Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

CLASSIFICAZIONE DELLE CURVE ELLITTICHE VISTE COME CURVE ALGEBRICHE PIANE

Tesi di Laurea in Geometria Proiettiva

Relatore:
Chiar.mo Prof.
ALESSANDRO GIMIGLIANO

Correlatore:
Chiar.mo Prof.
DAVIDE ALIFFI

Presentata da:
ANGELINA ZHENG

II Sessione
Anno Accademico 2015/2016

Indice

Introduzione

'It is possible to write endlessly on Elliptic Curves, (This is not a threat).'[1].

La teoria delle curve ellittiche, infatti, pur essendo oggetto di studio in Matematica da oltre un secolo, è varia, ricca e incredibilmente vasta; si deve al suo sviluppo, ad esempio, la dimostrazione della famosa congettura di Fermat. Essa ha anche molteplici applicazioni, ad esempio in Teoria dei numeri e Crittografia. Verso la metà degli anni 80, mentre H. Lenstra mostrò come usare le curve ellittiche per la fattorizzazione di interi, V. Miller e N. Koblitz proposero per la prima volta un sistema a chiave pubblica basato sulle curve ellittiche: ECC, e da allora le curve ellittiche hanno assunto un ruolo sempre più importante in Crittografia.

In questa tesi studieremo in particolare le curve ellittiche sotto la forma di curve algebriche piane, più precisamente come cubiche liscie nel piano proiettivo complesso, e ne forniremo una classificazione.

Nel primo capitolo tratteremo delle nozioni prelimirari, necessarie per introdurre e comprendere i capitoli successivi: definiremo le Superfici topologiche reali compatte e orientabili, le curve algebriche (limitandoci a considerare solo quelle definite sul piano proiettivo complesso) e, grazie al Teorema di classificazione delle Superfici compatte, forniremo una loro prima possibile classificazione basata sul genere della superficie e della curva, rispettivamen-

te.

Nel secondo capitolo, tramite la preliminare classificazione delle curve algebriche introdotta nel capitolo precedente, definiremo le curve ellittiche e le studieremo sotto l'aspetto di cubiche proiettive nel piano complesso. Inoltre, ne esamineremo più in dettaglio le principali proprietà, quali la possibilità di definirle tramite un'equazione affine nota come *equazione di Weierstrass* e la loro struttura intrinseca di gruppo abeliano.

Nel terzo capitolo, invece, si fornirà una classificazione delle cubiche lisce totalmente differente da quella fornita nel primo capitolo. Questa classificazione, infatti, segue dal Corollario del Teorema di Salmon e si basa su una relazione di equivalenza proiettiva, dove le classi sono individuate dal *modulo della cubica*, invariante per trasformazioni proiettive che analizzeremo nella prima parte dello stesso capitolo.

Infine, l'ultimo capitolo si concentrerà su un aspetto computazionale delle curve ellittiche, ovvero sulla loro applicazione nel campo della Crittografia. Grazie alla struttura che esse assumono sui campi finiti, sotto opportune ipotesi, i crittosistemi a chiave pubblica basati sul problema del logaritmo discreto definiti sulle curve ellittiche, a parità di sicurezza rispetto ai crittosistemi classici, permettono l'utilizzo di chiavi più corte, e quindi meno costose computazionalmente. Definiremo quindi il problema del logaritmo discreto classico e sulle curve ellittiche, e forniremo alcuni esempi di algoritmi crittografici classici definiti su quest'ultime.

Capitolo 1

Superfici compatte orientabili e curve algebriche

Questo primo capitolo è di carattere preliminare, in esso enunciamo definizioni e teoremi che sono basilari per comprendere lo svolgimento dei capitoli successivi, e in particolare per definire le curve ellittiche.

1.1 Superfici compatte orientabili

Introduciamo ora la nozione di superficie compatta orientabile e quella di genere di una superficie, un invariante topologico che ci permetterà di classificare le superfici compatte orientabili.

Definizione 1.1. Una *superficie* (*topologica*) S è uno spazio topologico connesso e di Hausdorff tale che $\forall s \in S$, $\exists U$ intorno di s omeomorfo ad un aperto di $\mathbb{R}^2$.

Definizione 1.2. Uno spazio topologico X si dice *compatto* se è di Hausdorff e *quasi compatto*, ossia se da ogni ricoprimento aperto di X si può estrarre un sottricoprimento finito.

Definizione 1.3. Una superficie S si dice *orientabile* se non contiene alcun nastro di Möbius, si dice invece *non orientabile* se ne contiene uno.

Esempi di superfici compatte e orientabili:

1. La sfera S^2;

2. Il toro.

Definizione 1.4. Data una superficie S, il *genere* di S è definito come il numero più grande di curve semplici chiuse e disgiunte contenute in S che non la sconnettono.

Esempio 1.1.
1. La sfera S^2 ha genere 0: ogni curva chiusa tracciata su di essa la divide in due;

2. Il toro ha genere 1: è possibile tagliare il toro lungo una curva chiusa che segue una delle due circonferenze generatrici senza sconnetterlo, ogni altro taglio supplementare produrrebbe due superfici sconnesse.

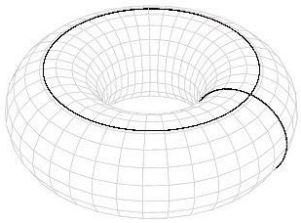


Figura 1.1: Due curve lungo cui si può tagliare il toro mantenendolo connesso.

Osservazione 1. Il genere di una superficie compatta orientabile corrisponde esattamente al numero di 'buchi' della superficie.

Enunciamo di seguito il Teorema di classificazione delle superfici compatte che ci permette di classificare le superfici in base al loro genere.

Teorema 1.1.1. (Teorema di classificazione delle superfici compatte, vedi [2]) *Ogni superficie compatta è omeomorfa ad una sfera, ad una somma connessa di tori oppure ad una somma connessa di piani proiettivi.*

Si ha di conseguenza che ogni superficie compatta orientabile è omoeomorfa ad una sfera o ad una somma connessa di tori, in quanto il piano proiettivo non è orientabile.

Corollario 1.1.2. *Siano S e P due superfici compatte orientabili, allora*

$$S \cong P \Leftrightarrow S \, e \, P \, hanno \, lo \, stesso \, genere;$$

dove $S \cong P$ indica che S e P sono omeomorfe tra loro, cioè topologicamente equivalenti.

Il genere di una superficie è dunque un invariante topologico e, in particolare, è possibile classificare le superfici compatte orientabili in base a questo.

1.2 Curve algebriche

Definiamo ora le curve algebriche, in particolare considereremo quelle definite sul piano proiettivo complesso. Analizzeremo poi alcune delle caratteristiche principali, quali il supporto, il grado e le singolarità.

Definizione 1.5. Una *curva algebrica* $\mathcal{C}$ nel piano complesso $\mathbb{C}^2$ è una classe di proporzionalità di polinomi non costanti di $\mathbb{C}[x, y]$, ossia un elemento dello spazio quoziente $\mathbb{C}[x, y]/\mathbb{C}^*$:

$$\mathcal{C} := [f]\,; \qquad f \in \mathbb{C}[x, y]/\mathbb{C}^*$$

Se $f(x, y)$ è un rappresentante della curva, l'equazione

$$f(x, y) = 0$$

si dice *equazione della curva.*
L' insieme dei punti che soddisfano l'equazione della curva

$$Supp(\mathcal{C}) := \big\{(X, Y) \in \mathbb{C}^2 \mid f(x, y) = 0\big\}$$

si dice *supporto* della curva.

Definizione 1.6. Il *grado* di una curva algebrica $\mathcal{C}$ è definito come il grado del polinomio f che la definisce, e si indica con $deg(\mathcal{C})$.

Definizione 1.7. Una curva algebrica $\mathcal{C}$ si dice *irriducibile* se il polinomio f che la definisce è irriducibile.

Consideriamo adesso le curve algebriche nel piano proiettivo complesso.

Siano $\mathbb{P}^2(\mathbb{C})$ il piano proiettivo complesso e $\mathbb{C}[x_0, x_1, x_2]$ l'anello (graduato) a coefficienti in $\mathbb{C}$ nelle incognite x_0, x_1 e x_2 (coordinate omogenee di $\mathbb{P}^2(\mathbb{C})$).

