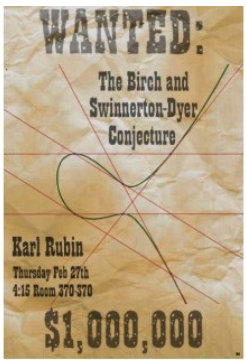
Block Notes Matematico

Congettura di Birch e Swinnerton-Dyer – Curve ellittiche – Fattorizzazione discreta - Crittografia

ing. Rosario Turco[1], prof. Maria Colonnese,

In questo lavoro presenteremo la *congettura di Birch e Swinnerton-Dyer* , il decimo problema di *Hilbert* ed uno dei sette "problemi del millennio", così definito dal ***Clay Mathematics Institute*** che, per questa "settima meraviglia intellettuale", ha messo in palio un milione di dollari, come anche per gli altri sei problemi.



Alla pagina del sito del Clay Mathematics Institute, si può scaricare alla voce "*Official Problem Description*" l'elegante definizione del problema formulata dal matematico *Andrew Wiles*[2]:
http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/

Nel leggere il documento ci si può subito rendere conto che il problema non è di immediata comprensione per chi non è del settore; a dire il vero anche chi sa qualcosina di più di matematica, a volte è in difficoltà a comprendere sempre appieno tutti i concetti concreti dietro ad un'apparente astrattezza. Inoltre spesso occorre una competenza che racchiuda molte branchie della matematica.

L'obiettivo di questo lavoro è, quindi, di evidenziare innanzitutto i concetti dietro la congettura, che ci avvicini a comprendere meglio la definizione finale del problema formulata da Wiles.

Nel lavoro sono mostrati i legami di tale argomento con la Teoria dei Numeri, le curve ellittiche, l'ultimo Teorema di Fermat, le terne pitagoriche, la funzione zeta di Riemann, le funzioni generalizzate di Dirichlet, di Hurwitz , la Teoria dei Gruppi, la Topologia e mostreremo l'interesse emergente per le curve ellittiche nella crittografia e nella fattorizzazione.

Nel lavoro mostreremo infine, in ambito crittografico, alcuni software didattici sviluppati all'uopo dagli stessi autori.

mailto:rosario_turco@virgilio.it

[1] *Rosario Turco è un ingegnere elettronico presso Telecom Italia (Napoli) ed ideatore di "Block Notes Matematico" insieme alla prof. Maria Colonnese del Liceo Classico "De Bottis" di Torre del Greco, provincia di Napoli*
2 Risolutore nel 1994 dell'Ultimo Teorema di Fermat, con una tecnica che coinvolgeva le curve ellittiche

INDICE

FIGURE

TABELLE

Il decimo problema di Hilbert

Il decimo problema di Hilbert diceva: “Trovare un algoritmo per decidere se f(x,y,z,…)=0 ha qualche soluzione razionale”.

Oggi è ancora aperta la seguente questione: “Trovare un algoritmo per decidere, dati due interi a,b se l’equazione $y^2 = x^3 + a * x + b$ ha una soluzione nei numeri razionali”.

Procederemo gradualmente per arrivare alle curve ellittiche, cercando di non appesantire troppo l’argomento per non far perdere il filo logico che ci dovrà condurre alla comprensione della congettura come descritta da Wiles e dei vari legami con altri settori.

Equazioni diofantee

Un argomento di base nella Teoria dei numeri classica, accanto ai concetti di massimo comun divisore, l’identità di Bézout e l’algoritmo di Euclide, è quello delle equazioni diofantine [1], che risalgono al III secolo a.c.

Un’equazione lineare diofantea (di primo grado) è del tipo:

$$ax + by = c \quad \text{con a,b,c} \in \mathbb{Z}$$

L’obiettivo della risoluzione di una equazione diofantea è la verifica dell’esistenza e dell’*ammissibilità di soluzioni intere di una equazione assegnata*.

Esistono vari Teoremi sulle equazioni diofantine (vedi [1]); tuttavia alcuni importanti sono i seguenti.

Nel seguito la scritta d | c significa che d è divisore di c.

Teorema: “ Condizione necessaria e sufficiente affinché l’equazione diofantea

$$ax + by = c \quad \text{con a,b,c} \in \mathbb{Z}$$

ammetta soluzioni intere è che il massimo comun divisore MCD(a,b) divida c, ovvero MCD(a,b)|c.”

Teorema:” Per l’equazione diofantea

$$ax + by = c \quad \text{con a,b,c} \in \mathbb{Z}$$

supponendo che la coppia $(\alpha,\beta) \in \mathbb{Z} \times \mathbb{Z}$ sia una soluzione particolare dell’equazione, allora tutte e sole le soluzioni sono le coppie ordinate $(x,y) = (\alpha + b1h, \beta - a1h)$ dove d = MCD(a,b), a=da1, b=db1, d | c e $h \in \mathbb{Z}$ ”.

Teorema di Bezout:”Siano $a,b \in \mathbb{Z}$ se MCD(a,b) esiste, allora esistono interi h,k tali che:

$$h\,a + k\,b = MCD(a,b)”$$

Esempi

3x+21y=5

L’equazione non ammette soluzioni intere perché MCD(3,21)=3 e 3 non è divisore di 5.

3x+5y=7
L'equazione ammette soluzioni intere perché MCD(3,5)=1 e 1|7.

9x+15y=21
L'equazione ammette soluzioni intere perché MCD(9,15)=3 e 3|21. Inoltre si poteva dividere per 3 entrambi i membri e si otteneva 3x+5y=7 ritornando nell'equazione precedente.

3x+15y=21
L'equazione ammette soluzioni intere perché MCD(3,15)=3 e 3|21. Una soluzione particolare però è data dalla coppia (2,1) con una soluzione generale data da x=2+5h, y=1-h con h$\in \mathbb{Z}$.

Equazioni diofantea di secondo grado

Un'equazione diofantea di secondo grado è un polinomio di secondo grado rispetto ad una variabile ma contiene anche una seconda variabile.

Vediamone un esempio:

$$3x^2 + x\,y - 2x + 5y + 7 = 0$$

Questa è una equazione di secondo grado in x ma presenta y di primo grado. Un modo per risolverla è mettere a fattor comune rispetto ad y:

$$(x+5)\,y = -3x^2 + 2x - 7$$

Da cui:

$$y = \frac{-3x^2 + 2x - 7}{(x+5)}$$

Per risolverla facilmente conviene che il polinomio a numeratore lo scomponiamo ulteriormente rispetto al denominatore con la regola di Ruffini per cui si ottiene:

$$3x^2 - 2x + 7 = (3x - 17)(x + 5) + 92$$

Per cui è:

$$y = -\frac{(3x - 17)(x + 5) + 92}{x + 5} = -\frac{(3x - 17)(x + 5)}{x + 5} - \frac{92}{x + 5} = -3x + 17 - \frac{92}{x + 5}$$

Ora se x e y devono essere interi, allora nel termine 92/(x+5) deve essere x+5 | 92.

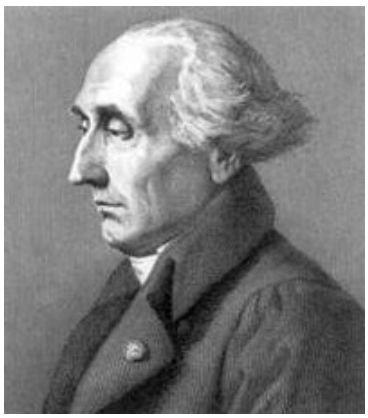
Se scomponiamo in fattori 92= 2*2*23 allora i suoi divisori sono ±1, ±2, ±4, ±23, ±46, ±92, valori che può assumere x+5; per cui x può assumere 12 valori (combinazione dei divisori + 5): −6, −4 −7, −3, −28, 18, −9, −1, −51, 41, −97, 87. Da qui otteniamo i 12 valori di y.

In conclusione le soluzioni x,y sono:

x = −6, x = −4, x = −7, x = −3, x = −28, x = 18, x = −9, x = −1, x = −51, x = 41, x = −97, x = 92,
y = 127, y = −63, y = 84, y = −20, y = 105, y = −41, y = 67, y = −3, y = 172, y = −108, y = 309,
y = −260.

