Three-gluings of elliptic curves (Revised slides)

Everett W. Howe

Center for Communications Research, La Jolla

GeoCrypt 2011
Bastia, Corsica, 20 June 2011

Motivation

Two topics of interest

- Genus-2 curves with maps to elliptic curves
- Genus-2 curves with Jacobians isogenous to a product of elliptic curves

These are really the same topic. . .

A construction

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi : E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

We will produce:

- A genus-2 curve C (possibly degenerate)
- Degree-n maps $C \to E_1$ and $C \to E_2$

A construction

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi : E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$E_1[n] \times E_1[n] \xrightarrow{\text{Weil}} \boldsymbol{\mu}_n$$

We will produce:

- A genus-2 curve C (possibly degenerate)
- Degree-n maps $C \to E_1$ and $C \to E_2$

A construction

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi : E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$E_1[n] \times E_1[n] \xrightarrow{\text{Weil}} \boldsymbol{\mu}_n$$

$$E_2[n] \times E_2[n] \xrightarrow{\text{Weil}} \boldsymbol{\mu}_n$$

We will produce:

- A genus-2 curve C (possibly degenerate)
- Degree-n maps $C \to E_1$ and $C \to E_2$

A construction

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi : E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$\begin{array}{ccc} E_1[n] \times E_1[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \\ \downarrow{\scriptstyle \psi\times\psi} & & \\ E_2[n] \times E_2[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \end{array}$$

We will produce:

- A genus-2 curve C (possibly degenerate)
- Degree-n maps $C \to E_1$ and $C \to E_2$

A construction

Given:

- Two elliptic curves E_1, E_2 over a field k
- An isomorphism $\psi : E_1[n] \to E_2[n]$ for some $n > 0$, such that ψ is an anti-isometry with respect to the Weil pairing

$$\begin{array}{ccc} E_1[n] \times E_1[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \\ {\scriptstyle \psi\times\psi}\downarrow & & \downarrow{\scriptstyle \text{inv.}} \\ E_2[n] \times E_2[n] & \xrightarrow{\text{Weil}} & \boldsymbol{\mu}_n \end{array}$$

We will produce:

- A genus-2 curve C (possibly degenerate)
- Degree-n maps $C \to E_1$ and $C \to E_2$

Completing a diagram

We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

Completing a diagram

We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$E_1 \times E_2 \xrightarrow{\text{mult. by } n} \widehat{E_1} \times \widehat{E_2}$$

Completing a diagram

We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\text{mult. by } n} & \widehat{E_1} \times \widehat{E_2} \\ \Big\downarrow{\scriptstyle \alpha} & & \\ A & & \end{array}$$

Completing a diagram

We have:

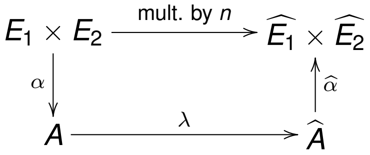
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map

$$
\begin{array}{ccc}
E_1 \times E_2 & \xrightarrow{\text{mult. by } n} & \widehat{E_1} \times \widehat{E_2} \\
\big\downarrow{\scriptstyle \alpha} & & \big\uparrow{\scriptstyle \widehat{\alpha}} \\
A & & \widehat{A}
\end{array}
$$

Completing a diagram

We have:

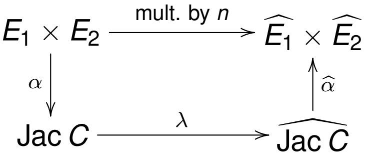
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

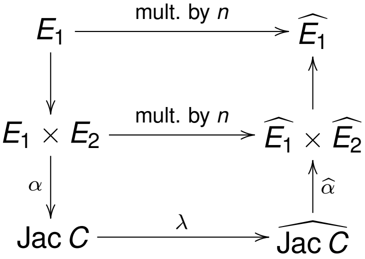
We have:

- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



We have:

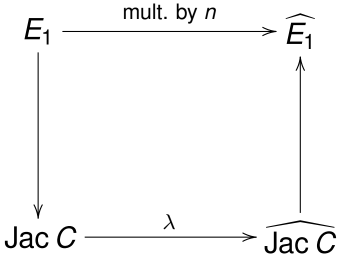
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

We have:

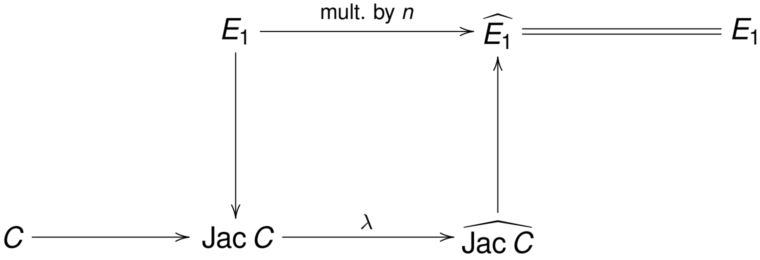
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

We have:

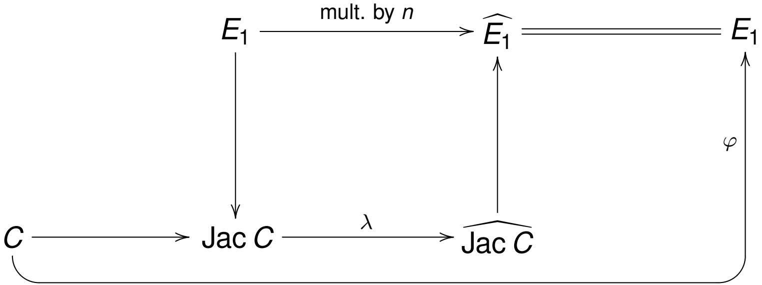
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

We have:

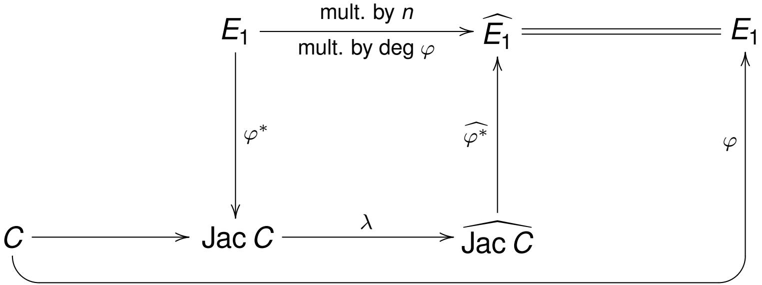
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

We have:

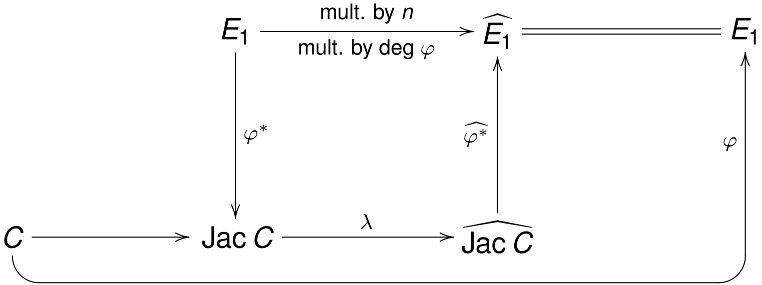
- $\mathrm{Graph}(\psi) \subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



Completing a diagram

We have:

- Graph(ψ) $\subset (E_1 \times E_2)[n]$, a maximal isotropic subgroup
- $A = (E_1 \times E_2)/\,\mathrm{Graph}(\psi)$
- $\alpha\colon E_1 \times E_2 \to A$, the natural map



This gives degree-n map $\varphi_1 : C \to E_1$. Get φ_2 similarly.

