# Arithmetic Progressions of Squares and Cubes over Quadratic Fields

Stephen Mussmann, Ronald Archer, Benny Martinez, Lirong Yuan, Han Liu

Department of Mathematics
Purdue University

July 31, 2012

# Background

## Abstract


- In 1640, Pierre de Fermat sent a letter to Bernard Frenicle de Bessy claiming that there are no four or more rational squares in a nontrivial arithmetic progression.
- Each 4-term arithmetic progression of perfect squares corresponds to a rational point (x : y : z) on the elliptical curve

$$E : y^2z = x^3 + 5x^2z + 4xz^2$$

and one shows that $E(\mathbb{Q}) \simeq Z_2 \times Z_4$ consists of finitely many rational points.

# Background


## Abstract

- Similar arithmetic progressions have also been studied. There are only finitely many 3-term arithmetic progressions whose terms are perfect cubes: {-1, 0 1} for example.
- Each 3-term arithmetic progressions of perfect cubes corresponds to a rational point (x : y : z) on the elliptic curve

$$E : y^2z = x^3 - 27z^3$$

and one shows that $E(\mathbb{Q}) \simeq Z_2$ consist of finitely many rational points

## Intro

- An m-term arithmetic progression is a collection of ration numbers $n_1, n_2, ., n_m$ such that there is a common difference $d = n_{i+1} - n_i$.
- Examples of non-constant 3 - term arithmetic progressions are {-1, 0 ,1} and {1, 25, 49}, where the common differences are d = 1 and d = 24, respectively.
- The latter example fits into a large family. There are infinitely many 3-term arithmetic progressions whose terms are perfect squares: consider for example the set

$$\{(x^2 - 2xz - z^2)^2, (x^2 + z^2)^2, (x^2 + 2xz - z^2)^2\}$$

for any rational numbers x and z.

# Overview

## Intro

- Both of these results can be generalized by working with larger fields. A 2009 paper in the ArXiv by Enrique Gonzalez-Jimenez and Jorn Steuding entitles "Arithmetic progressions of four squares over quadratic fields" discussed a slight generalization by looking at four squares in an arithmetic progression over quadratic extensions of the rational numbers.
- For example, one can use these results to construct the arithmetic progression

$$\{(9-5\sqrt{6})^2, (15-\sqrt{6})^2, (15+\sqrt{6})^2, (9+5\sqrt{6})^2\}$$

# Overview

## Intro

- Similarly, a 2010 paper by Enrique Gonzalez-Jimenez entitled "Three cubes in arithmetic progression over quadratic fields" discussed a slight generalization by looking at three cubes in an arithmetic progression over the same quadratic extensions.
- As an example, one can use these results to construct the arithmetic progression.

$$\{(4-21\sqrt{2})^3, 22^3, (4+21\sqrt{2})^3\}$$

# Motivation


## Summary

In this project, we seek to give explicit examples of four squares in arithmetic progressions as well as three cubes in arithmetic progression, and recast many ideas by performing a complete 2-descent of quadratic twists of certain elliptic curves. This will extend a 2010 paper Alexander Diaz, Zachary Flores, and Markus Vasquez entitled "Arithmetic Progression over Quadratic Fields"

# Definition

## Proposition

*Consider the curve*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

*Using a substitution, we find a curve in the form* $Y^2 = X^3 + AX + B$*. This is a nonsingular curve if and only if* $4A^3 + 27B^2 \neq 0$*.*

A nonsingular curve as in the proposition above is called an elliptic curve. They can be defined over any field K. K-rational points are points on the curve whose coordinates belong to K.

## Remark

*Elliptic curves are helpful because we can use it to generate solutions of diophantine equations, pythagorean triplets, heron triangles, and so on.*

# Chord-Tangent Method

- The idea behind considering non singular curves is we can draw lines - including tangent lines - to generate several points from a few known ones.
- If P and Q are K-rational points on an elliptic curve E, draw a line through them. If P=Q, then draw the line tangent to the curve at P; this line is well-defined because the gradient exists at all points on E.
- This line will intersect the curve as a third K-rational point, say P*Q. This process is known as the chord-tangent method.

# The Group Law

**Theorem**

*Denote $K$ as either $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. Consider the elliptic curve*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

*where $a_i \in K$. Let * denote the composition law which takes two $K$-rational points $P$ and $Q$ and computes the point of intersection $P*Q$ of the projective curve $E$ and the line through $P$ and $Q$. Define the composition law $P \oplus Q = (P * Q) * O$. This turns $(E(K), \oplus)$ into an abelian group.*

# The Mordell-Weil Group

**Theorem (L.J.Mordell, 1922)**

*Let $E$ be an elliptic curve defined over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a finitely generated abelian group. In particular,*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

*for some nonnegative integer $r$.*

# Squares in Arithmetic Progressions

**Theorem**

*Denote*

$$X_0(24) : y^2 = x^3 + 5x^2 + 4x$$

$$X_0^{(D)}(24) : y^2 = x^3 + 5Dx^2 + 4D^2x$$

*Then there exists a nonconstant / nontrivial progression of four squares over* $\mathbb{Q}(\sqrt{D})$*, if and only if rank* $X_0^{(D)}(24)(\mathbb{Q}) > 0$.

