Alma Mater Studiorum · Università di Bologna

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

FUNZIONI ZETA E FATTORIZZAZIONE UNICA IN ANELLI QUADRATICI DI CURVE SU CAMPI FINITI

Tesi di Laurea in Teoria dei Numeri

Relatore:
Chiar.ma Prof.ssa
Mirella Manaresi

Correlatore:
Chiar.mo Prof.
Umberto Zannier

Presentata da:
Francesca Malagoli

Prima Sessione
Anno Accademico 2011-2012

Introduzione

Nel primo capitolo affronteremo il problema di stabilire il numero dei punti di curve definite su campi finiti, partendo dal caso di rette e coniche, per le quali si può dare un risultato elementare.
Questo problema è stato studiato già nel 1801 da Carl Friedrich Gauss, che nell'Articolo 358 delle *Disquisitiones Arithmeticae* ha determinato il numero di punti della cubica di Fermat $X^3+Y^3+Z^3=0$ su un campo finito $\mathbb{F}_p$, con p primo.
Nella sua tesi del 1924 Emil Artin, lavorando nel contesto delle curve iperellittiche definite su campi finiti, ossia delle curve definite da un'equazione della forma $Y^2 = d(X)$, con $d \in \mathbb{F}_q[X]$, $q = p^\alpha$, p primo, ha introdotto un analogo della funzione zeta di Dedekind. Artin ha inoltre provato che questa può essere trasformata in una funzione razionale tramite un cambio di variabile ed ha congetturato che gli zeri di questa funzione razionale soddisfino un analogo dell'ipotesi di Riemann.
Helmut Hasse nel 1932 ha provato che la congettura di Artin implica che il numero n dei punti di una curva iperellittica definita su un campo finito $\mathbb{F}_q$ soddisfa la disequazione

$$|n - q - 1| \leq 2g\sqrt{q}$$

con g genere della curva. Hasse ha inoltre provato questo risultato nel caso delle curve ellittiche (cioè per $g = 1$).
Nel 1940 André Weil ha provato la congettura di Artin nel caso più generale delle curve non singolari definite su campi finiti, facendo uso di metodi avanzati di geometria algebrica.

Dimostrazioni più elementari sono poi state trovate da Sergei Stepanov, fra il 1969 e il 1974, per casi particolari e, con metodi diversi, da Wolfgang Schmidt e da Enrico Bombieri negli anni '70 per il caso generale. Seguiremo la dimostrazione data da Bombieri.

Per affrontare quest'ultimo tema dovremo usare strumenti di geometria algebrica.
La geometria algebrica è una branca della matematica che studia le varietà algebriche, ossia i luoghi geometrici delle soluzioni di sistemi di equazioni polinomiali. La geometria algebrica, pur basandosi anche su idee precedenti, è nata solo alla fine del XIX° secolo, con la dimostrazione, da parte di David Hilbert, dei teoremi degli zeri e della base. È stata sviluppata inizialmente dalla scuola italiana (Enriques, Chisini, Castelnuovo, Segre) ma il formalismo attuale è stato introdotto solo a partire dagli anni '30, principalmente grazie a Weil.

Nei capitoli successivi passeremo a studiare il numero di classi di ideali degli anelli delle coordinate associati a curve affini definite su campi finiti, sviluppando un'analogia con il problema classico di teoria dei numeri della determinazione del numero di classi di ideali per campi quadratici.
Già Gauss nelle *Disquisitiones Arithmeticae* ha affrontato il problema della determinazione del numero di classi di forme quadratiche di discriminante fissato, che si è poi rivelato equivalente allo studio del numero di classi dei campi quadratici. In particolare negli Articoli 303 e 304 Gauss ha espresso due congetture, distinguendo il caso dei campi quadratici reali e quello dei campi quadratici immaginari. Mentre la seconda congettura è stata provata da Heilbronn negli anni '30, la prima è ancora irrisolta.
La prima formula per il numero di classi è stata provata nel 1839 da Dirichlet, ancora lavorando nel contesto delle forme quadratiche.

Nel secondo capitolo vedremo risultati generali, validi per una generica curva piana non singolare definita su un campo finito. Questo argomento è stato trattato da F.K. Schmidt nel 1931 ed in seguito ripreso da altri. Nel terzo capitolo vedremo come, specializzando questi risultati al caso delle curve ellittiche, è possibile ricavare un analogo del teorema di Dirichlet e che possono essere dimostrati analoghi delle congetture di Gauss per campi quadratici immaginari e per campi quadratici reali.

Indice

Capitolo 1

Numero dei punti razionali di curve su campi finiti

1.0 Curve affini e proiettive

Sia $\mathbb{K}$ un campo, sia $\overline{\mathbb{K}}$ la sua chiusura algebrica. Siano $\mathbb{A}^n(\overline{\mathbb{K}})$, $\mathbb{P}^n(\overline{\mathbb{K}})$ rispettivamente lo spazio affine e lo spazio proiettivo di dimensione n su $\overline{\mathbb{K}}$.

Si definisce **varietà affine** un insieme della forma

$$V = \{P \in \mathbb{A}^n(\overline{\mathbb{K}}) |\ f(P) = 0\ \forall f \in I_V\}$$

con I_V ideale primo di $\overline{\mathbb{K}}[X_1, \ldots, X_n]$. I_V è allora detto l'ideale di V.
In particolare se I_V è generato da polinomi a coefficienti in $\mathbb{K}$ si dice che V è definita su $\mathbb{K}$.
Se V è definita su $\mathbb{K}$, si definisce l'**anello delle coordinate** di V come

$$\mathbb{K}[\boldsymbol{V}] = \mathbb{K}[X_1, \ldots, X_N]/I_V$$

Il campo dei quozienti di $\mathbb{K}[V]$, notato $\mathbb{K}(\boldsymbol{V})$, è detto il **campo di funzioni** di V.
Analogamente, si definiscono $\overline{\mathbb{K}}[V] = \overline{\mathbb{K}}[X_1, \ldots, X_N]/I_V$ e si nota $\overline{\mathbb{K}}(V)$ il suo campo dei quozienti.

Si definisce la **dimensione** di V come il grado di trascendenza di $\overline{\mathbb{K}}(V)$ su $\overline{\mathbb{K}}$.
In particolare si dice che V è una **curva** affine se l'estensione $\overline{\mathbb{K}} \subseteq \overline{\mathbb{K}}(V)$ ha grado di trascendenza 1.

Analogamente, si definisce **varietà proiettiva** un insieme della forma

$$\widetilde{V} = \{P \in \mathbb{P}^n(\overline{\mathbb{K}}) |\ f(P) = 0\ \forall f \in I_{\widetilde{V}}\}$$

con $I_{\widetilde{V}}$ ideale primo di $\overline{\mathbb{K}}[X_0, \ldots, X_n]$ *generato da polinomi omogenei*; $I_{\widetilde{V}}$ è detto ancora l'ideale di $\widetilde{V}$.
Le definizioni di anello delle coordinate, campo di funzioni e dimensione possono essere estese al caso proiettivo. Ancora, si definisce una curva proiettiva come una varietà proiettiva di dimensione 1.

Se V è una varietà affine definita su $\mathbb{K}$, si definisce l'insieme dei **punti $\mathbb{K}$-razionali** di V come $\mathbf{V}(\mathbb{K}) = V \cap \mathbb{A}^n(\mathbb{K})$.
Analogamente, se $\widetilde{V}$ è una varietà proiettiva definita su $\mathbb{K}$, si definisce l'insieme dei **punti $\mathbb{K}$-razionali** di $\widetilde{V}$ come

$$\widetilde{\mathbf{V}}(\mathbb{K}) = V \cap \mathbb{P}^n(\mathbb{K})$$

Sia C una curva affine. Se C può essere trasformata in C' tramite un'affinità A, allora A induce una corrispondenza biunivoca tra $C(\mathbb{K})$ e $C'(\mathbb{K})$, quindi $\#C(\mathbb{K}) = \#C'(\mathbb{K})$. Analogamente, se una curva proiettiva $\widetilde{C}$ può essere trasformata in $\widetilde{C}'$ tramite una proiettività B, allora B induce una corrispondenza biunivoca tra $\widetilde{C}(\mathbb{K})$ e $\widetilde{C}'(\mathbb{K})$, quindi $\#\widetilde{C}(\mathbb{K}) = \#\widetilde{C}'(\mathbb{K})$

Data una varietà affine $V = \{P \in \mathbb{A}^n(\overline{\mathbb{K}}) |\ f(P) = 0\ \forall f \in I_V\}$, la sua chiusura proiettiva è la varietà proiettiva $\widetilde{V} = \{P \in \mathbb{P}^n(\overline{\mathbb{K}}) |\ g(P) = 0\ \forall g \in \widetilde{I}_V\}$, con $\widetilde{I}_V$ ideale di $\overline{\mathbb{K}}[X_0, \ldots, X_n]$ generato dagli omogeneizzati rispetto a X_0 dei polinomi di I_V. Viceversa, poiché si può identificare $\mathbb{A}^n(\overline{\mathbb{K}})$ con un sottoinsieme di $\mathbb{P}^n(\overline{\mathbb{K}})$, data una varietà proiettiva $\widetilde{V}$ si può definire la sua parte

affine come $V = \widetilde{V} \cap \mathbb{A}^n(\overline{\mathbb{K}})$.
Certamente se V è una varietà affine e $\widetilde{V}$ è la sua chiusura proiettiva allora $\#\widetilde{V}(\mathbb{K}) = \#V(\mathbb{K}) + \#A$, con A insieme dei punti impropri di $\widetilde{V}$.

Osservazione 1.0.1.
Sia $C:\ Y^2 = f(X)$ una curva affine piana, con f polinomio a coefficienti in $\mathbb{F}_q$, campo finito di caratteristica diversa da 2, sia $\widetilde{C}$ la sua chiusura proiettiva.

Sia $x \in \mathbb{F}_q$. Se $f(x) = 0$, certamente $(x, 0) \in C(\mathbb{F}_q)$ e questo è l'unico punto razionale di C di ascissa x. Supponiamo $f(x) \neq 0$. Se $f(x)$ è un quadrato in $\mathbb{F}_q$, $f(x) = k^2$, allora C ha due punti razionali di ascissa x: $(x, k), (x, -k)$; se $f(x)$ non è un quadrato invece C non ha nessun punto razionale di ascissa x. Quindi per ogni valore di $x \in \mathbb{F}_q$, o C ha un unico punto razionale di ascissa x, oppure C ha con il 50% di probabilità 2 punti razionali di ascissa x e con il 50% di probabilità nessun punto razionale di ascissa x.
Inoltre, se $\deg f > 2$ allora C ha un unico punto all'infinito: $[0, 1, 0]$.
Ci si può quindi aspettare che il numero di punti proiettivi razionali di $\widetilde{C}$ sia $\#\widetilde{C}(\mathbb{F}_q) = q + 1 + \varepsilon$, con ε, termine d'errore, piccolo rispetto a q. Ci si può cioè aspettare che il numero dei punti razionali di $\widetilde{C}$ non differisca troppo dal numero dei punti razionali di una retta proiettiva.
Vedremo che effettivamente se $\widetilde{C}$ è una conica proiettiva non degenere allora $\#\widetilde{C}(\mathbb{F}_q) = q+1$ (corollario 1.2.5) e che se $\widetilde{C}$ è della forma $aX^3+bY^3+cZ^3 = 0$ allora $|\#\widetilde{C}(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$ (osservazione 1.3.5).
Vedremo poi che in generale se $\widetilde{C}$ è una curva proiettiva non singolare di genere g definita sul campo finito $\mathbb{F}_q$, allora

$$\#\widetilde{C}(\mathbb{F}_q) = q + 1 + \varepsilon, \text{ con } |\varepsilon| \leq 2g\sqrt{q} \quad \text{(Teorema di Weil 1.4.17)}$$

1.1 Rette

Osservazione 1.1.1.
Una retta r di $\mathbb{A}^2(\mathbb{F}_q)$ è individuata da un'equazione della forma
$aX + bY + c = 0$, con $a, b, c \in \mathbb{F}_q$ e $(a, b) \neq (0, 0)$.
Supponiamo, per esempio, che $b \neq 0$.

Allora $r(\mathbb{F}_q) = \{ (x, (-ax-c)b^{-1}) \mid x \in \mathbb{F}_q \}$, quindi r ha esattamente q punti razionali su $\mathbb{F}_q$.

Osservazione 1.1.2.
Una retta $\widetilde{r}$ di $\mathbb{P}^2(\mathbb{F}_q)$ è individuata da un'equazione della forma
$aX + bY + cZ = 0$, con $a, b, c \in \mathbb{F}_q$ e $(a, b, c) \neq (0, 0, 0)$.
Supponiamo, per esempio, che $b \neq 0$.
Allora $\widetilde{r}(\mathbb{F}_q) = \{ [x, (-ax-c)b^{-1}, 1] \mid x \in \mathbb{F}_q \} \cup \{[1, -ab^{-1}, 0]\}$, quindi $\widetilde{r}$ ha esattamente $q+1$ punti razionali su $\mathbb{F}_q$.

1.2 Coniche

D'ora in poi supporremo che $\mathbb{K}$ sia un campo tale che $\mathrm{car}(\mathbb{K}) \neq 2$ (cioè, se $\mathbb{K}$ è un campo finito, che $\mathbb{K} = \mathbb{F}_q$, con $q = p^n$, p primo e $p \neq 2$).

Osservazione 1.2.1.
Una conica C di $\mathbb{A}^2(\mathbb{K})$ è un curva definita da un'equazione della forma
$aX^2+bXY+cY^2+dX+eY+f = 0$, con $a, b, c, d, e, f \in \mathbb{K}$ e $(a, b, c) \neq (0, 0, 0)$.
La chiusura proiettiva di C, $\widetilde{C}$, ha quindi equazione della forma aX^2+bXY+ $+ cY^2 + dXZ + eYZ + fZ^2 = 0$, con $(a, b, c) \neq (0, 0, 0)$.

Allora $\widetilde{C} = \left\{ [X, Y, Z] \in \mathbb{P}^2(\mathbb{K}) \middle| \ \widetilde{F}(X, Y, Z) = 0 \right\}$, con $\widetilde{F}$ polinomio omogeneo di secondo grado, quindi forma quadratica. Ora, una forma quadratica su un campo di caratteristica diversa da 2 può sempre essere diagonalizzata, cioè esiste $B \in \mathrm{GL}_3(\mathbb{K})$ tale che, se M è la matrice che rappresenta $\widetilde{F}$ rispetto alla base assegnata, ${}^tBMB$ è diagonale. Dunque la proiettività di matrice B muta $\widetilde{C}$ in una conica proiettiva del tipo $\widetilde{C}' : \ \alpha X^2 + \beta Y^2 + \gamma Z^2 = 0$, quindi dà una biezione tra $\widetilde{C}(\mathbb{K})$ e $\widetilde{C}'(\mathbb{K})$.
É quindi sufficiente considerare le coniche proiettive della forma
$aX^2 + bY^2 + cZ^2 = 0$, con $a, b, c \in \mathbb{K}$ e $(a, b, c) \neq (0, 0, 0)$.

Proposizione 1.2.2.
Sia $C : aX^2 + bY^2 + cZ^2 = 0$ *una conica in* $\mathbb{P}^2(\mathbb{F}_q)$, *con* $(a, b, c) \neq (0, 0, 0)$.
Allora

$$C(\mathbb{F}_q) \neq \emptyset$$

Dimostrazione.
Se C è doppiamente degenere, cioè se è del tipo $aX^2 = 0$, certamente $[0, y, z] \in C(\mathbb{F}_q)$ per ogni $y, z \in \mathbb{F}_q$, quindi $C(\mathbb{F}_q) \neq \emptyset$.

Supponiamo che C non sia doppiamente degenere, cioè che almeno due tra a, b, c siano non nulli. Supponiamo, per esempio, $a, b \neq 0$.
Sia C' la conica affine definita da $aX^2 + bY^2 + c = 0$. Poiché C è allora la chiusura proiettiva di C', è sufficiente dimostrare che $C'(\mathbb{F}_q) \neq \emptyset$.

Consideriamo le applicazioni $f : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \mapsto & ax^2 + c \end{array}$ e $g : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \mapsto & -bx^2 \end{array}$.
Allora $f = f_1 \circ \psi$ e $g = g_1 \circ \psi$, con $\psi, f_1, g_1 : \mathbb{F}_q \to \mathbb{F}_q$ definite da $\psi(x) = x^2$, $f_1(y) = ay + c$, $g_1(y) = -by$. Certamente f_1 e g_1 sono biunivoche.
Si ha invece che $\#\text{Im}\ (\psi) = \dfrac{q+1}{2}$. Infatti se $x = 0$, $x^2 = y^2 \Leftrightarrow y = x = 0$ e se $x \neq 0$, $x^2 = y^2 \Leftrightarrow y = \pm x$, quindi $\#\text{Im}\ (\psi) = \dfrac{q-1}{2} + 1 = \dfrac{q+1}{2}$.
Allora $\#\text{Im}\ (f) = \#\text{Im}\ (f_1 \circ \psi) = \#\text{Im}\ (\psi) = \dfrac{q+1}{2}$ e, analogamente, $\#\text{Im}\ (g) = \dfrac{q+1}{2}$.
Poiché $\text{Im}\ (f), \text{Im}\ (g) \subseteq \mathbb{F}_q$, campo finito a q elementi, si deve avere
$\text{Im}\ (f) \cap \text{Im}\ (g) \neq \emptyset$, quindi $\exists x, y \in \mathbb{F}_q$ tali che $f(x) = g(y)$, cioè tali che $ax^2 + c = -by^2$, cioè tali che $(x, y) \in C(\mathbb{F}_q)$. □

Osservazione 1.2.3.
Sia $\mathbb{K}$ un campo di caratteristica diversa da 2, sia $\overline{\mathbb{K}}$ la sua chiusura algebrica.

- Una conica *non degenere* e una retta di $\mathbb{P}^2(\mathbb{K})$, se pensate in $\mathbb{P}^2(\overline{\mathbb{K}})$, si intersecano al più in due punti, non necessariamente $\mathbb{K}$-razionali. Tuttavia, se esse si intersecano in due punti distinti, uno dei quali è $\mathbb{K}$-razionale, necessariamente anche l'altro lo è.

- Se C è una conica *non degenere* di $\mathbb{P}^2(\mathbb{K})$ e se $O \in C(\mathbb{K})$, allora esiste una e una sola retta t di $\mathbb{P}^2(\mathbb{K})$ passante per O e tangente a C, cioè

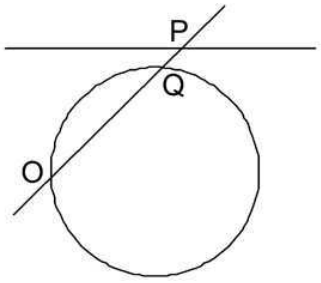
tale che $C \cap t = \{O\}$. Se $C: \ aX^2 + bY^2 + cZ^2 = 0$ e se $O = [\bar{x}, \bar{y}, \bar{z}]$, allora $t : a\bar{x}X + b\bar{y}Y + c\bar{z}Z = 0$.

Proposizione 1.2.4.
Sia C una conica non degenere definita su un campo $\mathbb{K}$ di caratteristica diversa da 2 tale che $C(\mathbb{K}) \neq \emptyset$. Allora $C(\mathbb{K})$ è in corrispondenza biunivoca con $r(\mathbb{K})$, con r retta a coefficienti in $\mathbb{K}$.

Dimostrazione.
Sia C una conica non degenere di $\mathbb{P}^2(\mathbb{K})$, sia $O \in C(\mathbb{K})$, sia r una retta di $\mathbb{P}^2(\mathbb{K})$ non passante per O.
Consideriamo le applicazioni:

$$\varphi: \begin{array}{ccc} r(\mathbb{K}) & \to & C(\mathbb{K}) \\ P & \mapsto & \begin{cases} Q \text{ con } \{Q\} = (r(O,P) \cap C) \setminus \{O\} & \text{se } r(O,P) \cap C \neq \{O\} \\ O & \text{altrimenti} \end{cases} \end{array}$$

$$\psi: \begin{array}{ccc} C(\mathbb{K}) & \to & r(\mathbb{K}) \\ Q & \mapsto & \begin{cases} P \text{ con } \{P\} = r(O,Q) \cap r & \text{se } Q \neq O \\ P \text{ con} \{P\} = t \cap r & \text{altrimenti} \end{cases} \end{array}$$



dove $r(O,P), r(O,Q)$ sono rispettivamente le rette per O, P e per O, Q e dove t è la retta per O tangente a C.
Per l'osservazione precedente, φ, ψ sono ben definite e sono l'una l'inversa dell'altra, quindi definiscono una corrispondenza biunivoca tra $r(\mathbb{K})$ e $C(\mathbb{K})$. □

Corollario 1.2.5.
Ogni conica non degenere definita su $\mathbb{F}_q$, con $\mathrm{car}(\mathbb{F}_q) \neq 2$, ha esattamente $q+1$ punti razionali.

Dimostrazione.
Sia C una conica non degenere di $\mathbb{P}^2(\mathbb{F}_q)$. Per la proposizione 1.2.2 si ha che $C(\mathbb{F}_q) \neq \emptyset$, quindi per la proposizione precedente $C(\mathbb{F}_q)$ è in corrispondenza

biunivoca con $r(\mathbb{F}_q)$, con r generica retta di $\mathbb{P}^2(\mathbb{F}_q)$. Per l'osservazione 1.1.2 allora $\#C(\mathbb{F}_q) = q + 1$. □

Vedremo che il risultato precedente in realtà è un caso particolare del Teorema di Weil.

Osservazione 1.2.6.

1. Sia $C : aX^2 + bY^2 = 0$ una conica semplicemente degenere su $\mathbb{P}^2(\mathbb{F}_q)$. $[x, y, z] \in C(\mathbb{F}_q) \Leftrightarrow ax^2 + by^2 = 0 \Leftrightarrow x^2 = -ba^{-1}y^2$.

   - Se $-ba^{-1}$ è un quadrato in $\mathbb{F}_q$, $-ba^{-1} = k^2$, allora $(x, y) \in C(\mathbb{F}_q) \Leftrightarrow x^2 = k^2y^2 \Leftrightarrow x = \pm ky$ (con $k \neq 0$), quindi $C(\mathbb{F}_q) = \{[k, 1, z] |\ z \in \mathbb{F}_q\} \cup \{[-k, 1, z] |\ z \in \mathbb{F}_q\} \cup \{[0, 0, 1]\}$, quindi C ha $2q + 1$ punti razionali.
   - Se $-ba^{-1}$ non è un quadrato in $\mathbb{F}_q$, allora $x^2 = -ba^{-1}y^2 \Leftrightarrow x = y = 0$, quindi C ha un unico punto razionale: $[0, 0, 1]$.

2. Sia $C : aX^2 = 0$ una conica doppiamente degenere su $\mathbb{P}^2(\mathbb{F}_q)$. Allora $C(\mathbb{F}_q) = \{[0, y, z] |\ y, z \in \mathbb{F}_q\} \subseteq \mathbb{P}^2(\mathbb{F}_q)$, quindi $C(\mathbb{F}_q)$ ha $q+1$ punti razionali ($C(\mathbb{F}_q)$ coincide con $r(\mathbb{F}_q)$, con r retta di equazione $X = 0$).

Osservazione 1.2.7.

1. Sia C una conica affine non degenere su $\mathbb{F}_q$, allora C è affinemente equivalente a $C_1 : aX^2 + bY^2 + c = 0$, con $a, b, c \neq 0$, oppure a $C_2 : aX^2 - bY = 0$, con $a, b \neq 0$.

   - La chiusura proiettiva di $C_1 : aX^2 + bY^2 + c = 0$ è $\widetilde{C}_1 : aX^2 + bY^2 + cZ^2 = 0$, conica proiettiva non degenere, con $\#\widetilde{C}_1(\mathbb{F}_q) = q + 1$. $[x, y, 0]$ è un punto improprio di $\widetilde{C}_1$ se e solo se $ax^2 + by^2 = 0$, cioè se e solo se $x^2 = -ba^{-1}y^2$.
     Se $-ba^{-1}$ è un quadrato in $\mathbb{F}_q$, $-ba^{-1} = k^2$, allora $\widetilde{C}_1$ ha due punti impropri, $[k, 1, 0]$ e $[-k, 1, 0]$, quindi C_1 ha $(q + 1) - 2 = q - 1$ punti razionali.

Se $-ba^{-1}$ non è un quadrato in $\mathbb{F}_q$, allora $\widetilde{C}_1$ non ha punti impropri, quindi C_1 ha $q+1$ punti razionali.

- La chiusura proiettiva di $C_2 : aX^2+bY = 0$ è $\widetilde{C}_2 : aX^2+bYZ = 0$, conica proiettiva non degenere, con $\#\widetilde{C}_2(\mathbb{F}_q) = q+1$. $[x, y, 0]$ è un punto improprio di $\widetilde{C}_2$ se e solo se $ax^2 = 0$, quindi l'unico punto improprio di $\widetilde{C}_2$ è $[0, 1, 0]$. Allora C_2 ha $(q + 1) - 1 = q$ punti razionali.

2. Sia C una conica affine semplicemente degenere su $\mathbb{F}_q$, allora C è affinemente equivalente a $C_3 : aX^2 + bY^2 = 0$, con $a, b \neq 0$, oppure a $C_4 : aX^2 + b = 0$, con $a, b \neq 0$.

   - La chiusura proiettiva di $C_3 : aX^2+bY^2 = 0$ è $\widetilde{C}_3 : aX^2+bY^2 = 0$. $[x, y, 0]$ è un punto improprio di $\widetilde{C}_3$ se e solo se $ax^2 + by^2 = 0$, cioè se e solo se $x^2 = -ba^{-1}y^2$.
     Se $-ba^{-1}$ è un quadrato in $\mathbb{F}_q$, $-ba^{-1} = k^2$, allora $\widetilde{C}_3$ ha $2q + 1$ punti razionali e 2 punti impropri, $[k, 1, 0]$ e $[-k, 1, 0]$, quindi C_3 ha $(2q + 1) - 2 = 2q - 1$ punti razionali.
     Se $-ba^{-1}$ non è un quadrato in $\mathbb{F}_q$, allora $\widetilde{C}_3$ ha un solo punto razionale e non ha punti impropri, quindi C_3 ha 1 punto razionale.
   - La chiusura proiettiva di $C_4 : aX^2 + b = 0$ è $\widetilde{C}_4 : aX^2 + bZ^2 = 0$. $[x, y, 0]$ è un punto improprio di $\widetilde{C}_4$ se e solo se $ax^2 = 0$, quindi l'unico punto improprio di $\widetilde{C}_4$ è $[0, 1, 0]$.
     Se $-ba^{-1}$ è un quadrato in $\mathbb{F}_q$, allora $\widetilde{C}_4$ ha $2q+1$ punti razionali, quindi C_4 ha $(2q + 1) - 1 = 2q$ punti razionali.
     Se $-ba^{-1}$ non è un quadrato in $\mathbb{F}_q$, allora $\widetilde{C}_4$ ha un solo punto razionale, quindi C_4 non ha nessun punto razionale.

3. Sia C una conica affine doppiamente degenere su $\mathbb{F}_q$, allora C è affinemente equivalente a $C_5 : aX^2 = 0$, con $a \neq 0$. La chiusura proiettiva di C_5, $\widetilde{C}_5 : aX^2 = 0$, ha $q + 1$ punti razionali. $[x, y, 0]$ è un punto improprio di $\widetilde{C}_5$ se e solo se $ax^2 = 0$, quindi l'unico punto improprio di $\widetilde{C}_5$ è $[0, 1, 0]$. Allora C_5 ha $(q + 1) - 1 = q$ punti razionali.

