MAT^2

MATerials MATemàtics
Volum 2006, treball no. 15, 13 pp. ISSN: 1887-1097
Publicació electrònica de divulgació del Departament de Matemàtiques
de la Universitat Autònoma de Barcelona
www.mat.uab.cat/matmat

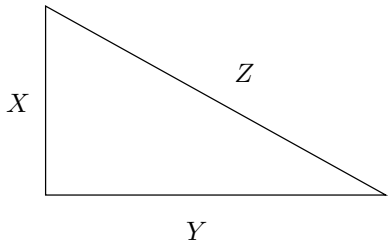
De Pitàgores a Fermat: un viatge a través de l'aritmètica

Xavier Xarles

En aquest treball farem un viatge fictici a través de la història de les matemàtiques, centrant-nos en el punt de vista de l'aritmètica. No he pretès ser rigorós des del punt de vista històric; si bé explico problemes que de fet van ser tractats per certs matemàtics, no són seus ni els mètodes, ni la notació. Tampoc parlaré de tots els matemàtics que van intervenir en la seva resolució; fins hi tot ignoraré alguns dels més importants!

1 Pitàgores

Tots recordem la fórmula de Pitàgores (569 aC -475 aC) que ens relaciona els tres costats d'un triangle rectangle:



$$X^2 + Y^2 = Z^2$$

Si us hi fixeu, a l'institut, la majoria dels exemples que ens posen són:

$$3^2 + 4^2 = 5^2$$

$$6^2 + 8^2 = 10^2$$

i, una mica menys,

$$5^2 + 12^2 = 13^2$$

Per què sempre posen els mateixos exemples? Doncs perquè són els exemples de triangles rectangles amb nombres més petits en què els tres costats són nombres naturals.

Aquests eren els triangles que interessaven més als matemàtics grecs, ja que per a ells els únics "nombres"eren els nombres naturals i, més en general, els nombres racionals positius.

2 Diofant

Tenint en compte que estaven interessats en els triangles rectangles de costats enters, era natural preguntar-se si hi havia alguna manera de trobar-los tots. Aquest problema el va tractar Diofant d'Alexandria (que va viure al voltant de l'any 200 dC) en el seu tractat *Aritmètica*. Aquest llibre és el primer tractat en la història dedicat exclusivament a l'aritmètica, i alguns dels problemes que conté no s'han resolt fins fa molt poc (l'últim l'any 1998!).

El nostre objectiu ara és resoldre l'equació

$$X^2 + Y^2 = Z^2$$

amb X, Y i Z nombres enters. Les solucions (X, Y, Z) s'anomenen **ternes pitagòriques**.

La primera observació a fer si volem resoldre aquesta equació és que sols hem de trobar les solucions (X, Y, Z) que no tinguin factors en comú. Totes les altres s'obtindran a partir d'aquestes multiplicant-les per nombres naturals.

Per exemple, de les solucions posades abans, tenim que la terna $(6, 8, 10)$ és el doble de la terna $(3, 4, 5)$: l'equació

$$6^2 + 8^2 = 10^2$$

és la mateixa que l'equació

$$2^2 3^2 + 2^2 4^2 = 2^2 5^2$$

i, dividint per 2^2 els dos costats de l'igualtat obtenim

$$3^2 + 4^2 = 5^2.$$

En general, si tenim una solució (X, Y, Z) de l'equació $X^2 + Y^2 = Z^2$, aleshores $(a \cdot X, a \cdot Y, a \cdot Z)$ és també una solució per a qualsevol a. Així que les ternes pitagòriques més interesants son les que no tenen factors en comú, que s'anomenen ternes **primitives**.

De les solucions que em posat abans, $(3, 4, 5)$ i $(5, 11, 12)$ són primitives, i $(6, 8, 10)$ no ho és.

El nostre objectiu és trobar una fórmula per a calcular totes les ternes pitagòriques primitives.

En lloc de seguir la demostració de Diofant, farem una demostració molt més geomètrica.

