SQUARES AND CUBES IN ARITHMETIC PROGRESSIONS

RONALD ARCHER, EDRAY HERBER GOINS, HAN LIU, BENITO MARTINEZ, STEPHEN MUSSMANN, JAMIE WEIGANDT, AND LIRONG YUAN

Abstract. In 1640, Pierre de Fermat sent a letter to Bernard Frénicle de Bessy claiming that that there are no four or more rational squares in a nontrivial arithmetic progression; this statement was shown in a posthumous work by Leonhard Euler in 1780. In 1823, Adrien-Marie Legendre showed that there are no three or more rational cubes in a nontrivial arithmetic progression. A modern proof of either claim reduces to showing that certain elliptic curves have no rational points other than torsion.

A 2009 paper by Enrique González-Jiménez and Jörn Steuding [4], extended by a 2010 paper by Alexander Diaz, Zachary Flores, and Markus Vasquez [1], discussed a generalization by looking at four squares in an arithmetic progression over quadratic extensions of the rational numbers. Similarly, a 2010 paper by Enrique González-Jiménez [3] discussed a generalization by looking at three cubes in an arithmetic progression over quadratic extensions of the rational numbers. In this project, we give explicit examples of four squares and three cubes in arithmetic progressions, and recast many ideas by performing a complete 2-descent of quadratic twists of certain elliptic curves.

1. Introduction

An *m-term arithmetic progression* is a collection of rational numbers $\{n_1, n_2, \dots, n_m\}$ 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. In fact, there 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. 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; this statement was shown in a posthumous work by Leonhard Euler in 1780. Indeed, each 4-term arithmetic progression of perfect squares corresponds to a rational point $(x : y : z)$ on the elliptical curve $E : y^2 = x^3 + 5\,x^2 + 4\,x$, and one shows that $E(\mathbb{Q}) \simeq Z_2 \times Z_4$ consists of finitely many rational points. A paper by Enrique González-Jiménez and Jörn Steuding [4] considered four squares in an arithmetic progression over quadratic extensions of the rational numbers. For example, one can use those results to construct the arithmetic progression

$$\big\{(9-5\sqrt{6})^2,\ (15-\sqrt{6})^2,\ (15+\sqrt{6})^2,\ (9+5\sqrt{6})^2\big\}. \tag{1}$$

Similar arithmetic progressions have also been studied. There are only finitely many 3-term arithmetic progressions whose terms are perfect cubes: $\{-1, 0, 1\}$ is one. In 1823, Adrien-Marie Legendre showed that there are no four or more rational cubes in a nontrivial

2000 *Mathematics Subject Classification.* 14H52, 11Axx, 05Bxx.

Key words and phrases. elliptic curve; arithmetic progressions.

arithmetic progression. Indeed, each 3-term arithmetic progressions of perfect cubes corresponds to a rational point $(x : y : z)$ on the elliptic curve $E : y^2 = x^3 - 27$, and one shows that $E(\mathbb{Q}) \simeq Z_2$ consist of finitely many rational points. A 2010 paper by Enrique González-Jiménez [3] considered three cubes in an arithmetic progression over the same quadratic extensions. One can use those results to construct the arithmetic progression.

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

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 extends a 2010 paper Alexander Diaz, Zachary Flores, and Markus Vasquez [1].

2. Elliptic Curves

We begin with a result in order to motivate a definition.

Proposition 1. *Consider the curve* $E : y^2 + a_1\, x\, y + a_3\, y = x^3 + a_2\, x^2 + a_4\, x + a_6$. *Using a substitution,*

$$\begin{aligned} X &= x + \frac{a_1^2 + 4\, a_2}{12} & & & x &= X - \frac{a_1^2 + 4\, a_2}{12} \\ Y &= y + \frac{a_1}{2}\, x + \frac{a_3}{2} & &\iff & y &= Y - \frac{a_1}{2}\, X + \frac{a_1^3 + 4 a_1\, a_2 - 12\, a_3}{24} \end{aligned} \tag{3}$$

we find a curve in the form $Y^2 = X^3 + A\, X + B$, *where*

$$\begin{aligned} A &= \frac{24\,(a_1\, a_3 + 2\, a_4) - (a_1^2 + 4\, a_2)^2}{48} \\ B &= \frac{216\,(a_3^2 + 4\, a_6) - 36\,(a_1^2 + 4\, a_2)\,(a_1\, a_3 + 2\, a_4) + (a_1^2 + 4\, a_2)}{864} \end{aligned} \tag{4}$$

This is a nonsingular curve, i.e., there is a well-defined tangent lined at every point on the curve, if and only if $4\, A^3 + 27\, B^2 \neq 0$.

A nonsingular curve as in the proposition above is called an *elliptic curve*. It can be defined over any field K, such as $K = \mathbb{Q}$, the rational numbers, or $K = \mathbb{Q}(\sqrt{D})$, a quadratic extension thereof. We say that the K-rational points are those projective points $(x : y : z)$ on the curve whose coordinates x, y, and z belong to K. To this end, we denote the set

$$E(K) = \left\{ (x : y : z) \in \mathbb{P}^2(K) \,\middle|\, y^2\, z + a_1\, x\, y\, z + a_3\, y\, z^2 = x^3 + a_2\, x^2\, z + a_4\, x\, z^2 + a_6\, z^3 \right\}. \tag{5}$$

The idea behind considering nonsingular 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 $P * Q$. If the line is parallel to the y-axis, we define the third point as the point "at infinity" which we denote by $\mathcal{O} = (0 : 1 : 0)$. This process is known as the *chord-tangent method*.

Theorem 2. *Denote $K \subseteq \mathbb{C}$ denote a field. Consider the elliptic curve*

$$E : y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6, \tag{6}$$

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 $P \oplus Q = (P * Q) * \mathcal{O}$. This turns $\bigl(E(K), \oplus\bigr)$ into an abelian group where the identity is $\mathcal{O} = (0 : 1 : 0)$ and the inverse of $P = (x : y : z)$ is $[-1]P = P * \mathcal{O} = (x : -y - a_1\,x - a_3\,z : z)$.

We will be interested in those elliptic curves defined over the field of rational numbers, that is, nonsingular curves in the form $E : y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$, where $a_i \in \mathbb{Q}$. Much is known about the abelian group $E(\mathbb{Q})$.

