Le problème 4 du numéro 558

d'Au fil des maths

Daniel PERRIN

La question

Trouver les quadruplets d'entiers naturels (a, b, c, d) tels que a^2, b^2, c^2 soient en progression arithmétique ainsi que $(a, b-d, c)$.

En fait, la question se ramène immédiatement à sa première partie : trouver a, b, c dont les carrés sont en progression arithmétique. En effet, si l'on a un tel triplet, il vérifie $2b^2 = a^2 + c^2$ ce qui impose que a et c ont même parité. On obtient alors l'unique d convenable en posant : $2d = 2b - a - c$. Sous cette forme simplifiée, la question est bien connue. On la trouve par exemple sur le site de Frédéric Laroche `http://laroche.lycee.free.fr/` qui est une source d'exercices passionnants. Pour ma part je l'ai traitée il y a quelque temps déjà, voir sur ma page web : `https://www.imo.universite-paris-saclay.fr/~daniel.perrin/Divers/Laroche1-56.pdf`. Je recopie (en noir ci-dessous) la solution que j'y donne. On verra qu'il y a de multiples manières d'aborder le problème, avec des approches différentes, certaines élémentaires et d'autres non.

Des carrés équidistants

Daniel PERRIN

1 Le problème

1.1 La question initiale

On sait que tous les entiers ne sont pas des carrés parfaits. Voici d'ailleurs la liste des vingt carrés ≤ 400 :

$$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225,$$

$$256, 289, 324, 361, 400.$$

Le thème de la recherche [1] est le suivant :

Trouver trois carrés d'entiers positifs régulièrement espacés, c'est-à-dire x, y, z avec $0 < x < y < z$ tels que $y^2 - x^2 = z^2 - y^2$. On appellera le triplet (x, y, z) une **triade**.

1.2 Quelques questions sur cette situation

Une rapide exploration à la main, avec la table ci-dessus, ou avec l'ordinateur (on a utilisé le logiciel SAGE) fournit de nombreuses solutions. La plus petite est $(x, y, z) = (1, 5, 7)$, donc $x^2 = 1 < y^2 = 25 < z^2 = 49$ avec un écart de 24 des deux côtés. SAGE en fournit beaucoup d'autres, y compris avec $x = 1$: outre $(1, 5, 7)$, déjà vue, il y a $(1, 29, 41)$; $(1, 169, 239)$, etc. Il y a aussi des solutions avec x plus grand : $(7, 13, 17)$, $(17, 25, 31)$, etc.

Parmi les questions les plus naturelles qui surgissent alors : y a-t-il beaucoup de solutions ? une infinité ? Comment les trouver toutes ? Tout nombre x (resp. y, resp. z) est-il partie d'une solution ? Sinon, quels sont ceux qui sont atteints ? Peuvent-ils l'être dans n'importe quelle position ? Si un nombre est atteint, de combien de manières l'est-il ? Quelles sont les valeurs possibles pour $y^2 - x^2 = z^2 - y^2$?

Nous verrons ci-dessous qu'il y a de nombreuses manières d'aborder ces questions, certaines élémentaires, d'autres moins.

1.3 Premières remarques

Les remarques suivantes permettent de baliser un peu le chemin :

1. Je me suis inspiré d'un exercice de Frédéric Laroche dont le site `http://laroche.lycee.free.fr/` est une véritable mine.

1.1 *Remarques.* 1) Il y a une unique solution entière de l'équation $x^2 - 2y^2 + z^2 = 0$ avec $xyz = 0$ qui est la solution $(0, 0, 0)$. C'est évident si $y = 0$ et si, par exemple, x est nul, on a $z^2 = 2y^2$ qui, comme $\sqrt{2}$ est irrationnel, n'a que $(0, 0)$ comme solution entière.

2) On peut supposer x, y, z premiers entre eux dans leur ensemble (sinon on obtient une solution plus petite en divisant par leur *pgcd*). On se limitera dans ce qui suit à la recherche de solutions **primitives**, c'est-à-dire avec x, y, z premiers entre eux.

3) Si x, y, z sont premiers entre eux dans leur ensemble et vérifient $x^2 + z^2 = 2y^2$ les entiers x, y, z sont tous trois impairs [2] et premiers entre eux deux à deux. En effet, si p premier divise x et y (resp. y et z) il divise z (resp. x) et c'est absurde. S'il divise x et z et pas y il est nécessairement égal à 2, mais alors $x^2 + z^2$ est multiple de 4, donc y est pair et c'est encore absurde.

4) Il est clair que, pour z fixé, il y a au plus un nombre fini de solutions pour x, y car x, y sont $< z$. Pour y fixé, il y a aussi au plus un nombre fini de solutions pour x, z car on a $x^2 + z^2 = 2y^2$, donc $x, z \leq y\sqrt{2}$. Nous verrons, en revanche, que, pour x fixé, il peut y avoir une infinité de y, z vérifiant l'équation (voir 5.9).

La remarque 3 ci-dessus (le fait que x, y, z soient impairs) donne une indication sur la différence des carrés en vertu du lemme suivant :

1.2 Lemme. *Si x et y sont impairs, avec $x < y$, $y^2 - x^2$ est multiple de 8.*

Démonstration. On pose $= 2p+1$, $y = 2q+1$ et on a $y^2-x^2 = 4(q^2+q-p^2-p)$ et $q(q + 1)$ et $p(p + 1)$ sont pairs.

Nous verrons plus loin que la différence des carrés d'une triade est aussi multiple de 3, donc de 24. Cela conduit à préciser la question :

1.3 Question. *Parmi les multiples de 24, lesquels sont les différences des carrés d'une triade ?*

L'expérience indique qu'il y en a assez peu. Par exemple les seules valeurs ≤ 1000 semblent être 24, 120, 240, 336, 720 et 840 (deux fois).

1.4 Reformulation du problème

Les remarques ci-dessus montrent que la recherche des solutions entières primitives de l'équation $y^2 - x^2 = z^2 - y^2$ est équivalente à la question suivante :

(♯) *Trouver des entiers positifs $x < y < z$ impairs et deux à deux premiers entre eux tels que $y^2 - x^2 = z^2 - y^2$.*

2. Exercice pour le lecteur. Il suffit de raisonner avec les congruences modulo 4.

2 Une approche élémentaire

Cette approche peut permettre d'aborder le problème dans une classe de lycée.