Observem que és el mateix trobar nombres (X, Y, Z) naturals sense factors en comú que verifiquen que $X^2 + Y^2 = Z^2$ que trobar nombres racionals estrictament positius (x, y) que verifiquen que $x^2 + y^2 = 1$. En efecte, donada una terna pitagòrica (X, Y, Z) prenem

$$x = \frac{X}{Z} \quad y = \frac{Y}{Z}.$$

A l'inrevés, donats dos nombres racionals (x, y) que són solució de $x^2 + y^2 = 1$, podem escriure $x = \frac{a}{d}$ i $y = \frac{b}{d}$ de manera única per certs nombres a, b, d naturals sense factors en comú; la terna buscada és aleshores (a, b, d).

Ara, tots reconeixem l'equació $x^2 + y^2 = 1$: és l'equació del cercle! El que volem, per tant, és trobar una fórmula pels punts amb coordenades racionals del cercle.

Ja sabem maneres de trobar els punts del cercle: per exemple, són els punts de la forma $(\sin(\theta), \cos(\theta))$, en que θ varia entre 0 i 2π. Però, compte, aquesta fórmula no ens diu quins punts són racionals.

El que farem és idear un mètode per trobar tots els punts racionals. La idea és senzilla: primer escollim un punt amb coordenades racionals; per exemple, el punt $(-1, 0)$ (o $(1, 0)$, o $(0, 1)$, o $(3/5, 4/5)$). Ara, considerem una recta que passi pel punt $(-1, 0)$ i amb pendent racional. Prenem l'altre punt de tall amb el cercle (una recta i un cercle es tallen sempre en 0, 1 o dos punts, i a més es tallen sols amb un punt si la recta és la recta tangent). Aleshores el punt de tall té coordenades racionals. I a l'inrevés: si el punt (a, b) té coordenades racionals, aleshores la recta que passa per $(-1, 0)$ i (a, b) té pendent racional.

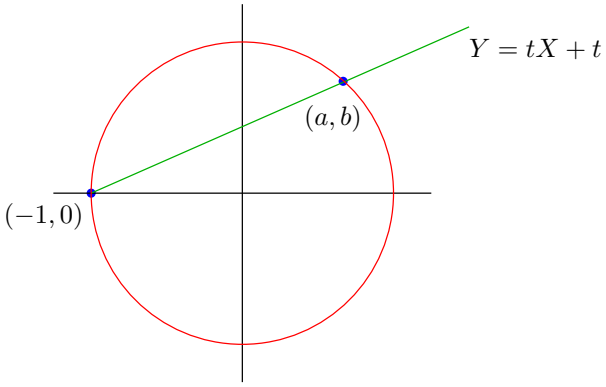
Tot seguit buscarem l'equació que ens determina aquest punt. Primer cal veure com són les rectes que passen pel punt $(-1,0)$: a part de la recta vertical (que és la recta tangent i per tant no ens interessa), totes tenen com a equació

$$Y = tX + s.$$

Però com que volem que passin per $(-1,0)$, han de complir que $0 = -t + s$, o sigui que $t = s$. Per tant, són les rectes de la forma

$$Y = tX + t$$

El seu pendent és t; així que ens interessen aquestes rectes en què t és un nombre racional.



Ara volem calcular el seu punt de tall amb el cercle $X^2 + Y^2 = 1$. És fàcil: substituïm Y per $tX + t$ a l'equació i obtenim una equació de segon grau:

$$(1 + t^2)X^2 + 2t^2X + t^2$$

que té com a solucions

$$X = \frac{-2t^2 \pm 2}{2(t^2+1)} = \begin{cases} -1 \\ \frac{1-t^2}{1+t^2} \end{cases}$$

La solució $X = -1$ correspon al punt que ja tenim: $(-1,0)$. L'altra solució és

$$(X, Y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

Observem que obtindrem solucions positives si t és un nombre racional entre 0 i 1.

