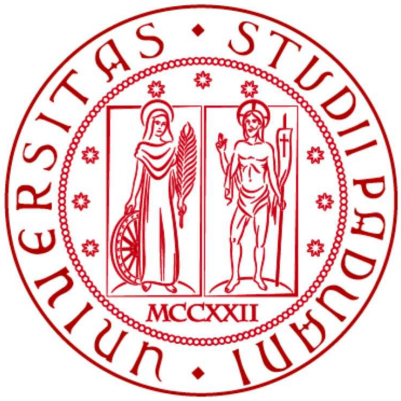

Università degli Studi di Padova

Dipartimento di Matematica
"Tullio Levi-Civita"

Corso di Laurea Triennale in Matematica

Numeri congruenti e curve ellittiche

Relatrice

Prof.ssa
LUISA FIOROT

Matricola

1201415

Laureando

VALERIA VICARD

Data ufficiale di laurea

23 Giugno 2022

Anno Accademico 2021-2022

Alla mia famiglia,
che in questi anni è sempre stata al mio fianco,
appoggiando ogni mia scelta

Indice

Introduzione

Fin dalla Grecia antica, matematici come Pitagora, Euclide e Diofante si sono interessati alla ricerca di un metodo che potesse generare tutte le terne pitagoriche, ossia terne di numeri X,Y,Z interi corrispondenti al valore della lunghezza dei cateti e dell'ipotenusa di un triangolo rettangolo. In particolare questo è possibile considerando due interi a e b con a>b e tracciando la retta passante per il punto (-1,0) sul piano uv e di pendente a/b. Il secondo punto sarà dato dall'intersezione tra la circonferenza unitaria e la retta appena costruita, come mostrato in Figura 1:

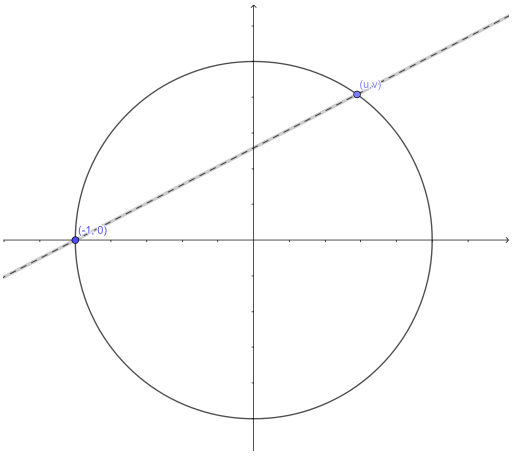

Figura 1: $u = \frac{a^2-b^2}{a^2+b^2}$, $v = \frac{2ab}{a^2+b^2}$

Ne ricaviamo quindi che i lati del triangolo rettangolo sono $X = a^2-b^2$, $Y = 2ab$, $Z = a^2+b^2$, ed inoltre il fatto che ci troviamo sulla circonferenza unitaria $u^2+v^2 = 1$ permette di ricavare che deve valere l'identità $X^2+Y^2 = Z^2$. Quindi al variare di a e b negli interi è facile ottenere tutte le terne pitagoriche facendo uso delle identità precedenti.

Dall'analisi di triangoli di questo tipo, si è presto giunti a quesiti più complessi, ad esempio la ricerca di interi n che potessero essere l'area di triangoli rettangoli, i cui lati sono numeri razionali, tali numeri sono detti *numeri congruenti*. Si potrebbe quindi pensare che ci sia una tecnica altrettanto semplice, come quella descritta per

le terne pitagoriche, per trovare tutti questi n o equivalentemente un criterio che ci fornisca in pochi passi la possibilità di sapere se il numero analizzato è congruente o meno. Questo fu un tema di particolare interesse nel mondo arabo, dove si tentò per lungo tempo di cercare razionali x tali per cui $x^2 - n$ e $x^2 + n$ siano entrambi numeri congruenti.

Solamente dopo il 1847 Fermat, facendo uso dell'Ultimo Teorema di Fermat, fu in grado di provare che n=1 non è un numero congruente in quanto non è soluzione non triviale dell'equazione $X^4 + Y^4 = Z^4$. Poco dopo si giunse a dedurre che anche n=2,3,4 non sono numeri congruenti, mentre 5 è il più piccolo intero positivo che rispetta la definizione.

Nel ventesimo secolo vi fu un avanzamento importante nello studio del quesito, quando si pensò di inserire il problema nell'ambito delle curve ellittiche.

Dando per assodate le poche nozioni appena presentate, nei prossimi capitoli tratteremo lo studio dei numeri congruenti e la loro relazione con le curve ellittiche, basandoci principalmente sul primo capitolo del testo *Introduction to Elliptic Curves and Modular Forms* [3].

In particolare nel primo capitolo ci focalizzeremo nel dare una definizione più accurata di numero congruente, che permetta di evidenziare alcune immediate proprietà che tali numeri hanno, restringendoci a considerare naturali liberi da quadrati. Successivamente, denotando con n un generico numero congruente, dimostreremo che la condizione algebrica equivalente alla definizione è che valga l'equazione $\left(\frac{X^2+Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$. Ciò ci permetterà non solo di osservare come 1 non goda della proprietà di congruenza, ma soprattutto di ricavare l'equazione cubica di una particolare curva ellittica, $y^2 = x^3 - n^2x$, intimamente connessa con il problema di trovare una condizione che permetta di affermare se un numero è congruente o meno.

Il secondo capitolo inizia definendo le funzioni doppiamente periodiche, di periodi ω_1 e ω_2, all'interno di un reticolo $L = \{m\omega_1 + n\omega_2\}$ e dimostra come le funzioni ellittiche siano applicazioni di questo tipo. Una funzione ellittica particolarmente importante è la funzione $\wp$ di Weierstrass, definita su L come $\wp(z, L) := \frac{1}{z^2} + \sum_{l\in L, l\neq 0}\left(\frac{1}{(z-l)^2} - \frac{1}{l^2}\right)$. In questa sezione ne vediamo la convergenza e ne descriviamo poli e zeri. Infine concludiamo individuando i tre zeri di $\wp'(z)^2$, $e_1 = \wp(\omega_1/2), e_2 = \wp(\omega_2/2), e_3 = \wp((\omega_1+\omega_2)/2)$, e mostrando come ogni curva ellittica sia esprimibile in funzione di $\wp(z)$ e $\wp'(z)$.

Proseguendo con il capitolo tre, si farà uso delle nozioni al capitolo precedente per definire la forma di Weierstrass per le curve ellittiche. Nel dettaglio si vedrà che ogni curva ellittica può essere riscritta come $\wp'(z) = f(\wp(z))$ con $f(x) = 4x^3 - g_2(L)x - g_3(L)$ e definiremo una legge di addizione per punti appartenenti alla curva dove, posti $P_1 = (\wp(z_1), \wp'(z_1))$ e $P_2 = (\wp(z_2), \wp'(z_2))$, chiamiamo $P_3 = P_1 + P_2$ il punto di coordinate $(\wp(z_1 + z_2), \wp'(z_1 + z_2))$. A seguito della deduzione algebrica della somma di due punti si riporterà anche una costruzione geometrica che ne

chiarificherà il significato. Concluderemo dimostrando che una curva ellittica C con l'operazione di addizione introdotta è un gruppo abeliano, $(C, +)$.

L'ultimo capitolo è incentrato principalmente sullo studio dei punti che si trovano sulla curva ellittica e che hanno ordine finito. Tra di essi troviamo sicuramente $(1, \wp(\omega_1/2),0)$, $(1, \wp(\omega_2/2),0)$ e $(1, \wp((\omega_1+\omega_2)/2),0)$, in quanto, annullando la derivata prima di $\wp(z)$, sono punti di ordine 2, come anche il punto all'infinito (0,0,1). Nell'ultima sezione studieremo le curve ellittiche su campi finiti $\mathbb{F}_p$ e introdurremo il concetto di rango. Questo risulterà centrale nelle conclusioni della tesi, in cui verranno esposti una condizione sulle curve ellittiche che individuerà una condizione utile a stabilire se un numero n sia congruente ed una discussione in merito all'impossibilità di individuare un algoritmo diretto che in pochi passi fornisca una risposta affermativa o negativa in merito alla congruenza di un numero. Di fatti, per poter trovare una tale condizione sarebbe necessaria la dimostrazione dell'equivalenza delle condizioni del Teorema di Tunnel, la quale dipende però dalla Congettura di Birich-Swinnerton-Dyer.

Capitolo 1

I numeri congruenti

Nella prima parte di questo capitolo ci occuperemo di definire in maniera più rigorosa il concetto di *numero congruente* e la corrispondenza biiettiva tra i triangoli di lati X, Y, Z ed area n, ed i numeri x tali che x, $x - n$ ed $x + n$ siano quadrati di numeri razionali.

Ricaveremo poi dalla dimostrazione dell'ultimo fatto che vi è un'equazione cubica utile a caratterizzare i numeri congruenti.

1.1 Cos'è un numero congruente?

Definizione 1.1.1. Un numero razionale positivo $r \in \mathbb{Q}$ è detto *numero congruente* se esso è l'area di un triangolo rettangolo di lati razionali.

Notiamo che, per ogni numero congruente $r \in \mathbb{Q} \setminus \{0\}$, area del triangolo rettangolo di lati $X, Y, Z \in \mathbb{Q}$, possiamo trovare un $s \in \mathbb{Q}$ tale per cui $s^2 r$ sia un intero libero da quadrati ed inoltre il triangolo di lati sX, sY, sZ abbia esattamente area $s^2 r$. Infatti: dall'affermazione che $r \in \mathbb{Q}$ segue che $r = \frac{m}{n}$, con m,n interi ed $n \neq 0$; per cui possiamo riscrivere $r = \frac{a^2 m'}{b^2 n'}$, in modo da esplicitarne tutti i quadrati che lo fattorizzano ed (m',n')=1. È quindi possibile definire s come $s = \frac{bn'}{a'}$, di modo che $s^2 r = \frac{b^2 n'^2}{a^2} \frac{a^2 m'}{b^2 n'} = m'n'$, che risulta libero da quadrati in quanto $(m', n') = 1$. Come conseguenza abbiamo ottenuto un numero intero positivo multiplo di r, numero congruente, che rispetta la definizione appena data e che per tanto a sua volta sarà congruente. In tal modo notiamo che è possibile trovare una classe di equivalenza in $\mathbb{Q}/(\mathbb{Q}^+)^2$ per numeri che siano relazionati come appena spiegato. È di interesse esprimere il concetto di numero congruente nel linguaggio dei gruppi notando che $r \in \mathbb{Q}^+$ è congruente se e solo se lo è ogni rappresentante della classe laterale di $r \in \mathbb{Q}^+/(\mathbb{Q}^+)^2$; infatti ognuna di queste classi laterali contiene un unico numero naturale libero da quadrati $r = n$. Da quest'ultima affermazione ne segue che per

studiare i numeri congruenti possiamo restringerci a studiare numeri naturali liberi da quadrati.

Da un punto di vista algebrico, la condizione che un numero n sia congruente equivale a domandare che, posti $X, Y, Z \in \mathbb{Q}$, con $0 < X < Y < Z$, le equazioni $X^2 + Y^2 = Z^2$ e $\frac{1}{2}XY = n$ abbiano una soluzione comune. Osserviamo a tal proposito che la condizione $X < Y < Z$ non è superflua, infatti non siamo interessati a considerare X, Y, Z e Y, X, Z come triangoli rettangoli distinti ed inoltre la disuguaglianza è necessariamente stretta. L'ultima affermazione deriva dal fatto che, se $X = Y$, la prima delle condizioni sopra riportate assumerebbe la forma $2X^2 = Z^2$ ma, sapendo che $X, Z \in \mathbb{Q}$, potremmo allora scrivere $X = a/b$ e $Z = c/d$, con $a, b, c, d \in \mathbb{Z}$, per cui ne ricaviamo un'equazione equivalente nella seguente forma: $2\left(\frac{a}{b}\right)^2 = \left(\frac{c}{d}\right)^2$ ora possiamo moltiplicare entrambi i membri per b^2 e per d^2 in modo da lavorare con l'equazione $2\bar{a}^2 = \bar{c}^2$, dove $\bar{a}, \bar{c} \in \mathbb{Z}$. Allora $2 = \left(\frac{\bar{c}}{\bar{a}}\right)^2$, per tanto 2 dovrebbe essere un quadrato in $\mathbb{Q}$, infatti il rapporto di interi è sempre un razionale, ma è ovviamente assurdo affermare che $\sqrt{2} \in \mathbb{Q}$.

Un'altra condizione affinché n sia un numero congruente è presentata dalla seguente proposizione

Proposizione 1.1.2. *Sia n un intero positivo privo di quadrati.*
Siano X, Y, Z, x ∈ ℚ tali che X < Y < Z.
Allora vi è una corrispondenza uno-ad-uno tra i triangoli rettangoli di cateti X e Y, ipotenusa Z ed area n, ed i numeri x tali che x, x-n ed x+n siano tutti quadrati di numeri razionali.
Tale corrispondenza è:

$$\alpha: \quad X, Y, Z \longrightarrow x = \left(\frac{Z}{2}\right)^2$$

$$\beta: \quad x \longrightarrow X = \sqrt{x+n} - \sqrt{x-n}, \qquad Y = \sqrt{x+n} + \sqrt{x-n}, \qquad Z = 2\sqrt{x}.$$

Dimostrazione. Iniziamo supponendo che X, Y, Z siano una terna con le proprietà desiderate, ossia: $\begin{cases} X^2 + Y^2 = Z^2 \\ \frac{1}{2}XY = n \end{cases}$.
Adesso, sommando o sottraendo alla prima equazione quattro volte la seconda ricaviamo: $\begin{cases} (X \pm Y)^2 = Z^2 \pm 4n \\ \frac{1}{2}XY = n \end{cases}$ e dividendo per 4 $\begin{cases} \left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n \\ \frac{1}{2}XY = n \end{cases}$.
A questo punto è evidente che ponendo $x = \left(\frac{Z}{2}\right)^2$ vale la condizione per cui i numeri del tipo $x \pm n$ sono quadrati di $\frac{X \pm Y}{2}$, dunque abbiamo appena verificato la buona definizione della prima funzione.
Dimostriamo che, considerati x e $x \pm n$, quadrati, anche la seconda delle funzioni è ben definita, per fare ciò sfruttiamo il risultato appena ottenuto: $x = \left(\frac{Z}{2}\right)^2$.

Innanzitutto vale $\begin{cases} \left(\frac{X\pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n \\ \frac{1}{2}XY = n \end{cases}$; infatti $X^2 = 2x - 2\sqrt{x^2-n^2}$, $Y^2 = 2x + 2\sqrt{x^2-n^2}$ e $Z^2 = 4x$, da cui otteniamo che $X^2 + Y^2 = 4x = Z^2$ e $\frac{1}{2}XY = \frac{1}{2}(\sqrt{x+n}-\sqrt{x-n})(\sqrt{x+n}+\sqrt{x-n}) = \frac{x+n-x+n}{2} = n$. Notiamo inoltre che $X < Y$ e $Y < Z$ perché $Y^2 = 2x + 2\sqrt{x^2-n^2} < 4x = Z^2$.

Mostriamo ora che le due funzioni, α e β, sono una l'inversa dell'altra calcolando:

$$\begin{aligned}\beta(\alpha(X,Y,Z)) &= \beta\left(\left(\frac{Z}{2}\right)^2\right) = \left(\sqrt{\frac{Z^2}{4}+n} - \sqrt{\frac{Z^2}{4}-n}, \sqrt{\frac{Z^2}{4}+n} + \sqrt{\frac{Z^2}{4}-n}, 2\sqrt{\frac{Z^2}{4}}\right) \\ &= \left(\frac{1}{2}(X+Y) - \frac{1}{2}(-X+Y), \frac{1}{2}(X+Y) + \frac{1}{2}(-X+Y), Z\right) \\ &= (X,Y,Z)\end{aligned}$$

$\alpha(\beta(x)) = \alpha(X,Y,2\sqrt{x}) = \left(\frac{2\sqrt{x}}{2}\right)^2 = x.$ □

Problema 1.1.3. Proviamo che 1 non è un numero congruente.

