

Equations Diophantiennes

Mots clés : Géométrie plane, Theorème de Ceva, Theorème de Menelaus, Point de Nagel, Point de Gergonne.

On appelle *équation diophantienne* une équation de la forme

$$f(x_1, x_2, \dots, x_n) = 0, \quad (1)$$

où f est une fonction à n variables, avec $n \geq 2$. Si f est un polynôme à coefficients entiers, on dit que (1) est une équation algébrique diophantienne.

Un n -uplet $(x_1^0, x_2^0, \dots, x_n^0) \in \mathbb{Z}^n$ vérifiant (1) est dit *solution* de l'équation. En théorie des équations diophantiennes, trois principales questions se posent :

1. Existe-t-il une ou plusieurs solutions ?
2. Le nombre de solutions est-t-il fini ou infini ?
3. Déterminer toutes les solutions.

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.
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 un 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 $z \geq 3$, 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 modulus 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 modulus 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 l'équation suivante dans $\mathbb{Z}^2$

$$x^2 - y^2 - x + 3y = 30. \quad (2)$$

On multiplie l'équation par 4

$$4x^2 - 4x - 4y^2 + 12y = 120$$

et on complète les carrés

$$(2x - 1)^2 - 1 - [(2y - 3)^2 - 9] = 120 \iff (2x - 1)^2 - (2y - 3)^2 = 112.$$

Posons $a = 2x - 1$ et $b = 2y - 3$, deux entiers impairs. Alors

$$(a - b)(a + b)^2 = 112.$$

et on a que $a - b$, $a + b$ sont pairs. Donc, il existe $k, k' \in \mathbb{Z}$ tel que $a - b = 2k$ et $a + b = 2k'$, ainsi que

$$a = k + k', \quad b = k' - k \quad \text{et} \quad kk' = 28.$$

Comme a est impair, k et k' sont de parités opposées. Les couples (k, k') possibles sont donc $(1, 28), (28, 1), (4, 7), (7, 4)$ et leurs opposés. Les couples $(2, 14)$ et $(14, 2)$ sont de même parité, et donc ils sont exclus. On a

$$x = \frac{a + 1}{2} \quad \text{et} \quad y = \frac{b + 3}{2}$$

Donc on obtient les solutions suivantes

(k, k')	$(1, 28)$	$(28, 1)$	$(4, 7)$	$(7, 4)$
(x, y)	$(15, 15)$	$(15, -12)$	$(6, 3)$	$(6, 0)$

Ainsi que

(k, k')	$(-1, -28)$	$(-28, -1)$	$(-4, -7)$	$(-7, -4)$
(x, y)	$(-14, -12)$	$(-14, 15)$	$(-5, 0)$	$(-5, 3)$

Exercice 2 : Soit x un entier strictement positif tel que $x + 100$ est un carré parfait, et $x + 168$ est un autre carré parfait. Déterminer toutes les valeurs possibles de x .

Soit $a, b \geq 0$ tels que $x + 100 = a^2$ et $x + 168 = b^2$. Alors

$$b^2 - a^2 = 68 = (b - a)(b + a).$$

Les deux facteurs ont la même parité et leur produit est pair, donc ils sont pairs. Comme $68 = 2 \cdot 34$ (et $1 \cdot 68, 4 \cdot 17$ sont de parités différentes), on obtient

$$b - a = 2 \quad \text{et} \quad b + a = 34$$

Soit

$$b = 18 \quad a = 16$$

D'où

$$x = 16^2 - 100 = 156 \quad (\text{et } 156 + 168 = 324 = 18^2).$$

Exercice 3 : (Allemagne) Déterminer les nombres premiers p tels que le système d'équations

$$\begin{cases} p+1 = 2x^2 \\ p^2+1 = 2y^2 \end{cases} \quad (3)$$

admet une solution entière (x, y) . On peut supposer $x, y \geq 0$ (en fait > 0). Comme $p+1 = 2x^2$, on exclut le cas où $p = 2$ car $3 = 2x^2$ est impossible. En soustrayant

