UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze
Matematiche, Fisiche
e Naturali

Corso di Laurea
Triennale in Matematica

Poligoni “biscritti” ad una curva ellittica

Biscribed polygons of an elliptic curve

Relatore
Prof. Giorgio Ottaviani

Candidato
Leonardo Campigli

Anno Accademico 2023/2024

Indice

Introduzione

L'obiettivo della tesi è contare il numero di poligoni "biscritti" a una generica curva ellittica, partendo dai triangoli, problema proposto da Shigeru Mukai in [Muk04]. Definiremo una curva ellittica e studieremo le sue proprietà, in particolare la struttura di gruppo che si può costruire sui punti della curva con un'operazione geometrica, dalla quale otterremo potenti strumenti algebrici per risolvere problemi come quello annunciato.

1 Le funzioni ellittiche

Ci occuperemo inizialmente di studiare le funzioni ellittiche, usando come riferimento di testo [Lan87, Capitolo 1].

Definizione 1.1 (Reticolo in $\mathbb{C}$)**.** *$\Lambda \subset \mathbb{C}$ è un reticolo se è un sottogruppo additivo di dimensione 2 su $\mathbb{Z}$ che genera $\mathbb{C}$ su $\mathbb{R}$.*

Notazione: Se $\omega_1, \omega_2 \in \mathbb{C}$ sono una base per Λ su $\mathbb{Z}$, indichiamo $\Lambda = [\omega_1, \omega_2]$.

Definizione 1.2 (Funzione ellittica)**.** *$A \subseteq \mathbb{C}$ discreto, $f : \mathbb{C} \setminus A \longrightarrow \mathbb{C}$ si dice ellittica se è meromorfa su $\mathbb{C}$ e se è Λ-periodica, ovvero $f(z+\omega) = f(z)\ \forall \omega \in \Lambda$.*

Osservazione: La definizione è equivalente a chiedere che, se $\Lambda = [\omega_1, \omega_2]$, allora $f(z + \omega_1) = f(z) = f(z + \omega_2)\ \forall z \in \mathbb{C}$.

Osservazione: Una funzione ellittica intera (ovvero, senza poli) è costante. Infatti, vedendola come funzione nel quoziente $\mathbb{C}/\Lambda$ (essendo Λ-periodica), che è omeomorfo a un toro, essendo compatto per il [Mir95, Teorema 1.37, Capitolo 1] è costante.

Definizione 1.3 (Parallelogramma fondamentale)**.** *Se $\Lambda = [\omega_1, \omega_2]$ e $\alpha \in \mathbb{C}$, definisco $P = \{\alpha + t_1\omega_1 + t_2\omega_2 | t_1, t_2 \in [0,1]\}$. P si chiama Parallelogramma fondamentale di Λ (con vertice in α).*

Teorema 1.1 (1° Teorema di Liouville)**.** *f funzione ellittica Λ-periodica, P parallelogramma fondamentale. Suppongo che f non abbia poli sul bordo di P (posso sempre scegliere il vertice $\alpha \in \mathbb{C}$ tale che questa condizione sia verificata). Allora la somma dei residui di f in P è 0.*

Dimostrazione. Dal Teorema del Residuo si ha $2\pi i \sum Res(f) = \displaystyle\int_{\partial P} f(z)dz$. Si osserva che l'integrale è nullo per la Λ-periodicità di f. Infatti, la funzione assume gli stessi valori sui lati opposti di P, per cui l'integrale curvilineo si annulla. □

Corollario 1.1.1. *Una funzione ellittica non costante ha almeno due poli sul toro (contati con molteplicità).*

Teorema 1.2 (2° Teorema di Liouville)**.** *Sia P un parallelogramma fondamentale per Λ. Sia f funzione ellittica per Λ tale che non abbia zeri o poli su ∂P. Siano $\{a_i | i \in I\}$ gli zeri e i poli. Sia m_i l'ordine di f in $a_i, \forall i$. Allora, $\sum m_i = 0$.*

Dimostrazione. f è una funzione ellittica, cioé meromorfa e Λ-periodica. Segue che la sua derivata é una funzione meromorfa e anch'essa Λ-periodica, da cui f' è ellittica. Il rapporto $\frac{f}{f'}$ dunque è una funzione ellittica. Per il teorema 1.1, si ha che $\sum Res(\frac{f}{f'}) = 0$. Infine, utilizziamo questo risultato di analisi complessa: $Res(\frac{f}{f'}g, z_0) = kg(z_0)$, con k zero/polo di f di ordine k. Nel nostro caso $g = 1$. Da qui la tesi. □

Teorema 1.3 (3° Teorema di Liouville)**.** *Nelle stesse ipotesi del teorema 1.2, si ha che* $\sum m_i a_i \in \Lambda$.

Dimostrazione. Per il risultato usato nel teorema 1.2, con $g = z$,si ha $2\pi i \sum m_i a_i = \int_{\partial P} z\frac{f'(z)}{f(z)}dz$.
Spezziamo l'integrale sui 4 lati del parallelogramma fondamentale: $\int_{\partial P} z\frac{f'(z)}{f(z)}dz = \int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz +$
$\int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_{\alpha}^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}dz$.
Siano $I = \int_{\alpha}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz$ e $II = \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_{\alpha}^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}dz$.
Lavorando su I, mi basta la sostituzione $u = z-\omega_2$ e il fatto che $\frac{f}{f'}$ sia una funzione ellittica, per ottenere che $I = -\omega_2 \int_{\alpha}^{\alpha+\omega_1} \frac{f'(z)}{f(z)}dz$. Da cui $I = 2\pi i k\omega_2, \exists k \in \mathbb{Z}$. Procedendo analogamente su II, si ottiene che $2\pi i \sum m_i a_i = 2\pi i k\omega_2 + 2\pi i h\omega_1, \exists k, h \in \mathbb{Z}$, da cui $\sum m_i a_i \in \Lambda$.

□

2 La funzione di Weierstrass

Adesso introduciamo una funzione ellittica di fondamentale importanza nello studio delle curve ellittiche, la funzione di Weierstrass.

Definizione 2.1 (Funzione di Weierstrass)**.** *Dato* $\Lambda' = \Lambda \setminus \{0\}$*, si dice funzione di Weierstrass la funzione*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'} \left[\frac{1}{(z-w)^2} - \frac{1}{\omega^2}\right] \tag{1}$$

Per mostrare che la funzione di Weierstrass è ben definita, è sufficiente dimostrare che converge uniformemente sui compatti che non contengono punti di Λ. Ci servirà questo lemma:

Lemma 2.1. *Se* $\lambda > 2$*, allora* $\sum_{\omega\in\Lambda'} \frac{1}{|\omega|^\lambda}$ *converge.*

Dimostrazione. Sia $N \in \mathbb{N}$. Allora $\sum_{|\omega|\le N} \frac{1}{|\omega|^\lambda} = \sum_{n=1}^{N} \sum_{n-1\le|\omega|\le n} \frac{1}{|\omega|^\lambda}$. Si osserva che $|\omega|^\lambda \approx n^\lambda$ se $n-1 \le |\omega| \le n$ e che $|\{\omega \in \Lambda | n-1 \le |\omega| \le n\}| \approx n$. Quindi, $\sum_{|\omega|\le N} \frac{1}{|\omega|^\lambda} \approx \sum_{n=1}^{N} \frac{n}{n^\lambda} = \sum_{n=1}^{N} \frac{1}{n^{\lambda-1}}$ che per $N \longrightarrow \infty$ converge. □

Infatti, se z appartiene ad un compatto, si ha che $\left[\frac{1}{(z-w)^2} - \frac{1}{\omega^2}\right] = \frac{\omega^2 - z^2 - \omega^2 + 2z\omega}{\omega^2(z-\omega)^2} \approx \frac{1}{|\omega|^3}$, che converge per il lemma con $\lambda = 3$.