# An Arithmetic Progression to a Point

Given a 4-term arithmetic progression of four squares $(n_1, n_2, n_3, n_4)$, let a rational point $(x : y : z)$ satisfy the following:

$$x = 2(\sqrt{n_1} - 3\sqrt{n_2} - 3\sqrt{n_3} + \sqrt{n_4})$$
$$y = 6(\sqrt{n_1} - \sqrt{n_2} + \sqrt{n_3} - \sqrt{n_4})$$
$$z = \sqrt{n_1} + 3\sqrt{n_2} + 3\sqrt{n_3} + \sqrt{n_4}$$

This constitutes a point on the curve $y^2z = x^3 + 5x^2z + 4xz^2$

Rational Points on $y^2z = x^3 + 5x^2z + 4xz^2$

| $(\sqrt{n_1} : \sqrt{n_2} : \sqrt{n_3} : \sqrt{n_4})$ | $(x : y : z)$ |
|---|---|
| (-1:-1:+1:+1) | (0:1:0) |
| (-1:+1:-1:+1) | (0:0:1) |
| (-1:-1:-1:+1) | (-2:+2:1) |
| (-1:+1:+1:+1) | (-2:-2:1) |
| (+1:+1:+1:+1) | (-1:0:1) |
| (+1:-1:-1:+1) | (-4:0:1) |
| (+1:+1:-1:+1) | (2:+6:1) |
| (+1:-1:+1:+1) | (2:-6:1) |

From this we can conclude that there are no nontrivial arithmetic progressions of four rational squares over $\mathbb{Q}$. Additionally we observe that $X_0(24) \cong Z_2 \times Z_4$ as an abelian group.

# A Point to an Arithmetic Progression

Given a nonzero rational number $D$, we say that $X_0^{(D)}(24) : y^2z = x^3 + 5Dx^2z + 4D^2xz^2$ has a nontrivial rational point $(x : y : z)$. We then have an arithmetic progression of four-squares $(n_1, n_2, n_3, n_4)$ over $\mathbb{Q}(\sqrt{D})$ given by the following:

$$\begin{aligned} n_1 &= (3Dx(x+2Dz) + \sqrt{D}y(x-2Dz))^2 \\ n_2 &= (Dx(x-2Dz) + \sqrt{D}y(x+2Dz))^2 \\ n_3 &= (Dx(x-2Dz) - \sqrt{D}y(x+2Dz))^2 \\ n_4 &= (3Dx(x+2Dz) - \sqrt{D}y(x-2Dz))^2 \end{aligned}$$

# Example

Consider the case when $D = 6$, then the rational point $(x : y : z) = (-8 : -16 : 1)$ is on the curve $X_0^{(D)}(24)$. Using this case, we get the following progression

$$(n_1, n_2, n_3, n_4) = ((9 - 5\sqrt{6})^2, (15 - \sqrt{6})^2, (15 + \sqrt{6})^2, (9 + 5\sqrt{6})^2)$$

.

# Lemma for Ranks

We have found that the 2-torsion subgroup of $X_0(24)$ is defined over $\mathbb{Q}$. From Kwon's (as cited by Gonzalez-Jimenez, Steuding) results we conclude that $X_0(24)(\mathbb{Q}(\sqrt{D}))_{tors}$ and $X_0(24)(\mathbb{Q})_{tors}$ are equal.

# Summary

We can conclude that if there exists a non-constant / nontrivial progression of four-squares over $\mathbb{Q}(\sqrt{D})$, then there are infinitely many arithmetic progressions of four-squares.
An equivalent statement would be: if there exists a non-constant / nontrivial progression of four-squares over $\mathbb{Q}(\sqrt{D})$, then rank $X_0(24)(\mathbb{Q}(\sqrt{D})) > 0$.

# Mordell-Weil Theorem

**Theorem**

*(L. J. Mordell, 1922). Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated Abelian group. In particular,*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times (\mathbb{Z})^r$$

*for some nonnegative integer $r$.*

# Mazur's theorem

**Theorem**

*(B. Mazur, 1978). Let $E$ be a rational elliptic curve, and let $E(\mathbb{Q})_{tors}$ denote its torsion subgroup. This finite group can only be one of fifteen types:*

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} Z_N, & \text{for } N = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12; \\ Z_2 \times Z_{2N} & \text{for } N = 1,\ 2,\ 3,\ 4. \end{cases}$$

In the case of arithmetic progressions of four squares, the torsion subgroup of the related elliptic curve $X_0^D(24)$ is always $Z_2 \times Z_4$.