Un polinomio si dice *omogeneo* di grado d se tutti i suoi monomi hanno lo stesso grado o, equivalentemente, se

$$F(\lambda x_0, \lambda x_1, ..., \lambda x_n) = \lambda^d F(x_0, x_1, ..., x_n) \qquad \forall \lambda \in \mathbb{C}^*$$

Si ha che in $\mathbb{P}^2(\mathbb{C})$ solo i polinomi omogenei hanno delle radici ben definite a meno di multipli.

Siccome gli elementi di $\mathbb{P}^2(\mathbb{C})$ sono definiti a meno di proporzionalità, per definire una curva algebrica (proiettiva) $\mathcal{C}$, è necessario considerare solo i polinomi omogenei F, $F \in \mathbb{C}[x_0, x_1, x_2]_d$, ove $\mathbb{C}[x_0, x_1, x_2]_d$ è lo spazio vettoriale generato dai polinomi di grado d.

Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ una curva algebrica definita dal polinomio omogeneo $F \in \mathbb{C}[x_0, x_1, x_2]_d$. È possibile studiarla in una delle carte affini $U_0 = \{x_0 \neq 0\}$, $U_1 = \{x_1 \neq 0\}$, $U_2 = \{x_2 \neq 0\}$, disomogeneizzando in U_i il polinomio $F(x_0, x_1, x_2)$ come $f(x, y) \in \mathbb{C}[x, y]$, ove $x = \frac{x_{i_1}}{x_i}$, $y = \frac{x_{i_1}}{x_i}$, $i \neq i_1, i_2$.

Esempio 1.2. Consideriamo $\mathcal{C} \longleftrightarrow F : x_0{x_1}^2 - {x_2}^2 x_0 + {x_2}^3 = 0$
Per disomogeneizzare il polinomio, mi pongo, ad esempio, nella carta affine $U_0 = \{x_0 \neq 0\}$, quindi suppongo $x_0 = 1$ e ottengo la seguente equazione, non

più omogenea:
$f : x^2 - y^2 + y^3 = 0$.

Definizione 1.8. Sia $\mathcal{C}$ una curva algebrica definita dal polinomio omogeneo $F(x_0, x_1, x_2)$; se ne consideri la sua disomogeneizzazione in una carta affine (ad esempio $U_0 = \{x_0 \neq 0\}$) che denotiamo $f = (x, y)$ e sia $P = (a, b) \in \mathcal{C}$. Allora si dice che P è un *punto singolare*, o una *singolarità*, per $\mathcal{C}$ se $(f_x|_P, f_y|_P) = (0, 0)$. Altrimenti P si dice un *punto semplice* per $\mathcal{C}$. Inoltre, se $P \in \mathcal{C}$ è punto singolare e in P si annullano tutte le derivate parziali di f fino all'ordine $r - 1$, allora P si dice punto $r - plo$, e se in P si hanno r rette tangenti distinte, P si dice *singolarità ordinaria*.

Definizione 1.9. Una curva algebrica $\mathcal{C}$ si dice *singolare* se contiene punti singolari, altrimenti si dice *non singolare* o *liscia*.

Esempio 1.3. Consideriamo la curva algebrica $\mathcal{C}$ dell'esempio precedente.

$$f : x^2 - y^2 + y^3 = 0$$

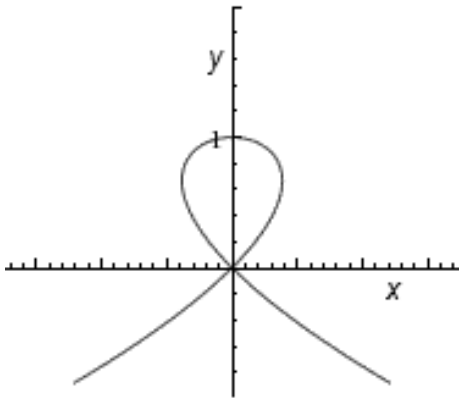


Figura 1.2: Curva algebrica dell'es 1.2 nella carta affine.

$f_x = 2x$
$f_y = -2y + 3y^2$

f_x e f_y si annullano in $(0,0)$, ma $f_{xx}(0,0) = 2 \neq 0$.
Si ha quindi che $(0,0)$ è un punto doppio ordinario (le tangenti sono $x-y=0$, $x+y=0$).

1.3 Classificazione delle curve algebriche

Illustreremo in questa sezione due importanti risultati. Il primo consiste nel fatto che ogni curva algebrica proiettiva complessa non singolare e irriducibile è topologicamente equivalente a una superficie compatta orientabile, e quindi è classificabile tramite il suo genere. Inoltre, si ha che è possibile definire il genere di una curva algebrica non singolare a partire dal grado del polinimio che la definisce.

Lemma 1.3.1. ([3]). *Ogni curva algebrica $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ è compatta.*

Lemma 1.3.2. ([3]). *Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ irriducibile e sia $\{P_i\}$ l'insieme dei punti singolari di $\mathcal{C}$. Allora $\mathcal{C} \setminus \{P_i\}$ è una superficie orientabile.*

Corollario 1.3.3. *Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ non singolare, allora è orientabile.*

Segue quindi il primo risultato:

Teorema 1.3.4. ([3]). *Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ una curva algebrica irriducibile, non singolare. Allora $\mathcal{C}$ è topologicamente equivalente a una superficie compatta orientabile.*

Infine, forniamo il seguente teorema che ci permette di calcolare il genere di una curva.

Teorema 1.3.5. ([3]). *Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ una curva algebrica irriducibile, non singolare definita dal polinomio omogeneo $F(x_0, x_1, x_2) \subset \mathbb{C}[x_0, x_1, x_2]$. Se $deg(F) = n$, allora il genere g di $\mathcal{C}$ è*

$$g = \frac{(n-1)(n-2)}{2}.$$

Capitolo 2

Curve Ellittiche

Ci dedicheremo, in questo secondo capitolo, allo studio delle curve ellittiche, principale oggetto d'interesse di questa tesi. In particolare, dopo averne fornito la definizione e mostrato alcune proprietà nella prima sezione, vedremo che è sempre possibile trovare un'equazione affine espressa in forma normale per una generica curva ellittica $\mathcal{C}$, e che, fissato un punto $O \in \mathcal{C}$, si può dotare l'insieme dei punti della curva della struttura di gruppo abeliano in modo che O sia l'elemento neutro.

2.1 Cubiche

Diamo la definizione di curva ellittica:

Definizione 2.1. Una *curva ellittica* è una curva algebrica proiettiva liscia di genere 1, su cui viene specificato un punto O.

Si ha quindi che, per quanto visto nel capitolo precedente, una curva ellittica definita sul campo complesso è topologicamente equivalente ad un toro puntato (cioè sul quale viene fissato un punto speciale O).

Ci limiteremo ora a studiare le cubiche lisce in $\mathbb{P}^2(\mathbb{C})$, cioè le curve algebriche definite sul piano proiettivo complesso descritte da un'equazione di grado 3 senza punti singolari.

Infatti, ogni curva ellittica può essere scritta come il luogo degli zeri di un'equazione cubica in $\mathbb{P}^2(\mathbb{C})$, con un solo punto sulla retta all'infinito. Per la dimostrazione si veda [4], ch.III§3, prop.3.1.

Forniamo di seguito alcuni risultati che ci serviranno per dedurre proprietà delle cubiche di grande interesse.

Definizione 2.2. Siano r e $\mathcal{C}$ una retta e una curva di $\mathbb{P}^2(\mathbb{C})$,

$$r : \lambda P + \mu Q, \quad P, Q \in \mathbb{P}^2(\mathbb{C}) \text{ fissati}, \quad \lambda, \mu \in \mathbb{C},$$

$$\mathcal{C} \longleftrightarrow F \in \mathbb{C}\left[x_0, x_1, x_2\right]_d .$$

Diremo che r e $\mathcal{C}$ hanno *molteplicità di intersezione* $I(\mathcal{C}, r, P_0)$ nel punto $P_0 = \lambda_0 P + \mu_0 Q \in r$, se $(\lambda_0, \mu_0) \in \mathbb{P}^1(\mathbb{C})$ è una radice di molteplicità $I(\mathcal{C}, r, P_0)$ del polinomio $F(\lambda P + \mu Q)$, ponendo $I(\mathcal{C}, r, P_0) = 0$ se $P_0 \notin \mathcal{C} \cap r$, e $I(\mathcal{C}, r, P_0) = \infty$ se $r \subset \mathcal{C}$.

