3. Equacions diofàntiques

Rep en general el nom d'*equació diofàntica* tota aquella equació les solucions de la qual es busquen entre els nombres enters.

El nom d'equació diofàntica fa honor al matemàtic Diofant qui, a Alexandria, a mitjans del segle III a.C., va treballar molts problemes relacionats amb la Teoria de Nombres. En particular, es coneix que ja utilitzava un símbol similar a la x per a designar la incògnita en les equacions.

L'EQUACIÓ LINEAL AMB DUES INCÒGNITES

Una equació diofàntica lineal amb dues incògnites és una expressió del tipus

$$\boxed{a\,x + b\,y = n} \tag{1}$$

on x, y són les incògnites i a, b, n són nombres enters coneguts que suposarem diferents a zero.

Propietat La condició necessària i suficient per tal que l'equació (1) tingui solució entera és que d màxim comú divisor dels coeficients a i b divideixi el terme independent n.

$$a\,x + b\,y = n \;\; (a, b, n \in \mathbb{Z}^*) \;\text{ té solució en } \mathbb{Z} \;\Leftrightarrow\; mcd(a,\, b)|n$$

($\Rightarrow$) Si l'equació (1) té solució en $\mathbb{Z}$, existeixen dos nombres x_0, $y_0 \in \mathbb{Z}$ tals que $a\,x_0 + b\,y_0 = n$.

Si $d = mcd(a,\, b)$ llavors $d|a\,x_0$ i $d|b\,y_0$, per tant $d|n$.

($\Rightarrow$) Suposem ara que $d|n$. Per la identitat de Bezout, existeixen dos nombres enters x_1, y_1 tals que $a\,x_1 + b\,y_1 = d$.

Si multipliquem ambdós membres per n/d:

$$a\,x_1\frac{n}{d} + b\,y_1\frac{n}{d} = d\frac{n}{d} = n.$$

Hem obtingut una solució per a l'equació (1) donada per

$$\boxed{x_0 = x_1 \frac{n}{d}, \quad y_0 = y_1 \frac{n}{d}.}$$

Els nombres x_0, y_0 són enters ja que el quocient n/d és un enter en ser d divisor de n.

Exemple Obtenir una solució entera de l'equació $17\,x + 14\,y = 302$.

En primer lloc comprovem si té o no solució.

Com que és $mcd(17,\, 14) = 1$ i $1|302$, sí té solució. Per tal d'obtenir-la de manera efectiva hem d'escriure el mcd 1 com a combinació lineal entera de 17 i 14. Segons l'algorisme d'Euclides:

	1	4	1	2
17	14	3	2	1
3	2	**1**	0	

$$\left.\begin{array}{r} 17 = 14 \cdot 1 + 3 \\ 14 = 3 \cdot 4 + 2 \\ 3 = 2 \cdot 1 + 1 \end{array}\right\} \Rightarrow \left.\begin{array}{r} 3 = 17 + 14 \cdot (-1) \\ 2 = 14 + 3 \cdot (-4) \\ 1 = 3 + 2 \cdot (-1) \end{array}\right\}.$$

Substituint a l'última expressió el residu anterior i després el primer residu,

$$1 = 3 + [14 + 3 \cdot (-4)] \cdot (-1) = 14 \cdot (-1) + 3 \cdot 5 = 14 \cdot (-1) + [17 + 14 \cdot (-1)] \cdot 5,$$

s'arriba a l'expressió per al $mcd(17,\, 14)$: $1 = 17 \cdot 5 + 14 \cdot (-6)$.

Ara és senzill obtenir una solució de l'equació diofàntica de l'enunciat. Comparem amb l'expressió obtinguda per al $mcd(17,\, 14)$:

$$\left.\begin{array}{r} 17\,x + 14\,y = 302 \\ 17 \cdot 5 + 14 \cdot (-6) = 1 \end{array}\right\}.$$

Tal i com estableix la propietat anterior, només cal multiplicar els coeficients de la combinació lineal entera per $n = 302$ i dividir per $d = mcd(17,\, 14) = 1$ fins a obtenir una solució de l'equació diofàntica:

$$x_0 = 5\,\frac{302}{1}, \quad y_0 = -6\,\frac{302}{1} \quad \Rightarrow \quad (x_0,\, y_0) = (1510,\, -1812).$$

Exemple Obtenir una solució entera de l'equació $14\,x + 12\,y = 15$.