# The Tate Pairing

Let E be an elliptic curve over K, with all four points of order 2 being K-rational i.e.,

$$E : Y^2 = (X - e_1)(X - e_2)(X - e_3)$$

where $e_i \in K$.
We define the map

$$e_2 : \frac{E(K)}{2E(K)} \times E[2] \to \frac{K^\times}{(K^\times)^2}, (P, T) \mapsto \begin{cases} 1 & \text{if } T = \mathcal{O} \\ X - e & otherwise; \end{cases}$$

where $P = (X : Y : 1)$ and $T = (e : 0 : 1)$. This map is sometimes called the Tate pairing.

# The Tate Pairing

**Theorem**

*(The Tate Pairing). Tate pairing is a perfect pairing, as it is*
*(1) Non-degenerate: If* $e_2(P, T) = 1$ *for all* $T \in E[2]$ *then* $P \in 2E(K)$.
*(2) Bilinear: for all* $P, Q \in E(K)$ *and* $T \in E[2]$ *we have*

$$e_2(P \oplus Q, T) = e_2(P, T) \times e_2(Q, T),$$

$$e_2(P, T_1 \oplus T_2) = e_2(P, T_1) \times e_2(P, T_2).$$

## Theorem

*(Complete 2-Descent). Let $E$ be an elliptic curve over $K$ with $E[2] \subseteq E(K)$ i.e.,*

$$E : Y^2 = (X - e_1)(X - e_2)(X - e_3)$$

*where $e_i \in K$.*
*1. Let $\delta_E : \frac{E(K)}{2E(K)} \to \frac{(K^*)}{(K^*)^2} \times \frac{(K^\times)}{(K^\times)^2}$, $P \mapsto (e_2(P, T_1), e_2(P, T_2))$; where $e_2$ is the Tate pairing and $T_i = (e_i : 0 : 1) \in E[2]$. This is an injective group homomorphism.*
*Furthermore the image of $\delta_i$ lies in the finitely generated Abelian group generated by the set $\mathbb{Q}(S_i, 2)$, which is the collection of all square-free divisors of $S_i$.*

# Complete 2-Descent

**Theorem**

*2. For each $d = (d_1, d_2) \in K^\times \times K^\times$, consider the projective curve*

$$\mathcal{C}_d : d_1 u^2 - d_2 v^2 = (e_2 - e_1),\ d_1 u^2 - d_z d_2 w^2 = (e_3 - e_1)$$

*If $d \equiv \delta_E(P)$ for some $P \in E(K)$ then there is an $K$-rational point $(u, v, w)$ on $\mathcal{C}_d$. Conversely, the map $\psi : \mathcal{C}_d \to E$ defined by*

$$(z_1 : z_2 : z_3 : z_4) \mapsto (d_1 z_1^2 z_0 + e_1 z_0^3 : d_1 d_2 z_1 z_2 z_3 : z_0^3)$$

*sends a point $Z \in \mathcal{C}_d(K)$ to a point $\psi(Z) \in E(K)$, and*

$$\delta_E(\psi(Z)) = (d_1( \mod (K^\times)^2), d_2( \mod (K^\times)^2)).$$

# Computing The Rank

As $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times Z^r \cong Z_2 \times Z_{2N} \times Z^r$, we have $2E(\mathbb{Q}) \cong Z_N \times (Z_2)^r$, thus $\frac{E(\mathbb{Z})}{2E(\mathbb{Z}} \cong (Z_2)^{r+2}$. We compute the image of the connecting homomorphism $\delta_E$; there will be $2^{r+2}$ elements, where $r$ is the rank of $E$.

# Motivation for Proving No Solutions

There is a motivation for eliminating points $(d_1, d_2)$ from the image of $\delta_E$ for a given $D = mp$. We will eliminate points by showing that the equations:

$$d_1 u'^2 - d_2 v'^2 = -D$$
$$d_2 v'^2 - d_1 d_2 w'^2 = -3D$$

do not have a rational solution $(u', v', w')$

# Key Equations

We can write $u' = \dfrac{u}{z}$, $v' = \dfrac{v}{z}$, and $w' = \dfrac{w}{z}$ such that $gcd(u, v, w, z) = 1$ and $z \neq 0$. Using these substitutions and multiplying through by $z^2$ we get:

$$d_1 u^2 - d_2 v^2 = -Dz^2$$
$$d_2 v^2 - d_1 d_2 w^2 = -3Dz^2$$

So if these equations don't have an integer solution $(u, v, w, z)$, we can eliminate $(d_1, d_2)$ from the image.

