Equidistribution Among Cosets of Elliptic Curve Points in Intervals

Kim Taechan Mehdi Tibouchi

NTT Secure Platform Laboratories

NutMiC, 2019–06–26

Our result, informally

- $E: y^2 = x^3 + ax^2 + bx + c$ elliptic curve over $\mathbb{F}_q$
- $H \subset E(\mathbb{F}_q)$ relatively large subgroup (for example, if $\#E(\mathbb{F}_q) = h \cdot n$, h small cofactor and n prime, think of H as the cyclic subgroup of order n)
- $I \subset \mathbb{F}_q$ interval (this is well-defined even for q a prime power)

Theorem (informal)

If I is large enough, then the points in $E(\mathbb{F}_q)$ with their x-coordinate in I are close to uniformly distributed among the cosets modulo H

Motivation: an attack on qDSA

- Fault attack on the signature scheme qDSA [TTA18]
- Signature scheme defined over Curve25519: Montgomery curve with group structure $E(\mathbb{F}_p) \cong \mathbb{Z}/8\mathbb{Z} \times H$ ($H = \langle P \rangle$ cyclic of large prime order n)
- Main operation during signing: compute scalar multiplication of the base point P by random nonce k, using x-only arithmetic
- Idea of the attack: perturb the point P to get a faulty point $\widetilde{P}$ with different x-coordinate. If lucky, $\widetilde{P}$ of order $8n$. Then, the signature leaks 3 bits of the nonce k
- Attack on biased nonces: with many such perturbed signatures, recover the signing key!
- Are we lucky often enough?

Motivation: fault injection

- How do we perturb P to get $\widetilde{P}$?
- Fault injection!
- One possible technique involves hitting the memory cells where the x-coordinate is stored with lasers
- Effect: randomly flip the bits in the memory region struck by the laser beam
- Question: does this reliably yield a lucky faulty point (of order $8n$)?

Motivation: connection with our result

- The fauly point obtained with lasers has an x-coordinate of the form: $\tilde{x} = x_0 + 2^k \cdot z$, with z a uniform ℓ-bit integer
  - ℓ: width of the laser beam
  - k: index of least significant bit struck by the beam
- The set of all $\tilde{x}$'s is an interval of $\mathbb{F}_p$, of length 2^ℓ
- By our result: for ℓ large enough, the points in $E(\mathbb{F}_p)$ of the form $\widetilde{P}$ are close to uniformly distributed among the cosets modulo H
  - note that some $\tilde{x}$ do not correspond to a point in $E(\mathbb{F}_p)$ (but on the twist): this is easy to detect, so ok

Motivation: success probability

- In particular, (still for ℓ large enough) the faulty points $\widetilde{P}$ in $E(\mathbb{F}_p)$ have probability very close to 1/2 of being of order $8n$ (4 suitable cosets mod H out of 8)
- Additional theorem (previously known): a faulty point has probability very close to 1/2 to end up on E rather than on the twist
- Conclusion: "lucky" with probability $\approx 1/4$, which is large enough for the attack to work!

An analogy

- To get a sense of how we obtain our result: suppose we wanted to prove something similar in the simpler group $\mathbb{F}_p^\times$
- The statement would become: consider a large subgroup $G \subset \mathbb{F}_p^\times$, and an interval $I \subset \mathbb{F}_p$; for I large enough, the elements of I are close to uniformly distributed among the cosets modulo G
- Simplest case: $G = (\mathbb{F}_p^\times)^2$ (subgoup of squares). Then, there are two cosets: quadratic residues and nonresidues
- Consider an interval $I = [x, \ldots, x + h)$. The elements of I are close to uniformly distributed among cosets mod G if the proportion $N^+(I)/h$ of quadratic residues in I and the proportion $N^-(I)/h$ of nonquadratic residues in I are both close to $1/2$

An analogy

- To get a sense of how we obtain our result: suppose we wanted to prove something similar in the simpler group $\mathbb{F}_p^\times$
- The statement would become: consider a large subgroup $G \subset \mathbb{F}_p^\times$, and an interval $I \subset \mathbb{F}_p$; for I large enough, the elements of I are close to uniformly distributed among the cosets modulo G
- Simplest case: $G = (\mathbb{F}_p^\times)^2$ (subgoup of squares). Then, there are two cosets: quadratic residues and nonresidues
- Consider an interval $I = [x, \ldots, x+h)$. The elements of I are close to uniformly distributed among cosets mod G if the proportion $N^+(I)/h$ of quadratic residues in I and the proportion $N^-(I)/h$ of nonquadratic residues in I are both close to $1/2$

