Equations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes

prérequis : les notions élémentaires d'arithmétiques (pgcd, ppcm, congruences), extensions de corps, et selon le plan, idéaux premier, nombres de classes

Le titre est relativement précis ; on attend du candidat qu'il expose en détail la résolution des équations diophantiennes de degré 1 en insistant sur l'aspect alogrithmique, puis qu'il traite d'autres exemples. Il n'est pas écrit que ces autres exemples doivent être de degré supérieur, on laisse donc la possibilité au candidat de ne traiter que le cas des systèmes d'équation du premier degré toutefois il parait difficile de ne pas traiter quelques exemples simples comme l'équation de Fermat pour $n = 2$. Bien entendu aucune connaissance générale n'est attendu du candidat lequel pourra toutefois avancer les questions suivantes :

- historiquement les équations diophantiennes sont particulières au sens où on les étudie indépendamment les unes des autres : si on change un coefficient tout le raisonnement s'écroule et il faut reprendre une étude nouvelle : existe-t-il des familles d'équations diophantiennes qui se traitent de façon uniforme ?
- au delà de déterminer l'ensemble des solutions, peut-on montrer qu'il en existe un nombre infini (ou fini) ; peut-on les compter ou en déterminer les solutions primitives à partir desquelles on obtient toutes les autres ?
- dispose-t-on d'un algorithme permettant de trouver toutes les solutions ?

1. Exemple de plan

Une équation diophantienne est une équation polynomiale

$$f(x_1, \cdots, x_n) = 0$$

à coefficients entiers dont on cherche les solutions entières, i.e. dans $\mathbb{Z}^n$, ou rationnelles, i.e. dans $\mathbb{Q}^n$. La plus célèbre d'entre elles est certainement l'équation de Fermat

$$x^n + y^n - z^n = 0$$

dont les solutions sont pour $n \geq 3$ données par $xyz = 0$.

I- *Equations du premier degré*

1) $ax + by = c$: elle n'a de solutions que si $a \wedge b | c$ auquel cas l'ensemble des solutions est $(x_0 + t\frac{b}{a\wedge b}, y_0 - t\frac{a}{a\wedge b})$ où (x_0, y_0) est une solution particulière que l'on obtient en multipliant par $\frac{c}{a\wedge b}$ une relation de Bezout $au + bv = a \wedge b$ obtenue par l'algorithme d'Euclide étendu.
Exemples : : - pour $a \wedge p = 1$, l'équation $x^n \equiv a \mod p$ possède $n \wedge (p-1)$ solutions si et seulement si $a^{\frac{p-1}{n\wedge(p-1)}} \equiv 1 \mod p$ et sinon elle n'en possède aucune

- le système de congruence $x \equiv a \mod n$ et $x \equiv b \mod m$ n'a de solutions que si $n \wedge m$ divise $a - b$.

Si on s'intéresse uniquement aux solutions entières, on a alors le résultat suivant : pour $a \wedge b = 1$ si $c_1 + c_2 = ab - a - b$ alors exactement un des paramètres c_1, c_2 possède des solutions dans $\mathbb{N}$. En particulier si $c > ab - a - b$ alors l'équation $ax + by = c$ a des solutions $(x, y) \in \mathbb{N}^2$; pour $c = ab - a - b$ elle n'en a pas et pour $c \leq ab - a - b$ exactement la moitié de ces c ont de solutions.

2) $a_1x_1 + \cdots + a_nx_n = b$: elle n'a de solutions que si $a \wedge \cdots \wedge a_n | b$ auquel cas ses solutions sont $x_i = c_i + \sum_{k=1}^{n-1} d_{i,k}v_k$ où $(c_1, \cdots, c_n)$ est une solution particulière, les v_i sont des paramètres parcourant $\mathbb{Z}$ et les $d_{i,k} \in \mathbb{Z}$ sont .....

Si on s'intéresse comme précédemment aux solutions dans $\mathbb{N}$ alors on a le résultat suivant : soient $(a_1, \cdots, a_n) \in \mathbb{Z}^n$ tels que $a_1 \wedge \cdots \wedge a_n = 1$ alors le nombre $p(m)$ des $(x_1, \cdots, x_n) \in \mathbb{N}^n$ tels que $a_1x_1 + \cdots + a_nx_n = m$ est tel que

$$\sum_{m=0}^{+\infty} p(m)t^m = \frac{1}{(1-t^{a_1})\cdots(1-t^{a_n})}$$

de sorte que $p(m) \sim \frac{m^{n-1}}{a_1\cdots a_n(m-1)!}$.

3) $AX = B$ où $A \in \mathbb{M}_{m,n}(\mathbb{Z})$ et $B \in \mathbb{M}_{n,1}(\mathbb{Z})$: soit $P, Q \in GL_n(\mathbb{Z})$ telles que $A = Q^{-1}DP$ avec $d = \mathrm{diag}(d_1, \cdots, d_r, 0, \cdots, 0) \in \mathbb{M}_{m,n}(\mathbb{Z})$ et où $d_1 | \cdots | d_r \neq 0$. En posant $X' = PX$ et $B' = QB$ le système s'écrit $DX' = B'$ qui se résoud aisément...