Equazione Fermat-Pell

In generale, l'equazione di **Fermat-Pell** è del tipo $x^2 - Dy^2 = 1$, dove D è un intero positivo che non deve essere un quadrato. Anche qui ci si pone l'obiettivo di trovare soluzioni intere.



Nel 1657 Fermat congetturò che questa equazione ha infinite soluzioni; mentre Lagrange, circa cento anni dopo, lo ha dimostrato.

Figura 1 – Joseph Louis Lagrange

Se non esistono soluzioni intere?

Se una equazione diofantea non ammette soluzioni intere, in realtà vedremo che potremmo essere interessati a trovare soluzioni razionali (interi o frazioni), cosa che esamineremo nel seguito.

Teorema di Pitagora e le coniche

Figura 2 - Pitagora

L'equazione del Teorema di Pitagora è una particolare equazione diofantea, applicata ad un triangolo rettangolo:

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

Supponendo a,b,c coprimi tra loro, l'equazione di sopra ci conduce, dividendo entrambi i membri per c^2, all'equazione:

$$x^2 + y^2 = 1 \quad x=a/c,\ y=b/c$$

che è l'equazione di una *particolare conica*, il *cerchio di raggio unitario*.

Un punto di questo cerchio P(-1,0) è, per la definizione di x e y, una soluzione razionale della equazione di sopra.

Se consideriamo una retta che interseca il cerchio passando per P(-1,0), con coefficiente angolare t = m/n razionale, allora l'equazione della retta è:

$$y = t(x+1)$$

Se nell'equazione del cerchio sostituiamo quest'ultima, otteniamo che:

$$x^2+t^2x^2+t^2+2xt^2-1=x^2(1+t^2)+2xt^2+t^2-1=0$$

Se P(-1,0) o x=-1 è una soluzione, allora è possibile dividere il polinomio di cui sopra per (x+1) e si ottiene:

$$(x+1)[(1+t^2)x+t^2-1)]$$

Da cui è:

$$x=\frac{1-t^2}{1+t^2} \quad y=\frac{2t}{1+t^2}$$

Poiché t è razionale, anche x e y sono razionali al variare di t in Q.

Ovviamente è possibile fare analoghi discorsi con ellissi, parabole e iperboli, anche qui con soluzioni razionali.

Pitagora, l'area di un triangolo rettangolo ed i numeri congruenti

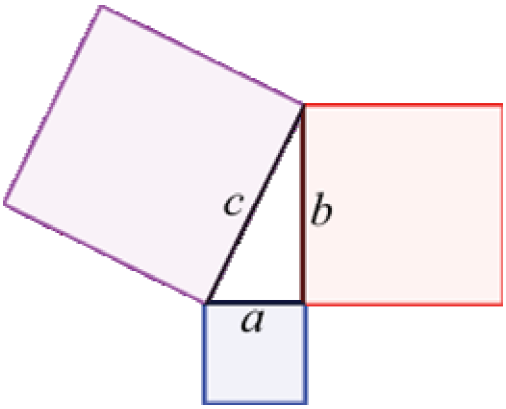


Figura 3 – Teorema di Pitagora

Se a,b,c∈ℚ, sono le misure razionali (interi o frazioni) dei lati di un triangolo rettangolo di area d=1/2 a * b, allora d è detto **numero congruente**.

In altri termini d rispetta le due equazioni del Teorema di Pitagora e dell'area del triangolo:

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

$$d=\frac{1}{2}ab$$

Se a,b,c sono coprimi tra loro abbiamo a che fare con una terna pitagorica primitiva. Se non sono primi tra loro ma hanno tutti un fattore comune è sufficiente dividere la relazione di Pitagora ad ambo i membri per il fattore comune.

Esempi di numeri congruenti

d=1 non è un numero congruente perché non rispetta il Teorema di Pitagora.
d=6 è un numero congruente con a=3,b=4,c=5
d=5 è un numero congruente con a=3/2,b=20/3,c=41/6
d=157? Questo lo lasciamo svolgere a voi. E' sicuramente congruente.

Ultimo Teorema di Fermat

Figura 4 - Pierre de Fermat

L'ultimo Teorema di Fermat afferma che:"L'equazione:

$$x^n + y^n = z^n$$

con x,y,z$\neq$0 non ha soluzioni intere per n$\geq$3".

L'equazione di sopra è una particolare equazione diofantea come lo è anche l'equazione del teorema di Pitagora. La dimostrazione di questo Teorema da parte di Wiles ha richiesto l'uso della congettura di Taniyama-Shimura, l'uso delle funzioni ellittiche e l'uso delle forme modulari. La dimostrazione del Teorema si fa per assurdo:

1. Si ipotizza che esistano degli interi a,b,c non nulli per l'equazione di sopra e per n$\geq$3.
2. Si considera l'equazione cubica $y^2 = x(x - a^n)(x + b^n)$ che è una curva piana, detta ellittica, e si dimostra che non può esistere perché sarebbe un contro-esempio della congettura di Taniyama-Shimura,

Come escono fuori le curve ellittiche? Ritorniamo a Pitagora e ai numeri congruenti visti prima!

Curve ellittiche e l'idea di Birch e Swinnerton-Dyer

Se ci rifacciamo alle equazioni del Teorema di Pitagora e dell'area del triangolo e poniamo:

$$x=(\frac{c}{2})^2 \quad y=\frac{(a^2-b^2)c}{8}$$

Otteniamo un'equazione cubica (*curva ellittica*):

$$y^2=x^3-d^2x$$

Non confondiamo però le curve ellittiche con le ellissi: sono cose diverse. Il nome delle curve ellittiche discende dagli integrali ellittici, cioè quando si iniziò a calcolare la dimensione di archi di curve ricavate da ellissi. Il nome più corretto per queste equazioni cubiche sarebbe "*varietà Abeliane di dimensione 1*".

Sono un ponte tra Algebra e Geometria dovuto ad *Abel, Gauss, Jacobi e Legendre*.

Mentre sulle equazioni quadratiche si sa tutto, le cubiche sono ancora oggetto di studio. In sostanza sono veri i seguenti Lemmi:

"*Esiste un triangolo rettangolo con lati razionali se l'equazione ellittica* $y^2=x^3-d^2x$ *ammette soluzioni per y*$\neq$*0*".

"*Dati due numeri razionali che soddisfano l'equazione ellittica* $y^2=x^3-d^2x$ *,con y*$\neq$*0, allora d è un numero congruente".*

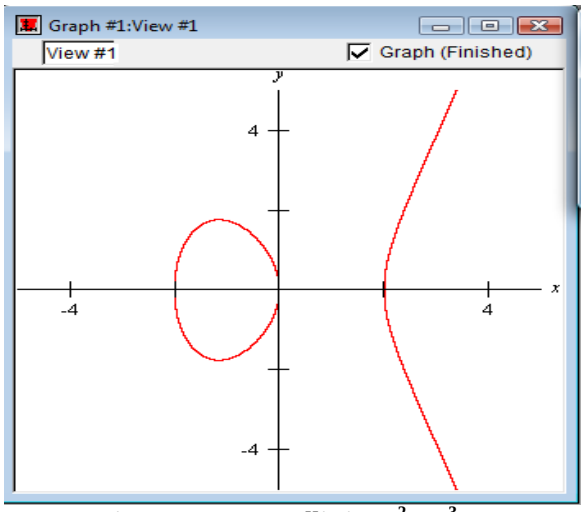


Figura 5 – curva ellittica $y^2 = x^3 - 4x$

Per $y^2=x^3- d^2x$, con y=0, si avrebbero le soluzioni banali: ($\pm$d,0) e (0,0). Una soluzione razionale y$\neq$0 è detta **punto di ordine infinito**. La sua esistenza equivale al l'esistenza di infinite soluzioni razionali.

Il problema è che, attualmente, non esiste un algoritmo che provi questo, cioè se l'equazione abbia per y$\neq$0 una soluzione razionale.

La congettura di Birch e Swinnerton-Dyer punta a risolvere questo problema, come vedremo.

La **forma generale di una equazione ellittica** (*forma normale di Weiestrass*) è del tipo:

$$y^2 = x^3 + ax + b$$

In realtà una forma anche con la presenza di x^2 è s Weiestrass con trasformazioni razionali del tipo:

$$x \to \frac{Ax + B}{Cx + D}$$

La quantità $\Delta=4a^3 + 27b^2$ è detta **discriminante** della equazione ellittica.

