Does There Exist an Elliptic Curve $E/\mathbb{Q}$ with Mordell-Weil Group $Z_2 \times Z_8 \times \mathbb{Z}^4$?

Edray Herber Goins

Department of Mathematics, Purdue University

Atkin Memorial Lecture and Workshop:
Elliptic Curves over $\mathbb{Q}(\sqrt{5})$

April 29, 2012

PURDUE UNIVERSITY

Abstract

An elliptic curve E defined over the rational numbers $\mathbb{Q}$ is an arithmetic-algebraic object: It is simultaneously a nonsingular projective curve with an affine equation $Y^2 = X^3 + A\,X + B$, which allows one to perform arithmetic on its points; and a finitely generated abelian group $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, which allows one to apply results from abstract algebra. The abstract nature of its rank r can be made explicit by searching for rational points (X, Y).

The largest possible subgroup of an elliptic curve E is $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$, and, curiously, these curves seem to have the least known information about the rank r. To date, there are twenty-seven known examples of elliptic curves over $\mathbb{Q}$ having Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$, yet no larger rank has been found.

In this talk, we give some history on the problem of determining properties of r and analyze various approaches to finding curves of large rank.

Outline of Talk

1. Motivation
   - Challenge Problem
   - Elliptic Integrals
   - Addition Formulas

2. Elliptic Curves
   - Mordell-Weil Group
   - Are the ranks unbounded?
   - $Z_2 \times Z_4$ and $Z_2 \times Z_8$

3. Ranks of $y^2 = (1 - x^2)(1 - k^2 x^2)$
   - Examples
   - Lower Bounds
   - 2-Descent

Challenge Problem

$$E: \ y^2 = x^3 + \left(5 - \sqrt{5}\right) x^2 + \sqrt{5}\, x$$

- The curve has invariant $j(E) = 86048 - 38496\sqrt{5}$.
- The curve has conductor $\mathfrak{f}_E = \mathfrak{p}_2^6 \, \mathfrak{p}_5^2$ in terms of the prime ideals $\mathfrak{p}_2 = 2\,\mathbb{Z}[\varphi]$ and $\mathfrak{p}_5 = \sqrt{5}\;\mathbb{Z}[\varphi]$, where $\varphi = \frac{1+\sqrt{5}}{2}$.
- This curve is 2-isogeneous to (a quadratic twist of) its Galois conjugate.

Theorem (G–, 1999)

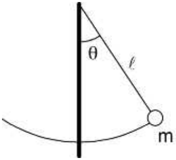
The elliptic curve E is modular. More precisely, there is a modular form $f(q) \in S_2\big(\Gamma_0(160), \epsilon\big)$ and a Dirichlet character $\chi : \mathbb{Z}[\varphi] \to \mathbb{C}$ such that $\chi^2 = \epsilon \circ \mathbb{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}$ and $a_{\mathfrak{p}}(f) = \chi(\mathfrak{p})\, a_{\mathfrak{p}}(E)$ for almost all primes $\mathfrak{p}$.

Challenge

Compute the Mordell-Weil group $E\big(\mathbb{Q}(\sqrt{5})\big)$ before the end of this talk!

My Favorite Elliptic Curve:

$$y^2 = \left(1 - x^2\right)\left(1 - k^2\, x^2\right)$$



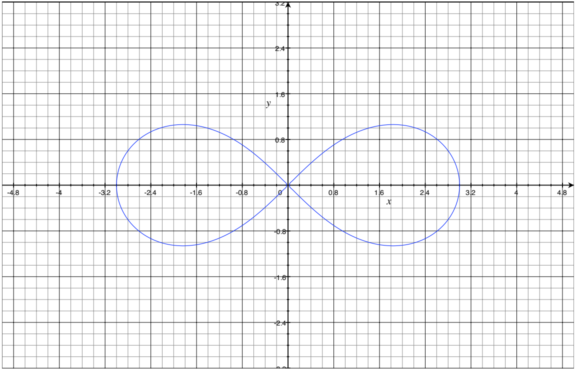
Theorem (Galileo Galilei, 1602; Christiaan Huygens, 1673)

Say we have a mass m attached to a rigid rod of length ℓ that is allowed to swing back and forth at one end. The period of the oscillation, given an initial angle θ_0, is

$$\text{Period} = 4\sqrt{\frac{\ell}{g}} \cdot K\left(\sin\frac{\theta_0}{2}\right) = 2\pi\sqrt{\frac{\ell}{g}}\left[1 + \frac{1}{4}\sin^2\frac{\theta_0}{2} + \cdots\right]$$

in terms of the **complete elliptic integral of the first kind**:

$$K(k) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2\,t^2)}} = \frac{\pi}{2}\sum_{n=0}^{\infty}\left[\frac{(2n-1)!!}{(2n)!!}\right]^2 k^{2n}.$$



Theorem (Jakob Bernoulli, 1694)

The circumference of the **lemniscus** $\left(x^2 + y^2\right)^2 = a^2 \left(x^2 - y^2\right)$ is

$$\text{Arc Length} = 4\,a \cdot K(\sqrt{-1}) = 2\pi a \sum_{n=0}^{\infty} (-1)^n \left[\frac{(2n-1)!!}{(2n)!!}\right]^2 .$$

Theorem (Giulio Fagnano, 1718)

Define $w = w(z)$ implicitly via $z = \int_0^w \frac{dt}{\sqrt{1-t^4}}$. Then

$$w(2\,z) = \frac{2\,w(z)\,w'(z)}{1+w(z)^4} \qquad \text{where} \qquad w'(z) = \sqrt{1-w(z)^4}.$$

Theorem (Leonhard Euler, 1751)

Fix a modulus k satisfying $|k| < 1$, and define $w = w(z)$ implicitly via the **incomplete elliptic integral** $z = \int_0^w \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}}$. Then

$$w(z \pm \xi) = \frac{w(z)\,w'(\xi) \pm w'(z)\,w(\xi)}{1-k^2\,w(z)^2\,w(\xi)^2}$$

where $w'(z) = \sqrt{[1-w(z)^2]\,[1-k^2\,w(z)^2]}$.