2.1 Détermination des solutions de (♯)

On part de la remarque suivante :

2.1 Proposition. *La question (♯) est équivalente à la suivante :*
(♯♯) *Trouver des entiers positifs p, q, r, s, avec $p < q$ tels que p, q (resp. r, s) soient premiers entre eux et qu'on ait les relations $pq = rs$ et $p + q = s - r$.*

Démonstration. Si l'on a une solution x, y, z de (♯), les entiers x, y, z sont impairs, de sorte que leurs différences et leurs sommes sont paires. On pose $2p = y - x$, $2q = x + y$, $2r = z - y$ et $2s = y + z$. On a bien $4pq = 4rs = y^2 - x^2 = z^2 - y^2$ et $p + q = y = s - r$. De plus, p et q sont premiers entre eux, sinon, si l est un nombre premier qui divise p, q, il divise $x = q - p$ et $y = p + q$ et c'est absurde. Le raisonnement est identique pour r, s.

Pour montrer la réciproque, nous aurons besoin d'un lemme :

2.2 Lemme. *Si p, q, r, s vérifient les conditions (♯♯), p et q sont de parités différentes, ainsi que r et s.*

Démonstration. Déjà, la condition $pq = rs$ montre qu'il suffit d'établir l'une des assertions, par exemple que p, q sont de parités différentes. Sinon, comme ils sont premiers entre eux, c'est que tous deux sont impairs, donc aussi r et s. On considère alors les congruences modulo 4. Les quatre nombres sont congrus à ± 1. Si p, q sont égaux modulo 4, on a $pq \equiv 1$ et donc r, s sont égaux modulo 4. Mais alors on a $p + q \equiv 2$ et $s - r \equiv 0$ et c'est absurde. Si p, q sont opposés modulo 4, r et s aussi et on conclut de la même manière avec $p + q = s - r$.

Revenons à 2.1. Si l'on a p, q, r, s vérifiant les conditions (♯♯), on pose $x = q - p$, $y = p + q = s - r$ et $z = r + s$ et on vérifie aussitôt que x, y, z vérifient les conditions (♯).

Voici encore une autre formulation :

2.3 Proposition. *La question (♯♯) est équivalente à la suivante :*
(♯♯♯) *Trouver des entiers positifs a, b, c, d deux à deux premiers entre eux vérifiant $ab + cd = bd - ac$.*

Démonstration. Si l'on a une solution p, q, r, s de (♯♯), on pose $a = pgcd(p, r)$, $b = pgcd(p, s)$, $c = pgcd(q, r)$, $d = pgcd(q, s)$. Je dis qu'on a $p = ab$, $q = cd$,

$r = ac$ et $s = bd$. En effet, si l'on décompose p, q, r, s en produit de facteurs primaires, la relation $pq = rs$, jointe au fait que r et s sont premiers entre eux, montre que p est produit des facteurs communs à p et r et de ceux communs à p et s et de même pour les autres. La relation $ab + cd = bd - ac$ est la traduction de $p + q = s - r$.

Inversement, si l'on a a, b, c, d vérifiant ($\sharp\sharp\sharp$), on a $ab \neq cd$ (sinon deux des nombres auraient un facteur commun car tous ne peuvent valoir 1 puisque $bd - ac$ est positif) et quitte à échanger a et c et b et d, on peut supposer $ab < cd$. On pose alors $p = ab$, $q = cd$, $r = ac$ et $s = bd$ et on a les conditions ($\sharp\sharp$).

En avant-première, montrons que cette approche permet déjà de construire une infinité de solutions de la question ($\sharp$) :

2.4 Corollaire. *Soit c un entier ≥ 1. Les entiers $x = 2c^2 - 1$, $y = 2c^2 + 2c + 1$ et $z = 2c^2 + 4c + 1$ vérifient les conditions ($\sharp$).*

Démonstration. On a une solution du problème ($\sharp\sharp\sharp$) en prenant pour c un entier positif quelconque et $a = 1$, $b = c + 1$ et $d = 2c + 1$. Cela donne $p = c + 1$, $q = 2c^2 + c$, $r = c$ et $s = 2c^2 + 3c + 1$ et on obtient les valeurs annoncées de x, y, z.

Mais elle permet surtout de montrer le théorème fondamental suivant, que nous reverrons en 3.1 :

2.5 Théorème. *Les solutions de la question ($\sharp$) sont données par les formules suivantes :*

$$(*) \qquad x = |-b^2 + 2bc + c^2|,\ y = b^2 + c^2,\ z = b^2 + 2bc - c^2,$$

avec b, c entiers positifs premiers entre eux, de parités différentes et tels que $b > c$. Précisément, on a $x = -b^2 + 2bc + c^2$ (resp. $x = b^2 - 2bc - c^2$) si $c > b(\sqrt{2} - 1) \sim 0.414b$ (resp. $c < b(\sqrt{2} - 1) \sim 0.414b$.

Démonstration. Si l'on a une solution x, y, z de ($\sharp$), elle provient d'une solution a, b, c, d de ($\sharp\sharp\sharp$). On a donc $d(b - c) = a(b + c)$. Cela montre déjà qu'on a $b > c$. Par ailleurs, si l est le *pgcd* de $b - c$ et $b + c$ il divise $2b$ et $2c$ et comme b, c sont premiers entre eux on a $l = 1$ ou $l = 2$.

Premier cas : $l = 1$, donc b, c de parités distinctes. On voit que $b - c$ divise a et on a $a = \lambda(b - c)$, $d = \lambda(b + c)$, ce qui, comme a, d sont premiers entre eux, donne $\lambda = 1$. On a donc $a = b - c$, $d = b + c$, donc $p = b^2 - bc$, $q = bc + c^2$, $r = bc - c^2$ et $s = b^2 + bc$ et on en déduit les valeurs de x, y, z de $(*)$. Si $-b^2 + 2bc + c^2$ est positif on garde cette valeur pour x et sinon on échange a, c d'une part et b, d de l'autre, comme on l'a vu dans 2.3, et on obtient les mêmes formules mais avec $x = b^2 - 2bc - c^2$.

