Aritmètica de corbes el·líptiques

Xavier Xarles

6 de Juny de 2017

Geometria Artimètica

L'objectiu principal de la geometria aritmètica és descriure totes les solucions d'equacions diofàntiques, tant les enteres com les racionals.

Geometria Artimètica

L'objectiu principal de la geometria aritmètica és descriure totes les solucions d'equacions diofàntiques, tant les enteres com les racionals.
En aquesta xerrada ens centrarem en les solucions racionals.
Exemples:

Geometria Artimètica

L'objectiu principal de la geometria aritmètica és descriure totes les solucions d'equacions diofàntiques, tant les enteres com les racionals.
En aquesta xerrada ens centrarem en les solucions racionals.
Exemples:

- Trobar tots els nombres racionals X i Y tal que

$$X^2 + Y^2 = 1$$

Geometria Artimètica

L'objectiu principal de la geometria aritmètica és descriure totes les solucions d'equacions diofàntiques, tant les enteres com les racionals.
En aquesta xerrada ens centrarem en les solucions racionals.
Exemples:

- Trobar tots els nombres racionals X i Y tal que

$$X^2 + Y^2 = 1$$

- Trobar tots els nombres racionals X i Y tal que

$$X^2 + Y^2 = 3$$

Geometria Artimètica

L'objectiu principal de la geometria aritmètica és descriure totes les solucions d'equacions diofàntiques, tant les enteres com les racionals.
En aquesta xerrada ens centrarem en les solucions racionals.
Exemples:

- Trobar tots els nombres racionals X i Y tal que

$$X^2 + Y^2 = 1$$

- Trobar tots els nombres racionals X i Y tal que

$$X^2 + Y^2 = 3$$

- Trobar tots els nombres racionals X i Y tal que

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

La idea principal és considerar les solucions (X, Y) en el pla (real), i utilitzem tècniques geometriques per a determinar tots les solucions racionals.

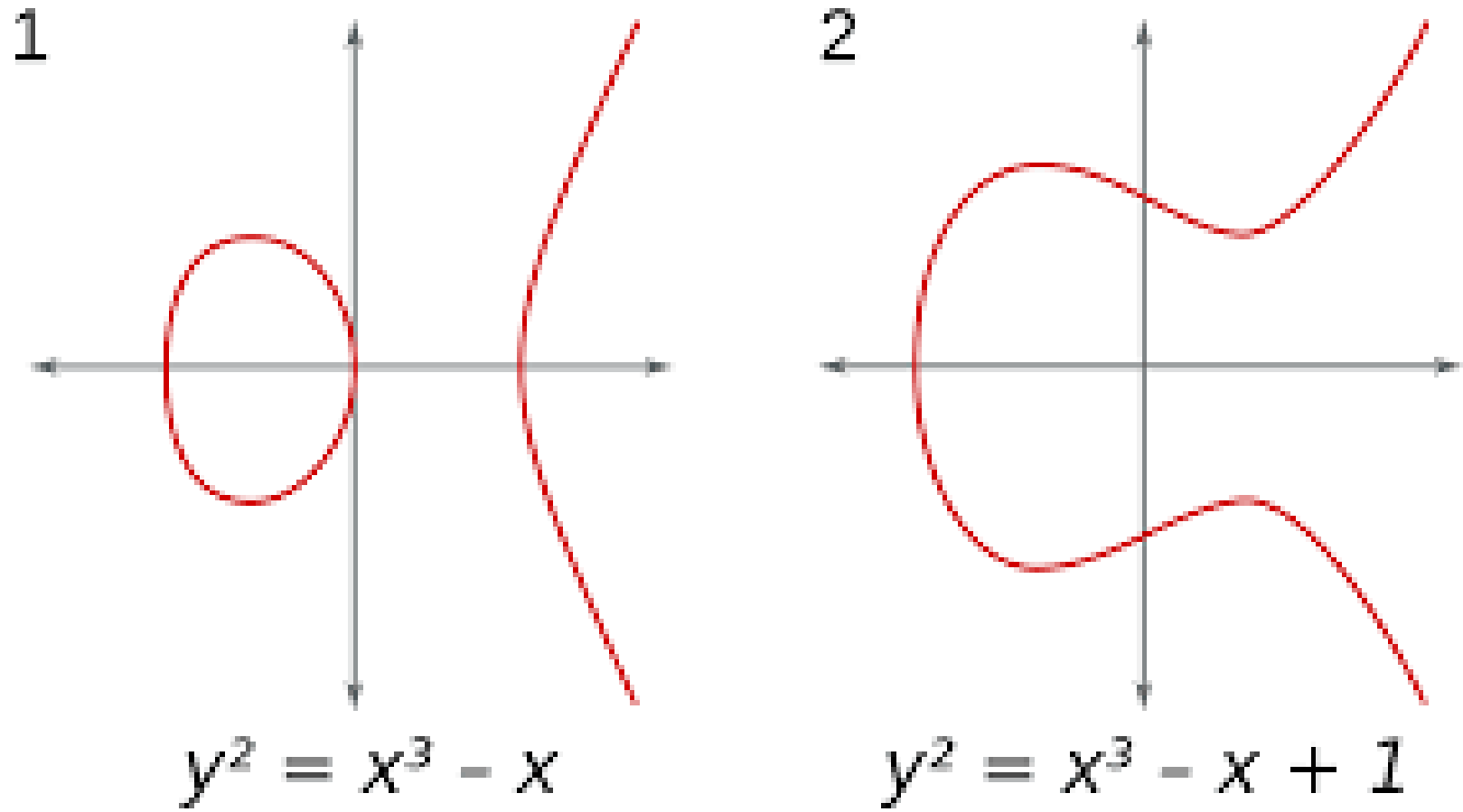


Figura: Dos corbes

Exemple $X^2 + Y^2 = 1$

Les solucions en el pla són els punts del cercle de radi 1 i centre $(0, 0)$

Exemple $X^2 + Y^2 = 1$

Les solucions en el pla són els punts del cercle de radi 1 i centre $(0, 0)$
Considerem un punt del cercle amb les dues coordenades racionals.
Per exemple

$$(1, 0) \text{ o } (0, 1) \text{ o } (-1, 0) \text{ o } (0, -1)$$

Utilitzarem el punt $(-1, 0)$ però podria servir qualsevol altre.

Exemple $X^2 + Y^2 = 1$

Les solucions en el pla són els punts del cercle de radi 1 i centre $(0, 0)$
Considerem un punt del cercle amb les dues coordenades racionals.
Per exemple

$$(1, 0) \text{ o } (0, 1) \text{ o } (-1, 0) \text{ o } (0, -1)$$

Utilitzarem el punt $(-1, 0)$ però podria servir qualsevol altre.
Qualsevol recta que passi per $(-1, 0)$ talla el cercle en un altre punt (excepte la recta vertical).

Exemple $X^2 + Y^2 = 1$

Les solucions en el pla són els punts del cercle de radi 1 i centre $(0, 0)$
Considerem un punt del cercle amb les dues coordenades racionals.
Per exemple

$$(1, 0) \text{ o } (0, 1) \text{ o } (-1, 0) \text{ o } (0, -1)$$

Utilitzarem el punt $(-1, 0)$ però podria servir qualsevol altre.
Qualsevol recta que passi per $(-1, 0)$ talla el cercle en un altre punt (excepte la recta vertical).
Els punts de coordenades racionals seràn exactament els punts de tall amb rectes amb pendent racional.

Demostració algebraica

Demostració algebraica

Una recta (no vertical) té equació

$$Y = r \cdot X + s$$

per algun r (pendent) i s.

Demostració algebraica

Una recta (no vertical) té equació

$$Y = r \cdot X + s$$

per algun r (pendent) i s.
La recta conté el punt $(-1, 0)$ si $0 = r \cdot (-1) + s$, o sigui si $s = r$.

Demostració algebraica

Una recta (no vertical) té equació

$$Y = r \cdot X + s$$

per algun r (pendent) i s.
La recta conté el punt $(-1, 0)$ si $0 = r \cdot (-1) + s$, o sigui si $s = r$.

Per tant estem considerant les
rectes amb equació

$$Y = r \cdot X + r$$

Demostració algebraica

Una recta (no vertical) té equació

$$Y = r \cdot X + s$$

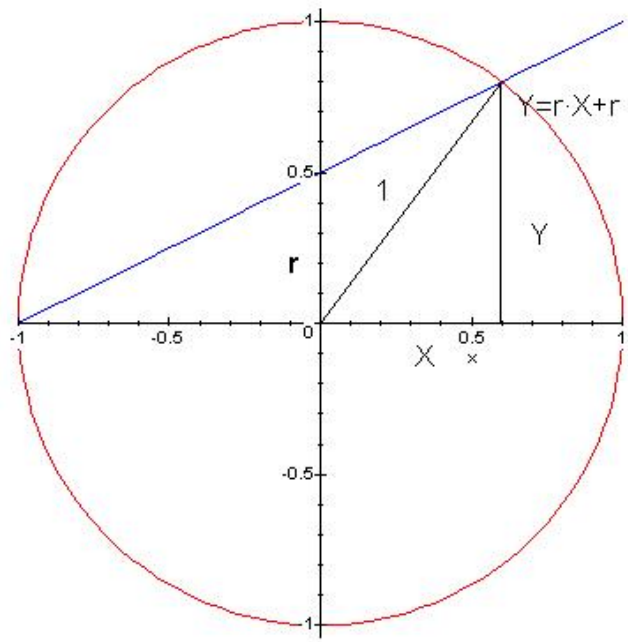
per algun r (pendent) i s.
La recta conté el punt $(-1, 0)$ si $0 = r \cdot (-1) + s$, o sigui si $s = r$.

Per tant estem considerant les rectes amb equació

$$Y = r \cdot X + r$$

La intersecció amb el cercle de radi 1 es calcula substituint Y per $r \cdot X + r$ a l'equació

$$X^2 + Y^2 = 1$$



Demostració algebraica

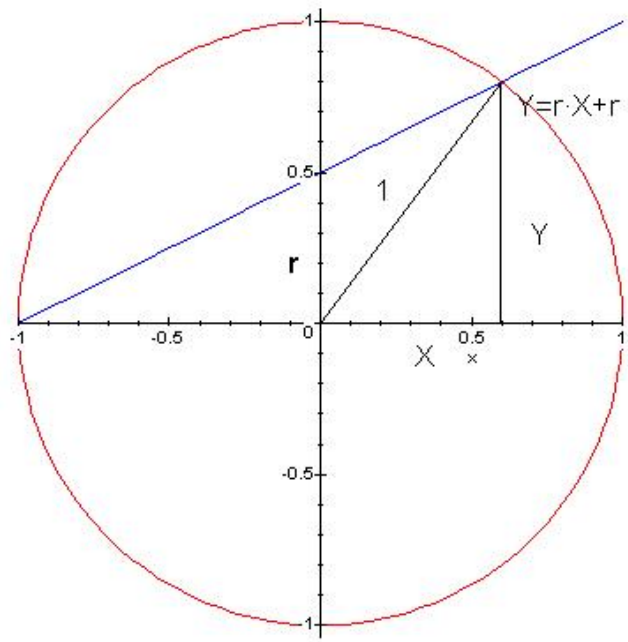
Una recta (no vertical) té equació

$$Y = r \cdot X + s$$

per algun r (pendent) i s.
La recta conté el punt $(-1, 0)$ si $0 = r \cdot (-1) + s$, o sigui si $s = r$.

