Elliptic Curves in Isogeny Classes

Liangyi Zhao
Joint work with I. E. Shparlinski

University of New South Wales, Sydney, Australia

17 December 2015

1. Introduction
   - Elliptic Curves
2. Sketching the Proof
   - Proof
3. Large Sieve with Quadratic Moduli

Elliptic Curves

- Let $p > 3$ be a prime and let E be an elliptic curve over the field $\mathbb{F}_p$ be an elliptic curve given by

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.

Elliptic Curves

- Let $p > 3$ be a prime and let E be an elliptic curve over the field $\mathbb{F}_p$ be an elliptic curve given by

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.

- It is known that these equations generate $J = 2p + O(1)$ distinct (non-isomorphic over $\mathbb{F}_p$) curves.

Elliptic Curves

- Let $p > 3$ be a prime and let E be an elliptic curve over the field $\mathbb{F}_p$ be an elliptic curve given by

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.

- It is known that these equations generate $J = 2p + O(1)$ distinct (non-isomorphic over $\mathbb{F}_p$) curves.
- The Hasse-Weil bound gives that

$$\#E(\mathbb{F}_p) - p - 1 \in [-T, T] \text{ where } T = [2\sqrt{p}].$$

Elliptic Curves

- Let $p > 3$ be a prime and let E be an elliptic curve over the field $\mathbb{F}_p$ be an elliptic curve given by

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.
- It is known that these equations generate $J = 2p + O(1)$ distinct (non-isomorphic over $\mathbb{F}_p$) curves.
- The Hasse-Weil bound gives that

$$\#E(\mathbb{F}_p) - p - 1 \in [-T, T] \text{ where } T = [2\sqrt{p}].$$

- Curves with the same value of $\#E(\mathbb{F}_p)$ are said to be isogenous.

Elliptic Curves

- Let $p > 3$ be a prime and let E be an elliptic curve over the field $\mathbb{F}_p$ be an elliptic curve given by

$$E : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.
- It is known that these equations generate $J = 2p + O(1)$ distinct (non-isomorphic over $\mathbb{F}_p$) curves.
- The Hasse-Weil bound gives that

$$\#E(\mathbb{F}_p) - p - 1 \in [-T, T] \text{ where } T = [2\sqrt{p}].$$

- Curves with the same value of $\#E(\mathbb{F}_p)$ are said to be isogenous.
- Let $I(t)$ be number of distinct isomorphism classes in the isogeny class of curves with $\#E(\mathbb{F}_p) = p + 1 - t$, with $|t| \leq T$.

Elliptic Curves

- The average value of $I(t)$ over $t \in [-T, T]$ is clearly

$$\frac{1}{2T+1} \sum_{-T \leq t \leq T} I(t) = \frac{J}{2T+1} = \frac{\sqrt{p}}{2} + O(1).$$

Elliptic Curves

- The average value of $I(t)$ over $t \in [-T, T]$ is clearly

$$\frac{1}{2T+1} \sum_{-T \leq t \leq T} I(t) = \frac{J}{2T+1} = \frac{\sqrt{p}}{2} + O(1).$$

- Therefore, on average, each isogeny class contains about $\sqrt{p}/2$ non-isomorphic curves.

Elliptic Curves

- The average value of $I(t)$ over $t \in [-T, T]$ is clearly

$$\frac{1}{2T+1} \sum_{-T \leq t \leq T} I(t) = \frac{J}{2T+1} = \frac{\sqrt{p}}{2} + O(1).$$

- Therefore, on average, each isogeny class contains about $\sqrt{p}/2$ non-isomorphic curves.
- This motivates the study of the distribution of the values of

$$\iota(t) = \frac{I(t)}{0.5\sqrt{p}}.$$

Elliptic Curves

- The average value of $I(t)$ over $t \in [-T, T]$ is clearly

$$\frac{1}{2T+1} \sum_{-T \leq t \leq T} I(t) = \frac{J}{2T+1} = \frac{\sqrt{p}}{2} + O(1).$$

- Therefore, on average, each isogeny class contains about $\sqrt{p}/2$ non-isomorphic curves.
- This motivates the study of the distribution of the values of

$$\iota(t) = \frac{I(t)}{0.5\sqrt{p}}.$$

- Lenstra showed that for any $t \in [-2\sqrt{p}, 2\sqrt{p}]$, we have

$$\iota(t) = O\left(\log p (\log\log p)^2\right).$$

Elliptic Curves

- Birch showed that the Sato-Tate conjecture over the family of all isomorphism classes of elliptic curves over $\mathbb{F}_p$ implies that for $\alpha, \beta \in [-1, 1]$,

$$\sum_{\alpha T \leq t \leq \beta T} \iota(t) = \mu(\alpha, \beta) T + o(p),$$

where $\mu(\alpha, \beta)$ is the Sato-Tate density given by

$$\mu(\alpha, \beta) = \frac{2}{\pi} \int_{\arccos \alpha}^{\arccos \beta} \sin^2 \theta \, \mathrm{d}\theta.$$