Theorem 3 (Louis J. Mordell, [7])**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group, that is, there exists a finite set $\{P_1,\, P_2,\, \dots,\, P_t\} \subseteq E(\mathbb{Q})$ such that each $P \in E(\mathbb{Q})$ can be expressed as the linear combination*

$$P = [m_1]P_1 \oplus [m_2]P_2 \oplus \cdots \oplus [m_t]P_t \tag{7}$$

for some integers $m_i \in \mathbb{Z}$. (Here, $[m]P = P \oplus P \oplus \cdots \oplus P$ is P added to itself m times.) In particular,

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r \tag{8}$$

for some finite group $E(\mathbb{Q})_{tors}$ and for some nonnegative integer r.

We call $E(\mathbb{Q})_{\text{tors}}$ the *torsion subgroup* of $E(\mathbb{Q})$. It consists of those elements $P \in E(\mathbb{Q})$ such that $[m]P = \mathcal{O}$ for some positive integer m. The nonnegative integer r is called the *rank* of the elliptic curve E. We will often denote $r = \operatorname{rank} E(\mathbb{Q})$. Observe that $r > 0$ if and only if there exists a rational point $(x : y : z) \notin E(\mathbb{Q})_{\text{tors}}$.

Theorem 4 (Barry Mazur, [6])**.** *Let E be a rational elliptic curve defined over $\mathbb{Q}$, and let $E(\mathbb{Q})_{tors}$ denote the torsion subgroup of $E(\mathbb{Q})$. This finite group can only be one of fifteen types:*

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

(Here Z_N denotes the cyclic group of order N.) Moreover, each of these possibilities does occur, that is, given one of these fifteen finite groups T, there exists an elliptic curve E defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{tors} \simeq T$.

As an example, the elliptic curve $E : y^2 = x^3 + 5\,x^2 + 4\,x$ has torsion subgroup

$$E(\mathbb{Q})_{\text{tors}} = \left\{ \begin{matrix} (0:1:0),\, (0:0:1),\, (-2:+2:1),\, (-2:-2:1), \\ (-1:0:1),\, (-4:0:1),\, (2:+6:1),\, (2:-6:1) \end{matrix} \right\} \simeq Z_2 \times Z_4; \tag{10}$$

whereas the elliptic curve $E : y^2 = x^3 - 27$ has torsion subgroup

$$E(\mathbb{Q})_{\text{tors}} = \bigl\{(0 : 1 : 0),\, (3 : 0 : 1)\bigr\} \simeq Z_2. \tag{11}$$

3. Squares in Arithmetic Progressions

An *arithmetic progression* over a field K is a collection of numbers $\{n_1, n_2, \dots, n_m\} \subseteq K$ such that there is a common difference $d = n_{i+1} - n_i$. There 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 x, $z \in K$. In 1640, Pierre de Fermat sent a letter to Bernard Frenicle de Bessy claiming that there are no four or more squares in a nontrivial arithmetic progression over $K = \mathbb{Q}$. We review a modern proof of this statement.

Theorem 5 (Enrique González-Jiménez and Jörn Steuding, [4])**.** *For each nonnegative integer D, denote the elliptic curves*

$$\begin{aligned} X_0(24):& \qquad y^2 = x^3 + 5\,x^2 + 4\,x \\ X_0^{(D)}(24):& \qquad y^2 = x^3 + 5\,D\,x^2 + 4\,D^2\,x \end{aligned} \tag{12}$$

There exists a nonconstant arithmetic progression $\{n_1, n_2, n_3, n_4\}$ of four squares over $\mathbb{Q}(\sqrt{D})$ if and only if rank $X_0^{(D)}(24)\big(\mathbb{Q}\big) > 0$. In this case, there are infinitely many arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{D})$.

Proof. This is the content of [4, Corollary 2], although we give a slightly expanded proof. First assume that we have a nonconstant 4-term arithmetic progression of squares $\{n_1, n_2, n_3, n_4\} \subseteq K$ for the quadratic field $K = \mathbb{Q}(\sqrt{D})$. We will show that $\operatorname{rank} X_0^{(D)}(24)\big(\mathbb{Q}\big) > 0$. Define the numbers

$$\begin{aligned} x &= 2\left(\sqrt{n_1} - 3\sqrt{n_2} - 3\sqrt{n_3} + \sqrt{n_4}\right) \\ y &= 6\big(\sqrt{n_1} - \sqrt{n_2} + \sqrt{n_3} - \sqrt{n_4}\big) \\ z &= \sqrt{n_1} + 3\sqrt{n_2} + 3\sqrt{n_3} + \sqrt{n_4} \end{aligned} \tag{13}$$

Using the equations $n_2 - n_1 = n_3 - n_2$, it is easy to verify that $y^2\,z = x^3 + 5\,x^2\,z + 4\,x\,z^2$. In other words, $(x : y : z) \in X_0(24)\big(K\big)$. One checks that this elliptic curve has at least eight torsion elements:

$$X_0(24)\big(K\big)_{\text{tors}} \supseteq X_0(24)\big(\mathbb{Q}\big)_{\text{tors}} = \left\{ \begin{matrix} (0:1:0),\ (0:0:1),\ (-2:\pm 2:1), \\ (-1:0:1),\ (-4:0:1),\ (2:\pm 6:1) \end{matrix} \right\} \simeq Z_2 \times Z_4. \tag{14}$$

Using Table 1, we see that these points correspond to the constant arithmetic progressions of squares $(n_1 : n_2 : n_3 : n_4) = (1 : 1 : 1 : 1)$. Note that $X_0(24) : y^2 = x\,(x + M)\,(x + N)$ where $M = 1^2$ and $N = 2^2$. Soonhak Kwon proved in [5, Theorem 1(iii)] that

$$X_0(24)\big(\mathbb{Q}(\sqrt{D})\big)_{\text{tors}} = X_0(24)\big(\mathbb{Q}\big)_{\text{tors}} \simeq Z_2 \times Z_4. \tag{15}$$

We conclude that if $(n_1 : n_2 : n_3 : n_4) \neq (1 : 1 : 1 : 1)$ is a nonconstant arithmetic progression of squares then $(x : y : z) \notin X_0(24)\big(\mathbb{Q}(\sqrt{D})\big)_{\text{tors}}$ is not a point of finite order. Hence $\operatorname{rank} X_0(24)\big(\mathbb{Q}(\sqrt{D})\big) > 0$. Following Joe Silverman's [8, Exercise 10.16], we have the result

$$\operatorname{rank} X_0(24)\big(\mathbb{Q}(\sqrt{D})\big) = \operatorname{rank} X_0(24)\big(\mathbb{Q}\big) + \operatorname{rank} X_0^{(D)}(24)\big(\mathbb{Q}\big). \tag{16}$$

We will see later that $\operatorname{rank} X_0(24)\big(\mathbb{Q}\big) = 0$, so we conclude that $\operatorname{rank} X_0^{(D)}(24)\big(\mathbb{Q}\big) > 0$.