Dimostriamo l'affermazione mediante il metodo discendente di Fermat.
Supponiamo che vi sia un triangolo rettangolo di area 1 e con lati X, Y, Z razionali. Possiamo denominare $X = a|d$, $Y = b|d$ e $Z = c|d$, da cui otteniamo che devono valere

$$a^2 + b^2 = c^2 \qquad ab = 2d^2. \tag{1.1}$$

In particolare possiamo supporre che $(a,b) = 1$, altrimenti sia $g = (a,b)$, allora $g|a$ e $g|b$; segue che $g^2|c^2$ e $g^2|2d^2$, dunque $g|c$ e $g|d$. Dividendo a, b, c, d per g otteniamo altri quattro interi positivi tali che soddisfino (1.1). Denotiamo a', b', c', d' i nuovi interi ricavati per cui vale che $(a', b') = 1$ e con $0 < c' < c$.
Iniziamo ora il processo discendente. Siccome $ab = 2d^2$ e a e b sono coprimi tra loro, almeno uno dei due dovrà sicuramente essere dispari. Dunque $c^2 = a^2 + b^2$ sarà dispari, cioè c lo è. Dal fatto che ab è il doppio di un quadrato e sapendo che $(a,b) = 1$ ne ricaviamo che uno dei due sarà un quadrato, mentre l'altro è equivalente a due volte un quadrato, senza perdere di generalità siano:

$$a = 2k^2, \qquad b = l^2$$

con $k, l \in \mathbb{Z}$ ed l dispari, in quanto lo era b. Sostituendo in (1.1) otteniamo che $4k^4 + b^2 = c^2$, ossia $\frac{c+b}{2}\frac{c-b}{2} = k^4$. Necessariamente $(c+b)/2$ e $(c-b)/2$ devono essere tra loro coprimi, in quanto lo erano b e c, per tanto

$$\frac{c+b}{2} = r^4, \qquad \frac{c-b}{2} = s^4$$

e per lo stesso ragionamento compiuto anteriormente r ed s sono tra loro coprimi. Sommando e sottraendo le ultime due equazione tra loro ricaviamo l'equivalenza

$$b = r^4 - s^4, \qquad c = r^4 + s^4.$$

Allora $l^2 = b = (r^2+s^2)(r^2-s^2)$ ed in particolare (r^2+s^2) e (r^2-s^2) sono tra loro coprimi, infatti entrambi devono essere dispari perché l lo è, inoltre ogni eventuale fattore comune dovrà dividere anche $2r^2$ e $2s^2$, per tanto $(r^2, s^2) = 1$. Dato che il prodotto di (r^2+s^2) con (r^2-s^2) è un quadrato dispari, è vero che

$$r^2 + s^2 = t^2 \qquad r^2 - s^2 = u^2$$

per u, t interi positivi, dispari e coprimi.

Dal fatto che $u \equiv_4 1$, $r^2 - s^2 \equiv_4 1$, che impone r dispari ed s pari; infatti i quadrati sono tutti congrui a 0 o a 1 modulo 4, dunque se fosse s dispari ed r pari avremmo che $r^2 - s^2 = -1 \equiv_4 3$. Risolvendo per r^2 l'equazione otteniamo

$$r^2 = \frac{t^2+u^2}{2} = \left(\frac{t+u}{2}\right)^2 + \left(\frac{t-u}{2}\right)^2,$$

con $(t \pm u)/2 \in \mathbb{Z}$, in quanto sia t che u sono dispari. Denotando

$$a' = \frac{t+u}{2}, \qquad b' = \frac{t-u}{2} \qquad c' = r$$

ritorniamo all'uguaglianza di partenza $a'^2 + b'^2 = c'^2$. Da quanto affermato fino ad ora discende che $(t, u) = 1$, $(a', b') = 1$ e inoltre

$$a'b' = \frac{t^2-u^2}{4} = 2\left(\frac{s}{2}\right)^2.$$

Ponendo $d' = s/2 \in \mathbb{Z}$ ricaviamo (a', b', c', d') come richiesti. Ma allora concludiamo che ciò è assurdo in quanto staremmo affermando che

$$0 < c' = r \leq r^4 \leq r^4 + s^4 = c.$$

Notiamo che ciò conclude la dimostrazione, infatti la seconda uguaglianza in (1.1) teneva in considerazione il fatto che $n = 1$. [1]

1.2 L'equazione cubica

Abbiamo visto che, dati X, Y, Z associati col numero congruente n, otteniamo $\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$.

Quindi, definendo $u = Z/2$ e $v = (X^2 - Y^2)/4$, vi è una soluzione razionale per l'identità $u^4 - n^2 = v^2$. Successivamente, moltiplicando per u^2, otteniamo $u^6 - n^2u^2 = (uv)^2$.
Possiamo ora trovare un punto di coordinate (x, y) che soddisfi all'equazione cubica

$$y^2 = x^3 - n^2x$$

infatti basta porre $x = u^2 = (Z/2)^2$ e $y = uv = (X^2 - Y^2)Z/8$.

Per cui, abbiamo appena ricavato che, dato un triangolo rettangolo di lati X, Y, Z e area n, otteniamo un punto (x, y) del piano cartesiano le cui coordinate sono razionali e che appartiene alla curva $y^2 = x^3 - n^2x$. Ci domandiamo però se sia vero anche il viceversa, ossia se sia possibile affermare che ogni punto del tipo (x, y) con $x, y \in \mathbb{Q}$ che appartiene alla cubica riportata precedentemente sia originata da un triangolo rettangolo. La risposta è no, innanzitutto, per quanto visto nell'ultima proposizione, la coordinata x, definita in questo modo $x = u^2 = (Z/2)^2$, deve trovarsi in $(\mathbb{Q}^+)^2$, perché è il quadrato di un numero razionale. Un'altra considerazione deriva dal fatto che il triangolo X, Y, Z può essere ottenuto da una terna pitagorica primitiva X', Y', Z', dove X', Y', Z' sono i lati del triangolo rettangolo che avrà area s^2n, dividendo per s. Tuttavia in una terna pitagorica primitiva X' e Y' hanno distinta parità e Z' è dispari, per cui $x = (Z/2)^2 = (Z'/2s)^2$ ha denominatore divisibile per 2 e la stessa potenza di 2 che divide il denominatore di Z, divide anche uno degli altri due lati, mentre il terzo è diviso da una potenza di 2 strettamente minore. Tutto ciò ci porta a dedurre che la coordinata x del punto (x, y) deve avere denominatore divisibile per 2.
In conclusione possiamo ricavare la condizione necessaria affinché un punto (x, y), con $x, y \in \mathbb{Q}$, appartenga alla curva $y^2 = x^3 - n^2x$ e derivi da un triangolo rettangolo: x deve essere un quadrato e il suo denominatore deve essere multiplo di 2.

Vediamo ora che questa condizione è anche sufficiente affinché il punto sia ricavabile da un triangolo rettangolo.

Proposizione 1.2.1. *Sia (x,y) un punto di coordinate razionali appartenente alla curva $y^2 = x^3 - n^2x$.*
Supponiamo che x soddisfi le seguenti due condizioni:

1. *è il quadrato di un numero razionale*
2. *ha il denominatore divisibile per 2*

Allora esiste un triangolo rettangolo di lati $X, Y, Z \in \mathbb{Q}$ ed area n tale che $x = \left(\frac{Z}{2}\right)^2$.

Dimostrazione. Sia $u = \sqrt{x} \in \mathbb{Q}^+$. Definiamo $v = y/u$ di modo che $v^2 = y^2/x$, allora utilizzando l'equazione $y^2 = x^3 - n^2x$ ricaviamo l'uguaglianza $v^2 = x^2 - n^2$ da cui $x^2 = v^2 + n^2$.

Sia ora t il denominatore di u (ossia il più piccolo numero tale per cui $tu \in \mathbb{Z}$) da cui, per ipotesi, t è pari. Notiamo che il denominatore di v^2 coincide con quello di x^2 e risulta essere t^4, in quanto $n \in \mathbb{N}$. Otteniamo così che i numeri t^2v, t^2n, t^2x sono una terna pitagorica di numeri tra loro coprimi (il fatto che non abbiano divisori comuni discende dalla possibilità di semplificare t^2 con i denominatori sia di x che di v, per cui l'unico dei valori multiplo di t rimane t^2n, che è anche l'unico intero presente nella terna) e tali per cui t^2n sia pari, infatti lo è t.
Dalle nozioni sulle terne pitagoriche sappiamo che esse si possono scrivere in forma generica come $X = a^2 - b^2$, $Y = 2ab$ e $Z = a^2 + b^2$, per cui esistono a e b tali che valgano le seguenti uguaglianze: $t^2v = a^2 - b^2$, $t^2n = 2ab$ e $t^2x = a^2 + b^2$. Allora il triangolo rettangolo di lati $2a/t$, $2b/t$, $2u$ ha area $2ab/t^2 = n$, come richiesto.
Utilizzando la corrispondenza definita nella Proposizione 1.1.2, troviamo che l'immagine del triangolo rettangolo di lati $X = 2a/t$, $Y = 2b/t$ e $Z = 2u$ è $x = (Z/2)^2 = u^2$. □

1.3 Curve ellittiche

Iniziamo la sezione ricordando alcune definizioni che ci torneranno utili.

Definizione 1.3.1. Siano $\bar{x}, \bar{y} \in K'$ le coordinate di un punto sulla curva algebrica piana C definita dall'equazione $F(x, y) = 0$, diremo che C è *liscia in* $(\bar{x}, \bar{y})$ se le derivate parziali $\partial F/\partial x$ e $\partial F/\partial y$ calcolate in $(\bar{x}, \bar{y})$ non sono entrambe nulle.

Ricordiamo che la derivata di un polinomio ha senso in ogni campo.

Definizione 1.3.2. Una cubica liscia C in $\mathbb{P}^2_K$, con $K = \overline{K}$, con un punto $O \in Supp C$ fissato, si dice *curva ellittica*.

Allora il luogo geometrico dei punti $P = (x, y)$ che soddisfano all'equazione $y^2 = x^3 - n^2x$ è un caso particolare di una curva ellittica.

In generale, sia K un campo e sia $f(x) \in K[x]$ un polinomio cubico con coefficienti in K e radici distinte, eventualmente in un'estensione di K, inoltre supponiamo che K non abbia caratteristica 2; allora le soluzioni dell'equazione

$$y^2 = f(x)$$

sono chiamate *punti in K' della curva ellittica*, dove K' è l'estensione di K dove troviamo anche le radici di $f(x)$.

In particolare, nella sezione precedente, abbiamo trattato il caso in cui $K = K' = \mathbb{Q}$; in questo esempio $y^2 = x^3 - n^2x$ soddisfa le condizioni per essere una curva ellittica in ogni campo K di caratteristica p, con p che non divide $2n$, infatti vogliamo trovare tre radici distinte per l'equazione $f(x) = x^3 - n^2x$, che possono

essere solamente 0 e $\pm n$. In questo caso poi, posto $F(x,y) = y^2 - f(x)$, le derivate parziali sono $-f'(\bar{x})$ e $2\bar{y}$ e queste si annullano simultaneamente se e solo se $\bar{y} = 0$ e se $\bar{x}$ è una radice multipla di $f(x)$.
Terminiamo l'analisi introduttiva della curva presentata, considerando la chiusura di $C \subseteq {\mathbb{P}_{\mathbb{C}}}^2$ ottenuta omogeneizzano il polinomio $y^2 = x^3 - n^2x$ troviamo $\tilde{F}(x_0, x_1, x_2) = x_2^2x_0 - x_1^3 + n^2x_1x_0^2$. Dunque i punti all'infinito sulla curva ellittica dovranno appartenere alla classe di equivalenza di $(0, x_1, x_2)$ e dovranno rispettare l'uguaglianza $0 = \tilde{F}(0, x_1, x_2) = x_2^2x_0 - x_1^3 + n^2x_1x_0^2 \iff 0 = -x_1^3 \iff 0 = x_1$; ne ricaviamo che l'unica classe di equivalenza rimasta sia quella di (0,0,1) e che questo sia anche l'unico punto all'infinito della curva ellittica.

Capitolo 2

Curve ellittiche e funzioni doppiamente periodiche

Nel presente capitolo tratteremo delle nozioni sulle funzioni doppiamente periodiche ed alcune proposizioni che le caratterizzano, per poter comprendere meglio le funzioni ellittiche.

Introdurremo poi la funzione $\wp$ di Wierstrass, che tornerà utile per parlare del campo delle funzioni ellittiche in quanto vedremo che ogni funzione ellittica può essere riscritta in termini di $\wp(z)$, di cui sono noti gli zeri ed i poli.

2.1 Le funzioni doppiamente periodiche

Sia L un reticolo sul piano complesso, cioè l'insieme di tutte le combinazioni lineari intere di due numeri complessi ω_1 e ω_2 che non giacciono sulla stessa retta passante per l'origine, ossia linearmente indipendenti su $\mathbb{R}$. Ad esempio se $\omega_1 = i$ e $\omega_2 = 1$, si ottiene il reticolo degli interi di Gauss, $\{mi + n | m, n \in \mathbb{Z}\}$.

Il parallelogramma fondamentale (rappresentato in Figura 2.1) creato da ω_1 e ω_2 si definisce nel seguente modo:

$$\Pi = \{a\omega_1 + b\omega_2 | 0 \leq a \leq 1, 0 \leq b \leq 1\}$$

Siccome $\{\omega_1, \omega_2\}$ è una base per $\mathbb{C}$ su $\mathbb{R}$, ogni numero $x \in \mathbb{C}$ può essere scritto nella forma $x = a\omega_1 + b\omega_2$, con $a, b \in \mathbb{R}$. Di conseguenza x può essere scritto come somma di un elemento nel reticolo $L = \{m\omega_1 + n\omega_2\}$ e di un elemento in Π; tale scrittura, per a e b non sulla frontiera di Π, è unica.

Notiamo che, al fine di ottenere la parte immaginaria positiva nel rapporto ω_1/ω_2, è necessario scegliere ω_1 e ω_2 in senso orario, tale operazione sarà sempre possibile, in quanto la base del reticolo L non è unica.

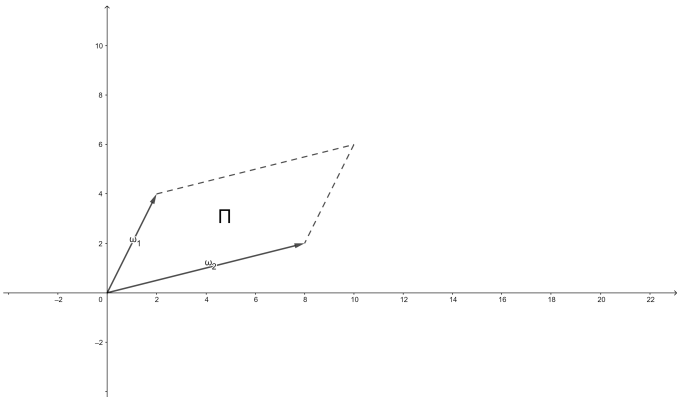

Figura 2.1

Problema 2.1.1. Dimostriamo l'unicità della base del reticolo a meno di trasformazioni per matrici 2×2 ad entrate intere con determinante ± 1.

Preso in considerazione il reticolo $L = \{m\omega_1 + n\omega_2\}$, una sua base è data da $\{\omega_1, \omega_2\}$, supponiamo ora che ve ne sia una seconda della forma $\{\omega_1', \omega_2'\}$. Allora esistono $a, b, c, d \in \mathbb{Z}$ tali che:

$$\omega_1' = a\omega_1 + b\omega_2$$

$$\omega_2' = c\omega_1 + d\omega_2$$

Quindi possiamo riscrivere il sistema sopra in forma matriciale:

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

È noto che il rapporto $\omega_2/\omega_1 \in \mathbb{C} \setminus \mathbb{R}$, infatti il parallelogramma Π deve essere generato da ω_1 e ω_2 linearmente indipendenti in $\mathbb{R}$, per tanto non possono essere quantità puramente reali. Allora, coniugando la formula precedente, otteniamo:

$$\begin{pmatrix} \omega_1' & \bar{\omega_1}' \\ \omega_2' & \bar{\omega_2}' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix}$$

Siccome anche $\{\omega_1', \omega_2'\}$ sono una base di L, lo stesso ragionamento deve valere, ossia devono esistere $a', b', c', d' \in \mathbb{Z}$ tali per cui

$$\begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \omega_1' & \bar{\omega_1}' \\ \omega_2' & \bar{\omega_2}' \end{pmatrix}$$

Per cui, sostituendo nelle precedenti otteniamo

$$\begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix}$$

Proviamo che $\omega_2/\omega_1 \in \mathbb{C} \setminus \mathbb{R}$ implica $det \begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix} \neq 0$:
Sia $\omega_1 = \alpha + \imath\beta$ e $\omega_2 = \gamma + \imath\delta$, allora

$$\frac{\omega_2}{\omega_1} = \frac{(\gamma + \imath\delta)(\alpha - \imath\beta)}{\alpha^2 + \beta^2} = \frac{(\alpha\gamma + \beta\delta) + \imath(\alpha\delta - \beta\gamma)}{\alpha^2 + \beta^2} \in \mathbb{C} \setminus \mathbb{R} \iff \alpha\delta - \beta\gamma \neq 0$$

Se $det \begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix} = \omega_1\bar{\omega_2} - \omega_2\bar{\omega_1} = 0$ ciò equivale ad affermare che

$$\omega_1\bar{\omega_2} = \omega_2\bar{\omega_1} \iff \overline{\left(\frac{\omega_2}{\omega_1}\right)} = \frac{\omega_2}{\omega_1}$$

che è assurdo perché contraddice la condizione che ω_1 e ω_2 siano indipendenti.
Allora è possibile moltiplicare per $\begin{pmatrix} \omega_1 & \bar{\omega_1} \\ \omega_2 & \bar{\omega_2} \end{pmatrix}^{-1} \in GL_2(\mathbb{C})$ e concludere che vale la seguente uguaglianza:

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Concludiamo, in quanto le ultime due matrici sono ad entrate intere ed il prodotto dei loro determinanti deve essere 1, dunque hanno determinate ± 1.