Elliptic Curves

- Birch showed that the Sato-Tate conjecture over the family of all isomorphism classes of elliptic curves over $\mathbb{F}_p$ implies that for $\alpha, \beta \in [-1, 1]$,

$$\sum_{\alpha T \leq t \leq \beta T} \iota(t) = \mu(\alpha, \beta) T + o(p),$$

where $\mu(\alpha, \beta)$ is the Sato-Tate density given by

$$\mu(\alpha, \beta) = \frac{2}{\pi} \int_{\arccos \alpha}^{\arccos \beta} \sin^2 \theta \, \mathrm{d}\theta.$$

- The definition of $I(t)$ and $\iota(t)$ can be extended to arbitrary finite fields with q elements and these are the objects of our study.

Main Result

Theorem 1 (Shparlinski, Z)

Let $R \in \mathbb{Z}$ with $0 < R < 2R < 2\sqrt{q}$. We have

$$\frac{1}{R} \sum_{R < t \leq 2R} \iota(t) \ll \frac{\log q}{\sqrt{\log R}} (\log \log q)^{7/2}.$$

- Now we get that for any fixed $\varepsilon > 0$, there is a constant $c(\varepsilon)$ such that for $R \geq q^{\varepsilon}$, we have

$$\frac{1}{R} \sum_{R < t \leq 2R} \iota(t) \leq c(\varepsilon) \sqrt{\log q} (\log \log q)^{7/2}.$$

Main Result

Theorem 1 (Shparlinski, Z)

Let $R \in \mathbb{Z}$ with $0 < R < 2R < 2\sqrt{q}$. We have

$$\frac{1}{R} \sum_{R<t\leq 2R} \iota(t) \ll \frac{\log q}{\sqrt{\log R}} (\log\log q)^{7/2}.$$

- Now we get that for any fixed $\varepsilon > 0$, there is a constant $c(\varepsilon)$ such that for $R \geq q^{\varepsilon}$, we have

$$\frac{1}{R} \sum_{R<t\leq 2R} \iota(t) \leq c(\varepsilon)\sqrt{\log q}(\log\log q)^{7/2}.$$

- Recall Lenstra's individual bound $\iota(t) \ll \log q(\log\log q)^2$.

Main Result

Theorem 1 (Shparlinski, Z)

Let $R \in \mathbb{Z}$ with $0 < R < 2R < 2\sqrt{q}$. We have

$$\frac{1}{R} \sum_{R<t\leq 2R} \iota(t) \ll \frac{\log q}{\sqrt{\log R}} (\log\log q)^{7/2}.$$

- Now we get that for any fixed $\varepsilon > 0$, there is a constant $c(\varepsilon)$ such that for $R \geq q^{\varepsilon}$, we have

$$\frac{1}{R} \sum_{R<t\leq 2R} \iota(t) \leq c(\varepsilon)\sqrt{\log q}(\log\log q)^{7/2}.$$

- Recall Lenstra's individual bound $\iota(t) \ll \log q(\log\log q)^2$.
- Our Theorem is better than what one gets from the individual bounds as soon as $R > (\log\log q)^{3+\varepsilon}$.

Proof of the Theorem

- Using an identity of Lenstra for $I(t)$, we get

$$I(t) \ll \sqrt{\Delta(t)}\mathcal{L}(t)(\log\log q)^3,$$

where $\Delta(t) = 4q - t^2$ and $\mathcal{L}(t)$ is essentially the value of the Dirichlet L-function associated with the primitive quadratic character modulo the square-free kernel of $\Delta(t)$ at $s = 1$.

Proof of the Theorem

- Using an identity of Lenstra for $I(t)$, we get
$$I(t) \ll \sqrt{\Delta(t)}\mathcal{L}(t)(\log\log q)^3,$$
where $\Delta(t) = 4q - t^2$ and $\mathcal{L}(t)$ is essentially the value of the Dirichlet L-function associated with the primitive quadratic character modulo the square-free kernel of $\Delta(t)$ at $s = 1$.
- We are led to investigate the sum $\sum_{t\sim R} |\mathcal{L}(t)|$, where $t \sim R$ means $R < t \leq 2R$.

Proof of the Theorem

- Using an identity of Lenstra for $I(t)$, we get
$$I(t) \ll \sqrt{\Delta(t)}\mathcal{L}(t)(\log\log q)^3,$$
where $\Delta(t) = 4q - t^2$ and $\mathcal{L}(t)$ is essentially the value of the Dirichlet L-function associated with the primitive quadratic character modulo the square-free kernel of $\Delta(t)$ at $s = 1$.
- We are led to investigate the sum $\sum_{t\sim R} |\mathcal{L}(t)|$, where $t \sim R$ means $R < t \leq 2R$.
- Using the Dirichlet series for $\mathcal{L}(t)$ and partial summation, it suffices to estimate
$$\sum_{t\sim R} \max_{L\sim N} \left| \sum_{n=1}^{N} \xi_t(n) \right|, \tag{1}$$
where ξ_t is a quadratic character modulo $\Delta(t)$and L is a large parameter to be optimized.