II- *Quelques méthodes en degré supérieur*

1) *Congruences* : il s'agit de trouver un p tel que l'équation n'a pas de solutions modulo p : par exemple :

- $y^2 = 41x + 3$ n'a pas de solutions car $(\frac{3}{41}) = -1$;
- $y^2 = x^3 + 7$ n'a pas de solutions entières, cf. l'exercice 3.5,
- $y^3 = px + 2$ avec $p \equiv 1 \mod 3$ a une solution si et seulement s'il existe $a, b \in \mathbb{Z}$ tels que $p = x^2 + 27y^2$; en effet l'équation est équivalent à demander que 2 soit un cube modulo p, le résultat découle alors du théorème **??**.

2) *Arithmétique élémentaire dans* $\mathbb{Z}$, par exemple le cas $n = 2$ de l'équation de Fermat : soit $(x, y, z) \in \mathbb{Z}^3$ une solution de $x^2 + y^2 = z^2$ avec $x \wedge y \wedge z = 1$. Si x et y étaient impairs alors $z^2 \equiv 2 \mod 4$ ce qui est impossible car $0, 1$ sont les seuls carrés de $\mathbb{Z}/4\mathbb{Z}$. Supposons donc x pair et y, z impairs de sorte que le pgcd δ de $(z-y)$ et $(z+y)$ est égal à $(z-y) \wedge 2y = 2$ car $z - y$ est pair. On écrit alors $x^2 = 4a^2 = (z-y)(z+y) = 4ts$ avec t et s premiers entre eux et $z - y = 2t$, $z + y = 2s$. On en déduit alors que $s = u^2$ et $t = v^2$ de sorte que les solutions sont paramétrées par u et v avec $u \not\equiv v \mod 2$, $(u, v) = 1$ et $x = 2uv$, $z = u^2 + v^2$ et $y = |u^2 - v^2|$. On renvoie aussi le lecteur à l'exercice 3.7 ;

3) *Méthode de descente* : l'exemple classique est $x^4+y^4 = z^2$: il s'agit à partir d'une solution dans $\mathbb{N}$ non triviale (x, y, z) d'en construire une autre (c, d, a) avec $0 < a < z$. La contradiction découle alors du fait qu'il n'est pas possible de construire une suite infinie d'entiers positifs strictement décroissante.

Exemples : *Théorème des* 4 *carrés* : (Lagrange 1770) tout entier positif est somme de 4 carrés. A la vue du résultat de Lagrange, Waring en 1770 a posé le problème suivant : étant donné un entier k existe-t-il un entier s tel que tout $n \in \mathbb{N}$ est la somme d'au plus s puissance k-ème d'entiers. En 1909 Hilbert a répondu par l'affirmative et on renvoie le lecteur intéressé à [**1**] pour une version simplifiée de la preuve de Hilbert : on note alors $g(k)$ le plus petit de ces s. On a clairement $g(1) = 1$; d'après le théorème de Lagrange $g(2) \leq 4$ et comme 7 n'est pas la somme de 3 carrés, on a donc $g(2) = 4$. Dans les années 1940, Dickson, Pillai, Rubugunday et Niven ont donné une formule exacte de $g(k)$ qui à un détail près cf. [**1**] théorème 4.1. est égal à $\lfloor (3/2)^k \rfloor + 2^k - 2$. En fait dès les travaux de Hardy et Littlewood dans les années 1920, il est apparu plus naturel d'étudier l'entier$G(k)$ défini comme étant le plus petit s tel que tout entier n assez grand puisse s'écrire comme une somme de s puissance k-ème. Par exemple comme tout entier congru à 7 $\mod 8$ ne peut pas s'écrire comme la somme de 3 carrés, on en déduit $G(2) \geq 4$ et donc comme $G(2) \leq g(2) = 4$, $G(2) = 4$. La valeur exacte de $G(k)$ n'est pas connu mais on dispose d'encadrements par exemple $G(k) \leq k(3 \log k + 11)$ et $G(k) \geq k+1$ pour tout $k \geq 1$.

4) *Utilisation d'une extension de corps* :

– l'exemple classique est $x^2+y^2=n$ via l'anneau des entiers de Gauss $\mathbb{Z}[i]$. L'équation a des solutions si et seulement si $v_p(n)\equiv 0$ pour tout $p\equiv 3 \mod 4$; dans l'exercice 3.6 nous traitons le cas de $x^2+2y^2=n$. En ce qui concerne le nombre de solutions de cette équation cf. la proposition **??** ;
– l'équation de Fermat pour $n=3$; on renvoie le lecteur à [**?**] chapitre 17 §8 où le résultat découle de l'étude de $\mathbb{Z}[j]$;
– le cas de Kummer de l'équation de Fermat, i.e. quand n est premier et ne divise pas le nombre de classe de $\mathbb{Q}[e^{2i\pi/n}]$, cf. [**?**] chapitre 17 §11. La proposition suivante est une illustration plus simple de cette technique.