La condizione $\Delta=4a^3 + 27b^2 \neq 0$ è *una condizione necessaria e sufficiente* affinché la curva ellittica in forma normale di Weiestrass abbia 3 radici distinte (reali o complesse).

Se $\Delta=4a^3 + 27b^2 = 0$ la curva ellittica è **singolare**. Se la curva ha tre radici il grafico è fatto da due parti di curve, se ha una radice il grafico si presenta come in figura 3 che rappresenta l'equazione ellittica $y^2 = x^3 - x + 1$

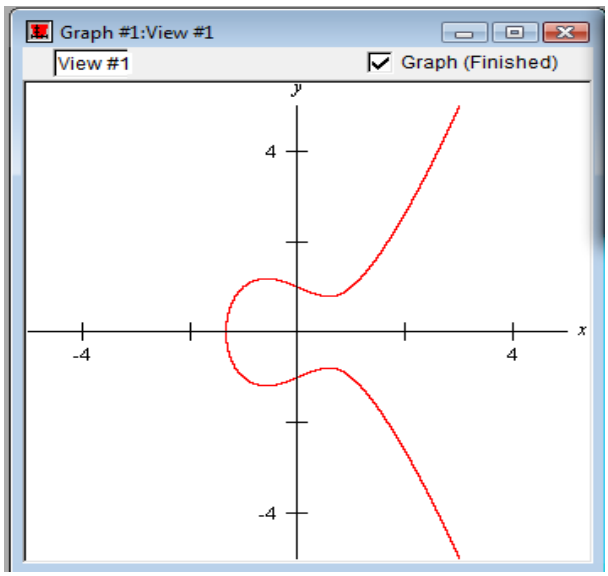


Figura 6 – curva ellittica $y^2 = x^3 - x + 1$

Una *curva ellittica non singolare* è l'insieme E di soluzioni (x,y) $\in \mathbb{R}$ x $\mathbb{R}$ dell'equazione

$$y^2 = x^3 + ax + b$$

insieme ad un punto speciale O detto punto all'infinito.

L'idea di Birch e Swinnerton-Dyer

In pratica potremmo trovarci di fronte a infiniti elementi sulla curva ellittica; a volte un modo per aggirare l'ostacolo e che funziona è quello di lavorare su un numero limitato di elementi, scegliendo un numero primo p (a piacere) e usando l'aritmetica modulare Z_p (classe dei resti modulo p).Ovviamente vedremo che parlare di Zp è lo stesso di parlare di Fp o campo.([3])

Figura 7 – Peter Swinnerton-Dyer (2 agosto 1927)

In particolare scegliamo un numero primo p perché così le divisioni in mod p restituiscano correttamente degli interi. Per cui anziché cercare le infinite soluzioni della equazione ellittica

$$y^2 = x^3 + ax + b$$

Cercheremo, invece, di contare le soluzioni (x,y) dell'equazione:

$$y^2 = x^3 + ax + b \mod p$$

Con **Np** indicheremo *il numero di coppie (x,y) aumentato di una unità* per tener conto del punto all'infinito; mentre chiamiamo $\mathbf{a_p}$ = p – Np.

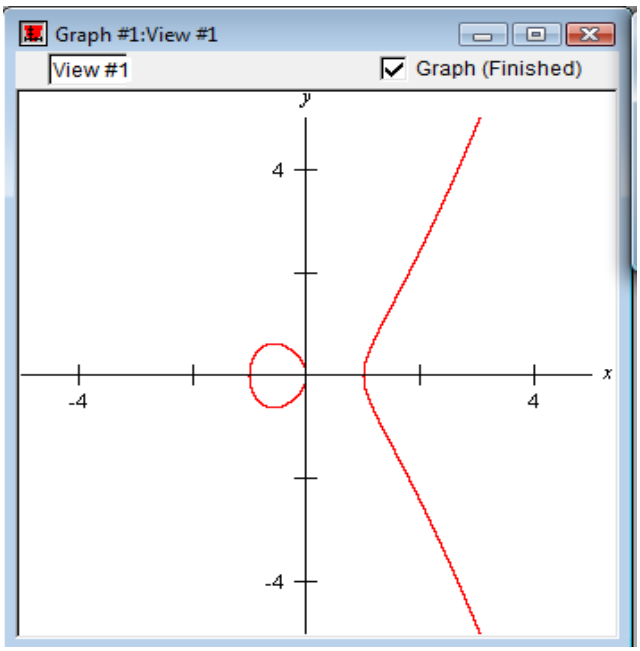


Figura 8 – equazione $y^2 = x^3 - x$

Supponiamo di voler studiare la curva di fig.4 con l'aritmetica modulare scegliendo p=5:

$$y^2 = x^3 - x \bmod 5$$

A questo punto per x = 0,…,4 e y = 0,…,4 le possibili soluzioni sono:

(0,0), (1,0), (4,0), (2,1), (3,2), (3,3), (2,4)

Per cui

$$N_5=7+1=8$$

In PARI/GP si può scrivere un piccolo algoritmo, ad esempio, e facendo variare x e y si verifica se l'identità $y^2 = x^3 - x \bmod 5$ è soddisfatta. Se è verificata si è trovata una coppia (x,y).

[3] un **campo** è una struttura algebrica, composta da un insieme *K* e due operazioni binarie, chiamate *somma* e *prodotto* e indicate rispettivamente con + e *, che godono di proprietà simili a quelle verificate dai numeri interi, complessi, razionali, reali, p-adici etc: ogni operazione deve dare un elemento appartenente al campo abeliano, il campo abeliano (K,+) è dotato di elemento neutro 0 e (K\{0},*) è dotato di elemento neutro 1 e $\forall a \neq 0 \ \exists (a^{-1})$ tale che $a*a^{-1} = a^{-1}*a = 1$ (elemento inverso) e la moltiplicazione è distributiva rispetto alla somma.

Il concetto che sta dietro a questa idea è che se (u,v) sono una soluzione dell'equazione generale $y^2 = x^3 + ax + b$ allora le coppie (u mod p, v mod p), per ogni p, soddisfano le congruenze mod p di $y^2 = x^3 + ax + b \bmod \mathrm{p}$.

Per cui se sulla curva ellittica di forma generale esiste un punto razionale allora sicuramente, per ogni numero primo p, esiste almeno una soluzione della congruenza mod p.

L'esistenza di molte soluzioni per le congruenze mod p, per molti numeri primi p, non è detto che corrisponde a una soluzione razionale sulla curva ellittica. O per lo meno non è stata ancora dimostrata.

E' quest'ultima cosa che, invece, supposero negli anni '60 come vero Birch e Swinnerton-Dyer. In altri termini hanno supposto che l'esistenza di molte soluzioni delle congruenza mod p, per molti p, comporta infinite soluzioni sulla equazione ellittica.

Il secondo passo: la verifica sui dati
Il problema era come fare a verificare che esistono molte soluzioni corrispondenti a molte soluzioni delle congruenze?

Si introduce una "funzione densità" $\prod_{\mathrm{p}\le \mathrm{M}} \frac{\mathrm{p}}{N_p}$ (una funzione in prima battuta semplificata per far comprendere il concetto).