An old story

Theorem

Every degree-n map $C \to E_1$ that does not factor through an isogeny arises in this manner.
The associated E_2 and $\psi\colon E_1[n] \to E_2[n]$ are unique up to isomorphism.

Theorem

Every genus-2 curve with non-simple Jacobian arises in this manner, perhaps in several ways.

These results are old. What I just presented is close to what appears in Kani, *J. Reine Angew. Math.* (1997), which is based on Frey/Kani, in *Arithmetic Algebraic Geometry* (1991).

An older story

Frey and Kani note:

They can't find this construction explicitly in literature, but it 'seems to be known in principle'. They cite:

- Serre, *Sem. Théorie Nombres Bordeaux* (1982/82)
- Ibukiyama/Katsura/Oort, *Compositio Math.* (1986)

But if we allow for a change in perspective, it's older than that.

An even older story

Kowalevski's dissertation, written 1874

- Published in *Acta Math.* (1884).
- Mentions unpublished result of Weierstrass (her advisor):

  Wenn aus einer Function $\vartheta(v_1, \ldots, v_\rho | \tau_{11}, \ldots, \tau_{\rho\rho})$ durch irgend eine Transformation k^{ten} Grades eine andere hervorgeht, die ein Produkt aus einer ϑ-Funktion von $(\rho - 1)$ Veränderlichen und einer elliptischen ist, so kann der erspründliche Funktion stets durch eine *lineare* Transformation (bei der $k = 1$ ist) in eine andere $\vartheta(v_1', \ldots, v_\rho' | \overline{\tau}_{11}, \ldots, \overline{\tau}_{\rho\rho})$ verwandelt werden, in der

  $$\overline{\tau}_{12} = \frac{\mu}{k}, \overline{\tau}_{13} = 0, \ldots, \overline{\tau}_{1\rho} = 0$$

  ist, wo μ einer der Zahlen $1, 2, \ldots, k - 1$ bedeutet.

An even older story, continued

Similar result, discovered independently by Picard

- Published in *Bull. Math. Soc. France* (1883).

  S'il existe une intégrale de premièr espèce correspondant à la relation algébrique

  $$y^2 = x(1-x)(1-k^2x)(1-l^2x)(1-m^2x)$$

  qui ait seulement deux périodes, on pourra trouver un système d'intégrales normales, dont le tableau des périodes sera

  $$\begin{matrix} 0 & 1 & G & \frac{1}{D} \\ 1 & 0 & \frac{1}{D} & G' \end{matrix}$$

  où D désigne un entier réel et positif.

A question of perspective

The result of Frey and Kani shows that degree-n covers of elliptic curves, and "n-gluings" of two elliptic curves, are essentially the same thing.

In the 19th century, there was more interest in the former.

But I think 19th-century mathematicians would have recognized Frey and Kani's result.

Explicit examples of genus-2 covers

Legendre's special ultra-elliptic integrals (1828)

- *Traité des fonctions elliptiques*, 3$^{\text{ième}}$ supplement, §12
- Shows that several integrals involving the expression

$$\sqrt{x(1-x^2)(1-k^2x^2)}$$

can be evaluated in terms of elliptic integrals.

Explicit examples of genus-2 covers

Jacobi's review of Legendre's book

- *J. Reine Angew. Math.* (1832)
- Generalizes Legendre's example to integrals involving

$$\sqrt{x(1-x)(1-\lambda x)(1-\mu x)(1-\lambda\mu x)}$$

Jacobi’s family is complete

Königsberger (*J. Reine Angew Math* (1867)) and Picard (*Bull. Soc. Math. France* (1883)) show:

Theorem

Every genus-2 curve over $\mathbb{C}$ with a degree-2 map to an elliptic curve occurs in Jacobi’s family.

