ROCKY MOUNTAIN JOURNAL OF MATHEMATICS
Vol. , No. , YEAR
https://doi.org/rmj.YEAR..PAGE

CONNECTIONS OF CLASS NUMBERS TO THE GROUP STRUCTURE OF GENERALIZED PYTHAGOREAN TRIPLES

THOMAS JAKLITSCH, THOMAS C. MARTINEZ, STEVEN J. MILLER, AND SAGNIK MUKHERJEE

ABSTRACT. Two well-studied Diophantine equations are those of Pythagorean triples and elliptic curves; for the first we have a parametrization through rational points on the unit circle, and for the second we have a structure theorem for the group of rational solutions. Recently Yekutieli discussed a connection between these two problems, and described the group structure of Pythagorean triples and the number of triples for a given hypotenuse. We generalize these methods and results to Pell's equation. We find a similar group structure and count on the number of solutions for a given z to $x^2+Dy^2=z^2$ when D is 1 or 2 modulo 4 and the class group of $\mathbb{Q}[\sqrt{-D}]$ is a $\mathbb{Z}/2\mathbb{Z}$ module, which always happens if the class number is at most 2. We give examples of when the results hold for a class number greater than 2, as well as an example with different behavior when the class group does not have this structure.

1. Introduction

1.1. ***Background.*** The study of the number and structure of rational solutions to Diophantine equations (polynomials of finite degree with integer coefficients) is related to numerous important problems in mathematics, from Pythagorean triples to elliptic curves. Much is known for these two problems, where we can parametrize the solutions, which form commutative groups; see for example [Kn, Maz1, Maz2, MT-B, ST]. A recent paper by Yekutieli [Ye] considered a structural description of Pythagorean triples in order to enumerate normalized solutions. We generalize these results to Pell's equation $x^2+Dy^2=z^2$, and show that for certain D, leading to class groups where every element has order at most 2, we have similar group structures.

The Pythagorean triples are integer solutions of the equation $x^2+y^2=z^2$, and correspond to rational points on the unit circle; thus to a triple (a,b,c) we associate the complex number

$$\zeta_{a,b,c} \;=\; x+iy \;=\; \frac{a}{c}+\frac{b}{c}i. \tag{1.1}$$

These can be parameterized by looking at lines with rational slope emanating from a fixed rational point, often taken to be $(-1,0)$. There are four solutions where either a or b is zero: $1, i, -1, -i$. These are the units of $\mathbb{Z}[i]=\{a+ib : a,b\in\mathbb{Z}\}$, and correspond to trivial Pythagorean triples. We now consider ζ where both a and b are non-zero. We cannot have $a=b$, as that would lead to $\sqrt{2}$ being rational. A straightforward calculation shows that given such a solution ζ there are seven other distinct conjugate solutions; we can multiply ζ by i, i^2 and i^3 (the units of $\mathbb{Z}[i]$ other than 1) and then we can take the complex

We thank Amnon Yekutieli for introducing us to the problem and sharing his work on the subject, and our colleagues from the 2021 Polymath REU, Leart Ajvazaj, Manyi Guo, Dylan Jamner, Yuan Lu, Jonathan Marvel-Zuccola, Sydney Morgan, and Bangqi (Blair) Yuan, for numerous helpful conversations and comments, especially Sydney and Blair, who worked with the third named author on a preliminary research project which was the springboard for this work. Those lectures, notes and questions were a valuable starting point for the present paper.

2020 *Mathematics Subject Classification.* 11D09 (primary), 11E41 (secondary).

Key words and phrases. Class numbers, Pythagorean Triples, Pell Equation, Diophantine Equations, Group Structure.

conjugates of these four solutions. We illustrate this in Figure 1; note, without loss of generality, given any Pythagorean triple not associated to a unit of $\mathbb{Z}[i]$ we may always adjust it, through multiplication by a unit and complex conjugation if needed, so that it lies in the shaded region (i.e., the second octant, or the part of the first quadrant where the imaginary part exceeds the real part).

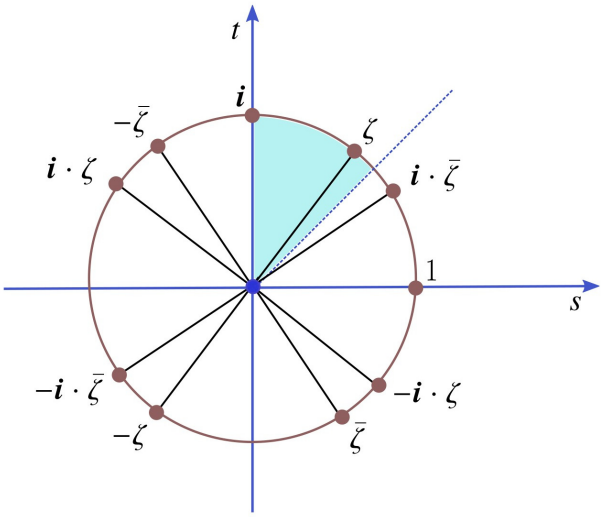

FIGURE 1. The four trivial solutions $(1,i,-1,-i)$ and the seven conjugates to a non-trivial solution ζ, which can be taken to lie in the second octant. Image from [Ye].

