Corrigé DM2

Quelques équations diophantiennes

Exercice 1. *Etudiez les solutions entières de l'équation* $(x^2-9)(x^2-16)=y^2$.
On pensera bien évidemment à factoriser le plus possible et à utiliser l'exercice (??)

Preuve: On va utiliser l'exercice (**??**). On est donc amené à introduire "le" pgcd δ de (x^2-9) et (x^2-16); celui-ci divise $(x^2-9)-(x^2-16)=7$, soit $\delta=1,7$.

Supposons $\delta=1$: d'après loc. cit., on en déduit que $x^2-9=\epsilon t^2$ et $x^2-9=\epsilon s^2$ avec $\epsilon=\pm1$ et $t,s\geqslant 0$ premiers entre eux. On obtient alors $7=\epsilon(t^2-s^2)=\epsilon(t-s)(t+s)$ d'où $t+s=7$ et $t-s=\epsilon$. Si $\epsilon=1$, on a $t=4$ et $s=3$ ce qui donne $x=\pm5$ et $y=\pm12$. Si $\epsilon=-1$ alors $t=3$ et $s=4$ ce qui donne $x=0$ et $y=\pm12$.
Remarque: Il nous faut bien sûr vérifier à chaque fois que les solutions obtenues conviennent, car on a simplement raisonné par implication.

Supposons $\delta=7$: $x^2-9=7u$, $x^2-16=7v$ et $y^2=7^2uv$ avec u et v premiers entre eux. On a alors $uv=(y/7)^2$ et l'exercice (**??**) donne $u=\epsilon t^2$ et $v=\epsilon s^2$ avec $\epsilon=\pm1$ et $s,t\geqslant 0$ premiers entre eux. On trouve alors les solutions $x=\pm3,4$ et $y=0$, qui conviennent.

□

Exercice 2. *On considère l'équation* $y^2=x^3+7$*:*

(i) Montrez qu'il n'y a pas de solutions avec x pair;

(ii) En écrivant l'équation sous la forme $y^2+1=x^3+8=(x+2)(x^2-2x+4)$ et en utilisant l'exercice 1 b, déduisez en qu'il n'existe pas de solutions entières.

Preuve: (i) Si x est pair, on a $y^2\equiv -1 \bmod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2=1+4k(k+1)\equiv 1 \bmod 8$ contradiction.

(ii) On a $x^3+8=(x+2)(x^2-2x+4)$ avec x impair de la forme $2k+1$; $(x^2-2x+4)=4k^2+3$. On en déduit donc qu'il existe un p premier divisant x^2-2x+4 avec $p\equiv 3 \bmod 4$. Or d'après l'exercice (**??**), si p premier divise y^2+1 alors $p\equiv 1 \bmod 4$, d'où la contradiction.

□

Exercice 3. *On cherche les solutions entières de l'équation* $x^2+y^2=z^2$ *avec* $(x,y,z)=1$*:*

(i) Montrez que z et y (ou x) sont impairs;

(ii) Montrez que $(z-y,z+y)=2$;

(iii) Déduisez en que les solutions sont paramétrées par u et v avec $u\not\equiv v \bmod 2$, $(u,v)=1$ et $x=2uv$, $z=u^2+v^2$ et $y=|u^2-v^2|$.

Preuve: (i) Si x et y sont impairs alors x^2 et y^2 sont congrus à 1 modulo 4 et donc $z^2\equiv 2 \bmod 4$. Or les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1. Supposons donc x pair; si y était pair alors z aussi ce qui n'est pas car $(x,y,z)=1$.

(ii) Evidemment 2 divise le pgcd δ de $(z-y)$ et $(z+y)$. En outre $\delta=(z-y,2y)=2(z-y,y)$ car $z-y$ est pair; $\delta=2(z,y)=2$.

(iii) On écrit $x^2 = 4a^2 = (z-y)(z+y) = 4ts$ avec t et s premiers entre eux et $z-y = 2t$, $z+y = 2s$. D'après l'exercice (**??**), on a $s = u^2$ et $t = v^2$ (on remarquera que l'on recherche essentiellement les solutions avec $x, y, z \geqslant 0$ et $z \geqslant y$); d'où le résultat.