Remark: $w(z) = \mathrm{sn}(z)$ is a **Jacobi elliptic function**.

Theorem

- The Jacobi elliptic function $\mathrm{sn} : \mathbb{C}/\Lambda \to \mathbb{C}$ is well-defined modulo the period lattice $\Lambda = \{m\,\omega_1 + n\,\omega_2 \mid m, n \in \mathbb{Z}\}$ in terms of the integrals

$$\omega_1 = 2 \int_{-1/k}^{1/k} \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}} = \frac{4}{k} \cdot K\left(\frac{1}{k}\right)$$
$$\omega_2 = 2 \int_{-1}^{1} \frac{dt}{\sqrt{(1-t^2)\,(1-k^2\,t^2)}} = 4 \cdot K(k)$$

- The map $\mathbb{C}/\Lambda \to \mathbb{C}^2$ which sends $z \mapsto \big(\mathrm{sn}(z), \mathrm{sn}'(z)\big)$ parametrizes all points (x, y) on the quartic curve $y^2 = \left(1 - x^2\right)\left(1 - k^2\,x^2\right)$. Moreover, $0 \mapsto (0, 1)$.

- Say that $P = \big(\mathrm{sn}(z), \mathrm{sn}'(z)\big)$ and $Q = \big(\mathrm{sn}(\xi), \mathrm{sn}'(\xi)\big)$ are on the quartic curve. Then $P \oplus Q = \big(\mathrm{sn}(z+\xi), \mathrm{sn}'(z+\xi)\big)$ has coordinate

$$x(P \oplus Q) = \frac{x(P)\,y(Q) \pm y(P)\,x(Q)}{1 - k^2\,x(P)^2\,x(Q)^2}.$$

Proposition

$y^2 = \left(1 - x^2\right)\left(1 - k^2 x^2\right)$ is a quadric intersection in $\mathbb{P}^3$ and has a Weierstrass model in $\mathbb{P}^2$. It is nonsingular if and only if $k \neq -1, 0, 1$.

$$y^2 = \left(1 - x^2\right)\left(1 - k^2 x^2\right) \qquad (x, y) = \left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$$

$$\uparrow$$

$$\begin{aligned} x_2^2 &= \left(x_3 - x_0\right)\left(k^2 x_3 - x_0\right) \\ x_1^2 &= x_3\, x_0 \end{aligned} \qquad \left(x_1 : x_2 : x_3 : x_0\right)$$

$$\downarrow$$

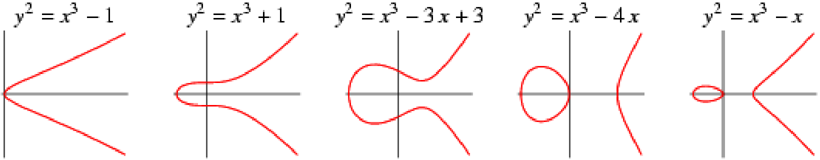
$$\begin{aligned} Y^2 Z &= X^3 + A\, X\, Z^2 + B\, Z^3 \\ A &= -27\left(k^4 + 14\, k^2 + 1\right) \\ B &= -54\left(k^6 - 33\, k^4 - 33\, k^2 + 1\right) \end{aligned} \qquad \begin{aligned} \frac{X}{Z} &= \frac{3\left(5\, k^2 - 1\right) x + 3\left(k^2 - 5\right)}{x - 1} \\ \frac{Y}{Z} &= \frac{54\left(1 - k^2\right) y}{(x - 1)^2} \end{aligned}$$

Elliptic Curves

More generally, we consider cubic curves

$$E: \quad Y^2 = X^3 + A X + B$$

where the rational numbers A and B satisfy $4 A^3 + 27 B^2 \neq 0$.



Given a field K such as either $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or even $\mathbb{Q}(\sqrt{5})$, denote

$$E(K) = \left\{ (X : Y : Z) \in \mathbb{P}^2(K) \;\middle|\; Y^2 Z = X^3 + A X Z^2 + B Z^3 \right\}.$$

Remark: $\mathcal{O} = (0 : 1 : 0)$ comes from $(x, y) = (1, 0)$ – not $(x, y) = (0, 1)$!

Mordell-Weil Group

Conjecture (Henri Poincaré, 1901)

Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a **finitely generated** abelian group.

Theorem (Louis Mordell, 1922; André Weil, 1928)

Let E be an elliptic curve over a number field K. There exists a group $E(K)_{\text{tors}}$ and a nonnegative integer r such that $E(K) \simeq E(K)_{\text{tors}} \times \mathbb{Z}^r$.

Theorem (Barry Mazur, 1977)

The torsion subgroup of an elliptic curve E over $\mathbb{Q}$ is one of fifteen types:

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} Z_N & \text{for } 1 \leq N \leq 10 \text{ or } N = 12; \\ Z_2 \times Z_{2N} & \text{for } 1 \leq N \leq 4. \end{cases}$$

Question: What can one say about the Mordell-Weil rank $r = r(E)$?