En aquest cas $mcd(14,\, 12) = 2$ però $2 \not| 15$; l'equació proposada no té cap solució en els enters.

Propietat Si $d = mcd(a,\, b)$ divideix n, la solució general de l'equació diofàntica lineal (1), $a\,x + b\,y = n$, resulta ser

$$\boxed{(x,\, y) = \Big(x_0 + \frac{b\,t}{d}\,,\, y_0 - \frac{a\,t}{d}\Big) \quad \forall\, t \in \mathbb{Z},}$$

on $(x_0,\, y_0)$ és una solució particular de l'equació (1) obtinguda segons la propietat anterior.

Demostració. És fàcil comprovar que totes les parelles de nombres enters de l'enunciat verifiquen l'equació (1). Substituint:

$$a\Big(x_0 + \frac{b\,t}{d}\Big) + b\Big(y_0 - \frac{a\,t}{d}\Big) = a\,x_0 + \frac{a\,b\,t}{d} + b\,y_0 - \frac{a\,b\,t}{d} = a\,x_0 + b\,y_0 = n,$$

on l'última igualtat és deguda a que $(x_0,\, y_0)$ és solució particular de (1).

Provem ara que totes les solucions de (1) són com estableix l'enunciat. Per ser $(x_0,\, y_0)$ solució particular, $a\,x_0 + b\,y_0 = n$.

Si dividim per $d = mcd(a,\, b)$, l'equació es transforma en

$$\frac{a}{d}\,x_0 + \frac{b}{d}\,y_0 = \frac{n}{d},$$

on ara $mcd(a/d,\, b/d) = 1$, és a dir, a/d y b/d són primers entre sí.

Qualsevol altra solució $(x_1,\, y_1)$ de l'equació (1) verifica

$$\frac{a}{d}\,x_1 + \frac{b}{d}\,y_1 = \frac{n}{d}.$$

Restant les dues últimes igualtats:

$$\frac{a}{d}\,(x_1 - x_0) + \frac{b}{d}\,(y_1 - y_0) = 0,$$

$$\frac{a}{d}\,(x_1 - x_0) = \frac{b}{d}\,(y_0 - y_1).$$

El nombre enter a/d divideix el producte del membre de la dreta. Com que a/d i b/d són primers entre sí, pel Lema d'Euclides, a/d divideix $y_0 - y_1$:

$$y_0 - y_1 = \frac{a}{d}\,t \quad \text{amb } t \in \mathbb{Z} \quad \Rightarrow \quad y_1 = y_0 - \frac{a\,t}{d}\,, \quad t \in \mathbb{Z}.$$

Un cop s'ha determinat que $y_0 - y_1$ és igual a $a\,t/d$, substituïm a la igualtat anterior:

$$\frac{a}{d}\,(x_1 - x_0) = \frac{b}{d}\,\frac{a\,t}{d} \quad \Rightarrow \quad x_1 - x_0 = \frac{b\,t}{d} \quad \Rightarrow \quad x_1 = x_0 + \frac{b\,t}{d}\,, \quad t \in \mathbb{Z}.$$

Exemple Resoldre en $\mathbb{Z}$ l'equació $17\,x + 14\,y = 302$.

Ja havíem determinat una solució particular $(x_0,\, y_0) = (1510,\, -1812)$.

Per tal de determinar totes les solucions enteres utilitzem el resultat de la propietat anterior. L'equació $a\,x + b\,y = n$ $(a, b, n \in \mathbb{Z}^*)$ té com a solució general

$$(x,\, y) = \left(x_0 + \frac{b\,t}{d}\,,\, y_0 - \frac{a\,t}{d}\right) \quad \forall t \in \mathbb{Z},$$

on $d = mcd(a,\, b)$ i $(x_0,\, y_0)$ és una solució particular. La solució només existeix en el supòsit en el qual $d|n$.

