Equations diophantiennes

Théo Lenoir

Déjà qu'est-ce qu'une équation diophantienne ? C'est une équation faisant intervenir des entiers. Souvent une équation diophantienne ressemble à ça : $2^x + z^2 = 3^y$ avec (x, y, z) entiers positifs. L'objectif est de trouver toutes les solutions (ou parfois de montrer qu'il y a en a une infinité). Pour cela, deux outils principaux : les factorisations et les modulos.

Quelques techniques :

1. Cela ne sert à rien de regarder une équation diophantienne modulo 6, puisque d'après le théorème des restes chinois, c'est la même chose que de la regarder modulo 2 et modulo 3. Il faut uniquement essayer de regarder modulo une puissance d'un nombre premier.
2. Souvent il est pratique de trouver les solutions (qui sont faciles à trouver car souvent les nombres solutions sont petits), en effet s'il y a une solution (par exemple dans l'équation initiale $(3, 1, 2)$ est solution), il ne peut y avoir de contradiction immédiate en regardant un modulo spécifique sans faire de supposition supplémentaire.
3. On aime avoir des carrés (ou des cubes) pour factoriser (car par exemple $z^2 - x^2 = (z - x)(z + x)$, pour cela si on a une facteur du type a^x, on essaie de regarder l'équation modulo quelque chose qui divise $a + 1$ pour montrer que x est pair, donc que a^x est un carré.
4. Souvent si on a un facteur a^x dans l'équation il est intéressant de regarder modulo un nombre premier qui divise a à une certaine puissance (plus grande que celle présente dans les solutions) : par exemple si on veut résoudre $2^z + 5 = 3^x$, on a une solution pour $z = 2$, $x = 3$, on peut donc regarder modulo 8, si $z \geqslant 3$, on a $3^x \equiv 5 \pmod 8$ ce qui est impossible car 3^x vaut 1 ou 3 modulo 8.
5. Quand on ne sait pas quoi faire, les modulos les plus utiles sont souvent $4, 8, 3$. Quand on ne sait pas quoi faire, ce n'est pas bête de regarder sur tous les modulos intéressants entre 1 et 10, c'est-à-dire $2, 3, 4, 5, 7, 8, 9$.
6. Quand il y a des carrés, regarder modulo 4 ou 8 est souvent très utile. Quand il y a des cubes, regarder modulo 7 ou 9 est souvent utile. De manière plus générale, quand il y a des cubes, il est utile de regarder modulo un nombre premier congru à 1 modulo 3 (par exemple 7 ou 13).
7. Quand il y a un facteur $n!$ dans l'équation, il faut souvent borner n. Souvent on peut prouver facilement que $n!$ ne peut pas être divisible par quelque chose et ceci donne une borne sur n. Il reste à traiter les autres cas à la main.
8. Souvent il est utile de factoriser par le pgcd pour simplifier l'équation. De plus, cela permet parfois d'obtenir une équation concernant des variables premières entre elles, ce qui est plus pratique pour regarder les divisibilités.
9. Parfois, les équations diophantiennes nécessitent des inégalités : quand on a des équations diophantiennes avec x, y, z à certaines puissances, souvent un des deux côtés de l'inégalité est bien trop grand lorsque x, y, z sont assez grands. Pour cela, souvent il est utile d'ordonner x, y, z et de borner chacun d'entre eux.

Exercice 1 Résoudre $x^2 + y^4 + 1 = 6^z$ où (x, y, z) sont des entiers positifs.

Exercice 2 Résoudre $3^x - 2^y = \pm 1$ pour x, y entiers positifs.

Exercice 3 Déterminer tous les quadruplets (a, b, c, k) d'entiers avec a, b, c des nombres premiers et k un entier strictement positif tels que $a^2 + b^2 + 16c^2 = 9k^2 + 1$

Exercice 4 Déterminer tous les couples d'entiers relatifs (m, n) tels que $m^5 - n^5 = 16mn$

Exercice 5 Déterminer tous les entiers n strictement positifs tels qu'il existe p premier tel que $p^n - (p - 1)^n$ soit une puissance de 3.

