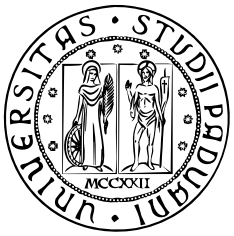

Università degli Studi di Padova

DIPARTIMENTO MATEMATICA

Università degli studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di laurea in Matematica

Il Weil pairing: costruzione, proprietà e applicazioni

Relatrice:
Prof.ssa Cristiana Bertolin

Candidata:
Giada Lentini
Matricola 2069425

Anno accademico 2025/2026 - 17.07.2026

Università degli Studi di Padova

DIPARTIMENTO MATEMATICA

Università degli studi di Padova
Dipartimento di Matematica "Tullio Levi-Civita"
Corso di laurea in Matematica

Il Weil pairing: costruzione, proprietà e applicazioni

Relatrice:
Prof.ssa Cristiana Bertolin

Candidata:
Giada Lentini
Matricola 2069425

Anno accademico 2025/2026 - 17.07.2026

Indice

Introduzione

Il Weil pairing, introdotto per la prima volta da André Weil nel 1940, rappresenta uno strumento fondamentale nello studio delle curve ellittiche e delle varietà abeliane e permette in particolare di trasferire alcuni problemi avanzati di geometria algebrica a problemi più classici sul gruppo delle radici m-esime dell'unità, contenuto nel gruppo moltiplicativo di un'opportuna estensione di campo, costituendo così un ponte tra questi due ambiti.
Negli ultimi decenni ha assunto un ruolo fondamentale anche nelle costruzioni crittografiche su curve ellittiche.
Un contributo significativo è stato dato da Victor S. Miller, che nel 1985 ha introdotto un algoritmo efficiente per calcolare il Weil pairing, oggi noto come algoritmo di Miller. Questo risultato ha posto le basi per gli sviluppi successivi, tra cui la riduzione del problema del logaritmo discreto su curve ellittiche al logaritmo discreto nel gruppo moltiplicativo e ha trovato applicazione anche nello studio della struttura di gruppo di una curva ellittica su campo finito. Successivamente, altri autori lo hanno applicato al problema Decision Diffie–Hellman (DDH) su curve ellittiche e alla costruzione della crittografia basata su identità (IBE) utilizzando curve ellittiche.

La tesi, facendo principalmente riferimento a *The Arithmetic of Elliptic Curves* di Silverman, analizza il Weil pairing nel contesto delle curve ellittiche, evidenziandone la costruzione e le proprietà principali. Nel primo capitolo, dopo un'introduzione alle curve ellittiche e alle loro caratteristiche fondamentali, vengono presentati i concetti di isogenia e di punti di torsione, necessari per lo sviluppo della teoria successiva. Si introduce poi il determinant pairing nel secondo capitolo, mettendone in evidenza le limitazioni che motivano l'introduzione del Weil pairing. Successivamente vengono presentati alcuni risultati sui divisori, strumenti essenziali per la costruzione del pairing. Si procede quindi nel terzo capitolo alla definizione del Weil pairing e alla dimostrazione delle sue proprietà fondamentali, tra cui bilinearità, alternanza e non degenerazione. Infine, nel quarto e ultimo capitolo, vengono discusse alcune conseguenze che derivano dalle sue proprietà, e si trattano brevemente alcune applicazioni di rilevante importanza, con particolare attenzione al suo ruolo in ambito crittografico.

Capitolo 1

Curve ellittiche

Definizione 1.0.1. Una curva ellittica è una coppia (E, O) dove $E \subset \mathbb{P}^2$ è una curva non singolare di genere 1 e $O \in E$ è un punto.
(Nel seguito indicheremo la curva ellittica con E, sottintendendo il punto O).
La curva ellittica E è definita su K se E è definita su K come curva e $O \in E(K)$.

Ogni curva ellittica può essere scritta come il luogo dei punti in $\mathbb{P}^2(K)$ di un'equazione cubica che ha un solo punto, O, sulla retta all'infinito.
Tale equazione, detta equazione di Weierstrass, è della forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Qui $O = [0 : 1 : 0]$ e $a_1, \ldots, a_6 \in K$, con K un campo su cui la curva è definita.

A seconda del contesto si possono usare forme semplificate di questa equazione, ad esempio la forma corta di Weierstrass

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

dove il campo K ha caratteristica diversa da 2 e 3.

Nel seguito si usano risultati classici della teoria delle curve ellittiche e della geometria algebrica. In particolare, si farà uso del teorema di Riemann–Roch per curve lisce di genere 1, delle proprietà del grado e della separabilità delle isogenie, delle proprietà del pull-back dei divisori e dei risultati di esistenza di funzioni con divisore assegnato. Per ulteriori dettagli si rimanda a Silverman, *The Arithmetic of Elliptic Curves*.

1.1 Struttura di gruppo

Sia E una curva ellittica, cioè $E \subset \mathbb{P}^2$ consiste nei punti $P = (x, y)$ che soddisfano l'equazione di Weierstrass, insieme al punto $O = [0 : 1 : 0]$ all'infinito.

Sia $L \subset \mathbb{P}^2$ una retta. Poiché l'equazione ha grado tre, per il teorema di Bézout la retta L interseca E in esattamente tre punti P, Q, R, non necessariamente distinti.

