il nous reste une dernière notion à définir pour achever notre parcours, c'est celle d'idéal premier. On prend une définition qui, dans le cas d'un idéal principal, n'est autre que le lemme d'Euclide :

7.9 Définition. *Un idéal I est dit* **premier** *s'il est différent de A et s'il vérifie :*

$$\forall a, b \in A, \quad ab \in I \Longrightarrow a \text{ ou } b \in I.$$

Avec toutes ces définitions, on montre (voir [S] ou [ST]) que l'anneau $\mathbf{Z}[i\sqrt{d}]$ (pour $d \equiv 1, 2 \mod 4$) est ce qu'on appelle un anneau de Dedekind[11], ce qui signifie qu'on a un théorème d'existence et d'unicité d'une décomposition, non plus de tout élément de A, mais de tout **idéal** en produit d'**idéaux** premiers, comme on l'a vu ci-dessus pour l'idéal (21).

7.4 Retour sur le théorème crucial

On peut alors reprendre la démonstration du théorème crucial 6.13. On suppose toujours d sans facteur carré et $d \equiv 1, 2 \mod 4$. On peut déjà formuler en termes d'idéaux la condition :

7.10 Lemme. *Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$. Alors les idéaux (z) et $(\overline{z})$ sont étrangers dans $\mathbf{Z}[i\sqrt{d}]$.*

Démonstration. L'idéal $(z, \overline{z})$ contient $z+\overline{z} = 2y$ et $z-\overline{z} = 2i\sqrt{d}$, donc aussi $2d$. Mais on a vu dans la preuve de 6.13 que x et $2d$ sont premiers entre eux et on a donc une relation de Bézout dans $\mathbf{Z}$: $\lambda x + 2\mu d = 1$, qui montre que 1 est dans $(z, \overline{z})$.

Ensuite le raisonnement est le même que celui mené dans le cas factoriel mais en utilisant la décomposition unique des idéaux en produits d'idéaux premiers. On décompose les idéaux (z), $(\overline{z})$ et (t) en produit d'idéaux premiers :

$$(z) = \mathcal{P}_1^{\alpha_1} \cdots \mathcal{P}_r^{\alpha_r}, \quad (\overline{z}) = \mathcal{Q}_1^{\beta_1} \cdots \mathcal{Q}_s^{\beta_s}, \quad (t) = \mathcal{R}_1^{\gamma_1} \cdots \mathcal{R}_n^{\gamma_n}.$$

Dire que (z) et $(\overline{z})$ sont étrangers signifie que les $\mathcal{P}_i$ et les $\mathcal{Q}_j$ sont distincts. On a alors

$$(t^3) = (t)^3 = \mathcal{R}_1^{3\gamma_1} \cdots \mathcal{R}_n^{3\gamma_n} = (z)(\overline{z}) = \mathcal{P}_1^{\alpha_1} \cdots \mathcal{P}_r^{\alpha_r}\, \mathcal{Q}_1^{\beta_1} \cdots \mathcal{Q}_s^{\beta_s}$$

et, en vertu de l'unicité de la décomposition, on voit que les $\mathcal{P}_i$ sont parmi les $\mathcal{R}_k$ et que leurs exposants sont multiples de 3 : $\alpha_i = 3\alpha_i'$. On aboutit donc à la conclusion que l'idéal principal (z) est le cube de l'idéal $I = \mathcal{P}_1^{\alpha_1'} \cdots \mathcal{P}_r^{\alpha_r'}$. Si ce dernier est principal, disons $I = (w)$, on a $z = \pm w^3$ et on conclut

[11] Dans le cas d congru à 3, c'est l'anneau $\mathbf{Z}[\alpha_d]$ vu au paragraphe 6.6 qui est un anneau de Dedekind.

comme précédemment. Le problème qui nous reste posé est donc le suivant : un idéal I dont le cube est principal est-il automatiquement principal ? Ce n'est pas toujours vrai et cela constitue la deuxième difficulté fondamentale de la théorie : repasser des idéaux aux nombres.