Definizione 2.1.2. Sia $\Omega \subseteq \mathbb{C}$ e sia $f : \Omega \longrightarrow \mathbb{C}$.
Si dice che f è una *funzione meromorfa in* Ω se f è quoziente di $\frac{h_1(z)}{h_2(z)}$, con h_1, h_2 olomorfe in Ω.

Definizione 2.1.3. Sia L un reticolo ed f una funzione meromorfa in $\mathbb{C}$.
Si dice che f è una *funzione ellittica relativa ad* L se è una funzione $f(z+l) = f(z)$ per ogni $l \in L$.

Siccome ci troviamo in un reticolo è sufficiente dimostrare la buona definizione per $l = \omega_1$ e per $l = \omega_2$, ossia stiamo affermando che la definizione di funzione ellittica sia equivalente a quella di funzione doppiamente periodica. Infatti, mediante opportune traslazioni, possiamo fissare l'origine del reticolo in un punto O a noi conveniente, di modo che la funzione considerata non abbia poli all'interno del parallelogramma Π, pertanto ci troviamo in presenza di un'applicazione olomorfa nell'insieme scelto, quindi derivabile in ogni punto del suo supporto. Per concludere facciamo vedere che il campo sia algebricamente chiuso e di $char(K) = 0$, questo risultato segue dalla discussione fatta al Problema 2.1.1, in cui abbiamo osservato che $\omega_2/\omega_1 \in \mathbb{C} \setminus \mathbb{R}$ perché devono essere indipendenti.

In altre parole una funzione ellittica è una funzione doppiamente periodica con periodi ω_1 e ω_2. Una tale funzione è determinata dai valori sul parallelogramma fondamentale Π ed inoltre tali valori coincidono lungo la frontiera di Π, per tanto $f(a\omega_1 + \omega_2) = f(a\omega_1)$ e $f(\omega_1 + b\omega_2) = f(b\omega_2)$. Da questa corrispondenza possiamo

trarne una conclusione topologica sulla forma della varietà complessa difatti, facendo coincidere i lati opposti del parallelogramma, una funzione ellittica $f(x)$ avrà valori su un toro.

D'ora in poi utilizzeremo il simbolo $\mathcal{E}_L$ per denotare l'insieme delle funzioni ellittiche rispetto al reticolo L. Notiamo poi che, per la proprietà discussa in precedenza, $\mathcal{E}_L$ è un sottocampo delle funzioni meromorfe, difatti somma, differenza, prodotto e quoziente di funzioni ellittiche sono funzioni ellittiche; tale sottocampo è inoltre chiuso per la differenziazione.

Di seguito riportiamo alcuni risultati utili a caratterizzare le funzioni ellittiche in campo complesso e diamo delle definizioni che si riveleranno successivamente necessarie alla trattazione.

Teorema 2.1.4 (**di Liouville**). *Ogni funzione intera e limitata, ovvero olomorfa su tutto $\mathbb{C}$, è costante [4].*

Dimostrazione. Sia $f(z)$ una funzione intera, dunque abbiamo che $f(z) = \sum_{k=0}^{\infty} a_k z^k$ e scegliendo un punto fissato z_0, si ha $a_k = \frac{f^{(k)}(z_0)}{k!}$ per $k > 0$.
Inoltre, per la limitatezza, $\exists M > 0$ tale che $|f(z)| < M$ per ogni $z \in \mathbb{Z}$. Dunque:

$$|a_k| \leq \frac{M}{r^k} \xrightarrow[r\to\infty]{} 0$$

Da ciò si conclude che $a_k = 0\ \forall k \geq 1$ e dunque $f(z)$ è costante. □

Proposizione 2.1.5. *Una funzione $f(z) \in \mathcal{E}_L$, con $L = \{m\omega_1 + n\omega_2\}$, e priva di poli all'interno del parallelogramma fondamentale Π, è una funzione costante.*

Dimostrazione. La definizione del parallelogramma fondamentale Π implica che esso sia compatto, quindi chiuso e limitato; ciò implica che ogni funzione ellittica e priva di poli in Π è limitata e per tanto $\exists M \in \mathbb{N} : |f(z)| < M\ \forall$ z. A questo punto per la periodicità ed, essendo $f(z)$ priva di poli, sappiamo che tale funzione è olomorfa e limitata in $\mathbb{C}$, allora per il teorema di Liouville è costante. □

Proposizione 2.1.6. *Facendo uso della stessa notazione della proposizione precedente, denotiamo con $\alpha + \Pi$ la traslazione del parallelogramma fondamentale per un numero complesso α, ossia $\{\alpha + z | z \in \Pi\}$.*
Supponiamo poi che $f(z) \in \mathcal{E}_L$ non abbia poli lungo la frontiera di $\alpha + \Pi$, che denoteremo con C.
Allora la somma dei residui di f(z) in $\alpha + \Pi$ è nulla.

Dimostrazione. Possiamo scrivere la somma dei residui della funzione in questione come

$$\frac{1}{2\pi i} \int_C f(z) dz.$$

Allora iniziamo scegliendo un verso di integrazione lungo il parallelogramma Π, come in Figura 2.2.

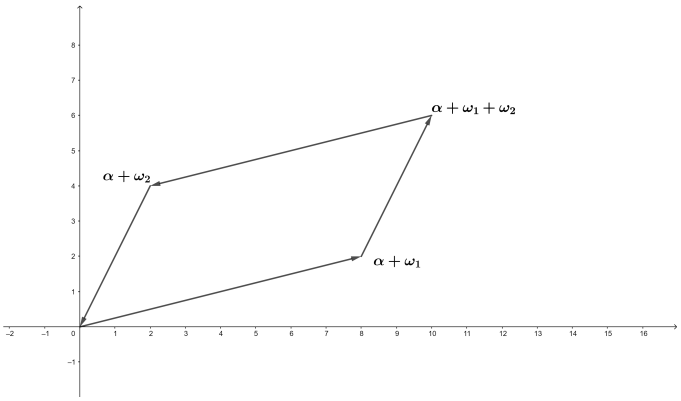

Figura 2.2

Ne segue dunque che, lungo versi opposti, l'integrale di f(z) si annulla, infatti abbiamo visto in precedenza che f(z) assume gli stessi valori lungo la frontiera di $\alpha + \Pi$ ed il segno opposto è fornito dal verso prescelto per integrare. Ciò permette di concludere che

$$\frac{1}{2\pi i} \int_C f(x)dz = 0.$$

□

Osserviamo che, siccome una funzione meromorfa possiede un numero finito di poli in una regione chiusa, è sempre possibile scegliere α di modo che nella frontiera di $\alpha + \Pi$ non vi siano poli di $f(z)$.

Inoltre la Proposizione 2.1.6 implica che ogni funzione $f(z) \in \mathcal{E}_L$ e non costante abbia almeno due poli, o equivalentemente un polo multiplo; infatti se così non fosse la somma dei residui non potrebbe essere zero.

Proposizione 2.1.7. *Supponiamo valgano le ipotesi della Proposizione* 2.1.6 *e supponiamo che f(z) non abbia zeri o poli lungo la frontiera di* $\alpha + \Pi$.
Siano inoltre $\{m_i\}$ *ed* $\{n_j\}$ *rispettivamente gli ordini degli zeri di f(z) e dei poli di f(z) all'interno di* $\alpha + \Pi$.
Allora $\sum m_i = \sum n_j$.

Dimostrazione. L'idea della dimostrazione consiste nell'applicare la Proposizione 2.1.6 alla funzione $f'(z)/f(z)$.
Ricordiamo che la derivata logaritmica $f'(z)/f(z)$ ha un polo semplice esattamente in corrispondenza dello zero di $f(z)$, per cui i residui attorno a tale polo saranno equivalenti all'ordine dello zero o del polo della funzione di origine $f(z)$.
Per tanto, posta $f(z) = c_m(z-a)^m + ...$, segue che $f'(z) = c_m m(z-a)^{m-1} + ...$, da cui ricaviamo

$$\frac{f'(z)}{f(z)} = m(z-a)^{-1} + ...$$

Concludiamo quindi che la somma dei residui per $f'(z)/f(z)$ è $\sum m_i - \sum n_j = 0$. □

2.2 La funzione $\wp$ di Weierstrass

Definizione 2.2.1. Sia $L = \{m\omega_1 + n\omega_2\}$ un reticolo.
Definiamo la funzione $\wp$ *di Weierstrass* relativa al reticolo L come

$$\wp(z, L) = \wp(z; \omega_1, \omega_2) := \frac{1}{z^2} + \sum_{l \in L, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right).$$

In particolare indicheremo la funzione appena definita solamente con $\wp(z)$ nei casi in cui il reticolo L sarà fissato e non vi siano quindi pericoli di ambiguità.

Proposizione 2.2.2. *La somma* $\sum \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$ *converge assolutamente ed uniformemente per* z *in ogni sottoinsieme compatto di* $\mathbb{C} \setminus L$.

L'idea della dimostrazione è quella di procedere come nel caso unidimensionale, anche se in questo contesto ci troviamo in presenza di un reticolo L bidimensionale, per far ciò è necessario l'utilizzo di due lemmi preliminari.

Lemma 2.2.3. *Se la sommatoria a termini positivi* $\sum b_l$ *è convergente, ove la sommatoria è calcolata sugli elementi non nulli del reticolo* L*, e se* $\sum f_l(z)$ *è tale per cui* $|f_l(z)/b_l|$ *raggiunge un limite finito per* $|l| \to \infty$ *uniformemente per* z *in un sottoinsieme di* $\mathbb{C}$*, allora la sommatoria* $\sum f_l(z)$ *converge assolutamente ed uniformemente per* z *in tale insieme.*

Dimostrazione. L'idea della dimostrazione di questo lemma è quella di generalizzare il teorema analogo per serie uniformemente convergenti nel caso unidimensionale.

Riportiamo solo la dimostrazione della convergenza assoluta, quella della convergenza uniforme segue in maniera analoga.

Per ipotesi sappiamo che la sommatoria $\sum_{l \in L} b_l$ converge ed inoltre

$$\left| \frac{f_l(z)}{b_l} \right| \xrightarrow[|l| \to \infty]{} M \qquad \forall z \in C \subseteq \mathbb{C}$$

Data la validità dell'ultimo limite per ogni z nel sottoinsieme C di $\mathbb{C}$, $\exists M' > 0, n \in \mathbb{N} : \forall l$ con $|l| > n$ il $\sup_{z \in C} |f_l(z)| \leq M'|b_l| = M'b_l$, osservando che i b_l sono tutti termini positivi.
Dunque, fissando z, la somma $\sum_{l \in L} |f_l(z)| \leq (C+M) \sum b_l$ e ciò equivale ad affermare che la serie è assolutamente convergente, in quanto per ipotesi $\sum_{l \in L} b_l$ converge. □

Lemma 2.2.4. *La sommatoria* $\sum |l|^{-s}$ *converge se s>2.*

Dimostrazione. Essendo quella in questione una serie sugli elementi del reticolo L, sarà una serie bidimensionale, vogliamo quindi scomporla in due sommatorie unidimensionali, in modo da ricondurci ad oggetti noti, come segue:

$$\sum_{\substack{l\in L\\ l\neq 0}} |l|^{-s} = \sum_{n\in\mathbb{N}} \sum_{n\leq|l|<n+1} |l|^{-s}$$

Così facendo abbiamo costruito dei dischi di diametro 1 in cui sono racchiusi tutti gli elementi l di modulo corrispondente. In totale vi saranno n di tali dischi ed ognuno di essi conterrà n elementi, per tanto la sommatoria è vera l'uguaglianza:

$$\sum_{n\in\mathbb{N}} \sum_{n\leq|l|<n+1} |l|^{-s} = \sum_{n=0}^{+\infty} n\cdot n^{-s} = \sum_{n=0}^{+\infty} \frac{1}{n^{s-1}}.$$

Come desideravamo, la serie a cui ci siamo ricondotti è unidimensionale e per di più è nota la sua convergenza per $s-1>1$, ossia $s>2$. □

Alla luce dei lemmi precedenti, dimostriamo ora la Proposizione 2.2.2, ossia vorremmo far vedere che

$$\sum_{\substack{l\in L\\ l\neq 0}} \frac{1}{(z-l)^2} - \frac{1}{l^2}$$

è una serie assolutamente e uniformemente convergente.

Dimostrazione. Iniziamo scrivendo la somma in questione di modo che ne sia più facile l'osservazione del comportamento asintotico:

$$\sum_{\substack{l\in L\\ l\neq 0}} \frac{1}{(z-l)^2} - \frac{1}{l^2} = \sum_{\substack{l\in L\\ l\neq 0}} \frac{l^2-(z-l)^2}{(z-l)^2 l^2} = \sum_{l\in L\ l\neq 0} \frac{2z-z^2/l}{(z-l)^2 l}$$

Notiamo dall'ultima sommatoria che la serie è asintoticamente equivalente alla serie $\sum_{\substack{l\in L\\ l\neq 0}} |l|^{-3}$, per tanto, dal Lemma 2.2.4 sappiamo che essa convergerà.
Utilizzando invece il Lemma 2.2.3, ponendo $b_l = |l|^{-3}$, otteniamo che la serie converge sia assolutamente che uniformemente per $z\in\mathbb{C}\setminus L$. □

Proposizione 2.2.5. *La funzione $\wp$ di Weierstrass è una funzione ellittica, $\wp\in\mathcal{E}_L$, ed il suo unico polo ha ordine due per ogni punto del reticolo.*

Dimostrazione. Fissato un punto $\bar{l}\in L$ nel reticolo, la funzione $\wp(z)-(z-\bar{l})^{-2}$ assume la forma:

$$\wp(z) - \frac{1}{(z-\bar{l})^2} = \frac{1}{z^2} + \sum_{\substack{l\in L \\ l\neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) - \frac{1}{(z-\bar{l})^2} =$$
$$= \frac{1}{z^2} - \frac{1}{\bar{l}^2} + \sum_{\substack{l\in L \\ l\neq \bar{l} \\ l\neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

Dunque la funzione è continua per $z = l$ in un intorno di $\bar{l}$; di conseguenza la funzione $\wp(z)$ è meromorfa ed ha poli di ordine due per ogni punto di L e per nessun altro z.
Successivamente notiamo che $\wp(z) = \wp(-z)$, ciò segue dal fatto che sommare su $l \in L$ o su $-l \in L$ è equivalente e che quindi possiamo sostituire l con $-l$ ed z con $-z$.
Per dimostrare la doppia periodicità della funzione, prendiamo in considerazione la differenziazione termine a termine:

$$\wp'(z) = -2 \sum_{l\in L} \frac{1}{(z-l)^3}$$

e questa è ovviamente una funzione doppiamente periodica, come possiamo notare dalla sostituzione di $z + l_0$ nelle occorrenze di z, con $l_0 \in L$.
Adesso proviamo che $\wp(z+\omega_i) - \wp(z) = 0$ per $i = 1{,}2$.
Sia $i = 1$, siccome la derivata di $\wp(z+\omega_1) - \wp(z)$ è $\wp'(z+\omega_1) - \wp'(z) = 0$, si ha che $\wp(z+\omega_1) - \wp(z) = C$, per un'opportuna costante C. Ponendo $z = -\frac{1}{2}\omega_1$ ed usando la parità di $\wp(z)$ ricaviamo che $C = \wp(\frac{1}{2}\omega_1) - \wp(-\frac{1}{2}\omega_1) = 0$.
Per tanto concludiamo la dimostrazione, infatti il caso considerando ω_2 è identico. □

Da quanto appena dimostrato e dalla Proposizione 2.1.6 segue che la funzione $\wp(z)$ ha due zeri semplici, oppure uno zero doppio; questo in quanto essa ha un unico polo doppio e la somma dei poli coincide con la somma degli zeri.

