Conjectural asymptotics for prime orders of points on elliptic curves over number fields

Michael Stoll
Universität Bayreuth

joint with Maarten Derickx

Representation Theory XVIII / Number Theory
Dubrovnik, June 19, 2023

The Problem

Goal.

Fix $d \geq 1$.
Determine the possible groups $E(K)_{\text{tors}}$
for elliptic curves E over a number field K of degree d!

The Problem

Goal.

Fix $d \geq 1$.
Determine the possible groups $E(K)_{\text{tors}}$
for elliptic curves E over a number field K of degree d!

The first step is to determine the prime divisors of $\#E(K)$.

Definition.

$$S(d) := \{p \text{ prime} \mid \exists \mathbb{Q} \subset K, [K:\mathbb{Q}] = d \; \exists E/K \text{ ell. curve } \exists P \in E(K): \text{ord}(P) = p\}$$

The Problem

Goal.

Fix $d \geq 1$.
Determine the possible groups $E(K)_{\text{tors}}$
for elliptic curves E over a number field K of degree d!

The first step is to determine the prime divisors of $\#E(K)$.

Definition.

$$S(d) := \{p \text{ prime} \mid \exists \mathbb{Q} \subset K, [K:\mathbb{Q}] = d \; \exists E/K \text{ ell. curve } \exists P \in E(K) \colon \text{ord}(P) = p\}$$

Merel: $S(d)$ is finite.

The Problem

Definition.

$$S(d) := \{p \text{ prime} \mid \exists \mathbb{Q} \subset K, [K : \mathbb{Q}] = d \; \exists E/K \text{ ell. curve } \exists P \in E(K) \colon \mathrm{ord}(P) = p\}$$

The Problem

Definition.

$$S(d) := \{p \text{ prime} \mid \exists \mathbb{Q} \subset K, [K:\mathbb{Q}] = d \ \exists E/K \text{ ell. curve } \exists P \in E(K)\colon \mathrm{ord}(P) = p\}$$

Problems.

❶ Determine $S(d)$ for small d!

The Problem

Definition.

$$S(d) := \{p \text{ prime} \mid \exists \mathbb{Q} \subset K, [K:\mathbb{Q}] = d\ \exists E/K \text{ ell. curve } \exists P \in E(K) \colon \operatorname{ord}(P) = p\}$$

Problems.

❶ Determine $S(d)$ for small d!

$S(1) = \{2, 3, 5, 7\}$	(Mazur)
$S(2) = \{2, 3, 5, 7, 11, 13\}$	(Kamienny)
$S(3) = \{2, 3, 5, 7, 11, 13\}$	(Parent)
$S(4) = \{2, 3, 5, 7, 11, 13, 17\}$	(DKSS)
$S(5) = \{2, 3, 5, 7, 11, 13, 17, 19\}$	(DKSS)
$S(6) = \{2, 3, 5, 7, 11, 13, 17, 19, \quad 37\}$	(DKSS)
$S(7) = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$	(DKSS)
$S(8) = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$	(DS, Khawaja)

The Problem

➊ Determine $S(d)$ for small d!

➋ Bound the elements of $S(d)$ for large d!

The Problem

❶ Determine $S(d)$ for small d!

❷ Bound the elements of $S(d)$ for large d!

We will focus on ❷ in this talk.

The Problem

❶ Determine $S(d)$ for small d!

❷ Bound the elements of $S(d)$ for large d!

We will focus on ❷ in this talk.

The best general result in this direction is due to Oesterlé:

$$\max S(d) \leq (3^{d/2}+1)^2 .$$

Relation With Rational Points

If $p \in S(d)$, then there is a number field K of degree d, an elliptic curve E over K and a point $P \in E(K)$ of order p.

Relation With Rational Points

If $p \in S(d)$, then there is a number field K of degree d, an elliptic curve E over K and a point $P \in E(K)$ of order p.

The pair (E, P) gives rise to a point $x \in X_1(p)(K)$ that is not a cusp.

Relation With Rational Points

If $p \in S(d)$, then there is a number field K of degree d,
an elliptic curve E over K and a point $P \in E(K)$ of order p.

The pair (E, P) gives rise to a point $x \in X_1(p)(K)$ that is not a cusp.

Then $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ is a $\mathbb{Q}$-rational effective divisor of degree d on $X_1(p)$.
Such divisors correspond to points on the dth symmetric power $X_1(p)^{(d)}$.