Adesso vogliamo provare un risultato fondamentale sulla funzione di Weierstrass:

Proposizione 2.1. *La funzione di Weierstrass $\wp$ è ellittica.*

Dimostrazione. Si osserva dalla (1) che $\wp$ è meromorfa, con poli di ordine 2 in ogni punto del reticolo. Inoltre, è pari, perché sommare su $\omega \in \Lambda$ è equivalente a sommare su $-\omega \in \Lambda$, infatti si ha che $(-z-\omega)^2 = (z+\omega)^2 = (z-(-\omega))^2$. Derivando ogni termine e raccogliendo si ha che

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3} \tag{2}$$

Si vede facilmente che $\wp'$ è dispari e Λ-periodica. $\wp'(z+\omega_1) = \wp'(z) \implies \wp(z+\omega_1) = \wp(z) + C, \exists C \in \mathbb{C}$. Calcolando in $z = -\frac{\omega_1}{2}$ si ha $\wp(\frac{\omega_1}{2}) = \wp(-\frac{\omega_1}{2}) + C$, ma essendo $\wp$ pari, si ha che $C = 0$. Ripetendo per ω_2 si ottiene che la funzione di Weierstrass è Λ periodica, quindi ellittica. □

Come abbiamo detto, la funzione di Weierstrass è centrale nello studio delle funzioni ellittiche. Infatti, si può dimostrare che $\wp$ e $\wp'$ generano su $\mathbb{C}$ il campo delle funzioni ellittiche rispetto a un dato reticolo.

Per dimostrare questo risultato ci servirà il seguente lemma:

Lemma 2.2. *Sia f una funzione pari ellittica. Sia u uno zero [polo] per f. Se $u \equiv -u$ mod Λ allora u è uno zero [polo] di ordine pari per f.*

Dimostrazione. Se $u \equiv -u \bmod \Lambda$, allora $2u \in \Lambda$. Gli unici punti del toro $\mathbb{C}/\Lambda$ che soddisfano quella equazione, visti nel parallelogramma fondamentale centrato in 0, sono questi: $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Se una funzione è pari ed ellittica, la sua derivata è dispari ed ellittica. Quindi $-f'(u) = f'(-u)$ ma $u \equiv -u \bmod \Lambda$, quindi $-f'(u) = f'(u), \implies f'(u) = 0$, ovvero u è uno zero di molteplicità maggiore o uguale a 2. Adesso useremo la funzione di Weierstrass e ci dividiamo in due casi.

Primo caso: $u \notin \Lambda$. Sia $g(z) := \wp(z) - \wp(u)$, con lo stesso argomento usato su f prima, si ha che g ha uno zero di molteplicità almeno 2 in u. Ma $\wp(z)$ ha un unico polo di molteplicità 2 sul toro (ho identificato il reticolo in un punto), quindi per il teorema 1.2 la molteplicità di u per g è necessariamente 2. Adesso consideriamo la funzione $\frac{f}{g}$. Chiaramente è pari, ellittica, ed olomorfa in u (per le ultime considerazioni fatte, la molteplicità dello zero di g in u è minore di quella di f). Se $\frac{f}{g}(u) \neq 0$, u ha molteplicità 2 per f, e ho finito. Altrimenti, u è uno zero per $\frac{f}{g}$ e posso riapplicare il procedimento dall'inizio. Il procedimento terminerà, poiché f è meromorfa, e sarà necessariamente una molteplicità pari.

Secondo caso: $u \in \Lambda$. In questo caso, definiamo $g(z) := \frac{1}{\wp(z)}$. Questa funzione ha uno zero di molteplicità 2 in u, quindi posso sfruttare argomenti analoghi al primo caso per concludere. □

Passiamo alla dimostrazione del teorema.

Teorema 2.1. *Il campo delle funzioni ellittiche $\mathbb{E}$ è generato da $\wp$ e $\wp'$.*

Dimostrazione. Sia $f \in \mathbb{E}$, posso scriverla come $f = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$, ovvero come la somma di una funzione ellittica pari e una funzione ellittica dispari. Quindi sarà sufficiente provare che $\wp, \wp'$ generano rispettivamente le funzioni ellittiche pari e quelle dispari.

Se $f \in \mathbb{E}$ è dispari, allora $f\wp'$ è pari. Quindi posso ricondurmi a dimostrare la tesi sulle funzioni pari, in particolare che il campo delle funzioni ellittiche pari è il campo delle funzioni razionali $\mathbb{C}(\wp)$.

Sia f una funzione ellittica pari. Se f ha uno zero di molteplicità m in u, allora ha anche uno zero di molteplicità m in $-u$, poiché $f^{(k)}(u) = (-1)^k f^{(k)}(-u)$. Per i poli vale lo stesso risultato.

Siano $u_1, .., u_r$ un sistema di rappresentanti nel parallelogramma fondamentale delle coppie $(u, -u)$ di zeri e poli di f (osservo che sono un numero finito perché i poli e zeri sono discreti e siamo in un compatto). Siano m_i definiti così per $i \in \{1, .., r\}$: se $2u_i \notin \Lambda, m_i = ord_{u_i}(f)$. Altrimenti, $m_i = \frac{ord_{u_i}(f)}{2}$. Ora, per quanto visto nella dimostrazione del lemma, se $a \notin \Lambda, \wp(z) - \wp(a)$ ha uno zero di ordine 2 in a $\iff 2a \in \Lambda$, altrimenti ha due zeri distinti di ordine 1 in a e $-a$.

Sia $g(z) := \prod_{i=1}^{r} [\wp(z) - \wp(u_i)]^{m_i}$. Per la definizione degli m_i, la funzione g ha lo stesso ordine di f $\forall z \notin \Lambda$. Ma per il teorema 1.2 l'ordine coincide anche nell'origine, cioè per $z \in \Lambda$. Quindi la funzione $\frac{g}{f}$ è una funzione ellittica senza zeri e poli, da cui segue che è costante. Questo prova la tesi.

□

Adesso vogliamo ricavare una relazione algebrica tra la funzione di Weierstrass e la sua derivata. Per fare ciò scriviamole come una serie di potenze centrata in zero. Con dei calcoli si ricava

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) S_{2n+2} z^{2n}$$

dove il termine S dipende dal reticolo ed è definito come

$$S_m(L) = \sum_{\omega \in \Lambda} \frac{1}{\omega^m}$$

Inoltre segue che

$$\wp'(z) = -\frac{2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1) S_{2n+2} z^{2n-1}$$

Da questi sviluppi possiamo ricavare il seguente fondamentale teorema:

Teorema 2.2. *Siano* $g_2 = 60S_4, g_3 = 140S_6$, *allora* $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$.

Dimostrazione. Sia $\phi(z) = (\wp')^2 - 4\wp^3 + g_2\wp + g_3$. Sviluppiamo la funzione in un intorno di zero utilizzando gli sviluppi sopra citati. $\phi(z) = (-\frac{2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1) S_{2n+2} z^{2n-1})^2 - 4(\frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) S_{2n+2} z^{2n})^3 + g_2(\frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) S_{2n+2} z^{2n}) + g_3$. Svolgendo le potenze e semplificando, si ottiene che tutti i termini con z al denominatore si cancellano. Quindi ϕ è una funzione intera, ed essendo ellittica è costante. Inoltre si semplificano i termini noti, quindi $\phi = 0$, e questo prova la tesi. □

Abbiamo quindi provato che i punti $(\wp(z), \wp'(z))$ stanno sulla cubica di equazione $y^2 = 4x^3 - g_2 x - g_3$.

3 Le cubiche come tori complessi

L'obiettivo di questa sezione è accennare la dimostrazione del fatto che una curva non singolare di grado 3 ha genere uno, ovvero è omeomorfa a un toro. Il testo di riferimento per l'intera sezione è [Kir92, Sezione 4.1.1], da cui ho anche ricavato l'immagine del primo passo. Per procedere, come prima cosa dimostriamo un semplice lemma.