Problema 2.2.6. Mostriamo che ogni funzione ellittica del tipo $\wp(z) - c$, con c una costante, ha esattamente due zeri semplici, oppure uno zero di molteplicità 2.

Abbiamo osservato che vi sono due zeri (eventualmente coincidenti) per la funzione $\wp(z)$, con $z \in \alpha + \Pi$, chiamiamo tali elementi a e a^*, infatti saranno tra loro simmetrici nel seguente senso: per ogni $a \in \Pi' = \alpha + \Pi$ esiste $a^* \in \Pi'$ tale che $a^* = \omega_1 + \omega_2 - a$ se a è un punto interno di Π', mentre $a^* = \omega_1 - a$ oppure $\alpha^* = \omega_2 - a$ se a si trova lungo uno dei lati di Π'. Siccome entrambi sono zeri in L è vero che $a + a^* = 0$.
Ora prendiamo in considerazione la funzione $\wp(z) - c$ fornita dal problema, essa avrà gli stessi poli di $\wp(z)$, in quanto c è una costante, allora questa funzione possiede due zeri, per quanto visto alla Proposizione 2.1.6.

Problema 2.2.7. Usando il fatto che $\wp'(z)$ è dispari, mostriamo che gli zeri di $\wp'(z)$ sono esattamente $\omega_1/2$, $\omega_2/2$ e $(\omega_1+\omega_2)/2$.
Definiti $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$ ed $e_3 = \wp((\omega_1+\omega_2)/2)$, mostriamo che essi sono i valori, tra loro distinti, di u tali per cui $\wp(z) - u$ ha uno zero doppio.

Iniziamo domandandoci quali siano gli z_1, z_2 tali che $\wp(z_1) = \wp(z_2) = c$ e per cui vale che $z_1 + z_2 = 0$ in L, come visto nel Problema 2.2.6. Trovandoci in $\Pi' = \alpha + \Pi$ sappiamo che $z_1 = -z_1$, allora seguirà che $z_1 = -z_2 = z_2$ in L e unicamente quattro dei punti nel parallelogramma fondamentale rispettano questa caratteristica: $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$. Il primo di essi ha ordine 2 ed è il polo di $\wp(z)$, e dunque di $\wp(z) - c$, mentre i rimanenti elementi dovranno essere zeri di $\wp'(z)$, in quanto sappiamo che tale funzione è dispari e periodica ed i punti appena elencati sono gli unici tali che $\wp'(\omega_i/2) = -\wp'(-\omega_i/2)$, dove $i = 1,2,3$ e $\omega_3 = \omega_1 + \omega_2$.

Osservando ora $\wp(z) - \wp(\omega_1/2) = 0$, tale equazione si annulla solo per $z = \omega_1/2$, tuttavia la funzione $\wp(z)$ ha un polo doppio, per tanto anche lo zero ottenuto deve avere molteplicità due. Il medesimo ragionamento si può ripetere per $\wp(z) - \wp(\omega_i/2) = 0$, con $i = 2,3$.
Infine, supponiamo che $e_1 = e_2$, allora $\wp(z) - e_1$ avrebbe uno zero in $\frac{1}{2}\omega_2$, tuttavia questo dovrebbe essere congruente con il già noto $\frac{1}{2}\omega_1$, in quanto altro zero unico, ma ciò è falso perché ci troviamo in L. Dunque, con lo stesso argomento, troviamo che $e_1 \neq e_2 \neq e_3$. [5]

2.3 Il campo delle funzioni ellittiche

Dalla Proposizione 2.2.5 abbiamo tratto un esempio concreto di funzione ellittica, desideriamo però ora studiarne l'intero campo, a partire da due funzioni fondamentali $\wp(z)$ e $\wp'(z)$.

Proposizione 2.3.1. *Ogni funzione ellittica in L è esprimibile come espressione razionale in $\wp(z;L)$ e $\wp'(z;L)$, quindi $\mathcal{E}_L = \mathbb{C}(\wp, \wp')$.*
Più precisamente, presa $f(z) \in \mathcal{E}_L$, esistono due funzioni $g(X)$ e $h(X)$ tali che $f(z) = g(\wp(z)) + \wp'(z)h(\wp(z))$.

Dimostrazione. Se f(z) è una funzione ellittica in L, allora anche le funzioni pari

$$f_1(z) := \frac{f(z) + f(-z)}{2} \quad e \quad f_2(z) := \frac{f(z) - f(-z)}{2\wp'(z)}$$

appartengono a $\mathcal{E}_L$, inoltre $f(z) = f_1(z) + \wp'(z)f_2(z)$. Quindi è sufficiente mostrare che le funzioni ellittiche in L pari appartengono a $\mathbb{C}(\wp)$.

Facciamo vedere che il campo delle funzioni ellittiche pari in un reticolo L è generato da $\wp(z)$, ossia che $\mathcal{E}_L^+ = \mathbb{C}(\wp)$. L'idea consiste nella creazione di una funzione con gli stessi zeri e poli di $f(z)$ a partire da una funzione del tipo $\wp(z) - c$,

dove c è una costante. In particolare, il rapporto tra $f(z)$ e $\wp(z) - c$ darà luogo ad una funzione ellittica priva di poli all'interno del parallelogramma considerato, di conseguenza, da quanto dimostrato nella Proposizione 2.1.5, sarà costante.

Supponiamo $f(z) \in \mathcal{E}_L$ sia pari ed elenchiamo tutti gli zeri ed i poli di $f(z)$: Sia $\Pi' = \{a\omega_1 + b\omega_2 | 0 \leq a < 1, 0 \leq b < 1\}$ il parallelogramma fondamentale a cui abbiamo rimosso due lati. Cerchiamo tutti gli zeri ed i poli situati in Π', ognuno con la rispettiva molteplicità, omettendo lo 0 nel caso fosse tra i punti trovati. Ricaviamo un insieme di zeri e poli che possiamo associare a coppie infatti, come detto al Problema 2.2.6, ognuno di essi possiede un simmetrico in L. Da ciascuna delle coppie scegliamo infine un elemento. Iniziamo con gli zeri.

Sia $a \in \Pi'$, con $a \neq 0$, uno degli zeri di $f(z)$, con $a \neq \omega_1/2$, $a \neq \omega_2/2$ oppure $a \neq (\omega_1 + \omega_2)/2$ e sia $a^* \in \Pi'$ il punto simmetrico di a. Supponiamo a sia uno zero per $f(z)$ di ordine m, affermiamo allora che anche a^* è uno zero con il medesimo ordine. Infatti, se $\alpha^* = \omega_1 + \omega_2 - \alpha$, si ha che, essendo $f(z) \in \mathcal{E}_L^+$, $f(\alpha^* - z) = f(\omega_1 + \omega_2 - \alpha - z) = f(\omega_2 - \alpha - z) = f(-\alpha - z) = f(\alpha + z) = 0$, dove le prime due uguaglianze derivano dalla definizione, quelle centrali dal fatto che f è doppiamente periodica e l'ultima dalla parità della funzione; infine questo stesso ragionamento vale anche per le derivate successive di $f(z)$, fino alla m-esima.

Sia ora $a \in \Pi'$ uno zero di $f(z)$, con, $a = \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$. In tal caso dimostriamo che l'ordine di a sia un numero pari, m. Infatti avremmo che $f(a+z) = f(\frac{1}{2}\omega_1 + z) = a_m x^m +$ termini di ordine superiore, allora per la doppia periodicità e per la parità di $f(z)$ abbiamo che $f(\frac{1}{2}\omega_1 - z) = f(-\frac{1}{2}\omega_1 + z) = f(\frac{1}{2}\omega_1 + z)$; segue immediatamente dalle uguaglianze appena riportate che $a_m(z)^m +$ termini di ordine superiore $= a_m(-z)^m +$ termini di ordine superiore. Ricaviamo che m deve essere pari.

Dunque, sia $\{a_i\}$ l'elenco degli zeri di $f(z)$ in Π', che non siano punti medi di punti del reticolo, ognuno ripetuto tante volte quante la propria molteplicità e, considerati a e a^* simmetrici, solo uno di essi verrà preso in considerazione all'interno dell'elenco. In aggiunta, in tale lista vanno considerati gli a tali che siano metà dei punti di fondamentali del parallelogramma, anch'essi presi con la propria molteplicità.

Sia poi $\{b_i\}$ l'elenco di tutti i poli di $f(z)$ non nulli in Π', contati con la stessa regola che è stata indicata per gli elementi di $\{a_i\}$.

Siccome nessuno degli a_i e dei b_i sono nulli, il valore di $\wp(a_i)$ e $\wp(b_i)$ sono finiti, per tanto ha senso definire la funzione ellittica

$$g(z) = \frac{\prod_i (\wp(z) - \wp(a_i))}{\prod_j (\wp(z) - \wp(b_j))}.$$

Allora vogliamo osservare che $g(z)$ ha gli stessi zeri e poli di $f(z)$, considerando anche la molteplicità di ognuno, da cui ne segue che $f(z) = c \cdot g(z)$, per una certa costante c. Per fare ciò, esaminiamo i punti non nulli di Π'. Siccome 0 è l'unico polo del numeratore, ne segue che gli zeri non nulli di $g(z)$ sono gli zeri di $\wp(z) - \wp(a_i)$, mentre i poli di $g(z)$ sono gli zeri di $\wp(z) - \wp(b_i)$. Come abbiamo visto dal Problema

2.2.6, $\wp(z) - u$ ha uno zero doppio in $z = u$ se u è metà del punto fondamentale del reticolo, mentre ha una coppia di zeri semplici in u ed in u^* se u si trova nell'interno di Π'; questi sono gli unici zeri di $\wp(z) - u$ in Π'. Dalla costruzione degli a_i e dei b_i sappiamo che $g(z)$ e $f(z)$ hanno lo stesso ordine di zeri e poli in tutto Π', con un'unica possibile eccezione per il punto 0.

Per tanto manca da dimostrare che essi hanno lo stesso ordine anche in 0. Scegliamo α tale che sulla frontiera di $\alpha + \Pi$ non vi siano punti del reticolo, zeri o poli di $f(z)$ o $g(z)$. Allora $\alpha + \Pi$ conterrà un punto del reticolo l e tutti gli zeri ed i poli di $f(z)$ e $g(z)$ avranno lo stesso ordine in $\alpha + \Pi$, fatta eccezione per l. Sia m_f l'ordine degli zeri di $f(z)$ in l (m_f è negativo nel caso si tratti di un polo) e dia m_g l'analogo per la funzione $g(z)$. Allora abbiamo che

$$\begin{aligned} m_f + &\quad \text{(totale degli ordini degli zeri di f) - (totale degli ordini dei poli di f)} \\ = m_g + &\quad \text{(totale degli ordini degli zeri di g) - (totale degli ordini dei poli di g).} \end{aligned}$$

Siccome gli elementi tra parentesi su entrambi i lati dell'equazione sono equivalenti, ne ricaviamo che $m_f = m_g$. Possiamo concludere allora ricordando la Proposizione 2.1.6, da cui otteniamo che, se in ogni punto eccetto uno sul parallelogramma fondamentale, gli ordini di zeri e poli di due funzioni ellittiche coincidono, allora, essendo la somma coincidente, questo varrà anche nel punto in questione. □

Notiamo che, l'ultima dimostrazione è di tipo costruttivo, infatti permettere di esprimere una funzione ellittica in termini di $\wp(z)$, una volta noti i suoi zeri ed i suoi poli.

In conclusione al capitolo, sempre a partire dall'ultima Proposizione (2.3.1), possiamo notare i seguenti fatti:

Osservazione 1. La funzione ellittica $\wp(Nz)$, con N intero positivo, è una funzione razionale in $\wp(z)$.

Osservazione 2. Dato che la funzione ellittica $\wp'(z)$ è dispari e ha tre zeri semplici ed un polo triplo in 0, ne segue che l'applicazione pari $\wp'(z)^2$ è esprimibile come polinomio cubico in $\wp(z)$.

Capitolo 3

Forma di Weierstrass e legge di addizione

Abbiamo concluso il capitolo precedente osservando che $\wp'(z)^2$ è un polinomio cubico in $\wp(z)$, inoltre, dal Problema 2.2.6, sappiamo che gli zeri di una tale funzione saranno e_1, e_2 e e_3, dove $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$ ed $e_3 = \wp((\omega_1+\omega_2)/2)$, ciascuno con molteplicità due. Nel presente capitolo vogliamo introdurre la forma di Weierstrass per le curve ellittiche e la legge di addizione per le funzioni $\wp$ di Weierstrass

3.1 Curve ellittiche nella forma di Weierstrass

Per quanto detto precedentemente:

$$\begin{aligned}\wp'(z)^2 &= C(\wp(z)-\wp(\omega_1/2))(\wp(z)-\wp(\omega_2/2))(\wp(z)-\wp((\omega_1+\omega_2)/2)) \\ &= C(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)\end{aligned}$$

con C una costante. Al fine di determinare C, compariamo l'espressione appena scritta con l'espansione in serie di Laurent nell'origine. Ricordando che $\wp(z)-z^{-2}$ è continua nell'origine e notiamo che anche $\wp'(z)+2z^{-3}$ gode della stessa proprietà. Per tanto il termine dominante in $\wp'(z)^2$ sarà $(-2z^{-3})^2 = 4z^{-6}$ ed invece a destra dell'uguale avremo $C(z^{-2})^3 = Cz^{-6}$; ne ricaviamo che $C = 4$.

Dunque $\wp(z)$ soddisfa all'equazione differenziale:

$$\wp'(z)^2 = f(\wp(z)) \qquad \text{con } f(x) = 4(x-e_1)(x-e_2)(x-e_3) \in \mathbb{C}[x]$$

Ora, sapendo che stiamo cercando un'equazione differenziale nella forma $\wp'(z)^2 = f(\wp(z))$ e che $f(x)$ deve essere un polinomio cubico, lo possiamo riscrivere in forma

generica come $f(x) = ax^3 + bx^2 + cx + d$. Vorremmo proseguire espandendo in serie di Laurent $f(\wp(z))$ e confrontarla con l'espansione di $\wp'(z)^2$; allora la differenza $\wp'(z)^2 - f(\wp(z))$ sarà una funzione ellittica, priva di poli in zero dato che $\wp(z)$ e $\wp'(z)$ posseggono gli stessi poli in L. Per quanto visto alla Proposizione 2.1.5, $\wp'(z)^2 - f(\wp(z))$ sarà una funzione costante, quindi, scegliendo opportunamente d, possiamo rendere tale costante 0.
Espandiamo $\wp(z)$ e $\wp'(z)^2$ in un opportuno intorno dell'origine. Sia c il minimo valore assoluto non nullo tra i punti l del reticolo ed $r < 1$ e appartenente al disco di centro 0 e raggio rc. Inoltre, essendo le funzioni in questione entrambe pari, compariranno unicamente le potenze pari dell'espansione.

È noto che la serie geometrica $\frac{1}{1-x} = 1 + x + x^2 + \dots$, per tanto si avrà che $\frac{1}{(1-z/l)^2} = 1 + 2\frac{z}{l} + 3\frac{z^2}{l^2} + 4\frac{z^3}{l^3} + \dots$. Ora, sottraendo 1 ad entrambi i membri e dividendoli per l^2, otteniamo dalla Definizione 2.2.1 che:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l\in L\\ l\neq 0}} 2\frac{z}{l^3} + 3\frac{z^3}{l^4} + 4\frac{z^3}{l^5} + \dots + (k-1)\frac{z^{k-2}}{l^k} + \dots$$

Affermiamo che la serie è assolutamente convergente per $|z| < rc$, infatti i termini della somma, con $|z| < r|l|$, saranno del tipo:

$$2|z| \cdot |l|^{-3} \cdot \left(1 + \frac{3}{2}r + \frac{4}{2}r^2 + \frac{5}{2}r^3 + \dots\right) < \frac{2|z|}{(1-r)^2}\frac{1}{|l|^3}$$

allora, utilizzando il Lemma 2.2.4, sappiamo che l'ultima delle quantità trovata converge assolutamente in L.