Per tant estem considerant les rectes amb equació

$$Y = r \cdot X + r$$



La intersecció amb el cercle de radi 1 es calcula substituint Y per $r \cdot X + r$ a l'equació

$$X^2 + Y^2 = 1$$

Tenim $X^2 + (rX + r)^2 = 1$ d'on $(1 + r^2)X^2 + 2r^2X + r^2 - 1 = 0$.

$$(1 + r^2)X^2 + 2r^2X + r^2 - 1 = 0.$$

$$(1+r^2)X^2+2r^2X+r^2-1=0.$$

Les solucions d'aquesta equació són

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

$$(1+r^2)X^2+2r^2X+r^2-1=0.$$

Les solucions d'aquesta equació són

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

La solució $X=-1$ és la que ja teniem. L'altre solució és

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

$$(1+r^2)X^2+2r^2X+r^2-1=0.$$

Les solucions d'aquesta equació són

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

La solució $X=-1$ és la que ja teniem. L'altre solució és

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

És clar que si r és un nombre racional, aleshores X i Y són nombres racionals.

$$(1+r^2)X^2+2r^2X+r^2-1=0.$$

Les solucions d'aquesta equació són

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

La solució $X=-1$ és la que ja teniem. L'altre solució és

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

És clar que si r és un nombre racional, aleshores X i Y són nombres racionals.
El que hem trobat és una parametrització del cercle.

$$(1+r^2)X^2+2r^2X+r^2-1=0.$$

Les solucions d'aquesta equació són

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

La solució $X=-1$ és la que ja teniem. L'altre solució és

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

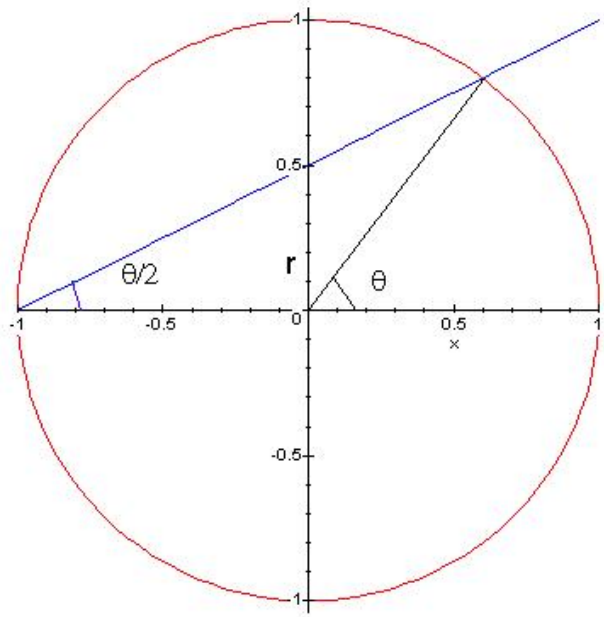
És clar que si r és un nombre racional, aleshores X i Y són nombres racionals.
El que hem trobat és una parametrització del cercle.
Tenim per tant una fòrmula per a totes les solucions racionals de l'equació $X^2+Y^2=1$.

Una aplicació del que hem fet (no aritmètica):
Com que els punts del cercle es poden parametritzar per funcions trigonomètriques

$$(\cos(\theta), \sin(\theta))$$

A més la pendent de la recta calculada abans és igual a $\tan(\frac{\theta}{2})$.
Per tant tenim que si $r = \tan\left(\frac{\theta}{2}\right)$ aleshores

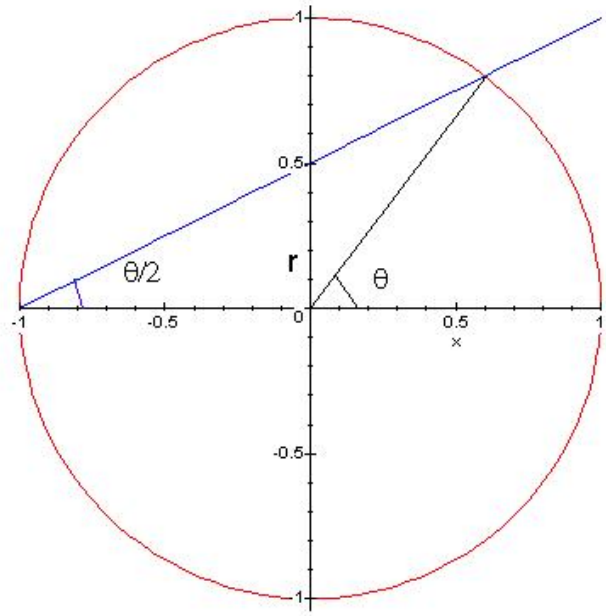
$$\cos(\theta) = \frac{1 - r^2}{1 + r^2} \quad \text{i} \quad \sin(\theta) = \frac{2r}{1 + r^2}.$$



Una aplicació del que hem fet (no aritmètica):
Com que els punts del cercle es poden parametritzar per funcions trigonomètriques

$$(\cos(\theta), \sin(\theta))$$

A més la pendent de la recta calculada abans és igual a $\tan(\frac{\theta}{2})$.
Per tant tenim que si $r = \tan\left(\frac{\theta}{2}\right)$ aleshores



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

Aquestes equacions són els que s'utilitzen per escriure integrals trigonomètiques com a integrals racionals.

Mètode

Aquest mètode funciona per què

Mètode

Aquest mètode funciona per què

1. Coneixem una solució racional.

Mètode

Aquest mètode funciona per què

1. Coneixem una solució racional.
2. Qualsevol recta talla el cercle en 0, 1 o dos punts.

Mètode

Aquest mètode funciona per què

1. Coneixem una solució racional.
2. Qualsevol recta talla el cercle en 0, 1 o dos punts.
3. Si talla en dos punts, un d'ell és racional i la recta té coeficients racionals, aleshores l'altre punt és racional.

Primera intuició

Aquest mètode el podrem utilitzar sempre que tinguem una equació de grau 2 (en dues variables).

Sospita

Si tenim una equació de grau 2 en dues variables, amb coeficients racionals, i coneixem una solució racional, aleshores coneixem totes les solucions, n'hi ha infinites i venen parametrizades per funcions racionals amb un parametre racional.

Contraexemples

Si considerem la equació $X^2 + Y^2 = 0$, és clar que té una solució $(0, 0)$ i és l'única.

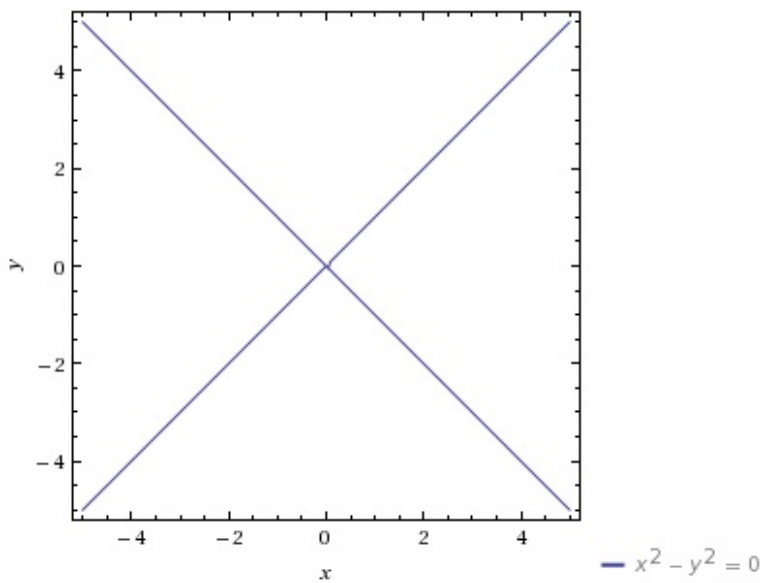
Contraexemples

Si considerem la equació $X^2 + Y^2 = 0$, és clar que té una solució $(0, 0)$ i és l'única.
Si considerem la equació $X^2 - Y^2 = 0$, i fem el mateix que abans amb el punt $(-1, 1)$, obtenim només les solucions del tipus (x, x), i ens deixem les solucions com $(-2, 2)$, o $(3, -3)$.

Contraexemples

Si considerem la equació $X^2 + Y^2 = 0$, és clar que té una solució $(0, 0)$ i és l'única.
Si considerem la equació $X^2 - Y^2 = 0$, i fem el mateix que abans amb el punt $(-1, 1)$, obtenim només les solucions del tipus (x, x), i ens deixem les solucions com $(-2, 2)$, o $(3, -3)$.

El problema és que les corbes anteriors són còniques degenerades, es a dir que tenen un punt singular.



Conclusió

Teorema

Si tenim una equació de grau 2 en dues variables, amb coeficients racionals, i sense punts singulars i coneixem una solució racional, aleshores coneixem totes les solucions, n'hi ha infinites i venen parametrizades per funcions racionals amb un parametre racional.

Més exemples: La equació $X^2 + Y^2 = 2$

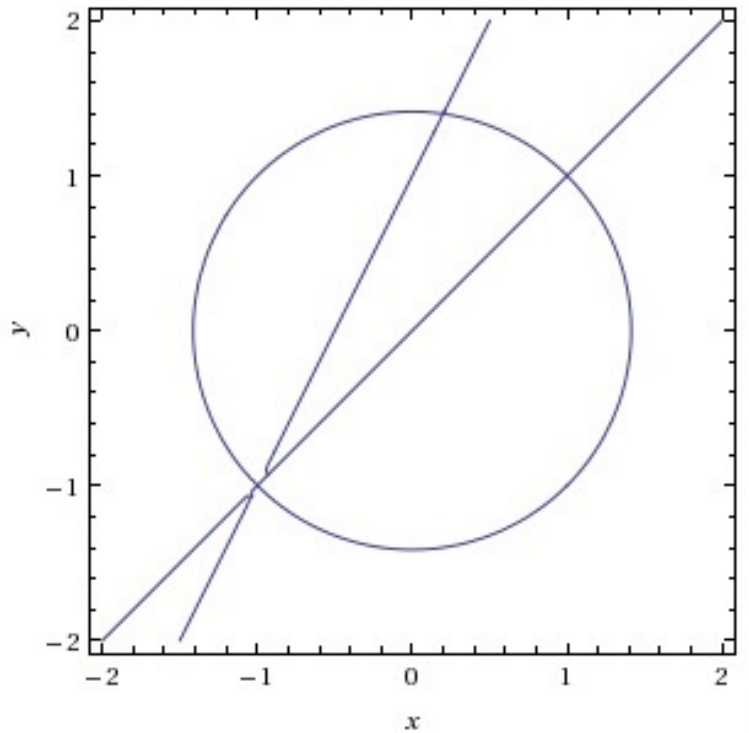
Tenim uns punts racionals fàcils: $(1, 1)$, $(-1, 1)$, $(1, -1)$ i $(-1, -1)$).
Considerem aquest últim punt $(-1, -1)$.
Les rectes que contenen aquest punt són: $Y = rX + (r - 1)$.

