3.4

Travail demandé :

Il vous est demandé d'étudier puis de présenter le texte joint à travers un exposé de synthèse d'une durée comprise entre 15 et 20 minutes.

Si l'étude de la totalité du dossier et la préparation d'un exposé cohérent dans la durée impartie ne vous paraît pas possible, vous pouvez décider de vous limiter à une partie du dossier.

Remarques générales :

1. Les textes proposés, quelle que soit leur origine, peuvent présenter des défauts (coquilles typographiques, négligences ou sous-entendus de l'auteur, voire erreurs...) qui, sauf exception, n'ont pas été corrigés.

2. Les textes proposés peuvent contenir des exercices qu'il n'est pas demandé de résoudre. Néanmoins, vous pouvez vous aider des énoncés de ces exercices pour enrichir votre exposé.

3. Vous pouvez annoter les documents qui vous sont fournis. Vos annotations ne seront pas regardées par l'examinateur.

Autour de l'équation diophantienne $t^3 = x^2 + d$

0. Introduction.

L'équation en x et t, $t^3 = x^2 + 2$, semble avoir été étudiée pour la première fois en 1621 par Bachet qui, à partir de la solution évidente $t = 3, x = 5$, a donné une méthode géométrique pour construire d'autres solutions **rationnelles**, cf. ci-après, 4.e. Fermat, lui, se pose le problème d'en trouver les solutions **entières** ([1]) :

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

Bien entendu, et 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 (cf. cependant [W] Ch.II, §XVI et ci-dessous §5). En revanche on imagine assez bien comment ses successeurs (Euler, Gauss, Kümmer) pouvaient aborder ce problème et sa généralisation à l'équation diophantienne (c'est-à-dire en nombres entiers) $t^3 = x^2 + d$, avec $d \in \mathbf{N}^*$, que nous désignerons ici sous le nom d'**équation de Bachet**.

Ce texte ne prétend nullement être un travail d'historien, mais son but est plutôt, en transposant sur cet exemple (qui a l'avantage d'être beaucoup plus simple, mais cependant non trivial) les tentatives de démonstration du "dernier théorème de Fermat" au siècle dernier, de montrer où et comment apparaissent les difficultés de la théorie et quels moyens ont été employés pour y faire face. Les indications historiques sont, pour la plupart, extraites du livre d'André Weil [W] (voir aussi [Bbki], [E], [EU], [R]).

1. Premiers pas.

On sait que Fermat s'est beaucoup intéressé aux nombres entiers qui sont sommes de deux carrés d'entiers, ou, plus généralement, qui sont de la forme $a^2 + db^2$ pour $d \in \mathbf{N}$,

$d \neq 0$ et $a, b \in \mathbf{N}$. C'est le cas, bien entendu, du deuxième membre de l'équation de Bachet.

Concernant ces entiers, il semble bien que l'identité

$$(1) \qquad (a^2+b^2)(u^2+v^2) = (au+\epsilon bv)^2 + (av-\epsilon bu)^2 \quad \text{avec} \quad \epsilon = \pm 1$$

(qui montre que les sommes de deux carrés sont stables par multiplication) ait été connue d'Euclide pour $u = v = 1$ (sous forme géométrique) et, dans le cas général, de Diophante, cf. [W] Ch.I §VI. De même sa généralisation, pour $d \in \mathbf{N}$,

$$(2) \qquad (a^2+db^2)(u^2+dv^2) = (au+\epsilon dbv)^2 + d(av-\epsilon bu)^2 \quad \text{avec} \quad \epsilon = \pm 1$$

(qui montre que les entiers de la forme $a^2 + db^2$ sont stables par multiplication) semble elle aussi avoir été connue depuis longtemps (et notamment du mathématicien indien Brahmagupta, 598-665?, cf. [W] Ch.I, §VIII) et, en tous cas, à l'époque de Fermat. On comprend mieux cette formule en utilisant les nombres complexes : on pose $z = a + bi\sqrt{d}$, $w = u + vi\sqrt{d}$ et on calcule $|z|^2 = z\overline{z} = a^2 + db^2$.([3]) La formule (2) exprime seulement l'égalité $(z\overline{z})(w\overline{w}) = (zw)(\overline{zw}) = (z\overline{w})(\overline{z}w)$. Fermat connaissait la formule (2), mais rien n'indique qu'il ait jamais fait usage des imaginaires, pourtant introduits, notamment par Bombelli, au siècle précédent. La méthode de calcul ci-dessus remonte à Euler et Lagrange, vers le milieu du XVIII-ème siècle.