An analogy

- To get a sense of how we obtain our result: suppose we wanted to prove something similar in the simpler group $\mathbb{F}_p^\times$
- The statement would become: consider a large subgroup $G \subset \mathbb{F}_p^\times$, and an interval $I \subset \mathbb{F}_p$; for I large enough, the elements of I are close to uniformly distributed among the cosets modulo G
- Simplest case: $G = (\mathbb{F}_p^\times)^2$ (subgoup of squares). Then, there are two cosets: quadratic residues and nonresidues
- Consider an interval $I = [x, \ldots, x + h)$. The elements of I are close to uniformly distributed among cosets mod G if the proportion $N^+(I)/h$ of quadratic residues in I and the proportion $N^-(I)/h$ of nonquadratic residues in I are both close to $1/2$

An analogy

- To get a sense of how we obtain our result: suppose we wanted to prove something similar in the simpler group $\mathbb{F}_p^\times$
- The statement would become: consider a large subgroup $G \subset \mathbb{F}_p^\times$, and an interval $I \subset \mathbb{F}_p$; for I large enough, the elements of I are close to uniformly distributed among the cosets modulo G
- Simplest case: $G = (\mathbb{F}_p^\times)^2$ (subgoup of squares). Then, there are two cosets: quadratic residues and nonresidues
- Consider an interval $I = [x, \ldots, x + h)$. The elements of I are close to uniformly distributed among cosets mod G if the proportion $N^+(I)/h$ of quadratic residues in I and the proportion $N^-(I)/h$ of nonquadratic residues in I are both close to $1/2$

Statistical distance

- This is measured by the statistical distance:

$$\Delta_1(I) = \frac{1}{2}\left(\left|\frac{N^+(I)}{h} - \frac{1}{2}\right| + \left|\frac{N^-(I)}{h} - \frac{1}{2}\right|\right)$$

- If at least half of the elements of I are quadratic residues, then $N^+(I)/h \geq 1/2 \geq N^-(I)/h$, and hence the statistical distance becomes:

$$\Delta_1(I) = \frac{1}{2}\left(\frac{N^+(I)}{h} - \frac{1}{2} + \frac{1}{2} - \frac{N^-(I)}{h}\right) = \frac{1}{2h}\left(N^+(I) - N^-(I)\right)$$

and similarly, if at least half the elements are nonquadratic residues, the opposite equality holds. Hence, we almost always have:

$$\Delta_1(I) = \frac{1}{2h}\left|N^+(I) - N^-(I)\right|$$

Statistical distance

- This is measured by the statistical distance:

$$\Delta_1(I) = \frac{1}{2}\left(\left|\frac{N^+(I)}{h} - \frac{1}{2}\right| + \left|\frac{N^-(I)}{h} - \frac{1}{2}\right|\right)$$

- If at least half of the elements of I are quadratic residues, then $N^+(I)/h \geq 1/2 \geq N^-(I)/h$, and hence the statistical distance becomes:

$$\Delta_1(I) = \frac{1}{2}\left(\frac{N^+(I)}{h} - \frac{1}{2} + \frac{1}{2} - \frac{N^-(I)}{h}\right) = \frac{1}{2h}\left(N^+(I) - N^-(I)\right)$$

and similarly, if at least half the elements are nonquadratic residues, the opposite equality holds. Hence, we almost always have:

$$\Delta_1(I) = \frac{1}{2h}\left|N^+(I) - N^-(I)\right|$$

Estimating the statistical distance

- Recall that $y \in N^+(I)$ if the Legendre symbol $\left(\frac{y}{p}\right) = +1$ and $y \in N^-(I)$ if $\left(\frac{y}{p}\right) = -1$. Therefore:

$$N^+(I) - N^-(I) = \sum_{y=x}^{x+h-1} \left(\frac{y}{p}\right)$$

- This is an example of character sum
- There is extensive research on establishing bounds on character sums. The epitome of such results in the Pólya–Vinogradov inequality:

$$\left| \sum_{y=x}^{x+h-1} \left(\frac{y}{p}\right) \right| < \sqrt{p} \log p,$$

independently of h.

