

Finding a rational point on the
elliptic curve $y^2 = x^3 + 7823$



Introduction

Mordell-Weil theorem

- The group of rational points on an elliptic curve over a number field is finitely generated
- So E/Q is finitely generated
- How to find the generators?

Mordell curve

- An elliptic curve of the form $y^2 = x^3 + D$

- Generators for $|D| \leq 10,000$:


<http://diana.math.uni-sb.de/~simath/MORDELL>

- All $|D| \leq 10,000$ except for...

The Mordell-Weil generator

- ...except for $D=7823$
- Stoll, January 2002: found Mordell-Weil generator via 4-descents
- Coordinates of generator:

$$x = \frac{2263582143321421502100209233517777}{11981673410095561^2}$$
$$y = \frac{186398152584623305624837551485596770028144776655756}{11981673410095561^3}.$$


$$y^2 = x^3 + 7823$$

[Points of finite order on 7823?]

- Nagell-Lutz: integer coordinates
- Calculate discriminant
- Check factors

7823: Points of finite order?

- Answer: no!
- So Mordell-Weil generator has infinite order

7823: Points of infinite order...

- Kolyvagin, Gross, Zagier: L -series of E has simple zero at $s = 1$
- So $E(\mathbb{Q})$ is isomorphic to \mathbb{Z} and E is of rank 1
- One rational point of infinite order generating the Mordell-Weil group



Descent

Descent: $\dots \rightarrow C \rightarrow D \rightarrow E$

- Idea: associate other objects (“covering spaces”) to E
- Points on these spaces correspond to points on E via polynomial mapping
- Goal: find rational points on these spaces

Descents

- Descent via isogeny: “first descent”

- Isogeny?

- “2-isogenies”: $E \rightarrow \bar{E} \rightarrow \overline{\bar{E}} \cong E$

- The curves: $E : y^2 = x^3 + ax + b$

$$\bar{E} : y^2 = x^3 + \bar{a}x + \bar{b}, \quad \bar{a} = -2a, \quad \bar{b} = a^2 - 4b$$

$$\overline{\bar{E}} : y^2 = x^3 + \overline{\bar{a}}x + \overline{\bar{b}}, \quad \overline{\bar{a}} = -2\bar{a}, \quad \overline{\bar{b}} = \bar{a}^2 - 4\bar{b}$$

Descent via 2-isogeny (algorithm)


- Given an elliptic curve with point of order 2, transform it to the form $E : y^2 = x^3 + ax^2 + bx$, sending point of order 2 to $(0,0)$
- For each square-free divisor d_1 of D , look at the homogeneous space $C_{d_1} : N^2 = d_1M^4 + aM^2e^2 + \frac{D}{d_1}e^4$ and find integer points (M, N, e) which correspond to points $x = \frac{d_1M^2}{e^2}, y = \frac{d_1MN}{e^3}$
- Repeat with \bar{E}
- Result: $E(\mathbb{Q})/2E(\mathbb{Q})$

2-descent

- If we can't find a rational point on some C_{d_1} , what went wrong?
 - (1) Either it has points, but they're too large to be found in the search
 - (2) Or has no rational points
- Carry out 2-descent to distinguish between two possibilities

[Problem!]

- But there's a fundamental problem with the descent via 2-isogeny for the 7823 curve
- $y^2 = x^3 + 7823$ is conspicuously lacking a point of order 2
- So what do we do if there's no point of order 2?
- Answer: general 2-descent



General 2-descent

General 2-descent (algorithm)

- Determine the invariants (I, J)
- Find the quartics with the given I, J
- Test equivalence of quartics
- Find roots of quartics
- Local and global solubility
- Recover points on E

General 2-descent

- Basic idea is to associate to E a collection of 2-covering homogeneous spaces

$$y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e$$

- a, b, c, d, e are in \mathbb{Q} and are such that certain invariants I and J satisfy

$$I = 12ae - 3bd + c^2, \quad J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$$

