Torsion points on elliptic curves and gonalities of modular curves

The "Torsion points" part

Maarten Derickx

Mathematisch Instituut
Universiteit Leiden

Intercity Number Theory Seminar
28-09-2012

Mazurs torsion theorem

Theorem (Mazur)

If $E/\mathbb{Q}$ is an elliptic curve then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

- $\mathbb{Z}/N\mathbb{Z}$ *for* $1 \leq N \leq 10$ *or* $N = 12$
- $\mathbb{Z}/2N\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *for* $1 \leq N \leq 4$

Question Does a similar finite list also exist for other number fields?
Answer Yes, in fact something much stronger is true.

Uniform Boundednes Conjecture

Definition

A group G is an elliptic torsion group of degree $\leq d$ if $G \cong E(K)_{tors}$ for some elliptic curve E/K with $\mathbb{Q} \subseteq K$, $[K : \mathbb{Q}] \leq d$. The set of all isomorphism classes of such groups is denoted by $\phi(d)$.

Theorem (Uniform Boundednes Conjecture)

$\phi(d)$ is finite for all d.

Definition

A prime p is a torsion prime of degree $\leq d$ if $p \mid \#E(K)_{tors}$ for some elliptic curve E/K with $Q \subseteq K$ and $[K : \mathbb{Q}] \leq d$. The set of all torsion primes of degree $\leq d$ is denoted by $S(d)$.

What is known

$$S(d) := \{p \text{ prime} \mid \exists K/\mathbb{Q}\colon [K:\mathbb{Q}] \leq d,\ \exists E/K\colon E(K)[p] \neq 0\}$$

$$Primes(n) := \{p \text{ prime} \mid p \leq n\}$$

- $\phi(d)$ is finite $\Leftrightarrow$ $S(d)$ is finite.
- $S(d)$ is finite (Merel)
- $S(d) \subseteq Primes((3^{d/2}+1)^2)$ (Oesterlé) not published
- $S(1) = Primes(7)$ (Mazur)
- $S(2) = Primes(13)$ (Kamienny, Kenku, Momose)
- $S(3) = Primes(13)$ (Parent)
- $S(4) = Primes(17)$ (Kamienny, Stein, Stoll) to be published.

New results in my thesis

$$S(d) := \{p \text{ prime} \mid \exists K/\mathbb{Q} \colon [K : \mathbb{Q}] \le d,\ \exists E/K \colon E(K)\,[p] \ne 0\}$$

$$Primes(n) := \{p \text{ prime} \mid p \le n\}$$

- $S(5) \subseteq Primes(19) \cup \{29, 31, 41\}$
- $S(6) \subseteq Primes(41) \cup \{73\}$
- $S(7) \subseteq Primes(43) \cup \{59, 61, 67, 71, 73, 113, 127\}$

Note These results depend on Oesterlé's unpublished results.
In fact it is now known that $S(5) = Primes(19)$. This is joint work with Michael Stoll and it will be published together with the $S(4)$ result of Kamienny, Stein and Stoll. The joint work with Stoll uses the gonality computations in part 1 of my thesis.

Reduce to Multiplicative Reduction

Let $K/\mathbb{Q}$ with $[K:\mathbb{Q}] \leq d$. Let E/Kbe an elliptic curve, l a prime $m \subseteq O_K$ a max. ideal lying over l with res. field $\mathbb{F}_q$, $P \in E(K)$ of order p and $\overline{E}$ the fiber over $\mathbb{F}_q$ of the Weierstrass minimal model at l. If $p \nmid q$ and $\overline{P}$ is not a singular point then $\overline{P} \in \overline{E}(\mathbb{F}_q)$ has order p. Consider the three cases:

- **Good reduction:** $p \leq \#\overline{E}(\mathbb{F}_q) \leq (q^{\frac{1}{2}}+1)^2 \leq (l^{d/2}+1)^2$
- **Additive reduction:** $p \nmid q$ so $P \notin E^{sm}(K)$ hence $p \mid \#(E(K)/E^{sm}(K)) \leq 4 < (l^{d/2}+1)^2$
- **Non singular multiplicative reduction:** If $P \in E^{sm}(K)$ then $p \mid \#G_{m,\mathbb{F}_q}(\mathbb{F}_q) = q-1$ or $p \mid \#\tilde{G}_{m,\mathbb{F}_q}(\mathbb{F}_q) = q+1$

Conclusion: $(l^{d/2}+1)^2$ is a bound for the torsion order in all these cases.