Rank Conjecture

Conjecture

Let T be one of the fifteen torsion groups in Mazur's Theorem. For any given nonnegative integer r_0, there exists an elliptic curve E over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq T$ and Mordell-Weil rank $r(E) \geq r_0$.

Project

Given T and r_0, find an elliptic curve E over with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq T$ and Mordell-Weil rank $r(E) \geq r_0$.

For each torsion group T, define the quantity

$$B(T) = \sup \left\{ r \in \mathbb{Z} \;\middle|\; \text{there exists a curve } E \text{ with } E(\mathbb{Q}) \simeq T \times \mathbb{Z}^r \right\}.$$

Question: Is $B(T)$ unbounded?

Competing Points of View

Conjecture (Taira Honda, 1960)

If E is an elliptic curve defined over $\mathbb{Q}$, and K is a number field, then the ratio of the Mordell-Weil rank of $E(K)$ to the degree $[K : \mathbb{Q}]$ should be uniformly bounded by a constant depending only on E.

Remark: If true, this would imply that there are infinite families of elliptic curves over the rational numbers which have a uniformly bounded rank.

Theorem (Igor Shafarevich and John Tate, 1967)

The ranks are not uniformly bounded for elliptic curves defined over function fields $\mathbb{F}_q(t)$.

$E(\mathbb{Q})_{\text{tors}}$	Highest Known Rank r	Found By	Year Discovered
Trivial	28	Elkies	2006
Z_2	19	Elkies	2009
Z_3	13	Eroshkin	2007, 2008, 2009
Z_4	12	Elkies	2006
Z_5	8	Dujella, Lecacheux Eroshkin	2009 2009
Z_6	8	Eroshkin Dujella, Eroshkin Elkies Dujella	2008 2008 2008 2008
Z_7	5	Dujella, Kulesz Elkies Eroshkin Dujella, Lecacheux Dujella, Eroshkin	2001 2006 2009 2009 2009
Z_8	6	Elkies	2006
Z_9	4	Fisher	2009
Z_{10}	4	Dujella Elkies	2005, 2008 2006
Z_{12}	4	Fisher	2008
$Z_2 \times Z_2$	15	Elkies	2009
$Z_2 \times Z_4$	8	Elkies Eroshkin Dujella, Eroshkin	2005 2008 2008
$Z_2 \times Z_6$	6	Elkies	2006
$Z_2 \times Z_8$	3	Connell Dujella Campbell, Goins Rathbun Flores, Jones, Rollick, Weigandt, Rathbun Fisher	2000 2000, 2001, 2006, 2008 2003 2003, 2006 2007 2009

http://web.math.hr/~duje/tors/tors.html

Classification

Theorem

Fix a rational $k \neq -1, 0, 1$ for the curve $E_k : y^2 = (1 - x^2)(1 - k^2 x^2)$.

- $E_k(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} Z_2 \times Z_8 & \text{if } k = \dfrac{t^4 - 6t^2 + 1}{(t^2+1)^2} \text{ for some rational } t, \\ Z_2 \times Z_4 & \text{otherwise.} \end{cases}$
- Conversely, if E is an elliptic curve over K with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_4$ or $Z_2 \times Z_8$, then $E \simeq E_k$ for some $k \in K$.

- The modular curve $X_0(24) : Y^2 = X^3 + 5\,X^2 + 4\,X$ has Mordell-Weil group $X_0(24)(\mathbb{Q}) \simeq Z_2 \times Z_4$, and so corresponds to $k = 1/3$.
- The modular curve $X_1(15) : Y^2 + X\,Y + Y = X^3 + X^2 - 10\,X - 10$ has $X_1(15)(\mathbb{Q}) \simeq Z_2 \times Z_4$, and so corresponds to $k = 1/9$. Moreover, $X_1(15)(\mathbb{Q}(\sqrt{5})) \simeq Z_2 \times Z_8$, and so $t = (3 - \sqrt{5})/2$.

$$\begin{tikzcd}
X(2,8) = \dfrac{\mathcal{H}^*}{\Gamma(2) \cap \Gamma_1(8)} \arrow[r, "2"] \arrow[d, "4"] & X_1(8) = \dfrac{\mathcal{H}^*}{\Gamma_1(8)} \arrow[r, "2"] \arrow[d, "4"] & X_0(8) = \dfrac{\mathcal{H}^*}{\Gamma_0(8)} \arrow[d, "2"] \\
X(2,4) = \dfrac{\mathcal{H}^*}{\Gamma(2) \cap \Gamma_1(4)} \arrow[r, "2"] \arrow[d, "2"] & X_1(4) = \dfrac{\mathcal{H}^*}{\Gamma_1(4)} \arrow[r, "1"] \arrow[d, "2"] & X_0(4) = \dfrac{\mathcal{H}^*}{\Gamma_0(4)} \arrow[d, "2"] \\
X(2) = \dfrac{\mathcal{H}^*}{\Gamma(2)} \arrow[r, "2"] \arrow[d, "6"] & X_1(2) = \dfrac{\mathcal{H}^*}{\Gamma_1(2)} \arrow[r, "1"] \arrow[d, "3"] & X_0(2) = \dfrac{\mathcal{H}^*}{\Gamma_0(2)} \arrow[d, "3"] \\
X(1) = \dfrac{\mathcal{H}^*}{SL_2(\mathbb{Z})} \arrow[r, "1"] & X_1(1) = \dfrac{\mathcal{H}^*}{SL_2(\mathbb{Z})} \arrow[r, "1"] & X_0(1) = \dfrac{\mathcal{H}^*}{SL_2(\mathbb{Z})}
\end{tikzcd}$$

