

Torsion Points on Elliptic Curves

Torsion Points on Elliptic Curves over Quartic Fields

William Stein

(this is joint work with Sheldon Kamienny)

University of Washington

May 2010



Motivating Problem

Let K be a number field.

Theorem (Mordell-Weil): If E is an elliptic curve over K , then $E(K)$ is a finitely generated abelian group.

Thus $E(K)_{\text{tor}}$ is a finite group.

Problem: Which finite abelian groups $E(K)_{\text{tor}}$ occur, as we vary over all elliptic curves E/K ?

Observation: $E(K)_{\text{tor}}$ is a finite subgroup of \mathbf{C}/Λ , so $E(K)_{\text{tor}}$ is cyclic or a product of two cyclic groups.

An Old Conjecture

Conjecture (Levi around 1908; re-made by Ogg in 1960s):

When $K = \mathbf{Q}$, the groups $E(\mathbf{Q})_{\text{tor}}$ as we vary over all E/\mathbf{Q} , are the following 15 groups:

$$\mathbf{Z}/m\mathbf{Z} \quad \text{for } m \leq 10 \text{ or } m = 12$$

$$(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2v\mathbf{Z}) \text{ for } v \leq 4.$$

Note:

1. This is really a conjecture about **rational points on certain curves of (possibly) higher genus**
2. Or, it's a conjecture in **arithmetic dynamics** about **periodic points**.

Modular Curves

The modular curves $Y_0(N)$ and $Y_1(N)$:

- Let $Y_0(N)$ be the affine **modular curve** over \mathbf{Q} whose points parameterize isomorphism classes of pairs (E, C) , where $C \subset E$ is a *cyclic subgroup* of order N .
- Let $Y_1(N)$ be ... of pairs (E, P) , where $P \in E(\overline{\mathbf{Q}})$ is a *point* of order N .

Let $X_0(N)$ and $X_1(N)$ be the compactifications of the above affine curves.

Observation: There is an elliptic curve E/K with $p \mid \#E(K)_{\text{tor}}$ if and only if $Y_1(p)(K)$ is nonempty.

Also, $Y_0(N)$ is a quotient of $Y_1(N)$, so if $Y_0(N)(K)$ is empty, then so is $Y_1(N)$.

Mazur's Theorem (1970s)

Theorem (Mazur) If $p \mid \#E(\mathbf{Q})_{\text{tor}}$ for some elliptic curve E/\mathbf{Q} , then $p \leq 13$

Combined with previous work of Kubert and Ogg, one sees that Mazur's theorem implies Levi's conjecture, i.e., a complete classification of the finite groups $E(\mathbf{Q})_{\text{tor}}$

Here are representative curves by the way (there are infinitely many for each j -invariant):

```
for ainvs in ([0,-2],[0,8],[0,4],[4,0],[0,-1,-1,0,0],[0,1],
             [1,-1,1,-3,3],[7,0,0,16,0],[1,-1,1,-14,29],
             [1,0,0,-45,81],[1,-1,1,-122,1721],[-4,0],
             [1,-5,-5,0,0],[5,-3,-6,0,0],[17,-60,-120,0,0]):
    E = EllipticCurve(ainvs)
    view((E.torsion_subgroup().invariants(), E))
```

- $([], y^2 = x^3 - 2)$
- $([2], y^2 = x^3 + 8)$
- $([3], y^2 = x^3 + 4)$
- $([4], y^2 = x^3 + 4x)$
- $([5], y^2 - y = x^3 - x^2)$
- $([6], y^2 = x^3 + 1)$
- $([7], y^2 + xy + y = x^3 - x^2 - 3x + 3)$
- $([8], y^2 + 7xy = x^3 + 16x)$
- $([9], y^2 + xy + y = x^3 - x^2 - 14x + 29)$
- $([10], y^2 + xy = x^3 - 45x + 81)$
- $([12], y^2 + xy + y = x^3 - x^2 - 122x + 1721)$
- $([2, 2], y^2 = x^3 - 4x)$
- $([4, 2], y^2 + xy - 5y = x^3 - 5x^2)$
- $([6, 2], y^2 + 5xy - 6y = x^3 - 3x^2)$
- $([8, 2], y^2 + 17xy - 120y = x^3 - 60x^2)$