Exercice 6 Existe-il un triplet (a, b, p) d'entiers strictement positifs, avec p un nombre premier, tel que $a^3 - b^3 = 4p^2$?

Exercice 7 Déterminer tous les triplets (p, q, r) de nombres premiers tels que $3p^4 - 5q^4 - 4r^2 = 26$

Exercice 8 Déterminer tous les couples (x, n) d'entiers positifs tels que $3 \cdot 2^x + 4 = n^2$.

Exercice 9 Trouver les (p, m, n) avec p premier et m, n des entiers positifs tels que $p^m - n^3 = 27$.

Exercice 10 Trouver tous les quintuplets (a, b, c, d, n) d'entiers positifs tels que $a^2 + b^2 + c^2 + d^2 = 7 \cdot 4^n$.

Solution de l'exercice 1 On regarde modulo 8. Les carrés valent $0, 1$ ou 4, donc le terme de droite vaut $1, 2, 3, 5, 6$ mais pas 0. Donc $z \leqslant 2$.

Si $z = 0$, on a forcément $x = y = 0$ qui réciproquement convient.

Si $z = 1$, $x^2 + y^4 = 5$, comme $y^4 \leqslant 5$, on a $y < 2$ donc $y = 1$ et $x = 2$ qui réciproquement convient.

Si $z = 2$, $x^2 + y^4 = 35$ donc $y^4 \leqslant 35 < 81 = 3^4$ donc $y < 3$. Si $y = 0$, $x^2 = 35$ ce qui n'est pas possible. Si $y = 1$, $x^2 = 34$ ce qui n'est pas possible non plus. Si $y = 2$, $x^2 = 19$ ce qui n'est pas possible non plus. Il n'y a pas de solution.

Solution de l'exercice 2 Pour $y = 1$, $(1, 1)$ est solution, pour $y = 0$ il n'y a pas de solution. Sinon $y \geqslant 2$, en regardant modulo 4, on a $3^x \equiv 1 \pmod 4$ donc x est pair. En posant $x = 2t$, on a $(3^t - 1)(3^t + 1) = 2^y$. Le pgcd de $3^t - 1$ et $3^t + 1$ divise leur différence donc 2. Comme ceux-ci ont même parité et sont de produit pair, leur pgcd vaut 2. Comme $3^t - 1$ et $3^t + 1$ sont des puissances de 2 de pgcd 2, avec $3^t - 1 < 3^t + 1$, on a forcément $3^t - 1 = 2$, donc $t = 1$ donc $x = 2$. En particulier pour $x = 2$, $2^y = 8$ donc $y = 3$. Réciproquement $(2, 3)$ est solution. Les solutions sont donc $(1, 1)$ et $(2, 3)$

Solution de l'exercice 3 Un carré modulo 3 vaut 0 ou 1, et on a $1 \equiv a^2 + b^2 + c^2 \pmod 3$ donc parmi (a, b, c) deux sont divisibles par 3 donc deux valent trois. Par symétrie comme a, b jouent le même rôle on peut supposer $a = 3$. On a donc deux cas :

— Si $b = 3$, on a $9k^2 = 16c^2 + 17$ donc $(3k - 4c)(3k + 4c) = 17$. Comme $3k + 4c$ est positif et strictement supérieur à $3k - 4c$ et 17 est premier, on a $3k - 4c = 1$, $3k + 4c = 17$ donc en faisant la différence, $8c = 16$ donc $c = 2$. On obtient $3k = 9$ donc $k = 3$. Réciproquement, $(3, 3, 2, 3)$ convient car $9 + 9 + 64 = 1 + 81 = 1 + 9 \times 3^2$.