Aquest procediment pot ser generalitzat a totes les còniques (ell·lipses, paràboles, hipèrboles); o sigui, equacions de la forma $f(x,y)=0$ amb $f(x,y)$ un polinomi amb coeficients racionals de grau 2 (i no degenerades: que no sigui el producte de dues equacions de grau 1). Proveu-ho per exemple amb l'el·lipse $x^2+3y^2=1$. I per a $x^2+y^2=3$, què passa?

Per obtenir les solucions enteres, expressem t de la forma $t=\frac{m}{n}$ en què m i n nombres naturals primers entre si que verifiquen $m<n$ (perquè volem que t estigui compresa entre 0 i 1). Substituint la t per $\frac{m}{n}$ en la fórmula obtinguda pels punts de coordenades racionals del cercle i simplificant, arribem a la següent fórmula per a les solucions:

$$(x,y)=\left(\frac{n^2-m^2}{n^2+m^2},\frac{2nm}{n^2+m^2}\right),$$

d'on obtenim les ternes pitagòriques

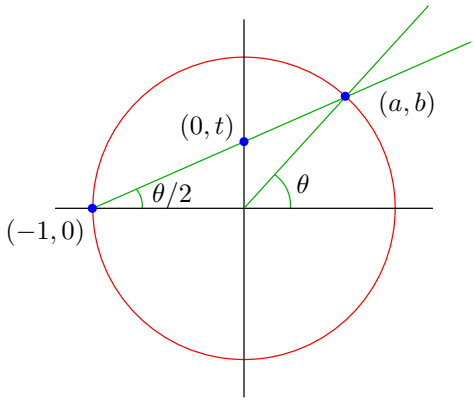
$$(X,Y,Z)=(n^2-m^2,2nm,n^2+m^2).$$

Per tal que siguin primitives, a part de demanar que m i n siguin primers entre si, ens cal demanar que m i n siguin l'una senar i l'altra parell. Tenim així el següent resultat.

Teorema. 1 *El conjunt de ternes pitagòriques primitives és el conjunt*

$$\{(n^2-m^2,2nm,n^2+m^2) \mid n \text{ i } m \text{ primers entre si i } n-m \text{ senar}\}$$

Finalment, fixeu-vos que amb aquest procediment hem obtingut, a més a més, certes fórmules trigonomètriques: en efecte, és fàcil veure que t és la tangent de la meitat de l'angle que forma la recta amb l'eix de les x.



Tenim així que, si

$$t = \tan\left(\frac{\theta}{2}\right)$$

aleshores

$$\cos(\theta) = \frac{1-t^2}{1+t^2} \quad \text{i} \quad \sin(\theta) = \frac{2t}{1+t^2}.$$

Aquestes fórmules són molt utilitzades en la teoria d'integració, ja que ens permeten transformar qualsevol integral trigonomètrica en una integral racional.

3 Fermat

El llibre de Diofant va ser oblidat durant molt anys (com molts dels altres llibres de matemàtics i filòsofs grecs) per molts dels matemàtics europeus. De fet, només van sobreviure sis dels tretze llibres que va escriure. Els matemàtics europeus no varen conèixer el llibre *Aritmètica* de Diofant fins que C. Bachet (Claude Gaspar Bachet de Méziriac, 1581-1638) el va traduir al llatí l'any 1621. I va ser precisament al marge d'aquesta traducció de Bachet on Pierre de Fermat (1601-1665) escrigué la seva famosíssima anotació:

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

que, traduïda a la notació actual, ens diu que,

> si n és un nombre natural més gran que 2, l'equació
>
> $$X^n + Y^n = Z^n$$
>
> no té cap solució en que X, Y i Z són nombres enters, tots ells diferents de 0. Tinc una demostració meravellosa d'aquest resultat, però el marge és massa és massa estret i no m'hi cap.

Aquest "teorema", anomenat l'últim teorema de Fermat, no ha estat provat fins molt recentment (l'any 1994).

Per poder donar alguna idea de les eines que s'utilitzen per demostrar l'últim teorema de Fermat, farem un salt enrera en el temps i reprenem el matemàtic que hem citat més amunt.

