Exercice

On veut résoudre l'équation $5^m - 2^n = 1$ d'inconnue $(m,n) \in \mathbb{N}^2$.

a) Déterminez les solutions telles que $n \leqslant 2$.
Désormais, on cherche les solutions telles que $n \geqslant 3$. Soit (m,n) une solution telle que $n \geqslant 3$.

b) En travaillant modulo 8, montrez que m est pair.

c) Montrez alors que $5^m - 1$ est divisible par 3.

d) Concluez : quelles sont les solutions ?

Problème 1 - Deux équations de Mordell

On appelle *équations de Mordell* les équations diophantiennes de la forme : $y^2 = x^3 + k$ d'inconnue $(x,y) \in \mathbb{Z}^2$ avec $k \in \mathbb{Z}$ fixé. On sait beaucoup de choses sur ces équations, en particulier qu'elles possèdent toujours un nombre fini de solutions — mais c'est un résultat difficile. Ce devoir se donne pour objectif modeste de vous aider à en résoudre deux.

On rappelle à toutes fins utiles que pour tous $a, b \in \mathbb{N}$ premiers entre eux, si ab est un cube parfait alors a et b en sont aussi.

Partie 1 - Équation de Mordell $y^2 = x^3 + 16$

Question 1) Soit $(x,y) \in \mathbb{Z}^2$. On suppose que $y^2 = x^3 + 16$ et que y est impair.

a) Montrez qu'il existe deux entiers impairs a, b tels que $y + 4 = a^3$ et $y - 4 = b^3$.

b) Montrez que $a = b + 8$, puis concluez.

Question 2) Soit $(x,y) \in \mathbb{Z}^2$. On suppose que : $y^2 = x^3 + 16$ et que y est pair.

a) Montrez que x et y sont divisibles par 4.
On peut donc se donner deux entiers x' et y' pour lesquels $x = 4x'$ et $y = 4y'$.

b) Montrez que y' est impair.
On peut donc se donner un entier n pour lequel $y' = 2n + 1$.

c) Montrez que n et $n+1$ sont des cubes parfaits, puis déduisez-en x.

Question 3) Résolvez l'équation de Mordell : $y^2 = x^3 + 16$ d'inconnue $(x,y) \in \mathbb{Z}^2$.

Partie 2 - Équation de Mordell $y^2 = x^3 - 5$

Question 1) Soit $(x,y) \in \mathbb{Z}^2$. On suppose que : $y^2 = x^3 - 5$.

a) Étudiez la parité de y et calculer le reste de la division euclidienne de x par 4.

b) Montrez que $x^2 + x + 1$ possède un facteur premier p congru à 3 modulo 4.

Question 2)

a) Montrez qu'il existe $n \in \mathbb{Z}$ tel que $n^2 \equiv -1\ [p]$.

b) Calculez n^{p-1} modulo p de deux manières différentes, puis concluez.

Problème 2 - Une équation diophantienne

On veut résoudre l'équation $x^2 + 2^x = y^2$ d'inconnue $(x,y) \in \mathbb{N}^2$.

Question 1) Déterminez les solutions (x,y) telles que $x \in [\![0, 10]\!]$.

Dans toute la suite, on s'intéresse aux solutions (x,y) telles que $x > 0$.

Question 2) Montrez qu'il existe $(\alpha, \beta) \in \mathbb{N}^2$ tel que $\begin{cases} y - x &= 2^\alpha \\ y + x &= 2^\beta \\ x &= \alpha + \beta \end{cases}$. Vérifiez que $\beta > \alpha$.

Question 3) Montrez que $\alpha \geqslant 1$, puis déduisez-en que $2^{\beta-1} - \beta = 2^{\alpha-1} + \alpha$.

Question 4) On suppose que $\alpha = 1$ dans cette question.

a) On pose $f : t \mapsto 2^{t-1} - t$. Étudiez les variations de f sur $[3, +\infty[$.

b) Aboutissez à une contradiction.

Question 5) Justifiez que x et y sont pairs, puis que $\beta \geqslant \alpha + 2$.

Question 6) On suppose que $\alpha \geqslant 3$.

a) Montrez que $2^{\alpha+1} - \alpha - 2 > 2^{\alpha-1} + \alpha$.

b) En réutilisant la fonction f, aboutissez à une contradiction.

