UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea Triennale
in Matematica

Il teorema di Nagell-Lutz

The Nagell-Lutz theorem

Relatore
Prof. Giorgio Ottaviani

Candidato
Antonio Sassone

Anno Accademico 2023/2024

Indice

Introduzione

L'obiettivo della tesi è presentare una dimostrazione del teorema di Nagell-Lutz, che dà una condizione necessaria forte per i punti razionali di ordine finito di una curva ellittica con forma di Weierstrass a coefficienti interi, e che fornisce quindi uno strumento molto potente per il calcolo di punti razionali di ordine finito di qualunque curva ellittica a coefficienti razionali, facendo degli opportuni cambi di coordinate. A tale scopo, saranno definite le curve ellittiche e la struttura di gruppo associata a esse. Successivamente si introdurranno delle nozioni di analisi complessa per motivare l'introduzione della forma canonica di Weierstrass. Dopo una breve trattazione sui punti di ordine finito a coordinate complesse, andremo a considerare il sottogruppo dei punti razionali di una curva ellittica, e procederemo con la dimostrazione del teorema, suddividendola in due parti. Infine, mostreremo tramite qualche esempio delle applicazioni del risultato ottenuto.

1 Curve ellittiche e la loro struttura di gruppo

Definizione 1.1 (Curva ellittica)**.** *Si dice* ***curva ellittica*** *una cubica piana proiettiva C non singolare.*

Nel seguito, studieremo anche le parti affini di curve ellittiche, che quindi denomineremo nello stesso modo. Per procedere inizialmente nel modo più generale possibile, per ora le tratteremo nel piano proiettivo $\mathbb{P}^2$. Ricordiamo che una curva piana è non singolare se essa non ammette punti singolari, ovvero punti che annullano tutte le derivate parziali dell'equazione che definisce la curva. Ciò assicura che è possibile definire in maniera univoca la retta tangente a ogni punto della curva.

La peculiarità delle curve ellittiche sta nel fatto che è possibile definire, scelto un punto qualunque come elemento neutro, un'operazione di somma tra punti della curva rispetto alla quale questi formano un gruppo abeliano. Andiamo a vedere come:

Definizione 1.2. *Data una curva proiettiva non singolare C, e P, $Q \in C$, diremo retta per P e Q in $\mathbb{P}^2$:*

i) se $P \neq Q$, la retta passante per P e Q;

ii) se $P = Q$, la retta tangente la curva C in P.

Sia quindi O il punto della curva ellittica C scelto come elemento neutro, e siano P e Q due punti della curva; si consideri la retta r per P e Q: poiché C è una cubica, r avrà necessariamente 3 intersezioni con C in $\mathbb{P}^2$ (tenendo conto delle molteplicità): sia Q' la terza intersezione oltre a P e a Q (Q' potrebbe anche essere P o Q stessi, nel caso in cui r fosse tangente a uno di questi ultimi); si consideri ora la retta s per Q' e O: si definisce $P + Q$ la terza intersezione tra s e C oltre a Q' e O.

A questo punto, si ha che vale il seguente:

Teorema 1.1. *Data una curva ellittica, sia C l'insieme dei suoi punti in $\mathbb{P}^2$. Scelto $O \in C$, $(C, +, O)$ con $+$ definita come sopra è un gruppo abeliano con elemento neutro O.*

Dimostrazione. [GRT85, Parte V, Sezione 2.7.3] □

Tale struttura di gruppo è trasportabile in modo del tutto analogo ai punti della curva sul piano affine, con l'accortezza di aggiungere dei punti in più, che corrispondono ai punti all'infinito.

Osservazione 1.1. La scelta del punto O non influisce sulla struttura di gruppo della curva, poiché dato un gruppo $(G, \cdot)$ con elemento neutro $e \in G$, si può scegliere un qualunque elemento $g \in G$ e definire l'operazione:

$$a * b := ag^{-1}b, \forall a, b \in G$$

In questo modo, si ha che $(G, *)$ è un gruppo con elemento neutro g isomorfo a $(G, \cdot)$ tramite il morfismo:

$$(G, *) \to (G, \cdot), \quad h \mapsto g^{-1}h$$

Osservazione 1.2. Dalla definizione dell'operazione di somma, si può già percepire che essa è continua: a piccole variazioni dei punti sommati, corrisponderà una piccola variazione della loro somma. Nella sezione successiva, vedremo ciò in maggior dettaglio, in particolare vedremo che il gruppo di una curva ellittica è un gruppo algebrico, ovvero l'operazione di somma è un morfismo algebrico da $C \times C$ in C.

2 Forma canonica di Weierstrass

Finora abbiamo trattato curve ellittiche qualsiasi, senza prestare attenzione alla forma delle cubiche usate per definirle. Esistono varie forme canoniche per esse, ma quella che adopereremo noi nel seguito è la forma di Weierstrass, sorta dallo studio della sua funzione $\wp$ e delle funzioni ellittiche. Procediamo ora con lo studio di tale forma canonica, da cui otterremo delle formule esplicite per la somma e la duplicazione di punti e ulteriori informazioni sul gruppo di una curva ellittica. Per molti dei risultati enunciati non forniremo le dimostrazioni, indicheremo semplicemente delle fonti in cui è possibile individuarle; inoltre è possibile trovare la trattazione dello stesso argomento in maggior dettaglio in [Cam24, Sezioni 1-5].

Iniziamo con l'introdurre strumenti analitici che ci faranno comprendere meglio il gruppo di una curva ellittica:

Definizione 2.1. *Sia Λ un sottogruppo additivo di $\mathbb{C}$ libero di dimensione 2 su $\mathbb{Z}$, e che genera $\mathbb{C}$ su $\mathbb{R}$. Λ si dice reticolo di $\mathbb{C}$.*

Definizione 2.2. *Sia $f : \mathbb{C} \setminus D \longrightarrow \mathbb{C}$, con D sottoinsieme discreto di $\mathbb{C}$, una funzione meromorfa. La funzione f si dice ellittica (rispetto a un reticolo $\Lambda \subseteq \mathbb{C}$) se è Λ-periodica, ovvero se $\forall z \in \mathbb{C}, f(z + \omega) = f(z), \forall \omega \in \Lambda$.*

Osservazione 2.1. Si ha che $\mathbb{C}/\Lambda$ è un gruppo di Lie compatto, e in particolare è un toro complesso.

Osservazione 2.2. Le funzioni ellittiche per definizione passano al quoziente $\mathbb{C}/\Lambda$, quindi si possono vedere anche come funzioni meromorfe sul toro associato al reticolo Λ.

Andiamo ora a definire una funzione ellittica rispetto a un qualunque reticolo, che ci porterà alla forma canonica di Weierstrass e al legame tra curve ellittiche e tori complessi. Le dimostrazioni dei risultati che enunciamo nel seguito di questa sezione si trovano su [Lan87, Capitolo 1, sezione 2].

Definizione 2.3. *Si definisce funzione $\wp$ di Weierstrass:*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

Tale funzione è ben definita ed è possibile provare che sia essa che la sua derivata prima sono funzioni ellittiche. Tramite queste riusciamo a ricavare informazioni essenziali sulle curve ellittiche, poiché si ha che vale il seguente teorema fondamentale (per la dimostrazione vd. [Kir92, Capitolo 5] e [Lan87, Capitolo 1]):

Teorema 2.1.

$$\mathcal{P} : \mathbb{C}/\Lambda \hookrightarrow \mathbb{P}^2, \quad z \mapsto \begin{cases} (1, \wp(z), \wp'(z)) & z \neq 0 \\ (0,1,0) & z = 0 \end{cases}$$

è un embedding olomorfo del toro $\mathbb{C}/\Lambda$ in $\mathbb{P}^2$; in particolare, è un biolomorfismo tra il toro e $V := Im\,\mathcal{P} = V(y^2z - 4x^3 + g_2(\Lambda)xz^2 + g_3(\Lambda)z^3) \subseteq \mathbb{P}^2$, dove il polinomio $y^2 - 4x^3 + g_2(\Lambda)x + g_3(\Lambda) \in \mathbb{C}[x,y]$ è non singolare, in quanto il discriminante di $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ è diverso da zero, ovvero: $g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$, e $g_2(\Lambda)$, $g_3(\Lambda)$ sono costanti associate al reticolo Λ.

