Curve ellittiche su campi finiti e applicazioni alla crittografia

Tesi di Laurea di Matteo Vaccargiu

Relatore: Professor Andrea Loi

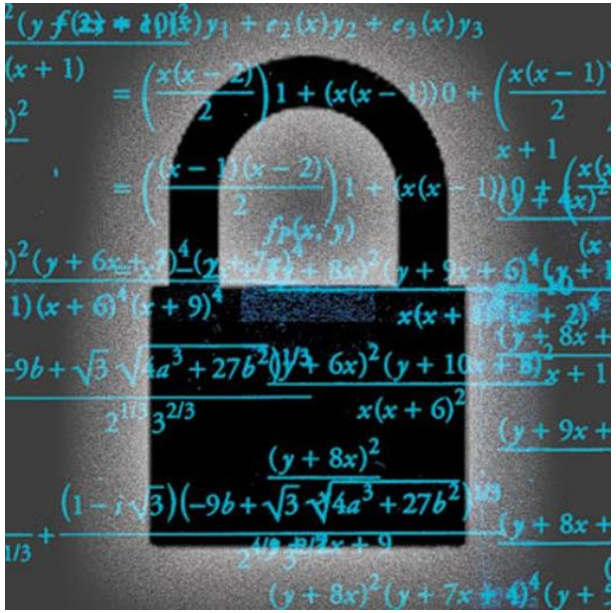
Corso di Studi in Matematica, Università degli Studi di Cagliari

Laurea di primo livello in scienze matematiche (L-35)

Definizione:

La **crittografia** è la scienza che si occupa di garantire una comunicazione efficiente e sicura tra due persone.

Il modello fondamentale della crittografia prevede un *mittente*, un *destinatario* e un *intruso*.



Possiamo suddividere i sistemi crittografici in due gruppi principali:

- Sistemi a chiave simmetrica
- Sistemi a chiave pubblica

In questa tesi ci focalizzeremo principalmente sulla crittografia di chiave pubblica ed in particolare sulla crittografia di curve ellittiche su campi finiti.

Un **crittosistema su curva ellittica** (1985) è costruito sul gruppo dei punti di una curva ellittica su un campo finito e si basa sulla difficoltà risolutiva del problema del logaritmo discreto.

Viene definito da un insieme di parametri $D = (q, a, b, P, n, h)$, chiamati parametri di dominio, che descrivono la curva.

A questi parametri verrà associata una coppia di chiavi $(\mathrm{Q}, d = \log_P Q)$.

Neal Koblitz

Victor Müller

Problema del logaritmo discreto

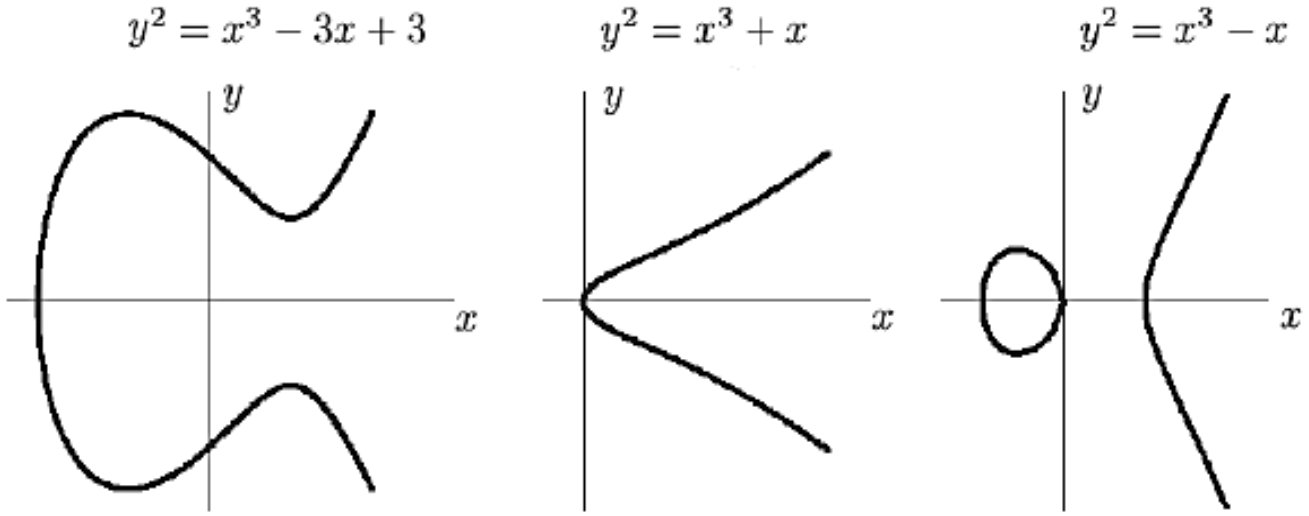
Sia E una curva ellittica su un campo finito F_q e sia P un punto della curva di ordine n e $Q = < P > = \{dP \mid d \in E(F_q)\}$.
Il problema consiste nel trovare l'intero $k \in \{1, \dots, n-1\}$ tale che $Q = kP$. Tale intero è chiamato logaritmo discreto di Q in base P e si indica con: $k = \log_P Q$.