1.3 Cubiche: teorema di Gauss

Sia $C : X^3 + Y^3 + Z^3 = 0$ la cubica di Fermat in $\mathbb{P}^2(\mathbb{F}_p)$, con p primo, $p > 3$; sia $M_p = \#C(\mathbb{F}_p)$.

Osservazione 1.3.1.
Supponiamo che p sia un numero primo tale che $p \equiv 1 \pmod 3$, sia m tale che $p = 3m + 1$.

Certamente $\mathbb{F}_p^*$ è un gruppo ciclico di ordine $p - 1$, multiplo di 3.
Sia $\widetilde{\varphi}$ la mappa di $\mathbb{F}_p^*$ in sé definita da $\widetilde{\varphi}(x) = x^3$, allora Ker $(\widetilde{\varphi}) = \left\{x \in \mathbb{F}_p^* \middle| \ |x| \middle| 3\right\}$, quindi $|\text{Ker } (\widetilde{\varphi})| = 3$ e $|\text{Im } (\widetilde{\varphi})| = \frac{p-1}{3} = m$.
Dunque $\mathbb{F}_p^*$ si ripartisce in tre classi modulo cubi: ponendo $R = \text{Im } (\widetilde{\varphi})$, $S = sR$ e $T = s^2R$, con $s \notin R$, si ha che $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$, unione disgiunta, con $\#R = \#S = \#T = m$. Gli elementi di R sono detti *residui cubici*, ognuno di essi ha esattamente 3 radici cubiche in $\mathbb{F}_p$.

Sia $x \in \mathbb{F}_p$, allora

$$x^{2m} + x^m + 1 \equiv \#\{t \in \mathbb{F}_p | \ x = t^3\} \pmod p \tag{1.1}$$

Infatti se $x = 0$ si ha $\#\{t \in \mathbb{F}_p | \ 0 = t^3\} \equiv \#\{0\} \equiv 1 \pmod p$; se $x \neq 0$ e $x \in R$, allora $x^m \equiv 1 \pmod p$, quindi $x^{2m} + x^m + 1 \equiv 3 \pmod p$, e d'altra parte $\#\{t \in \mathbb{F}_p | \ x = t^3\} = 3$; se $x \neq 0$ e $x \notin R$, allora $x^m \not\equiv 1 \pmod p$ quindi, poiché $x^{3m} - 1 = (x^m - 1)(x^{2m} + x^m + 1) \equiv 0 \pmod p$, $x^{2m} + x^m + 1 \equiv 0 \pmod p$, e d'altra parte $\#\{t \in \mathbb{F}_p | \ x = t^3\} = 0$.

La cubica di Fermat C ha 3 punti impropri.
Infatti $[x, y, 0] \in C(\mathbb{F}_p) \ \Leftrightarrow x^3 + y^3 = 0 \ \Leftrightarrow \ x^3 = (-y)^3 \ \Leftrightarrow$
$[x, y, z] \in \{[-1, 1, 0], [u, 1, 0], [u^2, 1, 0]\}$, dove $-1, u, u^2$ sono le tre radici cubiche di -1 in $\mathbb{F}_p$.

Poiché -1 è un residuo cubico, i punti affini di C sono in corrispondenza biunivoca con le soluzioni $(x, y) \in \mathbb{F}_p^2$ di $Y^3 = X^3 + 1$.

Allora per (1.1) si ha che $M_p \equiv 3 + \sum_{x\in\mathbb{F}_p} \left((x^3+1)^{2m} + (x^3+1)^m + 1\right) \equiv$

$$\equiv 3 + \sum_{x\in\mathbb{F}_p} \left(\sum_{l=0}^{2m} \binom{2m}{l} x^{3l} + \sum_{l=0}^{m} \binom{m}{l} x^{3l} + 1 \right) \equiv$$

$$\equiv 3 + \sum_{l=0}^{2m} \binom{2m}{l} \sum_{x\in\mathbb{F}_p} x^{3l} + \sum_{l=0}^{m} \binom{m}{l} \sum_{x\in\mathbb{F}_p} x^{3l} \pmod p.$$

Ora, $\sum_{x\in\mathbb{F}_p} x^h \equiv \begin{cases} -1 \pmod p & \text{se } (p-1)|h \\ 0 \pmod p & \text{altrimenti} \end{cases}$.

Infatti se $(p-1)|h$ allora $\sum_{x\in\mathbb{F}_p} x^h \equiv \sum_{x\in\mathbb{F}_p^*} 1 \equiv p-1 \pmod p$. Supponiamo che $(p-1) \nmid h$. Sia $\alpha \in \mathbb{F}_p^*$ tale che $\langle\alpha\rangle = \mathbb{F}_p^*$, allora $\sum_{x\in\mathbb{F}_p} x^h = \sum_{k=1}^{p-1} \alpha^{kh}$. D'altra parte, $\alpha^{(p-1)h} - 1 = (\alpha^h - 1)(\alpha^{(p-2)h} + \cdots + 1) = 0$, con $\alpha^h - 1 \neq 0$.

Quindi $\sum_{x\in\mathbb{F}_p} x^h \equiv 0 \pmod p$.

Allora $M_p \equiv 3 - \binom{2m}{m} - \binom{2m}{2m} - \binom{m}{m} \pmod p$.

Quindi $M_p \equiv 1 - \binom{2m}{m} \pmod p$.

Definizione 1.3.1.

Siano $A, B, C \subseteq \mathbb{F}_p$, si pone $[ABC] = \#\{(a,b,c) \in A \times B \times C |\ a+b+c = 0\}$.

Osservazione 1.3.2.

Siano $A, B, C, D \subseteq \mathbb{F}_p$, allora:

- se $C \cap D = \emptyset$ si ha $[AB(C \cup D)] = [ABC] + [ABD]$
- $[ABC] = [xA\ xB\ xC]$ per ogni $x \neq 0$
- $[ABC] = [ACB] = [BCA] = [BAC] = [CAB] = [CBA]$

Definizione 1.3.2.

Sia f un polinomio monico di terzo grado, $f(x) = x^3 + ax^2 + bx + c$, il **discriminante** di f è $D = 4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

Se $\alpha_1, \alpha_2, \alpha_3$ sono le radici di f si ha che $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$.

Teorema 1.3.3. Teorema di Gauss
Sia $C : X^3+Y^3+Z^3=0$ *la cubica di Fermat in* $\mathbb{P}^2(\mathbb{F}_p)$*, con* p *primo,* $p>3$*, sia* $M_p = \#C(\mathbb{F}_p)$.

(a) *Se* $p \equiv 2 \pmod 3$ *allora* $M_p = p+1$.

(b) *Se* $p \equiv 1 \pmod 3$ *allora esistono e sono unici* $A, B \in \mathbb{Z}$ *tali che*

$$4p = A^2 + 27B^2, \text{ con } A \equiv 1 \pmod 3, \ B > 0$$

Inoltre si ha che

$$M_p = p + 1 + A$$

Dimostrazione.

(a) Sia p primo tale che $p \equiv 2 \pmod 3$, allora la mappa $\widetilde{\varphi} : \ x \mapsto x^3$ di $\mathbb{F}_p$ in sé è una biezione. Infatti, $\mathbb{F}_p^*$ è un gruppo ciclico di ordine $p-1$, con $3 \nmid p-1$, quindi $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*, \ \varphi(x) = x^3$ è un morfismo di gruppi finiti iniettivo ($\varphi(x) = \varphi(y) \ \Leftrightarrow \ x^3 = y^3 \ \Leftrightarrow \ (xy^{-1})^3 = 1 \ \Leftrightarrow \ 3 \mid |xy^{-1}| \ \Leftrightarrow \ x = y$), quindi un isomorfismo. Poiché $x^3 = 0 \ \Leftrightarrow \ x = 0$, anche $\widetilde{\varphi}$ è una biezione, cioè ogni elemento di $\mathbb{F}_p$ ha una e una sola radice cubica.
Allora il numero della soluzioni di $X^3+Y^3+Z^3=0$ è uguale al numero delle soluzioni dell'equazione lineare $X+Y+Z=0$, quindi per l'osservazione 1.1.2

$$M_p = p+1$$

(b) Sia p primo tale che $p \equiv 1 \pmod 3$.
Nella notazione dell'osservazione 1.3.1 si ha che se $x, y, z \in \mathbb{F}_p^*$, allora
$x^3+y^3+z^3=0 \ \Leftrightarrow \ \exists x', y', z' \in R$ tali che $x'=x^3, \ y'=y^3, \ z'=z^3$,
$x'+y'+z'=0$. Per definizione il numero di tali terne (x', y', z') è $[RRR]$.
Poiché ad ogni x' (rispettivamente y', z') corrispondono 3 possibili scelte di x (rispettivamente di y, z), $\#\{(x,y,z) \in \mathbb{F}_p^3 |\ x^3+y^3+z^3=0, \ x,y,z \neq 0\} =$
$= 27[RRR]$. Allora $\#\{[x,y,z] \in \mathbb{P}^2(\mathbb{F}_p) |\ x^3+y^3+z^3=0, \ x,y,z \neq 0\} =$
$= \dfrac{27[RRR]}{p-1} = \dfrac{9[RRR]}{m}$.
D'altra parte, $\#\{(x,y,z) \in \mathbb{F}_p^3 \setminus \{(0,0,0)\} |\ x^3+y^3+z^3=0, \ xyz=0\} =$

$= 3\#\{(x,y,0) \in \mathbb{F}_p^3 |\ x^3+y^3=0,\ x,y \neq 0\}$. Fissato $x \in \mathbb{F}_p^*$, l'equazione $Y^3 = -x^3$ ha sempre 3 soluzioni distinte, quindi
$\#\{(x,y,z) \in \mathbb{F}_p^3 \setminus \{(0,0,0)\} |\ x^3+y^3+z^3=0,\ xyz=0\} = 9(p-1)$. Allora
$\#\{[x,y,z] \in \mathbb{P}^2(\mathbb{F}_p) |\ x^3+y^3+z^3=0,\ xyz=0\} = \dfrac{9(p-1)}{p-1} = 9$. Quindi

$$M_p = 9\left(\frac{[RRR]}{m}+1\right) \tag{1.2}$$

Poiché $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$, unione disgiunta, e $[RR\mathbb{F}_p] = m^2$
$\Big(\text{infatti } [RR\mathbb{F}_p] = \#\{(x,y,z) \in R \times R \times \mathbb{F}_p |\ z = -x-y\} = (\#R)^2\Big)$
si ha che $m^2 = [RR\{0\}] + [RRR] + [RRS] + [RRT]$. In maniera del tutto analoga si ottiene che $m^2 = [ST\{0\}] + [STR] + [STS] + [STT]$.
Ora, siano $s \in S,\ t \in T$, allora $[RRS] = [sR\ sR\ sS] = [SST]$ e $[RRT] =$
$= [tR\ tR\ tT] = [TTS]$. Inoltre, $[RR\{0\}] = \#\{(x,y,0) | x,y \in R, x+y=0\} =$
$= \#\{(x,-x,0), x \in R\} = m$ (perché $-R = R$) e
$[ST\{0\}] = \#\{(x,y,0),\ x \in S,\ y \in T,\ x+y=0\} = 0$ (perché $-S \cap T = \emptyset$).
Dunque si ha che $\begin{cases} m^2 = m + [RRR] + [SST] + [TTS] \\ m^2 = [RTS] + [SST] + [TTS] \end{cases}$
allora $[RRR] = [RTS] - m$ e sostituendo in (1.2) si ottiene che

$$M_p = \frac{9[RTS]}{m} \tag{1.3}$$

Sia $\zeta \in \mathbb{C}$ una radice primitiva p-esima dell'unità, allora ha senso considerare ζ^a per $a \in \mathbb{F}_p$. Siano

$$\alpha_1 = \sum_{r \in R} \zeta^r,\ \alpha_2 = \sum_{s \in S} \zeta^s,\ \alpha_3 = \sum_{t \in T} \zeta^t$$

Proviamo che $\alpha_1, \alpha_2, \alpha_3$ sono le tre radici di un polinomio di terzo grado a coefficienti interi.

$\alpha_2\alpha_3 = \displaystyle\sum_{\substack{s \in S \\ t \in T}} \zeta^{s+t} = \sum_{x \in \mathbb{F}_p^*} N_x \zeta^x$, con $N_x = \#\{(s,t) \in S \times T |\ s+t=x\} =$
$= [ST\{-x\}]$. Se $r \in R$, $N_x = N_{rx}$, quindi N_x dipende solo dalla classe di x modulo cubi. Allora $mN_x = \displaystyle\sum_{r \in R} N_{rx} = \left[ST \bigcup_{r \in R} \{rx\}\right] = [ST\ xR] =$

$$= \begin{cases} [STR] \text{ se } x \in R \\ [STS] \text{ se } x \in S \\ [STT] \text{ se } x \in T \end{cases} . \text{ Siano } a = N_r,\ b = N_s,\ c = N_t, \text{ con } r \in R,$$

$s \in S,\ t \in T$, allora $[RTS] = ma,\ [SST] = mb,\ [TTS] = mc$ e per (1.3)

$$M_p = 9a \tag{1.4}$$

Allora $\alpha_2\alpha_3 = \sum_{r\in R} N_r\zeta^r + \sum_{s\in S} N_s\zeta^s + \sum_{t\in T} N_t\zeta^t = a\alpha_1 + b\alpha_2 + c\alpha_3$.
Analogamente si ottiene che $\alpha_1\alpha_3 = \sum_{\substack{r\in R\\ t\in T}} \zeta^{r+t} = \sum_{x\in\mathbb{F}_p^*} M_x\zeta^x$ con

$$mM_x = \begin{cases} [RTR] \text{ se } x \in R \\ [RTS] \text{ se } x \in S \\ [RTT] \text{ se } x \in T \end{cases}, \text{ quindi con } M_x = \begin{cases} c \text{ se } x \in R \\ a \text{ se } x \in S \\ b \text{ se } x \in T \end{cases} \text{ e dunque si}$$

ha $\alpha_1\alpha_3 = c\alpha_1 + a\alpha_2 + b\alpha_3$.

$$\text{Similmente, } \alpha_1\alpha_2 = \sum_{\substack{r\in R\\ s\in S}} \zeta^{r+s} = \sum_{x\in\mathbb{F}_p^*} L_x\zeta^x \text{ con } mL_x = \begin{cases} [RSR] \text{ se } x \in R \\ [RSS] \text{ se } x \in S \\ [RST] \text{ se } x \in T \end{cases},$$

$$\text{quindi con } L_x = \begin{cases} b \text{ se } x \in R \\ c \text{ se } x \in S \\ a \text{ se } x \in T \end{cases}, \text{ dunque } \alpha_1\alpha_2 = b\alpha_1 + c\alpha_2 + a\alpha_3.$$

Ora, $0 = \zeta^p - 1 = (\zeta - 1)(\zeta^{p-1} + \cdots + \zeta + 1)$, quindi $\sum_{x\in\mathbb{F}_p} \zeta^x = 0$, cioè

$$\alpha_1 + \alpha_2 + \alpha_3 = -1 \tag{1.5}$$

Allora, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = (a + b + c)(\alpha_1 + \alpha_2 + \alpha_3) = -(a + b + c)$.
D'altra parte, $m(a + b + c) = [RTS] + [SST] + [TTS] = m^2$, quindi

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -m \tag{1.6}$$

Allora $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 1 + 2m$.
Inoltre, $\alpha_1\alpha_2\alpha_3 = \alpha_1(a\alpha_1 + b\alpha_2 + c\alpha_3) = \alpha_2(c\alpha_1 + a\alpha_+ b\alpha_3) = \alpha_3(b\alpha_1 +$
$+ c\alpha_2 + a\alpha_3)$, quindi $3\alpha_1\alpha_2\alpha_3 = a(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + (b + c)(\alpha_1\alpha_2 + \alpha_2\alpha_3 +$
$+ \alpha_1\alpha_3) = (1 + 2m)a - m(b + c)$. Ponendo $k = 2a - b - c = 3a - m$ si ha

$$3\alpha_1\alpha_2\alpha_3 = a + km \tag{1.7}$$

Con questa posizione inoltre sostituendo in (1.4) si ha che

$$M_p = 3(k+m) = 3k + p - 1 \tag{1.8}$$

Certamente $\alpha_1, \alpha_2, \alpha_3$ sono le tre radici complesse del polinomio $F(t) = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)$ e, per (1.5), (1.6), (1.7) si ha che $F(t) = t^3 + t^2 - mt - \dfrac{a+km}{3}$.
Sia D_F il discriminante di F, per definizione allora $D_F = d^2$, con $d = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$.
D'altra parte, $d = \alpha_1\alpha_2(\alpha_1-\alpha_2) + \alpha_1\alpha_3(\alpha_3-\alpha_1) + \alpha_2\alpha_3(\alpha_2-\alpha_3) =$
$= (b-c)(\alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_1\alpha_3-\alpha_2\alpha_3) = (b-c)(1+3m) = p(b-c)$.

Poniamo ora

$$\beta_i = 1 + 3\alpha_i,\ i = 1,2,3$$

utilizzando ancora (1.5), (1.6), (1.7) si ha quindi che:
• $\beta_1+\beta_2+\beta_3 = 3 + 3(\alpha_1+\alpha_2+\alpha_3) = 0$
• $\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = 3 + 6(\alpha_1+\alpha_2+\alpha_3) + 9(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) =$
$= -3 - 9m = -3p$
• $\beta_1\beta_2\beta_3 = 1 + 3(\alpha_1+\alpha_2+\alpha_3) + 9(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) + 27\alpha_1\alpha_2\alpha_3 =$
$= 1 - 3 - 9m + 9(a+km) = 1 - 3p + 3k + 3m + 9km = p(3k-2)$
$\beta_1, \beta_2, \beta_3$ sono dunque le tre radici complesse del polinomio
$G(t) = (t-\beta_1)(t-\beta_2)(t-\beta_3) = t^3 - 3pt - (3k-2)p$.

Sia $A = 3k-2$; per (1.8) allora

$$M_p = p + 1 + A \tag{1.9}$$

inoltre

$$A \equiv 1 \pmod 3$$

Sia D_G il discriminante di G, per definizione allora $D_G = 4\cdot 27p^3 - 27A^2p^2$.
D'altra parte, $D_G = (\beta_1-\beta_2)^2(\beta_1-\beta_3)^2(\beta_2-\beta_3)^2 = 3^6 D_F = 3^6(b-c)^2p^2$.
Quindi si ha che $4p - A^2 = 27(b-c)^2$. Ponendo $B = b-c$ si ha allora

$$4p = A^2 + 27B^2$$

A meno di scambiare i ruoli di S, T, cioè di cambiare la scelta del non residuo cubico s che li definisce, si può supporre che $[SST] \geq [TTS]$, cioè che $b \geq c$, cioè che $B \geq 0$.

Resta da dimostrare l'unicità di A, B.
Siano A_1, B_1 tali che $4p = A_1^2 + 27B_1^2$, con $A_1 \equiv 1 \pmod 3$ e $B_1 > 0$.
Allora $4p(B_1^2 - B^2) = (A^2 + 27B^2)B_1^2 - (A_1^2 + 27B_1^2)B^2 = A^2B_1^2 - A_1^2B^2 =$
$= (AB_1 - A_1B)(AB_1 + A_1B)$. Allora $p|AB_1 + A_1B$ o $p|AB_1 - A_1B$.
Ora, $(4p)^2 = (A^2+27B^2)(A_1^2+27B_1^2) = (AA_1 \mp 27BB_1)^2+27(AB_1 \pm A_1B)^2$, quindi si deve avere che $p|AA_1 \mp 27BB_1$.
Se si avesse $AB_1 \pm A_1B \neq 0$ si dovrebbe avere $16 > 16 - \left(\dfrac{AA_1 \mp 27BB_1}{p}\right)^2 =$
$= 27\left(\dfrac{AB_1 \pm A_1B}{p}\right)^2 \geq 27$, assurdo.
Quindi si deve avere $AB_1 \pm A_1B = 0$, cioè deve esistere λ tale che
$A = \lambda A_1,\ B = \mp\lambda B_1$.
Allora $4p = A^2 + 27B^2 = \lambda^2(A_1^2 + 27B_1^2) = \lambda^2 4p$, quindi $|\lambda| = 1$.
Inoltre, $1 \equiv A \equiv \lambda A_1 \equiv \lambda \pmod 3$, quindi $\lambda = 1$, cioè $A = A_1,\ B = \mp B_1$; poiché $B, B_1 > 0$ si deve avere $B = B_1$. □

Osservazione 1.3.4.
Consideriamo le curve ellittiche della forma $C : iX^3 + jY^3 + kZ^3 = 0$ con $i, j, k \in \mathbb{F}_p,\ i, j, k \neq 0$, per p primo, $p > 3$.

Se $p \equiv 2 \pmod 3$ allora si può dimostrare, come nel caso della cubica di Fermat, che $C(\mathbb{F}_p)$ è in corrispondenza biunivoca con $r(\mathbb{F}_p)$, con r retta di $\mathbb{P}^2(\mathbb{F}_p)$, cioè che

$$C(\mathbb{F}_p) = p + 1$$

Supponiamo che p sia tale che $p \equiv 1 \pmod 3$.
Nelle notazioni dell'osservazione 1.3.1 e della dimostrazione precedente si ha che la curva ellittica C può essere trasformata tramite una proiettività in una delle quattro curve ellittiche seguenti:
- $C_1 : X^3 + Y^3 + Z^3 = 0$

- $C_2 : sX^3 + Y^3 + Z^3 = 0$, con $s \in S$
- $C_3 : tX^3 + Y^3 + Z^3 = 0$, con $t \in T$
- $C_4 : X^3 + sY^3 + tZ^3 = 0$, con $s \in S,\ t \in T$

Ripetendo il procedimento della dimostrazione precedente si ha che:

$-\ \#C_1(\mathbb{F}_p) = \dfrac{9[RRR]}{m} + 9 = 9a$

$-\ \ \#C_2(\mathbb{F}_p) = \dfrac{9[SRR]}{m} + 3 = 9b + 3$

$-\ \ \#C_3(\mathbb{F}_p) = \dfrac{9[TRR]}{m} + 3 = 9c + 3$

$-\ \ \#C_4(\mathbb{F}_p) = \dfrac{9[RTS]}{m} = 9a.$

Certamente per quanto visto nella precedente dimostrazione, $\#C_1(\mathbb{F}_p) =$
$= \#C_4(\mathbb{F}_p) = p + 1 + A.$
D'altra parte, si ha che $b - c = B$ e $b + c = m - a = m - \dfrac{k+m}{3} =$
$= \dfrac{6m - A - 2}{9} = \dfrac{2p - 4 - A}{9}$. Quindi $b = \dfrac{2p - 4 - A + 9B}{18}$ e $c = \dfrac{2p - 4 - A - 9B}{18}$.
Allora:
- $\#C_1(\mathbb{F}_p) = p + 1 + A$
- $\#C_2(\mathbb{F}_p) = p + 1 - \dfrac{A - 9B}{2}$
- $\#C_3(\mathbb{F}_p) = p + 1 - \dfrac{A + 9B}{2}$
- $\#C_4(\mathbb{F}_p) = p + 1 + A.$

Osservazione 1.3.5.
Nelle notazioni dell'osservazione precedente, si ha che

$$|\#C_i(\mathbb{F}_p) - p - 1| < 2\sqrt{p},\ \ i = 1, 2, 3, 4$$

Infatti $A^2 = 4p - 27B^2 \Rightarrow |A| < 2\sqrt{p}$, quindi per $i = 1, 4$ si ha
$|\#C_i(\mathbb{F}_p) - p - 1| = |A| < 2\sqrt{p}$.
Per $i = 2, 3$ si ha $(\#C_i(\mathbb{F}_p) - p - 1)^2 - 4p = \left(\dfrac{A \pm 9B}{2}\right)^2 - (A^2 + 27B^2) =$
$= -\dfrac{3}{4}(A \mp 3B)^2 < 0$, quindi ancora $|\#C_i(\mathbb{F}_p) - p - 1| < 2\sqrt{p}$.

Vedremo che questo risultato è in realtà un caso particolare del Teorema di Weil (teorema 1.4.17).

1.4 Caso generale: teorema di Weil

Per affrontare lo studio del teorema di Weil, che permette di stimare il numero dei punti di una generica curva proiettiva non singolare, avremo bisogno di alcuni strumenti di geometria algebrica, in particolare serviranno il teorema di Riemann-Roch e lo studio della funzione zeta associata al campo di funzioni di una curva.

1.4.1 Teorema di Riemann-Roch e funzione zeta

Sia C una curva proiettiva non singolare definita su un campo finito $\mathbb{F} = \mathbb{F}_q$, con $q = p^\alpha$, p primo. Sia I_C l'ideale di C e sie $\mathbb{K} = \mathbb{F}(C)$ il campo di funzioni di C.
Il gruppo di Galois $Gal(\overline{\mathbb{F}} : \mathbb{F})$ agisce sui punti di C agendo sulle loro coordinate: se $C \subseteq \mathbb{P}^N(\overline{\mathbb{F}})$, se $P = [p_0, \dots, p_N] \in C(\overline{\mathbb{F}})$ e $\sigma \in Gal(\overline{\mathbb{F}} : \mathbb{F})$ si pone $\sigma P = [\sigma p_0, \dots, \sigma p_N]$.
Il gruppo di Galois $Gal(\overline{\mathbb{F}} : \mathbb{F})$ agisce sui polinomi di $\overline{\mathbb{F}}[X_0, \dots, X_N]$ agendo sui loro coefficienti. Poiché C è definita su $\mathbb{F}$, $Gal(\overline{\mathbb{F}} : \mathbb{F})$ fissa I_C, quindi è ben definita la sua azione su $\overline{\mathbb{F}}[V]$. Si può dimostrare che
$$\overline{\mathbb{K}} = \left\{ \frac{f(X_0, \dots, X_N)}{g(X_0, \dots, X_N)} \middle| \ f, g \text{ polinomi omogenei dello stesso grado, } g \notin I_C \right\} / \sim,$$
dove $\dfrac{f_1}{g_1} \sim \dfrac{f_2}{g_2} \Leftrightarrow f_1 g_2 - f_2 g_1 \in I_C$. Allora $Gal(\overline{\mathbb{F}} : \mathbb{F})$ agisce su $\overline{\mathbb{K}}$ agendo su numeratore e denominatore dei suoi elementi, visti come funzioni razionali. Si può provare che $\mathbb{F}[V], \mathbb{K}$ sono rispettivamente i sottoinsiemi di $\overline{\mathbb{F}}[V], \overline{\mathbb{K}}$ fissati da $Gal(\overline{\mathbb{F}} : \mathbb{F})$.

Definizione 1.4.1.
Sia $P \in C(\overline{\mathbb{F}})$ un punto di C.
A P può essere associato l'anello locale $\mathbb{F}[C]_P = \left\{ F = \dfrac{f}{g} \in \mathbb{K} \middle| \ g(P) \neq 0 \right\}$ e quindi il suo unico ideale massimale

$$(P) = \left\{ F = \frac{f}{g} \in \mathbb{F}[C]_P \middle| \ f(P) = 0 \right\}$$

In effetti, se $F \in \mathbb{F}[C]_P$, $F(P)$ è ben definito e $(P) = \{F \in \mathbb{F}[C]_P |\ F(P) = 0\}$. Si dice che (P) è un **divisore primo** di $\mathbb{K}$. Notiamo $\boldsymbol{S}_{\mathbb{K}}$ l'insieme dei divisori primi di $\mathbb{K}$.