$$2y^2 - 2x^2 = p^2 - p \iff (y-x)(y+x) = \frac{p(p-1)}{2} > 0.$$

Donc $y > x$. D'autre part $2y^2 = p^2 + 1 < 2p^2$, donc $y < p$, et

$$0 < y - x < p$$

Donc on en déduit que le nombre premier p divise $(y-x)(y+x)$ mais ne divise pas $y-x$, donc

$$p \mid y+x$$

Comme $0 < x+y < 2p$, on a $x+y = p$. Alors

$$y-x = \frac{p-1}{2}, \quad x = \frac{p+1}{4}.$$

En reportant dans $2x^2 = p+1$ on obtient

$$\frac{(p+1)^2}{8} = p+1 \iff p+1 = 8 \iff p = 7.$$

Réciproquement, $p = 7$ convient car $7+1 = 2 \cdot 2^2$ et $7^2+1 = 2 \cdot 5^2$.

Exercice 4 : (Russie) Déterminer les paires (p, q) de nombres premiers telles que :

$$p^3 - q^5 = (p+q)^2. \quad (4)$$

Supposons $p, q \neq 3$. Par Fermat,

$$p^3 \equiv p \pmod{3}$$

et

$$q^5 = q^3 q^2 \equiv q \cdot q^2 = q^3 \equiv q \pmod{3}$$

L'équation donne

$$p - q \equiv (p+q)^2 \pmod{3}, \quad \text{avec } p, q \in \{1, 2\} \pmod{3}$$

Étudions les possibilités suivantes

1. Si $p \equiv q$, le membre de gauche vaut 0, mais $p+q \equiv 2p \not\equiv 0$, donc $(p+q)^2 \equiv 1$
2. Si $p \equiv 1$ et $q \equiv 2$ alors $p - q \equiv 2$ mais $p+q \equiv 0$, donc $(p+q)^2 \equiv 0$
3. Si $p \equiv 2$ et $q \equiv 1$ alors $p - q \equiv 1$ mais $(p+q)^2 \equiv 0$.

Aucun cas n'est possible, donc $p = 3$ ou $q = 3$.

1. Cas $p = 3$: On a $27 - q^5 = (3+q)^2 > 0$, donc $q^5 < 27$, ce qui donne $q = 2$, mais $27 - 32 < 0$. Impossible.

2. Cas $q = 3$: On a $p^3 - 243 = (p + 3)^2$, soit $p^3 - p^2 - 6p - 252 = 0$, soit

$$(p - 7)(p^2 + 6p + 36) = 0.$$

Comme $p^2 + 6p + 36 > 0$, on a $p = 7$. On vérifie bien que $343 - 243 = 100 = 10^2$.

Exercice 5 : Résoudre $3^x - 2^y = 1$ pour tout x, y entiers positifs.

Si $y = 1$, alors $3^x = 3$ et $x = 1$: $(1, 1)$ est solution. Si $y \geq 2$, on regarde modulo 4

$$3^x \equiv 1 \pmod{4}$$

donc x est pair, alors il existe un $k \in \mathbb{Z}$ tel que $x = 2k$. Donc

$$3^{2k} - 1 = 2^y \iff (3^k - 1)(3^k + 1) = 2^y.$$

Les deux facteurs sont des puissances de 2 qui diffèrent de 2. Si $2^a < 2^b$ avec $2^b - 2^a = 2$, alors $2^a(2^{b-a} - 1) = 2$, d'où

$$a = 1 \quad \text{et} \quad b = 2$$

Donc

$$3^k - 1 = 2 \quad \text{et} \quad 3^k + 1 = 4$$

d'où

$$k = 1 \quad x = 2 \quad y = 3$$

L'ensemble des solutions $\{(x, y) \in \{(1, 1), (2, 3)\}\}$.