□

Exercice 4. *Soit $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \ / \ (a,b) \in \mathbb{Z}^2\}$. On définit pour $z = a + ib\sqrt{2} \in A$, $N(z) = a^2 + 2b^2$.*

(a) Montrez que B est euclidien et donc factoriel.

(b) Soient $(x,y) \in \mathbb{Z}^2$, vérifiant l'équation $y^2+2 = x^3$. Montrez que x est impair puis que dans B, $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux. En déduire qu'il existe $(a,b) \in \mathbb{Z}^2$ tels que $x = a^2 + 2b^2$ et $y + i\sqrt{2} = (a + ib\sqrt{2})^3$, puis décrire les solutions de l'équation précédente.

(c) Etudier comme dans l'exercice précédent l'ensemble $S = \{n \in \mathbb{N} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 + 2y^2\}$.
Indication: on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1, 3 \bmod 8$.

(d) Etudier de même l'ensemble $\{n \in \mathbb{Z} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.

Preuve: (a) On raisonne comme dans l'exercice précédent; soit $N(a+ib\sqrt{2}) = a^2+2b^2$ la norme qui est une fonction multiplicative, et soit $z \in A^\times$; on a $zz' = 1$ soit $N(z)N(z') = 1$ et donc $N(z) = 1$, soit $z = \pm 1$.
Pour montrer que A est euclidien, on remarque à nouveau que z_1/z_2 peut s'écrire sous la forme $q + e$ avec $q \in A$ et $e \in \mathbb{C}$ de norme strictement plus petite que 1. Ainsi on a $z_1 = qz_2 + r$, avec $r = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$.

(b) Si x est pair, on a $y^2 \equiv -2 \bmod 8$, ce qui ne se peut pas, car les carrés dans $\mathbb{Z}/8\mathbb{Z}$, sont $0, 1, 4$. On factorise ensuite dans A: $x^3 = (y + i\sqrt{2})(y - i\sqrt{2})$ et soit δ un pgcd de $y + i\sqrt{2}$ et $y - i\sqrt{2}$; on a $\delta = (y + i\sqrt{2}, (i\sqrt{2})^3)$, or $i\sqrt{2}$ est irréductible car de norme 2, et la seule factorisation de 2 est 1×2, de sorte que $i\sqrt{2} = zz'$ implique que $N(z) = 1$ soit z inversible (ou z'). Or $i\sqrt{2}$ ne divise pas y car sinon y^2 serait pair et donc y pair soit x pair, ce qui n'est pas; ainsi $\delta = 1$. On en déduit donc que $(y \pm i\sqrt{2})$ sont des cubes parfaits: $(y \pm i\sqrt{2}) = (a \pm i\sqrt{2})^3$ et $x = a^2 + 2b^2$. En séparant partie réelle et imaginaire, on trouve alors $y = a^3 - 6ab^2$ et $1 = b(3a^2 - 2b^2)$ soit $b = \epsilon = \pm 1 = 3a^2 - 2$, ce qui donne $b = 1$ et $a = \pm 1$ soit $y = \pm 5$ et $x = 3$ qui est bien une solution de l'équation.

(c) On a à nouveau $n \in S$ si et seulement si il existe $z \in A$ tel que $n = N(z)$. On étudie à nouveau les irréductibles de B; p est irréductible si et seulement si $A/(p)$ est intègre, i.e. $X^2 + 2$ n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si -2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $p \equiv 5, 7 \bmod 8$. En raisonnant comme dans l'exercice précédent, on trouve que les irréductibles de A, outre les premiers $p \equiv 5, 7 \bmod 8$, sont les $z \in A$ tels que $N(z)$ est premier. Toujours en suivant la même démarche, on trouve alors que $n \in S$ si et seulement si $v_p(n)$ est pair pour $p \equiv 5, 7 \bmod 8$.