Lemma 3.1. *$L \subset \mathbb{P}^2$ retta proiettiva, allora $L \simeq S^2$.*

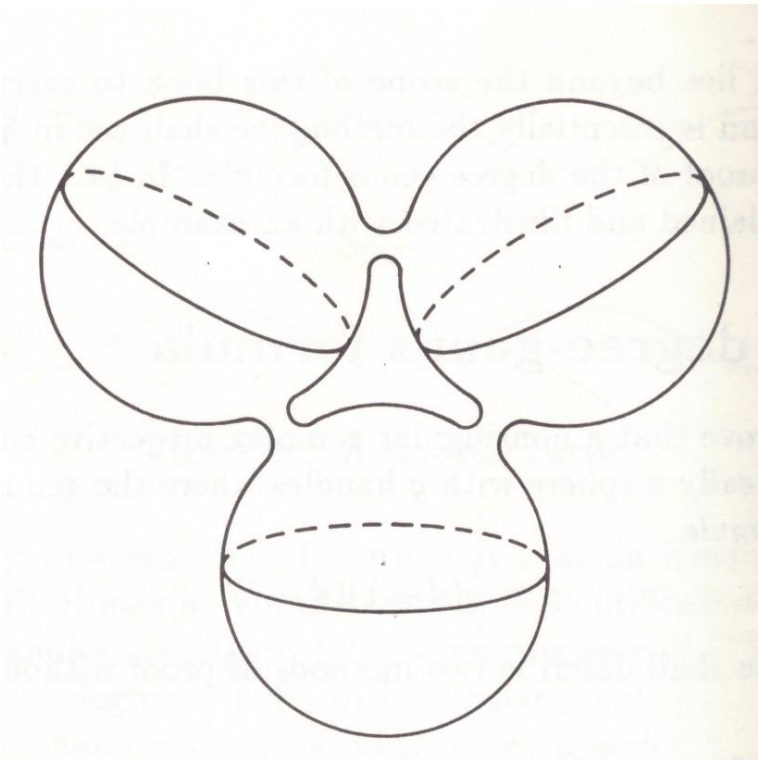
Dimostrazione. Suppongo, a meno di trasformazioni proiettive, che la retta sia $x_2 = 0$. Definisco la funzione $\phi : S^2 \longrightarrow L$ come $\phi(u, v, w) = [u + iv, 1 - w, 0]$ (attenzione: la funzione scritta così non è definita in $(0, 0, 1)$, ma posso scriverla come $[w + 1, u - iv, 0]$). Si osserva facilmente che la funzione è biettiva, e la sua inversa è data da: $\phi^{-1}[x_0, x_1, 0] = \left(\frac{2Re(x_0\bar{x}_1)}{|x_0|^2+|x_1|^2}, \frac{2Im(x_0\bar{x}_1)}{|x_0|^2+|x_1|^2}, \frac{|x_0|^2-|x_1|^2}{|x_0|^2+|x_1|^2}\right)$. Le due funzioni sono infine continue perché composizioni di funzioni continue. □

Adesso partiamo dal primo di tre passi che saranno necessari per la tesi finale.

Passo 1. *Esiste una cubica proiettiva C_1 che è omeomorfa a una sfera con un manico (toro).*

Dimostrazione. Considero una cubica singolare C_0 data dall'unione di tre rette in posizione generale in $\mathbb{P}^2$. Le tre rette si incontrano in 3 punti totali. Per il lemma precedente, posso vedere le 3 rette come 3 sfere tangenti in 3 punti. Adesso quello che posso fare è modificare i coefficienti di C_1 di una quantità sufficientemente piccola da farla diventare una curva non singolare, e questo è possibile poiché il sottoinsieme dei polinomi omogenei di grado 3 che definiscono curve non singolari è denso nello spazio di polinomi omogenei di grado 3, avendo complementare di codimensione reale due. Quello che succede alla curva a livello topologico è che i punti di intersezione delle sfere diventano dei manici che le uniscono. In questo modo rimane un manico in più ad unire le 3 sfere (unite già in un'unica sfera dagli altri due manici), col quale la curva diventa omeomorfa al toro. □

La figura sotto mostra il risultato finale della trasformazione avvenuta nel primo passo.



Ora enunciamo il secondo passo senza dimostrazione:

Passo 2. *Sia C curva non singolare, f polinomio che la definisce. Se i coefficienti di f variano di una quantità sufficientemente piccola, la classe di omeomorfismo della curva non varia.*

Infine il terzo passo:

Passo 3. *Sia $\mathbb{C}_3^{nonsing}[x_0, x_1, x_2] \subseteq \mathbb{C}_3[x_0, x_1, x_2]$ la sottovarietà dei polinomi omogenei di grado 3 che definiscono curve proiettive non singolari. Allora $\mathbb{C}_3^{nonsing}[x_0, x_1, x_2]$ è connesso per archi.*

Dimostrazione. Siano $P, Q \in \mathbb{C}_3^{nonsing}[x_0, x_1, x_2]$. Devo dimostrare che esistono dei polinomi $P_t \in \mathbb{C}_3^{nonsing}[x_0, x_1, x_2], \forall t \in [0, 1]$ tali che $P_0 = P, P_1 = Q$ e che la funzione $t \longmapsto P_t$ sia continua.

Se definissi il cammino come $P_t(x_0, x_1, x_2) = (1 - t)P(x_0, x_1, x_2) + tQ(x_0, x_1, x_2)$ sarebbe come richiesto, ad eccezione che potrebbe aver dei polinomi, in corrispondenza di un numero finito di valori di t, che non stanno in $\mathbb{C}_3^{nonsing}[x_0, x_1, x_2]$. Questo però è facilmente risolvibile: il cammino ha dimensione 1, il complementare di $\mathbb{C}_3^{nonsing}[x_0, x_1, x_2]$ ha codimensione 2, quindi si può spostare il cammino di poco per far sì che non si tocchino. Questo conclude la dimostrazione. □

Adesso uniamo i tre passi per poter dimostrare il seguente teorema:

Teorema 3.1. *Sia C_0 una cubica proiettiva non singolare. Allora C_0 ha genere 1 (omeomorfa al toro). [Kir92]*

Dimostrazione. Sia C_1 la cubica omeomorfa al toro descritta nel Passo 1. Sia γ il cammino che collega C_0 a C_1 in $\mathbb{C}_3^{nonsing}[x_0, x_1, x_2]$ che esiste per il Passo 3. Per il Passo 2, $\forall t \in [0, 1], \exists \epsilon(t)$ tale che se $s \in [0, 1], |t - s| < \epsilon(t)$ si ha $C_s \simeq C_t$. Sia $A_t \in [0, 1]$ l'insieme dei valori s per cui $C_s \simeq C_t$. Dal passo 2 segue che A_t è aperto. Inoltre, se considero il complementare di A_t, per ogni m in A_t trovo un intorno di raggio $\epsilon(m)$ in cui $C_m \simeq C_k, \forall k \in (m - \epsilon(m), m + \epsilon(m))$, da cui il complementare è aperto. A_t è aperto e chiuso, e non vuoto, ma [0,1] è connesso, quindi $A_t = [0, 1]$, da cui segue, per $t = 0$, $C_0 \simeq C_1$.