Question 7) Concluez : quel est l'ensemble des solutions de l'équation proposée ?

Devoir non surveillé 6 - Corrigé

Exercice

a) Les cas $n = 0$ et $n = 1$ ne donnent aucune solution. Le cas $n = 2$ donne la solution $(m, n) = (1, 2)$: $5 - 4 = 1$.

b) Si maintenant on suppose $n \geqslant 3$, alors $5^m \equiv 1$ [8] : or $5^2 \equiv 1$ [8] donc en écrivant la division euclidienne de m par 2, on a $m = 2q + r$ où $r \in \{0, 1\}$ puis $5^m = (5^2)^q \times 5^r \equiv 5^r \equiv 1$ [8] donc $r = 0$, autrement dit m est pair.

c) m est pair donc il existe $q \in \mathbb{N}$ tel que $m = 2q$, donc $5^m - 1 = 25^q - 1$; or $25 \equiv 1$ [3] donc $25^q - 1 \equiv 0$ [3], donc $5^m - 1$ est divisible par 3.

d) Or on a donc $25^q - 1 = 2^n$, on en déduit que 3 divise 2^n : impossible.
Conclusion : il n'existe aucune solution telle que $n \geqslant 3$, donc la seule solution est le couple $(m, n) = (1, 2)$.

Problème 1

Partie 1

Question 1)

a) $y^2 = x^3 + 16$ donc $x^3 = (y - 4)(y + 4)$
S'il existe p premier qui divise $y - 4$ et $y + 4$, alors p divise $(y + 4) - (y - 4) = 8$, donc $p = 2$. Or y est impair, donc $y + 4$ l'est aussi, donc 2 ne divise pas $y + 4$: contradiction. Donc $y - 4$ et $y + 4$ sont premiers entre eux.
Comme leur produit est un cube, alors eux-mêmes sont des cubes d'après un théorème du cours : il existe $(a, b) \in \mathbb{Z}^3$ tel que $y + 4 = a^3$ et $y - 4 = b^3$.
Puisque $y + 4$ est impair, alors a est impair aussi, ainsi que b.

b) On peut factoriser : $(y + 4) - (y - 4) = 8 = a^3 - b^3 = (a - b)(a^2 + ab + b^2)$. Or comme a et b sont impairs, a^2, b^2 et ab sont impairs donc $a^2 + ab + b^2$ est impair et divise 8 donc $a^2 + ab + b^2$ vaut 1 ou -1. De plus, $a^2 + ab + b^2 = \left(a + \dfrac{b}{2}\right)^2 + 3\dfrac{b^2}{4} \geqslant 0$, donc $a^2 + ab + b^2 = 1$ et donc $a - b = 8$.
Donc $1 = a^2 + ab + b^2 = 3b^2 + 24b + 64$ donc $b^2 + 8b + 21 = 0$. Or ce trinôme du second degré n'a pas de racines réelles : contradiction.
L'équation de Mordell $y^2 = x^3 + 16$ n'a donc pas de solution (x, y) telle que y soit impair.

Question 2)

a) y est pair, donc 4 divise y^2 donc 4 divise $x^3 + 16$ donc aussi x^3. Donc x est pair. On note $y = 2a$ et $x = 2b$ et on reporte dans l'équation : $a^2 = 2b^3 + 4$, donc a^2 est pair, donc a l'est aussi. On peut noter $a = 2y'$, puis on reporte : $2y'^2 = b^3 + 2$, donc b^3 est pair, donc b l'est aussi. On peut noter $b = 2x'$.
Donc finalement, $x = 4x'$ et $y = 4y'$.

b) Il vient donc l'égalité : $y'^2 = 4x'^2 + 1$. Donc y'^2 est impair et y' l'est aussi.

c) On peut noter $y' = 2n + 1$ et on reporte : $n^2 + n = x'^3$, ou encore $n(n + 1) = x'^3$.
Or n et $n+1$ sont premiers entre eux, donc d'après un th. du cours, n et $n+1$ sont deux cubes. Il existe $(p, q) \in \mathbb{Z}^3$ tel que $n + 1 = p^3$ et $n = q^3$.
Comme $n + 1 > n$, alors $p > q$, puis $1 = (n + 1) - n = (p - q)(p^2 + pq + q^2)$, donc on obtient $p - q = 1$ et $p^2 + pq + q^2 = 1$. Puis $3q^3 + 3q = 0$ donc $q = 0$ ou $q = -1$, donc $n = 0$ ou $n = -1$ donc $x = 4x' = 0$.