Mazur's Method

Theorem (Mazur) If $p \mid \#E(\mathbf{Q})_{\text{tor}}$ for some elliptic curve E/\mathbf{Q} , then $p \leq 13$

Basic idea of the proof:

1. Find a rank zero quotient A of $J_0(p)$ such that...
2. ... the induced map $f : X_0(p) \rightarrow A$ is a formal immersion at infinity (this means that the induced map on complete local rings is surjective).
3. Then consider the point $x \in Y_0(p)$ corresponding to a pair $(E, \langle P \rangle)$, where P has order p .
4. If E has potentially good reduction at 3 , get contradiction by injecting p -torsion mod 3 since $p > 13$, so E has multiplicative reduction. We may thus assume x reduces to the cusp ∞ .
5. The image of x in $A(\mathbf{Q})$ is thus in the kernel of the reduction map mod 3 . But this kernel of reduction is a formal group, hence torsion free. But $A(\mathbf{Q}) = A(\mathbf{Q})_{\text{tor}}$ is finite, so image of x is 0 .
6. Use that f is a formal immersion at infinity along with step 5, to show that $x = \infty$, which is a contradiction since $x \in Y_0(p)$.

Mazur uses for A the *Eisenstein quotient* of $J_0(p)$ because he is able to prove -- way back in the 1970s! -- that this quotient has rank 0 by doing a q -descent, for primes q that divide the numerator of $(p - 1)/24$. This is long before much was known toward the BSD conjecture. More recently one can:

- **Merel 1995**: use the bigger *winding quotient* of $J_0(p)$, which is the maximal *analytic* rank 0 quotient. This makes the arguments easier, and we know by Kolyvagin-Logachev et al. or by Kato that the winding quotient has rank 0. (For $p = 67$ the winding and Eisenstein quotients already differ, since $67a$ has trivial torsion and rank 0.)
- **Parent 1999**: use instead the winding quotient of $J_1(p)$, which leads to a similar argument as above. This quotient has rank 0 by Kato's theorem.



Kamienny-Mazur

A prime p is a **torsion prime for degree d** if there is a number field K of degree d and an elliptic curve E/K such that $p \mid \#E(K)_{\text{tor}}$

Let $S(d) = \{\text{torsion primes for degree } \leq d\}$

For example, $S(1) = \{2, 3, 5, 7\}$

Finding all possible torsion structure over all fields of degree $\leq d$ often involves determining $S(d)$, then doing some additional work (which we won't go into). E.g.,

Theorem (Frey, Faltings): If $S(d)$ is finite, then the set of groups $E(K)_{\text{tor}}$ as E varies over all elliptic curves over all number fields K of degree $\leq d$, is finite.

Kamienny and Mazur: Replace $X_0(p)$ by the symmetric power $X_0(p)^{(d)}$ and gave an explicit criterion in terms of independence of Hecke operators (or q -expansions of modular forms) for $f_d : X_0(p)^{(d)}$ to be a formal immersion at $(\infty, \infty, \dots, \infty)$. A point $y \in X_0(p)(K)$ where K has degree d , then defines a point $\tilde{y} \in X_0(p)^{(d)}(\mathbf{Q})$, etc.

Theorem (Kamienny and Mazur):

- $S(2) = \{2, 3, 5, 7, 11, 13\}$
- $S(d)$ is finite for $d \leq 8$,
- $S(d)$ has density 0 for all d .

Abromovich soon proved that $S(d)$ is finite for $d \leq 14$

Corollary (Uniform Boundedness): There is a fixed constant B such that if E/K is an elliptic curve over a number field of degree ≤ 8 , then $\#E(K)_{\text{tor}} \leq B$

(Very surprising!)

Torsion Structures over Quadratic Fields

Theorem (Kenku, Momose, Kamienny, Mazur): The complete list of subgroups that appear over quadratic fields is:

$$\begin{array}{ll} \mathbf{Z}/m\mathbf{Z} & \text{for } m \leq 16 \text{ or } m = 18 \\ (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2v\mathbf{Z}) & \text{for } v \leq 6. \\ (\mathbf{Z}/3\mathbf{Z}) \times (\mathbf{Z}/3v\mathbf{Z}) & \text{for } v = 1, 2 \\ (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/4v\mathbf{Z}) & \end{array}$$

and each occurs for infinitely many j -invariants.