□

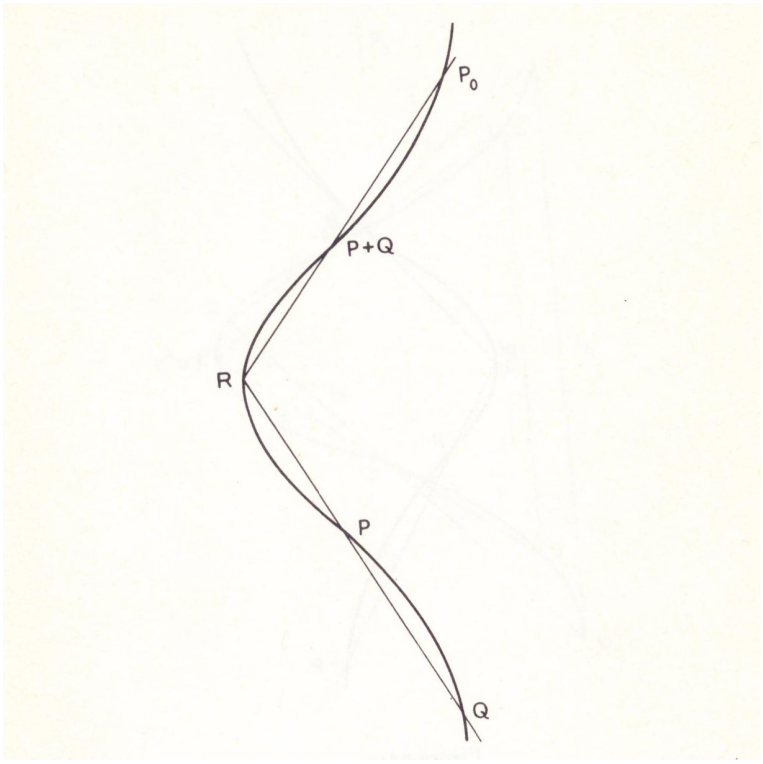
4 L'operazione di gruppo

Per parlare dell'operazione di gruppo su una curva ellittica, dobbiamo prima definire cosa sia una curva ellittica.

Definizione 4.1 (Curva ellittica)**.** *Una curva ellittica è una curva cubica proiettiva non singolare.*

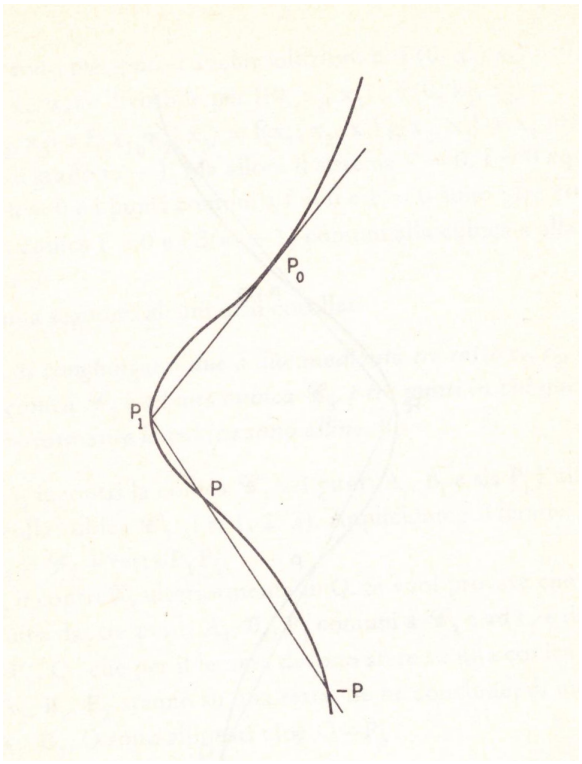
Sulla curva ellittica viene scelto un punto P_0 detto "origine", che nella nostra operazione di gruppo sarà l'elemento neutro. L'operazione che definiamo è inizialmente geometrica, ma si dimostra che dà una struttura algebrica di gruppo. I disegni e le dimostrazioni di questa sezione fanno parte di [GRT85, Sezione 2.7.3, Parte V].

Dati i punti P e Q sulla curva ellittica C, definiamo P+Q così: traccio la retta passante per P e Q, e chiamo R il suo terzo punto di intersezione con la curva C. A questo punto traccio la retta passante per R e P_0. Il suo terzo punto di intersezione con la curva è P+Q. Vediamo un esempio in figura:



Mi preme soffermarmi sull'operazione di duplicazione, ovvero la somma di un punto con se stesso. Ovviamente le rette per un punto sono infinite, quindi la costruzione in questo caso è leggermente diversa. La retta che si prende per la duplicazione è la retta tangente alla curva nel punto P (ottenuta in modo naturale come il limite della retta per P e un punto tendente a P), e la terza intersezione è il punto da cui far passare la retta per P_0 con cui ottenere il punto 2P. (attenzione: se si applica la duplicazione ad un punto di flesso, la cui retta tangente ha molteplicità di intersezione pari a 3, si otterrà come terza intersezione se stesso).

L'opposto rispetto a questa operazione (ovvero quell'elemento -P tale che P+(-P)=P_0) viene ricavato in questo modo: traccio la retta tangente al punto P_0 e prendo la sua ulteriore intersezione con la curva (in caso P_0 sia un flesso risulta se stesso), chiamo il punto P1. L'opposto di P è la terza intersezione della retta fra P1 e P con la curva C. Vediamolo:



L'operazione è banalmente commutativa. Meno banale è invece dimostrarne l'associatività. Dobbiamo prima dimostrare un lemma:

Lemma 4.1. *Sia C una cubica irriducibile e D_m una curva di grado m. Suppongo che 3 dei 3m punti di intersezione tra C e D_m stiano su una retta. Allora, i restanti 3(m-1) punti stanno su una curva di grado m-1, D_{m-1}.*

Dimostrazione. Partiamo con lo specificare che i 3m punti citati nell'enunciato sono punti contati con la loro molteplicità di intersezione, e sono quel numero per il Teorema di Bézout.

Posso supporre per semplicità che i tre punti allineati siano distinti, e che la retta che li contiene sia la retta $x_0 = 0$. Sia poi $f(x_0, x_1, x_2) = 0$ l'equazione che definisce la cubica, e $F(x_0, x_1, x_2) = 0$ quella per la curva D_m. La retta incontra la cubica in 3 punti, quindi l'equazione

$$f(0, x_1, x_2) = 0$$

ha tre soluzioni, e tutte sono anche soluzione di

$$F(0, x_1, x_2) = 0$$

Ottengo quindi per divisibilità:

$$F(0, x_1, x_2) = f(0, x_1, x_2)g(x_1, x_2)$$

per un qualche polinomio g. Per l'omogeneità dei polinomi segue che

$$F(x_0, x_1, x_2) = f(x_0, x_1, x_2)g(x_1, x_2) + x_0 h(x_0, x_1, x_2)$$

dove h è un polinomio di grado $m-1$. Quindi i punti nell'intersezione, che sono descritti dal sitema $f=0, F=0$ risultano anche descritti dal sistema $f=0, x_0 h=0$. Di questi, i punti sulla retta sono quelli tali che $x_0=0, f(0,x_1,x_2)=0$, mentre i restanti $3(m-1)$ punti sono dati dal sistema $f=0, h=0$ e quindi giacciono sulla curva definita da h, di grado $m-1$. □

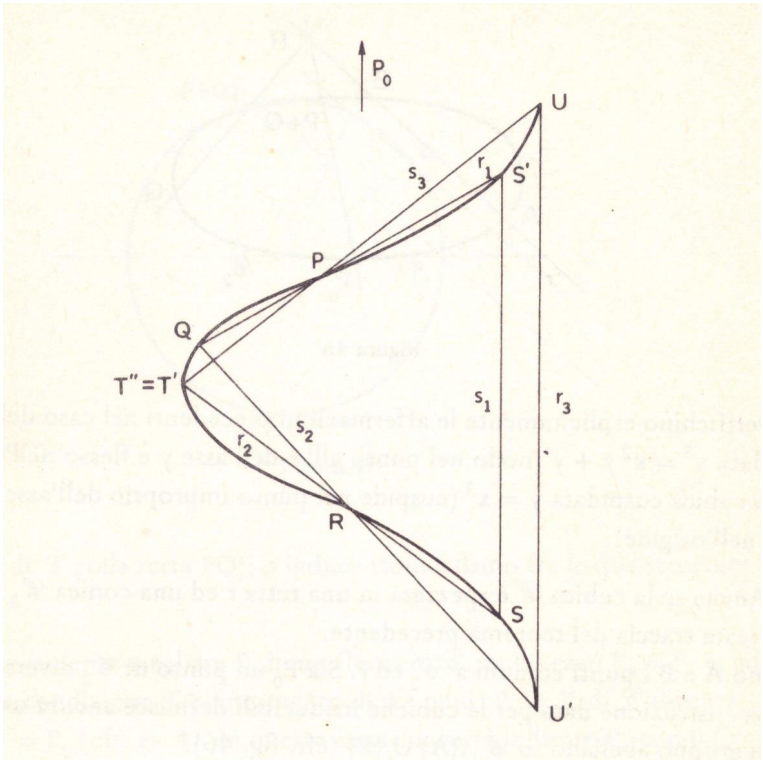
Teorema 4.1. *L'operazione di somma su una curva ellittica è associativa.*

Dimostrazione. Siano P,Q,R tre punti di C curva ellittica. Voglio provare che $(P+Q)+R = P+(Q+R)$.