Conversely, assume that $\operatorname{rank} X_0^{(D)}(24)\big(\mathbb{Q}\big) > 0$. We will show that there exists a nonconstant 4-term arithmetic progression of squares $\{n_1, n_2, n_3, n_4\} \subseteq K$ for the quadratic

Table 1. $\mathbb{Q}$-Rational Points on $X_0(24):\ y^2\,z = x^3 + 5\,x^2\,z + 4\,x\,z^2$

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

field $K = \mathbb{Q}(\sqrt{D})$. Choose a rational point $P = (x : y : z) \in X_0^{(D)}(24)\big(\mathbb{Q}\big)$ which is not in $X_0(24)\big(\mathbb{Q}\big)_{\text{tors}}$ or $X_0^{(D)}(24)\big(\mathbb{Q}\big)_{\text{tors}}$; such a point exists because $X_0^{(D)}(24)\big(\mathbb{Q}\big)$ contains infinitely many rational points. Define the numbers

$$\begin{aligned} n_1 &= \big(3\,D\,x\,(x + 2\,D\,z) + \sqrt{D}\,y\,(x - 2\,D\,z)\big)^2 \\ n_2 &= \big(D\,x\,(x - 2\,D\,z) + \sqrt{D}\,y\,(x + 2\,D\,z)\big)^2 \\ n_3 &= \big(D\,x\,(x - 2\,D\,z) - \sqrt{D}\,y\,(x + 2\,D\,z)\big)^2 \\ n_4 &= \big(3\,D\,x\,(x + 2\,D\,z) - \sqrt{D}\,y\,(x - 2\,D\,z)\big)^2 \end{aligned} \tag{17}$$

This is a nonconstant arithmetic progression of squares over $K = \mathbb{Q}(\sqrt{D})$. Since the rational point $P = (x : y : z)$ is a point of infinite order, each multiple $(x' : y' : z') = [m]P$ gives rise to an arithmetic progression $\{n_1', n_2', n_3', n_4'\}$ of four squares. □

For an example, consider the case when $D = 6$. Then the rational point $(x : y : z) = (-8 : -16 : 1)$ on the elliptic curve $X_0^{(6)}(24)$ is not a point of finite order; hence $X_0^{(6)}(24)$ has positive rank. We find the following arithmetic progression over $\mathbb{Q}(\sqrt{6})$:

$$\big\{n_1,\, n_2,\, n_3,\, n_4\big\} = \big\{(9 - 5\sqrt{6})^2,\, (15 - \sqrt{6})^2,\, (15 + \sqrt{6})^2,\, (9 + 5\sqrt{6})^2)\big\}. \tag{18}$$

In fact, there are infinitely many arithmetic progressions of four squares over $\mathbb{Q}(\sqrt{6})$. With the information we have above, we want to find an answer to the following question:

For which D does $X_0^{(D)}(24):\ y^2 = x^3 + 5\,D\,x^2 + 4\,D^2\,x$ have positive rank?

4. Cubes in Arithmetic Progressions

We may generalize the results in the previous section to arithmetic progressions of cubes. In 1823, Adrien-Marie Legendre showed that there are no three or more rational cubes in a nonconstant, nontrivial arithmetic progression – where we consider $(n_1 : n_2 : n_3) = (1 : 1 : 1)$ to be the constant progression and $(n_1 : n_2 : n_3) = (-1 : 0 : +1)$ to be the trivial progression. We review a modern proof of this statement.

Theorem 6 (Enrique González-Jiménez, [2]). *For each nonnegative integer D such that $\sqrt{-3\,D} \notin \mathbb{Q}$, denote the elliptic curves*

$$(19)\qquad \begin{aligned} X_0(36):& \qquad y^2 = x^3 - 27 \\ X_0^{(D)}(36):& \qquad y^2 = x^3 - 27\,D^3 \end{aligned}$$

There exists a nonconstant, nontrivial arithmetic progression $\{n_1, n_2, n_3\}$ of three cubes over $\mathbb{Q}(\sqrt{D})$ if and only if rank $X_0^{(D)}(36)(\mathbb{Q}) > 0$. In this case, there are infinitely many arithmetic progressions of three cubes over $\mathbb{Q}(\sqrt{D})$.

Proof. This is the content of [2, Theorem 7], although we give a slightly expanded proof. First assume that we have a nonconstant, nontrivial 3-term arithmetic progression of squares $\{n_1, n_2, n_3\} \subseteq K$ for the quadratic field $K = \mathbb{Q}(\sqrt{D})$. We will show that rank $X_0^{(D)}(36)\big(\mathbb{Q}\big) > 0$. Define the numbers

$$(20)\qquad \begin{aligned} x &= -6\left(\sqrt[3]{n_1} + \sqrt[3]{n_2} + \sqrt[3]{n_3}\right)\left(\sqrt[3]{n_1} - 2\sqrt[3]{n_2} + \sqrt[3]{n_3}\right) \\ y &= -27\left(\sqrt[3]{n_1}^2 - \sqrt[3]{n_3}^2\right) \\ z &= \left(\sqrt[3]{n_1} - 2\sqrt[3]{n_2} + \sqrt[3]{n_3}\right)^2 \end{aligned}$$

Using the equations $n_2 - n_1 = n_3 - n_2$, it is easy to verify that $y^2\,z = x^3 - 27\,z^3$. In other words, $(x : y : z) \in X_0(36)\big(K\big)$. One checks that this elliptic curve has at least two torsion elements:

$$(21)\qquad X_0(36)\big(K\big)_{\text{tors}} \supseteq X_0(36)\big(\mathbb{Q}\big)_{\text{tors}} = \big\{(0:1:0),\ (3:0:1)\big\} \simeq Z_2.$$

Using Table 2, we see that these points correspond either to the constant arithmetic progressions of cubes $(n_1 : n_2 : n_3) = (1 : 1 : 1)$ or the trivial arithmetic progressions of cubes $(n_1 : n_2 : n_3) = (-1 : 0 : 1)$. Note that $X_0^{(D)}(36) : y^2 = x^3 + M$ where $M = -27\,D^3$.