(d) De la même façon, la détermination de S se fait via l'étude de $A = \mathbb{Z}[\sqrt{2}]$, dont la norme est $a^2 - 2b^2$, avec le morphisme de corps $c(a + b\sqrt{2}) = a - \sqrt{2}b$ de sorte que N est multiplicative. Soit $z \in A^\times$, on a alors $N(z) = \pm 1$. A nouveau A est euclidien pour le stathme $|N|$. On remarque que -1 est une norme $-1 = 1^2 - 2 \times 1^2 = N(1 + \sqrt{2})$. Si n est un diviseur de $x^2 - 2y^2$ avec x, y premiers entre eux, alors au signe près n est de la forme $u^2 - 2v^2$. En effet soit $x + \sqrt{2}y = \pi_1 \cdots \pi_r$ une décomposition en produit d'irréductibles; aucun des π_i n'appartient

à $\mathbb{Z}$ car x et y sont premiers entre eux, de sorte que comme précédemment les $N(\pi_i)$ sont des premiers de $\mathbb{Z}$; on a alors $x^2 - 2y^2 = N(\pi_1)\cdots N(\pi_r)$ et n au signe près, est un produit de certains de ces $N(\pi_i)$ et donc n est de la forme $N(z) = u^2 - 2v^2$.
L'égalité $-(u^2 - 2v^2) = N((1+\sqrt{2})(u+v\sqrt{2})) = (u+2v)^2 - 2(u+v)^2$ permet de négliger le signe $\pm$. Ainsi un premier impair p est de la forme $x^2 - 2y^2$ si et seulement si 2 est un carré modulo p ce qui est équivalent à $p \equiv \pm \bmod 8$.

□

Exercice 5. *Etude de l'équation de Pell-Fermat: $x^2 - Ny^2 = 1$.*

(i) Traitez le cas $N \leqslant 0$.

(ii) Montrez que dans le cas où N est un carré parfait, les solutions triviales $x = \pm 1, y = 0$ sont les seules.

(iii) On suppose donc $N > 1$ et N n'est pas un carré parfait. En utilisant l'anneau $\mathbb{Z}[\sqrt{N}]$, montrez l'égalité:

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

En déduire que s'il existe un solution non triviale (x_0, y_0) à l'équation de Pell-Fermat, alors il en existe une infinité (x_n, y_n) définie par récurrence:

$$\begin{cases} x_{n+1} = x_0x_n + Ny_0y_n \\ y_{n+1} = x_0y_n + x_ny_0 \end{cases}$$

Calculez par exemple pour $N = 2$, les 3 premiers termes de cette suite en remarquant que $(3, 2)$ est solution.

(iv) Montrez que pour (x_1, y_1) et (x_2, y_2) des solutions positives de l'équation, les équivalences

$$x_1 < x_2 \Leftrightarrow y_1 < y_2 \Leftrightarrow (x_1 + y_1\sqrt{N}) < (x_2 + y_2\sqrt{N})$$

En déduire que s'il existe des solutions non triviales alors il existe une solution minimale (x_0, y_0) pour une relation d'ordre que l'on définira. Montrez ensuite que l'ensemble des solutions sont les (x_n, y_n) définis ci-dessus.

(v) On veut montrer l'existence d'une solution non triviale. Montrez qu'il existe une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$.

Indication: commencez par remarquer que p ou $p-1$ est la partie entière de $q\sqrt{N}$, puis appliquez le principe des chaussettes et des tiroirs ($n+1$ chaussettes rangées dans n tiroir, implique qu'un tiroir contient au moins deux chaussettes), où les chaussettes sont les $n\sqrt{N} - [n\sqrt{N}]$ pour $0 \leqslant n \leqslant q$ et les tiroirs sont les intervalles $[k/q, (k+1) : q]$ pour $0 \leqslant k < q$.