Teorema 2.1.1. *Sia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ una curva algebrica, $\mathcal{C} \longleftrightarrow F \in \mathbb{C}\left[x_0, x_1, x_2\right]_d$. Allora ogni retta $r \subset \mathbb{P}^2(\mathbb{C})$ o è una componente di $\mathcal{C}$, o $\sum_{P_0 \in r} I(\mathcal{C}, r, P_0) = d$, ossia r incontra $\mathcal{C}$ in d punti, contati con le loro molteplicità.*

Dimostrazione. Siano r e $\mathcal{C}$ date dalle seguenti equazioni

$$r : \begin{cases} x_0 = \alpha_0 \lambda + \beta_0 \mu \\ x_1 = \alpha_1 \lambda + \beta_1 \mu \\ x_2 = \alpha_2 \lambda + \beta_2 \mu \end{cases} \qquad \mathcal{C} : \ F(x_0, x_1, x_2) = 0.$$

Consideriamo $F(x_0(\lambda, \mu), x_1(\lambda, \mu), x_2(\lambda, \mu)) = 0$, $F(\lambda, \mu) \in \mathbb{C}\left[\lambda, \mu\right]$, ossia il polinomio i cui zeri corrispondono ai punti di intersezione di r e $\mathcal{C}$. Possono verificarsi due casi:

1. $F(\lambda, \mu) = 0$, $\forall \lambda, \mu$. Allora $P \in r \Rightarrow P \in \mathcal{C}$. Ponendo, in un opportuno sistema di coordinate, $r = \{x_0 = 0\}$, si ha che $F(0, x_1, x_2) = 0$. Segue quindi che $x_0 \mid F \Rightarrow F = x_0 F_1 \Rightarrow r$ è componente di $\mathcal{C}$;

2. $F(\lambda,\mu) \neq 0$, $F(\lambda,\mu) \in \mathbb{C}[\lambda,\mu]_d$. Allora F ha esattamente d radici contate con molteplicità, cioè $F(\lambda,\mu) = \prod_{i=1}^{d}(a_i\lambda + b_i\mu) \Rightarrow \forall\, P_i = (b_i, -a_i) \in \mathbb{P}^1(\mathbb{C})$, P_i annulla $F(\lambda,\mu)$. Ponendo $Q_i = (x_0(b_i,-a_i), x_1(b_i,-a_i), x_2(b_i,-a_i)) \in \mathcal{C}$ ottengo proprio d punti della retta. □

Proposizione 2.1.2. *Una cubica liscia è irriducibile.*

Dimostrazione. Consideriamo una cubica liscia $\mathcal{C} : F(x_0,x_1,x_2) = 0$, $deg(F) = 3$. Supponiamo che $\mathcal{C}$ sia riducibile, allora F si spezza come prodotto di polinomi di grado inferiore e distinguiamo i seguenti casi:

1. $F = F_1 \cdot F_2$, $degF_1 = 1$, $degF_2 = 2$, ossia $\mathcal{C}$ si scompone in una retta $r : F_1 = 0$ e una conica $\mathcal{C}_1 : F_2 = 0$. In particolare, applicando il teorema appena dimostrato, si hanno i seguenti sottocasi:

   a. $r \cap \mathcal{C}_1 = \{P_0\}$;

   b. $r \cap \mathcal{C}_1 = \{P_1, P_2\}$;

2. $F = G_1 \cdot G_2 \cdot G_3$, $degG_i = 1$, $i = 1,2,3$, ossia $\mathcal{C}$ è il prodotto di tre rette $r_i : G_i = 0$, $i = 1,2,3$.

   a. $r_1 \cap r_2 \cap r_3 = Q_0$;

   b. $r_1 \cap r_2 = Q_1$, $r_2 \cap r_3 = Q_2$, $r_1 \cap r_3 = Q_3$, Q_i distinti, $i = 1,2,3$;

   c. $r_1 = r_2 \neq r_3$;

   d. $r_1 = r_2 = r_3$.

In ognuno dei casi analizzati si verifica che $\mathcal{C}$ contiene almeno un punto singolare, ma questo è assurdo, essendo $\mathcal{C}$ una cubica liscia. Si ha quindi che una cubica liscia è irriducibile. □

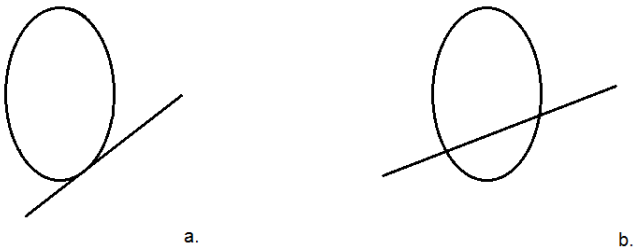


Figura 2.1: Esempi dei casi 1.a e 1.b.

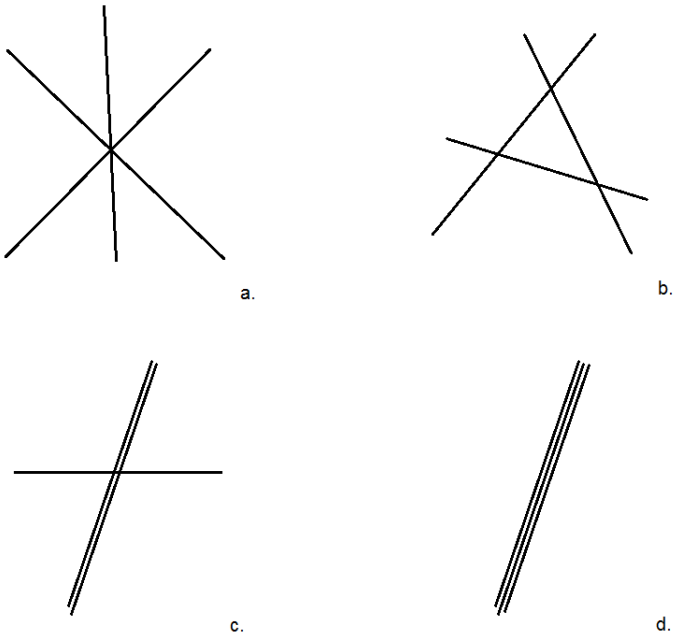


Figura 2.2: Esempi dei casi 2.a, 2.b, 2.c e 2.d.

2.2 Forma normale di una cubica

Vediamo in questa sezione che è possibile ottenere un'equazione affine per $\mathcal{C}$ che ci permetta di studiare la curva in maniera efficiente, espressa in forma normale, ossia del tipo

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx + c,\ a, b, c \in \mathbb{C}.$$

Per dimostrare ciò, ci serve innanzitutto introdurre il concetto di $flesso$ di una cubica e mostrarne alcune proprietà.

Definizione 2.3. Un punto semplice P di una curva affine o proiettiva $\mathcal{C}$ è un $flesso$ se $I(\mathcal{C}, \tau, P) \geq 3$, dove τ è la tangente a $\mathcal{C}$ in P. Un $flesso$ si dice *di specie* k (≥ 1) se $I(\mathcal{C}, \tau, P) = k + 2$. Un $flesso$ di specie $k = 1$ (risp. $k \geq 2$) si dice *ordinario* (*non ordinario*).

Una retta r è una curva non singolare che coincide con la sua tangente in ogni suo punto. Quindi $I(r, r, P) = \infty$, $\forall P \in r$, cioè ogni suo punto è un punto di flesso. Segue dal Teorema 2.1.1 che una conica irriducibile non può avere punti di flesso, e che una cubica liscia (quindi irriducibile per la Proposizione 2.1.2) può avere invece solo flessi ordinari.
Ci limitiamo ora ad enunciare il seguente teorema.