Proof of the Theorem

- Now after some manipulations of (1) using the orthogonality of characters, Hölder's inequality to amplify the n-sum and the Gauss sums, we are led to

$$\sum_{t\sim R}\sum_{\substack{v=1\\ \gcd(v,\Delta(t))=1}}^{\Delta(t)}\left|\sum_{k=1}^{K}\rho(k)e\left(\frac{kv}{\Delta(t)}\right)\right|^2,$$

where $K=(2L)^{\nu}$ with ν being the exponent when applying Hölder. $\rho(k)$ is bounded by a divisor function.

Proof of the Theorem

- Now after some manipulations of (1) using the orthogonality of characters, Hölder's inequality to amplify the n-sum and the Gauss sums, we are led to

$$\sum_{t\sim R}\sum_{\substack{v=1\\ \gcd(v,\Delta(t))=1}}^{\Delta(t)}\left|\sum_{k=1}^{K}\rho(k)e\left(\frac{kv}{\Delta(t)}\right)\right|^2,$$

  where $K=(2L)^{\nu}$ with ν being the exponent when applying Hölder. $\rho(k)$ is bounded by a divisor function.
- We now need a large sieve inequality of quadratic moduli.

Large Sieve with Quadratic Moduli

- The classical large sieve inequality is a mean-value estimate for character sums.

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ \gcd(a,q)}}^{q} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q}\right) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2.$$

where $\{a_n\}$ is an arbitrary sequence of complex numbers.

Large Sieve with Quadratic Moduli

- The classical large sieve inequality is a mean-value estimate for character sums.

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ \gcd(a,q)}}^{q} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q}\right) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2.$$

  where $\{a_n\}$ is an arbitrary sequence of complex numbers.
- We need an estimate like the above, but for q running over values of a quadratic polynomial.

Large Sieve with Quadratic Moduli

- The classical large sieve inequality is a mean-value estimate for character sums.

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ \gcd(a,q)}}^{q} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{an}{q}\right) \right|^2 \ll (Q^2 + N) \sum_{n=M+1}^{M+N} |a_n|^2.$$

  where $\{a_n\}$ is an arbitrary sequence of complex numbers.
- We need an estimate like the above, but for q running over values of a quadratic polynomial.
- As is often the case in analytic number theory, the problem becomes more difficult when the averaging is taken over a sparse set.

Large Sieve with Quadratic Moduli

- The large sieve inequality for square moduli has been studied by S. Baier and the speaker, both independently and jointly.

Large Sieve with Quadratic Moduli

- The large sieve inequality for square moduli has been studied by S. Baier and the speaker, both independently and jointly.
- The best known result is

$$\begin{aligned}\sum_{q\leq Q}\sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q^2}\left|\sum_{n=M+1}^{M+N}a_n e\left(\frac{an}{q^2}\right)\right|^2 \\ \ll \left(Q^3+N+\min\left\{\sqrt{Q}N, Q^2\sqrt{N}\right\}\right)\sum_{n=M+1}^{M+N}|a_n|^2.\end{aligned} \tag{2}$$

Large Sieve with Quadratic Moduli

- The large sieve inequality for square moduli has been studied by S. Baier and the speaker, both independently and jointly.
- The best known result is

$$\sum_{q\leq Q}\sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q^2}\left|\sum_{n=M+1}^{M+N}a_n e\left(\frac{an}{q^2}\right)\right|^2 \ll \left(Q^3+N+\min\left\{\sqrt{Q}N, Q^2\sqrt{N}\right\}\right)\sum_{n=M+1}^{M+N}|a_n|^2. \tag{2}$$

- (2) is obtained using intricate Fourier analysis and the method can be adapted to our situation.

Large Sieve with Quadratic Moduli

- We have

$$\sum_{t\sim R}\sum_{\substack{a=1\\ \gcd(a,\Delta(t))=1}}^{\Delta(t)}\left|\sum_{n=1}^{N}a_n e\left(\frac{an}{\Delta(t)}\right)\right|^2$$

$$\ll \left(qR+N+\min\left\{\sqrt{R}N+\sqrt{q}N^{3/4},\sqrt{N}q\right\}\right)\sum_{n=1}^{N}|a_n|^2. \tag{3}$$

Large Sieve with Quadratic Moduli

- We have

$$\sum_{t\sim R}\sum_{\substack{a=1\\ \gcd(a,\Delta(t))=1}}^{\Delta(t)}\left|\sum_{n=1}^{N}a_n e\left(\frac{an}{\Delta(t)}\right)\right|^2$$
$$\ll \left(qR+N+\min\left\{\sqrt{R}N+\sqrt{q}N^{3/4},\sqrt{N}q\right\}\right)\sum_{n=1}^{N}|a_n|^2. \tag{3}$$

- Using (3) at the appropriate places and optimizing everything, we get the desired result.