A BOUND ON THE RANK OF ELLIPTIC CURVES

CHRISTINE MCMEEKIN

Abstract. This paper is intended as an expository piece investigating an upper bound on the rank of elliptic curves defined over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve by a Weierstrass equation of the form $y^2 = f(x)$ where $f(x)$ is a cubic monic polynomial with integral coefficients and with x^2 term equal to 0. Let e_1, e_2, e_3 be the roots of $f(x)$ which we assume to be distinct. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. We prove that $R_{E(\mathbb{Q})} \leq 2(\mathrm{ord}_2(h(K)) + r_1 + r_2 + \nu(\Delta) - 1)$ where $h(K)$ is the class number of K , r_1 is the number of real embeddings of K into $\mathbb{C}$, r_2 is the number of pairs of non-real embeddings of K into $\mathbb{C}$, and $\nu(\Delta)$ is the number of prime ideals in the ring of integers of K dividing the ideal generated by the discriminant of $f(x)$. This bound is proven first in a couple of special cases for the sake of intuition and then more generally. We also investigate the usefulness of this bound through numerical examples and discuss cases in which this bound can be made sharper.

Contents

1. Introduction

The study of elliptic curves has long been an interesting topic to mathematicians since Diophantus, a Greek mathematician who was interested among other things in rational solutions to polynomials with integral coefficients, mainly quadratics and cubics. He observed that given one solution to a quadratic, it was possible to obtain infinitely many, in the following manner. Consider for example a circle described by the equation $x^2 + y^2 = 1$. We know at least one rational solution to this equation right off the bat; observe that $(x, y) = (-1, 0)$ is one such solution. Next, we construct a straight line passing through this point of rational slope. Begin with a general linear equation $y = mx + b$ where m and b are rational. Plugging in $(x, y) = (-1, 0)$, we obtain $0 = -m + b$, or in other words, $m = b$.

So the general equation of a line of rational slope m passing through the point $(-1,0)$ is $y = mx+m$ where m is any rational number we'd like. Next, we should take note that the line we just created will intersect the circle in exactly two points and we already know one of these points. The point (x,y) is in the intersection of this line with this circle exactly when $(mx+m)^2+x^2 = 1$. (This was obtained by plugging the equation of our line into the equation of our circle). By expanding this, we see that (x,y) is in the intersection when $(m^2+1)x^2+2m^2x+m^2-1 = 0$. Thus, to find the other point at which the line intersects the circle, we must find the second root of $(m^2+1)x^2+2m^2x+m^2-1 = 0$. Since we know one root is -1, we can divide out a factor of $x+1$ to obtain $(m^2+1)x+(m^2-1) = 0$, so the other root occurs when $x = \frac{1-m^2}{1+m^2}$. Solving for y, we get that $(x,y) = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$ is the other point of intersection of the line with the curve. Notice that since m is rational, these expressions are rational numbers. The other point of intersection of the line with the circle is, in particular, a point on the circle and thus satisfies the equation $x^2+y^2 = 1$. Thus for any choice of m, a rational number, we obtain $\left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$ which is a rational solution to the equation $x^2+y^2 = 1$, yielding infinitely many solutions to this quadratic.

Furthermore, this yields *all* rational solutions to the equation $x^2+y^2 = 1$ because given any rational point on the circle, we can find a line of the form $y = mx+m$ which passes through this point and $(-1,0)$ for some rational m.

In the context of the study of elliptic curves, the importance of this observation lies in its generalization to cubics, as an elliptic curve is a "smooth" cubic equation in two variables. While this method does not work in exactly the same way for cubics, there is a very important generalization. Notice that in the quadratic case, once we knew one solution and we picked a line passing through it of rational slope, there was exactly one other point in the intersection of that line with the quadratic. However, a line intersects a cubic in three points, not just two. For one thing, this means that in general, we are no longer ensured any other rational points on a cubic simply from having one and drawing a line through it of arbitrary rational slope; this is because if we draw an arbitrary line of rational slope through a given rational point on the curve, then the set of points in the intersection of the line with the curve are roots of a polynomial of the same degree as the curve we began with and when one solution to a quadratic is rational, it is necessarily true that the other root is rational [1], but when one solution to a cubic is rational, this tells us nothing about whether the other two roots are rational. For example, we could consider the elliptic curve defined by $y^2 = x^3-3x$. We can see that this has a rational solution at $(0,0)$. Next take a line of arbitrary rational slope passing through $(0,0)$. For example, we could take the line $y = 0$. The set of points in the intersection of this line with the curve are the roots of $x^3-3x = 0$, which has roots 0, and $\pm\sqrt{3}$. So there are no other rational points in the intersection of this line with the curve. In fact, $(0,0)$ is the *only* rational point on this particular curve. So for this curve, if we take *any* line of rational slope going through $(0,0)$, we will *never* get a pair of rational points as the other points of intersection of the curve with the line.

[1] The reader should check that this is true.

In order to generalize this method to cubics, we will need two (not necesarily distinct)[2] rational solutions to begin with, and then if we draw the line connecting them, we will be guaranteed a third rational solution. This seems much more restrictive. Before we only had to choose one rational point on the curve and could choose infinitely many lines of rational slope going through this point to obtain infinitely many new rational solutions. Now, we must choose two points (or choose one point "twice") and from them, we only get one line instead of infinitely many, and thus we only get one new rational solution instead of infinitely many. Furthermore, it is no longer obvious that we can obtain all rational points on the curve in this way as it was in the quadratic case, and if it is true that we can obtain all of them, can we start with just one as in the quadratic case or do we need more? How many more? Can we start with finitely many rational points and produce all rational points on the curve in this way? The answer to this non-trivial question was proved somewhat by accident by Louis Mordell in 1923 and is presented here in the Mordell-Weil Theorem which will be discussed in Section 2. Although the method of obtaining new rational points on the curve from old ones appears very restrictive, this seemingly unyielding tool will provide us with an unexpectedly rich and beautiful structure on elliptic curves, a structure that has yet to be fully understood by modern mathematicians, and a structure in which this paper will partially investigate.

2. The Group Law and the Mordell-Weil Theorem

In this section, we introduce the group law on elliptic curves. For our purposes, we will define an elliptic curve[3] to be a smooth cubic equation in two variables x, and y of the form $y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$. This curve is said to be smooth when $x^3 + Ax + B$ has no repeated roots, or equivalently, when $4A^3 + 27B^3 \neq 0$. We are interested in finding rational solutions to such equations.

In Section 1, we saw a way to obtain *all* rational solutions to a quadratic equation from knowing only one rational solution. Ideally, we would like a way to obtain all rational points on an elliptic curve. We saw that this was not quite as simple as the quadratic case. However, we did see one way to produce new rational points on an elliptic curve from old ones; given two rational points on an elliptic curve, we can draw a straight line connecting them and then the third point of intersection of the line with the curve is a new rational point on the curve. We could also begin with one point on the curve and draw the tangent line through that point.

First we point out why it is true that if we take two rational points on the curve and draw a line connecting them that the third point of intersection is rational. Also, if we take one point and do the same using its tangent line, then the third point of intersection is rational.

[2]These two points don't have to be distinct. If they are the same point, the line connecting them is the tangent line to the curve at that point.

[3]This is not the most general form of an elliptic curve, but it can be shown that any elliptic curve can be written in this way via a change of variables. This form is known as Weierstrass form. In general, an elliptic curve is simply a smooth cubic polynomial in two variables set equal to zero.

First note that any straight line will intersect a cubic in exactly three points. Some of these points may be complex, and in the case that the line is tangent to the curve at a point, the point at which it is tangent will be repeated. Indeed if we plug $y = mx + b$ into $y^2 = x^3 + Ax + B$, we get $x^3 + m^2x^2 + (A - 2mb)x + B + b^2 = 0$, so the points which lie on both the line and the curve are the points $(x, mx + b)$ whose x-coordinates are roots of this cubic. Vertical lines are an exception. If we plug in $x = c$, we get $y^2 = c^3 + Ac + B$, which only has two roots. This is dealt with formally using projective geometry. Although to simplify matters, we define the *point at infinity*, $\mathcal{O}$, to be the third point of intersection of a vertical line with an elliptic curve. With this convention, all lines intersect an elliptic curve in exactly three points[4].

Now suppose $(x_1, y_1), (x_2, y_2)$ are rational points on a given elliptic curve, $y^2 = x^3 + Ax + B$. That is $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ and satisfy $y_1^2 = x_1^3 + Ax_1 + B$ and $y_2^2 = x_2^3 + Ax_2 + B$. Then the line connecting them is given by $(y - y_1) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1)$ using the point-slope formula. Equivalently, $y = mx - mx_1 + y_1$ where $m = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)$. If we plug this into the equation of our elliptic curve, then after some algebraic manipulation, we obtain

$$x^3 - m^2x^2 + (A - 2my_1 + 2m^2x_1)x + B - (y_1 - mx_1)^2 = 0.$$

Thus, the points of intersection of the line with the curve have x-coordinate satisfying this cubic equation. We already know two of the roots are x_1 and x_2, so if we factor out $(x - x_1)(x - x_2)$ we will be left with a linear equation in x, the root of which is the x-coordinate of the third point of intersection of the line with the curve. Although, if we are only trying to show that the third point of intersection is rational, this is unnecessary. If we denote the third point of intersection (x_3, y_3), we get

$$\begin{aligned} x^3 - m^2x^2 + (A - 2my_1 + 2m^2x_1)x + B - (y_1 - mx_1)^2 &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 \end{aligned}$$

and we see by comparing the coefficients of x^2 on each side of the equation that $x_1 + x_2 + x_3 = m^2$. Solving for x_3, we get $x_3 = m^2 - x_1 - x_2$. So if x_1, x_2, y_1, y_2 are rational, then m is rational, and so x_3 is rational. Then since $y = mx - mx_1 + y_1$, y_3 is also rational. A similar procedure can be done for the case when $(x_1, y_1) = (x_2, y_2)$ and we consider the tangent line to the curve at this point.

Notice that whenever we have a point (x, y) on an elliptic curve of the form $y^2 = x^3 + Ax + B$, then $(x, -y)$ is also a point on the curve because the only y in the equation of our curve is squared. Also, if (x, y) is rational, so is $(x, -y)$. If $P = (x, y)$, we will use the notation $-P$ to mean $(x, -y)$. We define $-\mathcal{O}$ to simply be $\mathcal{O}$.

Definition 2.1. Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be rational points on the curve. (That is, $x_1, y_1, x_2, y_2 \in \mathbb{Q}$ and $y_1^2 = x_1^3 + Ax_1 + B$ and $y_2^2 = x_2^3 + Ax_2 + B$). Let $R = (x_3, y_3)$ be the third point of intersection of

[4]These three points are possibly complex and possibly repeated

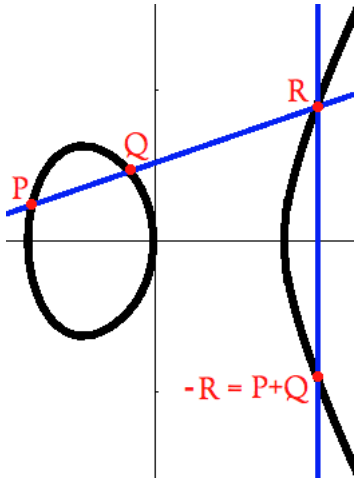

FIGURE 1. Addition of points on an elliptic curve

the curve with line through P and Q. (If $P = Q$, this is the third point of intersection of the curve with the tangent line to the curve at this point). Then we define the sum of P and Q to be $P+Q = -R$ as illustrated in figure 1. For $m \in \mathbb{N}$, we define $mP = P+P+...+P$ (m times) and $-mP = -P-P-...-P$ (m times).

Theorem 2.2. *The set of rational points on an elliptic curve together with the addition defined above form an abelian group where the identity is the point at infinity, $\mathcal{O}$.*

We will not prove this theorem here, but instead we refer the reader to [Sil09]. Most of the proof is relatively straight forward with the exception of associativity which is slightly more involved. In this group, notice that the inverse of a point P is $-P$ since the line connecting (x, y) and $(x, -y)$ is vertical, so the third point of intersection is $\mathcal{O}$. Thus $P - P = -\mathcal{O} = \mathcal{O}$.

Example 2.3. Let E be the elliptic curve defined by $y^2 = x^3 + 1$. We can see that $P = (0, 1)$ and $Q = (-1, 0)$ are points on this curve. To get another point, we could add $P+Q$. First notice that the line connecting P and Q is described by the equation $y = x+1$. So first we must find the third point of intersection of the curve with this line. We do so by plugging the equation for the line into the equation for the curve.

$$x^3 + 1 = (x+1)^2 = x^2 + 2x + 1$$
$$\implies x^3 - x^2 - 2x = 0$$

We already know two roots of this, namely, the x-coordinates of the two points we started with, -1 and 0. So we can factor out the roots we know and we could obtain via long division

$$x^3 - x^2 - 2x = x(x+1)(x-2).$$

So the third point of intersection of the line with the curve occurs when $x = 2$. Plugging into our linear equation for y, we get $y = 3$, so $R = (2, 3)$ is a point on the curve. If we check our work, $3^3 = 2^3 + 1$, which confirms that this point is on the curve. Then the sum of P and Q is $-R = (2, -3)$. Thus $P + Q = (2, -3)$.

Naturally, Theorem 2.2 raises some questions about the structure of elliptic curves, that is, about the structure of the group associated to an elliptic curve. Is this group finite or infinite? If it is infinite, is it at least finitely generated? If so, how do we find the generators? Is there an easy way to figure out what the group associated to a given curve is simply from knowing the coefficients A and B?

Modern mathematicians know the answers to some of these questions, but not everything is known. For example, we do not yet know how to completely determine the group associated to a given elliptic curve.

One very important theorem about the structure of this group was proven by Louis Mordell (and later generalized by André Weil). We will present this theorem here without proof.

Theorem 2.4 (Mordell-Weil)**.** *The group associated to an elliptic curve is a finitely generated abelian group. In other words, there exist finitely many rational points on the curve $P_1, P_2, ..., P_n$, such that any rational point on the curve, Q, is a linear combination of these points, so $Q = m_1P_1 + m_2P_2 + ... + m_nP_n$ for some $m_1, m_2, ..., m_n \in \mathbb{Z}$.*

We will call the group associated to an elliptic curve the Mordell-Weil group and denote it $E(\mathbb{Q})$.

Corollary 2.5. *By the fundamental theorem of finitely generated abelian groups, $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^{R_{E(\mathbb{Q})}}$ where T is a finite abelian group and $R_{E(\mathbb{Q})} \in \mathbb{Z}$ such that $R_{E(\mathbb{Q})} \geq 0$.*

Definition 2.6. $R_{E(\mathbb{Q})}$ is the *rank* of an elliptic curve.

Definition 2.7. The set of points of finite order, $T = \{P \in E(\mathbb{Q}) : mP = \mathcal{O}$ for some $m \in \mathbb{Z}\}$ is called the *torsion part* or the *torsion subgroup*. A point $P \in E(\mathbb{Q})$ of finite order is called a *torsion point*.

Definition 2.8. $E(\mathbb{Q})/T$ is called the *free part* of the Mordell-Weil group.

Example 2.9. Can we find the Mordell-Weil group of the curve considered in Example 2.3, $y^2 = x^3 + 1$? In example 2.3, we saw that $(0, 1), (-1, 0), (2, 3) \in E(\mathbb{Q})$. Taking the inverses of these points we also get $(0, -1), (2, -3) \in E(\mathbb{Q})$. Can we find any more points?

Let $P = (2, 3)$. To compute $2P$, we will take the derivative at P in order to find an equation of the tangent line.

$$\begin{aligned} y^2 &= x^3 + 1 \\ \implies 2ydy &= 3x^2 \end{aligned}$$

$$\implies \frac{dy}{dx} = \frac{3x^2}{2y}$$

Evaluating at $P = (2, 3)$, we get $\frac{3\times 2^2}{2\times 3} = \frac{12}{6} = 2$ so the slope of the tangent line through P is 2. Setting $y = 2x + b$ and plugging in $P = (2, 3)$, we obtain $b = -1$, so the tangent line to the curve at P is defined by $y = 2x - 1$.

Plugging this into our equation for the curve, we get

$$(2x-1)^2 = x^3 + 1$$
$$\implies x^3 - 4x^2 + 4x = 0$$
$$\implies x(x-2)^2 = 0$$

So the third point of intersection has x-coordinate 0 and $y = 2x - 1$, so the third point of intersection is $(0, -1)$, so $2P = (0, 1)$, which was a point we already knew.