— Si $c = 3$, on a $9k^2 = b^2 + 152$ donc $(3k - b)(3k + b) = 152$. Or $152 = 8 \times 19$. On a donc comme $3k + b$ est positif et strictement plus grand que $3k - b$, on a $(3k - b, 3k + b) = (1, 152), (2, 76), (4, 38), (8, 19)$. On obtient en sommant $6k = 153, 78, 42, 27$, ce qui exclut en particulier le premier et le dernier couple. On a donc $k = 13$ dans le deuxième cas et $b = 37$ et dans le troisième cas $k = 7$ et $b = 17$. Réciproquement $(3, 17, 3, 7)$, $(17, 3, 3, 7)$, $(3, 37, 3, 13)$ et $(37, 3, 3, 13)$ conviennent car $3^2 + 17^2 + 16 \times 9 = 17 \times 9 + 17^2 = 17 \times 26 = 21^2 + 1 = 9 \times 7^2 + 1$ et car $9 + 16 \times 9 + 37^2 = 37^2 + 1 + 152 = 1 + 37^2 + 4 + 4 \times 37 = 1 + 39^2 = 1 + 9 \times 13^2$.

Les solutions sont donc $(3, 3, 2, 3)$, $(3, 17, 3, 7)$, $(17, 3, 3, 7)$, $(3, 37, 3, 13)$ et $(37, 3, 3, 13)$.

Solution de l'exercice 4 Si m ou n vaut 0, on a forcément $m = n = 0$ qui convient. Supposons désormais m et n non nuls. Ici le terme de gauche a l'air grand, significativement plus grand que celui de droite. Posons k le pgcd de n et m, soit a, b des entiers tels que $m = ka$, $n = kb$, on a $k^3(a^5 - b^5) = 16ab$. On sait que $a^5 - b^5$ divise $16ab$. On sait que $a^5 - b^5$ et a sont premiers entre eux. En effet soit p premier divisant $a^5 - b^5$ et a, p divise donc a^5, il divise donc b^5. On a donc p divise b, contradiction. De même $a^5 - b^5$ et b sont premiers entre eux, donc $a^5 - b^5$ divise 16 On sait que $2^5 - 1^5 = 31$. En particulier,

— Si $a > 0$ et $b > 0$ on a forcément $a^5 > b^5$ donc $a > b$. En particulier $a^5 - b^5 \geqslant (b+1)^5 - b^5 \geqslant 2^5 - 1^5 = 31$ (l'inégalité vient de la croissance de $(b + 1)^5 - b^5$, conséquence immédiate de la formule du binôme) ce qui contredit le fait que $a^5 - b^5$ divise 16 donc $|a^5 - b^5| \leqslant 16$.

— De même si $a < 0$ et $b < 0$ (on peut remplacer (a, b) par $(-b, -a)$ qui est solution de la même équation et à valeurs strictement positives.

En particulier on a a et b de signes différents, on a donc forcément $a^5 - b^5 < 0$, donc $b \geqslant 0$, $a \leqslant 0$. Si $b \geqslant 2$, $b^5 - a^5 \geqslant 2^5 = 32$ contradiction, donc $b = 1$. De même $a = -1$, l'équation se réécrit $k^3 = 8$ donc $k = 2$ donc $m = -2$, $n = 2$, qui réciproquement convient car $-32 - 32 = -364 = 16 \times (-2) \times (-2)$ L'ensemble des solutions est donc $\{(0, 0), (-2, 2)\}$

Solution de l'exercice 5 Notons que $n = 1$ est clairement solution (prendre $p = 2$). Supposons $n \geqslant 2$.

Notons que si p est premier par la factorisation classique de $x^n - y^n$, $p^n - (p-1)^n \geqslant p^{n-1} \geqslant 2$ donc ne peut valoir 1. Soit p premier tel que $p^n - (p-1)^n$ est une puissance de 3, on a donc 3 divise $p^n - (p-1)^n$. On ne peut donc pas avoir $p \equiv 0, 1 \pmod 3$, on a donc nécessairement $p \equiv 2 \pmod 3$.

Ainsi si n admet un diviseur premier q impair, $p^q - (p-1)^q$ divise $p^n - (p-1)^n$ donc c'est nécessairement une puissance de 3 (et elle ne peut pas valoir 1), or $p^q - (p-1)^q \equiv 2 - 1 = 1 \pmod 3$ contradiction. Ainsi n est une puissance de 2.