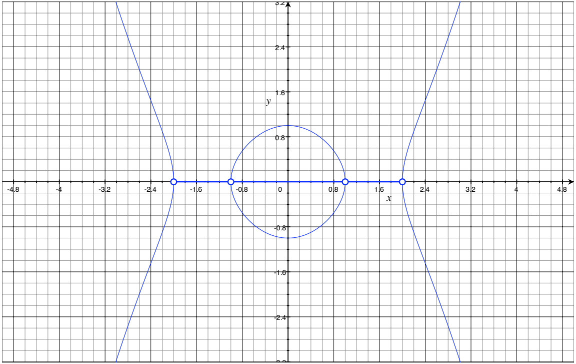
$$
\begin{tikzcd}
\begin{aligned} k(q) &= 4 \left[\frac{\eta(q)}{\eta(q^2)} \right]^4 \left[\frac{\eta(q^4)}{\eta(q^2)} \right]^8 \\ &= \frac{t(q)^4 - 6\,t(q)^2 + 1}{(t(q)^2+1)^2} \end{aligned} \arrow[r] \arrow[d] & \begin{aligned} \mu_4(q) &= \left[\frac{\eta(q^2)}{\eta(q)} \right]^8 \left[\frac{\eta(q^2)}{\eta(q^4)} \right]^{16} \\ &= \frac{16}{k(q)^2} \end{aligned} \arrow[r] \arrow[d] & \begin{aligned} \nu_4(q) &= \left[\frac{\eta(q)}{\eta(q^4)} \right]^8 \\ &= \mu_4(q) - 16 \end{aligned} \arrow[d] \\
\begin{aligned} \lambda(q) &= \frac{1}{16} \left[\frac{\eta(q)^3}{\eta(q^{1/2})\,\eta(q^2)^2} \right]^8 \\ &= \frac{4\,k(q)}{(k(q)+1)^2} \end{aligned} \arrow[r] \arrow[d] & \begin{aligned} \mu_2(q) &= \left[\frac{\eta(q)}{\eta(q^2)} \right]^{24} \\ &= 256\,\lambda(q)\,(\lambda(q) - 1) \\ &= \frac{(\mu_4(q) - 16)^2}{\mu_4(q)} \end{aligned} \arrow[r] \arrow[d] & \begin{aligned} \nu_2(q) &= \left[\frac{\eta(q)}{\eta(q^2)} \right]^{24} \\ &= \mu_2(q) \\ &= \frac{\nu_4(q)^2}{\nu_4(q) + 16} \end{aligned} \arrow[d] \\
j(q) = 256\,\frac{(\lambda(q)^2 - \lambda(q) + 1)^3}{\lambda(q)^2\,(\lambda(q) - 1)^2} \arrow[r] & j(q) = \frac{(\mu_2(q) + 256)^3}{\mu_2(q)^2} \arrow[r] & j(q) = \frac{\left[1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)\,q^n \right]^3}{q \prod_{n=1}^{\infty} (1 - q^n)^{24}}
\end{tikzcd}
$$

http://phobos.ramapo.edu/~kmcmurdy/research/Models/index.html

Example

On the quartic curve $y^2 = (1 - x^2)(1 - k^2 x^2)$, the rational point (x, y) has order 2 if and only if $[2](x, y) = (1, 0)$. There are only four:

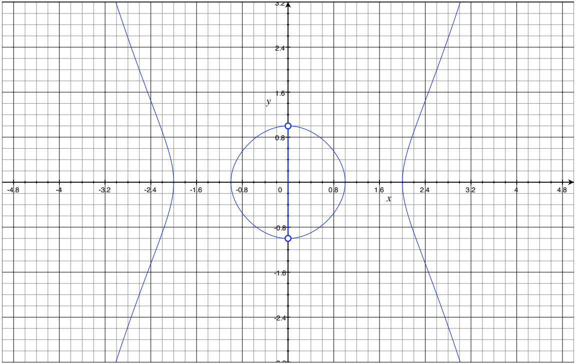
$$\left(\frac{1}{k}, 0\right), \qquad (1, 0), \qquad (-1, 0), \qquad \text{and} \qquad \left(-\frac{1}{k}, 0\right).$$



Example

On the quartic curve $y^2 = (1 - x^2)(1 - k^2 x^2)$, the rational point (x, y) has order 4 if and only if $[2]\,(x, y) = (*, 0)$. There are only four:

$(0, 1)$, $(0, -1)$, and (two points at infinity).



$E(\mathbb{Q}) \simeq Z_2 \times Z_4 \times \mathbb{Z}^r$

Rank r = 8:

Author(s)	Fiber k	Year Discovered
Elkies	556536737101/589636934451	2005
Eroshkin	14124977/18685325	2008
	9305732817/11123766133	2008
Dujella, Eroshkin	14426371/71784369	2008
	1082331841/1753952791	2008

Rank r = 7:

Author(s)	Fiber k	Year Discovered
Dujella	5759699/11291091	2005
	151092883/281864499	2005
	106979869/131157975	2006
	76547009/172129849	2006
	772368397/787678274	2006
	66285529/1515865129	2006
	2524013211/3323768713	2006
	2125660499/3416463309	2006
	1119101519/3685417369	2006
	3169123561/3910987351	2006
Eroshkin	2978252/8060923	2008
	1297409/8215809	2008
	85945462/122383087	2008
	249238749/403292341	2008
Dujella, Eroshkin	152618/204943	2008
	255739/328279	2008