$$(22)\qquad X_0(36)\big(\mathbb{Q}(\sqrt{D})\big)_{\text{tors}} = X_0(36)\big(\mathbb{Q}\big)_{\text{tors}} \simeq Z_2.$$

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, n_4) over $\mathbb{Q}(\sqrt{D})$ that satisfy the following:

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

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

$$(23)\qquad \{n_1, n_2, n_3\} = \{(4 - 21\sqrt{2})^3, 22^3, (4 + 21\sqrt{2})^3)\}.$$

□

Lemma 1. $X_0(36)(\mathbb{Q}(\sqrt{D}))_{\text{tors}} = X_0(36)(\mathbb{Q})_{\text{tors}}$, *when $D \neq -3$.*

Table 2. $\mathbb{Q}$-Rational Points on $X_0(36): \; y^2\,z = x^3 - 27\,z^3$

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

Proof. "Kamienny proved that the only primes possibly dividing the order of the torsion subgroup of an elliptic curve over a quadratic field are 2,3,5,7,11, and 13. Then it is enough to compute for which quadratic fields the elliptic curve $E : y^2 = x^3 - 27$ [Notice: this is the same as our $X_0(36)$] has a torsion point of order $n \in (2, 3, 4, 5, 7, 11, 13)$. Note that we need to check $n = 4$ since there is a point or order 2 defined over $\mathbb{Q}$.

To achieve this we look for the irreducible factors of degree one or two of the nth division polynomial of E [Our $X_0(36)$] in $\mathbb{Z}[x]$. The set of these factors is $x, x - 3, x^2 + 3x + 9, x^2 - 6x - 18$. Therefore the only possible values D such that $E(\mathbb{Q}(\sqrt{D}))_{tors}$ [Our $X_0(36)(\mathbb{Q}(\sqrt{D}))_{tors}$] increases with respect $E(\mathbb{Q})_{tors}$ [our $X_0(36)(\mathbb{Q})_{tors}$] are $D = 3$ and $D = -3$. A straightforward computation shows that $E(\mathbb{Q}(\sqrt{3}))_{tors}\mathbb{C}ong\mathbb{Z}/2\mathbb{Z}$ and $E(\mathbb{Q}(\sqrt{-3}))_{tors}\mathbb{C}ong\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$." [Quoted from Gonzalez-Jimenez paper]. □

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

Motivating Question: *With the information we have above, we want to find an answer to the following question, "For which D is the* rank $X_0^{(D)}(36)(\mathbb{Q}) > 0$?"

5. Elimination of points from the image for squares

As we have previously noted, there is a motivation for eliminating points from the image of δ and δ' for a given $D = mp$.

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

$$v'^2 = d - 18Du'^2 - \frac{27D^2}{d}u'^4 \tag{24}$$

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

$$v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4 \tag{25}$$

so it will also suffice to show there are no integer solutions to this equation.

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

$$v^2 = d + 9Du^2 + \frac{27D^2}{d}u^4 \tag{26}$$

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:

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

so it will also suffice to show there are no integer solutions to this equation.

Additionally, we know the image of the two 2-torsion points for both δ and δ'. Suppose we form co-sets with respect to these points. Since the images of δ and δ' are each groups, if we can show a point is not in the image, the other point in the corresponding co-set is not in the image.

5.1. **Checking for Real Solutions.**

Lemma 1. *If $d < 0$ then there is no rational solution to $v^2 = d + 9Du^2 + \frac{27D^2}{d}u^4$*

Proof. Let $f(u) = d + 9Du^2 + \frac{27D^2}{d}u^4$.

Suppose $f(u) = 0$. Let us use the quadratic equation with respect to u^2. The discriminant Δ is:

$$\Delta = (9D)^2 - 4(\frac{27D^2}{d})(d) \tag{28}$$

$$\Delta = 81D^2 - 108D^2 \tag{29}$$

$$\Delta = (81 - 108)D^2 \tag{30}$$

$$\Delta = -27D^2 \tag{31}$$

$$\Delta < 0 \tag{32}$$

Thus $f(u)$ is never 0. Since $f(u)$ is a polynomial it is a continuous function, and thus by the Intermediate Value Theorem, $f(a)f(b) > 0$ for all a and b.

$$f(0) = d + 0 + 0 = d \tag{33}$$

By our initial assumption $d < 0$ so $f(0) < 0$

$$f(u)f(0) > 0 \text{ for all u} \tag{34}$$

$$f(u) < 0 \text{ for all u} \tag{35}$$

$$v^2 < 0 \tag{36}$$

But this impossible over the real numbers. Thus there are no real solutions to $v^2 = d + 9Du^2 + \frac{27D^2}{d}u^4$ and thus there are no rational solutions □

5.2. **Modulo p Rules.**

Lemma 5.1. *There are no rational solutions to either of the integer equations if u,v, or z is 0.*

Proof. If z is 0, the denominators of u' and v' are 0 which is impossible.

If $u = 0$, then $u' = 0$. This implies the equations are $v'^2 = d$ which have no rational solution since d is a square free number.

If $v = 0$, then $v' = 0$. This implies the equations are:

$$0 = d - 18Du'^2 - \frac{27D^2}{d}u'^4 \tag{37}$$

$$0 = d + 9Du'^2 + \frac{27D^2}{d}u'^4 \tag{38}$$

Using the quadratic equation, we get the discriminants are:

$$\Delta = (-18D)^2 - 4(-\frac{27D^2}{d})(d) = 324D^2 + 108D^2 = 432D^2 = 3(12D)^2 \tag{39}$$

$$\Delta = (9D)^2 - 4(\frac{27D^2}{d})(d) = 81D^2 - 108D^2 = -27D^2 = -3(3D)^2 \tag{40}$$

Since neither of these discriminants are perfect squares, there are no rational solutions. □

Each of the integer equations can be written as the sum of four terms. Each of these terms is never 0 since $u, v, z, d, D \neq 0$. Suppose we have an integer k and define the k-order of a number X as the integer n such that $k^n \mid X$ but $k^{n+1} \mathbb{N} mid X$.

Lemma 5.2. *If one of the terms in the integer equations has a lower k-order than the other three terms, there are no solutions.*

Proof. Suppose the minimal k-order of the four terms is n. Then let us divide the equation through by k^n. Then if we look at the integer equation mod k, we will get an equation of the form $X \equiv 0 (mod\ k)$ where $k \mathbb{N} mid X$ and $X \neq 0$. This of course has no solutions mod k and thus the entire equation has no integer solution. □

Lemma 5.3. *Let $D = mp$ and suppose $p \mid d$. If $(\frac{3}{p}) = -1$ then there are no solutions to* $v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$

Proof. Let us look at the p-order of the four terms. Let U, V, and Z be the p-orders of u, v, and z, respectively. So the orders are, respectively:

$$(2V + 2Z)(1 + 4Z)(1 + 2U + 2Z)(1 + 4U) \tag{41}$$

$(2V + 2Z)$ cannot attain the minimal value because then the minimal value would be even and it would be the only term that could attain the minimal value, thus no solutions.