Deuxième cas : $l = 2$, donc b, c de même parité. Comme b et c sont premiers entre eux, ils sont donc tous deux impairs. On a $b-c = 2u$, $b+c = 2v$ avec $u \wedge v = 1$, ce qui donne $b = u+v$ et $c = v-u$. On en déduit $ud = av$ et comme a est premier avec d, a divise u, $u = \lambda a$, puis $v = \lambda d$. Mais comme u, v sont premiers entre eux on a $a = u$ et $d = v$. On en déduit $p = u^2 + uv$, $q = v^2 - uv$, $r = uv - u^2$ et $s = uv + v^2$. Quitte à échanger, au besoin, a, c et b, d on obtient les formules suivantes pour x, y, z :

$$x = |-u^2 - 2uv + v^2|,\ y = u^2 + v^2,\ z = -u^2 + 2uv + v^2$$

avec u, v entiers positifs, premiers entre eux et tels que $v > u$. Mais ces formules redonnent celles du premier cas en posant $u = c$ et $v = b$.

La dichotomie entre les deux valeurs possibles de x s'obtient en étudiant le signe du trinôme en c : $c^2 + 2bc - c^2$ dont les racines sont $-b(1+\sqrt{2})$ et $b(\sqrt{2}-1)$.

2.2 Applications

2.2.1 Infinitude des solutions de (♯)

Elle a été vue en 2.4, mais 2.5 montre qu'elles correspondent précisément aux couples d'entiers positifs (b, c) avec $b > c$, b, c de parités différentes et premiers entre eux.

2.2.2 Les différences $y^2 - x^2$

2.6 Lemme. *Si x, y, z est solution de (♯), $y^2 - x^2 = z^2 - y^2$ est multiple de 3 (donc de 24 en vertu de 1.2).*

Démonstration. On a, avec les notations de 2.5, $z^2 - y^2 = 4bc(b^2 - c^2)$. Le résultat est clair si b ou c est multiple de 3 et sinon ils sont congrus à ± 1 modulo 3, donc leurs carrés à 1 et $b^2 - c^2$ est multiple de 3.

2.2.3 Les solutions avec y donné

Le théorème 2.5 donne aussitôt le résultat :

2.7 Corollaire. *Soit y un entier positif impair. Le problème (♯) admet une solution x, y, z si et seulement si y est somme de deux carrés d'entiers premiers entre eux, c'est-à-dire si, dans sa décomposition en facteurs premiers, y n'a que des facteurs premiers congrus à 1 modulo 4.*

Démonstration. On a vu que y s'écrit sous la forme $b^2 + c^2$ ce qui donne la première assertion. La seconde est classique, voir par exemple [DP] Ch. 2. On trouvera des précisions sur cette question au §4.

2.8 *Exemple.* Considérons l'exemple $y = 1105 = 5 \times 13 \times 17$. Il admet quatre écritures sous forme de somme de deux carrés $b^2 + c^2$ avec pour c, b : $4, 33$; $9, 32$; $12, 31$; $23, 24$. Les trois premières relèvent du cas $x = b^2 - 2bc - c^2$ et la dernière du cas $x = -b^2 + 2bc + c^2$ et on trouve les solutions (x, z), dans l'ordre : $809, 1337$; $367, 1519$; $73, 1561$ et $1057, 1151$.

3 La paramétrisation du cercle

L'approche élémentaire a déjà donné nombre de résultats sur le problème (♯). Nous étudions maintenant d'autres voies, un peu plus élaborées. On va retrouver notamment le théorème 2.5.

3.1 Conique ou cercle

L'équation diophantienne qui apparaît dans (♯) est $2y^2 - x^2 - z^2 = 0$. C'est l'équation d'une conique projective propre Γ. On en connaît plusieurs points rationnels, par exemple $m_0 = (1, 1, 1)$. Une méthode bien connue pour trouver les autres consiste à couper par une droite rationnelle passant par un tel point. Il y a plusieurs façons de faire ce calcul selon le choix de la droite à l'infini. En se plaçant dans le plan affine $z = 1$ on a la conique $2y^2 - x^2 - 1 = 0$, qui est une hyperbole. Cependant il est sans doute plus simple, surtout pour des lycéens, de considérer le plan affine $y = 1$ car on obtient le cercle $x^2 + z^2 = 2$.

3.2 Paramétrisation du cercle

On considère le cercle Γ d'équation $x^2 + z^2 = 2$ dans le plan affine. On dispose des points $x = \pm 1, z = \pm 1$ de Γ. On choisit le point [3] $(-1, -1)$ et on coupe Γ par une droite passant par ce point, d'équation $z + 1 = t(x + 1)$. Elle recoupe le cercle en le point de coordonnées $x = \dfrac{-t^2 + 2t + 1}{1 + t^2}$ et $z = \dfrac{t^2 + 2t - 1}{1 + t^2}$. En posant $t = \dfrac{p}{q}$ avec p, q entiers, et en chassant les

3. Pour avoir des droites de pentes positives.

dénominateurs, on vérifie qu'on obtient des [4] solutions de l'équation initiale :

$$x = -p^2 + 2pq + q^2,\ y = p^2 + q^2,\ z = p^2 + 2pq - q^2.$$

Cette méthode redonne le théorème 2.5 :

3.1 Théorème. *Toute solution $x, y, z \in \mathbf{N}^*$ de l'équation diophantienne $x^2 - 2y^2 + z^2 = 0$, avec $x < y < z$ deux à deux premiers entre eux, s'écrit sous l'une des formes suivantes* [5] *:*

$$(*) \qquad x = -p^2 + 2pq + q^2,\ y = p^2 + q^2,\ z = p^2 + 2pq - q^2 \text{ ou}$$

$$(**) \qquad x = -p^2 + 2pq + q^2,\ y = p^2 + q^2,\ z = -p^2 - 2pq + q^2,$$

avec $p \in \mathbf{Z}$ et $q \in \mathbf{N}^*$ premiers entre eux et de parités différentes vérifiant $1 < \frac{p}{q} < 1 + \sqrt{2} \sim 2.414$ dans le cas $(*)$ (resp. $1 - \sqrt{2} \sim -0.414 < \frac{p}{q} < 0$ dans le cas $(**)$).