Siano $P, Q \in C(\overline{\mathbb{F}})$. P, Q sono coniugati (cioè esiste $\sigma \in Gal(\overline{\mathbb{F}} : \mathbb{F})$ tale che $\sigma P = Q$) se e solo se $\{f \in \mathbb{F}[C] |\ f(P) = 0\} = \{f \in \mathbb{F}[C] |\ f(Q) = 0\}$, quindi se e solo se $(P) = (Q)$.
Si definisce allora il **grado** di (P) come

$$\deg(P) = \#\{Q \in C(\overline{\mathbb{F}}) |\ Q, P \text{ sono coniugati}\} = \#\{Q \in C(\overline{\mathbb{F}}) |\ (P) = (Q)\}$$

Osservazione 1.4.1.
Sia $P = [p_0, \dots, p_N] \in C(\overline{\mathbb{F}})$, con $\mathbb{F} = \mathbb{F}_q$.
$P \in C(\mathbb{F}_{q^m}) \setminus \bigcup_{d|m\ d \neq m} C(\mathbb{F}_{q^d}) \ \Leftrightarrow\ p_0, \dots, p_N \in \mathbb{F}_{q^m}, \exists i$ tale che $p_i = 1, \exists j$ tale che $p_j \notin F_{q^d}$ per $d < m$.
Sia $\psi :\ Gal(\overline{\mathbb{F}} : \mathbb{F}) \to C(\overline{\mathbb{F}})$ l'applicazione definita da $\psi(\sigma) = \sigma P$.
Certamente $\sigma(\mathbb{F}_{q^m}) \subseteq \mathbb{F}_{q^m}$, cioè $\sigma_{|\mathbb{F}_{q^m}} \in Gal(\mathbb{F}_{q^m} : \mathbb{F}_q)$. D'altra parte, poiché $p_j \in \mathbb{F}_{q^m} \setminus \bigcup_{d|m\ d \neq m} \mathbb{F}_{q^d}$, $\sigma(p_j) \neq \tau(p_j)\ \forall \sigma, \tau \in Gal(\mathbb{F}_{q^m} : \mathbb{F}_q)$ con $\sigma \neq \tau$.
Dunque $|\text{Im }(\psi)| = |Gal(\mathbb{F}_{q^m} : \mathbb{F}_q)| = m$.
Allora $\deg(P) = m$ se e solo se $P \in C(\mathbb{F}_{q^m}) \setminus \bigcup_{d|m\ d \neq m} C(\mathbb{F}_{q^d})$.

Sia $\nu_m(C) = \#C(\mathbb{F}_{q^m})$, allora $\nu_m(C) = \sum_{d|m} \#\Big(C(\mathbb{F}_{q^d}) \setminus \bigcup_{k|m\ k \neq d} C(\mathbb{F}_{q^k})\Big) =$
$= \sum_{d|m} \#\{P \in C(\overline{\mathbb{F}}) |\ \deg(P) = d\}$.
Ponendo $a_d = \#\{(P) \in S_{\mathbb{K}} |\ \deg(P) = d\}$ quindi si ha che

$$\nu_m(C) = \sum_{d|m} d a_d \tag{1.10}$$

In particolare dunque i punti $\mathbb{F}$-razionali di C sono in corrispondenza biunivoca con i divisori primi di $\mathbb{K}$ di grado 1.

Definizione 1.4.2.
Si definisce il **gruppo dei divisori** di $\mathbb{K}$, $\mathrm{Div}(\mathbb{K})$, come il gruppo abeliano libero generato dai divisori primi di $\mathbb{K}$, cioè come

$$\mathbf{Div(\mathbb{K})} = \left\{ \sum_{P \in S_{\mathbb{K}}} \alpha_P(P) \,\middle|\, \alpha_P \in \mathbb{Z} \ \forall P \text{ e } \#\{P | \alpha_P \neq 0\} < \infty \right\}$$

Se $D = \sum_P \alpha_P(P)$ è un divisore di $\mathbb{K}$ si definisce il **grado** di D come

$$\mathbf{deg\,(\boldsymbol{D})} = \sum_P \alpha_P \deg(P)$$

Il nucleo dell'omomorfismo $\deg : \mathrm{Div}(\mathbb{K}) \to \mathbb{Z}$ è notato $\mathbf{Div^0(\mathbb{K})}$.

Definizione 1.4.3.
Sia $f \in \mathbb{K}$, si definisce il divisore di f come

$$\boldsymbol{(f)} = \sum_{P \in S_{\mathbb{K}}} \mathrm{ord}_P f(P)$$

(f) è ben definito perché se P, Q sono coniugati $\mathrm{ord}_P f = \mathrm{ord}_Q f \ \forall f \in \mathbb{K}$; inoltre, poiché f ha un numero finito di zeri e di poli, effettivamente $(f) \in \mathrm{Div}(\mathbb{K})$.
Il gruppo $\mathbf{\mathscr{P}(\mathbb{K})} = \{(f) | \ f \in \mathbb{K}\}$ è detto il gruppo dei **divisori principali** di $\mathbb{K}$; $\mathscr{P}(\mathbb{K})$ è effettivamente un sottogruppo di $\mathrm{Div}(\mathbb{K})$ perché se $f, g \in \mathbb{K}$ si ha $(f) + (g) = (fg)$.

Proposizione 1.4.2. [1]
Sia $f \in \mathbb{K}^*$, *allora* $\deg(f) = 0$. *Inoltre,* $(f) = 0 \Leftrightarrow f \in \mathbb{F}^*$.

Definizione 1.4.4.
Siano $D_1, D_2 \in \mathrm{Div}(\mathbb{K})$, si dice che D_1, D_2 sono **linearmente equivalenti** (e si nota $D_1 \sim D_2$) se $D_1 - D_2 = (f)$, con $f \in \mathbb{K}^*$.
Si definisce il gruppo delle classi di divisori come

$$\boldsymbol{Cl(\mathbb{K})} = \mathrm{Div}(\mathbb{K}) / \mathscr{P}(\mathbb{K})$$

[1] Si può trovare la dimostrazione in Silverman [12]

Poiché per la proposizione precedente $\mathscr{P}(\mathbb{K}) \subseteq \mathrm{Div}^0(\mathbb{K})$, ha senso parlare di grado di una classe di divisori, cioè l'omomorfismo deg passa al quoziente inducendo un omomorfismo da $Cl(\mathbb{K})$ in $\mathbb{Z}$; il suo nucleo è notato $Cl^0(\mathbb{K})$.

Definizione 1.4.5.
Un divisore $D = \sum_P \alpha_P(P)$ è detto **positivo**, o effettivo, se $\alpha_P \geq 0 \ \forall P$.
In questo caso si scrive $D \geq 0$.

Definizione 1.4.6.
Sia $D \in \mathrm{Div}(\mathbb{K})$, si definisce

$$\boldsymbol{L(D)} = \{f \in \mathbb{K}^* |\ (f) + D \geq 0\} \cup \{0\}$$

Si può dimostrare che allora $L(D)$ è un $\mathbb{F}$-spazio vettoriale di dimensione finita[2]; si nota inoltre

$$\boldsymbol{\ell(D)} = \dim_{\mathbb{F}} L(D)$$

Lemma 1.4.3.
Siano $A, B \in \mathrm{Div}(\mathbb{K})$. Se $A \sim B$ allora $L(A), L(B)$ sono isomorfi.
In particolare allora in questo caso $\ell(A) = \ell(B)$, cioè $\ell(A)$ dipende solo dalla classe di A.

Dimostrazione.
Sia $h \in \mathbb{K}^*$ tale che $A = B + (h)$, allora l'applicazione $\psi : L(A) \to L(B)$ data da $\psi(f) = fh$ è ben definita ed è un isomorfismo di $\mathbb{F}$-spazi vettoriali. □

Lemma 1.4.4.
Sia $D \in \mathrm{Div}(\mathbb{K})$. Se $\deg(D) \leq 0$ e $D \not\sim 0$ allora $\ell(D) = 0$; se $D \sim 0$ allora $\ell(D) = 1$.

Dimostrazione.
Sia $D \in \mathrm{Div}(\mathbb{K})$ tale che $\deg(D) < 0$. Se esistesse $f \in L(D)$, $f \neq 0$, si dovrebbe avere $0 \leq \deg((f) + D) = \deg(f) + \deg(D) < 0$, assurdo. Quindi $L(D) = \{0\}$, cioè $\ell(D) = 0$.

[2]Si può trovare la dimostrazione in Silverman [12] o in Rosen [9]

Sia $D \in \mathrm{Div}(\mathbb{K})$ tale che $\deg(D) = 0$ e $L(D) \neq \{0\}$. Sia $f \in L(D),\ f \neq 0$. Per definizione allora $(f) + D \geq 0$. D'altra parte, $\deg((f) + D) = 0$, quindi si deve avere $(f) + D = 0$, cioè $D \sim 0$.
Se $D \sim 0$ per il lemma precedente $L(D) \simeq L(0) = \mathbb{F}$, cioè $\ell(D) = 1$. □

Teorema 1.4.5. Teorema di Riemann-Roch[3]
Nelle notazioni precedenti si ha che esistono e sono unici $g \in \mathbb{N}$ *e* $\mathscr{C} \in Cl(\mathbb{K})$ *tali che* $\forall D \in \mathrm{Div}(\mathbb{K}),\ \forall K \in \mathscr{C}$ *vale*

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1$$

Si dice allora che g *è il* ***genere*** *di* C *e che* $\mathscr{C}$ *è la sua* ***classe canonica****.*

Corollario 1.4.6.

1. $\forall K \in \mathscr{C}$ *si ha che* $\ell(K) = g$ *e* $\deg(K) = 2g - 2$.

2. $\forall D \in \mathrm{Div}(\mathbb{K})$ *si ha che* $\ell(D) \geq \deg(D) - g + 1$ *(disuguaglianza di Riemann). Inoltre se* $\deg(D) > 2g - 2$ *o se* $\deg(D) = 2g - 2$ *e* $D \notin \mathscr{C}$*, allora* $\ell(D) = \deg(D) - g + 1$.

Dimostrazione.

1. Prendendo $D = 0$ il Teorema di Riemann-Roch diventa
   $1 - \ell(K) = 0 - g + 1$, quindi $\ell(K) = g$.
   Prendendo $D = K \in \mathscr{C}$ il Teorema di Riemann-Roch diventa
   $\ell(K) - 1 = \deg(K) - g + 1$, quindi $\deg(K) = 2g - 2$.

2. Certamente $\forall D$ si ha $\ell(D) \geq \ell(D) - \ell(K - D) = \deg(D) - g + 1$.
   Se $\deg(D) \geq 2g - 2$ e $D \notin \mathscr{C}$, allora $\deg(K - D) \leq 0$ e $K - D \not\sim 0$, quindi per il lemma 1.4.4 $\ell(K - D) = 0$, quindi $\ell(D) = \deg(D) - g + 1$.

□

[3]Si può trovare la dimostrazione in Rosen [9]

Osservazione 1.4.7.
Si può dimostrare che esistono sempre divisori di grado 1[4]. Si ha allora che la successione $\{0\} \to Cl^0(\mathbb{K}) \hookrightarrow Cl(\mathbb{K}) \xrightarrow{\deg} \mathbb{Z} \to \{0\}$ è una successione esatta. Vedremo che $Cl^0(\mathbb{K})$ è un gruppo finito; $h = |Cl^0(\mathbb{K})|$ è detto il **numero di classi** di C. In particolare $\forall n \in \mathbb{Z}$ si ha che

$$h = \#\{\overline{D} \in Cl(\mathbb{K}) |\ \deg \overline{D} = n\} \tag{1.11}$$

Definizione 1.4.7.
Come nell'osservazione 1.4.1, poniamo

$$\boldsymbol{a_n} = \#\{(P) \in S_{\mathbb{K}} | \deg(P) = n\}$$

Poniamo inoltre

$$\boldsymbol{b_n} = \#\{D \in \mathrm{Div}(\mathbb{K}) |\ \deg(D) = n,\ D \geq 0\}$$

Lemma 1.4.8.
$b_n < \infty\ \forall n \in \mathbb{N}$.

Dimostrazione.
Sia $D = \sum \alpha_P(P) \geq 0$ tale che $\deg(D) \leq n$. Se P è tale che $\alpha_P \neq 0$ si deve avere $\deg(P) \leq n$, cioè $P \in C(\mathbb{F}_{q^m})$ con $m \leq n$. Poiché $\#C(\mathbb{F}_{q^m}) < \infty\ \forall m$, solo un numero finito dei primi P può avere un coefficiente α_P non nullo. Inoltre, $0 \leq \alpha_P \leq n\ \forall P$, quindi i divisori positivi D tali che $\deg(D) \leq n$ sono in numero finito, quindi in particolare b_n è finito. □

Lemma 1.4.9.
$h = |Cl^0(\mathbb{K})| \leq b_g$, con g genere di C. In particolare quindi $h < \infty$.

Dimostrazione.
Sia $D \in \mathrm{Div}(\mathbb{K})$ fissato tale che $\deg(D) = 1$, sia $A \in \mathrm{Div}^0(\mathbb{K})$. Allora $\deg(gD + A) = g$, quindi per la disuguaglianza di Riemann (corollario 1.4.6) $\ell(gD + A) \geq 1$, cioè esiste $f \in L(gD + A),\ f \neq 0$. Sia $B = (f) + gD + A$,

[4]Si può trovare la dimostrazione in Schmidt [10]

allora $A \sim B - gD$, con $B \geq 0$ e $\deg(B) = g$. Abbiamo quindi costruito un'applicazione iniettiva tra $Cl^0(\mathbb{K})$ e $\{B \in \mathrm{Div}(\mathbb{K})|\ B \geq 0,\ \deg B = g\}$, quindi $h = |Cl^0(\mathbb{K})| \leq \#\{B \in \mathrm{Div}(\mathbb{K})|\ B \geq 0,\ \deg B = g\} = b_g$. □

Lemma 1.4.10.
Sia $A \in \mathrm{Div}(\mathbb{K})$, allora $\#\{D \in \overline{A}|\ D \geq 0\} = \dfrac{q^{\ell(A)} - 1}{q - 1}$, con $\overline{A}$ classe di A in $Cl(\mathbb{K})$.

Dimostrazione.
$\{D \in \overline{A}|\ D \geq 0\} \neq \emptyset \Leftrightarrow \exists f \in \mathbb{K}^*$ tale che $(f) + A \geq 0 \Leftrightarrow \ell(A) > 0$.
Per $\ell(A) = 0$ quindi si ha $\#\{D \in \overline{A}|\ D \geq 0\} = 0 = \frac{q^0 - 1}{q-1}$.
Supponiamo $\ell(A) > 0$. La mappa $\psi : L(A) \setminus \{0\} \to \{D \in \overline{A}|\ D \geq 0\}$ definita da $\psi(f) = A + (f)$ è certamente suriettiva. Inoltre $\psi(f) = \psi(f') \Leftrightarrow (f) + A = (f') + A \Leftrightarrow (f) = (f') \Leftrightarrow f'f^{-1} \in \mathbb{F}^*$.
Allora $\#\{D \in \overline{A}|\ D \geq 0\} = |\mathrm{Im}\ (\psi)| = \dfrac{\#\big(L(A) \setminus \{0\}\big)}{|\mathbb{F}^*|} = \dfrac{q^{\ell(A)} - 1}{q - 1}$. □

Lemma 1.4.11.
Sia $n \in \mathbb{N}$, per (1.11) si ha che $\#\{\overline{D} \in Cl(\mathbb{K})|\ deg\overline{D} = n\} = h$.
Sia $\{\overline{D} \in Cl(\mathbb{K})|\ deg\overline{D} = n\} = \{D_1, \ldots . D_h\}$, allora

$$b_n = \sum_{i=1}^{h} \frac{q^{l(D_i)} - 1}{q - 1} \tag{1.12}$$

Dimostrazione.
$b_n = \#\{D \in \mathrm{Div}(\mathbb{K})|\ D \geq 0,\ \deg(D) = n\} = \sum_{i=1}^{h} \#\{D \in \overline{D_i}|\ D \geq 0\} =$
$= \sum_{i=1}^{h} \dfrac{q^{l(D_i)} - 1}{q - 1}$ per il lemma precedente. □

Definizione 1.4.8.
Per $A \in \mathrm{Div}(\mathbb{K})$ si definisce la **norma** di A come

$$\boldsymbol{N(A)} = q^{\deg(A)}$$

Osservazione 1.4.12.
Siano $A, B \in \mathrm{Div}(\mathbb{K})$, allora $N(A+B) = N(A)N(B)$.
Inoltre, $N(A)$ dipende solo dalla classe di A, cioè ha senso considerare $N(\overline{A})$ per $\overline{A} \in Cl(\mathbb{K})$.

Definizione 1.4.9.
Si definisce la **funzione zeta** di $\mathbb{K}$ come

$$\boldsymbol{\zeta(s)} = \sum_{A \geq 0} N(A)^{-s}$$

Osservazione 1.4.13.
Poiché $N(A)^{-s} = q^{-ns} \Leftrightarrow \deg(A) = n$, formalmente $\zeta(s) = \sum_{n=0}^{\infty} \frac{b_n}{q^{ns}}$.
D'altra parte, per la moltiplicatività della norma si ha formalmente che

$$\zeta(s) = \prod_{P} (1 - N(P)^{-s})^{-1} = \prod_{n=1}^{\infty} (1 - q^{-ns})^{-a_n} \tag{1.13}$$

Nelle notazione del lemma 1.4.11, se $n > 2g-2$ per 1.4.6 si ha che $\ell(D_i) = n - g + 1 \ \forall i$, quindi, per (1.12), $b_n = h\dfrac{q^{n-g+1}-1}{q-1} = O(q^n)$, quindi $\sum b_n q^{-ns}$ converge assolutamente per $\mathrm{Re}(s) > 1$ e definisce una funzione analitica in questa regione.
Si può dimostrare analogamente che anche $\prod (1 - q^{-ns})^{-a_n}$ converge assolutamente per $\mathrm{Re}(s) > 1$ e definisce una funzione analitica in questa regione.

Teorema 1.4.14.
Nelle ipotesi e nelle notazioni precedenti si ha che esiste un polinomio $L(u) \in \mathbb{Z}[u]$ *con* $\deg L = 2g$ *tale che*

$$\zeta(s) = \frac{L(q^{-s})}{(1-q^{-s})(1-q^{1-s})} \quad \textit{su } \{s \in \mathbb{C} |\ \mathrm{Re}(s) > 1\} \tag{1.14}$$

Questa uguaglianza dà quindi un prolungamento di $\zeta(s)$ *a tutto* $\mathbb{C}$ *come funzione meromorfa, con poli semplici in* $s = 0$ *e* $s = 1$.
Si ha inoltre che $L(0) = 1,\ L(1) = h,\ L'(0) = a_1 - 1 - q$.
Sia inoltre $\xi(s) = q^{(g-1)s}\zeta(s)$, *allora*

$$\xi(s) = \xi(1-s)\ \forall s \in \mathbb{C}\ (\textit{equazione funzionale per } \zeta) \tag{1.15}$$

Dimostrazione.
Consideriamo la variabile $u = q^{-s}$; certamente se $\mathrm{Re}(s) > 1$ allora $|u| < 1$.
Sia $Z(u) = \zeta(s)$, allora $Z(u) = \sum_{n=0}^{\infty} b_n u^n$, quindi, per quanto visto nell'osservazione precedente, $Z(u) = \sum_{n=0}^{2g-2} b_n u^n + \sum_{n=2g-1}^{\infty} h\frac{q^{n-g+1}-1}{q-1}u^n =$
$= \sum_{n=0}^{2g-2} b_n u^n + \frac{h}{q-1}\left(\frac{q^g}{1-qu} - \frac{1}{1-u}\right)u^{2g-1}$.
Ponendo $L(u) = \sum_{n=0}^{2g-2} b_n u^n (1-qu)(1-u) + h\left(\frac{q^g-1}{q-1} - \frac{q^g-q}{q-1}u\right)u^{2g-1}$
(certamente allora $L(u) \in \mathbb{Z}[u]$ e $\deg L \leq 2g$) si ha che $Z(u) = \frac{L(u)}{(1-qu)(1-u)}$,
cioè che $\zeta(s) = \frac{L(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$.

Dall'osservazione 1.4.13 segue che se $g = 0$ necessariamente $h = 1$.
In questo caso allora si ha $L(u) = 1$, quindi in particolare $\deg L = 2g$,
$L(0) = 1, L(1) = h$ e $a_1 - 1 - q = b_1 - 1 - q = \frac{q^2-1}{q-1} - 1 - q = 0 = L'(0)$.
Inoltre, $\xi(s) = \frac{q^{-s}}{(1-q^{-s})(1-q^{1-s})}$, quindi $\xi(1-s) = \frac{q^{-1+s}}{(1-q^{-1+s})(1-q^s)} =$
$= \frac{q^{-1+s}}{q^{-1+s}(q^{1-s}-1)q^s(q^{-s}-1)} = \xi(s)$.

Supponiamo ora $g > 0$.
Certamente allora si ha che $L(0) = b_0 = 1$.
Confrontando i coefficienti di u inoltre si ottiene che $b_1 = Z'(u)\big|_{u=0} = L'(0) +$
$+ L(0) + L(0)q$, quindi $L'(0) = b_1 - q - 1 = a_1 - q - 1$.
Ora, $\lim_{u\to 1}(u-1)Z(u) = \lim_{u\to 1}\left(\sum_{n=0}^{2g-2} b_n u^n (u-1) + \frac{h}{q-1}\left(\frac{q^g}{1-qu}(u-1)+1\right)u^{2g-1}\right) =$
$= \frac{h}{q-1}$. D'altra parte, $\lim_{u\to 1}(u-1)Z(u) = \lim_{u\to 1}\frac{L(u)}{qu-1} = \frac{L(1)}{q-1}$, quindi si deve avere $L(1) = h$.
Per (1.12), $b_n = \sum_{\deg(\overline{D})=n} \frac{q^{\ell(\overline{D})}-1}{q-1}$ $\forall n \in \mathbb{N}$. Allora $(q-1)u^{1-g}Z(u) =$

$$= \sum_{n=0}^{2g-2} \left(\sum_{\deg(\overline{D})=n} q^{\ell(\overline{D})} - 1 \right) u^{n+1-g} + h \left(\frac{q^g}{1-qu} - \frac{1}{1-u} \right) u^g = R(u) + S(u),$$

con $R(u) = \sum_{\deg(\overline{D})\leq 2g-2} q^{\ell(\overline{D})} u^{\deg(\overline{D})+1-g}$, $S(u) = -h\frac{u^{1-g}}{1-u} + h\frac{q^g u^g}{1-qu}$.

$S(u)$ è invariante rispetto alla trasformazione $u \mapsto q^{-1}u^{-1}$. Infatti $S(q^{-1}u^{-1}) =$

$$= -h\frac{q^{-1+g}u^{-1+g}}{1-q^{-1}u^{-1}} + h\frac{u^{-g}}{1-u^{-1}} = S(u).$$

Proviamo che anche $R(u)$ è invariante rispetto a questa trasformazione. Per come è stato definito R, $R(q^{-1}u^{-1}) = \sum_{\deg(\overline{D})\leq 2g-2} q^{\ell(\overline{D})-\deg(\overline{D})+g-1} u^{-\deg(\overline{D})+g-1}$.

Per il teorema di Riemann-Roch, $\ell(\mathscr{C} - \overline{D}) = g - 1 - \deg(\overline{D}) + \ell(\overline{D})$, con $\mathscr{C}$ classe canonica di C, quindi $R(q^{-1}u^{-1}) = \sum_{\deg(\overline{D})\leq 2g-2} q^{\ell(\mathscr{C}-\overline{D})} u^{\deg(\mathscr{C}-\overline{D})-g+1}$.

Poiché l'applicazione $\overline{D} \mapsto \mathscr{C} - \overline{D}$ è una permutazione di $\{\overline{D} \in Cl(\mathbb{K}) |\ \deg(\overline{D}) \leq 2g-2\}$, si ha che $R(q^{-1}u^{-1}) = R(u)$.

Allora $(q-1)u^{1-g}Z(u)$ è invariante rispetto alla trasformazione $u \mapsto q^{-1}u^{-1}$, quindi lo è anche $u^{1-g}Z(u)$, cioè $q^{(g-1)s}\zeta(s) = \xi(s)$ è invariante rispetto alla trasformazione $q^{-s} \mapsto q^{-1+s}$, cioè rispetto alla trasformazione $s \mapsto 1-s$.

Inoltre, $u^{1-g}Z(u) = (q^{-1}u^{-1})^{1-g}Z(q^{-1}u^{-1}) \ \Rightarrow\ L(q^{-1}u^{-1}) =$

$$= \frac{u^{1-g}L(u)}{(1-qu)(1-u)} q^{1-g}u^{1-g}(1-u^{-1})(1-q^{-1}u^{-1}) = q^{-g}u^{-2g}L(u).$$

Quindi $1 = L(0) = \lim_{u\to\infty} L(q^{-1}u^{-1}) = \lim_{u\to\infty} q^{-g}u^{-2g}L(u)$, quindi $L(u)$ deve essere un polinomio di grado esattamente $2g$ e di coefficiente direttore q^{-g}.

Abbiamo già visto che $L(1) = h \neq 0$, inoltre $L(q^{-1}) = q^{-g}L(1) \neq 0$.

Allora $\zeta(s)$ ha effettivamente due poli (semplici), per $s = 0$ e per $s = 1$. □

Osservazione 1.4.15.

Siano $\omega_1, \ldots, \omega_{2g} \in \mathbb{C}$ interi algebrici tali che

$$L(u) = \prod_{i=1}^{2g} (1 - \omega_i u) \tag{1.16}$$

Poiché $L(q^{-1}u^{-1}) = q^{-g}u^{-2g}L(u)$, l'applicazione $\omega_i \mapsto \frac{q}{\omega_i}$ è una permutazione dell'insieme $\{\omega_1, \ldots, \omega_{2g}\}$. Ordinando opportunamente gli ω_i quindi si ha che

$$\omega_i\omega_{2g-i} = q \ \forall i \text{ (equazione funzionale)} \tag{1.17}$$

Osservazione 1.4.16.
Abbiamo visto che $Z(u) = \dfrac{\prod_{i=1}^{2g}(1-\omega_i u)}{(1-u)(1-qu)}$ e che $Z(u) = \prod_{d=1}^{\infty}(1-u^d)^{-a_d}$. Passando alla derivata logaritmica e moltiplicando per u le due espressioni precedenti si ha che $\sum_{i=1}^{2g} \dfrac{-\omega_i}{1-\omega_i u} + \dfrac{u}{1-u} + \dfrac{qu}{1-qu} = \sum_{d=1}^{\infty} \dfrac{da_d u^d}{1-u^d}$, quindi che $\sum_{n=1}^{\infty}\left(\sum_{i=1}^{2g} -\omega_i^n + 1 + q^n\right)u^n = \sum_{n,d=1}^{\infty} da_d u^{nd}$. Confrontando i coefficienti di u^m quindi si ha che $-\sum_{i=1}^{2g}\omega_i^m + 1 + q^m = \sum_{d|m} da_d$, cioè, per (1.10) che

$$\nu_m(C) = -\sum_{i=1}^{2g}\omega_i^m + 1 + q^m \tag{1.18}$$

con $\nu_m(C)$ numero dei punti di C definiti su $\mathbb{F}_{q^m}$.

1.4.2 Teorema di Weil

Sia C una curva proiettiva non singolare definita su un campo finito $\mathbb{F} = \mathbb{F}_q$, con $q = p^\alpha$, p primo. Per $m \geq 1$, sia $\nu_m(C)$ il numero dei punti $\mathbb{F}_{q^m}$-razionali di C, cioè sia $\nu_m(C) = \#C(\mathbb{F}_{q^m})$.
Abbiamo visto che $\nu_m(C) = q^m - \sum_{i=1}^{2g}\omega_i^m + 1$, dove gli ω_i sono interi algebrici indipendenti da m tali che $\omega_i\omega_{2g-i} = q$ (osservazioni 1.4.16,1.4.15).