Identifying Pythagorean triples with complex numbers yields a commutative group through the multiplicativity of the norm. While re-scaling a Pythagorean triple by k does not change the complex number associated to it, multiplying associated complex numbers (or raising one to a power) generates new solutions. For example, the triple $(3,4,5)$ yields $\zeta_{3,4,5} = 3/5+i4/5$, and

$$\zeta_{3,4,5}^2 \;=\; \left(\frac{3}{4}+\frac{4}{5}i\right)\left(\frac{3}{4}+\frac{4}{5}i\right) \;=\; -\frac{7}{25}+\frac{24}{25}i, \tag{1.2}$$

which corresponds to the triple $(7,24,25)$, while

$$\zeta_{3,4,5}\;\;\zeta_{5,12,13} \;=\; \left(\frac{3}{5}+\frac{4}{5}i\right)\left(\frac{5}{13}+\frac{12}{13}i\right) \;=\; -\frac{33}{65}+\frac{56}{65}i, \tag{1.3}$$

which corresponds to the triple $(33,56,65)$.

1.2. ***Results.*** Yekutieli [Ye] proved several results about the structure of the group of rational solutions to the unit circle version of the Pythagorean equation. Specifically, denote these solutions by

$$G(\mathbb{Q}) \;:=\; \{x+iy : x,y\in\mathbb{Q} \text{ and } x^2+y^2=1\}. \tag{1.4}$$

This is a group under complex multiplication, and decomposes as

$$G(\mathbb{Q}) \;=\; U\times F, \tag{1.5}$$

where $U=\{1,i,-1,-i\}$ is the units in $\mathbb{Z}[i]$ and F is a free abelian group with basis given by the collection $\{\zeta_p\}_{p\in\mathscr{P}_1}$, where the primes P decompose as

$$\mathscr{P} \;=\; \mathscr{P}_1\sqcup\mathscr{P}_2\sqcup\mathscr{P}_3, \quad \text{with} \quad \mathscr{P}_\ell \;:=\; \{p\in\mathscr{P} : p\equiv \ell \bmod 4\}. \tag{1.6}$$

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

He then proves results on which c yield Pythagorean triples, and how many there are.

Our goal is to generalize these results, in particular to look at the structure of solutions to $x^2+Dy^2=z^2$ for square-free $D>0$ (there is no loss in generality in having a positive sign, as $x^2+Dy^2=z^2$ is the same as $z^2-Dy^2=x^2$). In particular, we are interested in seeing how the structure of $\mathbb{Z}[\sqrt{-D}]$ influences the solutions; one way to measure this structure is through its class number. The proofs in [Ye] crucially use that $\mathbb{Z}[i]=\mathbb{Z}[\sqrt{-1}]$ has class number 1. There are 8 other square-free D such that $\mathbb{Z}[\sqrt{-D}]$ has class number 1; the complete set (see [Wa]) is

$$-D \;=\; \{-1,\;\; -2,\;\; -3,\;\; -7,\;\; -11,\;\; -19,\;\; -43,\;\; -67,\;\; -163\}. \tag{1.7}$$

For suitably restricted D, we can generalize the method in [Ye]. First we define *normalized solutions* to arbitrary Pell equations as follows.

Definition 1.1. *A solution (a,b,c) with $a,b,c\in\mathbb{N}$ to*

$$x^2+Dy^2 \;=\; z^2, \tag{1.8}$$

*is defined to be a **normalized solution** if $\gcd(a,b,c)=1$. A solution (a,b,c) with $a,b,c\in\mathbb{Z}$ is defined to be an **elementary solution** if c is prime.*

We also define

$$G_D(\mathbb{Q}) \;:=\; \{a+b\sqrt{-D}\in\mathbb{Q}[\sqrt{-D}] : a^2+Db^2=1\}, \tag{1.9}$$

and prove that, for $D>1$, $G_D(\mathbb{Q})=U\times F$ where $U:=\{1,-1\}$ and F is a free abelian group, which allow us to determine the number of normalized solutions of the form (a,b,c) to the equation (1.8) for any given $c\in\mathbb{N}$.

We do this by deriving three theorems which describe the factorization of elements in $G_D(\mathbb{Q})$ and how it relates to the number of normalized solutions of the equation $x^2+Dy^2=c^2$. Our generalization depends on properties of the class group, which leads to restrictions on what D we can analyze.

Generalization from $D=1$ to an arbitrary $D>0$ is difficult as the ring $\mathbb{Z}[\sqrt{-D}]$ is not necessarily a unique factorization domain, and hence the factorization of the elements of $\mathbb{Z}[\sqrt{-D}]$ into primes or irreducibles can be complicated (and sometimes not possible). Thus unlike the case of $D=1$, the factorization of the elements of $G_D(\mathbb{Q})$ is no longer automatically inherited from the factorization of the elements of $\mathbb{Z}[\sqrt{-D}]$.

We recall some definitions and results on class groups; see [Cox] for details. Throughout, we will often denote a binary quadratic form $f(x,y)=ax^2+bxy+cy^2$ as $[a,b,c]$.

Given a $K<0$, let

$$P \;:=\; \{\text{primitive, positive-definite binary quadratic forms with discriminant } K\}. \tag{1.10}$$

There is an equivalence relation on the set P given by the following condition. For two binary quadratic forms $f=[a,b,c]$ and $g=[a',b',c']$, $f\sim g$ if and only if there exists a matrix $A=\begin{pmatrix}p & q\\ r & s\end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x,y)=f^A(x,y):=f(px+qy,rx+sy)$.