Quindi, la mappa $\mathcal{P}$ parametrizza la curva ellittica V in $\mathbb{P}^2$, e tramite essa abbiamo rivelato che V è un toro complesso. Ma tale mappa ci rivela anche un altro fatto essenziale: infatti, si ha che essa è anche un isomorfismo di gruppi da $\mathbb{C}/\Lambda$ al gruppo di V, dove l'elemento neutro scelto è il punto all'infinito. Per avere ciò, basta provare che $\mathcal{P}$ è un morfismo di gruppi: questo può essere fatto sfruttando il teorema di addizione della $\wp$ enunciato e provato in [Lan87, Sezione 1.3]. Altra conseguenza fondamentale di tale teorema è il seguente:

Teorema 2.2. *Le curve ellittiche sono gruppi algebrici.*

Inoltre è possibile provare che per ogni g_2, $g_3 \in \mathbb{C}$ tali che $g_2^3 - 27g_3^2 \neq 0$, esiste un reticolo Λ tale che:

$$g_2 = g_2(\Lambda), \quad g_3 = g_3(\Lambda)$$

Infine col seguente, che dimostreremo seguendo [GRT85, Parte V, sezione 2.7.2], riusciremo a ottenere una caratterizzazione per le curve ellittiche:

Lemma 2.1. *Ogni curva ellittica è biolomorfa attraverso una trasformazione birazionale di $\mathbb{P}^2$ a una curva della forma:*

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

Dimostrazione. Non è difficile provare che ogni curva ellittica ha almeno un punto di flesso: scegliamo il sistema di riferimento di $\mathbb{P}^2$ in modo tale che il punto $(0,1,0)$

sia quindi di flesso per la curva e che la retta $z = 0$ sia la rispettiva tangente di flesso. Allora si ha che l'equazione della cubica è del tipo:

$$Ax^3 + z(\alpha x^2 + \beta xy + \gamma y^2) + z^2(Bx + Cy) + Dz^3 = 0$$

dove $\gamma \neq 0$ poiché altrimenti $(0, 1, 0)$ sarebbe un punto doppio per la curva. Si può quindi supporre, effettuando il cambio di coordinate opportuno, che si abbia $\gamma = 1$. Considero la retta $\beta x + 2y + \frac{C}{2}z = 0$ (componente irriducibile della polare del punto $(0, 1, 0)$ oltre a $z = 0$) ed effettuo il cambio di coordinate:

$$(x, y, z) \mapsto (x, \frac{\beta}{2}x + y + \frac{C}{2}z, z)$$

L'equazione della curva in questo modo diventa: $y^2z = ax^3 + bx^2z + cxz^2 + dz^3$. Ora tramite la trasformazione $x \mapsto x - \frac{b}{3}z$ l'equazione si riduce ulteriormente in: $y^2z = k(x^3 - pxz^2 - qz^3)$. Infine, col cambio $y \mapsto \frac{\sqrt{k}}{2}y$, si ottiene la forma voluta:

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

□

Tutto ciò ci porta al seguente risultato fondamentale:

Teorema 2.3. *Le curve proiettive non singolari di genere 1 sono tutte e sole le curve ellittiche.*

Osservazione 2.3. Tale teorema permette di dare una definizione ben più generale per le curve ellittiche che abbiamo provato essere equivalente a quella data nella sezione precedente: una curva ellittica è una curva proiettiva non singolare di genere 1. Questa è infatti la definizione che si trova maggiormente nella letteratura moderna.

Quindi quanto visto fino a questo momento motiva la seguente:

Definizione 2.4 (Forma canonica di Weierstrass)**.** *Una curva ellittica è in forma di Weierstrass se è data da un'equazione affine della forma:*

$$y^2 = 4x^3 - g_2x - g_3$$

con $g_2, g_3 \in \mathbb{C}$ tali che $g_2^3 - 27g_3^2 \neq 0$.

Per gli scopi di questa tesi, useremo una versione leggermente modificata della forma di Weierstrass, ma analoga e più generale, ovvero la seguente:

$$y^2 = x^3 + ax^2 + bx + c = f(x) \quad a, b, c \in \mathbb{C} \tag{1}$$

Perché questa equazione descriva effettivamente una curva ellittica, dobbiamo verificare per quali $a, b, c \in \mathbb{C}$ la curva descritta da tale equazione è non singolare: ciò è equivalente per com'è fatta l'equazione a richiedere che $f(x)$ abbia discriminante non nullo, quindi si ottiene la relazione:

$$-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$$

Concludiamo la sezione ricavandoci, seguendo [ST15, Sezione 1.4], delle formule esplicite per la somma di punti sul piano affine di curve ellittiche in forma di Weierstrass, che ci serviranno nel seguito.

Osservazione 2.4. Se la curva è in forma di Weierstrass, omogeneizzandola si vede che ha un unico punto all'infinito, ovvero $(0, 1, 0)$, quindi esso è necessariamente un flesso per la curva, con tangente di flesso la retta all'infinito.

Tale osservazione motiva la scelta del punto all'infinito come elemento neutro, che indicheremo con $\mathcal{O}$ quando aggiunto ai punti della curva sul piano affine: con tale scelta, si ottengono dei vantaggi nel calcolare esplicitamente la somma tra punti, in quanto si ha che la retta per il punto all'infinito e un qualunque punto P sul piano affine è la retta verticale per P, la cui terza intersezione con la curva è evidente per la parità della forma di Weierstrass nelle y: è la riflessione di P rispetto all'asse delle x. Da ciò segue intanto che:

$$P = (x, y) \Rightarrow -P = (x, -y) \tag{2}$$

per come si ottengono gli opposti secondo la legge definita nella prima sezione, ricordando che $\mathcal{O}$ è un flesso per la curva. In questo modo quindi, risulta anche più semplice descrivere geometricamente la somma tra punti: siano P e Q punti sulla curva, sia $P * Q$ la terza intersezione con la curva della retta per P e Q: si ottiene che

$$P + Q = -(P * Q)$$

(nel caso $P = Q$, $P * P$ sarà semplicemente la terza intersezione tra la retta tangente la curva in P e la curva). Possiamo a questo punto ottenere con maggiore semplicità le formule cercate:

Proposizione 2.1 (Formule di somma e duplicazione)**.** *Sia C una curva ellittica in forma di Weierstrass, e sia $(C(\mathbb{C}), +)$ il gruppo associato nel piano affine, con $\mathcal{O}$ punto all'infinito elemento neutro. Allora $\forall P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in C(\mathbb{C})\backslash\{\mathcal{O}\}$:*

- *se $P_1 \neq P_2$, $P_1 + P_2 = \mathcal{O} \Leftrightarrow x_1 = x_2$;*
- *se $P_1 \neq P_2$ e $P_1 + P_2 \neq \mathcal{O}$:*

  $$x(P_1 + P_2) = \lambda^2 - a - x_1 - x_2, \quad y(P_1 + P_2) = -(\lambda x(P_1 + P_2) + \nu)$$

  con $\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$;
- *se $P_1 = P_2 := P$ e $2P \neq \mathcal{O}$:*

  $$x(2P) = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c} = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4y_1^2}, \quad y(2P) = -(\lambda x(2P) + \nu)$$

  con $\lambda = \frac{f'(x_1)}{2y_1}$, $\nu = y_1 - \frac{x_1 f'(x_1)}{2y_1}$.

Dimostrazione. Abbiamo già visto in (2) che se P_1 e P_2 sono opposti, hanno medesima ascissa; viceversa, se $x_1 = x_2$, si ha che $y_1^2 = f(x_1) = f(x_2) = y_2^2$, e poiché per ipotesi $y_1 \neq y_2$, segue necessariamente che $y_1 = -y_2$ e quindi la tesi per quanto osservato in (2). Siano ora $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ punti distinti sulla curva,

con $x_1 \neq x_2$, cerchiamo il punto $P_1 * P_2 = (x_3, y_3)$ (da cui per quanto osservato si otterrà $P_1 + P_2 = (x_3, -y_3)$). Sia $r : y = \lambda x + \nu$ la retta per P_1 e P_2, con $\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. x_3 e y_3 dovranno soddisfare:

$$\begin{cases} y = \lambda x + \nu \\ x^3 + ax^2 + bx + c - y^2 = 0 \end{cases}$$

In particolare, x_1, x_2, x_3 sono le radici del polinomio di terzo grado:

$$x^3 + ax^2 + bx + c - (\lambda x + \nu)^2 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2)$$

quindi: $x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$. Da quest'ultima relazione, confrontando i coefficienti di secondo grado, si ottiene:

$$a - \lambda^2 = -x_1 - x_2 - x_3 \Rightarrow x_3 = \lambda^2 - a - x_1 - x_2$$

da cui si ricava anche y_3 dall'equazione di r. Nel caso invece della somma di un punto con sé stesso, supponendo $y_1 \neq 0$ (altrimenti si ha che $2P_1 = \mathcal{O}$, come vedremo nella prossima sezione), si farà la medesima procedura, dove r però è la retta tangente il punto: quindi per trovare $P_1 * P_1$, considero

$$r : (x - x_1)f'(x_1) - 2(y - y_1)y_1 = 0 \Leftrightarrow y = \frac{f'(x_1)}{2y_1}x + y_1 - \frac{x_1 f'(x_1)}{2y_1}$$