More memorable version of Jacobi's family over $\mathbb{C}$

Suppose we want to glue together the curves

$$E_1 : \quad y^2 = x(x-1)(x-\lambda)$$

$$E_2 : \quad y^2 = x(x-1)(x-\mu)$$

using the isomorphism $E_1[2] \to E_2[2]$ that sends $(0,0)$ to $(0,0)$ and $(1,0)$ and $(1,0)$.

The resulting genus-2 curve:

$$y^2 = \left(x^2 - 1\right)\left(x^2 - \frac{\lambda}{\mu}\right)\left(x^2 - \frac{\lambda - 1}{\mu - 1}\right)$$

Two-gluing over non-algebraically closed fields:

Howe/Leprévost/Poonen, *Forum Math.* (2000):

Given two elliptic curves:

$$y^2 = f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$y^2 = g = (x - \beta_1)(x - \beta_2)(x - \beta_3)$$

Set $\alpha_{ij} = \alpha_i - \alpha_j$ and $\beta_{ij} = \beta_i - \beta_j$, and define

$$A = \operatorname{disc}(g)\left(\frac{\alpha_{32}^2}{\beta_{32}} + \frac{\alpha_{21}^2}{\beta_{21}} + \frac{\alpha_{13}^2}{\beta_{13}}\right) \Big/ (\alpha_1\beta_{32} + \alpha_2\beta_{13} + \alpha_3\beta_{21})$$

$$B = \operatorname{disc}(f)\left(\frac{\beta_{32}^2}{\alpha_{32}} + \frac{\beta_{21}^2}{\alpha_{21}} + \frac{\beta_{13}^2}{\alpha_{13}}\right) \Big/ (\beta_1\alpha_{32} + \beta_2\alpha_{13} + \beta_3\alpha_{21})$$

Gluing gives the genus-2 curve

$$y^2 = -(A\alpha_{21}\alpha_{13}x^2 + B\beta_{21}\beta_{13}) \cdot (A\alpha_{32}\alpha_{21}x^2 + B\beta_{32}\beta_{21}) \cdot (A\alpha_{13}\alpha_{32}x^2 + B\beta_{13}\beta_{32})$$

Alternative view of 2-gluing formulas over arbitrary K

To a quadruple $(t, b, c, d) \in K^4$ with $dt \neq 0$ and

$$4b^3d - b^2c^2 - 18bcd + 4c^3 + 27d^2 \neq 0$$

associate curves

$$\begin{aligned} C_{t,b,c,d} &: \quad ty^2 = x^6 + bx^4 + cx^2 + d \\ E_{t,b,c,d,1} &: \quad ty^2 = x^3 + bx^2 + cx + d \\ E_{t,b,c,d,2} &: \quad ty^2 = dx^3 + cx^2 + bx + 1 \end{aligned}$$

Obvious degree-2 maps $C_{t,b,c,d} \to E_{t,b,c,d,1}$ and $C \to E_{t,b,c,d,2}$.

Theorem

Every pair of double covers $C \to E_1$ and $C \to E_2$ over K occurs in this family, and the quadruple (t, b, c, d) is unique up to scaling

$$(t, b, c, d) \mapsto (\lambda^6\mu^2 t, \lambda^2 b, \lambda^4 c, \lambda^6 d)$$

Similar framework for degree-3 maps

Howe/Lauter/Stevenhagen, draft preprint (2011):

Notation:

To every quintuple $(a, b, c, d, t) \in K^5$ such that

$$12ac + 16bd = 1, \quad a^3 + b^2 \neq 0, \quad c^3 + d^2 \neq 0, \quad t \neq 0$$

set $\Delta_1 := a^3 + b^2$ and $\Delta_2 := c^3 + d^2$.