# The Structure of $Im(\delta_E)$

- We know that the image of $\delta_E$ is a multiplicative group.
- We know that the points $(1, 1)$, $(1, D)$, $(-D, -3)$, and $(-D, -3D)$ are in the image of $\delta_E$.
- Thus, if we know a point $x$ is not in the image of $\delta_E$, we can conclude that the product of $x$ and any point in the image of $\delta_E$ is not in the image of $\delta_E$.

# The Form of the Equations

- Notice equation 1 and equation 2 can easily be rearranged to the form:

$$ax^2 + by^2 + cz^2 = 0$$

  Where $x$, $y$, and $z$ are integers such that $gcd(x, y, z) = 1$.
- Also notice that $a$, $b$, and $c$ are symmetric in this equation.
- Theorems have been formulated for conditions on $a$, $b$, and $c$ that yield no integer solutions to the equation.

## Solutions Modulo 9

**Theorem**

*If a, b, and c have the same sign and are all non-zero, there are no solutions to* $ax^2 + by^2 + cz^2 = 0$.

**Theorem**

*If* $a \not\equiv 0(mod 3)$, $a \equiv b(mod 3)$, *and* $c \equiv 3, 6(mod 9)$, *then* $ax^2 + by^2 + cz^2 = 0$ *has no integer solution.*

# Solutions Modulo 8

**Theorem**

*If* $a \equiv 3, 6(mod9)$, $a \equiv b(mod9)$, *and* $c \not\equiv 0(mod3)$, *then* $ax^2 + by^2 + cz^2 = 0$ *has no integer solution.*

**Theorem**

*If* $a \equiv \pm 1(mod4)$ *and* $a \equiv b \equiv c(mod4)$, *then* $ax^2 + by^2 + cz^2 = 0$ *has no integer solutions.*

**Theorem**

*If* $a \equiv 2, 6(mod8)$, $b + c \not\equiv 0(mod8)$, $a + b + c \not\equiv 0(mod8)$, *and* $a$ *and* $b$ *are odd, then* $ax^2 + by^2 + cz^2 = 0$ *has no integer solutions.*

**Theorem**

*Suppose $D \equiv 2, 6 (mod 8)$ and $d_1, d_2 \not\equiv 0, 4 (mod 8)$ and there is a solution to the homogeneous space, then one of the following holds.*

$$d_1 \equiv d_2 \equiv 1 (mod 8)$$

$$d_1 \equiv 3D (mod 4) \text{ and } d_2 \equiv 1 (mod 4)$$

$$d_2 \equiv D (mod 8)$$

$$d_1 \equiv 3D + 1 \text{ and } d_2 \equiv 1 (mod 8)$$

# The Simultaneous Equations Modulo 16

## Theorem

*Suppose $d_1$ and $d_2$ are odd, $D \equiv 1 (mod 8)$, and the equations have a solution, then $(d_1, d_2)$ is one of the following mod 8:*

$$(1, 1)$$

$$(5, 1)$$

$$(3, 5)$$

$$(7, 5)$$

- A computer program was written in python that uses the elimination theorems to eliminate points from the image of $\delta_E$ to gain an upper bound on the size.
- We can use these upper bounds on the size of the image to form an upper bound on the rank of $X_0^{(D)}(24)$ for $D = mp$

# Results

The columns correspond to $m$ while the rows correspond to $p(mod 24)$.

| | 1 | 2 | 3 | 6 | -1 | -2 | -3 | -6 |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 |
| 5 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 7 | 0 | 0 | 1 | 1 | 0 | 2 | 1 | 0 |
| 11 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 2 |
| 13 | 1 | 0 | 2 | 1 | 2* | 0 | 1 | 0 |
| 17 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 19 | 0 | 2 | 0 | 1 | 1 | 0 | 1 | 2 |
| 23 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 |

# Examples of Arithmetic Progressions of Squares

For $D = 11$, the rank is 1 so we can find a non-torsion point $(64, 720)$ on the elliptic curve which yields the arithmetic progression:

$$n_1 = (181632 - 30240\sqrt{11})^2$$

$$n_2 = (29568 - 61920\sqrt{11})^2$$

$$n_3 = (29568 + 61920\sqrt{11})^2$$

$$n_4 = (181632 + 30240\sqrt{11})^2$$

For $D = 13$, the rank is 1 so we can find a non-torsion point $(-25, 90)$ on the elliptic curve which yields the arithmetic progression:

$$n_1 = (-975 - 4590\sqrt{13})^2$$

$$n_2 = (16575 + 90\sqrt{13})^2$$

$$n_3 = (16575 - 90\sqrt{13})^2$$

$$n_4 = (-975 + 4590\sqrt{13})^2$$

**Theorem**

*Denote*

$$X_0(36) : y^2 = x^3 - 27$$

$$X_0^{(D)}(36) : y^2 = x^3 - 27D^3$$

*Then there exists a nonconstant / nontrivial progression of three cubes over* $\mathbb{Q}(\sqrt{D})$*, if and only if rank* $X_0^{(D)}(36)(\mathbb{Q}) > 0$.

