ROMA TRE
UNIVERSITÀ DEGLI STUDI

DIPARTIMENTO DI MATEMATICA E FISICA
Corso di Laurea Magistrale in Matematica

Sintesi della Tesi di Laurea

Primi supersingolari per curve ellittiche

Relatore:
Prof. Francesco Pappalardi

Candidata:
Sabrina Capaldi

A.A 2014-2015

Introduzione

Le curve ellittiche rappresentano uno dei più interessanti punti di contatto tra la matematica teorica e le applicazioni nel mondo reale. La teoria delle curve ellittiche si basa su varie discipline della matematica, essa trova inoltre molte applicazioni nella crittografia e nella sicurezza delle comunicazioni. Questa connessione fu suggerita per la prima volta da N. Koblitz e V.S. Miller negli anni '80, e molti studi sono stati fatti su ciò da allora. Le curve ellittiche sono state usate anche nella dimostrazione di uno dei teoremi più studiati della matematica, l'ultimo Teorema di Fermat.

Lo scopo di questa tesi è lo studio di una particolare classe di curve ellittiche, le curve ellittiche supersingolari. Esse vennero scoperte da Hasse nel 1936 durante il suo lavoro sull'ipotesi di Riemann per le curve ellittiche, osservando che in caratteristica positiva le curve ellittiche avrebbero potuto avere un anello degli endomorfismi insolitamente grande di rango 4. Deuring nel 1941 sviluppò la loro teoria di base.

Il termine supersingolare viene dall'espressione "valori singolari del $j-$invariante", usata per i valori del $j-$invariante per i quali una curva ellittica complessa ha moltiplicazione complessa. Queste sono quelle curve per le quali l'anello degli endomorfismi ha rango massimale possibile 2. In caratteristica positiva è possibile che l'anello degli endomorfismi sia ancora più grande, cioè un ordine in un'algebra di quaternioni di dimensione 4, che è il caso delle curve supersingolari.

La tesi è organizzata come segue:

- Il Capitolo 1 contiene alcuni concetti di base: la definizione di curva ellittica tramite l'equazione di Weierstrass e tramite l'equazione di Legendre, la legge di gruppo, e le principali proprietà delle curve ellittiche definite su campi finiti.

- Nel Capitolo 2 diamo la definizione di primo supersingolare e varie definizioni equivalenti di curva supersingolare. Dimostriamo poi l'equivalenza tra queste, dopo aver fornito gli strumenti necessari: l'anello degli endomorfimi di una curva ellittica, i moduli di Tate, definizione e prime proprietà dei gruppi formali.

- Nel Capitolo 3 introduciamo le curve definite sui complessi e le curve a moltiplicazione complessa. Studiamo la relazione tra l'insieme delle curve complesse a moltiplicazione complessa e l'insieme delle curve razionali a moltiplicazione complessa.

- La prima parte del Capitolo 4 è dedicata alla riduzione di curve definite su campi numerici in curve definite su campi finiti. Nella seconda parte definiamo il polinomio di classe di Hilbert e ne vediamo il comportamento in due casi particolari.

- Il Capitolo 5 è dedicato al teorema di Elkies, e alla sua dimostrazione, sull'esistenza di infiniti primi supersingolari per le curve ellittiche razionali. Concludiamo con degli esempi numerici.

1 Concetti di base

1.1 L'equazione di Weierstrass

Definizione 1.1. Dato un campo K, $\mathrm{char}(K) \neq \{2,3\}$, una curva ellittica E definita su K è il dato di un'equazione della forma

$$y^2 = x^3 + Ax + B$$

con $A,\ B \in K$ e tale che la curva da essa definita sia non singolare. Questa è detta **equazione di Weierstrass**.

Per includere tutti i possibili campi K, va considerata un'equazione più generale *l'equazione di Weierstrass generalizzata*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_0$$

con $a_1, a_2, a_3, a_4 \in K$.

Consideriamo solo curve ellittiche non singolari, cioè curve il cui discrimante non si annulla. Il discriminante Δ di una curva data dall'equazione di Weierstrass è

$$\Delta = -16(4A^3 + 27B^2)$$

La condizione di non-singolarità è data quindi da $4A^3 + 27B^2 \neq 0$.

Definizione 1.2. Sia E una curva ellittica, data dall'equazione di Weierstrass, definiamo il j-invariante di E

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Notiamo che il j-invariante ci permette di determinare quando due curve sono isomorfe su un campo algebricamente chiuso. Se siamo su un campo non algebricamente chiuso K, è possibile che esistano due curve con stesso j-invariante, che non possono essere trasformate l'una nell'altra usando funzioni razionali a coefficienti in K.

Diamo ora una variante dell'equazione di Weierstrass: *l'equazione di Legendre*. Il vantaggio è che ci permette di esprimere una curva ellittica su un campo algebricamente chiuso, di caratteristica diversa da 2, tramite un solo parametro.