Més exemples: La equació $X^2 + Y^2 = 2$

Tenim uns punts racionals fàcils: $(1, 1)$, $(-1, 1)$, $(1, -1)$ i $(-1, -1)$).
Considerem aquest últim punt $(-1, -1)$.
Les rectes que contenen aquest punt són: $Y = rX + (r - 1)$.

Al calcular la intersecció amb el cercle obtenim

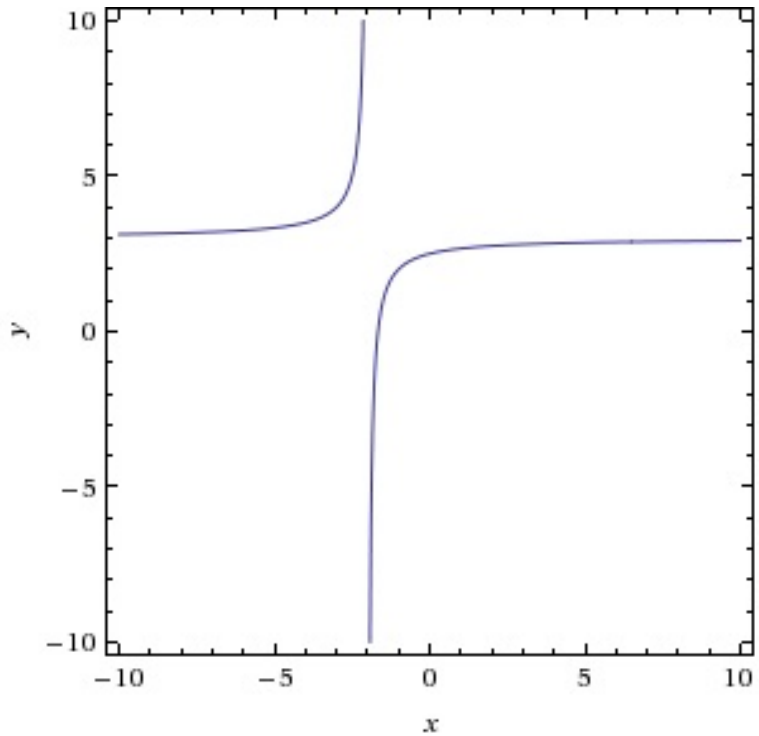
$$(X, Y) = \left(-\frac{r^2 - 2r - 1}{1 + r^2}, \frac{r^2 + 2r - 1}{1 + r^2} \right)$$



Més exemples: La equació $3X - XY + 6 - 2Y = 1$

Tenim un punt racional $(-1, 2)$.
Aplicant el mètode obtenim que les solucions (a part de $(-1, 2)$) són:

$$(X, Y) = \left(-\frac{2r - 1}{r}, 3 - r \right).$$



La equació $X^2 + Y^2 = 3$

Després de calcular una estona no trobem cap solució racional.
Com podem demostrar si n'hi ha o no?

La equació $X^2 + Y^2 = 3$

Després de calcular una estona no trobem cap solució racional.
Com podem demostrar si n'hi ha o no?
Tranformem-la a una problema de solucions enteres (posant $X = A/C$ i $Y = B/C$ i multiplicant per C^2):

$$A^2 + B^2 = 3C^2$$

La equació $X^2 + Y^2 = 3$

Després de calcular una estona no trobem cap solució racional.
Com podem demostrar si n'hi ha o no?
Tranformem-la a una problema de solucions enteres (posant $X = A/C$ i $Y = B/C$ i multiplicant per C^2):

$$A^2 + B^2 = 3C^2$$

La pregunta és: té alguna solució entera (A, B, C) diferent de $(0, 0, 0)$ (i tal que A, B i C son primers entre si?)

La equació $X^2 + Y^2 = 3$

Després de calcular una estona no trobem cap solució racional.
Com podem demostrar si n'hi ha o no?
Tranformem-la a una problema de solucions enteres (posant $X = A/C$ i $Y = B/C$ i multiplicant per C^2):

$$A^2 + B^2 = 3C^2$$

La pregunta és: té alguna solució entera (A, B, C) diferent de $(0, 0, 0)$ (i tal que A, B i C son primers entre si?)
Primer pas: 3 no pot dividir A o B. Ja que si ho fa, aleshores divideix A, B i C, i per tant no son primers entre si.

La equació $X^2 + Y^2 = 3$

Després de calcular una estona no trobem cap solució racional.
Com podem demostrar si n'hi ha o no?
Tranformem-la a una problema de solucions enteres (posant $X = A/C$ i $Y = B/C$ i multiplicant per C^2):

$$A^2 + B^2 = 3C^2$$

La pregunta és: té alguna solució entera (A, B, C) diferent de $(0, 0, 0)$ (i tal que A, B i C son primers entre si?)
Primer pas: 3 no pot dividir A o B. Ja que si ho fa, aleshores divideix A, B i C, i per tant no son primers entre si.
Segon pas: Fem mòdul 3. Obtenim la equació

$$A^2 + B^2 \equiv 0 (\text{mod } 3)$$

que no té solucions a part de $(0, 0)$.

Resposta General (de Legendre):

Per saber si una equació de grau dos amb dues variables té alguna solució racional, primer mira si en té en els reals.

Resposta General (de Legendre):

Per saber si una equació de grau dos amb dues variables té alguna solució racional, primer mira si en té en els reals.
Si en té, transforma-la a una equació homogenia en tres variables i coeficients enters i busca solucions enteres primeres entre si i diferents de $(0, 0, 0)$.

Resposta General (de Legendre):

Per saber si una equació de grau dos amb dues variables té alguna solució racional, primer mira si en té en els reals.
Si en té, transforma-la a una equació homogenia en tres variables i coeficients enters i busca solucions enteres primeres entre si i diferents de $(0, 0, 0)$.
Aleshores, hi ha un enter m (que es pot calcular explicitament en termes del coeficients de l'equació) tal que l'equació anterior té solucions enteres si i només si en té modul m i en els reals.

Resposta General (de Legendre):

Per saber si una equació de grau dos amb dues variables té alguna solució racional, primer mira si en té en els reals.
Si en té, transforma-la a una equació homogenia en tres variables i coeficients enters i busca solucions enteres primeres entre si i diferents de $(0, 0, 0)$.
Aleshores, hi ha un enter m (que es pot calcular explicitament en termes del coeficients de l'equació) tal que l'equació anterior té solucions enteres si i només si en té modul m i en els reals.
Per exemple, per les de la forma $AX^2 + BY^2 = C$ amb A, B i $C \in \mathbb{Z}$, lliures de quadrats i primeres entre si, es pot prendre $m = 4|ABC|$.

Claude Gaspar Bachet de Méziriac (1581-1638)

És famós ja que ell va traduir al llatí el llibre Aritmètica de Diofant d'Alexandria en el que Fermat va escriure la famosa nota al marge.

Claude Gaspar Bachet de Méziriac (1581-1638)

És famós ja que ell va traduir al llatí el llibre Aritmètica de Diofant d'Alexandria en el que Fermat va escriure la famosa nota al marge.
En un dels seus llibre diu (en llenguatge modern):
Sigui c un nombre racional.

Claude Gaspar Bachet de Méziriac (1581-1638)

És famós ja que ell va traduir al llatí el llibre Aritmètica de Diofant d'Alexandria en el que Fermat va escriure la famosa nota al marge.
En un dels seus llibre diu (en llenguatge modern):
Sigui c un nombre racional.
Suposem que (x, y) és una solució racional de la equació

$$Y^2 = X^3 + c.$$

Claude Gaspar Bachet de Méziriac (1581-1638)

És famós ja que ell va traduir al llatí el llibre Aritmètica de Diofant d'Alexandria en el que Fermat va escriure la famosa nota al marge.
En un dels seus llibre diu (en llenguatge modern):
Sigui c un nombre racional.
Suposem que (x, y) és una solució racional de la equació

$$Y^2 = X^3 + c.$$

Aleshores

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

també és una solució racional.

Interpretació Geomètrica: Intent

Considerem la corba donada com les solucions de

$$Y^2 = X^3 + c.$$

Volem fer un procediment semblant al que feiem amb les de graus 2.
Si (x, y) és una solució racional de l'equació, considerem una recta que passa per (x, y) i amb coeficients racionals.
Aquesta recta talla la corba en dos punts o menys.
Però aquests punts no seran necessàriament racionals!

Exemple

Si $c = -2$, tenim la solució $(3, 5)$. Les rectes que passen per $(3, 5)$ son de la forma $Y = rX + (5 - 3r)$.

Exemple

Si $c = -2$, tenim la solució $(3, 5)$. Les rectes que passen per $(3, 5)$ son de la forma $Y = rX + (5 - 3r)$.
Si substituim Y by $rX + (5 - 3r)$ a $Y^2 - X^3 + 2$ i expandim, i després dividim el polinomi resultant per $X - 3$ (sempre es pot fer), obtenim l'equació

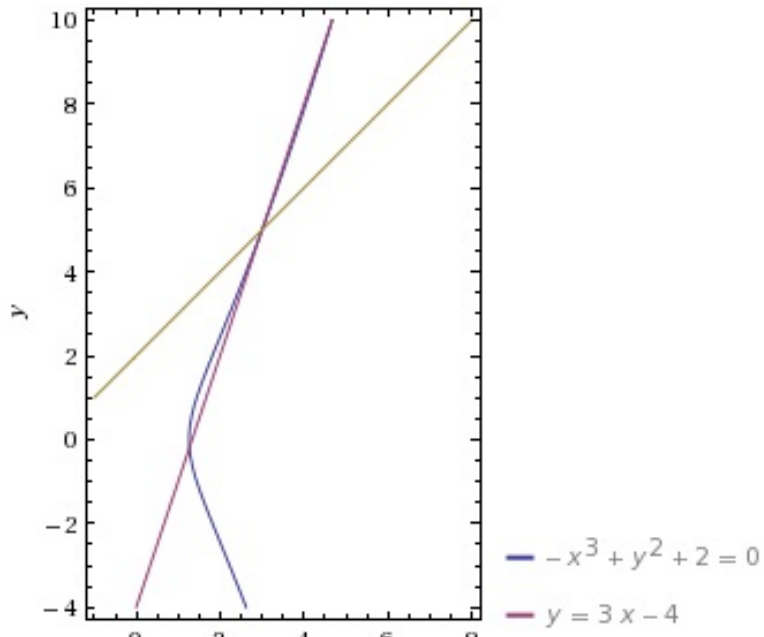
$$-X^2 + r^2X - 3X - 3r^2 + 10r - 9 = 0$$

Exemple

Si $c = -2$, tenim la solució $(3, 5)$. Les rectes que passen per $(3, 5)$ son de la forma $Y = rX + (5 - 3r)$.
Si substituim Y by $rX + (5 - 3r)$ a $Y^2 - X^3 + 2$ i expandim, i després dividim el polinomi resultant per $X - 3$ (sempre es pot fer), obtenim l'equació

$$-X^2 + r^2X - 3X - 3r^2 + 10r - 9 = 0$$

Les coordenades X dels punts d'intersecció amb la recta seran solucions d'aquesta equació.