# An Arithmetic Progression to a Point on $X_0(36)$

Given a 3-term arithmetic progression of three cubes $(n_1, n_2, n_3)$, define a rational point $(x : y : z)$:

$$x = -6(\sqrt[3]{n_1} + \sqrt[3]{n_2} + \sqrt[3]{n_3})(\sqrt[3]{n_1} - 2\sqrt[3]{n_2} + \sqrt[3]{n_3})$$
$$y = -27(\sqrt[3]{n_1}^2 - \sqrt[3]{n_3})^2)$$
$$z = (\sqrt[3]{n_1} - 2\sqrt[3]{n_2} + \sqrt[3]{n_3})^2$$

This point lies on the curve $y^2 z = x^3 - 27z^3$.

Rational Points on $y^2 z = x^3 - 27z^3$

| $(\sqrt[3]{n_1} : \sqrt[3]{n_2} : \sqrt[3]{n_3})$ | $(x : y : z)$ |
|---|---|
| (+1:+1:+1) | (0:1:0) |
| (-1:0:+1) | (3:0:1) |

From this we can conclude that there are no nontrivial arithmetic progressions of three rational cubes over $\mathbb{Q}$. Additionally we observe that $X_0(36) \cong Z_2$ as an abelian group.

# A Point to an Arithmetic Progression

Given a nonzero rational number $D$, we say that $X_0^{(D)}(36) : y^2 z = x^3 - 27D^3 z^3$ has a nontrivial rational point $(x : y : z)$. We then have an arithmetic progression of three cubes $(n_1, n_2, n_3)$ over $\mathbb{Q}(\sqrt{D})$ defined by the following:

$$
\begin{aligned}
n_1 &= ((x - 3Dz)^2 - \sqrt{D}yz)^3 \\
n_2 &= ((x - 3Dz)(x + 6Dz))^3 \\
n_3 &= ((x - 3Dz)^2 + \sqrt{D}yz)^3
\end{aligned}
$$

# Example

Consider the case when $D = 2$, then the rational point $(x : y : z) = (10 : 28 : 1)$ is on the curve $X_0^{(D)}(36)$. In this case, we get the following progression:

$$(n_1, n_2, n_3) = ((4 - 21\sqrt{2})^3, 22^3, (4 + 21\sqrt{2})^3)$$

.

# Lemma for Ranks

From Gonzalez-Jimenez's paper we conclude that $X_0(36)(\mathbb{Q}(\sqrt{D}))_{tors}$ and $X_0(36)(\mathbb{Q})_{tors}$ are equal, when $D \neq 3$.

# Summary

We conclude that points that we find for progressions of three cubes are not torsion points, and thus $\operatorname{rank} X_0(36)(\mathbb{Q}(\sqrt{D})) > 0$.

# Descent via Two Isogenies

Let $E$ denote an elliptic curve over $\mathbb{Q}$.
1) $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$
2) $E^{(D)}(\mathbb{Q}) \simeq E^{(D)}(\mathbb{Q})_{tors} \times \mathbb{Z}^{r(D)}$
3) $E(\mathbb{Q}(\sqrt{D})) \simeq E(\mathbb{Q}(\sqrt{D})_{tors} \times \mathbb{Z}^R, R = r + r(D)$
$X_0(36)(\mathbb{Q}) \simeq Z_2 \Rightarrow r = 0$. Thus, rank$(X_0(36)(\mathbb{Q}(\sqrt{D})) > 0$ if and only if rank $(X_0(36)^{(D)}(\mathbb{Q})) > 0$. Yet, $X_0(36)^{(D)}(\mathbb{Q}) : y^2 = x^3 - 27D^3 = (x - 3D)(x^2 + Dx + 9D^2)$, the set of the 2-torsion points of $X_0(36)^{(D)}$ is not a subset of $\mathbb{Q}$. Thus complete 2-descent is not useful in this case; we have to use descent via two isogenies instead.

# Isogenies

However, for any quadratic twist $X_0^{(D)}(36)(\mathbb{Q})$, there is a rational point $(x : y : z) = (-3D : 0 : 1)$ in $X_0(36)[2]$. Thus, we have the 2-isogeny
$\phi : X_0(36)^{(D)} \to E^{(D)}$

$$(x : y : z) \mapsto \left(\frac{x^2 - 3Dxz + 27D^2z^2}{x - 3Dz} : \frac{x^2 - 6Dxz - 18D^2z^2}{(x - 3Dz)^2}y : z\right)$$

where $E^{(D)} : y^2z = x^3 - 135D^2xz^2 - 594D^3z^3$. We have that
$\ker(\phi) = X_0^{(D)}(\mathbb{Q})_{tors}$.