Relation With Rational Points

If $p \in S(d)$, then there is a number field K of degree d,
an elliptic curve E over K and a point $P \in E(K)$ of order p.

The pair (E, P) gives rise to a point $x \in X_1(p)(K)$ that is not a cusp.

Then $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ is a $\mathbb{Q}$-rational effective divisor of degree d on $X_1(p)$.
Such divisors correspond to points on the dth symmetric power $X_1(p)^{(d)}$.

So we obtain a rational point on $X_1(p)^{(d)}$
whose support does not contain a cusp.

Relation With Rational Points

If $p \in S(d)$, then there is a number field K of degree d,
an elliptic curve E over K and a point $P \in E(K)$ of order p.

The pair (E, P) gives rise to a point $x \in X_1(p)(K)$ that is not a cusp.

Then $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ is a $\mathbb{Q}$-rational effective divisor of degree d on $X_1(p)$.
Such divisors correspond to points on the dth symmetric power $X_1(p)^{(d)}$.

So we obtain a rational point on $X_1(p)^{(d)}$
whose support does not contain a cusp.

Conclusion.
If all rational points on $X_1(p)^{(d)}$ have cusps in their support,
then $p \notin S(d)$.

Gonality (1)

Definition.

Let X be a (nice) curve over K.
The K-gonality of X, $\mathrm{gon}_K(X)$, is the minimal degree of a non-constant function $f \in K(X)$.

Gonality (1)

Definition.

Let X be a (nice) curve over K.
The K-gonality of X, $\mathrm{gon}_K(X)$, is the minimal degree of a non-constant function $f \in K(X)$.

Fact.

If D_1 and D_2 are linearly equivalent effective K-rational divisors on X with $\deg D_1 = \deg D_2 < \mathrm{gon}_K(X)$, then $D_1 = D_2$.

Gonality (1)

Definition.

Let X be a (nice) curve over K.
The K-gonality of X, $\mathrm{gon}_K(X)$, is the minimal degree
of a non-constant function $f \in K(X)$.

Fact.

If D_1 and D_2 are linearly equivalent effective K-rational divisors on X
with $\deg D_1 = \deg D_2 < \mathrm{gon}_K(X)$, then $D_1 = D_2$.

Fact (Abramovich; Kim-Sarnak).

$$\mathrm{gon}_{\mathbb{Q}}\big(X_1(p)\big) \geq \frac{325}{2^{16}}(p^2 - 1) \qquad \text{for prime } p.$$

Gonality (2)

Fact.
When $g\big(X_1(p)\big) \geq 2$,

$$\mathrm{gon}_{\mathbb{Q}}\big(X_1(p)\big) \leq g\big(X_1(p)\big) \leq \frac{p^2-1}{24}.$$

Better (by a constant) asymptotic upper bounds are known.

Gonality (2)

Fact.
When $g\big(X_1(p)\big) \geq 2$,

$$\mathrm{gon}_{\mathbb{Q}}\big(X_1(p)\big) \leq g\big(X_1(p)\big) \leq \frac{p^2-1}{24}.$$

Better (by a constant) asymptotic upper bounds are known.

This implies that

$$\{p : p \text{ prime and } p \leq \sqrt{24d+1}\} \subset S(d)$$

and these prime orders occur in infinite families.

Gonality (2)

Fact.
When $g\big(X_1(p)\big) \geq 2$,

$$\mathrm{gon}_{\mathbb{Q}}\big(X_1(p)\big) \leq g\big(X_1(p)\big) \leq \frac{p^2-1}{24}.$$

Better (by a constant) asymptotic upper bounds are known.

This implies that

$$\{p : p \text{ prime and } p \leq \sqrt{24d+1}\} \subset S(d)$$

and these prime orders occur in infinite families.

Since $\mathrm{gon}_{\mathbb{Q}}\big(X_1(p)\big) \asymp p^2 - 1$,
this gives the asymptotics for non-sporadic points
up to a constant factor.

Hecke Correspondences

Fix a prime p and let $\ell \neq p$ be another prime.
Let $X_{1,0}(p, \ell)$ denote the modular curve
whose points classify triples (E, P, C)
with $P \in E$ a point of order p and $C \subset E$ a subgroup of order ℓ.

Hecke Correspondences

Fix a prime p and let $\ell \neq p$ be another prime.
Let $X_{1,0}(p,\ell)$ denote the modular curve
whose points classify triples (E, P, C)
with $P \in E$ a point of order p and $C \subset E$ a subgroup of order ℓ.