En déduire qu'il existe une infinité de couples $(p, q) \in \mathbb{N}^2$ premiers entre eux tels que $-1 - 2\sqrt{N} < p^2 - Nq^2 < 1 + 2\sqrt{N}$. En utilisant à nouveau le principe des tiroirs, montrez qu'il existe un entier $l < 1 + 2\sqrt{N}$, $p_1 \equiv p_2 \bmod l$, $q_1 \equiv q_2 \bmod l$ tels que $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = \pm l$, et en déduire l'existence d'une solution non triviale.

Preuve: Evidemment, on se limite à chercher les solutions $x, y \geqslant 0$.

(i) Pour $N \leqslant -2$, les seules solutions sont clairement $x = 1$ et $y = 0$; pour $N = -1$, on obtient $(x, y) = (1, 0)$ ou $(0, 1)$.

(ii) Soit $N = d^2$; $x^2 - d^2y^2 = (x - dy)(x + dy) = 1$, soit $x + dy = 1 = x - dy$, d'où $x = 1$ et $y = 0$.

(iii) Soit $A = \mathbb{Z}[\sqrt{N}]$ et $N(a + b\sqrt{N}) = a^2 - Nb^2 = (a + b\sqrt{N})(a - b\sqrt{N})$. L'application N est multiplicative, d'où $N((a + b\sqrt{N})(c + d\sqrt{N})) = N(a + b\sqrt{N})N(c + d\sqrt{N})$ ce qui donne l'identité remarquable de l'énoncé.

Avec ces notations (x, y) est solution si et seulement si $N(x+y\sqrt{N}) = 1$, ainsi si (x_0, y_0) est solution alors (x_n, y_n) tel que $x_n + y_n\sqrt{N} = (x_0 + y_0\sqrt{N})^n$, est solution, ce qui donne la relation de récurrence de l'énoncé. On remarque simplement que la suite (x_n, y_n) prend une infinité de valeur car la solution (x_0, y_0) étant non triviale, $x_0 \geqslant 2$ et $y_0 \geqslant 1$ ce qui implique $x_{n+1} > x_n$ et $y_{n+1} > y_n$.

Avec $N = 2$ et $(x_0, y_0) = (3, 2)$, on obtient les premiers termes de la suite (x_n, y_n): $(17, 12)$, $(99, 70)$, $(577, 408)$.

(iv) Soient (x_1, y_1) et (x_2, y_2) des solutions positives; on a alors les équivalences:

$$x_1 < x_2 \Leftrightarrow x_1^2 < x_2^2 \Leftrightarrow 1 + Ny_1^2 < 1 + Ny_2^2 \Leftrightarrow y_1 < y_2 \Leftrightarrow x_1 + y_1\sqrt{N} < x_2 + y_2\sqrt{N}$$

On choisit alors la relation d'ordre suivante sur les solutions positives: $(x_1, y_1) \leqslant (x_2, y_2)$ si et seulement si $x_1 \leqslant x_2$. Parmi les solutions positives non triviales, soit donc (x_0, y_0) la solution minimale dont l'existence découle du fait que $\mathbb{N}$ est discret.

Soit alors (x, y) une solution (positive) et $n \geqslant 0$ tel que $x_n \leqslant x < x_{n+1}$; on a alors $y_n \leqslant y < y_{n+1}$ et donc $1 \leqslant \frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}} < x_0 + y_0\sqrt{N}$. Or $\frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}}$ est égal à $X + Y\sqrt{N}$ avec $X = xx_n - Nyy_n$ et $Y = yx_n - xy_n$ avec $X^2 - NY^2 = 1$. En outre, on a $X \geqslant 0$ car $x \geqslant y \geqslant 0$ et $x_n \geqslant y_n \geqslant 0$; de même $Y \geqslant 0$ car sinon $X + Y\sqrt{N} = \frac{1}{X+\sqrt{X^2+1}} < 1$ ce qui n'est pas. Ainsi (X, Y) est une solution positive et $X + Y\sqrt{N} < x_0 + y_0\sqrt{N}$ ce qui contredit la minimalité de (x_0, y_0).