What remains is the case where at all $(l) \subseteq m$ the curve E has multiplicative reduction and P reduces to the singular point.

The modular curve $Y_0(p)$

Over a field $K = \overline{K}$ the j-invariant gives a 1-1 correspondence:

$$j\colon \{E/K\}/_\sim \longleftrightarrow \mathbb{A}^1(K)$$

More general: There is a curve $Y_0(p)$ smooth of relative dimension 1 over $\mathbb{Z}[1/p]$ such that there is a 1-1 correspondence:

$$\psi\colon \{(E/K, C)\}/_\sim \longleftrightarrow Y_0(p)(K).$$

(Here C is a cyclic subgroup of E of order p.)
If $K \neq \overline{K}$ then there is still a map

$$\psi\colon \{(E/K, C)\}/_\sim \to Y_0(p)(K)$$

but this is not necessarily a 1-1 correspondance.
Over $\mathbb{C}$ we have $Y_0(p)(\mathbb{C}) \cong \mathbb{H}/\Gamma_0(p)$

The modular curve $X_0(p)$

Over $\mathbb{C}$ there is the compactification

$$Y_0(p)(\mathbb{C}) \cong \mathbb{H}/\Gamma_0(p) \subseteq \mathbb{H}^*/\Gamma_0(p)$$

In fact there is a projective curve smooth of relative dimension 1 over $\mathbb{Z}[1/p]$ such that $Y_0(p) \subseteq X_0(p)$ open. Moreover,

$$\#(X_0(p)(\mathbb{Z}[1/p]) \setminus Y_0(p)(\mathbb{Z}[1/p])) = 2.$$

These two elements are called the cusps, one is called 0 the other ∞ (these names come from the $\mathbb{C}$ valued points 0 and ∞ in $\mathbb{H}^*$).

Dealing with singular multiplicative reduction

This is an overview of how to deal with singular multiplicative reduction.

1. Suppose for contradiction that $\exists(E/K, P)$ s.t. $\forall m \subseteq 2\mathcal{O}_K$ the elliptic curve E has multiplicative reduction and $P_{\mathcal{O}_K/m}$ is singular.
2. Use $(E/K, P)$ to construct an $s \in X_0(p)(K)$ s.t. $s^{(d)} \neq \infty^{(d)}$ in $X_0(p)^{(d)}(\mathbb{Q})$ but $s^{(d)}_{\mathbb{F}_2} = \infty^{(d)}_{\mathbb{F}_2}$.
3. Construct a map $f\colon X_0(p)^{(d)} \to J_0(p)$ s.t. $f(s^{(d)}) = f(\infty^{(d)})$.
4. If f is a formal immersion $\infty^{(d)}_{\mathbb{F}_2}$ then $s^{(d)} = \infty^{(d)}$ giving a contradiction with 2 so $\nexists(E/K, P)$ as in 1.

I will now explain these steps in more detail.

Step 2

Let $x \in X_0(p)(K)$ and $\sigma_1, \ldots, \sigma_d$ be all embeddings of K in $\mathbb{C}$. Then

$$x^{(d)} := [(\sigma_1(x), \ldots, \sigma_d(x))] \in X_0(p)^{(d)}(\mathbb{Q}).$$

Let $s' = \psi(E/K, \langle P \rangle) \in Y_0(p)(K)$, with E/K and P as in Step 1. Then all specialisations of s' to characteristic 2 are the cusp 0, so $s'^{(d)}_{\mathbb{F}_2} = 0^{(d)}_{\mathbb{F}_2}$.
Define $s = W_p(s')$ then since $W_p(0) = \infty$ we have

$$s^{(d)}_{\mathbb{F}_2} = \infty^{(d)}_{\mathbb{F}_2}.$$

Since $s' \in Y_0(p)(K)$ also $s \in Y_0(p)(K)$ so for all i: $\sigma_i(s) \neq \infty$ and hence $s^{(d)} \neq \infty^{(d)}$.

Step 3

Proposition

Let $t_1, t_2 \in \mathbb{T} \subseteq \operatorname{End} J_0(p)$ *be Hecke operators such that* t_1 *factors via a Mordel-Weil rank* 0 *quotient of* $J_0(p)$ *and* t_2 *kills all* 2*-power torsion in* $J_0(p)(\mathbb{Q})$*. Let* $f : X_0(p)^{(d)} \to J_0(p)$ *be the canonical map normalized by* $f(\infty^{(d)}) = 0$ *then*

$$t_2 \circ t_1 \circ f(s^{(d)}) = 0 = t_2 \circ t_1 \circ f(\infty^{(d)}).$$

Proof.