Define curves $C_{a,b,c,d,t}$, $E_{a,b,c,d,t,1}$, $E_{a,b,c,d,t,2}$:

$$ty^2 = (x^3 + 3ax + 2b)(2dx^3 + 3cx^2 + 1)$$
$$ty^2 = x^3 + 12(2a^2d - bc)x^2 + 12(16ad^2 + 3c^2)\Delta_1 x + 512\Delta_1^2 d^3$$
$$ty^2 = x^3 + 12(2bc^2 - ad)x^2 + 12(16b^2c + 3a^2)\Delta_2 x + 512\Delta_2^2 b^3$$

The maps

Define rational functions:

$$u_1 = 12\Delta_1 \frac{-2dx + c}{x^3 + 3ax + 2b} \qquad v_1 = \Delta_1 \frac{16dx^3 - 12cx^2 - 1}{(x^3 + 3ax + 2b)^2}$$

$$u_2 = 12\Delta_2 \frac{x^2(ax - 2b)}{2dx^3 + 3cx^2 + 1} \qquad v_2 = \Delta_2 \frac{x^3 + 12ax - 16b}{(2dx^3 + 3cx^2 + 1)^2}$$

Simple verification:

$(x, y) \mapsto (u_i, yv_i)$ gives a degree-3 map

$$\varphi_{a,b,c,d,t,i} : C_{a,b,c,d,t} \to E_{a,b,c,d,t,i}.$$

General formulas for 3-gluings

Theorem (Howe/Lauter/Stevenhagen)

Given two degree-3 maps

$$\varphi_1 : C \to E_1 \qquad \varphi_2 : C \to E_2$$

with $\varphi_{2*}\varphi_1^* = 0$*, there exists a quintuple* (a, b, c, d, t) *whose associated triple covers are isomorphic to* φ_1 *and* φ_2*.*

The quintuple (a, b, c, d, t) *is unique up to scaling*:

$$(a, b, c, d, t) \mapsto (\lambda^2 a, \lambda^3 b, \lambda^{-2} c, \lambda^{-3} d, \lambda\mu^2 t).$$

Earlier work on explicit formulas for triple covers

- Hermite: *Ann. Soc. Sci. Bruxelles Sér. I* (1876)
  - Works over $\mathbb{C}$
  - Only gives 1-dimensional family
- Goursat: *Bull. Soc. Math. France* (1885)
  - Works over $\mathbb{C}$
- Kuhn: *Trans. Amer. Math. Soc.* (1988)
  - Doesn't give all curves and maps
  - Breaks into cases: 'generic' and 'special'
- Shaska: *Forum Math.* (2004) (inter alia)
  - Works over algebraically closed field
  - Gives formulas. . . with typographical errors
  - Breaks into cases: 'non-degenerate' and 'degenerate'

What we needed

Lauter, Stevenhagen, and I wanted a result that...

- works over finite fields
- does not involve special cases

We used Kuhn and Shaska's work, and tidied up.

The special cases

Ramification in a triple cover $\varphi : C \to E$

Two possibilities:

- Two points P and P', sharing same x-coordinate, each with ramification index 2; the points Q and Q' with $\varphi(Q) = \varphi(P)$ and $\varphi(Q') = \varphi(P')$ also have same x-coordinate.
- One ramification point P, with index 3. The point P must be a Weierstrass point.

The first case degenerates to the second as $x(P) \to x(Q)$.

Renormalizing

Kuhn and Shaska

Normalize first case so that $x(P) = 0$ and $x(Q) = \infty$.

- Formulas cannot possibly degenerate well.
- Lose symmetry between E_1 and E_2.

We normalized so that $x(P_1) = 0$ and $x(P_2) = \infty$.

Formulas degenerate well, and regain $E_1 \leftrightarrow E_2$ symmetry.

Everything old is new again

Our curve:

$$ty^2 = (x^3 + 3ax + 2b)(2dx^3 + 3cx^2 + 1)$$

where $12ac + 16bd = 1$.

Goursat's curve:

$$y^2 = (x^3 + ax + b)(x^3 + px^2 + q)$$

where $q = 4b + (4/3)ap$.