Le coordinate di $P_1 * P_1$ le otterremo quindi con le medesime formule del caso dei punti distinti, ponendo però:

$$\lambda = \frac{f'(x_1)}{2y_1}, \quad \nu = y_1 - \frac{x_1 f'(x_1)}{2y_1}$$

Inoltre, poiché $y_1^2 = f(x_1)$, è possibile ottenere un'equazione per l'ascissa di $P_1 * P_1$ unicamente in funzione di x_1, ovvero:

$$\begin{aligned} x(P_1 * P_1) &= \frac{f'(x_1)^2}{4y_1^2} - a - 2x_1 = \frac{f'(x_1)^2}{4f(x_1)} - a - 2x_1 = \frac{(3x_1^2 + 2ax_1 + b)^2}{4(x_1^3 + ax_1^2 + bx_1 + c)} - a - 2x_1 = \\ &= \frac{9x_1^4 + 4a^2x_1^2 + b^2 + 12ax_1^3 + 6bx_1^2 + 4abx_1 - 4a(x_1^3 + ax_1^2 + bx_1 + c) - 8x_1(x_1^3 + ax_1^2 + bx_1 + c)}{4(x_1^3 + ax_1^2 + bx_1 + c)} = \\ &= \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c} \left(= \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4y_1^2}\right) \end{aligned}$$

□

3 Teorema di Nagell-Lutz: Parte I

Per quanto provato nella sezione precedente, in particolare dal fatto che il gruppo di una curva ellittica è algebrico, risulta motivata la seguente:

Definizione 3.1. *Sia C una curva ellittica con forma di Weierstrass a coefficienti su un campo $\mathbb{K} \subseteq \mathbb{C}$, con $\mathcal{O}$ punto all'infinito. Si definisce:*

$$C(\mathbb{K}) = \{(x, y) \in C \mid x, y \in \mathbb{K}\} \cup \{\mathcal{O}\}$$

sottogruppo dei punti $\mathbb{K}$-razionali della curva. Se $\mathbb{K} = \mathbb{Q}$, denomineremo i punti di $C(\mathbb{Q})$ semplicemente punti razionali della curva.

Tali insiemi sono effettivamente sottogruppi del gruppo di tutti i punti della curva poiché quest'ultimo è algebrico, e quindi l'operazione è esprimibile tramite funzioni razionali nelle coordinate dei punti coinvolti (come abbiamo visto d'altronde esplicitamente nella proposizione 2.1).

Il teorema di Nagell-Lutz fornisce delle condizioni necessarie sui punti di ordine finito del sottogruppo $C(\mathbb{Q})$ quando la forma di Weierstrass della curva è a coefficienti interi. Osserviamo che tale richiesta non è restrittiva, poiché data una curva ellittica con forma di Weierstrass come in (1) a coefficienti razionali, posso ricondurmi a una a coefficienti interi tramite il cambio di variabile:

$$X = n^2 x \quad Y = n^3 y, \quad \text{con } n \in \mathbb{Z}$$

Se n è scelto opportunamente, potrò eliminare i denominatori di a, b e c:

$$\frac{Y^2}{n^6} = \frac{X^3}{n^6} + a\frac{X^2}{n^4} + b\frac{X}{n^2} + c \;\Leftrightarrow\; Y^2 = X^3 + an^2X^2 + bn^4X + cn^6$$

Dallo studio fatto sulla struttura di varietà di una curva ellittica, possiamo già conoscere completamente quali e quanti sono i punti di ordine finito di C($\mathbb{C}$):

Teorema 3.1. *Sia C una curva ellittica, allora $C(\mathbb{C})$ ha un unico sottogruppo isomorfo a $C_n \times C_n$, dove con C_n indichiamo un gruppo ciclico di ordine n, $\forall n \in \mathbb{N}$, e ogni punto di ordine finito appartiene a uno di questi.*

Dimostrazione. Abbiamo provato che a ogni curva ellittica corrisponde un toro complesso della forma $\mathbb{C}/\Lambda$, dove Λ è un reticolo opportuno, e che tale corrispondenza è anche un isomorfismo di gruppi. Basta quindi studiare i punti di ordine finito di $\mathbb{C}/\Lambda$. Per quanto riguarda l'esistenza di tali sottogruppi, presi $\omega_1, \omega_2 \in \Lambda$ generatori su $\mathbb{Z}$ di Λ, si ha che è semplice provare che

$$\left\langle \left[\frac{\omega_1}{n}\right], \left[\frac{\omega_2}{n}\right] \right\rangle \simeq C_n \times C_n, \quad \forall n \in \mathbb{N}$$

Sia ora $[z] \in \mathbb{C}/\Lambda$ tale che $nz \equiv 0 \mod \Lambda$, $\exists n \in \mathbb{N}$. Allora si ha che in $\mathbb{C}$ $\exists \alpha, \beta \in \mathbb{Z}$ tali che:

$$nz = \alpha\omega_1 + \beta\omega_2 \quad \Leftrightarrow \quad z = \alpha\frac{\omega_1}{n} + \beta\frac{\omega_2}{n}$$

Quindi si ha $[z] \in \left\langle \left[\frac{\omega_1}{n}\right], \left[\frac{\omega_2}{n}\right] \right\rangle$, da cui si ha che ogni elemento di ordine finito appartiene a un sottogruppo di questa forma. Ciò assicura anche l'unicità di tali sottogruppi. □

Corollario 3.1.1. *I punti tali che $2P = \mathcal{O}$ di una curva ellittica con forma di Weierstrass $y^2 = f(x)$ sono tutti e soli:*

$$\{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\} \simeq C_2 \times C_2$$

dove x_1, x_2, x_3 sono le radici (distinte poiché $discr(f) \neq 0$) di $f(x)$.

Dimostrazione. Se $\forall i = 1, 2, 3$, $P_i = (x_i, 0)$, si ha che $-P_i = (x_i, 0)$ poiché abbiamo visto che l'inverso di ogni punto è dato dalla riflessione di esso rispetto all'asse delle x. Quindi $2P_i = \mathcal{O}$, $\forall i = 1, 2, 3$, da cui la tesi poiché per il teorema precedente vi sono unicamente 4 punti che soddisfano ciò. □

Corollario 3.1.2. *I punti di una curva ellittica tali che 3P=$\mathcal{O}$, scelto un punto di flesso come elemento neutro, sono tutti e soli i suoi punti di flesso.*

Dimostrazione. Se P è un punto di flesso della curva, si ha che $P * P = P$, poiché la terza intersezione della tangente in P con la curva sarà P stesso. Quindi segue $2P = -P$, da cui $3P = \mathcal{O}$. Non ve ne sono altri poiché una curva ellittica, essendo cubica, ha 9 punti di flesso (contando anche il punto all'infinito), e per il teorema precedente gli elementi di ordine 3 formano un gruppo isomorfo a $C_3 \times C_3$, quindi con 9 elementi. □

Viste delle nozioni generali sui punti di ordine finito di una curva ellittica, possiamo andare ora a enunciare il teorema di Nagell-Lutz:

Teorema 3.2 (Nagell-Lutz)**.** *Sia C una curva ellittica con forma di Weierstrass:*

$$y^2 = x^3 + ax^2 + bx + c = f(x)$$

con $a, b, c \in \mathbb{Z}$, e sia $P = (x, y) \in C(\mathbb{Q})$ di ordine finito, $P \neq \mathcal{O}$. Allora si ha che:

I. $x, y \in \mathbb{Z}$;

II. posto $D = discr(f) \in \mathbb{Z}$, y=0 oppure $y^2 \mid D$.

In questa sezione, ci occuperemo di dimostrare la parte I. della tesi, ovvero che un punto razionale di ordine finito sulla curva è necessariamente a coordinate intere; nella prossima sezione, dimostreremo la II.. Gli argomenti che useremo per tali dimostrazioni sono fondamentalmente tratti da [ST15, Sezioni 2.3, 2.4, 2.5].

Osservazione 3.1. Sia $P \in C(\mathbb{Q})$ un punto di ordine 2: abbiamo visto allora che $y(P) = 0$, per cui la sua ascissa $x(P)$ è radice razionale di $f(x)$ polinomio monico a coefficienti interi. Poiché $\mathbb{Z}$ è integralmente chiuso, si ottiene che necessariamente $x(P) \in \mathbb{Z}$, per cui abbiamo provato che vale il teorema di Nagell-Lutz nel caso dei punti di ordine 2. D'ora in poi quindi potremo tralasciarli.

Per provare I., proveremo che i denominatori di x e y non possono essere divisi da p, $\forall\, p$ numero primo. Da ciò seguirà che necessariamente tali denominatori valgono 1, da cui si avrà la tesi. Fissiamo quindi un generico numero primo $p \in \mathbb{N}$, e studiamo delle condizioni sui punti razionali le cui coordinate ridotte ai minimi termini hanno denominatore diviso da p.

Osservazione 3.2. Sia $q \in \mathbb{Q}^*$, allora $\exists!\ k \in \mathbb{Z}$ tale che

$$q = \frac{m}{n} p^k$$

con $m \in \mathbb{Z}$, $n \in \mathbb{N}$ tali che $p \nmid m, n$, e $gcd(m, n) = 1$. Denominiamo tale rappresentazione di q rappresentazione p-adica di q.