En el nostre cas $d = 1$ i la solució general és

$$(x,\, y) = (\,1510 + 14\,t\,,\, -1812 - 17\,t\,) \quad \forall\, t \in \mathbb{Z}.$$

Exemple Resoldre l'equació diofàntica lineal $525\,x + 100\,y = 50$.

En primer lloc comprovem si té o no solució en $\mathbb{Z}$. En ser $25 = mcd(525,\, 100)$ i $25|50$ podem afirmar que sí té solució entera.

► A l'equació $a\,x + b\,y = n$ $(a, b, n \in \mathbb{Z}^*)$ si $d = mcd(a,\, b)$ compleix $d|n$ i a més a més $d \neq 1$, podem simplificar dividint ambdós membres per d. Obtenim així una equació diofàntica més senzilla amb les mateixes solucions. Ara el mcd dels nous coeficients de x i y és 1.

Apliquem en el nostre cas la simplificació per 25 obtenint la nova equació

$$21\,x + 4\,y = 2.$$

Ara $1 = mcd(21,\, 4)$ pot ser escrit com a combinació lineal entera considerant la divisió de 21 entre 4:

$$21 = 4 \cdot 5 + 1 \quad \Rightarrow \quad 21 \cdot 1 + 4 \cdot (-5) = 1.$$

A partir dels coeficients de la combinació lineal $(1,\, -5)$ pot obtenir-se una solució particular multiplicant pel terme independent 2:

$$(x_0,\, y_0) = (2,\, -10).$$

La solució general és

$$(x,\, y) = (\,2 + 4\,t\,,\, -10 - 21\,t\,) \quad \forall\, t \in \mathbb{Z}.$$

Problema En una sala de reunions es disposa de taules de dos tipus, unes *grans* per a 16 persones i altres *petites* per a 10 persones. Suposant que el nombre de persones assistents a un acte és de 232 i que es vol tenir totes les taules completes, ¿quantes taules de cada tipus s'han d'utilitzar?

El plantejament d'aquesta situació correspon a una equació diofàntica lineal amb dues incògnites. Suposem que x és el nombre de taules grans i y el de petites. Per les condicions de l'enunciat

$$16\,x + 10\,y = 232.$$

Comprovem que existeix solució: $mcd(16,\,10) = 2$ i $2|232$.

Simplifiquem l'equació dividint ambdós membres per 2:

$$8\,x + 5\,y = 116.$$

Com que $mcd(8,\,5) = 1$ hem d'escriure el nombre 1 com a combinació lineal entera de 8 i 5.

	1	1	1	2
8	5	3	2	1
3	2	**1**	0	

$$\left.\begin{array}{l} 8 = 5\cdot 1 + 3 \\ 5 = 3\cdot 1 + 2 \\ 3 = 2\cdot 1 + 1 \end{array}\right\} \Rightarrow \left.\begin{array}{l} 3 = 8 + 5\cdot(-1) \\ 2 = 5 + 3\cdot(-1) \\ 1 = 3 + 2\cdot(-1) \end{array}\right\};$$

$$1 = 3 + [5 + 3\cdot(-1)]\,(-1) = 5\cdot(-1) + 3\cdot 2 = 5\cdot(-1) + [8 + 5\cdot(-1)]\cdot 2.$$

Llavors,

$$8\cdot 2 + 5\cdot(-3) = 1,$$

de manera que una solució particular de l'equació és :

$$(x_0,\,y_0) = (\,232,\,-348\,).$$

La solució general resulta ser

$$(x,\,y) = (\,232 + 5\,t\,,\,-348 - 8\,t\,) \quad \forall\, t \in \mathbb{Z}.$$

La naturalesa del problema imposa certes condicions sobre els valors enters de la solució general. En aquest cas, s'ha d'exigir que les incògnites x i y siguin no negatives.

$$\left.\begin{array}{r} 232 + 5\,t \geq 0 \\ -348 - 8\,t \geq 0 \end{array}\right\} \Rightarrow \left.\begin{array}{l} t \geq -232/5 \\ t \leq -348/8 \end{array}\right\} \Rightarrow \left.\begin{array}{l} t \geq -46,4 \\ t \leq -43,5 \end{array}\right\}$$

Els valors de t han de complir $-46,4 \leq t \leq -43,5$.