Definiamo una legge di composizione $\oplus$ mediante la seguente regola:

Siano $P, Q \in E$, sia L la retta passante per P e Q (se $P = Q$ sia L la retta tangente a E in P) e sia R il terzo punto di intersezione di L con E. Sia poi L' la retta passante per R e O. Allora L' interseca E in R, O e in un terzo punto che indichiamo con $P \oplus Q$.

L'uso del simbolo $\oplus$ trova giustificazione nella proposizione seguente.

Proposizione 1.1.1. *La legge di composizione ha le seguenti proprietà:*

a. *se una retta L interseca E nei punti P,Q,R, allora $(P \oplus Q) \oplus R = O$*

b. *$P \oplus O = P$ per ogni $P \in E$*

c. *$P \oplus Q = Q \oplus P$ per ogni P,$Q \in E$*

d. *Sia $P \in E$, allora esiste un punto in E, denotato con $-P$, tale che $P \oplus (-P) = O$*

e. *Sia $P, Q, R \in E$, allora $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$*

In altre parole la legge di composizione rende E un gruppo abeliano, con elemento neutro O. Inoltre supponendo che E sia definito su K, si ha che

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}$$

è un sottogruppo di E.

Notazione: D'ora in poi useremo i simboli $+$ e $-$ al posto di $\oplus$ e $\ominus$
Inoltre per $m \in \mathbb{Z}$ e $P \in E$, poniamo

$$[m]P = \begin{cases} \underbrace{P + \cdots + P}_{m \text{ termini}} & \text{se } m > 0, \\ \underbrace{(-P) + \cdots + (-P)}_{|m| \text{ termini}} & \text{se } m < 0, \\ O & \text{se } m = 0. \end{cases}$$

1.2 Isogenie

Dopo aver esaminato brevemente la geometria delle singole curve ellittiche, passiamo ora allo studio delle mappe tra curve.

Ricordiamo che una funzione razionale $f = \frac{a}{b}$ è ben definita in P se $b(P) \neq 0$.

Definizione 1.2.1. Siano $V_1, V_2 \subseteq \mathbb{P}^n$ varietà proiettive. Una *mappa razionale* da V_1 a V_2 è un'applicazione della forma

$$\phi = [f_0, \ldots, f_n] : V_1 \dashrightarrow V_2,$$

dove $f_0, \ldots, f_n \in K(V_1)$ sono funzioni razionali tali che, per ogni punto $P \in V_1$ nel quale tutte le f_i sono ben definite, si ha

$$\phi(P) = [f_0(P) : \cdots : f_n(P)] \in V_2.$$

Definizione 1.2.2. Una mappa razionale $\phi = [f_0, \ldots, f_n] : V_1 \dashrightarrow V_2$ si dice *regolare* in un punto $P \in V_1$ se esiste una funzione $g \in K(V_1)$ tale che:

- ogni gf_i è regolare in P;
- esiste un indice i per cui $(gf_i)(P) \neq 0$.

In tal caso si pone $\phi(P) = [(gf_0)(P) : \cdots : (gf_n)(P)]$.

Un *morfismo* è una mappa razionale che è regolare in ogni punto.
Si enuncia il seguente teorema che sarà utile in seguito.

Teorema 1.2.3. *Sia $\varphi : C_1 \to C_2$ un morfismo tra curve proiettive, lisce e irriducibili. Allora φ è costante oppure suriettivo.*

Poiché una curva ellittica ha un punto O distinto, è naturale considerare le mappe che rispettano questa proprietà.

Definizione 1.2.4. Siano E_1 ed E_2 curve ellittiche. Una *isogenia* da E_1 a E_2 è un morfismo

$$\phi : E_1 \longrightarrow E_2$$

tale che $\phi(O) = O$.

Due curve ellittiche E_1 ed E_2 sono isogene se esiste un'isogenia da E_1 a E_2 tale che $\phi(E_1) \neq \{O\}$.

Dal teorema 1.2.3 segue che un'isogenia soddisfa necessariamente una delle due condizioni:

$$\phi(E_1) = \{O\} \quad \text{oppure} \quad \phi(E_1) = E_2$$

Quindi, ad eccezione della zero-isogenia definita da $[0](P) = O$ per ogni $P \in E_1$, ogni altra isogenia è un morfismo non costante tra curve ellittiche, quindi ha grado e nucleo finiti. Di conseguenza si ottiene l'iniezione tra campi di funzioni:

$$\begin{aligned} \phi^* : \overline{K}(E_2) &\longrightarrow \overline{K}(E_1) \\ f &\longmapsto f \circ \phi \end{aligned}$$

Il grado di un'isogenia ϕ, denotato $\deg \phi$, è il grado dell'estensione finita di campi $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$.

Si dice inoltre che il morfismo ϕ è *separabile* (risp. *inseparabile*, risp. *pura inseparabile*) secondo la proprietà corrispondente dell'estensione di campi. Analogamente a prima si definiscono il grado separabile e il grado inseparabile, denotati con $\deg_s(\phi)$ e $\deg_i(\phi)$.
Infine, per convenzione si pone:

$$\deg[0] = 0.$$

Definizione 1.2.5. Sia $\phi : E_1 \longrightarrow E_2$ un'isogenia. L'*isogenia duale* di ϕ è l'isogenia

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

tale che $\hat{\phi} \circ \phi = [m]$, con m il grado dell'isogenia.