Data la convergenza appena dimostrata, è giustificata la seguente scrittura:

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \dots \tag{3.1}$$

dove denotiamo con

$$G_k = G_k(L) = G_k(\omega_1, \omega_2) := \sum_{\substack{l\in L\\ l\neq 0}} l^{-k} = \sum_{\substack{m,n\in\mathbb{Z}\\ (m,n)\neq(0,0)}} \frac{1}{(m\omega_1 + n\omega_2)^k} \qquad \text{con } k > 2.$$

Ora, utilizzando la formula (3.1), eventualmente riordinandone i termini, otteniamo:

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \dots \tag{3.2}$$

$$\wp'(z)^2 = \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8)z^2 + \dots \tag{3.3}$$

$$\wp(z)^2 = \frac{1}{z^4} + 6G_4 + 10G_6 z^2 + \dots \tag{3.4}$$

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + (21G_8 + 27G_4^2)z^2 + \dots \tag{3.5}$$

Ricordando che siamo interessati a trovare i coefficienti a, b, c, d di $f(x) = ax^3 + bx^2 + cx + d$ tali per cui:

$$\wp'(z)^2 = a\wp(z)^3 + b\wp(z)^2 + c\wp(z) + d$$

moltiplicando l'equazione 3.5 per a, l'equazione 3.4 per b e l'equazione 3.1 per c e sommando poi questi risultati con d otteniamo che:

$$\begin{aligned}\wp'(z)^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8)z^2 + \dots \\ &= a\frac{1}{z^6} + a9G_4\frac{1}{z^2} + \dots + b\frac{1}{z^4} + b6G_4 + \dots + c\frac{1}{z^2} + \dots + d.\end{aligned}$$

Da ciò si ricava che $a = 4$, $b = 0$, $c = -60G_4$ e $d = -140G_6$.

La notazione tradizionale vuole che:

$$\begin{aligned}g_2 = g_2(L) &:= 60G_4 = 60\sum_{\substack{l\in L\\ l\neq 0}} l^{-4} \\ g_3 = g_3(L) &:= 104G_6 = 140\sum_{\substack{l\in L\\ l\neq 0}} l^{-6}\end{aligned}$$

Concludiamo dunque che l'equazione differenziale ha la forma:

$$\wp'(z)^2 = f(\wp(z)) \qquad \text{con } f(x) = 4x^3 - g_2x - g_3 \in \mathbb{C}[x]. \tag{3.6}$$

Problema 3.1.1. Utilizziamo il metodo appena visto per effettuare considerazioni sui coefficienti di ordine superiore dell'equazione differenziale e cercare relazioni tra i vari G_k.

Iniziamo scrivendo le equazioni riportate in precedenza, opportunamente riordinate ma, in quest'occasione includendo termini di ordine superiore. Dunque, per quanto visto, $a = 4$, $b = 0$, $c = -60G_4$ e $d = -140G_6$, per cui:

$$\begin{aligned}\wp'(z)^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + (36G_4^2 - 168G_8)z^2 + 240G_4G_6z^4 + (400G_6^2 + 504G_4G_8)z^6 + \dots \\ &= 4\frac{1}{z^6} + 36G_4\frac{1}{z^2} + 60G_6 + (108G_4^2 + 84G_8)z^2 + 4(27G_4^3 + 75G_6^2)z^6 + \dots \\ &+ \frac{-60G_4}{z^2} - 180G_4^2z^2 - 300G_4G_6z^4 - 420G_4G_8z^6 + \dots \\ &- 140G_6.\end{aligned}$$

Per tanto deve valere l'uguaglianza $36G_4^2 - 168G_8 = 108G_4^2 + 84G_8 - 180G_4^2$, da cui si ricava che $G_8 = \frac{3}{7}G_4^2$.

Ora vorremmo far vedere che $G_k \in \mathbb{Q}[G_4, G_6]$.

Questo risultato può essere visto in maniera intuitiva considerando che all'interno dell'equazione differenziale i termini G_k con k minore verranno introdotti

dal prodotto di $c \cdot \wp(z)$. Per tanto, procediamo in maniera induttiva notando che, estendendo le espressioni di $\wp'(z)^2$, $\wp(z)^3$ e $\wp(z)$ a potenze di z^{k-2} maggiori, ci troveremo a punto di incontrare un nuovo G_k in $\wp(z)$, senza che questo sia rilevante al confronto nelle espressioni di $\wp'(z)^2$ e $\wp(z)^3$, in quanto in esse sarà moltiplicato per termini superiori. Allora ognuno dei G_k con $k > 6$ comparirà una sola volta nell'uguaglianza che ricaviamo e potrà essere riscritto come espressione dipendente solamente da G_4 e G_6.

Ripartendo dall'equazione (3.6) e dalla conclusione topologica tratta alla Sezione 2.1, consideriamo una funzione dal toro $\mathbb{C}/L$ in $\mathbb{P}^2_{\mathbb{C}}$ definita come:

$$\begin{aligned} &z \mapsto (1, \wp(z), \wp'(z)) \qquad \text{con } z \neq 0 \\ &0 \mapsto (0,0,1) \end{aligned}$$

Notiamo che l'immagine di ogni z non nullo in $\mathbb{C}/\mathbb{L}$ è un punto del piano cartesiano le cui coordinate x e y soddisfano all'equazione $y^2 = f(x)$.

Proposizione 3.1.2. *L'applicazione*

$$\begin{aligned} &z \mapsto (1, \wp(z), \wp'(z)) \qquad \textit{con } z \neq 0 \\ &0 \mapsto (0,0,1) \end{aligned}$$

è analitica ed è una corrispondenza biiettiva tra $\mathbb{C}/L$ e i punti della curva ellittica di equazione $x_0x_2^2 = 4x_1^3 - g_2(L)x_0^2x_1 - g_3(L)x_0^3$ in $\mathbb{P}^2_{\mathbb{C}}$.

Dimostrazione. Mostriamo che la mappa definita è una corrispondenza uno ad uno. Ad ogni x_1, fatta eccezione per le radici di $f(x)$ ed il punto all'infinito, ci sono esattamente due z tali che $\wp(x_2) = x_1$, in quanto la funzione ellittica di Weierstrass è un'applicazione dal toro in $\mathbb{C}/L$. Allora le coordinate $x_2 = \wp'(z)$ associate ad i due z sono le radici quadrate di $f(x) = f(\wp(z))$.
Se invece x_1 fosse una delle radici di $f(x)$, allora vi sarebbe un unico z tale che $\wp(z) = x_1$ e la corrispondente coordinata x_2 sarebbe $x_2 = \wp'(z) = 0$, per tanto stiamo ritrovando le soluzioni a $x_2^2 = f(x)$ per una data x.

Vediamo ora l'analiticità della funzione.
La mappa da $\mathbb{C}/L$ in una curva ellittica in $\mathbb{P}^2_{\mathbb{C}}$ è analitica se in ogni intorno di un punto in $\mathbb{C}/L$ la funzione può essere espressa come terna di funzioni analitiche. In particolare, se il punto non appartiene al reticolo, consideriamo la mappa $z \mapsto (1, \wp(z), \wp'(z))$, invece per i punti di L possiamo prendere $z \mapsto (1/\wp'(z), \wp(z)/\wp'(z),1)$. □

Data la biiettività della mappa, vorremmo trovarne l'inversa. Integrando da un punto fissato fino ad un punto finale variabile otteniamo $dx/y = (4x^3 - g_2x - g_3)^{-1/2}dx$. Ovviamente l'integrale dipende dal cammino prescelto, tuttavia i differenti risultati differiranno solamente per un elemento di L.

3.2 La legge di addizione

Dalla Proposizione 3.1.2 sappiamo che vi è una corrispondenza biiettiva tra i punti di $\mathbb{C}/L$ e quelli dell'equazione $x_2^2 = 4x_1^3 + g_2(L)x_1 - g_3(L)$ in $\mathbb{P}^2_{\mathbb{C}}$; dunque sommare punti in $\mathbb{C}/L$ equivale ad eseguire la somma tra numeri complessi modulo L.

Vorremmo però estendere la definizione di legge di addizione anche per i punti della curva ellittica nel seguente modo:

Definizione 3.2.1. Siano $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ punti sulla curva ellittica e siano z_1, z_2 tali per cui $P_1 = (\wp(z_1), \wp'(z_1))$ e $P_2 = (\wp(z_2), \wp'(z_2))$. Allora definiamo $P_1 + P_2 = (\wp(z_1 + z_2), \wp'(z_1 + z_2))$.

Lemma 3.2.2. *Sia $f(z) \in \mathcal{E}_L$, sia $\Pi = \{a\omega_1 + b\omega_2 | 0 \leq a, b \leq 1\}$ il parallelogramma fondamentale per il reticolo L e scegliamo α tale che $f(z)$ non abbia zeri o poli nella frontiera di $\alpha + \Pi$. Sia poi $\{a_i\}$ l'elenco degli zeri di $f(z)$ in $\alpha + \Pi$, ognuno ripetuto tante volte quante la sua molteplicità, e $\{b_j\}$ quello dei poli.*
Allora $\sum a_i - \sum b_j \in L$.

Dimostrazione. Ricordiamo che la funzione $f'(z)/f(z)$ ha poli negli zeri e nei poli di $f(z)$. Inoltre la sua espansione in uno zero di $f(z)$, a, di ordine m sarà $m/(z-a)+\dots$ (mentre in un intorno di uno dei poli b con molteplicità $-m$ lo sviluppo in serie è $-m/(z-b)+\dots$). Allora la funzione $zf'(z)/f(z)$ presenta gli stessi poli, tuttavia usando l'uguaglianza $z = a + (z-a)$ notiamo che il primo elemento dell'espansione è $am/(z-a)$. Ne ricaviamo che $\sum a_i - \sum b_j$ coincide con la somma dei residui di $zf'(z)/f(z)$ all'interno di $\alpha + \Pi$. Per comodità indichiamo con C la frontiera del parallelogramma $\alpha + \Pi$ e utilizzando il teorema dei residui:

$$\sum a_i - \sum b_j = \frac{1}{2\pi\imath} \int_C \frac{zf'(z)}{f(z)} dz$$

Ricordando la Figura 2.2, iniziamo ad integrare lungo lati opposti da α ad $\alpha + \omega_2$ e da $\alpha + \omega_1$ ad $\alpha + \omega_1 + \omega_2$, ottenendo che:

$$\begin{aligned}
&\frac{1}{2\pi\imath} \left(\int_\alpha^{\alpha+\omega_2} z\frac{f'(z)}{f(z)} dz - \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)} dz \right) = \\
&= \frac{1}{2\pi\imath} \left(\int_\alpha^{\alpha+\omega_2} z\frac{f'(z)}{f(z)} dz - \int_\alpha^{\alpha+\omega_2} (z+\omega_1)\frac{f'(z)}{f(z)} dz \right) = \\
&= -\omega_1 \frac{1}{2\pi\imath} \int_\alpha^{\alpha+\omega_2} \frac{f'(z)}{f(z)} dz.
\end{aligned}$$

Usando il cambiamento di variabili $u = f(z)$, otteniamo che $f'(z)dz/f(z) = du/u$, indichiamo poi con C_1 il cammino chiuso da $f(\alpha)$ ad $f(\alpha + \omega_2) = f(\alpha)$, allora

$$\frac{1}{2\pi\imath} \int_\alpha^{\alpha+\omega_2} \frac{f'(z)}{f(z)} dz = \frac{1}{2\pi\imath} \int_{C_1} \frac{du}{u}$$

Tale integrale restituisce come risultato $-\omega_1 n$ dove $n \in \mathbb{Z}$ è il numero di volte che il cammino chiuso C_1 gira attorno all'origine.

Possiamo ripetere un ragionamento similare per i lati restanti, ossia da α ad $\alpha+\omega_1$ e da $\alpha+\omega_2$ ad $\alpha+\omega_1+\omega_2$, ottenendo come risultato $-\omega_2 m$, per un opportuno $m \in \mathbb{Z}$.

In conclusione $\sum a_i - \sum b_j = -n\omega_1 - m\omega_2 \in L$, come richiesto dall'enunciato. □

Vediamo il significato della somma da un punto di vista geometrico.

Per $z \in \mathbb{C}/L$, siano $P_z = (1, \wp(z), \wp'(z))$ e $P_0 = (0,0,1)$ punti della curva ellittica $x_2^2 = f(x_1) = x_1^3 - g_2(L)x_1 - g_3(L)$. Supponiamo di voler sommare $P_{z_1} = (1, x_1^1, x_2^1)$ a $P_{z_2} = (1, x_1^2, x_2^2)$ per ottenere $P_{z_1+z_2} = (1, x_1^3, x_2^3)$.
Iniziamo trattando alcuni casi particolari:

- Sia $P_0 = 0 = (0,0,1)$ il punto all'infinito e supponiamo che z_2 sia nullo, in questo caso la somma è banalmente $P_{z_1} + P_0 = P_{z_1}$.
- Nella situazione in cui $P_{z_1} = (1, x_1^1, x_2^1)$ e $P_{z_2} = (1, x_1^1, -x_2^1)$ abbiamo che $z_1 = -z_2$ in quanto gli unici punti per cui il valore di $\wp(z)$ coincide sono i simmetrici rispetto al reticolo L (come definiti all'esercizio 2.2.6). Dunque $P_{z_1} + P_{z_2} = P_0 = 0$ e tali punti sono uno l'opposto dell'altro. Da un punto di vista geometrico ciò significa che la somma di punti appartenenti alla medesima retta verticale è nulla.
- Un sottocaso dell'ultimo punto è quello per cui $P_{z_1} = P_{z_2}$. Notiamo che $x_2^1 = -x_2^2 = 0$, per tanto si ha che $P_{z_1} + P_{z_2} = 2P_{z_1} = 0$.

Proposizione 3.2.3. *L'opposto del punto* $(1, x_1, x_2)$ *è* $(1, x_1, -x_2)$.

Dimostrazione. La dimostrazione è stata vista poco sopra: siano $P_1 = (1, x_1, x_2)$ e $P_2 = (1, x_1, -x_2)$, siccome i due punti sono distinti ma hanno la seconda coordinata coincidente, $x_1 = \wp(z_1)$, ne segue che stiamo cercando due punti z_1 e z_2 simmetrici in L, ossia $z_1 = -z_2$. Dunque anche $P_1 = -P_2$. □

Consideriamo ora due punti $P_1 = P_{z_1} = (1, \alpha_1, \alpha_2)$ e $P_2 = P_{z_2} = (1, \beta_1, \beta_2)$ appartenenti alla curva $x_2^2 = 4x_1^3 - g_2(L)x_1 - g_3(L)$ ed entrambi distinti da P_0, allora esiste una retta passante per essi, $l = \overline{P_1 P_2}$. Se $P_1 = P_2$ allora poniamo l la retta tangente alla curva ellittica in P_1, mentre quando l è verticale abbiamo visto che $P_1 + P_2 = 0$.
Supponiamo che l non sia descritta dai casi precedenti e cerchiamo $P_1 + P_2 = P_3 = (1, \gamma_1, \gamma_2)$ tale per cui $-P_3 = (1, \gamma_1, -\gamma_2)$ è il terzo punto di intersezione tra la retta e la curva.

Scriviamo l'equazione di $l = \overline{P_1 P_2}$ nella forma $y = mx + q$. Un punto $(x, y) \in l$ appartiene alla curva ellittica se $(mx+q)^2 = f(x) = 4x^3 - g_2 x - g_3$, ossia se e solo se x è una radice del polinomio cubico $f(x) - (mx+q)^2$. Tale polinomio ha tre radici coincidenti con i punti di intersezione tra l e la curva ellittica. Se x fosse una sua radice di molteplicità maggiore di 1, allora l interseccherebbe $4x^3 - g_2 x - g_3$ in

un punto (x, y) di molteplicità due o tre.
Notiamo che anche nel caso in cui l sia una retta verticale il numero di intersezioni totali rimane invariato, infatti oltre ai punti affini (coincidenti o distinti) è necessario considerare anche il punto all'infinito.
Quanto appena affermato è stato provato nel Teorema di Bezout.