There are two degeneracy maps $\alpha, \beta \colon X_{1,0}(p,\ell) \to X_1(p)$
given by $\alpha \colon (E, P, C) \mapsto (E, P)$ and $\beta \colon (E, P, C) \mapsto (E/C, P + C)$.

Hecke Correspondences

Fix a prime p and let $\ell \neq p$ be another prime.
Let $X_{1,0}(p, \ell)$ denote the modular curve
whose points classify triples (E, P, C)
with $P \in E$ a point of order p and $C \subset E$ a subgroup of order ℓ.

There are two degeneracy maps $\alpha, \beta \colon X_{1,0}(p, \ell) \to X_1(p)$
given by $\alpha \colon (E, P, C) \mapsto (E, P)$ and $\beta \colon (E, P, C) \mapsto (E/C, P + C)$.

They induce the correspondence $T_\ell = \beta_* \circ \alpha^*$ on $X_1(p)$,
which gives an endomorphism T_ℓ of the divisor group $\operatorname{Div} X_1(p)$,
which in turn induces $T_\ell \in \operatorname{End} J_1(p)$.

Hecke Correspondences

Fix a prime p and let $\ell \neq p$ be another prime.
Let $X_{1,0}(p, \ell)$ denote the modular curve
whose points classify triples (E, P, C)
with $P \in E$ a point of order p and $C \subset E$ a subgroup of order ℓ.

There are two degeneracy maps $\alpha, \beta \colon X_{1,0}(p, \ell) \to X_1(p)$
given by $\alpha \colon (E, P, C) \mapsto (E, P)$ and $\beta \colon (E, P, C) \mapsto (E/C, P + C)$.

They induce the correspondence $T_\ell = \beta_* \circ \alpha^*$ on $X_1(p)$,
which gives an endomorphism T_ℓ of the divisor group $\operatorname{Div} X_1(p)$,
which in turn induces $T_\ell \in \operatorname{End} J_1(p)$.

On (non-cuspidal) points, it is given by

$$T_\ell(E, P) = \sum_{C \leq E, \#C = \ell} (E/C, P + C) \,.$$

Properties of the Hecke Correspondence

For each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have the diamond operator $\langle a \rangle$ of $X_1(p)$ given by $\langle a \rangle \colon (E, P) \mapsto (E, aP)$; it is an automorphism of $X_1(p) \to X_0(p)$.

Properties of the Hecke Correspondence

For each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have the diamond operator $\langle a \rangle$ of $X_1(p)$ given by $\langle a \rangle \colon (E, P) \mapsto (E, aP)$; it is an automorphism of $X_1(p) \to X_0(p)$.

Theorem. (D-S)

Let F be a monic polynomial whose coefficients are integral linear combinations of diamond operators.
Then the kernel of $F(T_\ell)$ on $\operatorname{Div} X_1(p)$ ($\ell \neq p$ primes) consists of divisors supported in cusps.

Properties of the Hecke Correspondence

For each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have the diamond operator $\langle a \rangle$ of $X_1(p)$ given by $\langle a \rangle \colon (E, P) \mapsto (E, aP)$; it is an automorphism of $X_1(p) \to X_0(p)$.

Theorem. (D-S)

Let F be a monic polynomial whose coefficients are integral linear combinations of diamond operators.
Then the kernel of $F(T_\ell)$ on $\operatorname{Div} X_1(p)$ ($\ell \neq p$ primes) consists of divisors supported in cusps.

Proposition (Eichler-Shimura).

Let $\ell \neq p$ be an odd prime.
Then $T_\ell - \ell\langle \ell \rangle - 1 \in \operatorname{End} J_1(p)$ kills $J_1(p)(\mathbb{Q})_{\text{tors}}$.

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.

If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.

If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}}$$

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\text{tors}} \overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\text{tors}}$$

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.

If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$\begin{aligned}(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}} &\overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}} \\ &\Longrightarrow (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)([x]) = 0\end{aligned}$$

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.