Teorema 2.2.1. ([5]).
Una curva non singolare di grado ≥ 3 *ha almeno un flesso.*

Possiamo quindi dimostrare il teorema principale di questa sezione:

Teorema 2.2.2. *Ogni cubica non singolare* $\mathcal{C} \subset \mathbb{P}^2(= \mathbb{P}^2(\mathbb{C}))$ *è proiettivamente equivalente ad una cubica di equazione affine*

$$y^2 = g(x), \tag{2.1}$$

dove $g(x)$ *è un polinomio di grado 3, avente radici distinte.*

Dimostrazione. Dal Teorema 2.2.1, $\mathcal{C}$ ha almeno un flesso P. Applicando un'opportuna proiettività, si può supporre che:

a) $P = [0, 0, 1]$;

b) la tangente inflessionale in P sia $r : x_0 = 0$.

Rappresento $\mathcal{C}$ con un generico polinomio omogeneo di grado 3: $F(x_0, x_1, x_2) = 0$, $F \in \mathbb{C}[x_0, x_1, x_2]_3$:

$$F(x_0, x_1, x_2) = ax_0^3 + bx_1^3 + cx_2^3 + d{x_0}^2x_1 + e{x_0}^2x_2 + fx_0x_1^2 + gx_0x_2^2 + h{x_1}^2x_2 + i{x_1}{x_2}^2 + lx_0x_1x_2,$$

disomogeinizzo rispetto una delle carte affini, ad esempio $U_2 = \{x_2 \neq 0\}$, con coordinate affini $x = \frac{x_0}{x_2}$, $y = \frac{x_1}{x_2}$; avremo:

$$f(x, y) = ax^3 + by^3 + c + dx^2y + ex^2 + fxy^2 + gx + hy^2 + iy + lxy,$$

imponiamo poi le condizioni a) e b), tradotte nel piano affine:

a) $P = (0, 0) \in \mathcal{C} \rightarrow f(0, 0) = 0 \Rightarrow c = 0$;

b) $r : x = 0$ tangente inflessionale in P:

$$\frac{\partial f}{\partial y}(0, 0) = 0 \Rightarrow\ i = 0$$

,

$$\frac{\partial f}{\partial x}(0, 0) \neq 0 \Rightarrow\ g \neq 0$$

(altrimenti P sarebbe punto singolare).

Inoltre, sapendo che P è punto di flesso, $I(\mathcal{C}, r, P) = 3 \Rightarrow h = 0$. Si ha quindi:

$$F(x_0, x_1, x_2) = ax_0^3 + bx_1^3 + dx_0{}^2x_1 + ex_0{}^2x_2 + fx_0x_1^2 + gx_0x_2^2 + lx_0x_1x_2,$$

e disomogeneizzando ora in $U_0 = \{x_0 \neq 0\}$, $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$:

$$f'(x, y) = a + bx^3 + c + dx + ey + fx^2 + gy^2 + lxy.$$

Quindi in coordinate affini $\mathcal{C}$ avrà equazione

$$x^3 + \phi(x, y) = 0, \tag{2.2}$$

dove ϕ è di grado due, ed ha un termine gy^2, $g \neq 0$. Quindi, risolvendo (2.2) rispetto a y, otteniamo

$$y = \alpha x + \beta \pm \sqrt{g(x)}, \tag{2.3}$$

dove $g(x)$ è un polinomio in x di grado 3. Applicando la seguente sostituzione: $\bar{y} = y - \alpha x - \beta$, $\bar{x} = x$, si trasforma l'equazione (2.3) in (2.1). Infine, se $g(x)$

avesse una radice multipla x^*, un ulteriore sostituzione del tipo: $\bar{\bar{y}} = \bar{y}$, $\bar{\bar{x}} = \bar{x} - x^*$ trasformerebbe l'equazione nella forma

$$\bar{\bar{y}}^2 = \bar{\bar{x}}^2(\gamma\bar{\bar{x}} - \delta),$$

e quindi la curva avrebbe un punto singolare nell'origine. Segue quindi la tesi. □

Osservazione 2. Segue dal teorema appena dimostrato che ogni cubica liscia $\mathcal{C}$ nel piano proiettivo complesso è definita da un'equazione affine del tipo $\mathcal{C} : y^2 = g(x)$, $g(x)$ un polinomio di grado 3, avente radici distinte, cioè $g(x) = a(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, $a \neq 0$, $\alpha_i \in \mathbb{C}$, $i, j = 1, 2, 3$ e $\alpha_i \neq \alpha_j$, $i \neq j$. Applicando l'affinità corrispondente alla seguente sostituzione:

$$x = (\alpha_2 - \alpha_1)\bar{x} + \alpha_1$$

$$y = \sqrt{a(\alpha_2 - \alpha_1)^3}\bar{y}$$

si trasforma l'equazione (2.1) nella forma

$$y^2 = x(x-1)(x-c), \tag{2.4}$$

con $c \in \mathbb{C}\setminus\{0, 1\}$, più precisamente $c = (\alpha_3 - \alpha_1)/(\alpha_2 - \alpha_1)$.

Osservazione 3. Mostriamo che attraverso una semplice sostituzione, è inoltre possibile considerare un'equazione della cubica nella forma (2.1) dove il coefficiente di x^2 vale 0. Siano r_1, r_2, r_3 le tre radici distinte di $g(x) = x^3 + ax^2 + bx + c$.
Vediamo che $r_1+r_2+r_3 = -a$: dall'osservazione precedente, possiamo scrivere $g(x) = (x - r_1)(x - r_2)(x - r_3)$, sviluppando i prodotti, otteniamo

$$g(x) = x^3 - r_1x^2 - r_2x^2 - r_3x^2 + xr_1r_2 + xr_1r_3 + xr_2r_3 - r_1r_2r_3$$

segue banalmente che $r_1 + r_2 + r_3 = -a$. Applicando ora la sostituzione:$x = x_1 - a/3$, avremo:

$$x^3 + ax^2 + bx + c = {x_1}^3 + b'x_1 + c',$$

dove $b' = b - (1/3)a^2$, $c' = c - (l/3)ab + (2/27)a^3$; cioè

$$y^2 = x^3 + ax + b. \tag{2.5}$$

Questa si chiama *equazione di Weierstrass*.

Vediamo ora alcuni esempi di cubiche lisce e le rispettive equazioni di Weierstrass affini:

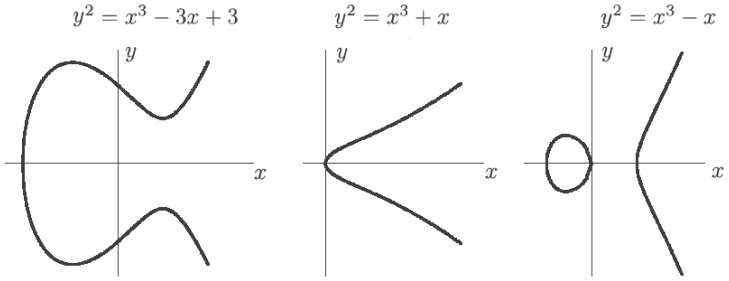


Figura 2.3: Esempi di tre cubiche nel piano affine e rispettive equazioni affini.

2.3 Legge di gruppo su una cubica

Tratteremo, in questa sezione del capitolo, un'altra proprietà fondamentale delle cubiche lisce $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ che consiste nella possibilità di definire sull'insieme dei punti della cubica $\mathcal{C}$ un'operazione $+$ in modo tale che $(\mathcal{C}, +)$ sia un gruppo abeliano.