Question 3) $x = 0$ donc il vient $y^2 = 16$ donc $y = 4$ ou $y = -4$

L'équation de Mordell $y^2 = x^3 + 16$ a donc deux solutions : les couples $(x, y) = (0, 4)$ et $(x, y) = (0, -4)$.

Partie 2

Question 1)

a) Si y est impair, alors $y^2 \equiv 1$ [4] donc $x^3 \equiv 2$ [4]. Or une petite vérification rapide montre qu'un cube ne peut être congru qu'à 0, 1 ou 3 modulo 4 ($0^3 = 0$, $1^3 = 1$, $2^3 = 8 \equiv 0$ [4] et $3^3 \equiv (-1)^3 \equiv -1$ [4]), d'où une contradiction. Donc y est pair. On note $y = 2n$.
Il vient alors x impair, donc le reste de la division euclidienne de x par 4 est 1 ou 3.
Si $x = 4q + 3$, alors $x^3 = 64q^3 + 144q^2 + 36q + 27 = 4p^2 + 5$ donc $32q^3 + 72q^2 + 18q = 2p^2 - 11$, ce qui est absurde car 2 ne divise pas 11.
Donc le reste de la division euclidienne de x par 4 est 1.

b) $x \equiv 1$ [4] donc $x^2 + x + 1 \equiv 3$ [4]. Or les nombres premiers sont 2 (qui ne divise pas $x^2 + x + 1$), ou congrus à 1 modulo 4 ou congrus à 3 modulo 4.
Si tous les facteurs premiers de $x^2 + x + 1$ sont congrus à 1 modulo 4, alors lui-même est congru à 1 modulo 4. Donc $x^2 + x + 1$ possède au moins un facteur premier congru à 3 modulo 4.

Question 2)

a) $x^2 + x + 1 \equiv 0$ $[p]$ donc $x^3 - 1 = (x-1)(x^2+x+1) \equiv 0$ $[p]$ donc $y^2 + 4 \equiv 0$ $[p]$. Or $y = 2n$, donc p divise $y^2 + 4 = 4(n^2+1)$. Comme p est premier différent de 2, on en déduit que p divise $n^2 + 1$, autrement dit $n^2 \equiv -1$ $[p]$.

b) D'une part, n est premier avec p (sinon p diviserait n donc n^2) donc d'après le petit th. de Fermat, $n^{p-1} \equiv 1$ $[p]$.
D'autre part, $n^{p-1} = (n^2)^{(p-1)/2}$ (car p est impair) donc $n^{p-1} \equiv (-1)^{(p-1)/2}$ $[p]$. Or $p \equiv 3$ [4] donc $\dfrac{p-1}{2}$ est un entier impair, donc $(-1)^{(p-1)/2} = -1$, donc $n^{p-1} \equiv -1$ $[p]$.
On obtient donc $1 \equiv -1$ $[p]$, donc p divise 2 : contradiction car p est impair.
Conclusion : l'équation de Mordell $y^2 = x^3 - 5$ n'a pas de solutions.

Problème 2

Question 1) On essaye systématiquement les valeurs de x de 0 à 10 : on trouve $(x,y) = (0,1)$ et $(x,y) = (6,10)$.

Question 2) $x^2 + 2^x = y^2 \iff 2^x = y^2 - x^2 = (y-x)(y+x)$.

Le seul facteur premier de la décomposition primaire de 2^x est 2 donc il en va de même pour les décompositions primaires de $y - x$ et $y + x$, qui sont des diviseurs de 2^x.

Donc il existe $(\alpha, \beta) \in \mathbb{N}^2$ tel que $\left\{ \begin{array}{lcl} y - x & = & 2^\alpha \\ y + x & = & 2^\beta \end{array} \right.$, et pour avoir $2^x = 2^\alpha \times 2^\beta$, il faut bien sûr que $x = \alpha + \beta$.