Si $n \geqslant 4$, on a 4 divise n, donc $p^2+(p-1)^2$ divise $p^4-(p-1)^4$ qui divise $p^n-(p-1)^n$ donc $p^2+(p-1)^2$ est une puissance de 3. Or $p^2+(p-1)^2 \equiv 1+1 \equiv 2 \pmod 3$ ce qui est impossible car c'est une puissance de 3 contradiction. On a donc $n=2$. Pour $n=2$ prendre $p=2$ convient, les entiers solutions sont donc 1 et 2.

Solution de l'exercice 6 Supposons qu'il existe a et b deux entiers strictement positifs et p un nombre premier tel que $a^3-b^3=4p^2$. Si $p>2$, notons que a et b sont premiers entre eux. Soit d leur pgcd, d^3 divise $4p^2$, qui ne contient aucun facteur cube dans sa décomposition en facteurs premiers, donc $d=1$.

Notons que a et b ne peuvent être de parité différente, sinon a^3 et b^3 sont de parité différente, donc a^3-b^3 est impair contradiction. De plus comme $a^3>b^3$, $a>b$.

Plaçons nous dans le cas où a et b sont premiers entre eux. Dans ce cas $(a-b)(a^2+ab+b^2)=4p^2$. Soit l le pgcd de $a-b$ et a^2+ab+b^2 et q un de ses facteurs premiers. q divise $a-b$ donc il divise $(a-b)^2=a^2-2ab+b^2$. Comme q divise a^2+ab+b^2, il divise $a^2+ab+b^2-(a^2-2ab+b^2)=3ab$. S'il divise a ou b comme il divise $a-b$, il divise a et b contradiction. Donc q étant premier avec a et b, il divise 3. En particulier l est une puissance de 3, et divise $4p^2$. Si $p\neq 3$, on obtient que $l=1$, donc les deux termes sont premiers entre eux. On a donc comme chaque facteur est positif, $(a-b, a^2+ab+b^2)=(1,4p^2),(4p^2,1),(4,p^2)$ ou $(p^2,4)$. On sait déjà que $a-b$ est pair donc on peut exclure la première et la seconde possibilité (la seconde est impossible si $p=2$ car les deux nombres ne seront pas premiers entre eux).

On a $a^2+ab+b^2 \geqslant 3$ donc la seconde est impossible. On a donc $a-b=4$ et $a^2+ab+b^2=p^2$. En particulier a et b sont impairs (sinon comme a et b sont de même parité, ils sont tous les deux pairs donc non premiers entre eux) et $a \equiv b \pmod 4$. Ainsi $p^2 \equiv 3a^2 \equiv 3 \pmod 4$ ce qui est impossible, un carré valant 0 ou 1 modulo 4, on aboutit à une absurdité.

Reste le cas où $p=3$ et le cas où $p=2$ mais a et b ne sont pas premiers entre eux.

— Si $p=3$, l est une puissance de 3. On a donc $(a-b, a^2+ab+b^2) = (1,4p^2),(4p^2,1),(4p,p),(p,4p),(4,p^2),(p^2,4)$. La première quatrième et sixième possibilité sont impossibles car a et b sont premiers entre eux. La seconde est impossible car $a^2+ab+b^2 \geqslant 3$. La troisième donne $a^2+ab+b^2=3$, donc on a égalité dans l'inégalité précédente. On a donc $a=b=1$, donc $4p^2=0$ contradiction. La cinquième se traite comme dans le paragraphe précédent (la preuve n'utilise pas que $p\neq 3$).

— Si $p=2$ et a et b ne sont pas premiers entre eux, on a d^3 qui divise 2^4. Comme $d\neq 1$, on a $d=2$. Soit a' et b' les deux entiers tels que $a=2a'$ et $b=2b'$. On a $8(a'^3-b'^3)=16$ donc $a'^3-b'^3=2$. On a alors $(a'-b')(a'^2+a'b'+b'^2)=2$, donc $a'^2+a'b'+b'^2$ divise 2, mais il vaut au moins 3 contradiction.