Proposizione 1.1. *Sia K un campo di caratteristica diversa da 2 e sia*

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$$

una curva ellittica E su K con $e_1, e_2, e_3 \in K$. Sia

$$x_1 = (e_2 - e_1)^{-1}(x - e_1), \quad y_1 = (e_2 - e_1)^{-3/2}y, \quad \lambda = \frac{e_3 - e_1}{e_2 - e_1}.$$

Allora $\lambda \neq 0, 1$ e

$$y_1^2 = x_1(x_1 - 1)(x_1 - \lambda).$$

1.2 La legge di gruppo

Definiamo l'insieme dei punti a coordinate in K di una curva ellittica E come

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Su questi punti si può definire un'operazione di somma nel seguente modo:
consideriamo due punti

$$P_1(x_1, y_1) \quad e \quad P_2(x_2, y_2)$$

su E e tramite questi definiamo un terzo punto $P_3(x_3, y_3)$. Tracciamo la linea l tra P_1 e P_2, questa intersecherà E in un terzo punto P_3'. Riflettendo P_3' rispetto all'asse x otteniamo P_3.

Tramite quest'operazione l'insieme dei punti di una curva ellittica è un gruppo additivo, con elemento neutro il punto all'∞.

Si può quindi definire anche il multiplo $n-$esimo di un punto come la somma di sè stesso n volte. Definiamo allora il gruppo di torsione.

Definizione 1.3. Sia E una curva ellittica definita su K. Sia n un intero positivo. Definiamo il *gruppo di n-torsione*

$$E[n] = \{P \in E(\overline{K}) \,:\, nP = \infty\}.$$

.

1.3 Curve ellittiche su campi finiti

Vediamo ora il caso in cui il campo K, su cui è definita la curva ellittica, è un campo finito. Notiamo subito che anche il gruppo dei punti della curva sarà chiaramente un gruppo finito. Vediamo alcuni risultati riguardo la cardinalità di questo gruppo.

Teorema 1.2. *Sia E una curva ellittica definita su $\mathbb{F}_q$. Allora*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \quad o \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

per un intero $n \geq 1$, o per due interi $n_1, n_2 \geq 1$ con n_1 che divide n_2.

Teorema 1.3 (Teorma di Hasse)**.** *Sia E una curva ellittica definita su un campo finito $\mathbb{F}_q$. Allora l'ordine di $E(\mathbb{F}_q)$ soddisfa*

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

Un ruolo fondamentale nella teoria delle curve ellittiche sui campi finiti è svolto dalla *mappa di Frobenius* ϕ_q.

Sia E una curva ellittica definita su $\mathbb{F}_q$, allora ϕ_q agisce sulle coordinate dei punti in $E(\overline{\mathbb{F}}_q)$:

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty.$$

Teorema 1.4. *Sia E una curva ellittica definita su $\mathbb{F}_q$. Sia $a = q + 1 - \#E(\mathbb{F}_q)$. Allora*

$$\phi_q^2 - a\phi_q + q = 0$$

come endomorfismi di E, e a è unico intero k tale che

$$\phi_q^2 - k\phi_q + q = 0.$$

Se abbiamo una curva definita su un campo finito $\mathbb{F}_q$ piccolo, e siamo interessati all'ordine di $E(\mathbb{F}_{q^n})$, possiamo applicare il seguente metodo.

Teorema 1.5. *Sia $\#E(\mathbb{F}_q) = q + 1 - a$. Scriviamo $X^2 - aX + q = (X - \alpha)(X - \beta)$. Allora*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n) \qquad \forall n \geq 1.$$

Ricordiamo la definizione del *simbolo di Legendre generalizzato*: Sia $x \in \mathbb{F}_q$ con q dispari, allora

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{se } t^2 = x \text{ ha una soluzione t} \in \mathbb{F}_q^\times \\ -1 & \text{se } t^2 = x \text{ non ha una soluzione t} \in \mathbb{F}_q \\ 0 & \text{se } x = 0. \end{cases}$$

Enunciamo un ulteriore risultato riguardo la cardinalità del gruppo dei punti di una curva ellittica.

Teorema 1.6. *Sia E una curva ellittica definita da $y^2 = x^3 + Ax + B$ su $\mathbb{F}_q$. Allora*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right).$$

2 Curve supersingolari

Definiamo una *curva supersingolare* su un campo finito.

Definizione 2.1. Una curva ellittica E in caratteristica p è detta supersingolare se $E[p] = \{\infty\}$. In altre parole se non ci sono punti di ordine p, anche tra quelli con coordinate nella chiusura algebrica del campo.

Una curva ellittica definita su $\mathbb{Q}$ si dice supersingolare se la sua riduzione sul campo finito $\mathbb{F}_p$ è una curva supersingolare. Il primo p in tal caso, viene detto primo supersingolare. Chiaramente consideriamo solo primi di buona riduzione, cioè tali che la curva ridotta sia ancora non singolare.