# Isogenies

We may construct
$\phi' : E^{(D)} \to X_0(36)^{(D)}$
$(x : y : z) \mapsto (\frac{1}{4}[\frac{x^2 + 6Dxz - 27D^2z^2}{x + 6Dz}] : \frac{1}{8}[\frac{x^2 + 12Dxz + 63D^2z^2}{(x + 6Dz)^2}y] : z)$
We have that $\ker(\phi') = \{P = (-6D : 0 : 1), \mathcal{O}\}$. By the property noted earlier, we have that $\phi \circ \phi' = 2X_0^{(D)}(36)(\mathbb{Q})$. Note that $P = (-6D : 0 : 1)$ has order two, so we see that $\ker(\phi) = X_0^{(D)}(\mathbb{Q})[2]$ and $ker(\phi') = E^{(D)}(\mathbb{Q})[2]$.

# Computing The Rank

$$X_0^{(D)}(36)(\mathbb{Q}) \simeq Z_2 \times \mathbb{Z}^{r(D)} \Rightarrow \frac{X_0^{(D)}(36)(\mathbb{Q})}{2X_0^{(D)}(36)(\mathbb{Q})} \simeq Z_2 + \mathbb{Z}^{r(D)+1}$$, where

$r(D)$ is the rank of $X_0(36)^{(D)}(\mathbb{Q})$.

So, in order to compute $r(D)$, we need to count the cosets in $\dfrac{X_0^{(D)}(36)(\mathbb{Q})}{2X_0^{(D)}(36)(\mathbb{Q})}$.

# Counting Cosets in $\frac{X_0^{(D)}(36)(\mathbb{Q})}{2X_0^{(D)}(36)(\mathbb{Q})}$

We have $|\frac{E^{(D)}(\mathbb{Q})[\phi]}{\phi(X_0(36)^{(D)}(\mathbb{Q})[2]}||\frac{X_0(36)^{(D)}(\mathbb{Q})}{2X_0(36)^{(D)}(\mathbb{Q})}| =$
$|\frac{E^{(D)}(\mathbb{Q})}{\phi(X_0(36)^{(D)}(\mathbb{Q}))}||\frac{X_0(36)^{(D)}(\mathbb{Q})}{\phi(E^{(D)}(\mathbb{Q}))}| = |\mathrm{coker}(\phi)||\mathrm{coker}(\phi')|$.

# Counting Cosets in $\frac{X_0^{(D)}(36)(\mathbb{Q})}{2X_0^{(D)}(36)(\mathbb{Q})}$

Note that $|\frac{E^{(D)}(\mathbb{Q})[\phi]}{\phi(X_0(36)^{(D)}(\mathbb{Q})[2]}| = 2$, since $|E^{(D)}(\mathbb{Q})[\phi]| = 2$ and $\phi(X_0(36)^{(D)}(\mathbb{Q})[2])$ consists only of the point at infinity, so $|\frac{E^{(D)}(\mathbb{Q})[\phi]}{\phi(X_0(36)^{(D)}(\mathbb{Q})[2]}| = \frac{2}{1} = 2$. Thus,

$$|\frac{E^{(D)}(\mathbb{Q})[\phi]}{\phi(X_0(36)^{(D)}(\mathbb{Q})[2]}||\frac{X_0(36)^{(D)}(\mathbb{Q})}{2X_0(36)^{(D)}(\mathbb{Q})}| = |\frac{E^{(D)}(\mathbb{Q})}{\phi(X_0(36)^{(D)}(\mathbb{Q}))}||\frac{X_0(36)^{(D)}(\mathbb{Q})}{\phi(E^{(D)}(\mathbb{Q}))}| \Rightarrow$$

$$2|\frac{X_0(36)^{(D)}(\mathbb{Q})}{2X_0(36)^{(D)}(\mathbb{Q})}| = |\frac{E^{(D)}(\mathbb{Q})}{\phi(X_0(36)^{(D)}(\mathbb{Q}))}||\frac{X_0(36)^{(D)}(\mathbb{Q})}{\phi(E^{(D)}(\mathbb{Q}))}| \Rightarrow$$

$$|\frac{X_0(36)^{(D)}(\mathbb{Q})}{2X_0(36)^{(D)}(\mathbb{Q})}| = \frac{1}{2}|\frac{E^{(D)}(Q)}{\phi(X_0(36)^{(D)}(\mathbb{Q}))}||\frac{X_0(36)^{(D)}(\mathbb{Q})}{\phi(E^{(D)}(\mathbb{Q}))}| \Rightarrow$$

$$|\frac{X_0(36)^{(D)}(\mathbb{Q})}{2X_0(36)^{(D)}(\mathbb{Q})}| = \frac{|\text{coker}(\phi)||\text{coker}(\phi')|}{2}.$$