Also, define the binary operation known as Dirichlet composition as follows. Suppose $f=[a,b,c]$ and $g=[a',b',c']$ are primitive, positive-definite binary quadratic forms of discriminant $K<0$ which satisfy $(a,a',\frac{b+b'}{2})=1$. Then the Dirichlet composition of f and g is the form

$$F(x,y) \;:=\; aa'x^2+Bxy+\frac{B^2-K}{4aa'}y^2$$

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

where B is the unique integer satisfying

$$\begin{aligned} B &\equiv b \pmod{2a} \\ B &\equiv b' \pmod{2a'} \\ B^2 &\equiv K \pmod{4aa'}. \end{aligned}$$

The class group, $C(K)$, is the set $P/\sim$ together with the operation of Dirichlet composition. The identity element of the group is

$$\text{Identity of } C(K) \;=\; \begin{cases} \text{the class of } [1,0,\frac{-K}{4}], & \text{if } K \equiv 0 \pmod 4, \\ \text{the class of } [1,1,\frac{1-K}{4}], & \text{if } K \equiv 1 \pmod 4. \end{cases} \tag{1.11}$$

The inverse of the class of $[a,b,c]$ is the class of $[a,-b,c]$. We say that a binary quadratic from $f(x,y)$ represents an integer m if for some $x,y \in \mathbb{Z}$, $f(x,y)=m$. If $(x,y)=1$, then we say that $f(x,y)$ properly represents m. The following is our main result.

Theorem 1.2. *Assume $-D \equiv 2$ or $3 \pmod 4$ and $D>1$. Suppose the class group of $\mathbb{Q}[\sqrt{-D}]$ is a $\mathbb{Z}/2\mathbb{Z}$ module*[1]*. Then $G_D(\mathbb{Q}) = U \times F$, where $U=\{\pm 1\}$ and F is a free abelian group. If $c = p_1^{n_1}\cdots p_k^{n_k}$ such that $\left(\frac{-D}{p_i}\right)=1$ for all $1 \le i \le k$, then the number of normalized solutions of the form (a,b,c) is 2^{k-1}. Otherwise, there are no normalized solutions of the form (a,b,c).*

Remark 1.3. *As the case for $D=1$ is known (see* [Ye]*), we only consider $D>1$. It is worth noting that the result and argument for $D=1$ are slightly different, because the group of units of $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$ while the group of units for $\mathbb{Z}[\sqrt{-D}]$ when $D>1$ is just $\{\pm 1\}$. Also, the definition of normalized solutions must be altered to account for the fact that if (a,b,c) is a solution then so is (b,a,c), which is not true for $D>1$. See Remark 4.3 for greater detail on the case of $D=1$. We also note that we give some examples of when Theorem 1.2 applies in §5.*

After recalling needed facts, we show that if we assume the hypotheses of Theorem 1.2, then c is a normalized solution to the equation x^2+Dy^2. The fact that each element of the class group has order at most 2 is crucial here for the following reason. The integer c is properly represented by some binary quadratic form. Therefore, if every element of $C(-4D)$ has order at most 2, then c^2 is properly represented by the identity element of $C(-4D)$, which is the form x^2+Dy^2. So, there exists a normalized solution to the equation (a,b,c) for some $a,b \in \mathbb{Z}$. If it is the case that there exists $f \in C(-4D)$ such that the order of the class f is greater than 2, then there may exist an integer c such that c is represented by f but c^2 is not represented by the identity element. In this case c might not be a solution to the equation even though it satisfies $\left(\frac{-D}{p}\right)=1$ for all prime factors p of c. We refer to the remarks in Section 5 for a concrete example.

Next, we prove that $G_D(\mathbb{Q})$ factors into the direct product of the group of units of $\mathbb{Z}[\sqrt{-D}]$ and a free abelian group. Finally, this factorization allows us to determine the number of solutions to $x^2+Dy^2=z^2$ for a fixed integer z. We conclude with examples of these theorems as well as cases where the theorem does not hold (e.g., when $C(-4D)$ is not a $\mathbb{Z}/2\mathbb{Z}$ module).

[1] Note that as $\mathbb{Z}/2\mathbb{Z}$ is a field, every $\mathbb{Z}/2\mathbb{Z}$ module is free

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

2. Units and Complex Multiplication

The number field $\mathbb{Q}[\sqrt{-D}]$ has the multiplicative norm

$$N(a+b\sqrt{-D}) \;:=\; a^2+Db^2.$$

It contains the ring $\mathbb{Z}[\sqrt{-D}]$ whose group of units is formed by the elements $x+y\sqrt{-D}$ where $x,y\in\mathbb{Z}$ and $N(x+y\sqrt{-D})=1$. This corresponds to those elements such that $x^2+Dy^2=1$. As $D>1$ the only integer solutions to this equation are $\{\pm 1\}$, so the group of units is $U=\{\pm 1\}$.

We note that

$$G_D(\mathbb{Q}) \;:=\; \{z=a+b\sqrt{-D}\in\mathbb{Q}[\sqrt{-D}] : a^2+Db^2=1\} \tag{2.1}$$

is a group as the above norm is multiplicative, and the inverse of any $a+b\sqrt{-D}\in G_D(\mathbb{Q})$ is given by its complex conjugate $a-b\sqrt{-D}$.

The group $G_D(\mathbb{Q})$ can be geometrically viewed as the rational points on the ellipse $x^2+Dy^2=1$. Given two points (x_1,y_1) and (x_2,y_2) on this ellipse, we can multiply them as follows:

$$(x_1,y_1)*(x_2,y_2) \;:=\; (x_1x_2-Dy_1y_2,\; x_1y_2+x_2y_1), \tag{2.2}$$

which yields another rational point on this ellipse. Note that each such rational point on this ellipse corresponds to a unique normalized solution to the equation $x^2+Dy^2=z^2$ up to the sign, since by definition normalized solutions are positive. Our aim is to find *elementary normalized solutions* so that we can generate any normalized solution by multiplying (as above) these elementary normalized solutions, similar to building composite numbers by multiplying prime numbers.

As multiplying normalized solutions using the above rule does not always yield a normalized solution, we work with the *elementary solutions*. We see this in detail while studying Lemma 3.6 and Theorem 3.8.