  - under GRH, a bound of the form $O(\sqrt{p} \log\log p)$ can also be obtained, but the square root is provably optimal

Estimating the statistical distance

- Recall that $y \in N^+(I)$ if the Legendre symbol $\left(\frac{y}{p}\right) = +1$ and $y \in N^-(I)$ if $\left(\frac{y}{p}\right) = -1$. Therefore:

$$N^+(I) - N^-(I) = \sum_{y=x}^{x+h-1} \left(\frac{y}{p}\right)$$

- This is an example of character sum
- There is extensive research on establishing bounds on character sums. The epitome of such results in the Pólya–Vinogradov inequality:

$$\left| \sum_{y=x}^{x+h-1} \left(\frac{y}{p}\right) \right| < \sqrt{p} \log p,$$

independently of h.

  - under GRH, a bound of the form $O(\sqrt{p} \log\log p)$ can also be obtained, but the square root is provably optimal

Estimating the statistical distance

- Recall that $y \in N^+(I)$ if the Legendre symbol $\left(\frac{y}{p}\right) = +1$ and $y \in N^-(I)$ if $\left(\frac{y}{p}\right) = -1$. Therefore:

$$N^+(I) - N^-(I) = \sum_{y=x}^{x+h-1} \left(\frac{y}{p}\right)$$

- This is an example of character sum
- There is extensive research on establishing bounds on character sums. The epitome of such results in the Pólya–Vinogradov inequality:

$$\left| \sum_{y=x}^{x+h-1} \left(\frac{y}{p}\right) \right| < \sqrt{p} \log p,$$

independently of h.

  - under GRH, a bound of the form $O(\sqrt{p} \log\log p)$ can also be obtained, but the square root is provably optimal

Equidistribution of squares and non squares

- In the case of the previous setting, this says that:

$$\Delta_1(I) < \frac{\sqrt{p}\log p}{2h}.$$

- In particular, if $h \geq p^{1/2+\epsilon}$, $\Delta_1(I)$ is negligible: if you flip a little over half of the bits of an element of $\mathbb{F}_p^\times$, the result is close to uniformly distributed between quadratic and nonquadratic residues
- Actually, in the case of character sums over $\mathbb{F}_p^\times$, we can improve things further using the Burgess bound, which gives non-trivial bounds as soon as $h \geq p^{1/4+\epsilon}$: flipping $> 1/4$ of the bits is OK
  - best we can do we current techniques (?)
  - no counterpart of the Burgess bound in our setting (character sums on elliptic curves)

Equidistribution of squares and non squares

- In the case of the previous setting, this says that:

$$\Delta_1(I) < \frac{\sqrt{p}\log p}{2h}.$$

- In particular, if $h \geq p^{1/2+\epsilon}$, $\Delta_1(I)$ is negligible: if you flip a little over half of the bits of an element of $\mathbb{F}_p^\times$, the result is close to uniformly distributed between quadratic and nonquadratic residues
- Actually, in the case of character sums over $\mathbb{F}_p^\times$, we can improve things further using the Burgess bound, which gives non-trivial bounds as soon as $h \geq p^{1/4+\epsilon}$: flipping $> 1/4$ of the bits is OK
  - best we can do we current techniques (?)
  - no counterpart of the Burgess bound in our setting (character sums on elliptic curves)

Equidistribution of squares and non squares

- In the case of the previous setting, this says that:

$$\Delta_1(I) < \frac{\sqrt{p}\log p}{2h}.$$

- In particular, if $h \geq p^{1/2+\epsilon}$, $\Delta_1(I)$ is negligible: if you flip a little over half of the bits of an element of $\mathbb{F}_p^\times$, the result is close to uniformly distributed between quadratic and nonquadratic residues
- Actually, in the case of character sums over $\mathbb{F}_p^\times$, we can improve things further using the Burgess bound, which gives non-trivial bounds as soon as $h \geq p^{1/4+\epsilon}$: flipping $> 1/4$ of the bits is OK
  - best we can do we current techniques (?)
  - no counterpart of the Burgess bound in our setting (character sums on elliptic curves)

What about other subgroups?

- Does the above discussion generalize to other subgroups $G \subset \mathbb{F}_p^\times$?
- Yes, using higher-power residue symbols. For a subgroup of index d, it suffices to obtain bounds on short character sums of the form:

$$\sum_{y \in I} \chi(y)$$

  for χ all non trivial powers of the d-th power residue symbols
- Intuition: this gives the discrete Fourier transform. From there, we can apply Parseval to express the Euclidean distance between the desired distribution and uniform. Then apply Cauchy–Schwarz to get the L^1 distance, which is the statistical distance!

What about other subgroups?