Si valuta, poi, tale densità sui dati, per valori di M crescenti, e si cerca di descrivere l'andamento di questa funzione di densità con una formula migliore e rivista

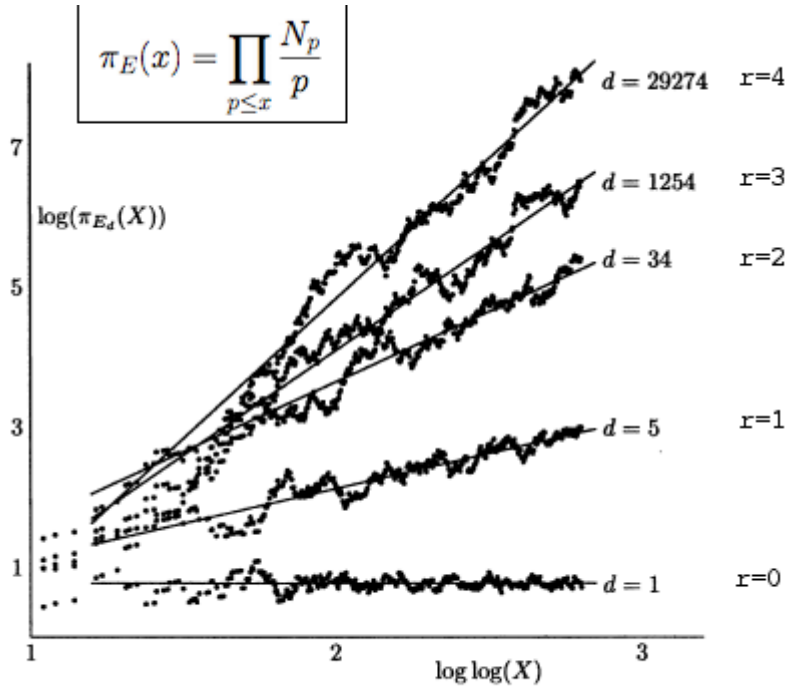
Perché usare la funzione densità? Il ragionamento è una conseguenza di prima: se sulla curva ellittica esistono infiniti punti razionali ci attendiamo che per molti numeri primi p avremo molte soluzioni sulle congruenze mod p e di conseguenza il prodotto del rapporto tende a zero (perché per molti p il rapporto p/Np è molto inferiore di 1).

Birch e Swinnerton-Dyer consideravano che se r = rango(E($\mathbb{Q}$)) era grande (molte soluzioni) allora si aspettavano di avere molti punti su E(Fp). In pratica era una "*reduction map*" $\mathrm{E}(\mathbb{Q}) \to \mathrm{E}(\mathrm{Fp})$.

Adottarono una ipotesi di densità iniziale come quella descritta nel paragrafo precedente;anzi per comodità inizialmente usarono la quantità inversa:

$$\pi_E(x) = \prod_{\mathrm{p}\le x} \frac{\mathrm{Np}}{p}$$

Per varie curve ellittiche calcolarono $\pi_E(x)$ con la speranza che esso dovesse crescere rapidamente al crescere di r = $r_{E.}$



Birch and Swinnerton-Dyer data for $y^2 = x^3 - d^2x$

Dall'analisi dei dati essi osservarono che $\log \pi_E(x)$ cresce come $r_E \log\log x$. La loro prima formulazione della congettura fu:

"Per varie curve ellittiche definite su $\mathbb{Q}$,

$$\pi_E(x) \sim C_E(\log x)^{r_E}$$

per qualche costante C_E e r_E rango di $E(\mathbb{Q})$".

La L-function

La densità definita prima, ricordava molto da vicino l'espressione della funzione zeta di Riemann [12] attraverso il prodotto infinito di Eulero:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

In [12] abbiamo visto che è possibile generalizzare la funzione di Riemann passando alla L-function di Dirichlet che qua va applicata ai campi finiti E/Fp; per cui - consentiteci un volo pindarico di enorme semplificazione a vantaggio del filo logico - Birch e Swinnerton-Dyer ipotizzarono che era possibile dimostrare (ma nel 1960 non era così) che esistesse una funzione L(E,s) su tutto l'insieme delle curve ellittiche E, che dava una soluzione per ogni numero complesso s e che potesse essere studiata con i metodi di calcolo infinitesimale, tale che

$$L(E,1) = \prod_p \frac{p}{Np} = 0$$

Con L dipendente da E, perché Np dipende dalla curva ellittica con s=1 e L(E,1)=0 perché il produttorio tende a zero.

In sostanza l'espressione completa che Birch e Swinnerton-Dyer usarono fu la funzione densità di *Hasse-Weil*:

$$\zeta(\text{En/Fp, s}) = \text{L(En, s)} = \prod_p \frac{1}{1\text{-a}_p\text{p}^{\text{-s}} + p^{1-2s}}$$

Dove En è la curva ellittica e p varia tra i primi che non dividono n. Nota: se si pone s=1 nella funzione di Hasse-Weil si ottiene quella semplificata.

Il prodotto infinito di sopra può essere visto come il limite per k che tende all'infinito del prodotto finito per $p \leq k$. Il prodotto infinito converge per $s \geq 3/2$ (lo vedremo dopo).

Dagli anni '60 ad oggi
In particolare negli anni '60 la prima formulazione della congettura di Birch e Swinnerton-Dyer fu:
"$y^2=x^3-n^2x$ ha una soluzione razionale per $y \neq 0$, se e solo se L(En,1)=0"

Negli anni '70 si era arrivati al ***Teorema di Coates - Wiles****: "Se $y^2=x^3-n^2x$ ha una soluzione razionale per $y \neq 0$, allora L(En,1)=0". Il viceversa era la congettura da dimostrare!*

Solo dagli anni '90 sappiamo che esiste una funzione L(E,s) ben definita per ogni s grazie alla *congettura di Taniyama-Shimura* dimostrata da Andrew *Wiles e Richard Taylor* per la dimostrazione dell'Ultimo Teorema di Fermat.

Oggi occorre dimostrare che poiché esiste L(En,s) che è ben definita, allora esistono infiniti punti razionali su E se e solo se L(En,1)=0. Sappiamo inoltre che se $\text{L(En,1)} \neq 0$ allora n non è un numero congruente. D'altra parte se L(En,1)=0 e vale la congettura di Birch e Swinnerton-Dyer allora n è congruente,

Esiste un algoritmo che ci permette di determinare se è vero che L(En,1)=0?

Negli anni '80 è stato introdotto il **Teorema di Tunnel**: "Se n è dispari, allora L(En,1)=0 se e solo se il numero delle soluzioni intere dell'equazione $2x^2+y^2+8z^2=n$ è uguale due volte al numero delle soluzioni intere dell'equazione $2x^2+y^2+32z^2=n$. Se n è pari , allora L(En,1)=0 se e solo se il numero delle soluzioni intere dell'equazione $4x^2+y^2+8z^2=n$ è uguale due volte al numero delle soluzioni intere dell'equazione $4x^2+y^2+32z^2=n$"

Questo Teorema permette di mettere su un **algoritmo effettivo congetturale** per vedere se L(En,1)=0.

Nel 1990 è stato formulato anche il **Teorema di Monski**: "Sia n un numero primo, se n è della forma 3+8k allora n non è congruente e 2n è congruente. Se n è della forma 5+8k allora n è congruente e 2n non è congruente. Se n è della forma 7+8k allora n e 2n sono congruenti"

La dimostrazione di quest'ultimo teorema, usando la **teoria della moltiplicazione complessa**, porta alla costruzione di soluzioni non banali per le equazioni $y^2=x^3-n^2x$ e $y^2=x^3-(2n)^2x$

Infine esiste il **Teorema**:
"Se $\text{L(E,1)} \neq 0$ allora $\text{E} : \text{y2} = \text{x3} + \text{ax} + \text{b}$ ha un numero finito di soluzioni razionali".

"Se L(E,s) ha uno zero semplice in s=1, cioè L(E,1)=0 e $\lim_{s \to 1} \frac{L(E,s)}{(s-1)} \neq 0$ allora $\text{E} : \text{y2} = \text{x3} + \text{ax} + \text{b}$ ha infinite soluzioni razionali".

Questo Teorema mette insieme tutti i risultati precedenti.

Adesso affrontiamo l'argomento in ambito sia della Topologia (come da impostazione di Wiles) che della Teoria dei gruppi. Non ci sembra un caso che si dovesse passare anche per la Teoria dei Gruppi, già Abel e Galois avevano mostrato che per verificare se un'equazione ammette soluzioni occorre farlo nell'ambito della Teoria dei Gruppi.

Andrew Wiles

Figura 9 – Andrew Wiles

Per comprendere a fondo il documento di Wiles, si deve affrontare lo stesso argomento della congettura introducendo concetti di topologia [13], il cui fondatore è Poincarè.

Se consideriamo il problema di trovare le soluzioni ad una equazione polinomiale (assolutamente irriducibile) in due variabili con coefficienti interi o razionali f(x,y)=0, il problema aumenta di difficoltà appena aumenta il grado dell'equazione. Una misura del grado di difficoltà nel risolvere l'equazione f(x,y)=0 è il *genus o genere* di una equazione o di una superfice (il numero di manici …)

Nelle figure successive facciamo vedere esempi di superfici (varietà topologiche), che permettono un po' di comprendere il genere g.