So the minimal value of the p-order is attained by at least two of the terms on the right. However, if any two of the terms have the same p-order, $U = Z$, and thus all three of the terms have the same p-order. So divide the equation through by $p^(1+2U+2Z)$ and take it mod p. Let $d = \bar{d}p$, $D = \bar{D}p$, $\bar{u}$ be the p-free part of u, and $\bar{z}$ be the p-free part of z.

(42)
$$0 \equiv \bar{d}\bar{z}^4 - 18\bar{D}\bar{u}^2\bar{z}^2 - \frac{27\bar{D}^2}{\bar{d}}\bar{u}^4 \ (mod\ p)$$

Since we are working mod a prime. We can divide through by $\bar{d}\bar{z}^4$.

(43)
$$0 \equiv 1 - 18\frac{\bar{D}}{\bar{d}}\frac{\bar{u}^2}{\bar{z}^2} - 27\frac{\bar{D}^2}{\bar{d}^2}\frac{\bar{u}^4}{\bar{z}^4} \ (mod\ p)$$

Let $x = \frac{\bar{D}}{\bar{d}}\frac{\bar{u}^2}{\bar{z}^2}$

(44)
$$0 \equiv 1 - 18x - 27x^2 \ (mod\ p)$$

Since mod p is a finite field, usual algebra including the quadratic equation holds. In a necessary condition for a solution is that the square root of the discriminant is defined.

(45)
$$\Delta \equiv (-18)^2 - 4(-27) \ \equiv 324 + 108 \equiv 432 \equiv 3(12)^2 \ (mod\ p)$$

So $\sqrt{3}$ must be defined mod p which means that $(\frac{3}{p}) = 1$. So if $(\frac{3}{p}) = -1$, there are no solutions. □

Lemma 5.4. *Let $D = mp$ and suppose $p \mid d$. If $(\frac{-3}{p}) = -1$ then there are no solutions to $v^2z^2 = dz^4 + 9Du^2z^2 + \frac{27D^2}{d}u^4$*

Proof. Because of the similarities between the two equations, the same proof as the one above works to show that the equation has a solution only if the following has a solution:

(46)
$$0 \equiv 1 + 9x + 27x^2 \ (mod\ p)$$

Since mod p is a finite field, usual algebra including the quadratic equation holds. In a necessary condition for a solution is that the square root of the discriminant is defined.

(47)
$$\Delta \equiv (9)^2 - 4(27) \ \equiv 81 - 108 \equiv -27 \equiv -3(3)^2 \ (mod\ p)$$

So $\sqrt{-3}$ must be defined mod p which means that $(\frac{-3}{p}) = 1$. So if $(\frac{-3}{p}) = -1$, there are no solutions. □

Lemma 5.5. *Let $D = mp$ and suppose $p\mathbb{N}middd$. If $(\frac{d}{p}) = -1$ and $(\frac{-3d}{p}) = -1$ then there are no solutions to $v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$*

Proof. Let us look at the p-order of the four terms. Let U, V, and Z be the p-orders of u, v, and z, respectively. So the orders are, respectively:

(48)
$$(2V + 2Z)(4Z)(1 + 2U + 2Z)(2 + 4U)$$

I. If the minimal value is odd, then only $(1 + 2U + 2Z)$ attains the minimal value, which is impossible.

II. If the minimal value is even but not divisible by four, then $(2V + 2Z)$ and $(2 + 4U)$ attain the minimal value. Then let us divide the equation through by p^{2+4U} and take it mod p. Let $D = \bar{D}p$ and let $\bar{u}$, $\bar{v}$, and $\bar{z}$ be the p-free part of u, v, and z, respectively.

$$\bar{v}^2\bar{z}^2 \equiv -\frac{27\bar{D}^2}{d}\bar{u}^4 \ (mod\ p) \tag{49}$$

$$\frac{\bar{v}^2\bar{z}^2d^2}{9\bar{D}^2\bar{u}^4} \equiv -3d \ (mod\ p) \tag{50}$$

$$(\frac{\bar{v}\bar{z}d}{3\bar{D}\bar{u}^2})^2 \equiv -3d \ (mod\ p) \tag{51}$$

So it must be true that $(\frac{-3d}{p}) = 1$

III. If the minimal value is divisible by four, then $(2V + 2Z)$ and $(4Z)$ attain the minimal value. Then let us divide the equation through by p^{4Z} and take it mod p. Let $D = \bar{D}p$ and let $\bar{u}$, $\bar{v}$, and $\bar{z}$ be the p-free part of u, v, and z, respectively.

$$\bar{v}^2\bar{z}^2 \equiv d\bar{z}^4 \ (mod\ p) \tag{52}$$

$$\frac{\bar{v}^2\bar{z}^2}{\bar{z}^4} \equiv d \ (mod\ p) \tag{53}$$

$$(\frac{\bar{v}\bar{z}}{\bar{z}^2})^2 \equiv d \ (mod\ p) \tag{54}$$

So it must be true that $(\frac{d}{p}) = 1$

In conclusion, either $(\frac{-3d}{p}) = 1$ or $(\frac{d}{p}) = 1$ if there is a solution. So if $(\frac{d}{p}) = -1$ and $(\frac{-3d}{p}) = -1$ then there are no solutions □

5.3. **Modulo 3 rules.**

Lemma 5.6. *Suppose* $3\mathbb{N}midd$ *and* $3 \mid D$. *If* $d \equiv -1 \ (mod\ 3)$ *then there is no integer solution to either* $v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$ *or* $v^2z^2 = dz^4 + 9Du^2z^2 + \frac{27D^2}{d}u^4$.

Proof. Let us look at the 3-order of the four terms. Let U, V, and Z be the 3-orders of u, v, and z, respectively. So the orders are, respectively:

$$(2V + 2Z)(4Z)(3 + 2U + 2Z)(5 + 4U) \tag{55}$$

I. Suppose the minimal value is odd. Thus,

$$3 + 2U + 2Z = 5 + 4U \tag{56}$$

$$2Z = 2 + 2U \tag{57}$$

$$4Z = 4 + 4U \tag{58}$$

$$4Z < 5 + 4U \tag{59}$$

Which means that the minimal value isn't actually odd.