If we continue in this fashion (which is left as an exercise), we will see that for $P = (2, 3)$,

$$2P = (0, 1)$$
$$3P = (-1, 0)$$
$$4P = (0, -1)$$
$$5P = (2, -3)$$
$$6P = \mathcal{O}$$

so all of the points we have seen so far are part of the torsion subgroup since they are of finite order. This tells us that for this curve, $\mathbb{Z}/6\mathbb{Z}$ is a subgroup of the Mordell-Weil group. However, we do not yet have the tools to figure out much more about the Mordell-Weil group for this curve.

There are many unanswered questions about this example. How do we know whether there are more generators? Is $T \cong \mathbb{Z}/6\mathbb{Z}$ or are there more torsion points? Are there any points of infinite order, and if there were, how would we recognize them?

Next, we address those questions having to do with the torsion points. These are the easier questions to answer. Many questions about the rank or the free part of the Mordell-Weil group are still not known.

In this section we focus on $T = \{P \in E(\mathbb{Q}) : mP = \mathcal{O} \text{ for some } m \in \mathbb{Z}\}$, the torsion part of the Mordell-Weil group. To better understand the torsion part, we introduce the Nagell-Lutz theorem and Mazur's theorem, which we will state here without proof. A more detailed discussion can be found in [Sil09] or [LR].

Theorem 2.10 (Nagell-Lutz)**.** *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$. If $P = (x_0, y_0) \in E(\mathbb{Q})$ is a torsion point, then P satisfies the following.*

1. *The coordinates of P are integers. (i.e $x_0, y_0 \in \mathbb{Z}$)*
2. *If P is of order 2, then $y_0 = 0$ and $x_0^3 + Ax_0 + B = 0$*

(3) *If P is a point of order $n \geq 3$, then $y_0^2 | \Delta$ where Δ is the discriminant*[5] *of x^3+Ax+B for $A, B \in \mathbb{Z}$.*

Corollary 2.11. *If for some $P \in E(\mathbb{Q})$, there exists $m \in \mathbb{Z}$ such that mP does not have integer coefficients, then P has infinite order in $E(\mathbb{Q})$.*

Corollary 2.12. *Given $P = (x_0, y_0) \in E(\mathbb{Q})$, if $y_0 \neq 0$ and $y_0^2 \nmid \Delta$, then P has infinite order.*

The Nagell-Lutz theorem is very useful to show that a given point has infinite order and also to completely determine the torsion subgroup. Let's revisit our previous example applying the Nagell-Lutz theorem to determine the torsion subgroup.

Example 2.13. Recall that we were working over the elliptic curve defined by $y^2 = x^3 + 1$ and we found that $P = (2, 3)$, $2P = (0, 1)$, $3P = (-1, 0)$, $4P = (0, -1)$, $5P = (2, -3)$, and $6P = \mathcal{O}$ were all points on the curve which showed that the torsion subgroup, T has a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z}$, but we could not tell if there were any more torsion points on the curve.

The discriminant of $x^3 + Ax + B$ is $\Delta = -4A^3 - 27B^2$, so the discriminant of $x^3 + 1$ is -27. Thus by the Nagel-Lutz theorem, if (x, y) is a torsion point, then $y = 0$ or $y^2 | -27$. So for a torsion point (x, y), the possible values of y are $0, \pm 1, \pm 3$.

We saw that if $y = 0$, then $x^3 = -1$ has only one real solution, which gave us the point $(-1, 0)$. When $y = \pm 1$, we have $x = 0$ which gives us $(0, 1)$. When $y = \pm 3$, $9 = x^3 + 1$, which has one real solution $x = 2$.

These are all the points we already had and there are no more values of y such that $y^2 | -27$. Thus, we have tested all possible y coordinates of rational points on the curve of finite order, so this tells us by the Nagell-Lutz theorem that $P = (2, 3)$, $2P = (0, 1)$, $3P = (-1, 0)$, $4P = (0, -1)$, $5P = (2, -3)$, and $6P = \mathcal{O}$ are the *only* points of finite order on this curve. Therefore the torsion subgroup of the Mordell-Weil group of this curve is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

Although we have successfully nailed down the torsion subgroup of this curve, we still don't know the complete Mordell-Weil group because we do not yet have the tools to understand the points of infinite order.

Example 2.14. As another application of the Nagell-Lutz theorem, consider the elliptic curve E defined by $y^2 = x^3 - 2$. We can see that $P = (3, 5)$ is a point on the curve. If we compute $2P$, we will see that $2P = \left(\frac{129}{100}, \frac{-383}{1000}\right)$, which does not have integer coefficients so P is of infinite order.

Alternatively, we could have computed $\Delta = -108$ so since $5 \neq 0$ and $5^2 \nmid -108$, this also shows P has infinite order.

In particular, the fact that we have shown that there exists a point of infinite order in $E(\mathbb{Q})$ tells us that the rank of E, $R_{E(\mathbb{Q})} \neq 0$, so $R_{E(\mathbb{Q})} \geq 1$, so in particular, $E(\mathbb{Q})$ is infinite.

[5]The discriminant of $f(x) = (x - e_1)(x - e_2)(x - e_3)$ is $\Delta = ((e_1 - e_2)(e_1 - e_3)(e_2 - e_3))^2$. In the case that f is of the form $x^3 + Ax + B$ for integers A, B, it can be shown that $\Delta = -4A^3 - 27B^2$. In particular this makes it clear that $\Delta \in \mathbb{Z}$ when f is of the form $x^3 + Ax + B$

Curve	Torsion	Generators
$y^2 = x^3 - 2$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$(2, 0), (0, 0)$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$(3, 6), (0, 0)$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$(-3, 18), (2, -2)$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$(30, -90), (-40, 400)$

TABLE 1. Table taken from [LR]

There is another very useful theorem about the torsion subgroup proven by Mazur which says that there are only 15 particular groups which will ever arise as the torsion subgroup of the Mordell-Weil group of an elliptic curve.

Theorem 2.15 (Mazur)**.** *The torsion subgroup of the Mordell-Weil group of an elliptic curve is isomorphic to one of the following:*

(1) $\mathbb{Z}/N\mathbb{Z}$ *for* $1 \leq N \leq 10$ *or* $N = 12$,
(2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *for* $1 \leq N \leq 4$.

Corollary 2.16. *For* $P \in E(\mathbb{Q})$*, if* $mP \neq \mathcal{O}$ *for* $1 \leq m \leq 12$*, then* P *has infinite order. This is because all points of finite order must be of order no more than* 12*.*

Furthermore, all of these groups do actually arise as the torsion part of the Mordell-Weil group of some elliptic curve. Table 1, taken from [LR], gives examples of elliptic curves which have each of the possible torsion subgroups.

The rest of the Mordell-Weil group is considerably less understood than the torsion part. In fact, given an arbitrary elliptic curve, there is no known algorithm to even tell us the rank of the curve. There are algorithms which work for some curves. (For a more extensive discussion of this see [LR]). There are also various ways to bound the rank of an arbitrary elliptic curve.

Furthermore, it has been conjectured that there exist elliptic curves of arbitrarily high rank and yet the curve of the highest rank anyone has ever found, discovered by Noam Elkies in 2006, could have rank as low as 28. It has been shown that the rank of this curve

is at least 28 and no elliptic curve has ever been found whose rank can be proven to be greater than this. A table of elliptic curve rank records can be found at [Duj].

To find a lower bound on the rank, consider a curve E. If we have n points on E which we can show to be linearly independent[6], then $R_{E(K)} \geq n$. Linear independence of points on elliptic curves can be shown using the Néron-Tate pairing, which will not be discussed here. Instead, we refer the reader to [LR] for a discussion of the Néron-Tate pairing and showing linear independence of points.

This paper focuses on proving an upper bound on the rank of elliptic curves. It is shown first in specific cases and finally in Section 5, it is shown for an arbitrary elliptic curve.

3. A Restricted Case

Our goal is ultimately to prove an upper bound on the rank of elliptic curves defined over $\mathbb{Q}$. However, for the sake of simplicity and intuition, we begin with a restriction on the set of curves we consider. Let E be an elliptic curve defined by the Weierstrass equation $y^2 = f(x)$ where $f(x) = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$. Let K denote the splitting field of $f(x)$ over $\mathbb{Q}$ and let $h(K)$ denote the class number of K. We denote the ring of integers of K by $\mathcal{O}_K$. The case we would like to consider in this section is the case in which $h(K) = 1$. This condition gives us unique prime factorization in $\mathcal{O}_K$, or equivalently[7], it gives us that $\mathcal{O}_K$ is a principal ideal domain. This will provide us with the necessary tools for a sleek intuitive proof of this bound.

The reader should note that what is presented in this section is only a slight modification of what is shown in Section 2.8 of [LR], where the same bound is proven in the case where $K = \mathbb{Q}$. However, generalizing to the case where $K \neq \mathbb{Q}$ necessarily, but still assuming $h(K) = 1$ does not change very much. The key property of K being used in [LR] is that $\mathcal{O}_K$ has unique prime factorization, which is true for any number field K of class number one.

The method for proving this bound begins by considering a certain homomorphism, δ defined out of $E(K)$, the set of points in K^2 which satisfy the equation defining the curve. This homomorphism will induce an injection from $E(K)/\ker(\delta)$ into image(δ) so if we can show that the size of image(δ) is finite, then we can use this injection to bound the size of $E(K)/\ker(\delta)$ by the size of image(δ), which we will then use to bound the size of the rank of $E(K)$.

Theorem 3.1. *Let E be an elliptic curve defined by the Weierstrass equation $y^2 = f(x)$ where $f(x) = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$ with distinct roots e_1, e_2, e_3. Let $K = \mathbb{Q}[e_1, e_2, e_3]$ be the splitting field of $f(x)$.*

Let $P = (x_0, y_0) \in E(K)$. We define a map $\delta : E(K) \to (K^\times/(K^\times)^2)^3$ by

[6]A set of points $\{P_1, P_2, ..., P_n \in E(\mathbb{Q})\}$ are linearly independent over $\mathbb{Z}$ if $m_1P_1 + m_2P_2 + ... + m_nP_n \neq 0$ for any $m_1, m_2, ..., m_n \in \mathbb{Z}$.

[7]These conditions are equivalent because $\mathcal{O}_K$ is a Dedekind domain.

$$\delta(P) = \begin{cases} (1,1,1) & \text{if } P = \mathcal{O}, \\ (x_0 - e_1, x_0 - e_2, x_0 - e_3) & \text{if } y_0 \neq 0, \\ ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) & \text{if } P = (e_1, 0), \\ (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) & \text{if } P = (e_2, 0), \\ (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)) & \text{if } P = (e_3, 0). \end{cases}$$

Then δ is a homomorphism with $\ker(\delta) = 2E(K)$

Remark 3.2. Note that $x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$, so comparing x^2 terms, $e_1 + e_2 + e_3 = 0$.

Remark 3.3. Note that if $\delta(P) = (\delta_1, \delta_2, \delta_3)$, then $\delta_1\delta_2\delta_3 = 1$ in $K^\times/(K^\times)^2$ so image(δ) can be embedded into $(K^\times/(K^\times)^2)^2$.

Proof. Most of this proof is taken from [LR] with the slight modification that K is not necessarily equal to $\mathbb{Q}$, but still assuming $h(K) = 1$.

First, we show that δ is a homomorphism. Let $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ be points on $E(K)$. Note that $\delta(x_0, y_0) = \delta(P) = \delta(-P) = \delta(x_0, -y_0)$ because δ does not depend on the sign of y. So to show $\delta(P)\delta(Q) = \delta(P+Q)$ is the same as to show $\delta(P)\delta(Q) = \delta(-(P+Q))$.

Let $R = -(P + Q) = (x_2, y_2)$. First we assume $y_i \neq 0$ for $i = 1, 2, 3$. The points P,Q, and R are collinear, so let $L = \overline{PQ}$ be the line connecting the three points and suppose it has the equation $y = ax + b$. Substituting y into the equation for the curve, we obtain a polynomial,

$$p(x) = (ax + b)^2 - (x - e_1)(x - e_2)(x - e_3).$$

The roots of $p(x)$ are exactly the x-coordinates of P, Q, and R, namely, x_0, x_1, and x_2. Hence $p(x)$ factors as

$$p(x) = (ax + b)^2 - (x - e_1)(x - e_2)(x - e_3) = (x_0 - x)(x_1 - x)(x_2 - x)$$

Evaluating $p(x)$ at e_i, we obtain,

$$p(e_i) = (ae_i + b)^2 = (x_0 - e_i)(x_1 - e_i)(x_2 - e_i).$$

Thus,

$$\begin{aligned} &\delta(P)\delta(Q)\delta(R) \\ &= (x_0 - e_1, x_0 - e_2, x_0 - e_3) \times (x_1 - e_1, x_1 - e_2, x_1 - e_3) \times (x_2 - e_1, x_2 - e_2, x_2 - e_3) \\ &= ((x_0 - e_1)(x_1 - e_1)(x_2 - e_1), (x_0 - e_2)(x_1 - e_2)(x_2 - e_2), (x_0 - e_3)(x_1 - e_3)(x_2 - e_3)) \\ &= ((ae_1 + b)^2, (ae_2 + b)^2, (ae_3 + b)^2) \\ &= (1, 1, 1) \in K^\times/(K^\times)^2 \end{aligned}$$

Thus $\delta(P)\delta(Q)\delta(R) = 1$ in $K^\times/(K^\times)^2$. Multiplying both sides by $\delta(R)$, we obtain $\delta(P) \times \delta(Q) = \delta(R)$, i.e. $\delta(P) \times \delta(Q) = \delta(-(P + Q)$, which completes the proof that δ is a homomorphism in the case when $y_i \neq 0$ for $i = 1, 2, 3$.

There are three more cases to consider. Either $y_i = 0$ for exactly one of $i = 1, 2$, or 3 or $y_i = 0$ for $i = 1, 2$ and 3, or one of the points is $\mathcal{O}$.

Next we consider the case when $y_i = 0$ for exactly one of $i = 1, 2$, or 3. Recall that we need to show $\delta(P)\delta(Q)\delta(R) = 1$ in $K^\times/(K^\times)^2$. Without loss of generality suppose that $y_0 = 0$. Then $x_0 = e_i$ for some $i = 1, 2, 3$. Without loss of generality, let $x_0 = e_1$. So $P = (x_0, y_0) = (e_1, 0)$. Then one can check that the line connecting P, Q, and R is $y = \left(\frac{y_1}{x_1 - e_1}\right)(e_1 - x)$. Substituting this into our equation of the curve as in the previous case, we obtain a polynomial,

$$p(x) = \left(\frac{y_1}{x_1 - e_1}\right)^2 (e_1 - x)^2 - (x - e_1)(x - e_2)(x - e_3).$$

Again, the roots of $p(x)$ are exactly the x-coordinates of P,Q, and R, namely, $x_0 = e_1$,x_1, and x_2. Hence $p(x)$ factors as

$$p(x) = \left(\frac{y_1}{x_1 - e_1}\right)^2 (e_1 - x)^2 - (x - e_1)(x - e_2)(x - e_3) = (e_1 - x)(x_1 - x)(x_2 - x).$$

Dividing by $(e_1 - x)$, we obtain

$$\left(\frac{y_1}{x_1 - e_1}\right)^2 (e_1 - x) + (x - e_2)(x - e_3) = (x_1 - x)(x_2 - x).$$

Then evaluating at $x = e_1$,

$$(e_1 - e_2)(e_1 - e_3) = (x_1 - e_1)(x_2 - e_1).$$

Thus,

$$\begin{aligned}
&\delta(P)\delta(Q)\delta(R) \\
&= ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) \times (x_1 - e_1, x_1 - e_2, x_1 - e_3) \times (x_2 - e_1, x_2 - e_2, x_2 - e_3) \\
&= ((e_1 - e_2)(e_1 - e_3)(x_1 - e_1)(x_2 - e_1), (x_0 - e_2)(x_1 - e_2)(x_2 - e_2), (x_0 - e_3)(x_1 - e_3)(x_2 - e_3)) \\
&= (((e_1 - e_2)(e_1 - e_3))^2, (ae_2 + b)^2, (ae_3 + b)^2) \\
&= (1, 1, 1) \in K^\times/(K^\times)^2
\end{aligned}$$

which completes this case.