# Computing Cokernels

To avoid working directly with coker($\phi$) and coker($\phi$'), whose structure may be difficult to work with, we define the group homomorphism

$$\delta : \frac{E^{(D)}(\mathbb{Q})}{\phi(X_0(36)^{(D)}(\mathbb{Q}))} \to \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$$

$(x, y) \mapsto x + 6D \bmod (\mathbb{Q}^\times)^2$, if $x + 6D \neq 0$

$\mathcal{O} \mapsto 1 \bmod (\mathbb{Q}^\times)^2$, if $x + 6D = 0$

($\delta$ maps the elements of $\dfrac{E^{(D)}(\mathbb{Q})}{\phi(X_0(36)^{(D)}(\mathbb{Q}))}$ to their square-free parts)

and we define the group homomorphism

$$\delta' : \frac{X_0(36)^{(D)}(\mathbb{Q})}{\phi'(E^{(D)}(\mathbb{Q}))} \to \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$$

$(x, y) \mapsto x - 3D \bmod (\mathbb{Q}^\times)^2$

($\delta$' maps the elements of $\dfrac{X_0(36)^{(D)}(\mathbb{Q})}{\phi'(E^{(D)}(\mathbb{Q}))}$ to their square-free parts.)

# Computing Cokernels

Both $\delta : \text{coker}(\phi) \to \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$ and

$\delta' : \text{coker}(\phi') \to \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$ are injective group homomorphisms

$2^{(r+1)} = \frac{|\text{Im}(\delta)||\text{Im}(\delta')|}{2}$.

Let $S = \{\text{k}|\ \text{k prime, k}|27D^2\}$. Notice that $\text{Im}(\delta)$ is a subset of $\mathbb{Q}(S,2)$. Hence, $|\text{Im}(\delta)| \leq |\mathbb{Q}(S,2)|$ Likewise, $\text{Im}(\delta')$ is a subset of $\mathbb{Q}(S,2)$. Hence, $|\text{Im}(\delta')| \leq |\mathbb{Q}(S,2)|$.

# Homogeneous Space

To compute $|\text{Im}(\delta)|$, we may consider values of $d$ in $\frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$ such that the equation $D_d : v^2 = d - 18Du^2 - \frac{27D^2}{d}u^4$ has a rational solution $(u, v)$.

To compute $|\text{Im}(\delta')|$, we may consider values of $d'$ in $\frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}$ such that the equation

$D_{d'} : w^2 = d' + 9Dz^2 + \frac{27D^2}{d'})z^4$

has a rational solution $(w, z)$.

# Motivation

- There is a motivation for eliminating points from the image of $\delta$ and $\delta'$ for a given $D = mp$.
- If we can eliminate points from the image, we can find an upper bound on the size of the image, and thus an upper bound on the rank.

# Eliminating Points from $Im(\delta)$

In order to show a point $d$ is not in the image $\delta$, it will suffice to show that there are no rational solutions to:

$$v'^2 = d - 18Du'^2 - \frac{27D^2}{d}u'^4$$

If we let $v' = \frac{v}{z}$ and $u' = \frac{u}{z}$ such that $gcd(u, v, z) = 1$, and multiply through by $z^4$, we get:

$$v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$$

It will suffice to show there are no integer solutions to this equation to eliminate a point from the image.

In order to show a point $d$ is not in the image of $\delta'$, it will suffice to show that there are no rational solutions to:

$$v^2 = d + 9Du^2 + \frac{27D^2}{d}u^4$$

Let $v' = \frac{v}{z}$ and $u' = \frac{u}{z}$ such that $gcd(u, v, z) = 1$, and multiply through by $z^4$.

$$v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$$

It will suffice to show there are no integer solutions to this equation to eliminate a point from the image.

# Structures of the Images

- We know that 1 and -3 are in the image of $\delta$ and that 1 and 3 are in the image of $\delta'$
- Since the images are multiplicative groups, if we know a point $x$ is not in the image, the product of $x$ and a point from the image is not in the image.

# Checking for Real Solutions

If there are no real solutions to the equations. Then there will be no rational solutions.