La relazione 'E_1 e E_2 sono isogene' definisce una relazione di equivalenza:

- (riflessività) siccome $\mathrm{id}_E : E \longrightarrow E$ è un'isogenia, allora $E \sim E$.
- (simmetria) se esiste un'isogenia $\phi : E_1 \longrightarrow E_2$ allora possiamo prendere l'isogenia duale $\hat{\phi} : E_2 \longrightarrow E_1$, quindi $E_1 \sim E_2 \Rightarrow E_2 \sim E_1$
- (transitività) se $\phi : E_1 \longrightarrow E_2$ e $\psi : E_2 \longrightarrow E_3$ sono isogenie, allora la composizione $\psi \circ \phi : E_1 \longrightarrow E_3$ è ancora un morfismo che manda O in O. Segue che se $E_1 \sim E_2$ e $E_2 \sim E_3$ allora $E_1 \sim E_3$.

Teorema 1.2.6. *Sia $\phi : E_1 \longrightarrow E_2$ un'isogenia separabile non nulla.*
Allora abbiamo che $|\ker(\phi)| = \deg(\phi)$.

Dimostrazione: L'isogenia ϕ è un morfismo finito di grado $\deg(\phi)$. Segue che per quasi tutti i punti $Q \in E_2$, il numero di punti $P \in E_1$ con $\phi(P) = Q$ è costante, e questo numero è il grado separabile del morfismo, cioè $\deg_s(\phi)$.
Siccome ϕ è separabile, cioè l'estensione dei campi di funzione è separabile, il grado separabile coincide con il grado totale

$$\deg(\phi) = \deg_s(\phi).$$

Dato che il nucleo $\ker(\phi) = \phi^{-1}(O)$ è l'insieme dei punti che vengono mandati nello zero, ponendo $Q = O$ otteniamo:

$$|\ker(\phi)| = |\phi^{-1}(O)| = \deg_s(\phi) = \deg(\phi).$$

□

1.3 Punti di torsione

Definizione 1.3.1. Sia E una curva ellittica definita su un campo K e sia m un numero intero positivo. Allora

$$E[m] = \{P \in E \mid [m]P = O\}$$

è il sottogruppo dei *punti di torsione* di E di ordine che divide m.

Supponiamo $char(K) \nmid m$.
L'applicazione $[m] : E \to E$ è un morfismo, e siccome chiaramente manda O in O è un'isogenia. Inoltre se E è definita su K, allora anche $[m]$ è definita su K.
Il risultato più importante, e interessante per i nostri scopi, è che il suo grado è

$$deg([m]) = m^2.$$

La dimostrazione del fatto precedente può essere ricavata utilizzando le isogenie duali, ma esistono anche dimostrazioni elementari ma lunghe, basate su formule esplicite e induzione.
Il nucleo di $[m]$ è per definizione il sottogruppo

$$ker([m]) = \{P \in E \mid [m]P = O\} = E[m].$$

Per l'ipotesi sulla caratteristica del campo, l'isogenia $[m]$ è separabile, quindi il teorema 1.2.6 implica che il numero di elementi del nucleo coincide con il grado dell'isogenia, quindi:

$$|E[m]| = deg([m]) = m^2.$$

Infine per il Teorema Fondamentale dei gruppi abeliani finiti si ha che ogni gruppo abeliano finito G può essere scritto come somma diretta di gruppi ciclici:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

con $n_1 \mid n_2 \mid \cdots \mid n_k$.

Siccome $\text{char}(K) \nmid m$, per un risultato standard sulla struttura dei punti di torsione delle curve ellittiche si ha che $E[m]$ è generato da al massimo due elementi, pertanto si ha

$$E[m] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \text{ con } a \mid b.$$

Ne consegue che l'ordine di $E[m]$ è

$$|E[m]| = a \cdot b.$$

Ma sapendo che $|E[m]| = m^2$ e siccome $a \mid b$, l'unica possibilità è $a = m,\ b = m$. Da cui si conclude che

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Capitolo 2

Determinant pairing

Sia E una curva ellittica su K. Sia fissato un intero $m \geq 2$ che si assume essere primo rispetto a $p = char(K)$, se $p > 0$.

Allora si ha $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Definizione 2.0.1. Sia R un anello. Un modulo su R è un insieme M munito di:

1. un'operazione binaria + su M rispetto alla quale M è un gruppo abeliano;
2. un'azione di R su M (cioè un'applicazione $R \times M \to M$) indicata con rm, per ogni $r \in R$ e $m \in M$, che soddisfa:
   (a) $(r+s)m = rm + sm$, per ogni $r, s \in R$, $m \in M$;
   (b) $(rs)m = r(sm)$, per ogni $r, s \in R$, $m \in M$;
   (c) $r(m+n) = rm + rn$, per ogni $r \in R$, $m, n \in M$.
   (d) $1m = m$, per ogni $m \in M$ (richiesto solo se l'anello ha un'unità).

Un modulo è libero se possiede una base, ed il rango di un modulo libero M è la cardinalità della sua base.

Una base per $E[m]$ è una coppia di punti $\{T_1, T_2\} \subset E[m]$ tale che:

1. (indipendenza) se $aT_1 + bT_2 = O$ con $a, b \in \mathbb{Z}/m\mathbb{Z}$, allora $a \equiv b \equiv 0 \pmod{m}$;
2. (generazione) ogni punto $R \in E[m]$ si può scrivere in modo unico come combinazione lineare $R = aT_1 + bT_2$ con $a, b \in \mathbb{Z}/m\mathbb{Z}$.

Quindi $E[m]$ è modulo libero su $\mathbb{Z}/m\mathbb{Z}$ di rango 2. Ogni modulo libero è dotato naturalmente di un'applicazione multilineare alternante non degenere, il determinante.