Dans tous les cas il n'y a pas de solutions, donc de tels (a,b,p) n'existent pas.

Solution de l'exercice 7 Regardons modulo 3, on a $q^4-r^2 \equiv 2 \pmod 3$. Or modulo 3 les carrés sont 0 ou 1, donc forcément $q^4 \equiv 0 \pmod 3$ et $r^2 \equiv 1 \pmod 3$. En particulier 3 divise q^4 donc 3 divise q donc $q=3$. L'équation devient $3p^4-4r^2=431$. Modulo 5, comme p^4 vaut 0 ou 1 par Petit Fermat, $3p^4$ vaut 0 ou 3. Or r^2 vaut $0,1$ ou -1 donc $-4r^2$ vaut 0 4 ou 1. Comme $431 \equiv 1 \pmod 5$, on a forcément $3p^4 \equiv 0 \pmod 5$ donc 5 divise $3p^4$ ou $-4r^2$ donc $p=5$. L'équation est équivalente à $1444=4r^2$ soit $r^2=361=19^2$ soit à $r=19$. donc $(p,q,r)=(5,3,19)$ est bien l'unique solution.

Solution de l'exercice 8 Pour $x=0$, l'équation devient $n^2=7$ qui n'a pas de solution. Supposons $x>0$, on factorise : $3\cdot 2^x=(n-2)(n+2)$. Les deux facteurs sont de même parité donc tous les deux pairs et on a deux cas :

Cas 1 : $3\cdot 2^a=n-2$ et $2^b=n+2$, ce qui se réécrit $2^b=3\cdot 2^a+4$. Regarder modulo 8 donne que a ou b est inférieur ou égal à 2. Comme $2^b>4$, on a $a\leqslant 2$, en testant chaque cas on obtient que $(a,b)=(2,4)$ donc $(x,n)=(6,14)$ qui est solution.

Cas 2 : $3\cdot 2^a=n+2$ et $2^b=n-2$, ce qui se réécrit $2^b+4=3\cdot 2^a$. Regarder modulo 8 donne que a ou b est inférieur ou égal à 2. En testant chaque cas on obtient que $(a,b)=(1,1),(2,3)$ donc $(x,n)=(2,4)$ ou $(5,10)$ qui sont solutions.

On peut aussi voir que les deux facteurs sont pairs, mais leur pgcd divisant 4, l'un est divisible par 4 au maximum, ce qui borne a ou b.

Solution de l'exercice 9 Notons que $p^m \geqslant 27$ donc $m\neq 0$. On réécrit $p^m=(3+n)(n^2-3n+9)$. Si p divise les deux facteurs, p divise donc $n^2-3n+9=(n+3)^2-9n$ donc p divise $9n$ donc p divise n ou 9. Mais si p divise n, p divise $n+3-n=3$, donc dans tous les cas $p=3$. Comme $m\geqslant 1$, n est divisible par 3, on pose $n=3k$ avec $k>0$, on a $3^m=27(1+k^3)$ donc $m\geqslant 3$ et $3^{m-3}=1+k^3=(k+1)(k^2-k+1)$. Notons d le pgcd de $k+1$ et k^2-k+1, d divise $k^2-k+1=(k+1)(k-2)+3$ donc d divise 3. En particulier, le pgcd vaut 1 ou 3. On ne peut avoir $k=1$ car sinon $k+1=2$ divise 3^{m-3}.

De plus notons qu'on a $k+1\leqslant k^2-k+1$ car cette inégalité est équivalente à $k^2-2k=k(k-2)\geqslant 0$. Comme $k+1$ et k^2-k+1 divisent 3^{n-3}, ce sont tous les deux des puissances de 3. En particulier, si le pgcd

vaut 1, on a forcément comme $k+1 \leqslant k^2-k+1$, $k+1=1$ donc $k=0$ ce qui est impossible. Si le pgcd vaut 3, on a $k+1=3$ donc $k=2$. De plus $3^{m-3}=k^3+1=9$ donc $m=5$ et $n=6$. Réciproquement le triplet $(3,5,6)$ est solution car $3^5-6^3=243-216=27$ donc $(3,5,6)$ est bien solution.