What is $S(d)$?

Kamienny, Mazur: "We expect that $\max(S(3)) \leq 19$ but it would simply be too embarrassing to parade the actual astronomical finite bound that our proof gives."

But soon, Merel in a *tour de force*, proves (by using the winding quotient and a deep modular symbols

argument about independence of Hecke operators):

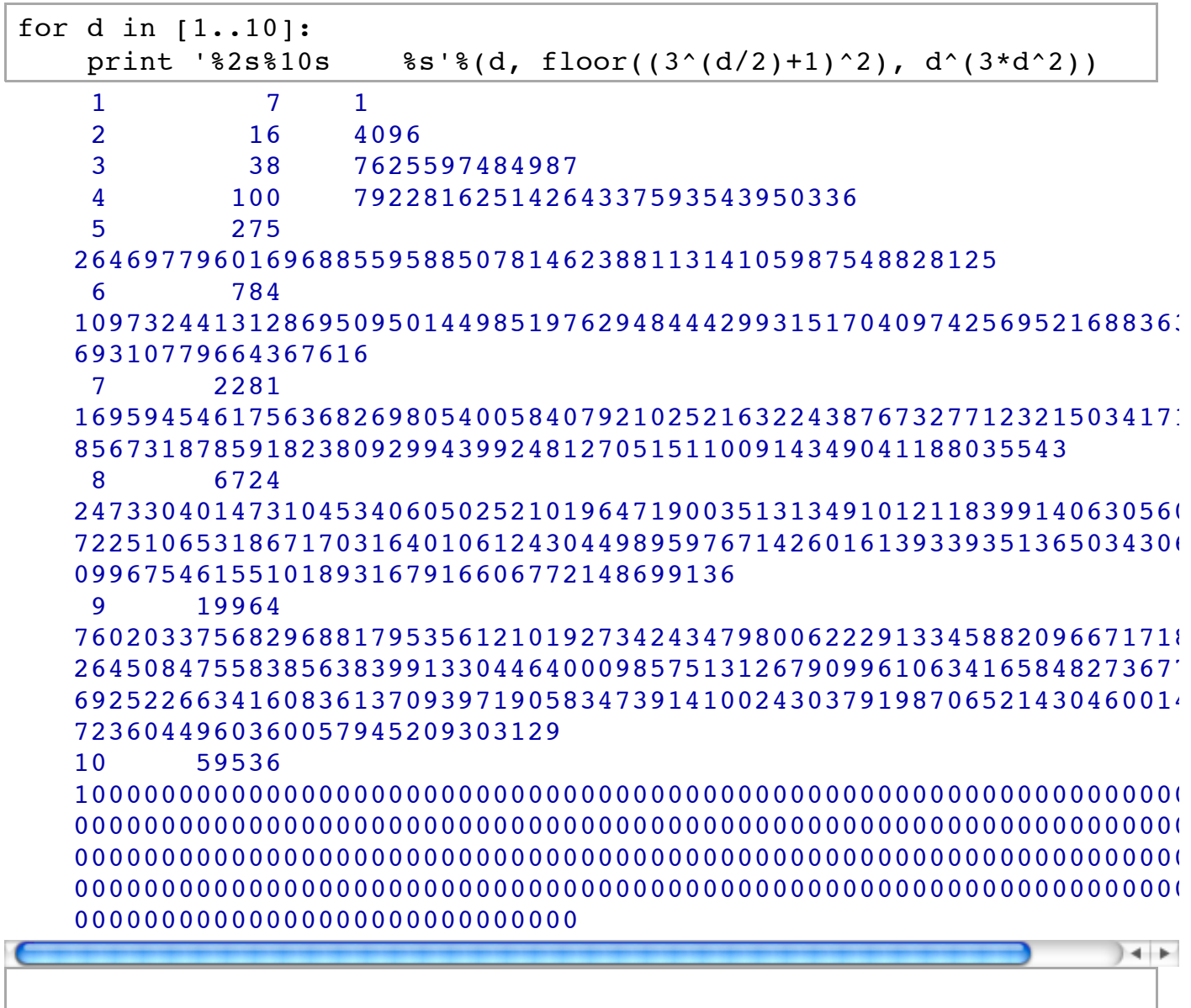
Theorem (Merel, 1996): $\max(S(d)) < d^{3d^2}$, for $d \geq 2$.

thus proving the full Universal Boundedness Conjecture, which is a huge result.