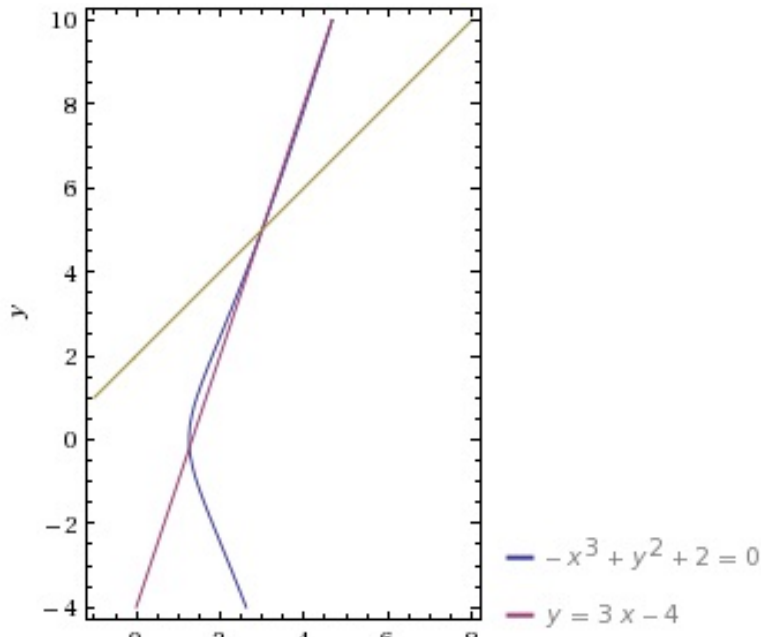


Exemple

Si $c = -2$, tenim la solució $(3, 5)$. Les rectes que passen per $(3, 5)$ son de la forma $Y = rX + (5 - 3r)$.
Si substituim Y by $rX + (5 - 3r)$ a $Y^2 - X^3 + 2$ i expandim, i després dividim el polinomi resultant per $X - 3$ (sempre es pot fer), obtenim l'equació

$$-X^2 + r^2X - 3X - 3r^2 + 10r - 9 = 0$$

Les coordenades X dels punts d'intersecció amb la recta seran solucions d'aquesta equació.



Per exemple, per $r = 1$ tenim

$$-X^2 - 2X - 2 = 0$$

que no té solucions reals!
I per $r = 3$ tenim

$$-X^2 + 6X - 6 = 0$$

amb solucions $3 + \sqrt{3}$.

Interpretació Geomètrica: Intent millorat

Que podem fer? Considerar la recta que talla dues vegades a la corba en el punt (x, y): la recta tangent!

Interpretació Geomètrica: Intent millorat

Que podem fer? Considerar la recta que talla dues vegades a la corba en el punt (x, y): la recta tangent!
De l'equació $Y^2 = X^3 + c$ podem obtenir fent derivades implicites que la pendent de la recta tangent al punt (x, y) is $3x^2/2y$.

Interpretació Geomètrica: Intent millorat

Que podem fer? Considerar la recta que talla dues vegades a la corba en el punt (x, y): la recta tangent!
De l'equació $Y^2 = X^3 + c$ podem obtenir fent derivades implicites que la pendent de la recta tangent al punt (x, y) is $3x^2/2y$.
En el cas $c = -2$ y $(x, y) = (3, 5)$ tenim la recta amb pendent $r = 27/10$.

Interpretació Geomètrica: Intent millorat

Que podem fer? Considerar la recta que talla dues vegades a la corba en el punt (x, y): la recta tangent!
De l'equació $Y^2 = X^3 + c$ podem obtenir fent derivades implicites que la pendent de la recta tangent al punt (x, y) is $3x^2/2y$.
En el cas $c = -2$ y $(x, y) = (3, 5)$ tenim la recta amb pendent $r = 27/10$.
Aplicant la fòrmula obtenim

$$-X^2 + \frac{429}{100}X - \frac{387}{100}$$

amb solucións $X = 3$ i $X = 129/100$.

Interpretació Geomètrica: Intent millorat

Que podem fer? Considerar la recta que talla dues vegades a la corba en el punt (x, y): la recta tangent!
De l'equació $Y^2 = X^3 + c$ podem obtenir fent derivades implicites que la pendent de la recta tangent al punt (x, y) is $3x^2/2y$.
En el cas $c = -2$ y $(x, y) = (3, 5)$ tenim la recta amb pendent $r = 27/10$.
Aplicant la fòrmula obtenim

$$-X^2 + \frac{429}{100}X - \frac{387}{100}$$

amb solucións $X = 3$ i $X = 129/100$.
Podeu comporvar que és el mateix nombre que ens dona la fòrmula de Bachet.

Interpretació Geomètrica: Intent millorat

Que podem fer? Considerar la recta que talla dues vegades a la corba en el punt (x, y): la recta tangent!
De l'equació $Y^2 = X^3 + c$ podem obtenir fent derivades implicites que la pendent de la recta tangent al punt (x, y) is $3x^2/2y$.
En el cas $c = -2$ y $(x, y) = (3, 5)$ tenim la recta amb pendent $r = 27/10$.
Aplicant la fòrmula obtenim

$$-X^2 + \frac{429}{100}X - \frac{387}{100}$$

amb solucións $X = 3$ i $X = 129/100$.
Podeu comporvar que és el mateix nombre que ens dona la fòrmula de Bachet.
En general la fòrmula de Bachet ens dóna les coordenades de la intersecció entre la recta tangent a (x, y) i la corba donada per la equació.

Aplicant la formula obtenim

Aplicant la formula obtenim

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

Aplicant la formula obtenim

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

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

Aplicant la formula obtenim

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

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

$$\left(\frac{3003708872463045080338203553850350592 1}{3010683982898763071786842993779918400},\right.$$

$$\left.-\frac{16445572175197962564391437668666769566189815587201059328 1}{52239349235257199745636414537449786558312275098747520 00}\right)$$

Aplicant la formula obtenim

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

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

$$\left(\frac{3003708872463045080338203553850350592 1}{3010683982898763071786842993779918400},\right.$$

$$\left.-\frac{16445572175197962564391437668666769566189815587201059328 1}{52239349235257199745636414537449786558312275098747520 00}\right)$$

etc...

Corbes el·líptiques

En general una equació de la forma

$$Y^2 = X^3 + aX^2 + bX + c$$

que no té punts singulars ens determina una corba el·líptica.

Corbes el·líptiques

En general una equació de la forma

$$Y^2 = X^3 + aX^2 + bX + c$$

que no té punts singulars ens determina una corba el·líptica.
No punts singulars $\Longleftrightarrow$ $X^3 + aX^2 + bX + c$ no té arrels dobles.

Corbes el·líptiques

En general una equació de la forma

$$Y^2 = X^3 + aX^2 + bX + c$$

que no té punts singulars ens determina una corba el·líptica.
No punts singulars $\Longleftrightarrow$ $X^3 + aX^2 + bX + c$ no té arrels dobles.
Qualsevol equació de grau 3 que té algun punt racional es pot "transformar" mitjançant un canvi de variables a una d'aquesta forma.

Corbes el·líptiques

En general una equació de la forma

$$Y^2 = X^3 + aX^2 + bX + c$$

que no té punts singulars ens determina una corba el·líptica.
No punts singulars $\Longleftrightarrow$ $X^3 + aX^2 + bX + c$ no té arrels dobles.
Qualsevol equació de grau 3 que té algun punt racional es pot "transformar" mitjançant un canvi de variables a una d'aquesta forma.
Si ara tenim un punt racional (x, y), podem calcular la recta tangent a la corba en aquest punt, calcular la seva interesecció amb la corba i el punt que obtenim (si n'hi ha algun més!) sempre és un punt racional.

Fórmula

Si (x, y) és una solució racional de

$$Y^2 = X^3 + aX^2 + bX + c$$

aleshores (x', y') és una altre solució racional, on

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}.$$

Fórmula

Si (x, y) és una solució racional de

$$Y^2 = X^3 + aX^2 + bX + c$$

aleshores (x', y') és una altre solució racional, on

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}.$$

Us podria semblar que hem obtingut un procediment per a obtenir infinites solucions racionals d'una donada. Però això no és cert!

Fórmula

Si (x, y) és una solució racional de

$$Y^2 = X^3 + aX^2 + bX + c$$

aleshores (x', y') és una altre solució racional, on

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}.$$

Us podria semblar que hem obtingut un procediment per a obtenir infinites solucions racionals d'una donada. Però això no és cert! Per exemple, if $y = 0$, x' no està ni tant sols definit (de fet diem que ens dóna el "punt de l'infinit").

Fórmula

Si (x, y) és una solució racional de

$$Y^2 = X^3 + aX^2 + bX + c$$

aleshores (x', y') és una altre solució racional, on

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}.$$

Us podria semblar que hem obtingut un procediment per a obtenir infinites solucions racionals d'una donada. Però això no és cert! Per exemple, if $y = 0$, x' no està ni tant sols definit (de fet diem que ens dóna el "punt de l'infinit").
Per exemple: si $x' = x$ i $y' = y$ aleshores no obtenim cap punt nou.

Fórmula

Si (x, y) és una solució racional de

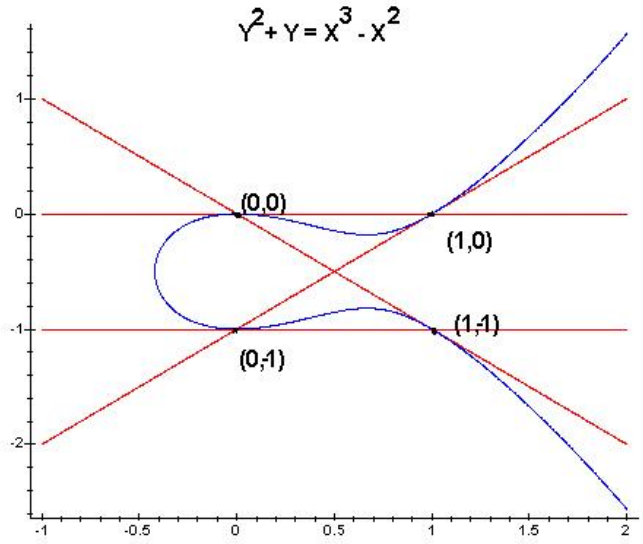
$$Y^2 = X^3 + aX^2 + bX + c$$

aleshores (x', y') és una altre solució racional, on

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}.$$

Us podria semblar que hem obtingut un procediment per a obtenir infinites solucions racionals d'una donada. Però això no és cert! Per exemple, if $y = 0$, x' no està ni tant sols definit (de fet diem que ens dóna el "punt de l'infinit").
Per exemple: si $x' = x$ i $y' = y$ aleshores no obtenim cap punt nou.
Que més pot passar?