Da tale osservazione si ha che è ben posta la seguente:

Definizione 3.2. *Si definisce valutazione p-adica in $\mathbb{Q}^*$ la mappa $\nu_p : \mathbb{Q}^* \to \mathbb{Z}$ tale che, $\forall q \in \mathbb{Q}^*$, presa la sua rappresentazione p-adica $q = \frac{m}{n} p^k$, si ha: $\nu_p(q) := k$.*

Osservazione 3.3. ν_p è una valutazione discreta su $\mathbb{Q}^*$, quindi in particolare è un morfismo suriettivo di gruppi tra $(\mathbb{Q}^*, \cdot)$ e $(\mathbb{Z}, +)$, e il suo anello di valutazione è la localizzazione di $\mathbb{Z}$ su (p), che denotiamo con $\mathbb{Z}_{(p)}$.

Sia quindi $P = (x, y) \in C(\mathbb{Q})$ con coordinate:

$$x = \frac{m}{np^a} \quad y = \frac{u}{vp^b}$$

tali che $p \nmid m, n, u, v$. Poiché $P \in C(\mathbb{Q})$, le sue coordinate soddisfano l'equazione della curva, e quindi si ha, mettendo a denominatore comune:

$$\frac{u^2}{v^2 p^{2b}} = \frac{m^3 + am^2 np^a + bmn^2 p^{2a} + cn^3 p^{3a}}{n^3 p^{3a}}$$

Ora, poiché $p \nmid m$, si ha che p non divide il numeratore del membro di destra dell'uguaglianza, e quindi applicando ν_p da ambo i lati, si ottiene:

$$-2b = \nu_p(y^2) = \nu_p\left(\frac{m^3 + am^2 np^a + bmn^2 p^{2a} + cn^3 p^{3a}}{n^3 p^{3a}}\right) = -3a$$

Quindi in particolare $2b = 3a$, da cui si ottiene che $a = 2k$ e $b = 3k$, $\exists k \in \mathbb{Z}$. Abbiamo perciò provato che:

Proposizione 3.1. *Se p divide il denominatore di una delle due coordinate di $P = (x, y)$ punto della curva, divide necessariamente entrambi i denominatori, e in particolare $\exists k \in \mathbb{N}$ tale che:*

$$\nu_p(x) = -2k \quad \nu_p(y) = -3k$$

Ciò motiva la seguente:

Definizione 3.3. $\forall k \in \mathbb{N}$, *poniamo:*

$$C(p^k) = \{(x, y) \in C(\mathbb{Q}) \mid \nu_p(x) \leq -2k, \nu_p(y) \leq -3k\} \cup \{\mathcal{O}\}$$

Osservazione 3.4. Si ha la seguente catena di inclusioni:

$$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset \cdots \supset C(p^k) \supset \ldots$$

Quindi, con le nuove notazioni introdotte, ciò che vorremo provare è che non vi sono punti di ordine finito in $C(p)$ (abbiamo già escluso quelli di ordine 2 da come abbiamo definito i $C(p^k)$, poiché hanno la $y = 0$ come visto). In tal senso, la prima cosa che faremo è provare che $C(p^k)$ è un sottogruppo di $C(\mathbb{Q})$, $\forall\, k \in \mathbb{N}$. Per fare ciò, ci converrà considerare un'altra parte affine della chiusura proiettiva della nostra curva rispetto a quella della forma canonica di Weierstrass: vogliamo avere l'elemento neutro nell'origine e mandare i punti di ordine 2 all'infinito. Consideriamo la trasformazione proiettiva di $\mathbb{P}^2$ che permuta l'asse delle y con l'asse delle z, ovvero, dando un nome diverso alle nuove coordinate di $\mathbb{P}^2$, tale che:

$$(x, y, z) \mapsto (t, s, u) \quad \text{dove } t = x,\ s = z,\ u = y$$

Ricordando che nel proiettivo la nostra curva è data dall'omogeneizzazione dell'equazione di Weierstrass $y^2z = x^3 + ax^2z + bxz^2 + cz^3$, una volta applicata la trasformazione scelta, la nuova equazione ottenuta per la curva nel piano affine, con $u = 1$, è:

$$s = t^3 + at^2s + bts^2 + cs^3$$

e il legame tra le variabili (x, y) e le variabili (t, s) nell'affine è :

$$t = \frac{x}{y} \quad s = \frac{1}{y}, \quad x = \frac{t}{s} \quad y = \frac{1}{s} \tag{3}$$

dove tali relazioni sono ben poste per tutti i punti della curva sul piano (x, y) tranne quelli di ordine 2, che infatti tramite la trasformazione scelta sono mappati nel proiettivo sulla retta all'infinito, mentre $\mathcal{O}$, che nel proiettivo corrisponde a $(0, 1, 0)$, viene mappato nell'origine del piano (t, s) come volevamo.

Osservazione 3.5. Essendo tale trasformazione un automorfismo proiettivo di $\mathbb{P}^2$, l'immagine di una retta tramite essa è una retta, quindi la somma tra punti della curva del nuovo piano affine si può ricavare nel modo standard, come definito nella prima sezione, ricordando che l'elemento neutro è dato da $(0, 0)$.

Osservazione 3.6. Dalla forma dell'equazione affine della curva sul piano (t, s), si osserva che se (t, s) è un punto della curva, anche $(-t, -s)$ lo è, quindi si ha che la somma di punti sulla curva è facilmente descrivibile: se $P, Q \in C$, chiamata $P * Q = (t, s)$ la terza intersezione tra la curva e la retta per P e Q, si ha che $P + Q = (-t, -s)$, poiché quest'ultimo è la terza intersezione tra la curva e la retta per $P * Q$ e $(0, 0)$. Da ciò segue anche che se $P = (t_1, s_1)$, si ha che $-P = (-t_1, -s_1)$ (poiché l'elemento neutro $(0, 0)$ è un flesso), e quindi $P + Q = -(P * Q)$.

Studiamo i punti di $C(p^k)$ nelle nuove coordinate (t, s):

Proposizione 3.2. *Sia P un punto sulla curva non di ordine 2, e siano (t, s) le sue coordinate nel piano (t, s). Allora si ha che:*

$$P \in C(p^k) \quad \iff \quad t \in p^k\mathbb{Z}_{(p)} \text{ ed } s \in p^{3k}\mathbb{Z}_{(p)}$$

Dimostrazione. '$\Rightarrow$': Sia $P \in C(p^k)$. Se P è l'elemento neutro del gruppo della curva, si ha $t = 0$, $s = 0$. Altrimenti, siano (x, y) le sue coordinate sul piano (x, y), quindi si ha che $\exists i \in \mathbb{N}$ tale che:

$$\nu_p(x) = -2(k + i) \quad \nu_p(y) = -3(k + i)$$

Allora, ricordando l'osservazione 3.3 e le relazioni (3), per le sue nuove coordinate valgono le seguenti uguaglianze:

$$\nu_p(t) = \nu_p\left(\frac{x}{y}\right) = \nu_p(x) - \nu_p(y) = -2(k + i) + 3(k + i) = k + i$$
$$\nu_p(s) = \nu_p\left(\frac{1}{y}\right) = -\nu_p(y) = 3(k + i)$$

da cui segue la tesi.

'$\Leftarrow$': se $(t,s) = (0,0)$, nel piano (x,y) $P = \mathcal{O} \in C(p^k)$, $\forall k \in \mathbb{N}$. Altrimenti, la tesi segue procedendo in modo analogo a sopra semplicemente dal fatto che le coordinate di P sul piano (x,y) per le relazioni (3) sono tali che $y = \dfrac{1}{s}$ e $x = \dfrac{t}{s}$. □

Corollario 3.2.1. *$\forall k \in \mathbb{N}$, se $P \in C(p^k)$, $-P \in C(p^k)$.*

Dimostrazione. Segue dalla proposizione precedente e dall'osservazione 3.6. □

Possiamo ora provare che $C(p^k)$ è un sottogruppo di $C(\mathbb{Q})$, $\forall k \in \mathbb{N}$, usando le nuove coordinate (t,s). In realtà proveremo qualcosa di ancora più forte, ovvero il seguente:

Teorema 3.3. *$\forall k \geq 1$, $C(p^k)$ è un sottogruppo di $C(\mathbb{Q})$ e si ha che:*

$$\frac{C(p^k)}{C(p^{3k})} \simeq \leq \frac{p^k \mathbb{Z}_{(p)}}{p^{3k}\mathbb{Z}_{(p)}}$$

dove il morfismo iniettivo di gruppi è indotto dal morfismo:

$$P \mapsto \begin{cases} [t(P)] = \left[\dfrac{x}{y}\right] & \text{se } P = (x,y) \neq \mathcal{O} \\ 0 & \text{se } P = \mathcal{O} \end{cases}$$