Proposition 1.1. — *(cf.* [**?**] *p.290) Soit $d>1$ sans facteurs carrés avec $d\equiv 1,2 \mod 4$. Supposons que le nombre de classes de $\mathbb{Q}(i\sqrt{d})$ n'est pas divisible par 3. Alors $y^2=x^3-d$ a une solution entière si et seulement si d est de la forme $3t^2\pm 1$ auquel ses solutions sont $(t^2+d,\pm t(t^2-3d))$.*

5) *méthode de Strassmann et de Skolem* : c'est plus évolué et on renvoie au cours

III- *Solutions fondamentales*

Dans ce paragraphe on s'intéresse à des équations diophantiennes possèdant une infinité de solutions qui s'obtiennent toutes à partir d'un nombre fini d'entre elles dites fondamentales.

1) *équation de Pell-Fermat* : il s'agit de trouver les solutions entières de $x^2-dy^2=1$. toutes les solutions sont obtenues à partir le solution minimale (x_0,y_0) vial la formule $(x_n+\sqrt{d}y_n)=(x_0+\sqrt{d}y_0)^n$; l'existence d'une solution non triviale peut se prouver par des applications multiples du lemme des tiroirs, son obtention explicite se fait via le développement en fractions continues de $\sqrt{d}$.

2) *équations d'Hurwitz* : il s'agit de résoudre dans $\mathbb{N}$ des équations du type

$$x_1^2+\cdots+x_n^2=z.\prod_{i=1}^{n}x_i. \tag{1}$$

Dans le cas où $z>n$ Hurwitz (1907) a montré qu'il n'y avait pas de solutions : le raisonnement procède par descente cf. par exemple [**2**] 4.37. La construction de nouvelles solutions découle alors du fait suivant : si $z,x_1,\cdots,x_n$ une solution alors $z,x_1,\cdots,x_{i-1},x_i',x_{i+1},\cdots,x_n$ où

$$x_i+x_i'=z\prod_{k\neq i}x_i$$

est aussi une solution. Les n solutions ainsi construites sont dites « voisines » de $z,x_1,\cdots,x_n$. Les solutions fondamentales sont alors celles telles que $x_1+\cdots+x_n$ est minimale.

3) *Equations de Thue* : c'est une équation de la forme $F(X,Y)=m$ avec $F(X,Y)\in\mathbb{Z}[X,Y]$ homogène de degré au moins 3. En admettant un résultat difficile d'approximation des entiers algébrique, la preuve de la finitude du nombre de solutions d'une équation de Thue est relativement aisée.

4) *Aspect algorithmique* : en 1970 Yu. V. Matiyasevich))) a résolu par la négative une question posée par Hilbert en 1900 : il n'y a pas d'algorithme général permettant de déterminer si une équation en nombre entiers $\mathrm{f}(x_1,\cdots,x_n)=0$ a ou non une infinité de solutions dans $\mathbb{Z}^n$. Cependant en restreignant le problème à des familles d'équations la réponse peut devenir positive : par exemple pour les équations de Thue (via l'algorithme LLL), les équations d'Hurwitz, ou plus simple encore les formes quadratiques.

IV- *Changeons d'anneau* :

1) *Solutions rationnelles* : dans le cas homogène l'application qui à une solution entière $(x_1, \cdots, x_n)$ associe l'ensemble des $(\frac{x_1}{t}, \cdots, \frac{x_n}{t})$ où t décrit $\mathbb{Q}^\times$ induit une surjection sur l'ensemble des solutions rationnelles (ainsi trouver les solutions entières revient à trouver les solutions rationnelles). En général cela ne se passe pas du tout ainsi : par exemple une courbe elliptique possède en général un nombre infini de solutions rationnelles alors qu'elle ne possède qu'un nombre fini de solutions entières. Plus simplement l'équation $y(y-1) = x^2$ a deux solutions entières à savoir $(0,0)$ et $(0,1)$ tandis qu'elle a une infinité de solutions rationnelles $(\frac{t}{t^2-1}, \frac{t^2}{t^2-1})$.

1 bis) *Méthode géométrique* : cela concerne les courbes unicursales, en particulier les coniques $f(x,y) = 0$: la méthode consiste à partir d'une solution particulière (x_0, y_0) à considérer les droite de pente $t \in \mathbb{Q}$ passant par (x_0, y_0) : le second point d'intersection qui s'obtient en résolvant une équation linéaire est alors une solution rationnelle et on les obtient toutes ainsi.

