Come fare soldi con le curve ellittiche

L. Göttsche

Le curve ellittiche sono un gioiello della matematica.
Sono state studiate per secoli per la loro bellezza e importanza.

È difficile spiegare la bellezza e l'importanza nella matematica.
Spiegherò solo perché sono utili.

Allora, come si fa a diventare ricchi con le curve ellittiche?

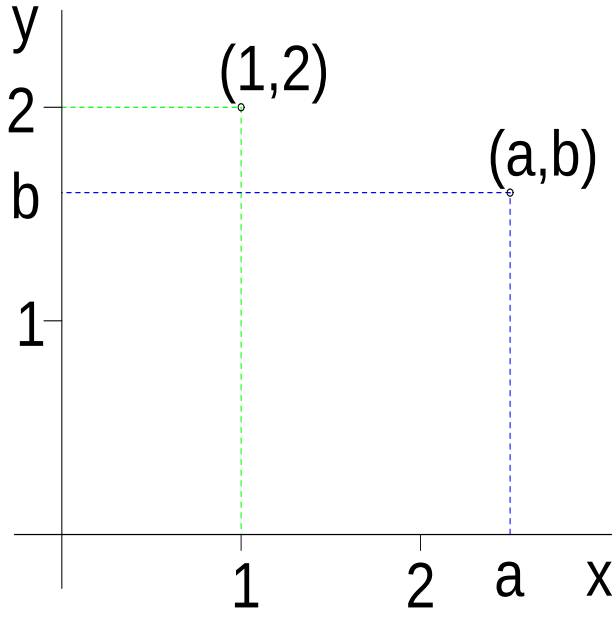
- Rubare soldi dalla banca (illegale)
  impedire che derubino la banca (legale).
- Vincere un premio di un milione di dollari.

Parlerò principalmente del primo punto.

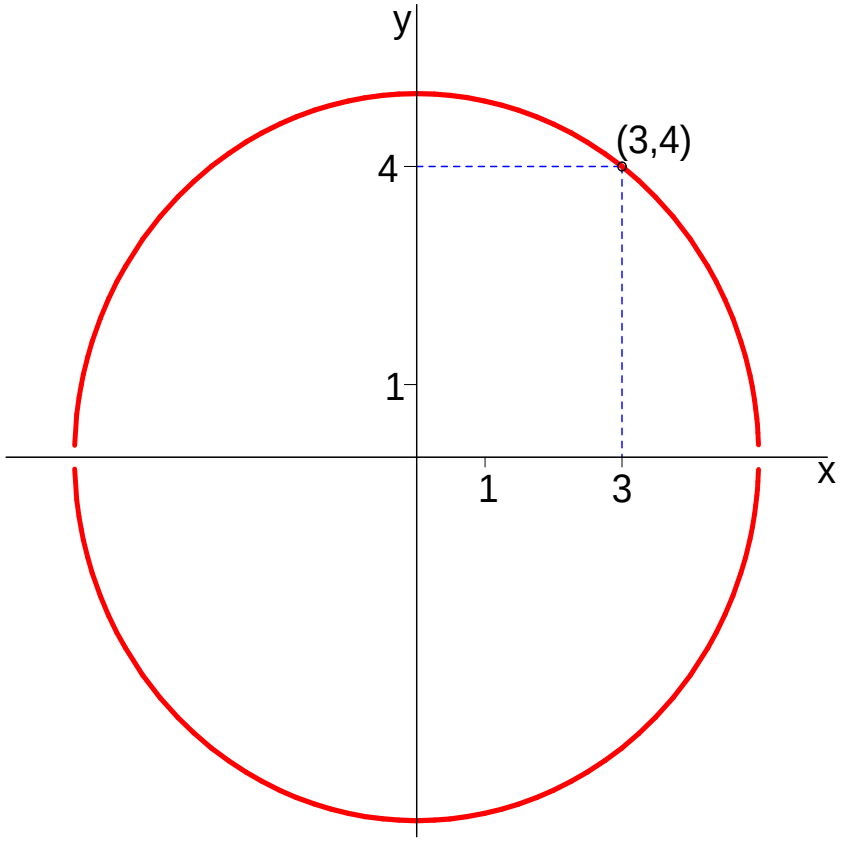
(1) Cosa sono le curve ellittiche

Non sono ellissi! Il nome viene dal fatto che sono legate alla lunghezza di un arco di ellisse.