Teorema 1.4.17. Teorema di Weil

$$|\nu_m(C) - q^m - 1| \leq 2gq^{\frac{m}{2}} \tag{1.19}$$

Questo risultato è stato congetturato da Artin nel caso iperellittico nel 1924, poi provato nel caso ellittico (cioè per $g = 1$) da Hasse nel 1936. Weil nel

1940 ne ha dato per la prima volta una dimostrazione generale, facendo però uso di metodi avanzati di geometria algebrica. Dimostrazioni più elementari sono poi state date da Stepanov, per casi particolari, e da Schmidt e Bombieri nel caso generale. Seguiremo l'impostazione data da Bombieri in [2].

Osservazione 1.4.18.
Poiché si può dimostrare che le coniche non degeneri sono curve di genere 0 e che le cubiche hanno genere 1, il corollario 1.2.5 e l'osservazione 1.3.5 in effetti sono casi particolari del Teorema di Weil.
Infatti se C è una curva di genere 0 la formula (1.19) diventa $|\nu_m(C) - q^m - 1| \leq 0$, quindi in particolare si ha che $\#C(\mathbb{F}_q) = \nu_1(C) = q+1$.
Analogamente, se C è una curva di genere 1 definita su $\mathbb{F}_p$, allora (1.19) diventa $|\nu_m(C) - p^m - 1| \leq 2p^{\frac{m}{2}}$, quindi in particolare $|\#C(\mathbb{F}_p) - p - 1| = |\nu_1(C) - p - 1| \leq 2\sqrt{p}$.

Osservazione 1.4.19.
il precedente Teorema è equivalente alla cosiddetta **ipotesi di Riemann per campi di funzioni**

$$|\omega_i| = q^{\frac{1}{2}} \ \forall i \tag{1.20}$$

Infatti certamente $|\omega_i| = q^{\frac{1}{2}} \ \Rightarrow \ |\nu_m(C) - q^m - 1| = \left| \sum_{i=1}^{2g} \omega_i^m \right| \leq 2gq^{\frac{m}{2}}$.

D'altra parte, $|\nu_m(C) - q^m - 1| \leq 2gq^{\frac{m}{2}} \ \forall m \ \Rightarrow \ \left| \sum_{i=1}^{2g} \omega_i^m \right| \leq 2gq^{\frac{m}{2}} \ \forall m \ \Rightarrow$ $|\omega_i| \leq q^{\frac{1}{2}} \ \forall i$. Poiché $\omega_i \omega_{2g-i} = q \ \forall i$ si deve avere $|\omega_i| = q^{\frac{1}{2}} \ \forall i$.
In effetti, è sufficiente provare che $\sum \omega_i^m = O(q^{\frac{m}{2}})$ per un'infinità di m, o equivalentemente che $\nu_m(C) = q + O(q^{\frac{m}{2}})$ per un'infinità di m.
A sua volta, questo è equivalente a provare che $\nu_1(C) = q + O\left(q^{\frac{1}{2}}\right)$ dopo avere eventualmente sostituito $\mathbb{F}_q$ con una sua estensione finita $\mathbb{F}_{q^m}$, con m sufficientemente grande.

Osservazione 1.4.20.
Sia $\varphi : C(\overline{\mathbb{F}}) \to C(\overline{\mathbb{F}})$ il morfismo di Frobenius $\big($se $P = [p_0, \ldots, p_N] \in C(\overline{\mathbb{F}})$, $\varphi(P) = [p_0^q, \ldots, p_N^q]\big)$.

Allora $\varphi(P) = P \Leftrightarrow P \in C(\mathbb{F})$, cioè $\nu_1(\mathbb{F}) = \#\{P \in C(\overline{\mathbb{F}})|\ \varphi(P) = P\}$.
Analogamente, $\nu_m(C) = \#\{P \in C(\overline{\mathbb{F}})|\ \varphi^m(P) = P\}$.

Teorema 1.4.21.
Se $q = p^\alpha$ con α pari e se $q > (g+1)^4$, allora

$$\nu_1(C) < q + (2g+1)q^{\frac{1}{2}} + 1$$

Osservazione 1.4.22.
Possiamo supporre che φ abbia almeno un punto fisso, P_0 (in caso contrario infatti $\nu_1 = 0$, non c'è nulla da dimostrare).
Consideriamo il gruppo dei divisori di $\overline{\mathbb{K}} = \overline{\mathbb{F}}(C)$.
Per $m \in \mathbb{N}$, sia $R_m = L(m(P_0)) = \{f \in \overline{\mathbb{K}}|\ (f) + m(P_0) \geq 0\}$; si può dimostrare che R_m è un $\overline{\mathbb{F}}$-spazio vettoriale di dimensione finita, sia $\ell_m = \dim_{\overline{\mathbb{F}}} R_m$.
Se A, B sono sottospazi vettoriali, rispettivamente, di R_m, R_n, notiamo AB il sottospazio vettoriale di R_{n+m} generato da $\{fg|\ f \in A, g \in B\}$ (questa definizione è ben posta perché $f \in R_m, g \in R_n \Rightarrow (fg) - (m+n)(P_0) =$
$= (f) + (g) - m(P_0) - n(P_0) \geq 0 \ \Rightarrow fg \in R_{n+m}$).
Notiamo inoltre $R_l^{(p^\mu)} = \{f^{p^\mu}|\ f \in R_l\}$; $R_l^{(p^\mu)}$ è dunque un sottospazio di R_{lp^μ}.

Lemma 1.4.23.
Nelle ipotesi e nelle notazioni precedenti si ha che:

1. $\ell_m \leq \ell_{m+1} \leq \ell_m + 1$
2. $\ell_m \leq m + 1$
3. $\ell_m \geq m + 1 - g$ *e se* $m > 2g - 2$ *allora* $\ell_m = m + 1 - g$
4. $R_m \circ \varphi \subseteq R_{mq}$
5. *Ogni elemento* $f \circ \varphi$ *di* $R_m \circ \varphi$ *è una potenza q-esima e si ha che* $(f \circ \varphi) = \sum_P q\ \mathrm{ord}_{\varphi(P)} f(P)$
6. $\dim R_l^{(p^\mu)} = \ell_l$

7. $\dim(R_m \circ \varphi) = \ell_m$

Dimostrazione.

1. Certamente $R_m \subseteq R_{m+1}$, quindi $\ell_m \leq \ell_{m+1}$.
   Per il Teorema di Riemann-Roch, se $K \in \mathscr{C}$, con $\mathscr{C}$ classe canonica di C, $\ell_{m+1} = \ell(K-(m+1)(P_0))+m+1-g+1$ e $\ell_m = \ell(K-m(P_0))+m-g+1$, quindi $\ell_{m+1} \leq \ell_m + 1 \Leftrightarrow \ell(K-(m+1)(P_0)) \leq \ell(K-m(P_0))$, certamente vero perché $L(K-(m+1)(P_0)) \subseteq L(K-m(P_0))$.

2. Per $m = 0$ si ha $R_0 = \{f \in \overline{\mathbb{K}} |\ (f) \geq 0\} = \overline{\mathbb{F}}$, cioè $\ell_0 = 1$. Per quanto provato al punto 1. allora per induzione si ha che $\ell_m \leq m+1\ \forall m$.

3. Segue immediatamente dal corollario 1.4.6.

4.-5. Si può provare[5] che $(f \circ \varphi) = q \sum_P \mathrm{ord}_{\varphi(P)} f(P)$. Se $f \in R_m$ dunque $(f \circ \varphi) + mq(P_0) \geq 0$, cioè $f \circ \varphi \in R_{mq}$.
   Sia $g \in \overline{\mathbb{K}}$ tale che $\varphi g = f$, dove φ agisce sui coefficienti di g (g esiste certamente perché φ è iniettivo e suriettivo), allora $f \circ \varphi = g^q$.

6. Sia $\{f_1, \ldots, f_n\}$ una base di R_l, allora $R_l^{(p^\mu)}$ è generato da $\{f_1^{p^\mu}, \ldots, f_n^{p^\mu}\}$. Si prova facilmente che se questi fossero linearmente dipendenti anche $f_1, \ldots, f_n$ lo sarebbero, assurdo. Quindi $\{f_1^{p^\mu}, \ldots, f_n^{p^\mu}\}$ deve essere una base per $R_l^{(p^\mu)}$, quindi $\dim R_l^{(p^\mu)} = \ell_l$.

7. Sia $\{f_1, \ldots, f_n\}$ una base di R_m, allora $R_m \circ \varphi$ è generato da $\{f_1 \circ \varphi, \ldots, f_n \circ \varphi\}$. Come nel caso precedente, se questi fossero linearmente dipendenti anche $f_1, \ldots, f_n$ lo sarebbero, assurdo.
   Quindi $\{f_1 \circ \varphi, \ldots, f_n \circ \varphi\}$ deve essere una base per $R_m \circ \varphi$, quindi $\dim R_m \circ \varphi = \ell_m$.

□

Lemma 1.4.24.
Se $lp^\mu < q$, l'omomorfismo naturale $\delta : R_l^{(p^\mu)} \otimes_{\overline{\mathbb{F}}} (R_m \circ \varphi) \to R_l^{(p^\mu)}(R_m \circ \varphi)$ è un isomorfismo.

[5] Si può trovare la dimostrazione in Silverman [12]

Dimostrazione.
Per $f \in \overline{\mathbb{K}}$ notiamo $\mathrm{ord} f = \mathrm{ord}_{P_0} f$.
In particolare allora allora $f \in R_m \Rightarrow \mathrm{ord} f \geq -m$.
Per il punto 1. del lemma precedente esiste una base $\{s_1, \dots s_r\}$ di R_m tale che $\mathrm{ord} s_i < \mathrm{ord} s_{i+1}\ \forall i$. Abbiamo visto che allora $\{s_1 \circ \varphi, \dots, s_r \circ \varphi\}$ è una base di $R_m \circ \varphi$.
Certamente δ è un omomorfismo suriettivo, quindi per provare che è un isomorfismo è sufficiente provare che è iniettivo, cioè che se $\sigma_1, \dots, \sigma_r \in R_l$ sono tali che $\sum_{i=1}^{r} \sigma_i^{p^\mu}(s_i \circ \varphi) = 0$, allora necessariamente $\sigma_1 = \cdots = \sigma_r = 0$.
Supponiamo per assurdo che esistano $\sigma_1, \dots, \sigma_r \in R_l$, non tutti nulli, tali che $\sum_{i=1}^{r} \sigma_i^{p^\mu}(s_i \circ \varphi) = 0$.

Sia ρ il minimo indice tale che $\sigma_\rho \neq 0$, allora $\sum_{i=\rho}^{r} \sigma_i^{p^\mu}(s_i \circ \varphi) = 0$.

Ora, $\mathrm{ord}(\sigma_\rho^{p^\mu}(s_\rho \circ \varphi)) = \mathrm{ord}\left(-\sum_{i=\rho+1}^{r} \sigma_i^{p^\mu}(s_i \circ \varphi)\right) \geq \min_{i>\rho} \mathrm{ord}\left(\sigma_i^{p^\mu}(s_i \circ \varphi)\right) \geq$
$\geq l p^\mu + q\ \mathrm{ord} s_{\rho+1}$, infatti $\mathrm{ord}\left(\sigma_i^{p^\mu}(s_i \circ \varphi)\right) = \mathrm{ord}\left(\sigma_i^{p^\mu}\right) + \mathrm{ord}(s_i \circ \varphi) =$
$= p^\mu \mathrm{ord}(\sigma_i) + q\ \mathrm{ord}(s_i) \geq -l p^\mu + q\ \mathrm{ord}(s_{\rho+1})$.
D'altra parte, $\mathrm{ord}\left(\sigma_\rho^{p^\mu}(s_\rho \circ \varphi)\right) = p^\mu \mathrm{ord}(\sigma_\rho) + q \mathrm{ord}(s_\rho)$.
Allora $p^\mu \mathrm{ord}(\sigma_\rho) \geq -l p^\mu + q\big(\mathrm{ord}(s_{\rho+1}) - \mathrm{ord}(s_\rho)\big) \geq -l p^\mu + q$.
Poiché per ipotesi $q > l p^\mu$ si deve avere $\mathrm{ord}(\sigma_\rho) > 0$, cioè σ_ρ si deve annullare in P_0. D'altra parte, per ipotesi $\sigma_\rho \in R_l$, quindi σ_ρ non ha poli tranne, eventualmente, P_0.
Allora σ_ρ non ha poli, cioè $\sigma_\rho \in \overline{\mathbb{F}}$. Poiché σ_ρ si annulla in P_0 si deve avere $\sigma_\rho = 0$, contraddizione.
Dunque δ è iniettivo, dunque è un isomorfismo. □

Corollario 1.4.25.
Se $l p^\mu < q$, *allora* $\dim\left(R_l^{(p^\mu)}(R_m \circ \varphi)\right) = \ell_l \ell_m$.

Dimostrazione.
Per il lemma precedente se $lp^\mu < q$ si ha che $\dim\left(R_l^{(p^\mu)}(R_m \circ \varphi)\right) =$
$= \dim\left(R_l^{(p^\mu)} \otimes_{\overline{\mathbb{F}}} (R_m \circ \varphi)\right) = \dim R_l^{(p^\mu)} \dim(R_m \circ \varphi)$. Per i punti 6. e 7. del lemma 1.4.23 allora $\dim\left(R_l^{(p^\mu)}(R_m \circ \varphi)\right) = \ell_l \ell_m$. □

Possiamo ora affrontare la dimostrazione del Teorema 1.4.21.

Dimostrazione.
Siano l, μ tali che $lp^\mu < q$, sia $m \in \mathbb{N}$.
Per il lemma 1.4.24 allora la mappa $\delta : R_l^{(p^\mu)}(R_m \circ \varphi) \to R_l^{(p^\mu)} R_m \subseteq R_{lp^\mu+m}$ data, nelle notazioni del lemma 1.4.24, da $\delta\big(\sum \sigma_i^{p^\mu}(s_i \circ \varphi)\big) = \sum \sigma_i^{p^\mu} s_i$ è ben definita ed è un'applicazione $\overline{\mathbb{F}}$-lineare.
Certamente $\dim \mathrm{Ker}\ (\delta) \geq \dim\left(R_l^{(p^\mu)}(R_m \circ \varphi)\right) - \ell_{lp^\mu+m}$.
Per il corollario precedente allora $\dim \mathrm{Ker}\ (\delta) \geq \ell_l \ell_m - \ell_{lp^\mu+m}$.
Supponiamo che $l, m \geq g$, certamente allora $lp^\mu + m > 2g - 2$, quindi per il punto 3. del lemma 1.4.23 si ha che $\dim \mathrm{Ker}\ (\delta) \geq (l + 1 - g)(m + 1 - g) -$
$-\ (lp^\mu + m + 1 - g)$.

Supponiamo che esista $f \in \mathrm{Ker}\ (\delta)$, $f \neq 0$.
Una tale funzione f deve avere uno zero di ordine almeno p^μ in ogni punto fisso di φ, tranne eventualmente in P_0.
Infatti se $f = \sum \sigma_i^{p^\mu}(s_i \circ \varphi) \neq 0$ è tale che $\delta(f) = 0$ e se $P \in C(\overline{\mathbb{F}}),\ P \neq P_0$, è tale che $\varphi(P) = P$, allora ha senso considerare $f(P)$ e si ha che
$f(P) = \sum \sigma_i^{p^\mu}(P) s_i(\varphi(P)) = \sum \sigma_i^{p^\mu}(P) s_i(P) = (\delta(f))\,(P) = 0$.
Ora, ogni elemento di $R_l^{(p^\mu)}(R_m \circ \varphi)$ è una potenza p^μ-esima, infatti ogni elemento di $R_l^{(p^\mu)}$ per definizione lo è e per il punto 5. del lemma 1.4.23 ogni elemento di $R_m \circ \varphi$ è una potenza q-esima, quindi, poiché $q = p^\alpha > lp^\mu \geq p^\mu$, una potenza p^μ-esima.
Quindi se $f \in \mathrm{Ker}\ (\delta)$, f deve avere in ogni punto fisso di φ, tranne eventualmente in P_0, uno zero di ordine almeno p^μ.

Una tale funzione f dunque ha almeno $p^\mu(\nu_1(C) - 1)$ zeri (contati con molteplicità).

D'altra parte, $f \in R_l^{(p^\mu)}(R_m \circ \varphi) \subseteq R_{lp^\mu+mq}$, quindi f può avere un polo solo in P_0, di molteplicità al più $lp^\mu + mq$.

Poiché il numero degli zeri e il numero dei poli di f, contati con molteplicità, devono coincidere, si deve avere $p^\mu(\nu_1(C) - 1) \leq lp^\mu + mq$, cioè $\nu_1(C) \leq l + \dfrac{mq}{p^\mu} + 1$.
Per ottenere questo risultato abbiamo sfruttato le seguenti ipotesi aggiuntive:

- $lp^\mu < q$
- $l, m \geq g$
- Ker $(\delta) \neq \{0\}$, certamente vero se $(l + 1 - g)(m + 1 - g) -$ $- (lp^\mu + m + 1 - g) > 0$.

Se $q = p^\alpha$, con α pari, è tale che $q > (g+1)^4$, allora si possono considerare $\mu = \dfrac{\alpha}{2},\ m = p^\mu + 2g,\ l = \left[\dfrac{g}{g+1}p^\mu\right] + g + 1$. Infatti in questo caso si ha:

- $lp^\mu < q \Leftrightarrow l < p^\mu \Leftrightarrow \left[\dfrac{g}{g+1}p^\mu\right]+g+1 < p^\mu \Leftrightarrow \left[-\dfrac{1}{g+1}p^\mu\right]+g+1 < 0$ $\Leftrightarrow \left[\dfrac{1}{g+1}p^\mu\right] > g$, vero perché $p^\mu > (g+1)^2$
- Certamente $m = p^\mu + 2g \geq g$ e $l = \left[\dfrac{g}{g+1}p^\mu\right] + 1 + g \geq g$
- $(l + 1 - g)(m + 1 - g) - (lp^\mu + m + 1 - g) = \left(\left[\dfrac{g}{g+1}p^\mu\right] + 2\right) \cdot$ $\cdot (p^\mu + g + 1) - \left(\left(\left[\dfrac{g}{g+1}p^\mu\right] + g + 2\right)p^\mu + g + 1\right) =$ $= \left(\left[\dfrac{g}{g+1}p^\mu\right] + 1\right)(g + 1) - gp^\mu > 0$

Con questa posizione quindi si ha che $\nu_1(C) \leq l + \dfrac{mq}{p^\mu} + 1 =$
$= \left[\dfrac{g}{g+1}p^\mu\right]+g+2+(p^\mu+2g)p^\mu < p^{2\mu}+(2g+1)p^\mu+1 = q+(2g+1)q^{\frac{1}{2}}+1.$ $\square$

Osservazione 1.4.26.
Il teorema 1.4.21 dà solo una maggiorazione di $\nu_1(C)$, mentre per provare che $\nu_1(C) = q + O\left(q^{\frac{1}{2}}\right)$, cioè per provare il Teorema di Weil, è necessaria anche una sua opportuna minorazione.

Osservazione 1.4.27.
Il campo di funzioni $\mathbb{K} = \mathbb{F}(C)$ contiene un sottocampo puramente trascendente su $\mathbb{F}$, $\mathbb{F}(t)$, tale che l'estensione $\mathbb{K}/\mathbb{F}(t)$ è separabile.
Sia $\mathbb{L}$ la chiusura di Galois di $\mathbb{K} \supset \mathbb{F}(t)$, cioè la più piccola estensione algebrica di $\mathbb{K}$ che sia di Galois su $\mathbb{F}(t)$.
Sia $G = Gal(\mathbb{L} : \mathbb{F}(t))$ e sia $H = Gal(\mathbb{L} : \mathbb{K})$; in particolare allora H è un sottogruppo di G.
A meno di sostituire $\mathbb{F}$ con una sua estensione finita possiamo supporre che $Gal(\overline{\mathbb{L}} : \overline{\mathbb{F}}(t)) \simeq Gal(\mathbb{L} : \mathbb{F}(t))$ e che $Gal(\overline{\mathbb{L}} : \overline{\mathbb{K}}) \simeq Gal(\mathbb{L} : \mathbb{K})$. Notiamo ancora $G = Gal(\overline{\mathbb{L}} : \overline{\mathbb{F}}(t))$ e $H = Gal(\overline{\mathbb{L}} : \overline{\mathbb{K}})$.
Possiamo identificare il morfismo di Frobenius φ con i morfismi di
Frobenius di $\overline{\mathbb{F}}(t), \overline{\mathbb{K}}$ e $\overline{\mathbb{L}}$; si può allora dimostrare che φ commuta con gli elementi di G, visti come automorfismi di $\overline{\mathbb{L}}/\mathbb{K}$, e con gli elementi di H, visti come automorfismi di $\overline{\mathbb{L}}/\mathbb{F}(t)$.

Osservazione 1.4.28.
Sia C' una curva tale che $\mathbb{L} = \mathbb{F}(C')$ (si può dimostrare che una tale curva esiste ed è unica a meno di isomorfismi[6]).
Identificando i punti di $C'(\overline{\mathbb{F}})$ con i divisori primi di $\overline{\mathbb{L}}$ si possono vedere G e H come gruppi che agiscono su $C'(\overline{\mathbb{F}})$.

Ora, $\mathbb{F}(t) = \mathbb{F}(\mathbb{P}^1)$; siano i_1, i_2 le inclusioni $\overline{\mathbb{F}}(t) \xrightarrow{i_1} \overline{\mathbb{F}}(C) \xrightarrow{i_2} \overline{\mathbb{F}}(C')$. Si può dimostrare[7] che allora esistono $\phi_1 : C \to \mathbb{P}^1$, $\phi_2 : C' \to C$ tali che $i_1(f) = f \circ \phi_1 \ \forall f \in \overline{\mathbb{F}}(t)$ e $i_2(g) = g \circ \phi_2 \ \forall g \in \overline{\mathbb{K}}$. In particolare se $i = i_2 \circ i_1$ e $\phi = \phi_1 \circ \phi_2$ allora $\forall f \in \overline{\mathbb{F}}(t)$ si ha che $i(f) = f \circ \phi$.

[6] Si può trovare la dimostrazione in Hartshorne [6]
[7] Si può trovare la dimostrazione in Hartshorne [6]

Osservazione 1.4.29.
Sia $T = \mathbb{P}^1(\mathbb{F})$. Sia $\widetilde{T} = \phi^{-1}(T)$.
Sia $P \in T$, sia $\{Q_1, \dots, Q_m\} = \phi^{-1}(\{P\})$.
Identificando i Q_i con i corrispondenti divisori primi di $\mathbb{L}$ si prova che $\phi(\varphi(Q_i)) = \varphi(\phi(Q_i)) = P \ \forall i$, cioè che $\varphi(Q_i) \in \phi^{-1}(\{P\}) \ \forall i$. Dunque, poiché φ è biunivoca, $\{\varphi(Q_1), \dots, \varphi(Q_m)\} = \{Q_1, \dots, Q_m\}$.
Se $\eta \in G$, η commuta con ϕ, quindi permuta i Q_i.
Si può dimostrare che se Q_i è non ramificato per ϕ, allora $\exists! \eta \in G$ tale che $\varphi(Q_i) = \eta Q_i$. Si dice allora che η è la sostituzione di Frobenius di G in Q_i.
Sia $\widetilde{T}' = \{Q \in \widetilde{T} |\ Q \text{ è non ramificato}\}$.
Per $\eta \in G$, sia $\widetilde{T}'(\eta) = \{Q \in \widetilde{T}' |\ \varphi(Q) = \eta Q\}$. Sia $\nu_1(C', \eta) = |\widetilde{T}'(\eta)|$.
Se $P \in T$ è non ramificato, allora $|\phi^{-1}(\{P\})| = |G|$.
Si ha dunque che $|\widetilde{T}| = |G||T| + O(1) = |G|\nu_1(\mathbb{P}^1) + O(1)$, dove il termine d'errore $O(1)$, che tiene conto dei punti ramificati, è indipendente da q.
D'altra parte, poiché $\widetilde{T}' = \bigcup_{\eta \in G} \widetilde{T}'(\eta)$, unione disgiunta, $|\widetilde{T}'| = \sum_{\eta \in G} \nu_1(C', \eta)$.
Quindi $\sum_{\eta \in G} \nu_1(C', \eta) = |G|\nu_1(\mathbb{P}^1) + O(1)$.
Poiché $\nu_1(\mathbb{P}^1) = q + 1$, $\sum_{\eta \in G} \nu_1(C', \eta) = |G|(q+1) + O(1)$.

Proposizione 1.4.30.
Se q è una potenza pari di p tale che $(g'+1)^4 < q$, con g' genere di C', allora nelle notazioni precedenti per ogni $\eta \in G$ si ha che

$$\nu_1(C', \eta) \leq q + 1 + (2g' + 1)q^{\frac{1}{2}}$$

Dimostrazione.
Supponiamo che esista $Q_0 \in C'(\mathbb{F})$, cioè supponiamo che esista $Q_0 \in C'(\overline{\mathbb{F}})$ tale che $\varphi(Q_0) = Q_0$.
Per $m \in \mathbb{N}$, sia $R_m = L(m(Q_0))$, con (Q_0) divisore primo di $\overline{\mathbb{L}}$.
Riprendendo le notazioni dell'osservazione 1.4.22 e del lemma 1.4.24, sia $\delta_\eta : R_l^{(p^\mu)}(R_m \circ \varphi) \to R_l^{(p^\mu)}(R_m \circ \eta)$ l'applicazione definita da $\delta_\eta \left(\sum_{i=1}^{r} \sigma_i^{p^\mu} (s_i \circ \varphi) \right) =$

$= \sum_{i=1}^{r} \sigma_i^{p^\mu}(s_i \circ \eta)$, con $\{s_1, \dots, s_r\}$ base di R_m.
Per il lemma 1.4.23 applicato a $\mathbb{L}$ e Q_0, δ_η è ben definita.
Ora, $\dim_{\overline{\mathbb{F}}} \mathrm{Im}\,(\delta_\eta) \leq \dim_{\overline{\mathbb{F}}} \left(R_l^{(p^\mu)}(R_m \circ \eta)\right) \leq \dim_{\overline{\mathbb{F}}} L(lp^\mu(Q_0) + m(\eta^{-1}Q_0))$.
Supponendo che $l, m \geq g'$ quindi si ha che $\dim_{\overline{\mathbb{F}}} \mathrm{Im}\,(\delta_\eta) \leq lp^\mu + m - g' + 1$.
Procedendo come nella dimostrazione del teorema 1.4.21 allora si ottiene che $\nu_1(C', \eta) \leq q + 1 + (2g' + 1)q^{\frac{1}{2}}$. □

Osservazione 1.4.31.
Per la proposizione precedente $\nu_1(C', \eta) \leq q + O\left(q^{\frac{1}{2}}\right)\ \forall \eta \in G$. Proviamo che in effetti per ogni $\eta \in G$ si ha

$$\nu_1(C', \eta) = q + O\left(q^{\frac{1}{2}}\right)$$

Per la proposizione precedente $q+1+(2g'+1)q^{\frac{1}{2}} - \nu_1(C', \eta) \geq 0\ \forall \eta \in G$, quindi
$q + 1 + (2g' + 1)q^{\frac{1}{2}} - \nu_1(C', \eta) \leq \sum_{\eta \in G} \left(q + 1 + (2g' + 1)q^{\frac{1}{2}} - \nu_1(C', \eta)\right) =$
$= \left(q + 1 + (2g' + 1)q^{\frac{1}{2}}\right)|G| - |G|\nu_1(\mathbb{P}^1) + O(1)$. Quindi $\nu_1(C', \eta) \geq$
$\geq q+1+(2g'+1)q^{\frac{1}{2}} + (\nu_1(\mathbb{P}^1) - q - 1)|G| - (2g'+1)q^{\frac{1}{2}}|G| + O(1) = q + O\left(q^{\frac{1}{2}}\right)$.
Allora $\nu_1(C', \eta) = q + O\left(q^{\frac{1}{2}}\right)\ \forall \eta \in G$.