C. Bachet

P. de Fermat

4 Bachet

Bachet es va preguntar com determinar els nombres que eren resta d'un quadrat menys un cub. O sigui, volia trobar els nombres enters c tals que l'equació

$$Y^2 - X^3 = c$$

té solucions (X, Y), en que X i Y són nombres racionals.

Estudiant aquesta equació, Bachet es va adonar que si donat c tenim una solució (x, y) de l'equació amb $y \neq 0$, aleshores

$$\left(\frac{x^4 - 8\,cx}{4y^2} \, , \, \frac{-x^6 - 20\,cx^3 + 8\,c^2}{8y^3} \right)$$

també és una solució de l'equació.

Com va arribar a aquesta fórmula? És difícil de saber, però nosaltres podem interpretar-la geomètricament d'una manera semblant al que fèiem per a l'equació $x^2 + y^2 = 1$. Comencem per considerar, fixada c, les solucions reals de l'equació $y^2 - x^3 = c$ en el pla; formen una corba que anomenarem C.

En aquest cas la corba C no és una cònica, i per tant no és cert que una recta talla la corba en com a màxim dos punts. Però sí que és cert que tota recta talla la corba en com a màxim tres punts! En efecte, si tenim una recta

$$y = ax + b,$$

substituint y en l'equació $y^2 - x^3 = c$, obtenim una equació de tercer grau

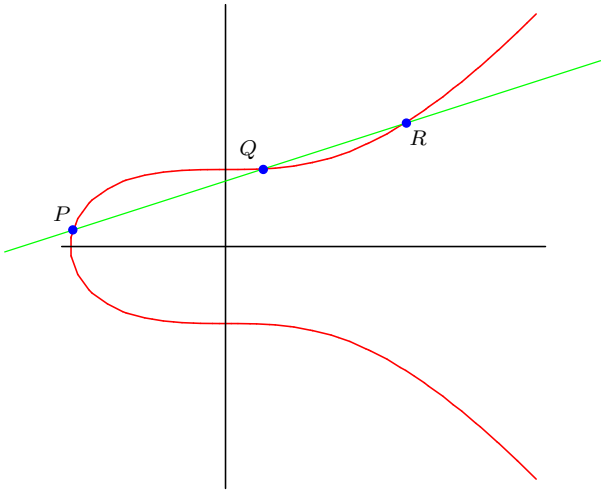
$$(ax + b)^2 - x^3 - c = 0$$

que pot tenir com a màxim tres solucions reals.

Així, tenim un mètode per, donats dos punts P i Q de la corba, construir un tercer punt de la corba: el punt d'intersecció R de la recta que passa per P i Q amb la corba. Aquest procediment ens dona una mena d'operació

$$P * Q = R$$

que verifica propietats semblants a la suma de nombres.



En el cas particular en què agafem P i Q que siguin el mateix punt, el que farem és prendre la recta tangent a la corba en P; podeu veure que, de fet, és la recta natural que s'ha de prendre considerant punts propers a P i fent-los tendir cap a P. El punt obtingut és el que ens dóna la fórmula de Bachet! (Vegeu l'apèndix per una demostració). Escrit en la notació anterior, tenim per tant que

$$(x, y) * (x, y) = \left(\frac{x^4 - 8\,cx}{4y^2} \ , \ \frac{-x^6 - 20\,cx^3 + 8\,c^2}{8y^3} \right)$$

Aplicant la fórmula de Bachet a una solució racional podem anar obtenint solucions racionals. I de fet, es pot veure que, si la solució original verifica que $x \neq 0$, i $c \neq 1$, $c \neq -432$, totes les solucions que obtenim són diferents.

Per exemple, en el cas $c=-2$, tenim la solució $x=3$ i $y=5$

$$5^2=25=27-2=3^3-2$$

Aplicant el procediment anterior obtenim les solucions

$$\left(\frac{129}{100},\frac{383}{1000}\right)$$

$$\left(\frac{2340922881}{58675600},\frac{113259286337279}{449455096000}\right)$$

$$\left(\frac{300370887246304508033820355385035059 21}{30106839828987630717868429937799184 00},\right.$$

$$\left.-\frac{16445572175197962564391437668666769566189815587201059 3281}{52239349235257199745636414537449786558312275098747520 00}\right)$$

Observeu que els numeradors i els denominadors creixen espectacularment!