Figura 10 - sfera g=0 e toro g=1

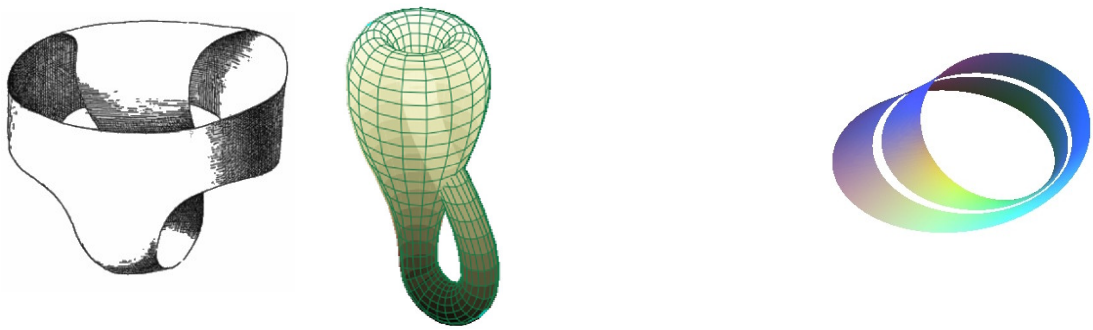


Figura 11 – slip di Moebius g=2 – bottiglia di Klein g=2 – nastro di Moebius g=1

Ci si pone ovviamente la domanda: “Ma le curve ellittiche sono figure nel piano, equazioni cubiche, perché arrivare alle superfici?”. La risposta è molteplice: da una parte i matematici si sforzano di generalizzare e quindi salgono di grado sui polinomi, perché sperano che ci sia già un Teorema risolto che possa aiutare (abbastanza raro), sia per battere nuove strade; spesso la fama di alcuni di loro è dipesa da questo “cambiar strada”. Anche perché ormai si è compreso che quasi tutti i settori della matematica sono collegati ed i risultati in uno di essi possono essere utili in altri.

Cerchiamo adesso di approfondire da un punto di vista topologico.

Se consideriamo l’insieme $X(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 : f(x, y) = 0\}$ di soluzioni complesse di f(x,y)=0 e lo completiamo aggiungendo i punti all’infinito ed eliminiamo eventuali singolarità, otteniamo una superfice di Riemann $\hat{X}$.

In topologia $\hat{X}$ è una superfice compatta orientata e indichiamo con g il suo genere.

A grandi linee quello che oggi sappiamo circa le soluzioni razionali di f(x,y)=0 è che ci sono vari casi a seconda del valore di g, rientrando ovviamente in quello visto precedentemente.

Caso g=0

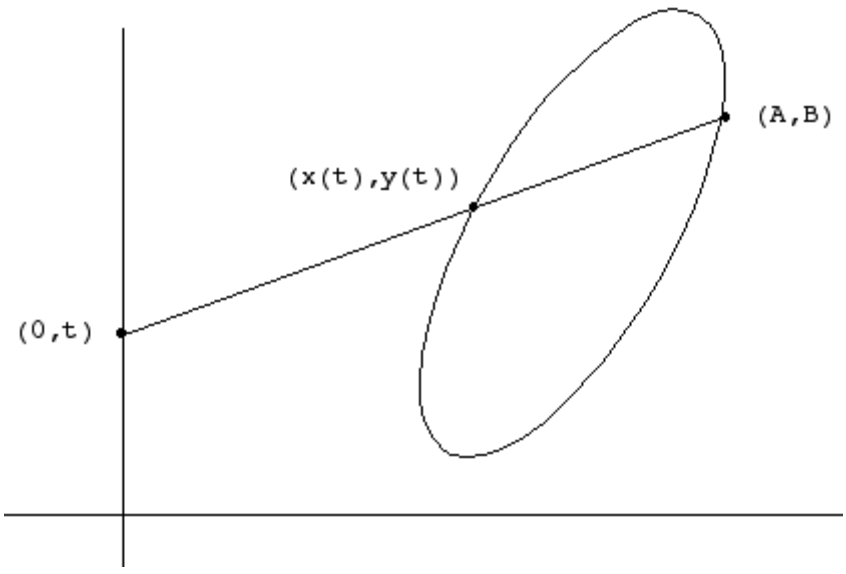
Questo, ad esempio, è quello che succede se il grado(f) = 1 o 2. L’insieme $X(\mathbb{Q})$ delle soluzioni razionali dipende dal grado(f).

Se grado(f)=1 abbiamo infiniti punti (che formano una “1-parameter family” o famiglia parametrica 1).

Se grado(f)=2 è un problema decidere se $X(\mathbb{Q})$ è vuoto. In realtà il problema è risolto con il **principio di Hasse**: “*$X(\mathbb{Q})$ è non vuoto se e solo se vi sono soluzioni reali e soluzioni p-adiche per ogni numero primo p*”; ovvero:

$$X(\mathbb{Q}) \neq \varnothing \Leftrightarrow X(\mathbb{R}) \neq \varnothing \text{ and } X(\mathbb{Q}p) \neq \varnothing \ \forall p$$

Comunque appena si ottiene una soluzione $(A,B) \in X(\mathbb{Q})$ possiamo avere parecchi punti razionali e possiamo parametrizzarli su una retta.



Caso g=1

Questo è il caso se $f(x,y) = y^2 - x^3 - ax - b$ e $x^3 + ax + b$ hanno radici distinte. In questo l'insieme delle soluzioni X(ℚ) può essere finito (anche vuoto) o infinito. E non esistono algoritmi che possano decidere questo al momento. Se permettiamo l'uso dei punti all'infinito, quando X(ℚ) non è vuoto possiamo costruire un gruppo Abeliano.

Caso g>1

Esiste il risultato dovuto a *Faltings*: X(ℚ) è finito. Ma anche qui non esiste un algoritmo per decidere se è vuoto oppure no e quali sono gli elementi.

A questo punto esamineremo nel dettaglio il caso g=1, quello più sfruttabile al momento esaminandolo con le curve ellittiche.

Le curve ellittiche e la Teoria dei gruppi

Figura 12 – Henri Poincarè

L'interesse per le curve ellittiche è nato nel 1901 col contributo di Henri Poincarè, il quale mostrò che ad ogni curva ellittica è associato un particolare gruppo.

Gli elementi del gruppo sono i punti della curva che hanno per coordinate dei numeri razionali.

Indicheremo con E(ℚ) l'insieme della curva i cui elementi (x,y) ∈Q e a cui dobbiamo aggiungere il punto all'infinito che giace su tutte le rette verticali.

Per fare di E(ℚ) di un gruppo è necessario definire un'operazione somma.

.

Data un curva **E su** ℝ vogliamo calcolare **P + Q** dove P = (x1,y1) e Q = (x2, y2).

Esistono tre casi:

- Caso x1≠x2
- Caso x1=x2 e y1 = - y2
- Caso x1 = x2 e y1 = y2

In tal caso otterremo che **(E, +) è un gruppo Abeliano**, nel quale **O** è l'elemento **identità**, tale che:

$$\forall P \in E \quad P+O=O+P=P$$

Caso x1≠x2

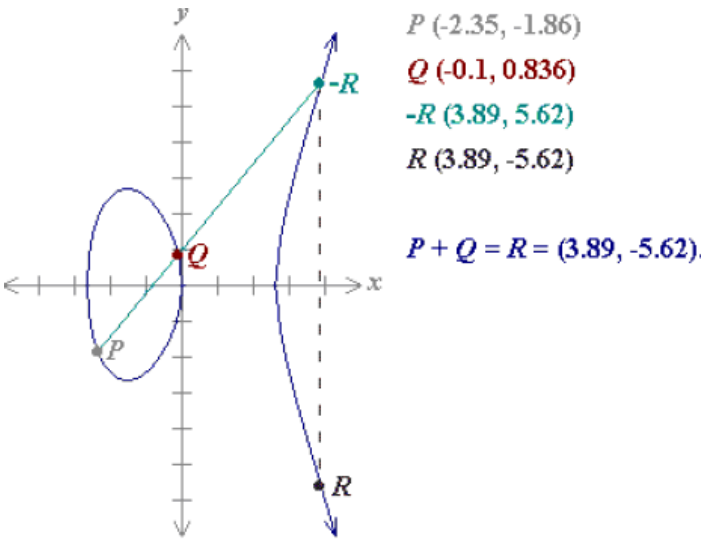


Figura 13 – $y^2 = x^3 - 7x$

Effettuiamo i seguenti passi:

- sia L la retta passante per P e per Q
- L interseca E in un terzo punto, che chiamiamo R'
- sia R il simmetrico di R' rispetto all'asse delle x
- poniamo P + Q = R

In pratica, le coordinate di R = (x3, y3) sono:

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Caso x1=x2 e y1 = - y2

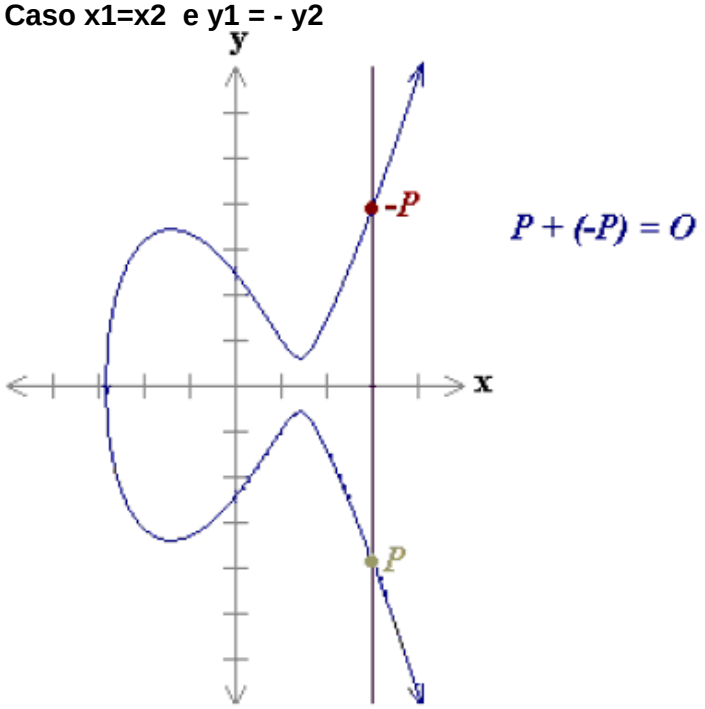


Figura 14 – $y^2 = x^3 - 6x + 6$

Se x1 = x2 e y1 = -y2 allora

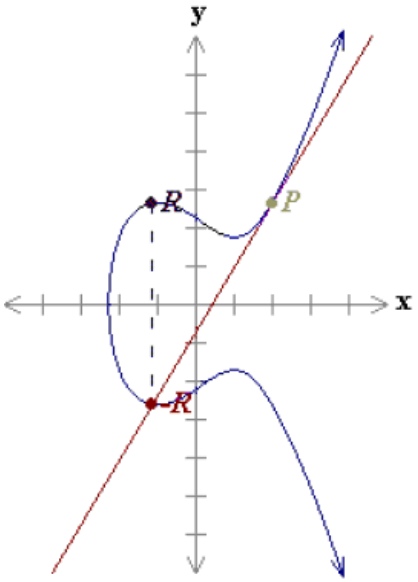
P+Q=O

Infatti:

(x,y) + (x,-y) = O per ogni (x,y)∈E

Questo vuol dire che (x,y) è l'**inverso** rispetto a (x,-y).

Caso x1=x2 e y1 = y2



P (2, 2.65)

$-R$ (-1.11, -2.64)

R (-1.11, 2.64)

$2P = R = (-1.11, 2.64)$

Figura 15 – $y^2 = x^3 - 3x + 5$

In questo caso stiamo sommando P a sé stesso.

Assumiamo $y1 \neq 0$ altrimenti ricadiamo nel secondo caso di prima.

Questo caso viene trattato come il primo, dove L è la retta tangente ad E nel punto P.

In pratica, le coordinate di R = (x3, y3) sono:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1}$$

Avendo definito l'addizione allora (E(Q),+) è un gruppo Abeliano.

Figura 16 – Lewis Mordell

Lewis Mordell, nel 1922, mostrò che E(Q) è generato in modo finito, sebbene abbia infiniti elementi.

Il che vuol dire che in E(Q) esiste un numero finito di punti, tale che tutti gli altri punti possono essere raggiunti con una sequenza finita di addizioni.

Tale sequenza di punti ha solo due possibilità:

1. si chiude su sé stessa in un ciclo
2. continuerà all'infinito.

Nel caso 1 si produce un sottogruppo interno al gruppo; mentre nel caso 2 produce una copia dei numeri interi $\mathbb{Z}$.

I matematici indicano ciò con:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_f \ (^4)$$

$\mathbb{Z}$ è il gruppo infinito di interi che si sommano, r è un intero non negativo, $E(\mathbb{Q})_f$ è il gruppo finito ovvero il sottogruppo finito di $E(\mathbb{Q})$ (detto anche sottogruppo *di torsione o periodico*). Il numero **r** è definito "**rango di E**".

Il rango di E dà una misura della dimensione dell'insieme dei punti sulla curva: maggiore è r maggiore è il numero di punti; per cui sarebbe un parametro importante per una eventuale

[4] Un **sottogruppo di torsione** (talvolta detto **componente di torsione** o semplicemente **torsione**) di un gruppo abeliano è l'insieme dei suoi elementi aventi ordine finito.

dimostrazione, però ancora oggi è un elemento poco approfondito e non si sa nemmeno un metodo con cui calcolarlo.

Nel 1935 *Trygve Nagell* e *Elisabeth Lutz* dimostrarono il Teorema: "se un punto (x,y) è un punto di torsione (un elemento di $E(\mathbb{Q})_f$), allora x e y devono essere entrambi numeri interi e ciò può avvenire per due casi:

- y=0
- $y^2 \mid 4a^3 + 27b^2$".

Nel 1977 *Barry Mazur* ha dimostrato che $E(\mathbb{Q})_f$ deve essere uno di undici gruppi $\mathbb{Z}/n\mathbb{Z}$, per n=0,1,…,11 oppure uno dei quattro gruppi $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ con m=1,2,3,4

Nel caso in cui $E: y^2 = x^3 - d^2x$ allora $E(\mathbb{Q})_f = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Riprendiamo la Congettura e la funzione Hasse-Weil

Abbiamo visto che Birch e Swinnerton-Dyer per enumerare i punti razionali sulle curve ellittiche presero in considerazione di contare le soluzioni mod p e indicarono con Np il numero di soluzioni + 1 (il punto all'infinito). Il numero di soluzioni Np sostanzialmente è l'ordine del gruppo $E(\mathbb{Z}/p\mathbb{Z})$.

Il problema era determinare r. Come?

Birch e Swinnerton-Dyer sfruttarono i risultati di Hasse; difatti considerando che:

$$E(\mathbb{F}p) = \left\{(x, y) \in \mathbb{F}p^2 : y^2 \equiv x^3 + ax + b \bmod p\right\} \bigcup \{O\}$$

Se $p \neq 0$ e non divisibile per il discriminante, allora E(Fp) stiamo in un gruppo. A questo punto ci si pone la domanda, allora Np che rappresenta? Al variare di x=0,...,p-1 otteniamo:

- Nessun punto se l'equazione $y^2 = x^3 + ax + b$ non è un quadrato mod p
- Un punto se $y^2 = x^3 + ax + b \equiv 0 \bmod p$
- Due punti se $y^2 = x^3 + ax + b$ è un quadrato non nullo mod p

più il punto all'infinito.

Cosicché scegliendo elementi non nulli di Fp è equivalente probabilisticamente a prendere quadrati al 50% e non quadrati al 50%; per cui prima e terza possibilità dovrebbero essere circa uguali; il che suggeriva che Np era circa p+1.

Facendo in questo modo giunsero a considerare la funzione di Hasse-Weil:

$$L(En, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Dove $a_p = p - Np$

Hasse col suo Teorema del 1934 affermava che:

$$|p + 1 - Np| < 2\sqrt{p} \quad p>2 \text{ e p non divisore del discriminante}$$

Hasse aveva precedentemente dimostrato che Np è sostanzialmente p+1, con una variazione massima di $2\sqrt{p}$ ovvero $|a_p| < 2\sqrt{p}$ .e, usando quest'ultima disuguaglianza, si ottiene che L(En,s) ha una soluzione ogni volta che s > 3/2.