Teorema 3.2.4 (di Bezout). *Siano $\tilde{F}(x_0, x_1, x_2)$ e $\tilde{G}(x_0, x_1, x_2)$ due polinomi omogenei rispettivamente di grado m ed n in un campo algebricamente chiuso K. Supponiamo inoltre che non vi siano fattori comuni tra $\tilde{F}$ e $\tilde{G}$.*
Allora le curve $\tilde{F}$ e $\tilde{G}$ in $\mathbb{P}^2_K$ si intersecano in esattamente mn punti, contati con molteplicità.

Nel caso di nostro interesse poniamo $\tilde{F}(x_0, x_1, x_2) = x_2^2 x_0 - 4x_1^3 + g_2 x_1 x_0^2 + g_3 z_0^3$ e $\tilde{G}(x_0, x_1, x_2) = x_1 - mx_1 + qx_0$.

Proposizione 3.2.5. *Se $P_1 + P_2 = P_3$, allora $-P_3$ è il terzo punto di intersezione di $l = \overline{P_1 P_2}$ con la curva ellittica.*
Se invece $P_1 = P_2$, allora con $\overline{P_1 P_2}$ facciamo riferimento alla retta tangente in P_1.

Dimostrazione. I casi particolari per cui P_1 o P_2 coincide con P_0 e quando $P_1 = -P_2$ sono stati trattati in precedenza.
Analizziamo quindi la situazione generica in cui $l = \overline{P_1 P_2}$ ad ha equazione $y = mx + q$, mentre $P_1 = P_{z_1}$ e $P_2 = P z_2$ sono punti distinti. Affermare che un punto $P_z = (\wp(z), \wp'(z))$ appartiene ad l equivale alla validità dell'equazione $\wp'(z) = m\wp(z) + q$. La curva ellittica $\wp'(z) - m\wp(z) - q$ ha tre poli e dunque tre zeri in $\mathbb{C}/L$, due dei quali sono z_1 e z_2. Per il Lemma 3.2.2, la somma dei tre zeri e dei tre poli è nulla modulo L; tuttavia nel presente caso la somma dei poli è zero in quanto tutti coincidono con i poli di $\wp'(z)$, che si trovano in 0, per tanto il terzo zero della curva deve trovarsi in $-(z_1 + z_2)$ modulo L. Concludiamo che il terzo punto di intersezione tra l e la curva di origine è $P_{-(z_1+z_2)} = P_{z_3}$.
Manca lo studio della situazione in cui l'intersezione tra l e la curva $\tilde{F}(x_0, x_1, x_2)$ avviene in un punto di molteplicità maggiore di 1. Siano z_1, z_2 e $-z_3$ gli zeri di $\wp'(z) - m\wp(z) - q$, contati con molteplicità e dove nessuno di questi è opposto di un altro, dato che abbiamo supposto l non verticale. Per costruzione $-z_1, -z_2$ e z_3 sono gli zeri di $\wp'(z) + m\wp(z) + q$. Dunque $\pm z_1, \pm z_2$ e $\pm z_3$ sono i sei zeri di $\wp'(z)^2 - (m\wp(z)+q)^2 = f(\wp(z)) - (m\wp(z)+b)^2 = 4(\wp(z)-\alpha_1)(\wp(z)-\alpha_2)(\wp(z)-\alpha_3)$, con $\alpha_1, \alpha_2, \alpha_3$ le radici di $f(x) - (mx + q)^2$. Poniamo caso sia $\wp(z) = \alpha_1$, allora la molteplicità di α_1 dipende dal numero di $\pm z_2, \pm z_3$ che eguagliano $\pm z_1$; questo è equivalente al numero di $z_2, -z_3$ che coincidono con z_1.
Il ragionamento appena proposto permette di concludere che è coincidente il significato di molteplicità di uno degli zeri e quello di molteplicità di intersezione tra le due curve, ossia supposto z_i di molteplicità 2 o 3, la molteplicità di intersezione tra $\tilde{F}$ e $\tilde{G}$ sarà 2 o 3, rispettivamente. □

Dall'ultima proposizione ricaviamo un metodo grafico per sommare due punti tra loro. Considerati P_1 e P_2 reali, tracciamo la retta passante per essi e troviamo il terzo punto di intersezione con la cubica, $-P_3$, i simmetrico di questo rispetto all'asse x sarà $P_3 = P_1 + P_2$, come mostrato in Figura 3.1.

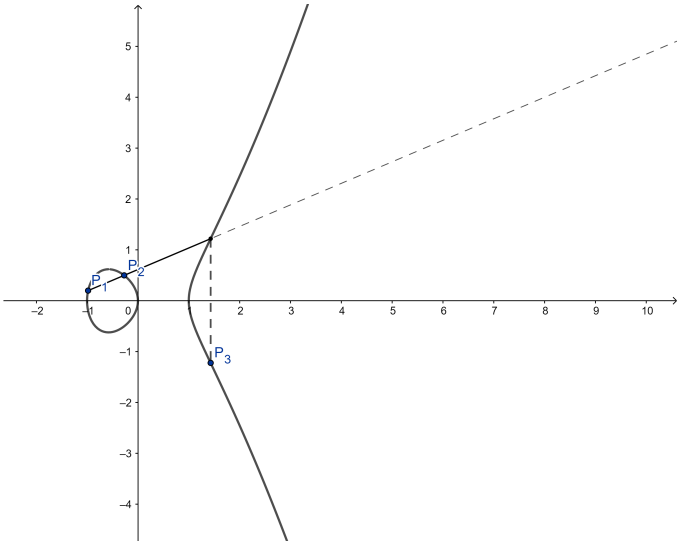

Figura 3.1

Dalla procedura geometrica alla Proposizione 3.2.5, vorremmo ora ricavare una formula unicamente dipendente dalle coordinate dei punti e con valore per ogni curva ellittica.

Proposizione 3.2.6. *Considerata una curva ellittica $C \subseteq \mathbb{P}^2_{\mathbb{C}}$, $(C, +)$ è un gruppo abeliano.*

Dimostrazione. Definiamo con $P_1 * P_2$ il terzo punto di intersezione tra la curva ellittica C e la retta $l = \overline{P_1 P_2}$.
Abbiamo verificato in precedenza l'esistenza dell'elemento neutro, P_0, e quella di un inverso, dunque è sufficiente vedere che il gruppo sia abeliano e che valga l'associatività.
Siano $P_1, P_2 \in C$, allora $P_1 + P_2 = -(P_1 * P_2) = P_0 * (P_1 * P_2)$, dall'ultima uguaglianza notiamo che i punti $P_1 * P_2$ e $P_2 * P_1$ coincidono in quanto la retta $l = \overline{P_1 P_2} = \overline{P_2 P_1}$.
Siano $P_1, P_2, P_3 \in C$, allora definiamo $S = P_1 + (P_2 + P_3)$ e $T = (P_1 + P_2) + P_3$. Calcolando la somma $P_2 + P_3$ stiamo costruendo 2 rette, l_1, l_2, in più sommando al punto $P_2 + P_3$ il punto P_1 troviamo altre due rette, l_3, l_4. Analogamente si trovano quattro rette anche nella costruzione di T, chiamiamole d_1, d_2, d_3, d_4. Definiamo ora due cubiche distinte $F = l_1 \cup l_3 \cup d_2$ e $G = d_1 \cup d_3 \cup l_2$ e le intersechiamo con la curva ellittica C ottenendo $F \cap C = \{P_0, P_1, P_2, P_3, P_1 * P_2, P_2 * P_3, P_1 + P_2, P_2 + P_3, (P_1 + P_2) * P_3\}$ e $G \cap C = \{P_0, P_1, P_2, P_3, P_1 * P_2, P_2 * P_3, P_1 + P_2, P_2 + P_3, (P_2 + P_3) * P_1\}$. Ora è noto

che otto dei nove punti delle due cubiche coincidono, per tanto esse coincideranno anche in $(P_1 + P_2) * P_3 = (P_2 + P_3) * P_1$, ne concludiamo che $P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$. □

Essendo $(C, +)$ un gruppo abeliano possiamo osservare che la legge di addizione non vale solamente per la curva ellittica $y^2 = f(x) = x^3 - g_2(L)x - g_3(L)$ per un reticolo L, ma per tutte le cubiche generiche $y^2 = f(x) = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$ con radici distinte.
Siano $P_1, P_2 \neq P_0$ e $P_1 \neq -P_2$, dunque $l = \overline{P_1P_2}$ può essere scritta nella forma $y = mx + q$, con $m = \frac{y_2 - y_1}{x_2 - x_1}$ se $P_1 \neq P_2$, mentre $m = dx/dy|_{(x_1,y_1)}$ se $P_1 = P_2$, invece $q = y_1 - mx_1$. Chiamiamo x_3 l'ascissa del terzo punto di intersezione $-P_3$ tra la retta l e la cubica, allora $x_1 + x_2 + x_3 = -(b - m)^2/a$, da cui ricaviamo che:

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \quad \text{se } P_1 \neq P_2 \tag{3.7}$$

$$x_3 = -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right) \quad \text{se } P_1 = P_2 \tag{3.8}$$

Osservando che $-y_3 = mx_3 + q$, ricaviamo anche

$$y_3 = -y_1 + m(x_1 - x_3).$$

Concludiamo il capitolo notando che, se una curva ellittica fosse stata nella forma di Weierstrass, $y^2 = 4x^3 - g_2x - g_3$, allora avremmo avuto $a = 4, b = 0$ e $f'(x_1) = 12x_1^2 - g_2$, come già visto in precedenza.

Capitolo 4

Punti di ordine finito e su campi finiti

A conclusione del capitolo precedente abbiamo visto che, fissata una curva ellittica C, $(C,+)$ è un gruppo abeliano. Nel presente capitolo analizzeremo il suo sottogruppo di torsione, studieremo il caso di campi finiti e daremo alcune conclusioni in merito ai numeri congruenti.

4.1 Punti di ordine finito

In ogni gruppo abeliano gli elementi di ordine finito formano un sottogruppo, detto sottogruppo di torsione; in particolare, nel gruppo dei punti in $\mathbb{P}^2_{\mathbb{C}}$ sulla curva ellittica $y^2 = f(x)$, vediamo che i punti del tipo $P_z = (x, y)$ hanno ordine finito se e solo se $Nz \in L$, ossia se e solo se z è una combinazione lineare razionale di ω_1 e ω_2.
Nel seguente isomorfismo

$$\begin{aligned} \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z} &\longrightarrow C \\ (a, b) &\mapsto P_{a\omega_1 + b\omega_2} \end{aligned}$$

il sottogruppo di torsione della curva ellittica C è l'immagine di $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$.

Sia $N \in \mathbb{Z}$ fissato e sia $f(x) = ax^3 + bx^2 + cx + d = a(x - e_1)(x - e_2)(x - e_3)$ un polinomio cubico a coefficienti in un campo K, con $char(K) \neq 2$, e con radici distinte, eventualmente in un estensione di K. Dunque vogliamo descrivere le coordinate dei punti di ordine N sulla curva $y^2 = f(x)$. Se $N = 2$, i punti di ordine N sono il punto all'infinito ed i punti $(e_i,0)$ con i = 1,2,3. Definiamo un punto non triviale di ordine N un punto P tale che $NP = 0$ ma $P \neq 0$ e $2P \neq 0$.

Proposizione 4.1.1. *Sia K' un'estensione di K, non necessariamente algebrica e sia $\sigma : K' \longrightarrow \sigma K'$ un isomorfismo di campi che lascia fissi gli elementi di K.*

Sia poi $P = (x_0, x_1, x_2) \in \mathbb{P}^2_{K'}$ un punto di ordine esattamente N (i.e. $NP = 0$ ma $mP \neq 0\ \forall m < N$) sulla curva ellittica di equazione affine $y^2 = f(x)$, dove $f(x) \in K[x]$.
Allora $\sigma P = (\sigma x_0, \sigma x_1, \sigma x_2)$ ha esattamente ordine N.

Dimostrazione. Siccome l'isomorfismo definito lascia fissi i punti di K, σ(0,0,1) = (0,0,1). Inoltre dalla formule di addizione segue che $\sigma P_1 + \sigma P_2 = \sigma(P_1 + P_2)$, per cui $N(\sigma P) = \sigma(NP) = \sigma P_0 = P_0 = (0,0,1)$.
Concludiamo mostrando che se esistesse N' distinto da N e tale per cui $N'(\sigma P) = 0$ allora avremmo che $\sigma(N'P) = \sigma P_0 = P_0$ dunque $N'P = (0,0,1)$. In conclusione dunque σP ha esattamente ordine N. □

Proposizione 4.1.2. *Sia K un sottocampo di $\mathbb{C}$ e sia $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ un automorfismo che lascia fissi gli elementi di K. Denotiamo con $K_N \subset \mathbb{C}$ il campo ottenuto da K aggiungendo le coordinate x_1, x_2 di tutti i punti di ordine N; mentre indichiamo con K_N^+ il campo K a cui aggiungiamo solo le coordinate x_1 di tali punti.*
Allora sia K_N che K_N^+ sono estensioni di Galois finite di K.

Dimostrazione. Le stensioni K_N e K_N^+ sono ottenute da K aggiungendo un insieme finito di numeri complessi, ciò è esattamente la definizione di estensione finita, permutati da un automorfismo di $\mathbb{C}$ che fissa K. Ne segue che l'estensione è di Galois, perché $Gal(\mathbb{C}/K) = Aut_K(\mathbb{C})$. □

Ad esempio, sia $N = 2$, dunque $K_2 = K_2^+$ è il campo di spezzamento di $f(x)$ su K. Come abbiamo detto il gruppo dei punti di ordine N in una curva ellittica in $\mathbb{P}^2_{\mathbb{C}}$ è isomorfo a $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Siccome ogni $\sigma \in Gal(K_N/K)$ rispetta la legge di addizione vista al capitolo precedente abbiamo che ogni σ fornisce un automorfismo da $(\mathbb{Z}/N\mathbb{Z})^2$ in sé.

Sia R un anello commutativo e sia $GL_n(R)$ il gruppo delle matrici $n \times n$ invertibili ad entrate in R. Dalla definizione di invertibilità di una matrice A sappiamo che $det(A) \in R^*$, dove R^* è il gruppo moltiplicativo degli elementi invertibili dell'anello.
Nel caso dei punti di ordine N su una curva ellittica, vi è un isomorfismo tra $Gal(K_N/K)$ e un sottogruppo del gruppo delle funzioni lineari invertibili, $(\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$. Per cui ad ogni $\sigma \in Gal(K_N/K)$ corrisponde una matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z})$. Le entrate della matrice saranno individuate da:

$$\sigma P_{\omega_1/N} = P_{a\omega_1/N + c\omega_2/N}, \qquad \sigma P_{\omega_2/N} = P_{b\omega_1/N + d\omega_2/N}$$

Tornando alla situazione in cui $f(x) = y^2 = 4x^3 - g_2x - g_3$ è la curva ellittica nella forma di Weierstrass in $K \subset \mathbb{C}$, con $K = \mathbb{Q}(g_2, g_3)$, vorremmo utilizzare la funzione $\wp$ per determinare un polinomio le cui radici siano le coordinate x di punti di ordine N. K_N^+ sarà il campo di spezzamento di un tale polinomio.

Costruiamo una funzione ellittica $f_N(z)$ i cui zeri siano esattamente i valori non nulli di z tali per cui P_z è un punto di ordine N. Per far ciò seguiamo il procedimento utilizzato nella dimostrazione della Proposizione 2.3.1. Se $u \in \mathbb{C}/L$ è un punto di ordine N, allora anche il suo simmetrico u^* all'interno del parallelogramma fondamentale Π avrà ordine N. Consideriamo due casi:

1. Sia N dispari e allora u e u^*, sono sempre distinti modulo L, ossia $u \neq \omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2$ se u ha ordine N. Definiamo

$$f_N(z) = N \prod_{\substack{u\in\mathbb{C}/L \\ Nu\in L}} (\wp(z) - \wp(u)),$$

dove un solo u è preso dalla coppia u, u^* e $u \neq 0$. Allora $f_N(z) = F_N(\wp(z))$, dove $F_N(x) \in \mathbb{C}[x]$ è un polinomio di grado $(N^2-1)/2$. La funzione ellittica $f_N(z)$ ha N^2-1 zeri ed un singolo polo in 0 di ordine N^2-1. Ne concludiamo che il termine dominante nell'espansione con $z=0$ è N/z^{N^2-1}.