Vista la definizione, è chiaro che, per determinare se un primo è o meno supersingolare, è sufficiente studiare una curva su un campo finito, cioè la sua riduzione modulo p.

Esistono varie definizioni di supersingolarità per una curva ellittica definita su un campo finito, tutte equivalenti tra loro.

2.1 La traccia di Frobenius

La prima definizione equivalente che trattiamo viene data sfruttando le proprietà della traccia di Frobenius.

Proposizione 2.1. *Sia E una curva ellittica su $\mathbb{F}_q$, dove q è la potenza di un numero primo p. Sia $a = q + 1 - \#E(\mathbb{F}_q)$. Allora E è supersingolare se e solo se $a \equiv 0 (\mathrm{mod} p)$, cioè se e solo se $\#E(\mathbb{F}_q) \equiv 1 (\mathrm{mod} p)$.*

Corollario 2.2. *Sia $p \geq 5$ un primo. Allora E è supersingolare se e solo se $a = 0$, cioè se e solo se $\#E(\mathbb{F}_p) = p + 1$.*

Nel Corollario precedente i casi $p = 2$ e $p = 3$ non sono inclusi, infatti ci sono esempi di curve supersingolari con $a \neq 0$.

Vediamo una conseguenza della Proposizione precedente, per determinare curve ellittiche supersingolari con una particolare equazione definite su dato campo finito $\mathbb{F}_q$.

Proposizione 2.3. *Sia q un numero dispari e $q \equiv 2 (\mathrm{mod} 3)$. Sia $B \in \mathbb{F}_q^{\times}$. Allora la curva ellittica E data da $y^2 = x^3 + B$ è supersingolare.*

2.2 Supersingolarità nella forma di Legendre

Come abbiamo visto, una curva ellittica definita su un campo algebricamente chiuso di caratteristica diversa da 2 può essere scritta attraverso l'equazione di Legendre. Mostriamo come ottenere una curva ellittica supersingolare su $\overline{\mathbb{F}}_q$ usando quest'equazione.

Teorema 2.4. *Sia p un primo dispari. Definiamo il polinomio*

$$H_p(T) = \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 T^i$$

La curva ellittica data da $y^2 = x(x-1)(x-\lambda)$ con $\lambda \in \overline{\mathbb{F}}_p$ è supersingolare se e solo se $H_p(\lambda) = 0$.

Se abbiamo due curve ellittiche su un campo e un cambiamento di coordinate su un'estensione del campo, che trasforma la prima curva nella seconda, allora per verificare la supersingolarità di una è sufficiente mostrare la supersingolarità dell'altra. Vediamo allora come verificare la supersingolarità di due specifiche curve, poniamo particolare attenzione per il loro j-invariante.

Proposizione 2.5. *Sia $p \geq 5$ un primo. Allora la curva ellittica $y^2 = x^3 + 1$ su $\mathbb{F}_p$ è supersingolare se e solo se $p \equiv 2(\mathrm{mod}3)$, e la curva ellittica $y^2 = x^3 + x$ su $\mathbb{F}_p$ è supersingolare se e solo se $p \equiv 3(\mathrm{mod}4)$.*

2.3 Endomorfismi di curve ellittiche

Illustrtriamo in questa Sezione le isogenie tra curve ellittiche, gli endomorfismi e l'anello degli endomorfismi.

2.3.1 Le isogenie

Consideriamo qui le mappe tra curve ellittiche. Dato che le curve ellittiche hanno un punto distinto ∞, è naturale individuare quelle mappe che rispettano questa proprietà.

Definizione 2.2. Siano E_1 e E_2 due curve ellittiche. Un'*isogenia* tra E_1 e E_2 è un morfismo

$$\phi : E_1 \to E_2$$

tale che $\phi(\infty) = \infty$. Due curve ellittiche E_1 e E_2 sono isogene se esiste un'isogenia ϕ tale che $\phi(E_1) \neq \infty$.

Il grado di un'isogenia ϕ è dato dalla corrispondente proprietà dell'estensione finita $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$.
Per convenzione usiamo che $deg[0] = 0$.

Osserviamo ioltre che per ogni $m \in \mathbb{Z}$, $m \neq 0$, la moltplicazione per m

$$[m] : E \to E$$

è un'isogenia. Inoltre $[m]$ è una mappa non costante.

Defiamo ora l'*isogenia duale*.

Teorema 2.6. *Sia $\phi : E_1 \to E_2$ un'isogenia non costante di grado m. Allora esiste un'unica isogenia $\hat{\phi} : E_2 \to E_1$ tale che*

$$\hat{\phi} \circ \phi = [m],$$

con $[m]$ la moltiplicazione per m.

Definizione 2.3. Sia $\phi : E_1 \to E_2$ un'isogenia. L'*isogenia duale* a ϕ è l'isogenia

$$\hat{\phi} : E_2 \to E_1$$

tale che verifica il Teorema precedente.