Nella funzione di Hasse-Weil i termini $a_p p^{-s}$ sono da considerarsi dei termini di correzione dello scostamento di Np da p+1.

Se i termini a_p, positivi e negativi, fossero in uguale quantità allora il prodotto infinito potrebbe non essere nullo; ma se, invece, fossero preponderanti i negativi, il che vuol dire che c'è una asimmetria che comporta che Np > p+1, allora L potrebbe essere nulla.

Hasse aveva congetturato che, sul fac-simile della zeta di Riemann, si potesse estendere L(E,s) ad una funzione con un valore per ogni se a cui si potesse applicare il calcolo infinitesimale. Questo fu dimostrato proprio dimostrando la congettura di Taniyama-Shimura.

In base a quanto visto con la Teoria dei gruppi diremo correttamente che la *congettura di Birch e Swinnerton-Dyer si traduce col dire che:"E(ℚ) è infinito se e solo se L(E,1)=0"*.

Tuttavia, inizialmente, Birch e Swinnerton-Dyer la introdussero diversamente. Essi ipotizzarono che se la congettura di Hasse fosse stata vera (all'epoca non era stata dimostrata) allora era possibile sviluppare L(E,s) ad esempio in serie di Taylor intorno a s=1:

$$L(E,s) = c_0 + c_1(s-1) + c_2(s-1)^2 + c_3(s-1)^3 + \ldots$$

Dalla teoria delle serie affinchè E(ℚ) sia infinito, e quindi L(E,s)=0, è che c_0=0. Però Birch e Swinnerton-Dyer posero una condizione molto più stringente cioè E(ℚ) è infinito se e solo se $c_r \neq 0$ mentre ogni cn=0 per n=0,..,r-1 dove r = rango(E(ℚ)). Il che significa che E(ℚ) è infinito se è vero che:

$$L(E,s) = c_r(s-1)^r + \ldots$$

Per cui contare nello sviluppo di Taylor il numero di elementi nulli iniziale equivale a contare il rango di E e tale rango dà una misura esatta del grado in cui L(E,1)=0.

Divagazione sulla Zeta di Riemann e la L(E,s)

La funzione zeta di Riemann e le sue stupefacenti proprietà possono essere traslate anche nel mondo dei campi (massimali ideali etc).

Hasse mostrò che $\zeta(E/\mathbb{F}p) = \frac{1-a_p x+px^2}{(1-x)(1-px)}$ dove $x = p^{-s}$, $a_p = p+1-Np$

Da notare che gli zeri della funzione $\zeta(E/\mathbb{F}p)$ si hanno dove p^{-s} è una radice di $1-a_p x+px^2$. Se si usa la stima di Hasse che $|a_p|<2\sqrt{p}$ si può trovare che gli zeri di $\zeta(E/\mathbb{F}p)$ corrispondono a quelli sulla retta critica a Re(s)=1/2.

Crittografia con curve ellittiche

I crittosistemi basati sulle curve ellittiche (ECC) sembrano offrire lo stesso livello di sicurezza di analoghi sistemi di crittografia asimmetrici tradizionali come l'RSA, ma con chiavi più corte.

Lunghezza chiave RSA	Lunghezza chiave ECC
1024	160
2048	210
5120	320

Tabella 1 – Lunghezze chiavi a confronto

I vantaggi di questi soli elementi sono:

- maggiore velocità cifratura/decifratura
- memorizzazione efficiente (minore memoria)
- minore utilizzo della larghezza di banda nelle trasmissioni

Tali vantaggi sono quindi di grosso interessa non solo per dispositivi con poca memoria (telefonini, etc) ma anche per la minore occupazione di banda nelle trasmissioni.

In crittografia ellittica non si usano le curve su $\mathbb{R}$ ma su GF(p) o su GF(2^m). Il loro uso è stato proposto nel 1985 da *Victor Miller* e *Neal Koblitz*.

Non esiste una sostanziale differenza di sicurezza nell'usare GF(p) o GF(2^m) ma da un "punto di vista implementativo" usare GF(2^m) è semplice ed economico.

GF(p)

Qui p è un primo p>3. Le curve su GF(p) sono definite esattamente come su $\mathbb{R}$ ma si adottano le operazioni modulo. In altri termini si lavora sull'equazione:

$$y^2 = x^3 + ax + b \bmod \mathrm{p}$$

La curva è formata da tutte le coppie (x,y) che soddisfano l'equazione più il punto O = (0,0).

GF(p): somma tra due punti

Se $x^3 + ax + b = 0$ non contiene radici cubiche in GF(p) ovvero il discriminante $4a^3 + 27b^2 \neq 0 \bmod p$ allora la curva ellittica può essere usata per definire un gruppo abeliano (E,+) finito.

La somma su E usa le stesse formule viste in $\mathbb{R}$.

GF(2^m)

Poiché GF(2^m) ha caratteristica 2, qui le curve hanno equazione diversa.

$$y^2 + xy = x^3 + ax + b$$

GF(2^m): somma tra due punti

Poiché l'equazione è modificata va aggiustata la formula della somma.

Inoltre l'opposto di un punto (x,y) è il punto (x, x + y) dove x + y è l'xor bit a bit tra x e y.

RSA basato su curve ellittiche

Siano p e q due numeri primi grandi da rimanere segreti, n = p * q.

Si scelgono a caso due numeri a e b tali che: $E : y^2 = x^3 + ax + b$ che definisce una curva ellittica sia su GF(p) che GF(q).

Per cifrare il testo in chiaro P∈E occorre calcolare e P mod n dove e è la chiave pubblica.

Per decifrare occorre conoscere i punti su E sia modulo p che modulo q.

Problema del Logaritmo discreto (ECDLP)

E' noto come ECDLP (Elliptic Curve Discrete Logarithm Problem). E' un problema di fattorizzazione.

E' il seguente problema: "Dato un punto P appartenente ad E, trovare un intero k (se esiste) tale che k * B = P. In tal caso k è il logaritmo discreto di P in base B".

Lo chiariremo meglio nel seguito con l'algoritmo EL GAMAL.

Attacchi al Logaritmo discreto

Attualmente esistono due grosse categorie di algoritmi per la risoluzione dei logaritmi discreti:

- *index calculus method* (metodo di calcolo dell'indice)
- *collision search method* (metodo della ricerca di collisioni)

L'algoritmo più usato in questi casi è il metodo **Pollard's rho** che appartiene alla categoria degli algoritmi per la ricerca di collisioni.

Quest'algoritmo produce una lunga serie di numeri che graficamente rappresentano la lettera greca rho (formata da un cerchietto e da una coda), lo scopo è capire dove il cerchietto interseca la coda.

Il Pollard's rho method lavora a passi, dove n rappresenta la grandezza del gruppo da risolvere.

Altro algoritmo usato per il DLP è il Pohlig-Hellman, leggermente meno performante rispetto al primo.

Tuttavia nessuno dei due è capace in tempi brevi di arrivare alla soluzione.

Fattorizzazione classica con curve ellittiche (Lenstra)

Circa la fattorizzazione classica, quella non discreta (ad esempio fattorizzare 69=3*23), esiste un metodo dovuto a Lenstra, come modifica del metodo di Pollard, basato sulle curve ellittiche.

Spesso è adottato anche per semiprimi RSA di una 20.na cifre; ulteriormente non è conveniente.

EL GAMAL una implementazione didattica

L' algoritmo è costituito da due parti:

- scambio delle chiavi pubbliche (metodo Diffie - Hellman)
- critto sistema basato sulle curve ellittiche

Nella crittografia asimmetrica, ovvero a chiave pubblica e privata, algoritmi interessanti basati sulla teoria delle curve ellittiche, che fanno leva sulla grossa difficoltà di risolvere in tempi brevi un "problema di fattorizzazione discreta" noto anche come problema del logaritmo discreto.

Qui addirittura le chiavi pubbliche scambiate tra Alice e Bob, rispetto al RSA, hanno anche maggiori informazioni.