En appliquant la formule (2) avec $u = a$, $v = b$ et $\epsilon = -1$ on trouve $(a^2 + db^2)^2 = (a^2 - db^2)^2 + d(2ab)^2$ ce qui montre que si un entier est de la forme $a^2 + db^2$ il en est de même de son carré (et ce de façon non banale si a et b sont non nuls). La même formule appliquée avec $u = a^2 - db^2$, $v = 2ab$ et $\epsilon = -1$ ([4]) (ce qui revient encore à calculer $(z\overline{z})^3 = z^3\overline{z}^3$) donne la décomposition du cube, c'est-à-dire l'identité

$$(3) \qquad (a^2+db^2)^3 = (a^3-3dab^2)^2 + d(3a^2b-db^3)^2.$$

L'hypothèse que formule André Weil ([W] Ch. II, §XVI) est que Fermat, pour $d = 1$ ou 2, connaissait (savait prouver ?, cf. §5 pour une discussion) une réciproque de la formule (3), c'est-à-dire, précisément, l'assertion suivante que nous appellerons "Conjecture naïve pour l'entier d" :

Conjecture naïve pour l'entier d. *Soit $d \in \mathbf{N}^*$. On suppose que l'on a $t^3 = x^2 + dy^2$ avec $x, y, t \in \mathbf{Z}$, et x et y premiers entre eux. Alors il existe des entiers a, b tels que l'on ait $t = a^2 + db^2$, $x = a^3 - 3dab^2$ et $y = 3a^2b - db^3$.*

Cette conjecture est exactement la réciproque de (3), à ceci près que l'on suppose les entiers x et y premiers entre eux. Nous verrons plus loin l'intérêt de cette hypothèse, qui est évidemment vérifiée dans le cas de l'équation de Bachet puisqu'alors on a $y = 1$. Notons

([3]) Les arithméticiens notent $N(z)$ ("norme" de z) le carré du module de z. Cette quantité joue un rôle capital en théorie des nombres, cf. par exemple ci-dessous Lemme 2, Proposition 5 et encadrés 1 et 2.

([4]) On vérifiera que les autres choix de signes ne donnent rien, cf. §5.

dès maintenant que la conjecture naïve, si elle est vraie, fournit la solution de l'équation de Bachet pour $d = 2$ annoncée par Fermat (pour le cas $d = 4$ cf. §4 b)). En effet, si on a $t^3 = x^2 + 2$, comme x et 1 sont premiers entre eux, il existe des entiers a et b tels que $t = a^2 + 2b^2$, $x = a^3 - 6ab^2$ et $1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2)$. La dernière égalité montre que l'on a $b = \pm 1$ et donc $3a^2 - 2 = b = \pm 1$. On en déduit $b = 1$ et $a = \pm 1$, d'où $t = 3$ et $x = 5$, comme annoncé.

En fait, si la conjecture naïve est vraie pour un entier d elle donne toutes les solutions de l'équation de Bachet $t^3 = x^2 + d$ par le même calcul que ci-dessus. On voit en effet qu'on a encore $b = \pm 1$, donc que l'équation ne peut avoir de solutions que si d est de la forme $d = 3a^2 \pm 1$ avec $a \in \mathbf{N}$ et qu'alors, les solutions positives sont données par les formules :

$$t = a^2 + d, \quad x = |a^3 - 3ad| = 3ad - a^3. \tag{4}$$

En tout état de cause, même si la conjecture n'est pas vraie, les formules (4) fournissent des solutions de l'équation de Bachet dès que d est de la forme $3a^2 + \epsilon$ avec $\epsilon = \pm 1$. Les tableaux ci-dessous donnent les plus petits exemples d'entiers d pour lesquels on a de telles solutions et les valeurs de t et x correspondantes.

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

a	0	1	2	3	4	5
d	1	4	13	28	49	76
t	1	5	17	37	65	101
x	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
t	3	15	35	63	99
x	5	58	207	500	985

2. Une tentative de démonstration de la conjecture naïve.

S'il n'est pas évident de savoir comment Fermat pouvait procéder, nous connaissons aujourd'hui une méthode (qui remonte sans doute à Euler) pour aborder ce type de problèmes. Elle consiste, comme on l'a déjà vu, à décomposer $x^2 + dy^2$ dans $\mathbf{C}$:

$$x^2 + dy^2 = (x + iy\sqrt{d})(x - iy\sqrt{d}) = z\overline{z} \tag{5}$$

en notant que les complexes z et $\overline{z}$ sont à coefficients entiers, donc sont dans l'anneau ([5])

$$\mathbf{Z}[i\sqrt{d}] = \{z = x + iy\sqrt{d} \in \mathbf{C} \ \mid \ x, y \in \mathbf{Z}\ \}.$$

([5]) Dire que $\mathbf{Z}[i\sqrt{d}]$ est un sous-anneau de $\mathbf{C}$ signifie simplement qu'il contient $\mathbf{Z}$ et qu'il est stable par addition et multiplication.