Sia r_1 la retta per P e Q, ed S' la sua ulteriore intersezione con C. Sia s_1 la retta per S' e P_0, ed S=(P+Q) la sua terza intersezione con C. Sia r_2 la retta per S e R, e T' la sua terza intersezione con C. Sia s_2 la retta per Q e R, e U' la sua terza intersezione con C. Sia r_3 la retta per U' e P_0, ed U=(R+Q) la sua terza intersezione con C. Sia s_3 la retta per P e U, e T'' la sua terza intersezione con C.

Si vuole essenzialmente provare che $T'=T''$. L'unione delle tre rette $r_1+r_2+r_3$ forma una curva singolare di grado $m=3$, che incontra la cubica C nei punti P,Q,S',S,R,T',P_0,U',U. Di questi, O,S,S' stanno sulla retta s_1. Segue dal lemma che i restanti 6 punti stanno su una curva di grado $m-1=2$. Ma di questi, Q,R,U' stanno sulla retta s_2, da cui ottengo che P,U,T' sono allineati. Ma anche T'' è allineato con P ed U, e sta sulla curva. Quindi $T'=T''$. □

Vediamo la costruzione in un'immagine (come P_0 è stato scelto il punto all'infinito).



5 L'operazione di gruppo è algebrica

Data una curva ellittica qualsiasi, abbiamo visto che questa è omeomorfa a un toro. Sia questo toro dato da $\mathbb{C}/\Lambda$. Sia poi $\wp(z)$ la funzione di Weierstrass associata al reticolo Λ. Dunque, si è visto come la funzione

$$z \longmapsto (\wp(z), \wp'(z))$$

parametrizzi i punti sulla curva ellittica $y^2 = 4x^3 - g_2x - g_3$, con le due costanti che dipendono dal toro stesso. Adesso voglio vedere la curva in $\mathbb{P}^2$: per fare ciò devo omogenizzare il polinomio, e aggiungere una terza variabile alla mappa. Quindi, la funzione

$$z \longmapsto (1, \wp(z), \wp'(z)) \tag{3}$$

adesso parametrizza i punti sulla curva $y^2z = 4x^3 - g_2xz^2 - g_3z^3$. I punti del reticolo sono i poli della funzione di Weierstrass, e infatti sono mappati nel punto all'infinito $(0, 1, 0)$.

Estendendo la funzione (3) nell'origine (dove non era definita), imponendo che l'immagine in P_0 sia il punto all'infinito, otteniamo una biezione. In particolare, si dimostra che è un isomorfismo dal gruppo additivo del toro a quello della curva ellittica di cui abbiamo parlato, prendendo come origine P_0 il punto all'infinito, e questo isomorfismo sarà razionale, ovvero si può scrivere la somma di due punti come funzione razionale dei due addendi. Vediamolo in un teorema:

Teorema 5.1. *[Lan87] Siano $P_1 = (1, x_1, y_1), P_2 = (1, x_2, y_2)$ due punti distinti sulla curva ellittica C. Sia $P_3 = (1, x_3, y_3) = P_1 + P_2$. Allora $x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2$.*

Dimostrazione. Siano $u_1, u_2 \in \mathbb{C}, u_1, u_2 \notin \Lambda, u_1 - u_2 \notin \Lambda$. Siano $a, b \in \mathbb{C}$ tali che

$$\wp'(u_1) = a\wp(u_1) + b \text{ e } \wp'(u_2) = a\wp(u_2) + b \tag{4}$$

ovvero $y = ax + b$ è la retta per (x_1, y_1) e (x_2, y_2). La funzione

$$\wp'(z) - (a\wp(z) + b) \tag{5}$$

ha un polo di ordine 3 in O (si vede da 2). Per il teorema 1.2, ha 3 zeri contati con molteplicità. Se uno dei due punti avesse molteplicità 2 (flesso), non trovo un terzo punto e la somma diventa banale. Suppongo che abbiano entrambi molteplicità 1. Allora il terzo zero della (5), che chiamo u_3, per il teorema 1.3 è tale che $u_1 = -(u_2 + u_3) mod \Lambda$. Inoltre, $\wp'(u_3) = a\wp(u_3) + b$. Allora le tre radici di $4x^3 - g_2x - g_3 - (ax + b)^2 = 0$ sono $\wp(u_1), \wp(u_2), \wp(u_3)$. Quindi ho l'uguaglianza polinomiale $4(x - \wp(u_1))(x - \wp(u_2))(x - \wp(u_3)) = 4x^3 - g_2x - g_3 - (ax+b)^2$, da cui si ha, confrontando il termine di secondo grado:

$$\wp(u_1) + \wp(u_2) + \wp(u_3) = \frac{a^2}{4}$$

Sottraendo le due equazioni in (4), si ottiene $a = \frac{\wp'(u_1)-\wp'(u_2)}{\wp(u_1)-\wp(u_2)}$. Inoltre,

$$\wp(u_3) = \wp(-(u_1 + u_2)) = \wp(u_1 + u_2)$$

dove la prima uguaglianza segue dalla periodicità e la seconda dalla parità. Unendo le ultime tre equazioni trovate, si ottiene:

$$\wp(u_3) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left(\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)}\right)^2$$

che riscritta in termini algebrici risulta la formula del teorema:

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2$$

□

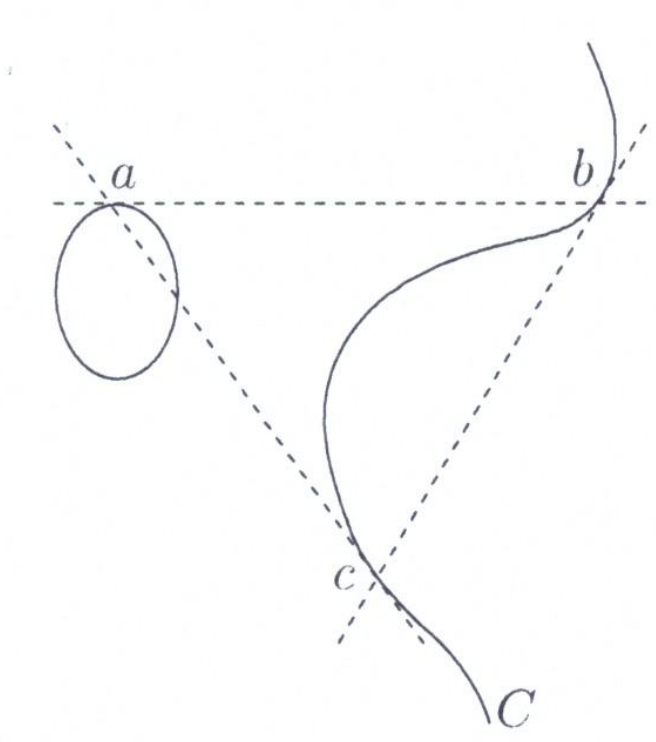
Corollario 5.1.1. *La somma di un punto con se stesso segue questa legge: $u \in \Lambda$, allora* $\wp(2u) = -2\wp(u) + \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2$.