Exemples : $x^2+y^2 = 1$: une solution particulière est $(-1, 0)$, on considère donc les droites d'équation $y = t(x+1)$ le deuxième point d'intersection s'obtient en résolvant l'équation $x^2 + t^2(x+1)^2 - 1 = 0$ qui possède la solution $x = -1$ de sorte qu'en divisant par $x+1$ on obtient

$$x - 1 + t^2(x+1) = 0$$

ce qui donne

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}.$$

En écrivant $t = a/b$, on retrouve alors les formules

$$x = \frac{b^2-a^2}{b^2+a^2}, \qquad y = \frac{2ab}{b^2+a^2}$$

qui conduisent à la solution générale en nombre entiers de l'équation homogène $x^2+y^2 = z^2$.

Remarque : pour une cubique, à partir d'une solution rationnelle, le troisième point d'intersection de la tangente passant par ce point fournit une autre solution. De même à partir de deux solutions rationnelles, le troisième point d'intersection de la droite passant par ces deux solutions, est une troisième solution.

Remarque : les solutions rationnelles de l'équation de Pell-Fermat $x^2 - dy^2$ où d est un entier qui n'est pas un carré, sont paramétrées par

$$x = \frac{dt^2+1}{dt^2-1}, \qquad y = \frac{2t}{dt^2-1}.$$

2) *corps finis* : au delà du théorème de Chevalley-Waring, via les sommes de Gauss et de Jacobi, on sait très bien encadrer le nombre de solutions d'une équation diophantienne

3) *corps des fractions rationnelles* : l'arithmétique est favorable puisque $\mathbb{C}[X]$ est principal et que les irréductibles sont parfaitement connus. On dispose en outre de la dérivation que l'on exploite via le fameux théorème de Mason qui permet alors de prouver, par exemple, le théorème de Liouville (Fermat sur $\mathbb{C}[X]$), l'équation de Catalan...

4) *corps p-adiques* : il s'agit de regarder si notre équation a des solutions dans tous les corps p-adique et d'en déduire, c'est le principe de Hasse, qu'il y a des solutions dans $\mathbb{Q}$: malheureusement ce principe n'est pas vérifiée en général. Toutefois en ce qui concerne

les formes quadratiques l'existence de solutions globales est bien équivalente à celle de solutions locales (théorème de Hasse-Minkowski) (de Legendre pour les formes ternaires)

V- *Résultats récents*

1) *courbes elliptiques* : il s'agit de trouver les points entiers et rationnels de la courbe régulière $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Le fait remarquable est que ces courbes peuvent être munis d'une loi de groupe, cf. §**??**. Le théorème de Mordell-Weil dit que pour tout corps K, $E(K)$ est un groupe abélien de type fini dont le rang est conjecturalement égal à l'ordre du zéro en $s = 1$ de la fonction L attachée à E ; c'est la version faible de la conjecture de Birch-Swinnerton-Dyer ;

2) *Travaux de Siegel* : en 1929 Sigel a donné des CNS sur le polynôme $f \in \mathbb{Z}[X, Y]$ pour qu'il possède une infinité de solutions.

3) *théorème de Faltings* : soit C une courbe algébrique non singulière de genre g alors :
- si $g = 0$, il y a soit aucun point rationnel soit une infinité (cf. l'exercice 3.6 ;
- si $g = 1$, i.e. C est une courbe elliptique, il y a soit un nombre fini de points formant un groupe abélien soit l'ensemble des points rationnels est un groupe abélien de type fini (théorème de Mordell) ;
- si $g > 1$ il n'y a qu'un nombre fini de points rationnels.

4) *Grand théorème de Fermat* : (1995) preuve due à Wiles en suivant la stratégie Frey-Serre-Ribet via la conjecture de Shimura-Taniyama-Weil sur les courbes elliptiques

5) *Conjecture de Catalan* : (2003) il s'agit de $x^m - y^n = 1$ dont les seules solutions sont $(x, y, m, n) = (3, 2, 2, 3)$ (c'est un exemple d'équation diophantienne exponentielle)

6) *Conjecture abc* : version arithmétique du théorème de Mason qui implique bcp de résultats sur les équations diophantiennes.

2. Développements

- résolution d'une équation diophantienne de degré 1 [**5**] ou d'un système [**3**]
- théorème de Fermat pour $n = 2$ et $n = 4$ [**6**]
- théorème des 4 carrés
- équation de Pell [**5**]
- théorème de Carathéodort (comme lemme) + satisfaisabilité des systèmes linéaires homogènes diophantiens
- équivalent asymptotique du nombre de solutions d'une équation diophantienne de degré 1 [**4**] [**?**]
- $y^2 = x^3 - d$ a une solution entière ssi $d = 3t^2 \pm 1$ auquel cas ses solutions sont $(t^2 + d, \pm t(t^2 - 3d))$;
- équation d'Hurwitz ;
- finitude du nombre de solutions d'une équation de Thue en utilisant un résultat d'approximation