Osservazione 1.4.32.
Poiché H è un sottogruppo di G si può considerare $\nu_1(C', \tau)$ per $\tau \in H$; in particolare si ha che $\sum_{\tau \in H} \nu_1(C', \tau) = q|H| + O\left(q^{\frac{1}{2}}\right)$.

Per $\tau \in H$, poniamo $\widetilde{\nu}_1(C', \tau) = \#\{R \in C'(\overline{\mathbb{F}}) |\ \phi_2(R) \in C(\mathbb{F}), R \text{ è non ramificato per } \phi_2, \varphi(R) = \tau R\}$.
Per l'osservazione 1.4.29 applicata all'estensione $\overline{\mathbb{K}} \subseteq \overline{\mathbb{L}}$, cioè applicata a C' e C, si ha che $\sum_{\tau \in H} \widetilde{\nu}_1(C', \tau) = |H|\nu_1(C) + O(1)$.
Poiché ϕ_2 commuta con φ e con gli elementi di H e poiché ogni elemento di H fissa $C(\overline{\mathbb{F}})$ si ha che $\nu_1(C', \tau) \leq \widetilde{\nu}_1(C', \tau)\ \forall \tau \in H$.
Allora $q|H| + O\left(q^{\frac{1}{2}}\right) = \sum_{\tau \in H} \nu_1(C', \tau) \leq \sum_{\tau \in H} \widetilde{\nu}_1(C', \tau) = |H|\nu_1(C) + O(1)$.
Dunque $\nu_1(C) \geq q + O\left(q^{\frac{1}{2}}\right)$.

Poiché per il teorema 1.4.21 $\nu_1(C) \leq q + O\left(q^{\frac{1}{2}}\right)$ dunque

$$\nu_1(C) = q + O\left(q^{\frac{1}{2}}\right)$$

Per ottenere questo risultato abbiamo supposto che q sia una potenza pari di p sufficientemente grande ma, per quanto visto nell'osservazione 1.4.19, questo è sufficiente per dimostrare completamente il Teorema di Weil.

Capitolo 2

Il gruppo delle classi di ideali

Sia $q = p^n \in \mathbb{N}$, con p primo, sia $C : f(X, Y) = 0$ una curva affine piana definita su $\mathbb{F}_q$. Supponiamo che C sia liscia e supponiamo che $f \in \mathbb{F}_q[X, Y]$ sia un polinomio assolutamente irriducibile.

Sia $\widetilde{C} : \widetilde{f}(X, Y, Z) = 0$ la chiusura proiettiva di C.
Supponiamo che $\widetilde{C}$ sia una curva liscia, o comunque che esista una sua desingolarizzazione, cioè una curva proiettiva $\widetilde{C}'$, eventualmente non piana, liscia e tale che la sua parte affine sia isomorfa a C.
Siano $\infty_1, \ldots, \infty_n$ i punti all'infinito di $\widetilde{C}$ (o della sua desingolarizzazione $\widetilde{C}'$) definiti su $\overline{\mathbb{F}}_q$, cioè sia $\{\infty_1, \ldots, \infty_n\} = \widetilde{C}(\overline{\mathbb{F}}_q) \cap \{X_0 = 0\}$. È possibile che alcuni di questi punti siano coniugati fra di loro, certamente però essi non sono coniugati con alcun punto affine di C.
Siano $(\infty_1), \ldots, (\infty_k)$ i divisori primi di C individuati dai suoi punti all'infinito (cioè siano $\infty_1, \ldots, \infty_k$ tali che $\forall i \in \{1, \ldots, n\}\ \exists! j \in \{1, \ldots, k\}$ con ∞_i, ∞_j coniugati).

Osservazione 2.1.
Sia $R = \mathbb{F}_q[C]$ l'anello delle coordinate di C, cioè sia $R = \mathbb{F}_q[X, Y]/(f)$. Proviamo che R è un dominio di Dedekind.

Certamente R è un anello commutativo unitario. R è un dominio di integrità perché per ipotesi f è assolutamente irriducibile.

R è noetheriano, infatti certamente $\mathbb{F}_q$ è noetheriano, quindi anche $\mathbb{F}_q[X,Y]$ lo è. Dunque $R = \mathbb{F}_q[X,Y]/(f)$, quoziente di un anello noetheriano, è noetheriano.

Inoltre, ogni ideale primo non nullo di R è massimale.
Infatti se J è un ideale di R non nullo, esiste $g \in \mathbb{F}_q[X]$ tale che $g + (f) \in J$. Allora, se $\deg_Y f = m$, $\deg g = n$, ogni elemento di R/J può essere scritto come $\overline{\alpha_0(X) + \alpha_1(X)Y + \cdots + \alpha_{m-1}(X)Y^{m-1}}$, con $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_q[X]$ tali che $\deg \alpha_0, \ldots, \deg \alpha_{m-1} < n$, dunque R/J è un anello finito.
Allora R/J è un dominio di integrità se e solo se è un campo, cioè J è primo se e solo se è massimale.

Per come è definito, certamente R è integralmente chiuso.
Dunque R è un dominio di Dedekind.

Teorema 2.2. Teorema degli zeri di Hilbert
Sia $\mathbb{K}$ un campo algebricamente chiuso, sia J un ideale di $\mathbb{K}[X_1, \ldots, X_n]$. Allora $J \neq \mathbb{K}[X_1, \ldots, X_n]$ se e solo se esiste $(x_1, \ldots, x_n) \in \mathbb{K}^n$ tale che $p(x_1, \ldots, x_n) = 0 \ \forall p \in J$.

Proposizione 2.3.
Sia $P \in C(\overline{\mathbb{F}}_q)$ un punto affine di C, sia $(P) = \{r \in R |\ r(P) = 0\}$, allora (P) è un ideale primo di R. Inoltre, tutti gli ideali primi di R sono di questo tipo, con $(P) = (Q)$ se e solo se P, Q sono coniugati.

Dimostrazione.
Certamente (P) è ben definito ed è un ideale proprio di R. (P) è primo perché se $r, s \in R$, allora $rs \in (P) \Leftrightarrow (rs)(P) = 0 \Leftrightarrow r(P) = 0$ o $s(P) = 0 \Leftrightarrow r \in (P)$ o $s \in (P)$.
Sia $I = (f) \subseteq \mathbb{F}_q[X,Y]$. Certamente gli ideali di R sono in corrispondenza biunivoca con gli ideali di $\mathbb{F}_q[X,Y]$ che contengono I.
Sia J un ideale proprio di $\mathbb{F}_q[X,Y]$, sia $\overline{J}$ l'ideale di $\overline{\mathbb{F}}_q[X,Y]$ generato da J. $\overline{J}$ è ancora un ideale proprio, infatti $\min_{r \in J} \deg r = \min_{s \in \overline{J}} \deg s$. Dunque per il Teorema degli zeri di Hilbert esiste $(x_0, y_0) \in \overline{\mathbb{F}}_q^2$ tale che $r(x_0, y_0) = 0 \ \forall r \in \overline{J}$. In particolare dunque se $I \subseteq J$ si ha che $f(x_0, y_0) = 0$, cioè che (x_0, y_0) è un

punto affine di C.
Dunque ad ogni ideale J di R può essere associato un ideale di $\mathbb{F}_q[X,Y]$ contenente I, quindi almeno un punto affine P della curva C definito su $\overline{\mathbb{F}}_q$ tale che $J \subseteq (P)$.
Ora, $P_1, P_2 \in C(\overline{\mathbb{F}}_q)$ sono coniugati se e solo se esiste $\sigma \in Gal(\overline{\mathbb{F}}_q : \mathbb{F}_q)$ tale che $\sigma(P_1) = P_2$, se e solo se per ogni $r \in \mathbb{F}_q[X,Y]$ sono equivalenti $r(P_1) = 0$ e $r(P_2) = 0$, cioè se e solo se $(P_1) = (P_2)$. Ad ogni ideale proprio di R possono dunque essere associati uno o più sistemi di punti affini coniugati di C definiti su $\overline{\mathbb{F}}_q$.
In particolare allora se $J \subseteq R$ è un ideale primo non nullo, poiché R è un dominio di Dedekind, J deve essere anche massimale, quindi deve esistere $P \in C(\overline{\mathbb{F}}_q)$ tale che $J = (P)$. □

Osservazione 2.4.
Sia A il gruppo degli ideali frazionari di R.
Poiché R è un dominio di Dedekind, A è il gruppo abeliano libero generato dagli ideali primi di R, cioè dagli ideali (P), con P punto affine di C. Ogni ideale frazionario di R può cioè essere scritto in modo unico (in notazione additiva) nella forma $\sum_{P \in C(\overline{\mathbb{F}}_q)} a_P(P)$, con $a_P \in \mathbb{Z}$ e con $\#\{P |\ a_P \neq 0\} < \infty$.

Osservazione 2.5.
Sia $\mathbb{K} = \mathbb{F}_q(C)$ il campo di funzioni di C, cioè sia $\mathbb{K}$ il campo dei quozienti di R.
Sia $r \in \mathbb{K}$, allora l'ideale frazionario $rR = \{kr |\ k \in R\}$ è detto l'ideale principale generato da r.
Ora, $s \in rR \ \Leftrightarrow\ s = kr$ con $k \in R \ \Leftrightarrow\ \mathrm{ord}_P s \geq \mathrm{ord}_P r\ \forall P \in C(\overline{\mathbb{F}}_q)$ punto affine di $C \ \Leftrightarrow\ s \in \sum_P \mathrm{ord}_P r(P)$. Dunque $rR = \sum_P \mathrm{ord}_P r(P)$.

Notiamo A' l'insieme degli ideali principali di R; certamente A' è un sottogruppo di A.

Definizione 2.1.
Il gruppo $G = A/A'$ è detto il **gruppo delle classi di ideali** di R.

Denotiamo con $\mathrm{Div}^0(C)$ il gruppo dei divisori di grado 0 di $\widetilde{C}$, chiusura proiettiva di C (o di una sua desingolarizzazione); denotiamo con $\mathscr{P}(C)$ il suo sottogruppo dei divisori principali e poniamo $Cl^0(C) = \mathrm{Div}^0(C)/\mathscr{P}(C)$.

Proposizione 2.6.
Sia $\varphi : \mathrm{Div}^0(C) \to A$ l'omomorfismo di gruppi (additivi) definito da $\varphi\big(\sum_P a_P(P) + a_1(\infty_1) + \cdots + a_k(\infty_k)\big) = \sum_P a_P(P)$, siano $\pi_{\mathscr{P}} : \mathrm{Div}^0(C) \to Cl^0(C)$, $\pi_{A'} : A \to G$ le proiezioni canoniche, sia $\psi = \pi_{A'} \circ \varphi$. Allora ψ passa al quoziente e induce un omomorfismo $\varphi' : Cl^0(C) \to G$.

$$\begin{array}{ccc} \mathrm{Div}^0(C) & \xrightarrow{\varphi} & A \\ {\scriptstyle \pi_{\mathscr{P}}}\downarrow & \searrow^{\psi} & \downarrow{\scriptstyle \pi_{A'}} \\ Cl^0(C) & \xrightarrow{\varphi'} & G \end{array}$$

Dimostrazione.
Sia $(r) \in \mathscr{P}(C)$, allora $\psi\big((r)\big) = \pi_{A'}\big(\sum \mathrm{ord}_P r(P)\big) = \pi_{A'}(rR) = 0$.
Dunque $\mathscr{P}(C) \subseteq \mathrm{Ker}\ (\psi)$, dunque ψ passa al quoziente. □

L'equivalenza come divisori implica l'equivalenza come ideali; il viceversa in generale non è vero, infatti nel primo caso è necessario tenere conto anche dei punti all'infinito, che invece nel secondo caso sono ignorati.

Osservazione 2.7.
Sia $m = \mathrm{MCD}\big(\deg(\infty_1), \ldots, \deg(\infty_k)\big)$, allora nelle notazioni della proposizione precedente si ha che $\mathrm{Im}\ (\varphi) = A_m$, con $A_m = \big\{\sum a_P(P) \in A \big|\ m \big| \sum a_P \deg(P)\big\}$.
Infatti $\sum a_P(P) \in \mathrm{Im}\ (\varphi) \Leftrightarrow \exists a_1, \ldots, a_k \in \mathbb{Z}$ tali che $\sum a_P(P) + a_1(\infty_1) + \cdots + a_k(\infty_k) \in \mathrm{Div}^0(C) \Leftrightarrow \exists a_1, \ldots, a_k \in \mathbb{Z}$ tali che $\sum a_P(P)\deg(P) + a_1\deg(\infty_1) + \cdots + a_k\deg(\infty_k) = 0 \Leftrightarrow m \big| \sum a_P \deg(P)$.
Dunque $\mathrm{Im}\ (\psi) = \mathrm{Im}\ (\varphi') = \pi_{A'}(A_m)$.
Sia $rR \in A'$; poiché $rR = \varphi\big((r)\big)$, certamente $rR \in A_m$. Allora $A' \subseteq A_m$, quindi

$$\mathrm{Im}\ (\varphi') = A_m/A' \tag{2.1}$$

Osservazione 2.8.
Supponiamo che esista $\sum a_P(P) \in A$ tale che $\sum a_P \deg(P) = 1$, cioè supponiamo che $\widetilde{C}$ abbia divisori di grado 1 in cui compaiono solo punti affini della curva (questo è certamente vero per esempio se C ha almeno un punto definito su $\mathbb{F}_q$).

In questo caso allora A_m è un sottogruppo di A di indice m, quindi A_m/A' è un sottogruppo di G di indice m.

Abbiamo visto che $Cl^0(C)$ è un gruppo finito, sia $h = |Cl^0(C)|$.
Allora anche Im $(\varphi') =$ Im (ψ) deve essere finito, cioè A_m/A' è finito.

Dunque anche G è un gruppo finito e si ha che $|G| = m|A_m/A'| =$
$= m|\text{Im } (\varphi')|$.
D'altra parte, certamente $|\text{Im } (\varphi')| = \dfrac{h}{|\text{Ker } (\varphi')|}$, dunque

$$|G| = m\frac{h}{|\text{Ker } (\varphi')|}$$

In particolare, poiché $\dfrac{h}{|\text{Ker } (\varphi')|} = |\text{Im } (\varphi')| \in \mathbb{N}$, si può avere $|G| = 1$ solo se $m = 1$, cioè il dominio di Dedekind R può essere un anello a fattorizzazione unica solo se $\deg(\infty_1), \ldots, \deg(\infty_k)$ sono primi fra loro.

Osservazione 2.9.
Sia $\overline{D} = \overline{\sum_P a_P(P) + a_1(\infty_1) + \cdots + a_k(\infty_k)} \in Cl^0(C)$. Allora, $\overline{D} \in \text{Ker } (\varphi') \Leftrightarrow$
$\psi(D) = 0$, con $D = \sum_P a_P(P) + a_1(\infty_1) + \cdots + a_k(\infty_k) \Leftrightarrow \exists r \in \mathbb{K}$ tale che
$\sum_P a_P(P) = \sum_P \text{ord}_P r(P) \Leftrightarrow \exists r \in \mathbb{K}$ tale che $D = (r) + a'_1(\infty_1) +$
$+ \cdots + a'_k(\infty_k) \Leftrightarrow \overline{D} = \overline{a'_1(\infty_1) + \cdots + a'_k(\infty_k)}$.
Dunque Ker $(\varphi') = \left\{\overline{a'_1(\infty_1) + \cdots + a'_k(\infty_k)} \in Cl^0(C)\right\} =$
$= \left\{\overline{a'_1(\infty_1) + \cdots + a'_k(\infty_k)} \in Cl(C) |\ a'_1 \deg(\infty_1) + \cdots + a'_k \deg(\infty_k) = 0\right\}$.

Abbiamo quindi dimostrato il seguente teorema:

Teorema 2.10.
Sia $C : f(X, Y) = 0$ una curva affine piana regolare, con $f \in \mathbb{F}_q[X, Y]$ assolutamente irriducibile, sia $\widetilde{C}$ la chiusura proiettiva di C (o una sua desingolarizzazione), siano $(\infty_1), \ldots, (\infty_k)$ i divisori primi di $\widetilde{C}$ individuati dai suoi

punti all'infinito.
Sia R l'anello delle coordinate di C, sia G il suo gruppo delle classi di ideali, allora

$$G = m\frac{h}{|Ker\ (\varphi')|} \tag{2.2}$$

con $m = \mathrm{MCD}\big(\deg(\infty_1), \ldots, \deg(\infty_k)\big)$ *e dove*

$$Ker\ (\varphi') = \left\{ \overline{a'_1(\infty_1) + \cdots + a'_k(\infty_k)} \in Cl(C) |\ \sum_i a'_i \deg(\infty_i) = 0 \right\} \tag{2.3}$$

La formula (2.2) è detta anche Formula di Schmidt, poiché è stata provata da F.K. Schmidt in [10].

Capitolo 3

Anelli quadratici: teorema di Dirichlet ed equazione di Pell

Un problema classico di teoria dei numeri è la determinazione del numero di classi di ideali degli anelli quadratici. Questo problema è stato affrontato già da Gauss e Dirichlet, nel contesto però della teoria delle forme quadratiche, e poi sviluppato da Dedekind.

Vedremo una traccia di dimostrazione della formula di Dirichlet sul numero di classi e proveremo che si può ottenere un risultato simile per il numero di classi dell'anello associato ad una curva ellittica definita su un campo finito. Vedremo inoltre che in questo caso possono essere dimostrati gli analoghi delle congetture di Gauss.

3.1 Formula di Dirichlet sul numero di classi

Sia $D \in \mathbb{Z}$ libero da quadrati, consideriamo il campo quadratico $\mathbb{K} = \mathbb{Q}(\sqrt{D})$; sia R l'anello degli interi algebrici di $\mathbb{K}$.
Si può provare che R è l'insieme degli elementi della forma $\dfrac{x + y\sqrt{d}}{2}$, con $x, y \in \mathbb{Z}$ e con d discriminante di $\mathbb{K}$, cioè con $d = \begin{cases} 4D & \text{se } D \equiv 2,3 \pmod 4 \\ D & \text{se } D \equiv 1 \pmod 4 \end{cases}$.

R è un dominio di Dedekind, quindi ha senso considerare il suo gruppo delle classi di ideali G, quoziente del gruppo degli ideali frazionari di R modulo il sottogruppo degli ideali principali.

Sia $\varepsilon = \dfrac{x + y\sqrt{d}}{2} \in R$, con $x, y \in \mathbb{Z}$. ε è invertibile in R se e solo se x, y verificano l'**equazione di Pell**, cioè se e solo se

$$x^2 - dy^2 = \pm 4 \tag{3.1}$$

Si può provare che se $D > 0$, cioè se $\mathbb{K}$ è un campo quadratico reale, allora le uniche radici dell'unità in R sono ± 1 ed esiste un'unità $\varepsilon_0 \in R$, $\varepsilon_0 > 1$, tale che tutte le unità di R sono della forma $\pm\varepsilon_0^m$, con $m \in \mathbb{Z}$. Si dice allora che ε_0 è l'**unità fondamentale** di R.
Se invece $D < 0$, cioè se $\mathbb{K}$ è un campo quadratico immaginario, allora tutte le unità di R sono radici dell'unità. Si prova facilmente che in $\mathbb{Q}(\sqrt{-3})$ ci sono 6 radici dell'unità, in $\mathbb{Q}(\sqrt{-1})$ ci sono 4 radici dell'unità e in tutti gli altri casi soltanto 2.

Se I è un ideale di un dominio di Dedekind R, si definisce la **norma assoluta** di I, notata $N(I)$, come l'indice di I in R.
Per ogni I, J ideali di R si ha allora che $N(IJ) = N(I)N(J)$, cioè la norma considerata è moltiplicativa.
Questa definizione può essere estesa agli ideali frazionari: se $J = P_1^{n_1} \cdots P_k^{n_k}$ è un ideale frazionario di R, con $P_1, \ldots, P_k$ ideali primi e $n_1, \ldots, n_k \in \mathbb{Z}$, si pone $N(J) = N(P_1)^{n_1} \cdots N(P_k)^{n_k}$.
Si può provare che se P è un ideale primo di un dominio di Dedekind R allora $N(P) = p^k$, con $p \in \mathbb{Z}$ primo.

Sia $\mathbb{K}$ un campo, sia R l'anello degli interi algebrici di $\mathbb{K}$. Si definisce la **funzione zeta di Dedekind** di $\mathbb{K}$ come

$$\zeta_{\mathbb{K}}(s) = \sum_I N(I)^{-s} \tag{3.2}$$

con $I \neq 0$ che varia nell'insieme degli ideali di R.
Dunque $\zeta_{\mathbb{K}}(s) = \sum_{n=1}^{\infty} \frac{F(n)}{n^s}$, con $F(n) = \#\{I|\ I \text{ ideale di } R,\ N(I) = n\}$.
Si può provare che la serie considerata converge assolutamente ad una funzione continua su $\{s \in \mathbb{C}|\ \mathrm{Re}(s) > 1\}$.
Inoltre per $\mathrm{Re}(s) > 1$ si ha che

$$\zeta_{\mathbb{K}}(s) = \prod_{P} (1 - N(P)^s)^{-1} \tag{3.3}$$

con P che varia nell'insieme degli ideali primi di $\mathbb{K}$.

Sia $\theta \in \mathbb{C}$, sia $\mathbb{K} = \mathbb{Q}(\theta)$. Siano $\theta_1, \ldots, \theta_n$ i coniugati di θ, supponiamo che $\theta_1 \ldots, \theta_{r_1} \in \mathbb{R}$ e che $\theta_{r_1+1}, \ldots, \theta_{r_1+2r_2} \in \mathbb{C} \setminus \mathbb{R}$, con $n = r_1 + 2r_2$.
Si può provare che allora

$$\chi|G| = \lim_{s \to 1^+} (s-1)\zeta_{\mathbb{K}}(s) \tag{3.4}$$

con G gruppo delle classi di ideali di R, anello degli interi algebrici di $\mathbb{K}$, e

$$\chi = \frac{2^{r_1+r_2}\pi^{r_2}\mathscr{R}}{w\sqrt{|d|}} \tag{3.5}$$

dove $\mathscr{R}$ è il regolatore di $\mathbb{K}$ e w è il numero delle radici dell'unità in $\mathbb{K}$.

Nel caso dei campi quadratici $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ in particolare si può provare che se $p \in \mathbb{Z}$ è un numero primo allora:

- (p) si fattorizza come prodotto di due ideali primi distinti di R se e solo se $\left(\frac{d}{p}\right) = 1$
- (p) è un ideale primo di R se e solo se $\left(\frac{d}{p}\right) = 0$
- (p) è il quadrato di un ideale primo di R se e solo se $\left(\frac{d}{p}\right) = -1$

con $\left(\frac{d}{p}\right)$ simbolo di Kronecker.
Inoltre, tutti gli ideali primi di R possono essere ottenuti in uno dei modi

precedenti.

Da questo segue che $\zeta_{\mathbb{K}}(s) = \zeta(s)L(s)$ per $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$, con ζ funzione zeta di Riemann e $L(s) = \prod_{p \text{ primo}} \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}$.
Poiché $\lim_{s \to 1^+} \zeta(s)(s-1) = 1$, per (3.4) nel caso dei campi quadratici si ha che

$$\chi|G| = \lim_{s \to 1^+} L(s) \tag{3.6}$$

dove, per quanto visto prima, $\chi = \begin{cases} \frac{2 \log \varepsilon_0}{\sqrt{d}} & \text{se } D > 0 \\ \frac{2\pi}{w\sqrt{|d|}} & \text{se } D < 0 \end{cases}$, con ε_0 unità fondamentale e w numero delle radici dell'unità in R.

Ora, si può provare che $L(s)$ converge ad una funzione continua per $\mathrm{Re}(s) > \frac{1}{2}$, quindi si può concludere che $\chi|G| = L(1)$.

Teorema 3.1.1. Teorema di Dirichlet
Sia $D \in \mathbb{Z}$, $D \neq 1$, libero da quadrati, sia $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, sia R l'anello degli interi algebrici di $\mathbb{K}$, sia G il gruppo delle classi di ideali di R. Allora

- *se $D > 0$ si ha che*
$$|G| = L(1)\frac{\sqrt{d}}{2 \log \varepsilon_0}$$
con $\varepsilon_0 = \dfrac{x + y\sqrt{d}}{2} > 1$ unità fondamentale, quindi soluzione dell'equazione di Pell $X^2 - dY^2 = \pm 4$

- *se $D < 0$ si ha che*
$$|G| = L(1)\frac{w\sqrt{|d|}}{2\pi}$$
con w numero delle radici dell'unità in $\mathbb{K}$, cioè $w = \begin{cases} 6 & \text{se } D = -3 \\ 4 & \text{se } D = -1 \\ 2 & \text{altrimenti} \end{cases}$

dove d è il discriminante di $\mathbb{K}$ e dove $L(s) = \prod_{p \text{ primo}} \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}$.

3.1.1 Congetture di Gauss

Il problema di Gauss sul numero di classi per campi quadratici immaginari, come usualmente inteso, consiste nel fornire, per ciascun $n \geq 1$, una lista completa di campi quadratici immaginari con numero di classi n, problema che può anche essere formulato in termini di discriminanti di forme quadratiche. Sono state anche sollevate questioni sul comportamento del numero di classi quando il discriminante tende a $-\infty$ e sul caso dei campi quadratici reali.

Il problema della determinazione del numero di classi è stato affrontato, già all'inizio dell'800, da Gauss e Dirichlet, nel contesto però delle forme quadratiche.
Una teoria generale delle forme quadratiche è stata sviluppata alla fine del '700, in particolare da Lagrange e Legendre, per trattare il problema generale di determinare, fissati $a, b, c \in \mathbb{Z}$, per quali interi m esistono $x, y \in \mathbb{Z}$ tali che $m = ax^2 + bxy + cy^2$.
Due forme quadratiche sono dette equivalenti se possono essere ottenute l'una dall'altra per moltiplicazione per una matrice ortogonale speciale a coefficienti in $\mathbb{Z}$. Due forme quadratiche equivalenti hanno lo stesso discriminante; il viceversa in generale però non è vero. Quindi è sorto il problema di determinare il numero di classi di forme quadratiche equivalenti di discriminante d fissato.

Gauss ha trattato questo tema nelle *Disquisitiones Artihmeticae* (1801), definendo la composizione di due forme quadratiche e provando che le classi di forme quadratiche di discriminante d fissato, con questa legge di composizione, formano un gruppo finito. Gauss ha inoltre dimostrato che tale gruppo può essere rappresentato come un prodotto diretto di gruppi ciclici.

Nell'Articolo 303 Gauss congettura che, fissato $g \in \mathbb{N}$, il numero dei discriminanti negativi d tali che $g(d) = g$ sia finito, dove, per $d \in \mathbb{Z}$, notiamo $g(d)$ il numero di classi di forme quadratiche di discriminante d. Nello stesso

articolo, per g piccoli Gauss dà un elenco di discriminanti $d < 0$ tali che $g(d) = g$ e congettura che tali elenchi siano completi.
Nell'Articolo 304 Gauss congettura che esistano infiniti discriminanti positivi d tali che $g(d) = 1$.

Gauss però considera solo le forme quadratiche del tipo $aX^2+2bXY+cY^2$, con $a, b, c \in \mathbb{Z}$, definendo il loro discriminante come $d = b^2 - ac$.