Les écritures précédentes sont uniques. Si l'on a [6] *$x + z \equiv 0 \pmod 4$, on est dans le cas $(*)$ et on a la formule $\frac{p}{q} = \frac{y+z}{x+y}$, si l'on a $x+z \equiv 2 \pmod 4$ on est dans le cas $(**)$ et on a $\frac{p}{q} = \frac{x-z}{x+2y+z}$.*

3.2 *Remarque.* Ce résultat est exactement le même que 2.5 *mutatis mutandis.* Pour obtenir la deuxième forme des solutions il suffit de poser $c = -p$ et $b = q$. J'ai laissé l'énoncé sous cette forme, plutôt plus compliquée que 2.5 parce que c'est le premier que j'ai trouvé [7], mais le lecteur garde le droit de penser que l'autre est bien meilleur.

Démonstration. 1) Le calcul précédent montre que les x, y, z de $(*)$ comme ceux de $(**)$ vérifient l'équation $x^2 + z^2 = 2y^2$.

Pour voir qu'ils sont deux à deux premiers entre eux, il suffit de voir qu'ils le sont dans leur ensemble en vertu de 1.1.3. Mais, si un nombre premier l divise x, y, z il divise $x \pm z = 4pq$ donc c'est soit 2 soit un diviseur de p ou de q. Comme p, q sont de parités différentes, $y = p^2 + q^2$ est impair ce qui exclut le cas $l = 2$. Si l divise p ou q il divise les deux, comme on le voit en considérant y, et c'est absurde.

4. Attention, il y a une subtilité : toutes les solutions ne sont pas exactement de cette forme.

5. Avec les mêmes x, y mais des z opposés.

6. Rappelons que x et z sont impairs.

7. Les voies de la découverte sont impénétrables.

Enfin, les inégalités imposées montrent que x, y, z sont positifs comme on le voit en divisant par q^2 et en étudiant les trinômes du second degré. Elles montrent aussi qu'on a $x^2 < y^2$ (l'inégalité est équivalente à $p^3 > pq^2$ et elle vaut à la fois si $p > 1$ et si $-1 < p < 0$). On en déduit $y^2 < z^2$ avec l'équation diophantienne.

2) Inversement, soit x, y, z une solution entière de l'équation avec $0 < x < y < z$ et x, y, z premiers entre eux. On pose $X = \dfrac{x}{y}$ et $Z = \dfrac{z}{y}$, de sorte qu'on a $X^2 + Z^2 = 2$, puis on pose $t = \dfrac{Z+1}{X+1}$ (X est positif) et le calcul ci-dessus montre qu'on a $X = \dfrac{x}{y} = \dfrac{-t^2+2t+1}{1+t^2}$ et $Z = \dfrac{z}{y} = \dfrac{t^2+2t-1}{1+t^2}$. Comme t est un rationnel positif, on peut l'écrire $t = \dfrac{p}{q}$ avec $p, q \in \mathbf{N}^*$ et p, q premiers entre eux. On a les égalités

$$x(p^2+q^2) = y(-p^2+2pq+q^2) \text{ et } z(p^2+q^2) = y(p^2+2pq-q^2).$$

Comme p, q sont premiers entre eux, on voit que le seul facteur premier commun possible entre $y_1 := p^2+q^2$ et $x_1 := -p^2+2pq+q^2$ ou $z_1 := p^2+2pq-q^2$ est le facteur 2, ce qui advient si p et q sont impairs [8].

Supposons d'abord que ce ne soit pas le cas. On voit alors que p^2+q^2 divise y et que y divise p^2+q^2. Comme ils sont positifs, ils sont égaux et on a les égalités annoncées.

Supposons maintenant p et q impairs, $p = 2p'-1$, $q = 2q'+1$. Dans ce cas les nombres x_1, y_1 et z_1 sont tous pairs et on note $x_1 = 2x_2$, $y_1 = 2y_2$ et $z_1 = 2z_2$. On pose alors $P = q'-p'+1$ et $Q = p'+q'$ et on vérifie par un calcul sans malice qu'on a $x_2 = -P^2+2PQ+Q^2$, $y_2 = P^2+Q^2$ et $z_2 = -(P^2+2PQ-Q^2)$. Comme on avait $xy_1 = yx_1$ et $zy_1 = yz_1$, on a aussi $xy_2 = yx_2$ et $zy_2 = yz_2$ mais cette fois on a le lemme suivant :

3.3 Lemme. *Les entiers x_2 et y_2 sont premiers entre eux.*

Démonstration. D'abord, comme x_1 et y_1 n'ont pas de facteur premier commun autre que 2, il en est de même de x_2 et y_2. Pour 2, on note que P et Q ne sont pas de même parité (car $P+Q = 2q'+1$ est impair), donc $y_2 = P^2+Q^2$ est impair.

En appliquant le théorème de Gauss, comme y et y_2 sont positifs, on en déduit $y = y_2$, puis $x = x_2$, et enfin $z = z_2$ et on a obtenu les expressions annoncées, avec le signe $-$ pour z.

8. C'est la petite subtilité promise.

Les formules donnant p/q sont immédiates dans les deux cas et les inégalités annoncées s'obtiennent en étudiant les divers trinômes du second degré.

Dans le cas $(*)$ on a $x+z=4pq\equiv 0 \pmod 4$ tandis que dans le cas $(**)$ on a $x+z=2(p^2+q^2)\equiv 2 \pmod 4$ (car p,q sont de parités distinctes).

3.4 *Exemples.* 1) Voici un exemple du cas $(*)$: $(x,y,z)=(1,5,7)$ donne $p=2, q=1$.

2) Voici un exemple du cas $(**)$: $(x,y,z)=(7,17,23)$ donne $p=-1$, $q=4$.

3.5 *Remarque.* Voici ce qui se passe aux points frontières des domaines régissant l'ordre de x,y,z. Les cas $\dfrac{p}{q}=1-\sqrt{2}$ ou $1+\sqrt{2}$ sont impossibles car p/q est rationnel. Le cas $p=0$ impose $q=1$ (sinon il y a un facteur commun) et il donne le point $x=y=z=1$ qui a été écarté. Le cas $\dfrac{p}{q}=1$ donne $p=q=1$ et il est à rejeter car p et q sont de même parité.