So Goursat's family only misses case $d = 0$.

Up to symmetry, only misses case $b = d = 0$.

That's just one curve!

Application 1: Building a genus-2 curve with N points

Basic idea in Howe/Lauter/Stevenhagen:

- Given N, use Bröker/Stevenhagen *Contemp. Math.* (2008): Find an elliptic curve $E_1/\mathbb{F}_p$ with N points, for some p.
- Find a supersingular curve $E_2/\mathbb{F}_p$.
- Glue them together along n-torsion for some n.
- Resulting curve has N points.

Problem:

- Must have $E_1[n] \cong E_2[n]$ as Galois modules ...
- So $\text{Trace}(E_1) \equiv \text{Trace}(E_2) \bmod n \ldots$.
- So n divides $N - p - 1$.
- Can't take $n = 2$ if N is odd.

Higher-order gluings to the rescue!

If $N \not\equiv 1 \bmod 3$:

The Bröker/Stevenhagen algorithm can produce $E_1/\mathbb{F}_p$ having N points, and with $p \equiv N - 1 \bmod 3$.

End result:

If $N \not\equiv 1 \bmod 6$, we can use 2- or 3-gluings to produce a genus-2 curve with N points.

This was our motivation for finding nice formulas for 3-gluing.

Application 2: Jacobians over $\mathbb{Q}$ with large torsion

Howe/Leprévost/Poonen, *Forum Math.* (2000)

- Choose elliptic curves E_1, E_2 over $\mathbb{Q}$ such that
  - E_1 and E_2 have large rational torsion subgroups;
  - $E_1[2]$ and $E_2[2]$ are isomorphic Galois modules.
- Glue E_1 and E_2 along 2-torsion, get a genus-2 curve C.
- Jac C has large rational torsion:
  - Odd part is same as $E_1 \times E_2$.
  - Even part is generally smaller.
  - With effort, can choose E_1 and E_2 so that even part does not shrink too much.

Obtained many torsion groups, including $\mathbb{Z}/63\mathbb{Z}$.

What about using 3-gluing?

New strategy

- Choose elliptic curves E_1, E_2 over $\mathbb{Q}$ such that
  - E_1 and E_2 have large rational torsion subgroups;
  - There is a Galois-equivariant anti-isometry $E_1[3] \to E_2[3]$.
- Glue E_1 and E_2 along 3-torsion, get a genus-2 curve C.
- Jac C has large rational torsion:
  - Non-3 part is same as $E_1 \times E_2$.
  - 3-part is generally smaller.

Choosing the elliptic curves

Implementation

- Make a list of low-height elliptic curves with large torsion.
- Find E_1, E_2 having an anti-isometry $E_1[3] \to E_2[3]$.

Checking for an anti-isometry

- Do 3-division polynomials define isomorphic $\mathbb{Q}$-algebras?
- If so, apply 3-gluing formulas and see if you get anything!

Disadvantage: Will get isolated examples, not families.

Examples of new torsion groups obtained so far...

Torsion group $\mathbb{Z}/36\mathbb{Z}$

Glue an elliptic curve with $\mathbb{Z}/9\mathbb{Z}$ to one with $\mathbb{Z}/12\mathbb{Z}$.
Found two examples.

Torsion group $\mathbb{Z}/56\mathbb{Z}$

Glue an elliptic curve with $\mathbb{Z}/7\mathbb{Z}$ to one with $\mathbb{Z}/8\mathbb{Z}$.
Found one example.

Torsion group $\mathbb{Z}/70\mathbb{Z}$

Glue an elliptic curve with $\mathbb{Z}/7\mathbb{Z}$ to one with $\mathbb{Z}/10\mathbb{Z}$.
Found one example, giving a new record torsion point order!

$$y^2 = 4x^6 - 36x^5 - 35x^4 + 390x^3 + 1237x^2 + 924x + 4356$$