Com que t són nombres enters, els únics valors admissibles són:

$$t = -46,\ -45,\ -44.$$

Escrivim les solucions per als valors admissibles de t.

$$\begin{aligned} t = -46: &\quad (x,\, y) = (\,2,\, 20\,) \\ t = -45: &\quad (x,\, y) = (\,7,\, 12\,) \\ t = -44: &\quad (x,\, y) = (\,12,\, 4\,) \end{aligned}$$

► En algunes equacions diofàntiques convé considerar restriccions sobre les incògnites (no negativitat, positivitat, ...). El procediment de resolució consisteix a determinar la solució general i després imposar les restriccions sobre les incògnites.

UNA EQUACIÓ EN DIFERÈNCIA DE QUADRATS

Considerem l'equació diofàntica de segon grau

$$\boxed{x^2 - y^2 = n} \tag{2}$$

on x, y són les incògnites i $n > 0$ és un nombre enter conegut.

Propietat L'equació (2) té tantes solucions enteres com descomposicions de n en producte de dos nombres de la mateixa paritat.

Per a qualsevol descomposició de n:

$$\boxed{n = a\,b \quad (a,\, b \text{ d'igualtat paritat}) \quad \Rightarrow \quad x = \frac{a+b}{2}\,,\ y = \frac{a-b}{2}\,.}$$

Per tal de demostrar la propietat només cal escriure l'equació (2) en la forma

$$n = (x+y)\,(x-y),$$

on $x + y = x - y + 2\,y$ garanteix la igual paritat dels factors.

Suposem ara que $n = a\,b$ amb a, b d'igual paritat. Identificant

$$\left.\begin{aligned} x + y &= a \\ x - y &= b \end{aligned}\right\} \quad \text{obtenim} \quad \left.\begin{aligned} x &= (a+b)/2 \\ y &= (a-b)/2 \end{aligned}\right\}.$$

Per tal de comprovar que tots aquests valors són solució de l'equació només cal substituir en (2):

$$\Big(\frac{a+b}{2}\Big)^2 - \Big(\frac{a-b}{2}\Big)^2 = \frac{a^2+2\,a\,b+b^2}{4} - \frac{a^2-2\,a\,b+b^2}{4} = a\,b = n.$$

Exemple Obtenir les solucions enteres de l'equació $x^2 - y^2 = 440$.

En primer lloc determinem de quantes maneres pot descompondre's 440 com a producte de dos nombres d'igual paritat. Per fer-ho escrivim la seva factorització en producte de primers i obtenim la taula dels seus divisors positius.

$$440 = 2^3 \cdot 5 \cdot 11$$

	2^0	2^1	2^2	2^3
	1	2	4	8
5	5	10	20	40
11	11	22	44	88
	55	110	220	440

El nombre de divisors enters positius és $(3+1)(1+1)(1+1) = 16$, de manera que les descomposicions com a producte de dos nombres són vuit. Escrivim sempre primer l'enter major i després el menor:

$$440 = 440 \cdot 1 = \underline{220 \cdot 2} = \underline{110 \cdot 4} = 55 \cdot 8 = 88 \cdot 5 = \underline{44 \cdot 10} = \underline{22 \cdot 20} = 40 \cdot 11.$$

Els quatre productes subratllats són els que corresponen a factors d'igual paritat. Per tal d'obtenir les solucions enteres positives construïm una taula com es detalla a continuació.