Exercice 6 : (JBMO SL 2022) Déterminer toutes les paires (k, n) d'entiers positifs tel que

$$1! + 2! + \dots + k! = 1 + 2 + \dots + n.$$

On note $S_k = 1! + 2! + \dots + k!$ and $T_n = \frac{n(n+1)}{2}$. Petit calcul on trouve $S_1 = 1$, $S_2 = 3$, $S_3 = 9$, $S_4 = 33$, $S_5 = 153$. De même $T_1 = 1$, $T_2 = 3$, $T_3 = 6$, $T_4 = 10$, $T_5 = 15$, $T_6 = 21$, $T_7 = 28$, $T_8 = 36$. On remarque

1. $S_1 = 1 = T_1$ donc $(k, n) = (1, 1)$
2. $S_2 = 3 = T_2$ donc $(k, n) = (2, 2)$
3. $S_3 = 9$ et $S_4 = 33$ ne sont pas triangulaires (9 est entre $T_3 = 6$ et $T_4 = 10$ et 33 est entre $T_7 = 28$ et $T_8 = 36$);
4. $S_5 = 153 = \frac{17 \cdot 18}{2}$ donc $(k, n) = (5, 17)$.
5. Cas $k \geq 6$, on regarde modulo 7. On a $n! \equiv 0$ pour $n \geq 7$, donc

$$S_k \equiv S_6 = 873 = 7 \cdot 124 + 5 \equiv 5 \pmod{7}.$$

Or les nombres triangulaires $\frac{n(n+1)}{2}$ modulo 7 valent, pour $n \equiv 0, 1, \dots, 6$: 0, 1, 3, 6, 3, 1, 0. Ils ne prennent jamais la valeur 5 modulo 7. Donc il n'y a pas de solution pour $k \geq 6$.

L'ensemble de solutions : $(k, n) \in \{(1, 1), (2, 2), (5, 17)\}$.

Exercice 7 : (JBMO 2019) Résoudre $45^x - 6^y = 2019^z$ pour tout x, y, z entiers positifs.

On a $2019 = 3 \cdot 673$. L'équation s'écrit

$$3^{2x}5^x - 2^y3^y = 3^z673^z.$$

1. Cas $2x < y$. Alors $3^{2x}(5^x - 2^y3^{y-2x}) = 3^z673^z$. Le crochet n'est pas divisible par 3 (car $3 \nmid 5^x$), donc $z = 2x$ et $5^x - 2^y3^{y-2x} = 673^{2x}$. Or le membre de gauche est $< 5^x < 673^{2x}$. Contradiction.

2. Cas $2x = y$. Alors $9^x(5^x - 4^x) = 3^z 673^z$, d'où $z \geq 2x$ et $5^x - 4^x = 3^{z-2x} 673^z \geq 673^z \geq 673^{2x} > 5^x$. Contradiction.
3. Cas $2x > y$. Alors $3^y(3^{2x-y} 5^x - 2^y) = 3^z 673^z$ et le crochet n'est pas divisible par 3, donc $z = y$ et

$$3^{2x-y} 5^x = 673^y + 2^y.$$

Le membre de gauche est divisible par 5 (car $x \geq 1$) et par 3. On a $673 \equiv 3 \pmod{5}$, donc $3^y \equiv -2^y \pmod{5}$, c'est-à-dire $(3 \cdot 3)^y \equiv 4^y \equiv -1$, ce qui impose y impair. On utilise le lemme de l'exposant (y impair, $3, 5 \nmid 673 \cdot 2$) avec $673 + 2 = 675 = 3^3 \cdot 5^2$:

$$v_3(673^y + 2^y) = 3 + v_3(y), \quad v_5(673^y + 2^y) = 2 + v_5(y).$$

Comme $673^y + 2^y = 3^{2x-y} 5^x$ n'a que 3 et 5 pour facteurs premiers,

$$673^y < 673^y + 2^y = 3^{3+v_3(y)} 5^{2+v_5(y)} \leq 675 y^2.$$

Pour $y \geq 2$, $673^y > 675 y^2$ (c'est vrai pour $y = 2$, et le rapport $673^y/y^2$ est croissant). Donc $y = 1$, $z = 1$, et $3^{2x-1} 5^x = 675 = 3^3 \cdot 5^2$ donne $x = 2$. On vérifie qu'on a bien $45^2 - 6 = 2025 - 6 = 2019$.