Next consider when $y_i = 0$ for $i = 1$, 2, and 3. Then without loss of generality, $x_0 = e_1$, $x_1 = e_2$, $x_2 = e_3$ and again, we wish to show $\delta(P)\delta(Q)\delta(R) = 1$ in $K^\times/(K^\times)^2$. Then,

$$\begin{aligned}\delta(P)\delta(Q)\delta(R) &= ((e_1-e_2)(e_1-e_3), e_1-e_2, e_1-e_3)\\ &\quad\times(e_2-e_1,(e_2-e_1)(e_2-e_3),e_2-e_3)\\ &\quad\times(e_3-e_1,e_3-e_2,(e_3-e_1)(e_3-e_2))\\ &= (((e_1-e_2)(e_1-e_3))^2,((e_2-e_1)(e_2-e_2))^2,((e_3-e_1)(e_3-e_2))^2)\\ &= (1,1,1)\in K^\times/(K^\times)^2.\end{aligned}$$

Next, we consider the case when one of these points is $\mathcal{O}$. Let $P=\mathcal{O}$ without loss of generality. Then the line connecting Q and R is vertical, so if $x_1=x_2$ and $y_1=-y_2$. Then,

$$\begin{aligned}\delta(P)\delta(Q)\delta(R) &= (1,1,1)\times(x_1-e_1,x_1-e_2,x_1-e_3)\times(x_2-e_1,x_2-e_2,x_2-e_3)\\ &= ((x_1-e_1)(x_2-e_1),(x_1-e_2)(x_2-e_2),(x_1-e_3)(x_2-e_3))\\ &= ((x_1-e_1)^2,(x_1-e_2)^2,(x_1-e_3)^2)\\ &= (1,1,1)\in K^\times/(K^\times)^2.\end{aligned}$$

which completes the proof that δ is a homomorphism.

Next, we show that $\ker(\delta)=2E(K)$. It is clear that $2E(K)\subseteq\ker(\delta)$ since δ is a homomorphism; $\delta(2P)=(\delta(P))^2=1$. Next we need to show the reverse containment.

Let $Q=(x_1,y_1)\in\ker(\delta)$. Then $Q\in E(K)$ such that $\delta(Q)=(1,1,1)$ in $K^\times/(K^\times)^2$. We need to show there exists some $P=(x_0,y_0)\in E(K)$ such that $Q=2P$. It is enough to show that $x_0=x_1$ since then $Q=\pm P$.

Working out the arithmetic of adding two points on the curve, we obtain a duplication formula for x-coordinate of elliptic curves. This is taken from [LR], Exercise 2.11.16. Denoting the x-coordinate of a point $P\in E(K)$ by $x(P)$, the duplication formula says that $x(Q)=x(2P)$ when

$$x_1=x(2P)=\frac{x_0^4-2Ax_0^2-8Bx_0+A^2}{4y_0^2}.$$

Here, we only show the case in which $y_1\neq 0$. The remaining cases are left to the reader. Then $\delta(Q)=(1,1,1)$ in $K^\times/(K^\times)^2$ implies that x_0-e_i is a square for $i=1,2,3$. Let $x_0-e_i=t_i^2$ for some $t_i\in K^\times$.

Define $p(x)\in K[x]$ by

$$t_1\frac{(x-e_2)(x-e_3)}{(e_1-e_2)(e_1-e_3)}+t_2\frac{(x-e_1)(x-e_3)}{(e_2-e_1)(e_2-e_3)}+t_3\frac{(x-e_1)(x-e_2)}{(e_3-e_1)(e_3-e_2)}.$$

This polynomial is designed so that $p(e_i)=t_i$. Notice that $p(x)$ is a quadratic, so let $p(x)=a+bx+cx^2$. Define $q(x)=x_1-x-p(x)^2$. Then

$$q(e_i)=x_1-e_i-t_i^2=0$$

for $i = 1, 2, 3$. Thus $(x - e_i)$ divides $q(x)$ for each of these i. Thus $(x - e_1)(x - e_2)(x - e_3) = x^3 + Ax + B = f(x)$ divides $q(x)$. In other words, $q(x) \equiv 0$ modulo $f(x)$. Thus $x_1 - x \equiv p(x)^2 \equiv (a + bx + cx^2) \bmod f(x)$. If we expand the right hand side, we get that $x_1 - x \equiv c^2x^4 + 2bcx^3 + (2ac + b^2)x^2 + 2abx + a^2$.

Next notice that $x^3 \equiv -Ax - B$ and $x^4 \equiv -Ax^2 - Bx$. Then, substituting this and recollecting terms, we get $x - x_1 \equiv (2ac + b^2 - Ac^2)x^2 + (2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB) \bmod f(x)$. Thus $x - x_1 - ((2ac + b^2 - Ac^2)x^2 + (2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB)) \equiv 0 \bmod f(x)$. Thus $f(x)$ divides $x - x_1 - ((2ac + b^2 - Ac^2)x^2 + (2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB))$, which is a polynomial of degree at most two. Since $f(x)$ is of degree three, this means $x - x_1 - ((2ac + b^2 - Ac^2)x^2 + (2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB)) = 0$, or equivalently, $x - x_1 = ((2ac + b^2 - Ac^2)x^2 + (2ab - Bc^2 - 2Abc)x + (a^2 - 2bcB))$. Matching coefficients, we see that

$$2ac + b^2 - Ac^2 = 0 \tag{1}$$

$$2ab - Bc^2 - 2Abc = -1 \tag{2}$$

$$a^2 - 2bcB = x_1. \tag{3}$$

If $c = 0$, then $b = 0$ by equation (1). Then $p(x) = a$ is constant so $t_1 = t_2 = t_3$. Since $t_i^2 = x_1 - e_i$ by definition, it follows that $e_1 = e_2 = e_3$, which would make the curve singular and is thus a contradiction. Thus $c \neq 0$. Multiplying equation (2) by $\frac{1}{c^2}$ and equation (1) by $\frac{b}{c^3}$, we get

$$\frac{2ab}{c^2} - B - \frac{2Ab}{c} = \frac{-1}{c^2} \tag{4}$$

$$\frac{2ab}{c^2} + \frac{b^3}{c^3} - \frac{Ab}{c} = 0 \tag{5}$$

Subtracting equation (4) from equation (5), we get

$$\left(\frac{b}{c}\right)^3 + A\left(\frac{b}{c}\right) + B = \left(\frac{1}{c}\right)^2. \tag{6}$$

Thus the point $P = (x_0, y_0) = \left(\frac{b}{c}, \frac{1}{c}\right)$ is on the curve. Since $p(x) \in K[x]$, $a, b, c \in K$, so $P \in E(K)$.

From equation (5), we can deduce that $a = \frac{A - x_0^2}{2y_0}$. Substituting this into equation (3), we get

$$\begin{aligned} x(Q) = x_1 &= \left(\frac{A - x_0^2}{2y_0}\right)^2 - 2bcB \\ &= \frac{(A^2 - 2Ax_0^2 + x_0^4) - (2bcB)(4y_0^2)}{4y_0^2} \\ &= \frac{(A^2 - 2Ax_0^2 + x_0^4) - (2bcB)(\frac{4}{c^2})}{4y_0^2} \\ &= \frac{(A^2 - 2Ax_0^2 + x_0^4) - 8Bx_0}{4y_0^2} \\ &= \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4y_0^2} = x(2P) \end{aligned}$$

The case in which $y_1 = 0$ is left to the reader. □

Corollary 3.4. *δ induces an injection,*

$$E(K)/2E(K) \hookrightarrow (K^\times/(K^\times)^2)^2$$

Proof. This follows from Theorem 3.1 together with the remark that image(δ) can be embedded into $(K^\times/(K^\times)^2)^2$. □

Our goal is to show that image(δ) can be embedded into something finite in order to bound the rank. $(K^\times/(K^\times)^2)^2$ is not finite, so we are not quite done. However, the image of δ is in fact much smaller than $(K^\times/(K^\times)^2)^2$. The next proposition shows that the only primes in $K^\times$ which can divide the square-free parts of the elements of the image of δ are those dividing the discriminant of the curve. (See Examples 2.8.2 and 2.8.4 in [LR] for an example of this). Thus showing image(δ) is in fact finite.

Proposition 3.5. *Let E be the elliptic curve defined over $\mathbb{Q}$ by $y^2 = f(x)$ where K is the splitting field of $f(x)$ and let $e_1, e_2, e_3 \in K$ be the roots of $f(x)$ as before. Suppose $h(K) = 1$. Let $P = (x_0, y_0) \in E(\mathbb{Q})$ and let*

$$(x_0 - e_1) = au^2$$
$$(x_0 - e_2) = bv^2$$
$$(x_0 - e_3) = cw^2$$

where $u, v, w \in K^\times$ and where $a, b, c \in \mathcal{O}_K$ are square-free. Then if $p|abc$ then $p|\Delta$ where $\Delta = (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$ and where p is a prime element of $\mathcal{O}_K$

Remark 3.6. It only makes sense to take a, b, c to be square-free because $h(K) = 1$ so $\mathcal{O}_K$ has unique prime factorization. Without unique prime factorization, the notion of a "square-free" element of $\mathcal{O}_K$ becomes unclear. This will be addressed in Section 4

Remark 3.7. Note that abc is a square in $\mathcal{O}_K$ since $(x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = y_0^2$ so $abc(uvw)^2 = y_0^2$

Remark 3.8. Also note that $\Delta \in \mathcal{O}_K$ because $e_i \in \mathcal{O}_K$ for each i.

A similar proposition is proven on pages 55-56 of [LR] as Proposition 2.8.5. Here, $K = \mathbb{Q}$, but a similar argument shows that this proposition holds for any K so long as $h(K) = 1$. The key property used in this proof is that $\mathcal{O}_K$ has unique factorization when $K = \mathbb{Q}$, but this is true of any K such that $h(K) = 1$.

We are now fully equipped to show that image(δ) can be embedded into something finite.

Corollary 3.9. *Let r_1 be the number of real embedings of K into $\mathbb{C}$ and let r_2 be the number of pairs of non-real embedings of K into $\mathbb{C}$. Let $\{p_i\}_{1 \le i \le n}$ be the set of primes in $\mathcal{O}_K$ dividing Δ and let $\{u_i\}_{0 \le i \le r_1+r_2-1}$ be a set of generators of the unit group, ${\mathcal{O}_K}^\times$. Let $\Gamma = \{u_0^{a_0}...u_{r_1+r_2-1}^{a_{r_1+r_2-1}} p_1^{t_1}...p_n^{t_n} : a_i, t_i \in \mathbb{Z}/2\mathbb{Z}\}$. Then δ induces an injection*

$$E(K)/2E(K) \hookrightarrow \Gamma^2$$

Proof. Any unit $u \in {\mathcal{O}_K}^\times$ is of the form $u_0^{a_0}...u_{r_1+r_2-1}^{a_{r_1+r_2-1}}$ by Dirichlet's Unit Theorem. The rest is a result of the previous proposition and corollary 3.4. □

Corollary 3.9 is very useful, because now we know that the size of $E(K)/2E(K)$ is at most the size of Γ^2, which is finite. Next, an examination of the structure of $E(K)/2E(K)$ will allow us to bound the rank.

The Mordell-Weil theorem states that $E(K)$ is a finitely generated abelian group, so by the fundamental theorem of finitely generated abelian groups,

$$E(K) \cong T \times \mathbb{Z}^{R_E(K)}$$

where T is the torsion subgroup (i.e. T is a finite group).

So what is the structure of $E(K)/(2E(K))$? We know that $(e_1, 0), (e_2, 0), (e_3, 0) \in E(K)$ by the definition of K being the splitting field of $f(x)$, and any point of this form is of order exactly 2 (one can easily check this from the definition of addition), which means that T must have exactly 3 points of order 2. Thus T is not cyclic, so by Mazur's theorem,

$$T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2M\mathbb{Z} \quad \text{for } M = 1, 2, 3, \text{ or } 4.$$

Therefore T has two generators, both of which are of even order. When we take $T/2T$, all even multiples of these generators become $\mathcal{O}$ and all odd multiples of these generators are now in a single class. So ultimately, we are left with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

To understand what happens to the free part after taking this quotient, again look at the generators. There are $R_{E(K)}$ generators of the free part. Again, the even multiples of each of them become $\mathcal{O}$ and the odd multiples are now in a single class. So the free part becomes $(\mathbb{Z}/2\mathbb{Z})^{R_{E(K)}}$.

So overall, $E(K)/2E(K) \cong (\mathbb{Z}/2\mathbb{Z})^{2+R_{E(K)}}$. Therefore, $|E(K)/2E(K)| = 2^{(2+R_{E(K)})}$. We are now ready to prove our bound.

Theorem 3.10. *Let E be an elliptic curve defined by the Weierstrass equation $y^2 = f(x) = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$. Let K be the splitting field of $f(x)$ and let $e_1, e_2, e_3 \in K$ be the roots of $f(x)$ as before. Assume that $h(K) = 1$. Let $\nu(\Delta)$ be the number of primes in $\mathcal{O}_K$ dividing Δ and let r_1 be the number of real embeddings of K into $\mathbb{C}$ and let r_2 be the number of pairs of non-real embeddings of K into $\mathbb{C}$ as in Corollary 3.9. Then,*

$$R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) - 1)$$

Proof. Counting elements of Γ, we can see that

$$|\Gamma| = 2^{r_1 + r_2 + \nu(\Delta)}.$$

So since $E(K)/2E(K) \hookrightarrow \Gamma^2$ by Corollary 3.9, $|E(K)/2E(K)| \leq |\Gamma^2|$, which means

$$\begin{aligned} 2^{(2+R_{E(K)})} &\leq 2^{2(r_1+r_2+\nu(\Delta))} \\ \implies 2 + R_{E(K)} &\leq 2(r_1 + r_2 + \nu(\Delta)) \\ \implies R_{E(K)} &\leq 2(r_1 + r_2 + \nu(\Delta) - 1) \end{aligned}$$

proving the bound.

□

4. Odd Class Number and Canonical Factorization

Next, we generalize to the case when $h(K)$ is only assumed to be odd. The proof of the bound in this case is similar to the previous case. However, Proposition 3.5 relied on unique factorization and we can no longer assume that $\mathcal{O}_K$ has unique prime factorization, so in this section we introduce the concept of a "canonical factorization"[8] of elements in $\mathcal{O}_K$ raised to the power of the class number, which leads to a sort of generalization of the notion of square-free parts of elements as far as we are concerned with this notion.

Example 4.1. let $K = \mathbb{Q}[\sqrt{79}]$. Then $h(K) = 3$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{79}]$. In $\mathcal{O}_K$, 45 can be factored into the product of irreducible elements in two ways.

$$45 = 3^2 \times 5$$

$$45 = 3 \times (\sqrt{79} + 8) \times (\sqrt{79} - 8)$$

One can check that $3, 5, (\sqrt{79}+8)$, and $(\sqrt{79}+8)$ are all irreducible. If we only saw the second factorization, we might be naively tempted to say that 45 is "square-free" because it is the product of distinct irreducibles, but the first factorization tells us that there is indeed a square dividing 45.

[8]This is not standard terminology.

A natural question to consider is what this notion of "square-free" actually *means* when we cannot assume unique factorization. One might be tempted to try the quick-fix of defining an element to be square-free when there does not exist an irreducible element whose square divides it, but perhaps even more troublesome is the notion of the square-free part of an element. Consider the following example.

Example 4.2. Consider the element $\alpha = 360+45\sqrt{79} \in \mathcal{O}_K$. Using this quick-fix definition of square-free, what is the square-free part of α? Notice that $\alpha = 45 \times (\sqrt{79}+8)$, so from our previous two factorizations of 45, we obtain two factorizations of α.

$$\alpha = 3^2 \times 5 \times (\sqrt{79}+8)$$

$$\alpha = 3 \times (\sqrt{79}+8)^2 \times (\sqrt{79}-8).$$

The first factorization suggests that $5 \times (\sqrt{79}+8)$ is the square-free part and the second factorization suggests that $3 \times (\sqrt{79}-8)$ is the square-free part and indeed both of these satisfy the quick-fix definition of square-free and divide α.

This example tells us we still have ambiguity in the notion of square-free parts of elements when the class number is higher than one. For this reason, we will need something more.

The reader should check that if we define a map[9] from $K^\times$ into $K^\times/(K^\times)^2$ in the natural way, this map is well-defined for arbitrary K. So it does make sense to consider $K^\times/(K^\times)^2$ regardless of whether or not we have unique factorization. The trouble arises in deterministically choosing a representative of $K^\times/(K^\times)^2$ for class number higher than one.

When $h(K) = 1$ and we take the square-free part of an element $a \in \mathcal{O}_K$, what we are doing is pinning down a unique[10] representative of the class of a in $K^\times/(K^\times)^2$ in a deterministic fashion. The reason our previous attempt at generalizing the notion of square-free parts failed is because it failed to pin down a unique representative of the equivalence class of α in $K^\times/(K^\times)^2$. Thus, our goal will be to devise a way to choose a unique representative of a given equivalence class in $K^\times/(K^\times)^2$.

Coming back to our failed quick-fix generalization of the notion of square-free parts, notice that if we had a deterministic way to choose one factorization of an element rather than another, then perhaps this quick-fix idea could be salvaged into an idea which successfully pins down a unique representative of a given equivalence class in $K^\times/(K^\times)^2$. This is the role that canonical factorization plays.