By definition of t_1 we have that $t_1 \circ f(s^{(d)})$ is torsion. Since $s^{(d)}_{\mathbb{F}_2} = \infty^{(d)}_{\mathbb{F}_2}$ we have $t_1 \circ f(s^{(d)})_{\mathbb{F}_2} = t_1 \circ f(\infty^{(d)})_{\mathbb{F}_2} = 0$, hence $t_1 \circ f(s^{(d)})$ must be 2-power torsion giving $t_2 \circ t_1 \circ f(s^{(d)}) = 0$ □

Constructing t_2

Proposition

Let $q \neq p$ be primes. Then $T_q - q - 1(Q) = 0$ for all $Q \in J_0(p)(\mathbb{Q})$ of order coprime to q.

Proof.

$(T_q - q - 1)(Q)$ is also a point of order coprime to q. The Eichler-Shimura relation $T_{q,\mathbb{F}_q} = Frob_q + Ver_q$ together with the relation $Ver_q \circ Frob_q = q$ in End $J_0(p)_{\mathbb{F}_q}$ give:

$$T_{q,\mathbb{F}_q}(Q_{\mathbb{F}_q}) = Frob_q(Q_{\mathbb{F}_q} + Ver_q(Q_{\mathbb{F}_q}) = q + 1(Q_{\mathbb{F}_q})$$

so $T_{q,\mathbb{F}_q} - q - 1(Q_{\mathbb{F}_q}) = 0$, implying that the order of $T_q - q - 1(Q)$ is a power of q. Its order was asumed to also be coprime to q hence $T_q - q - 1(Q) = 0$. □

Constructing t_1

The winding quotient has rank 0

Definition (winding element)

The winding element $e \in H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$ is the element $\omega \mapsto \int_0^{i\infty} \omega \in H^0(X_0(p)(\mathbb{C}), \Omega^1)^\vee \cong H_1(X_0(p)(\mathbb{C}), \mathbb{R})$

Definition (winding quotient)

Let $A_e \subseteq \mathbb{T}$ be the annihilator of e then $J_e(p) = J_0(p)/A_e J_0(p)$ is called the winding quotient.

Proposition

$J_e(p)$ has rank zero.

This was proved by Parent using a result of Kolyvagin-Logachev.

Corollary

Let t_1 be such that $t_1 A_e = 0$ then $t_1 : J_0(p) \to J_0(p)$ factors via $J_e(p)$

Formal immersions

Definition

A morphism $f : X \to Y$ of noetherian schemes is a formal immersion at $x \in X$ if the following two equivalent conditions hold:

- $\widehat{f} : \widehat{O_{Y,f(x)}} \to \widehat{O_{X,x}}$ is surjective;
- $k(x) = k(f(x))$ and $f^* : \mathrm{Cot}_{f(x)}\, Y \to Cot_x X$ is surjective.

Proposition

Let $f : X \to Y$ be a formal immersion at a point $x \in X(k)$, let R be a d.v.r., m its maximal ideal and $k = R/m$. Suppose $P, Q \in X(R)$ are two points such that $x = P_k = Q_k$ and $f(P) = f(Q)$. Then $P = Q$.

Using this proposition with $R = \mathbb{Z}_{(2)}$, $X = X_0(p)^{(d)}$, $Y = J_0(p)$, $P = \infty^{(d)}$, $Q = s^{(d)}$ and $x = \infty_{\mathbb{F}_2}^{(d)}$ gives the contradiction in step 4.

Step 4: Kamienny's criterion

Parent's version translated to $X_0(p)$

Theorem (Kamienny's criterion)

Let $l \neq p$ be a prime and $f : X_0(p)^{(d)} \to J_0(p)$ be the canonical map normalized by $f(\infty^{(d)}) = 0$. Let $t \in \mathbb{T}$.
Then $t \circ f$ is a formal immersion at $\infty^{(d)}_{\mathbb{F}_l}$ if and only if

$$T_1 t, \ldots, T_d t$$

are $\mathbb{F}_l$ linearly independent in $\mathbb{T} \otimes \mathbb{F}_l$.

