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, $\mathbb{Q} \to k$ finite. Then $E(k)_{\mathrm{tors}}$ is finite. **Question:** which finite groups arise?? Say, for k of degree $\le d$. Are there only finitely many??

What is known.

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

$d=2$. Kamienny: universal bound. Kenku-Momose, Kamienny-Mazur: $\mathbb{Z}/n\mathbb{Z}$, $n \le 18$ $n \neq 17$; $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n \le 6$; $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$ $n \le 2$, 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: $d \le 8$ Abramovich: $d \le 14$).
For $d > 2$: no list of possible groups known, but for $d = 3, 4$: known which groups occur infin. often.

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

$d=4$ (Jeon, Kim, Park 2006): $\mathbb{Z}/n\mathbb{Z}$, $n \le 24$ $n \notin \{19, 23\}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$: $n \le 9$
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$ $n \le 3$
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}$ $n \le 2$, $(\mathbb{Z}/5\mathbb{Z})^2$, $(\mathbb{Z}/10\mathbb{Z})^2$.

Now about the proof of a univ. bound

Key step: bound the primes that can occur.

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

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. $S(4) \supseteq \{2, 3, 5, 7, 11, 13, 17\}$.

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

The first general bound is due to Merel: $\max S(d) \le d^{3d^2}$. (2^{96} for $d=4$)
Oesterlé: $\max(S(d)) \le (3^{d/2}+1)^2$ (100 for $d=4$).

Rough sketch of idea of proof of this:

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

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

winding quotient, $A(\mathbb{Q})$ finite.

a formal immersion at the cusps over ℓ ($\ell \neq p$). $\ell = 2$

Kamienny & 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: $S(4) \subset \{2,3,5,7,11,\dots,31\}$. To do: exclude 31, 29, 23, 19.

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

Let $C \subset X_1(p)$ be the set of rat'l cusps. ($\#C = \frac{p-1}{2}$ (if $p>2$)).

If $d < \frac{p-1}{2}$ then $X_1(p)^{(d)}(\mathbb{Q}) = C^{(d)} \iff p \notin S(d)$. (clear)

(other cusps / $\mathbb{Q}(\zeta_p)^+$ / 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 $\ell = 2$: then $J(\mathbb{Q})[2] \hookrightarrow J(\mathbb{F}_2)$.
3. $\nexists\ X \twoheadrightarrow \mathbb{P}^1$ of degree $\leq d$.
4. $X(\mathbb{Q}) \twoheadrightarrow X(\mathbb{F}_\ell)$
5. the images of $X^{(d)}(\mathbb{F}_\ell)$ and of $J(\mathbb{Q})$ in $J(\mathbb{F}_\ell)$ meet only in the image of $X(\mathbb{F}_\ell)^{(d)}$.

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

Proof.

$$\begin{array}{ccccc} X(\mathbb{Q})^{(d)} & \hookrightarrow & X^{(d)}(\mathbb{Q}) & \xhookrightarrow{\text{(by 3.: } X^{(d)} \hookrightarrow J\text{)}} & J(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X(\mathbb{F}_\ell)^{(d)} & \hookrightarrow & X^{(d)}(\mathbb{F}_\ell) & \longrightarrow & J(\mathbb{F}_\ell) \end{array}$$

4. $\twoheadrightarrow$; $\ell \neq 2$.

$$\begin{array}{ccccc} Q' & \overset{!}{\longmapsto} & P & \longmapsto & \\ \downarrow & & \downarrow & & \downarrow \\ Q & \longmapsto & & \hookrightarrow & \text{in intersection} \end{array}$$

apply 5.

∎

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

Application. $19 \le k \le 23$: $\#J_1(p)(\mathbb{Q})$ is odd. Hence 2 is o.k. 2.

4. is satisfied ($l=2$) by Hasse-Weil

5. $X_1(p)^{(4)}(\mathbb{F}_2) = X_1(p)(\mathbb{F}_{2^4})^{(4)}$ bec. there are no $E/\mathbb{F}_{16}$ with p points.

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

4 & 5 are again true from H-W.

$p=29$. $\#J_1(p)(\mathbb{Q})$ is even, and 2-torsion is not known. Hence 2 cannot be verified. So, use larger l.

(try it!)

5 holds for $l=11$. (assuming worst case for $J_1(29)(\mathbb{Q}^{ab})(2)$.)