Definizione:

Una **curva ellittica** definita su un campo K, con caratteristica diversa da 2 e da 3, può essere descritta come il grafico di un'equazione, detta equazione di Weierstrass, della forma:

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

con $a, b \in K$, in modo che non sia singolare $(4a^3 + 27b^2 \neq 0)$



Sia data una curva ellittica E, il punto $(0 : 1 : 0)$ è detto **punto all'infinito** della curva e si indica con O.

L'insieme dei punti di una curva ellittica definita su un campo K si denota con *E(K)* ed è definito come:

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \cup \{O\}$$

Definizione:

Siano E_1 e E_2 due curve ellittiche su un campo K. Un **morfismo** $\varphi: E_1(K) \to E_2(K)$ è un'applicazione tale che per ogni p, $q \in E_1(K)$ risulta $\varphi(pq) = \varphi(p)\varphi(q)$.

Definizione:

Due curve ellittiche $E_1(K)$ ed $E_2(K)$ si dicono **isomorfe** se esistono due morfismi $\varphi: E_1(K) \to E_2(K)$ e $\psi: E_2(K) \to E_1(K)$ tali che $\varphi \circ \psi$ e $\psi \circ \varphi$ siano le funzioni identità rispettivamente in $E_2(K)$ e in $E_1(K)$ e si denota con $E_1 \cong E_2$

Definizione:

Sia data $E(F_q)$ curva ellittica e sia $|E(F_q)| = q + 1 - t$ la sua *cardinalità*.
L'intero t è detto *traccia di Frobenius*.

Teorema di Hasse

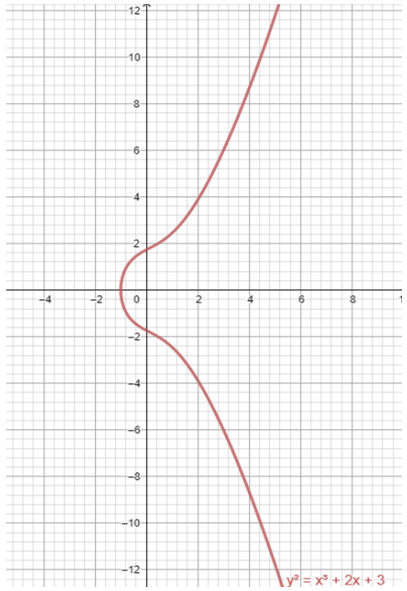
La traccia di Frobenius t soddisfa la disequazione $|t| \leq 2\sqrt{q}$

Esempio

Consideriamo $F_q = \mathbb{Z}_5$ e definiamo su di esso la seguente curva ellittica:

$$y^2 = x^3 + 2x + 3 \ (mod\ 5)$$

I possibili valori di x mod 5 sono 0, 1, 2, 3, 4. Sostituendoli nell'equazione troviamo i possibili valori di y che la risolvono.