- I and J are related to certain invariants of E ,

$$I = \lambda^4 c_4, \quad J = 2\lambda^6 c_6 \quad \text{for } \lambda \in \mathbb{Q}^*$$

General 2-descent (algorithm)

- Determine the invariants (I, J)

with mwrnk:

Enter curve: $[0, 0, 0, 0, 7823]$

Curve $[0, 0, 0, 0, 7823]$

Two (I, J) pairs

$I=0, J=-211221$

$I = 0, J = -13518144$

General 2-descent (algorithm)

- Find the quartics with the given I, J

$$\phi^3 - 3I\phi + J = 0,$$
$$\frac{1}{3}\phi - \sqrt{\frac{4}{27}(\phi^2 - I)} \leq a \leq \frac{1}{3}\phi + \sqrt{\frac{4}{27}(\phi^2 - I)}$$

$$-2|a| < b \leq 2|a|$$

$$\frac{9a^2 - 2a\phi + \frac{1}{3}(4I - \phi^2) + 3b^2}{8|a|} \leq c \cdot \text{sign}(a) \leq \frac{4a\phi + 3b^2}{8|a|}$$

$$e = (I + 3bd - c^2)/(12a)$$

d : substitute into original equation

General 2-descent (algorithm)

- Find the quartics with the given I, J

```
disc=-44614310841
```

```
Looking for quartics with
```

```
I = 0, J = -211221
```

```
Looking for Type 3 quartics:
```

```
Trying positive a from 1 up to 17
```

```
Trying negative a from -1 down to -11
```

```
Finished looking for Type 3 quartics.
```

General 2-descent (algorithm)

- Find the quartics with the given I, J

Looking for quartics with

$I = 0, J = -13518144$

Looking for Type 3 quartics:

Trying positive a from 1 up to 68

$(30, -12, 48, 116, -18)$

$(41, -16, -6, 112, -11)$

Trying negative a from -1 down to -45

$(-11, -20, 408, 1784, 2072)$

$(-18, -28, 312, 996, 838)$

Finished looking for Type 3 quartics.

General 2-descent (algorithm)

- Test equivalence of quartics

equivalence relation: $g_1 \sim g_2$ if

$$g_2(x) = \mu^2 (\gamma x + \delta)^4 g_1\left(\frac{\alpha x + \beta}{\gamma x + \delta}\right) \quad \text{for rational constants}$$

(30, -12, 48, 116, -18) new (B) #1

(41, -16, -6, 112, -11) equivalent to (B) #1

(-11, -20, 408, 1784, 2072) equivalent to (B) #1

(-18, -28, 312, 996, 838) equivalent to (B) #1

General 2-descent (algorithm)

- Our 2-covering space:

$$C : y^2 = -18x^4 + 116x^3 + 48x^2 - 12x + 30.$$

- Local and global solubility?

`mwrnk: locally soluble`

- Global solubility? Local doesn't imply global, so we have to search for points...
- Recovering points on E?



Local (-to-global) solubility

[Local solubility?]

- Given an equation:
 - Check solutions over \mathbb{Q}_p for all p
 - Check solutions over \mathbb{R}

[Global solubility?]

- Checking for a solution over \mathbb{Q} if local solubility is known
- Local does not imply global (“failure of Hasse principle”)

Failure of Hasse principle



The curve $C: 3x^3 + 4y^3 + 5z^3 = 0$ has nonisomorphic companions. This equation possesses nontrivial solutions over \mathbb{Q}_p for all prime numbers p and over \mathbb{R} , but it possesses no nontrivial solutions over \mathbb{Q} .