Essendo le curve ellittiche dei gruppi, allora le isogenie tra loro formano dei gruppi. Siano

$$\mathrm{Hom}(E_1, E_2) = \{isogenie \quad \phi : E_1 \to E_2\}.$$

Questo è un gruppo rispetto all'addizione

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

Se $E_1 = E_2$ possiamo anche comporre le isogenie. Allora se E è una curva ellittica, sia

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

l'anello con l'addizione descritta sopra e moltiplicazione data dalla composizione

$$(\phi\psi)(P) = \phi(\psi(P)).$$

$\mathrm{End}(E)$ è detto *l'anello degli endomorfismi di E*. Gli elementi invertibili di $\mathrm{End}(E)$ formano il *gruppo degli automorfismi di E*, il quale viene indicato con $\mathrm{Aut}(E)$.

2.3.2 Classificazione dell'anello degli endomorfismi

Vediamo le possibile forme che un anello degli endomorfismi può assumere.

Ricordiamo la definizione di ordine e di algebra di quatenioni.

Definizione 2.4. Sia K un'algebra (non necessariamente commutativa) finitamente generata su $\mathbb{Q}$. Un *ordine* R di K è un sottoanello di K che è finitamente generato come $\mathbb{Z}$-modulo e che soddisfa $R \otimes \mathbb{Q} = K$.

Osservazione 2.7. Sia K un campo quadratico immaginario, $K = \mathbb{Q}(\sqrt{-d})$. Sia $\mathcal{O}_K$ il suo anello degli interi

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & \text{se } d \equiv 3 \,(\mathrm{mod} 4) \\ \mathbb{Z}[\sqrt{-d}] & \text{se } d \equiv 1, 2 \,(\mathrm{mod} 4) \end{cases}.$$

Scriviamo i due casi come $\mathbb{Z}[\delta]$. Un *ordine* in un campo quadratico immaginario è un anello R tale che $\mathbb{Z} \subset R \subseteq \mathcal{O}_K$, è inoltre un gruppo abeliano finitamente generato ed è della forma

$$R = \mathbb{Z} + \mathbb{Z} f\delta,$$

dove $f > 0$ è detto il *conduttore* di R ed è l'indice di R in $\mathcal{O}_K$. Il discriminante di R è

$$D_R = \begin{cases} -f^2 d & \text{se } d \equiv 3 \,(\mathrm{mod} 4) \\ -4f^2 d & \text{se } d \equiv 1, 2 \,(\mathrm{mod} 4) \end{cases}.$$

Definizione 2.5. Un'*algebra di quaternioni* è un'algebra della forma

$$K = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

con costanti di struttura

$$\alpha^2, \beta^2 \in \mathbb{Q}, \qquad \alpha^2 < 0, \qquad \beta^2 < 0, \qquad \beta\alpha = -\alpha\beta.$$

Corollario 2.8. *L'anello di endomorfismi di una curva ellittica E su un campo K è uno dei seguenti:*

1. *$\mathbb{Z}$;*
2. *un ordine in un campo quadratico immaginario;*
3. *un ordine in un'algebra di quaternioni.*

Se char(K)=0, allora solo i primi due casi sono possibili.
Se K è un campo finito $\mathbb{F}_q$, allora $\mathrm{End}(E)$ *è sempre più grande di $\mathbb{Z}$.*

2.4 I moduli di Tate

Iniziamo col definire un *sistema inverso di gruppi e omomorfismi.*

Sia $(I, \leq)$ un insieme parzialmente ordinato. Sia $(A_i)_{i\in I}$ una famiglia di gruppi e supponiamo di avere una famiglia di omomorfismi $f_{ij} : A_j \to A_i$ per ogni $i \leq j$, dette mappe di incollamento, con le seguenti proprietà:

- f_{ii} è l'identità su A_i,
- $f_{ik} = f_{ij} \circ f_{jk} \quad i \leq j \leq k.$

Allora la coppia $((A_i)_{i\in I}, (f_{(ij)})_{i\leq j\in I})$ è detta sistema inverso di gruppi e morfismi su I, e i morfismi f_{ij} sono detti morfismi di transizione del sistema.

Ora definiamo il limite inverso.