$n = a\,b\ (a \geq b)$	$x = \dfrac{a+b}{2}$	$y = \dfrac{a-b}{2}$	Comprovació
$220 \cdot 2$	111	109	$111^2 - 109^2 = 440$
$110 \cdot 4$	57	53	$57^2 - 53^2 = 440$
$44 \cdot 10$	27	17	$27^2 - 17^2 = 440$
$22 \cdot 20$	21	1	$21^2 - 1^2 = 440$

Considerar $a \geq b$ garanteix obtenir les solucions enteres positives:

$$(x,\, y) = (\,111,\, 109\,),\ (\,57,\, 53\,),\ (\,27,\, 17\,),\ (\,21,\, 1\,).$$

► Cadascuna de les solucions enteres positives de l'equació $x^2 - y^2 = n$ dóna lloc a quatre solucions enteres de l'equació, considerant el producte per ± 1 sobre cadascun dels valors de x i de y.

Per exemple, la solució entera positiva $(x,\, y) = (\,111,\, 109\,)$ dóna lloc a les quatre solucions enteres següents:

$$(x,\, y) = (\,111,\, 109\,),\ (\,-111,\, 109\,),\ (\,-111,\, -109\,),\ (\,111,\, -109\,).$$

Aplicació: L'algorisme de factorització de Fermat

A partir de l'estudi d'equacions del tipus (2), Fermat establí l'any 1643 un algorisme per saber si un nombre natural n imparell és primer o és compost, sense tenir que recórrer a tots els primers menors que $\sqrt{n}$.

Donat un nombre $n > 1$ imparell, si n és compost, $n = a\,b$, els nombres a i b han de ser també imparells. Suposem $a \geq b > 1$. Hem vist que n pot escriure's de forma:

$$\Big(\frac{a+b}{2}\Big)^2 - \Big(\frac{a-b}{2}\Big)^2 = a\,b = n.$$

Llavors, estudiar si un nombre imparell és compost equival a resoldre l'equació $x^2 - y^2 = n$, que escrivim en la forma:

$$x^2 - n = y^2.$$

• El primer pas de l'algorisme de Fermat consisteix a trobar el menor enter positiu que satisfaci

$$q^2 \geq n$$

• A continuació s'haurà d'estudiar si algun dels següents nombres és un quadrat:

$$q^2 - n,\ (q+1)^2 - n,\ (q+2)^2 - n,\ (q+3)^2 - n,\ \ldots$$

• El procés és finit ja que

$$\Big(\frac{n+1}{2}\Big)^2 - n = \frac{n^2 + 2\,n + 1 - 4\,n}{4} = \Big(\frac{n-1}{2}\Big)^2.$$

Aquesta solució correspon a la descomposició trivial $n = n \cdot 1$. Per tant, els únics nombres que s'han de provar són els $m \in \mathbb{N}$ tals que

$$q \leq m < \frac{n+1}{2}$$

Exemple Determinar si el nombre 23711 és primer o compost.

Aplicant l'algorisme de Fermat, busquem un nombre q tal que $q^2 \geq 23711$. Aquest nombre és $q = 154$. D'altra banda, $(23711 + 1)/2 = 11856$.

Hem de comprovar els naturals m tals que $154 \leq m < 11856$.

Calculem $m^2 - 23711$ per a veure si és un quadrat:

$$\begin{aligned} 154^2 - 23711 &= 23716 - 23711 = 5, \\ 155^2 - 23711 &= 24025 - 23711 = 314, \\ 156^2 - 23711 &= 24336 - 23711 = 625 = 25^2. \end{aligned}$$

Hem obtingut $156^2 - 25^2 = 23711$.

Identificant $x = 156$ i $y = 5$:

$$\left.\begin{array}{l} (a+b)/2 = 156 \\ (a-b)/2 = 25 \end{array}\right\} \Rightarrow \left.\begin{array}{l} a+b = 312 \\ a-b = 50 \end{array}\right\} \Rightarrow \quad a = 181,\ b = 131.$$

El nombre 23711 és compost i es descompon com a $23711 = 181 \cdot 131$.

L'EQUACIÓ PITAGÒRICA

Es coneix com a *equació pitagòrica* l'equació diofàntica de segon grau amb incògnites x, y, z l'expressió de les quals és

$$\boxed{x^2 + y^2 = z^2} \tag{3}$$

El nom d'aquesta equació prové del teorema de Pitàgores. Si a és la longitud de la hipotenusa d'un triangle rectangle i b i c són les longituds respectives dels seus catets, el teorema afirma que

$$a^2 = b^2 + c^2.$$

▶ Anomenem *triangle pitagòric* a aquell triangle rectangle en el qual les longituds dels costats són nombres naturals.

