Elliptic Curves with good reduction away from $\{2,3,5,7,11,13\}$

(how do you find the generators of a large Mordell curve).

Alex Best - VU

joint work w/ Benjamin Matschke

§ Motivation:

Recall: Part of Wiles' proof of FLT:

1) Given $Aa^p + Bb^p = Cc^p \in \mathbb{Z}$

there exists a Frey-Hellegouarch curve

$$E_{a,b,c} : Y^2 = X(X - Aa^p)(X + Bb^p)/\mathbb{Q}$$

elliptic curve.

with semistable reduction away from $2 \cdot \gcd(a,b,c)\, ABC$

⇝ level lowering

2) There exists an elliptic curve $E'/\mathbb{Q}$ with good reduction away from

$2 \cdot \gcd(a,b,c)$. ABC
and potentially good away from 2. ABC

Above may be generalized to Fermat curve with coeffs, see Kara-Ozman '19.

Problem: Can we write down the set

$$E_{good}(S) = \left\{ E/K : \begin{array}{l} E \text{ has good red}^n \\ \text{away from } S \end{array} \right\}$$

for S a finite set of primes of K.

Thm (Shafarevich): For S a finite set of rational primes

$$|E_{good}(S)| < \infty.$$

For some arithmetic applications we want to know more than just finiteness, can we write this set down?

History of the problem: From now $K = \mathbb{Q}$,

let $S(n) = \{$ first n rational primes $\}$

Note: $E_{good}(S)$ is preserved by twisting by primes in S and ± 1, when $2 \in S$: so

$$2^{|S|+1} \cdot |j(E_{good}(S))| \approx |E_{good}(S)|.$$

Summary of previous work:

n	$\lvert E_{good}(S(n)) \rvert$	Reference:
0	0	Tate / Ogg
1	24	Coghlan, Stephens, Ogg
2	752	〃
3	7600	von Känel - Matschke
4	71520	〃
5	592192	+ Bennett-Gherga-Rechnitzer.
6	4576128*	B.-Matschke

Reduction to S-integral points:

Let $E/\mathbb{Q}$ be any elliptic curve, then E can be written as

$$y^2 = x^3 - 27c_4 x - 54c_6 \qquad c_4, c_6 \in \mathbb{Z}$$

and $1728\Delta(E) = c_4^3 - c_6^2$

↑ this expresses c_4, c_6 as points on an elliptic curve defined by Δ.

Δ is the discriminant.

If $E \in E_{good}(S)$ then

$$q | \Delta \Rightarrow q \in S.$$

So $\Delta = \pm \prod p_i^{e_i}$ for $p_i \in S$.

To reduce to a finite set of Δ's divide by p^6 for each $p \in S$, until

$$\Delta' \in \{ \pm \prod p_i^{e_i} : p_i \in S, 0 \leq e_i \leq 5 \}$$

Now c_4, c_6 are only S-integral

The set of S-integral points is finite! $\mathbb{Z}[\frac{1}{p} : p \in S] = \mathbb{Z}_S$.

To find $E_{good}(S)$ we can simply find

$E_{\Delta'}(\mathbb{Z}_S)$ for each Mordell curve

$E_{\Delta'} : y^2 = x^3 - \Delta'$ for $\Delta' \in \{ \pm \prod p^{e_p} : 0 \leq e_p \leq 5 \}$

call this set $M(S)$. Cf. Cremona–Lingham.

Now fix $S = S(6)$ so there are 93312 possible Δ', for which we want to find $E_{\Delta'}(\mathbb{Z}_S)$.

We do this as follows:

1. Work of Matschke–von Känel $\Rightarrow$ can reduce the problem to finding $E_\Delta(\mathbb{Q})$ for each $E_{\Delta'} \in M(S)$.
2. Curves in $M(S)$ come in pairs, linked by a 3-isogeny:
$$\varphi: Y^2 = X^3 + A \to Y^2 = X^3 - 27A.$$
so only need to consider half of them.

In general pick the one with smallest regulator (gens smaller).

Sometimes easier to find independent points by finding one on each of a 3-isogenous pair.

rank	0	1	2	3	4
# pairs	20215	23186	3112	142	1.