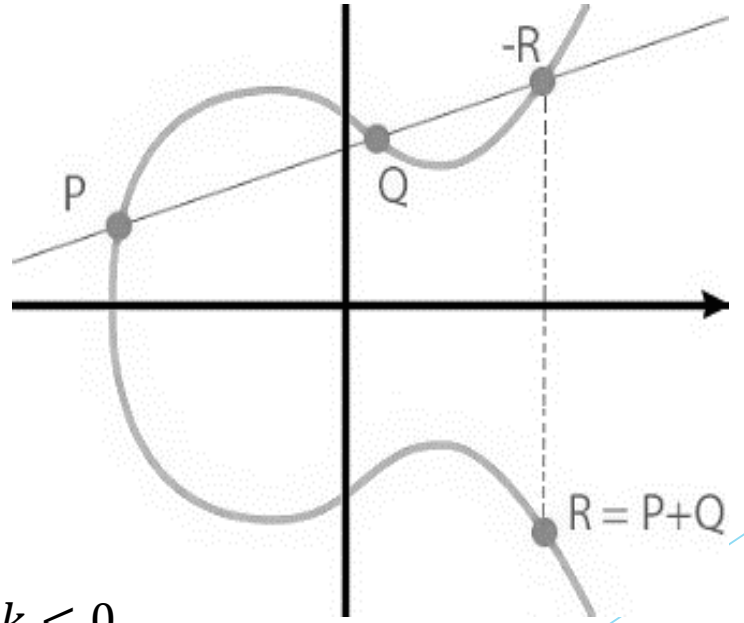
1. $x = \infty \Rightarrow y = \infty$
2. $x = 0 \Rightarrow y^2 = 3 \Rightarrow$ non ci sono soluzioni
3. $x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1, 4 \ (mod\ 5)$
4. $x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \ (mod\ 5)$
5. $x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1, 4 \ (mod\ 5)$
6. $x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \ (mod\ 5)$

Otteniamo quindi i punti: $(\infty, \infty), (1,1), (1,4), (2,0), (3,1), (3,4), (4,0)$ cioè 7 punti.
Segue dal teorema di Hasse che se $t = 7$ è il numero di punti della curva si ha:
$(q + 1) - 2\sqrt{q} \leq t \leq (q + 1) + 2\sqrt{q}$ ovvero $2 \leq t = 7 \leq 10$

Somma di due punti su una curva ellittica

Sia E una curva ellittica e $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ punti su E con $P_1, P_2 \neq O$.
Definisco $P_1 + P_2 = P_3 = (x_3, y_3)$ come segue:

1. Se $x_1 \neq x_2$ allora: $x_3 = m^2 - x_1 - x_2 \quad e \quad y_3 = m(x_1 - x_3) - y_1$ con $m = \frac{y_2 - y_1}{x_2 - x_1}$
2. Se $x_1 = x_2$ ma $y_1 \neq y_2$ allora: $P_1 + P_2 = O$
3. Se $P_1 = P_2$ e $y_1 \neq 0$, allora: $x_3 = m^2 - 2x_1 \quad e \quad y_3 = m(x_1 - x_3) - y_1$ con $m = \frac{3\,{x_1}^2 + a}{2\,y_1}$
4. Se $P_1 = P_2$ e $y_1 = 0$, allora: $P_1 + P_2 = O$
5. Se $P_2 = O$, allora: $P_1 + O = P_1$

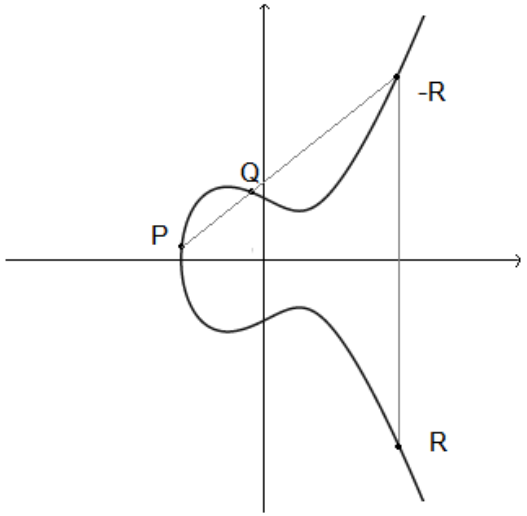


Se P è il punto di coordinate (x, y), allora
$-P = (x, -y)$.