Le premier avantage de ce cadre est qu'il permet de formuler très simplement la conjecture naïve : on a $t^3 = x^2 + dy^2 = z\overline{z}$ et il s'agit de montrer que z est **un cube** dans $\mathbf{Z}[i\sqrt{d}]$ (en effet, la relation $z = w^3$ avec $w = a + ib\sqrt{d}$ est exactement équivalente aux formules de la conjecture naïve).

Le second avantage de l'écriture ci-dessus réside dans le fait que les deux membres de l'équation $t^3 = z\overline{z}$ sont maintenant décomposés en produits, ce qui va permettre d'utiliser des raisonnements de divisibilité dans l'anneau $\mathbf{Z}[i\sqrt{d}]$. Pour s'en convaincre, remarquons que, dans les entiers ordinaires, on montre aisément par ce type de méthodes (divisibilité, nombres premiers) une proposition analogue :

Proposition 1. *Si un produit de deux entiers premiers entre eux est un cube, chacun d'eux est un cube.*

Démonstration. Supposons qu'on ait $ab = t^3$ avec a et b premiers entre eux. On décompose a et b en produits de nombres premiers :

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad b = q_1^{\beta_1} \cdots q_s^{\beta_s}.$$

Comme a et b sont premiers entre eux, les p_i sont distincts des q_j. Décomposons aussi $t = \pi_1^{\gamma_1} \cdots \pi_n^{\gamma_n}$. On a alors

$$t^3 = \pi_1^{3\gamma_1} \cdots \pi_n^{3\gamma_n} = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}.$$

Mais, en vertu de l'unicité de la décomposition, ceci montre que les p_i sont parmi les π_k et, puisqu'ils sont distincts des q_j, cela prouve que leurs exposants sont multiples de 3, donc que a est un cube (et de même pour b).

Deux remarques s'imposent sur cette démonstration. D'abord, on y utilise de façon essentielle l'existence et l'unicité de la décomposition d'un entier en produit de facteurs premiers. Ensuite, on voit clairement l'intérêt de l'hypothèse a et b premiers entre eux pour éviter que les facteurs premiers ne se mélangent (sinon le résultat peut être en défaut, cf. par exemple $8 = 2 \times 4$). C'est cette remarque qui justifie l'hypothèse x et y premiers entre eux dans la conjecture naïve, afin d'éviter des facteurs communs évidents de z et $\overline{z}$, cf. ci-dessous lemmes 3 et 4.

Afin de prouver la conjecture naïve, nous allons essayer de copier la démonstration précédente en faisant dans l'anneau $\mathbf{Z}[i\sqrt{d}]$ des raisonnements de divisibilité comme ceux que nous avons faits ci-dessus dans $\mathbf{Z}$. C'est d'ailleurs ce que faisaient allègrement, au moins au début, Euler, Legendre et certains de leurs successeurs.

En termes modernes nous allons supposer que cet anneau est **factoriel**, c'est-à-dire que tout élément y admet une décomposition **unique** (à l'ordre près et à des inversibles près) en produit d'éléments irréductibles (ces éléments généralisent les nombres premiers de $\mathbf{Z}$, voir encadré 1 pour des définitions plus précises).

Nous verrons plus loin que cette hypothèse est très optimiste, mais pour l'instant nous allons faire comme si elle était vérifiée. Notons déjà que dans le cas de $\mathbf{Z}[i\sqrt{d}]$ les éléments inversibles ne sont pas très nombreux, ([6]) ce qui simplifie notre tâche :

([6]) Ce ne serait pas le cas dans l'anneau $\mathbf{Z}[\sqrt{d}]$ qui en contient une infinité, cf. [S] IV 6.

Lemme 2. *Pour $d > 1$ les seuls éléments inversibles de $\mathbf{Z}[i\sqrt{d}]$ sont 1 et -1. Pour $d = 1$ les éléments inversibles de $\mathbf{Z}[i]$ sont $\pm 1, \pm i$.*

Démonstration. C'est le moment de se servir de la norme : si $z = a + ib\sqrt{d}$ est inversible dans $\mathbf{Z}[i\sqrt{d}]$ il existe w dans $\mathbf{Z}[i\sqrt{d}]$ avec $zw = 1$. Comme la norme $N(z) = |z|^2$ est multiplicative, on en déduit $N(z)N(w) = 1$. Comme $N(z)(= a^2 + db^2)$ et $N(w)$ sont des entiers ≥ 0 cela n'est possible que si $N(z) = 1$. Si $d > 1$ on voit que cela impose $b = 0$, $a = \pm 1$, tandis que pour $d = 1$ on a, en outre, les solutions $a = 0$, $b = \pm 1$.