3. Questions

Exercice 3.1. — *Pour $a \wedge p = 1$, montrer que le nombre de solutions de l'équation $x^n \equiv a \mod p$ est égal à $n \wedge (p-1)$ si $a^{\frac{p-1}{n\wedge(p-1)}} \equiv 1 \mod p$ et nul sinon.*

Exercice 3.2. — *Montrer que le système $x \equiv a \mod n$ et $x \equiv b \mod m$ a des solutions si et seulement si $n \wedge m | (a - b)$.*

Exercice 3.3. — *Montrer que les solutions rationnelles de l'équation de Pell-Fermat x^2-dy^2 où d est un entier qui n'est pas un carré, sont paramétrées par*

$$x = \frac{dt^2+1}{dt^2-1}, \qquad y = \frac{2t}{dt^2-1}.$$

Exercice 3.4. — $y^2-4=x^3$, $y^2+2=x^3$, $y^2+4=x^3$

Exercice 3.5. — *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.

Exercice 3.6. — *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) Étudiez 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 $p \equiv 1,3 \mod 8$.

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

Exercice 3.7. — – *On considère l'équation $x^2+y^2 = z^2$ avec $z \neq 0$. Soit alors $w = \frac{x+iy}{z} \in \mathbb{Q}[i]$. Montrez en utilisant le théorème de Hilbert 90 qu'il existe $(m,n) \in \mathbb{Z}^2$ tel que (x,y,z) est proportionnel à $(m^2-n^2, 2mn, m^2+n^2)$.*

– *On considère désormais l'équation diophantienne $x^2+Axy+By^2 = z^2$ avec $A,B \in \mathbb{Z}$ tel que le discriminant A^2-4B n'est pas un carré. Soit alors $w = \frac{x+ry}{z} \in \mathbb{Q}[r]$ où r est une solution de $r^2-Ar+B = 0$. Montrez alors que (x,y,z) est proportionnel à $(m^2-Bn^2, 2mn+An^2, m^2+Amn, Bn^2)$.*

– *Soit plus généralement $x^2+Axy+By^2 = Cz^2$ avec $A,B,C \in \mathbb{Z}$ avec $A^2-4B \notin (\mathbb{Q}^\times)^2$. Soit alors $w = \frac{x+ry}{z} \in \mathbb{Q}(r)$. On suppose que l'on connaît une solution (x_0,y_0,z_0) avec $z_0 \neq 0$ et soit $w_0 = \frac{x_0+ry_0}{z_0}$; en considérant w/w_0, trouvez en utilisant le théorème de Hilbert 90, toutes les solutions de cette équation.*

– *Comparez cette technique à la méthode géométrique.*

Exercice 3.8. — *Le plan $\mathcal{P}$ étant rapporté à un repère orthonormal $(O,\vec{u},\vec{v})$, on considère l'hyperbole $\mathcal{H}$ d'équation $x^2-3y^2 = 1$ et on désigne par $\mathfrak{S}$ l'ensemble des points du plan dont les deux coordonnées sont des éléments de $\mathbb{Z}$. On se propose d'étudier l'ensemble $\mathcal{H} \cap \mathfrak{S}$.*

(1) A tout point M de coordonnées (x,y) dans $(O,\vec{u},\vec{v})$, on associe son affixe $z = x+iy \in \mathbb{C}$. On définit une application $f : \mathbb{C} \to \mathbb{C}$ par $f(z) = (2-i)z+2i\bar{z}$. A f on associe l'application $F : \mathcal{P} \to \mathcal{P}$ qui au point d'affixe z associe $M' = F(M)$ d'affixe $z' = f(z)$.

(i) Montrez que F est une application affine et bijective qui conserve les aires des triangles. Est-ce une isométrie ?

(ii) Montrez que M appartient à $\mathcal{H}$ (resp. $\mathfrak{S}$) si et seulement si M' aussi.

(2) On construit par récurrence une suite de points $(A_n)_{n\in\mathbb{N}}$ en posant pour tout n : $A_{n+1} = F(A_n)$, A_0 étant le point de coordonnées $(1,0)$.

(i) Calculez les coordonnées de A_1 et A_2 puis montrez que pour tout n, $A_n \in \mathcal{H} \cap \mathfrak{S}$.

(ii) Quels sont les points de $\mathfrak{S}$ situés sur l'arc $[A_0, A_1]$ de $\mathcal{H}$?