3. Group Structure on the Rational Solutions on Ellipse

In this section we prove that $G_D(\mathbb{Q})$ is of the form $U\times F$ where $U:=\{1,-1\}$ and F is a free abelian group provided that $-D\equiv 2,3 \pmod 4$ and $C(-4D)$ is a $\mathbb{Z}/2\mathbb{Z}$ module.

We begin with the following results necessary for factoring $G_D(\mathbb{Q})$.

3.1. *Conditions for Existence of Solutions.*

Lemma 3.1. *Given a $D>0$ such that $-D\equiv 2,3 \pmod 4$, if (a,b,c) is a normalized solution to*

$$x^2+Dy^2 \;=\; z^2, \tag{3.1}$$

then c must be an odd natural number.

Proof. We have $a^2+Db^2=c^2$. Assume $2\mid c$. Then $4\mid a^2+Db^2$. Note that $a^2\equiv 0,1 \pmod 4$ and $b^2\equiv 0,1 \pmod 4$. Therefore, since $4\mid a^2+Db^2$, we have $b^2\equiv a^2\equiv 0 \pmod 4$. This implies $2\mid a,b,c$, which contradicts the fact (a,b,c) is a normalized solution. □

Since we are focusing our attention on the case when $-D\equiv 2,3 \pmod 4$, by Lemma 3.1 we are only concerned with normalized solutions (a,b,c) when c is odd.

The next result determines when $x^2+Dy^2=z^2$ has a normalized solution for fixed z. In all arguments below $\left(\frac{a}{p}\right)$ represents the Legendre symbol; it is 1 if a is a non-zero square modulo p, 0 if a is congruent to zero modulo p, and -1 otherwise.

The following lemma will be important for determining when a normalized solution to (3.1) exists.

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

Lemma 3.2. *Suppose $C(-4D) \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some $n \geq 0$ such that $-D = 2,3 \pmod 4$. Let $c = p_1^{n_1} \cdots p_k^{n_k}$ be an odd positive integer. There exists a normalized solution (a,b,c) to $x^2 + Dy^2 = z^2$ if and only if $\left(\frac{-D}{p_i}\right) = 1$ for $1 \leq i \leq k$.*

Proof. First suppose $\left(\frac{-D}{p_i}\right) = 1$ for all $1 \leq i \leq k$. Fix some prime p_i and consider the polynomial $f(x) = x^2 + D$. Since $-D$ is a non-zero quadratic residue modulo p_i, there exists $r \in \mathbb{Z}$ which is a simple root of $f(x) = x^2 + D \pmod{p_i}$. By Hensel's lemma, there exists $\tilde{r} \in \mathbb{Z}$ which is a simple root of $f(x) = x^2 + D \pmod{p_i^{n_i}}$. Thus $-D$ is a quadratic residue modulo $p_i^{n_i}$.

Since $-D$ is a quadratic residue modulo $p_i^{n_i}$ for each i, by applying the Chinese remainder theorem, we have that $-4D$ is a quadratic residue modulo c. Then by Lemma 2.5 of [Cox], c is properly represented by a primitive form f of discriminant $-4D$. Now if we apply Lemma 2.3 of [Cox], we get $f \sim [c, \alpha, \beta]$ for some integers α, β.

Note that $\alpha^2 - 4c\beta = -4D$. Suppose for contradiction that $(\alpha, c) > 1$. Then this implies that $(\alpha, c) | c$ and $(\alpha, c) | D$. However, since $\left(\frac{-D}{p_i}\right) = 1$ for all $i \leq k$, c and D are co-prime. This is a contradiction, so $(\alpha, c) = 1$. Therefore, $(c, c, \alpha) = 1$, and hence the Dirichlet composition is well defined in this case, and we we have that $f^2 \sim [c^2, \alpha', \beta']$ for $\alpha', \beta' \in \mathbb{Z}$. This implies f^2 properly represents c^2, since $C(-4D) \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some n, so each element of $C(-4D)$ has order at most 2. Therefore, the class $[f]$ in $C(-4D)$ has order at most 2, so $[f]^2$ is the identity and hence $f^2 \sim [1,0,D]$. Thus, by the above, $[1,0,D] \sim [c^2, \alpha', \beta']$. From this, using Lemma 2.3 of [Cox] once again, we infer that $x^2 + Dy^2$ properly represents c^2. Therefore, there exists a normalized solution (a,b,c) to (3.1) for some $a, b \in \mathbb{Z}$. This completes the first implication.

Conversely, let (a,b,c) be a normalized solution to (3.1). First, suppose for contradiction that $(c, D) = h_0 > 1$. Then we have $h_0 | a^2$. Suppose $h_0 = q_1^{m_1} \cdots q_r^{m_r}$ for primes q_i. Define $h_1 := q_1 \cdots q_r$. This gives us $h_1 > 1$ and $h_1 \mid c$, $h_1 \mid h_0$, and $h_1 \mid a$. Therefore, $h_1^2 | a^2$ and $h_1^2 | c^2$. This implies that $h_1^2 \mid Db^2$ but h_1^2 does not divide D, because D is square free. Thus, h_1 divides b, and therefore $(a,b,c) > 1$, which is a contradiction. Hence $(c, D) = 1$.

Let p be a prime factor of c. We claim that $(b, p) = 1$. Suppose not. Then since $p \mid b$, and $p \mid c$ we get $p \mid a$. This contradicts the assumption that $(a,b,c) = 1$, and thus $(b, p) = 1$ as claimed. Thus $a^2 + Db^2 = c^2$ implies $a^2 + Db^2 \equiv 0 \pmod p$ which gives us $-D \equiv (ab^{-1})^2 \pmod p$ where b^{-1} is the inverse of b modulo p which exists as $(b, p) = 1$. So, $\left(\frac{-D}{p}\right) = 1$ for any prime factor p of c. □

3.2. ***Factorization of*** $G_D(\mathbb{Q})$***:*** In order to state and prove the theorems which provide a factorization of $G_D(\mathbb{Q})$, we will first need the following two lemmas.