Dimostrazione. La formula segue direttamente dal teorema, applicando il limite con $u_1 \longrightarrow u_2$ alla $\wp(u_3) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left(\frac{\wp'(u_1)-\wp'(u_2)}{\wp(u_1)-\wp(u_2)}\right)^2$

□

6 Triangoli "biscritti"

Ci siamo prefissati l'obiettivo di calcolare il numero di triangoli "biscritti" a una curva ellittica, ovvero quei triangoli formati da tre rette distinte tali che sono contemporaneamente inscritti (i loro vertici giacciono sulla curva) e circoscritti (i lati sono tangenti alla curva). Nella figura sottostante, presa da [Muk04] vi è un esempio.



Osserviamo una proprietà importante: ogni vertice di un triangolo "biscritto" è l'intersezione di due rette con la cubica. Necessariamente, il vertice sarà tangente in una di queste e non nell'altra. Questo perché, se considerassimo un triangolo ABC in cui il vertice C non ha nessuna retta tangente come lato, necessariamente le due rette passanti per quel

punto devono essere tangenti ai due restanti vertici, per costruire un triangolo (altrimenti avrei più di tre vertici). Ora, ho ottenuto che i due vertici A e B hanno come rette tangenti la retta AC e la retta BC. A questo punto, che retta congiunge A e B? Non esistono altre rette tangenti per i due punti, quindi dovrà essere la retta secante ai due punti, che incontrerà la cubica in un quarto punto D diverso da C, quindi non è un triangolo "biscritto".

A questo punto diamo la dimostrazione di un risultato enunciato da Shigeru Mukai in [Muk04] in cui la dimostrazione veniva lasciata al lettore:

Proposizione 6.1. *[Muk04, 1 Biscribed triangles, Proposition] Il numero di triangoli "biscritti" a una curva ellittica è 24.*

Dimostrazione. Lo strumento che utilizzeremo per contare i triangoli è la struttura di gruppo associata alla curva, che abbiamo studiato nei capitoli precedenti. Intanto scegliamo come origine sulla curva un qualsiasi punto di flesso, che seguendo la notazione additiva indicheremo con $\mathcal{O}$. In particolare, avendo compiuto questa scelta, si osserva che l'intersezione della curva con la retta tangente al punto P è data dall'opposto del punto 2P, siccome nel sommare due punti uguali si considera la tangente al punto.

A questo punto ci accorgiamo per costruzione che per i vertici di triangoli "biscritti" vale la seguente formula

$$-2(-2(-2P)) = P$$

da cui $9P = \mathcal{O}$. Ecco che dobbiamo contare quanti sono i punti di ordine divisore di 9 sulla curva. Ricollegandoci all'isomorfismo fra la curva e il toro, avevamo che i punti di ordine divisore di n sulla curva sono precisamente n^2, dimostrato in [Sas24, Teorema 3.1]. Quindi, il numero di punti con ordine divisore di 9 è 81. Fra questi sono compresi anche i punti di ordine 3, ovvero i 9 flessi. Loro non formeranno un triangolo, perché la retta tangente in quel punto non incontra la curva in un altro punto. Sarebbe un triangolo degenere con 1 vertice e non lo contiamo. Quindi i vertici corretti sono 72. Osserviamo infine che il numero di triangoli sarà un terzo di 72, poiché ogni vertice sta in uno e un solo triangolo per l'unicità della retta tangente e della sua seconda intersezione con la curva (essendo una cubica). Da tutte queste considerazioni, otteniamo che il numero di triangoli "biscritti" a una curva ellittica è 24.

□

Un problema matematico interessante a questo punto sarebbe quello di trovare nel concreto un triangolo "biscritto" a una data curva ellittica, quindi dando le coordinate dei vertici. Per fare ciò, utilizzeremo il software Macaulay2, che permette di fare calcoli su ideali di anelli di polinomi che a mano risulterebbero complicati.

Per i nostri scopi, vogliamo scrivere la cubica in forma di Hesse, ovvero una forma del tipo

$$x^3 + y^3 + z^3 + \lambda xyz = 0$$

Si può dimostrare che una qualsiasi cubica può essere scritta in questa forma (vedi [Hes01, 3 The Hessian Form of an Elliptic Curve]), e che gli unici valori di lambda per cui risulta singolare sono $-3, -3\theta, -3\theta^2$, con θ la radice cubica dell'unità.

La forma di Hesse risulta essere particolarmente utile per lo studio dell'operazione di gruppo, poiché si hanno formule algebriche esplicite per calcolare la somma di due punti, e la duplicazione di un punto. Con l'aiuto di Macaulay2 si trovano facilmente imponendo

le condizioni geometriche di somma, e le si possono trovare anche in [Hes01, 4 The Hessian Group Law]. Come origine è stato scelto il punto $\mathcal{O} = (1, -1, 0)$. Vediamole:

Dato il punto $P = (x_1, y_1, z_1)$, e il punto $Q = (x_2, y_2, z_2)$, definisco $P+Q = (x_3, y_3, z_3)$. Allora si ha che

$$x_3 = y_1^2 x_2 z_2 - y_2^2 x_1 z_1$$
$$y_3 = x_1^2 y_2 z_2 - x_2^2 y_1 z_1$$
$$z_3 = z_1^2 y_2 x_2 - z_2^2 y_1 x_1$$

Per la duplicazione invece, se $Q = 2P$ le formule sono

$$x_2 = y_1(z_1^3 - x_1^3)$$
$$y_2 = x_1(y_1^3 - z_1^3)$$
$$z_2 = z_1(x_1^3 - y_1^3)$$

Implementando queste formule su Macaulay2 ho potuto ricavare la formula per $3P$, applicando la duplicazione e poi la somma con il punto stesso. In questo modo, imponendo la condizione che $3P = F$, dove F è un flesso della curva, si ottiene una condizione analoga a quella vista sopra per essere vertice di un triangolo "biscritto". Infatti, il flesso è tale che $3F = \mathcal{O}$, e quindi $9P = \mathcal{O}$. A questo punto ottengo delle condizioni su P, ma sono complesse da studiare poiché coinvolgono tutte e 3 le componenti. Una prima semplificazione che si può fare è quella di imporre la terza componente di P uguale a 1. Questo è possibile poiché stiamo lavorando nel proiettivo, e abbiamo la certezza che il punto P non abbia una componente uguale zero. Infatti, se la avesse sarebbe un flesso della curva (si capisce studiando l'Hessiano della curva), e quindi non potrebbe esser un vertice di un triangolo "biscritto". Il flesso F che scegliamo è $F = (0, 1, -1)$, per semplicità di calcolo, avendo esso componenti reali.