Supponiamo che Alice compia i seguenti passi:

- sceglie randomicamente un numero primo p>1 a molte cifre, poi un intero g compreso tra 1 e p ed un intero a compreso tra 1 e p.
- calcola il valore g ^ a mod p
- crea la propria chiave pubblica KpuA = (p, g, g ^a) e la dà ai suoi amici (esempio Bob)
- la propria chiave privata è Kpr = a

Ricevuta KpuA da Alice, Bob farà i seguenti passi:

- genera un proprio intero b: b appartenga a Zp (ovvero tra 1 e p)
- costruisce la propria chiave pubblica KpuB = (p, g, g ^ b) e la da ad Alice
- custodisce la propria chiave privata KprB = b
- sceglie un messaggio M appartenente a Zp

Bob adesso cripta M e lo trasmette ad Alice. Bob esegue il crypting nel seguente modo:

$$Mc = M(g \hat{} a)\hat{}b \bmod p$$

Alice conosce KpuB, quindi g ^ b. Da qui calcola (g ^ b)^a mod p

A questo punto Alice è in grado di decriptare il messaggio Mc perchè:

$$Mc(g \hat{} b)\hat{}a)\hat{}(-1)=M(g \hat{}a)((g \hat{}b)\hat{}a)\hat{}-1=M$$

Cosa c'entra il logaritmo e perchè discreto?

Alice conosce la chiave pubblica di Bob in cui c'è p e g ^ b o meglio g ^ b mod p; per cui per sapere la chiave privata di Bob dovrebbe ricavarsi b da g ^ b mod p. In pratica g è la base b l'esponente dell'elevazione a potenza. L'operazione inversa di ricavare l'esponente (b) a cui elevare la base (g) per ottenere l'argomento è il logaritmo! Solo che lavoriamo in aritmetica modulo, ecco perchè si parla di logaritmo discreto.

Ebbene l'operazione di ricavarsi il logaritmo discreto, tenendo conto che sia g che b sono a molte cifre, è banale ma richiede molto tempo. E' questo il punto di forza di questa crittografia!

Considerazioni finali

In tutto l'articolo abbiamo mostrato i legami tra tutti i settori matematici con la congettura di Birch e Swinnerton-Dyer ed i settori dove vengono impiegate le curve ellittiche.

Il settore matematico dove si colloca la congettura è ancora da esplorare maggiormente ed i risultati apparentemente inutili e astratti sui campi finiti etc potrebbero fornire idee e soluzioni per nuovi sistemi crittografici veloci, con poca occupazione di memoria e soprattutto inviolabili.

Esiste un legame tra RH e la congettura di Birch. La dimostrazione dell'una potrebbe avere effetti decisivi anche sulla risoluzione dell'altra.

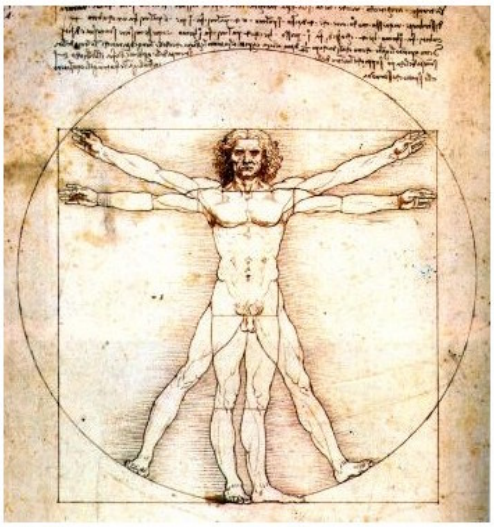
Software didattico EL GAMAL

Segue un esempio di algoritmo didattico su EL GAMAL. La libreria invece è disponibile su INTERNET grazie agli autori.

```
/*
* EL GAMAL
*
* External function
*
*/

{createCryptElG() = local (KPEG, p, g, a, b, ga, gb);

KPEG=vector(6); /* It's Public Key of El Gamal */

p = nextprime(random(10^40));
g = random(p);
a = random(p); /* It's Private Key of El Gamal user A */
b = random(p); /* It's Private Key of El Gamal user B */

ga=lift(Mod(g,p)^a);
gb=lift(Mod(g,p)^b);

/* I put them in a vector KPEG for convenience in the test*/

KPEG[1]=g;
KPEG[2]=a; /* a for user A and b for user B */
KPEG[3]=ga; /* ga for user A and gb for user B */
KPEG[4]=p; /* p is shared */
KPEG[5]=b;
KPEG[6]=gb;
return(KPEG);
}

/*
* External function
*/

{cryptWordElG(mc, p, a, gb) = local (msecret);


msecret = lift(mc*Mod(gb,p)^a);
print("\nsecret value: ", msecret);
print(" ");
return(msecret);

}

/*
* External function
*/

{decryptWordElG(secretElG, p, b, ga) = local (desecretElG, msg);

desecretElG = lift(secretElG*(Mod(ga,p)^b)^-(1));
```

```
print("decrypt value: ", desecretElG);
return(desecretElG);

}

{testElG(strMyWordTest) = local (msc,Msecret,Mdesecret,msgs);

/* B has got a KeyPub and transmit to A a message */
Key=vector(6);
Key=createCryptElG();

/* B tx to A */
msc = get26Ascii(strMyWordTest);
print("msc : ", msc);


Msecret=cryptWordElG(msc, Key[4], Key[2],Key[6]);

/* A decrypts */
Mdesecret=decryptWordElG(Msecret,Key[4],Key[5],Key[3]);

print("Decodifica\n");
msgs = getMsg(Mdesecret);
print("\nmsg decriptato: ", msgs);


return;
}

/*
*  External Function
*/

{get26Ascii(str) = local (MyW, weight, i, a, m);

 weight = length(str);
MyW=Vecsmall(str);

 m=0;

 /*
    I use a power of 27 otherwise char Z will have
    26*26^weight and this doesn't work well
    with getMsg
 */

 for( i=1,weight,

      a = MyW[i]-65+1;
      m = a*(27^weight) + m;
      weight--;
  );

 return(m);

}
```

```
/*
*   External function
*/
{getMsg(num) = local (a=num,d=27,r=0, msgM="", amax=0);

 print("num :", num);
 print("d :", d);
 while( d>26,

        amax = maxk26k(a);
        d = floor(a/(27^amax));
        r = a%(27^amax);
        msgM=concat(msgM,Strchr(d+64));

        if( r>=26, a = r; d=27;);
        if( r<26 & r!=0, msg=concat(msgM,Strchr(r+64)); d=1;);

      );

  return(msgM);

}

/*
*  Internal function
*/

{maxk26k(n) = local (k);
 k=0;
 while( 27^k <= n, k++;);
 return(k-1);

}
```



Riferimenti

[1] Introduzione alla matematica discreta – Maria Grazia Bianchi e Anna Gillio – McGraw Hill
[2] John Derbyshire, "L'ossessione dei numeri primi: Bernhard Riemann e il principale problema irrisolto della matematica ", Bollati Boringhieri.
[3] J. B. Conrey, "The Riemann Hypothesis", Notices of the AMS, March 2003.
[4] E. C. Titchmarsh, "The Theory of the Riemann Zeta-function", Oxford University Press 2003.
[5] A. Ivic, "The Riemann Zeta-Function: Theory and Applications", Dover Publications Inc 2003.
[6] Zeev Rudnick - Number Theoretic Background
[7] Victor Shoup - A computational Introduction to number theory and Algebra
[8] G.H. Hardy and E.M. Wright - An Introduction to the theory of numbers
[9] Neal Koblitz - Course in Number Theory and Crittography
[10] Fattorizzazione con algoritmo generalizzato con quadrati perfetti in ambito delle forme 6k±1" – Rosario Turco, Michele Nardelli, Giovanni Di Maria, Francesco Di Noto, Annarita Tulumello, Maria Colonnese – CNR SOLAR
[11] Semiprimi e fattorizzazione col modulo – Rosario Turco, Maria Colonnese – CNR SOLAR Maggio 2008
[12] Sulle spalle dei giganti - Rosario Turco, Michele Nardelli, Giovanni Di Maria, Francesco Di Noto, Annarita Tulumello, Maria Colonnese – CNR SOLAR
[13] George G. Szpiro - L'enigma di Poincarè – La congettura e la misteriosa storia del matematico che l'ha dimostrata - APOGEO

Siti vari

CNR SOLAR
http://150.146.3.132/

Aladdin's Lamp (ing. Rosario Turco)
www.geocities.com/SiliconValley/Port/3264 menu' MISC sezione MATEMATICA

gruppo ERATOSTENE
http://www.gruppoeratostene.com

dott. Michele Nardelli
http://xoomer.alice.it/stringtheory/