II. If the minimal value is even, then $(2V + 2Z)$ and $(4Z)$ attain the minimal value. Then let us divide the equation through by 3^{4Z} and take it mod 3. Let $\bar{v}$ and $\bar{z}$ be the 3-free part of v and z, respectively.

$$\bar{v}^2\bar{z}^2 \equiv d\bar{z}^4 \ (mod\ 3) \tag{60}$$

$$\frac{\bar{v}^2}{\bar{z}^2} \equiv d \ (mod\ 3) \tag{61}$$

$$(\frac{\bar{v}}{\bar{z}})^2 \equiv d \ (mod\ 3) \tag{62}$$

So $(\frac{d}{3}) = 1$ which means $d \equiv 1 \ (mod\ 3)$.

In conclusion, if there is an integer solution to the one of the equations then $d \equiv 1 \ (mod\ 3)$. So if $d \equiv -1 \ (mod\ 3)$, then there are not any integer solutions. □

Lemma 5.7. *Suppose* $3\mathbb{N}midd$ *and* $3\mathbb{N}midD$*. If* $d \equiv -1 \ (mod\ 3)$ *then there is no integer solution to either* $v^2z^2 = dz^4 - 18Du^2z^2 - \frac{27D^2}{d}u^4$ *or* $v^2z^2 = dz^4 + 9Du^2z^2 + \frac{27D^2}{d}u^4$*.*

Proof. Let us look at the 3-order of the four terms. Let U, V, and Z be the 3-orders of u, v, and z, respectively. So the orders are, respectively:

$$(2V + 2Z)(4Z)(2 + 2U + 2Z)(3 + 4U) \tag{63}$$

I. Suppose the minimal value is odd. Since only one term has odd 3-order, the minimal value is attained by only one term which is impossible.

II. Suppose the minimal value is even and $(2 + 2U + 2Z)$ is the minimal value. Then,

$$2 + 2U + 2Z < 3 + 4U \tag{64}$$

$$2Z < 1 + 2U \tag{65}$$

$$4Z < 1 + 2U + 2Z \tag{66}$$

$$4Z < 2 + 2U + 2Z \tag{67}$$

Which contradicts our initial assumption since $(2 + 2U + 2Z)$ was the minimal value.

III.Suppose the minimal value is even and $(2 + 2U + 2Z)$ is not the minimal value. So then only $(2V + 2Z)$ and $(4Z)$ attain the minimal value. Then let us divide the equation through by 3^{4Z} and take it mod 3. Let $\bar{v}$ and $\bar{z}$ be the 3-free part of v and z, respectively.

$$\bar{v}^2\bar{z}^2 \equiv d\bar{z}^4 \ (mod\ 3) \tag{68}$$

$$\frac{\bar{v}^2}{\bar{z}^2} \equiv d \ (mod\ 3) \tag{69}$$

$$(\frac{\bar{v}}{\bar{z}})^2 \equiv d \ (mod\ 3) \tag{70}$$

So $(\frac{d}{3}) = 1$ which means $d \equiv 1\ (mod\ 3)$.

In conclusion, if there is an integer solution to the one of the equations then $d \equiv 1\ (mod\ 3)$. So if $d \equiv -1\ (mod\ 3)$, then there are not any integer solutions.

□

5.4. **Modulo 8 rules.**

Lemma 5.8. *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* $2\ (mod\ 8)$.

Proof. Let us look at the 2-order of the four terms. Let U, V, and Z be the 2-orders of u, v, and z, respectively. So the orders are, respectively:

$$(2V + 2Z)(4Z + 1)(2U + 2Z + 2)(4U + 1) \tag{71}$$

I. Suppose the minimal value is even. Thus, $2V + 2Z = 2U + 2Z + 2$.

If $U \le Z$, then $2V + 2Z \ge 4U + 2 > 4U + 1$ which contradicts the assumption

If $Z \le U$, then $2V + 2Z \ge 4Z + 2 > 4Z + 1$ which contradicts the assumption

II. Suppose the minimal value is odd. Then $4Z + 1 = 4U + 1$ which implies $Z = U$. Then let us divide the equation through by 2^{4Z+1} and take it mod 8. Let $\bar{u}$ and $\bar{z}$ be the 2-free part of u and z, respectively. And let $\bar{v} = \frac{v}{2^{2Z+2}}$.

$$2\bar{v}^2\bar{z}^2 \equiv \bar{d}\bar{z}^4 - 18\bar{D}\bar{u}^2\bar{z}^2 - 27\frac{27\bar{D}^2}{\bar{d}}\bar{u}^4\ (mod\ 8) \tag{72}$$

But all odd squares are 1 mod 8

$$2\bar{v}^2 \equiv \bar{d} - 18\bar{D} - 27\frac{27\bar{D}^2}{\bar{d}}\ (mod\ 8) \tag{73}$$

Also $2\bar{v} \equiv 0, 2\ (mod\ 8)$

So in conclusion, if there is a solution to the equation, then $\bar{d}z^4 - 18\bar{D} - \frac{27\bar{D}^2}{\bar{d}} \equiv 0$ or $2\ (mod\ 8)$ □

Lemma 5.9. *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* $2\ (mod\ 8)$.

Proof. Let us look at the 2-order of the four terms. Let U, V, and Z be the 2-orders of u, v, and z, respectively. So the orders are, respectively:

$$(2V + 2Z)(4Z + 1)(2U + 2Z + 1)(4U + 1) \tag{74}$$

I. Suppose the minimal value is even. Since only one term has even 2-order, this is impossible.

II. Suppose the minimal value is odd.

If $4Z+1 < 4U+1$, then $Z < U$ so $4Z+1 < 2U+2Z+1$. Which cannot be because then the minimal value is only attained by one term

If $4U+1 > 4Z+1$, then $U < Z$ so $4U+1 < 2U+2Z+1$. Which cannot be because then the minimal value is only attained by one term

Thus it must be the case that $4Z+1 = 4U+1$ which implies $Z = U$. Then let us divide the equation through by 2^{4Z+1} and take it mod 8. Let $\bar{u}$ and $\bar{z}$ be the 2-free part of u and z, respectively. And let $\bar{v} = \frac{v}{2^{2Z+2}}$.