- Does the above discussion generalize to other subgroups $G \subset \mathbb{F}_p^\times$?
- Yes, using higher-power residue symbols. For a subgroup of index d, it suffices to obtain bounds on short character sums of the form:

$$\sum_{y \in I} \chi(y)$$

  for χ all non trivial powers of the d-th power residue symbols
- Intuition: this gives the discrete Fourier transform. From there, we can apply Parseval to express the Euclidean distance between the desired distribution and uniform. Then apply Cauchy–Schwarz to get the L^1 distance, which is the statistical distance!

What about other subgroups?

- Does the above discussion generalize to other subgroups $G \subset \mathbb{F}_p^\times$?
- Yes, using higher-power residue symbols. For a subgroup of index d, it suffices to obtain bounds on short character sums of the form:

$$\sum_{y \in I} \chi(y)$$

  for χ all non trivial powers of the d-th power residue symbols
- Intuition: this gives the discrete Fourier transform. From there, we can apply Parseval to express the Euclidean distance between the desired distribution and uniform. Then apply Cauchy–Schwarz to get the L^1 distance, which is the statistical distance!

Character bounds on intervals

- Most general theorems only provide character sum bounds over all of the base field, not intervals of it
- However, general convolution approach to bounds on intervals from bounds on twisted (or "mixed") character sums over all of $\mathbb{F}_p$:

$$\sum_{y \in \mathbb{F}_p} \chi(y) e^{2i\pi\alpha y/p}$$

for all $\alpha \in \mathbb{F}_p$ (in other words, sums of the form $\sum_y \chi(y)\psi(y)$ with ψ additive character of $\mathbb{F}_p$)

- Consequence of the following general bound:

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| \leq p(1 + \log p)$$

(Ψ group of additive characters of $\mathbb{F}_p$). Generalizes to non prime finite fields too

Character bounds on intervals

- Most general theorems only provide character sum bounds over all of the base field, not intervals of it
- However, general convolution approach to bounds on intervals from bounds on twisted (or "mixed") character sums over all of $\mathbb{F}_p$:

$$\sum_{y \in \mathbb{F}_p} \chi(y) e^{2i\pi\alpha y/p}$$

for all $\alpha \in \mathbb{F}_p$ (in other words, sums of the form $\sum_y \chi(y)\psi(y)$ with ψ additive character of $\mathbb{F}_p$)

- Consequence of the following general bound:

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| \leq p(1 + \log p)$$

(Ψ group of additive characters of $\mathbb{F}_p$). Generalizes to non prime finite fields too

Character bounds on intervals

- Most general theorems only provide character sum bounds over all of the base field, not intervals of it
- However, general convolution approach to bounds on intervals from bounds on twisted (or "mixed") character sums over all of $\mathbb{F}_p$:

$$\sum_{y \in \mathbb{F}_p} \chi(y) e^{2i\pi\alpha y/p}$$

for all $\alpha \in \mathbb{F}_p$ (in other words, sums of the form $\sum_y \chi(y)\psi(y)$ with ψ additive character of $\mathbb{F}_p$)

- Consequence of the following general bound:

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| \leq p(1 + \log p)$$

(Ψ group of additive characters of $\mathbb{F}_p$). Generalizes to non prime finite fields too

Back to our problem

- How does this analogy play out in our original context?
- Recall: we have an elliptic curve E over $\mathbb{F}_q$, a subgroup $H \subset E(\mathbb{F}_q)$ and an interval $I \subset \mathbb{F}_q$
- We would like to argue that points in $E(\mathbb{F}_q)$ with their x-coordinate in I are equidistributed among the cosets mod H. Nothing special about x, so more generally, we can consider the problem for any rational function f on E

Back to our problem

- How does this analogy play out in our original context?
- Recall: we have an elliptic curve E over $\mathbb{F}_q$, a subgroup $H \subset E(\mathbb{F}_q)$ and an interval $I \subset \mathbb{F}_q$
- We would like to argue that points in $E(\mathbb{F}_q)$ with their x-coordinate in I are equidistributed among the cosets mod H. Nothing special about x, so more generally, we can consider the problem for any rational function f on E

Back to our problem

- How does this analogy play out in our original context?
- Recall: we have an elliptic curve E over $\mathbb{F}_q$, a subgroup $H \subset E(\mathbb{F}_q)$ and an interval $I \subset \mathbb{F}_q$
- We would like to argue that points in $E(\mathbb{F}_q)$ with their x-coordinate in I are equidistributed among the cosets mod H. Nothing special about x, so more generally, we can consider the problem for any rational function f on E