Let $a \in K^\times$ and let $(a) = \wp_1^{e_1}...\wp_n^{e_n}$ be the factorization of (a) into prime ideals where $e_i \in \mathbb{Z}$ for $1 \leq i \leq n$. Raising this equation to the power of $h(K)$, we obtain

[9]Note that $K^\times/(K^\times)^2$ is the set of equivalence classes in $K^\times$ where $\alpha, \beta \in K^\times$ are equivalent when there is some $\gamma \in K^\times$ such that $\alpha = \beta\gamma^2$

[10]When we say the representative is unique, we mean it is unique up to multiplication by units

$$\begin{aligned}
&(a)^{h(K)} = (\wp_1^{e_1}...\wp_n^{e_n})^{h(K)} \\
\implies &(a^{h(K)}) = {\wp_1}^{e_1 h(K)}...{\wp_n}^{e_n h(K)} \\
\implies &(a^{h(K)}) = ({\wp_1}^{h(K)})^{e_1}...({\wp_n}^{h(K)})^{e_n}
\end{aligned}$$

Note that ${\wp_i}^{h(K)}$ must be principal for each i since $h(K)$ is the order of the ideal class group and any element of a group raised to the order of that group is the identity. Let ${\wp_i}^{m_i} = (p_i)$ where m_i is the order of $\wp_i$ in the class group. Then note that p_i is an irreducible element of $\mathcal{O}_K$ because if $p_i = ab$ then ${\wp_i}^{m_i} = (a)(b)$ so (a) and (b) are both powers of $\wp_i$, but ${\wp_i}^{m_i}$ is the smallest power of $\wp_i$ that is principal. Therefore, one of a or b must be ${\wp_i}^{m_i}$ and the other must be a unit. Thus, p_i is irreducible. Suppose $h(K) = m_i k_i$. (Recall $m_i | h(K)$ since m_i is the order of p_i in $Cl(K)$.) Then,

$$\begin{aligned}
&(a^{h(K)}) = ({\wp_1}^{h(K)})^{e_1}...({\wp_n}^{h(K)})^{e_n} \\
\implies &(a^{h(K)}) = (p_1)^{k_1 e_1}...(p_n)^{k_n e_n} \\
\implies &(a^{h(K)}) = (p_1^{k_1 e_1})...(p_n^{k_n e_n}) \\
\implies &a^{h(K)} = u p_1^{k_1 e_1}...p_n^{k_n e_n} \quad \text{for some } u \in {\mathcal{O}_K}^\times
\end{aligned}$$

Since p_i is irreducible for each i, this is a factorization of $a^{h(K)}$ into irreducibles. Also notice that the choices of p_i are unique up to multiplication by units in $\mathcal{O}_K$.

Definition 4.3. We define the factorization above, $a^{h(K)} = u p_1^{k_1 e_1}...p_n^{k_n e_n}$ to be the canonical factorization of $a^{h(K)}$ in ${K^\times}$ into irreducibles.

Note that $a^{h(K)} \equiv a$ in ${K^\times}/({K^\times})^2$ because $h(K)$ is odd. Similarly, for $a \in {K^\times}$ a representative of $\bar{a} \in {K^\times}/({K^\times})^2$, we define the canonical factorization of a in ${K^\times}/({K^\times})^2$ into irreducibles to be $a \equiv u p_1^{k_1 e_1}...p_n^{k_n e_n}$ where $u \in {\mathcal{O}_K}^\times$ and where $k_i e_i \in \mathbb{Z}/2\mathbb{Z}$.

It is very important that the canonical factorization of $a^{h(K)}$ stems directly from the factorization of (a) as an *ideal* because factorization of ideals is unique so the canonical factorization of a given element in ${K^\times}/({K^\times})^2$ is completely determined by that element, thus giving us a deterministic way to choose one particular factorization of $a^{h(K)}$ up to multiplication by units.

Next, we wish to define a generalization of the notion of the square-free part of an element. Since we will ultimately be working in ${K^\times}/({K^\times})^2$, it makes sense to define the square-free part of an element $a \in \mathcal{O}_K$ to be an element $b \in \mathcal{O}_K$ such that $\bar{a} = \bar{b}$ in ${K^\times}/({K^\times})^2$ which is invariant under our choice of representative of $\bar{a}$ in ${K^\times}/({K^\times})^2$. More explicitly, if $\bar{a_1} = \bar{a_2}$ in ${K^\times}/({K^\times})^2$, then the square-free part of a_1 should be equal to the square-free part of a_2, and we want that $\bar{a_1} = \bar{a_2} = \bar{b}$ where b is the square-free part of a_1 (and thus also of a_2).

Definition 4.4. Let $K^\times$ be a number field such that $h(K)$ is odd and let $a \in \mathcal{O}_K$. Let $a^{h(K)} = up_1^{k_1 e_1}...p_n^{k_n e_n}$ be the canonical factorization of $a^{h(K)}$ in $K^\times$. We will denote the square-free part of a as $s(a)$. Then we define the square free part of a in $K^\times$ to be

$$s(a) = u \prod_{odd\ e_i} p_i.$$

where the p_i are the irreducibles appearing in the canonical factorization of $a^{h(K)}$.

Remark 4.5. Notice that $s(a) \equiv a$ in $K^\times/(K^\times)^2$. This is because $a^{h(K)}$ is a square times $s(a)$ by the definition of $s(a)$ and $a^{h(K)} \equiv a$ in $K^\times/(K^\times)^2$ since $h(K)$ is odd.

Proposition 4.6. *If $a_1, a_2 \in \mathcal{O}_K$ and $a_1 \equiv a_2$ in $K^\times/(K^\times)^2$, then $s(a_1) = u^2 s(a_2)$ for some $u \in \mathcal{O}_K^\times$ and conversely.*

Proof. Suppose $a_1, a_2 \in \mathcal{O}_K$ and $a_1 \equiv a_2$ in $K^\times/(K^\times)^2$. Let $(a_1) = \wp_1{}^{E_1}...\wp_l{}^{E_l}$ and let $(a_2) = \wp_1{}^{E_1}...\wp_l{}^{E_l}\wp_{l+1}{}^{E_{l+1}}...\wp_n{}^{E_n}$ where $\wp_i$ are prime ideals for $1 \le i \le n$, where $E_i \in \mathbb{Z}$ for $1 \le i \le n$, and where E_i is even for $l+1 \le i \le n$.

Letting $h(K) = k_i m_i$ where m_i is the order of $\wp_i$ in the class group, and letting $(p_i) = \wp_i^{m_i}$, we have that

$$(a_1)^{h(K)} = (p_1)^{k_1 E_1}...(p_l)^{k_l E_l} \quad \text{and}$$

$$(a_2)^{h(K)} = (p_1)^{k_1 E_1}...(p_l)^{k_l E_l}(p_{l+1})^{k_{l+1} E_{l+1}}...(p_n)^{k_n E_n}.$$

Therefore,

$$a_1^{h(K)} = u_1 {p_1}^{k_1 E_1}...{p_l}^{k_l E_l} \quad \text{and}$$

$$a_2^{h(K)} = u_2 {p_1}^{k_1 E_1}...{p_l}^{k_l E_l}{p_{l+1}}^{k_{l+1} E_{l+1}}...{p_n}^{k_n E_n}$$

for units $u_1, u_2 \in \mathcal{O}_K^\times$. Then by definition, we have

$$s(a_1) = u_1 \prod_{\text{odd } E_i \text{ for } 1 \le i \le l} p_i \quad \text{and}$$

$$s(a_2) = u_2 \prod_{\text{odd } E_i \text{ for } 1 \le i \le n} p_i.$$

(Recall that $h(K)$ is odd, so k_i is odd and thus $k_i E_i$ is odd exactly when E_i is odd). Since E_i is even for $l+1 \le i \le n$, all we have left to show is that $u_1 u_2^{-1}$ is a square. Then $s(a_1) = u_1 u_2^{-1} s(a_2)$ by the previous equations, so we will be done with this direction. By remark 4.5, $s(a_1) \equiv a_1$ in $K^\times/(K^\times)^2$ and $s(a_2) \equiv a_2$ in $K^\times/(K^\times)^2$, so since $a_1 \equiv a_2$, $s(a_1) \equiv s(a_2)$ in $K^\times/(K^\times)^2$, which proves that $u_1 u_2^{-1}$ is a square.

Next suppose $s(a_1) = u^2 s(a_2)$ for some $u \in \mathcal{O}_K$. Then $s(a_1) \equiv s(a_2)$ in $K^\times/(K^\times)^2$, so since $s(a_1) \equiv a_1$ and $s(a_2) \equiv a_2$, we have $a_1 \equiv a_2$.

□

This proposition tells us that choosing the square-free part of an element via our definition uniquely determines an equivalence class in $K^\times/(K^\times)^2$ and all elements of an equivalence class in $K^\times/(K^\times)^2$ share the same square-free part up to multiplication by square units.

Note that the definition we decided on is slightly different than what we might expect as given an element $a \in \mathcal{O}_K$, the square-free part of a does not necessarily divide a; we know that $s(a)|a^{h(K)}$, but this does not imply that $s(a)|a$. This will be evident in the next example. Although we can't say that the square-free part of a divides a, as mentioned in remark 4.5, they are congruent in $K^\times/(K^\times)^2$, which is all we really need.

Example 4.7. Coming back to our previous example of $\alpha = 360 + 45\sqrt{79} \in \mathcal{O}_K$ where $K = \mathbb{Q}[\sqrt{79}]$, what is the canonical factorization of $\alpha^{h(K)}$ and what is the square-free part of α determined by this factorization?

First, we take the factorization of (α) into prime ideals.

$$(360 + 45\sqrt{79}) = (3, 1 + \sqrt{79})^2 \times (3, -1 + \sqrt{79})^3 \times (5, 2 + \sqrt{79}) \times (5, -2 + \sqrt{79})^2$$

Next, we raise to the power of $h(K)$, which is 3 in this example.

$$(360 + 45\sqrt{79})^3 = (3, 1 + \sqrt{79})^6 \times (3, -1 + \sqrt{79})^9 \times (5, 2 + \sqrt{79})^3 \times (5, -2 + \sqrt{79})^6$$

Note that since the class number is prime, all non-principal ideals must have order exactly equal to $h(K)$. Next we find the p_i by raising each prime ideal to its order.

$$(3, 1 + \sqrt{79})^3 = (-17 - 2\sqrt{79})$$
$$(3, -1 + \sqrt{79})^3 = (17 - 2\sqrt{79})$$
$$(5, 2 + \sqrt{79})^3 = (21 - 2\sqrt{79})$$
$$(5, -2 + \sqrt{79})^3 = (21 + 2\sqrt{79})$$

So the canonical factorization of $\alpha^{h(K)}$ is

$$\alpha^{h(K)} = u(-17 - 2\sqrt{79})^2 \times (17 - 2\sqrt{79})^3 \times (21 - 2\sqrt{79}) \times (21 + 2\sqrt{79})^2$$

for some unit $u \in \mathcal{O}_K^\times$. If we compute $(-17-2\sqrt{79})^2 \times (17-2\sqrt{79})^3 \times (21-2\sqrt{79}) \times (21+2\sqrt{79})^2$, we find that this is $3736125 - 729000\sqrt{79}$, and $\frac{\alpha^{h(K)}}{3736125-729000\sqrt{79}} = (-80 - 9\sqrt{79})$ so the proper unit is $u = (-80 - 9\sqrt{79})$.

From this, we get that the square-free part of α is $s(\alpha) = (-80 - 9\sqrt{79}) \times (-2\sqrt{79} + 17) \times (-2\sqrt{79} + 21) = 196 + 23\sqrt{79}$, which is neither of the guesses we had in our previous example before introducing canonical factorization. Note that α, $196 + 23\sqrt{79}$, $5\sqrt{79} + 40$, and $3\sqrt{79} - 24$ are in the same congruence class in $K^\times/(K^\times)^2$ because

$$360 + 45\sqrt{79} = (196 + 23\sqrt{79}) \times \left(\frac{-2 + \sqrt{79}}{5}\right)^2$$
$$196 + 23\sqrt{79} = (5\sqrt{79} + 40) \times \left(\frac{1 + 2\sqrt{79}}{5}\right)^2$$

$$5\sqrt{79}+40=(3\sqrt{79}-24)\times\left(\frac{8+\sqrt{79}}{3}\right)^2.$$

This is what we wanted the definition to accomplish and so in fact, due to Proposition 4.6, $s(\alpha)=196+23\sqrt{79}$ is the square-free part of all of these elements.

Also notice that $\alpha=s(\alpha)\times\frac{83-4\sqrt{79}}{25}$, so since $\frac{83-4\sqrt{79}}{25}\notin\mathcal{O}_K$, $s(a)\nmid a$.

Next, we wish to apply this concept to proving a generalization of Theorem 3.10. The first place in the previous section where the assumption that $h(K)=1$ was used was in Proposition 3.5. So first, we will need a new version of this proposition which does not rely on this assumption. In order to state this new version of Proposition 3.5, we will use the following Lemma.

Lemma 4.8. *Let $h(K)$ be odd. Given $\alpha\in K^\times$, there exists $a\in\mathcal{O}_K$ such that $\alpha\equiv a$ in $K^\times/(K^\times)^2$ and such $ord_\wp(a)$ is odd whenever $\wp$ is a prime ideal dividing (a).*

Proof. Given $\alpha\in K^\times$, let $\alpha=\frac{b_1}{b_2}$ where $b_1,b_2\in\mathcal{O}_K$. Then $\alpha b_2^2=b_1b_2\in\mathcal{O}_K$ and $b_1b_2\equiv\alpha$ in $K^\times/(K^\times)^2$. For simplicity of notation, let $b=b_1b_2$.

Let a be the square-free part of b. Then $a\equiv b$ so $a\equiv\alpha$ in $K^\times/(K^\times)^2$. Also note that each (p_i) is a prime ideal to the power of its order in $Cl(K)$, and since $h(K)$ is odd, each (p_i) is a prime ideal to an odd power, so we are done. □

Proposition 4.9. *Let E be the elliptic curve defined over $\mathbb{Q}$ by $y^2=f(x)$ where K is the splitting field of $f(x)$ and let $e_1,e_2,e_3\in K$ be the roots of $f(x)$ as before. Let $P=(x_0,y_0)\in E(\mathbb{Q})$ and let*

$$x_0-e_1\equiv a$$
$$x_0-e_2\equiv b$$
$$x_0-e_3\equiv c$$

in $K^\times/(K^\times)^2$ where $a,b,c\in\mathcal{O}_K$ such that whenever $\wp$ divides $(a),(b)$, or (c), $ord_\wp(a)$, (respectively $ord_\wp(b)$ and $ord_\wp(c)$) is odd. Then $\wp|(abc)\implies\wp|(\Delta)$ where $\wp$ is a prime ideal in $\mathcal{O}_K$

Remark 4.10. Such a,b,c exist by Lemma 4.8.

Remark 4.11. Throughout the paper, I use the notation (Δ) to mean $\Delta\mathcal{O}_K$.

Remark 4.12. Note that when I write (γ), for $\gamma\in K^\times$, I do not mean the ideal in $K^\times$ generated by γ. Ideals in fields are of course trivial. This is a fractional ideal, meaning if $\gamma=\frac{n}{m}$ for $n,m\in\mathcal{O}_K$, then $(\gamma)=(n)(m)^{-1}$.

Proof. Suppose $\wp$ is a prime ideal in $\mathcal{O}_K$ such that $\wp|(abc)$.

If $\wp$ divides $(a),(b)$, and (c), then letting $a=(x_0-e_1)A^2$ where $A\in K^\times$, $\mathrm{ord}_\wp(a)=\mathrm{ord}_\wp((x_0-e_1)A^2)$, so $\mathrm{ord}_\wp(a)=\mathrm{ord}_\wp(x_0-e_1)+2\mathrm{ord}_\wp(A)$, which means that $\mathrm{ord}_\wp(x_0-e_1)$ is odd. Similarly $\mathrm{ord}_\wp(x_0-e_2)$ and $\mathrm{ord}_\wp(x_0-e_3)$ odd, thus $\mathrm{ord}_\wp((x_0-e_1)(x_0-e_2)(x_0-e_3))=\mathrm{ord}_\wp(x_0-e_1)+\mathrm{ord}_\wp(x_0-e_2)+\mathrm{ord}_\wp(x_0-e_3)$ is odd. But the product, $(x_0-e_1)(x_0-e_2)(x_0-$

$e_3) = y_0^2$ so $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3))$ is even, which is a contradiction. So it cannot be the case that all three of $(a), (b)$, and (c) are divisible by $\wp$.