Definizione 2.0.2. Scegliendo una base $\{T_1, T_2\}$ per $E[m]$, il determinant pairing su $E[m]$ è dato da

$$\begin{array}{rcl} \det : E[m] \times E[m] & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ (aT_1 + bT_2, cT_1 + dT_2) & \longmapsto & ad - bc \end{array}$$

dove $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$.

Il valore del determinant pairing è indipendente dalla scelta della base.

Per dimostrare l'alternanza, sia $P = aT_1 + bT_2$. Allora

$$\det(P, P) = \det \begin{pmatrix} a & b \\ a & b \end{pmatrix} = ab - ab = 0.$$

Mentre è non degenere se

$$\det(P, Q) = 0 \quad \forall Q \quad \Longrightarrow \quad P = 0.$$

Sia $P = aT_1 + bT_2 \neq 0$. Allora almeno uno tra a e b è non nullo modulo m.
Si può scegliere $Q = T_2$ se $a \neq 0$, altrimenti $Q = T_1$ se $b \neq 0$.
Allora $\det(P, Q) = ad - bc \neq 0$ Quindi non esiste $P \neq 0$ che dia pairing zero per tutti gli altri elementi. Questo dimostra la non degeneranza.

Tuttavia uno svantaggio del determinant pairing su $E[m]$ è che non è invariante rispetto all'azione di Galois. Chiariamo ora cosa questo significa.

Sia $Gal(\overline{K}/K)$ il gruppo di Galois.
L'azione di un elemento $\sigma \in Gal(\overline{K}/K)$ su un punto $P = (x, y) \in E[m]$ è data da $P^\sigma = (x^\sigma, y^\sigma)$. Inoltre l'azione di Galois commuta con la legge di gruppo:

$$\begin{aligned} (P + Q)^\sigma &= P^\sigma + Q^\sigma \\ ([m]P)^\sigma &= [m]P^\sigma. \end{aligned}$$

Se $P \in E[m]$, allora $[m]P = O$. Quindi:

$$[m]P^\sigma = ([m]P)^\sigma = O^\sigma = O.$$

Segue che se P è un punto di m-torsione, anche P^σ è un punto di m-torsione. Il fatto che il determinant pairing non sia invariante rispetto all'azione di Galois implica che se $P, Q \in E[m]$ e $\sigma \in Gal(\overline{K}/K)$, allora non è detto che il valore di $\det(P^\sigma, Q^\sigma)$ e $\det(P, Q)^\sigma$ sia lo stesso. Per risolvere il problema della non invarianza sotto Galois, verrà introdotto un pairing modificato.

2.1 Divisori

Il gruppo dei divisori su una curva C, denotato con $\mathrm{Div}(C)$, è il gruppo abeliano libero generato dai punti di C. Quindi un divisore $D \in Div(C)$ è una somma formale

$$D = \sum_{P \in C} n_p(P)$$

dove $n_p \in \mathbb{Z}$ e $n_p = 0$ per tutti tranne un numero finito di punti $P \in C$.

Il grado di D è definito da

$$\deg D = \sum_{P \in C} n_P.$$

I divisori di grado zero formano un sottogruppo di $\mathrm{Div}(C)$, che denotiamo con

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) | \deg D = 0\}.$$

Se la curva C è definita su K, si fa agire $Gal(\overline{K}/K)$ su $\mathrm{Div}(C)$ e su $\mathrm{Div}^0(C)$ nel modo ovvio:

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma).$$

Allora si dice che D è definito su K se $D^\sigma = D$ per ogni $\sigma \in Gal(\overline{K}/K)$.

Si osservi che, se $D = n_1(P_1) + \cdots + n_r(P_r)$ con $n_1, \ldots, n_r \neq 0$, dire che D è definito su K non significa che $P_1, \ldots, P_r \in C(K)$. È sufficiente che il gruppo di Galois $Gal(\overline{K}/K)$ permuti i punti P_i in modo appropriato.

Indichiamo con $\mathrm{Div}_K(C)$ il gruppo dei divisori definiti su K, e analogamente con $\mathrm{Div}^0_K(C)$ il gruppo dei divisori di grado zero definiti su K.

Supponiamo ora che la curva C sia liscia, e sia $f \in \overline{K}(C),\ f \neq 0$. Si può allora associare a f il divisore $\mathrm{div}(f)$ dato da

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)\,(P)$$

dove $\mathrm{ord}_p(f)$ è l'ordine della funzione f in P. Un divisore di questo tipo, ovvero che proviene da una funzione razionale f sulla curva, è detto divisore principale. Due divisori $D_1, D_2 \in \mathrm{Div}(C)$ sono linearmente equivalenti se $D_1 - D_2$ è principale, e scriviamo $D_1 \sim D_2$.

Se $\sigma \in Gal(\overline{K}/K)$, allora si ha che

$$\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma.$$

In particolare, se $f \in K(C)$, allora $\mathrm{div}(f) \in \mathrm{Div}_K(C)$.

Si ha inoltre il seguente teorema.

Teorema 2.1.1. *Sia E una curva ellittica e sia $D = \sum_{P\in E} n_P(P) \in \mathrm{Div}(E)$. Allora D è un divisore principale se e solo se*

$$\sum_{P\in E} n_P = 0 \quad e \quad \sum_{P\in E} [n_P]P = O.$$

(Si noti che la prima somma è di numeri interi, mentre la seconda è la somma dei punti sulla curva E secondo la legge di gruppo).