Donc on obtient $x = 2^{\beta-1} - 2^{\alpha-1}$ et $y = 2^{\beta-1} + 2^{\alpha-1}$.

Puisque $x > 0$, il vient $\beta - 1 > \alpha - 1$ donc $\beta > \alpha$.

Question 3) Si $\alpha = 0$, alors $x = 2^{\beta-1} - \dfrac{1}{2}$ n'est pas un entier, donc $\alpha \geqslant 1$.

Puis on a aussi $x = \alpha + \beta = 2^{\beta-1} - 2^{\alpha-1}$, ce qui donne $2^{\beta-1} - \beta = 2^{\alpha-1} + \alpha$.

Question 4)

a) Pour tout $t \in \mathbb{R}$, $f(t) = e^{(t-1)\ln 2} - t$ donc f est dérivable sur $\mathbb{R}$.
Pour tout $t \in \mathbb{R}$, $f'(t) = \ln 2 \times 2^{t-1} - 1$ donc si $t \geqslant 3$, alors $\ln 2 \times 2^{t-1} \geqslant 4 \ln 2 > 1$ donc $f'(t) > 0$.
La fonction f est donc strictement croissante sur $[3, +\infty[$.

b) Si $\alpha = 1$, alors $2^{\beta-1} - \beta = 2$, c'est-à-dire $f(\beta) = 2$. Comme $\beta > \alpha$, on essaye avec $\beta = 2$: ça ne marche pas, puis avec $\beta = 3$, non plus, puis avec $\beta \geqslant 4$, on a $f(\beta) \geqslant f(4) = 5$. Conclusion : il n'existe aucune valeur de $\beta \in \mathbb{N}$ telle que $f(\beta) = 2$, d'où la contradiction.

Question 5) Puisque $\alpha \geqslant 2$, alors $\beta \geqslant 3$, donc $2^{\beta-1}$ et $2^{\alpha-1}$ sont pairs, donc x et y le sont aussi.

Et comme $x = \beta + \alpha$, on en déduit que α et β ont la même parité. Mais comme $\beta \geqslant \alpha + 1$ et que $\alpha + 1$ n'a pas la même parité que α, on en déduit que $\beta \geqslant \alpha + 2$.

Question 6)

a) On pose $g : t \mapsto 2^{t+1} - 2^{t-1} - 2t - 2$. g est dérivable sur $\mathbb{R}$ et pour tout $t \in \mathbb{R}$, $g'(t) = \ln 2(2^{t+1} - 2^{t-1}) - 2 = 3 \ln 2 \times 2^{t-1} - 2$.
Si $t \geqslant 3$, alors $g'(t) \geqslant 12 \ln 2 - 2 > 0$ donc g est strictement croissante sur $[3, +\infty[$.
Or $g(3) = 16 - 4 - 6 - 2 = 4 > 0$ donc pour tout $t \geqslant 3$, $g(t) > 0$, et comme $\alpha \geqslant 3$, on a donc $g(\alpha) > 0$, ce qu'on voulait montrer.

b) Comme $\beta \geqslant \alpha + 2 \geqslant 3$ et que f est croissante sur $[3, +\infty[$, on en déduit que $f(\beta) = 2^{\beta-1} - \beta \geqslant f(\alpha+2) = 2^{\alpha+1} - \alpha - 2 > 2^{\alpha-1} + \alpha$, ce qui contredit l'égalité de la question 3.

Question 7) Quand on cherche les solutions telles que $x > 0$, on voit que les cas $\alpha = 0$, $\alpha = 1$ et $\alpha \geqslant 3$ sont impossibles, il reste donc le cas $\alpha = 2$, qui donne l'équation $2^{\beta-1} - \beta = 4$, qui a pour seule solution $\beta = 4$ (unique solution car f est strictement croissante sur $[3, +\infty[$), autrement dit $x = 2^3 - 2^1 = 6$ et $y = 2^3 + 2^1 = 10$, c'est-à-dire la solution trouvée dans la question 1.

Conclusion : il y a exactement deux couples solutions qui sont ceux trouvés initialement.