Data una generica cubica liscia $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$, ne consideriamo la parte affine, ad esempio nella carta $U_0 = \{x_0 \neq 0\}$, e poniamo $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$. Per il Teorema 2.2.2 della sezione precedente, avremo:

$$\mathcal{C} : \ f(x, y) = 0, \ f(x, y) = y^2 - g(x),$$

dove $g(x) = ax^3 + bx^2 + cx + d$, $a, b, c, d \in \mathbb{C}$ t.c $g(x)$ abbia tre radici distinte. Omogeneizziamo il polinomio $f(x, y)$ in $F(x_0, x_1, x_2) \in \mathbb{C}[x_0, x_1, x_2]_3$:

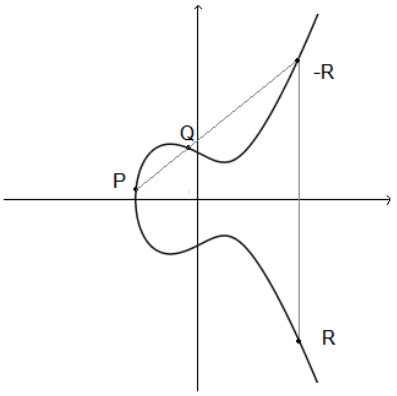
$$F(x_0, x_1, x_2) = x_0^3 \left[\left(\frac{x_2}{x_0} \right)^2 - a \left(\frac{x_1}{x_0} \right)^3 - b \left(\frac{x_1}{x_0} \right)^2 - c \left(\frac{x_1}{x_0} \right) - d \right].$$

Cioè:

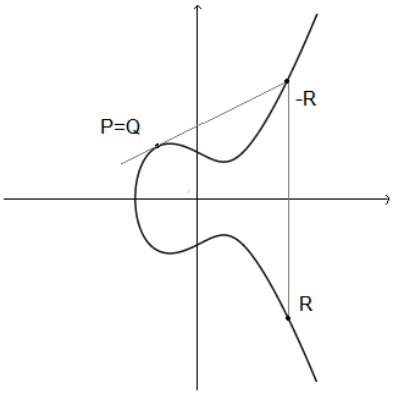
$$F(x_0, x_1, x_2) = x_2^2 x_0 - a x_1 - b {x_1}^2 x_0 - c x_1 {x_0}^2 - d x_0^3.$$

Cerco quindi i punti all'infinito della cubica ponendo $x_0 = 0$ e trovo un unico punto $O = [0, 0, 1]$, che è anche punto di flesso, per quanto visto nella dimostrazione del Teorema 2.2.2. Più precisamente, il punto all'infinito O, così definito, corrisponde al punto 'speciale' della curva ellittica, ossia all'elemento neutro del gruppo formato dall'insieme dei punti della curva stessa, dotato dell'operazione + che ora definiremo.

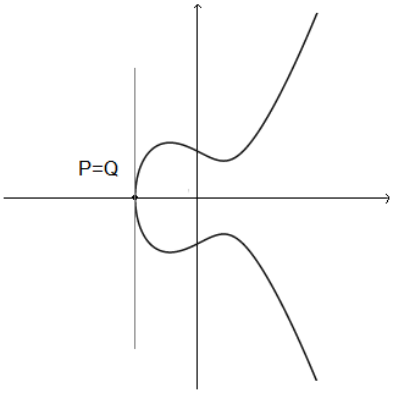
Geometricamente, definiamo l'operazione + come segue:



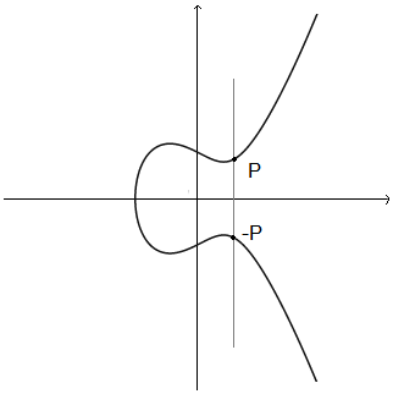
Se $P \neq Q$, allora $P + Q = R$, dove $-R$ è il terzo punto di intersezione tra $\mathcal{C}$ e la retta per P e Q, ed R è il suo opposto, cioè il terzo punto di intersezione tra $\mathcal{C}$ e la retta per $-R$ e O.



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



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



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

In forma analitica, si ha che: dati $P, Q \in \mathcal{C}$, dove $\mathcal{C}$ si suppone espressa nella forma (2.5), $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P + Q = (x_3, y_3)$,

$$x_3 = \lambda^2 - (x_1 + x_2),$$

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

Dove

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2; \\ \frac{3x_1^2 + a}{2y_1}, & P = Q,\ y_1 \neq 0. \end{cases}$$

con $a \in \mathbb{C}$, coefficiente del termine di grado 1 del polinomio $g(x)$.
Se invece $x_1 = x_2$, $y_1 \neq y_2$ oppure $P = Q$, $y_1 = 0$, allora $P + Q = O$.

Data una curva ellittica $\mathcal{C}$, definendo su di essa l'operazione $+$ come sopra, si verifica facilmente il seguente risultato:

Proposizione 2.3.1. *$(\mathcal{C}, +)$ è un gruppo abeliano, cioè:*

1. *$\mathcal{C}$ è chiuso rispetto al $+$;*
2. *$+$ è commutativa;*
3. *$+$ è associativa;*
4. *O è l'elemento neutro.*

Capitolo 3

Classificazione delle cubiche lisce

Abbiamo visto nel primo capitolo che le curve algebriche si possono classificare in base al genere: dalla definizione data di curva ellittica nel capitolo precedente, sappiamo che le cubiche lisce proiettive complesse hanno genere 1, cioè sono topologicamente equivalenti al toro. Tratteremo ora la questione della classificazione delle cubiche lisce in $\mathbb{P}^2(\mathbb{C})$. In particolare, nella prima sezione introdurremo un invariante per trasformazioni proiettive detto *modulo della cubica*, su cui si basa la classificazione, che invece affronteremo nell'ultima sezione.

3.1 Il modulo della cubica

Introduciamo innanzitutto il concetto di *birapporto* di 4 punti su un retta proiettiva.

Definizione 3.1. Sia $\mathbb{P}(=\mathbb{P}^1(\mathbb{C}))$ una retta proiettiva e siano $P_1, P_2, P_3, P_4 \in \mathbb{P}$, con P_1, P_2, P_3 distinti. Il *birapporto* di P_1, P_2, P_3, P_4 è

$$\beta(P_1, P_2, P_3, P_4) = \frac{y_1}{y_0} \in \mathbb{C} \cup \{\infty\},$$

dove y_0, y_1 sono le coordinate omogenee di P_4 nel riferimento proiettivo in cui P_1 e P_2 sono i punti fondamentali e P_3 è il punto unità.

Cerchiamo ora un'espressione esplicita per calcolarlo.
Supponiamo che in $\mathbb{P}$ sia assegnato un riferimento proiettivo rispetto al quale i 4 punti siano $P_i = [\lambda_i, \mu_i]$, $i = 1, 2, 3, 4$. Consideriamo ora il riferimento proiettivo $[P_1, P_2, P_3]$quindi:

$$P_3 = \begin{pmatrix} \lambda_3 \\ \mu_3 \end{pmatrix} = \alpha \begin{pmatrix} \lambda_1 \\ \mu_1 \end{pmatrix} + \beta \begin{pmatrix} \lambda_2 \\ \mu_2 \end{pmatrix}, \quad \alpha, \beta \in \mathbb{C}.$$

E, in particolare:

$$P_4 = \begin{pmatrix} \lambda_4 \\ \mu_4 \end{pmatrix} = \gamma \begin{pmatrix} \alpha\lambda_1 \\ \alpha\mu_1 \end{pmatrix} + \delta \begin{pmatrix} \beta\lambda_2 \\ \beta\mu_2 \end{pmatrix}, \quad \gamma, \delta \in \mathbb{C}.$$

Per definizione,

$$\beta(P_1, P_2, P_3, P_4) = \frac{\delta}{\gamma}.$$

Calcolando $\alpha, \beta, \gamma, \delta$ con la regola di Cramer ed eliminando i denominatori otteniamo:

$$\gamma = \begin{vmatrix} \lambda_2 & \lambda_4 \\ \mu_2 & \mu_4 \end{vmatrix} \begin{vmatrix} \lambda_1 & \lambda_3 \\ \mu_1 & \mu_3 \end{vmatrix},$$

$$\delta = \begin{vmatrix} \lambda_1 & \lambda_4 \\ \mu_1 & \mu_4 \end{vmatrix} \begin{vmatrix} \lambda_2 & \lambda_3 \\ \mu_2 & \mu_3 \end{vmatrix},$$

e di conseguenza:

$$\beta(P_1, P_2, P_3, P_4) = \frac{\begin{vmatrix} \lambda_1 & \lambda_4 \\ \mu_1 & \mu_4 \end{vmatrix} \begin{vmatrix} \lambda_2 & \lambda_3 \\ \mu_2 & \mu_3 \end{vmatrix}}{\begin{vmatrix} \lambda_2 & \lambda_4 \\ \mu_2 & \mu_4 \end{vmatrix} \begin{vmatrix} \lambda_1 & \lambda_3 \\ \mu_1 & \mu_3 \end{vmatrix}}. \tag{3.1}$$