Si approfondiscono ora alcune proprietà del divisore che saranno utili in seguito.

1. **Linearità del divisore:** se $D_1 = \mathrm{div}(f_1)$ e $D_2 = \mathrm{div}(f_2)$, allora $\mathrm{div}(f_1 f_2) = \mathrm{div}(f_1) + \mathrm{div}(f_2)$.

   Si ha infatti

   $$\begin{aligned}\mathrm{div}(f_1 f_2) &= \sum_P \mathrm{ord}_P(f_1 f_2)\, P = \sum_P \big(\mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)\big)P \\ &= \sum_P \mathrm{ord}_P(f_1)\, P + \sum_P \mathrm{ord}_P(f_2)\, P = \mathrm{div}(f_1) + \mathrm{div}(f_2).\end{aligned}$$

   Da cui generalizzando segue che

   $$\mathrm{div}\Big(\prod_i f_i\Big) = \sum_i \mathrm{div}(f_i).$$

2. **Divisore di una potenza:** $\mathrm{div}(g^m) = m\ \mathrm{div}(g)$.
   Osserviamo che

   $$\begin{aligned}\mathrm{div}(g^m) &= \sum_P \mathrm{ord}_P(g^m)\, P = \sum_P m\ \mathrm{ord}_P(g)\, P \\ &= m \sum_P \mathrm{ord}_P(g)\, P = m\ \mathrm{div}(g).\end{aligned}$$

3. **Costanza delle funzioni con divisore nullo:** se $\mathrm{div}(g) = 0$ allora g è costante.
   Infatti $\mathrm{div}(g) = 0$ significa che la funzione non ha zeri né poli, ma una funzione senza zeri né poli su una curva proiettiva, liscia e irriducibile è necessariamente costante.

4. **Pullback del divisore:** abbiamo che $\mathrm{div}(f\circ\varphi) = \varphi^*\big(\mathrm{div}(f)\big)$ dove $\varphi : E \to E$ è un morfismo.

   Questa, che è una proprietà generale dei morfismi, verrà usata per $\varphi = [m]$.

5. **Linearità del pullback del divisore:**

   $$[m]^*(aD_1 + bD_2) = a\,[m]^*D_1 + b\,[m]^*D_2.$$

6. **Traslazioni dei divisori:** se $\tau_P(Q) = Q + P$, allora

   $$\mathrm{div}(f \circ \tau_P) = \tau_P^*(\mathrm{div}(f)) = \text{divisore traslato di } f.$$

Capitolo 3

Weil pairing

3.1 Costruzione

Procediamo ora alla costruzione del Weil pairing.
Sia $T \in E[m]$. Allora esiste una funzione $f \in \overline{K}(E)$ tale che

$$\mathrm{div}(f) = m(T) - m(O).$$

Sia poi $T' \in E$ un punto tale che $[m]T' = T$. Allora esiste una funzione $g \in \overline{K}(E)$ tale che

$$\mathrm{div}(g) = [m]^*(T') - [m]^*(O) = \sum_{R \in E[m]} \big((T' + R) - (R)\big).$$

Verifichiamo che la somma dei punti è il punto neutro O.
Siccome $|E[m]| = m^2$, ci sono m^2 punti di m-torsione, ed il gruppo è finito. Inoltre si ha che $[m^2]T' = O$, infatti

$$[m^2]T' = [m]([m]T') = [m]T = O.$$

Quindi

$$\sum_{R \in E[m]} (T' + R) = m^2 T' + \sum_{R \in E[m]} R = \sum_{R \in E[m]} R.$$

Da cui segue che

$$\sum_{R \in E[m]} \big((T' + R) - R\big) = \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} R = O.$$

Osserviamo ora che le funzioni $f \circ [m]$ e g^m hanno lo stesso divisore.

$$\begin{aligned}
\operatorname{div}(f \circ [m]) &= [m]^*(\operatorname{div}(f)) \\
&= [m]^*(m(T) - m(O)) \\
&= m\ ([m]^*(T) - [m]^*(O)) \\
&= m\ (\sum_{R \in E[m]} ((T' + R) - R)) \\
&= m \cdot \operatorname{div}(g) \\
&= \operatorname{div}(g^m)
\end{aligned}$$

Segue che moltiplicando f per una costante appropriata in $\overline{K}^*$, si può assumere che

$$f \circ [m] = g^m.$$

Sia ora $S \in E[m]$ un altro punto di m-torsione, dove permettiamo anche che sia $S = T$. Allora per ogni punto $X \in E$ si ha

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Cioè

$$\left(\frac{g(X + S)}{g(X)}\right)^m = 1.$$

Considerata come funzione di X, la funzione $\frac{g(X+S)}{g(X)}$ ha immagine contenuta nel gruppo finito μ_m. In particolare l'immagine del morfismo è finita e quindi non può essere suriettiva su $\mathbb{P}^1$.
Siccome il morfismo

$$E \longrightarrow \mathbb{P}^1, \quad S \longmapsto \frac{g(X + S)}{g(X)}$$

non è suriettivo, per il teorema 1.2.3 è costante.
Questo permette di definire il pairing

$$\begin{aligned}
e_m : E[m] \times E[m] &\longrightarrow \mu_m \\
(S, T) &\longmapsto e_m(S, T) = \frac{g(X + S)}{g(X)}
\end{aligned}$$