Nel 1902 Landau, mantenendo le ipotesi di Gauss, ha provato che la lista di discriminanti $d < 0$ tali che $g(d) = 1$ data da Gauss era completa. Il fatto di considerare b pari però semplifica molto il problema.

La prima formula per il numero di classi è stata provata nel 1839 da Dirichlet, ancora nel contesto delle forma quadratiche.

Questo problema sulle forme quadratiche può essere tradotto nel linguaggio dei campi quadratici. Infatti ad ogni forma quadratica binaria $aX^2 + bXY + cY^2$ di discriminante d può essere associato un ideale dell'anello degli interi algebrici di $\mathbb{Q}(\sqrt{d})$. Si può provare che, nel caso $d < 0$, due forme sono equivalenti nel senso di Lagrange se e solo se gli ideali ad esse associati sono equivalenti. Il numero di classi di forme quadratiche di discriminante $d < 0$ quindi coincide con il numero di classi di ideali di $\mathbb{Q}(\sqrt{d})$. Nel caso $d > 0$ invece si può provare che il numero di forme quadratiche di discriminante d o coincide con il numero di classi di ideali di $\mathbb{Q}(\sqrt{d})$ o è il suo doppio.

Sia $D \in \mathbb{Z}$ libero da quadrati, sia $g(D)$ il numero delle classi di ideali di $\mathbb{K} = \mathbb{Q}(\sqrt{D})$; le congetture di Gauss allora possono essere tradotte come:

- il numero di classi dei campi quadratici immaginari $\mathbb{Q}(\sqrt{D}), D < 0$ tende all'infinito per $D \to -\infty$, cioè $\lim_{D\to-\infty} g(D) = \infty$
- esistono infiniti campi quadratici reali con una sola classe di ideali, cioè $\#\{D > 0|\ g(D) = 1\} = \infty$

All'inizio del '900 Hecke ha provato che se l'ipotesi di Riemann generalizzata è vera, allora lo è anche la congettura di Gauss sui campi quadratici immaginari. In seguito (1933 - 1934) Deuring ha provato che dall'esistenza di infiniti campi quadratici immaginari con numero di classi 1 seguirebbe l'ipotesi di Riemann classica e, generalizzando questo risultato, Heilbronn ha provato che la falsità dell'ipotesi di Riemann generalizzata implica la congettura di Gauss per campi quadratici immaginari.
La congettura di Gauss per campi quadratici immaginari è quindi completamente dimostrata.

Negli anni '60 Stark e Baker hanno provato che esistono esattamente 9 discriminanti $d < 0$ tali che $g(d) = 1$. Baker (1971) e Stark (1975) hanno poi risolto indipendentemente il problema del numero di classi per $g = 2$. Oesterlé (1985) ha risolto il caso $g = 3$, Arno (1992) il caso $g = 4$ e
Wagner (1996) i casi $g = 5, 6, 7$. Watkins (2004) ha poi risolto il problema per $g \leq 100$.

Goldfeld, Gross e Zagier nel 1985 hanno provato che per ogni $\varepsilon > 0$
esiste una costante $c > 0$ effettivamente computabile tale che per ogni $d < 0$ si ha che $g(d) > c(\log(|d|))^{1-\varepsilon}$. Questo quindi risolve completamente il problema generale di determinare tutti i campi quadratici immaginari con un fissato numero di classi, riducendolo ad un calcolo finito.

La congettura di Gauss per campi quadratici reali è invece ancora irrisolta.

3.2 Curve iperellittiche

Sia $q = p^k \in \mathbb{N}$, con p primo, $p \neq 2$, sia C una curva iperellittica definita su $\mathbb{F}_q$, cioè una curva definita da un'equazione della forma $Y^2 = d(X)$, con $d \in \mathbb{F}_q[X]$ polinomio libero da quadrati, sia $n = \deg d$. Sia g il genere di C; si può dimostrare[1] che $g = \begin{cases} \frac{n-1}{2} & \text{se } n \text{ è dispari} \\ \frac{n-2}{2} & \text{se } n \text{ è pari} \end{cases}$

[1]Segue dal lemma di Hurwitz, la cui dimostrazione può essere trovata in Silverman [12]

Osservazione 3.2.1.
C è non singolare come curva affine.
Infatti se $(x_0, y_0) \in \mathbb{F}_q^2$ fosse un punto singolare di C si avrebbe che $\begin{cases} 2y_0 = 0 \\ d'(x_0) = 0 \end{cases}$ con inoltre $y_0^2 = d(x_0)$. Si avrebbe dunque $y_0 = 0$ e $d(x_0) = d'(x_0) = 0$, cioè x_0 sarebbe una radice doppia di d, contraddizione.

Sia $\widetilde{C} : Y^2 Z^{n-2} = \widetilde{d}(X, Z)$ la chiusura proiettiva di C.

Se $\deg d = 1, 2$ (cioè se C è una conica) allora $\widetilde{C}$ è una curva non singolare. Se $\deg d = 1$ allora $\widetilde{C}$ ha un unico punto all'infinito, che è definito su $\mathbb{F}_q$; se $\deg d = 2$ allora $\widetilde{C}$ ha due punti all'infinito, entrambi definiti su $\mathbb{F}_q$ e distinti se il coefficiente direttore di d è un quadrato in $\mathbb{F}_q$, definiti su $\mathbb{F}_{q^2}$ e coniugati altrimenti.

Supponiamo ora che $\deg d > 2$; $\widetilde{C}$ allora ha un unico punto all'infinito, $[0, 1, 0]$, ed è singolare in questo punto.
Infatti se $\widetilde{f}(X, Y, Z) = Y^2 Z^{n-2} - \widetilde{d}(X, Z)$, con $\widetilde{d}(X, Z) = a_n X^n + \cdots +$
$+ a_0 Z^n$, allora $\dfrac{\partial \widetilde{f}}{\partial X}\Big|_{(0,1,0)} = (n a_n X^{n-1} + \cdots + a_1 Z^{n-1})|_{(0,1,0)} = 0$,
$\dfrac{\partial \widetilde{f}}{\partial Y}\Big|_{(0,1,0)} = 2Y Z^{n-2}|_{(0,1,0)} = 0$, $\dfrac{\partial \widetilde{f}}{\partial Z}\Big|_{(0,1,0)} = (a_{n-1} X^{n-1} + \cdots + n a_0 Z^{n-1})|_{(0,1,0)} = 0$.

Si può però considerare una desingolarizzazione di $\widetilde{C}$.
Sia $\phi : \mathbb{A}^2(\overline{\mathbb{F}}_q) \to \mathbb{P}^{g+2}(\overline{\mathbb{F}}_q)$ l'applicazione definita da
$\phi(x, y) = [1, x, x^2, \ldots, x^{g+1}, y]$. Allora $\phi(C) = \big\{ [x_0, \ldots, x_{g+2}] \in \mathbb{P}^{g+2}(\overline{\mathbb{F}}_q) |$
$x_0 = 1,\ x_{g+2}^2 = a_n x_1^n + \cdots + a_0,\ x_1^2 = x_2, \ldots, x_1^{g+1} = x_{g+1} \big\}$. Sia $\widetilde{C}'$ la chiusura di $\phi(C)$ in $\mathbb{P}^{g+2}(\overline{\mathbb{F}}_q)$.

Supponiamo n pari, quindi supponiamo $n = 2g + 2$, allora si ha che
$\phi(C) = \big\{ [x_0, \ldots, x_{g+2}] \in \mathbb{P}^{g+2}(\overline{\mathbb{F}}_q) |\ x_0 = 1,\ x_{g+2}^2 = a_n x_{g+1}^2 + a_{n-1} x_{g+1} x_g +$
$+ \cdots + a_{g+2} x_{g+1} x_1 + a_{g+1} x_{g+1} + \cdots + a_1 x_1 + a_0,\ x_1^2 = x_2, \ldots, x_1^{g+1} = x_{g+1} \big\}$.
Dunque $\widetilde{C}'$ è la curva definita dalle equazioni $X_{g+2}^2 = a_n X_{g+1}^2 + \cdots + a_{g+1} X_{g+1} X_0 +$

$+\cdots+a_1X_1X_0+a_0X_0^2,\ X_1^2=X_2X_0,\ldots,\ X_1^{g+1}=X_{g+1}X_0^g$.
Ora, $\widetilde{C}'\cap\{X_0\neq 0\}$ è isomorfo alla curva affine C, quindi è non singolare.
D'altra parte, se $[x_0,\ldots,x_{g+2}]\in\widetilde{C}'$, con $x_0\neq 0$, per $i\leq g$ si ha che $x_1^i=x_ix_0^{i-1},\ x_1^{i+1}=x_{i+1}x_0^i$, quindi che $x_i^{i+1}x_0^{i^2-1}=x_{i+1}^ix_0^{i^2}$, dunque
$x_i^{i+1}=x_0x_{i+1}^i$.
Questo deve valere per ogni punto di $\widetilde{C}'$, dunque se
$[0,x_1,\ldots,x_{g+2}]\in\widetilde{C}'\cap\{X_0=0\}$ si deve avere $x_0=x_1=\cdots=x_g=0$, quindi
$\widetilde{C}'\cap\{X_0=0\}=\big\{[0,\ldots,0,x_{g+1},x_{g+2}]\in\mathbb{P}^{g+2}(\overline{\mathbb{F}}_q)|\ x_{g+2}^2=a_nx_{g+1}^2\big\}$.

Dunque i punti di $\widetilde{C}'$ su $\{X_0=0\}$ sono $\infty_+=[0,\ldots,0,1,\alpha]$,
$\infty_-=[0,\ldots,0,1,-\alpha]$, con $\alpha\in\overline{\mathbb{F}}_q$ tale che $\alpha^2=a_n$.
Se a_n è un quadrato in $\mathbb{F}_q$ allora ∞_+,∞_- sono definiti su $\mathbb{F}_q$ e distinti, dunque certamente non sono coniugati (cioè $(\infty_+)\neq(\infty_-)$) e
$\deg(\infty_+)=\deg(\infty_-)=1$.
Se a_n non è un quadrato in $\mathbb{F}_q$ allora ∞_+,∞_- sono definiti su $\mathbb{F}_{q^2}$ e sono coniugati, dunque $(\infty_+)=(\infty_-)$. Notiamo $(\infty)=(\infty_+)=(\infty_-)$; certamente allora $\deg(\infty)=2$.

$\widetilde{C}'$ è non singolare anche nei punti ∞_+,∞_-, infatti si può provare che la disomogeneizzazione di $\widetilde{C}'$ rispetto a X_{g+1} è la curva affine definita dalle equazioni $X_{g+2}^2=a_n+a_{n-1}X_g+\cdots+X_g^n,\ X_1^2=X_2X_0,\ \ldots,X_1^{g+1}=X_0^g$, non singolare perché C è non singolare come curva affine.

Se n è dispari, quindi se $n=2g+1$, si prova analogamente che $\widetilde{C}'$, chiusura di $\phi(C)$, è la curva definita dalle equazioni
$X_{g+2}^2=a_nX_{g+1}X_g+\cdots+a_{g+1}X_{g+1}X_0+\cdots+a_1X_1X_0+a_0X_0^2$,
$X_1^2=X_2X_0,\ldots,\ X_1^{g+1}=X_{g+1}X_0^g$ e che $\widetilde{C}'\cap\{X_0\neq 0\}$ è isomorfa a C, quindi non singolare.
In questo caso però $\widetilde{C}'$ ha un unico punto su $\{X_0=0\}$, $\infty=[0,\ldots,0,1,0]$. Come prima, si può dimostrare che $\widetilde{C}'$ è non singolare anche in questo punto. Certamente ∞ è definito su $\mathbb{F}_q$, quindi $\deg(\infty)=1$.

Osservazione 3.2.2.
Sia $f(X,Y) = Y^2 - d(X)$; poiché per ipotesi d non è un quadrato in $\mathbb{F}_q[X]$, f è assolutamente irriducibile.
Infatti, se esistessero $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q[X]$ tali che $(\alpha(X) + \beta(X)Y)\,(\gamma(X) + \delta(X)Y) =$

$= Y^2 - d(X)$, cioè tali che $\begin{cases} \beta(X)\delta(X) = 1 \\ \alpha(X)\delta(X) + \beta(X)\gamma(X) = 0 \\ \alpha(X)\gamma(X) = -d(X) \end{cases}$, allora si dovrebbe avere che $\beta, \delta \in \mathbb{F}_q,\ \beta = \delta^{-1},\ \gamma(X) = -\delta^2\alpha(X),\ d(X) = \delta^2\alpha^2(X)$, quindi d dovrebbe essere un quadrato in $\mathbb{F}_q[X]$, contraddizione.

Denotiamo ancora con R l'anello delle coordinate di C, cioè sia
$R = \mathbb{F}_q[C] = \mathbb{F}_q[X,Y]/(Y^2 - d(X))$.
Utilizzando ancora le notazioni del capitolo precedente, si ha che, per 2.1, 2.3, 2.4, R è un dominio di Dedekind e il gruppo dei suoi ideali frazionari è (in notazione additiva) $A = \left\{ \sum_{P \in C(\overline{\mathbb{F}}_q)} m_P(P) \,\middle|\, m_P \in \mathbb{Z},\ \#\{P |\ m_P \neq 0\} < \infty \right\}$.
Notiamo ancora A' l'insieme degli ideali principali di R, cioè sia
$A' = \{fR |\ f \in \mathbb{K}\}$, con $\mathbb{K} = \mathbb{F}_q(C)$ campo dei quozienti di R.
Sia $G = A/A'$ il gruppo delle classi di ideali di R.

Osservazione 3.2.3.
Supponiamo per il momento che n sia pari e che il coefficiente direttore di d, a_n, sia un quadrato in $\mathbb{F}_q$, ipotesi aggiuntiva che resterà valida nelle successive osservazioni 3.2.4 e 3.2.5.
Abbiamo già visto che in questo caso la curva C considerata ha due punti all'infinito, che noteremo ∞_+, ∞_-, distinti e definiti su $\mathbb{F}_q$.

L'omomorfismo $\varphi : \mathrm{Div}^0(C) \to A$ definito in 2.6 allora diventa l'applicazione $\varphi\big(\sum_P m_P(P) + m_+(\infty_+) + m_-(\infty_-)\big) = \sum_P m_P(P)$.
Sia $x = \sum_P m_P(P) \in A$, allora, nelle notazioni della proposizione 2.6,
$x = \varphi\big(\sum_P m_P(P) + m_+(\infty_+)\big)$ con $m_+ = -\sum_P m_P \deg(P)$.
Allora $\varphi : \mathrm{Div}^0(C) \to A$ è un omomorfismo suriettivo, dunque anche $\psi,\ \varphi'$

sono tali, quindi Im $(\varphi') = G$ e per (2.2) si ha che

$$|G| = \frac{h}{|\text{Ker } (\varphi')|}$$

Osservazione 3.2.4.
Per l'osservazione 2.9 si ha che Ker $(\varphi') = \left\{\overline{m_+(\infty_+) + m_-(\infty_-)} \in Cl^0(C)\right\} =$

$= \left\{\overline{m_+(\infty_+) + m_-(\infty_-)} \in Cl(C) |\ m_+ + m_- = 0\right\} = \left\{\overline{m\big((\infty_+) - (\infty_-)\big)} \in Cl(C)\right\}$,
cioè Ker (φ') è il sottogruppo di $Cl^0(C)$ generato da $\overline{(\infty_+) - (\infty_-)}$.
Allora $|\text{Ker } (\varphi')| = m_0$, con m_0 ordine di $\overline{(\infty_+) - (\infty_-)}$ in $Cl^0(C)$, cioè con
$m_0 = \min\big\{m \in \mathbb{N} |\ \exists f \in \mathbb{K}$ tale che $m\big((\infty_+) - (\infty_-)\big) = (f)\big\}$.
Si avrà allora che

$$|G| = \frac{h}{m_0} \tag{3.7}$$

Osservazione 3.2.5.
Sia $f(X,Y) = \dfrac{a_1(X) + Yb_1(X)}{a_2(X) + Yb_2(X)} \in \mathbb{K}$. Se $(f) = m\big((\infty_+) - (\infty_-)\big)$ allora in particolare f non ha poli in nessun punto affine di C, cioè il polinomio $a_2(X) + Yb_2(X)$ non si annulla in nessun punto affine di C.
Per il Teorema degli zeri di Hilbert questo è equivalente al fatto che $\big(Y^2 - d(X), a_2(X) + Yb_2(X)\big) = \mathbb{F}_q[X,Y]$, cioè che $a_2(X) + Yb_2(X)$ sia invertibile in R. Dunque se $(f) = m\big((\infty_+) - (\infty_-)\big)$ allora esistono $a, b \in \mathbb{F}_q[X]$ tali che $f(X,Y) = a(X) + Yb(X)$, cioè $f \in R$.

Sia $f(X,Y) = a(X) + Yb(X) \in \mathbb{K}$, con $a, b \in \mathbb{F}_q(X)$, sia $f'(X,Y) = a(X) - Yb(X)$. Sia $P = (x,y) \in \overline{\mathbb{F}}_q$ un punto affine di C, allora $P' = (x,-y)$ è ancora un punto affine di C e, poiché $f'(X,Y) = f(X,-Y)$, si ha che $\text{ord}_P f = \text{ord}_{P'} f'$. Analogamente si ha che $\text{ord}_{\infty_+} f = \text{ord}_{\infty_-} f'$ e che $\text{ord}_{\infty_-} f = \text{ord}_{\infty_+} f'$.

In particolare dunque se $f(X,Y) = a(X) + Yb(X) \in R$, cioè se f non ha poli in alcun punto affine di C, il divisore di f sarà della forma $(f) = \sum m_P(P) + m_+(\infty_+) + m_-(\infty_-)$ con $m_P \geq 0\ \forall P$ e, di conseguenza, il divisore di f' sarà $(f') = \sum m'_P(P) + m_-(\infty_+) + m_+(\infty_-)$, con $m'_P = m_{P'}$,

dove $P' = (x, -y)$ se $P = (x, y)$, quindi con $m'_P \geq 0 \ \forall P$.
Dunque $(ff') = \sum (m_P + m'_P)(P) + (m_+ + m_-)\big((\infty_+) + (\infty_-)\big)$, con $m_P + m'_P \geq 0 \ \forall P$.

Allora $(f) = m\big((\infty_+) - (\infty_-)\big)$ se e solo se $m_P = 0 \ \forall P$ e $m_+ = -m_-$, se e solo se $(ff') = 0$, se e solo se (per 1.4.2) $ff' = k \in \mathbb{F}_q^*$.
Dunque $m_0 = \min\big\{m \in \mathbb{N} |\ m = \mathrm{ord}_{\infty_+} f \text{ con } f \in R \text{ tale che } ff' \in \mathbb{F}_q^*\big\}$.

D'altra parte, $f(X,Y)f'(X,Y) = \big(a(X) + Yb(X)\big)\big(a(X) - Yb(X)\big) = = a^2(X) - Y^2 b^2(X) = a^2(X) - d(X)b^2(X)$, quindi $\big(f\big) = m\big((\infty_+) - (\infty_-)\big)$ se e solo se

$$a^2(X) - d(X)b^2(X) \in \mathbb{F}_q^* \tag{3.8}$$

Abbiamo cioè trovato nell'ambito delle curve ellittiche definite su campi finiti un analogo dell'equazione di Pell (3.1). Certamente affinché questa equazione abbia soluzioni non nulle è necessario che il coefficiente direttore di d, a_n, sia un quadrato in $\mathbb{F}_q$.
Allora $m_0 = \min\big\{m \in \mathbb{N} |\ m = \mathrm{ord}_{\infty_+}\big(a(X) + Yb(X)\big),\ a, b \in \mathbb{F}_q[X] \text{ tali che } a^2(X) - d(X)b^2(X) \in \mathbb{F}_q^*\big\}$.

Osservazione 3.2.6.
Supponiamo ora che n sia pari e che a_n non sia un quadrato in $\mathbb{F}_q$.
Anche in questo caso la curva C considerata ha due punti all'infinito, ∞_+ e ∞_-, ma questi sono ora definiti su $\mathbb{F}_{q^2}$ e si ha che $(\infty_+) = (\infty_-)$. Ponendo $(\infty) = (\infty_+) = (\infty_-)$ si avrà dunque che $\deg(\infty) = 2$.
L'omomorfismo di gruppi additivi $\varphi : \mathrm{Div}^0(C) \to A$ definito in 2.6 allora è dato da $\varphi\big(\sum_P m_P(P) + m(\infty)\big) = \sum_P m_P(P)$.
Per l'osservazione 2.7 si ha che Im $(\varphi) = A_2$, con
$A_2 = \big\{\sum m_P(P) \in A \big|\ 2 | \sum m_P \deg(P)\big\}$, quindi Im $(\psi) = \pi_{A'}(A_2) = A_2/A'$.

Supponiamo ancora che esista $\sum m_P(P) \in A$ tale che $\sum m_P \deg(P) = 1$,

allora A_2 è un sottogruppo di A di indice 2, quindi, per (2.2), si ha che

$$|G| = 2\frac{h}{|\text{Ker } (\varphi')|}$$

Per l'osservazione 2.9 inoltre Ker $(\varphi') = \{\overline{m(\infty)} \in Cl^0(C)\}$.
Ora, però, $\overline{m(\infty)} \in Cl^0(C) \Leftrightarrow m = 0$, quindi in questo caso φ' è iniettiva e

$$|G| = 2h \tag{3.9}$$

Osservazione 3.2.7.
Supponiamo ora che n sia dispari, quindi che C abbia un unico punto all'infinito, che denoteremo con ∞, definito su $\mathbb{F}_q$.
Come nel primo caso visto φ è suriettiva, infatti se $x = \sum_P m_P(P) \in A$ si ha che $x = \varphi\big(\sum_P m_P(P) + m(\infty)\big)$ con $m = -\sum_P m_P \deg(P)$.
Dunque anche ψ, φ' sono suriettive, dunque per (2.2)

$$|G| = \frac{h}{|\text{Ker } (\varphi')|}$$

Si può provare come nel caso precedente che φ' è iniettiva, quindi si ottiene che

$$|G| = h \tag{3.10}$$

Abbiamo quindi provato il seguente teorema:

Teorema 3.2.8.
Sia $C : Y^2 = d(X)$ una curva iperellittica affine definita su $\mathbb{F}_q$, con $q = p^k$, p primo, $p \neq 2$. Sia R l'anello delle coordinate di C, sia G il suo gruppo delle classi di ideali. Sia $h = |Cl^0(C)|$ l'ordine del gruppo delle classi dei divisori di grado 0 della chiusura proiettiva di C (o di una sua desingolarizzazione).

- *Se d ha grado pari e il suo coefficiente direttore è un quadrato in $\mathbb{F}_q$ allora*

  $$|G| = \frac{h}{m_0}$$

  con $m_0 = \min\{m \in \mathbb{N} |\ m = \text{ord}_{\infty_+}\big(a(X)+Yb(X)\big),\ a, b \in \mathbb{F}_q[X]$ tali che $a^2(X) - d(X)b^2(X) \in \mathbb{F}_q^*\}$.

- *Se d ha grado pari e il suo coefficiente direttore è un non quadrato in $\mathbb{F}_q$ allora*

$$|G| = 2h$$

- *Se d ha grado dispari allora*

$$|G| = h$$

3.3 Coniche

Sia ora C la curva definita da $Y^2 = d(X)$, con $d(X) \in \mathbb{F}_q[x]$ polinomio di grado 1 o 2 (dove $q = p^k$, con p primo, $p \neq 2$); C è dunque una conica e ha genere $g = 0$. Supponiamo ancora che d sia libero da quadrati e notiamo α il suo coefficiente direttore.

Osservazione 3.3.1.
Per l'osservazione 1.4.13 si ha che $b_n = h\dfrac{p^{n-g+1}-1}{p-1} = h\dfrac{p^{n+1}-1}{p-1}$ se $n > 2g-2 = -2$. Per $n = 0$ quindi si ha in particolare che $b_0 = h$.
D'altra parte, $b_0 = \#\{D \in \mathrm{Div}(\mathbb{K}) |\ \deg(D) = 0, D \geq 0\} = \#\{0\} = 1$, quindi si deve avere

$$h = 1 \tag{3.11}$$

Osservazione 3.3.2.
Supponiamo che d abbia grado 2 e che α sia un quadrato in $\mathbb{F}_q$, cioè supponiamo che C abbia 2 punti all'infinito, definiti su $\mathbb{F}_q$.
Allora, nelle notazioni della sezione precedente, per l'osservazione 3.2.3, si ha che $|G| = \dfrac{h}{|\mathrm{Ker}\ (\varphi')|}$. Per (3.11) dunque $|G| = \dfrac{1}{|\mathrm{Ker}\ (\varphi')|}$.
Necessariamente allora si deve avere che $|\mathrm{Ker}\ (\varphi')| = 1$, cioè φ' deve essere iniettiva. Di conseguenza si deve avere che

$$|G| = 1$$

In particolare dunque si è ottenuto che se $\alpha X^2 + \beta X + \gamma$ è libero da quadrati, con α quadrato in $\mathbb{F}_q$, allora il dominio di Dedekind

$R = \mathbb{F}_q[X,Y]/(Y^2 - \alpha X^2 - \beta X - \gamma)$ è sempre un anello a fattorizzazione unica.

Osservazione 3.3.3.
Supponiamo ora che d abbia grado 2 e che α sia un non quadrato in $\mathbb{F}_q$, cioè supponiamo che C abbia due punti all'infinito, definiti su $\mathbb{F}_{q^2}$ e coniugati.
Per quanto visto nella dimostrazione della proposizione 1.2.2, C ha almeno un punto affine definito su $\mathbb{F}_q$, cioè esiste $(P) \in A$ tale che $\deg(P) = 1$. Dunque per l'osservazione 3.2.6 si avrà che

$$|G| = 2h = 2$$

Osservazione 3.3.4.
Se d ha grado 1, quindi se C ha un unico punto all'infinito, definito su $\mathbb{F}_q$, per l'osservazione 3.2.7 si avrà che

$$|G| = h = 1$$

I domini di Dedekind $F_q[X,Y]/(Y^2 - \alpha X - \beta)$, con $\alpha, \beta \in \mathbb{F}_q$ sono dunque domini a fattorizzazione unica.

3.4 Curve ellittiche

Sia C la curva definita da $Y^2 = d(X)$, con $d \in \mathbb{F}_q[x]$ polinomio di quarto grado libero da quadrati (con $q = p^k$, p primo, $p \neq 2$); sia α il coefficiente direttore di d.

Osservazione 3.4.1.
Per l'osservazione 1.4.13 si ha che $b_n = h\dfrac{p^{n-g+1}-1}{p-1} = h\dfrac{p^n-1}{p-1}$ se $n > 2g - 2 = 0$. Per $n = 1$ quindi si ha in particolare che $b_1 = h$.
D'altra parte, $b_1 = \#\{D \in \mathrm{Div}(\mathbb{K}) |\ \deg(D) = 1, D \geq 0\} =$
$= \#\{(P) \in \mathrm{Div}(\mathbb{K}) |\ (P)$ divisore primo, $\deg(P) = 1\} = a_1$, quindi si deve avere

$$h = a_1 \tag{3.12}$$

Osservazione 3.4.2.
Supponiamo che $\alpha \neq 0$ sia un quadrato in $\mathbb{F}_q$, cioè supponiamo che ∞_+, ∞_- siano definiti su $\mathbb{F}_q$ (e distinti).
Per (3.7) e per (3.12) allora

$$|G| = \frac{a_1}{m_0}$$

dove, per l'osservazione 3.2.5,

$$m_0 = \min\{m \in \mathbb{N} |\ \exists f \in \mathbb{K} \text{ tale che } m\big((\infty_+) - (\infty_-)\big) = (f)\} =$$

$$= \min\big\{m \in \mathbb{N} |\ m = \mathrm{ord}_{\infty_+}\big(a(X)+Yb(X)\big),\ a, b \in \mathbb{F}_q[X] \text{ tali che } a^2(X) - d(X)b^2(X) \in \mathbb{F}_q^*\big\}$$

Osservazione 3.4.3.
Supponiamo ora che α non sia un quadrato in $\mathbb{F}_q$, cioè supponiamo che ∞_+, ∞_- siano definiti su $\mathbb{F}_{q^2}$ e siano coniugati. Sia $(\infty) = (\infty_+) = (\infty_-)$, certamente allora $\deg(\infty) = 2$.