Considerando invece le coordinate non omogenee $z_i = \mu_i/\lambda_i$ dei punti P_i, si deduce da (3.1) la seguente espressione:

$$\beta(P_1, P_2, P_3, P_4) = \frac{(z_4 - z_1)(z_3 - z_2)}{(z_4 - z_2)(z_3 - z_1)}.$$

Teorema 3.1.1. ([6]) *Siano $\mathbb{P}$ e $\mathbb{P}'$ rette proiettive, e siano $P_1, P_2, P_3, P_4 \in \mathbb{P}$, $Q_1, Q_2, Q_3, Q_4 \in \mathbb{P}'$, con P_1, P_2, P_3 distinti e Q_1, Q_2, Q_3 distinti. Esiste un isomorfismo $f : \mathbb{P} \to \mathbb{P}'$ tale che $f(P_i) = Q_i$, $i = 1, 2, 3, 4$ se e solo se*

$$\beta(P_1, P_2, P_3, P_4) = \beta(Q_1, Q_2, Q_3, Q_4).$$

Il birapporto di quattro punti di una retta proiettiva $\mathbb{P}$ dipende dall'ordine in cui vengono considerati: se $P_1, P_2, P_3, P_4 \in \mathbb{P}$ sono distinti, il birapporto di una qualsiasi pemutazione è definito, e ponendo $\beta = \beta(P_1, P_2, P_3, P_4)$ si possono ottenere al più 6 birapporti distinti dai 24 possibili ottenuti permutando i 4 punti, e sono:

$$\beta, \qquad 1/\beta, \qquad 1-\beta, \qquad 1/(1-\beta), \qquad (\beta-1)/\beta, \qquad \beta/(\beta-1).$$

Dunque, ad una quaterna di punti distinti in $\mathbb{P}$ non è associato un solo valore del birapporto.

Da qui nasce la necessità di introdurre una nuova grandezza definita a partire dal birapporto, che sia invariante per permutazioni:

Lemma 3.1.2. ([6]) *Si consideri la funzione razionale*

$$j(\beta) = \frac{(\beta^2 - \beta + 1)^3}{\beta^2(\beta-1)^2},$$

definita per ogni $\beta \in \mathbb{C}\setminus\{0,1\}$. Si ha $j(\beta) = j(\beta')$, $\beta, \beta' \in \mathbb{C}\setminus\{0,1\}$, se e solo se $\beta' \in \{\beta, 1/\beta, 1-\beta, 1/(1-\beta), (\beta-1)/\beta, \beta/(\beta-1)\}$.

Si ha come conseguenza del lemma che, se β è il birapporto di 4 punti distinti su una retta proiettiva, allora $j(\beta)$ non dipende dall'ordine con cui vengono scelti i punti. Segue perciò che per ogni quaterna non ordinata di punti distinti $\{P_1, P_2, P_3, P_4\}$, $j(P_1, P_2, P_3, P_4) = j(\beta(P_1, P_2, P_3, P_4))$ è ben definito e si chiama *modulo della quaterna* $\{P_1, P_2, P_3, P_4\}$.

Teorema 3.1.3. ([6]) *Due quaterne non ordinate di punti distinti $\{P_1, P_2, P_3, P_4\}$, $\{Q_1, Q_2, Q_3, Q_4\}$ di una retta proiettiva $\mathbb{P}$ sono proiettivamente equivalenti se e solo se*

$$j(P_1, P_2, P_3, P_4) = j(Q_1, Q_2, Q_3, Q_4).$$

Osservazione 4. La definizione di modulo di una quaterna di punti si può applicare al caso di una quaterna di rette nel piano proiettivo $\mathbb{P}^2$: considero $\mathcal{F}$, un fascio di rette proiettive passanti per un punto $P = [a_0, a_1, a_2]$; $\mathcal{F}$ è identificabile con una retta r non passante per P: $r \cong \mathbb{P}^1$ tramite, ad esempio, la proiettività che ad ogni retta s del fascio associa il punto di intersezione tra r e s. Quindi è ben definito il modulo di quattro rette del fascio $\mathcal{F}$ e corrisponde al modulo della quaterna composta dai punti di intersezione tra ciascuna retta con la retta che identifica il fascio.

Tornando alle cubiche non singolari, vale il seguente risultato:

Teorema 3.1.4. (Salmon) *Sia $\mathcal{C}$ una cubica non singolare di $\mathbb{P}^2(\mathbb{C})$ e sia P un suo flesso. $\mathcal{C}$ possiede esattamente quattro tangenti distinte che contengono P, inclusa la tangente in P. Il loro modulo è indipendente dalla scelta di P.*

Dimostrazione. Se $\mathcal{C}$ è nella forma (2.4): $y^2 = x(x-1)(x-c)$, per qualche $c \neq 0, 1$, e $P = [0, 0, 1]$ come nel Teorema 2.2.2, allora $\mathcal{C}$ possiede quattro tangenti distinte per P: le rette $y = 0$, $y = 1$, $y = c$ e la retta impropria. Sia ora $\mathcal{C}$ una cubica non singolare qualsiasi. Considero $f : \mathbb{P}^2 \to \mathbb{P}^2$ una proiettività che trasforma $\mathcal{C}$ in una cubica nella forma (2.4), in modo tale che $f(P) = [0, 0, 1]$. Poichè le tangenti a $\mathcal{C}$ passanti per P corrispondono biunivocamente alle tangenti a $f(\mathcal{C})$ per $f(P)$, la prima parte del teorema è dimostrata. Per dimostrare anche la seconda parte, basta applicare il Teorema 3.1.1: il birapporto delle 4 tangenti in P è lo stesso delle loro trasformate, prese nello stesso ordine, perchè f induce un isomorfismo dei due fasci di rette P e $[0, 0, 1]$ rispettivamente. □

Possiamo ora dare la seguente definizione:

Definizione 3.2. Il modulo comune delle quaterne di tangenti passanti per i flessi di una cubica non singolare $\mathcal{C}$ di $\mathbb{P}^2(\mathbb{C})$ si chiama *modulo della cubica*, e si indica con $j(\mathcal{C})$.

Se la cubica $\mathcal{C}$ ha equazione (2.4), allora

$\beta(0, \infty, 1, c) = c$.

Poichè le rette del fascio di rette di centro $P = [0, 0, 1]$ sono associate al loro punto di intersezione con la retta $r : x_2 = 0$ ($P \notin r$) attraverso un isomorfismo di rette proiettive, segue che c è anche il birapporto delle quattro corrispondenti rette tangenti a $\mathcal{C}$ e passanti per P (sono rispettivamente le rette: $y = 0$, la retta impropria, $y = 1$, $y = c$):

$$j(\mathcal{C}) = j(c) = \frac{(c^2 - c + 1)^3}{c^2(c-1)^2}. \tag{3.2}$$

ne individua la classe di equivalenza proiettiva.