If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$\begin{aligned}
(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}} &\overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}} \\
&\Longrightarrow (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)([x]) = 0 \\
&\Longrightarrow (T_3\langle a \rangle + 3\langle 3 \rangle + 1)x \sim (T_3 + 3\langle 3a \rangle + \langle a \rangle)x
\end{aligned}$$

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion (†).
If $8d < \text{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$
\begin{aligned}
(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\text{tors}} &\overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\text{tors}} \\
&\Longrightarrow (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)([x]) = 0 \\
&\Longrightarrow (T_3\langle a \rangle + 3\langle 3 \rangle + 1)x \sim (T_3 + 3\langle 3a \rangle + \langle a \rangle)x \\
&\overset{8d < \text{gon}}{\Longrightarrow} \ (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)(x) = 0
\end{aligned}
$$

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion (†).
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$
\begin{aligned}
(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}} &\overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\mathrm{tors}} \\
&\Longrightarrow (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)([x]) = 0 \\
&\Longrightarrow (T_3\langle a \rangle + 3\langle 3 \rangle + 1)x \sim (T_3 + 3\langle 3a \rangle + \langle a \rangle)x \\
&\overset{8d < \mathrm{gon}}{\Longrightarrow} (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)(x) = 0 \\
&\Longrightarrow \langle a \rangle x - x \in \ker\big(T_3 - 3\langle 3 \rangle - 1 \mid \mathrm{Div}\, X_1(p)\big)
\end{aligned}
$$

A Global Criterion

Theorem. (D-S)
Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion (†).
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.
Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$
\begin{aligned}
(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\text{tors}} &\overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\text{tors}} \\
&\Longrightarrow (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)([x]) = 0 \\
&\Longrightarrow (T_3\langle a \rangle + 3\langle 3 \rangle + 1)x \sim (T_3 + 3\langle 3a \rangle + \langle a \rangle)x \\
&\overset{8d < \text{gon}}{\Longrightarrow} (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)(x) = 0 \\
&\Longrightarrow \langle a \rangle x - x \in \ker\big(T_3 - 3\langle 3 \rangle - 1 \mid \mathrm{Div}\, X_1(p)\big) \\
&\Longrightarrow \langle a \rangle x - x \text{ supported in cusps} \Longrightarrow \text{claim.}
\end{aligned}
$$

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion $(\dagger)$.
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Proof.

Fix a rational cusp c on $X_1(p)$ and consider $[x - d \cdot c] \in J_1(p)(\mathbb{Q})$.

$$\begin{aligned}
(\langle a \rangle - 1)([c]) \in J_1(p)(\mathbb{Q})_{\text{tors}} &\overset{(\dagger)}{\Longrightarrow} (\langle a \rangle - 1)([x]) \in J_1(p)(\mathbb{Q})_{\text{tors}} \\
&\Longrightarrow (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)([x]) = 0 \\
&\Longrightarrow (T_3\langle a \rangle + 3\langle 3 \rangle + 1)x \sim (T_3 + 3\langle 3a \rangle + \langle a \rangle)x \\
&\overset{8d < \text{gon}}{\Longrightarrow} (T_3 - 3\langle 3 \rangle - 1)(\langle a \rangle - 1)(x) = 0 \\
&\Longrightarrow \langle a \rangle x - x \in \ker\big(T_3 - 3\langle 3 \rangle - 1 \mid \operatorname{Div} X_1(p)\big) \\
&\Longrightarrow \langle a \rangle x - x \text{ supported in cusps} \Longrightarrow \text{claim.}
\end{aligned}$$

(In some cases, one can replace 8 by a smaller number.)

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion.

If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion.
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Corollary.

In the Theorem, assume x has no cusps in its support.

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.

Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion.

If $8d < \text{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Corollary.

In the Theorem, assume x has no cusps in its support.

If we can take a to generate $(\mathbb{Z}/p\mathbb{Z})^\times$,

then x is a sum of (set-theoretic) pull-backs of points on $X_0(p)$.

A Global Criterion

Theorem. (D-S)

Let $p \geq 5$ be a prime, $d \geq 1$, and $x \in X_1(p)^{(d)}(\mathbb{Q})$.
Let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ and assume that $(\langle a \rangle - 1)\big(J_1(p)(\mathbb{Q})\big)$ is torsion.
If $8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, then x is a sum of cusps plus a divisor fixed by $\langle a \rangle$.

Corollary.

In the Theorem, assume x has no cusps in its support.
If we can take a to generate $(\mathbb{Z}/p\mathbb{Z})^\times$,
then x is a sum of (set-theoretic) pull-backs of points on $X_0(p)$.