Prima di procedere con la dimostrazione del teorema, proviamo un lemma che ci fornisce una condizione sufficiente più debole di quella fornita dalla proposizione 3.2 per l'appartenenza a $C(p^k)$:

Lemma 3.1. *Sia $P \in C(\mathbb{Q})$ non di ordine 2, e siano (t,s) le sue coordinate sul piano (t,s). Supponiamo che $\nu_p(s) = k \geq 1$. Allora $\exists h \in \mathbb{N}$ tale che $k = 3h$ e si ha che $\nu_p(t) = h$, e quindi $P \in C(p^h)$.*

Dimostrazione. Dalle relazioni (3), poste (x,y) le coordinate di P sul piano (x,y), si ha:

$$\nu_p(y) = \nu_p\left(\frac{1}{s}\right) = -\nu_p(s) = -k$$

Quindi dalla proposizione 3.1 segue che $\exists h \in \mathbb{N}$ tale che:

$$\nu_p(x) = -2h \quad \nu_p(y) = -3h$$

per cui $k = 3h$ dalla seconda equazione. Inoltre si ottiene:

$$\nu_p(t) = \nu_p\left(\frac{x}{y}\right) = \nu_p(x) - \nu_p(y) = -2h + 3h = h$$

come volevamo. Infine da $\nu_p(t) = h$, $\nu_p(s) = 3h$ si ottiene $P \in C(p^h)$ per la proposizione 3.2. □

Procediamo quindi con la dimostrazione del teorema 3.3. La nostra dimostrazione segue [ST15], in cui ci sono però alcune lacune, in parte colmate da [ST24]; non viene però corretto il caso di P_1 e P_2 aventi stessa t: la parte **(1)** della dimostrazione indirizza tale problema con un argomento originale di questa tesi:

Dimostrazione (Teorema 3.3). Dal corollario 3.2.1, segue che è sufficiente provare che i $C(p^k)$ sono chiusi rispetto alla somma di punti per provare che sono sottogruppi di $C(\mathbb{Q})$: per provare ciò, dall'osservazione 3.6 segue che sul piano (t, s) è sufficiente dimostrare che la terza intersezione tra la curva e la retta per due punti di $C(p^k)$ è in $C(p^k)$. Questo è quello che proveremo per ottenere che i $C(p^k)$ sono sottogruppi di $C(\mathbb{Q})$.

La dimostrazione sarà suddivisa in tre parti: nelle prime due proveremo che $C(p^k)$ è un sottogruppo di $C(\mathbb{Q})$, $\forall k \in \mathbb{N}$, separando il caso speciale di due punti distinti aventi la stessa t nella prima parte e trattando tutti gli altri punti nella seconda; nella terza parte proveremo che la funzione definita nell'enunciato è un morfismo di gruppi, il cui nucleo è $C(p^{3k})$. Lavoreremo principalmente sul piano (t, s), quindi ricordiamo l'equazione della curva:

$$s = t^3 + at^2 s + bts^2 + cs^3 \tag{4}$$

con $a, b, c \in \mathbb{Z}$. Inoltre ricordiamo che, come visto nella sezione precedente, affinché la curva sia non singolare, deve valere:

$$-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0 \tag{5}$$

1) Proveremo che non esistono punti distinti in $C(p^k)$ aventi stessa coordinata t. Siano per assurdo $P_1 = (t_1, s_1)$, $P_2 = (t_2, s_2) \in C(p^k)$ tali che $P_1 \neq P_2$ e $t_1 = t_2 =: \tilde{t}$. Quindi la retta per P_1 e P_2 è la retta verticale $t = \tilde{t}$.

Se $c = 0$, dalla (5) segue che necessariamente $b \neq 0$; inoltre s_1, s_2 sono radici del polinomio di secondo grado in s:

$$b\tilde{t}s^2 + (a\tilde{t}^2 - 1)s + \tilde{t}^3$$

poiché P_1, P_2 soddisfano la (4). Per ipotesi s_1 ed s_2 sono distinti, quindi intanto si osserva che $\tilde{t} \neq 0$ (poiché altrimenti $s_1 = 0 = s_2$), da cui segue $s_1 \neq 0 \neq s_2$, ed essendo s_1, s_2 le radici del polinomio, vale:

$$s_1 s_2 = \frac{\tilde{t}^3}{b\tilde{t}} = \frac{\tilde{t}^2}{b} \tag{6}$$

Inoltre dalla proposizione 3.2 e dal lemma 3.1 $\exists h \geq k \geq 1$ tale che:

$$\nu_p(\tilde{t}) = h \quad \nu_p(s_1) = 3h \quad \nu_p(s_2) = 3h$$

Applicando quindi ν_p da ambo i lati nella (6) si ottiene:

$$6h = \nu_p(s_1) + \nu_p(s_2) = \nu_p(s_1 s_2) = \nu_p\left(\frac{\tilde{t}^2}{b}\right) = 2\nu_p(\tilde{t}) - \nu_p(b) \leq 2h$$

poiché b è un intero. Ciò è assurdo poiché $h \geq 1$.

Supponiamo ora $c \neq 0$: sia $P_3 = (\tilde{t}, s_3)$ la terza intersezione tra la retta $t = \tilde{t}$ e la curva, dove s_3 è dalla (4) la terza radice oltre a s_1, s_2 del polinomio in s:

$$cs^3 + b\tilde{t}s^2 + (a\tilde{t}^2 - 1)s + \tilde{t}^3$$

quindi s_3 è razionale poiché lo sono s_1, s_2 e i coefficienti del polinomio.

Se $\tilde{t} = 0$, si ha che s_1, s_2 ed s_3 soddisfano l'equazione:

$$s = cs^3$$

le cui soluzioni sono $0, \frac{1}{\sqrt{c}}, -\frac{1}{\sqrt{c}}$. Poiché per ipotesi s_1 ed s_2 sono distinti, si ha che uno dei due deve essere uguale a $\pm\frac{1}{\sqrt{c}}$, senza perdita di generalità supponiamo sia s_1. Poiché $c \in \mathbb{Z}$ ed $s_1 \in \mathbb{Q}$, c deve essere un quadrato perfetto, e si ha:

$$\nu_p(s_1) = \nu_p\left(\pm\frac{1}{\sqrt{c}}\right) = -\nu_p(\sqrt{c}) \leq 0$$

ma ciò è assurdo, poiché $P_1 \in C(p^k)$, quindi, dato che s'è supposto $s_1 \neq 0$, $\nu_p(s_1) \geq 1$.

Quindi necessariamente si ha $\tilde{t} \neq 0$, da cui segue per la (4) che anche s_1, s_2 ed s_3 sono diversi da zero. Dalla proposizione 3.2 e dal lemma 3.1 $\exists h \geq k \geq 1$ tale che:

$$\nu_p(\tilde{t}) = h \quad \nu_p(s_1) = 3h \quad \nu_p(s_2) = 3h \tag{7}$$

Ora, poiché s_1, s_2, s_3 sono radici del polinomio in s:

$$cs^3 + b\tilde{t}s^2 + (a\tilde{t}^2 - 1)s + \tilde{t}^3$$

si ha che valgono le seguenti (siamo nel caso $c \neq 0$):

$$-(s_1 + s_2 + s_3) = \frac{b}{c}\tilde{t} \qquad -s_1\, s_2\, s_3 = \frac{\tilde{t}^3}{c}$$

da cui si ottiene (abbiamo visto che $s_1 \neq 0 \neq s_2$):

$$\frac{b}{c}\tilde{t} + s_1 + s_2 = -s_3 = \frac{\tilde{t}^3}{c\, s_1\, s_2}$$

Quindi moltiplicando tutto per cs_1s_2 si ottiene:

$$\tilde{t}^3 = b\tilde{t}s_1s_2 + cs_1^2s_2 + cs_1s_2^2$$

Applicando ν_p da ambo i lati si ottiene un assurdo, infatti per le proprietà delle valutazioni discrete si ha:

$$\begin{aligned} 3h = \nu_p(\tilde{t}^3) = \nu_p(b\tilde{t}s_1s_2 + cs_1^2s_2 + cs_1s_2^2) \geq \\ \geq \min\{\nu_p(b\tilde{t}s_1s_2), \nu_p(cs_1^2s_2), \nu_p(cs_1s_2^2)\} \geq 7h \end{aligned}$$

dove quest'ultima disuguaglianza segue dal fatto che b e c sono interi e dalle (7), e ciò è una contraddizione poiché $h \geq 1$. Questo conclude la parte **(1)**.