Per concludere utilizziamo il comando *eliminate* di Macaulay2, che permette di eliminare una delle due componenti dall'ideale e ottenere le condizioni che deve soddisfare una sola delle due. Quello che succede è che otteniamo un polinomio di grado nove, riducibile a uno di grado 3 con una sostituzione, le cui nove radici sono le componenti di 9 vertici, i quali formano 3 triangoli "biscritti" associati al flesso F. Vediamo il programma:

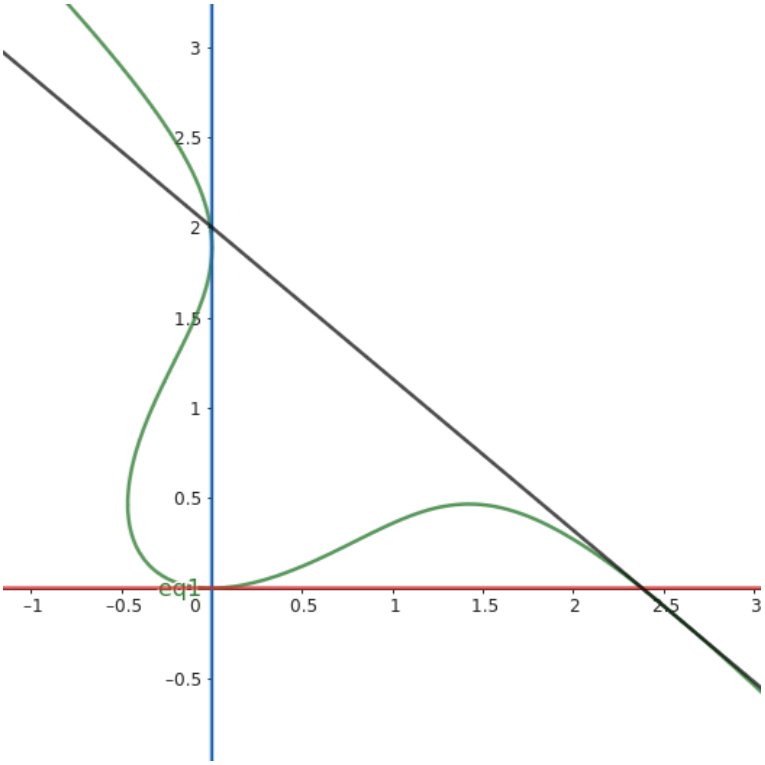
```
R=QQ[x,y,z,a,b,c,k]

---condizioni di duplicazione di Hesse
duex=y*(z^3-x^3)
duey=x*(y^3-z^3)
duez=z*(x^3-y^3)
---sostituisco nella formula generica le coordinate del vertice
duepics=sub(duex, {x=>a,y=>b,z=>c})
duepips=sub(duey, {x=>a,y=>b,z=>c})
duepiz=sub(duez, {x=>a,y=>b,z=>c})
--- condizioni di somma di due punti di Hesse
sommax=b^2*x*z-y^2*a*c
```

```
sommay=a^2*y*z-x^2*b*c
sommaz=c^2*y*x-z^2*a*b
---somma di P con 2P per ottenere 3P
trepx=sub(sommax, {x=>duepics,y=>duepips,z=>duepiz})
trepy=sub(sommay, {x=>duepics,y=>duepips,z=>duepiz})
trepz=sub(sommaz, {x=>duepics,y=>duepips,z=>duepiz})
---impongo la condizione terza componente=1
sub(trepx, c=>1)
sub(trepy, c=>1)
sub(trepz, c=>1)
----condizione 3P=Flesso (0,1,-1)
vertici=minors(2,matrix{{0,1,-1},{trepx,trepy,trepz}})
---aggiungo la condizione che il punto stia sulla curva
J=vertici+ideal(a^3+b^3+1+k*a*b)
H=sub(J,c=>1)
---elimino la prima e poi la seconda componente,
      ottenendo i polinomi sottostanti
S=eliminate({a},H)
T=eliminate({b},H)
---polinomio di grado 9 sulla prima componente
(k+3)*a^9-3*(k+3)*a^6-(k^3-3*k+18)*a^3-(k+3)
---polinomio di grado 9 sulla seconda componente
(k+3)*b^9+(k^3-3*k+18)b^6+3*(k+3)*b^3-(k+3)
```

Dallo studio del polinomio di grado 9, al variare di lambda (k, nel codice), si può osservare che il suo discriminante si annulla quando λ è uguale a $\frac{3}{2}$. Questo semplifica i calcoli per trovare un possibile vertice, poiché si ha una radice doppia, quindi il polinomio può essere semplificato a uno di grado 6, riducibile con una sostituzione a uno di grado 2. Qui possiamo osservare questi polinomi:

$$2x_1^6 - 7x_1^3 - 4, \qquad 4y_1^6 - 7y_1^3 - 2$$

Si risolve facilmente e si ottiene che la prima componente può assumere i valori reali $\sqrt[3]{4}, -\sqrt[3]{\frac{1}{2}}$ e la seconda $-\sqrt[3]{2}, \sqrt[3]{\frac{1}{4}}$. Controllando quali combinazioni di questi valori siano un punto della curva, ho ottenuto che un vertice del triangolo è $V_1 = \left(-\sqrt[3]{\frac{1}{2}}, -\sqrt[3]{2}, 1\right)$. Applicando quindi le formule di Hesse si ottiene anche il secondo vertice $V_2 = \left(\sqrt[3]{4}, -\sqrt[3]{2}, 1\right)$ e il terzo $V_3 = \left(-\sqrt[3]{\frac{1}{2}}, \sqrt[3]{\frac{1}{4}}, 1\right)$. Trovandoci nell'affine, con tutte le terze componenti uguali a 1 (e reali), ho potuto disegnare la curva su Geogebra per trovare un esempio esplicito di triangolo (rettangolo!) "biscritto" ad una curva ellittica, dove per maggior chiarezza del disegno ho traslato la curva per far coincidere V_1 con l'origine:



7 Poligoni "biscritti"

Il calcolo del numero di triangoli "biscritti" risulta piuttosto semplice, ma ci si potrebbe chiedere come cambia la situazione se consideriamo dei poligoni con più lati. Analizziamo ad esempio il caso di quadrilateri e pentagoni.

Nel caso di quadrilateri "biscritti", si ha che, seguendo il procedimento utilizzato nei triangoli, deve valere che

$$-2(-2(-2(-2P))) = P$$

ovvero $15P = \mathcal{O}$. Dovendo studiare i punti di ordine divisore di 15, sappiamo già il loro numero: $15^2 = 225$. Però fra questi sono compresi i punti di ordine 3 (flessi) che come detto prima vanno eliminati. Inoltre, potremmo chiederci se un punto di ordine 5 "va bene" o se abbiamo bisogno che abbia proprio ordine 15. Si può osservare che un punto di ordine 5 è tale che i vertici del quadrilatero da lui generato sono a due a due opposti tra loro (infatti, $4P = -P, -8P = 2P$). Quindi verrebbe una sorta di quadrilatero "incrociato", che possiamo contare nel nostro numero. Otteniamo quindi 216 vertici, di cui 4 alla volta formano un quadrilatero. Il numero di quadrilateri "biscritti" è dunque 54.

Il caso dei pentagoni risulta più diretto. Con lo stesso procedimento, la formula che si ricava è:

$$(-2P)^5 = P$$

da cui $33P = \mathcal{O}$. Quindi dobbiamo nuovamente contare questi tipi di punti. Saranno come sappiamo $33^2 = 1089$, a cui dobbiamo sottrarre come sempre i nove flessi. I punti di ordine 11 sono "a posto", quindi poi non ci resta che dividere per 5. Il numero di pentagoni "biscritti" è dunque $(1089 - 9)/5 = 216$.

Voglio svolgere il calcolo degli esagoni perché porta delle considerazioni interessanti. In particolare, essendo 6 un numero composto, ci saranno problemi di conto sui triangoli "doppi". Vediamo in che senso.

Un esagono "biscritto" sarà composto da punti che soddisfano

$$(-2P)^6 = P$$

ovvero $63P = \mathcal{O}$. Questo lo sappiamo calcolare. $63^2 = 3969$, togliamo i flessi e otteniamo 3960. Divido per 6 e ho 660. Questo sembrerebbe essere il numero giusto. Invece, bisogna fare attenzione a una cosa: 63 è divisibile per 9, e infatti nei 3960 sto contando anche i vertici dei triangoli. Un triangolo percorso due volte è effettivamente un qualcosa con 6 lati e 6 vertici, ma non rientra nella definizione che diamo di esagono, quindi dobbiamo toglierli. Il numero allora diventa $3960 - 72 = 3888$ e poi per il numero di esagoni $3888/6 = 648$.

Più in generale, dato un numero naturale n, quanti sono i poligoni con n lati (n-agoni, da ora in poi) "biscritti" a una curva ellittica? Per procedere al conteggio definiamo alcune quantità che saranno utili.