Pour prouver la conjecture nous allons faire plusieurs **hypothèses simplificatrices**, voir §4 pour des compléments sur les autres cas. Nous supposerons donc que d n'a pas de facteur carré (i.e., qu'il s'écrit $d = p_1 \cdots p_r$ avec les p_i premiers distincts) et qu'il est congru à 1 ou 2 (mod.4). De plus, nous supposerons $d \neq 1$, de sorte que les seuls éléments inversibles de $\mathbf{Z}[i\sqrt{d}]$ sont 1 et -1 (cf. lemme 2).

On a alors le lemme suivant qui ne met en jeu que les entiers ordinaires :

Lemme 3. *Soit d un entier > 0 sans facteur carré et congru à 1 ou 2 modulo 4. Si on a $t^3 = x^2 + dy^2$, avec $x, y, t \in \mathbf{Z}$, et x, y premiers entre eux, alors t est impair et premier avec d et x est premier avec d.*

Démonstration. Dans les deux cas on raisonne par l'absurde :

Si t est pair on a $t^3 \equiv 0 \pmod 4$. Si y est pair, x l'est aussi ce qui est absurde car x et y sont premiers entre eux. Si y est impair on a $y^2 \equiv 1 \bmod 4$ donc $-d \equiv x^2$, mais, comme $-d \equiv -1$ ou $2 \bmod 4$, c'est impossible (-1 et 2 ne sont pas des carrés modulo 4).

Si p est un nombre premier qui divise t et d il divise x, donc p^2 divise dy^2, mais p ne divise pas y, donc p^2 divise d ce qui est absurde car d n'a pas de facteur carré.

Passons à notre "démonstration" de la conjecture naïve, sous les hypothèses ci-dessus et en supposant $\mathbf{Z}[i\sqrt{d}]$ factoriel. Soient t, x, y vérifiant $t^3 = x^2 + dy^2$. On écrit, dans l'anneau $\mathbf{Z}[i\sqrt{d}]$, $t^3 = z\overline{z}$ avec $z = x + iy\sqrt{d}$. Le lemme suivant va nous ramener dans la situation de la proposition 1 :

Lemme 4. *On reprend les hypothèses du lemme 3 et on pose $z = x + iy\sqrt{d}$. Alors les nombres z et $\overline{z}$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$.*

Démonstration. Sinon, soit $p \in \mathbf{Z}[i\sqrt{d}]$ un facteur irréductible commun de z et $\overline{z}$. Comme p divise $z\overline{z} = t^3$ il divise t d'après le lemme d'Euclide (cf. encadré 1). Par ailleurs, p divise aussi $z + \overline{z}$ et $z - \overline{z}$ i.e., $2x$ et $2iy\sqrt{d}$. Comme x et y sont premiers entre eux, le théorème de Bézout dans $\mathbf{Z}$ montre qu'il existe $\lambda, \mu \in \mathbf{Z}$ avec $\lambda x + \mu y = 1$, d'où $2i\sqrt{d} = 2x(\lambda i\sqrt{d}) + \mu(2iy\sqrt{d})$. On en déduit que p divise $2i\sqrt{d}$, donc, *a fortiori*, $2d$ dans $\mathbf{Z}[i\sqrt{d}]$. Il divise donc à la fois t et $2d$. Or, par le lemme 3, t et $2d$ sont premiers entre eux et en écrivant encore Bézout dans $\mathbf{Z}$: $1 = at + b(2d)$, on voit que cela implique que p est inversible dans $\mathbf{Z}[i\sqrt{d}]$ ce qui est absurde.

La démonstration de la conjecture (c'est-à-dire du fait que z est un cube) se fait alors exactement comme si on était dans $\mathbf{Z}$, on décompose z et $\overline{z}$ en produits d'irréductibles dans $\mathbf{Z}[i\sqrt{d}]$:

$$z = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad \overline{z} = q_1^{\beta_1} \cdots q_s^{\beta_s}$$

où les p_i sont distincts des q_j en vertu du lemme 4. Décomposons aussi $t = \pi_1^{\gamma_1} \cdots \pi_n^{\gamma_n}$. On a alors

$$t^3 = \pi_1^{3\gamma_1} \cdots \pi_n^{3\gamma_n} = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_S}$$

Mais, **en vertu de l'unicité de la décomposition**, ceci montre que les p_i sont (au signe près) parmi les π_k et, puisqu'ils sont distincts des q_j, cela prouve que leurs exposants sont multiples de 3. On en déduit que $\pm z$ est un cube dans $\mathbf{Z}[i\sqrt{d}]$, puis que z est un cube car $-1 = (-1)^3$. On a donc $z = w^3$ avec $w = a + ib\sqrt{d}$, avec $a, b \in \mathbf{Z}$ et si on développe cette expression on trouve exactement les valeurs de x et y annoncées. De plus, on a alors $t^3 = (w\overline{w})^3$, donc $t = w\overline{w} = a^2 + db^2$ et on a prouvé la conjecture naïve.