On entre là au plus profond de la théorie et il n'est pas raisonnable d'aller plus loin. Donnons simplement un nom[12] au phénomène constaté :

7.11 Définition. *Soit A un anneau de Dedekind. Un nombre premier p sera dit* **régulier** *pour A si tout idéal dont la puissance p-ième est principal est lui-même principal.*

Avec cette définition, on peut énoncer :

7.12 Théorème. *On suppose que d est un entier sans facteur carré et congru à 1 ou 2 modulo 4 et que 3 est régulier pour $\mathbf{Z}[i\sqrt{d}]$. Soient x, y des entiers vérifiant $x^3 = y^2 + d$. On pose $z = y + i\sqrt{d}$. Alors les nombres z et $\overline{z}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$ et sont des cubes de $\mathbf{Z}[i\sqrt{d}]$.*

7.13 Corollaire. *Soit d un entier sans facteur carré, $\equiv 1, 2 \mod 4$, et tel que 3 est régulier pour $\mathbf{Z}[i\sqrt{d}]$. Alors :*
1) Si d n'est pas de la forme $3a^2 \pm 1$ l'équation de Bachet $x^3 = y^2 + d$ n'a pas de solutions dans $\mathbf{Z}$.
2) Si $d = 3a^2 \pm 1$, les solutions positives de l'équation de Bachet sont

$$x = a^2 + d, \qquad y = a(3d - a^2).$$

7.14 *Remarques.*
1) Si 3 n'est pas régulier pour $\mathbf{Z}[i\sqrt{d}]$, il se peut que l'équation admette des solutions même si d n'est pas de la forme $3a^2 \pm 1$. C'est le cas pour $d = 89$ où on a la solution $5^3 = 125 = 6^2 + d = 36 + 89$. Si 3 n'est pas régulier et si d est de la forme $3a^2 \pm 1$, il peut y avoir des solutions autres que celles annoncées dans le corollaire 10. Par exemple, pour $d = 26 = 3.3^2 - 1$ la solution annoncée est $x = 35, y = 207$, mais il y a aussi la solution évidente $x = 3, y = 1$).
2) Les deux difficultés rencontrées ci-dessus (la non unicité de la décomposition en irréductibles, le problème du retour des idéaux aux nombres) sont aussi celles qui se rencontrent dans l'approche de Kümmer du dernier théorème de Fermat : i.e., la recherche des solutions entières de $x^p + y^p = z^p$, avec p

[12]Cette définition n'est pas habituelle. Ce qu'on définit, en fait, c'est un entier $h(A)$ associé à A et appelé nombre de classes d'idéaux de A et notre condition signifie exactement que p ne divise pas $h(A)$.

premier. L'idée initiale est analogue : on décompose le premier membre de l'équation dans les complexes

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

où l'on note ζ (ou ζ_p) une racine primitive p-ième de l'unité. On est ainsi amené à travailler dans l'anneau $\mathbf{Z}[\zeta]$ des nombres complexes de la forme $a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ avec $a_i \in \mathbf{Z}$, (notamment on voudrait montrer que les $x+\zeta^i y$ sont des puissances p-ièmes dans cet anneau), et ce, en faisant des raisonnements de divisibilité comme ceux faits ci-dessus pour l'équation de Bachet. Bien entendu (et c'est ce que disait Kümmer dans le texte cité plus haut), cet anneau n'est pas factoriel en général (c'est vrai seulement pour $p \leq 19$). Comme pour l'équation de Bachet on contourne cette difficulté en utilisant la décomposition en idéaux premiers mais on tombe ici encore sur la deuxième difficulté, qui est ici de savoir si un idéal I tel que I^p soit principal est lui-même principal. Si p est régulier, la méthode de Kümmer démontre le théorème de Fermat. Malheureusement si p n'est pas régulier on ne sait pas conclure par cette méthode. Or il y a beaucoup de nombres premiers irréguliers : on sait qu'il y en a une infinité alors qu'on ne le sait pas pour les réguliers. Cependant on conjecture (et on vérifie expérimentalement) que la densité des réguliers est environ égale à $0,6065$, donc plus grande que celle des irréguliers. Les plus petits irréguliers sont $37, 59$ et 67.

Cette difficulté n'est toujours pas entièrement surmontée à l'heure actuelle et la démonstration du théorème de Fermat qu'Andrew Wiles a donnée en 1993-94 est fondée sur une approche radicalement différente.

8 Références

[Hu] D. Husemoller, Elliptic Curves, Springer, 1987.

[K] G. Kümmer, Oeuvres complètes, Tome 1, éditées par A. Weil, Springer Verlag, 1975.

[P] D. Perrin, Cours d'algèbre, Ellipses, 1995.

[S] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[ST] I. Stewart-D.O. Tall, Algebraic Number Theory, Chapmann-Hall, 1987.

[W] A. Weil, Number Theory, An approach through history, Birkhaüser, 1984.