Lemma 3.3. *For some odd prime p such that $\left(\frac{-D}{p_i}\right) = 1$, let $x_0^2 + Dy_0^2 = p^{2\alpha}$ where $(x_0, y_0) = 1$. Also assume $p^{2\alpha} | c^2 + Dd^2$ for some c, d such that $(c, d) = 1$. Then exactly one of the following is true:*

$$x_0 + y_0\sqrt{-D} \mid c + d\sqrt{-D} \tag{3.2}$$

or

$$x_0 - y_0\sqrt{-D} \mid c + d\sqrt{-D} \tag{3.3}$$

in $\mathbb{Z}[\sqrt{-D}]$.

Proof. First, we have $p^{2\alpha} \mid x_0^2 + Dy_0^2$, $p^{2\alpha} \mid c^2 + Dd^2$. Therefore, $p^{2\alpha} \mid x_0^2 d^2 - c^2 y_0^2$ which implies $p^{2\alpha} \mid (dx_0 + cy_0)(dx_0 - cy_0)$.

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

We claim that $p^{2\alpha}$ divides *exactly one* of dx_0+cy_0 and dx_0-cy_0. If not, and p divides both (dx_0+cy_0) and (dx_0-cy_0), then p divides $2dx_0$. Since p is odd, $p \mid dx_0$. If $p \mid d$ then $p \mid c$, which is a contradiction, while if $p \mid x_0$, then $p \mid Dy_0^2$. However, if $p \mid y_0$, then $(x_0,y_0) > 1$. Therefore, $p \mid D$, contradicting Lemma 3.2.

Therefore, $p^{2\alpha}$ divides *exactly one* of (dx_0+cy_0) and (dx_0-cy_0). Now let us look at these two cases separately.

Case 1: $p^{2\alpha} \mid (dx_0-cy_0)$**.** In this case we have

$$p^{4\alpha} \mid (x_0^2+Dy_0^2)(c^2+Dd^2) \;=\; (cx_0+Ddy_0)^2+D(dx_0-cy_0)^2, \tag{3.4}$$

and since $p^{4\alpha} \mid (dx_0-cy_0)^2$ by assumption, we get $p^{4\alpha} \mid (cx_0+Ddy_0)^2$. Therefore, $p^{2\alpha} \mid (cx_0+Ddy_0)$.

Consider the number $\alpha+\beta\sqrt{-D}$ where $\alpha = \frac{cx_0+Ddy_0}{p^{2\alpha}}$ and $\beta = \frac{dx_0-cy_0}{p^{2\alpha}}$. Note that

$$(\alpha+\beta\sqrt{-D})(x_0+y_0\sqrt{-D}) \;=\; (c+d\sqrt{-D}).$$

Therefore, $(x_0+y_0\sqrt{-D}) \mid (c+d\sqrt{-D})$ in $\mathbb{Z}[\sqrt{-D}]$.

Case 2: $p^{2\alpha} \mid (dx_0+cy_0)$**.** We proceed in a similar fashion and show that

$$(\gamma+\delta\sqrt{-D})(x_0-y_0\sqrt{-D}) \;=\; (c+d\sqrt{-D}), \tag{3.5}$$

where $\gamma = \frac{cx_0-Ddy_0}{p^{2\alpha}}$ and $\delta = \frac{dx_0+cy_0}{p^{2\alpha}}$. □

Lemma 3.4. *Let $D>1$ and p be an odd prime. Then there are unique co-prime integers x_0, y_0 such that $p^2 = x_0^2+Dy_0^2$.*

Proof. Let a,b,c,d be integers. We first want to show, if $a+b\sqrt{-D} \mid c+d\sqrt{-D}$ and $c+d\sqrt{-D} \mid a+b\sqrt{-D}$ in $\mathbb{Z}[\sqrt{-D}]$, then $c=\pm a$ and $b=\pm d$.

We can take $(\frac{a+b\sqrt{-D}}{c+d\sqrt{-D}}) = x+y\sqrt{-D}$ and $(\frac{c+d\sqrt{-D}}{a+b\sqrt{-D}}) = w+z\sqrt{-D}$. then we get $(x+y\sqrt{-D})(w+z\sqrt{-D}) = 1$. This implies $(x+y\sqrt{-D}),(w+z\sqrt{-D})$ are units, but the only units in $\mathbb{Z}[\sqrt{-D}]$ are ± 1. Therefore, we get $z=y=0$ and $x=\pm 1$, $w=\pm 1$. Therefore, $a=\pm b$ and $c=\pm d$.

Now suppose that $p^2 = x_0^2+Dy_0^2 = x_1^2+Dy_1^2$ such that $(x_0,y_0)=(x_1,y_1)=1$. This implies, by Lemma 3.2, that $\left(\frac{-D}{p}\right) = 1$. Then by Lemma 3.3 we have one of the following four cases:

(1) $x_0+y_0\sqrt{-D} \mid x_1+y_1\sqrt{-D}$ and $x_1+y_1\sqrt{-D} \mid x_0+y_0\sqrt{-D}$,
(2) $x_0+y_0\sqrt{-D} \mid x_1+y_1\sqrt{-D}$ and $x_1-y_1\sqrt{-D} \mid x_0+y_0\sqrt{-D}$,
(3) $x_0-y_0\sqrt{-D} \mid x_1+y_1\sqrt{-D}$ and $x_1+y_1\sqrt{-D} \mid x_0+y_0\sqrt{-D}$, or
(4) $x_0-y_0\sqrt{-D} \mid x_1+y_1\sqrt{-D}$ and $x_1-y_1\sqrt{-D} \mid x_0+y_0\sqrt{-D}$.