Examples, continued

Theorem 1. *Selmer's curve $C: 3x^3 + 4y^3 + 5z^3 = 0$ has, counting itself, precisely five companions:*

$$3x^3 + 4y^3 + 5z^3 = 0,$$

$$12x^3 + y^3 + 5z^3 = 0,$$

$$15x^3 + 4y^3 + z^3 = 0,$$

$$3x^3 + 20y^3 + z^3 = 0,$$

$$60x^3 + y^3 + z^3 = 0.$$

Examples, continued

(2) All five equations on this list have nontrivial rational solutions over \mathbb{Q}_p for all prime numbers p and over \mathbb{R} . The first four equations on the list possess no nontrivial rational solutions. The fifth equation possesses a nontrivial rational solution $(0, 1, -1)$, and this solution is unique up to scalar multiplication (cf. [Ca2, §18]). If we take this point as “origin” of the projective curve E defined by the equation

$$60x^3 + y^3 = z^3 = 0,$$

then E is an elliptic curve over \mathbb{Q} isomorphic to the jacobian of all five curves on the list.

Local-to-global article

- “On the Passage from Local to Global in Number Theory” (B. Mazur)

- <http://www.ams.org/bull/pre-1996-data/199329-1/mazur.pdf>

Checking local solubility

- Back to original problem: we have

$$y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e$$

- We want to check solubility over p-adics and reals
- For reals, this is just solving a quartic
- For p-adics, situation is a little more complicated

P-adics?

(Subroutine for determining p-adic solubility)

SUBROUTINE Qp_soluble(a,b,c,d,e,p)

INPUT: a, b, c, d, e (integer coefficients of a quartic $g(x)$)

p (a prime)

OUTPUT: TRUE/FALSE (solubility of $y^2=g(x)$ in \mathbb{Q}_p)

1. BEGIN
2. IF Zp_soluble(a,b,c,d,e,0,p,0) THEN RETURN TRUE FI;
3. IF Zp_soluble(e,d,c,b,a,0,p,1) THEN RETURN TRUE FI;
4. RETURN FALSE
5. END

P-adics, continued

(Recursive \mathbb{Z}_p -solubility subroutine)

SUBROUTINE Zp_soluble(a,b,c,d,e,x_k,p,k)

INPUT: a, b, c, d, e (integer coefficients of a quartic $g(x)$)
 p (a prime)
 x_k (an integer)
 k (a non-negative integer)

OUTPUT: TRUE/FALSE (solubility of $y^2=g(x)$ in \mathbb{Z}_p , with $x \equiv x_k \pmod{p^k}$)

```
1. BEGIN
2. IF p=2
3. THEN code = lemma7(a,b,c,d,e,x_k,k)
4. ELSE code = lemma6(a,b,c,d,e,x_k,p,k)
5. FI;
6. IF code=+1 THEN RETURN TRUE FI;
7. IF code=-1 THEN RETURN FALSE FI;
8. FOR t = 0 TO p-1 DO
9. BEGIN
10.     IF Zp_soluble(a,b,c,d,e,x_k+t*p^k,p,k+1) THEN RETURN TRUE FI
11. END;
12. RETURN FALSE
13. END
```

P-adics, continued

(\mathbb{Z}_p lifting subroutine: odd p)

```
SUBROUTINE lemma6(a,b,c,d,e,x,p,n)
```

1. BEGIN
2. $gx = a*x^4 + b*x^3 + c*x^2 + d*x + e$;
3. IF p_adic_square(gx,p) THEN RETURN +1 FI;
4. $gdx = 4*a*x^3 + 3*b*x^2 + 2*c*x + d$;
5. $l = \text{ord}(p, gx)$; $m = \text{ord}(p, gdx)$;
6. IF $(l \geq m+n)$ AND $(n > m)$ THEN RETURN +1 FI;
7. IF $(l \geq 2*n)$ AND $(m \geq n)$ THEN RETURN 0 FI;
8. RETURN -1
9. END