3.2 Classificazione delle cubiche lisce in base al modulo

Nella sezione precedente abbiamo visto che ad ogni cubica non singolare $\mathcal{C}$ è associato un valore $j(\mathcal{C}) \in \mathbb{C}$, detto il modulo della cubica. Abbiamo inoltre definito una relazione di equivalenza proiettiva per una quaterna di punti su una retta proiettiva in base al modulo della quaterna (vedi Teorema 3.1.3), e possiamo ora estenderla al caso di una cubica liscia. Il modulo della cubica ne individua infatti la classe di equivalenza rispetto ad una relazione di equivalenza proiettiva definita come nel seguente corollario del Teorema di Salmon (Teorema 3.1.4):

Corollario 3.2.1. *Due cubiche non singolari $\mathcal{C}$ e $\mathcal{C}'$ di $\mathbb{P}^2(\mathbb{C})$ sono proiettivamente equivalenti se e solo se $j(\mathcal{C}) = j(\mathcal{C}')$.*

Dimostrazione. $\Rightarrow$: Se $\mathcal{C}$ e $\mathcal{C}'$ sono proiettivamente equivalenti, allora entrambe sono equivalenti ad una stessa cubica nella forma (2.4), quindi:

$$j(\mathcal{C}) = j(\mathcal{C}') = j(c),$$

con $j(c)$ come in (3.2).

$\Leftarrow$: Viceversa, supponiamo che $\mathcal{C}$ e $\mathcal{C}'$ abbiano equazione nella forma (2.4):

$$\mathcal{C} : y^2 = x(x-1)(x-c), \tag{3.3}$$

$$\mathcal{C}' : y^2 = x(x-1)(x-c'), \tag{3.4}$$

con $j(c) = j(c')$. Se $c \neq c'$, allora, per il Lemma 3.1.2, c' è necessariamente equivalente ad una delle seguenti espressioni in c :

$$\frac{1}{c}, \quad 1-c, \quad \frac{1}{1-c}, \quad \frac{c}{c-1}, \quad \frac{c-1}{c}.$$

Basterà quindi determinare una proiettività che trasformi (3.3) in (3.4) nei due casi:

a) $c' = \frac{1}{c}$,
la proiettività corrisponde alla seguente sostituzione:

$$x = c\bar{x},$$

$$y = c^{3/2}\bar{y};$$

b) $c' = 1 - c$,
la proiettività corrisponde alla seguente sostituzione:

$$x = -\bar{x} + 1,$$

$$y = i\bar{y}.$$

Negli altri casi le proiettività si otterranno componendo opportunamente queste due. □

Data la relazione di equivalenza proiettiva:

$$\mathcal{C} \sim \mathcal{C}' \Leftrightarrow j(\mathcal{C}) = j(\mathcal{C}'),$$

definiamo

$$\mathcal{M} = \left\{ [\mathcal{C}]_{\sim}, \mathcal{C} \text{ cubica liscia } \in \mathbb{P}^2(\mathbb{C}) \right\},$$

cioè l'insieme delle classi di equivalenza proiettiva rispetto $\sim$, definita come sopra.

Osservazione 5. Il corollario 3.2.1 stabilisce una corrispondenza biunivoca tra $\mathcal{M}$ e l'insieme $\mathcal{J} = \{j(c), c \in \mathbb{C}\setminus\{0,1\}\} \subset \mathbb{C}$, Dove ciascun $j(c)$ proviene al più da sei valori distinti di c. Essendo $\mathbb{C}$ infinito, segue quindi che anche $\mathcal{M}$ è infinito.

Capitolo 4

Crittografia ellittica

In questo capitolo presenteremo il grande vantaggio che comporta l'utilizzo delle curve ellittiche in crittografia. Ciò si basa sul fatto che defininendo un sistema crittografico sulla struttura di gruppo abeliano dei punti di una curva ellittica, definita come nel capitolo 2.3, si ottiene un livello di sicurezza paragonabile ai classici sistemi crittografici a chiave pubblica, che richiedono chiavi pubbliche di dimensione maggiore e quindi meno facilmente utilizzabili. La Crittografia a chiave pubblica che si basa sulle curve ellittiche definiti su campi diniti si dice *Crittografia ellittica* (*ECC*).

4.1 Curve ellittiche su campi finiti

Innanzitutto, analizziamo in questa prima sezione la struttura che le curve ellittiche assumono se definite su campi finiti.

Sia ora $K = \mathbb{F}_q$ campo finito con $q = p^r$ elementi e sia $\mathcal{E}$ una curva ellittica definita su $\mathbb{F}_q$. D'ora in avanti considereremo solo campi finiti di caratteristica maggiore di 3, possiamo quindi supporre che $\mathcal{E}$ sia espressa da un'equazione di Weierstrass (2.2), ossia $\mathcal{E} : y^2 = x^3 + ax + b$ (vedi oss.4, cap.2).
$\mathcal{E}$ può avere al più $2q + 1$ punti in $\mathbb{F}_q$, ovvero il punto all'infinito e $2q$ coppie

(x, y), $x, y \in \mathbb{F}_q$ che soddisfano (2.2): per ogni valore di x possono esistere al massimo due valori di y che soddifano (2.2). Tuttavia, poichè solo metà degli elementi di $\mathbb{F}_q^*$ ha radici quadrate, possiamo supporre che $x^3 + ax + b$ sia un quadrato solo metà delle volte rispetto a quelle ipotizzate in precedenza. Quando è un quadrato, otteniamo due possibili radici quadrate: $-y$, y. Quindi, possiamo dedurre che, approssimativamente, i punti di $\mathcal{E}$ in $\mathbb{F}_q$ sono circa $q + 1$.

Più precisamente, vale la seguente stima

Teorema 4.1.1. (Hasse) *Sia N il numero di punti di una curva ellittica $\mathcal{E}$ definita su $\mathbb{F}_q$. Allora*

$$|N - (q + 1)| \leq 2\sqrt{q}$$

Per la dimostrazione si veda [4], ch.V§1.

Esempio 4.1. Consideriamo $\mathbb{F}_q = \mathbb{Z}_5$ $(p = 5, r = 1)$ e definiamo su di esso la seguente curva ellittica:

$$\mathcal{E} : y^2 \equiv x^3 + 2x + 3 \,(\text{mod}5)$$

e ne contiamo i punti. I possibili valori per x mod 5 sono $0, 1, 2, 3, 4$. Sostituiamo ognuno di questi valori all'interno dell'equazione e troviamo i possibili valori di y che la risolvono:

1. $x \equiv \infty \Rightarrow y \equiv \infty$;
2. $x \equiv 0 \Rightarrow y^2 \equiv 3 \Rightarrow$ non ci sono soluzioni;
3. $x \equiv 1 \Rightarrow y^2 \equiv 6 \equiv 1 \Rightarrow y \equiv 1, 4\,(mod5)$;
4. $x \equiv 2 \Rightarrow y^2 \equiv 15 \equiv 0 \Rightarrow y \equiv 0\,(mod5)$;
5. $x \equiv 3 \Rightarrow y^2 \equiv 36 \equiv 1 \Rightarrow y \equiv 1, 4\,(mod5)$;
6. $x \equiv 4 \Rightarrow y^2 \equiv 75 \equiv 0 \Rightarrow y \equiv 0\,(mod5)$.

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

Si ha inoltre che, se $\mathcal{E}$ è una curva ellittica definita su $\mathbb{F}_q$, l'analogo del prodotto tra due punti su $\mathbb{F}_q^*$ è la somma di due punti su $\mathcal{E}$; pertanto, l'elevamento alla k-esima potenza di un punto in $\mathbb{F}_q^*$ corrisponde al prodotto di un punto in $\mathcal{E}$ per l'intero k.

4.2 Il problema del logaritmo discreto sulle curve ellittiche

Il problema del logaritmo discreto ha grande rilevanza nei sistemi a chiave pubblica perchè si suppone che questo sia un problema intrattabile: se sui numeri reali, calcolare l'esponenziale (calcolare g^x) con una certa precisione, non è significativamente più facile rispetto all'operazione inversa (calcolare $log_g x$), su alcuni gruppi finiti quest'ultima operazione risulta essere un problema difficile da risolvere. Per questa ragione, molti sistemi a chiave pubblica si basano su questo problema.
Di seguito, dopo aver richiamato il problema del logaritmo discreto, vedremo un possibile attacco ad esso, basto sulla fattorizzazione in numeri primi (se piccoli).

Definizione 4.1. Sia G un gruppo finito, $a, b \in G$ tali che $a^x = b$, x intero. Allora x si dice il *logaritmo discreto* di b in base a e si scrive

$$x = Dlog_a b.$$

Il problema del logaritmo discreto consiste nel trovare tale valore x.