L'ensemble de solutions : $(x, y, z) = (2, 1, 1)$.

Exercice 8 : (JBMO 2015) Trouver tous les a, b, c, k avec a, b, c des nombres premiers et k un entier positif tel que $a^2 + b^2 + 16c^2 = 9k^2 + 1$.

On a

$$16c^2 \equiv c^2 \pmod{3} \quad \text{et} \quad 9k^2 + 1 \equiv 1 \pmod{3}$$

donc

$$a^2 + b^2 + c^2 \equiv 1 \pmod{3}$$

Le carré d'un premier vaut 0 modulo 3 s'il est égal à 3, et 1 sinon. Le nombre de premiers parmi a, b, c différents de 3 est donc $\equiv 1 \pmod{3}$, donc égal à 1. Deux des trois premiers valent 3.

1. Cas $a = b = 3$. On a $18 + 16c^2 = 9k^2 + 1$, soit $(3k - 4c)(3k + 4c) = 17$. Donc $3k - 4c = 1$ et $3k + 4c = 17$, d'où $k = 3$ et $c = 2$.
2. Cas $a = c = 3$. On a $9 + b^2 + 144 = 9k^2 + 1$, soit $(3k - b)(3k + b) = 152 = 2^3 \cdot 19$. Les facteurs ont même parité, donc $(3k - b, 3k + b) \in \{(2, 76), (4, 38)\}$:

$$(2, 76) : 3k = 39, k = 13, b = 37; \quad (4, 38) : 3k = 21, k = 7, b = 17.$$

Les nombres 37 et 17 sont premiers.

3. Cas $b = c = 3$. Symétrique du précédent, avec $a = 37$ ou $a = 17$.

L'ensemble des solutions :

$$(a, b, c, k) \in \{(3, 3, 2, 3), (3, 37, 3, 13), (37, 3, 3, 13), (3, 17, 3, 7), (17, 3, 3, 7)\}$$

Exercice 9 : (JBMO 2020) Déterminer s'il existe un entier naturel n tel que $8^n + 47$ est un nombre premier.

On distingue trois cas, selon n modulo 4.

1. Si n pair, on a $8^n \equiv (-1)^n \equiv 1 \pmod{3}$ et $47 \equiv 2$, donc $3 \nmid 8^n + 47$.
2. Si $n \equiv 1 \pmod{4}$ on a $8^n \equiv 3^n \equiv 3 \pmod{5}$ (car $3^4 \equiv 1$) et $47 \equiv 2$, donc $5 \nmid 8^n + 47$.
3. Si $n \equiv 3 \pmod{4}$ on a $8^2 = 64 \equiv -1 \pmod{13}$, donc $8^4 \equiv 1$ et $8^n \equiv 8^3 \equiv 5 \pmod{13}$. Comme $47 \equiv 8 \pmod{13}$, $13 \mid 8^n + 47$.

Dans tous les cas $8^n + 47$ est divisible par 3, 5 ou 13 et est strictement supérieur à 13, donc il est composé. Il n'existe aucun tel n .

Exercice 10 : (JBMO 2023) Trouvez toutes les paires (a, b) d'entiers positifs tels que $a! + b$ et $b! + a$ sont tous deux des puissances de 5.

Le problème est symétrique, on suppose $a \leq b$.

1. Cas $a = b$. On a $a! + a = a((a-1)! + 1) = 5^k$, donc $a = 5^i$ et $(a-1)! + 1$ est une puissance de 5.
 (a) $a = 1 : 1! + 1 = 2$, non.
 (b) $a = 5 : 5 \cdot 25 = 125 = 5^3$, oui.
 (c) $a = 5^i$ avec $i \geq 2 : (a-1)!$ est divisible par 5, donc $(a-1)! + 1 \equiv 1 \pmod{5}$ est une puissance de 5 strictement supérieure à 1 : impossible.

On obtient $(5, 5)$.