Exemples



L'equació

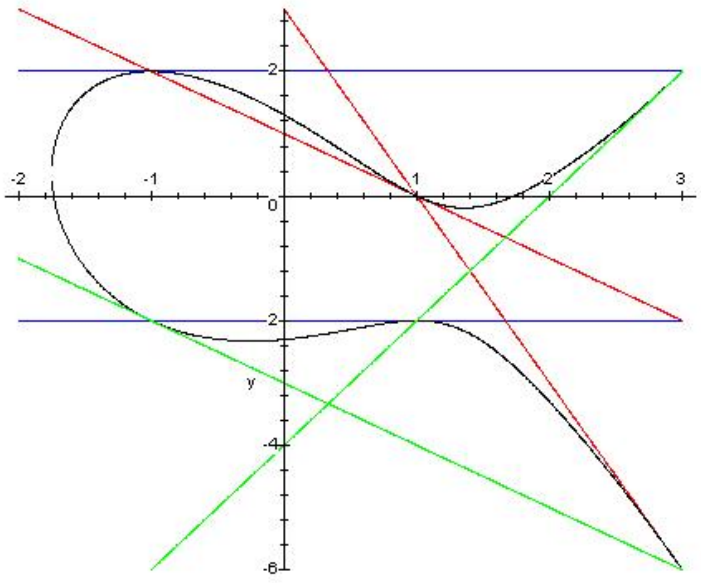
$$Y^2 + Y = X^3 - X^2$$

amb el punt $(x, y) = (1, 0)$
Tenim $x'' = x$ (i $y'' = -y$).
(El canvi de Y per $Y - 1/2$ ens dóna una equació com abans.)

L'equació

$$Y^2+XY+Y = X^3-X^2-3X+3$$

amb el punt $(x, y) = (1, 0)$.
Tenim $x''' = x$ (and $y''' = -y$).
(Idem amb el canvi Y per $Y - \frac{1}{2}(X + 1)$.)



Beppo Levi (1875-1961)

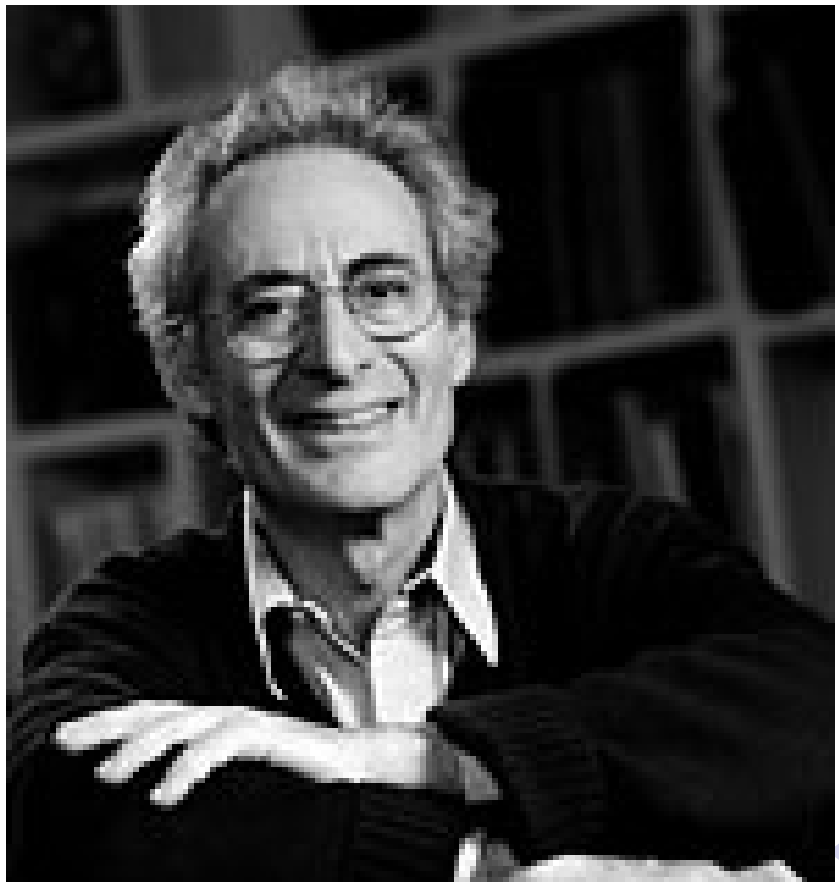
Va conjecturar el 1908 que hi havia un nombre finit de possibilitats. Posteriorment tant T. Nagell (1952) com A. Ogg (1971) ho van tornar a conjecturar (sense saber que ho havien fet abans). Finalment, el B. Mazur va demostrar aquesta conjectura el 1977 en un article molt famós.

Teorema de Mazur

Sigui (x, y) un punt racional en una corba el·líptica. Calculeu x', x'', x''' i x''''. Si ho pots fer, i tots són diferents, aleshores el procediment anterior ens donen infinits punts racionals.

Normalment s'enuncia com

Si (x, y) és un punt racional de torsió en una corba el·líptica d'ordre N, aleshores $N \leq 12$ i $N \neq 11$.



Més enllà de la tangent

Hi ha alguna altra manera de produïr punts racionals a partir d'altres punts? Utilitzant les cordes.

Més enllà de la tangent

Hi ha alguna altra manera de produïr punts racionals a partir d'altres punts? Utilitzant les cordes.
Si tenim dos punts P i Q racionals de la corba, la recta que passa per ells dos talla la corba en un altre punt que necessàriament és racional.

Més enllà de la tangent

Hi ha alguna altra manera de produïr punts racionals a partir d'altres punts? Utilitzant les cordes.
Si tenim dos punts P i Q racionals de la corba, la recta que passa per ells dos talla la corba en un altre punt que necessàriament és racional.
Aquesta operació, que en el cas que $P = Q$ es correspon al procediment que ja hem explicat, s'assembla a una operació de grup.

Més enllà de la tangent

Hi ha alguna altra manera de produïr punts racionals a partir d'altres punts? Utilitzant les cordes.
Si tenim dos punts P i Q racionals de la corba, la recta que passa per ells dos talla la corba en un altre punt que necessàriament és racional.
Aquesta operació, que en el cas que $P = Q$ es correspon al procediment que ja hem explicat, s'assembla a una operació de grup.
Però no ho és! Per exemple, no té element neutre. La idea és utilitzar un punt fixat O per tal que sigui el neutre repetint l'operació corda.

Més enllà de la tangent

Hi ha alguna altra manera de produïr punts racionals a partir d'altres punts? Utilitzant les cordes.
Si tenim dos punts P i Q racionals de la corba, la recta que passa per ells dos talla la corba en un altre punt que necessàriament és racional.
Aquesta operació, que en el cas que $P = Q$ es correspon al procediment que ja hem explicat, s'assembla a una operació de grup.
Però no ho és! Per exemple, no té element neutre. La idea és utilitzar un punt fixat O per tal que sigui el neutre repetint l'operació corda.
Tot i així tenim un problema, sobretot per que les rectes verticals no tallen en un tercer punt. Per això ens cal afegir un punt "a l'infinit"que correspon a les rectes verticals.

Més enllà de la tangent

Hi ha alguna altra manera de produïr punts racionals a partir d'altres punts? Utilitzant les cordes.
Si tenim dos punts P i Q racionals de la corba, la recta que passa per ells dos talla la corba en un altre punt que necessàriament és racional.
Aquesta operació, que en el cas que $P = Q$ es correspon al procediment que ja hem explicat, s'assembla a una operació de grup.
Però no ho és! Per exemple, no té element neutre. La idea és utilitzar un punt fixat O per tal que sigui el neutre repetint l'operació corda.
Tot i així tenim un problema, sobretot per que les rectes verticals no tallen en un tercer punt. Per això ens cal afegir un punt "a l'infinit"que correspon a les rectes verticals.
Això és anàleg a quan diem que un parabola és com una el·lípse a la que hi hem afegit el punt de l'infinit.

L'operació de grup

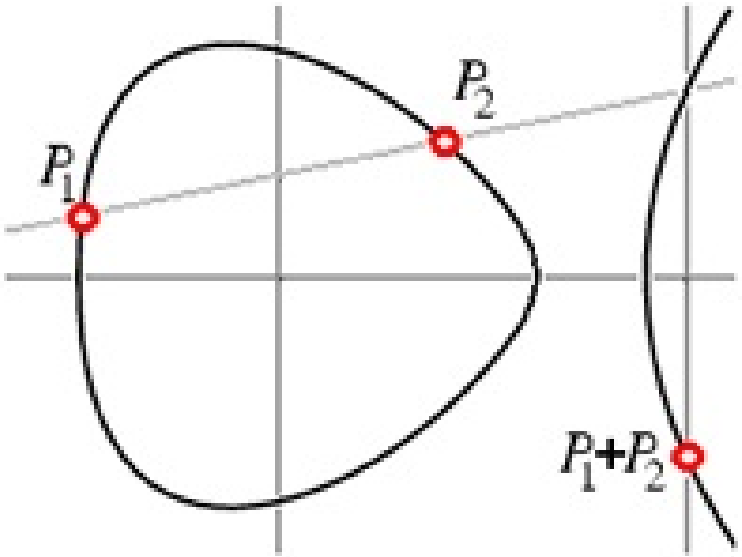
Normalment es pren com a punt 0 el propi punt de l'infinit. Aleshores la operació es defineix de la següent manera.

L'operació de grup

Normalment es pren com a punt 0 el propi punt de l'infinit.
Aleshores la operació es defineix de la següent manera.
Si P i Q són punts racionals de la corba E, diem $P \oplus Q$ al punt de tall amb E de la recta vertical que passa pel punt de tall de la recta que passa per P i Q.