3.3 Applications au problème initial

3.6 Corollaire. *Il y a une infinité de triplets $x<y<z$ d'entiers positifs premiers entre eux qui vérifient $2y^2=x^2+z^2$.*

Démonstration. On choisit un entier q premier impair avec $q\geq 5$. On va montrer qu'on peut trouver un entier convenable p dans l'intervalle ouvert $]q, 2.414\,q[$ ce qui prouvera le corollaire puisqu'il y a une infinité de nombres premiers. Il y a au moins 7 entiers dans cet intervalle. Il faut que p soit premier avec q, ce qui élimine le nombre $2q$, et qu'il soit pair. Il y a au moins trois nombres pairs dans l'intervalle dont deux sont différents de $2q$. On en choisit un comme p.

3.7 *Exemple.* Avec $q=5$, les entiers de l'intervalle sont $6,7,8,9,10,11,12$. On élimine 7, 9 et 11 pour la raison de parité et 10 qui n'est pas premier à q. Il reste $p=6$ ou $p=8$ ou $p=12$ qui donnent respectivement pour (x,y,z), $(49,61,71)$, $(41,89,119)$ et $(1,169,239)$.

4 Les solutions avec y donné

Le théorème précédent décrit toutes les solutions de l'équation $x^2+z^2=2y^2$. Il reste à préciser s'il y a de telles solutions pour x,y ou z donnés. On commence par le cas de y. Il s'agit d'écrire $2y^2$ sous la forme x^2+z^2. Bien entendu on a une solution triviale en prenant $x=z=y$, mais elle est clairement non pertinente.

4.1 La méthode *via* $\mathbf{Z}[i]$

4.1.1 Existence

Le résultat qui nous intéresse est le suivant :

4.1 Proposition. *Soit $y \in \mathbf{N}^*$. L'équation en x, z : $x^2 + z^2 = 2y^2$ admet des solutions x, z entières telles que x, z, y soient premiers entre eux si et seulement si l'entier y n'a, dans sa décomposition en produit de facteurs premiers, que des facteurs congrus à 1 modulo 4.*

Démonstration. 1) Supposons qu'on a $x^2 + z^2 = 2y^2$ avec x, y, z premiers entre eux. On a vu ci-dessus en 1.1.3 que y est impair. On a vu aussi en 3.1 que y est somme de deux carrés premiers entre eux, ce qui donne le résultat (voir [DP] Ch.2). On peut retrouver ce point directement. Supposons que y admette un facteur premier $\equiv -1 \pmod 4$. Ce nombre p divise $x^2 + z^2 = (x+iz)(x-iz) := w\overline{w}$. Dans $\mathbf{Z}[i]$, le p en question est premier (*loc. cit.*) donc il divise w ou $\overline{w}$, donc les deux puisqu'il est réel. Il divise donc $w + \overline{w} = 2x$ et $w - \overline{w} = 2z$ donc x et z, puisque y est impair, et c'est absurde.

2) Réciproquement, si y n'a que des facteurs premiers $\equiv 1 \pmod 4$, $y = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, chacun d'eux s'écrit $p_k = w_k\overline{w_k}$ et ces deux éléments sont premiers dans $\mathbf{Z}[i]$, cf. *loc. cit.* On pose alors (par exemple, mais il y a beaucoup d'autres solutions, voir ci-dessous) $w = (1+i)\prod_k w_k^{2\alpha_k} := x + iz$. On a $w\overline{w} = 2y^2 = x^2 + z^2$. De plus, x, y, z sont premiers entre eux. En effet, si p est un facteur commun de x, y, z, c'est un des p_j. Cela implique que $\overline{w_j}$ divise x et z donc le produit des w_k dans $\mathbf{Z}[i]$, ce qui est absurde car $\overline{w}_j$ et les w_k sont des éléments premiers distincts.

4.2 Corollaire. *Soit $y = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ un entier dont tous les facteurs premiers sont congrus à 1 modulo 4. Le nombre d'écritures de la forme $2y^2 = x^2 + z^2$ avec x, y, z premiers entre eux et $x < y < z$ est égal à 2^{r-1}.*

Démonstration. Pour chaque k on a le choix entre w_k et $\overline{w_k}$, donc 2^r choix. Mais les choix donnant w et $\overline{w}$ correspondent à $x + iz$ et $z + ix$ et à la même solution $x < y < z$ à permutation près de x, z. Cela divise par deux le nombre de choix possibles.

4.3 *Exemple.* Par exemple, pour $y = 1105 = 5 \times 13 \times 17$ on a 4 solutions : $73, 1561$; $367, 1519$; $809, 1337$ et $1057, 1151$.

4.1.2 Un algorithme

Soit donc y un entier n'ayant que des facteurs premiers congrus à 1 modulo 4. Comment écrire $2y^2 = x^2 + z^2$? La réponse est ci-dessus : on décompose

chaque p_k en somme de deux carrés, on choisit w_k ou $\overline{w_k}$ et on multiplie le produit des carrés par $1+i$.

Traitons l'exemple ci-dessus : $1105 = 5\times 13\times 17$. Les décompositions sont $5 = 1^2+2^2$, $13 = 3^2+2^2$ et $17 = 1^2+4^2$. On peut fixer l'un des facteurs, disons $(1+2i)^2$ et faire varier les autres : $(3\pm 2i)^2$ et $(1\pm 4i)^2$. On obtient : avec $++$, $-1337+809i$, avec $+-$, $73+1561i$, avec $-+$, $-367-1519i$ et avec $--$, $1057-1151i$.

4.4 *Remarque.* Comme on l'a vu en 2.7, on peut retrouver la plupart des résultats précédents grâce au théorème 2.5 ou à sa variante 3.1.

5 L'approche *via* l'anneau $\mathbf{Z}[\sqrt{2}]$

L'étude des solutions avec x ou z donnés est un peu plus délicate. Si l'on fixe x, par exemple, on a à résoudre $z^2-2y^2 = -x^2$ et on reconnaît dans le premier membre de cette équation la norme dans l'anneau $\mathbf{Z}[\sqrt{2}]$. On va donc étudier cet anneau [9].