$$2\bar{v}^2\bar{z}^2 \equiv \bar{d}\bar{z}^4 + 9\bar{D}\bar{u}^2\bar{z}^2 + 27\frac{27\bar{D}^2}{\bar{d}}\bar{u}^4 \ (mod\ 8) \tag{75}$$

But all odd squares are 1 mod 8

$$2\bar{v}^2 \equiv \bar{d} + 9\bar{D} + 27\frac{27\bar{D}^2}{\bar{d}} \ (mod\ 8) \tag{76}$$

Also $2\bar{v} \equiv 0, 2 \ (mod\ 8)$

So in conclusion, if there is a solution to the equation, then $\bar{d}z^4 + 9\bar{D} + \frac{27\bar{D}^2}{\bar{d}} \equiv 0$ or $2 \ (mod\ 8)$ □

Lemma 5.10. *Suppose* $2\mathbb{N}midd$ *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.*

$$d + 2 * 9\bar{D} + 4 * \frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8) \tag{77}$$

$$d \equiv 1 \ (mod\ 8) \tag{78}$$

$$4 * d + 2 * 9\bar{D} + \frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8) \tag{79}$$

$$\frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8) \tag{80}$$

Proof. Let us look at the 2-order of the four terms. Let U, V, and Z be the 2-orders of u, v, and z, respectively. So the orders are, respectively:

$$(2V + 2Z)(4Z)(2U + 2Z + 1)(4U + 2) \tag{81}$$

I. Suppose the minimal 2-order is odd. Since there is only one term with odd 2-order, this is impossible.

II. Suppose the minimal 2-order is divisible by 4. So the minimal 2-order is attained by $(2V + 2Z)$ and $(4Z)$.

1. Suppose $U = Z$. Divide the equation through by 2^{4Z} and take it mod 8. Note all 2-free squares are 1 mod 8.

$$d + 2 * 9\bar{D} + 4 * \frac{27\bar{D}^2}{d} \equiv 1 \ (mod\ 8) \tag{82}$$

2. Suppose $U > Z$. Divide the equation through by 2^{4Z} and take it mod 8. Note all 2-free squares are 1 mod 8.

$$d \equiv 1\ (mod\ 8) \tag{83}$$

III. Suppose the minimal 2-order is even but not divisible by 4. So the minimal 2-order is attained by $(2V + 2Z)$ and $(4U + 2)$.

1. Suppose $Z = U + 1$. Divide the equation through by 2^{4U+2} and take it mod 8. Note all 2-free squares are 1 mod 8.

$$4 * d + 2 * 9\bar{D} + \frac{27\bar{D}^2}{d} \equiv 1\ (mod\ 8) \tag{84}$$

2. Suppose $Z > U + 1$. Divide the equation through by 2^{4U+2} and take it mod 8. Note all 2-free squares are 1 mod 8.

$$\frac{27\bar{D}^2}{d} \equiv 1\ (mod\ 8) \tag{85}$$

In conclusion, we see that if the equation has a solution, one of the four conditions must be satisfied. □

6. Results

After applying the previous lemmas to eliminate points from the images, we are left with upper bounds for the size of the images. And we can use these to form an upper bound for the rank. Here is the table for the upper bounds on the rank for $X_0^{(D)}(36)$. The columns correspond to an m and the rows correspond to a 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

In the previous table, we have found examples with ranks of the upper bound and if the upper bound is 2 or 3, we have found examples with rank 2 less than the upper bound. All these examples can be found by looking at the first ten primes except for the cases with rank 3. For these cases, if we let $p = 2521$ we get curves of rank 3.