Statistical distance again

- Define:

$$N(I) := \left|\{P \in E(\mathbb{F}_q) : f(P) \in I\}\right|$$
$$N(P_0; I) := \left|\{P \in P_0 + H : f(P) \in I\}\right|$$

- The statistical distance between the uniform distribution over cosets and the distribution among cosets of points with $f(P) \in I$ is given by:

$$\Delta_1 = \frac{1}{2} \sum_{P_0 \in E(\mathbb{F}_q)/H} \left| \frac{N(P_0; I)}{N(I)} - \frac{1}{[E(\mathbb{F}_q) : H]} \right|$$

  where $[E(\mathbb{F}_q) : H] = \left|E(\mathbb{F}_q)/H\right|$ is the index of H in $E(\mathbb{F}_q)$

- How do we bound this?

Statistical distance again

- Define:

$$N(I) := \left|\{P \in E(\mathbb{F}_q) : f(P) \in I\}\right|$$
$$N(P_0; I) := \left|\{P \in P_0 + H : f(P) \in I\}\right|$$

- The statistical distance between the uniform distribution over cosets and the distribution among cosets of points with $f(P) \in I$ is given by:

$$\Delta_1 = \frac{1}{2} \sum_{P_0 \in E(\mathbb{F}_q)/H} \left| \frac{N(P_0; I)}{N(I)} - \frac{1}{[E(\mathbb{F}_q) : H]} \right|$$

  where $[E(\mathbb{F}_q) : H] = \left|E(\mathbb{F}_q)/H\right|$ is the index of H in $E(\mathbb{F}_q)$

- How do we bound this?

Statistical distance again

- Define:

$$N(I) := \left|\{P \in E(\mathbb{F}_q) : f(P) \in I\}\right|$$
$$N(P_0; I) := \left|\{P \in P_0 + H : f(P) \in I\}\right|$$

- The statistical distance between the uniform distribution over cosets and the distribution among cosets of points with $f(P) \in I$ is given by:

$$\Delta_1 = \frac{1}{2} \sum_{P_0 \in E(\mathbb{F}_q)/H} \left| \frac{N(P_0; I)}{N(I)} - \frac{1}{[E(\mathbb{F}_q) : H]} \right|$$

  where $[E(\mathbb{F}_q) : H] = \left|E(\mathbb{F}_q)/H\right|$ is the index of H in $E(\mathbb{F}_q)$

- How do we bound this?

Ingredients we need

- This is again carried out using character sum bounds. We use the Kohel–Shparlinski bound on the sums:

$$S(\omega, \psi, f) := \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} \omega(P)\psi(f(P))$$

(ω character of the group $E(\mathbb{F}_q)$, ψ additive character of $\mathbb{F}_q$, not both trivial)

- Kohel and Shparlinski show:

$$\left|S(\omega, \psi, f)\right| \leq 2\deg(f)q^{1/2}.$$

- This bound + convolution technique to get bounds on intervals + Cauchy–Schwarz: enough to bound the statistical distance

Ingredients we need

- This is again carried out using character sum bounds. We use the Kohel–Shparlinski bound on the sums:

$$S(\omega, \psi, f) := \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} \omega(P)\psi(f(P))$$

(ω character of the group $E(\mathbb{F}_q)$, ψ additive character of $\mathbb{F}_q$, not both trivial)

- Kohel and Shparlinski show:

$$\left|S(\omega, \psi, f)\right| \leq 2\deg(f)q^{1/2}.$$

- This bound + convolution technique to get bounds on intervals + Cauchy–Schwarz: enough to bound the statistical distance

Ingredients we need

- This is again carried out using character sum bounds. We use the Kohel–Shparlinski bound on the sums:

$$S(\omega, \psi, f) := \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} \omega(P)\psi(f(P))$$

(ω character of the group $E(\mathbb{F}_q)$, ψ additive character of $\mathbb{F}_q$, not both trivial)

- Kohel and Shparlinski show:

$$\left|S(\omega, \psi, f)\right| \leq 2\deg(f)q^{1/2}.$$

- This bound + convolution technique to get bounds on intervals + Cauchy–Schwarz: enough to bound the statistical distance

Our result, formally

Theorem

For any interval $I \subset \mathbb{F}_q$, the statistical distance Δ_1 between the uniform distribution on the set of points $P \in E(\mathbb{F}_q)$ such that $f(P) \in I$ and the uniform distribution on $E(\mathbb{F}_q)/H$ is bounded as:

$$\Delta_1 \leq \frac{1}{N(I)} \cdot [E(\mathbb{F}_q) : H]^{1/2} \cdot 2 \deg(f) q^{1/2} (1 + \log p).$$

If $|I| = \Omega(q^{1/2+\epsilon})$ for some $\epsilon > 0$ and $\deg f = O(1)$, we have:

$$\Delta_1 = O\Big(\frac{[E(\mathbb{F}_q) : H]^{1/2} q^{1/2} \log p}{|I|} \Big).$$

Negligible as soon as $|I| \geq \sqrt{[E(\mathbb{F}_q) : H]} \cdot q^{1/2+\epsilon}$.