Piano cartesiano: Due numberi a, b determinano un punto $p = (a, b)$ del piano



Curve: Equazione in $x, y \implies$ curva nel piano:



Esempio: (a, b) è sul cerchio $x^2 + y^2 = 25$ con raggio 5 se

$$a^2 + b^2 = a \cdot a + b \cdot b = 25$$

$3^2 + 4^2 = 9 + 16 = 25$,

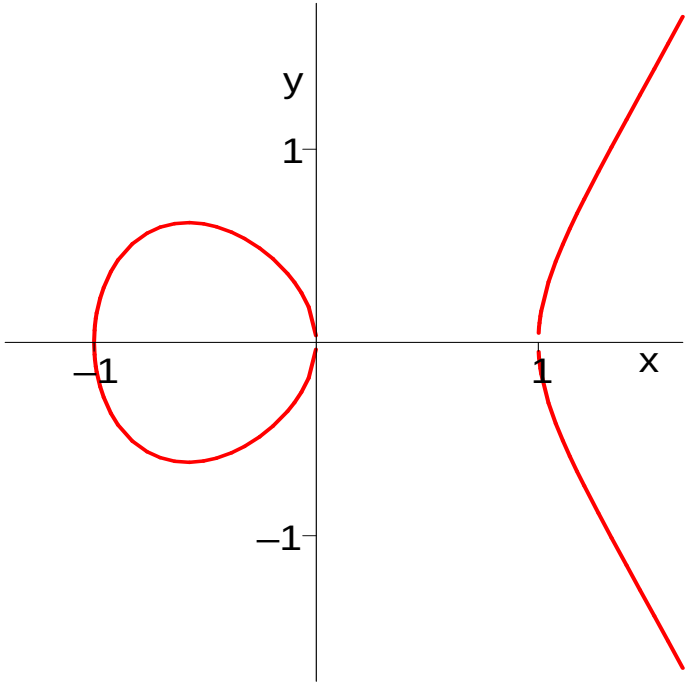
$\implies (3, 4)$ è sulla curva

Curve ellittiche: Equazione $y^2 = x^3 + ax + b$, con a, b numeri fissati

Esempio:

$$y^2 = x^3 - x, \quad (a = -1, b = 0)$$

Le curve ellittiche sono simmetriche rispetto all'asse x:
Se (x, y) e sulla curva, allora anche $(x, -y)$ perché $y^2 = (-y)^2$
(meno per meno fa più)

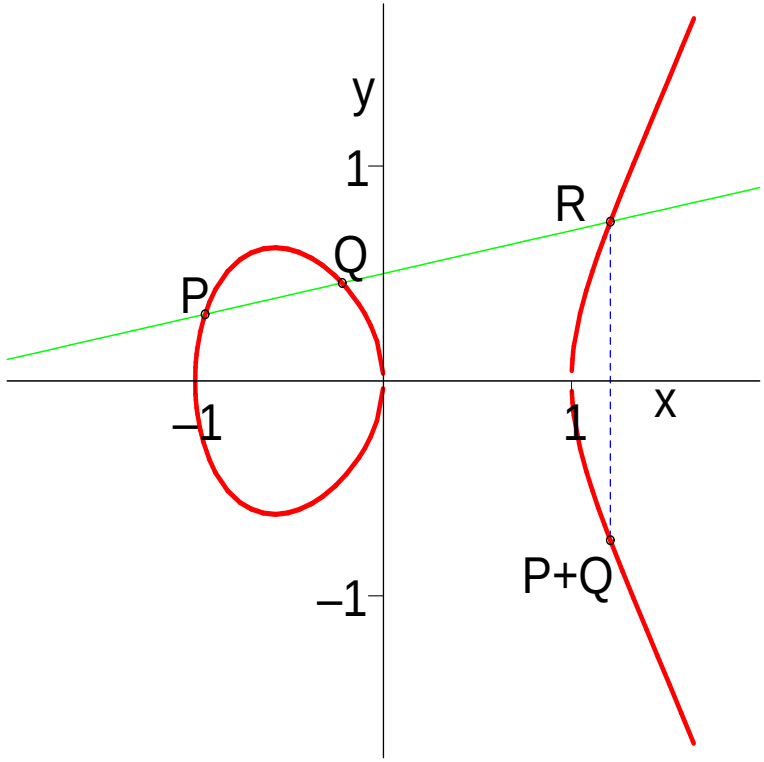


Tutto questo sembra facile, però le curve ellittiche sono fra gli oggetti più difficili e più affascinanti della matematica

(2) Addizione sulle curve ellittiche

Prima sorpresa: Punti su curve ellittiche si possono sommare come se fossero numeri:

Prendiamo due punti P, Q sulla curva. La retta da P a Q interseca la curva in un terzo punto R. $P+Q$ è il punto simmetrico (risp. asse x)



funziona come con i numeri:

Legge commutativa (ovvio)

$P + Q = Q + P$

Legge associativa (per niente ovvio)

$(P + Q) + R = P + (Q + R)$

Si dice: I punti della curva ellittica sono un gruppo commutativo

La somma è molto facile da calcolare

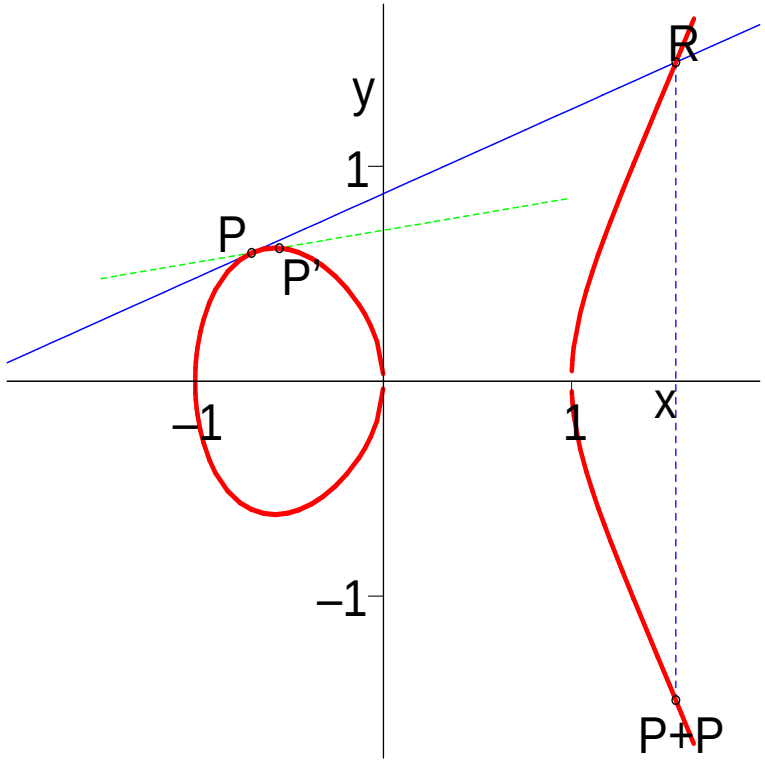
Formula: Per $P = (x_1, y_1)$, $Q = (x_2, y_2)$
la somma è $P + Q = (x_3, y_3)$ con

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,$$
$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1.$$

(Esercizio per il liceo scientifico).

Come si fa $P + P$?

Ci vuole una retta che interseca la curva due volte in P: la tangente (la retta che va nella stessa direzione della curva).
La tangente è il "limite" delle rette che passano per P e per un punto vicino P'.

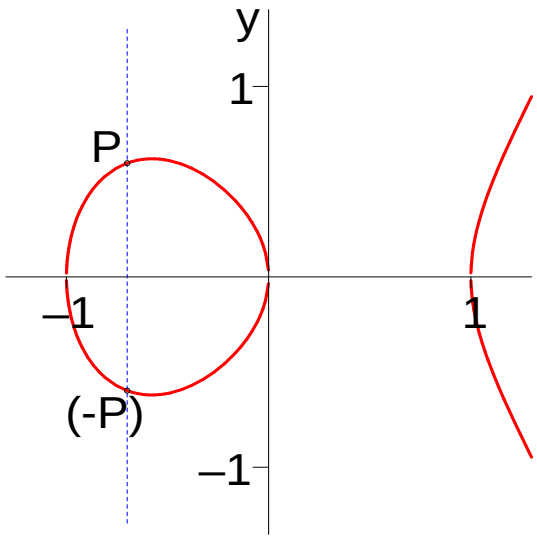


Quindi si possono calcolare multipli di P:

$$5P = P + P + P + P + P.$$

Come si fa $P + (-P)$?

$(-P)$ è il punto simmetrico a P (risp. asse x). Cos'è $P + (-P)$? La retta verticale interseca la curva solo in $P, (-P)$!

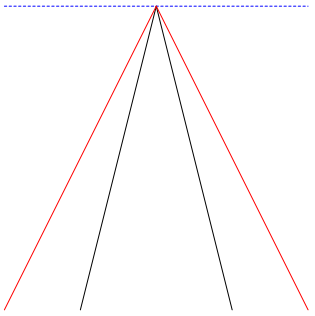


Il terzo punto è all'infinito!! Tutte le rette verticale si intersecano al infinito nello stesso punto 0. (Le rette parallele si intersecano sull'orizzonte). Si vede che per ogni P

$P + (-P) = 0$

$P + 0 = P$

Con queste regole i punti sulla curva sono davvero un gruppo commutativo.