Resoldre l'equació diofàntica (3) equival a determinar tots els triangles pitagòrics. El triangle pitagòric de menors longituds és aquell en el que

$$a = 5,\ b = 4,\ c = 3: \quad 5^2 = 4^2 + 3^2.$$

En conseqüència, la terna de nombres $(x, y, z) = (4, 3, 5)$ és solució de l'equació (3). És evident que qualsevol múltiple de la terna és, a la seva

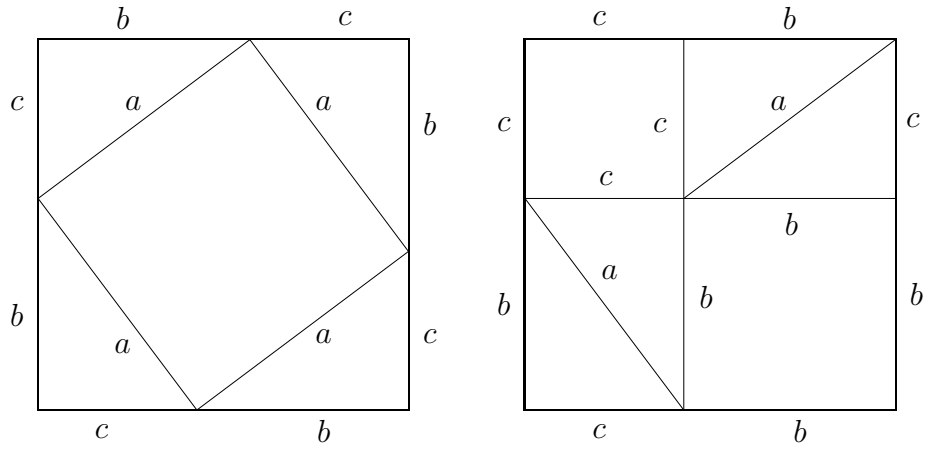
vegada, solució de l'equació. Es tracta de triangles similars a l'inicial. Per exemple, $(x,\, y,\, z) = (16,\, 12,\, 20)$ també és solució: $16^2 + 12^2 = 20^2$.

Aquesta observació ens porta a la següent definició.

► Anomenem *terna pitagòrica primitiva* a tota terna $(x,\, y,\, z)$ de nombres naturals tal que

$$\text{(i)} \quad x^2 + y^2 = z^2, \qquad \text{(ii)} \quad mcd(x,\, y,\, z) = 1.$$

Abans d'enunciar la propietat que determina totes les ternes pitagòriques primitives oferim una demostració geomètrica del teorema de Pitàgores. Construïm dos quadrats d'igual àrea i en el seu interior es disposa de forma diferent quatre rectangles iguals a cadascun d'ells.



Si al quadrat de l'esquerra s'eliminen els quatre triangles s'obté un quadrat d'àrea a^2. El mateix procés en el triangle de la dreta condueix a dos quadrats en els quals la suma d'àrees és $b^2 + c^2$. Queda provat que $a^2 = b^2 + c^2$.

Teorema Les ternes pitagòriques primitives solució de $x^2 + y^2 = z^2$ complint, a més a més, que x és un nombre parell, venen donades per l'expressió

$$\boxed{(x,\, y,\, z) = (\, 2\, s\, t,\, s^2 - t^2,\, s^2 + t^2\,)}$$

per a qualssevol nombres naturals s i t tals que

$$\boxed{\text{(i) } s > t > 0 \quad \text{(ii) } mcd(s,\, t) = 1 \quad \text{(iii) } s,\, t \text{ de diferent paritat.}}$$

Demostració. Donada la naturalesa de la prova, pot ometre's i deixar-se per a una lectura posterior.

En primer lloc provem que tota solució de $x^2 + y^2 = z^2$ és de la forma establerta a l'enunciat.