3. Discussion.

La question qui se pose maintenant est de savoir pour quels entiers $d > 0$ l'anneau $\mathbf{Z}[i\sqrt{d}]$ est factoriel. La réponse est rapide et décevante :

Proposition 5. *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 l'anneau est euclidien (i.e., on a une division euclidienne comme dans les entiers) et cela implique qu'il est factoriel, voir encadré 2.

Si $d \geq 3$ on vérifie d'abord que 2 est irréductible dans l'anneau. Sinon, on aurait $2 = zw$ donc $N(2) = 4 = N(z)N(w)$ avec z et w non inversibles donc de normes $\neq 1$. Ceci donne $N(z) = N(w) = a^2 + db^2 = 2$ et on voit aussitôt que c'est impossible.

Mais alors le nombre 2 contredit le lemme d'Euclide :
— si d est pair, on a $d = -(i\sqrt{d})(i\sqrt{d}) = 2d'$ et 2 ne divise pas $i\sqrt{d}$,
— si d est impair, on a $d + 1 = (1 + i\sqrt{d})(1 - i\sqrt{d}) = 2m$ et on conclut de la même façon.

On voit donc que la démonstration proposée ci-dessus ne fonctionne en réalité que pour $d = 1$ ou $d = 2$ (et, avec une variante, pour $d = 4$, cf. §4.b), c'est-à-dire les cas connus de Fermat.

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-ème siècle, mais au début du XIX-ème 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 "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 ([7]) :

$$21 = 3 \times 7 = (4 + i\sqrt{5})(4 - i\sqrt{5}). \tag{6}$$

([7]) Note pour les experts : cet exemple n'est pas le plus simple mais il est choisi pour que les facteurs 3 et 7 admettent dans $\mathbf{Z}[i\sqrt{d}]$ des décompositions en produits de deux idéaux premiers distincts, ce qui ne serait plus le cas si on utilisait les nombres 2 ou 5 qui sont ramifiés dans $\mathbf{Z}[i\sqrt{d}]$: $(2) = (2, 1 + i\sqrt{5})^2$ et $(5) = (i\sqrt{5})^2$.

On vérifie aisément que les facteurs sont des irréductibles (il suffit de noter que 3 et 7 ne sont pas des normes d'éléments de $\mathbf{Z}[i\sqrt{d}]$) et on est donc en présence d'un cas de non-unicité de la décomposition. Une hypothèse plausible consiste à imaginer que Kümmer a interprété l'égalité (6) comme l'analogue de la décomposition dans $\mathbf{Z}$:

$$14 \times 15 = 10 \times 21. \tag{7}$$

Dans ce dernier cas la non unicité de la décomposition vient, bien entendu, du fait que les nombres ne sont pas irréductibles et (7) s'écrit simplement

$$(2 \times 7) \times (5 \times 3) = (2 \times 5) \times (7 \times 3). \tag{8}$$

Si on désigne par (a, b) le pgcd de a et b dans $\mathbf{N}$, on peut encore écrire (8) sous la forme suivante :

$$(14, 10)(14, 21)(15, 10)(15, 21) = (14, 10)(15, 10)(14, 21)(15, 21) \tag{9}$$

que l'on peut généraliser au cas $ab = uv$ grâce au lemme évident suivant :

Lemme 6. *Soient $a, u, v \in \mathbf{N}$. On suppose que a divise uv et qu'on a $(u, v) = 1$. Alors, on a $a = (a, u)(a, v)$.*
Si on a $a, b, u, v \in \mathbf{N}$ avec $ab = uv$ et $(a, b) = (u, v) = 1$, on peut écrire l'égalité $ab = uv$ sous la forme

$$(a, u)(a, v)(b, u)(b, v) = (a, u)(b, u)(a, v)(b, v). \tag{10}$$

Revenons alors à l'égalité (6) que l'on interprète sous la forme $ab = uv$. Dans cette décomposition, les divers facteurs : $a = 3$, $b = 7$, $u = 4 + i\sqrt{5}$ et $v = 4 - i\sqrt{5}$ 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 sont non seulement premiers entre eux, mais étrangers, c'est-à-dire, cf. encadré 1, vérifient une relation de Bézout dans $\mathbf{Z}[i\sqrt{d}]$. C'est clair pour 3 et 7 et pour les autres on a

$$(4 + i\sqrt{5})(14 + 9i\sqrt{5}) + (4 - i\sqrt{5})(10 - 10i\sqrt{5}) = 1.$$

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, 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 (7) 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 (6) s'écrive alors sous la forme analogue à (9) ou (10) :