2) Consideriamo inizialmente $P_1 = (t_1, s_1), P_2 = (t_2, s_2) \in C(p^k)$ distinti tali che $t_1 \neq t_2$. Sia $s = \alpha t + \beta$ la retta per P_1 e P_2, quindi si ha $\alpha = \dfrac{s_2 - s_1}{t_2 - t_1}$. Ora dall'equazione (4) e, sommando e sottraendo opportunamente, si ha che:

$$\begin{aligned} s_2 - s_1 = (t_2^3 - t_1^3) + a(t_2^2s_2 - t_1^2s_1) + b(t_2s_2^2 - t_1s_1^2) + c(s_2^3 - s_1^3) = \\ = (t_2^3 - t_1^3) + a[(t_2^2 - t_1^2)s_2 + t_1^2(s_2 - s_1)] + b[(t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)] + c(s_2^3 - s_1^3) \end{aligned}$$

da cui si ottiene:

$$(s_2-s_1)-at_1^2(s_2-s_1)-bt_1(s_2^2-s_1^2)-c(s_2^3-s_1^3)=(t_2^3-t_1^3)+a(t_2^2-t_1^2)s_2+b(t_2-t_1)s_2^2$$

e quindi raccogliendo $(s_2 - s_1)$ a sinistra e dividendo per $(t_2 - t_1)$ da ambo i lati (abbiamo supposto $t_1 \neq t_2$) si ricava:

$$\alpha(1-at_1^2-bt_1(s_1+s_2)-c(s_1^2+s_1s_2+s_2^2))=t_1^2+t_1t_2+t_2^2+a(t_1+t_2)s_2+bs_2^2 \quad (8)$$

Ora, poiché $P_1, P_2 \in C(p^k)$, si ha che $t_1, t_2, s_1, s_2 \in p^k\mathbb{Z}_{(p)}$ per la proposizione 3.2, quindi:

$$-at_1^2-bt_1(s_1+s_2)-c(s_1^2+s_1s_2+s_2^2) \in p^{2k}\mathbb{Z}_{(p)}$$

per cui è diverso da -1, perciò possiamo dividere da ambo i lati la (8) per il fattore $1-at_1^2-bt_1(s_1+s_2)-c(s_1^2+s_1s_2+s_2^2)$ e ottenere:

$$\alpha=\frac{t_1^2+t_1t_2+t_2^2+a(t_1+t_2)s_2+bs_2^2}{1-at_1^2-bt_1(s_1+s_2)-c(s_1^2+s_1s_2+s_2^2)} \quad (9)$$

Inoltre, se $P_1 = P_2$, posto $f(t,s) = s - t^3 - at^2s - bts^2 - cs^3$, si ha che la derivata parziale di f rispetto a s calcolata in P_1 è $f_s(P_1) = 1 - at^2 - 2bts - 3cs^2 \neq 0$ per motivi analoghi a quelli appena descritti sopra, per cui il coefficiente angolare della retta tangente la curva in P_1 è dato da:

$$\alpha=-\frac{f_t}{f_s}(P_1)=\frac{3t_1^2+2at_1s_1+bs_1^2}{1-at_1^2-2bt_1s_1-3cs_1^2}$$

che è uguale a quello ottenuto nella (9) sostituendo $t_2 = t_1$ ed $s_2 = s_1$, quindi possiamo adoperare sempre la (9).

Ora, si osserva dalla (9) che il numeratore di α appartiene a $p^{2k}\mathbb{Z}_{(p)}$ poiché $t_1, t_2 \in p^k\mathbb{Z}_{(p)}$ ed $s_1, s_2 \in p^{3k}\mathbb{Z}_{(p)}$ per la proposizione 3.2; inoltre il denominatore è invertibile in $\mathbb{Z}_{(p)}$ poiché della forma $1-pq$ con $q \in \mathbb{Z}_{(p)}$ e $\mathbb{Z}_{(p)}$ anello locale con unico ideale massimale (p), per cui si ha che $\alpha \in p^{2k}\mathbb{Z}_{(p)}$. Da questo si ottiene anche:

$$\beta = s_1 - \alpha t_1 \in p^{3k}\mathbb{Z}_{(p)}$$

Sia $P_3 = (t_3, s_3)$ la terza intersezione tra la curva e la retta $s = \alpha t + \beta$, quindi dalla (4) si ha che t_1, t_2, t_3 sono le soluzioni dell'equazione di terzo grado in t:

$$\alpha t+\beta = t^3+at^2(\alpha t+\beta)+bt(\alpha t+\beta)^2+c(\alpha t+\beta)^3$$

Sviluppando si ottiene che t_1, t_2, t_3 sono le radici del polinomio:

$$(1+a\alpha+b\alpha^2+c\alpha^3)t^3+(a\beta+2b\alpha\beta+3c\alpha^2\beta)t^2+\dots \text{ termini di grado inferiore}$$

In modo analogo a quanto visto precedentemente, si osserva che $1+a\alpha+b\alpha^2+c\alpha^3 \neq 0$ poiché $a\alpha + b\alpha^2 + c\alpha^3 \in p^2k\mathbb{Z}_{(p)}$, quindi vale la relazione:

$$t_1+t_2+t_3=-\frac{a\beta+2b\alpha\beta+3c\alpha^2\beta}{1+a\alpha+b\alpha^2+c\alpha^3}$$

In più, il numeratore appartiene a $p^{3k}\mathbb{Z}_{(p)}$ poiché $\beta \in p^{3k}\mathbb{Z}_{(p)}$ e il denominatore è invertibile in $\mathbb{Z}_{(p)}$ per motivi analoghi a quelli visti in precedenza, quindi si ottiene:

$$t_1 + t_2 + t_3 \in p^{3k}\mathbb{Z}_{(p)} \tag{10}$$

da cui segue che $t_3 \in p^k\mathbb{Z}_{(p)}$ poiché $t_1, t_2 \in p^k\mathbb{Z}_{(p)}$. Dall'equazione della retta si ottiene:

$$s_3 = \alpha t_3 + \beta \in p^{3k}\mathbb{Z}_{(p)}$$

Dal lemma 3.1 si ottiene che $P_3 \in C(p^k)$, e quindi abbiamo dimostrato quello che volevamo, ovvero che $C(p^k)$ è un sottogruppo di $C(\mathbb{Q})$, concludendo la parte **(2)**.

3) La relazione (10) ci assicura che la funzione definita nell'enunciato:

$$C(p^k) \to \frac{p^k\mathbb{Z}_{(p)}}{p^{3k}\mathbb{Z}_{(p)}}, \quad P \mapsto \begin{cases} [t(P)] = \left[\dfrac{x}{y}\right] & \text{se } P = (x, y) \\ 0 & \text{se } P = \mathcal{O} \end{cases}$$

è un morfismo di gruppi, poiché implica che:

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3k}\mathbb{Z}_{(p)}$$

Vogliamo provare che il nucleo di tale morfismo è $C(p^{3k})$, da cui seguirà la tesi per il primo teorema di omomorfismo, ovvero vogliamo:

$$\{P \in C(p^k) \mid t(P) \in p^{3k}\mathbb{Z}_{(p)}\} \cup \{\mathcal{O}\} = C(p^{3k})$$

Dalla proposizione 3.2 e il lemma 3.1, segue l'inclusione '$\supseteq$', proviamo ora l'altra. Sia quindi $P \in C(p^k)$ tale che $t(P) \in p^{3k}\mathbb{Z}_{(p)}$, quindi si ha che $\exists i \in \mathbb{N}$ tale che:

$$\nu_p(t(P)) = 3(k + i)$$

Poiché $P \in C(p^k)$, si ha che $s(P) \in p^{3k}\mathbb{Z}_{(p)}$, da cui si ha per il lemma 3.1:

$$\nu_p(s(P)) = 3\nu_p(t(P)) = 9(k + i)$$

Quindi $s(P) \in p^{9k}\mathbb{Z}_{(p)}$. Per la proposizione 3.2 ciò implica che $P \in C(p^{3k})$, e quindi abbiamo dimostrato anche l'inclusione '$\subseteq$'. Abbiamo quindi provato che la funzione definita nell'enunciato induce effettivamente un morfismo iniettivo da $\dfrac{C(p^k)}{C(p^{3k})}$ in $\dfrac{p^k\mathbb{Z}_{(p)}}{p^{3k}\mathbb{Z}_{(p)}}$, completando così la dimostrazione del teorema. □

Corollario 3.3.1.

$$\frac{C(p^k)}{C(p^{3k})} \simeq C_{p^\omega}$$

con $0 \leq \omega \leq 2k$, $\forall k \in \mathbb{N}_{\geq 1}$

Dimostrazione. Segue dal teorema 3.3 e dal fatto che $\left(\dfrac{p^k\mathbb{Z}_{(p)}}{p^{3k}\mathbb{Z}_{(p)}}, +\right)$ è un gruppo ciclico di ordine p^{2k}. □

Diretta conseguenza del teorema 3.3 è la parte I. del teorema di Nagell-Lutz, che finalmente possiamo andare a provare.

Teorema 3.4 (Nagell-Lutz, parte I.)**.** *Sia C una curva ellittica con forma di Weierstrass:*

$$y^2 = x^3 + ax^2 + bx + c = f(x)$$

con $a, b, c \in \mathbb{Z}$. Sia $P \in C(\mathbb{Q})$ un punto di ordine finito, $P \neq \mathcal{O}$. Allora si ha che $x(P), y(P) \in \mathbb{Z}$.