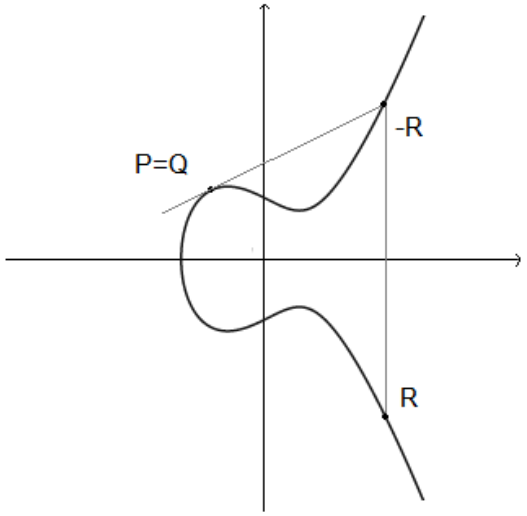
Definiamo kP come segue:

1. $kP = O \; se \; k = 0$
2. $kP = P + P + \cdots + P \; (k \; volte) \; se \; k > 0$
3. $kP = (-P) + (-P) + \cdots + (-P)(|k| volte) \; se \; k < 0$

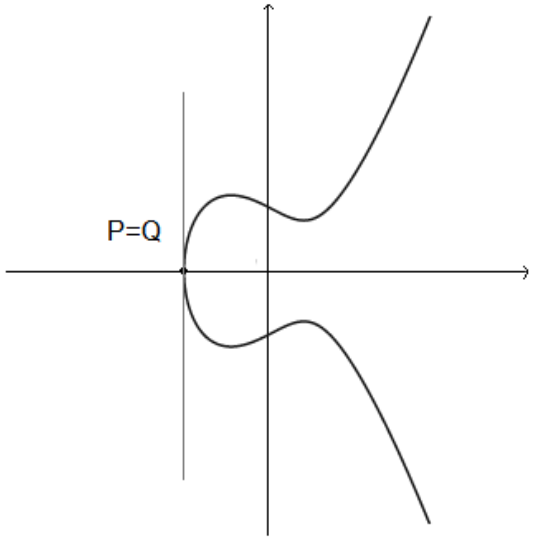
Geometricamente, definiamo l'operazione + come segue:



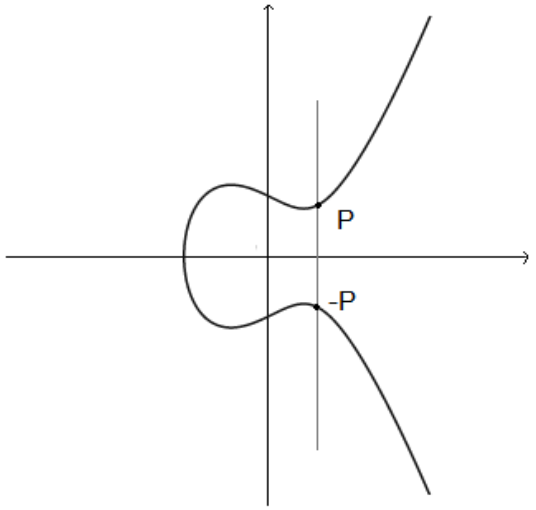
Se $P \neq Q$, allora $P + Q = R$ dove -R è il terzo punto di intersezione tra la curva e la retta per P e Q, ed R è il suo opposto, cioè il punto di intersezione tra la curva e la retta per -R e O.



Se $P = Q$, allora $P + Q = R$ dove R si trova come prima, con -R punto di intersezione tra la curva e la tangente in P.