Shortly thereafter Oesterle modifies Merel's argument to get a much better upper bound:

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

```
for d in [1..10]:
  print '%2s%10s      %s'%(d, floor((3^(d/2)+1)^2), d^(3*d^2))
1          7          1
2          16         4096
3          38         7625597484987
4          100        79228162514264337593543950336
5          275
26469779601696885595885078146238811314105987548828125
6          784
109732441312869509501449851976294844429931517040974256952168836:
69310779664367616
7          2281
169594546175636826980540058407921025216322438767327712321503417:
856731878591823809299439924812705151100914349041188035543
8          6724
247330401473104534060502521019647190035131349101211839914063056:
722510653186717031640106124304498959767142601613933935136503430:
09967546155101893167916606772148699136
9          19964
760203375682968817953561210192734243479800622291334588209667171:
264508475583856383991330446400098575131267909961063416584827367:
692522663416083613709397190583473914100243037919870652143046001:
7236044960360057945209303129
10         59536
100000000000000000000000000000000000000000000000000000000000000:
000000000000000000000000000000000000000000000000000000000000000:
000000000000000000000000000000000000000000000000000000000000000:
000000000000000000000000000000000000000000000000000000000000000:
000000000000000000000000000000000000000000000000000000000000000:
000000000000000000000000000000000000000000000000000000000000000
```



Remark (Merel, personal communication, 2010-05-10)

- 1. The known bounds for $S(d)$ are exponential in d . However, a polynomial bound on $S(d)$ in d is expected. Therefore, one can not expect to computationally determine the exact list of torsion primes in degree for many more d 's.

2. The bound is obtained by considering (essentially) two cases (according to the type of reduction modulo ℓ of your elliptic curve) : in one case it is easily seen to be exponential in d , the hard case finally yields a bound which is polynomial in d (something like $O(d^8)$ in my paper, $O(d^6)$ after Oesterlé, I suspect one can lower it to $O(d^2)$). Unsatisfying!
3. If you want a bound depending on the field K (instead of just the degree of K), you can obtain a bound like $O(\text{size of the residue field of } K \text{ of smallest order})$.



Parent's Kamienny Method: Nailing Down $S(3)$

By Oesterle, we know that $\max(S(3)) \leq 37$

In 1999, **Parent** made Kamienny's method applied to $J_1(p)$ explicit and computable, and used this to bound $S(3)$ explicitly, showing that $\max(S(3)) \leq 17$. This makes crucial use of Kato's theorem toward the Birch and Swinnerton-Dyer conjecture!

In subsequent work, Parent rules out 17 finally giving the answer:

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

The list of groups $E(K)_{\text{tor}}$ that occur for K cubic is still *unknown*. However, using the notion of *trigonality* of modular curves (having a degree 3 map to P^1), [Jeon, Kim, and Schweizer, 2004] showed that the groups that appear for infinitely many j -invariants are:

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{for } m \leq 16, 18, 20 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^v\mathbb{Z} & \text{for } v \leq 7 \end{array}$$

Remark: Parent also gave an explicit bound for the torsion of order powers of prime numbers in his thesis...



What about Degree 4?

By Oesterle, we know that $\max(S(4)) \leq 97$

Recently, Jeon, Kim, and Park (2006), again used gonality (and big computations with Singular), to show that the groups that appear for infinitely many j -invariants for curves over quartic fields are:

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{for } m \leq 18, \text{ or } m=20, m=21, m=22, m=24 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^v\mathbb{Z} & \text{for } v \leq 9 \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^v\mathbb{Z} & \text{for } v \leq 3 \end{array}$$

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4v\mathbb{Z}$ for $v \leq 2$
 $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
 $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Question: Is $S(4) = \{2, 3, 5, 7, 11, 13, 17\}$?