Rank r = 6:

Author(s)	Fiber k	Year Discovered
Ansaldi, Ford, George, Mugo, Phifer	307100/384569	2005
	94939/471975	2005

http://web.math.pmf.unizg.hr/~duje/tors/z2z4.html
http://web.math.pmf.unizg.hr/~duje/tors/z2z4old67.html

$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$

Author(s)	Fiber t	Year Discovered
Connell, Dujella	5/29	2000
Dujella	18/47	2001
	87/407	2006
	143/419	2006
	145/444	2006
	352/1017	2008
Dujella, Rathbun	230/923	2006
	223/1012	2006
Campbell, Goins	15/76	2003
Campbell, Goins (with Watkins)	19/220	2005
Rathbun	47/219	2003
	74/207	2006
	17/439	2006
	159/569	2006
Flores - Jones - Rollick - Weigandt (with Rathbun)	86/333	2007
	101/299	2007
	65/337	2007
Fisher	47/266	2009
	104/321	2009
	97/488	2009
	145/527	2009
	119/579	2009
	223/657	2009
	161/779	2009
	177/815	2009
	76/999	2009
	285/1109	2009

http://web.math.pmf.unizg.hr/~duje/tors/z2z8.html

Example

In 2006, Dujella discovered the elliptic curve

$$E: \begin{aligned} Y^2 + X\,Y = X^3 &- 15343063417941874422081256126489574987160\,X \\ &+ 486503741336910955243717595559583892156442731284430865537600 \end{aligned}$$

with conductor

$$\begin{aligned} N_E &= 178537663111997545240602 90 \end{aligned}$$

$$= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 97 \cdot 313 \cdot 449 \cdot 47351$$

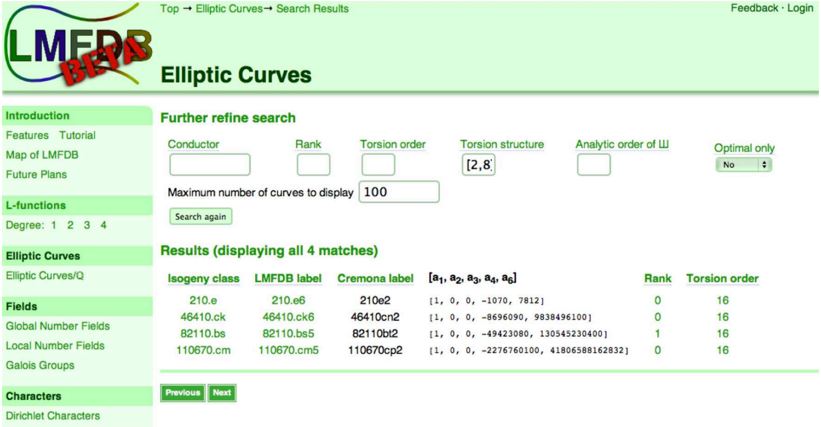
has Mordell-Weil group $E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$. Using the substitutions

$$X = -\frac{6240(4083958238540477\,x + 3711823331862791 8)}{x - 1},$$

$$Y = \frac{1560}{(x-1)^2} \left(\begin{aligned} &19609862486034251499973867 95\,y \\ &+ 8167911647708095 4\,x^2 \\ &+ 6606855016017488 2\,x - 7423646663725583 6 \end{aligned} \right)$$

we see that it is birationally equivalent to the quartic curve with

$$k = \frac{14435946721}{47594221921} = \frac{t^4 - 6\,t^2 + 1}{(t^2+1)^2} \qquad \text{where} \qquad t = \frac{145}{444}.$$



Top → Elliptic Curves → Search Results

Feedback · Login

LMFDB BETA

Elliptic Curves

Introduction
Features Tutorial
Map of LMFDB
Future Plans

L-functions
Degree: 1 2 3 4

Elliptic Curves
Elliptic Curves/Q

Fields
Global Number Fields
Local Number Fields
Galois Groups

Characters
Dirichlet Characters

Further refine search

Conductor | Rank | Torsion order | Torsion structure [2,8] | Analytic order of Ш | Optimal only No

Maximum number of curves to display 100

Search again

Results (displaying all 4 matches)

Isogeny class	LMFDB label	Cremona label	$[a_1, a_2, a_3, a_4, a_6]$	Rank	Torsion order
210.e	210.e6	210e2	[1, 0, 0, -1070, 7812]	0	16
46410.ck	46410.ck6	46410cn2	[1, 0, 0, -8696090, 9838496100]	0	16
82110.bs	82110.bs5	82110bt2	[1, 0, 0, -49423080, 130545230400]	1	16
110670.cm	110670.cm5	110670cp2	[1, 0, 0, -2276760100, 41806588162832]	0	16

Previous Next

`http://www.lmfdb.org/`

Can we do better than

$$E(\mathbb{Q}) \simeq Z_2 \times Z_4 \times \mathbb{Z}^8$$

or

$$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3?$$

Elliptic Surfaces

We will focus on the cases where the quartic curve $E_k : y^2 = (1 - x^2)(1 - k^2 x^2)$ has torsion subgroup $E_k(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. We express our results in terms of elliptic surfaces.