(3) On définit sur $\mathcal{H}$ une opération $*$ ainsi : M et N étant deux points de $\mathcal{H}$, on leur associe la droite $D_{M,N}$ issue de A_0 et parallèle à la droite (MN) (ou à la tangente en M à $\mathcal{H}$ si $M = N$). Dans le cas où $D_{M,N}$ est tangente à $\mathcal{H}$ en A_0, on pose $M * N = A_0$ et sinon $M * N$ est le second point de rencontre de $D_{M,N}$ avec $\mathcal{H}$, cf. la figure **??**

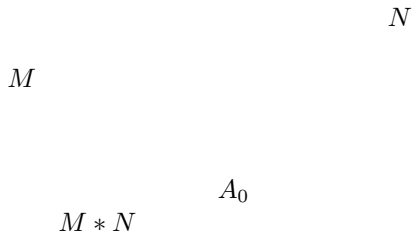

FIG. 1. Loi de groupe sur une hyperbole

(i) Montrez qu'il existe un repère $\mathcal{R}$ de $\mathcal{P}$ dans lequel $\mathcal{H}$ a pour équation $XY = 1$. Exprimez alors dans ce repère l'abscisse de $M * N$ en fonction de celle de M et N. En déduire que $(\mathcal{H}, *)$ est un groupe isomorphe au groupe multiplicatif $(\mathbb{R}^*, \times)$.

(ii) Montrez que pour tout $M \in \mathcal{H}$, $F(M) = A_1 * M$ et calculez les coordonnées (X_n, Y_n) de A_n dans $\mathcal{R}$ en fonction de X_1 et n.

(iii) Montrez que la tangente en A_n à $\mathcal{H}$ est parallèle à la droite $(A_{n-1}A_{n+1})$ puis calculez l'aire du triangle $A_{n-1}A_nA_{n+1}$.

(iv) Prouvez que M est un point de l'arc $[A_n, A_{n+1}]$ de $\mathcal{H}$ si et seulement si $M' = A_1 * M$ appartient à l'arc $[A_{n+1}, A_{n+2}]$ de $\mathcal{H}$. Décrivez alors l'ensemble $\mathcal{H} \cap \mathfrak{S}$.

(4) Donnez tous les couples (x, y) de nombres entiers naturels solutions de l'équation $x^2 - 3y^2 = 1$.

Exercice 3.9. — *Étude de l'équation de Pell-Fermat : $x^2 - Ny^2 = 1$.*

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

(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 :

$$\begin{cases} x_{n+1} = x_0 x_n + N y_0 y_n \\ y_{n+1} = x_0 y_n + x_n y_0 \end{cases}$$

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 $0 \leq n \leq q$ et les tiroirs sont les intervalles $[k/q, (k+1) : q]$ pour $0 \leq k < q$.

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 $l < 1 + 2\sqrt{N}$, $p_1 \equiv p_2 \mod l$, $q_1 \equiv q_2 \mod l$ 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.

Exercice 3.10. — ***Théorème de Sophie Germain***, *cf. par exemple* [**?**] *p.275 : soit p premier impair tel que $q = 2p + 1$ est premier, le but est de montrer qu'il n'existe pas de solutions entières à l'équation $x^p + y^p + z^p$ telle que $p \nmid xyz$. On raisonne par l'absurde en considérant une solution (x, y, z) avec $p \nmid xyz$:*

(i) On écrit $-x^p = (y + z)(z^{p-1} - z^{p-2}y + \cdots + y^{p-1})$; montrez que les deux facteurs du membre de droite sont premiers entre eux.

(ii) En déduire qu'il existe des entiers $A, B, C, T \in \mathbb{Z}$ tels que

$$y + z = A^p, \quad x + z = B^p, \quad x + y = C^p, \quad z^{p-1} - z^{p-2}y + \cdots + y^{p-1} = T^p.$$

(iii) Montrez quitte à échanger les rôles de x, y, z, que $q|x$ et $q|A$.

(iv) Montrez que q ne divise pas T et aboutissez à une contradiction.

4. Solutions

3.1 Via l'isomorphisme $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, l'équation devient $ny \equiv b \mod (p-1)$ soit à résoudre l'équation suivante dans $\mathbb{Z}$, $ny + \lambda(p-1) = b$, qui possède des solutions si et seulement si $n \wedge (p-1)|b$, i.e. si b appartient au groupe engendré par $n \wedge (p-1)$ et donc si et seulement si l'ordre de b est un diviseur de $\frac{p-1}{n\wedge(p-1)}$. Dans ce cas les solutions sont de la forme $y = y_0 + t\frac{p-1}{n\wedge(p-1)}$ modulo $p-1$ et donc de cardinal celui du sous-groupe de $\mathbb{Z}/(p-1)\mathbb{Z}$ engendré par $\frac{p-1}{n\wedge(p-1)}$ i.e. $n \wedge (p-1)$.

3.2 On passe dans $\mathbb{Z}$ soit à résoudre $x+\alpha n = a$ et $x+\beta m = b$ et donc $\alpha n - \beta m = (a-b)$ qui ne possède des solutions que si $n \wedge m$ divise $a-b$.

3.3

3.4

3.5 (i) Si x est pair, on a $y^2 \equiv -1 \mod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2 = 1+4k(k+1) \equiv 1 \mod 8$ 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 $p \equiv 3 \mod 4$. Or si p premier divise y^2+1 alors $p \equiv 1 \mod 4$, d'où la contradiction.