Definizione 2.6. Il limite inverso di un sistema inverso $((A_i)_{i\in I}, (f_{(ij)})_{i\leq j\in I})$ è definito come un particolare sottogruppo del prodotto diretto degli A_i:

$$\varprojlim_{i\in I} A_i = \left\{ \vec{a} \in \prod_{i\in I} A_i \quad t.c. \quad a_i = f_{ij}(a_j)\ \forall i \leq j\ in\ I \right\}.$$

Sia ℓ un numero primo. Consideriamo la sequenza delle riduzioni di $\mathbb{Z}$ tramite le potenze di ℓ

$$\cdots \to \mathbb{Z}/\ell^{n+1}\mathbb{Z} \xrightarrow{r_n} \mathbb{Z}/\ell^n\mathbb{Z} \to \cdots \xrightarrow{r_2} \mathbb{Z}/\ell^2\mathbb{Z} \xrightarrow{r_1} \mathbb{Z}/\ell\mathbb{Z}.$$

Il limite inverso di questa sequenza, denotato $\varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$, consiste in tutte le $a = (a_n)$ del prodotto $\prod_{1\leq n} \mathbb{Z}/\ell^n\mathbb{Z}$ tale che $r_n(a_{n+1}) = a_n(\mod \ell^n)$ per ogni $n \geq 1$. Questo limite è $\mathbb{Z}_\ell$, cioè l'anello degli *interi ℓ-adici.*

Possiamo ora definire il *modulo di Tate*

Definizione 2.7. Sia E una curva ellittica e $\ell \in \mathbb{Z}$ un primo. Il modulo di Tate ℓ-adico di E è il gruppo

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

con la mappa

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

2.5 Il teorema di Deuring

Il Teorema di Deuring fornisce cinque caratterizzazioni di curva ellittica supersingolare definita su un campo perfetto K. Prima di enunciarlo illustriamo alcune nozioni sui gruppi formali, necessarie per la comprensione del Teorema.

Definizione 2.8. Un gruppo formale $\mathscr{F}$ (con un parametro commutativo) definito su un anello R è una serie di potenze $F(X,Y) \in R[\![X,Y]\!]$ che soddisfa:

(a) $F(X,Y) = X + Y +$ (termini di grado ≥ 2).

(b) $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (associatività).

(c) $F(X,Y) = F(Y,X)$ (commutatività).

(d) Esiste un'unica serie di potenze $i(T) \in R[\![T]\!]$ tale che $F(T,i(T)) = 0$ (inverso).

(e) $F(X,0) = X$ e $F(0,Y) = Y$.

Chiamiamo $F(X,Y)$ la legge di gruppo formale di $\mathscr{F}$.

Definizione 2.9. Siano $(\mathscr{F},F)$ e $(\mathscr{G},G)$ due gruppi formali definiti su un anello R. Un omomorfismo da $\mathscr{F}$ a $\mathscr{G}$ su R è una serie di potenze (senza termini costanti) $f(T) \in R[\![T]\!]$ che soddisfa

$$f(F(X,Y)) = G(f(X),f(Y)).$$

$\mathscr{F}$ e $\mathscr{G}$ sono *isomorfi* su R se esiste un omomorfismo $f : \mathscr{F} \to \mathscr{G}$ e $g : \mathscr{G} \to \mathscr{F}$ definiti su R con

$$f(g(T)) = g(f(T)) = T.$$

Ci interessiamo in particolare ai gruppi formali definiti su un anello R di caratteristica un primo p.

Definizione 2.10. Sia R un anello con caratteristica $p > 0$. Siano $\mathscr{F},\mathscr{G}$ gruppi formali su un anello R e sia $f : \mathscr{F} \to \mathscr{G}$ un omomorfismo definito su R. L'*altezza di f*, denotata con $ht(f)$, è il più grande intero h tale che

$$f(T) = g(T^{p^h})$$

per una serie di potenze $g(T) \in R[\![T]\!]$. (Se $f = 0$ allora $ht(f) = \infty$.) L'*altezza di* $\mathscr{F}$, denotata $ht(\mathscr{F})$, è l'altezza della mappa di moltiplicazione per p $[p] : \mathscr{F} \to \mathscr{F}$.

Enunciamo il teorema di Deuring.

Teorema 2.9. *Sia K un campo (perfetto) di caratteristica p e E/K una curva ellittica. Per ogni intero $r \geq 1$, siano*

$$\phi_r : E \to E^{(p^r)} \quad e \quad \hat{\phi}_r : E^{(p^r)} \to E$$

la mappa p^r-esima di Frobenius e il suo duale. Le seguenti sono equivalenti.

(i) $E[p^r] = 0$ *per ogni* $r \geq 1$.

(ii) $\hat{\phi}_r$ *è (puramente) inseparabile per ogni* $r \geq 1$.

(iii) La mappa $[p] : E \to E$ *è puramente inseparabile e* $j(E) \in \mathbb{F}_{p^2}$.

(iv) $\mathrm{End}(E)$ *è un ordine in un'algebra di quaternioni. (Notiamo che* $\mathrm{End}(E)$ *indica* $End_{\overline{K}}(E)$.*)*

(v) Il gruppo formale $\hat{E}/K$ *associato ad* E *ha altezza 2.*

3 Curve ellittiche su $\mathbb{C}$

3.1 Curve ellittiche e tori

Definizione 3.1. Siano $w_1,\ w_2$ numeri complessi linearmente indipendenti su $\mathbb{R}$. Allora

$$\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 = \{n_1w_1 + n_2w_2 \mid n_1, n_2 \in \mathbb{Z}\}$$

è detto *reticolo*.