2. Cas $a < b \leq 4$. On teste : $(1, 2) : 3$, non ; $(1, 3) : 4$, non ; $(1, 4) : 1! + 4 = 5$ et $4! + 1 = 25$, oui ; $(2, 3) : 3! + 2 = 8$, non ; $(2, 4) : 2! + 4 = 6$, non ; $(3, 4) : 3! + 4 = 10$, non.
3. Cas $a < b$ et $b \geq 5$. Montrons que c'est impossible. Comme $b! + a > 1$ est une puissance de 5 et $5 \mid b!$, on a $5 \mid a$, donc $a \geq 5$. Comme $a! + b > 1$ est une puissance de 5 et $5 \mid a!$, on a $5 \mid b$. Deux sous-cas :
 (a) $a \geq 10$ (multiple de 5 avec $a \geq 6$) : $v_5(a!) = v_5(a) + v_5((a-1)!) \geq v_5(a) + 1$, donc $v_5(b!) \geq v_5(a!) > v_5(a)$.
 (b) $a = 5$: alors $5 \mid b$ et $b > 5$ donne $b \geq 10$, donc $v_5(b!) \geq 2 > 1 = v_5(a)$.
 Dans les deux cas $v_5(b!) > v_5(a)$, donc $v_5(b! + a) = v_5(a)$ et $b! + a = 5^{v_5(a)} \leq a$, ce qui est absurde car $b! + a > a$.

L'ensemble de solutions : $(a, b) \in \{(1, 4), (4, 1), (5, 5)\}$.

Exercice 11 : Déterminer les nombres premiers p pour lesquels $\frac{2^{p-1}-1}{p}$ est un carré parfait.

Pour $p = 2$, $\frac{2-1}{2}$ n'est pas entier. Soit p impair, il existe un $k \geq 1$ tel que $p-1 = 2k$ et $2^{p-1} - 1 = p a^2$. Donc

$$(2^k - 1)(2^k + 1) = p a^2.$$

Les facteurs $2^k - 1$ et $2^k + 1$ sont impairs et diffèrent de 2, donc sont premiers entre eux. Le premier p divise l'un des deux, et alors l'un des facteurs est un carré, l'autre étant p fois un carré. Deux cas sont possibles

1. Si $2^k + 1 = b^2$. Alors $2^k = (b-1)(b+1)$, deux puissances de 2 qui diffèrent de 2, donc $b-1 = 2$, $b+1 = 4$, $k = 3$ et $p = 7$. On vérifie qu'on a bien $\frac{2^6-1}{7} = 9 = 3^2$.
2. Si $2^k - 1 = b^2$. Pour $k \geq 2$, $2^k - 1 \equiv 3 \pmod{4}$ n'est pas un carré. Donc $k = 1$, $p = 3$. On vérifie qu'on a bien $\frac{2^2-1}{3} = 1 = 1^2$.

L'ensemble de solutions est $p \in \{3, 7\}$.

Exercice 12 : Trouver les (p, m, n) avec p premier et m, n des entiers positifs tels que $p^m - n^3 = 27$. On a

$$p^m = n^3 + 27 = (n+3)(n^2 - 3n + 9)$$

Les deux facteurs sont des puissances de p , avec $n+3 \geq 4$. De plus,

$$n^2 - 3n + 9 - (n+3) = n^2 - 4n + 6 = (n-2)^2 + 2 > 0,$$

donc $n+3$ est la plus petite des deux puissances, et divise l'autre

$$n+3 \mid n^2 - 3n + 9$$

Or

$$n^2 - 3n + 9 = (n+3)(n-6) + 27,$$

donc $n+3 \mid 27$. Avec $n+3 \geq 4$, on a $n+3 \in \{9, 27\}$.

1. Si $n = 6$ alors $6^3 + 27 = 243 = 3^5$. Convient avec $p = 3$, $m = 5$.

2. Si $n = 24$: $24^3 + 27 = 13851 = 3^6 \cdot 19$ n'est pas une puissance de premier.

L'ensemble de solutions est $(p, m, n) = (3, 5, 6)$.