3. Naive point searching
4. Apply BSD in analytic rank 0 (torsion is easy)
5. For the remaining curves we apply:
- 2-, 4-, descent:
  n-descent finds sets of curves covering the original reduces height of a point by ~ $2n$.
- Heegner points in analytic rank 1.
  CM ⇒ can find a_p efficiently, and compute the modular parameterization fast.
- 3-isogeny descent,
  Work of Fisher describes how 3-descent can be combined with 4-descent to do explicit 12-descent
  produces several 12-covers

These methods resolve all but 306 of the 93312 curves.
needed to find $E_{good}(\delta(6))$

Some tricky rank 1 E_Δ's remain:

e.g.

$$y^2 = x^3 - 904509009004500900000.$$
$$\quad\quad\quad \shortparallel$$
$$-2^5 \cdot 3^2 \cdot 5^5 \cdot 7^5 \cdot 11^5 \cdot 13^5.$$

has rank 1 and $\mathrm{Reg} \cdot |Ш| \approx 17628.52$

Thm: (B.-Matschke): Assuming these 306 Mordell curves have no S-integral points:

There are 4576128 elliptic curves $/\mathbb{Q}$
in 34960 $\overline{\mathbb{Q}}$-isomorphism classes
in 3688192 $\mathbb{Q}$-isogeny classes.

With good reduction outside $\{2,3,5,7,11,13\}$

Why is this theorem likely still true unconditionally?

The remaining Mordell curves are tough because their generators are large $\Rightarrow$ unlikely to give rise to any S-integral points.

1. We formulate an S-integral analogue of the Hall conjecture, which follows from the abc conjecture.
$\Rightarrow$ the remaining curves should not have any S-integral points.

2. Work in progress of Matschke confirms this result using a different unconditional method (solving S-unit eq'ns)

Observations on this set.

$$|E_{good}(S(6))| \approx |\{E/\mathbb{Q} : N_E \leq 500{,}000\}|$$

↑ computed by Cremona

but the overlap is only around 5%.

We can compare the effect of ordering by N vs by S:

For instance rank distribution.

rank	$E_{good}(S(6))$	$N_E \leq 500{,}000$
0	1884428	1632686
1	2267261	2124004
2	406309	461670
3	18003	11243
4	127	1

↑ thanks to Edgar Costa

there are 14216 curves of the maximal possible conductor

$$2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \approx 10^{12}.$$

6

12 11 26

4.1 4.2

https://github.com/elliptic-curve-data/ec-data-S6

8

36

40

12 11

7

9 37

6 1

13

25

22

4 3

13 25

1 1.1 1.2

1.3

2.1

2.2

2.3 2.4

3

4

1

29

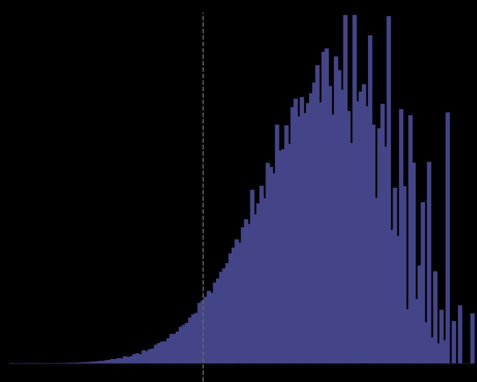
9 37 29

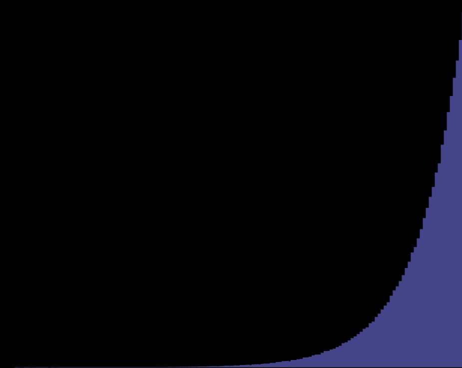
9 37

22

22

22 3

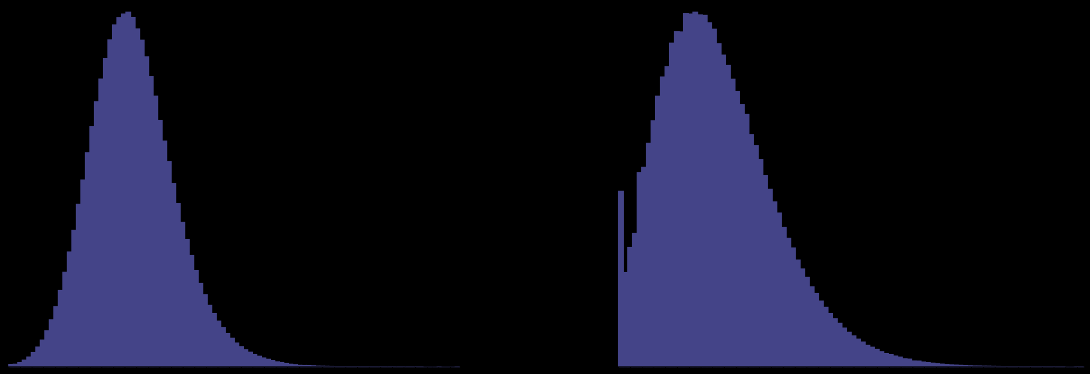




1

1

2



858.k2 *2574.j2*

910.e1 *9438.m2*

12 11

1 2

https://github.com/elliptic-curve-data/ec-data-S6
https://github.com/bmatschke/solving-classical-
diophantine-equations/
22