Sappiamo che $\mathbb{C}/\Lambda$ è un toro, e vogliamo mostrare che ogni toro ci fornisce una curva ellittica, e viceversa. L'insieme

$$\Pi = \{a_1w_1 + a_2w_2 \mid 0 \leq a_i < 1,\ i = 1, 2\}$$

è detto *parallelogramma fondamentale* per Λ.

Definizione 3.2. Una *funzione ellittica*, o *funzione doppiamente periodica*, su un reticolo complesso Λ è una funzione complessa analitica $f : \mathbb{C} \to \mathbb{C} \cup \infty$ tale che $f(z + w) = f(z)$ $\forall z \in \mathbb{C}$ e $w \in \Lambda$. Equivalentemente

$$f(z + w_i) = f(z), \quad i = 1, 2.$$

Un esempio non banale di funzione ellittica è la *$\wp$-funzione di Weierstrass*. Dato un reticolo Λ, la definiamo nel seguente modo

$$\wp(z) = \wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Ora vediamo che dato un toro, possiamo ottenre una curva ellittica.

Definizione 3.3. Dato un reticolo Λ, per $k \geq 3$, definiamo la *serie di Eisenstein*

$$G_k = G_k(\Lambda) = \sum_{\substack{w\in\Lambda \\ w\neq 0}} w^{-k}.$$

La serie converge, inoltre notiamo che per k dispari $G_k = 0$.

Teorema 3.1. *Sia $\wp(z)$ la $\wp$-funzione di Weierstrass per un reticolo Λ. Allora*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Facendo un cambio di variabili, otteniamo $y^2 = 4x^3 - g_2x - g_3$, che è l'equazione di una curva ellittica. Le funzioni ellittiche dipendono dal reticolo su cui vengono definite, ma a volte reticoli diversi possono avere le stesse funzioni ellittiche.

Diciamo che due reticoli Λ e Λ' sono *omotetici* se esiste un numero complesso non nullo $\lambda \in \mathbb{C}-\{0\}$ tale che $\Lambda' = \lambda\Lambda$. L'omotetia è una relazione d'equivalenza. L'omotetia influisce sulle funzioni ellittiche: se $f(z)$ è una funzione ellittica per Λ, allora $f(\lambda z)$ è una funzione ellittica per $\lambda\Lambda$. Inoltre la $\wp-$funzione di Weierstrass subisce la seguente trasformazione

$$\wp(\lambda z;\lambda\Lambda) = \lambda^{-2}\wp(z;\Lambda).$$

Per classificare i reticoli a meno di omotetie usiamo il $j-$invariante.

Definizione 3.4. il $j-$invariante $j(\Lambda)$ di un reticolo Λ è il numero complesso

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Il fatto notevole è che il $j-$invariante $j(\Lambda)$ caratterizza il reticolo Λ a meno di omotetie.

Ora dobbiamo mostrare il viceversa, cioè che data una curva ellittica $E(\mathbb{C})$, allora possiamo ottenere un unico reticolo Λ, a meno di omotetie.

Teorema 3.2. *Sia $y^2 = 4x^3 - Ax - B$ una curva ellittica E su $\mathbb{C}$. Allora esiste un reticolo Λ tale che $g_2(\Lambda) = A$ e $g_3(\Lambda) = B$ e c'è un isomorfismo di gruppi $\mathbb{C}/\Lambda \equiv E(\mathbb{C})$.*

3.2 Moltiplicazione complessa

L'anello degli endomorfismi di una curva ellittica E include sempre la moltiplicazione per un intero. Quando l'anello degli endomorfismi di E è strettamente più grande di $\mathbb{Z}$ diciamo che *E ha moltiplicazione complessa.*

Abbiamo già illustrato, in generale, quali sono le possibilità per un anello di endomorfismi di una curva ellittica definita su un campo K. Ora ci interessiamo di ciò nel caso in cui $K = \mathbb{C}$.

Teorema 3.3. *Sia E una curva ellittica su $\mathbb{C}$. Allora* $\mathrm{End}(E)$ *è isomorfo o a $\mathbb{Z}$ o a un ordine in un campo quadratico immaginario.*

In particolare per le curve a moltiplicazione complessa definite su $\mathbb{Q}$, ci sono 13 possibili valori per i j-invariante noti, e quindi 13 possibili ordini.

3.3 Classificazione di CM curve e modelli razionali

Vediamo ora, che esistono solo un numero finito di classi, a meno di $\overline{\mathbb{Q}}$-isomorfismi, di curve ellittiche con moltiplicazione complessa tramite un ordine $\mathcal{O}$. Ci limitiamo ad approfondire solo il caso in cui le curve ellittiche hanno moltiplicazione complessa tramite l'anello degli interi $\mathcal{O}_K$, con K campo quadratico immaginario.