Rappelons que $A := \mathbf{Z}[\sqrt{2}]$ est l'ensemble des nombres réels de la forme $z = x+y\sqrt{2}$ avec $x, y \in \mathbf{Z}$. C'est un anneau principal, de corps des fractions $\mathbf{Q}(\sqrt{2})$. Il est muni de la conjugaison $\sigma(z) = \overline{z} = x-y\sqrt{2}$ qui est un automorphisme et de la norme $N(z) = z\overline{z} = x^2-2y^2$. La norme est à valeurs entières et multiplicative : $N(zw) = N(z)N(w)$.

5.1 Les inversibles

Le résultat crucial est le suivant :

5.1 Théorème. *1) Les inversibles de A sont les éléments de normes ± 1.*

2) Ce sont exactement les éléments de la forme $\pm(1+\sqrt{2})^n$ avec $n \in \mathbf{Z}$. Pour n impair (resp. pair) ces éléments sont de norme -1 (resp. 1).

3) Posons, pour $n \in \mathbf{N}$, $(1+\sqrt{2})^n = x_n + y_n\sqrt{2}$. On a $x_0 = 1$, $y_0 = 0$ et les relations de récurrence $x_{n+1} = x_n + 2y_n$ et $y_{n+1} = x_n + y_n$.

Démonstration. 1) Il est clair que si z est de norme 1 (resp. -1) il est inversible d'inverse $\overline{z}$ (resp. $-\overline{z}$). Inversement, si l'on a $zw = 1$ on a $N(z)N(w) = 1$ et dans les entiers cela impose $N(z) = \pm 1$.

2) On a $N(1+\sqrt{2}) = 1-2 = -1$, d'où le résultat, sauf le fait que tous les inversibles sont de la forme annoncée. Il suffit de traiter le cas d'un z de

9. Les résultats sont analogues à ceux utilisés sur $\mathbf{Z}[i]$ dans le paragraphe précédent, mais l'anneau $\mathbf{Z}[\sqrt{2}]$ est un peu moins connu que l'anneau des entiers de Gauss et un peu plus compliqué du fait de la présence d'une infinité d'éléments inversibles.

norme -1. Soit donc $z = x + y\sqrt{2}$ avec $N(z) = x^2 - 2y^2 = -1$. On a $x \neq 0$. Quitte à changer de signe, on peut supposer $x > 0$. Si $x = 1$, on a $y = \pm 1$ et z est de la forme voulue car $\sqrt{2} - 1$ est l'inverse de $1 + \sqrt{2}$. S'il existe z qui n'est pas de la forme annoncée, on le choisit avec $x \geq 2$ et x minimum. On note qu'on a $|y| \geq 3$. En effet, $y = 0$ est impossible, $y = \pm 1$ donne $x = 1$ qui a été écarté et $y = \pm 2$ donne $x^2 = 7$, impossible. On considère alors $w = z(3 - 2\sqrt{2})$. Comme $3 - 2\sqrt{2} = (1 - \sqrt{2})^2 = (1 + \sqrt{2})^{-2}$ est de norme 1, w est encore de norme -1 et il s'écrit $w = 3x - 4y + (3y - 2x)\sqrt{2} := X + Y\sqrt{2}$. On a le lemme suivant :

5.2 Lemme. *Sous les hypothèses précédentes, on a $0 < X < x$.*

Démonstration. Si $0 \geq 3x - 4y$ on a $x \leq \frac{4}{3}y$, donc $2y^2 - 1 = x^2 \leq \frac{16}{9}y^2$, d'où $y \leq \frac{3}{\sqrt{2}} \sim 2.12$ et on a vu que c'est impossible. Si $3x - 4y \geq x$ on a $x \geq 2y$ donc $-1 = x^2 - 2y^2 \geq 2y^2$ et c'est absurde.

On peut alors conclure. L'hypothèse de minimalité sur x montre que l'on a $X = 1$, donc $|Y| = 1$ et $w = 1 \pm \sqrt{2}$ est de la forme annoncée, donc aussi $z = w(1 + \sqrt{2})^2$ et c'est absurde.

Le point 3) est immédiat.

5.2 Les entiers de la forme $x^2 - 2y^2$

Nous aurons besoin du lemme suivant :

5.3 Lemme. *1) Un entier $n \in \mathbf{Z}$ est de la forme $n = x^2 - 2y^2$ avec $x, y \in \mathbf{Z}$ si et seulement si c'est la norme d'un élément de $\mathbf{Z}[\sqrt{2}]$. Les entiers de cette forme sont stables par multiplication.*

2) Si n est une norme il en est de même de $-n$.

3) a) Un nombre premier p est une norme de $\mathbf{Z}[\sqrt{2}]$ si et seulement si il est réductible dans cet anneau.

b) Si $p = N(z)$, z est irréductible dans l'anneau A. Si p n'est pas une norme il est irréductible dans A.

Démonstration. La première assertion du point 1) est évidente. La seconde vient de la formule $N(z)N(w) = N(zw)$.

Pour 2), si $n = N(z)$, on a $-n = N(z(1 + \sqrt{2}))$.

3) a) Si p est une norme il est réductible car on a $p = z\overline{z}$ et z n'est pas inversible. Inversement, si l'on a $p = zw$ avec z, w non inversibles, donc de norme $\neq \pm 1$, on a $p^2 = N(z)N(w)$, donc $N(z) = p$ ou $-p$ et on conclut avec 2).

b) Si $N(z) = p$ et si $z = wt$ avec $w, t \in A$ on a $N(z) = p = N(w)N(t)$, de sorte que w ou t est de norme ± 1, donc inversible et z est irréductible.

Si p n'est pas une norme, il est irréductible. En effet, si $p = zw$ on a $p^2 = N(z)N(w)$ et, comme p n'est pas une norme, c'est qu'on a $N(z) = \pm p^2$ et $N(w) = \pm 1$ ou l'inverse et la conclusion en découle.