Definizione 7.1 (Numero di n-agoni "biscritti")**.** *Indicheremo con $B(n)$ il numero di poligoni con n lati "biscritti" a una curva ellittica, dove gli n lati ed n vertici sono distinti.*

Definizione 7.2 (Vertici di n-agoni "biscritti")**.** *Indicheremo con $V(n)$ il numero di vertici appartenenti a poligoni con n lati come nella definizione precedente.*

Attenzione: un poligono con "un lato" solo esiste! O almeno nelle nostre intenzioni. I flessi, infatti, sono tali che la retta tangente incontra la curva solo in quel punto, risultando l'unico vertice e lato dell' 1-agono. Teniamo quindi presente da ora in avanti che $V(1) = 9$.

Osserviamo subito che, con la stessa giustificazione utilizzata per i triangoli, il numero di poligoni è dato dal numero di vertici diviso per n, perché ogni vertice appartiene a uno e un solo poligono:

$$B(n) = \frac{V(n)}{n}$$

Adesso, ricordandosi la costruzione fatta coi triangoli, diamo una terza definizione:

Definizione 7.3 (Punti n-circolari)**.** *Indicheremo con $T(n)$ il numero di punti n-circolari, ovvero quei punti che facendo n volte la costruzione di una tangente nel successivo punto di intersezione, tornano nel punto di partenza.*

Abbiamo già studiato questi punti nei triangoli. In quel caso avevamo visto che i punti 3-circolari erano 81, ovvero tutti i punti di ordine un divisore di 9. Questo numero deriva dal fatto che i punti di ordine divisore di k sono k^2 su una curva ellittica. k in questo caso è quel numero che si ottiene facendo la potenza di -2 n volte e sottraendo uno. Infatti, la costruzione richiedeva di applicare $-2P$ n volte, e che questo fosse uguale a P. Quindi abbiamo la formula per i punti n-circolari generici:

$$T(n) = ((-2)^n - 1)^2$$

Ricavare T risulta facile, e anche B conoscendo V, ma calcolare V, in generale, non lo è.

Dobbiamo osservare inanzitutto una cosa:

Proposizione 7.1. *Sia $n \in \mathbb{N}$, allora*

$$T(n) = \sum_{d|n} V(d) \tag{6}$$

Dimostrazione. Ricordiamo che i punti n-circolari si chiudono dopo n "iterazioni". Se un punto si chiude per la prima volta dopo n iterazioni, allora quel punto è un vertice di un n-agono "biscritto". Viceversa, se è vertice di un n-agono "biscritto", si chiude dopo n iterazioni. Ma se un punto si chiude in n-iterazioni può aver percorso il giro più volte. In particolare, per terminare esattamente nel punto di partenza, deve averlo compiuto un numero di volte pari a un divisore di n. Quindi, i punti che si chiudono sono tutti e soli i vertici di d-agoni "biscritti", con d naturale che divide n. Da questa uguaglianza insiemistica segue l'uguaglianza numerica della proposizione □

Per proseguire, dobbiamo introdurre un teorema fondamentale nella Combinatoria, la cosiddetta "Formula di inversione di Moebius", e per fare ciò definiamo una funzione speciale, la funzione di Moebius.

Definizione 7.4 (Funzione di Moebius)**.** *La funzione di Moebius $\mu : \mathbb{N} \longrightarrow \mathbb{Z}$ viene definita così:*

$$\mu(n) = \begin{cases} 1 \text{ } se \text{ } n{=}1 \\ (-1)^s \text{ } se \text{ } n{=}p_1...p_s \\ 0 \text{ } altrimenti \end{cases} \tag{7}$$

Enunciamo la formula senza dimostrarla (per la dimostrazione, vedi [Sta11, Sez 3.7]):

Teorema 7.1 (Formula di inversione di Moebius)**.** *Siano $f, g : \mathbb{N} \longrightarrow \mathbb{R}$ due funzioni, allora vale*

$$f(n) = \sum_{d|n} g(d)$$

se e solo se

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

Teorema 7.2. *Sia $n \in \mathbb{N}$, allora*

$$V(n) = \sum_{d|n} \mu(d) T\left(\frac{n}{d}\right)$$

e di conseguenza

$$B(n) = \frac{\sum_{d|n} \mu(d) T\left(\frac{n}{d}\right)}{n} = \frac{\sum_{d|n} \mu(d)((-2)^{\frac{n}{d}} - 1)^2}{n}$$

Dimostrazione. La formula segue direttamente applicando la Formula di Inversione di Moebius alla (6). □

Osservazione fondamentale: si osserva che $T(1) = T(2)$, questo è l'unico caso in cui la T assume due valori uguali. E infatti il caso dei 2-agoni è un caso particolare. Questo perché, applicando la formula, otteniamo che $V(2) = \mu(1)T(2) + \mu(2)T(1) = 9 - 9 = 0$.

Effettivamente, non esistono vertici di 2-agoni, poiché la retta che unisce i due vertici dovrebbe essere tangente in entrambi i punti, ma è impossibile per il teorema di Bezout.

I calcoli quindi "tornerebbero" anche se noi eliminassimo semplicemente $V(2)$ dalle sommatorie, ma per poter utilizzare la formula di Moebius abbiamo bisogno di tutti i divisori, e 2 divide ogni numero pari. In ogni caso, essendo uguale a zero, non causa problemi e la formula vale sia per numeri pari che per numeri dispari.

Osserviamo un semplice corollario sul calcolo dei poligoni:

Corollario 7.2.1. *Siano p,q primi dispari distinti. Allora si ha:*
1) $V(p) = (2^p + 1)^2 - 9$
2) $V(pq) = (2^{pq} + 1)^2 - (2^p + 1)^2 - (2^q + 1)^2 + 9$.
3)$V(p^2) = (2^{p^2} + 1)^2 - (2^p + 1)^2$

Dimostrazione. Segue direttamente dal teorema 7.2, osservando che $\mu(p) = \mu(q) = -1$, $\mu(p^2) = 0$ e $\mu(pq) = \mu(1) = 1$. □

Rappresentiamo in una tabella il numero di vertici e di poligoni per i primi 12 numeri naturali. Si osserva come il numero di vertici cresca molto velocemente, una crescita approssimativamente esponenziale di base 4.

Numero di lati	V(n)	B(n)
1	9	9
2	0	0
3	72	24
4	216	54
5	1080	216
6	3888	648
7	16.632	2376
8	64.800	8100
9	263.088	29.232
10	1.045.440	104.544
11	4.198.392	381.672
12	16.764.840	1.397.070

Riferimenti bibliografici

[Geo] M. Hohenwarter. *Geogebra, Interactive geometry software*, `www.geogebra.org`

[GRT85] F. Gherardelli, L.A. Rosati and G. Tomassini. *Lezioni di Geometria: Vol II* Cedam, 1985.

[Hes01] N. Smart. *The Hessian Form of an Elliptic Curve*, Dept. Computer Science, University of Bristol, 2001

[Kir92] F. Kirwan. *Complex Algebraic Curves* Cambridge University Press, 1992.

[Lan87] S. Lang. *Elliptic Functions*. Springer New York, second edition, 1987.

[Mir95] R. Miranda. *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Mathematics, Volume 5, American Mathematical Society, 1995

[Muk04] S. Mukai. *Plane quartics and Fano threefolds of genus twelve*. The Fano Conference, 563–572. Università di Torino, Dipartimento di Matematica, Torino, 2004.

[M2] D. Grayson and M. Stillman. *Macaulay2, a software system for research in algebraic geometry*, `www.macaulay2.com`

[Sas24] A. Sassone. *Il teorema di Nagell-Lutz*, Università di Firenze, Tesi di Laurea Triennale, 2024.

[Sta11] R. Stanley. *Enumerative combinatorics, Volume I, Second edition* Cambridge Stud. Adv. Math., 49 Cambridge University Press, 2012.