Next, suppose $\wp$ divides exactly one of $(a), (b)$, and (c). Without loss of generality, suppose $\wp|(a)$. Then by the same argument as above, $\text{ord}_\wp(x_0 - e_1)$ is odd and since $\wp \nmid (b)$ and $\wp \nmid (c)$, $\text{ord}_\wp(x_0 - e_2) \equiv \text{ord}_\wp(x_0 - e_3) \equiv 0 \bmod 2$. But then $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3)) = \text{ord}_\wp(x_0 - e_1) + \text{ord}_\wp(x_0 - e_2) + \text{ord}_\wp(x_0 - e_3)$ is odd. But the product, $(x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = y_0^2$ so $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3))$ is even, and we arrive at the same contradiction.

So $\wp$ divides exactly two of $(a), (b)$, and (c). Without loss of generality, suppose $\wp|(a)$, $\wp|(b)$ and $\wp \nmid (c)$. Then $\text{ord}_\wp(x_0 - e_1)$ and $\text{ord}_\wp(x_0 - e_2)$ are odd by the same argument as above. The rest of the proof is divided into three cases.

First, we consider the case when $\text{ord}_\wp(x_0 - e_1) \neq \text{ord}_\wp(x_0 - e_2)$. Then $\text{ord}_\wp(e_1 - e_2) = \min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(x_0 - e_2)\}$ since $e_1 - e_2$ is the difference of $x_0 - e_1$ and $x_0 - e_2$. Then $\text{ord}_\wp(e_1 - e_2)$ is odd, so in particular, $\text{ord}_\wp(e_1 - e_2) \neq 0$. Thus $\wp|(e_1 - e_2)$ so $\wp|(\Delta)$ since $\Delta = (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. (Recall that e_i is a root of a monic polynomial with integral coefficients by definition, so $e_i \in \mathcal{O}_K$ so $(e_i - e_j) \in \mathcal{O}_K$ so it makes sense to say that $\wp|(e_1 - e_2)$.)

Next, we suppose $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) < 0$. Then $\text{ord}_\wp(x_0 - e_1) \neq \text{ord}_\wp(e_1)$ because $\text{ord}_\wp(e_1) \geq 0$ and $\text{ord}_\wp(x_0 - e_1) < 0$. Therefore $\text{ord}_\wp(x_0) = \min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(e_1)\}$ and $\min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(e_1)\} = \text{ord}_\wp(x_0 - e_1)$. So $\text{ord}_\wp(x_0) = \text{ord}_\wp(x_0 - e_1)$. So $\text{ord}_\wp(x_0) < 0$. If $\text{ord}_\wp(x_0 - e_3) < 0$, the same argument will show that $\text{ord}_\wp(x_0) = \text{ord}_\wp(x_0 - e_3)$ and that $\text{ord}_\wp(x_0) = \text{ord}_\wp(x_0 - e_2)$ so we would have $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) = \text{ord}_\wp(x_0 - e_3)$ so $\text{ord}_\wp(y_0^2) = 3\text{ord}_\wp(x_0 - e_1)$ but we showed $\text{ord}_\wp(x_0 - e_1)$ is odd so this is a contradiction. If $\text{ord}_\wp(x_0 - e_3) \geq 0$, we also know $\text{ord}_\wp(e_3) \geq 0$ since $e_3 \in \mathcal{O}_K$ so $\text{ord}_\wp(x_0) \geq \min\{\text{ord}_\wp(x_0 - e_3), \text{ord}_\wp(e_3)\}$, but then $\text{ord}_\wp(x_0) \geq 0$ which is a contradiction. Therefore, the case when $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) < 0$ is impossible.

Finally, we consider the case when $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) > 0$. (Note that we do not need to consider the case when $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) = 0$ because we showed $\text{ord}_\wp(x_0 - e_1)$ and $\text{ord}_\wp(x_0 - e_2)$ are odd.) We know $\text{ord}_\wp(e_1 - e_2) \geq \min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(x_0 - e_2)\}$. Since both $\text{ord}_\wp(x_0 - e_1)$ and $\text{ord}_\wp(x_0 - e_2)$ are greater than zero, $\text{ord}_\wp(e_1 - e_2) > 0$, so $\wp|(e_1 - e_2)$, and thus $\wp|(\Delta)$, completing our proof. □

The point of this proposition is to aid us in creating an injective map from the image of δ to a finite set, the size of which will be easy to count. Let π_i be the projection of image(δ) onto the i^{th} coordinate of $(K^\times/(K^\times)^2)^3$ for $i = 1, 2, 3$. We will define a map μ_i from $\pi_i(\text{image}(\delta))$ to $\Gamma'/(\Gamma'^2)$ where $\Gamma' = \{\alpha \in K^\times : \text{ord}_\wp(\alpha) \neq 0 \implies \wp|(\Delta)$ for prime ideals $\wp\}$. Note that $\Gamma = \Gamma'/(\Gamma'^2)$ when $h(K) = 1$, so this is consistent with Corollary 3.9. We will refer to μ_i as μ and π_i as π with the understanding that μ is μ_i for an arbitrary coordinate of $(K^\times/(K^\times)^2)^3$. We define μ as follows.

Given $\bar{\alpha} \in \pi(\text{image}(\delta)) \subseteq K^\times/(K^\times)^2$, choose a representative $\alpha \in K^\times$ and let $(\alpha) = \wp_1{}^{f_1}\wp_2{}^{f_2}...\wp_n{}^{f_n}$ be the factorization of (α) into prime ideals $\wp_i$ where $f_i \in \mathbb{Z}$, $f_i \neq 0$ for $1 \leq i \leq n$. Let $m_i = \text{ord}(\wp_i)$ in $Cl(K)$.

$$\text{Define } E_i = \begin{cases} f_i & \text{if } f_i > 0, \\ \text{lcm}(2|f_i|, m_i) + e_i & \text{if } f_i < 0. \end{cases}$$

Consider the product ${\wp_1}^{E_1}{\wp_2}^{E_2}...{\wp_n}^{E_n}$. Note that this product forms a principal ideal because ${\wp_1}^{E_1}{\wp_2}^{E_2}...{\wp_n}^{E_n} = (\alpha)I$ where I is the product of ${\wp_i}^{\text{lcm}(2|f_i|,m_i)}$ such that f_i is negative. Since $m_i = \text{ord}(\wp_i)$ in $Cl(K)$, and since m_i divides the exponent of $\wp_i$ for each $\wp_i$ dividing I, we have that I is principal, and so ${\wp_1}^{E_1}{\wp_2}^{E_2}...{\wp_n}^{E_n}$ is principal. So let ${\wp_1}^{E_1}{\wp_2}^{E_2}...{\wp_n}^{E_n} = (a)$. Note that $a \in \mathcal{O}_K$ since $E_i > 0$ for all i. Note that since these ideals are principal, $a \equiv u_1\alpha$ in $K^\times/(K^\times)^2$ for some unit $u_1 \in \mathcal{O}_K^\times$.

Next, let $m_ik_i = h(K)$, and let $(p_i) = {\wp_i}^{m_i}$. Notice that $s(a) \in \mathcal{O}_K$ such that $s(a) \equiv x_0 - e_i$ in $K^\times/(K^\times)^2$ and $\text{ord}_\wp(s(a)) \neq 0$ implies that $\text{ord}_\wp(s(a))$ is odd. Therefore, $s(a)$ plays the role of a, b, and c in the hypotheses of Proposition 4.9, so the result of this proposition tells us that $\wp|(\Delta)$ whenever $\wp|(s(a))$ (or equivalently, whenever $\text{ord}_\wp(s(a)) \neq 0$ since $s(a) \in \mathcal{O}_K$). Notice that this tells us $s(a) \in \Gamma'$. Finally, we define $\mu(\bar{\alpha}) = \bar{s(a)}$ where $\bar{s(a)}$ is the equivalence class of $s(a)$ in $\Gamma'/({\Gamma'}^2)$. Next, we show μ is well-defined and injective, providing an analogue of Corollary 3.9 for odd class number.

Proposition 4.13. *The map $\mu : \pi(\text{image}(\delta)) \to \Gamma'/({\Gamma'}^2)$ is well defined and injective.*

Proof. Let $\alpha_1, \alpha_2 \in \pi(\text{image}(\delta))$ such that $\alpha_1 \equiv \alpha_2$ in $K^\times/(K^\times)^2$. Then let $\alpha_2 = \alpha_1\gamma^2$ where $\gamma \in K^\times$. Let $(\alpha_1) = {\wp_1}^{f_1}...{\wp_l}^{f_l}$ and let $(\gamma) = {\wp_{l+1}}^{f_{l+1}}...{\wp_n}^{f_n}$ be the factorizations of (α_1) and (γ) into prime ideals. Then $(\alpha_2) = {\wp_1}^{f_1}...{\wp_l}^{f_l}{\wp_{l+1}}^{2f_{l+1}}...{\wp_n}^{2f_n}$. Following the definition of μ, let $(a_1) = {\wp_1}^{E_1}...{\wp_l}^{E_l}$ and let $(a_2) = {\wp_1}^{E_1}...{\wp_l}^{E_l}{\wp_{l+1}}^{E_{l+1}}...{\wp_n}^{E_n}$ where for $1 \leq i \leq l$,

$$E_i = \begin{cases} f_i & \text{if } f_i > 0, \\ \text{lcm}(2|f_i|, m_i) + f_i & \text{if } f_i < 0 \end{cases}$$

and for $l+1 \leq i \leq n$,

$$E_i = \begin{cases} 2f_i & \text{if } f_i > 0, \\ \text{lcm}(4|f_i|, m_i) + 2f_i & \text{if } f_i < 0. \end{cases}$$

Notice that E_i is even for $l+1 \leq i \leq n$ and that $a_1, a_2 \in \mathcal{O}_K$. Also notice that $a_1 \equiv \alpha_1$ and $a_2 \equiv \alpha_2$ in $K^\times/(K^\times)^2$. So since $\alpha_1 \equiv \alpha_2$, we have $a_1 \equiv a_2$ in $K^\times/(K^\times)^2$. Then applying Proposition 4.6, $s(a) = u^2s(b)$ for some unit $u \in \mathcal{O}_K$. Since units are in Γ', this shows $s(a) \equiv s(b)$ in $\Gamma'/(\Gamma')^2$ showing μ is well-defined.

Suppose $\mu((\bar{\alpha}_1)) = \mu((\bar{\alpha}_2))$. This means that $s(a_1) \equiv s(a_2)$ in $\Gamma'/({\Gamma'}^2)$, so $s(a_1) = s(a_2)\delta^2$ for some $\delta \in \Gamma'$. Since $\Gamma' \subseteq K^\times$, $s(a_1) \equiv s(a_2)$ in $K^\times/(K^\times)^2$. Since $\alpha_1 \equiv s(a_1)$ and $\alpha_2 \equiv s(a_2)$, we get that $\alpha_1 \equiv \alpha_2$ in $K^\times/(K^\times)^2$, so $\bar{\alpha}_1 = \bar{\alpha}_2$, proving that μ is injective. □

Next, we wish to count the size of $\Gamma'/({\Gamma'}^2)$. Note that $\Gamma' = \{\alpha \in K^\times : (\alpha) = {\wp_1}^{t_1}{\wp_2}^{t_2}...{\wp_n}^{t_n}\}$ where $\{\wp_i\}_{1\leq i\leq n}$ is the set of primes dividing (Δ) and $t_i \in \mathbb{Z}$ for $1 \leq i \leq n$. Then each congruence class in $\Gamma'/(\Gamma')^2$ is uniquely determined by the values of t_i taken modulo 2 because if $(\alpha) = {\wp_1}^{t_1}{\wp_2}^{t_2}...{\wp_n}^{t_n}$ and $(\beta) = {\wp_1}^{t'_1}{\wp_2}^{t'_2}...{\wp_n}^{t'_n}$, then $\alpha \equiv \beta$ in $\Gamma'/(\Gamma')^2$

exactly when $\alpha = \beta \times \gamma^2$ for some $\gamma \in \Gamma'$, which happens exactly when $t_i \equiv t_i' \bmod 2$ for each i. There is one more subtlety to make note of, which is that even if we take the set of equivalence classes $\{\wp_1{}^{\bar{t_1}}\wp_2{}^{\bar{t_2}}...\wp_n{}^{\bar{t_n}} : \bar{t_i} \in \mathbb{Z}/2\mathbb{Z}\}$, it is not immediately obvious that each class will correspond to a class in $\Gamma'/(\Gamma')^2$ because it is not immediately obvious that for each choice of $\{\bar{t_i}\}$, there exists a principal ideal $(\alpha) = \wp_1{}^{t_1}\wp_2{}^{t_2}...\wp_n{}^{t_n}$ for integers t_i in the class $\bar{t_i} \in \mathbb{Z}/2\mathbb{Z}$. However, this is in fact true because the class number is odd, so for each $\wp_i$, we can raise to the power of $h(K)$ to get a principal ideal. Thus $\Gamma'/(\Gamma')^2 = \{\wp_1{}^{\bar{t_1}}\wp_2{}^{\bar{t_2}}...\wp_n{}^{\bar{t_n}} : \bar{t_i} \in \mathbb{Z}/2\mathbb{Z}\}$.

Thus, there are $2^{\nu(\Delta)}$ choices of $\bar{t_1}, ..., \bar{t_n}$ which will yield an element of $\Gamma'/(\Gamma'^2)$ where $\nu(\Delta)$ is now interpreted to be the number of prime *ideals*[11] dividing (Δ). So there are $2^{\nu(\Delta)}$ choices for the class $\wp_1{}^{\bar{t_1}}\wp_2{}^{\bar{t_2}}...\wp_n{}^{\bar{t_n}}$. Then we choose a representative from each class, a principal ideal $(\alpha) = \wp_1{}^{t_1}...\wp_n{}^{t_n}$. Then there are $2^{r_1+r_2}$ choices of a generator of this ideal up to squares where r_1 is the number of real embeddings of K into $\mathbb{C}$ and r_2 is the number of pairs of non-real embeddings of K into $\mathbb{C}$. This is by Dirichlet's Unit Theorem[12]; given one generator of the ideal, any unit multiple is also a generator of the same ideal and there are $r_1 + r_2$ generators of the unit group which only matter up to squares. This yields a total of $2^{\nu(\Delta)+r_1+r_2}$ elements of $\Gamma'/(\Gamma'^2)$. We are now fully equipped to generalize Theorem 3.10 to the odd class number case.

Theorem 4.14. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation $y^2 = f(x) = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$ and let K be the splitting field of $f(x)$ and let $e_1, e_2, e_3 \in K$ be the roots of $f(x)$ as before. Assume that $h(K)$ is odd. Then letting $\nu(\Delta)$ be the number of prime ideals in $\mathcal{O}_K$ dividing (Δ), and letting r_1 and r_2 be as before,*

$$R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) - 1).$$

Notice that we did not have to make the bound any looser by making this generalization, a luxury we will not have in the next section.

Proof. $|E(K)/2E(K)| = 2^{(2+R_{E(K)})}$ as was shown before Theorem 3.10.

We just showed that $|\Gamma'/(\Gamma'^2)| = 2^{(r_1+r_2+\nu(\Delta))}$.

Notice that $E(K)/2E(K) \hookrightarrow (\Gamma'/(\Gamma'^2))^2$ by composing μ and δ, so $|E(K)/2E(K)| \leq |(\Gamma'/(\Gamma'^2))^2|$, which means

$$\begin{aligned} 2^{2+R_{E(K)}} &\leq 2^{2(r_1+r_2+\nu(\Delta))} \\ \implies 2 + R_{E(K)} &\leq 2(r_1 + r_2 + \nu(\Delta)) \\ \implies R_{E(K)} &\leq 2(r_1 + r_2 + \nu(\Delta) - 1). \end{aligned}$$

[11]Note that this is consistent with our previous usage of this notation in section 2 because when $h(K) = 1$, the number of prime ideals dividing (Δ) is exactly the number of prime elements of $\mathcal{O}_K$ dividing Δ.

[12]Dirichlet's Unit Theorem states that there are $r_1 + r_2 - 1$ generators of the free part of the unit group. In the cases we are concerned with, the finite part of the unit group (i.e. the roots of unity) is always cyclic, yielding a total of $r_1 + r_2$ generators of the unit group

□

Corollary 4.15. $R_{E(\mathbb{Q})} \leq 2(r_1 + r_2 + \nu(\Delta) - 1)$.