Forniamo ora un possibile tipo di attacco al problema del logaritmo discreto in aritmetica modulare. Consideriamo quindi $\mathbb{Z}_p^*$ e una sua radice primitiva a.
Vogliamo risolvere $b = a^x \, (mod\, p)$.

1. Sia B fissato e siano $p_1, p_2, ..., p_m$ primi minori di B. Questo insieme di primi si dice *base di fattori*. Calcoliamo $a^k (mod\, p)$, al variare di k, e proviamo a scriverlo come prodotto di potenze degli elementi della base di fattori. Se questo non è possibile, si scarta a^k, altrimenti si avrà

$$a^k \equiv \prod_{i=1,..m} p_i^{\alpha_i} (mod\, p),$$

cioè

$$k \equiv \sum_{i=1,..m} \alpha_i Dlog_a p_i (mod\, p-1).$$

Una volta ottenute abbastanza relazioni di questo tipo, possiamo risolvere $Dlog_a p_i$, $\forall i$.

2. Ora, al variare di r intero casuale, calcoliamo $ba^r (mod\, p)$. Proviamo a scrivere ognuno di questi come prodotto di potenze degli elementi della base di fattori e, nel caso di successo, avremo

$$ba^r \equiv \prod_{i=1,..m} p_i^{\beta_i} (mod\, p),$$

cioè

$$Dlog_a b \equiv -r + \sum_{i=1,..m} \beta_i Dlog_a p_i (mod\, p-1).$$

Osserviamo che questo algoritmo è efficiente se p è di dimensioni non troppo elevate. Inoltre, una volta concluso il passo 1, i valori ottenuti si possono riutilizzare per calcolare più logaritmi discreti, per lo stesso primo p.
Bisogna comunque osservare che il problema della fattorizzazione è anch'esso considerato intrattabile.

Un metodo analogo a questo sembra non esistere per le curve ellittiche. Lavorare con le curve ellittiche, invece che con interi mod p, rappresenta quindi un enorme vantaggio: a parità di livello di sicurezza, è possibile usare primi più piccoli, senza incorrere nel rischio che il problema del logaritmo discreto venga risolto, e di conseguenza campi finiti più piccoli. Si presume

infatti che trovare il logaritmo discreto di un elemento di una curva ellittica casuale rispetto a una base nota sia impossibile: questo fa sì che si possano usare chiavi pubbliche molto più corte, ad esempio, a parità di sicurezza, una chiave di 3072 bit in un sistema crittografico classico corrisponde ad una di 256 bit in un sistema crittografico ellittico e questo permette grandi risparmi nella fase di implementazione del sistema.
Definiamo quindi il logaritmo discreto nel caso delle curve ellittiche:

Definizione 4.2. Sia $\mathcal{E}$ una curva ellittica definita su un campo finito $\mathbb{F}_q$, e siano $A, B \in \mathcal{E}$ tali che $xA = B$, x intero. Allora x si dice il *logaritmo discreto* di B in base A.

4.3 Crittosistemi ellittici

Vedremo in questa sezione come si opera nei crittosistemi ellittici: di seguito, descriviamo tre sistemi crittografici definiti su curve ellittiche a partire da classici algoritmi crittografici che si basano sul problema del logaritmo discreto, ossia il protocollo per lo scambio delle chiavi di Diffie-Hellman, ElGamal e la firma digitale di ElGamal.

4.3.1 Scambio delle chiavi di Diffie-Hellman su curve ellittiche

Alice e Bob vogliono scambiarsi una chiave segreta attraverso un canale insicuro.

1. Per prima cosa, si accordano su un punto fisso G su una curva ellittica $\mathcal{E} : y^2 \equiv x^3 + ax + b$ definita su un campo finito $\mathbb{F}_q$, dove $G, \mathcal{E}$ e $\mathbb{F}_q$ sono pubblici;

2. Alice e Bob, scelgono casualmente due valori in $\mathbb{F}_q$: N_A e N_B rispettivamente, che rappresentano la loro chiave privata che non verrà mai condivisa;

3. Calcolano N_AG e N_BG e li pubblicano sul canale insicuro;

4. Alice prende N_BG e calcola $N_A(N_BG)$. Analogamente Bob prende N_AG e calcola $N_B(N_AG)$.

Ora entrambi possiedono una stessa chiave segreta: N_AN_BG. Osserviamo che la sicurezza dello scambio delle chiavi si basa sul problema del logaritmo discreto nella misura in cui, pur conoscendo N_AG e N_BG, non è possibile calcolare le chiavi segrete N_A e N_B di Alice e Bob senza risolvere il problema del logaritmo discreto.

4.3.2 ElGamal su curve ellittiche

Alice vuole mandare un messaggio segreto x a Bob

1. Bob sceglie un campo finito $\mathbb{F}_q$ e una curva ellittica definita su di esso $\mathcal{E}$, pubblici. Sceglie inoltre un punto α in $\mathcal{E}$ e un intero a;

2. Calcola
$$\beta = \alpha a,$$
rende pubblici α e β, mentre mantiene segreto a;

3. Alice esprime il messagio x come un punto su $\mathcal{E}$ (si veda [8]), sceglie un intero k casuale, calcola
$$y_1 = k\alpha \qquad y_2 = x + k\beta,$$
e manda y_1, y_2 a Bob;

4. Bob decifra il messaggio calcolando
$$x = y_2 - ay_1.$$

Anche qui, pur conoscendo y_1, y_2, calcolare x significherebbe risolvere $x = y_2 - ay_1$, cioè $\beta = \alpha a$ e quindi il problema del logaritmo discreto.

4.3.3 Firma digitale di ElGamal su curve ellittiche

Alice vuole firmare un messaggio m (supponiamo che sia un intero).

1. Alice fissa un campo finito $\mathbb{F}_q$, una curva ellittica $\mathcal{E}$ definita su di esso e un punto $A \in \mathcal{E}$. Si suppone inoltre che il numero di punti N di $\mathcal{E}$ sia stato calcolato e $0 \leq m < N$ (altrimenti si sceglie un campo più grande);

2. Alice sceglie un intero segreto a e calcola $B = aA$. Rende poi pubblici $\mathbb{F}_q, \mathcal{E}, N, A, B$;

3. Sceglie un intero k con $1 \leq k < N$ e MCD(k, n)=1, e calcola $R = kA \in \mathcal{E}$. Si può quindi pensare $R = (x, y)$;

4. Calcola $S = k^{-1}(m - ax) \, (mod\, N)$ e manda il messaggio firmato (m, R, S) a Bob.

Bob verifica la firma di Alice

1. Avendo a disposizione $\mathbb{F}_q, \mathcal{E}, N, A, B$ pubblici, Bob calcola $V_1 = xB + SR$ e $V_2 = mA$;

2. il messaggio è autentico se $V_1 = V_2$.

La procedura di verificazione funziona poichè

$$V_1 = xB + SR = xaA + k^{-1}(m - ax)(kA) = xaA + (m - ax)A = mA = V_2.$$

Essendo l'unica a conoscere a, solo Alice può firmare il messaggio, mentre chiunque può verificarne l'autenticità. Anche questo, come negli esempi precedenti, dipende dalla difficoltà di risoluzione del problema del logaritmo discreto.

Bibliografia

[1] Serge Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag New York (1978).

[2] Manfredo P. do Carmo, *Differential Geometry of Curves and Surfaces*, Prentice-Hall (1976).

[3] K. Kendig, *Elementary Algebraic Geometry*, Springer (1977).

[4] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (2009).

[5] Robert J. Walker, *Algebraic Curves*, Springer (1978).

[6] Edoardo Sernesi, *Geometria 1*, Bollati Boringhieri (1989).

[7] Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer (2000).

[8] W. Trappe, L. C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice-Hall (2006).

Ringraziamenti

Desidero ringraziare innnanzitutto il mio Relatore, Prof. Alessandro Gimigliano, per la paziente attenzione e la disponibilità dimostratemi in ogni fase della stesura del presente lavoro. Ringrazio parimenti il Correlatore, Prof. Davide Aliffi, per il tempo dedicatomi per il lavoro finale.

Infine ringrazio la mia famiglia e i miei amici più stretti che mi sono stati vicini.