Explicit Kamienny-Parent for $d = 4$

To attack the above unsolved problem about $S(4)$, I made Parent's (1999) approach very explicit in case $d = 4$ and $\ell = 2$ (he gives a general criterion for any $d...$). One arrives that the following (where t is a certain explicitly computable element of the Hecke algebra). With $\ell = 2, d = 4$ we have $(1 + \ell^{d/2}$

Proposition 3.3. *Let $p > 25$ be a prime and consider Hecke operators T_n in the Hecke algebra $\mathbb{T} = \mathbb{T}_{\Gamma_1(p)} \otimes \mathbb{F}_2$ associated to $S_2(\Gamma_1(p); \mathbb{F}_2)$. Consider the following sequences of 4 elements of the Hecke algebra mod 2:*

1. Partition $4=4$: (t, tT_2, tT_3, tT_4)
2. Partition $4=1+3$: $(t, t\langle d \rangle, t\langle d \rangle T_2, t\langle d \rangle T_3)$,
for $1 < d < p/2$.
3. Partition $4=2+2$: $(t, tT_2, t\langle d \rangle, t\langle d \rangle T_2)$,
for $1 < d < p/2$.
4. Partition $4=1+1+2$: $(t, t\langle d_1 \rangle, t\langle d_2 \rangle, t\langle d_2 \rangle T_2)$,
for $1 < d_1 \neq d_2 < p/2$.
5. Partition $4=1+1+1+1$: $(t, t\langle d_1 \rangle, t\langle d_2 \rangle, t\langle d_3 \rangle)$,
for $1 < d_1 \neq d_2 \neq d_3 < p/2$.

If the entries in every single one of these sequences (for all choices of d_i) are linearly independent then there is no elliptic curve over a degree 4 number field with a rational point of order p .

NOTES:

1. This looks pretty crazy, but this is *really just a way of expressing the condition that a certain map is a formal immersion.*
2. As p gets large, there are a **LOT** of 4-tuples of elements of the Hecke algebra to test for independence mod 2.
3. Here is code that implements this algorithm: [code.sage](#)

Running the Algorithm

After a *day* we find that the criterion is **not satisfied** for $p = 29, 31$ but it is for $37 \leq p \leq 97$

Conclusion:

Theorem (Kamienny, Stein): $\max(S(4)) \leq 31$

Last Week...

A complete solution!?!

Theorem (Kamienny, Stein, Stoll): $S(4) = \{2, 3, 5, 7, 11, 13, 17\}$

Proofs uses that $\text{rank}(J_1(p)) = 0$ for the above p , informed by calculations from [Conrad-Edixhoven-Stein] about the arithmetic of $J_1(p)$ for small p , so one can use much more direct geometric arguments.

This also involves some large computations with Magma on explicit algebraic curves, e.g., Riemann-Roch spaces, enumerating and reducing divisors, etc., built on top of Florian Hess's function fields package. **Stoll:** "Finding the degree 4 points takes about 3 hours [...] The other problem is that Magma crashes once in a while when turning a point into a place. This will be fixed in the next release, but for now, one may have to try the actual checking a few times until it runs through."

Related Conjecture (Stein): $J_1(p)(\mathbf{Q})_{\text{tor}}$ is generated by differences of rational cusps.

(See extensive data about this conjecture in Conrad-Edixhoven-Stein.)

Future Work

1. Determine if $J_1(p)(\mathbf{Q})_{\text{tor}}$ is cuspidal.
2. Make the algorithm for showing that $\max(S(4)) \leq 31$ much more efficient. Then...
3. Repeat my calculations, but for $d = 5$ and hope to replace the Oesterle bound of $\max(S(5)) \leq 271$
by

$$\max(S(5)) \leq 43 \quad (\text{or something close}).$$

4. **Isogeny degrees** -- still an open problem even over *quadratic fields*!

- **Cremona** (a few minutes ago on Google Buzz): "I'm also very interested in the corresponding question for $X_0(\ell)$, so we know what the possible prime degrees of isogenies are for a given field (or degree). I had some interesting correspondence about this with Parent about 6 months ago; *he says that is still wide open for quadratic fields!* My student Kimi is implementing isogenies of degree 11, 17, 19 (the genus 1 cases) in Sage (work in progress). But to have a genuine `isogeny_class()` function over any non-Q number fields we need a bound." and
- **Mazur** (email): "It would be also interesting if you could, say, rule out a few primes p occurring as p -isogenies over such fields (for non CM curves)?"

5. Modular abelian varieties

```
float((1+2^(5/2))^2)
```

```
44.313708498984766
```

```
previous_prime(275)
```

```
271
```