P-adics, continued

(\mathbb{Z}_2 lifting subroutine)

```
SUBROUTINE lemma7(a,b,c,d,e,x,n)
```

```
1. BEGIN
2. gx = a*x4+b*x3+c*x2+d*x+e;
3. IF p_adic_square(gx,2) THEN RETURN +1 FI;
4. gdx = 4*a*x3+3*b*x2+2*c*x+d;
5. l = ord(p,gx); m = ord(p,gdx);
6. gxodd = gx; WHILE even(gxodd) DO gxodd = gxodd/2;
7. gxodd = gxodd (mod 4);
8. IF (l $\geq$ m+n) AND (n>m) THEN RETURN +1 FI;
9. IF (n>m) AND (l=m+n-1) AND even(l) THEN RETURN +1 FI;
10. IF (n>m) AND (l=m+n-2) AND (gxodd=1) AND even(l) THEN RETURN +1 FI;
11. IF (m $\geq$ n) AND (l $\geq$ 2*n) THEN RETURN 0 FI;
12. IF (m $\geq$ n) AND (l=2*n-2) AND (gxodd=1) THEN RETURN 0 FI;
13. RETURN -1
14. END
```

[Global solubility?]

- If locally soluble, then check global solubility
- Check up to a certain height on a homogeneous space
- If not sure about existence of a rational point, take another descent

General 2-descent (algorithm)

- Our 2-covering space:

$$C : y^2 = -18x^4 + 116x^3 + 48x^2 - 12x + 30.$$

- Local and global solubility?

`mwrnk: locally soluble`

- Global solubility? Local doesn't imply global, so we have to search for points...
- Recovering points on E?



4-descent

4-descent

- 4-coverings: intersection of two quadric surfaces
- Represent these by matrices M_1 and M_2
- $\text{Det}(xM_1 + M_2) = g(x)$

$$M_1 = \begin{pmatrix} -22181252 & -12522843 & 485492211 & 2218020408 \\ -12522843 & 485492211 & 2218020408 & -2954387682 \\ 485492211 & 2218020408 & -2954387682 & -65148580179 \\ 2218020408 & -2954387682 & -65148580179 & -185865980697 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 383480 & 60588 & -9008739 & -37014651 \\ 60588 & -9008739 & -37014651 & 71170650 \\ -9008739 & -37014651 & 7117650 & 1173510018 \\ -37014651 & 71170650 & 1173510018 & 2915000865 \end{pmatrix}$$

[Stoll]

- Found matrices with smaller entries with same property
- Do this by making substitutions: elements with sums
- Swap matrices; repeat
- Apply generators of $SL_4(\mathbb{Z})$; if made smaller, repeat

[Stoll]

- Found matrices with smaller entries with same property
- Do this by making substitutions: elements with sums
- Swap matrices; repeat
- Apply generators of $SL_4(\mathbb{Z})$; if made smaller, repeat

4-covering, descent

- Simultaneous equations:

$$\begin{aligned}x_1^2 + 4x_1x_2 - 2x_1x_3 - 2x_1x_4 - 2x_2^2 - 3x_3^2 + 4x_3x_4 + x_4^2 &= 0 \\x_1^2 - 6x_1x_4 + 2x_2^2 + 4x_2x_3 + 3x_3^2 + 2x_3x_4 + x_4^2 &= 0\end{aligned}$$

- This has the point $(-681 : 116 : 125 : -142)$
- Which gets us $\left(\frac{53463613}{32109353}, \frac{23963346820191122}{32109353^2}\right)$ on the 2-covering

- Resulting in $x = \frac{2263582143321421502100209233517777}{11981673410095561^2}$
 $y = \frac{186398152584623305624837551485596770028144776655756}{11981673410095561^3}$.

on the elliptic curve



Calculating “matrixes” [sic]¹

¹via Nick Rozenblyum

Matrices?

- $\text{Det}(xM_1 + M_2) = g(x)$
- The M 's are 4 x 4, symmetric: so 20 unknowns
- g is a quartic
- Summing, det-ing, equating coefficients...

THE END