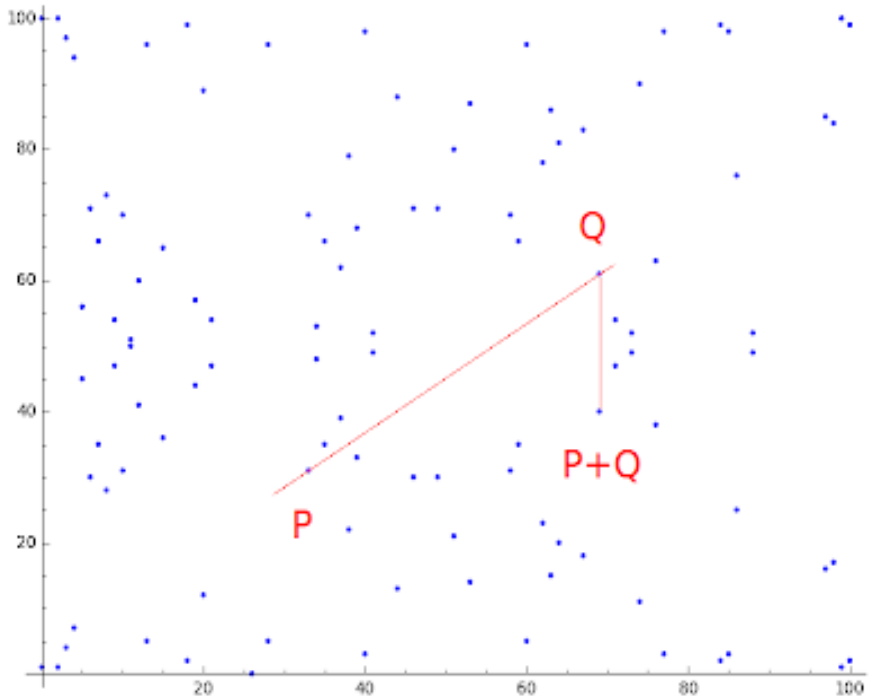
Se P $= Q$ e la tangente in P è verticale, allora $P + Q = 2P = O$.



Se $Q = -P$, allora $P + Q = O$.

Teorema

L'insieme dei punti di una curva ellittica $E(K)$ non singolare è un gruppo abeliano rispetto all'operazione + e con elemento neutro O.



Dimostrazione

Verifichiamo che l'operazione di somma precedentemente definita soddisfa gli assiomi di gruppo.

- L'operazione è chiusa.
- L'elemento neutro è O.
- L'inverso di un punto P sulla curva è l'unico altro punto P' avente la stessa ascissa di P.
- La somma è commutativa.
- La proprietà associativa è anch'essa provata.

■

Struttura di gruppo abeliano dei punti di una curva ellittica su campo finito

Sia $\mathrm{E}(F_q)$ il gruppo dei punti di una curva ellittica su un campo finito F_q. Si può provare che $\mathrm{E}(F_q)$ è isomorfo al prodotto di al più due gruppi ciclici:

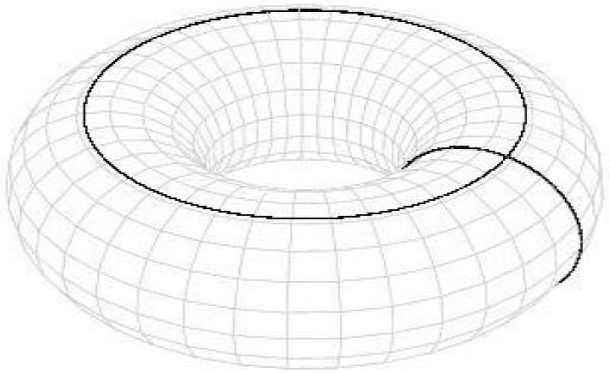
$$\mathrm{E}(F_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \text{ dove } n_1 | n_2 \text{ e } n_1 | q - 1 \, .$$

Se $\mathrm{E}(F_q)$ è ciclico allora $n_1 = 1$.

Nel caso in cui si lavori con una curva ellittica E su un anello del tipo $\mathbb{Z}_{n_1 n_2}$ con n_1, n_2 dispari e $mcd(n_1, n_2) = 1$ allora:

$$E(\mathbb{Z}_{n_1 n_2}) \cong E(\mathbb{Z}_{n_1}) \times E(\mathbb{Z}_{n_2})$$

Struttura di gruppo sul toro



Il **toro** è una superficie compatta e orientabile con genere 1, dove per genere si intende il numero più grande di curve semplici chiuse e disgiunte contenute nella superficie che non la sconnettono. Diamo un idea del fatto che la struttura di gruppo vista con le curve ellittiche è la stessa di quella del toro visto come prodotto diretto di cerchi.