Dimostrazione. Se P è di ordine 2, la tesi segue dall'osservazione 3.1. Supponiamo quindi che P abbia ordine $n > 2$, quindi son ben definite $t(P), s(P)$. Sia $p \in \mathbb{N}$ un primo qualunque, proviamo che $P \notin C(p)$. Supponiamo per assurdo che vi appartenga, allora $\exists K := \max\{k \in \mathbb{N} \mid P \in C(p^k)\}$, poiché i denominatori delle coordinate di P non possono essere divisi da potenze arbitrariamente grandi di p. In particolare, dalla proposizione 3.1 si ha che $2K = -\nu_p(x(P))$

Supponiamo che $p \nmid n$: dal morfismo del teorema 3.3 si ha che vale la seguente congruenza:

$$t(nP) \equiv nt(P) \mod p^{3K}\mathbb{Z}_{(p)}$$

Poiché P ha ordine n, si ha che $t(nP) = t(\mathcal{O}) = 0$ per com'è definito il morfismo; inoltre poiché $p \nmid n$, n è invertibile in $\mathbb{Z}_{(p)}$, quindi si ottiene che vale la seguente:

$$t(P) \equiv 0 \mod p^{3K}\mathbb{Z}_{(p)}$$

da cui segue che P appartiene al nucleo del morfismo del teorema 3.3, che si è dimostrato essere $C(p^{3K})$. Ma ciò è assurdo per com'è definito K.

Quindi necessariamente si ha che $p \mid n$: sia $n = pm$, $\exists m \in \mathbb{N}$, e consideriamo il punto $Q = mP$: chiaramente Q ha ordine p, inoltre si ha che $Q \in C(p)$ poiché dal teorema 3.3 sappiamo che $C(p)$ è un sottogruppo di $C(\mathbb{Q})$. Si osserva intanto che quindi necessariamente $p \neq 2$, altrimenti si avrebbe già una contraddizione poiché i $C(p)$ non contengono punti di ordine 2 per l'osservazione 3.1, quindi sono ben definite $t(Q), s(Q)$. Sia $K' := \max\{k \in \mathbb{N} \mid Q \in C(p^k)\} \geq 1$, allora si ha che, per la proposizione 3.2, il lemma 3.1 e com'è definito K':

$$\nu_p(t(Q)) = K' \quad \nu_p(s(Q)) = 3K'$$

Per il morfismo del teorema 3.3 in modo analogo a come fatto sopra si ottiene la congruenza:

$$0 = t(\mathcal{O}) = t(pQ) \equiv pt(Q) \mod p^{3K'}\mathbb{Z}_{(p)}$$

da cui segue che $t(Q) \in p^{3K'-1}\mathbb{Z}_{(p)}$. Ma ciò è assurdo, poiché si otterrebbe:

$$K' = \nu_p(t(Q)) \geq 3K' - 1$$

ma $K' \geq 1$.

Quindi $P \notin C(p)$, $\forall p \in \mathbb{N}$ primo: ciò assicura che P è necessariamente a coordinate intere. □

4 Teorema di Nagell-Lutz: Parte II, alcuni esempi

Andiamo ora a provare la parte II. dell'enunciato del teorema. Faremo uso del seguente:

Lemma 4.1. *Sia $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ con discriminante $D \neq 0$ e sia $\phi(x) = f'(x)^2 - 4f(x)(a + 2x) \in \mathbb{Z}[x]$. Allora $\exists F, \Phi \in \mathbb{Z}[x]$ tali che:*

$$D = F(x)f(x) + \Phi(x)\phi(x)$$

Dimostrazione. $\phi(x)$ per come è definito è esattamente il numeratore dell'ascissa di $2P$ su una curva ellittica, ottenuta nella proposizione 2.1, quindi vale la seguente espressione: $\phi(x) = x^4 - 2bx^2 - 8cx + b^2 - 4ac$. Inoltre abbiamo visto che il discriminante D vale $-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. A questo punto, è possibile ricavarsi esplicitamente F e Φ effettuando una divisione tra polinomi in più variabili, e si ottiene:

$$D = (3x^3 - ax^2 - 5bx + 2ab - 27c)f(x) - (3x^2 + 2ax - a^2 + 4b)\phi(x)$$

□

Possiamo ora provare la parte II. del teorema di Nagell-Lutz:

Teorema 4.1. *Sia C una curva ellittica in forma di Weierstrass $y^2 = f(x)$ a coefficienti interi, e sia $P = (x, y) \in C(\mathbb{Q})$ tale che $x, y \in \mathbb{Z}$ e $2P$ è anch'esso a coordinate intere. Allora $y = 0$ oppure $y^2 \mid D$, con $D = discr(f)$.*

Dimostrazione. Supponiamo $y \neq 0$ e proviamo che $y^2 \mid D$. Poiché $y \neq 0$, si ha che P non è un punto di ordine 2, quindi $2P \neq \mathcal{O}$. Siano (X, Y) le coordinate di $2P$: per ipotesi si ha che $X, Y \in \mathbb{Z}$. Inoltre dalle formule di duplicazione ottenute nella proposizione 2.1 si ha che, usando le stesse notazioni del lemma:

$$X = \frac{\phi(x)}{4f(x)} = \frac{\phi(x)}{4y^2}$$

Per ipotesi $x \in \mathbb{Z}$, quindi $\phi(x) \in \mathbb{Z}$, e poiché $X \in \mathbb{Z}$, si ottiene che necessariamente $4y^2 \mid \phi(x)$, da cui segue che $y^2 \mid \phi(x)$. Dal lemma precedente si ha che $\exists F, \Phi \in \mathbb{Z}[x]$ tali che:

$$D = F(x)f(x) + \Phi(x)\phi(x) = F(x)y^2 + \Phi(x)\phi(x)$$

da cui segue che $y^2 \mid D$, poiché abbiamo provato che $y^2 \mid \phi(x)$. □

Corollario 4.1.1 (Nagell-Lutz, II.)**.** *Sia C una curva ellittica in forma di Weierstrass $y^2 = f(x)$ a coefficienti interi, e sia $P = (x, y) \in C(\mathbb{Q})$ di ordine finito. Allora $y = 0$ oppure $y^2 \mid D$, con $D = discr(f)$.*

Dimostrazione. Segue semplicemente dal fatto che per la parte I. del teorema di Nagell-Lutz, P e $2P$ sono necessariamente a coefficienti interi poiché entrambi di ordine finito, e quindi valgono le ipotesi del teorema precedente per P. □

Abbiamo quindi completato la dimostrazione del teorema di Nagell-Lutz. Per quanto riguarda le possibili classi di isomorfismo dei sottogruppi di torsione dei punti razionali di una curva ellittica, è stato provato il seguente sorprendente risultato, che determina tutte le possibili strutture di tali gruppi:

Teorema 4.2 (Teorema di Mazur)**.** *Data C curva ellittica, chiamato $C(\mathbb{Q})^{tors}$ il gruppo dei punti razionali di ordine finito della curva, si ha che vale una delle seguenti:*

- $C(\mathbb{Q})^{tors} \simeq C_n$, *con* $1 \leq n \leq 10$ *oppure* $n = 12$*;*
- $C(\mathbb{Q})^{tors} \simeq C_2 \times C_{2n}$ *con* $1 \leq n \leq 4$*;*

ed esistono esempi per ciascuna di tali classi di isomorfismo.

Concludiamo la tesi con degli esempi in cui applichiamo il teorema dimostrato per ricavare i punti razionali di ordine finito di certe curve ellittiche. Tali esempi saranno tratti da [ST15, Esercizio 2.12] e [Cas91, Sezione 12]. In quest'ultimo testo, si segnala che è possibile trovare una dimostrazione del teorema di Nagell-Lutz diversa da quella presentata in questo lavoro, che sfrutta i numeri p-adici. Le figure sono state realizzate tramite [Geo].