dove $X \in E$ è un punto qualunque tale che $g(X + S)$ e $g(X)$ siano entrambi definiti e non nulli, mentre μ_m denota il gruppo delle radici m-esime dell'unità

$$\mu_m = \{\zeta \in \overline{K}^* \mid \zeta^m = 1\}.$$

Si osservi che la scelta della funzione g non è unica: se g è una scelta valida, anche

$$g' = c \cdot g, \quad c \in \overline{K}^*,$$

lo è, cioè la funzione g è ben definita a meno della moltiplicazione per un elemento di $\overline{K}^*$. Ma si ha anche che

$$e_m(S,T) = \frac{g(X+S)}{g(X)} \quad \text{diventa} \quad \frac{g'(X+S)}{g'(X)} = \frac{c \cdot g(X+S)}{c \cdot g(X)} = \frac{g(X+S)}{g(X)}.$$

Quindi il valore di $e_m(S,T)$ non dipende dalla scelta della funzione g.

Il pairing che abbiamo appena definito si chiama *Weil pairing* e_m.

3.2 Proprietà

In questa sezione enunceremo e dimostreremo il teorema principale del Weil pairing, che ne esplicita le proprietà fondamentali.

Teorema 3.2.1. *Il Weil pairing e_m ha le seguenti proprietà:*

a. *È bilineare*
$$e_m(S_1+S_2,T) = e_m(S_1,T)\, e_m(S_2,T)$$
$$e_m(S,T_1+T_2) = e_m(S,T_1)\, e_m(S,T_2).$$

b. *È alternante*
$$e_m(T,T) = 1$$
in particolare
$$e_m(S,T) = e_m(T,S)^{-1}.$$

c. *È non degenere*
$$e_m(S,T) = 1 \ \ \forall\, S \in E[m] \implies T = O.$$

d. *È invariante rispetto al gruppo di Galois*
$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) \qquad \forall\, \sigma \in \mathrm{Gal}(\overline{K}/K).$$

e. *È compatibile*
$$e_{mm'}(S,T) = e_m([m']S,T) \qquad \forall\, S \in E[mm'],\ T \in E[m].$$

Dimostrazione:

a. La linearità del primo fattore è semplice.
$$\begin{aligned} e_m(S_1+S_2,T) &= \frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_1)} \cdot \frac{g(X+S_1)}{g(X)} \\ &= e_m(S_2,T)\, e_m(S_1,T). \end{aligned}$$

Si noti quanto sia utile che, nel calcolare $e_m(S_2, T) = g(Y + S_2)/g(Y)$, possiamo scegliere qualunque valore di Y, ad esempio, possiamo prendere $Y = X + S_1$.

Per dimostrare la linearità nel secondo fattore, siano $f_1, f_2, f_3, g_1, g_2, g_3$ le funzioni appropriate per i punti T_1, T_2 e $T_3 = T_1 + T_2$.

Sia scelta una funzione $h \in \overline{K}(E)$ con divisore

$$\operatorname{div}(h) = (T_1 + T_2) - (T_1) - (T_2) + (O).$$

Allora per la linearità del divisore rispetto a prodotto e quoziente

$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = m \operatorname{div}(h),$$

quindi

$$f_3 = c\, f_1\, f_2\, h^m \quad \text{per qualche } c \in \overline{K}^*.$$

Componiamo con il morfismo di moltiplicazione per m, usiamo il fatto che

$$f_i \circ [m] = g_i^m,$$

e prendiamo la radice m-esima per ottenere

$$g_3 = c'\, g_1\, g_2\, (h \circ [m]) \quad \text{per qualche } c' \in \overline{K}^*.$$

Questo ci permette di calcolare

$$\begin{aligned} e_m(S, T_1 + T_2) &= \frac{g_3(X + S)}{g_3(X)} \\ &= \frac{g_1(X + S)\, g_2(X + S)\, h([m]X + [m]S)}{g_1(X)\, g_2(X)\, h([m]X)} \\ &= e_m(S, T_1)\, e_m(S, T_2), \end{aligned}$$

poiché $[m]S = O$.

b. Da (a) abbiamo

$$e_m(S + T, S + T) = e_m(S, S)\, e_m(S, T)\, e_m(T, S)\, e_m(T, T),$$

quindi è sufficiente dimostrare che

$$e_m(T, T) = 1 \quad \text{per ogni } T \in E[m].$$

Per ogni $P \in E$, $\tau_P : E \to E$ denota la traslazione per P, cioè $\tau_P(X) = X + P$. Calcoliamo

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m \sum_{i=0}^{m-1} \big([1 - i]T - [-i]T\big) = 0.$$

Ne segue che

$$\prod_{i=0}^{m-1} f \circ \tau_{[i]T}$$

è costante. Se scegliamo un punto $T' \in E$ tale che $[m]T' = T$, allora anche

$$\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}$$

è costante, poiché la sua potenza m-esima è il prodotto precedente delle f.