$p \equiv 1 \bmod 6$ and $j = 0$:	pull-backs have degree $(p-1)/6$.
$p \equiv 1 \bmod 4$ and $j = 1728$:	pull-backs have degree $(p-1)/4$.
Else:	pull-backs have degree $(p-1)/2$.

A Global Criterion

Corollary.

In the Theorem, assume x has no cusps in its support.

If we can take a to generate $(\mathbb{Z}/p\mathbb{Z})^{\times}$,

then x is a sum of (set-theoretic) pull-backs of points on $X_0(p)$.

$p \equiv 1 \bmod 6$ and $j = 0$:	pull-backs have degree $(p-1)/6$.
$p \equiv 1 \bmod 4$ and $j = 1728$:	pull-backs have degree $(p-1)/4$.
Else:	pull-backs have degree $(p-1)/2$.

A Global Criterion

Corollary.

In the Theorem, assume x has no cusps in its support.

If we can take a to generate $(\mathbb{Z}/p\mathbb{Z})^\times$,

then x is a sum of (set-theoretic) pull-backs of points on $X_0(p)$.

$p \equiv 1 \bmod 6$ and $j = 0$: pull-backs have degree $(p-1)/6$.

$p \equiv 1 \bmod 4$ and $j = 1728$: pull-backs have degree $(p-1)/4$.

Else: pull-backs have degree $(p-1)/2$.

Points on $X_0(p)$ with $j = 0$ or $j = 1728$ have degree ≥ 2.

$\rightsquigarrow$ $p = 3d+1$ for $j = 0$, $p = 2d+1$ for $j = 1728$ (d even)

A Global Criterion

Corollary.

In the Theorem, assume x has no cusps in its support.

If we can take a to generate $(\mathbb{Z}/p\mathbb{Z})^\times$,

then x is a sum of (set-theoretic) pull-backs of points on $X_0(p)$.

$p \equiv 1 \bmod 6$ and $j = 0$:	pull-backs have degree $(p-1)/6$.
$p \equiv 1 \bmod 4$ and $j = 1728$:	pull-backs have degree $(p-1)/4$.
Else:	pull-backs have degree $(p-1)/2$.

Points on $X_0(p)$ with $j = 0$ or $j = 1728$ have degree ≥ 2.

$\rightsquigarrow$ $p = 3d+1$ for $j = 0$, $p = 2d+1$ for $j = 1728$ (d even)

$8d < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$ holds when $p > \sqrt{\gamma d + 1}$ for some $\gamma > 0$.

If d is large, then $p \in S(d)$ implies (under the assumption on a)

that $p \leq 2d+1$, or else d is even and $p = 3d+1$.

Strange Primes

We say that a prime p is strange
if $(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ has positive rank for a generator a of $(\mathbb{Z}/p\mathbb{Z})^{\times}$
(i.e., the assumption on a does not hold.)

Strange Primes

We say that a prime p is strange
if $(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ has positive rank for a generator a of $(\mathbb{Z}/p\mathbb{Z})^\times$
(i.e., the assumption on a does not hold.)

We can split $J_1(p) \sim J_0(p) \times A_1 \times \cdots \times A_n$ up to isogeny
with simple abelian varieties $A_1, \ldots, A_n$ over $\mathbb{Q}$.
If a generates $(\mathbb{Z}/p\mathbb{Z})^\times$, then $(\langle a \rangle - 1)(J_1(p)) \sim A_1 \times \cdots \times A_n$.

Strange Primes

We say that a prime p is strange
if $(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ has positive rank for a generator a of $(\mathbb{Z}/p\mathbb{Z})^\times$
(i.e., the assumption on a does not hold.)

We can split $J_1(p) \sim J_0(p) \times A_1 \times \cdots \times A_n$ up to isogeny
with simple abelian varieties $A_1, \ldots, A_n$ over $\mathbb{Q}$.
If a generates $(\mathbb{Z}/p\mathbb{Z})^\times$, then $(\langle a \rangle - 1)(J_1(p)) \sim A_1 \times \cdots \times A_n$.

So p is strange iff $\operatorname{rk} A_j(\mathbb{Q}) > 0$ for some $1 \le j \le n$.

Strange Primes

We say that a prime p is strange
if $(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ has positive rank for a generator a of $(\mathbb{Z}/p\mathbb{Z})^\times$
(i.e., the assumption on a does not hold.)