In tal caso la funzione $f_N(z)$ gode della proprietà

$$f_N(z)^2 = N^2 \prod_{\substack{0\neq u\in\mathbb{C}/L \\ Nu\in L}} (\wp(z) - \wp(u))$$

2. Sia N pari e consideriamo $u \in \mathbb{C}/L$ tale che $Nu \in L$ e u non sia di ordine 2, cioè $u \neq 0, \omega_1/2, \omega_2, (\omega_1+\omega_2)/2$. Definiamo $\tilde{f}_N(z)$ come in precedenza

$$\tilde{f}_N(z) = N \prod_{\substack{u\in\mathbb{C}/L \\ Nu\in L}} (\wp(z) - \wp(u)).$$

Quindi $\tilde{f}_N(z) = F_N(\wp(z))$, ove $F_N(x) \in \mathbb{C}[x]$ è un polinomio di grado $(N^2-4)/2$. Allora la curva ellittica pari $\tilde{f}_N(z)$ ha N^2-4 zeri semplici e un polo singolo di ordine N^2-4 in 0. Da ciò segue che il termine dominante dell'espansione in $z=0$ è N/z^{N^2-4}.

Consideriamo la funzione $f_N(z) := \frac{1}{2}\wp'(z)\tilde{f}_N(z)$, allora vale che

$$\begin{aligned} f_N(z)^2 &= \frac{1}{4}\wp'(z)\tilde{f}_N(z) = \\ &= N^2(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3) \prod_{\substack{u\in\mathbb{C}/L \\ Nu\in L \\ 2u\notin L}} (\wp(z) - \wp(u)) = \\ &= N^2 \prod_{\substack{u\in\mathbb{C}/L \\ Nu\in L}} (\wp(z) - \wp(u)). \end{aligned}$$

Notiamo che un punto $(x,y) = (\wp(z), \wp'(z))$ ha ordine N pari se e solo se $F_N(x) = 0$; in particolare un punto ha ordine N se $y=0$, in questo caso è un ponto di ordine due, oppure se $F_N(x) = 0$.

Dalle Proposizioni 4.1.1 e 4.1.2 segue che ogni automorfismo di $\mathbb{C}$ che tiene fisso $K = \mathbb{Q}(g_2, g_3)$ permuta le radici di $F_N(x)$, infatti tali automorfismi appartengono a $Gal(\mathbb{C}/K)$; dunque i coefficienti di $F_N(x)$ sono in $K = \mathbb{Q}(g_2, g_3)$.

Consideriamo una curva ellittica nella sua forma generica, $y^2 = f(x) = ax^3 + bx^2 + cx + d$, ed evitando di usare la funzione $\wp(z)$ possiamo utilizzare le formule (3.7) e (3.8) per trovare una funzione razionale in x ed y che è l'ascissa di NP, dove $P = (x, y)$. Semplificando le espressioni trovate e utilizzando l'uguaglianza $y^2 = f(x)$ troveremo un denominatore che si annulla se e solo se NP è il punto all'infinito, ossia se e solo se P ha ordine N. Dunque vorremmo trovare tale espressione per il denominatore; in particolare, se N è dispari il denominatore sarà un'espressione in $K[x, y]$, dove $K = \mathbb{Q}(a, b, c, d)$, che si annulla se e solo se x è uno degli $(N^2 - 1)/2$ valori delle coordinate x di punti non triviali di ordine N. Per cui l'espressione deve essere polinomiale solamente in x, con $(N^2 - 1)/2$ radici. Allo stesso modo, se N è pari, il denominatore ha la forma seguente

$$y \cdot (\text{polinomio esclusivamente in x})$$

dove il polinomio deve avere coefficienti in $K[x, y]$ ed il polinomio in x deve avere $(N^2 - 4)/2$ radici.

Osservazione 3. Il procedimento appena illustrato si può applicare ad una generica curva ellittica $y^2 = f(x)$ su un campo K di caratteristica diversa da 2 e non solamente a sottocampi di $\mathbb{C}$; tuttavia non è detto che i punti non banali di ordine N siano esattamente $N^2 - 1$. Infatti potremmo avere un campo non algebricamente chiuso, per tanto le coordinate x di punti di ordine N potrebbero trovarsi in un'estensione di K.

Inoltre, se K ha caratteristica finita $p \neq 2$, potrebbero esserci un numero inferiore di punti di ordine N, in quanto il polinomio che appare a denominatore potrebbe avere come coefficiente dominante un multiplo di p, nonostante il campo fosse algebricamente chiuso.

La discussione appena effettuata dimostra anche la seguente proposizione.

Proposizione 4.1.3. *Sia $y^2 = f(x)$ una curva ellittica in un campo K di caratteristica distinta da 2. Allora vi sono al più N^2 punti, eventualmente triviali, di ordine N in un'estensione K' di K.*

Studiamo ora le applicazioni della Proposizione 4.1.3 ad un campo finito. Il campo $\mathbb{P}^2_{\mathbb{F}_q}$ ha $q^2 + q + 1$ punti, dunque anche la curva ellittica C di equazione $y^2 = f(x) \in \mathbb{F}_q[x]$ sarà composta da un numero finito di punti; ne segue che il gruppo $(C, +)$ è un gruppo abeliano finito.

Proposizione 4.1.4. *Sia $q = p^f$ con $p \nmid 2n$. Supponiamo che $q \equiv 3 \pmod 4$. Allora vi sono $q + 1$ $\mathbb{F}_q$-punti appartenenti alla curva ellittica $y^2 = x^3 - n^2 x$.*

Dimostrazione. Iniziamo osservando che vi sono quattro punti di ordine 2: il punto all'infinito (0,0,1), (1,0,0) e $(1, \pm n, 0)$.
Vorremmo ora contare le coppie del tipo (x, y), con $x \neq 0, n, -n$. Ordiniamo i $q-3$ valori di x cercati in coppie del tipo $\{x, -x\}$. Siccome $f(x) = x^3 - n^2x$ è una funzione dispari e siccome -1 non è un quadrato in $\mathbb{F}_q$, infatti abbiamo supposto che $q \equiv_4 3$, segue che uno tra $f(x)$ ed $f(-x) = -f(x)$ è un quadrato in $\mathbb{F}_q$. A seconda di quale tra x e $-x$ sia un quadrato, otteniamo esattamente due punti; nel primo caso saranno $(x, \pm\sqrt{f(x)})$, mentre nel secondo $(-x, \pm\sqrt{f(-x)})$. Concludiamo che $(q-3)/2$ coppie forniscono $q-3$ punti che, sommati assieme ai quattro di ordine due precedentemente individuati, si hanno $q+1$ punti in totale in $\mathbb{F}_q$. □

4.2 Punti su un campo finito

Finora abbiamo trattato curve ellittiche $E \in \mathcal{E}_L$ principalmente in $\mathbb{Q}$ o $\mathbb{C}$; nella presente sezione siamo interessati allo studio della curva $y^2 = x^3 - n^2x$, che denoteremo con E_n, su campi K finiti la cui caratteristica $p \nmid 2n$.

L'equazione $y^2 = x^3 - \bar{n}^2x$ rappresenta una curva ellittica in K, dove $\bar{n} \equiv n \pmod{p}$. Denotiamo con $E_n(K)$ l'insieme dei punti sulla curva con coordinate in K. Per tanto, dalla Proposizione 4.1.4, se $q \equiv 3 \pmod 4$, allora $\#E_n(\mathbb{F}_q) = q + 1$.

Definizione 4.2.1. La curva ellittica E_n definita su $\mathbb{F}_p$ è detta *riduzione modulo p.*

Definizione 4.2.2. Diremo che una curva ellittica E_n ha una *buona riduzione* se p non divide $2n$.

Il gruppo $E(\mathbb{C})$ composto dai punti complessi sulla curva ellittica è isomorfo a $\mathbb{C}/L$, che è isomorfo a $\mathbb{R}/\mathbb{Z}\times\mathbb{R}/\mathbb{Z}$. Dunque il sottogruppo di torsione è $\mathbb{Q}/\mathbb{Z}\times\mathbb{Q}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ e in $\mathbb{C}/L$ ciò coincide con tutte le combinazioni lineari razionali di ω_1 ed ω_2.

Ricordiamo il seguente teorema, di cui non daremo la dimostrazione.

Teorema 4.2.3 (di Mordell-Weil). *Sia E una curva ellittica su $\mathbb{Q}$. Allora $E(\mathbb{Q})$ è un gruppo abeliano finitamente generato.*

Segue dal teorema che il sottogruppo di torsione $E(\mathbb{Q})_{tors}$ è finito e che $E(\mathbb{Q})$ è isomorfo alla somma diretta di un numero finito di $\mathbb{Z}$, $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \bigoplus \mathbb{Z}^r$. Chiamiamo *rango di $E(\mathbb{Q})$* l'intero non negativo r. Notiamo che $r > 0$ se e solo se $E(\mathbb{Q})$ ha infiniti punti.

Proposizione 4.2.4. *Gli unici punti razionali di ordine finito in E_n sono i quattro punti di ordine 2: $P_0 = (0,0,1), (1,0,0), (1, \pm n, 0)$.*

Ossia $\#E_n(\mathbb{Q}_{tors}) = 4$.

L'idea della dimostrazione consiste nella costruzione di un omomorfismo tra $E_n(\mathbb{Q})_{tors}$ e $E_n(\mathbb{F}_p)$ che sia iniettivo per quasi tutti i primi p. Siccome $\#E(\mathbb{F}_p)$ è equivalente ad un intero nella forma $p+1$ con $p \equiv 3 \pmod 4$, per quanto visto alla Proposizione 4.1.4. Dunque l'unica possibilità è che $\#E_n(\mathbb{Q}_{tors}) = 4$.

Per far ciò abbiamo però bisogno di un lemma preliminare.

Lemma 4.2.5. *Siano $P_1 = (x_0, x_1, x_2)$ e $P_2 = (y_0, y_1, y_2)$, dove le coordinate di uno stesso punto sono tra loro coprime, e consideriamo l'applicazione che riduce i punti modulo un primo p. Allora $\overline{P_1} = \overline{P_2}$ se e solo se ogni entrata del loro prodotto vettoriale (considerando i punti come vettori di $\mathbb{R}^3$) è multipla di p, ossia se e solo se $x_1y_2 - y_1x_2$, $y_0x_2 - x_0y_2$ e $x_0y_1 - y_0x_1$ sono divisibili per p.*

Dimostrazione. Supponiamo che p divida il prodotto vettoriale. Si verificano due casi:

- p divide x_0. Allora p divide y_0x_2 e y_0x_1, per tanto divide y_0, infatti non può dividere sia x_1 che x_2. Supponiamo $p \nmid x_1$, allora $\overline{P_2} = (0, \bar{y_1}, \bar{y_2}) = (0, \bar{x_1}\bar{y_1}, \bar{x_1}\bar{y_2}) = (0, \bar{x_1}\bar{y_1}, \bar{y_1}\bar{x_2}) = (0, \bar{x_1}, \bar{x_2}) = \overline{P_1}$.
- p non divide x_0. Allora
  $\overline{P_2} = (\bar{y_0}, \bar{y_1}, \bar{y_2}) = (\bar{x_0}\bar{y_0}, \bar{x_0}\bar{y_1}, \bar{x_0}\bar{y_2}) = (\bar{x_0}\bar{y_0}, \bar{y_0}\bar{x_1}, \bar{y_0}\bar{x_2}) = (\bar{x_0}, \bar{x_1}, \bar{x_2}) = \overline{P_1}$.

Supponiamo che $\overline{P_1} = \overline{P_2}$. Senza perdere di generalità sia $p \nmid x_0$, ma argomenti analoghi si applicano per $p \nmid x_1$ e $p \nmid x_2$. Allora, siccome $\overline{P_1} = \overline{P_2} = (\bar{y_0}, \bar{y_1}, \bar{y_2})$, varrà anche che $p \nmid y_0$ e otteniamo $(\bar{x_0}\bar{y_0}, \bar{x_0}\bar{y_1}, \bar{x_0}\bar{y_2}) = \overline{P_1} = \overline{P_2} = (\bar{x_0}\bar{y_0}, \bar{x_1}\bar{y_0}, \bar{x_2}\bar{y_0})$. Siccome la prima coordinata dei punti uguagliati è equivalente, i due punti possono coincidere solamente se anche la seconda e la terza sono uguali, quindi $p|(x_0y_1 - x_1y_0)$ e $p|(x_0y_2 - x_2y_0)$.

Manca ora da dimostrare la divisibilità di $x_1y_2 - y_1x_2$. Nel caso in cui p divida sia x_1 che x_2 concludiamo banalmente. Altrimenti la conclusione segue dalla ripetizione degli argomenti utilizzati sopra, sostituendo x_0, y_0 con x_1, y_1 o x_2, y_2. □

Possiamo ora procedere alla dimostrazione della Proposizione 4.2.4.

Dimostrazione. Definiamo una mappa da $\mathbb{P}^2_{\mathbb{Q}}$ in $\mathbb{P}^2_{\mathbb{F}_p}$. Per ogni primo fissato p, definiamo $\overline{P} = (\overline{x_0}, \overline{x_1}, \overline{x_2}) \in \mathbb{P}^2_{\mathbb{F}_p}$ come l'immagine di $P = (x_0, x_1, x_2) \in \mathbb{P}^2_{\mathbb{Q}}$, tale per cui x_0, x_1, x_2 siano coprimi tra loro e dove la barretta indichi la riduzione modulo p. Per tale ragione $\overline{P} \neq (0,0,0)$, inoltre notiamo che otteniamo un punto equivalente, moltiplicando tutte le entrate (x_0, x_1, x_2) per un intero coprimo con p.

Allora se $P \in \mathbb{P}^2_{\mathbb{Q}}$ e $P \in E_n(\mathbb{Q})$, si ha che $\overline{P} \in E_n(\mathbb{F}_p)$. Inoltre l'immagine di $P_1 + P_2$ sarà $\overline{P_1} + \overline{P_2}$, in quanto non vi è distinzione nell'ordine in cui si sommano due punti con le formule di addizione e si riducono modulo p. Concludiamo che la funzione creata è un omomorfismo da $E_n(\mathbb{Q})$ in $E_n(\mathbb{F}_p)$, per ogni $p \nmid 2n$.

Procediamo per assurdo supponendo che vi siano punti in $E_n(\mathbb{Q})$ di ordine superiore a 2, dunque di ordine dispari o multiplo di 4. In tal caso avremmo un sottogruppo $S = \{P_1, P_2, \ldots, P_m\} \subset E_n(\mathbb{Q})$, con $m = \#S$ uguale ad 8 oppure ad un numero dispari.

Come illustrato in precedenza, indichiamo un generico punto con $P_i = (x_i, y_i, z_i)$ $\forall i = 1, \ldots, m$. Essendo $P_i \neq P_j$ $\forall i \neq j$ in $\mathbb{P}^2_{\mathbb{Q}}$, il prodotto vettoriale $(y_i z_j - y_j z_i, x_j z_i - x_i z_j, x_i y_j - x_j y_i) \in \mathbb{R}^3$ sarà non nullo. Sia n_{ij} il massimo comune divisore delle entrate del prodotto vettoriale. Dal Lemma 4.2.5, $\overline{P_i} = \overline{P_j} \in E_n(\mathbb{F}_p)$ se e solo se $p|n_{ij}$, tuttavia se p è un primo di buona riduzione per definizione non deve dividere $2n$ ne segue che, per essere certi che l'immagine di due punti distinti e non allineati sia non coincidente basta richiedere che $p > n_{ij}$ $\forall i, j$. La riduzione modulo p è una mappa iniettiva da S in $E_n(\mathbb{F}_p)$.

Da ciò segue che per tutti i primi p, ad eccezione di un numero finito di essi, il numero m deve dividere $\#E_n(\mathbb{F}_p)$ perché l'immagine di S è un sottogruppo di ordine m. Allora per quasi tutti i primi p tali che $p \equiv 3 \pmod 4$, essendo $\#E_n(\mathbb{F}_p) = p+1$, varrà che $p \equiv -1 \pmod m$, per la Proposizione 4.1.4. Ciò è però in contraddizione con il Teorema di Dirichlet, infatti se $m = 8$ staremmo affermando che vi sono solamente finiti numeri primi della forma $8k + 3$, mentre se m fosse dispari ciò implicherebbe che dovrebbero essere finiti i numeri primi del tipo $4mk + 3$ se $3 \nmid m$ o $12mk + 7$ se $3|m$. In tutti questi casi il teorema di Dirichlet viene contraddetto per cui si troverebbe un assurdo e non si potrebbero avere sottogruppi di ordini diversi da 4. □

Problema 4.2.6. Proviamo che, se P è un punto di ordine diverso da 2 con coordinate razionali sulla curva $y^2 = x^3 - n^2 x$, allora la coordinata x di $2P$ è il quadrato di un numero razionale con denominatore pari.