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

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] p. 298 ou [EU] Article Kümmer, (il s'agit du cas de $\mathbf{Z}[\zeta]$ et non de $\mathbf{Z}[i\sqrt{d}]$, cf. Rem. 11.2, mais le problème est identique) : *"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 :*

$$a_0 + a_1\zeta + \cdots + a_{n-1}\zeta^{n-1}$$

mais qu'on peut la sauver en introduisant un nouveau genre de nombres complexes que j'ai nommé nombre complexe idéal. Les applications de cette théorie à la démonstration du Th. de Fermat m'ont occupé depuis longtemps et j'ai réussi à faire dépendre l'impossibilité de l'équation de deux propriétés d'un nombre premier, en sorte qu'il ne reste plus qu'à rechercher si elles appartiennent à tous les nombres premiers.".

En termes modernes le facteur commun "idéal" à 3 et $4+i\sqrt{5}$ c'est simplement l'idéal (non principal) engendré à la fois par 3 et $4+i\sqrt{5}$, noté aussi $(3,\ 4+i\sqrt{5})$ et il "divise" les autres au sens où il contient les idéaux engendrés par 3 et $4+i\sqrt{5}$, cf. encadré 3. De plus, cet idéal est exactement la somme des deux autres, ce qui correspond bien au pgcd.

Précisément, on montre aujourd'hui que l'anneau $\mathbf{Z}[i\sqrt{d}]$ (pour $d \equiv 1, 2 \bmod 4$, cf. compléments pour le cas $d \equiv -1 \bmod 4$) est ce qu'on appelle un anneau de Dedekind, et qu'on a dans un tel anneau un théorème d'existence et d'unicité d'une décomposition de tout **idéal** en produit d'**idéaux** premiers (cf. encadré 3 pour les définitions et [S] III 4 ou [ST] I 5 pour les démonstrations). Ainsi pour revenir à l'exemple précédent, l'idéal (21) de $\mathbf{Z}[i\sqrt{5}]$ se décompose de manière unique en produit de quatre idéaux premiers :

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

En effet, cette formule résulte du lemme suivant, généralisation du lemme 6 :

Lemme 7. *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 $I = (a^2, av, au, uv)$, cf. encadré 3. 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 premiers. 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 (9) explique la formule (7).

On peut alors reprendre la démonstration de la conjecture naïve dans le cas d sans facteur carré et $\equiv 1, 2 \bmod 4$. Le lemme 4 est essentiellement inchangé, pourvu qu'on le formule en termes d'idéaux :

Lemme 8. *On reprend les hypothèses du lemme 3 et on pose $z = x + iy\sqrt{d}$. Alors les idéaux (z) et $(\overline{z})$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{d}]$.*

Démonstration. Sinon, cf. encadré 3, ils seraient tous deux contenus dans un idéal premier m (donc vérifiant $m \neq A$). Alors, $t^3 = z\overline{z}$ serait dans m, donc aussi t puisque m est premier. De même $2x = z + \overline{z}$ et $2iy\sqrt{d} = z - \overline{z}$ seraient dans m. Comme x et y sont premiers entre eux on a une relation de Bézout dans $\mathbf{Z}$, $ux + vy = 1$. En multipliant cette relation par $2i\sqrt{d}$ on en déduit $2i\sqrt{d} \in m$ et *a fortiori* $2d \in m$. Mais, en vertu du lemme 3, t et $2d$ sont premiers entre eux et on a encore une relation de Bézout dans $\mathbf{Z}$: $\lambda t + 2\mu d = 1$, ce qui montre que 1 serait dans m, contrairement à l'hypothèse $m \neq A$.

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 premiers entre eux 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 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.

Pour comprendre ce phénomène, on introduit, pour un anneau de Dedekind A, le groupe $C(A)$ des classes d'idéaux. Il s'agit de l'ensemble des idéaux de A, avec comme loi le produit des idéaux, comme élément neutre l'idéal unité $(1) = A$, mais où on passe au quotient par les idéaux principaux, c'est-à-dire qu'on les identifie tous à l'élément neutre. On montre, cf. [ST] II 9, que le groupe $C(A)$, dans le cas des anneaux de nombres, est un groupe abélien fini dont l'ordre (i.e. le cardinal) est noté $h(A)$ (et même $h(d)$ si $A = \mathbf{Z}[i\sqrt{d}]$).