Consider the affine curve

$$C = \left\{ t = (a : b) \in \mathbb{P}^1 \;\middle|\; a\, b\, \left(a^4 - b^4\right) \left(a^4 - 6\, a^2\, b^2 + b^4\right) \neq 0 \right\}.$$

Fix the rational functions $A,\ B : C \to \mathbb{P}^1$ defined by

$$\begin{aligned} A(t) &= -27 \left(k^4 + 14\, k^2 + 1\right) \\ B(t) &= -54 \left(k^6 - 33\, k^4 - 33\, k^2 + 1\right) \end{aligned} \qquad \text{where} \qquad k = \frac{t^4 - 6\, t^2 + 1}{\left(t^2 + 1\right)^2}$$

and consider the surface

$$\mathcal{E} = \left\{ \left[(X : Y : Z),\ t\right] \in \mathbb{P}^2 \times C \;\middle|\; Y^2\, Z = X^3 + A(t)\, X\, Z^2 + B(t)\, Z^3 \right\}.$$

Theorem (G–, 2008)

- With respect to $\mathcal{E} \to C$ which sends $\big[(X : Y : Z),\ t\big] \mapsto t$, the variety $\mathcal{E}$ is an elliptic surface. Each of the fibers E_t is semistable.

- We have two sections

$$P: \quad t \mapsto \left[\left(12\,\frac{t^8 - 4\,t^6 - 26\,t^4 - 4\,t^2 + 1}{(t^2+1)^4} : 0 : 1\right), t\right]$$

$$Q: \quad t \mapsto \left[\left(12\,\frac{t^8 - 4\,t^6 - 12\,t^5 - 2\,t^4 + 20\,t^2 + 12\,t + 1}{(t^2+1)^4} : 864\,\frac{t^7 - 5\,t^5 - 4\,t^4 + 3\,t^3 + 4\,t^2 + t}{(t^2+1)^5} : 1\right), t\right]$$

- All elliptic curves E over a number field K with torsion subgroup $\langle P(t),\, Q(t)\rangle \simeq Z_2 \times Z_8$ arise from such a fiber, i.e., are birationally equivalent to E_t for some $t \in C(K)$.

- The automorphisms $\sigma : (a : b) \mapsto (a - b : a + b)$ and $\tau : (a : b) \mapsto (-a : b)$ act on C, yet leave A and B invariant. Moreover, $D_8 = \langle \sigma, \tau \rangle \hookrightarrow \mathrm{Aut}(C)$ is the dihedral group.

Proposition (A. O. L. Atkin and François Morain, 1993)

- The elliptic curve $C_1 : v^2 = u^3 - 8u - 32$ has Mordell-Weil group $C_1(\mathbb{Q}) \simeq Z_2 \times \mathbb{Z}$ as generated by $(u : v : 1) = (12 : 40 : 1)$.
- One can construct infinitely many fibers E_t having positive rank via the map $C_1 \to C$ defined by $(u : v : 1) \mapsto 2(u-9)/(3u+v-2)$.

Theorem (Garikai Campbell and G–, 2003)

- The elliptic curve $C_2 : v^2 = u^3 - u^2 - 9u + 9$ has Mordell-Weil group $C_2(\mathbb{Q}) \simeq Z_2 \times Z_2 \times \mathbb{Z}$ as generated by $(u : v : 1) = (5 : 8 : 1)$.
- One can construct infinitely many fibers E_t having positive rank via the map $C_2 \to C$ defined by $(u : v : 1) \mapsto t = (u+v-3)/(2u)$. Indeed, upon setting $w = 3(u^2 - 2u + 4v + 9)/(u^2 - 18u + 9)$, we have a section

$$R : \quad (u : v : 1) \mapsto \left[\left(\frac{3(w^2-2w-3)^4 + 12(w^2-w-3)(w^2+2w-3)^3}{(w^4-2w^2+9)^2} : \frac{54(w^4-9)(w^2-2w-3)(w^2+2w-3)^3}{(w^4-2w^2+9)^3} : 1 \right), \frac{u+v-3}{2u} \right]$$

Infinite Families

There are infinitely many choices of rational t such that

$$E_t : y^2 = (1 - x^2)(1 - k^2 x^2) \qquad \text{where} \qquad k = \frac{t^4 - 6t^2 + 1}{(t^2+1)^2}$$

has torsion subgroup $E_t(\mathbb{Q}) \simeq Z_2 \times Z_8$ and rank $r \geq 1$. These choices of t correspond to rational points on elliptic curves.

Open Questions

- Are there other elliptic curves besides C_1 and C_2 which work?
- Is there a curve of genus 0 which gives E_t having rank $r \geq 1$?
- Are there infinitely many rational t which give E_t having rank $r \geq 2$?

Finding Curves of High Rank

Approach #1

Fix a square-free integer D, and consider the **quadratic twist**

$$E^{(D)}: \qquad Y^2 = X^3 + D^2 A X + D^3 B.$$

This is very efficient (i.e., no redundant curves), but $E^{(D)}(\mathbb{Q})_{\text{tors}}$ changes with each D.

Approach #2

Fix polynomials $A = A(t)$ and $B = B(t)$ such that $\Delta(t) = -16\left(4A^3 + 27B^2\right) \neq 0$, and consider the **elliptic surface**

$$E_t: \qquad Y^2 = X^3 + A(t)\,X + B(t).$$

This is not very efficient (i.e., different t's may give the same curves), polynomials can be chosen to fix $E_t(\mathbb{Q})_{\text{tors}}$ for all t.

Algorithm

#1. Classify those elliptic curves E over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{\text{tors}} \simeq Z_2 \times Z_8$. Express these curves as an elliptic surface E_t.

#2. Find a criterion on t such that any $t \in \mathbb{Q}$ may be associated to an element from a fundamental region $\alpha < t < \beta$.

#3. Create a list of candidate elliptic curves E_t for this fundamental region.