The proof of the lemma for Case (1) follows directly from the above argument. For Case (2), we have $x_0-y_0\sqrt{-D} \mid x_1-y_1\sqrt{-D} \mid x_0+y_0\sqrt{-D}$. Therefore, $x_0+y_0\sqrt{-D} | x_0-y_0\sqrt{-D}$ and $x_0-y_0\sqrt{-D} | x_0+y_0\sqrt{-D}$, so we get that $x_0=-x_0$ or $y_0=-y_0$, which implies $x_0=\pm p$, since x_0 cannot be 0. Case (3) is the same argument as Case (2). For Case (4) we have $x_0-y_0\sqrt{-D} \mid x_1+y_1\sqrt{-D}$ and $x_1+y_1\sqrt{-D} \mid x_0-y_0\sqrt{-D}$, so this case is equivalent to Case (1). □

Now, let us define the set

$$S_D \;:=\; \left\{\text{odd primes } q : \left(\frac{-D}{q}\right) = 1\right\}.$$

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

For each $q \in S_D$, we also define

$$\zeta_q := \frac{x_0 + y_0\sqrt{-D}}{q}, \tag{3.6}$$

where $q^2 = x_0^2 + Dy_0^2$ and $x_0, y_0 > 0$.

Note that x_0, y_0 exist due to Lemma 3.2 by the definition of the set S_D and they are unique by Lemma 3.4. These ζ_q's correspond to the *elementary solutions*. Our objective is to determine a bijective correspondence between the products of powers of ζ_q's and the set of normalized solutions of the form (a,b,c) for a given c. Here the primes q correspond to the prime factors of c.

Now we are ready to state and prove the first theorem.

Theorem 3.5. *Let $z = \frac{a+b\sqrt{-D}}{c} \in G_D(\mathbb{Q})$ where $(a,b) = 1$, $c > 1$. Let $c = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Then*

$$z = \pm\zeta_{p_1}^{\pm\alpha_1} \cdots \zeta_{p_k}^{\pm\alpha_k}. \tag{3.7}$$

Proof. Note that given such a z, we have $a^2 + Db^2 = c^2$ and thus (a,b,c) is a normalized solution to $x^2 + Dy^2 = z^2$. Thus according to Lemma 3.2, for all the prime factors q of c, $\left(\frac{-D}{q}\right) = 1$. Thus ζ_{p_i} is well defined.

Consider z as in the statement. Then

$$a^2 + Db^2 = c^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k}.$$

Note that each $p_i^2 = \gamma_i^2 + D\beta_i^2$ for some $\gamma_i, \beta_i \in \mathbb{Z}$ such that $(\gamma_i, \beta_i) = 1$. Therefore,

$$p_i^{2\alpha_i} = (\gamma_i^2 + D\beta_i^2)^{\alpha_i} = \left(\gamma_i + \beta_i\sqrt{-D}\right)^{\alpha_i}\left(\gamma_i - \beta_i\sqrt{-D}\right)^{\alpha_i} := (x_i + y_i\sqrt{-D})(x_i - y_i\sqrt{-D}) \tag{3.8}$$

for each i. Here we used the fact that product of numbers of the form $x^2 + Dy^2$ is again of the form $x^2 + Dy^2$ Thus for each i,

$$p_i^{2\alpha_i} = x_i^2 + Dy_i^2 \tag{3.9}$$

and $p_i^{2\alpha_i} \mid a^2 + Db^2$. Hence by Lemma 3.3, we have exactly one of the following:

$$x_i + y_i\sqrt{-D} \mid a + b\sqrt{-D} \Leftrightarrow x_i - y_i\sqrt{-D} \mid a - b\sqrt{-D} \tag{3.10}$$

or

$$x_i - y_i\sqrt{-D} \mid a + b\sqrt{-D} \Leftrightarrow x_i + y_i\sqrt{-D} \mid a - b\sqrt{-D}. \tag{3.11}$$

As

$$a^2 + Db^2 = c^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k},$$

we have

$$\begin{aligned}(a + b\sqrt{-D})(a - b\sqrt{-D}) = {} & (x_1 + y_1\sqrt{-D})(x_2 + y_2\sqrt{-D}) \cdots (x_k + y_k\sqrt{-D}) \\ & \cdot (x_1 - y_1\sqrt{-D})(x_2 - y_2\sqrt{-D}) \cdots (x_k - y_k\sqrt{-D}),\end{aligned} \tag{3.12}$$

which implies that

$$(a_1 + b_1\sqrt{-D})(a_1 - b_1\sqrt{-D}) = (x_2 + y_2\sqrt{-D}) \cdots (x_k + y_k\sqrt{-D}) \cdot (x_2 - y_2\sqrt{-D}) \cdots (x_k - y_k\sqrt{-D}) \tag{3.13}$$

where

$$a_1 + b_1\sqrt{-D} := \begin{cases} \frac{a+b\sqrt{-D}}{x_1+y_1\sqrt{-D}}, & \text{if } x_1 + y_1\sqrt{-D} \mid a + b\sqrt{-D} \\ \\ \frac{a+b\sqrt{-D}}{x_1-y_1\sqrt{-D}}, & \text{if } x_1 - y_1\sqrt{-D} \mid a + b\sqrt{-D}. \end{cases} \tag{3.14}$$