Iniziamo ricordando le nozioni viste in conclusione alla Sezione 3.2, presi due punti $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$, la loro somma, $P_1 + P_2 = P_3 = (x_3, y_3)$ avrà coordinate:

$$\begin{aligned} x_3 &= -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}m^2 \\ y_3 &= -y_1 + m(x_1 - x_3) \end{aligned}$$

dove $m = (y_2 - y_1)/(x_2 - x_1)$ se $P_1 \neq P_2$, mentre $m = f'(x_1)/2y_2$ se $P_1 = P_2$.

Dunque, nel problema in questione,

$$y^2 = f(x) = x^3 - n^2 x \quad \Rightarrow \quad f'(x) = 3x^2 - n^2$$

e supponendo $P_1 = P_2$ non di ordine 2 si avrà $y_1 = y_2 \neq 0$. Sostituendo questo

risultato nelle formule precedenti troviamo che:

$$\begin{aligned} x_3 = -2x_1 + \left(\frac{f'(x_1)}{2y_1}\right)^2 &= -2x_1 + \left(\frac{3x^2 - n^2}{2y_1}\right)^2 = \\ &= \frac{-8x_1y_1^2 + (3x_1^2 - n^2)^2}{(2y_1)^2} = \\ &= \frac{-8x_1(x_1^3 - n^2x_1) + 9x_1^4 - 6x_1^2n^2 + n^4}{(2y_1)^2} = \\ &= \frac{x_1^4 + 2x_1^2n^2 + n^4}{(2y_1)^2} = \\ &= \left(\frac{x_1^2 + n^2}{2y_1}\right)^2. \end{aligned}$$

Possiamo così concludere il problema; infatti, essendo originariamente x_1 ed y_1 razionali ed essendo n intero e privo di quadrati, ne ricaviamo che anche $\frac{x_1^2+n^2}{2y_1} \in \mathbb{Q}$ e quindi x_3 sarà il quadrato di un razionale.

4.3 Conclusione: problema sui numeri congruenti

Nella sezione precedente abbiamo osservato che non vi sono punti razionali non ovvi che abbiano ordine finito.

Concludiamo la tesi osservando l'equivalenza tra lo studio dell'esistenza di punti di ordine infinito in $E_n(\mathbb{Q})$ e se n sia o meno un numero congruente.

Proposizione 4.3.1. *n è un numero congruente se e solo se $E_n(\mathbb{Q})$ ha rango $r \neq 0$.*

Dimostrazione. Supponiamo che n sia un numero congruente. Nella Sezione 1.2 abbiamo visto che esiste un triangolo rettangolo di lati razionali e area n tale da fornire un punto in E_n la cui coordinata x sia in $(\mathbb{Q}^+)^2$. Siccome la coordinata x dei tre punti di ordine 2 non banali sono note essere $0, \pm n$, vi deve essere un punto di ordine non 2. Dalla Proposizione 4.2.4 ne ricaviamo che tale punto ha ordine infinito, ossia $r \geq 1$.

Supponiamo ora che P sia un punto di ordine infinito. Dal Problema 4.2.6 segue che la coordinata x del punto $2P$ è il quadrato di un numero razionale il cui denominatore è pari. Dalla Proposizione 1.2.1, il punto $2P$ corrisponde ad un triangolo rettangolo di lati razionali ed area n, come indicato della corrispondenza presentata alla Proposizione 1.1.2. □

Notiamo che, dalla Proposizione 4.1.4, utilizzata nella dimostrazione precedente, segue che gli unici punti non triviali nella forma $2P$ sono quelli di ordine infinito. Sia $2E_n(\mathbb{Q})$ il sottogruppo composto dal doppio dei punti razionali di $E_n(\mathbb{Q})$. Dunque

$2E_n(\mathbb{Q})$ è un gruppo abeliano privo di sottogruppi di torsione, per tanto deve essere isomorfo ad un certo numero di copie di $\mathbb{Z}$, supponiamo siano r. Allora $2E_n(\mathbb{Q}) \setminus \{(0,0,1)\}$ è vuoto se e solo se $r = 0$.

È noto che punti in $2E_n(\mathbb{Q}) \setminus \{(0,0,1)\}$ compongono triangoli rettangoli con lati razionali ed area n, secondo la corrispondenza alla Proposizione 1.1.2. Ci chiediamo dunque se tutti i punti corrispondenti a triangoli rettangoli, come da Proposizione 1.2.1, siano in $2E_n(\mathbb{Q}) \setminus \{(0,0,1)\}$.

Proposizione 4.3.2. *Esiste un corrispondenza biiettiva tra triangoli rettangoli di lati razionali $X < Y < Z$ ed area n, e coppie di punti $(1, x, \pm y) \in 2E_n(\mathbb{Q}) \setminus \{(0,0,1)\}$.*
Tale corrispondenza è:

$$(1, x, \pm y) \mapsto \sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x}$$
$$(X, Y, Z) \mapsto \left(\frac{Z^2}{4}, \pm \frac{(Y^2 - X^2)Z}{8} \right)$$

Tale proposizione segue direttamente dalla successiva.

Proposizione 4.3.3. *Sia E la curva ellittica $y^2 = (x - e_1)(x - e_2)(x - e_3)$, con $e_1, e_2, e_3 \in \mathbb{Q}$. Sia poi $P = (x_0, y_0) \in E(\mathbb{Q}) \setminus \{(0,0,1)\}$.*
Allora $P \in 2E_n(\mathbb{Q}) \setminus \{(0,0,1)\}$ se e solo se $x_0 - e_1, x_0 - e_2, x_0 - e_3$ sono tutti quadrati di numeri razionali.

Dimostrazione. Senza perdita di generalità, assumiamo che $x_0 = 0$, infatti se così non fosse potremmo usare il cambio di variabili $x' = x - x_0$. Dunque, denotando $e'_i = e_i - x_0$, otteniamo che $P' = (0, y_0) \in E'$ di equazione $y^2 = (x - e'_1)(x - e'_2)(x - e'_3)$ appartiene a $2E'(\mathbb{Q}) \setminus \{(0,0,1)\}$ se e solo se P era in $2E(\mathbb{Q}) \setminus \{(0,0,1)\}$. Dunque $x_0 - e_i$ sono tutti quadrati se e solo se lo sono $(0 - e'_i)$, quindi basta provare la proposizione per $x_0 = 0$.

Se esiste $Q \in E(\mathbb{Q})$ tale che $2Q = P$, allora vi sono esattamente quattro punti $Q, Q_1, Q_2, Q_3 \in E(\mathbb{Q})$ tali che $2Q_i = P$, dove per ottenere i Q_i abbiamo semplicemente sommato i punti di ordine 2, $(e_i, 0) \in E(\mathbb{Q})$, a Q.
Consideriamo un generico $Q = (x, y)$ tale che $2Q = P = (0, y_0)$, vorremmo trovare delle condizioni affinché le coordinate di Q siano razionali. Sappiamo che un punto Q su una curva ellittica soddisfa $2Q = P$ se e solo se la retta tangente alla curva in Q passa per $-P = (0, -y_0)$. I quattro punti Q si ottengono da $-P$ come intersezioni tra le rette passanti per tale punto e tangenti alla curva ellittica.

Le coordinate (x, y) sono razionali se lo è il coefficiente angolare della retta da $-P$ in Q.
L'implicazione ($\Rightarrow$) è banale, infatti se le coordinate di Q sono razionali, lo sarà anche il coefficiente angolare m.

Mostriamo invece che, se la retta ha equazione $y = mx + q$ ed m è razionale, allora (x, y) sono razionali. La coordinata x di Q sarà lo zero doppio dell'equazione

$(mx-y_0)^2 = (x-e_1)(x-e_2)(x-e_3)$ e quindi $x = (e_1+e_2+e_3+m^2)/2$; dunque x sarà razionale. In questo caso poi, anche la coordinata $y = mx - y_0$ di Q è razionale, basta allora vedere quando rette distinte passanti per $-P$ e tangenti alla curva ellittica E hanno coefficiente angolare razionale.

Un numero $m \in \mathbb{C}$ è il coefficiente angolare di una retta passante per P e tangente ad E se e solo se la seguente equazione ha uno zero doppio:

$$(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c$$

con

$$a = -e_1 - e_2 - e_3, \qquad b = e_1e_2 + e_1e_3 + e_2e_3, \qquad c = -e_1e_2e_3 = y_0^2$$

In particolare l'ultima uguaglianza, $c = y_0^2$ deriva dal fatto che $(0, y_0)$ si trova sulla curva $y^2 = x^3 + ax^2 + bx + c$. L'equazione precedente diventa:

$$\begin{aligned} &m^2x^2 + y_0^2 - 2mxy_0 = x^3 + ax^2 + bx + c \\ &x^3 - (m^2 - a)x^2 + (2my_0 + b)x - (y_0^2 - c) = 0 \\ &x^2 + (a - m^2)x + (b + 2my_0) = 0 \end{aligned}$$

Ciò equivale a chiedere che il discriminante si annulli, ossia:

$$(a - m^2)^2 - 4(b + 2my_0) = 0.$$

Cerchiamo una condizione in termini di e_i per determinare la razionalità o meno di m. Notiamo dalla definizione di a e b che essi sono polinomi in e_i, simmetrici rispetto ad essi. A differenza però, y_0 è simmetrico rispetto a $\sqrt{e_i}$, per tanto introduciamo la funzione f_i, tale che $f_i^2 = e_i$. Ci sono allora due possibili scelte per f_i, a meno che $e_i = 0$, tra le possibilità prendiamo f_i tale per cui $y_0 = f_1f_2f_3$. Ciò significa che, se gli e_i sono tutti distinti da 0, sceglieremo il segno di f_1 ed f_2 arbitrariamente, mentre quello di f_3 sarà tale per cui y_0 ed $f_1f_2f_3$ abbiano le stesse radici di $-e_1e_2e_3$. A differenza, per $e_3 = 0$ la scelta dei segni di f_1 ed f_2 è indifferente, ma avremo $f_3 = 0$.
In tutti i casi indicati comunque, vi sono quattro possibili scelte per gli f_i consistenti con la richiesta che $y_0 = f_1f_2f_3$, elenchiamole di seguito:

$$f_1, f_2, f_3; \quad f_1, -f_2, -f_3; \quad -f_1, f_2, -f_3; \quad -f_1, -f_2, f_3$$

dove chiaramente almeno $e_1, e_2 \neq 0$.

Proseguiamo definendo $s_1 := f_1+f_2+f_3$, $s_2 := f_1f_2+f_2f_3+f_1f_3$ ed $s_3 := f_1f_2f_3$. Ricaviamo allora che:

$$\begin{aligned} &a = f_1^2 + f_2^2 + f_3^2 = s_1^2 - 2s_2 \\ &b = f_1^2f_2^2 + f_1^2f_3^2 + f_2^2f_3^2 = s_2^2 - 2s_1s_3 \\ &y_0 = s_3 \end{aligned}$$

Ne segue che possiamo riscrivere la condizione sul discriminante dell'equazione come:

$$\begin{aligned} 0 &= (m^2 - s_1^2 + 2s_2)^2 - 4(s_2^2 - 2s_1s_3 + 2ms_3) = \\ &= (m^2 - s_1^2)^2 + 4s_2(m^2 - s_1^2) - 8s_3(m - s_1). \end{aligned}$$

Dall'ultima uguaglianza notiamo che il discriminante è divisibile per $(m - s_1)$, ossia $m = s_1 = f_1 + f_2 + f_3$ è una radice. Siccome avremmo potuto compiere altre tre scelte differenti sui segni di f_i, queste dovranno corrispondere ad altrettante radici, in tutto dunque otterremo le quattro soluzioni:

$$\begin{aligned} m_1 &= f_1 + f_2 + f_3; & m_2 &= f_1 - f_2 - f_3; \\ m_3 &= -f_1 + f_2 - f_3; & m_4 &= -f_1 - f_2 + f_3. \end{aligned}$$

Siamo interessati a capire quali tra gli m_i sono razionali.
Se tutti gli f_i sono razionali, allora anche gli m_i saranno tutti razionali.
Supponiamo che tutti gli m_i siano razionali, allora $f_1 = (m_1 + m_2)/2$, $f_2 = (m_1 + m_3)/2$ e $f_3 = (m_1 + m_4)/2$ sono razionali.
In conclusione le coordinate (x, y) di Q tale per cui $2Q = P$ sono razionali se e solo se $f_i = \sqrt{e_i}$ sono razionali. □

[2] Terminiamo notando che questa tesi aveva l'obiettivo di evidenziare la connessione tra i numeri congruenti ed una particolare famiglia di curve ellittiche; tuttavia questo non risolve nella sua interezza il problema dei numeri congruenti, in quanto non fornisce un criterio diretto che permetta di determinare se, preso un generico n, esso sia congruente o meno.
A tal proposito, una soluzione sarebbe fornita dal teorema di Tunnell, il quale però fa parzialmente riferimento alla congettura di Birch-Swinnerton-Dyer, che rimane tutt'oggi un problema aperto della matematica.

Definizione 4.3.4. Consideriamo una generica curva ellittica E, avente la forma $y^2 = x^3 + ax + b$, con $a, b \in \mathbb{Q}$. Chiamiamo allora *discriminante della curva* la quantità non nulla:

$$\Delta = -16(4a^3 + 27b^2).$$

Con la simbologia $E(\mathbb{F}_p)$, indichiamo la riduzione modulo p dei coefficienti della curva ellittica E. I punti affini di tale curva saranno in tutto al più $p + 1$, per tanto ha senso denotare l'errore nel seguente modo:

$$a_p := \left| \#E(\mathbb{F}_p) - p - 1 \right|.$$

Definizione 4.3.5. Chiamiamo *L-serie* di una curva ellittica E in un numero complesso z la serie

$$L(E, z) := \prod_{p \nmid \Delta} (1 - a_p p^{-z} + p^{1-2z})^{-1} \cdot \prod_{p \mid \Delta} (1 - a_p p^{-z})^{-1}.$$

Discende da un teorema di Weil che la L-serie converge qualora la parte reale di z sia maggiore di $\frac{3}{2}$.

Definizione 4.3.6. Sia E una curva ellittica. Allora con il termine *rango analitico* di una curva ellittica E facciamo riferimento all'ordine in cui si annulla la $L-$serie in $z = 1$, ossia:

$$r_{an}(E) = ord_{z=1}L(E, z).$$

Abbiamo ora gli strumenti per introdurre la Congettura di Birch-Swinnerton-Dyer ed enunciare successivamente il Teorema di Tunnell.

Teorema 4.3.7 (**Congettura di Birch-Swinnerton-Dyer**)**.** *Sia E una curva ellittica su $\mathbb{Q}$. Allora il rango analitico ed il rango algebrico di tale curva coincidono:*

$$r(E) = r_{an}(E).$$

Teorema 4.3.8 (**di Tunnell**)**.** *Sia n un numero naturale, dispari e privo di quadrati. Consideriamo le condizioni:*

1. *n è un numero congruente,*
2. *il numero di terne (x, y, z) che soddisfano l'equazione $2x^2 + y^2 8z^2 = n$ è il doppio del numero di terne che soddisfano $2x^2 + y^2 + 32z^2 = n$.*

Allora 1 *implica* 2*.*
Inoltre, se vale la congettura di Birch-Swinnerton-Dyer, anche 2 *implicherà* 1*.*

Bibliografia

[1] Godfrei Harold Hardy e Edward Maitland Wright. *Introduction to Elliptic Curves and Modular Forms*. fourth edition. Springer-Verlag New York Inc, 1960, p. 438.

[2] Brent Johnson. «An Introduction to the Birch and Swinnerton-Dyer Conjecture». In: *Rose-Hulman Undergraduate Mathematics Jurnal* 16 (2015), p. 280. URL: https://scholar.rose-hulman.edu/cgi/viewcontent.cgi?article=1028&context=rhumj.

[3] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. A cura di Hamilton P.R., Gehring F.W. e Moore C.C. first edition. Springer-Verlag New York Inc., 1984, p. 248.

[4] Francescopaolo Montefalcone. *Dispense del Corso: "Metodi Matematici"*. 2021, p. 258.

[5] Jamie Snape. «Application of Elliptic Functions in Classical and Algebraic Geometry». In: *Collingwood College, University of Durham* (), p. 110. URL: https://www.jamiesnape.io/assets/publications/mmath/dissertation.pdf.