La curva C ha almeno un punto affine definito su $\mathbb{F}_q$.
Infatti poiché i punti all'infinito di C non sono definiti su $\mathbb{F}_q$, il numero di punti affini di C definiti su $\mathbb{F}_q$ coincide con il numero di punti di C definiti su $\mathbb{F}_q$, a_1, e per il Teorema di Weil (Teorema 1.4.17) $a_1 \geq p + 1 - 2\sqrt{p} > 0$.

Dunque, per (3.9) si ha che

$$|G| = 2a_1$$

Osservazione 3.4.4.
Per il teorema 1.4.14, se $L \in \mathbb{Z}[X]$ è il polinomio tale che $\zeta(s) = \dfrac{L(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$ su $\{s \in \mathbb{C} |\ \mathrm{Re}(s) > 1\}$, con $\deg L = 2g$, allora $L(1) = h$, quindi in particolare nel caso delle curve ellittiche si ha che $L(1) = a_1$.

Abbiamo quindi dimostrato il seguente teorema:

Teorema 3.4.5.
Sia C la curva ellittica definita da $Y^2 = d(X)$, con $d(X) \in \mathbb{F}_q[X]$ polinomio di grado 4 libero da quadrati, sia α il coefficiente direttore di d.
Sia $R = \mathbb{F}_q[X,Y]/(Y^2 - d(X))$, sia G il gruppo delle classi di ideali di R.

- *Se α è un quadrato in $\mathbb{F}_q$ allora*

$$|G| = \frac{L(1)}{m_0} \tag{3.13}$$

con $m_0 = \min\left\{m \in \mathbb{N} |\ m = \mathrm{ord}_{\infty_+}\big(a(X)+Yb(X)\big),\ a, b \in \mathbb{F}_q[X]\ \textit{tali che}\ a^2(X) - d(X)b^2(X) \in \mathbb{F}_q^*\right\}$.

- *Se α non è un quadrato in $\mathbb{F}_q$ allora*

$$|G| = 2L(1) \tag{3.14}$$

Il precedente teorema richiama dunque la forma del Teorema di Dirichlet per il numero di classi di ideali (teorema 3.1.1). Abbiamo quindi trovato, nel contesto degli anelli delle coordinate associati a curve ellittiche, un risultato analogo a questo classico teorema sugli anelli quadratici.

3.4.1 Congetture di Gauss

Nel caso degli anelli delle coordinate associati a curve ellittiche valgono dei risultati analoghi alle congetture di Gauss per gli anelli quadratici, che però, in questo contesto, possono essere provati in modo più semplice.

Sia E l'insieme dei polinomi di quarto grado, irriducibili, liberi da quadrati ed a coefficienti in un campo finito $\mathbb{F}_q$, per tutti i $q = p^k$, con p primo, $p \neq 2, 3$. Sia E_+ il sottoinsieme di E formato dai polinomi con coefficiente direttore quadrato e sia E_- il sottoinsieme di E formato dai polinomi con coefficiente direttore non quadrato.
Fissato un polinomio $d \in E$, la curva di equazioni $Y^2 = d(X)$ è dunque una curva ellittica; denotiamo ancora con R il suo anello delle coordinate e con G il gruppo delle classi di ideali di R.

La congettura di Gauss sui campi quadratici reali ha un analogo in E_+ e la congettura di Gauss sui campi quadratici immaginari ha un analogo in E_-.

Osservazione 3.4.6.
Sia $d \in E_-$ un polinomio a coefficienti in $\mathbb{F}_q$, sia C la curva ellittica di equazione $Y^2 = d(X)$; per il teorema 3.4.5 si ha che $|G| = 2a_1$.
D'altra parte, per il Teorema di Weil (1.4.17) $q+1-2\sqrt{q} \leq a_1 \leq q+1+2\sqrt{q}$, dunque $2(\sqrt{q}-1)^2 \leq |G| \leq 2(\sqrt{q}+1)^2$.

Fissato $n \in \mathbb{N}$ dunque può esistere $d \in E_-$ a coefficienti in $\mathbb{F}_q$ tale che la curva ellittica di equazione $Y^2 = d(X)$ abbia esattamente n classi di ideali soltanto se $2(\sqrt{q}-1)^2 \leq n$, cioè soltanto se $q \leq \left(\sqrt{\frac{n}{2}}+1\right)^2$.

Dunque per ogni fissato $n \in \mathbb{N}$ esiste solo un numero finito di polinomi $d \in E_-$ tali che l'anello delle coordinate della curva di equazione $Y^2 = d(X)$ abbia numero di classi di ideali n.

Inoltre, per ogni $q > 3$ certamente si può trovare un polinomio $d_q \in E_-$ a coefficienti in $\mathbb{F}_q$. Denotiamo con C_q la curva ellittica di equazione
$C_q : Y^2 = d_q(X)$. Sia G_q il gruppo delle classi di ideali dell'anello delle coordinate associato a C_q, allora si dovrà avere che $2(\sqrt{q}-1)^2 \leq |G_q| \leq$
$\leq 2(\sqrt{q}+1)^2$, quindi

$$|G_q| \to \infty \text{ per } q \to \infty$$

Per trattare il caso di E_+ sono necessarie alcune considerazioni preliminari.

Osservazione 3.4.7.
Nelle notazioni della sezione precedente si ha che, nel caso delle curve ellittiche, m_0 non può essere 1.

Sia C una curva ellittica definita su $\mathbb{F}_q$, cioè una curva di genere $g = 1$. Per il corollario 1.4.6 al teorema di Riemann-Roch allora per ogni divisore $D \in \mathrm{Div}(\mathbb{K})$, con $\mathbb{K}$ campo di funzioni di C, tale che $\deg(D) > 2g-2 = 0$ si deve avere che $l(D) = \deg(D) - g + 1 = \deg(D)$. In particolare dunque per ogni punto $Q \in C(\mathbb{F}_q)$ si ha che $l\big((Q)\big) = \deg\big((Q)\big) = 1$, cioè $L\big((Q)\big)$ è un $\mathbb{F}_q$-spazio vettoriale di dimensione 1, cioè $L\big((Q)\big) = \mathbb{F}_q$.

Ora, se esistesse $f = a(X) + Yb(X) \in R$ tale che $(f) = (\infty_+) - (\infty_-)$ si avrebbe che $f \in L\big((\infty_-)\big) \setminus \mathbb{F}_q$, contraddizione.
Quindi $m_0 = \min\big\{m \in \mathbb{N} |\ \exists f \in R \text{ tale che } (f) = m\big((\infty_+) - (\infty_-)\big)\big\} > 1$.

Teorema 3.4.8. Teorema di Deuring[2]
Sia $q = p^k$, con p primo, sia $t \in \mathbb{Z}$ tale che $|t| \leq 2\sqrt{q}$. Allora esiste una curva ellittica C_t definita su $\mathbb{F}_q$ tale che $C_t(\mathbb{F}_q) = q + 1 - t$ se e solo se vale una delle seguenti condizioni:

- $\mathrm{MCD}(t, p) = 1$
- *k è dispari e*
  - $t = 0$
  - $t = \pm\sqrt{pq}$ *con* $p = 2, 3$
- *k è pari e*
  - $t = 0$ *con* $p = 2$ *o* $p \equiv 3 \pmod 4$
  - $t = \pm\sqrt{q}$ *con* $p = 3$ *o* $p \equiv 2 \pmod 3$
  - $t = \pm 2\sqrt{q}$

Osservazione 3.4.9.
In particolare dal teorema precedente segue che per ogni primo p, per ogni $t \in \mathbb{Z}$ tale che $|t| \leq 2\sqrt{p}$ esiste almeno una curva ellittica C_t definita su $\mathbb{F}_p$ tale che $C_t(\mathbb{F}_p) = p + 1 - t$.

Nel caso dei campi con un numero primo di elementi si può ottenere un risultato più preciso.
Sia p primo, $p \geq 5$; per $\alpha, \beta \in \mathbb{F}_p$, sia $C_{\alpha,\beta}$ la curva ellittica di equazione $Y^2 = X^3 + \alpha X + \beta$ (si può provare che ogni curva ellittica definita su $\mathbb{F}_q$, con $\mathrm{car}\, \mathbb{F}_q \neq 2, 3$ è equivalente ad una tale curva che, così espressa, viene detta "in forma di Weierstrass").

[2]Questo teorema è stato provato da Deuring nel 1941 in [3]

Si può allora provare[3] che per ogni fissato $t \in \mathbb{Z}$, con $|t| \leq 2\sqrt{p}$, si ha che $\#\{(\alpha, \beta) \in \mathbb{F}_p^2 |\ \#C_{\alpha,\beta}(\mathbb{F}_p) = p+1-t\} = g(t^2-4p)$, con $g(d)$ numero di classi di ideali di $\mathbb{Q}(\sqrt{d})$.

Osservazione 3.4.10.
Sia $C : Y^2 = f(X)$ una curva iperellittica definita su un campo finito $\mathbb{F}_q$.
Per il teorema di Weil se q è sufficientemente grande (rispetto ad una funzione del genere di C, quindi del grado di f) deve esistere $a \in \mathbb{F}_q$ tale che $f(a)$ sia un quadrato in $\mathbb{F}_q$.
La trasformazione $\begin{cases} X_1 = X + a \\ Y_1 = Y \end{cases}$ allora muta C in una curva iperellittica $C_1 : Y^2 = f_1(X)$, con $\deg f_1 = \deg f$, tale che il termine noto di f_1 è un quadrato in $\mathbb{F}_q$.

In particolare si ha che per $q \geq 7$ ogni curva ellittica definita su $\mathbb{F}_q$ è equivalente ad una curva di equazione $Y^2 = X^3 + \alpha X^2 + \beta X + \gamma$ con γ quadrato in $\mathbb{F}_q$.

Osservazione 3.4.11.
Sia $C : Y^2 = X^3 + \alpha X^2 + \beta X + \gamma$ una curva ellittica definita su $\mathbb{F}_q$; supponiamo che γ sia un quadrato in $\mathbb{F}_q$.
Siano $x_1, x_2, x_3 \in \overline{\mathbb{F}}_q$ tali che $X^3 + \alpha X^2 + \beta X + \gamma = (X - x_1)(X - x_2)(X - x_3)$ e sia $e \in \mathbb{F}_q$. Sia C_1 la curva di equazione $Y^2 = d_1(X)$,
con $d_1(X) = (X - e)(-x_1 X + 1 + x_1 e)(-x_2 X + 1 + x_2 e)(-x_3 X + 1 + x_3 e)$.
C_1 è ancora una curva ellittica definita su $\mathbb{F}_q$ e, poiché $-x_1 x_2 x_3 = \gamma$, $d_1 \in E_+$.
Inoltre, l'applicazione $\varphi(x, y) = (x^{-1} + e, yx^{-2})$, ovviamente definita su $\mathbb{F}_q \setminus \{0\} \times \mathbb{F}_q$, dà una corrispondenza biunivoca tra $C(\mathbb{F}_q) \setminus \{(0, c), (0, -c), \infty\}$, con $c^2 = \gamma$, e $C_1(\mathbb{F}_q) \setminus \{(e, 0), \infty_+, \infty_-\}$.
Dunque $\#C(\mathbb{F}_q) = \#C_1(\mathbb{F}_q)$.

Se C è una curva ellittica definita su $\mathbb{F}_q$ da un'equazione della forma $Y^2 = X^3 + \alpha X^2 + \beta X + \gamma$, con γ non quadrato, si può provare analogamente

[3] Si veda Birch [1]

che esiste una curva $C_1 : Y^2 = d_1(X)$, con d_1 polinomio di quarto grado di coefficiente direttore γ, tale che $\#C(\mathbb{F}_q) = \#C_1(\mathbb{F}_q)$.

Osservazione 3.4.12.
Per il teorema 3.4.8 e per le osservazioni 3.4.10, 3.4.11, per ogni q potenza di un primo sufficientemente grande, per ogni primo p tale che $q + 1 - 2\sqrt{q} \leq \leq p \leq q + 1 + 2\sqrt{q}$ e che soddisfi le ipotesi del teorema di Deuring esiste un polinomio $d_{q,p} \in E_+$ a coefficienti in $\mathbb{F}_q$ tale che, notando $C_{q,p}$ la curva di equazione $Y^2 = d_{q,p}(X)$, si abbia $\#C_{q,p}(\mathbb{F}_q) = p$.
Denotiamo con $G_{q,p}$ il gruppo delle classi di ideali dell'anello delle coordinate associato a $C_{q,p}$, allora per il teorema 3.4.5 $|G_{q,p}| = \dfrac{p}{m^0_{q,p}}$.
Poiché p è un numero primo e poiché per l'osservazione 3.4.7 $m^0_{q,p} > 1$ si dovrà avere $m^0_{q,p} = p$, cioè

$$|G_{q,p}| = 1$$

Dunque esiste un'infinità di polinomi $d \in E_+$ tali che l'anello delle coordinate della curva di equazione $Y^2 = d(X)$ sia un dominio di Dedekind a fattorizzazione unica.

Abbiamo quindi dimostrato il seguente teorema, analogo per gli anelli delle coordinate di curve ellittiche alle congetture di Gauss:

Teorema 3.4.13.
Sia E l'insieme dei polinomi di quarto grado, irriducibili, liberi da quadrati ed a coefficienti in un campo finito $\mathbb{F}_q$, per tutti i $q = p^k$, con p primo, $p \neq 2, 3$. Sia E_+ il sottoinsieme di E formato dai polinomi il cui coefficiente direttore è un quadrato e sia $E_- = E \setminus E_+$. Allora:

- *per ogni fissato $n \in \mathbb{N}$ esiste solo un numero finito di polinomi $d \in E_-$ tali che l'anello delle coordinate della curva di equazione $Y^2 = d(X)$ abbia numero di classi di ideali n*
- *esiste un'infinità di polinomi $d \in E_+$ tali che l'anello delle coordinate della curva di equazione $Y^2 = d(X)$ sia un dominio di Dedekind a fattorizzazione unica.*

Si possono in effetti trovare risultati più precisi. Per esempio, per il caso di E_+, C. Friesen e P. van Wamelen hanno provato in [5] i due seguenti teoremi:

Teorema 3.4.14.
Sia $\mathbb{F}_q$ un campo finito con $\operatorname{car} \mathbb{F}_q > 3$. *Allora esistono almeno* $\dfrac{q^{\frac{7}{2}}}{10 \log\log q}$ *polinomi $d \in \mathbb{F}_q[x]$ di quarto grado, monici, irriducibili e liberi da quadrati tali che l'anello delle coordinate della curva $Y^2 = d(X)$ ha una sola classe di ideali (cioè è un dominio a fattorizzazione unica).*

Teorema 3.4.15.
Sia $h \in \mathbb{N}$ dispari, allora esiste $N \in \mathbb{N}$ tale che per ogni $q > N$, con $q = p^k$, p primo, $p > 3$, esiste $d \in \mathbb{F}_q[X]$ polinomio di quarto grado, monico, irriducibile e libero da quadrati tale che l'anello delle coordinate della curva $Y^2 = d(X)$ ha esattamente h classi di ideali.

Conclusioni

Abbiamo quindi provato un risultato analogo al Teorema di Dirichlet per anelli quadratici nel caso degli anelli delle coordinate di curve ellittiche definite su campi finiti. Questa analogia risulta particolarmente evidente ponendo in parallelo i due enunciati:

Sia $D \in \mathbb{Z}$, $D \neq 1$, libero da quadrati, sia $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, sia R l'anello degli interi algebrici di $\mathbb{K}$, sia d il discriminante di $\mathbb{K}$. Sia G il gruppo delle classi di ideali di R e sia $L(s) = \prod_{p \text{ primo}} \left(1 - \left(\frac{d}{p}\right) p^{-s}\right)^{-1}$.

- Se $D > 0$ allora

$$|G| = L(1)\frac{\sqrt{d}}{2\log \varepsilon_0}$$

con $\varepsilon_0 = \dfrac{x + y\sqrt{d}}{2} > 1$ unità fondamentale, quindi soluzione dell'equazione di Pell $X^2 - dY^2 = \pm 4$.

Sia C la curva ellittica definita da $Y^2 = d(X)$, con $d(X) \in \mathbb{F}_q[X]$ polinomio di grado 4 libero da quadrati, sia α il coefficiente direttore di d. Sia R l'anello delle coordinate di C, sia G il gruppo delle classi di ideali di R.

- Se α è un quadrato in $\mathbb{F}_q$ allora

$$|G| = \frac{L(1)}{m_0}$$

con $m_0 = \min\big\{m \in \mathbb{N} | \; m = \mathrm{ord}_{\infty_+}\big(a(X) + Yb(X)\big), \; a, b \in \mathbb{F}_q[X] \text{ tali che } a^2(X) - d(X)b^2(X) \in \mathbb{F}_q^*\big\}$.

- Se $D < 0$ allora

$$|G| = L(1)\frac{w\sqrt{|d|}}{2\pi}$$

con w numero delle radici dell'unità in $\mathbb{K}$.

- Se α non è un quadrato in $\mathbb{F}_q$ allora

$$|G| = 2L(1)$$

Per quanto visto, tale parallelo vale anche per le curve iperellittiche.
In effetti, come provato da Rosen in [9], si può trovare un risultato ancora più vicino al Teorema di Dirichlet; la sua dimostrazione però prevede l'utilizzo di tecniche più complesse.

Il parallelo fra anelli quadratici e anelli delle coordinate di curve ellittiche può essere ulteriormente sviluppato ed in particolare si può trovare un analogo delle congetture di Gauss:

- Per ogni $n \in \mathbb{N}$ esiste solo un numero finito di campi quadratici *immaginari* con numero di classi n

- Per ogni $n \in \mathbb{N}$ esiste solo un numero finito di polinomi d di quarto grado, irriducibili, liberi da quadrati, a coefficienti in un campo finito e di *coefficiente direttore non quadrato* tali che l'anello delle coordinate della curva di equazione $Y^2 = d(X)$ abbia numero di classi n

- Esistono infiniti campi quadratici *reali* con una sola classe di ideali

- Esiste un'infinità di polinomi d di quarto grado, irriducibili, liberi da quadrati, a coefficienti in un campo finito e di *coefficiente direttore quadrato* tali che l'anello delle coordinate della curva di equazione $Y^2 = d(X)$ sia un dominio di Dedekind a fattorizzazione unica.

Questa situazione non è eccezionale: nello studio delle curve definite su campi finiti si possono ritrovare gli analoghi di diversi risultati fondamentali di teoria dei numeri che, in genere, in questo contesto sono più facilmente dimostrabili che nel contesto classico. Per esempio, abbiamo visto come l'ipotesi di Riemann e le congetture di Gauss, ancora irrisolte, hanno analoghi, rispettivamente nel contesto delle curve non singolari e in quello delle curve ellittiche, che invece possono essere provati.

Appendice A

Domini di Dedekind

A.1 Anelli noetheriani

Definizione A.1.1.
Sia A un anello commutativo unitario; si dice che A è **noetheriano** se ogni ideale di A è finitamente generato.

Proposizione A.1.1.
Un anello commutativo unitario A è noetheriano se e solo se ogni catena ascendente di ideali distinti di A è finita.

Dimostrazione.

Sia A un anello noetheriano, sia $I_1 \subsetneq I_2 \subseteq \cdots$ una catena ascendente di ideali di A. Certamente $\mathscr{I} = \cup_i I_i$ è ancora un ideale di A, quindi per ipotesi deve essere finitamente generato. Per k sufficientemente grande tutti i generatori di $\mathscr{I}$ dovranno appartenere ad I_k, dunque $\mathscr{I} = I_k$, cioè la catena considerata è finita.

Sia A un anello tale che ogni catena ascendente di ideali distinti di A è finita. Se esistesse un ideale I di A non finitamente generato, si potrebbero trovare $x_1, x_2, \ldots \in I$ tali che $x_{i+1} \notin (x_1, \ldots, x_i)\ \forall i$, quindi
$(x_1) \subsetneq (x_1, x_2) \subsetneq \cdots$ sarebbe una catena ascendente infinita di ideali distinti di A, contraddizione. Dunque A deve essere noetheriano. □

Osservazione A.1.2.
Sia A un anello noetheriano e sia I un suo ideale; allora, poiché gli ideali di A/I sono in corrispondenza biunivoca con gli ideali di A che contengono I, A/I è ancora un anello noetheriano.

Proposizione A.1.3.
Sia A un anello noetheriano, allora $A[x]$ è ancora un anello noetheriano.

Dimostrazione.
Sia I un ideale di A; proviamo che I è finitamente generato.
Per $n \in \mathbb{N}$, sia $M_n = \{p \in A[X] |\ \deg p \leq n\}$, M_n è allora un sottomodulo di $A[X]$ finitamente generato. Sia $I_n = I \cap M_n$, I_n è dunque un sottomodulo di $A[X]$. Sia $f_n : M_n \to A$ l'omomorfismo di A-moduli definito da
$f_n(a_0 + \cdots + a_n X^n) = a_n$, sia $J_n = f_n(I_n)$; J_n è un sottomodulo di A, cioè un ideale di A. Certamente $J_{n+1} \supset J_n\ \forall n \in \mathbb{N}$, dunque $(J_n)_{n\in\mathbb{N}}$ è una catena ascendente di ideali di A. Poiché per ipotesi A è noetheriano, la successione (J_n) deve essere stazionaria, cioè $\exists N \in \mathbb{N}$ tale che $J_m = J_N\ \forall m \geq N$.
Ora, I_N è un sottomodulo di M_N, quindi è finitamente generato, siano $a_1, \ldots, a_m$ generatori di I_N. Sia I' l'ideale di $A[X]$ generato dagli a_i,
$I' = (a_1, \ldots, a_n)$; proviamo che $I' = I$.
Certamente $a_i \in I\ \forall i$, quindi $I' \subseteq I$.
Sia $p \in I$; se $\deg p \leq N$ certamente $p \in I_N$, quindi $p \in I'$. Sia $m > N$, supponiamo per ipotesi induttiva che $p \in I'\ \forall p \in I$ con $\deg p < m$; sia $p \in I$ tale che $\deg p = m$. Sia $a_m = f_m(p)$, allora $a_m \in J_m = J_N$, quindi esiste $p_0 \in I_N$ di coefficiente direttore a_m, sia $\deg p_0 = n$. Allora $p = X^{m-n}p_0 + q$, con $\deg q < m$. Ora, $X^{m-n}p_0 \in I'$, quindi $X^{m-n}p_0 \in I$, quindi $q \in I$. Poiché $\deg q < m$, per ipotesi induttiva $q \in I'$, quindi si ha che $p \in I'$. □

Corollario A.1.4.
Se A è un anello noetheriano allora $A[X_1, \ldots, X_n]$ è noetheriano $\forall n \in \mathbb{N}$.

A.2 Anelli a fattorizzazione unica

Definizione A.2.1.
Sia A un dominio di integrità; si dice che A è un dominio a **fattorizzazione unica** se ogni suo elemento non nullo e non invertibile si decompone in modo essenzialmente unico come prodotto di irriducibili.

Proposizione A.2.1.
Sia A un dominio a fattorizzazione unica, allora:

1. *per ogni $x, y \in A$ si ha che $x|y$ se e solo se tutti i fattori di x compaiono, con esponente maggiore o uguale, anche nella decomposizione di y*
2. *ogni famiglia finita di elementi di A ha massimo comun divisore e minimo comune multiplo*
3. *se $x|yz$ e $(x, y) = 1$ si ha che $x|z$*
4. *se $x \in A$ è irriducibile e $x|a_1 \cdots a_m$ deve esistere i tale che $x|a_i$*

A.3 Anelli a ideali principali

Definizione A.3.1.
Sia A un dominio di integrità, si dice che A è un dominio a **ideali principali** se ogni ideale di A è principale.

Proposizione A.3.1.
Sia A un dominio a ideali principali, allora A è noetheriano.

Dimostrazione.
È sufficiente provare che ogni catena ascendente di ideali principali distinti è finita.
Sia $(a_0) \subsetneq (a_1) \subsetneq \cdots$ una tale catena, sia $I = \cup_i (a_i)$, allora I è ancora un ideale di A, quindi esiste $a \in A$ tale che $I = (a)$. Certamente esiste m tale che $a \in (a_m)$; allora $(a) = (a_m)$ e la catena considerata è finita. □

Proposizione A.3.2.
Sia A un anello a ideali principali, allora:

1. *se $F \subseteq A \setminus \{0\}$, d è un massimo comun divisore di F se e solo se $(d) = (F)$ e m è un minimo comune multiplo di F se e solo se $(m) = \bigcap_{x \in F} (x)$.*
2. *se $x, y \in A$ si ha che $(x, y) = 1$ se e solo se esistono $u, v \in A$ tali che $xu + yv = 1$*
3. *se $x|yz$ e $(x, y) = 1$ si ha che $x|z$*
4. *se $x \in A$ è irriducibile e $x|a_1 \cdots a_m$ esiste i tale che $x|a_i$.*

Proposizione A.3.3.
Sia A un dominio a ideali principali, allora A è un dominio a fattorizzazione unica.

Dimostrazione.
Sia $x \in A \setminus \{0\}$ non invertibile, allora x ha almeno un divisore irriducibile. Questo è certamente vero se x è irriducibile. Supponiamo che $x = x_0$ sia riducibile, sia x_1 un divisore proprio di x; se x_1 è riducibile, sia x_2 un suo divisore proprio, e così via. Per la proposizione A.3.1, la catena $(x) = (x_0) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$ così ottenuta deve essere finita, cioè deve esistere n tale che x_n è un divisore irriducibile di x.
Ora, sia $x \in A$; se x non è irriducibile esiste p_1 irriducibile tale che $p_1|x$. Sia $x = p_1 y_1$, ancora, se y_1 non è irriducibile, esiste p_2 irriducibile tale che $p_2|y_1$. Iterando questo procedimento si ottiene la catena $(y_1) \subsetneq (y_2) \subsetneq \cdots$; poiché questa deve essere finita deve esistere k tale che $y_k = p_k$ è irriducibile, quindi tale che $p_1 \dots p_k$ è una decomposizione in irriducibili di x.

Supponiamo che esistano elementi non invertibili di $A \setminus \{0\}$ che ammettano diverse scomposizioni come prodotti di irriducibili. Sia $x = p_1 \cdots p_r = q_1 \cdots q_s$ un tale elemento di A, con $p_1, \dots, p_r, q_1, \dots, q_s \in A$ irriducibili;

supponiamo che x sia scelto in modo che il numero r di irriducibili che compaiono nella prima decomposizione sia minimo. Ora, $p_1|q_1 \cdots q_s$, quindi esiste i tale che $p_1|q_i$; supponiamo che $p_1|q_1$. Poiché p_1, q_1 sono irriducibili, si deve avere $p_1 = \varepsilon_1 q_1$, con $\varepsilon_1 \in A$ invertibile. Sia $y = p_1^{-1}x$, allora $y = \varepsilon_1 p_2 \cdots p_r = q_2 \cdots q_s$, cioè y avrebbe due diverse fattorizzazioni, una delle quali formata da $r-1$ elementi irriducibili, contraddizione. □

A.4 Anelli integralmente chiusi

Definizione A.4.1.
Sia A un dominio, sia $\mathbb{K}$ un campo tale che $A \subseteq \mathbb{K}$, sia $x \in \mathbb{K}$; si dice che x è **intero** su A se $\exists a_0, \ldots, a_{n-1} \in A$ tali che $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = 0$.