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

Also note that $a_1^2+Db_1^2 = p_2^{2\alpha_2}\cdots p_k^{2\alpha_k}$. If we continue this process inductively and keep defining subsequent terms $a_i+b_i\sqrt{-D}$ as above, at the final step we get the following

$$(a_k+b_k\sqrt{-D})(a_k-b_k\sqrt{-D}) \;=\; 1 \tag{3.15}$$

where $a_k, b_k \in \mathbb{Z}$. But that would mean $a_k = \pm 1, b_k = 0$. Thus,

$$(a+b\sqrt{-D}) \;=\; \pm 1\cdot(x_1\pm y_1\sqrt{-D})(x_2\pm y_2\sqrt{-D})\cdots(x_k\pm y_k\sqrt{-D}), \tag{3.16}$$

and dividing by c, we obtain

$$\frac{a+b\sqrt{-D}}{c} \;=\; \pm 1\cdot\frac{x_1\pm y_1\sqrt{-D}}{p_1^{\alpha_1}}\cdot\frac{x_2\pm y_2\sqrt{-D}}{p_2^{\alpha_2}}\cdots\frac{x_k\pm y_k\sqrt{-D}}{p_k^{\alpha_k}}. \tag{3.17}$$

Now note that

$$\zeta_{p_i}^{\pm\alpha_i} \;=\; \left(\frac{\gamma_i+\beta_i\sqrt{-D}}{p_i}\right)^{\pm\alpha_i} \;=\; \left(\frac{x_i\pm y_i\sqrt{-D}}{p_i^{\alpha_i}}\right). \tag{3.18}$$

□

3.3. ***Obtaining Solutions from Factorization.*** We explore consequences of being able to factor every element of $G_D(\mathbb{Q})$. Given a factorization of some $z \in G_D(\mathbb{Q})$, we determine c where (a,b,c) is the normalized solution to (3.1) corresponding to z.

We first prove a needed result.

Lemma 3.6. *Let* $z_1 = \frac{a_1+b_1\sqrt{-D}}{c_1} \in G_D(\mathbb{Q})$ *and* $z_2 = \frac{a_2+b_2\sqrt{-D}}{c_2} \in G_D(\mathbb{Q})$ *such that* $(a_1,b_1) = (a_2,b_2) = (c_1,c_2) = 1$. *Then*

$$(a_1a_2-Db_1b_2, a_1b_2+a_2b_1, c_1c_2) \tag{3.19}$$

is a normalized solution, and $a_1a_2-Db_1b_2$ *and* $a_1b_2+a_2b_1$ *are co-prime.*

Proof. It suffices to show that there are no common prime divisor of $a_1a_2-Db_1b_2$ and $a_1b_2+a_2b_1$. Assume for contradiction that there exists some prime q that divides them. We then have $q \mid a_1a_2-Db_1b_2$ and $q \mid a_1b_2+a_2b_1$, and

$$q \mid (-b_2)(a_1a_2-Db_1b_2)+(a_2)(a_1b_2+a_2b_1)$$

implies $q \mid b_1(a_2^2+Db_2^2)$. However if $q \mid b_1$ then $q \mid a_1a_2$ and $q \mid a_1b_2$. Since $(a_1,b_1) = 1$ and $q \mid b_1$, we have $q \nmid a_1$. Therefore, $q \mid a_2$ and $q \mid b_2$. This is a contradiction, and thus $q \mid (a_2^2+Db_2^2)$.

Also note that $q|(a_1)(a_1a_2-Db_1b_2)+(Db_1)(a_1b_2+a_2b_1) = a_2(a_1^2+Db_1^2)$ implies $q \mid a_2$, or $q \mid a_1^2+Db_1^2$. Now assume that $q \mid a_2$. Then $q \mid Db_1b_2$ and $q \mid a_1b_2$ which implies $q \mid a_1$, and we have $q \nmid b_2$. Suppose for contradiction that $q \mid D$. Then $q \mid a_2^2+Db_2^2 = c_2^2$ and since q is a prime, $q^2 \mid c_2^2$ implies $q^2 \mid Db_2^2$ which yields $q^2 \mid D$ as $q \nmid b_2$. This contradicts that D is square-free.

Thus $q \mid a_2$ implies $q \mid b_1$ and $q \mid a_1$, which contradicts that $(a_2,b_2) = 1$. Therefore $q \nmid a_2$ implies $q \mid a_1^2+Db_2^2$, and q is a common divisor of c_1 and c_2, which is a contradiction.

Hence there cannot be a common prime factor of $a_1a_2-Db_1b_2$ and $a_1b_2+a_2b_1$. □

Remark 3.7. *Note that this proof does not depend on the fact that the class group is a* $\mathbb{Z}/2\mathbb{Z}$ *module. So, given two normalized solutions* (a,b,c) *and* (a',b',c') *such that* $(c,c') = 1$, *one can multiply them together to get a new normalized solution of the form* (x,y,cc').

We now state the theorem that retrieves solutions from the factorization of an element in $G_D(\mathbb{Q})$.