Proof. Note that if $P \in E(\mathbb{Q})$ is of infinite order in $E(\mathbb{Q})$, then it is also of infinite order in $E(K)$ because $\mathbb{Q} \subset K$ so each power of P is in $E(K)$, and none of them are the identity. □

5. Arbitrary Class Number

While in the case of odd class number, canonical factorization worked very well to help us generalize the notion of the square-free part of an element, the same approach will not work if we allow the class number to be even. While we could still define canonical factorization of elements raised to the power of the class number, it is no longer true that for $\alpha \in K^\times$, we have $\alpha \equiv \alpha^{h(K)}$ in $K^\times/(K^\times)^2$, which was needed so that for $a \in \mathcal{O}_K$, $s(a) \equiv a$ in $K^\times/(K^\times)^2$ as was pointed out in Remark 4.5. Thus defining this no longer helps us choose a representative of a given class in $K^\times/(K^\times)^2$. Furthermore, we can find no odd number n such that $(\alpha)^n$ is guaranteed to be principal for all elements $\alpha \in \mathcal{O}_K$. Simply take any ideal of exact order two in the class group; then raising to any odd power brings us back to the original ideal class we began with, and thus we will never have a principal ideal as the odd power of an ideal of order two. So we can never find n such that $\alpha \equiv \alpha^n$ in $K^\times/(K^\times)^2$ and $(\alpha)^n$ is always principal.

This means we need a new approach. The same underlying approach to proving our bound will still be used, that is, we want to show that image(δ) embeds into something finite. Then if we can count the size of the range, we can get a bound on the size of our domain which will yield a bound on the rank as in the previous two cases. In the second case, we used our expanded notion of the square-free part of an element to show that image(δ) could be embedded into $(\Gamma'/(\Gamma')^2)^2$ and this was easy to count the size of, yielding the proof of our bound.

Recall that $\Gamma' = \{\alpha \in K^\times : \text{ord}_\wp(\alpha) \neq 0 \implies \wp|(\Delta)\}$, or equivalently, $\Gamma' = \{\alpha \in K^\times : \wp \nmid (\Delta) \implies \text{ord}_\wp(\alpha) = 0\}$. Another way we could describe this set is to say that $\Gamma' = \ker(\Phi)$ where

$$\Phi : K^\times \to \bigoplus_{\wp \nmid (\Delta)} \mathbb{Z} \tag{7}$$

is defined so that $\pi(\Phi(\alpha)) = \text{ord}_\wp(\alpha)$ where π is the projection of the direct sum onto the $\wp$ coordinate and where the direct sum is taken over the set of prime ideals $\wp \in \mathcal{O}_K$ such that $\wp \nmid (\Delta)$. More explicitly, given $\alpha \in K^\times$, suppose $(\alpha) = {\wp_1}^{t_1}{\wp_2}^{t_2}...{\wp_n}^{t_n}$ where $t_i \in \mathbb{Z}$ for $1 \leq i \leq n$. Then the coordinate in $\Phi(\alpha)$ in $\bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}$ corresponding to the ideal $\wp_i$ (where $\wp_i \nmid (\Delta)$) is t_i. In general, we will denote an element of $\bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}$ by $(a_\wp)_{\wp \nmid (\Delta)}$. With this notation, $\Phi(\alpha) = (\text{ord}_\wp(\alpha))_{\wp \nmid (\Delta)}$.

Notice that in our definition of the map Φ, had we taken the direct sum over *all* prime ideals instead of only the prime ideals $\wp$ such that $\wp \nmid (\Delta)$, $\ker(\Phi) = \Gamma'$ would be the unit group, $\mathcal{O}_K^\times$. Essentially Γ' is the what the unit group would be if we introduced inverses of the prime ideals dividing (Δ).

What we have shown in the previous cases is that the projection onto one coordinate of the image of δ can be embedded into $\ker(\Phi)/(\ker(\Phi))^2 = \Gamma'/(\Gamma')^2$.

Here, we will consider the map

$$\varphi : K^\times/(K^\times)^2 \to \bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}/2\mathbb{Z} \tag{8}$$

We will denote $\ker(\varphi)$ by N. For $\alpha \in \Gamma'$, let $\bar{\alpha} = \{\beta \in \Gamma' : \beta = \alpha\gamma^2 \text{ for some } \gamma \in \Gamma'\}$ be the equivalence class of α in $\Gamma'/(\Gamma')^2$. For $\alpha \in K^\times$, let $\overline{\bar{\alpha}} = \{\beta \in K^\times : \beta = \alpha\gamma^2 \text{ for some } \gamma \in K^\times\}$ be the equivalence class of α in $K^\times/(K^\times)^2$.

What is the relationship between N and $\Gamma'/(\Gamma')^2$? They are not the same. N is a subset of $K^\times/(K^\times)^2$ such that $\overline{\bar{\alpha}} \in N$ means that for $\wp \nmid (\Delta)$, $\mathrm{ord}_\wp(\alpha) \equiv 0 \bmod 2$ for a representative $\alpha \in K^\times$ of $\bar{\alpha}$. However, $\overline{\bar{\alpha}} \in \Gamma'/(\Gamma')^2$ means that $\mathrm{ord}_\wp(\alpha) = 0$ for $\wp \nmid (\Delta)$, a stronger condition.

One might think for a second that these two conditions are not terribly different. After all, given $\alpha \in K^\times$ a representative of $\bar{\alpha} \in N$, then $\mathrm{ord}_\wp(\alpha) \equiv 0 \bmod 2$ for $\wp \nmid (\Delta)$ implies that we could multiply by A^2 for some ideal A to obtain an ideal $I = (\alpha)A^2$ such that $\mathrm{ord}_\wp I = 0$. The problem with this is that A may not be principal, and thus I may not be principal, so multiplication by A^2 may not yield another representative of $\bar{\alpha}$. However, this leads us to an important observation that when $\mathcal{O}_K$ is a principal ideal domain, N and $\Gamma'/(\Gamma')^2$ are in fact not very different. We will see in the next proposition that when $h(K)$ is odd, there is a bijection between N and $\Gamma'/(\Gamma')^2$. In fact, they are isomorphic. We will also see that regardless of class number, $\Gamma'/(\Gamma')^2$ can be embedded into N.

Although N cannot actually be equal to $\Gamma'/(\Gamma')^2$ as described above, essentially what is going on is that the size of the equivalence classes in $\Gamma'/(\Gamma')^2$ are slightly smaller; namely, they don't include those elements of $K^\times$ which are not in Γ' but are in the same class as an element of Γ'. When $h(K)$ is odd, each class in $\Gamma'/(\Gamma')^2$ corresponds exactly to a unique class in $N \subset K^\times/(K^\times)^2$ and the only difference is that the equivalence class in $\Gamma'/(\Gamma')^2$ is possibly missing some elements of $K^\times$ which are not in Γ'.

Proposition 5.1. *There is an injective homomorphism from $\Gamma'/(\Gamma')^2$ to N. Furthermore, when $h(K)$ is odd, this map is onto, yielding an isomorphism between N and $\Gamma'/(\Gamma')^2$.*

Proof. Define the map $\mu : \Gamma'/(\Gamma')^2 \to N$ so that $\mu(\bar{\alpha}) = \overline{\bar{\alpha}}$ where for $\alpha \in K^\times$, $\bar{\alpha} = \{\beta \in \Gamma' : \beta = \alpha\gamma^2 \text{ for some } \gamma \in \Gamma'\}$ is the equivalence class of α in $\Gamma'/(\Gamma')^2$ and where $\overline{\bar{\alpha}} = \{\beta \in K^\times : \beta = \alpha\gamma^2 \text{ for some } \gamma \in K^\times\}$ is the equivalence class of α in $K^\times/(K^\times)^2$.

First note that although this map is naturally defined from $\Gamma'/(\Gamma')^2$ to $K^\times/(K^\times)^2$, $\mathrm{image}(\mu) \subset N$. Let $\alpha \in \Gamma'$. Any representative of $\overline{\bar{\alpha}}$ is of the form $\alpha\gamma^2$ for some $\gamma \in K^\times$. Since $\alpha \in \Gamma'$, α has the property that $\wp \nmid (\Delta)$ implies that $\mathrm{ord}_\wp(\alpha) = 0$. Thus $\alpha\gamma^2$ has the

property that $\wp \nmid (\Delta)$ implies that $\text{ord}_\wp(\alpha\gamma^2) \equiv 0 \bmod 2$, showing that $\varphi(\overline{\overline{\alpha}}) = 0$. Thus $\mu(\bar{\alpha}) \in \ker(\varphi) = N$.

Next, we will show that μ is well-defined. Let $\alpha, \beta \in \Gamma'$ be representatives of the same equivalence class in $\Gamma'/(\Gamma')^2$. Then $\alpha = \beta\gamma^2$ for some $\gamma \in \Gamma'$. Since $\Gamma' \subset K^\times$, this shows $\alpha \in \mu(\bar{\beta})$. Thus $\mu(\bar{\alpha}) = \mu(\bar{\beta})$ showing that μ is well-defined.

Next note that μ is a homomorphism of abelian groups because $\overline{\overline{\overline{\alpha_1\alpha_2}}} = \overline{\overline{\alpha}}_1\overline{\overline{\alpha}}_2$ by definition of multiplication in $K^\times/(K^\times)^2$.

Next, we will show that μ is injective by showing that the kernel of μ is trivial. If $\bar{\alpha} \in \ker(\mu)$, then $\overline{\overline{\alpha}} = \overline{\overline{1}}$, so $\alpha = 1 \times \gamma^2$ for some $\gamma \in K^\times$. Since $\alpha \in \Gamma'$, $\gamma^2 \in \Gamma'$, so $\gamma \in \Gamma'$. Thus $\alpha \in \bar{1}$, so $\bar{1} = \bar{\alpha}$ and we're done.

To show that μ is onto will require the assumption that $h(K)$ is odd. Consider $B \in N$ and let $\alpha \in \mathcal{O}_K$ be a representative of B. (Note that given any class in $K^\times/(K^\times)^2$, we can find a representative in $\mathcal{O}_K$). Then for any prime ideal $\wp$ such that $\wp \nmid (\Delta)$, we have $\text{ord}_\wp(\alpha) \equiv 0 \bmod 2$.

Let $(\alpha) = IA'$ where I is the product of prime ideals (to their respective powers) dividing (α) which also divide the discriminant and A' is the product of prime ideals (to their respective powers) which do not divide the discriminant. More explicitly, if $(\alpha) = \wp_1^{e_1}\wp_2^{e_2}...\wp_n^{e_n}$ is the prime factorization of (α), then

$$I = \prod_{\wp_i|(\Delta)} \wp_i^{e_i} \quad \text{and}$$

$$A' = \prod_{\wp_i \nmid (\Delta)} \wp_i^{e_i}.$$

where $1 \leq i \leq n$. Note that A' is a square because $\text{ord}_\wp(\alpha) \equiv 0 \bmod 2$ whenever $\wp \nmid (\Delta)$, so let $A' = A^2$.

Then $(\alpha) = IA^2$. So $(\alpha)^{h(K)} = I^{h(K)}(A^{h(K)})^2$ and raising any ideal to the power of the class number yields a principal ideal, so let $I^{h(K)} = (\beta)$ and let $A^{h(K)} = (\gamma)$. Then $(\alpha)^{h(K)} = (\beta)(\gamma)^2$, so $\alpha^{h(K)} \equiv u\beta\gamma^2 \equiv u\beta$ in $K^\times/(K^\times)^2$ for some $u \in \mathcal{O}_K^\times$. Since $h(K)$ is odd, $\alpha^{h(K)} \equiv \alpha$ in $K^\times/(K^\times)^2$, so $\alpha \equiv u\beta$ in $K^\times/(K^\times)^2$.

Recall that $(u\beta) = (\beta) = I^{h(K)}$ and I was constructed so that $\wp|I$ implies that $\wp|(\Delta)$. Thus, $\wp|(\beta)$ implies that $\wp|(\Delta)$. Therefore, $u\beta \in \Gamma'$. And since $\alpha \equiv u\beta$ in $K^\times/(K^\times)^2$, $\alpha \in \overline{\overline{u\beta}} = \mu(\overline{u\beta})$ so $B = \mu(\overline{u\beta})$ showing that μ is onto when $h(K)$ is odd.

□

This proposition will be proved another way in Lemma 5.4, but the point of presenting this now is to suggest that a natural generalization of $\Gamma'/(\Gamma')^2$ would be to instead consider N. They are isomorphic when $h(K)$ is odd and $\Gamma'/(\Gamma')^2$ embeds into N in general. This is the approach we will take, that is, we wish to show that the projection of the image of δ onto a given coordinate can be embedded into N. We then wish to bound the size of N. First we focus on showing that the projection of the image of δ onto a given coordinate can be embedded into N.

Recall that in the previous section, we showed $\pi(\text{image}(\delta))$ embeds into $\Gamma'/(\Gamma')^2$ in Proposition 4.9. However, we used that $h(K)$ was odd in Lemma 4.8 which was used in the statement of this proposition to ensure the existence of a, b, and c. However, an investigation of the proof of this proposition will reveal that it also showed that $\text{ord}_\wp(x_0 - e_i) \equiv 0 \mod 2$ implies that $\wp|(\Delta)$ whenever $x_0 - e_i \in \pi(\text{image}(\delta))$, which shows that $\pi(\text{image}(\delta))$ embeds into N. In fact, a, b, c were only actually needed to show that $\beta \in \Gamma'$, thus showing $\mu(\pi(\text{image}(\delta))) \in \Gamma'/(\Gamma')^2$. For clarity, we state a version of Proposition 4.9 which does not rely on the existence of a, b, and c and we revisit the same proof without using a, b, and c.

Proposition 5.2. *Let E be the elliptic curve defined over $\mathbb{Q}$ by $y^2 = f(x)$ where K is the splitting field of $f(x)$ and let $e_1, e_2, e_3 \in K$ be the roots of $f(x)$ as before. Let $P = (x_0, y_0) \in E(\mathbb{Q})$. Then $ord_\wp(x_0 - e_i)$ is odd $\implies$ $\wp|(\Delta)$ where $\wp$ is a prime ideal in $\mathcal{O}_K$*

Proof. Suppose $\wp$ is a prime ideal in $\mathcal{O}_K$ such that $\text{ord}_\wp(x_0 - e_1)$ is odd. (The same argument will hold choosing $\text{ord}_\wp(x_0 - e_2)$ or $\text{ord}_\wp(x_0 - e_3)$ to be odd).

If $\text{ord}_\wp(x_0 - e_2)$ and $\text{ord}_\wp(x_0 - e_3)$ are also both odd, then $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3)) = \text{ord}_\wp(x_0 - e_1) + \text{ord}_\wp(x_0 - e_2) + \text{ord}_\wp(x_0 - e_3)$ is odd. But the product, $(x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = y_0^2$ so $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3))$ is even, which is a contradiction. So it cannot be the case that all three of $\text{ord}_\wp(x_0 - e_1)$, $\text{ord}_\wp(x_0 - e_2)$, and $\text{ord}_\wp(x_0 - e_3)$ are all odd.

Next, suppose only $\text{ord}_\wp(x_0 - e_1)$ is odd, and $\text{ord}_\wp(x_0 - e_2)$ and $\text{ord}_\wp(x_0 - e_3)$ are even. But then $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3)) = \text{ord}_\wp(x_0 - e_1) + \text{ord}_\wp(x_0 - e_2) + \text{ord}_\wp(x_0 - e_3)$ is odd. But the product, $(x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = y_0^2$ so $\text{ord}_\wp((x_0 - e_1)(x_0 - e_2)(x_0 - e_3))$ is even, and we arrive at the same contradiction.

So exactly two of $\text{ord}_\wp(x_0 - e_1)$, $\text{ord}_\wp(x_0 - e_2)$, and $\text{ord}_\wp(x_0 - e_3)$ are odd. Let $\text{ord}_\wp(x_0 - e_1)$ and $\text{ord}_\wp(x_0 - e_2)$ be odd and $\text{ord}_\wp(x_0 - e_3)$ be even. The rest of the proof is divided into three cases.

First, we consider the case when $\text{ord}_\wp(x_0 - e_1) \neq \text{ord}_\wp(x_0 - e_2)$. Then $\text{ord}_\wp(e_1 - e_2) = \min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(x_0 - e_2)\}$ since $e_1 - e_2$ is the difference of $x_0 - e_1$ and $x_0 - e_2$. Then $\text{ord}_\wp(e_1 - e_2)$ is odd, so in particular, $\text{ord}_\wp(e_1 - e_2) \neq 0$. Thus $\wp|(e_1 - e_2)$ so $\wp|(\Delta)$. (Note that e_i is an algebraic integer since it is the root of a monic polynomial with integral coefficients. Thus $(e_i - e_j) \in \mathcal{O}_K$ so it makes sense to say that $\wp|(e_1 - e_2)$).