Corollary

Take $l = 2$. If the independence holds for a prime $p > (2^{d/2} + 1)^2$ and $t = t_2 t_1 \in \mathbb{T}$ with $t_1 A_e = 0$ and t_2 kills all 2-power torsion in $J_0(p)(\mathbb{Q})$. Then $p \notin S(d)$.

Kamienny's Criterion

Parent's original version

Theorem

Let $p > (2^{d/2}+1)^2$ *be prime. Let* $t = t_2 t_1 \in \mathbb{T}$ *with* $t_1 A_e = 0$ *and* t_2 *kills all 2-power torsion in* $J_1(p)(\mathbb{Q})$*. Suppose that for all partitions* $\sum_{i=0}^{m} n_i = d$ *and all* $1 = d_0 \leq d_1, \ldots, d_m \leq \frac{p-1}{2}$ *pairwise distinct:*

$$(t\langle d_i\rangle T_j)_{\substack{i\in 0,\ldots,k \\ j\in 1,\ldots,n_i}}$$

are $\mathbb{F}_l$ *linearly independent in* $\mathbb{T}\otimes\mathbb{F}_l$*.*
Then $p \notin S(d)$*.*

Comparison

Criterion for $X_1(p)$ is more powerful but is expensive to verify

- Advantage $X_1(p)$ over $X_0(p)$: Higher chance of success
- Disadvantage $X_1(p)$ over $X_0(p)$: Much slower
  1. Hecke matrices of size $(p-5)(p-7)/24$ vs. $p/12$
  2. partition $d = 1 + \ldots + 1$ already gives $\binom{(p-3)/2}{d-1}$ dependency's to check instead of 1.

Luckily 2 can be worked around since t.f.a.e:

- $t\langle d_0\rangle, t\langle d_1\rangle, \ldots t\langle d_d\rangle$ are linearly independent for all $1 = d_0 \leq d_1, \ldots, d_m \leq \frac{p-1}{2}$ pairwise distinct.
- The smallest dependency between $t\langle 1\rangle, t\langle 2\rangle, \ldots t\langle \frac{p-1}{2}\rangle$ is of weight $> d$

Similar things can be done for other partitions.

Result of testing the criterion

d	5	6	7
$(2^{d/2}+1)^2$	$44.3\ldots$	81	$151.6\ldots$
$(3^{d/2}+1)^2$	$275.1\ldots$	784	$2281.5\ldots$

$p = 271$ using $X_1(p)$ in sage takes about 12h and 21GB.
I used $X_0(p)$ to show $S(d) \subseteq Primes(193)$ for $d = 5, 6, 7$
After that I used $X_1(p)$ to show $S(d) \subseteq Primes((2^{d/2}+1)^2)$ for $d = 5, 6, 7$.
The criterion is also satisfied for some $p \leq (2^{d/2}+1)^2$. The condition $p > (2^{d/2}+1)^2$ in Kamienny's criterion comes from good reduction. So we can improve the results by looking at good reduction.

Elliptic curves over $\mathbb{F}_{2^d}$

Let $E/\mathbb{F}_{2^d}$ be an elliptic curve. Consider the two cases:

1. $j(E) \neq 0$ then it can be shown that E has a point of order 2
2. $j(E) = 0$.

In case (1) we see that $\frac{1}{2}(2^{d/2} + 1)^2$ bounds the torsion of prime order. In case (2) E is super singular so there will be very few possibilities for E.The numbers of rational points over $\mathbb{F}_{2^d}$ are well known for such E. This gives:

d	$S(d) \subseteq$	$(2^{(d/2)} + 1)^2$
5	$Primes(19) \cup \{29, 31, 41\}$	$44.3\ldots$
6	$Primes(41) \cup \{73\}$	$81.0\ldots$
7	$Primes(43) \cup \{59, 61, 67, 71, 73, 113, 127\}$	$151.6\ldots$

Summary

Michael Stoll has a strategy for showing $29, 31, 41 \notin S(5)$

- $S(5) = Primes(19)$ (was $\subseteq Primes(271)$)
- $S(6) \subseteq Primes(41) \cup \{73\}$ (was $\subseteq Primes(773)$)
- $S(7) \subseteq Primes(127)$ (was $\subseteq Primes(2281)$)

Work in progress:
Applying Michael Stoll his strategy to $S(6)$ I am close to proving:

$$Primes(19) \cup \{37\} \subseteq S(6) \subseteq Primes(19) \cup \{37, \mathbf{73}\}$$