#4. Compute the 2-Selmer ranks to find upper bounds on the Mordell-Weil ranks.

#5. Compute the Mordell-Weil ranks.

$E(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$

Author(s)	Fiber t	Year Discovered
Connell, Dujella	5/29	2000
Dujella	18/47	2001
	87/407	2006
	143/419	2006
	145/444	2006
	352/1017	2008
Dujella, Rathbun	230/923	2006
	223/1012	2006
Campbell, Goins	15/76	2003
Campbell, Goins (with Watkins)	19/220	2005
Rathbun	47/219	2003
	74/207	2006
	17/439	2006
	159/569	2006
Flores - Jones - Rollick - Weigandt (with Rathbun)	86/333	2007
	101/299	2007
	65/337	2007
Fisher	47/266	2009
	104/321	2009
	97/488	2009
	145/527	2009
	119/579	2009
	223/657	2009
	161/779	2009
	177/815	2009
	76/999	2009
	285/1109	2009

http://web.math.pmf.unizg.hr/~duje/tors/z2z8.html

Fundamental Region

Theorem (G–, 2006)

Fix a rational number $t \neq -1, 0, 1$ and consider

$$E_t : \qquad y^2 = \left(1 - x^2\right)\left(1 - k^2 x^2\right) \quad \text{where} \quad k = \frac{t^4 - 6\,t^2 + 1}{(t^2+1)^2}.$$

- $D_8 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\,\sigma\,\tau = \sigma^{-1} \rangle$ in terms of

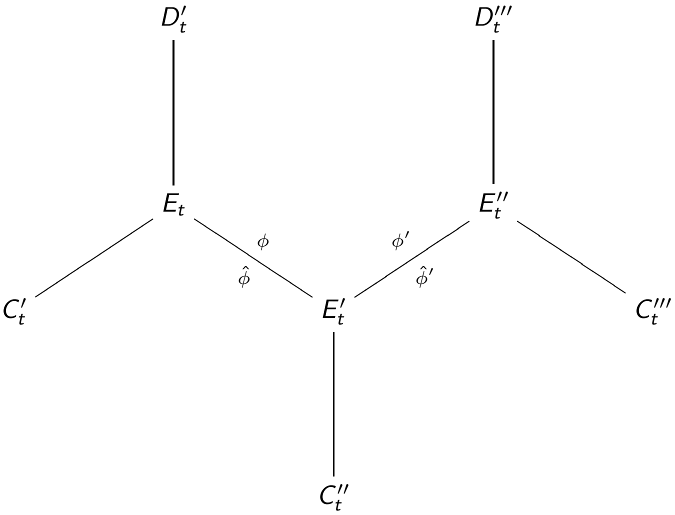
$$\sigma : \ t \mapsto \frac{t-1}{t+1} \qquad \text{and} \qquad \tau : \ t \mapsto -t.$$

- We may assume that t satisfies $0 < t < \sqrt{2} - 1$.

Remark: Given a bound N, choose coprime integers a and b satisfying

$$0 < \left(1 + \sqrt{2}\right) a < b < N \qquad \text{and set} \qquad t = \frac{a}{b}.$$

Isogeny Graph



Isogeny Graph

Curve	Weierstrass Model $Y^2 = X^3 + A\,X + B$	Torsion
E_t	$A = -27\left(k^4 + 14\,k^2 + 1\right)$ $B = -54\left(k^6 - 33\,k^4 - 33\,k^2 + 1\right)$	$Z_2 \times Z_8$
E_t'	$A = -27\left(k^4 - k^2 + 1\right)$ $B = -27\left(2\,k^6 - 3\,k^4 - 3\,k^2 + 2\right)$	$Z_2 \times Z_4$
C_t'	$A = -27\left(k^4 - 60\,k^3 + 134\,k^2 - 60\,k + 1\right)$ $B = -54\left(k^6 + 126\,k^5 - 1041\,k^4 + 1764\,k^3 - 1041\,k^2 + 126\,k + 1\right)$	Z_8
D_t'	$A = -27\left(k^4 + 60\,k^3 + 134\,k^2 + 60\,k + 1\right)$ $B = -54\left(k^6 - 126\,k^5 - 1041\,k^4 - 1764\,k^3 - 1041\,k^2 - 126\,k + 1\right)$	Z_8
E_t''	$A = -27\left(k^4 - 16\,k^2 + 16\right)$ $B = -54\left(k^6 + 30\,k^4 - 96\,k^2 + 64\right)$	$Z_2 \times Z_2$
C_t''	$A = -27\left(16\,k^4 - 16\,k^2 + 1\right)$ $B = -54\left(64\,k^6 - 96\,k^4 + 30\,k^2 + 1\right)$	Z_4
C_t'''	$y^2 = x^3 - 2\left(1 + 24\,t + 20\,t^2 + 24\,t^3 - 26\,t^4 - 24\,t^5 + 20\,t^6 - 24\,t^7 + t^8\right) x^2$ $+ \left(1 - 2\,t - t^2\right)^8 x$	Z_2
D_t'''	$y^2 = x^3 - 2\left(1 - 24\,t + 20\,t^2 - 24\,t^3 - 26\,t^4 + 24\,t^5 + 20\,t^6 + 24\,t^7 + t^8\right) x^2$ $+ \left(1 + 2\,t - t^2\right)^8 x$	Z_8