Considero l'embedding tra il toro e il piano proiettivo complesso, definito mediante la mappa:

$$\wp(z)\wp'(z) \quad \text{dove} \quad z \longmapsto [1 : \wp(z) : \wp'(z)/2]$$

Questa mappa è un isomorfismo di gruppo che garantisce che, topologicamente, *una curva ellittica nel piano proiettivo sia un toro.*

Il toro è omeomorfo al prodotto $S^1 \times S^1$, che è un gruppo, perché prodotto diretto di gruppi. Utilizzando il precedente embeddig si può far vedere che la struttura gruppo definito dai punti del toro è lo stesso di quella definita sui punti di una curva ellittica.

Crittosistema RSA

Il crittosistema RSA (1977) è uno dei sistemi a chiave pubblica maggiormente utilizzati per cifrare e per fornire la firma digitale. Si basa sul problema della fattorizzazione intera.

La base del sistema RSA sono 2 numeri primi p $\neq q$ grandi e di dimensione simile a partire dai quali si calcola $N = pq$. Si considera un numero e tale che $1 < e < (p-1)(q-1)$ e $mcd(e;(p-1)(q-1)) = 1$, e si calcola $1 < d < (p-1)(q-1)$ tale che:

$$ed \equiv 1 \; mod \; (p-1)(q-1)$$

In questo sistema la *chiave pubblica* è $(N;e)$, e la *chiave privata* è $(p;q;d)$.

La comunicazione consiste in tre passi:

1. Il mittente codifica un testo chiaro con un numero $m < N$,
2. Calcola $c \equiv m^e \; mod \; N$ e lo invia a la persona che ha la chiave privata,
3. Il destinatario calcola $c^d \equiv m \; mod \; N$.

Alcuni vantaggi di ECC su RSA

L'utilizzo delle curve ellittiche in crittografia è vantaggioso grazie al fatto che:

- per avere un livello di sicurezza analogo a quello garantito dall'RSA con 1024 bit (circa 338 cifre decimali) è sufficiente utilizzare curve con chiavi lunghe solo 160 bit (circa 53 cifre decimali);
- il numero di gruppi abeliani dei punti di una curva che si possono costruire su uno stesso campo finito sono molteplici;
- non esistono algoritmi sub-esponenziali per risolvere il problema del logaritmo discreto sulle curve ellittiche;
- all'aumentare del livello di sicurezza cresce l'efficienza dei sistemi basati su curve ellittiche rispetto ai sistemi tradizionali come l'RSA.

L'unico vantaggio scientificamente stabilito dell'RSA rispetto alla crittografia su curve ellittiche è che le operazioni a chiave pubblica sono più veloci con RSA.

Utilizzi attuali

Nella pratica i campi utilizzati sono solamente F_P con p primo molto grande e F_{2^m} con m grande.
Il NIST (National Institute of Standards and Technology) ha consigliato 15 curve ellittiche:

- 5 campi principali per p di dimensioni 192, 224, 256, 384, e 521 bit.
- 5 campi binari per m uguale a 163, 233, 283, 409 e 571.

L'ambito dove probabilmente le curve ellittiche hanno più successo è quello delle ***smartcard***. Ad esempio, sono utilizzate per le schede telefoniche, per i pagamenti elettronici (*Contactless*), per l'identificazione, per le memory card e altre componentistiche di dispositivi tecnologici e per molte altre applicazioni.

Anche ***Blockchain*** utilizza tecnologie basate su curve ellittiche. In particolare sia **Bitcoin** che **Ethereum** utilizzano per la firma digitale un sistema crittografico a chiave pubblica basato su curve ellittiche, caratterizzato da efficienza e velocità nei processi di firma e verifica. Con l'avvento dei computer post-quantistici si pensa che queste tecniche crittografiche saranno a rischio in un periodo, oggi stimato in circa 10 anni.

Bibliografia

- Elliptic curves and theis applications to cryptography, Andreas Enge, Kluwer Academic Publishers
- Introduction to Coding Theory, Third Edition, J.H. van Lint, Springer-Verlag
- Cryptography: Theory and Practice, Douglas Stinson, CRC Press
- Post-Quantum Elliptic Curve Cryptography, Soukharev Vladimir, University of Waterloo

Vi ringrazio per l'attenzione!!