Next, we suppose $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) < 0$. Then $\text{ord}_\wp(x_0 - e_1) \neq \text{ord}_\wp(e_1)$ because $\text{ord}_\wp(e_1) \geq 0$ and $\text{ord}_\wp(x_0 - e_1) < 0$. Therefore $\text{ord}_\wp(x_0) = \min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(e_1)\}$ and $\min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(e_1)\} = \text{ord}_\wp(x_0 - e_1)$. So $\text{ord}_\wp(x_0) = \text{ord}_\wp(x_0 - e_1)$. So $\text{ord}_\wp(x_0) < 0$. If $\text{ord}_\wp(x_0 - e_3) < 0$, the same argument will show that $\text{ord}_\wp(x_0) = \text{ord}_\wp(x_0 - e_3)$ and that $\text{ord}_\wp(x_0) = \text{ord}_\wp(x_0 - e_2)$ so we would have $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) = \text{ord}_\wp(x_0 - e_3)$ so $\text{ord}_\wp(y_0^2) = 3\text{ord}_\wp(x_0 - e_1)$ but we showed $\text{ord}_\wp(x_0 - e_1)$ is odd so this is a contradiction. If $\text{ord}_\wp(x_0 - e_3) \geq 0$, we also know $\text{ord}_\wp(e_3) \geq 0$ since $e_3 \in \mathcal{O}_K$ so $\text{ord}_\wp(x_0) \geq \min\{\text{ord}_\wp(x_0 - e_3), \text{ord}_\wp(e_3)\}$, but then $\text{ord}_\wp(x_0) \geq 0$ which is a contradiction. Therefore, the case when $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) < 0$ is impossible.

Finally, we consider the case when $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) > 0$. (Note that we do not need to consider the case when $\text{ord}_\wp(x_0 - e_1) = \text{ord}_\wp(x_0 - e_2) = 0$ because we showed $\text{ord}_\wp(x_0 - e_1)$ and $\text{ord}_\wp(x_0 - e_2)$ are odd.) We know $\text{ord}_\wp(e_1 - e_2) \geq \min\{\text{ord}_\wp(x_0 - e_1), \text{ord}_\wp(x_0 - e_2)\}$. Since both $\text{ord}_\wp(x_0 - e_1)$ and $\text{ord}_\wp(x_0 - e_2)$ are greater than zero, $\text{ord}_\wp(e_1 - e_2) > 0$, so $\wp|(e_1 - e_2)$, and thus $\wp|(\Delta)$, completing our proof. □

Since $N = \{\bar{\alpha} \in K^\times/(K^\times)^2 : \text{ord}_\wp(\alpha) \text{ odd} \implies \wp|(\Delta)\}$, this version of the proposition immediately yields the following corollary.

Corollary 5.3. $\pi(\text{image}(\delta)) \hookrightarrow N$. *Furthermore, applying Proposition 3.4, this implies* $\text{image}(\delta) \hookrightarrow N^2$.

We have succeeded in showing that $\text{image}(\delta) \hookrightarrow N^2$, which was the first of our two goals. Next we need to figure out a way to bound the size of N. Note that it is no longer easy to count the size of N as it was for $\Gamma'/(\Gamma')^2$.

We will do so by showing that there are maps μ and ν such that the following is an exact sequence where $(C_\Delta)_2$ is the 2-torsion[13] of C_Δ and where φ is as defined in (8).

$$0 \to \Gamma'/(\Gamma')^2 \xrightarrow{\mu} N \xrightarrow{\nu} (C_\Delta)_2 \tag{9}$$

If we can show this, then $(\Gamma'/(\Gamma')^2)/\ker(\mu) \cong \text{image}(\mu)$ and by the exactness, $\ker(\mu)$ is trivial so $\Gamma'/(\Gamma')^2 \cong \text{image}(\mu)$. Also, $N/\ker(\nu) \cong \text{image}(\nu)$ and by the exactness of the sequence, $\text{image}(\mu) = \ker(\nu)$ so then $N/(\Gamma'/(\Gamma')^2) \cong \text{image}(\nu)$ and $\text{image}(\nu) \subset (C_\Delta)_2$ so this yields the following bound on the size of N.

$$|N| \leq |\Gamma'/(\Gamma')^2||(C_\Delta)_2|.$$

We already know how to count the size of $\Gamma'/(\Gamma')^2$ and we will see that $(C_\Delta)_2$ is not difficult to count either. First we will show that (9) is an exact sequence.

Let $C_\Delta = \text{coker}(\Phi)$. Recall that $\Gamma' = \ker(\Phi)$. Thus the following is an exact sequence.

$$0 \to \Gamma' \hookrightarrow K^\times \xrightarrow{\Phi} \bigoplus_{\wp \nmid (\Delta)} \mathbb{Z} \to C_\Delta \to 0 \tag{10}$$

where Φ is as defined in (7). The injection from Γ' to $K^\times$ is just inclusion and the map from $\bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}$ to C_Δ takes elements to their class modulo $\text{image}(\Phi)$. Both of these maps are homomorphisms and Φ is also a homomorphism.

Notice that just like Γ' resembles $\mathcal{O}_K^\times$, C_Δ resembles the class group, $Cl(K)$. In fact the class group is sometimes defined as fitting into the exact sequence above without the condition that $\wp \nmid (\Delta)$. Notice that $\bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}$ is a way to represent ideals modulo those prime ideals dividing the discriminant and $\text{image}(\Phi)$ is essentially ideals that are principal (or would be principal if multiplied by an ideal A such that all prime ideals dividing A also divide the discriminant), so it makes sense that $C_\Delta = \text{coker}(\Phi) = (\bigoplus_{\wp \nmid (\Delta)} \mathbb{Z})/\text{image}(\Phi)$ should remind us of the class group because we are taking the set of ideals (modulo prime

[13]If A is an abelian group, then for $n \in \mathbb{N}$, the n-torsion of A is $(A)_n = \{a \in A \text{ such that } na = 0\}$ where the operation in A is denoted additively.

ideals dividing (Δ)) and moding out by "principal" ideals (or ideals that are equivalent to a principal ideal modulo prime ideals dividing (Δ)).

Recall that we defined $N = \ker(\varphi)$ and $(C_\Delta)_2$ is the 2-torsion of C_Δ. Then similarly, we obtain the following exact sequence where φ is as defined in (8).

$$0 \to N \hookrightarrow K^\times/(K^\times)^2 \xrightarrow{\varphi} \bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}/2\mathbb{Z} \tag{11}$$

where again the map from N to $K^\times/(K^\times)^2$ is inclusion.

Now using (11) and (10), we can prove the following lemma which will allow us to bound the size of N as discussed earlier.

Lemma 5.4. *There exist maps μ and ν such that the following is an exact sequence.*

$$0 \to \Gamma'/(\Gamma')^2 \xrightarrow{\mu} N \xrightarrow{\nu} (C_\Delta)_2$$

Proof. This proof is an expanded version of one found in [Mil06] on page 117. Let $A \in N$ have representative $\alpha \in K^\times$. Then since $N = \ker(\Phi)$, $\mathrm{ord}_\wp(\alpha) \equiv 0 \bmod 2$ for all $\wp \nmid (\Delta)$. Then define a map $\nu : N \to C_{(\Delta))}$ such that

$$\nu : A \to \left[\left(\frac{\mathrm{ord}_\wp(\alpha)}{2} \right)_{\wp \nmid (\Delta)} \right]$$

Note that $\left(\frac{\mathrm{ord}_\wp(\alpha)}{2}\right)_{\wp \nmid (\Delta)} \in \bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}$ and for $\mathcal{A} \in \bigoplus_{\wp \nmid (\Delta)} \mathbb{Z}$, I use the notation $[\mathcal{A}]$ to mean the class of $\mathcal{A}$ modulo the image of Φ. (Recall that C_Δ is $(\bigoplus_{\wp \nmid (\Delta)} \mathbb{Z})/\operatorname{image}\Phi$).

Since as it is written, this may appear to depend on a representative of N, we first show that ν is well-defined. Suppose $\alpha, \beta \in K^\times$ are representatives of the same class $A \in N$. Then $\alpha = \beta\gamma^2$ for some $\gamma \in K^\times$. Then

$$\begin{aligned} & \mathrm{ord}_\wp(\alpha) = \mathrm{ord}_\wp(\beta) + 2\mathrm{ord}_\wp(\gamma) \quad \text{for all } \wp \\ \implies & \frac{\mathrm{ord}_\wp(\alpha)}{2} = \frac{\mathrm{ord}_\wp(\beta)}{2} + \mathrm{ord}_\wp(\gamma) \quad \text{in particular, for all } \wp \nmid (\Delta) \\ \implies & \left(\frac{\mathrm{ord}_\wp(\alpha)}{2} \right)_{\wp \nmid (\Delta)} = \left(\frac{\mathrm{ord}_\wp(\beta)}{2} \right)_{\wp \nmid (\Delta)} + \left(\mathrm{ord}_\wp(\gamma)\right)_{\wp \nmid (\Delta)}. \end{aligned}$$

Note that $\left(\mathrm{ord}_\wp(\gamma)\right)_{\wp \nmid (\Delta)} = \Phi(\gamma)$, so $[(\mathrm{ord}_\wp(\gamma))_{\wp \nmid (\Delta)}] = 0$ in C_Δ. Thus

$$\left[\left(\frac{\mathrm{ord}_\wp(\alpha)}{2} \right)_{\wp \nmid (\Delta)} \right] = \left[\left(\frac{\mathrm{ord}_\wp(\beta)}{2} \right)_{\wp \nmid (\Delta)} \right]$$

which shows that ν is well-defined.

Next we will show that image$(\nu) \subset (C_\Delta)_2$. (Notice that $(C_\Delta)_2$ is a subgroup of C_Δ). Let $A \in N$ have representative $\alpha \in K^\times$. Then

$$\nu(A) = \left[\left(\frac{\text{ord}_\wp(\alpha)}{2} \right)_{\wp \nmid (\Delta)} \right]$$
$$\implies 2\nu(A) = \left[(\text{ord}_\wp(\alpha))_{\wp \nmid (\Delta)} \right] = [\Phi(\alpha)] = 0 \quad \text{in } C_\Delta.$$

Thus image$(\nu) \subset (C_\Delta)_2$. Next we show that $\ker(\nu) \cong \Gamma'/(\Gamma')^2$. (Notice that $\Gamma'/(\Gamma')^2$ is not actually a subset of $K^\times/(K^\times)^2$ so it doesn't make sense to say that $\ker(\nu) = \Gamma'/(\Gamma')^2$). To do so, define a map $f : \ker(\nu) \to \Gamma'/(\Gamma')^2$ as follows.

Let $A \in \ker(\nu) \subset N$. Then $\nu(A) = 0$ in C_Δ implies that

$$\left(\frac{\text{ord}_\wp(\alpha)}{2} \right)_{\wp \nmid (\Delta)} \in \text{image}(\Phi).$$

Then there exists $\beta \in K^\times$ such that

$$\Phi(\beta) = (\text{ord}_\wp(\beta))_{\wp \nmid (\Delta)} = \left(\frac{\text{ord}_\wp(\alpha)}{2} \right)_{\wp \nmid (\Delta)}$$
$$\implies \text{ord}_\wp(\alpha) = 2\text{ord}_\wp(\beta) \quad \text{for all } \wp \nmid (\Delta)$$
$$\implies (\alpha) = (\beta)^2(\gamma) \quad \text{for some } \gamma \in \Gamma'$$

Notice that β is unique up to multiplication by elements of Γ', so γ is unique up to multiplication by elements of $(\Gamma')^2$. So it makes sense to define $f(A) = \bar{\gamma}$ where $\bar{\gamma}$ is the class of γ in $\Gamma'/(\Gamma')^2$. It is left to the reader to verify that f is an isomorphism. □

Corollary 5.5. $|N| \leq |\Gamma'/(\Gamma')^2||(C_\Delta)_2|$

Proof. See the map defined in (9). The discussion following this map proves this corollary. □

Next we need to bound $|(C_\Delta)_2|$. Notice that $C_\Delta \subset C$ where $C \cong Cl(K)$ is considered with additive notation to be consistent with C_Δ. Thus $(C_\Delta)_2 \subset (C)_2$, so $|(C_\Delta)_2| \leq |(C)_2| = |(Cl(K))_2|$. Note that $(Cl(K))_2 \cong Cl(K)/(Cl(K))^2$. So we wish to find the size of $Cl(K)/(Cl(K))^2$ since $|(C_\Delta)_2| \leq |Cl(K)/(Cl(K))^2|$. First we consider some examples.

Example 5.6. Let $Cl(K) \cong \mathbb{Z}/5\mathbb{Z}$. Then $Cl(K)/2(Cl(K)) \cong \{1\}$ because if $Cl(K)$ is generated by g where the order of g is 5, and we set squares of all elements to be 1, then $g^6 = g$ so $g \equiv 1$. So $|Cl(K)/(Cl(K))^2| = 1$.

Example 5.7. If $Cl(K) \cong \mathbb{Z}/4\mathbb{Z}$, then $Cl(K)/2(Cl(K)) \cong \{\mathbb{Z}/2\mathbb{Z}\}$ because if $Cl(K)$ is generated by g of order 4 and we set squares of elements to be zero, then $g^{2m+1} \equiv g$ and $g^{2m} \equiv 1$ for $m \in \mathbb{N}$. Also $g \neq 1$, so $|Cl(K)/(Cl(K))^2| = 2$.

Lemma 5.8. *Let $Cl(K) \cong C_1 \times ... \times C_n$ and the C_i are finite cyclic groups and let $e(K) = |\{C_i : |C_i| \text{ is even }\}|$. Then $|Cl(K)/(Cl(K))^2| = 2^{e(K)}$.*

Proof. Let $n \in \mathbb{N}$. Let $Cl(K) \cong C_1 \times ... \times C_n$ where $C_i \cong \mathbb{Z}/k_i\mathbb{Z}$ generated by $\{g_1, g_2, ...g_n\}$ where the order of g_i is k_i. For odd k_i, let $k_i = 2n_i + 1$. Then $g_i^{2n_i+2} = g_i$. Setting the squares of all elements to be 1, $(g_i^{n_i+1})^2 \equiv 1$ so $g_i \equiv 1$. For even k_i, $g_i^{2m+1} \equiv g_i$ and $g_i^{2m} \equiv 1$ for all $m \in \mathbb{N}$. Therefore, we are left with $Cl(K)/(Cl(K))^2 = \{\bar{g_i} : k_i \text{ is even}\}$ where the order of $\bar{g_i}$ is 2 for each i. In other words, $Cl(K)/(Cl(K))^2 \cong (\mathbb{Z}/2\mathbb{Z})^{e(K)}$, which proves our claim. □

Theorem 5.9. *Let E be an elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation $y^2 = f(x) = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$ and let K be the splitting field of $f(x)$ and let $e_1, e_2, e_3 \in K$ be the roots of $f(x)$ as before. Then letting $\nu(\Delta)$ be the number of prime ideals in $\mathcal{O}_K$ dividing (Δ), and let r_1 and r_2 be the number of embeddings of K into $\mathbb{C}$ which are real and not real respectively. Then,*

$$R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) + ord_2(h(K)) - 1).$$

Proof. Recall that $|\Gamma'/(\Gamma')^2| \leq 2^{r_1+r_2+\nu(\Delta)}$ as in the proof of Theorem 4.14.

By Lemma 5.8, $|(C_\Delta)_2| \leq 2^{e(K)}$ where $e(K) = |\{C_i : |C_i| \text{ is even }\}|$ where $Cl(K) \cong C_1 \times ... \times C_n$ and the C_i are finite cyclic groups.

Note that $e(K)$ can be no greater than $\text{ord}_2(h(K))$ with equatlity when each C_i such that $|C_i|$ is even has order *exactly* 2.

By Corollary 5.5,

$$\begin{aligned} &|N| \leq |\Gamma'/(\Gamma')^2||(C_\Delta)_2| \\ \implies &|N| \leq 2^{(r_1+r_2+\nu(\Delta)+e(K))} \\ \implies &|\text{Image}(\delta)| \leq 2^{2(r_1+r_2+\nu(\Delta)+e(K))} \text{ by Corollary 5.3} \end{aligned}$$

Just as before, $|E(K)/2E(K)| = 2^{(2+R_{E(K)})}$, so by Theorem 3.1,

$$\begin{aligned} &2^{2+R_{E(K)}} \leq 2^{2(r_1+r_2+\nu(\Delta)+e(K))} \\ \implies &2 + R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) + e(K)) \\ \implies &R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) + e(K) - 1) \\ \implies &R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) + \text{ord}_2(h(K)) - 1) \end{aligned}$$

proving Theorem 5.9. □

Corollary 5.10. *The proof in fact shows a slightly tighter bound. Letting $e(K) = |\{C_i : |C_i| \text{ is even }\}|$ where $Cl(K) \cong C_1 \times ... \times C_n$ and the C_i are finite cyclic groups, we get*

$$R_{E(K)} \leq 2(r_1 + r_2 + \nu(\Delta) + e(K) - 1).$$

Corollary 5.11. *Since $R_{E(\mathbb{Q})} \leq R_{E(K)}$ as discussed in the previous section, we obtain the following.*

$$R_{E(\mathbb{Q})} \leq 2(r_1 + r_2 + \nu(\Delta) + e(K) - 1),$$
$$R_{E(\mathbb{Q})} \leq 2(r_1 + r_2 + \nu(\Delta) + ord_2(h(K)) - 1).$$

6. Examples, Conclusions, and Further Inquiries

We have successfully proven an upper bound on the rank of an arbitrary elliptic curve. However, there are many more questions left unaddressed. Can we find examples of curves for which this bound is tight or could the bound be made tighter in general? If not in general, could it be made tighter under specific conditions? Does the class group even contribute to the rank as would be the case if this bound was tight?