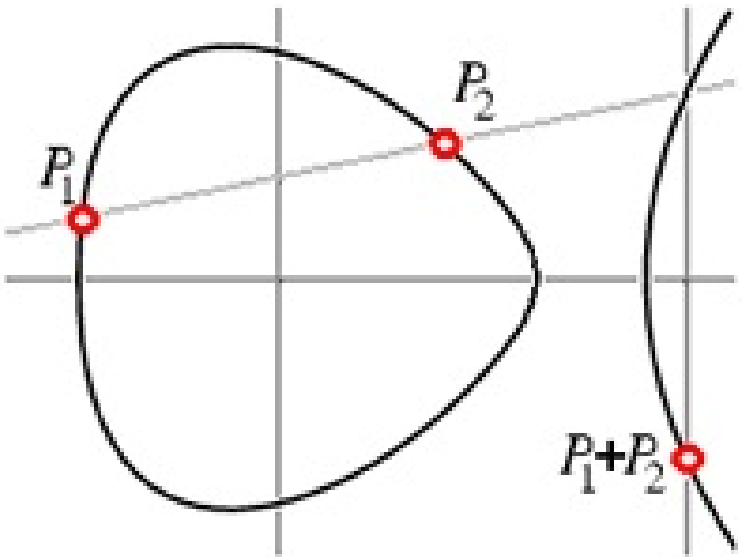
L'operació de grup

Normalment es pren com a punt 0 el propi punt de l'infinit.
Aleshores la operació es defineix de la següent manera.
Si P i Q són punts racionals de la corba E, diem $P \oplus Q$ al punt de tall amb E de la recta vertical que passa pel punt de tall de la recta que passa per P i Q.
Si $P = Q$ prenem la recta tangent. Si la recta que passa per P i Q és vertical, diem que $P \oplus Q = O$.



L'operació de grup

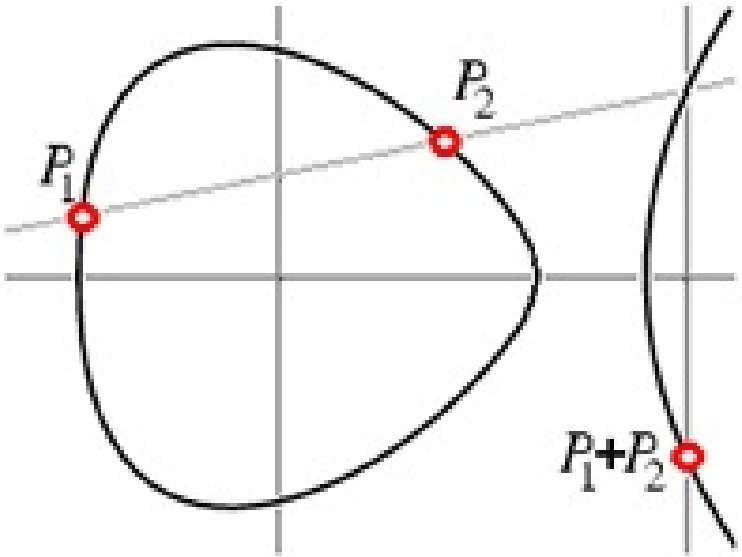
Normalment es pren com a punt 0 el propi punt de l'infinit.
Aleshores la operació es defineix de la següent manera.
Si P i Q són punts racionals de la corba E, diem $P \oplus Q$ al punt de tall amb E de la recta vertical que passa pel punt de tall de la recta que passa per P i Q.
Si $P = Q$ prenem la recta tangent. Si la recta que passa per P i Q és vertical, diem que $P \oplus Q = O$.



Tenim que $P \oplus O = P$, ja que la recta que passa per P i O és la recta vertical, que talla en un altre punt P', i la recta vertical que passa per P' és la mateixa recta, que talla en P.

L'operació de grup

Normalment es pren com a punt 0 el propi punt de l'infinit.
Aleshores la operació es defineix de la següent manera.
Si P i Q són punts racionals de la corba E, diem $P \oplus Q$ al punt de tall amb E de la recta vertical que passa pel punt de tall de la recta que passa per P i Q.
Si $P = Q$ prenem la recta tangent. Si la recta que passa per P i Q és vertical, diem que $P \oplus Q = O$.



Tenim que $P \oplus O = P$, ja que la recta que passa per P i O és la recta vertical, que talla en un altre punt P', i la recta vertical que passa per P' és la mateixa recta, que talla en P. A més aquest P' és l'invers per la suma, i per tant $P \oplus P' = O$.

El teorema de Mordell-Weil

L'any 1922 L. Mordell va respondre una pregunta posada per H. Poincaré, demostrant que el grup dels punts racionals $E(\mathbb{Q})$ d'una corba el·líptica és sempre finitament generat.

El teorema de Mordell-Weil

L'any 1922 L. Mordell va respondre una pregunta posada per H. Poincaré, demostrant que el grup dels punts racionals $E(\mathbb{Q})$ d'una corba el·líptica és sempre finitament generat.
O sigui, si $E(\mathbb{Q})$ és el conjunt de punts racionals (amb el punt de l'infinit) amb l'operació $\oplus$, aleshores

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

on $r \geq 0$ s'anomena el rang de E i T és un grup abelià finit.

El teorema de Mordell-Weil

L'any 1922 L. Mordell va respondre una pregunta posada per H. Poincaré, demostrant que el grup dels punts racionals $E(\mathbb{Q})$ d'una corba el·líptica és sempre finitament generat.
O sigui, si $E(\mathbb{Q})$ és el conjunt de punts racionals (amb el punt de l'infinit) amb l'operació $\oplus$, aleshores

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

on $r \geq 0$ s'anomena el rang de E i T és un grup abelià finit.
Dit d'una altre manera, donada una corba el·líptica E hi ha un nombre finit de punts racionals tals que tots els altres punts s'obtenen d'aquests punts pels procediments de cordes i tangents.

El teorema de Mordell-Weil

L'any 1922 L. Mordell va respondre una pregunta posada per H. Poincaré, demostrant que el grup dels punts racionals $E(\mathbb{Q})$ d'una corba el·líptica és sempre finitament generat.
O sigui, si $E(\mathbb{Q})$ és el conjunt de punts racionals (amb el punt de l'infinit) amb l'operació $\oplus$, aleshores

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

on $r \geq 0$ s'anomena el rang de E i T és un grup abelià finit.
Dit d'una altre manera, donada una corba el·líptica E hi ha un nombre finit de punts racionals tals que tots els altres punts s'obtenen d'aquests punts pels procediments de cordes i tangents.
El teorema del Mazur dit abans ens diu també quines són totes les possibilitats per a T: són $T = \mathbb{Z}/n\mathbb{Z}$ amb $n = 1, 2, \ldots, 10, 12$ o $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ per $n = 1, 2, 3, 4$.

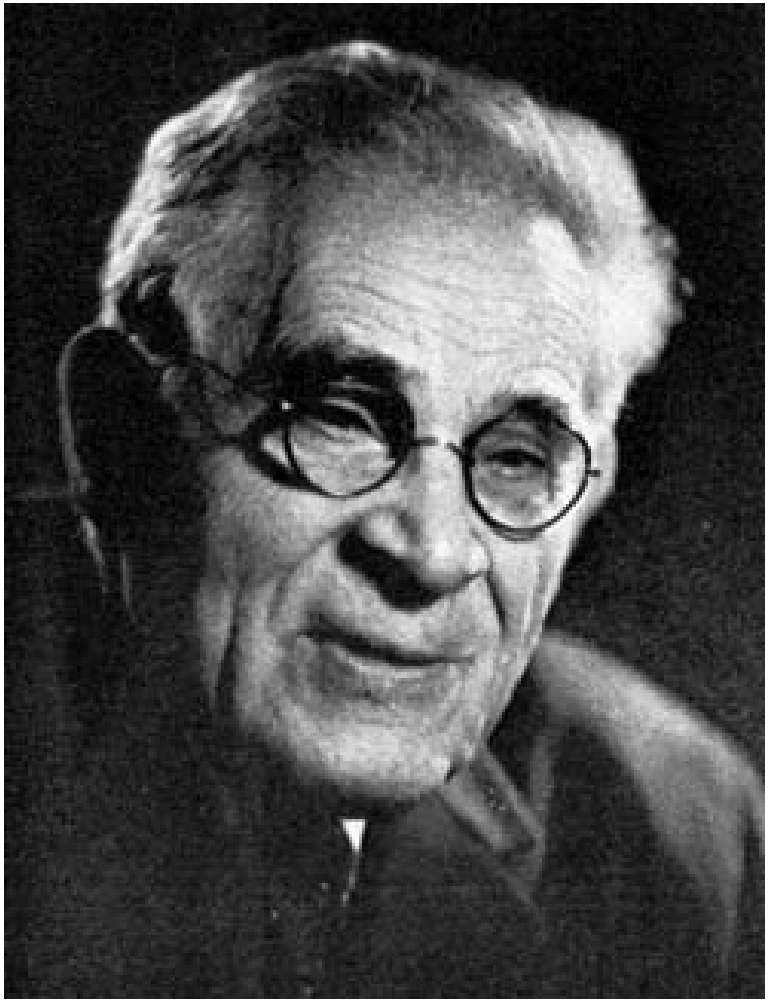
El teorema de Mordell-Weil

L'any 1922 L. Mordell va respondre una pregunta posada per H. Poincaré, demostrant que el grup dels punts racionals $E(\mathbb{Q})$ d'una corba el·líptica és sempre finitament generat.
O sigui, si $E(\mathbb{Q})$ és el conjunt de punts racionals (amb el punt de l'infinit) amb l'operació $\oplus$, aleshores

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

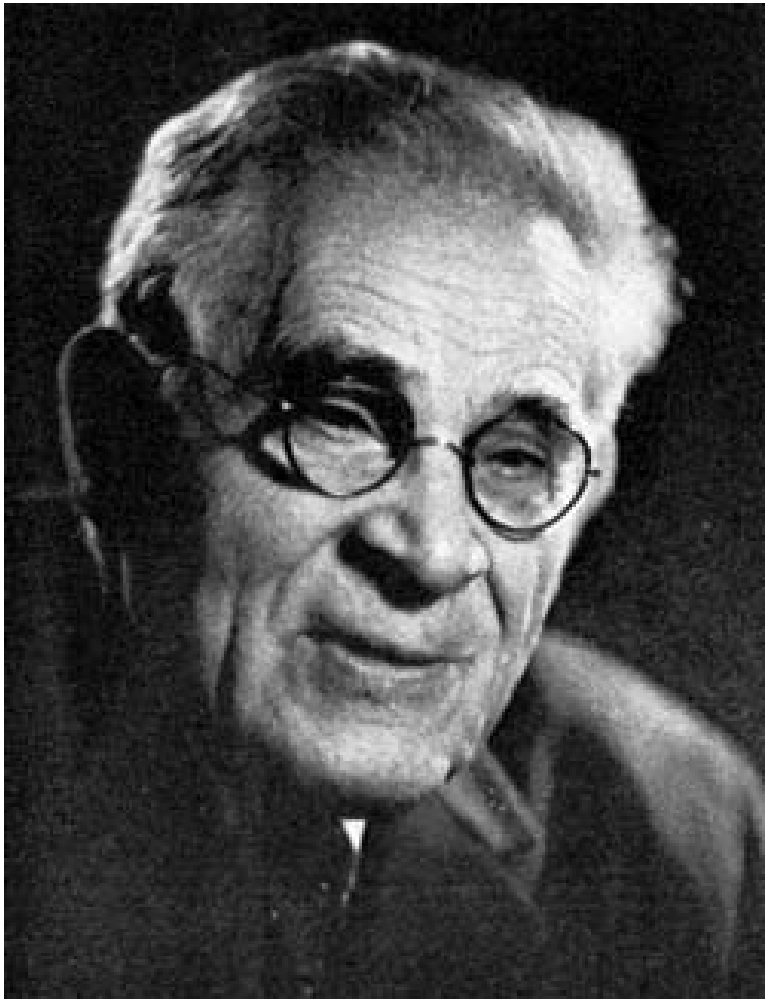
on $r \geq 0$ s'anomena el rang de E i T és un grup abelià finit.
Dit d'una altre manera, donada una corba el·líptica E hi ha un nombre finit de punts racionals tals que tots els altres punts s'obtenen d'aquests punts pels procediments de cordes i tangents.
El teorema del Mazur dit abans ens diu també quines són totes les possibilitats per a T: són $T = \mathbb{Z}/n\mathbb{Z}$ amb $n = 1, 2, \ldots, 10, 12$ o $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ per $n = 1, 2, 3, 4$.
El teorema de Mordell va ser generalizat per A. Weil a cossos de nombres (com $\mathbb{Q}(\sqrt{2})$), i també a varietats abelianes (que és l'equivalent a les corbes el·líptiques en dimensió superior).