Si par contre p ne divise pas un des facteurs, comme $n+3$ et n^2-3n+9 divisent p^m, ce sont à signe près des puissances de p. En particulier l'une d'entre elles vaut ± 1. Or $n+3>1$ et $n^2-3n+9=n(n-3)+9>1$ si $n \geqslant 3$, et cette inégalité est encore vraie pour $n=0,1$ et 2. En particulier, aucun des facteurs ne vaut ± 1, contradiction.

Ainsi la seule solution est $(3,5,6)$.

Solution de l'exercice 10 Soit (a,b,c,d,n) un quintuplet solution. On ne peut avoir $a=b=c=d=0$, donc on peut définir k le pgcd de a,b,c,d. Posons $a=ka'$, $b=kb'$, $c=kc'$, $d=kd'$ avec a',b',c',d' premiers entre eux. On a $k^2(a'^2+b'^2+c'^2+d'^2))=7\times 4^n$. Ainsi d^2 divise 7×4^n, donc d est nécessairement une puissance de 2. Posons $d=2^k$, on a que 4^k divise 7×4^n donc $k \leqslant n$, et $a'^2+b'^2+c'^2+d'^2=7\times 4^{n-k}$.

Si $n-k \geqslant 2$, modulo 8 on a $a'^2+b'^2+c'^2+d'^2 \equiv 0 \pmod 8$. On a donc, comme un carré vaut $0,1,4$ mod 8, que soit tous les carrés valent 0, soit ils valent tous 4, soit deux valent 4 et deux 0. Ainsi a'^2,b'^2,c'^2,d'^2 sont pairs donc a',b',c',d' sont pairs ce qui contredit le fait qu'ils sont premiers entre eux. Ainsi on a $n-k=0$ ou 1.

Si $n-k=0$, on a $a'^2+b'^2+c'^2+d'^2=7$. En particulier $a'^2 \leqslant 7<9$ donc $0 \leqslant a'<3$, donc $a'=0,1$ ou 2. Idem pour b',c',d'. On voit que les seuls quadruplets (a',b',c',d') qui conviennent sont ceux de la forme $(2,1,1,1)$. On a donc $(a,b,c,d,n)=(2^{k+1},2^k,2^k,2^k,k)$ (à permutations près pour (a,b,c,d). On vérifie aisément que ceux-ci sont solution.

Si $n-k=1$, on a $a'^2+b'^2+c'^2+d'^2=28$. Quitte à réarranger a',b',c',d', on a $a' \leqslant b' \leqslant c' \leqslant d'$. On a donc $d'^2 \leqslant 28$ donc $d' \leqslant 4$. De plus $28 \leqslant 4d'^2$, donc $d'^2 \geqslant 7$, donc $d' \geqslant 3$. Si $d'=4$ $a'^2+b'^2+c'^2=12$. En regardant mod 4, comme un carré vaut 0 ou 1, on obtient que a',b',c' sont pairs, ce qui contredit le fait qu'ils sont premiers entre eux. Si $d'=3$, on obtient $a'^2+b'^2+c'^2=19$. Ainsi $19 \leqslant 3c'^2$ donc $c' \geqslant 3$. Or $c' \leqslant d'=3$, donc $c'=3$, on obtient $a'^2+b'^2=10$. Les carrés inférieurs à 10 valant $0,1,4,9$, la seule possibilité est $b'=3$ et $a'=1$. On a donc un quintuplet de la forme $(a,b,c,d,n)=(2^k,3\times 2^k,3\times 2^k,3\times 2^k,k+1)$. Réciproquement ces quintuplets sont solution.

Les quintuplets solutions sont les quintuplets de la forme $(a,b,c,d,n)=(2^k,3\times 2^k,3\times 2^k,3\times 2^k,k+1)$ et $(a,b,c,d,n)=(2^{k+1},2^k,2^k,2^k,k)$ à permutation près de (a,b,c,d).