Pertanto il prodotto delle g assume lo stesso valore in X e in $X + T'$:

$$\prod_{i=0}^{m-1} g\big(X + [i]T'\big) = \prod_{i=0}^{m-1} g\big(X + [i+1]T'\big).$$

Cancellando i termini uguali da entrambi i lati si ottiene

$$g(X) = g\big(X + [m]T'\big) = g(X + T),$$

e quindi

$$e_m(T, T) = \frac{g(X + T)}{g(X)} = 1.$$

c. Se $e_m(S, T) = 1$ per ogni $S \in E[m]$, allora

$$g(X + S) = g(X) \quad \text{per ogni } S \in E[m],$$

ovvero g dipende solo dall'immagine tramite [m], segue che esiste una funzione $h \in \overline{K}(E)$ tale che

$$g = h \circ [m].$$

Ma allora

$$(h \circ [m])^m = g^m = f \circ [m],$$

il che implica

$$f = h^m.$$

Ne segue che

$$m \ \mathrm{div}(h) = \mathrm{div}(f) = m(T) - m(O),$$

perciò

$$\mathrm{div}(h) = (T) - (O).$$

Ovvero $(T) \sim (O)$. Poichè E è una curva di genere uno e $T, O \in E$, per un lemma sulla equivalenza lineare dei divisori, si ha

$$(T) \sim (O) \quad \Leftrightarrow \quad T = O.$$

Ne segue che $T = O$.

d. Sia $\sigma \in G_{K/\overline{K}}$. Se f e g sono le funzioni associate a T come sopra, allora chiaramente f^σ e g^σ sono le funzioni corrispondenti a T^σ.

Allora

$$e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = e_m(S,T)^\sigma.$$

e. Prendendo f e g come al solito, abbiamo

$$\operatorname{div}(f^{mm'}) = mm'(T) - mm'(O)$$

e

$$(g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}.$$

Direttamente dalla definizione di $e_{mm'}$ ed e_m, calcoliamo

$$e_{mm'}(S,T) = \frac{g \circ [m'](X+S)}{g \circ [m'](X)} = \frac{g(Y + [m']S)}{g(Y)} = e_m([m']S, T).$$

□

Ricordiamo che ad ogni isogenia $\phi : E_1 \to E_2$ è associata l'isogenia duale $\hat{\phi} : E_2 \to E_1$. La prossima proposizione afferma che ϕ e $\hat{\phi}$ sono duali rispetto al Weil pairing.

Proposizione 3.2.2. *Sia $\phi : E_1 \to E_2$ un'isogenia tra curve ellittiche. Allora per ogni punto di m-torsione $S \in E_1[m]$ e $T \in E_2[m]$ si ha che*

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T).$$

Dimostrazione: Sia $\operatorname{div}(f) = m(T) - m(O)$ e $f \circ [m] = g^m$, come di consueto. Allora

$$e_m(\phi(S), T) = \frac{g(X + \phi(S))}{g(X)}.$$

Scegliamo una funzione $h \in \overline{K}(E_1)$ tale che

$$\phi^*(T) - \phi^*(O) = (\hat{\phi}(T)) - (O) + \operatorname{div}(h).$$

Inoltre si ha

$$\operatorname{div}\left(\frac{f \circ \phi}{h^m}\right) = \phi^*(\operatorname{div}(f)) - m\operatorname{div}(h) = m(\hat{\phi}T) - m(O)$$

e

$$\left(\frac{g \circ \phi}{h \circ [m]}\right)^m = \frac{f \circ [m] \circ \phi}{(h \circ [m])^m} = \left(\frac{f \circ \phi}{h^m}\right) \circ [m].$$

Allora, direttamente dalla definizione del Weil pairing si ottiene

$$e_m(S, \hat{\phi}(T)) = \frac{(g \circ \phi / h \circ [m])(X+S)}{(g \circ \phi / h \circ [m])(X)} = \frac{g(\phi X + \phi S)}{g(\phi X)} \cdot \frac{h([m]X)}{h([m]X + [m]S)} = e_m(\phi(S), T).$$

□

Capitolo 4

Conseguenze e applicazioni

4.1 Corollari

Corollario 4.1.1. *Sia $\{T_1, T_2\}$ una base di $E[n]$. Allora $e_n(T_1, T_2)$ è una radice n-esima primitiva dell'unità.*

Dimostrazione: Poniamo $e_n(T_1, T_2) = \zeta$ e supponiamo che $\zeta^d = 1$ per un certo intero d. Per bilinearità si ha

$$e_n(T_1, dT_2) = e_n(T_1, T_2)^d = \zeta^d = 1.$$

Inoltre, siccome $e_n(T_2, T_2) = 1$,

$$e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1.$$

Sia ora $S \in E[n]$. Poiché $\{T_1, T_2\}$ è una base di $E[n]$, esistono $a, b \in \mathbb{Z}$ tali che $S = aT_1 + bT_2$. Pertanto,

$$\begin{aligned} e_n(S, dT_2) &= e_n(aT_1 + bT_2, dT_2) \\ &= e_n(T_1, dT_2)^a \, e_n(T_2, dT_2)^b \\ &= 1. \end{aligned}$$

Poiché tale uguaglianza vale per ogni $S \in E[n]$, dalla non degenerazione segue che $dT_2 = O$. Essendo T_2 un elemento di una base di $E[n]$, esso ha ordine esattamente n. Di conseguenza,

$$dT_2 = O \qquad \Longleftrightarrow \qquad n \mid d.$$

Abbiamo quindi mostrato che ogni intero d tale che $\zeta^d = 1$ è necessariamente multiplo di n. Quindi l'ordine di ζ è esattamente n.