One should note that this bound is by no means ground-breaking and in its generality, it does lose quite a bit of tightness. Many tighter bounds are known. In the examples to come you will notice that it does not seem to be the case that this bound is very tight. This is very much the nature of the topic of elliptic curves; different curves often behave radically differently from one another, which makes it very difficult to have a bound that is both general and relatively tight.

Example 6.1. The best example I've been able to find of this bound being close to the actual rank is the curve $y^2 = x^3 + 8x$. The actual rank of this curve is 1. Using SAGE, one can determine that $r_1 + r_2 - 1 = 0$, $\nu(\Delta) = 1$, and $\text{ord}_2(h(K)) = 0$, so the bound is $2(0 + 1 + 0) = 2$.

Unfortunately, for most curves, the bound was not nearly this tight.

Example 6.2. The following is a program I wrote in SAGE which considers all non-singular curves of the form $y^2 = x^3 + Ax + B$, where $i \leq A \leq j$ and $n \leq B \leq m$, and prints "$(A, B), [R_{E(K)}, 2(r_1 + r_2 + \nu(\Delta) - 1)], \text{ord}_2(h(K))$" where A and B are the coefficients of the curve.

Although computing $B(-10, 10, -10, 10)$ only tests 431 curves[14], this does give us *some* sort of statistics indicating the strength of this bound.

```
sage: def B(i,j,n,m):
....:     a=i
....:     b=n
....:     while i<=a & a<=j:
....:         while n<=b & b<=m:
....:             R.<x>=QQ[]
....:             f=x^3 + a*x + b
....:             if f.discriminant()!=0:
....:                 r=EllipticCurve([a,b]).rank()
....:                 if f.is_irreducible():
....:                     K.<k>=NumberField(f)
```

[14]There are $21^2 = 441$ combinations of A and B, but only 431 of them are non-singular.

```
....:                     G.<g>=K.galois_closure()
....:                 if len(f.factor())==2:
....:                     if b==0:
....:                         A=0
....:                         B=a
....:                     if b!=0:
....:                         D=divisors(b)
....:                         for d in D:
....:                             if d^3 + a*d + b == 0:
....:                                 A=d
....:                             if -d^3 - a*d + b ==0:
....:                                 A=-d
....:                         B=a+A^2
....:                     G.<g>=NumberField(x^2 + A*x + B)
....:                 if len(f.factor())==3:
....:                     G=QQ
....:                 M=G.class_number().ord(2)
....:                 if G.degree()>1:
....:                     R=G.unit_group().rank()
....:                     L=prime_factors(f.discriminant())
....:                     S=0
....:                     p=0
....:                     while 0<=p & p<=len(L)-1:
....:                         S=S+len(G.primes_above(L[p]))
....:                         p=p+1
....:                 if G.degree()==1:
....:                     R=0
....:                     S=len(prime_factors(f.discriminant()))
....:                 print (a,b),[r, 2*(R+S+M)],M
....:             b=b+1
....:         if b>m:
....:             b=n
....:             a=a+1
```

It would consume too much space to include the actual results of this program for all 431 curves, but Figure 2 is a graph which indicates the number of curves for which the difference between the bound and the rank is a given value. The horizontal axis represents the difference between the bound and the rank and the vertical axis represents the number of curves for which the difference between the bound and the rank is the given value. More explicitly, letting x denote the difference $2(r_1 + r_2 + \nu(\Delta) + \mathrm{ord}_2(h(K)) - 1) - R_{E(\mathbb{Q})}$, then $f(x)$ is the number of curves tested which yield this difference.

The average difference between the bound and the rank over all was about 13.7968, where the smallest gap was 1 and the largest was 30. However, I cannot stress enough that

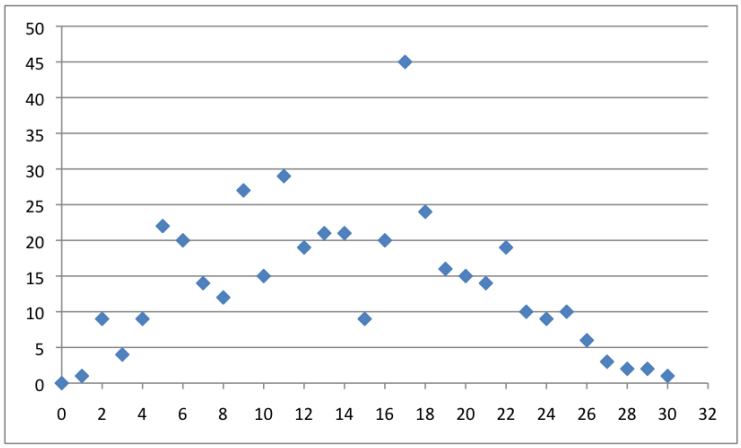

FIGURE 2. $f(x)$ is the number of curves $y^2 = x^3 + Ax + B$ for $-10 \leq A, B \leq 10$ such that $2(r_1 + r_2 + \nu(\Delta) + \mathrm{ord}_2(h(K)) - 1) - R_{E(\mathbb{Q})} = x$.

we are working with a rather small sample size and we only consider curves with small coefficients.

Investigating the graphs in Figures 2, 3, 4, and 5, we do see something vaguely like normal distributions, but it still appears to also be fairly random, possibly a consequence of our small sample size.

Figure 3 is the same idea as Figure 2 but considering only the curves for which $\mathrm{ord}_2(h(K))$ is 0. Here, the average difference between the bound and the rank is 10.8512, which was lower than the average difference for all curves.

Figure 4 is the same, considering only the curves for which $\mathrm{ord}_2(h(K)) = 1$. Here, the average difference between the bound and the rank is 17.2255, already higher than the overall average difference.

Figure 5 is the same, considering only the curves for which $\mathrm{ord}_2(h(K)) > 1$. Here, the average difference between the bound and the rank is 19.9783.

These three charts indicate that for small $\mathrm{ord}_2(h(K))$, as $\mathrm{ord}_2(h(K))$ gets larger, the bound seems to get looser. So as $\mathrm{ord}_2(h(K))$ increases, perhaps the rank of curves on average is staying about the same.

While example 6.1 is somewhat tight, it would be more satisfying to see a curve for which the bound is relatively tight where all of the components of the bound are non-zero. For example, what if $\mathrm{ord}_2(h(K))$ does not even contribute to the bound? What I mean by this

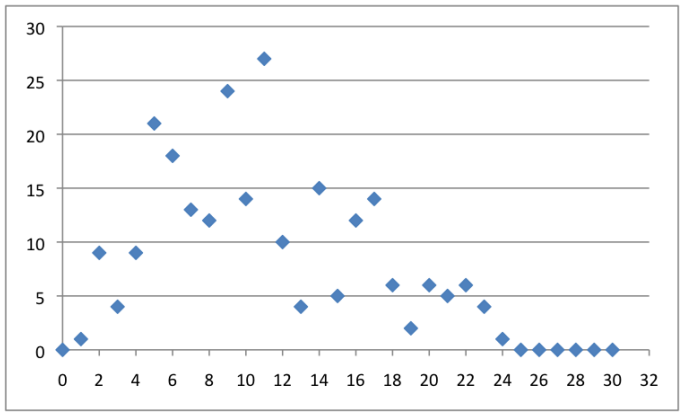

FIGURE 3. same as Figure 2 but only considering curves such that $\mathrm{ord}_2(h(K)) = 0$.

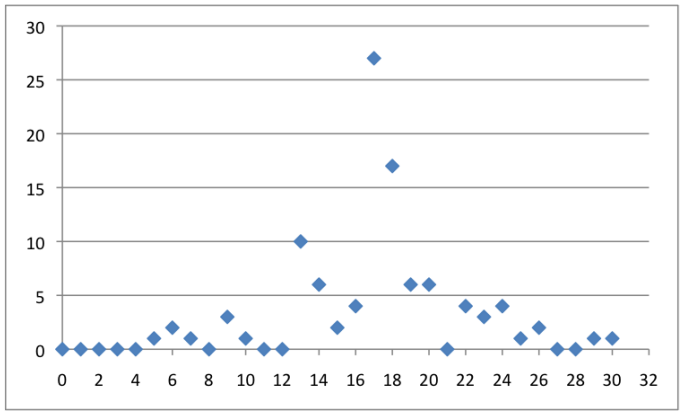

FIGURE 4. same as Figure 2 but only considering curves such that $\mathrm{ord}_2(h(K)) = 1$.

is, can we find a curve such that the rank of this curve is greater than $2(r_1+r_2+\nu(\Delta)-1)$? Note that this is what the bound would be if we set $\mathrm{ord}_2(h(K)) = 0$. I ran a program on SAGE which tested a number of curves by iterating over the coefficients to see if I could find any example in which the class group actually necessarily contributed to the bound. Had this given me an example, we would know for sure that this is an important part of the bound if we wish to keep the bound general. However, the program returned no such examples, which leaves the question of whether the class group contributes to the bound inconclusive. This program was of course limited in many ways. It is difficult to test a very large number of curves without running into problems computing the rank of all of

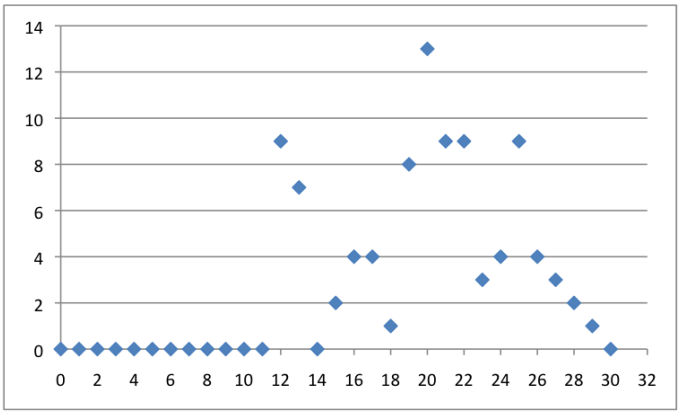

FIGURE 5. same as Figure 2 but only considering curves such that $\mathrm{ord}_2(h(K)) > 1$.

them. It would be better to narrow down certain classes of curves in which we expect we may find such examples and then run the program only on those curves.

Example 6.3. The following program was written in SAGE to consider all curves $y^2 = x^3 + Ax + B$, where $i \leq A \leq j$ and $n \leq B \leq m$, and when the curve is nonsingular, it computes $2(r_1 + r_2 + \nu(\Delta) - 1)$ which is the hypothetical bound in which the class number plays no role, and it computes the actual rank. If it finds a curve in which $R_{E(\mathbb{Q})} > 2(r_1 + r_2 + \nu(\Delta) - 1)$, it prints "$(A, B), [R_{E(\mathbb{Q})}, 2(r_1 + r_2 + \nu(\Delta) - 1)], \mathrm{ord}_2 h(K)$" where A and B are the coefficients of the curve in which $R_{E(\mathbb{Q})} > 2(r_1 + r_2 + \mathrm{ord}_2(h(K)) + \nu(\Delta) - 1)$

```
sage: def B(i,j,n,m):
....:     a=i
....:     b=n
....:     while i<=a & a<=j:
....:         while n<=b & b<=m:
....:             R.<x>=QQ[]
....:             f=x^3 + a*x + b
....:             if f.discriminant()!=0:
....:                 r=EllipticCurve([a,b]).rank()
....:                 if f.is_irreducible():
....:                     K.<k>=NumberField(f)
....:                     G.<g>=K.galois_closure()
....:                 if len(f.factor())==2:
....:                     if b==0:
....:                         A=0
....:                         B=a
....:                     if b!=0:
```

```
....:                         D=divisors(b)
....:                         for d in D:
....:                             if d^3 + a*d + b == 0:
....:                                 A=d
....:                             if -d^3 - a*d + b ==0:
....:                                 A=-d
....:                         B=a+A^2
....:                     G.<g>=NumberField(x^2 + A*x + B)
....:                 if len(f.factor())==3:
....:                     G=QQ
....:                 M=G.class_number().ord(2)
....:                 if G.degree()>1:
....:                     R=G.unit_group().rank()
....:                     L=prime_factors(f.discriminant())
....:                     S=0
....:                     p=0
....:                     while 0<=p & p<=len(L)-1:
....:                         S=S+len(G.primes_above(L[p]))
....:                         p=p+1
....:                 if G.degree()==1:
....:                     R=0
....:                     S=len(prime_factors(f.discriminant()))
....:                 if r>2*(R+S):
....:                     print (a,b),[r, 2*(R+S+M)],M
....:             b=b+1
....:         if b>m:
....:             b=n
....:             a=a+1
....:
```

I ran $B(-10, 10, -10, 10)$, which returned nothing. Thus for all curves tested, $R_{E(\mathbb{Q})} \leq 2(r_1 + r_2 + \nu(\Delta) - 1)$. However, this is *not* a very strong suggestion that the class group does not contribute to the rank. This has only checked $21^2 = 441$ potential[15] curves and since the bound is not very tight anyway, it seems unlikely that we would have found such an example, especially by such a brute force approach. It may be necessary for the bound to be sharper in the case when $\mathrm{ord}_2(h(K)) = 0$ to expect to find such examples.

However, if one continues to consider the average difference between the bound and the rank as $\mathrm{ord}_2(h(K))$ increases, perhaps we could find that this difference grows rapidly or perhaps we would find that it levels off. If it grows rapidly, that seems to suggest the possibility that the class group does not contribute that much to the bound, but if it levels off, perhaps we could gain some insight into a better way to find an example in which $R_{E(\mathbb{Q})} > 2(r_1 + r_2 + \nu(\Delta) - 1)$.

[15]It checks less than 441 curves, since some of them are singular

Note that all of the above examples used the bound $R_{E(\mathbb{Q})} \leq 2(r_1 + r_2 + \nu(\Delta) + \text{ord}_2(h(K)) - 1)$. This is the weaker of our two bounds in Corollary 5.11. We should point out that it does make a difference to use the bound presented in Corollary 5.10 which considers not only the class number, but the *structure* of the class group. We illustrate with the following example, which is a curve taken from [JAP].

Example 6.4. Consider the elliptic curve $y^2 = x^3 - 1033477836241777x$. $\nu(\Delta) = 7$, and $r_1+r_2-1 = 1$ and $h(K) = 256$, so $\text{ord}_2(h(K)) = 8$. Thus $2(r_1+r_2+\nu(\Delta)+\text{ord}_2(h(K))-1) = 32$. This is not very tight because the actual rank is 10. However, the class group in this example is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times since\mathbb{Z}/4\mathbb{Z}$ so the structure of the class group reveals that while $\text{ord}_2(h(K)) = 8$, in fact $e(K) = 4$, so we can tighten the bound a little, by using $2(r_1 + r_2 + \nu(\Delta) + e(K) - 1) = 24$.

There is of course much more that could be done from here. One could work on sharpening the bound in various ways or in various cases. One could continue to study the statistics of the weakness of this bound in relation to the growth of $\text{ord}_2(h(K))$, or in relation to other factors. One could also do the same sort of statistical analysis using the stronger bound presented in Corollary 5.10.

Acknowlegements

I would like to thank my thesis advisor, Álvaro Lozano-Robledo for his patience and dedication in working with me on this project and also Keith Conrad for his help and the University of Connecticut Honors Program for their support.

References

[Duj] Andrej Dujella, *History of elliptic curves rank records*, http://web.math.hr/ duje/tors/rankhist.html.
[JAP] Álvaro Lozano-Robledo Julian Aguirre and Juan Carlos Peral, *Elliptic Curves of Maximal Rank.*
[LR] Álvaro Lozano-Robledo, *Elliptic Curves, Modular Forms and their L-functions.*
[Mil06] J.S. Milne, *Elliptic curves*, BookSurge Publishers, 2006.
[Sil09] J.H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, 2009.