3.6 (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 $y^2 \equiv -2 \mod 8$, 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 $p \equiv 5, 7 \mod 8$. En raisonnant comme dans l'exercice précédent, on trouve que les irréductibles de A, outre les premiers $p \equiv 5, 7 \mod 8$, 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 $p \equiv 5, 7 \mod 8$.

(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 $p \equiv \pm \mod 8$.

3.7

3.8 (1) On a $f(z) = 2x + 3y - i(x + 2y)$ de sorte que F est affine avec $F(O) = O$ et de partie linéaire $\vec{F} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ de déterminant 1, de sorte qu'elle est inversible, conserve les volumes. Ce n'est pas une isométrie puisque ses vecteurs colonnes ne sont pas de norme 1.

Le déterminant étant égal à 1, son inverse est aussi à coefficients dans $\mathbb{Z}$ de sorte que $M \in \mathfrak{S}$ si et seulement si $F(M) \in \mathfrak{S}$. En ce qui concerne $\mathcal{H}$, on a $(2x+3y)^2-3(x+2y)^2 = x^2-3y^2 = 1$.

(2) (i) On calcule $A_1 = (2, 1)$ et $A_2 = (7, 4)$. Par récurrence on montre que $A_n \in \mathcal{H} \cap \mathfrak{S}$ en utilisant (1 ii).

(ii) Un point $M(x, y)$ de l'arc $[A_0, A_1]$ de $\mathcal{H}$ est caractérisé par $x^2 - 3y^2 = 1$, $1 \leq x \leq 2$ et $0 \leq y \leq 1$. Si on veut $x, y \in \mathbb{Z}$, on a alors que deux possibilités qui donnent A_0 et A_1.

(3) (i) On se place dans le repère dont les axes sont les asymptotes de sorte que l'équation est $XY = a$. Il suffit alors d'imposer que A_0 soit de coordonnées $(1, 1)$. Soient alors $M(a, b)$ et $M'(a', b')$. Supposons dans un premier temps $M \neq N$ et donc $a \neq a'$. La droite $D_{M,N}$ a alors pour équation $\frac{Y-1}{X-1} = \frac{b'-b}{a'-a}$. L'intersection avec $\mathcal{H}$ revient à prendre $Y = 1/X$ avec $X \neq 0$ ce qui donne alors $X = aa'$.

Si $M = N$, la tangente en M à H a pour pente $-1/a^2$ ce qui donne $\frac{Y-1}{X-1} = -1/a^2$ et donc avec $XY = 1$, $X = a^2$. Ainsi l'application $\phi : \mathcal{H} \to \mathbb{R}^\times$ qui à M associe l'abscisse de M dans le repère $\mathcal{R}$, induit un isomorphisme de $(\mathcal{H}, *)$ avec $(\mathbb{R}^\times, \times)$.

Remarque : le résultat est valable pour toute hyperbole.

(ii) Si $M \neq A_1$ et $M' \neq A_0$, il s'agit de vérifier que (A_0M')et (MA_1) sont parallèles, ce qui revient à montrer que $\begin{vmatrix} 2x + 3y - 1 & x - 2 \\ x + 2y & y - 1 \end{vmatrix} = 3y^2 - x^2 + 1 = 0$. Si $M = A_1$, la tangente en A_1 a pour équation $2x - 3y = 1$ et a pour vecteur directeur $(3, 2)$. Il suffit alors de vérifier que $\begin{vmatrix} 7-1 & 3 \\ 4 & 2 \end{vmatrix} = 0$. Si $M' = A_0$ alors M a pour coordonnées $(2, -1)$ et (A_1M) est parallèle à Oy donc à la tangente en A_0 à $\mathcal{H}$. Ainsi on a $A_n = A_1 * \cdots * A_1$ et donc $X_n = X_1^n$.

(iii) $A_n * A_n$ et $A_{n-1} * A_{n+1}$ sont sur $\mathcal{H}$ et ont même abscisse dans $\mathcal{R}$, ils coincident donc et la construction de $M * N$ donne le résultat. En ce qui concerne l'aire elle est égale à celle de $A_0A_1A_2$ et donc à $\frac{1}{2}\begin{vmatrix} 2-1 & 7-1 \\ 1 & 4 \end{vmatrix} = 1$.

(iv) L'arc $[A_n, A_{n+1}]$ de$\mathcal{H}$ est l'ensemble des points M de coordonnées $(X, 1/X)$ avec $X_1^{n+1} \leq X \leq X_1^n$ (quitte à échanger les axes, on choisit le repère pour que $X_1 < 1$). L'application F se traduit par $X \mapsto X_1.X$ et induit donc la bijection de l'énoncé. En particulier d'après (2 ii), on en déduit que $\mathcal{H} \cap \mathfrak{S}$ est formé des A_n et de leurs symétriques par rapport à Ox, Oy et O.