I due risultati principali sono dati da due seguenti teoremi.

Proposizione 3.4. *(a) Sia Λ un reticolo con $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$, e siano $\mathfrak{a}$ e $\mathfrak{b}$ ideali frazionari non nulli di K. Allora*

(i) $\mathfrak{a}\Lambda$ è un reticolo in $\mathbb{C}$.

(ii) La curva ellittica $E_{\mathfrak{a}\Lambda}$ soddisfa $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}_K$.

(iii) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ se e solo se $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in $\mathcal{CL}(\mathcal{O}_K)$.

Quindi c'è un'azione ben definita di $\mathcal{O}_K$ su $\mathcal{ELL}(\mathcal{O}_K)$ determinata da

$$\overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

(b) L'azione di $\mathcal{CL}(\mathcal{O}_K)$ su $\mathcal{ELL}(\mathcal{O}_K)$ descritta in (a) è semplicemente transitiva. In particolare

$$\#\mathcal{CL}(\mathcal{O}_K) = \#\mathcal{ELL}(\mathcal{O}_K).$$

Proposizione 3.5. *(a) Sia $E/\mathbb{C}$ una curva ellittica, e sia $\sigma : \mathbb{C} \to \mathbb{C}$ un automorfismo di $\mathbb{C}$. Allora*

$$\mathrm{End}(E^\sigma) = \mathrm{End}(E).$$

(b) Sia $E/\mathbb{C}$ una curva ellittica con moltiplicazione complessa tramite $\mathcal{O}_K$, cioè l'anello degli interi di un campo quadratico immaginario K. Allora $j(E) \in \overline{\mathbb{Q}}$.

(c)

$$\mathcal{ELL}(\mathcal{O}_K) \cong \frac{\{ \textit{ curve ellittiche } E/\overline{\mathbb{Q}} \textit{ con } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\textit{isomorfismi su } \overline{\mathbb{Q}}}.$$

Dai risultati delle due proposizioni precedenti e dal fatto che $\#\mathcal{CL}(\mathcal{O}_K)$ è un numero finito, abbiamo quindi che ci sono un numero finito di classi di curve ellittiche con moltiplicazione complessa tramite $\mathcal{O}_K$ a meno di $\overline{\mathbb{Q}}$-isomorfismi.

Inoltre,sia E una curva ellittica con moltiplicazione complessa tramite $\mathcal{O}_K$, $h_K = \#\mathcal{CL}(\mathcal{O}_K)$ e $E = E_1, \ldots, E_{h_K}$ un insieme completo di rappresentanti di $\mathcal{ELL}(\mathcal{O}_K)$, allora $j(E_1), \ldots, j(E_{h_K})$ sono un insieme completo di coniugati di $j(E)$.

4 Riduzione $\mathrm{mod}\,\mathfrak{p}$ e il polinomio di classe di Hilbert

Analizziamo la relazione tra curve ellittiche definite su campi numerici e curve definite su campi finiti

4.1 Il Lemma di riduzione di Deuring

Vediamo l'operazione di riduzione di una curva.

Sia K un campo numerico e consideriamo la curva ellittica

$$E : y^2 = x^3 + Ax + B$$

con $A, B \in K$. Siamo interessati all'operazione di riduzione di E modulo un primo $\mathfrak{p}$ di $\mathcal{O}_K$ che giace sopra p, cioè tale che $\mathfrak{p} \cap \mathbb{Z} = p$. Ciò non può essere fatto in generale, ma supponiamo che A e B possono essere scritti nella forma α/β, dove α, $\beta \in \mathcal{O}_K$ e $\beta \notin \mathfrak{p}$. Allora possiamo definire le immagini $\overline{A}, \overline{B}$, nel campo finito $\mathbb{F}_p = \mathcal{O}_K/\mathfrak{p}$. Inoltre se abbiamo

$$\Delta = -16(4\overline{A}^3 + 27\overline{B}^2) \neq 0 \in \mathcal{O}_K/\mathfrak{p}$$

allora

$$\overline{E} : y^2 = x^3 + \overline{A}x + \overline{B}$$

definisce una curva ellittica su $\mathcal{O}_K/\mathfrak{p}$, e diciamo che E ha *buona riduzione* modulo $\mathfrak{p}$, o che $\mathfrak{p}$ è *un primo di buona riduzione.*

Deuring arrivò a dei risultati riguardo il comportamento dell'anello degli endomorfismi sotto la riduzione modulo un primo.

Lemma 4.1. *Siano E/L una curva ellittica definita su un campo numerico L con moltiplicazione complessa tramite un ordine $\mathcal{O}$ di un campo quadratico immaginario K, $\mathfrak{p}$ un ideale primo in $\overline{\mathbb{Q}}$ su un primo razionale p, e $\widetilde{E}$ la riduzione di E modulo $\mathfrak{p}$. Allora p è un primo supersingolare per E se e solo se p è ramificato o inerte in K.*

Concludiamo con un altro risultato di Deuring, che permette di sollevare la moltiplicazione complessa in caratteristica p alla caratteristica 0.