7. Computer Program

This following computer program is written in python. It uses the elimination theorems to eliminate points from the image to gain an upper bound on the rank.

```
##############general functions

def squarefree(a):
    if a==0: return 0
    while (a%4 == 0): a /= 4
    while (a%9 == 0): a /= 9
    return a

def legendre(a,p): #assume a only has factors of -1, 2, and 3 and that p is prime > 3
    a=squarefree(a)
    if a==0: return 1

    legendre = 1
    if a<0 and p%4 == 3: legendre *= -1
    if a%2==0 and p%8 in [3,5]: legendre *= -1
    if a%3==0 and p%12 in [5,7]: legendre *= -1
    return legendre

def floorLog2(imageCount):
    for x in range(0,4):
        if imageCount < 2**(x+1): return x

def initializeTorsionImageSquares(m): # initializes the four points we know are in the i
    image0=[ [1,0] , [1,0]  ]
    image1=[ [1,0] , [m,1]  ]
    image2=[ [-m,1] , [-3,0] ]
    image3=[ [-m,1] , [squarefree(-3*m),1]  ]

    return [image0,image1,image2,image3]

def initializeDs(m,include_2_in_d,include_3_in_d): #returns a set of all possible d's
    #d is a double such that the first entry is a multiplier and the second entry is for
    QS=[]
    for a in range(0,2):
        for b in range(0,1 + include_2_in_d):
            for c in range(0,1 + include_3_in_d):
                for d in range(0,2):
                    QS.append([ (-1)**a * (2)**b * (3)**c, d ])
    return QS

def multiply(d1,d2): #this multiplies two d's in the double form
```

```
    return [squarefree(d1[0]*d2[0]), (d1[1] + d2[1])%2]

def convertD(d,p): #this converts a d in the double form to an integer
    if d[1] == 0: return d[0]
    if d[1] == 1: return d[0]*p

################# elimination for squares

def eliminateSquares(d1,d2,m,p):
    D = m*p
    d1 = convertD(d1,p)
    d2 = convertD(d2,p)

    for i in range(0,6):
        if evaluateLemmas(permute(d1,-d2,D,i)):return 1
        if evaluateLemmas(permute(d2,-d1*d2,3*D,i)):return 1

    if lemma7(d1,d2,D): return 1
    if lemma8(d1,d2,D): return 1

    return 0

def permute(a,b,c,i):
    if i==0: return [a,b,c]
    if i==1: return [a,c,b]
    if i==2: return [b,a,c]
    if i==3: return [b,c,a]
    if i==4: return [c,a,b]
    if i==5: return [c,b,a]

def evaluateLemmas(X):
    #these are the first six lemmas which apply to a*x1^2 + b*x2^2 + c*x0^2 = 0 such tha
    [a,b,c] = X
    if a*b>0 and b*c>0: return 1
    if a%3 != 0 and a%3 == b%3 and c%9 in [3,6]: return 1
    if a%9 in [3,6] and a%9 == b%9 and c%3 != 0: return 1
    if a%4 in [1,3] and a%4 == b%4 and b%4 == c%4: return 1
    if a%8 in [2,6] and a%8 == b%8 and b%8 == c%8: return 1
    if a%8 in [2,6] and b%2 == 1 and c%2 == 1 and (b+c)%8 != 0 and (a+b+c)%8 != 0: retur

    return 0

def lemma7(d1,d2,D):
    if not(D%8 in [2,6]):return 0
    if d1%8 in [0,4]:return 0
    if d2%8 in [0,4]:return 0

    if d1%8 == d2%8 and d2%8 == 1: return 0
    if d1%4 == (3*D)%4 and d2%4 == 1: return 0
    if d2%8 == D%8: return 0
    if d1%8 == (3*D + 1)%8 and d2%8 == 1: return 0

    return 1

def lemma8(d1,d2,D):
    if D%8 != 1: return 0
    if d1%2 != 1: return 0
    if d2%2 != 1: return 0

    if [d1%8,d2%8] in [[1,1], [5,1], [3,5], [7,5]]: return 0

    return 1

################# elimination for cubes

def eliminateCubes(d,m,p,equation):
    D=m*p
    divByP = d[1]
    d = convertD(d,p)

    if cubesRealSol(d,p,equation): return 1
    if cubesModP(d,p,equation,divByP): return 1
    if cubesMod3(d,p,equation): return 1
    if cubesMod8(d,D,p,equation): return 1

    return 0

def cubesRealSol(d,p,equation):
    if d < 0 and equation==2: return 1
    return 0

def cubesModP(d,p,equation,divByP):
    if divByP==1:
        if equation==1 and legendre(3,p) == -1: return 1
        if equation==2 and legendre(-3,p) == -1: return 1

    if divByP==0:
        if equation==1 and legendre(d,p) == -1 and legendre(-3*d,p) == -1: return 1
        if equation==2 and legendre(d,p) == -1 and legendre(3*d,p) == -1: return 1
    return 0

def cubesMod3(d,p,equation):
    if d % 3 == 2: return 1
    return 0

def cubesMod8(d,D,p,equation):
    if D%2 == 0: Dbar = D / 2
    else: return 0

    if d%2 == 0:
        dbar = d / 2
        if equation==1 and (dbar - 18*Dbar - 27*Dbar*Dbar/dbar) % 8 in [0,2]: return 0
        if equation==2 and (dbar + 9*Dbar + 27*Dbar*Dbar/dbar) % 8 in [0,2]:return 0

    if d%2 != 0:
        if equation==1: return 0

        if d%8 == 1: return 0
        if (d + 2*9*Dbar + 4*27*Dbar*Dbar/d)%8 == 1: return 0
        if (27*Dbar*Dbar/d)%8 == 1: return 0
        if (4*d + 2*9*Dbar + 27*Dbar*Dbar/d)%8 == 1: return 0

    return 1

############## the two functions for computing the upper bounds for a given m and p

def computeBoundSquares(m,p):
    Image = initializeTorsionImageSquares(m)

    remaining = 0

    for d1 in initializeDs(m,1,m%3==0):
        for d2 in initializeDs(m,m%2==0,1):
            eliminate = 0

            for im in Image:
                if eliminateSquares(multiply(d1,im[0]),multiply(d2,im[1]),m,p):
                    eliminate =1

            if not( eliminate ):
                remaining += 1

    return floorLog2(remaining/4)
```

```
def computeBoundCubes(m,p):
    remaining1=0
    remaining2=0

    for d in initializeDs(m,m%2==0,1):
        if not( eliminateCubes(d,m,p,1) or eliminateCubes(multiply(d,[-3,0]),m,p,1) ):
            remaining1 += 1

    for d in initializeDs(m,m%2==0,1):
        if not( eliminateCubes(d,m,p,2) or eliminateCubes(multiply(d,[3,0]),m,p,2) ):
            remaining2 += 1

    return floorLog2(remaining1/2) + floorLog2(remaining2/2)


for conductor in [24,36]: # this is the function that prints the results
    if conductor==36: print "\mathbb N\mathbb N\mathbb N"
    print "For X0(%d):\mathbb N" %(conductor)
    print "\t1\t2\t3\t6\t-1\t-2\t-3\t-6\mathbb N"

    for p in [1,5,7,11,13,17,19,23]:
        print "%d\t" %(p),
        for m in [1,2,3,6,-1,-2,-3,-6]:
            if conductor==24: upper = computeBoundSquares(m,p)
            if conductor==36: upper = computeBoundCubes(m,p)
            print "%d\t" %(upper),
        print "\mathbb N"
```

References

[1] Alexander Diaz, Zachary Flores, and Markus Vasquez. Arithmetic Progressions over Quadratic Fields. *MSRI-UP Journal*, 2010.

[2] Enrique Gonzalez-Jimenez. Three Cubes in Arithmetic Progression Over Quadratic Fields. *arXiv.org*, 2009.

[3] Enrique Gonzalez-Jimenez. Three cubes in arithmetic progression over quadratic fields. *Archiv der Mathematik*, 2010.

[4] Enrique Gonzalez-Jimenez and Jörn Steuding. Arithmetic progressions of four squares over quadratic fields. *arXiv.org*, 2009.

[5] Soonhak Kwon. Torsion subgroups of elliptic curves over quadratic extensions. *Journal of Number Theory*, 1997.

[6] Barry Mazur. Modular curves and the Eisenstein ideal. *Institut des Hautes Etudes Scientifiques. Publications Mathématiques*, 1977.

[7] L J Mordell. *Diophantine Equations*. 1969.

[8] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. 2009.

Purdue University, Department of Mathematics, Mathematical Sciences Building, 150 North University Street, West Lafayette, IN 47907-2067
E-mail address: rlarcher@purdue.edu

Purdue University, Department of Mathematics, Mathematical Sciences Building, 150 North University Street, West Lafayette, IN 47907-2067
E-mail address: egoins@math.purdue.edu

1022 1st Street, West Lafayette, IN 47906
E-mail address: liu457@purdue.edu

1212 Comer Avenue, Indianapolis, IN 46203
E-mail address: marti249@purdue.edu

17424 Lochner Road, Spencerville, IN 46788
E-mail address: somussma@purdue.edu

Purdue University, Department of Mathematics, Mathematical Sciences Building, 150 North University Street, West Lafayette, IN 47907-2067
E-mail address: jweigand@math.purdue.edu

132 Andrew Place, Apartment Room #208, West Lafayette, IN 47906
E-mail address: yuan27@purdue.edu