Pour étudier les nombres de la forme $x^2 - 2y^2$ généraux, introduisons une notion :

5.4 Définition. *Deux écritures d'un entier n comme normes : $n = N(z) = N(w)$ sont dites* **essentiellement équivalentes** *si z/w est dans $\mathbf{Z}[\sqrt{2}]$.*

Le résultat suivant fait un bilan sur les entiers de la forme $x^2 - 2y^2$:

5.5 Théorème. *1) Soit p un nombre premier.*

a) Il s'écrit sous la forme $p = x^2 - 2y^2$ avec $x, y \in \mathbf{N}$ si et seulement si 2 est un carré modulo p (c'est-à-dire si $p = 2$ ou $p \equiv \pm 1 \pmod 8$) ; ces nombres sont les **bons** *nombres premiers, les autres étant les mauvais).*

b) Si $p = 2$, toutes les écritures de la forme $x_n^2 - 2y_n^2 = 2$ sont données par la formule $x_n + y_n\sqrt{2} = \pm(2 + \sqrt{2})(1 + \sqrt{2})^n$ avec $n \in \mathbf{Z}$. Toutes ces écritures sont essentiellement équivalentes.

c) Si p est un bon nombre premier impair, il s'écrit $p = a^2 - 2b^2$ et on choisit une telle écriture avec $a > 0$ minimum. Alors, toutes les écritures de la forme $x_n^2 - 2y_n^2 = p$ sont données par les formules $x_n + y_n\sqrt{2} = \pm(a + b\sqrt{2})(1 + \sqrt{2})^{2n}$ ou $x_n + y_n\sqrt{2} = \pm(a - b\sqrt{2})(1 + \sqrt{2})^{2n}$ avec $n \in \mathbf{Z}$. À équivalence essentielle près, il y a deux écritures de p.

2) Soit $n \in \mathbf{Z}$ un entier quelconque décomposé en produit de facteurs premiers : $n = \epsilon\, p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $\epsilon = \pm 1$.

a) Il s'écrit sous la forme $n = x^2 - 2y^2$ avec $x, y \in \mathbf{N}$ si et seulement si ses mauvais facteurs premiers sont à une puissance paire.

b) Notons $p_1, \ldots, p_s$ les bons nombres premiers impairs intervenant dans la décomposition de n. À équivalence essentielle près, il y $\prod_{i=1}^{s} \alpha_i + 1$ décompositions de n.

Démonstration. 1) a) Si l'on a $p = x^2 - 2y^2$, y n'est pas multiple de p (sinon x le serait aussi et le second membre serait multiple de p^2) et on a, modulo p, $2 \equiv (\frac{x}{y})^2$, donc 2 est un carré. Inversement, si 2 est un carré modulo p, l'anneau $\mathbf{Z}[\sqrt{2}]/(p) \simeq (\mathbf{Z}/p\mathbf{Z})[X]/(X^2 - 2)$ n'est pas intègre, donc p n'est pas premier dans A et, comme A est principal, il est réductible, donc une norme par 5.3, donc de la forme $x^2 - 2y^2$.

b) et c) On écrit $p = z\overline{z}$ avec $z = a + b\sqrt{2}$ et z est premier dans A en vertu de 5.3.3. Si l'on a $p = x^2 - 2y^2 = w\overline{w}$, on voit que z divise w ou $\overline{w}$. Si z divise w on a $w = uz$ et l'égalité des normes montre que u est inversible, donc que z est de la forme annoncée (on n'oubliera pas qu'il faut que n soit

pair sinon on obtient $-p$). Si z divise $\overline{w}$, $\overline{z}$ divise w et on conclut de la même manière. Dans le cas $p = 2$, $z = 2 + \sqrt{2}$ et $\overline{z} = 2 - \sqrt{2}$ sont associés car on a $2 + \sqrt{2} = (2 - \sqrt{2})(3 + 2\sqrt{2}) = (2 - \sqrt{2})(1 + \sqrt{2})^2$.

On note que les décompositions correspondant à $a + b\sqrt{2}$ et $a - b\sqrt{2}$ ne sont pas essentiellement équivalentes (sinon $\dfrac{a + b\sqrt{2}}{a - b\sqrt{2}}$ serait dans $\mathbf{Z}[\sqrt{2}]$, ce qui impliquerait que $p = a^2 - 2b^2$ divise $2ab$ et c'est impossible).

2) a) Il est clair que si les mauvais facteurs sont à une puissance paire l'entier est de la bonne forme. Inversement, supposons qu'il existe $n = N(z)$ avec un mauvais facteur premier p présent à une puissance impaire, choisissons n de sorte que l'exposant de cette puissance soit minimum. Comme on a $n = z\overline{z}$, p, qui est irréductible (donc premier) dans A (cf. 5.3), divise z ou $\overline{z}$, donc les deux et n/p^2 est encore de la bonne forme, ce qui contredit l'hypothèse de minimalité.

b) Le nombre p_i a deux décompositions essentielles distinctes : $p_i = N(z_i) = N(\overline{z}_i)$. Il en résulte que $p_i^{\alpha_i}$ admet les décompositions correspondant à $z_i^{\alpha_i}$, $z_i^{\alpha_i - 1}\overline{z}_i$, ..., $\overline{z}_i^{\alpha_i}$ et on en déduit le résultat.

5.6 *Exemples.* 1) Le nombre 7 s'écrit sous la forme $x^2 - 2y^2$. Il y a une unique écriture avec x minimum, $x = 3$, qui est $7 = 3^2 - 2 \times 1^2$, mais cette écriture est double : $7 = N(3 + \sqrt{2}) = N(3 - \sqrt{2})$ et, à équivalence essentielle près, les autres écritures s'obtiennent à partir de ces deux là en les multipliant par des inversibles de norme 1. Ainsi on a $13 + 9\sqrt{2} = (3 + \sqrt{2})(1 + \sqrt{2})^2 = (3 + \sqrt{2})(3 + 2\sqrt{2})$ et $5 + 3\sqrt{2} = (3 - \sqrt{2})(1 + \sqrt{2})^2 = (3 - \sqrt{2})(3 + 2\sqrt{2})$.