(4) Les asymptotes de $\mathcal{H}$ ont pour vecteurs directeurs $\vec{u}' = \alpha(\sqrt{3}\vec{u} - \vec{v})$ et $\vec{v}' = \beta(\sqrt{3}\vec{u} + \vec{v})$. Pour que A_0 ait pour coordonnées $(1, 1$ dans $\mathcal{R}$, on doit avoir $\vec{u}' + \vec{v}' = \vec{u}$ ce qui donne $\alpha = \beta = \frac{1}{2\sqrt{3}}$. On obtient alors $X_1 = 2 - \sqrt{3}$ (et $Y_1 = 2 + \sqrt{3}$). On en déduit alors $X_n = (2 - \sqrt{3})^n$ et $Y_n = (2 + \sqrt{3})^n$ et donc

$$|x| = \frac{(2 + \sqrt{3})^n + (2 - \sqrt{3})^n}{2} \qquad |y| = \frac{(2 + \sqrt{3})^n - (2 - \sqrt{3})^n}{2\sqrt{3}}.$$

3.9 Evidemment, on se limite à chercher les solutions $x, y \geq 0$.

(i) Pour $N \leq -2$, 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, $x_0 \geq 2$ et $y_0 \geq 1$ 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 : $(x_1, y_1) \leq (x_2, y_2)$ si et seulement si $x_1 \leq x_2$. 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 $n \geq 0$ tel que $x_n \leq x < x_{n+1}$; on a alors $y_n \leq y < y_{n+1}$ et donc $1 \leq \frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}} < x_0 + y_0\sqrt{N}$. 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 $X \geq 0$ car $x \geq y \geq 0$ et $x_n \geq y_n \geq 0$; de même $Y \geq 0$ 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 $q \leq q_0$ et p tel que $|\sqrt{N} - p/q| < 1/qq_0 \leq 1/q^2$ ce qui est en contradiction avec le fait que l'on devrait avoir $|\sqrt{N} - p/q| \geq \epsilon$. 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 $\bar{p}$. 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 $\bar{q}$, 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 $p_1 \equiv p_2 \mod l$ et $q_1 \equiv q_2 \mod l$. 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.

3.10 (i) Par hypothèse $p \nmid x$ et donc $p \nmid y + z$. Soit alors $r \neq p$ premier divisant les deux facteurs de sorte que $y \equiv -z \mod r$ et donc

$$0 \equiv z^{p-1} - z^{p-2}y + \cdots + y^{p-1} \equiv py^{p-1} \mod r$$

et donc $r|y$ ce qui implique $r|z$ contredisant l'hypothèse $x \wedge y \wedge z = 1$.

(ii) Comme le produit de $y + z$ et $z^{p-1} - z^{p-2}y + \cdots + y^{p-1}$ est une puissance p-ème et que d'après (i), ces deux facteurs sont premiers entre eux, ce sont tous deux des puissances p-ème, i.e. il existe A, T tels que $y + z = A^p$ et $z^{p-1} - z^{p-2}y + \cdots + y^{p-1} = T^p$. On reprend le raisonnement avec $-y^p = (x + z)(z^{p-1} - \cdots + x^{p-1}$ et $-z^p = (x + y)(x^{p-1} - \cdots + y^{p-1})$ de sorte qu'il existe B, C tels que $x + y = C^p$ et $x + z = B^p$.

(iii) On a $p = \frac{q-1}{2}$ avec $x^{\frac{q-1}{2}} + y^{\frac{q-1}{2}} + z^{\frac{q-1}{2}} \equiv 0 \mod q$; or si $q \nmid xyz$, chacun de ces trois termes est égal à ± 1 ce qui est impossible car $q > 5$. Ainsi quitte à échanger les rôles de x, y, z, supposons $q|x$. On a alors $2x = B^p + C^p - A^p$ soit

$$B^{\frac{q-1}{2}} + C^{\frac{q-1}{2}} - A^{\frac{q-1}{2}} \equiv 0 \mod q$$

ce qui impose en suivant le raisonnement précédent que $q|ABC$. Or si $q|B$ (resp. $q|C$) alors $q|z = B^p - x$ (resp. $q|y = C^p - x$) ce qui n'est pas et donc $q|A$.

(iv) Comme $A \wedge T = 1$, q ne divise pas T. D'après (iii), on a $y \equiv -z \mod q$ et donc $T \equiv py^{p-1} \mod q$. Or $y \equiv B^p \equiv \pm 1 \mod q$ et donc $\pm 1 \equiv T^p \equiv \pm p \mod q$ ce qui est impossible.

Références

[1] W. J. Elison. Waring's problem. *Amer. Math. Monthly.*, 78 :10–76, 1971.

[2] S. Francinou and Gianella H. *Exercices de mathématiques oraux X-ENS, algèbre 1.* Cassini, 2001.

[3] J. Fresnel. *Algèbre des matrices.* Hermann, 1997.

[4] Gourdon. *Les maths en têtes : algèbre.* Ellipses, 1996.

[5] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Oxford University Press, 1980.

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