(v) Commençons par montrer l'existence d'une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$, soit $-1/q < q\sqrt{N} - p < 1/q$ et donc soit $p = [q\sqrt{N}]$ soit $p = [q\sqrt{N}] + 1$. On raisonne par l'absurde, en supposant la finitude de l'ensemble E de ces rationnels. Soit alors $\epsilon = \min_{p/q \in E} |\sqrt{N} - p/q|$. Comme $\sqrt{N} \notin \mathbb{Q}$, on a $\epsilon > 0$. Soit donc $q_0 > 0$ tel que $1/q_0 < \epsilon$, on va montrer qu'il existe $q \leqslant q_0$ et p tel que $|\sqrt{N} - p/q| < 1/qq_0 \leqslant 1/q^2$ ce qui est en contradiction avec le fait que l'on devrait avoir $|\sqrt{N} - p/q| \geqslant \epsilon$. Considérons donc les q_0-tiroirs $[k/q_0, (k+1)/q_0]$ pour $k = 0, \cdots, q_0 - 1$, et les chaussettes $|q\sqrt{N} - [q\sqrt{N}]|$ pour $n = 1, \cdots, q_0$. Si une chaussette est dans le premier tiroir, c'est gagné. Plaçons-nous dans la situation contraire et soient $q_1 \neq q_2$ deux chaussettes dans le même tiroir, soit $|(q_1 - q_2)\sqrt{N} - [q_1\sqrt{N}] + [q_2\sqrt{N}]| < 1/q_0$. Ainsi en posant $q = |q_1 - q_2|$ et $p = [q_1\sqrt{N}] - [q_2\sqrt{N}]$, on a bien $|a\sqrt{N} - p| < 1/q_0$, d'où le résultat.

Des inégalités $-1/q^2 < \sqrt{N} - p/q < 1/q^2$ avec $p, q > 0$, on obtient $-1/q < q\sqrt{N} - p < 1/q$, soit $0 < p + q\sqrt{N} < 1 : q + 2q\sqrt{N}$ soit $-1 - 2\sqrt{N} < p^2 - Nq^2 < 1 + 2\sqrt{N}$. On obtient de la sorte une infinité de couples (p, q) avec p et q premiers entre eux, et $p^2 - Nq^2$ appartenant à l'intervalle $[-1 - 2\sqrt{N}, 1 + 2\sqrt{N}]$ dans lequel il y a un nombre fini d'entiers (de tiroirs). Selon le principe des tiroirs, il existe un entier l de l'intervalle précédent tel qu'il existe une infinité de couples (p, q) (les chaussettes) avec p et q premiers entre eux, tels que $p^2 - Nq^2 = l$. Comme ${}^s qrtN \notin \mathbb{Q}$, l n'est pas nul; si $l = \pm 1$ c'est gagné, sinon les nouveaux tiroirs sont les éléments de $\mathbb{Z}/l\mathbb{Z}$ et on place la chaussette (p, q) dans le tiroir $\overline{p}$. On en déduit donc l'existence d'une infinité de couples (p, q) comme ci-dessus, tels que tous les p ont la même congruence modulo l.

En envoyant ces chaussettes (p, q) dans le tiroir $\overline{q}$, on obtient finalement l'existence d'un infinité de couples (p_i, q_i) tels que p_i et q_i sont premiers entre eux, $p_i^2 - Nq_i^2 = l$, tous les p_i ont la même congruence modulo l; de même que tous les q_i.

Soient alors (p_1, q_1) et (p_2, q_2) des éléments distincts de cet ensemble; on a $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = l$ et $p_1 \equiv p_2 \bmod l$ et $q_1 \equiv q_2 \bmod l$. Ainsi $p_1q_2 - p_2q_1$ est divisible par l. De l'égalité $(p_1p_2 - Nq_1q_2)^2 - N(p_1q_2 - p_2q_1)^2 = l^2$, on en déduit que l divise $p_1p_2 - Nq_1q_2$ et $(\frac{p_1p_2 - Nq_1q_2}{l}, \frac{p_1q_2 - p_2q_2}{l})$ est alors une solution non triviale de l'équation.

□