Exemples



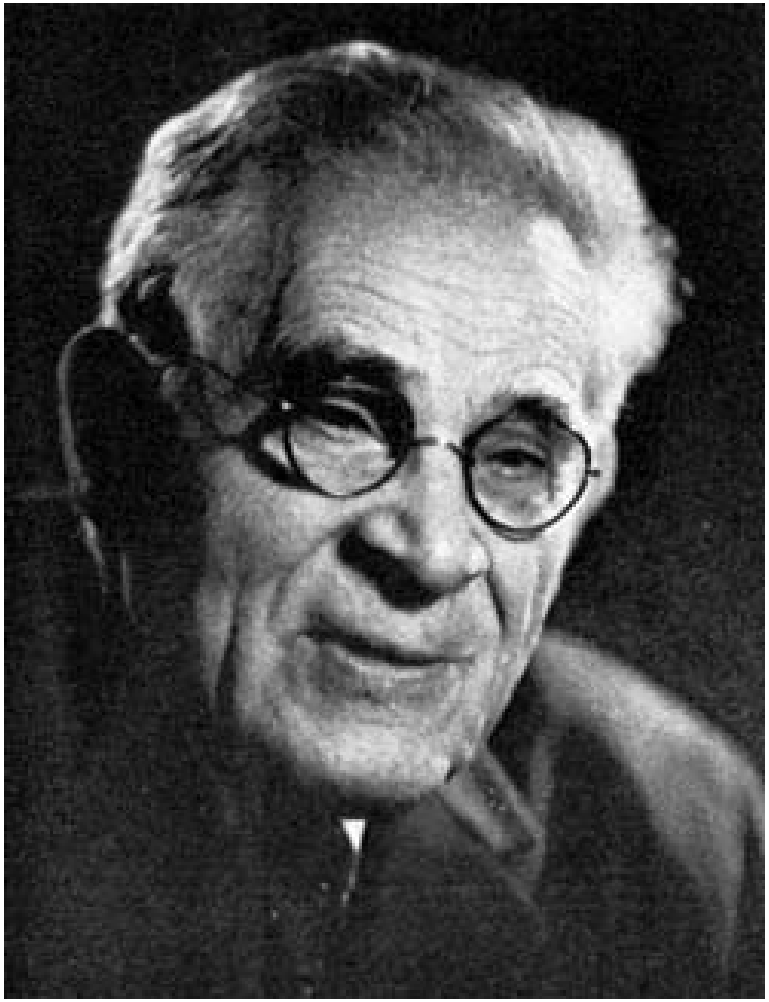
- $E : y^2 = x^3 - x$,
  $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Exemples



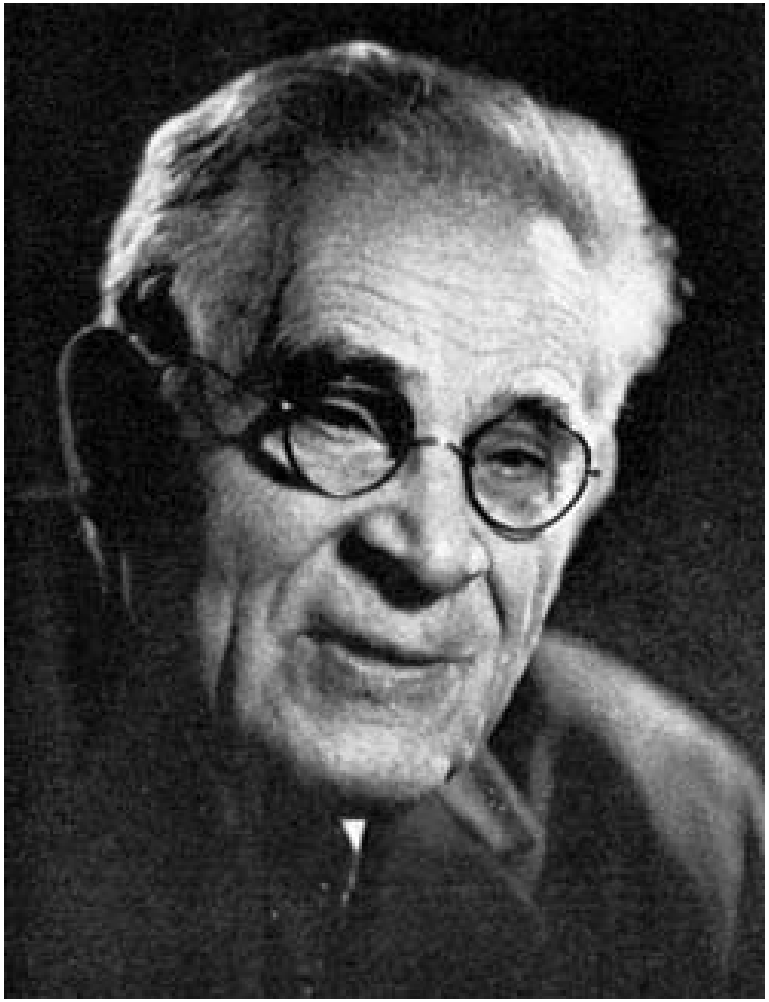
- $E : y^2 = x^3 - x$,
  $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E : y^2 = x^3 - x + 1$,
  $E(\mathbb{Q}) = \langle (1,1) \rangle \cong \mathbb{Z}$.

Exemples



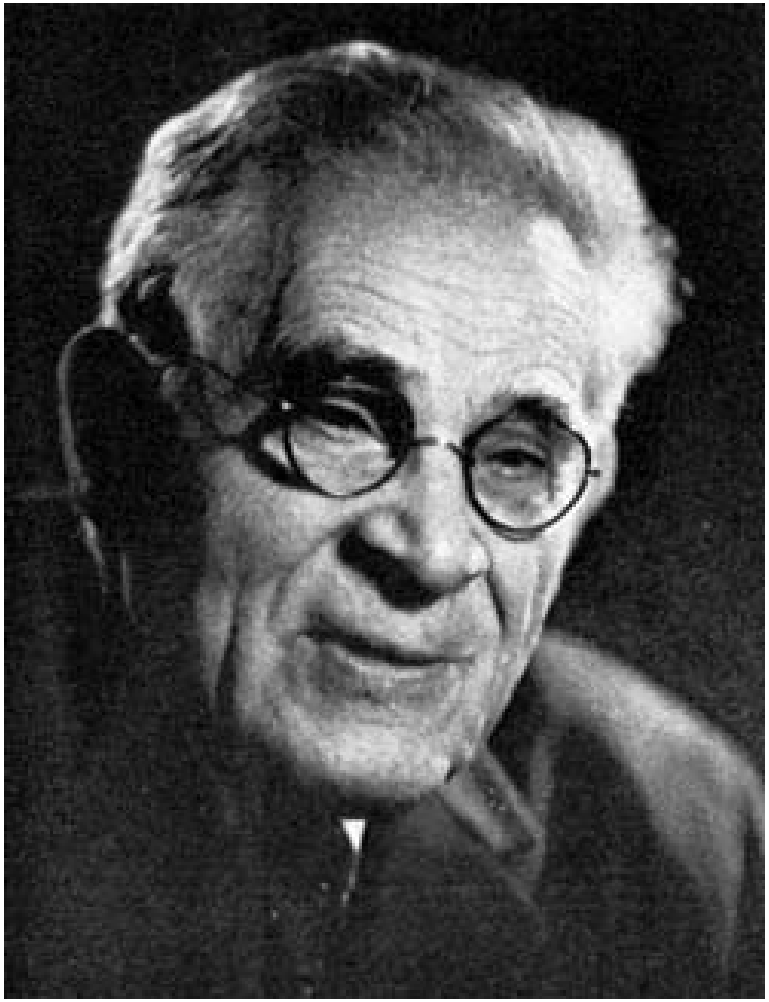
- $E : y^2 = x^3 - x$,
  $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E : y^2 = x^3 - x + 1$,
  $E(\mathbb{Q}) = \langle (1,1) \rangle \cong \mathbb{Z}$.
- $E : y^2 = x^3 - 2$,
  $E(\mathbb{Q}) = \langle (3,5) \rangle \cong \mathbb{Z}$.

Exemples



- $E : y^2 = x^3 - x$, $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E : y^2 = x^3 - x + 1$, $E(\mathbb{Q}) = \langle (1,1) \rangle \cong \mathbb{Z}$.
- $E : y^2 = x^3 - 2$, $E(\mathbb{Q}) = \langle (3,5) \rangle \cong \mathbb{Z}$.
- $E : y^2 + y = x^3 - x^2$, aleshores $E(\mathbb{Q}) = \langle (0,0) \rangle \cong (\mathbb{Z}/5\mathbb{Z})$.

Exemples



- $E : y^2 = x^3 - x$,
  $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
- $E : y^2 = x^3 - x + 1$,
  $E(\mathbb{Q}) = \langle (1,1) \rangle \cong \mathbb{Z}$.
- $E : y^2 = x^3 - 2$,
  $E(\mathbb{Q}) = \langle (3,5) \rangle \cong \mathbb{Z}$.
- $E : y^2 + y = x^3 - x^2$,
  aleshores $E(\mathbb{Q}) =$
  $\langle (0,0) \rangle \cong (\mathbb{Z}/5\mathbb{Z})$.
- $E : y^2 + y = x^3 + x^2 - 2x$,
  aleshores $E(\mathbb{Q}) =$
  $\langle (1,0), (0,1) \rangle \cong (\mathbb{Z})^2$.

Que sabem del rang?

Hi ha qui conjectura que el rang pot ser tant gran com es vulgui (o sigui que hi ha corbes el·líptiques de rank tant gran com es vulgui).

Que sabem del rang?

Hi ha qui conjectura que el rang pot ser tant gran com es vulgui (o sigui que hi ha corbes el·líptiques de rank tant gran com es vulgui).