Define the curves and homogeneous spaces

$$E_t : y^2 = \left(1 - x^2\right)\left(1 - k^2 x^2\right) \qquad \mathcal{C}_d : d\, w^2 = \left(1 - d\, z^2\right)\left(1 - d\, k^2 z^2\right)$$

$$E_t' : y^2 = \left(1 - x^2\right)\left(1 - \kappa'^2 x^2\right) \qquad \mathcal{C}_d' : d\, w^2 = \left(1 + d\, z^2\right)\left(1 + d\, \kappa^2 z^2\right)$$

$$E_t'' : y^2 = \left(1 + x^2\right)\left(1 + k'^2 x^2\right) \qquad \mathcal{C}_d'' : d\, w^2 = \left(1 + d\, z^2\right)\left(1 + d\, k'^2 z^2\right)$$

where

$$\kappa = \frac{1-k}{1+k}, \qquad \kappa' = \frac{1-k'}{1+k'}, \qquad \text{and} \qquad k^2 + k'^2 = 1.$$

$$\begin{tikzcd}
D_t''' \arrow[r] \arrow[d, dotted, leftrightarrow] & E_t'' \arrow[r, "\hat{\phi}'"] \arrow[d, dotted, leftrightarrow] & E_t' \arrow[r, "\hat{\phi}"] \arrow[d, dotted, leftrightarrow] & E_t \\
\mathcal{C}_d''' \arrow[r, "\Phi'"] \arrow[ur] & \mathcal{C}_d'' \arrow[r, "\Phi"] \arrow[ur, "\psi'"] & \mathcal{C}_d' \arrow[ur, "\psi"] &
\end{tikzcd}$$

Descent via 4-Isogeny

Theorem (G–, 2006)

- There are 2-isogenies $\phi : E_t \to E_t'$ and $\phi' : E_t' \to E_t''$.
- If $E \simeq E_t$ and $E' \simeq E_t'$, then $\left|\dfrac{E(\mathbb{Q})}{2\,E(\mathbb{Q})}\right| = \left|\dfrac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right| \left|\dfrac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))}\right|$.
- Write $k = p/q$ for relatively prime integers p and q. The image of δ_ϕ (of $\delta_{\hat{\phi}}$, respectively) is the set of those square-free divisors d of $p\,q$ (of $p^2 - q^2$, respectively) such that $\mathcal{C}_d$ ($\mathcal{C}_d'$, respectively) has a $\mathbb{Q}$-rational point.
- $\left(\delta_{\hat{\phi}} \circ \psi\right)(z,w) \equiv \left(\delta_\phi \circ \psi'\right)(z,w) \equiv d \mod (\mathbb{Q}^\times)^2$ for the maps

$$\psi : \mathcal{C}_d' \to E_t \qquad (z,w) \mapsto \left(\frac{1 - d\,\kappa\,z^2}{1 + d\,\kappa\,z^2}, \frac{4\,d\,\kappa\,z\,w}{(1+\kappa)\,(1 + d\,\kappa\,z^2)^2}\right)$$

$$\psi' : \mathcal{C}_d'' \to E_t' \qquad (z,w) \mapsto \left(\frac{1 - d\,k'\,z^2}{1 + d\,k'\,z^2}, \frac{4\,d\,k'\,z\,w}{(1+k')\,(1 + d\,k'\,z^2)^2}\right)$$

Example

Proposition (Samuel Ivy, Brett Jefferson, Michele Josey, Cheryl Outing, Clifford Taylor, and Staci White, 2008)

When $t = 9/296$ we have

$$\langle -1, 6477590, 2, 7 \rangle \subseteq \delta_{\hat{\phi}} \subseteq \langle -1, 6477590, 2, 7, 37 \rangle.$$

Hence E_t has Mordell-Weil group $E_t(\mathbb{Q}) \simeq Z_2 \times Z_8 \times \mathbb{Z}^3$ if and only if at least one of the following homogeneous spaces corresponding to $d = 37$ contains a rational point (z, w):

$$\begin{aligned} \mathcal{C}'_{37} : \quad w^2 &= 21723443482974742731 25\, z^4 \\ &\quad + 58712815268370607681\, z^2 + 21779862847488; \\ \mathcal{C}''_{37} : \quad w^2 &= 21884703747354949737 97\, z^4 \\ &\quad + 60017913360731350081\, z^2 + 23515280943436800. \end{aligned}$$

Challenge Problem Revisited

$$E: \ y^2 = x^3 + \left(5 - \sqrt{5}\right) x^2 + \sqrt{5}\, x$$

- The curve has invariant $j(E) = 86048 - 38496\sqrt{5}$.
- The curve has conductor $\mathfrak{f}_E = \mathfrak{p}_2^6\, \mathfrak{p}_5^2$ in terms of the prime ideals $\mathfrak{p}_2 = 2\,\mathbb{Z}[\varphi]$ and $\mathfrak{p}_5 = \sqrt{5}\ \mathbb{Z}[\varphi]$, where $\varphi = \frac{1+\sqrt{5}}{2}$.
- This curve is 2-isogeneous to (a quadratic twist of) its Galois conjugate.

Theorem (G–, 1999)

The elliptic curve E is modular. More precisely, there is a modular form $f(q) \in S_2\left(\Gamma_0(160), \epsilon\right)$ and a Dirichlet character $\chi : \mathbb{Z}[\varphi] \to \mathbb{C}$ such that $\chi^2 = \epsilon \circ \mathbb{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}$ and $a_{\mathfrak{p}}(f) = \chi(\mathfrak{p})\, a_{\mathfrak{p}}(E)$ for almost all primes $\mathfrak{p}$.

Question

Did you compute the Mordell-Weil group $E\left(\mathbb{Q}(\sqrt{5})\right)$?

Questions?