**Theorem**

*If $d < 0$ then there is no rational solution to* $v^2 = d + 9Du^2 + \frac{27D^2}{d}u^4$

# The Legendre Symbol

- Let us denote the Legendre symbol as $(\frac{a}{b})$
- Let $(\frac{a}{b}) = 1$ if there exists an integer $x$ such that $x^2 \equiv a(modb)$
- Otherwise, let $(\frac{a}{b}) = -1$

# Checking for solutions Modulo $p$

**Theorem**

*Let $D = mp$ and suppose $p \mid d$. If $(frac3p) = -1$ then there are no solutions to* $v^2z^2 = dz^4 - 18Du^2z^2 - \dfrac{27D^2}{d}u^4$

**Theorem**

*Let $D = mp$ and suppose $p \mid d$. If $(\frac{-3}{p}) = -1$ then there are no solutions to* $v^2z^2 = dz^4 + 9Du^2z^2 + \dfrac{27D^2}{d}u^4$

**Theorem**

*Let $D = mp$ and suppose $p \nmid d$. If $(\frac{d}{p}) = -1$ and $(\frac{-3d}{p}) = -1$ then there are no solutions to* $v^2z^2 = dz^4 - 18Du^2z^2 - \dfrac{27D^2}{d}u^4$

# Checking for Solutions Modulo $p$

**Theorem**

*Suppose $3 \nmid d$ and $3 \mid D$. If $d \equiv -1 \pmod 3$ then there is no integer solution to either $v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$ or $v^2z^2 = dz^4 + 9Du^2z^2 + \frac{27D^2}{d}u^4$.*

**Theorem**

*Suppose* $3 \nmid d$ *and* $3 \nmid D$. *If* $d \equiv -1 \pmod 3$ *then there is no integer solution to either* $v^2z^2 = dz^4 - 18Du^2z^2 - \dfrac{27D^2}{d}u^4$ *or* $v^2z^2 = dz^4 + 9Du^2z^2 + \dfrac{27D^2}{d}u^4$.

# Checking for solutions Modulo 8

**Theorem**

*Suppose* $2 \mid d$ *which implies* $2 \mid D$. *Let* $d = 2\bar{d}$ *and* $D = 2\bar{D}$. *Then* $v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$ *has a solution only if* $\bar{d}z^4 - 18\bar{D} - \frac{27\bar{D}^2}{\bar{d}} \equiv 0$ *or* $2 \pmod 8$.

**Theorem**

*Suppose* $2 \mid d$ *which implies* $2 \mid D$. *Let* $d = 2\bar{d}$ *and* $D = 2\bar{D}$. *Then* $v^2z^2 = dz^4 + 9Du^2z^2 + \frac{27D^2}{d}u^4$ *has a solution only if* $\bar{d}z^4 + 9\bar{D} + \frac{27\bar{D}^2}{\bar{d}} \equiv 0$ *or* $2 \pmod 8$.

# Checking for solutions Modulo 8

## Theorem

*Suppose* $2 \nmid d$ *but* $2 \mid D$. *Let* $D = 2\bar{D}$. *Then* $v^2z^2 = dz^4 + 9Du^2z^2 + \frac{27D^2}{d}u^4$ *has a solution only if one of the following holds.*

$$d + 2 * 9\bar{D} + 4 * \frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8)$$

$$d \equiv 1 \ (mod\ 8)$$

$$4 * d + 2 * 9\bar{D} + \frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8)$$

$$\frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8)$$

# Computer Program

- A computer program was written in python that uses the elimination theorems to eliminate points from the image of $\delta$ and $\delta'$ to gain an upper bound on the size.
- We can use these upper bounds on the size of the images to form an upper bound on the rank of $X_0^{(D)}(36)$ for $D = mp$

# Results

The columns correspond to $m$ while the rows correspond to $p(mod 24)$.

| | 1 | 2 | 3 | 6 | -1 | -2 | -3 | -6 |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 |
| 5 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 7 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 11 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 |
| 13 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 1 |
| 17 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 19 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 |
| 23 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 |

For $D = 7$ and $D = 11$, the rank is 1 and thus we can find a points on the elliptic curves.
For $D = 7$, we can find the non-torsion point $(\frac{1785}{4}, \frac{75411}{8})$ on the elliptic curve which yields the arithmetic progression:

$$n_1 = (11573604 - 1809864\sqrt{7})^3$$

$$n_2 = (13288212)^3$$

$$n_3 = (11573604 + 1809864\sqrt{7})^3$$

For $D = 11$, we can find the non-torsion point $(\frac{55977}{1369}, \frac{9121140}{50653})$ on the elliptic curve which yields the arithmetic progression:

$$n_1 = (159680160000 - 1386039313260\sqrt{11})^3$$

$$n_2 = (2163533101200)^3$$

$$n_3 = (159680160000 + 1386039313260\sqrt{11})$$

# Acknowledgements

Dr. Edray Goins

James Weigant
National Science Foundation

Thank You for Your Attention

Questions?