We can split $J_1(p) \sim J_0(p) \times A_1 \times \cdots \times A_n$ up to isogeny
with simple abelian varieties $A_1, \ldots, A_n$ over $\mathbb{Q}$.
If a generates $(\mathbb{Z}/p\mathbb{Z})^\times$, then $(\langle a \rangle - 1)(J_1(p)) \sim A_1 \times \cdots \times A_n$.

So p is strange iff $\operatorname{rk} A_j(\mathbb{Q}) > 0$ for some $1 \leq j \leq n$.
By results of Kolyvagin-Logachëv and Kato, this implies that
there is a newform f of weight 2 for $\Gamma_1(p)$ with nontrivial character χ
such that $L(f, 1) = 0$.

Strange Primes

We say that a prime p is strange
if $(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ has positive rank for a generator a of $(\mathbb{Z}/p\mathbb{Z})^\times$
(i.e., the assumption on a does not hold.)

We can split $J_1(p) \sim J_0(p) \times A_1 \times \cdots \times A_n$ up to isogeny
with simple abelian varieties $A_1, \ldots, A_n$ over $\mathbb{Q}$.
If a generates $(\mathbb{Z}/p\mathbb{Z})^\times$, then $(\langle a \rangle - 1)(J_1(p)) \sim A_1 \times \cdots \times A_n$.

So p is strange iff $\operatorname{rk} A_j(\mathbb{Q}) > 0$ for some $1 \leq j \leq n$.
By results of Kolyvagin-Logachëv and Kato, this implies that
there is a newform f of weight 2 for $\Gamma_1(p)$ with nontrivial character χ
such that $L(f, 1) = 0$.
This can be checked by a computation with modular symbols.

Strange Primes

We say that a prime p is strange
if $(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ has positive rank for a generator a of $(\mathbb{Z}/p\mathbb{Z})^\times$
(i.e., the assumption on a does not hold.)

We can split $J_1(p) \sim J_0(p) \times A_1 \times \cdots \times A_n$ up to isogeny
with simple abelian varieties $A_1, \ldots, A_n$ over $\mathbb{Q}$.
If a generates $(\mathbb{Z}/p\mathbb{Z})^\times$, then $(\langle a \rangle - 1)(J_1(p)) \sim A_1 \times \cdots \times A_n$.

So p is strange iff $\operatorname{rk} A_j(\mathbb{Q}) > 0$ for some $1 \leq j \leq n$.
By results of Kolyvagin-Logachëv and Kato, this implies that
there is a newform f of weight 2 for $\Gamma_1(p)$ with nontrivial character χ
such that $L(f, 1) = 0$.
This can be checked by a computation with modular symbols.

Define $\mathrm{strdim}(p)$ to be the number of such "strange newforms" of level p.

Strange Primes Below 10^5

p	61	97	101	181	193	409	421	733	853	1021
ord(χ)	6	12	10	6	12	12	6	6	6	30
strdim(p)	2	4	4	2	4	4	2	2	2	8

p	1777	1801	1861	2377	2917	3229	3793	4201	4733	5441
ord(χ)	3	5	6	12	6	3	12	3	7	10
strdim(p)	2	4	6	4	2	2	4	2	6	4

p	5821	5953	6133	6781	7477	8681	8713	10093	11497	12941
ord(χ)	6	3	6	6	14	10	4, 12	6	3	10
strdim(p)	2	2	2	2	6	4	$4+4$	2	2	4

p	14533	15061	15289	17041	17053	17257	18199	20341	22093	23017
ord(χ)	6	6	12	3	6	12	3	6	6	12
strdim(p)	2	4	4	2	2	4	4	2	2	4

p	23593	26161	26177	28201	29569	31033	31657	32497	35521	35537
ord(χ)	12	3	4	3	2	3	3	3	3	4
strdim(p)	4	2	4	2	2	2	2	2	2	4

p	36373	39313	41081	41131	41593	42793	48733	52561	52691	53113
ord(χ)	6	12	5	3	12	3	6	3	5	12
strdim(p)	2	4	4	2	4	2	2	2	4	4

p	53857	63313	63901	65171	65449	66973	68737	69061	69401	69457
ord(χ)	12	12	6	5	12	6	12	6	5	4
strdim(p)	4	4	2	4	4	2	4	2	4	4

p	73009	86113	86161	96289						
ord(χ)	12	12	4	12						
strdim(p)	4	4	4	4						

A More General Statement

We can fix a bound s on $\mathrm{strdim}(\mathfrak{p})$.
Then our conclusions remain valid for sufficiently large d (depending on s) and all primes $\mathfrak{p}$ with $\mathrm{strdim}(\mathfrak{p}) \leq s$.