Lemma 4.2. *Sia E una curva ellittica definita su un campo finito e sia α un endomorfismo di E. Allora esiste una curva $\tilde{E}$, definita su un'estensione K di $\mathbb{Q}$ e un endomorfismo $\tilde{\alpha}$ di $\tilde{E}$, tale che E è la riduzione di $\tilde{E}$ modulo un ideale primo dell'anello degli interi algebrici di K e la riduzione di $\tilde{\alpha}$ è α.*

4.2 Il polinomio di classe di Hilbert

Sia $H_{\mathcal{O}}(X)$ il polinomio monico le cui radici sono i j-invarianti delle curve ellittiche definite su $\overline{\mathbb{Q}}$ con moltiplicazione complessa tramite $\mathcal{O}$, a meno di $\overline{\mathbb{Q}}$-isomorfismi.

Possiamo identificare $\mathcal{O}$ con il suo discriminante D. Indicheremo quindi $H_{\mathcal{O}}(X) = H_D(X)$. Quindi

$$H_D(X) = \prod_{E \in \mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O})} (X - j(E)).$$

Questo polinomio è il *polinomio di classe di Hilbert.* Ci concentriamo ora solo su due casi: $H_\ell(X)$ e $H_{4\ell}(X)$, con ℓ un primo tale che $\ell \equiv 3(\mathrm{mod}4)$ e $\ell > 3$, così da avere il numero delle classi $\mathcal{O}_D$, $h(\mathcal{O}_D)$, dispari.

Abbiamo due principali risultati su questi due particolari casi.

Proposizione 4.3. *Il polinomio $H_\ell(X)H_{4\ell}(X)$ è un quadrato modulo ℓ.*

Proposizione 4.4. *Le uniche radici reali di $H_\ell(X)$ e $H_{4\ell}(X)$ sono $j((1+\sqrt{-\ell})/2)$ e $j(\sqrt{-\ell})$ rispettivamente.*

Il fatto che $H_\ell(X)$ e $H_{4\ell}(X)$ hanno ciascuno solo una radice reale, implica che le altre radici siano in coppie complesse coniugate. Con $\ell \to \infty$, le radici reali di $H_\ell(X)$ e di $H_{4\ell}(X)$ tendono a $-\infty$ e a ∞, rispettivamente. Così per un z fissato, $H_\ell(j(z)) > 0$ e $H_{4\ell}(j(z)) < 0$ per un ℓ sufficientemente grande.

5 L'esistenza di infiniti primi supersingolari per curve razionali

Abbiamo visto un criterio per determinare i primi supersingolari per curve razionali a moltiplicazione complessa, e da questo è semplice dedurre che questi primi sono infiniti. Elkies nel 1987 riuscì a dare questo risultato per ogni curva razionale, anche per quelle non a moltiplicazione complessa.

Teorema 5.1. *Sia $E/\mathbb{Q}$ una curva ellittica e sia S un insieme finito di primi razionali. Allora E ha un primo supersingolare fuori da S.*

Riferimenti bibliografici

[1] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.

[2] Harold Davenport. *Multiplicative number theory*, volume 74. Springer Science & Business Media, 2013.

[3] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pages 197–272. Springer, 1941.

[4] Noam D. Elkies. Supersingular primes for elliptic curves over real number fields. *Compositio Mathematica*, 72(2):165–172, 1989.

[5] Benedict H. Gross. Arithmetic on elliptic curves with complex multiplication. With an appendix by B. Mazur. Lecture Notes in Mathematics. 776. Berlin-Heidelberg-New York: Springer-Verlag. V, 95 p. DM 18.00; $ 10.10 (1980)., 1980.

[6] Benedict H Gross and Don B Zagier. *On singular moduli.* Universität Bonn. SFB 40. Theoretische Mathematik/Max-Planck-Institut für Mathematik, 1984.

[7] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III. *Journal für die Reine und Angewandte Mathematik*, pages 55–62, 69–88, 193–208, 1936.

[8] http://math.stackexchange.com/users/55081/yannickvda. On hilbert class polynomial. Mathematics Stack Exchange.

[9] Dale Husemöller. *Elliptic curves.* Graduate texts in mathematics. Springer, New York, 2004.

[10] Serge Lang. *Elliptic functions.* Graduate texts in mathematics. Springer, New York, Berlin, 1987.

[11] Gorō Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1. Princeton University Press, 1971.

[12] Joseph H. Silverman. *The arithmetic of elliptic curves.* Graduate texts in mathematics. Springer, New York, Berlin, 1986.

[13] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[14] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem: Third Edition.* Ak Peters Series. Taylor & Francis, 2001.

[15] Lawrence C Washington. *Elliptic curves: number theory and cryptography.* CRC press, 2008.