Sia E una curva ellittica definita su un campo $\mathbf{F}_q$ di q elementi. In questa nota stimiamo $\#E(\mathbf{F}_{q^2})$ seguendo il metodo di Stepanov.

Teorema 1. *Sia $\mathbf{F}_q$ un campo di $q \geq 5$ elementi e sia E una curva ellittica su $\mathbf{F}_q$. Allora si ha che*

$$\#E(\mathbf{F}_{q^2}) \leq q^2 + 3q.$$

Supponiamo che E sia data tramite un'equazione di Weierstrass:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \qquad \text{con } a_i, a_2, a_3, a_4, a_6 \in \mathbf{F}_q.$$

Sia ∞ l'unico punto all'infinito. Allora l'anello R di funzioni su E senza poli fuori ∞ è la $\mathbf{F}_q$-algebra generato dalle funzioni X e Y. Ogni elemento $f \in R$ ha la forma $g(X)+Yh(X)$ per polinomi unici $g, h \in \mathbf{F}_q[X]$. Per ogni $f \in R$ non nullo, sia $\deg f$ l'ordine del polo di f in ∞. Si ha quindi che $\deg X = 2$ e $\deg Y = 3$. In generale, se $f = g(X) + Yh(X)$ con $g, h \in \mathbf{F}_q[X]$ polinomi di grado d, e rispettivamente, allora $\deg f = \max(2d, 3 + 2e)$.

Per $a \geq 1$ sia H_a lo $\mathbf{F}_q$-spazio vettoriale di funzioni

$$H_a = \{f \in R : \deg f \leq a\}.$$

Poiché E ha genere 1, non esistono funzioni $f \in R$ con $\deg f = 1$. Questo implica che per $a = 1$ lo spazio H_a consiste solo nelle funzioni costanti $\mathbf{F}_q$ ed ha dimensione 1. Per $a = 2$ lo spazio H_a è generato dalle funzioni 1 e X ed ha dimensione 2. In generale si ha il seguente risultato.

Lemma 2. *Per $a \geq 1$ si ha che* $\dim H_a = a$.

Dimostrazione. Dopo quello che è già stato detto, possiamo supporre che $a > 2$. Allora per a pari, le funzioni

$$1, X, \ldots, X^{a/2}, Y, YX, \ldots YX^{a/2-2}$$

formano una base di H_a, mentre per a dispari sono le funzioni

$$1, X, \ldots, X^{(a-1)/2}, Y, YX, \ldots YX^{(a-3)/2}$$

che formano una base di H_a. In ogni caso la base ha esattamente a elementi, come richiesto.

Per $a \geq 1$ l'insieme $H_a^q = \{f^q : f \in H_a\}$ è uno spazio vettoriale di dimensione $a = \dim H_a$. Infatti, l'applicazione $f \mapsto f^q$ è una biezione $H_a \leftrightarrow H_a^q$.

Lemma 3. *Siano $a, b \geq 1$ e sia $H_a^q H_b$ lo $\mathbf{F}_q$-spazio vettoriale generato dalle funzioni fg con $f \in H_a^q$ e $g \in H_b$. Se $b < q$, allora lo spazio $H_a^q H_b$ ha dimensione ab.*

Dimostrazione. Per il Lemma 2 esiste una base $e_1, \ldots, e_a$ di H_a e una base $f_1, \ldots, f_b$ di H_b. È chiaro che le funzioni $e_i^q f_j$ con $1 \leq i \leq a$ e $1 \leq j \leq b$ generano $H_a^q H_b$. Si ha che

$$\deg e_i^q f_j = q\deg e_i + \deg f_i.$$

Dal fatto che $\deg f_i \leq b < q$ segue che le funzioni $e_i^q f_j$ hanno $\deg e_i^q f_j$ *distinti.* Se una combinazione $\mathbf{F}_q$-lineare $\sum_{i,j} \lambda_{ij} e_i^q f_j$ si annulla, si ha quindi necessariamente $\lambda_{ij} = 0$ per ogni i, j. Questo dimostra che le funzioni $e_i^q f_j$ sono indipendenti e formano una $\mathbf{F}_q$-base. Come consequenza la dimensione di $H_a^q H_b$ è ab come richiesto.

Da ora in poi supponiamo che $a, b \geq 1$ con $b < q$. Grazie al Lemma 3, l'applicazione $\mathbf{F}_q$-lineare

$$\vartheta : H_a^q H_b \longrightarrow H_a H_b^q$$

data da

$$e_i^q f_j \mapsto e_i f_j^q, \qquad \text{per } 1 \leq i \leq a \text{ e } 1 \leq j \leq b,$$

è ben definita. L'osservazione chiave è la seguente.

Osservazione. *Se $F \in H_a^q H_b$ sta in $\ker \vartheta$, allora F si annulla nei punti di $E(\mathbf{F}_{q^2}) - \{\infty\}$.*

Dimostrazione. Sia $P \neq \infty$ in $E(\mathbf{F}_{q^2})$. Scriviamo $F = \sum \lambda_{ij} e_i^q f_j$ per certi $\lambda_{ij} \in \mathbf{F}_q$ e supponiamo che F sta nel nucleo di ϑ. Allora

$$F(P)^q = \sum \lambda_{ij} e_i^{q^2}(P) f_j^q(P) = \sum \lambda_{ij} e_i(P) f_j^q(P) = (\sum \lambda_{ij} e_i f_j^q)(P) = 0$$

e quindi $F(P) = 0$. La seconda uguaglianza segue dal fatto che $P \in E(\mathbf{F}_{q^2})$ e quindi $f^{q^2}(P) = f(P)$ per ogni funzione $f \in R$.

Se la funzione F nella osservazione *non* è la funzione zero, allora otteniamo la stima

$$\#E(\mathbf{F}_{q^2}) - 1 \;\leq\; \#\{\text{zeri di } F\} \;=\; \#\{\text{poli di } F\} \;=\; \deg(F) \;\leq\; aq + b. \qquad (*)$$

La seconda disugaglianza segue dal fatto che $F \in H_a^q H_b \subset H_{aq+b}$. L'esistenza di una tale funzione F è garantita quando $a, b \geq 1$ hanno la proprietà che

$$\dim H_a^q H_b \;>\; \dim H_a H_b^q.$$

Poiché $b < q$, il Lemma 3 ci dice che $H_a^q H_b$ ha dimensione ab. Non è detto che il Lemma 3 si applica allo spazio $H_a H_b^q$. Usiamo invece il fatto che $H_a H_b^q$ è sottospazio di H_{a+bq} ed ha quindi dimensione $\leq a + bq$. Una funzione F non nulla in $\ker \vartheta$ esiste quindi quando

$$ab \;>\; a + bq.$$

Per dedurre una stima buona dalla disuguglianza $(*)$, scegliamo a più piccolo possibile. Per soddisfare la disuguglianza $ab > a + bq$, la scelta minimale di a è $a = q + 2$. In questo caso possiamo prendere $b = q - 1$, almeno per $q \geq 5$. Con questa scelta la quantità $aq + b$ della stima $(*)$ diventa $(q + 2)q + q - 1 = q^2 + 3q - 1$, implicando il Teorema 1.