Què passa per a $c=1$ i per a $c=-432$? Doncs que certes solucions ens donen solucions repetides. Per exemple, per a $c=1$, si prenem la solució $(2,3)$ i apliquem la fórmula de Bachet, obtenim la solució $(0,-1)$. I al tornar-la a aplicar obtenim $(0,-1)$ altra vegada. I així indefinidament.

5 Fermat altre cop

Quina relació té això amb l'últim teorema de Fermat? Doncs més de la que sembla a primera vista. Per exemple, l'equació de Fermat per a $n=3$

$$x^3+y^3=1$$

és equivalent a una d'aquestes equacions. Per veure-ho, feu el següent canvi:

$$x=\frac{36+v}{6u} \quad \text{i} \quad y=\frac{36-v}{6u}$$

Operant arribareu a l'equació

$$v^2-u^3=-432$$

O sigui que és l'equació de Bachet amb $c=-432$. I podeu tornar enrere fent el canvi

$$u=\frac{12}{x+y} \quad \text{i} \quad v=36\frac{x-y}{x+y}.$$

Així, resoldre l'equació de Fermat és equivalent a resoldre l'equació de Bachet.

Fixeu-vos que l'equació de Fermat té, de fet, dues solucions racionals clares: $(1,0)$ i $(0,1)$. Aquestes solucions ens donen, aplicant les fórmules anteriors, les solucions: $(12,36)$ i $(12,-36)$ de l'equació de Bachet. Què passa si apliquem la fórmula de Bachet a aquestes solucions? Doncs que ens dóna que en aplicar-la obtenim la solució original!

De fet, resulta (clar, ens ho diu l'últim teorema de Fermat) que l'equació de Bachet amb $c=-432$ només té aquestes dues solucions.

6 Més enllà de Fermat

Aquest procediment geomètric que hem aplicat a les equacions de Bachet es pot aplicar de fet a qualsevol equació de grau 3 amb dues variables (fora de les "degenerades"); un cas particular (en principi) són les de la forma

$$y^2 = x^3 + ax^2 + bx + c$$

en que a, b i c són nombres prefixats. Les corbes que ens donen aquestes equacions s'anomenen corbes el·líptiques i han tingut i tenen una importància molt gran aquests últims anys. Acabarem destacant tres raons importants que ens mostren l'importància de les corbes el·líptiques

1. Les corbes el·líptiques s'han aplicat de forma fonamental en la resolució de l'últim teorema de Fermat per G. Frey, K. Ribet i A. Wiles (i R. Taylor). La idea del lligam entre corbes el·líptiques i l'últim teorema de Fermat va venir de G. Frey, que va associar la corba el·líptica

   $$y^2 = x(x-a^n)(x+b^n)$$

   a una hipotètica solució (a,b,c) de l'equació de Fermat $a^n+b^n=c^n$. Frey va observar que aquesta corba el·líptica tenia unes propietats bastant estranyes. Ribet va veure que, de fet, aquesta corba el·líptica no verificava una conjectura de les corbes el·líptiques que, finalment, A. Wiles va demostrar. Podeu veure per exemple a

   `http://www.mbay.net/~cgd/flt/flt01.htm`

   un resum de la prova de Wiles.

2. Les corbes el·líptiques són en l'actualitat una de les eines més importants que es fan servir en criptografia, concretament en la criptografia de clau pública i en la signatura digital. De fet, l'últim estàndard de signatura digital aprovat als Estats Units utilitza les corbes el·líptiques. Així que resulta que els nostres ordinadors faran servir les corbes el·líptiques!