(3) Il primo modo di fare soldi: crittografia

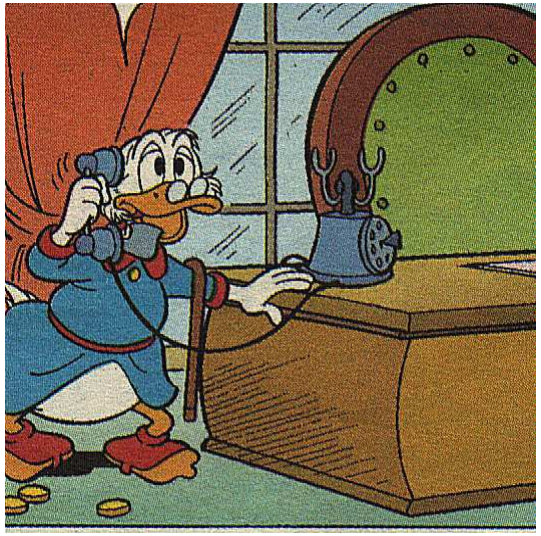
Imbrogliare la banca o impedire che altri lo facciano.

Crittografia: Trasmetti un numero, senza che altri lo capiscano. Siamo in un mondo digitale, allora tutto può essere un numero: codice segreto, carta di credito, telefonata, immagine, lettera.

Idea: Fai qualcosa di facile con in numero, che è molto difficile da disfare (come sciogliere zucchero nel caffé).

Con le curve ellittiche: Molto facile calcolare un multiplo $n \cdot P$ di un punto P su una curva ellittica. Però se tu conosci P e un multiplo $Q = n \cdot P$, è molto difficile calcolare n. Più o meno devi provare tutti i numeri possibili. Anche col computer ci vogliono anni.

In pratica: Zio Paperone telefona a Paperino per dargli la combinazione $N = 23214$ della cassaforte.



Però qualcuno ascolta la telefonata.

Allora Paperone e Paperino si mettono d'accordo su un numero (la chiave) $C = 11234$. Poi Paperone dice $N + C = 34448$ e Paperino sa $N = 34448 - C = 23214$.

Problema: Come far sì che solo Paperino e Paperone sappiano C.

Soluzione: Paperone e Paperino si mettono d'accordo su una curva ellittica e un punto P sulla curva.
Paperone sceglie (segretamente) un numero intero $a = 11$ e dice $A = a \cdot P$ a Paperino
Paperino sceglie (segretamente) un numero intero $b = 13$ e dice $B = b \cdot P$ a Paperone.
Tutti e due calcolano $Q = ab \cdot P$ ($Q = a \cdot B$ per Paperone, $Q = b \cdot A$ per Paperino). Allora la chiave C è la prima coordinata di Q.

I Bassotti conoscono la curva e anche P, A, B. Però anche con il computer ci vogliono anni per trovare a e b e quindi Q.

Tutto questo viene davvero fatto dal computer. È usato per cifrare telefonate col cellulare, il codice segreto (in Francia), comunicazione via internet (pagare con la carta di credito).

Questo metodo è facilissimo per il computer che può essere un chip sul Bancomat o nel telefonino. Ci sono ditte specializzate che hanno molti brevetti sulle curve ellittiche e vivono di questo.

È sicuro? Non c'è un trucco per i Bassotti per determinare più in fretta n da P e nP?

Risposta: Nessuno conosce un trucco. Però non si sa se esiste. Se qualcuno lo trova, sono guai! Può rubare soldi, spiare segreti ecc.
Infatti i matematici hanno trovato trucchi, che funzionano per alcune curve ellittiche. Queste curve non vengono più usate, ma si possono sempre trovare nuovi trucchi.

(4) Vincere 1000 000 $ con le curve ellittiche

Alcuni dei problemi più profondi della matematica sono sulle curve ellittiche. Per la soluzione di quello più importante c'è un premio di 1000 000 $.

Sul cerchio $x^2+y^2=1$ cerchiamo punti $p=(u,v)$ con le coordinate $u=\frac{a}{b}, v=\frac{c}{d}$ frazioni di numeri interi. Per esempio il punto $(\frac{3}{5},\frac{4}{5})$ è sul cerchio.