Suposem que $(x_0,\, y_0,\, z_0)$ és solució de (3) amb $mcd(x_0,\, y_0,\, z_0) = 1$.

(a) Els nombres x_0 i y_0 han de ser de diferent paritat.

Si x_0 i y_0 fossin parells, llavors x_0^2 i y_0^2 serien parells i també ho seria $z_0^2 = x_0^2 + y_0^2$. Si un quadrat és parell, també és parell el nombre base, així doncs z_0 seria parell. Això contradiu que $mcd(x_0,\, y_0,\, z_0) = 1$.

Si x_0 i y_0 fossin imparells podríem escriure $x_0 = 2\,s + 1$, $y_0 = 2\,t + 1$, per a certs naturals s i t. Llavors

$$z_0^2 = x_0^2 + y_0^2 = (2\,s + 1)^2 + (2\,t + 1)^2 = 4\,s^2 + 4\,s + 1 + 4\,t^2 + 4\,t + 1;$$

$$z_0^2 = 4\,(s^2 + s + t^2 + t) + 2 = 4\,m + 2, \quad \text{per a cert } m \in \mathbb{N}.$$

No obstant, cap quadrat dóna residu 2 en dividir-lo per 4. En efecte, tant si és parell com si és imparell, el quadrat d'un nombre enter només dóna residu 0 ó 1 en dividir-lo entre 4.

$$\left.\begin{array}{lll} z_0 = 2\,q & \Rightarrow & z_0^2 = 4\,q^2 \quad \text{(residu 0)} \\ z_0 = 2\,q + 1 & \Rightarrow & z_0^2 = 4\,q^2 + 4\,q + 1 = 4\,(q^2 + q) + 1 \quad \text{(residu 1)} \end{array}\right\}$$

En conseqüència, suposar x_0 i y_0 imparells també condueix a contradicció.

L'única possibilitat és que x_0 i y_0 tinguin diferent paritat. Donat el paper simètric que representen x i y a l'equació pitagòrica:

▶ Escollim que x_0 sigui parell i que y_0 sigui imparell.

(b) Donats x_0 i y_0 de diferent paritat, z_0 és sempre un nombre imparell.

Només cal pensar que $x_0^2 + y_0^2 = z_0^2$. Si x_0 és parell, x_0^2 és parell. Si y_0 és imparell, y_0^2 és imparell. La suma d'un parell amb un imparell és imparell: z_0^2 és imparell. Llavors, z_0 és imparell.

(c) Expressió per a les ternes pitagòriques primitives $(x_0,\, y_0,\, z_0)$.

Aïllant en l'igualtat $x_0^2 + y_0^2 = z_0^2$:

$$x_0^2 = z_0^2 - y_0^2 = (z_0 + y_0)(z_0 - y_0).$$

Els nombres $z_0 + y_0$ i $z_0 - y_0$ són parells, per ser z_0 i y_0 imparells.

$$\left.\begin{array}{l} z_0 + y_0 = 2\,p \\ z_0 - y_0 = 2\,q \end{array}\right\} \;\Rightarrow\; x_0^2 = (z_0 + y_0)(z_0 - y_0) = 4\,p\,q \;\Rightarrow\; \left(\frac{x_0}{2}\right)^2 = p\,q,$$

on, a més a més, es compleix que $mcd(p,\, q) = 1$.

El nombre $x_0/2$ és un nombre natural. En la descomposició en producte d'un nombre al quadrat com $(x_0/2)^2$ sempre apareixen nombres al quadrat. Només cal pensar en la factorització en primers de qualsevol nombre: si elevem el nombre al quadrat tots els exponents queden multiplicats per 2.