Hi ha qui conjectura que hi ha un valor màxim pel rank.

Que sabem del rang?

Hi ha qui conjectura que el rang pot ser tant gran com es vulgui (o sigui que hi ha corbes el·líptiques de rank tant gran com es vulgui).

Hi ha qui conjectura que hi ha un valor màxim pel rank.

El rank més gran que sabem segur que es pot aconseguir és 28, i ho va fer Elkies l'any 2006. La corba és

$$y^2+xy+y=x^3-x^2-2006776241557552658503320820933854275093023031217895650 2x+$$

$$+3448161179503055646703298569039072037485594435931918036126600829629193944873224 3429$$

La conjectura de Birch i Swinnerton-Dyer

Hi ha alguna manera de calcular el rang d'una corba el·líptica sense trobar generadors?

La conjectura de Birch i Swinnerton-Dyer

Hi ha alguna manera de calcular el rang d'una corba el·líptica sense trobar generadors?

La conjectura BSD afirma que el rang és igual a l'ordre d'anulació d'una funció (complexa) L en el punt $x = 1$.

La conjectura de Birch i Swinnerton-Dyer

Hi ha alguna manera de calcular el rang d'una corba el·líptica sense trobar generadors?

La conjectura BSD afirma que el rang és igual a l'ordre d'anulació d'una funció (complexa) L en el punt $x = 1$.

És un dels problemes del mil·leni!

Corbes el·líptiques sobre cossos finits.

Si E és una corba el·líptica definida a $\mathbb{Z}/p\mathbb{Z}$, on p és un nombre primer, o més en general, definida sobre un cos finit $\mathbb{F}_q$, on q és una potència d'un nombre primer, aleshores $E(\mathbb{F}_q)$ és un grup finit.

Corbes el·líptiques sobre cossos finits.

Si E és una corba el·líptica definida a $\mathbb{Z}/p\mathbb{Z}$, on p és un nombre primer, o més en general, definida sobre un cos finit $\mathbb{F}_q$, on q és una potència d'un nombre primer, aleshores $E(\mathbb{F}_q)$ és un grup finit.

Aquest grup finit $E(\mathbb{F}_q)$ no pot ser qualsevol grup.

Corbes el·líptiques sobre cossos finits.

Si E és una corba el·líptica definida a $\mathbb{Z}/p\mathbb{Z}$, on p és un nombre primer, o més en general, definida sobre un cos finit $\mathbb{F}_q$, on q és una potència d'un nombre primer, aleshores $E(\mathbb{F}_q)$ és un grup finit.

Aquest grup finit $E(\mathbb{F}_q)$ no pot ser qualsevol grup.

Teorema (Hasse):

$$|\sharp E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Corbes el·líptiques sobre cossos finits.

Si E és una corba el·líptica definida a $\mathbb{Z}/p\mathbb{Z}$, on p és un nombre primer, o més en general, definida sobre un cos finit $\mathbb{F}_q$, on q és una potència d'un nombre primer, aleshores $E(\mathbb{F}_q)$ és un grup finit.

Aquest grup finit $E(\mathbb{F}_q)$ no pot ser qualsevol grup.

Teorema (Hasse):

$$|\sharp E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

A més el grup $E(\mathbb{F}_q)$ és cíclic o bé és producte de dos cíclics, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, amb m dividint n, i m dividint $q-1$.

Corbes el·líptiques sobre $\mathbb{F}_3$.

$$|E(\mathbb{F}_3) - 4| < 2\sqrt{3} = 3,4641016$$

Per tant

$$\sharp E(\mathbb{F}_3) \in \{1, \ldots, 7\}.$$

E	$E(\mathbb{F}_3)$	Grup
$y^2 = x^3 - x - 1$	$\{\infty\}$	0
$y^2 = x^3 - x^2 - 1$	$\{\infty, (2,0))\}$	$\mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + x^2 - 1$	$\{\infty, (1,1), (1,2)\}$	$\mathbb{Z}/3\mathbb{Z}$
$y^2 = x^3 + x$	$\{\infty, (0,0), (2,1), (2,2)\}$	$\mathbb{Z}/4\mathbb{Z}$
$y^2 = x^3 - x$	$\{\infty, (1,0), (2,0), (0,0)\}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 - x^2 + 1$	$\{\infty, (0,1), (0,2), (1,1), (1,2), \}$	$\mathbb{Z}/5\mathbb{Z}$
$y^2 = x^3 + x^2 + 1$	$\{\infty, (0,1), (0,2), (1,0), (2,1), (2,2)\}$	$\mathbb{Z}/6\mathbb{Z}$
$y^2 = x^3 - x + 1$	$\{\infty,(0,1),(0,2),(1,1),(1,2),(2,1),(2,2)\}$	$\mathbb{Z}/7\mathbb{Z}$

Funcions L.

Donada una corba el·líptica E sobre $\mathbb{Q}$, fent un canvi de variables adequat podem suposar que la seva equació té coefficients a $\mathbb{Z}$.

Funcions L.

Donada una corba el·líptica E sobre $\mathbb{Q}$, fent un canvi de variables adequat podem suposar que la seva equació té coefficients a $\mathbb{Z}$.

Per a tots els primers p fora d'un nombre finit S_E, la equació reduïda mòdul p ens dóna una corba el·líptica E_p sobre $\mathbb{F}_p$.

Funcions L.

Donada una corba el·líptica E sobre $\mathbb{Q}$, fent un canvi de variables adequat podem suposar que la seva equació té coefficients a $\mathbb{Z}$.

Per a tots els primers p fora d'un nombre finit S_E, la equació reduïda mòdul p ens dóna una corba el·líptica E_p sobre $\mathbb{F}_p$.
Definim $a_p(E) := p + 1 - \sharp(E_p(\mathbb{F}_p))$.

Funcions L.

Donada una corba el·líptica E sobre $\mathbb{Q}$, fent un canvi de variables adequat podem suposar que la seva equació té coefficients a $\mathbb{Z}$.

Per a tots els primers p fora d'un nombre finit S_E, la equació reduïda mòdul p ens dóna una corba el·líptica E_p sobre $\mathbb{F}_p$.
Definim $a_p(E) := p + 1 - \sharp(E_p(\mathbb{F}_p))$.
Definim la funció

$$L(E,s) = \prod_{p \notin S} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} = \sum_{n \geq 1} a_n n^{-s}$$

Funcions L.

Donada una corba el·líptica E sobre $\mathbb{Q}$, fent un canvi de variables adequat podem suposar que la seva equació té coefficients a $\mathbb{Z}$.

Per a tots els primers p fora d'un nombre finit S_E, la equació reduïda mòdul p ens dóna una corba el·líptica E_p sobre $\mathbb{F}_p$.
Definim $a_p(E) := p + 1 - \sharp(E_p(\mathbb{F}_p))$.
Definim la funció

$$L(E,s) = \prod_{p \notin S} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} = \sum_{n \geq 1} a_n n^{-s}$$

Es verifica que

$$a_1 = 1,\ a_{p^e} = a_p a_{p^{e-1}} - p a_{p^{e-2}}\ a_{nm} = a_n a_m \text{ si } MCD(n,m) = 1$$

Funcions L.

Donada una corba el·líptica E sobre $\mathbb{Q}$, fent un canvi de variables adequat podem suposar que la seva equació té coefficients a $\mathbb{Z}$.

Per a tots els primers p fora d'un nombre finit S_E, la equació reduïda mòdul p ens dóna una corba el·líptica E_p sobre $\mathbb{F}_p$.
Definim $a_p(E) := p + 1 - \sharp(E_p(\mathbb{F}_p))$.
Definim la funció

$$L(E,s) = \prod_{p \notin S} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} = \sum_{n \geq 1} a_n n^{-s}$$

Es verifica que

$$a_1 = 1,\ a_{p^e} = a_p a_{p^{e-1}} - p a_{p^{e-2}}\ a_{nm} = a_n a_m \text{ si } MCD(n,m) = 1$$

Compareu amb la funció zeta de Riemann

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p} \frac{1}{(1 - p^{-s})}$$

Continuació analítica.

La funció $L(E, s)$ està ben definida per la serie si $s \in \mathbb{C}$ i $\mathrm{Re}(s) > 3/2$.

Continuació analítica.

La funció $L(E, s)$ està ben definida per la serie si $s \in \mathbb{C}$ i $\mathrm{Re}(s) > 3/2$.

Teorema(A. Wiles,Breuil-Conrad-Diamond-Taylor) La funció $L(e, s)$ es pot extendre a una funció meromorfa definida a to $\mathbb{C}$ (analítica si hi afeguim algun factor més).

Continuació analítica.

La funció $L(E, s)$ està ben definida per la serie si $s \in \mathbb{C}$ i $\mathrm{Re}(s) > 3/2$.

Teorema(A. Wiles,Breuil-Conrad-Diamond-Taylor) La funció $L(e, s)$ es pot extendre a una funció meromorfa definida a to $\mathbb{C}$ (analítica si hi afeguim algun factor més).
Equivalentment, la funció L és modular.

Continuació analítica.

La funció $L(E, s)$ està ben definida per la serie si $s \in \mathbb{C}$ i $\mathrm{Re}(s) > 3/2$.

Teorema(A. Wiles,Breuil-Conrad-Diamond-Taylor) La funció $L(e, s)$ es pot extendre a una funció meromorfa definida a to $\mathbb{C}$ (analítica si hi afeguim algun factor més).
Equivalentment, la funció L és modular.

És un teorema molt profund i difícil, i que té com a conseqüència una demostració de la última conjectura de Fermat, utilitzant idees de Frey i resultats de Ribet.

La conjectura de Birch i Swinnerton-Dyer

La conjectura BSD afirma que el rang és igual a l'ordre d'anulació la funció (complexa) L en el punt $x = 1$.

La conjectura de Birch i Swinnerton-Dyer

La conjectura BSD afirma que el rang és igual a l'ordre d'anulació la funció (complexa) L en el punt $x = 1$.

S'ha demostrat que si l'ordre d'anulació és 0, el rang és 0, i igualment si és 1.

La conjectura de Birch i Swinnerton-Dyer

La conjectura BSD afirma que el rang és igual a l'ordre d'anulació la funció (complexa) L en el punt $x = 1$.

S'ha demostrat que si l'ordre d'anulació és 0, el rang és 0, i igualment si és 1.

La conjectura també afirma quin és el valor de $L(e, 1)$ si no és zero, o en general del coeficient de Taylor no nul més petit.

La conjectura de Birch i Swinnerton-Dyer

La conjectura BSD afirma que el rang és igual a l'ordre d'anulació la funció (complexa) L en el punt $x = 1$.

S'ha demostrat que si l'ordre d'anulació és 0, el rang és 0, i igualment si és 1.

La conjectura també afirma quin és el valor de $L(e, 1)$ si no és zero, o en general del coeficient de Taylor no nul més petit.

Aquest valor depen de uns quants nombres associats a E, un dels quals és l'ordre d'un grup que no es sap si és finit!