Si impara al liceo che c'è un numero infinito di questi punti: Per ogni frazione $t=\frac{a}{b}$, il punto $\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$ è sul cerchio, e questi sono tutti. Per esempio per $t=\frac{1}{2}$ si ottiene $(\frac{3}{5},\frac{4}{5})$.

Domanda: Per una curva ellittica, $y^2 = x^3 + ax + b$ il numero dei punti $p = (\frac{c}{d}, \frac{e}{f})$ è infinito?

Risposta: A volte sì a volte no, non c'è nessuna regola.

Congettura di Birch e Swinnerton-Dyer: Basta giocare a battaglia navale.

Battaglia navale ellittica:

Un numero primo è un numero intero che non è un prodotto di altri numeri, per esempio $2, 3, 5, 7, 11$ sono numeri primi ma $6 = 2 \cdot 3$ no.

Fissiamo un numero primo p (per es. $p = 5$) e una curva ellittica $y^2 = x^3 + ax + b$ (per es. $y^2 = x^3 - x$):

Disegniamo una tabella $p \times p$. Per ogni quadratino (u, v) sulla tabella si calcola $v^2 - (u^3 - u)$.

Se questo è divisibile per 5 si fa un punto nel quadratino (u, v) altrimenti no. Per esempio

$1^2 - (1^3 - 1) = 1$ (niente punto a $(1, 1)$),

$4^2 - (2^3 - 2) = 10$ (punto a $(2, 4)$).

Chiama a_p il numero dei punti.

Per esempio per $y^2 = x^3 - x$ abbiamo $a_5 = 7$.

4			•		
3				•	
2				•	
1			•		
0	•	•			•
	0	1	2	3	4

Congettura di Birch e Swinnerton-Dyer (1965): Fissiamo una curve ellittica. Calcoliamo il numero

$$L = \text{Prodotto per tutti numeri primi di} \frac{1}{(1 - \frac{a_p}{p})}$$

La formula corretta è un po' più complicata. (È un prodotto infinito, difficile da calcolare.)
(a) Se $L = 0$ il numero di punti $(\frac{c}{d}, \frac{e}{f})$ sulla curva è infinito.
(b) Se $L \neq 0$ il numero di punti è finito.

È uno dei problemi più difficili della matematica. Alcuni dei matematici migliori hanno lavorato su questo problema usando metodi molto profondi.

Parte della congettura è stata dimostrata da Wiles:

- Il numero L si puo sempre calcolare.

- Se $L \neq 0$ alora il numero di punti è finito.

Lo stesso che nel 1995 ha dimostrato

Ultimo Teorema di Fermat: È impossibile avere $a^n + b^n = c^n$ se $n > 2$.

In realtà, Wiles ha dimostrato una proprietà delle curve ellittiche, da cui seguono entrambi i resultati.

(6) **Ultimo Teorema di Fermat:** $3^2 + 4^2 = 5^2$. L'ultimo teorema di Fermat dice che è diverso per una potenza diversa da 2:

Ultimo Teorema di Fermat (1630): $a^n + b^n = c^n$ per $n > 2$ e numeri interi a, b, c solo se uno di a, b, c è zero.

È stato studiato da alcuni dei migliori matematici di tutti i tempi. È stato dimostrato da Wiles nel 1995 usando le curve ellittiche. Funziona cosi:
Supponiamo che esistano $a, b, c \neq 0$ con $a^n + b^n = c^n$ per $n > 2$. Dimostra che la curva ellittica $y^2 = x(x - a^n)(x - b^n)$ ha proprietà così strane che non può esistere, allora non esistono neanche a, b, c.
La cosa strana di questa curva ellittica è che i numeri a_p (della bataglia navale) non sono distribuiti in modo regolare. Però Wiles ha dimostrato che per ogni curva ellittica questi numeri si comportano in modo regolare.

Un applicazione della conjectura

Domanda: Prendiamo un numero intero n. Esiste un triangolo rettangolo con aria n e le lungezze dei lati frazioni?
È un problema studiato gia da più di mille anni.

Esempio: Per $n = 6$ poi prendere i lati di lungezza $3, 4, 5$.

Risposta: Se la conjettura è vera allora si sa precisamente per quale n funziona:
Funziona per n (dispari) se e solo se ci sono due volte tanti tripli (x, y, z) di numeri interi con $2x^2 + y^2 + 8z^2 = n$ che tripli con $2x^2 + y^2 + 32z^2 = n$. (per ess. $n = 1$ no, $n = 5$ si).

Ragione: Funziona per n precisamente se $y^2 = x^3 - n^2x$ ha un numero infinito di punti.