Proposizione A.4.1.
Nelle ipotesi della definizione precedente si ha che sono equivalenti:

1. *x è intero su A*
2. *$A[x]$ è un A-modulo finitamente generato*
3. *Esiste un A-modulo finitamente generato non nullo $M \subseteq \mathbb{K}$ tale che $xM \subseteq M$.*

Dimostrazione.

1. $\Rightarrow$ 2. Sia $n \in N$ tale che esistano $a_0, \ldots, a_{n-1} \in A$ con $a_0 + \cdots + a_{n-1}x^{n-1} + + a_n x^n = 0$, allora $A[x]$ è l'A-modulo generato da $\{1, \ldots, x^{n-1}\}$.

2. $\Rightarrow$ 3. Sia $M = A[x]$, certamente $xA[x] \subseteq A[x]$.

3. $\Rightarrow$ 1. Siano $z_1, \ldots, z_m$ generatori di M; poiché $xM \subseteq M$, $\forall i = 1, \ldots, m$ $\exists b_{ij} \in A,\ j = 1, \ldots m$, tali che $xz_i = \sum_j b_{ij} z_j$. Ora, poiché M è non nullo, gli z_i non sono tutti nulli, quindi $(z_1, \ldots, z_m)$ è una soluzione non banale del sistema lineare omogeneo $(b_{ij} - x\delta_{ij}) = Z$, quindi si deve avere $\det(b_{ij} - x\delta_{ij}) = 0$, equazione polinomiale in x a coefficienti in A con coefficiente direttore ± 1. □

Corollario A.4.2.
Sia $\mathbb{K}$ *un campo, sia* A *un suo sottoanello, allora gli elementi di* $\mathbb{K}$ *interi su* A *formano un anello*

Dimostrazione.
Siano $a, b \in \mathbb{K}$ interi su A. Per la proposizione precedente esistono M, N A-moduli finitamente generati non nulli tali che $aM \subseteq M,\ bN \subseteq N$.
Certamente MN è ancora un A-modulo finitamente generato. Inoltre, $(a \pm b)MN \subseteq MN$ e $(ab)MN \subseteq MN$, quindi $a \pm b, ab$ sono interi su A. □

Definizione A.4.2.
Nelle notazioni precedenti, l'anello degli elementi di $\mathbb{K}$ interi su A è detto la **chiusura integrale** di A in $\mathbb{K}$.
Sia $\mathbb{K}$ il campo dei quozienti di A; se A coincide con la sua chiusura integrale in $\mathbb{K}$ si dice che A è **integralmente chiuso**.

A.5 Ideali frazionari

Definizione A.5.1.
Sia A un dominio di integrità, sia $\mathbb{K}$ il suo campo dei quozienti.
Un **ideale frazionario** di A è un A-modulo $I \subseteq \mathbb{K}$ non nullo tale che $\exists a \in A,\ a \neq 0$, con $aI \subseteq A$.

Osservazione A.5.1.
Ogni ideale frazionario di A contenuto in A è un ideale di A.
Ogni ideale non nullo di A è un suo ideale frazionario.

Definizione A.5.2.
Siano I_1, I_2 ideali frazionari di A. Si definisce il prodotto di I_1, I_2 come $I_1 I_2 = \left\{ \sum_{i=1}^{m} a_i b_i |\ m \in \mathbb{N}, a_i \in I_1,\ b_i \in I_2\ \forall i \right\}$.

Osservazione A.5.2.
Se I_1, I_2 sono ideali frazionari di A anche $I_1 I_2$ lo è. Infatti certamente $I_1 I_2 \subseteq \mathbb{K}$ è un A-modulo non nullo e se $x, y \in A \setminus \{0\}$ sono tali che $xI_1 \subseteq A,\ yI_2 \subseteq A$ allora $(xy) I_1 I_2 \subseteq A$.
L'insieme degli ideali frazionari di A dunque forma un semigruppo abeliano con unità (A).

Osservazione A.5.3.
Sia A un dominio di integrità, sia $\mathbb{K}$ il suo campo dei quozienti. Sia $I \subseteq \mathbb{K}$ un ideale frazionario di A, sia $I' = \{x \in \mathbb{K} |\ xI \subseteq A\}$.
Certamente I' è un A-modulo non nullo.
Sia $y \in I,\ y \neq 0$, sia $a \in A,\ a \neq 0$, tale che $ay \in A$. Allora $ay \in A \cap I$, dunque $\forall x \in I'$ si ha che $x(ay) \in A$. I' è quindi un ideale frazionario.
Certamente $II' \subseteq A$, dunque II' è un ideale di A.
Se I è tale che $II' = A$ si dice che I è **invertibile** e si nota $I' = I^{-1}$.

Osservazione A.5.4.

Ogni ideale frazionario principale, cioè ogni ideale frazionario della forma aA con $a \in \mathbb{K}$, è invertibile e il suo inverso è $a^{-1}A$.

Se I_1, I_2 sono ideali frazionari di A tali che $I_1 I_2 = A$ allora $I_2 = I_1^{-1}$. Infatti certamente $I_2 \subseteq I_1'$, quindi $A = I_1 I_2 \subseteq I_1 I_1' \subseteq A$, quindi I_1 è invertibile e $I_1' = I_1' A = I_1' I_1 I_2 = A I_2 = I_2$.

Se I_1, I_2 sono ideali frazionari invertibili di A anche $I_1 I_2$ è un ideale invertibile (di inverso $I_1^{-1} I_2^{-1}$). Gli ideali frazionari invertibili di A dunque formano un gruppo moltiplicativo.

A.6 Domini di Dedekind

Definizione A.6.1.
Sia A un dominio di integrità; si dice che A è un **dominio di Dedekind** se A è noetheriano, se ogni ideale primo non nullo di A è massimale e se A è integralmente chiuso.

Teorema A.6.1.
Sia A un dominio; A è un dominio di Dedekind se e solo se ogni ideale frazionario di A è invertibile

Lemma A.6.2.
Sia A un dominio noetheriano, sia $I \neq (0), A$ un ideale di A. Allora esistono $P_1, \dots, P_r$ ideali primi di A tali che $P_1 \cdots P_r \subseteq I \subseteq P_1 \cap \cdots \cap P_r$.

Dimostrazione.
Supponiamo per assurdo che esistano ideali di A, diversi da (0) e A, per cui non vale la proprietà considerata. Sia I un elemento massimale di tale insieme.
Certamente I non è primo, quindi esistono $m, n \notin I$ tali che $mn \in I$.
Siano $M = I + mA,\ N = I + nA$, allora $MN \subseteq I \subseteq M \cap N$.
Si deve avere che $M, N \neq A$. Infatti se si avesse $M = A$ si avrebbe $N = AN \subseteq I \subseteq A \cap N = N$, quindi $I = N$, quindi in particolare $n \in I$, contraddizione.
Poiché $I \subseteq M,\ I \subseteq N$, per come è stato scelto I certamente M, N soddisfano la proprietà considerata, cioè esistono $P_1, \dots, P_r, Q_1, \dots, Q_s$ ideali primi di A tali che $P_1 \cdots P_r \subseteq M \subseteq P_1 \cap \cdots \cap P_r$ e $Q_1 \cdots Q_s \subseteq N \subseteq Q_1 \cap \cdots \cap Q_s$.
Allora $P_1 \cdots P_r Q_1 \cdots Q_s \subseteq MN \subseteq I \subseteq M \cap N \subseteq P_1 \cap \cdots \cap P_r \cap Q_1 \cdots \cap Q_s$, assurdo. □

Lemma A.6.3.
Sia A un dominio noetheriano integralmente chiuso tale che ogni ideale primo non nullo di A è massimale. Allora ogni ideale primo non nullo di A è invertibile.

Dimostrazione.
Sia P un ideale primo non nullo di A. Sia $a \in P,\ a \neq 0$, siano $P_1, \dots, P_k$ ideali primi di A tali che $P_1 \cdots P_k \subseteq aA$, con k minimo.
Ora, certamente esiste i tale che $P_i \subseteq P$; supponiamo che $P_1 \subseteq P$. Poiché per ipotesi gli ideali primi non nulli di A sono massimali, si deve avere $P = P_1$.
$P_2 \cdots P_k \nsubseteq aA$, quindi esiste $b \in P_2 \cdots P_k \setminus aA$. Allora $bP \subseteq PP_2 \cdots P_k \subseteq aA$,

dunque $ba^{-1}P \subseteq A$, cioè $ba^{-1} \in P'$.
Poiché P è un ideale di A, certamente $A \subseteq P'$; d'altra parte, $ba^{-1} \notin A$, dunque $A \subsetneq P'$.
Abbiamo visto che in generale PP' è un ideale di A; proviamo che in questo caso $PP' = A$.
Si ha che $P = AP \subseteq P'P \subseteq A$. Poiché P è primo, quindi massimale, o $PP' = A$ o $PP' = P$. Supponiamo che $PP' = P$, allora $P(P')^n = P \ \forall n \in \mathbb{N}$, quindi $\forall x \in P,\ x \neq 0,\ \forall y \in P' \setminus A$ si ha che $xy^n \in P \subseteq A$. Quindi $xA[y] \subseteq A$, quindi $xA[y]$ è un ideale di A. Poiché A è un dominio noetheriano, $xA[y]$ deve essere finitamente generato; sia $\{a_1, \ldots, a_m\}$ un sistema di generatori per $xA[y]$. L'A-modulo $A[y]$ è dunque generato da $\{x^{-1}a_1, \ldots, x^{-1}a_m\}$.
Per la proposizione A.4.1 allora y è intero su A quindi, poiché per ipotesi A è integralmente chiuso, $y \in A$, contraddizione.
Si deve dunque avere $PP' = A$, cioè P deve essere invertibile. □

Lemma A.6.4.
Sia A un dominio noetheriano integralmente chiuso tale che ogni ideale primo non nullo di A è massimale. Allora ogni ideale proprio di A coincide con un prodotto di ideali primi.

Dimostrazione.
Supponiamo per assurdo che esistano ideali propri di A che non coincidono con un prodotto di ideali primi. Sia I un tale ideale; per il lemma A.6.2 esistono $P_1, \ldots, P_k$ ideali primi di A tali che $P_1 \cdots P_k \subseteq I$. Supponiamo che I sia stato scelto in modo che k sia minimo.
Si deve avere $k \geq 2$, infatti se si avesse $k = 1$ si avrebbe $P_1 \subseteq I$, quindi, poiché ogni ideale primo di A è massimale, $P_1 = I$, contraddizione.
Per il lemma A.6.3 P_1 è invertibile e $P_2 \cdots P_k \subseteq P_1^{-1}I \subseteq P_1^{-1}P_1 = A$, quindi $P_1^{-1}I$ è ancora un ideale di A.
Per come è stato scelto I, $P^{-1}I$ deve coincidere con un prodotto di ideali primi di A, cioè devono esistere $Q_1, \ldots, Q_s \subseteq A$ tali che $Q_1 \cdots Q_s = P^{-1}I$. Allora $I = PQ_1 \cdots Q_s$, I è un prodotto di ideali primi di A, contraddizione. □

Dimostrazione. Teorema A.6.1

Sia A un dominio di Dedekind, sia I un ideale frazionario di A, sia $a \in A,\ a \neq 0$, tale che $aI \subseteq A$. Poiché aI è un ideale di A, per il lemma A.6.4 esistono $P_1, \ldots, P_k$ ideali primi di A tali che $P_1 \cdots P_k = aI$, quindi tali che $I = (a^{-1}A)P_1 \cdots P_k$. Per il lemma A.6.3, e poiché tutti gli ideali principali sono invertibili, I è un prodotto di invertibili, quindi è invertibile.

Sia A un dominio tale che tutti i suoi ideali frazionari siano invertibili. Sia I un ideale non nullo di A, allora $II' = A$, dunque esistono $a_1, \ldots, a_m \in I$, $b_1, \ldots, b_m \in I'$ tali che $a_1b_1 + \cdots + a_mb_m = 1$, quindi tali che $x = (xb_1)a_1 + + \cdots + (xb_m)a_m\ \forall x \in I$. $\{a_1, \ldots, a_m\}$ è quindi un sistema di generatori per I. Ogni ideale di A quindi è finitamente generato, cioè A è noetheriano.
Sia P un ideale primo non nullo di A, sia Q un ideale massimale di A tale che $P \subseteq Q$. Allora $PQ^{-1} \subseteq QQ^{-1} = A$, quindi PQ^{-1} è un ideale di A. Poiché $(PQ^{-1})Q = P$ e P è un ideale primo, o $PQ^{-1} \subseteq P$ o $Q \subseteq P$. Se si avesse $PQ^{-1} \subseteq P$ si avrebbe che $Q^{-1} = P^{-1}PQ^{-1} \subseteq P^{-1}P = A$. D'altra parte, poiché Q è un ideale di A, certamente $A \subseteq Q^{-1}$, quindi si avrebbe $Q^{-1} = A$, quindi $Q = A$, contraddizione. Allora si deve avere $Q \subseteq P$, quindi $Q = P$, cioè P deve essere massimale.
Sia ora $\mathbb{K}$ il campo dei quozienti di A, sia $x \in \mathbb{K}$ intero su A. Per la proposizione A.4.1 allora $A[x]$ è un A-modulo finitamente generato, sia $\{a_1, \ldots, a_m\}$ un suo sistema di generatori. Sia $b \neq 0$ tale che $ba_i \in A$ per $i = 1, \ldots, m$, allora $bA[x] \subseteq A$, quindi $A[x]$ è un ideale frazionario di A. Inoltre, poiché $A[x]$ è un anello, $A[x]^2 = A[x]$. Dunque $A[x] = AA[x] = A[x]^{-1}A[x]A[x] = = A[x]^{-1}A[x] = A$, quindi $x \in A$, quindi A è integralmente chiuso. □

Teorema A.6.5.
Sia A un dominio di Dedekind, allora ogni ideale proprio non nullo di A può essere rappresentato come prodotto di ideali primi, in modo unico a meno dell'ordine.

Dimostrazione.
Per il lemma A.6.4 ogni ideale proprio non nullo di A può essere scritto come prodotto di ideali primi.

Supponiamo che esistano ideali propri non nulli di A che ammettono diverse rappresentazioni come prodotti di ideali primi. Sia $I = P_1 \cdots P_r = Q_1 \cdots Q_s$ un tale ideale, con $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ ideali primi di A; supponiamo che I sia scelto in modo che il numero di ideali primi che compaiono nella prima decomposizione sia minimo. Ora, $Q_1 \cdots Q_s \subseteq P_1$, quindi esiste i tale che $Q_i \subseteq P_1$; supponiamo che $Q_1 \subseteq P_1$. Poiché P_1, Q_1 sono primi, quindi massimali, si deve avere $P_1 = Q_1$. Allora $P_2 \cdots P_r = P_1^{-1} I = Q_1^{-1} I = Q_2 \cdots Q_s$, cioè l'ideale $P_1^{-1} I$ ha due diverse fattorizzazioni, una delle quali formata da $r - 1$ ideali primi, contraddizione. □

Corollario A.6.6.
Il gruppo degli ideali frazionari di un dominio di Dedekind è il gruppo abeliano libero generato dai suoi ideali primi.

Dimostrazione.
Sia A un dominio di Dedekind. Certamente ogni elemento del gruppo abeliano libero generato dagli ideali primi di A è un ideale frazionario di A.
Sia I un ideale frazionario di A, sia $a \in A,\ a \neq 0$, tale che $aI \subseteq A$, cioè tale che aI sia un ideale di A. Poiché per il teorema precedente $aA,\ aI$ possono essere rappresentati in modo unico come prodotti di ideali primi, $I = (aI)(aA)^{-1}$ può essere rappresentato come prodotto di potenze di ideali primi con esponenti interi e questa rappresentazione è ancora unica. □

Osservazione A.6.7.
Sia A un dominio di Dedekind, sia H il gruppo degli ideali frazionari di A. Gli ideali frazionari principali di A formano un sottogruppo di H, H', quindi ha senso considerare $G = H/H'$; G è detto il **gruppo delle classi di ideali** di A.

Definizione A.6.2.
Sia A un dominio di Dedekind, siano I, J ideali di A. Si dice che I è **divisibile** per J se $I = JK$, con K ideale di A.
Un **massimo comun divisore** di I, J è un ideale che divide I, J e che è divisibile per ogni divisore comune di I, J.

Un **minimo comune multiplo** di I, J è un ideale divisibile per I e per J e che divide ogni ideale divisibile per I, J.

Osservazione A.6.8.
Siano $I = \prod P^{i_P},\ J = \prod P^{j_P}$, con $\#\{P|\ i_P \neq 0\} < \infty,\ \#\{P|\ j_P \neq 0\} < \infty$, ideali frazionari di A.
I, J sono ideali di A se e solo se $i_P, j_P \geq 0\ \forall P$ e I divide J, se e solo se $i_P \leq j_P\ \forall P$.
Il massimo comun divisore di I, J è $K = \prod P^{k_P}$ con $k_P = \min\{i_P, j_P\}$;
il minimo comune multiplo di I, J è $L = \prod P^{l_P}$ con $l_P = \max\{i_P, j_P\}$.
Dunque massimo comun divisore e minimo comune multiplo di ideali di un dominio di Dedekind esistono sempre e sono unici. Il massimo comun divisore di I, J sarà notato (I, J).

Proposizione A.6.9.
Sia A un dominio di Dedekind, allora:

1. *se I, J sono ideali frazionari di A si ha che $I \subseteq J$ se e solo se esiste K, ideale di A, tale che $I = JK$*

2. *se I è un ideale frazionario di A esiste un ideale frazionario principale aA tale che $(aA)I^{-1} \subseteq A$*

3. *se I, J sono ideali di A primi fra loro si ha che $IJ = I \cap J$*

4. *se I, J sono ideali di A si ha che $(I, J) = I + J$*

Dimostrazione.

1. Certamente se $I = JK$ allora $I \subseteq J$.
   Se $I \subseteq J$ allora $IJ^{-1} \subseteq JJ^{-1} = A$, quindi $K = IJ^{-1}$ è un ideale di A tale che $JK = I$.

2. Sia $a \in I,\ a \neq 0$, certamente allora $aA \subseteq I$, quindi per il punto 1. $(aA)I^{-1}$ è un ideale di A.

3. Per il punto 1. I, J dividono $I \cap J$, quindi, poiché I, J sono primi fra loro, IJ divide $I \cap J$, dunque, ancora per 1., $I \cap J \subseteq IJ$.
   D'altra parte, $IJ \subseteq I, IJ \subseteq J$, quindi $IJ \subseteq I \cap J$.
   Dunque $IJ = I \cap J$.

4. Certamente $I, J \subseteq I + J$, quindi $I + J$ divide I e J, quindi $I + J$ divide (I, J), quindi $(I, J) \subseteq I + J$.
   D'altra parte, (I, J) divide I e J, quindi (I, J) divide $I + J$, quindi $(I, J) \subseteq I + J$.
   Dunque $(I, J) = I + J$.

□

Definizione A.6.3.
Sia A un dominio, sia I un ideale di A. Siano $a, b, x \in A$, si scrive $ax \equiv b \pmod{I}$ se esiste $y \in I$ tale che $ax = b + y$.

Proposizione A.6.10.
Sia A un dominio, sia I un suo ideale, siano $a, b \in A$. La congruenza $aX \equiv b \pmod{I}$ ha una soluzione $x \in A$ se e solo se $b \in I + aA$.

Dimostrazione.
Esiste $x \in A$ tale che $ax \equiv b \pmod{I}$ se e solo se esistono $x \in A,\ y \in I$ tali che $b = ax - y$, se e solo se $b \in aA + I$. □

Corollario A.6.11.
Sia A un dominio di Dedekind, sia P un ideale primo di A, sia $a \in A \setminus P$. Allora $\forall b \in A,\ \forall n \in \mathbb{N}$ la congruenza $aX \equiv b \pmod{P^n}$ ha soluzioni in A.

Dimostrazione.
$P^n + aA = (P^n, aA) = A$, dunque per la proposizione precedente la congruenza $aX \equiv b \pmod{P^n}$ ha soluzione in A per ogni $b \in A$ □

Corollario A.6.12.

Sia A un dominio di Dedekind, siano $P_1, \dots, P_m$ ideali primi di A, con $P_i \neq P_j$ $\forall i \neq j$, siano $a_1, \dots, a_m \in A$, sia $n \in \mathbb{N}$. Allora il sistema di congruenze $\begin{cases} X \equiv a_1 \pmod{P_1^n} \\ \dots \\ X \equiv a_m \pmod{P_m^n} \end{cases}$ *ha sempre soluzione in A.*

Dimostrazione.

Per $i = 1, \dots, m$ sia $b_i \in (P_1 \cdots P_{i-1} P_{i+1} \cdots P_m)^n \setminus P_i$, sia $x_i \in A$ una soluzione della congruenza $b_i X \equiv a_i \pmod{P_i^n}$ (per il corollario precedente una tale x_i esiste sempre). Sia $x = \sum_{i=1}^{m} b_i x_i$, allora per $j = 1, \dots, m$ si ha che

$$x \equiv \sum_{i=1}^{m} b_i x_i \equiv b_j x_j \equiv a_j \pmod{P_j^n}.$$ □

Corollario A.6.13.

Sia A un dominio di Dedekind, siano $I_1, \dots, I_m$ ideali di A a due a due primi fra loro. Allora per ogni $a_1, \dots, a_m \in A$ il sistema di congruenze $\begin{cases} X \equiv a_1 \pmod{I_1} \\ \dots \\ X \equiv a_m \pmod{I_m} \end{cases}$ *ha soluzione in A.*

Dimostrazione.

Per $j = 1, \dots, m$ sia $I_j = \prod P^{\alpha_P^j}$. Il sistema di congruenze considerato allora è equivalente al sistema di congruenze $X \equiv a_j \pmod{P^{\alpha_P^j}}$, $j = 1, \dots, m$, P ideale primo di A. Poiché gli I_j sono a due a due primi fra loro, per ogni P al più uno degli α_P^j è non nullo. Per il corollario precedente, con $n = \max_{j,P} \alpha_P^j$, questo sistema ha soluzione in A. □

Corollario A.6.14.

Sia A un dominio di Dedekind, siano I, J ideali di A primi fra loro. Allora esiste $x \in I$ tale che $(xA, J) = 1$ e $(xI^{-1}, I)1$. Inoltre, se I_1 è primo con I, esiste $y \in I$ tale che $(yA, I_1) = 1$, $(yI^{-1}, I) = 1$ e $xA + yA = I$.

Dimostrazione.
Sia $I = \prod_{i=1}^{m} P_i^{\alpha_i}$, con $P_1, \dots, P_m$ ideali primi di I, $P_i \neq P_j \ \forall i \neq j$. Per $i = 1, \dots, m$ sia $a_i \in P_i^{\alpha_i} \setminus P_i^{\alpha_i+1}$. Per il corollario precedente esiste $x \in A$ tale che $\begin{cases} x \equiv a_1 \pmod{P_1^{\alpha_1+1}} \\ \dots \\ x \equiv a_m \pmod{P_m^{\alpha_m+1}} \\ x \equiv 1 \pmod{J} \end{cases}$. Dunque $(xA, J) = 1$ e $x \in P_i^{\alpha_i} \setminus P_i^{\alpha_i+1} \ \forall i$, quindi $x \in I$, dunque xI^{-1} è un ideale di A, e $(xP_i^{-\alpha_i}, P_i) = 1 \ \forall i$, quindi $(xI^{-1}, I) = 1$.
Sia $xA = II_2$, allora $(I_2, IJ) = 1$. Per il corollario precedente esiste $y \in A$ tale che $\begin{cases} y \equiv a_1 \pmod{P_1^{\alpha_1+1}} \\ \dots \\ y \equiv a_m \pmod{P_m^{\alpha_m+1}} \\ y \equiv 1 \pmod{I_1 I_2} \end{cases}$. Come prima allora $y \in I$, $(yI^{-1}, I) = 1$ e $(yA, I_1) = 1$. Inoltre, sia $yA = II_3$, allora $(I_3, I_2) = 1$.
Dunque $xA + yA = II_2 + II_3 = (II_2, II_3) = I(I_2, I_3) = I$. □

Corollario A.6.15.
Sia A un dominio di Dedekind, allora ogni ideale di A è generato da al più due elementi di A

Dimostrazione.
Sia I un ideale proprio di A, allora esistono J, I_1 ideali di A primi con I.
Per il corollario precedente allora si possono trovare $x, y \in I$ tali che
$I = xA + yA$. □

Teorema A.6.16.
Sia A un dominio di Dedekind, sia G il suo gruppo delle classi di ideali, allora sono equivalenti le seguenti affermazioni:

1. *$|G| = 1$*
2. *A è un dominio a ideali principali*
3. *A è un dominio a fattorizzazione unica*

Dimostrazione.

1. $\Rightarrow$ 2. Sia I un ideale di A. Poiché $G = \{\overline{0}\}$ deve esistere $a \in A$ tale che $I = aA$, cioè I è principale.

2. $\Rightarrow$ 3. Abbiamo già visto che ogni dominio a ideali principali è un dominio a fattorizzazione unica (proposizione A.3.3).

3. $\Rightarrow$ 1. Sia $a \in A$ irriducibile, proviamo che allora aA è un ideale primo.
Supponiamo che si abbia $aA = P_1 \cdots P_s$ con $P_1, \ldots, P_s$ ideali primi di A, $s \geq 2$. Per $i = 1, \ldots, s$ siano $a_i, b_i \in A$ tali che $P_i = a_iA + b_iA$.
Per ogni i, o $a \nmid a_i$ o $a \nmid b_i$ (altrimenti si avrebbe che $P_i \subseteq aA$, quindi $P_i = aA$, contraddizione). Supponiamo che $a \nmid a_i \ \forall i$.
Ora, $a_1 \cdots a_s \in P_i \cdots P_s = aA$, quindi $a | a_1 \cdots a_s$, assurdo perché per ipotesi a è irriducibile e A è un anello a fattorizzazione unica.
Se si avesse $|G| > 1$ esisterebbe un ideale primo P di A non principale. Siano $a, b \in A$ tali che $P = aA + bA$. Sia $a = a_1 \cdots a_r$ la fattorizzazione in irriducibili di a in A. Allora gli a_iA sono ideali primi, quindi massimali, e sono tutti e soli gli ideali massimali di A che contengono a. Poiché P è un ideale primo, quindi massimale, di A e $a \in P$, si dovrà avere $P = a_iA$ per qualche i, cioè P dovrà essere principale, contraddizione.

□

Bibliografia

[1] Bryan J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math Soc. 43, 1968

[2] Enrico Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, in *Séminaire Bourbaki: vol. 1972/73: exposés 418-435*, Springer, 1974

[3] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14, 1941

[4] Michael D. Fried, Moshe Jarden, *Field arithmetic*, Springer, 1986

[5] Christian Friesen, Paul van Wamelen, *Class numbers of real quadratic function fields*, Acta Arithmetica LXXXI.1, 1997

[6] Robin Hartshorne, *Algebraic Geometry*, Springer, 1977

[7] Erich Hecke, *Lectures on the theory of algebraic numbers*, translated by George U. Brauer and Jay R. Goldman, Springer, 1981

[8] Wladyslaw Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, 1990

[9] Michael Rosen, *Number theory in function fields*, Springer, 2002

[10] Friedrich K. Schmidt, *Analytischen Zahlenthorie in Körpern der Characteristik p*, Math. Zeit. 33, 1931

[11] Wolfgang M. Schmidt, *Equations over finite fields: an elementary approach*, Springer, 1976

[12] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer, 2009.

[13] Joseph H. Silverman, John Tate, *Rational points on elliptic curves*, Springer, 1992