Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

Riassunto

Geometric quadratic Chabauty and other topics in number theory

Questa tesi si compone di tre parti.

Nella prima parte mostriamo una generalizzazione del metodo di Chabauty che, in alcuni casi, permette di calcolare l'insieme dei punti razionali di una curva C di genere $g > 1$. Dato un numero primo p, il metodo di Chabauty consiste nell'intersecare, all'interno del gruppo p-adico di Lie formato dai $\mathbb{Q}_p$-punti della jacobiana J, la chiusura del gruppo di Mordell-Weil con i $\mathbb{Q}_p$-punti della curva. Se il rango di Mordell-Weil r è minore del genere, questo metodo permette di determinare un sottoinsieme finito di $C(Q_p)$ contenente $C(\mathbb{Q})$. Nel nostro metodo sostituiamo J con un prodotto di $\mathbb{G}_{\mathrm{m}}$-torsori su di esso, che denotiamo T. I $\mathbb{G}_{\mathrm{m}}$-torsori che usiamo sono pull-back del torsore di Poincaré della jacobiana. Questo ci permette di parametrizzare i punti interi su T usando la struttura di biestensione presente sul torsore di Poincaré. Quando $r+g-1$ è minore del rango del gruppo di Néron-Severi della jacobiana, il nostro metodo permette di determinare un sottoinsieme finito di $C(\mathbb{Q}_p)$ contenente $C(\mathbb{Q})$.

La seconda parte della tesi è dedicata allo studio degli automorfismi delle curve modulari di tipo Cartan. In letteratura è comune incontrare curve di Cartan di livello primo p, in quanto i loro punti non-cuspidali corrispondono a curve ellittiche la cui rappresentazione di Galois associata alla p-torsione non è surgettiva. Noi studiamo anche curve di Cartan di livello composto e dimostramo che, se il livello è sufficientemente alto, gli unici automorfismi di queste curve sono quelli "attesi", ovvero quegli automorfismi che sollevano ad automorfismi del semipiano superiore $\mathbb{H}$. Quando il livello p è primo, dimostriamo che questo risultato vale per $p > 11$. Nella nostra dimostrazione, la maggiore novità è uno studio accurato, per una classe molto estesa di curve modulari, dell'azione degli operatori di Hecke sui punti cuspidali ed ellittici di una curva modulare. Inoltre, generalizziamo metodi classici per dare un bound sul campo di definizione di un automorfismo u e per dedurre che u commuta, o quasi, con gli operatori di Hecke. Ne concludiamo

che u preserva sia l'insieme delle cuspidi che l'insieme dei punti ellittici. Dimostriamo infine che u si solleva al semipiano superiore $\mathbb{H}$ utilizzando propriet'a topologiche di base dei rivestimenti.

L'ultima parte della tesi riguarda il problema del logaritmo discreto su campi finiti di piccola caratteristica: dato un campo finito K di caratteristica p e ordine maggiore di p^p, dato un generatore g del gruppo $K^\times$ e dato un altro elemento $h \in K^\times$, il problema è determinare un intero z tale che $g^z = h$. Nell'ultimo capitolo della tesi descriviamo un algoritmo probabilistico che risolve questo problema in tempo quasi-polinomiale, ovvero in $\log(\#K)^{O(\log\log\#K)}$ operazioni. Un algoritmo *euristicamente quasi-polinomiale* era già stato proposto da Joux, Barbulescu, Gaudry and Thomé, la cui idea principale è cercare un elemento di K su cui l'automorfismo di Frobenius agisce in un modo "semplice". Noi utilizziamo un'idea simile e cerchiamo due elementi $x, y \in K$ su cui l'automorfismo di Frobenius agisce in un modo "semplice". In particolare, richiediamo che questi due elementi siano coordinate di un punto su una curva ellittica E e definiamo "semplice" utilizzando la struttura di gruppo di E. Data l'abbondanza di curve ellittiche, è facile dimostrare che ogni campo finito di caratteristica piccola è contenuto in un'altro campo finito, leggermente più grande, in cui si trovano tali elementi x, y. Questo rende il nostro approccio rigoroso.