Aleshores,

$$\left(\frac{x_0}{2}\right)^2 = p\,q \quad \text{amb } mcd(p,\, q) = 1 \;\Rightarrow\; \left(\frac{x_0}{2}\right)^2 = s^2\,t^2 \quad \text{amb } mcd(s,\, t) = 1.$$

Aïllant:

$$x_0 = 2\,s\,t \quad \text{amb } mcd(s,\, t) = 1.$$

Tornant al sistema en el que apareixen $z_0 + y_0$ i $z_0 - y_0$, substituint p per s^2 i q per t^2 s'aconsegueix determinar les expressions per a y_0 i z_0.

$$\left.\begin{array}{l} z_0 + y_0 = 2\,p = 2\,s^2 \\ z_0 - y_0 = 2\,q = 2\,t^2 \end{array}\right\} \;\Rightarrow\; \text{(sumant) } z_0 = s^2 + t^2;\ \text{(restant) } y_0 = s^2 - t^2.$$

(d) És evident que $s > t$ i la condició $mcd(s,\, t) = 1$ deriva de la condició $mcd(p,\, q) = 1$, que provem a continuació.

Si $mcd(p,\, q) = d \neq 1$ llavors $d|p$ i $d|q$, la qual cosa implica $d|(p+q)$ i $d|(p-q)$. Però $p + q = z_0$ i $p - q = y_0$, d'on $d|z_0$ i $d|y_0$. A més a més,

$$x_0^2 = z_0^2 - y_0^2 = (z_0 + y_0)(z_0 - y_0),$$

així doncs $d^2|x_0^2$ i $d|x_0$. En conseqüència $d \neq 1$ divideix x_0, y_0 i z_0, la qual cosa entra en contradicció amb $mcd(x_0,\, y_0,\, z_0) = 1$.

(e) Per últim, els nombres s i t han de ser de diferent paritat.

Si s i t fossin de la mateixa paritat, s^2 i t^2 també serien d'igual paritat i la seva diferència $s^2 - t^2$ seria parell. Però $y_0 = s^2 - t^2$ i estem suposant que y_0 és imparell. Contradicció!

Recíprocament, les ternes de l'enunciat satisfan l'equació pitagòrica $x^2 + y^2 = z^2$:

$$(2\,s\,t)^2 + (s^2 - t^2)^2 = 4\,s^2\,t^2 + s^4 - 2\,s^2\,t^2 + t^4 = s^4 + 2\,s^2\,t^2 + t^4 = (s^2 + t^2)^2.$$

Falta provar que són ternes primitives.

Suposem que $mcd(x,\, y,\, z) = d \neq 1$ i que p^* és un factor primer de d. Ja que $p^*|z$ i z és imparell, $p^* \neq 2$. D'altra banda, $p^*|y$ i $p^*|z$, d'on $p^*|(z+y)$ i $p^*|(z-y)$, és a dir, $p^*|2\,s^2$ i $p^*|2\,t^2$. Com $p^* \neq 2$, $p^*|s^2$ i $p^*|t^2$, així doncs $p^*|s$ i $p^*|t$, la qual cosa contradiu que $mcd(s,\, t) = 1$. Això conclou la demostració.

► La següent taula recull les ternes pitagòriques primitives per a valors petits de s.

s	t	$x = 2\,s\,t$	$y = s^2 - t^2$	$z = s^2 + t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85

► Sabent que les ternes pitagòriques primitives tenen com a expressió

$$(x,\, y,\, z) = (\, 2\,s\,t,\, s^2 - t^2,\, s^2 + t^2\,),$$

podem obtenir totes les solucions de l'equació pitagòrica $x^2 + y^2 = z^2$ considerant els seus múltiples enters:

$$(x,\, y,\, z) = (\, \pm\, 2\,\lambda\,s\,t,\, \pm\,\lambda\,(s^2 - t^2),\, \pm\,\lambda\,(s^2 + t^2)\,), \quad \forall\,\lambda \in \mathbb{Z},$$

on $s,\, t \in \mathbb{N}$, $s > t > 0$, $mcd(s,\, t) = 1$ i $s,\, t$ de diferent paritat.

Exercicis

1. Resodre l'equació diofàntica lineal $180\,x + 70\,y = 1840$.

2. Obtenir les solucions enteres positives de $90\,x + 65\,y = 3275$.

3. Resoldre l'equació diofàntica $x^2 - y^2 = 252$.

4. Provar si són o no compostos els nombres 22733 i $2^{11} - 1$.

5. Demostrar que la longitud del radi de la circumferència inscrita en un triangle pitagòric és un nombre natural.