Alors, pour revenir à notre problème, si l'idéal I^3 est principal sans que I le soit, cela signifie que I^3 est l'élément neutre dans $C(\mathbf{Z}[i\sqrt{d}])$ mais pas I, autrement dit que I est un élément d'ordre 3 dans le groupe $C(\mathbf{Z}[i\sqrt{d}])$. Comme l'ordre d'un élément divise l'ordre du groupe ceci n'est possible que si $h(d)$ est multiple de 3. Si $h(d)$ n'est pas multiple de 3 notre preuve de la conjecture naïve est complète et on a donc prouvé les théorèmes suivants (cf. pour plus de détails [IR] Ch.17 §10) :

Théorème 9. *Soit d un entier ≥ 2, sans facteur carré, $\equiv 1, 2 \bmod 4$, et tel que 3 ne divise pas $h(d)$. Alors la conjecture naïve est vraie pour l'entier d.*

Corollaire 10. *Soit d un entier ≥ 2, sans facteur carré, $\equiv 1, 2 \bmod 4$, et tel que 3 ne divise pas $h(d)$. Alors,*
1) Si d n'est pas de la forme $3a^2 \pm 1$ l'équation de Bachet $t^3 = x^2 + d$ n'a pas de solutions dans $\mathbf{Z}$.
2) Si $d = 3a^2 \pm 1$, les solutions positives de l'équation de Bachet sont

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

Remarques 11.
0) Bien entendu, pour appliquer ces résultats, il faut savoir calculer le nombre de classes $h(d)$ pour le d que l'on considère. En fait, ce nombre s'interprète aussi (pour $d \equiv 1, 2 \bmod 4$) comme le nombre de classes de formes quadratiques $ax^2 + bxy + cy^2$ à coefficients entiers de discriminant $-4d$ (modulo les changements de bases à coefficients entiers et de déterminant 1), le lien entre les deux étant donné, une fois encore, par la norme $N(x + iy\sqrt{d}) = x^2 + dy^2$. Sous cette forme, Gauss savait calculer ce nombre au moyen d'un algorithme très simple, cf. [G], numéros 171-175 et 234-256. Évidemment, à l'époque (1801), les idéaux n'avaient pas encore été inventés par Kümmer et la notion de groupe de classes d'idéaux et son lien avec les formes quadratiques entières ne seront clairement élucidés que par Kümmer et surtout Dedekind (vers 1860-70). C'est pourtant l'algorithme de Gauss qui a permis d'élaborer des tables donnant $h(d)$ pour $d \leq 4000000$ (Buell, 1976), voir pour tout cela [ST] II 9 ou [BS] ou encore l'excellent exposé d'Oesterlé [O].
1) Si 3 divise $h(d)$ il se peut que l'équation admette des solutions même si d n'est pas de la forme $3a^2 \pm 1$. Par exemple pour $d = 89$ on a $h(d) = 12$ et la solution de l'équation

est $5^3 = 125 = 6^2 + d = 36 + 89$. Si 3 divise $h(d)$ 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 $t = 35, x = 207$, mais il y a aussi la solution évidente $t = 3, x = 1$, (ici on a $h(26) = 6$).
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 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 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, autrement dit, si p divise ou non $h_p = h(\mathbf{Z}[\zeta_p])$. Si p ne divise pas h_p on dit que p est un nombre premier régulier et, pour ces nombres, 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 récente démonstration du théorème de Fermat par A. Wiles est fondée sur une approche radicalement différente.

Divisibilité

Soit A un anneau commutatif et intègre (par exemple un sous-anneau de $\mathbf{C}$).

Si a et b sont dans A on dit que b **divise** a s'il existe $c \in A$ avec $a = bc$.

Un élément z de A est dit **inversible** s'il existe $w \in A$ avec $wz = 1$. Les éléments inversibles divisent tous les éléments de A.

Un élément p de A, non nul et non inversible, est dit **irréductible** s'il n'a pas de diviseur non trivial, i.e. si $p = ab$ entraîne a ou b inversible. Si p est irréductible et u inversible pu est encore irréductible.

Deux éléments a, b de A sont dits **premiers entre eux** s'ils n'ont pas de diviseur commun non inversible. Une condition suffisante (mais non nécessaire) pour cela est qu'ils vérifient une égalité de Bézout $\lambda a + \mu b = 1$ avec $\lambda, \mu \in A$. On dira alors qu'ils sont **étrangers** dans A. Ils sont alors premiers entre eux dans tout anneau contenant A.

Un anneau intègre A est dit **factoriel** si tout élément non nul a de A s'écrit de manière unique (à permutation près et à des inversibles près) sous la forme $a = p_1 \cdots p_r$ où les p_i sont irréductibles.

Contrairement à ce qu'on pourrait penser le point crucial de cette définition n'est pas l'existence d'une décomposition, qui est le plus souvent banale, cf. ci-dessous, mais son unicité. Cette dernière équivaut au "lemme d'Euclide" : si un irréductible p divise un produit xy il divise x ou y, comme on le voit aussitôt en décomposant x, y et xy en produits d'irréductibles.