3. Un dels "problemes del mil·lenni", dotat amb un milió de dolars per a qui el solucioni, és de corbes el·líptiques: és l'anomenada conjectura de Birch i Swinnerton-Dyer. Així que si voleu guanyar un milió de dolars, ja sabeu el que heu de fer!, encara que segur que hi ha maneres més fàcils de guanyar-los. En podeu trobar més informació a la pàgina web

`http://www.claymath.org/prizeproblems/birchsd.htm`

7 Apèndix

En aquest apèndix veurem formalment com es pot obtenir la fórmula de Bachet. Però les matemàtiques necessàries ja són una mica més sofisticades que en la resta d'aquesta exposició.

Volem veure que si considerem la corba donada per

$$Y^2 - X^3 = c$$

en què c és un nombre enter fixat, i tenim que (a, b) és una solució, aleshores l'intersecció de la recta tangent a la corba en (a, b) amb la corba és

$$\left(\frac{a^4 - 8\,ca}{4b^2} \, , \, \frac{-a^6 - 20\,ca^3 + 8\,c^2}{8b^3} \right).$$

En efecte, la recta tangent a la corba donada per $f(x, y) = 0$ en el punt (a, b) és la recta amb equació

$$\frac{\partial f}{\partial x}(a, b)(X - a) + \frac{\partial f}{\partial y}(a, b)(Y - b) = 0$$

En el nostre cas

$$\frac{\partial f}{\partial x}(a, b) = -3a^2 \quad \frac{\partial f}{\partial y}(a, b) = 2b$$

i per tant tenim la recta

$$Y = b + \frac{3a^2(X-a)}{2b}.$$

Substituint aquesta expressió en l'equació original, i utilitzant que (a, b) és una solució (i per tant que $c = b^3 - a^2$), obtenim

$$\left(b + \frac{3a^2(X-a)}{2b}\right)^2 = X^3 + b^2 - a^3$$

que ens dóna

$$3a^2(X-a) + \frac{9a^4(X-a)^2}{4b^2} = X^3 - a^3 = (X-a)(X^2 + aX + a^2)$$

Una solució és $X = a$, com ja sabiem. Dividint per $(X - a)$ els dos costats obtenim

$$3a^2 + \frac{9a^4(X-a)}{4b^2} = (X^2 + aX + a^2)$$

d'on

$$9a^4(X-a) = 4b^2(X^2 + aX - 2a^2) = 4b^2(X-a)(X+2a)$$

Tenim altre cop la solució $X = a$ ja que com la recta que hem considerat era la recta tangent, "talla la corba dues vegades a (a, b)". Tornant a dividir per $(X - a)$, obtenim

$$X = \frac{9a^4}{4b^2} - 2a = \frac{a^4 - 8ac}{4b^2}$$

fent servir altre vegada que $c = b^3 - a^2$. L'expressió per a la Y es troba fàcilment de la expressió de la X i de l'equació

$$Y = b + \frac{3a^2(X-a)}{2b}.$$

Bibliografia

Si voleu més informació sobre les ternes pitagòriques podeu consultar molts dels llibres sobre teoria de nombres elemental. Per exemple:

- J. Cilleruelo i A. Cordoba. *La Teoría de los números*, Biblioteca Mondadori. Madrid, 1992.

- També podeu consultar la pàgina web:

  `http://teoriadenumeros.4d2.net`

Per obtenir més informació sobre corbes el·líptiques, podeu consultar:

- J.H. Silverman i J. Tate. *Rational Points on Elliptic Curves* Undergraduate Text in Mathematics, Springer 1992.
- O bé visitar la pàgina web:

  `http://www.jmilne.org/math/CourseNotes/math679.html`

Si voleu tenir una idea de com s'ha demostrat l'últim teorema de Fermat, podeu visitar

- `http://www.mbay.net/~cgd/flt/flt01.htm`

Trobareu informació bàsica sobre criptografia amb corbes el·líptiques a la pàgina web

- `http://www.criptored.upm.es/guiateoria/gt_m044a.htm`
- O bé al llibre de Neal Koblitz, *A Course in number theory and cryptography*, Springer-Verlag 1994.

Xavier Xarles
Departament de Matemàtiques
Universitat Autònoma de Barcelona
`xarles@mat.uab.cat`

Publicat el 8 de novembre de 2006