Consequence for our original problem

- By the previous theorem: a random fault on a little more than half the bits of the x-coordinates yields a point equidistributed among cosets
  - note $\sqrt{[E(\mathbb{F}_p) : H]} = \sqrt{8}$ in our case of interest
- Is this satisfactory?
- Not completely: intuitively, we expect to have a similar equidistribution result over much shorter intervals (flipping only a few bits should suffice)
- However, character sum techniques seem to be fundamentally limited to square-root bounds

Consequence for our original problem

- By the previous theorem: a random fault on a little more than half the bits of the x-coordinates yields a point equidistributed among cosets
  - note $\sqrt{[E(\mathbb{F}_p) : H]} = \sqrt{8}$ in our case of interest
- Is this satisfactory?
- Not completely: intuitively, we expect to have a similar equidistribution result over much shorter intervals (flipping only a few bits should suffice)
- However, character sum techniques seem to be fundamentally limited to square-root bounds

Consequence for our original problem

- By the previous theorem: a random fault on a little more than half the bits of the x-coordinates yields a point equidistributed among cosets
  - note $\sqrt{[E(\mathbb{F}_p) : H]} = \sqrt{8}$ in our case of interest
- Is this satisfactory?
- Not completely: intuitively, we expect to have a similar equidistribution result over much shorter intervals (flipping only a few bits should suffice)
- However, character sum techniques seem to be fundamentally limited to square-root bounds

Consequence for our original problem

- By the previous theorem: a random fault on a little more than half the bits of the x-coordinates yields a point equidistributed among cosets
  - note $\sqrt{[E(\mathbb{F}_p) : H]} = \sqrt{8}$ in our case of interest
- Is this satisfactory?
- Not completely: intuitively, we expect to have a similar equidistribution result over much shorter intervals (flipping only a few bits should suffice)
- However, character sum techniques seem to be fundamentally limited to square-root bounds

Could the result be improved?

- Sometimes, bounds on very short intervals can be obtained using averaging techniques
- For example: consider a character sum on average over varying base fields, varying curves, etc.
- However, seems hard to apply to our setting: one would need a family of curves that all share a subgroup with the given structure
  - average over the corresponding modular curve?
  - the bound would at least need to grow with the genus of the curve...
- Even if such a result could be obtained, not clear it would be meaningful in practice
  - interested in a specific curve, not a randomly chosen curve in a family

Could the result be improved?

- Sometimes, bounds on very short intervals can be obtained using averaging techniques
- For example: consider a character sum on average over varying base fields, varying curves, etc.
- However, seems hard to apply to our setting: one would need a family of curves that all share a subgroup with the given structure
  - average over the corresponding modular curve?
  - the bound would at least need to grow with the genus of the curve...
- Even if such a result could be obtained, not clear it would be meaningful in practice
  - interested in a specific curve, not a randomly chosen curve in a family

Could the result be improved?

- Sometimes, bounds on very short intervals can be obtained using averaging techniques
- For example: consider a character sum on average over varying base fields, varying curves, etc.
- However, seems hard to apply to our setting: one would need a family of curves that all share a subgroup with the given structure
  - average over the corresponding modular curve?
  - the bound would at least need to grow with the genus of the curve...
- Even if such a result could be obtained, not clear it would be meaningful in practice
  - interested in a specific curve, not a randomly chosen curve in a family

Could the result be improved?

- Sometimes, bounds on very short intervals can be obtained using averaging techniques
- For example: consider a character sum on average over varying base fields, varying curves, etc.
- However, seems hard to apply to our setting: one would need a family of curves that all share a subgroup with the given structure
  - average over the corresponding modular curve?
  - the bound would at least need to grow with the genus of the curve...
- Even if such a result could be obtained, not clear it would be meaningful in practice
  - interested in a specific curve, not a randomly chosen curve in a family

Thank you!