□

Corollario 4.1.2. *Se $E[n] \subseteq E(K)$, allora $\mu_n \subset K$.*

Dimostrazione: Sia σ un qualsiasi automorfismo di $\overline{K}$ che fissa K, cioè tale che

$$a^\sigma = a \qquad \forall a \in K.$$

Siano T_1, T_2 una base di $E[n]$. Poiché T_1 e T_2 hanno coordinate in K, si ha

$$T_1^\sigma = T_1, \qquad T_2^\sigma = T_2.$$

Usando l'invarianza rispetto al gruppo di Galois si ha

$$\zeta = e_n(T_1, T_2) = e_n(T_1^\sigma, T_2^\sigma) = e_n(T_1, T_2)^\sigma = \zeta^\sigma.$$

Quindi ζ è fissata da ogni automorfismo σ.
Per il teorema fondamentale della teoria di Galois, se un elemento di $\overline{K}$ è fissato da tutti gli automorfismi che fissano K, allora appartiene a K. Quindi $\zeta \in K$.
Poiché ζ è una radice n-esima primitiva dell'unità, segue che $\mu_n \subset K$.

□

Corollario 4.1.3. *Sia E una curva ellittica definita su $\mathbb{Q}$. Allora $E[n] \nsubseteq E(\mathbb{Q})$ per $n \geq 3$.*

Dimostrazione: Se $E[n] \subseteq E(\mathbb{Q})$, allora $\mu_n \subseteq \mathbb{Q}$. Ma questo non è possibile per $n \geq 3$. Segue che $E[n] \nsubseteq E(\mathbb{Q})$.

□

4.2 Problema del logaritmo discreto e crittografia

Sia p un numero primo e siano a, b interi non nulli modulo p. Supponiamo di sapere che esiste un intero k tale che

$$a^k \equiv b \pmod{p}.$$

Il problema del logaritmo discreto classico (DLP) consiste nel trovare k. Poiché anche $k + (p-1)$ è una soluzione, la risposta k deve essere considerata definita modulo $p-1$, oppure modulo un divisore d di $p-1$ se $a^d \equiv 1 \pmod{p}$.
Più in generale, sia G un gruppo, e siano $a, b \in G$. Supponiamo di sapere che $a^k = b$ per qualche intero k. In questo contesto, il problema del logaritmo discreto consiste ancora nel trovare k.
Ad esempio G potrebbe essere $E(\mathbb{F}_q)$ per una certa curva ellittica, con $\mathbb{F}_q$ campo finito, nel qual caso a e b sono punti su E e si cerca un intero k tale che $ka = b$.
Esistono diverse applicazioni crittografiche del problema del logaritmo discreto, e la sicurezza dei crittosistemi dipenderà dalla difficoltà nel risolvere tali problemi.
Un modo per affrontare il problema del logaritmo discreto è quello di provare tutti i valori di k fino a quando uno funziona, ma questo è impraticabile quando la soluzione k può essere un intero di diverse centinaia di cifre, come spesso avviene in crittografia. Sono quindi necessarie tecniche migliori.

Un esempio di metodo che cerca di ottimizzare il processo è quello detto Baby Step, Giant Step. Questo metodo, sviluppato da D. Shanks, richiede circa $\sqrt{N}$ passi e circa $\sqrt{N}$ di memoria, dove N è l'ordine del gruppo, e per questo funziona bene solo per valori moderati di N.
Il problema di tale metodo è che richiede una grande quantità di memoria, mentre esistono altri algoritmi, come ad esempio ρ e λ di Pollard, che pur avendo un tempo di esecuzione approssimativamente equivalente, riducono di molto la memoria utilizzata. Nonostante questi miglioramenti, per gruppi di grandi dimensioni rimangono algoritmi computazionalmente proibitivi.
Ed è qui che entrano in gioco le curve ellittiche. Infatti tali curve forniscono un livello di sicurezza equivalente a quello dei sistemi crittografici classici utilizzando però un numero inferiore di bit.
Un esempio di sistema crittografico basato sulle curve ellittiche è il Diffie-Hellman Key Exchange. In tale metodo Alice e Bob concordano su una curva ellittica E su un campo finito F_q e su un punto $P \in F_q$. Alice e Bob scelgono rispettivamente interi segreti a e b. Alice pubblica $A = aP$, mentre Bob pubblica $B = bP$. Dopo di che entrambi moltiplicano il punto ricevuto per il proprio scalare scelto. Entrambi ottengono quindi lo stesso punto abP, che può essere utilizzato per derivare una chiave condivisa. In questo modo un osservatore esterno per trovare la chiave dovrebbe risolvere un problema di logaritmo discreto, ma come abbiamo visto è complicato e questo costituisce il fondamento della sicurezza del sistema crittografico.
Infine il Weil pairing assume un ruolo importante nello studio della sicurezza dei sistemi crittografici basati su curve ellittiche. Infatti esso permette di mettere in relazione il problema del logaritmo discreto su una curva ellittica con il problema del logaritmo discreto nel gruppo moltiplicativo di un campo finito e questa è proprio l'idea alla base dell'attacco MOV (Menezes–Okamoto–Vanstone).
In questo contesto il Weil pairing assume un ruolo centrale e queste considerazioni, insieme a molte altre, motivano lo studio sia dal punto di vista teorico che applicativo.

Bibliografia

[1] David S. Dummit e Richard M. Foote. *Abstract Algebra*. 3rd. John Wiley & Sons, Inc., 2004.

[2] Victor S. Miller. «The Weil Pairing, and Its Efficient Calculation». In: *Journal of Cryptology* 17.4 (2004), pp. 235–261. DOI: 10.1007/s00145-004-0315-8.

[3] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd. Springer, 2009.

[4] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. 2nd. Chapman & Hall/CRC, 2008.