Montrons l'existence de la décomposition en irréductibles dans $\mathbf{Z}[i\sqrt{d}]$. On utilise la norme : supposons qu'il existe $z \in \mathbf{Z}[i\sqrt{d}]$ qui ne se décompose pas et choisissons un tel z de norme $N(z)$ minimum (c'est possible car $N(z)$ est un entier > 0). Alors z n'est pas irréductible, donc s'écrit $z = z'z''$ avec z' et z'' non inversibles, donc de normes > 1 (cf. Lemme 2). Mais alors on a $N(z') < N(z)$ et $N(z'') < N(z)$, donc, vu le choix de z, z' et z'' sont produits d'irréductibles, donc z aussi, ce qui est absurde.

Pour des précisions sur tous ces sujets d'arithmétique on pourra consulter [P] Ch. II, [S] I ou [ST] I 4.

Encadré 1

Factorialité de $\mathbf{Z}[i\sqrt{d}]$ pour $d = 1, 2$

On montre d'abord l'existence d'une division euclidienne dans $\mathbf{Z}[i\sqrt{d}]$: étant donnés z et w non nuls dans $\mathbf{Z}[i\sqrt{d}]$, il existe q et r dans $\mathbf{Z}[i\sqrt{d}]$ tels que l'on ait $z = wq + r$ et $N(r) < N(z)$ (ou encore $|r| < |z|$).

Notons que les points de $\mathbf{Z}[i\sqrt{d}]$ dans le plan complexe forment un réseau : ce sont les points à coordonnées entières sur la base $1, i\sqrt{d}$. On considère alors le quotient exact $z/w = x+i\sqrt{d}y \in \mathbf{C}$ et on l'approche par le point de $\mathbf{Z}[i\sqrt{d}]$ le plus proche, soit $q = a + i\sqrt{d}b$ où a et b sont les entiers les plus proches de x et y. On a donc $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$ et on en déduit $\left|\dfrac{z}{w} - q\right| \leq \dfrac{\sqrt{1+d}}{2} < 1$ (car $d \leq 2$, on notera que la dernière inégalité ne vaut plus pour $d \geq 3$). Si on pose $r = z - wq$ on a alors $r \in \mathbf{Z}[i\sqrt{d}]$ et $|r| < |w|$ comme annoncé.

On déduit de l'existence de la division le lemme d'Euclide. On montre d'abord le théorème de Bézout par des divisions successives (c'est l'algorithme d'Euclide pour trouver le pgcd, exactement comme dans $\mathbf{Z}$) : si $x, y \in \mathbf{Z}[i\sqrt{d}]$ sont premiers entre eux il existe $\lambda, \mu \in \mathbf{Z}[i\sqrt{d}]$ avec $\lambda x + \mu y = 1$. Alors, si p est irréductible, divise ab et ne divise pas a on a $\lambda p + \mu a = 1$ d'où $b = \lambda pb + \mu ab$ et p divise b.

Encadré 2

Idéaux d'un anneau

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 $a \in A$, $ax \in I$.

L'exemple le plus simple d'idéal est l'idéal **principal** (a) engendré par $a \in A$, c'est l'ensemble des multiples de a. Les idéaux principaux sont liés à la divisibilité par la relation évidente :

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

Plus généralement l'idéal $(a_1, \cdots, a_n)$ engendré par les éléments $a_1, \cdots, a_n \in A$ est l'ensemble des éléments de la forme

$$\lambda_1 a_1 + \cdots + \lambda_n a_n \quad \text{avec les } \lambda_i \in A.$$

On montre que dans $\mathbf{Z}[i\sqrt{d}]$ tous les idéaux sont de cette forme (on dit qu'ils sont de type fini).

Si I et J sont des idéaux quelconques on dira, de manière analogue à $(*)$ que I **divise** J si on a $J \subset I$. Deux idéaux ont toujours un "plus grand commun diviseur" qui est l'idéal somme $I+J$, ensemble des $x+y$ pour $x \in I$ et $y \in J$. Ainsi, l'idéal $(a, b) = (a) + (b)$ apparaît comme pgcd des idéaux principaux engendrés par a et b. Il n'est pas principal en général. Les idéaux I et J seront dits **premiers entre eux** 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 où I et J sont principaux cela signifie que leurs générateurs sont étrangers.

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.

Un idéal I est dit **premier** s'il est différent de A et vérifie $\forall a, b \in A, \quad ab \in I \Longrightarrow a$ ou $b \in I$. Dans le cas d'un idéal principal (p) cela signifie que p vérifie le "lemme d'Euclide".

Pour montrer que deux idéaux sont premiers entre eux il suffit de montrer qu'ils n'ont pas de facteur premier (idéal) commun, c'est-à-dire qu'ils ne sont pas contenus dans un même idéal premier (cela résulte de l'existence d'idéaux maximaux et du fait que ceux-ci sont premiers, cf. [P] Ch. II).

Encadré 3