

work with ^{S.}Kamienny & W. Stein.

Michael Stoll, Oldenburg, 2010/11/19.

Torsion points on ell. curves / number fields, quartic.

Motivation. Let E/k be an ell. curve, $\mathbb{Q} \rightarrow k$ finite. Then $E(k)_{tors}$ is finite. Question: which finite groups arise ?? Say, for k of degree $\leq d$. Are there only finitely many ??

What is known.

$d=1$: $k = \mathbb{Q}$. conjecture by Lersi, Ogg, proved by Mazur: only $\mathbb{Z}/n\mathbb{Z}$ $n \leq 12$ $n \neq 11$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n \leq 4$. Each occurs infinitely many j -invariants.

$d=2$. Kamienny: universal bound. & Kenku-Mumose, Kamienny-Mazur: $\mathbb{Z}/n\mathbb{Z}$, $n \leq 18$ $n \neq 17$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n \leq 6$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ $n \leq 2$, and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$; all occur for ∞ many j -invariants.

General d : Merel (1996) universal bound (Kamienny-Mazur: $d \leq 8$ For $d > 2$: no list of possible groups known, Abramovich: $d \leq 11$).

but for $d=3, 4$: known which groups occur infin. often.

$d=3$ (Jeon, Kim, Schweizer 2004): $\mathbb{Z}/n\mathbb{Z}$ $n \leq 20$ $n \notin \{17, 19\}$
 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$: $n \leq 7$.

$d=4$ (Jeon, Kim, Park 2006): $\mathbb{Z}/n\mathbb{Z}$, $n \leq 24$ $n \notin \{19, 23\}$
 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$: $n \leq 9$
 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ $n \leq 3$
 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ $n \leq 2$, $(\mathbb{Z}/5\mathbb{Z})^2, (\mathbb{Z}/6\mathbb{Z})^2$.

Now about the proof of a univ. bound

Key step: bound the primes that can occur.

Def. $S(d) := \{ p \text{ prime} \mid \exists E/k, P \in E(k) : \mathbb{Q} \rightarrow k \text{ degree } \leq d, \# \text{order}(P) = 1. \}$

Eg. $S(1) = \{2, 3, 5, 7\}$

$S(2) = \{2, 3, 5, 7, 11, 13\}$

$S(3) = \{2, 3, 5, 7, 11, 13\}$ (Parent)

$S(4) = ??$ Today's subject. $S(4) \supset \{2, 3, 5, 7, 11, 13, 17\}$.

Guess: = . So, must exclude all $p > 17$.

The first general bound is due to Merel: $\max S(d) \leq d^{3d^2}$. (2^{96} for $d=4$)

Oesterle: $\max(S(d)) \leq (3^{d/2} + 1)^2$ (100 for $d=4$).

Rough sketch of idea of proof of this:

$X_1(p)$, $X_1(p)^{(d)}$ det. symm. power.

$X_1(p)^{(d)} \rightarrow J_1(p) \rightarrow A$ use the largest one possible.

(winding quotient, $A(\mathbb{Q})$ ~~not~~ finite.
a formal immersion at the cusps over l ($l \neq p$), $l=2$

Kamisky & Stein (after Parent) have an explicit computational criterion for testing this. (check lin. indep. of a bunch of tuples in some Hecke algebra / \mathbb{F}_2 .)

They did this computation and were able to rule out all $p \geq 37$.

Hence: $S(n) \subset \{2, 3, 5, 7, 11, \dots, 31\}$. To do: exclude 31, 29, 23, 19.

This was the situation in May 2000. Then Michael started on this.

(if $p \geq 2$)

Let $C \subset X_1(p)$ be the set of rat'l cusp. ($\#C = p-1$).

If $d < p-1$ then $X_1(p)^{(d)}(\mathbb{Q}) = C^{(d)} \iff p \notin S(d)$. (clear)

(other cusps / $\mathbb{Q}(\mu_p)^+$ / orbit)

Proposition. X/\mathbb{Q} curve, embedded into its Jacobian J using $P_0 \in X(\mathbb{Q})$, l prime of good reduction, $d \in \mathbb{Z}_{>0}$.

Assume: 1. $J(\mathbb{Q})$ is finite.

2. if $l=2$: then $J(\mathbb{Q})[2] \hookrightarrow J(\mathbb{F}_2)$.

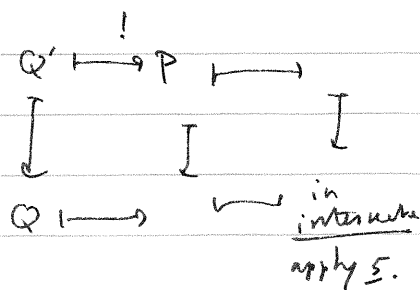
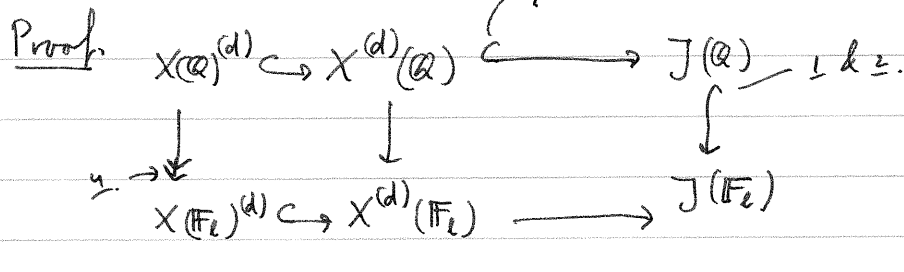
3. $\nexists X \rightarrow \mathbb{P}^1$ of degree $\leq d$.

4. $X(\mathbb{Q}) \twoheadrightarrow X(\mathbb{F}_l)$

5. the images of $X^{(d)}(\mathbb{F}_l)$ and of $J(\mathbb{Q})$ in $J(\mathbb{F}_l)$ meet only in the image of $X(\mathbb{F}_l)^{(d)}$.

Then $X^{(d)}(\mathbb{Q}) = X(\mathbb{Q})^{(d)}$, so the only pts. of degree $\leq d$ are rat. pts.

(by 3.: $X^{(d)} \rightarrow J$)



① $J_1(\mathbb{Q})$ finite for $p \leq 31$ (Conrad, Edixhoven, Stein). ③ satisfied for $d=4$ & $p \geq 19$. (gonality).

Application. $19 \nmid 23$: $\# J_1(p)(\mathbb{Q})$ is odd. Hence \underline{z} is o.k. \underline{z} .

\underline{y} is satisfied ($l=2$) by Hase-Weil

Σ . $X_1(p)^{(9)}(\mathbb{F}_2) = X_1(p)(\mathbb{F}_2)^{(9)}$ bec. there are no E/\mathbb{F}_6 with p points.

$p=31$. $\# J_1(31)(\mathbb{Q})$ is even, but can check that ② holds. ^{cuspidal,}

\underline{y} & \underline{z} are again true from H-W.

$p=29$. $\# J_1(p)(\mathbb{Q})$ is even, and z -gonion is not known. Hence \underline{z} cannot

be verified. So, use larger l .

try it!

\underline{z} holds for $l=11$. (assuming worst case for $J_1(29)(\mathbb{Q})$.)