31

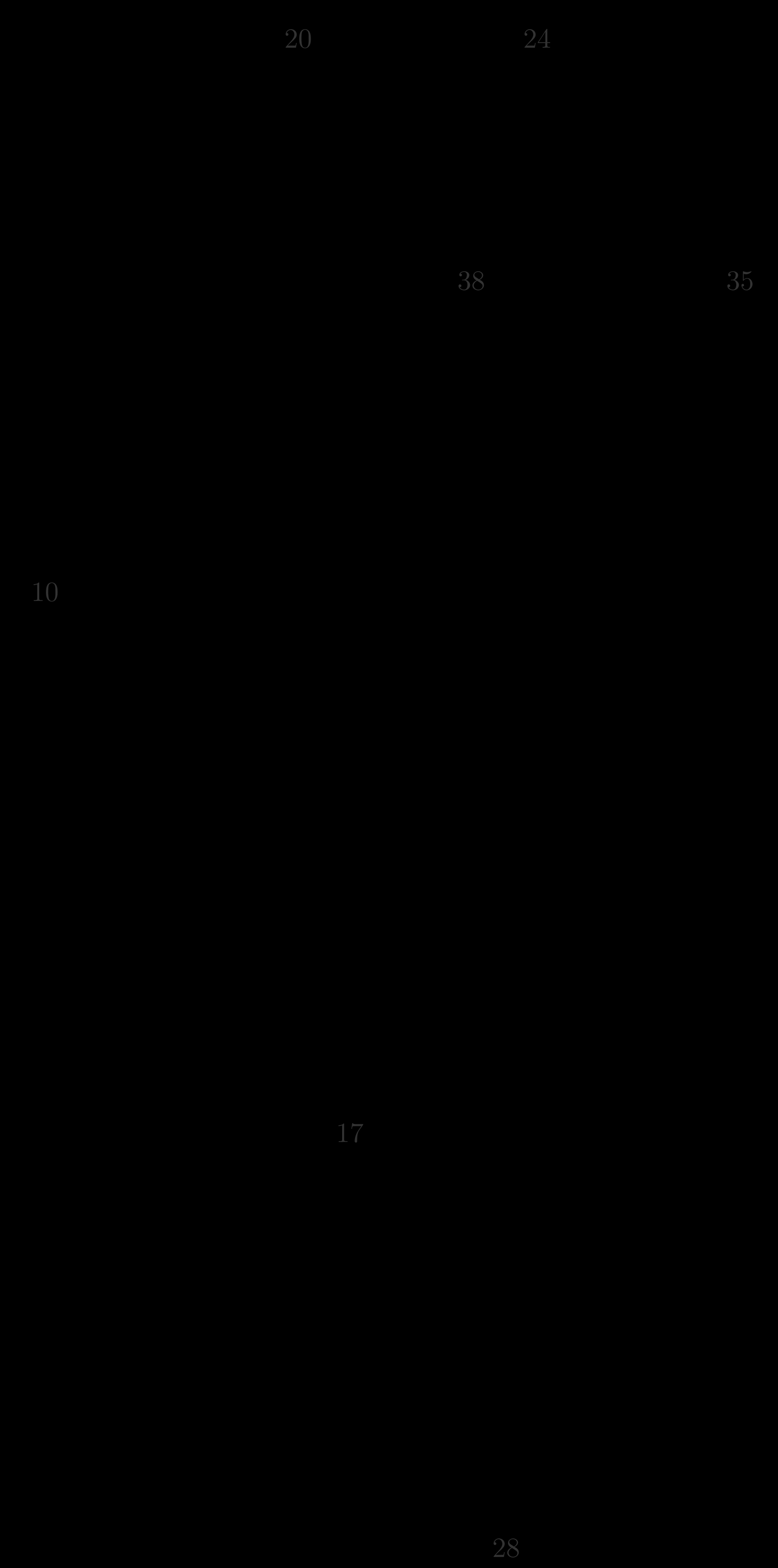
32 33

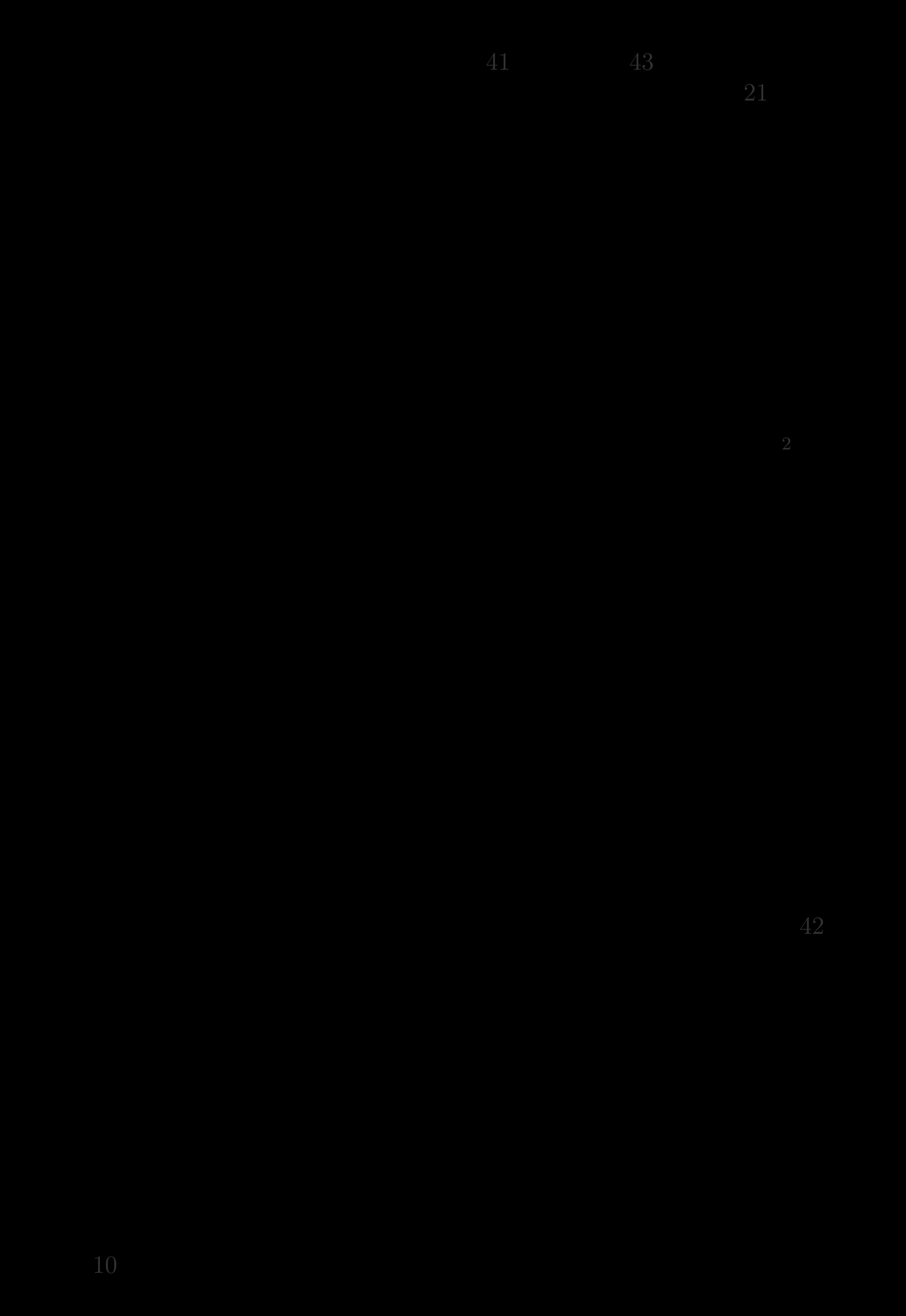
22

2.2

19

39 16


20
24
38
35
10
17
28


41
43
21
2
42
10

22

30

2 2.4

39

3

22 22

2.8

2.6

30

2.6

2.12

2.12 2.11

2.1

2.5 2.10

14

https://github.com/elliptic-curve-data/ec-data-S6/blob/master/docs/paper.pdf

34

32 27 32 33

4.1

4.1

15

4.1

22 4.1

25

2.3

5

18

https://johncremona.github.io/ecdata/

https://www.math.leidenuniv.nl/~desmit/abc/

http://www.sagemath.org

arXiv:0711.3774

arXiv:1605.06079
https://bmatschke.github.io/solving-classical-diophantine-equations/

https://www.lmfdb.org

https://simond.users.lmno.cnrs.fr/ellQ.gp

arXiv:math/0803.3165

http://pari.math.u-bordeaux.fr/

http://magma.maths.usyd.edu.au/∼watkins/papers/padic.ps

arXiv:math/0506325