2) Il y a trois décompositions essentielles du nombre 49. On les obtient à partir des nombres $z = 3 + \sqrt{2}$ et $\overline{z}$, ce sont $49 = N(z^2) = N(11 + 6\sqrt{2})$, $49 = N(\overline{z}^2) = N(11 - 6\sqrt{2})$ et $49 = N(z\overline{z}) = N(7)$. Toutes les autres décompositions sont de la forme $N(z^2u)$ ou $N(\overline{z}^2u)$ ou $N(7u)$ avec u inversible de norme 1.

5.7 *Remarque.* Attention, les décompositions $n = x^2 - 2y^2$ fournies par la procédure précédente ne sont peut-être pas celles qui ont les plus petits x, y. Ainsi, pour $n = 49$ on trouve $11 + 6\epsilon\sqrt{2}$ avec $\epsilon = \pm 1$, mais il y a des solutions plus petites : $9 + 4\epsilon\sqrt{2} = (11 - 6\epsilon\sqrt{2})(3 + 2\epsilon\sqrt{2})$.

5.3 Retour au problème initial

Il s'agit maintenant, x étant donné, d'écrire x^2 sous la forme $x^2 = 2y^2 - z^2$. Il y a bien entendu une solution triviale qui consiste à prendre $y = z = x$, solution non pertinente puisque x, y, z ne sont ni premiers entre eux (ni même distincts). Une solution un peu moins triviale est de partir de la formule

$1 = 3^2 - 2 \times 2^2$ et de multiplier par x^2 : $x^2 = (3x)^2 - 2(2x)^2$, solution inintéressante aussi, pour la même raison. Voici le résultat pertinent :

5.8 Corollaire. *Soit x un entier. L'équation $2y^2 - z^2 = x^2$ admet des solutions entières avec $0 < x < y < z$ premiers entre eux si et seulement si x est impair et n'a que de bons facteurs premiers (i.e. $\equiv \pm 1 \pmod 8$).*

Démonstration. Si l'on a $x^2 = 2y^2 - z^2$ avec x pair, z est pair et y aussi ce qui est absurde. La condition signifie que $-x^2$ est une norme, donc aussi x^2. On a donc $x^2 = N(z+y\sqrt{2}) := N(w)$. Supposons que x admette un mauvais facteur premier p. On sait qu'il est premier dans $\mathbf{Z}[\sqrt{2}]$ donc il divise w ou $\overline{w}$, donc z et y et c'est absurde.

Inversement, supposons que x n'a que de bons facteurs premiers : $x = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. On décompose chacun des facteurs en $p_k = w_k\overline{w_k}$ et on pose $w_0 = \prod_{k=1}^{r} w_k^{2\alpha_k} = z_0 + y_0\sqrt{2}$. On a $N(w) = \prod_k N(w_k)^{2\alpha_k} = z_0^2 - 2y_0^2 = x^2$. Quitte à changer w_0 en $\overline{w_0}$ ou $-w_0$ ou $-\overline{w_0}$ (ce qui change éventuellement les w_k de la même manière), on peut supposer que y_0 et z_0 sont positifs et on a alors $x < z_0$ et $y_0 < z_0$. On pose $w = (1+\sqrt{2})w_0 := z + y\sqrt{2}$, ce qui, comme on a $N(1+\sqrt{2}) = -1$, donne la relation voulue : $x^2 + z^2 = 2y^2$. On a $z = z_0 + 2y_0 > z_0 > x$ et, comme y, z sont positifs, on en déduit $x < y < z$. Si l'on suppose qu'un nombre premier p divise x, y et z, c'est l'un des p_k, de sorte que w_k et $\overline{w_k}$ divisent w, mais comme les $w_k, \overline{w_k}$ sont des irréductibles distincts, c'est impossible.

5.9 Corollaire. *Soit x un entier positif impair qui n'a que de bons facteurs premiers. Il existe une infinité d'entiers y et z tels que l'on ait $x^2 + z^2 = 2y^2$ avec $x < y < z$ premiers entre eux.*

Démonstration. On a vu dans la preuve de 5.8 qu'il existe y_0, z_0 vérifiant $x^2 = z_0^2 - 2y_0^2$ et il suffit de considérer les entiers y_n, z_n définis par $(z_0 + y_0\sqrt{2})(1+\sqrt{2})^{2n+1} = z_n + y_n\sqrt{2}$. Les relations de récurrence $z_{n+1} = z_n + 2y_n$ et $y_{n+1} = z_n + y_n$ assurent qu'on a les conditions d'ordre et de primalité.

5.10 *Exemples.* 1) Si l'on prend $x = 1$, on a la solution banale $1^2 = 1^2 - 2\times 0^2$ qui correspond à $w_0 = 1$ et on obtient une infinité de solutions en prenant les $w_n = (1+\sqrt{2})^{2n+1}$. On a ainsi, successivement, les solutions $(y, z) = (5, 7)$ puis $(29, 41)$, puis $(169, 239)$, $(985, 1393)$, $(5741, 8119)$, etc.

2) Avec $x = 7$ on part de la relation vue ci-dessus : $49 = N(11 + 6\sqrt{2}) = 11^2 - 2 \times 6^2$ et on pose $w = (1+\sqrt{2})(11 + 6\sqrt{2}) = 23 + 17\sqrt{2}$. On obtient la solution $(y, z) = (17, 23)$ et en multipliant par les puissances de $1 + \sqrt{2}$ on en a une infinité : $(97, 137)$, $(565, 799)$, $(3293, 4657)$, etc.

5.11 *Remarque.* Dans la question de trouver des triades, le résultat est très différent selon que l'on impose le premier terme x^2 (on a alors une infinité de solutions dès qu'on en a une) ou les autres y^2, z^2 où l'on n'a qu'un nombre fini de solutions.

5.12 *Remarque.* Les entiers qui n'ont que des facteurs premiers congrus à 1 modulo 8 (comme 17, 41, 73, 89, etc.) sont en quelque sorte universels : ils interviennent dans les triades dans les trois positions x, y et z. Ainsi, avec $697 = 17 \times 41$ on a les solutions : $z = 697$ avec $329^2 + 697^2 = 2 \times 545^2$, $y = 697$ avec $487^2 + 857^2 = 2 \times 697^2$ et enfin $x = 697$ avec $697^2 + 1127^2 = 2 \times 937^2$.

Références

[DP] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.