Esempio 1. Consideriamo la seguente curva ellittica:

$$C: \quad y^2 = x^3 + 1$$

Sfruttiamo il teorema di Nagell-Lutz per trovare i suoi punti razionali di ordine finito, che indicheremo con $C(\mathbb{Q})^{tors}$. Innanzitutto, si osserva che vi è un unico punto razionale avente $y = 0$, cioè: $(-1, 0)$. Quindi questo è l'unico punto razionale di ordine 2 della curva. Supponiamo quindi che $P = (x, y)$ sia un punto razionale di ordine finito tale che $y \neq 0$: dal teorema di Nagell-Lutz abbiamo che necessariamente $y^2 \mid \text{discr}(x^3 + 1) = -27$, quindi gli unici possibili valori per y sono ± 1 e ± 3. Dall'equazione della curva si ricava che i punti aventi tale ordinata sono:

$$(0, 1),\ (0, -1),\ (2, 3),\ (2, -3)$$

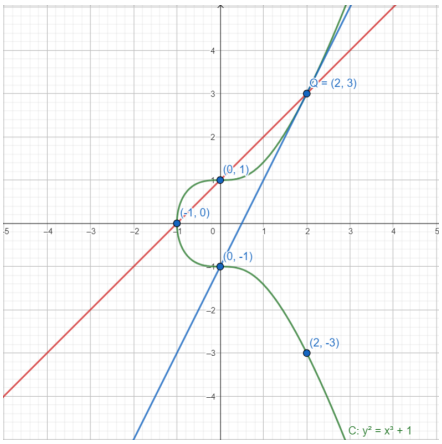
dove nelle coppie aventi medesima ascissa sono uno l'inverso dell'altro, e che, poiché sono tutti a coordinate intere, sono tutti possibili punti razionali di ordine finito. Ora, non è difficile provare che il punto $(0, 1)$ è di flesso per la curva (la tangente di flesso è semplicemente la retta $y = 1$), quindi per quanto provato nel corollario 3.1.2 si ha che $(0, 1)$ ha ordine 3, e quindi anche $(0, -1)$ in quanto opposto di $(0, 1)$. Ci rimane da studiare quindi unicamente il punto $Q = (2, 3)$: dalle formule di duplicazione ottenute nella proposizione 2.1 otteniamo che:

$$x(2Q) = \frac{2^4 - 16}{12} = 0 \quad y(2Q) = -\left(3 - \frac{2(12)}{6}\right) = 1$$

quindi $2Q = (0, 1)$, che sappiamo già essere di ordine 3, per cui si ha che anche Q ha ordine finito. In particolare poiché $6Q = 3(2Q) = 3(0, 1) = \mathcal{O}$, l'ordine di Q divide 6, ma non è un punto di ordine 2 per quanto detto, inoltre non può avere

ordine 3 poiché si ha che $2Q \neq -Q$, per cui possiamo concludere che Q ha ordine 6, e quindi anche $-Q = (2, -3)$ ha ordine 6; da questo segue che necessariamente $3Q = 3(-Q) = (-1, 0)$ in quanto unico punto razionale di ordine 2 della curva (ciò può essere verificato chiaramente anche tramite le formule della proposizione 2.1). Concludiamo che:

$$C(\mathbb{Q})^{tors} = \{\mathcal{O}, (2,3), (0,1), (-1,0), (0,-1), (2,-3)\} = \langle (2,3) \rangle \simeq C_6$$

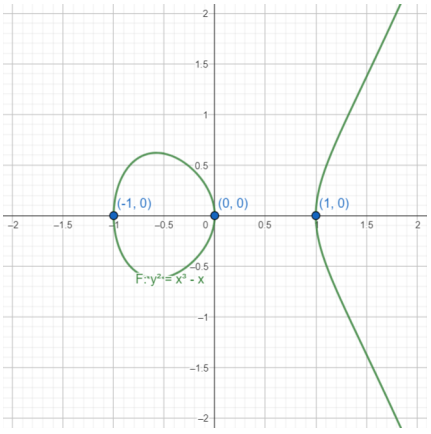


Esempio 2. Consideriamo la curva ellittica:

$$F: \quad y^2 = x^3 - x$$

Cerchiamo di ricavarci $F(\mathbb{Q})^{tors}$ utilizzando il teorema di Nagell-Lutz. Si osserva che il polinomio $x^3 - x = x(x-1)(x+1)$ ha tre radici intere, quindi otteniamo i seguenti punti di ordine 2: $(-1, 0)$, $(0, 0)$, $(1, 0)$. Supponiamo quindi ora $y \neq 0$: dal teorema di Nagell-Lutz, poiché $\text{discr}(x^3 - x) = 4$, si ha che gli unici possibili valori per la y sono ± 1 oppure ± 2. Dobbiamo verificare quindi, inserendo tali valori per la y nell'equazione della curva, se i polinomi $x^3 - x - 1$ e $x^3 - x - 4$ ammettono radici intere. Andando ad analizzare tali polinomi, studiandone la derivata e il segno, si ottiene che entrambi hanno un'unica radice reale compresa tra 1 e 2, per cui non si hanno valori razionali ammissibili per la x. Abbiamo quindi esaurito tutte le possibili y di punti razionali di ordine finito, e quindi si è ottenuto:

$$F(\mathbb{Q})^{tors} = \{\mathcal{O}, (-1,0), (0,0), (1,0)\} \simeq C_2 \times C_2$$



Esempio 3. Consideriamo la curva ellittica:

$$E: \quad y^2 = x^3 - 43x + 166$$

Nuovamente cerchiamo $E(\mathbb{Q})^{tors}$. Studiamo intanto $f(x) = x^3 - 43x + 166$: studiandone derivata e segno, si ottiene che esso ha un'unica radice reale compresa tra -9 e -8, quindi sappiamo dal teorema di Nagell-Lutz che non vi possono essere punti razionali di ordine 2. Supponiamo quindi $y \neq 0$: si ha che il discriminante di f vale $-425\,984 = -2^{15} \cdot 13$, quindi i possibili valori assumibili dalla y sono $\pm 2^n$, con $0 \leq n \leq 7$. Analizzando i primi n, il primo valore per cui si ottiene un candidato punto razionale di ordine finito per la curva è 3: infatti, si ha che $(3, \pm 8) \in E(\mathbb{Q})$. Studiamo quindi i multipli del punto $P = (3, 8)$. Dalle formule ottenute nella proposizione 2.1, si ottiene:

$$x(2P) = \frac{3^4 + 2 \cdot 43 \cdot 3^2 - 8 \cdot 166 \cdot 3 + 43^2}{4 \cdot 64} = -5 \quad y(2P) = -\left(\frac{27 - 43}{16} \cdot (-5) + 8 - \frac{3(27 - 43)}{16}\right) = -16$$

Abbiamo quindi ottenuto un nuovo punto a coordinate intere avente y soddisfacente le condizioni imposte dal teorema trovate inizialmente, il che fa ben sperare al momento sulla possibilità che si tratti effettivamente di punti di ordine finito. Applicando nuovamente le formule della proposizione 2.1 per calcolare le coordinate di $3P$ e $4P$, si ottiene $3P = (11, -32)$, che nuovamente è un punto a coordinate intere soddisfacente le proprietà trovate, e $4P = (11, 32)$, ma quindi ciò implica:

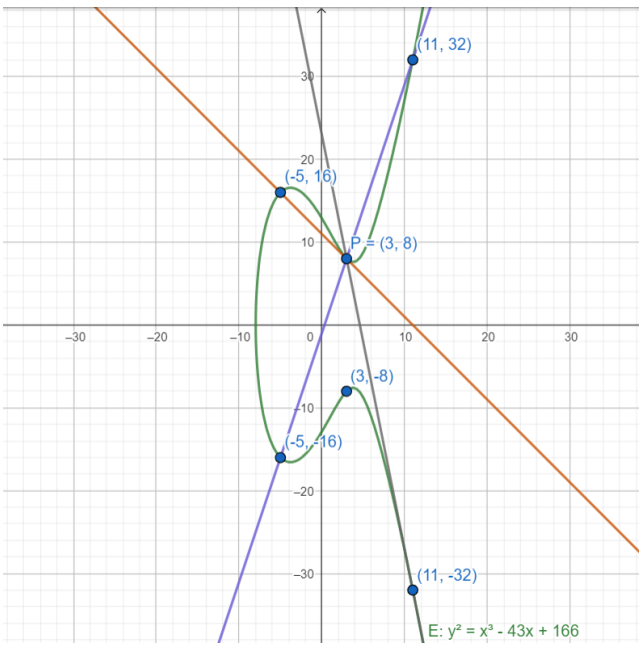
$$4P = (11, 32) = -(11, -32) = -3P$$

da cui segue:

$$7P = \mathcal{O}$$

Ciò implica che P ha ordine 7, ma quindi anche tutti i multipli di P che abbiamo trovato hanno tale ordine, per cui essi e i loro opposti compongono un gruppo ciclico di ordine 7. Inoltre, dal teorema di Mazur, ovvero il 4.2, si ha che non vi possono essere altri punti razionali di ordine finito, per cui possiamo concludere:

$$E(\mathbb{Q})^{tors} = \{\mathcal{O}, (3, 8), (-5, -16), (11, -32), (11, 32), (-5, 16), (3, -8)\} \simeq C_7$$



Riferimenti bibliografici

[Cam24] L. Campigli. Poligoni "biscritti" ad una curva ellittica, Università di Firenze, Tesi di laurea triennale, 2024.

[Cas91] J.W.S. Cassels. *Lectures on Elliptic Curves*. London Mathematics Society Student Texts 24. Cambridge University Press, 1991.

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

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

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

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

[ST15] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Springer International Publishing, second edition, 2015.

[ST24] J.H. Silverman and J.T. Tate. Errata and corrections to *Rational Points on Elliptic Curves* 2nd edition. `https://www.math.brown.edu/johsilve/RPEC/RPEC2ndEdErrata13June2024.pdf`, Last updated in 2024.