A More General Statement

We can fix a bound s on $\text{strdim}(p)$.

Then our conclusions remain valid for sufficiently large d (depending on s) and all primes p with $\text{strdim}(p) \leq s$.

Sketch of proof.

There is a monic polyomial F of degree $\text{strdim}(p)$
and with bounded (in terms of $\text{strdim}(p)$) coefficients
such that $F(T_2)(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ is torsion.

We can then run a similar argument as before.

A More General Statement

We can fix a bound s on $\mathrm{strdim}(p)$.
Then our conclusions remain valid for sufficiently large d (depending on s) and all primes p with $\mathrm{strdim}(p) \leq s$.

Sketch of proof.
There is a monic polyomial F of degree $\mathrm{strdim}(p)$ and with bounded (in terms of $\mathrm{strdim}(p)$) coefficients such that $F(T_2)(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ is torsion.

We can then run a similar argument as before.

Conjecture.

$\mathrm{strdim}(p)$ is uniformly bounded (or at least grows very slowly).

A More General Statement

We can fix a bound s on $\mathrm{strdim}(\mathfrak{p})$.
Then our conclusions remain valid for sufficiently large d (depending on s) and all primes $\mathfrak{p}$ with $\mathrm{strdim}(\mathfrak{p}) \leq s$.

Sketch of proof.
There is a monic polyomial F of degree $\mathrm{strdim}(\mathfrak{p})$ and with bounded (in terms of $\mathrm{strdim}(\mathfrak{p})$) coefficients such that $F(T_2)(\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ is torsion.

We can then run a similar argument as before.

Conjecture.

$\mathrm{strdim}(\mathfrak{p})$ is uniformly bounded (or at least grows very slowly).

This would imply $\max S(d) \leq 3d + 1$ for all sufficiently large d.

A Refined Result

A similar conjecture on the "even rank part" of $J_0(p)$:

Conjecture.

There is a uniform (or sufficiently slowly growing) bound for the number of newforms f of weight 2 for $\Gamma_0(p)$ (p prime) such that $w_p(f) = -f$ and $L(f, 1) = 0$.

A Refined Result

A similar conjecture on the "even rank part" of $J_0(p)$:

Conjecture.

There is a uniform (or sufficiently slowly growing) bound for the number of newforms f of weight 2 for $\Gamma_0(p)$ (p prime) such that $w_p(f) = -f$ and $L(f,1) = 0$.

Together, both conjectures imply:

There is $C > 0$ such that for d sufficiently large,

$$S(d) \subset \{p \le \sqrt{Cd} + 1\} \cup \begin{cases} \{\frac{2d}{m} + 1 : m \mid d, m = h\left(-\left\{\begin{smallmatrix} 1 \\ \text{or} \\ 4 \end{smallmatrix}\right\}\left(\frac{2d}{m} + 1\right)\right)\} & d \text{ odd}, \\ \{\frac{d}{m} + 1 : m \mid d\} \cup \{2d+1, 3d+1\} & d \text{ even}. \end{cases}$$

A Refined Result

A similar conjecture on the "even rank part" of $J_0(p)$:

Conjecture.

There is a uniform (or sufficiently slowly growing) bound for the number of newforms f of weight 2 for $\Gamma_0(p)$ (p prime) such that $w_p(f) = -f$ and $L(f, 1) = 0$.

Together, both conjectures imply:

There is $C > 0$ such that for d sufficiently large,

$$S(d) \subset \{p \le \sqrt{Cd+1}\} \cup \begin{cases} \{\frac{2d}{m}+1 : m \mid d, m = h\big(-\left\{\begin{smallmatrix}1\\ \text{or}\\ 4\end{smallmatrix}\right\}\left(\frac{2d}{m}+1\right)\big)\} & d \text{ odd}, \\ \{\frac{d}{m}+1 : m \mid d\} \cup \{2d+1, 3d+1\} & d \text{ even}. \end{cases}$$

In particular,

$$\limsup_{n\to\infty} \frac{\max S(2n)}{2n} = 3 \qquad \text{and} \qquad \limsup_{n\to\infty} \frac{\max S(2n+1)}{2n+1} = 0.$$

Thank You!