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

Theorem 3.8. *For some $z \in G_D(\mathbb{Q})$ let $z = \pm\zeta_{p_1}^{\pm\alpha_1} \cdots \zeta_{p_k}^{\pm\alpha_k}$ where $\left(\frac{-D}{p_i}\right) = 1$ for all i. Then if z corresponds to the normalized triple (a,b,c), we must have $c = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.*

Proof. By definition of $G_D(\mathbb{Q})$, z corresponds to the normalized triple (a,b,c) if and only if $z = \frac{a+b\sqrt{-D}}{c}$ where $(a,b) = 1$, so we write $z = \frac{a+b\sqrt{-D}}{c}$ where $(a,b) = 1$. Due to Lemma 3.2, for each p_i, we have $\zeta_{p_i}^{\pm\alpha_i} = \frac{a_i + b_i\sqrt{-D}}{p_i^{\alpha_i}}$ where $(a_i,b_i) = 1$, since we can write $p_i^{2\alpha_i} = a_i^2 + Db_i^2$ where $(a_i,b_i) = 1$. By Lemma 3.6, $\pm\zeta_{p_1}^{\pm\alpha_1} \cdot \zeta_{p_2}^{\pm\alpha_2} \cdots \zeta_{p_k}^{\pm\alpha_k}$ corresponds to a normalized solution of the form $(\alpha, \beta, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})$, z already corresponds to the normalized solution (a,b,c) and we know that an element of $G_D(\mathbb{Q})$ can correspond to just one normalized solution. So we must have $c = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. □

We have now proved two of our main results. First, Theorem 3.5, which factorizes elements of $G_D(\mathbb{Q})$, and second, Theorem 3.8, which retrieves normalized solutions from the factorization of an element of $G_D(\mathbb{Q})$. Using these tools we can enumerate the number of normalized solution of the form (a,b,c) for a given c.

4. Cardinality of Rational Solutions

Theorem 4.1. *Suppose that $-D \equiv 2,3 \pmod 4$, $D > 1$ and $c = p_1^{n_1} \cdots p_k^{n_k}$. Then there is a normalized solution to (1.8) of the form (a,b,c) if and only if all the $p_i \in S$. Further, if all the $p_i \in S_D$, we have exactly 2^{k-1} normalized solutions to (1.8) of the form (a,b,c).*

Proof. The first statement is proven by Lemma 3.2. Let us fix $c = p_1^{n_1} \cdots p_n^{n_k}$ such that $\left(\frac{-D}{p_i}\right) = 1$ for $1 \le i \le k$ and represent the solutions to $a^2 + Db^2 = c^2$ as $\frac{a+b\sqrt{-D}}{c}$. Define the sets

$$T_1 := \left\{ \frac{a+b\sqrt{-D}}{c} : a^2 + Db^2 = c^2, (a,b) = 1, c > 1 \right\}$$

and

$$T_2 := \left\{ \pm\zeta_{p_1}^{\varepsilon_1 n_1} \cdots \zeta_{p_k}^{\varepsilon_k n_k} : \varepsilon_i \in \{\pm 1\} \right\}.$$

By Theorem 3.5, we have $T_1 \subset T_2$ and, by Theorem 3.8, we get $T_2 \subset T_1$. Now for every solution (a,b) to $x^2 + Dy^2 = c^2$, we can find other solutions by negating $z = \frac{a+b\sqrt{-D}}{c}$ or by taking the complex conjugate of c. Therefore, for every (a,b) there are four distinct solutions corresponding to the integers a and b. They are $\frac{a+b\sqrt{-D}}{c}$, $\frac{-a+b\sqrt{-D}}{c}$, $\frac{a-b\sqrt{-D}}{c}$, and $\frac{-a-b\sqrt{-D}}{c}$. If Γ is the abelian group of order 4 generated by multiplication by -1 and complex conjugation that acts on $G_D(\mathbb{Q})$, then the four solutions corresponding to the integers a,b is the orbit of $\frac{a+b\sqrt{-D}}{c}$ under the action of Γ. Therefore, the normalized solutions to $x^2 + Dy^2 = c^2$ give a system of unique representatives for T_1/Γ.

As complex conjugation on an element $z \in T_2$ corresponds to the map $\varepsilon_i \to -\varepsilon_i$, we get

$$T_2/\Gamma = \left\{ \zeta_{p_1}^{n_1} \zeta_{p_2}^{\varepsilon_2 n_2} \cdots \zeta_{p_k}^{\varepsilon_k n_k} : \varepsilon_i \in \{\pm 1\} \right\}. \tag{4.1}$$

Since $T_2/\Gamma = T_1/\Gamma$, we have that the set of normalized solutions give a system of unique representatives for T_2/Γ. Therefore, since there are $k-1$ numbers ε_i with two choices for each, we obtain $|T_2/\Gamma| = 2^{k-1}$. □

Remark 4.2. *While the theorems above are stated and proved for $-D \equiv 2,3 \pmod 4$, we can generalize them to $-D \equiv 1 \pmod 4$ as well. In that case all of these theorems remain valid only when c is odd, because when $-D \equiv 1 \pmod 4$, there could exist normalized solutions of the form (a,b,c) where c is even, which cannot happen when $-D \equiv 2,3 \pmod 4$ (see Lemma 3.1).*

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

Remark 4.3. *For the case when $D = 1$, the argument must be modified, because in this case the group of units of $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$. Also for a solution (a,b,c) to $x^2 + Dy^2 = z^2$ to be normalized when $D = 1$, there is the added condition that $a < b$. This is necessary, because if (a,b,c) is a solution then so is (b,a,c). The following proofs must be changed to account for these differences.*

Lemma 3.4 does not hold in this case, because it relies on the fact that the group of units of $\mathbb{Z}[\sqrt{-D}]$ is $\{\pm 1\}$. We use this lemma to prove that our definition of ζ_p is well defined. We can rectify this problem by defining ζ_p in the same way as [Ye]. That is, for a prime p such that $\left(\frac{-1}{p}\right) = 1$, $p = m^2 + n^2$ for $m, n \in \mathbb{Z}$. Because p is odd, we have $|m| \neq |n|$. Therefore, we can assume $0 < m < n$. We can then define $q = m + ni$ and $\zeta_p = \frac{q}{\overline{q}}$ where $\overline{q}$ is the complex conjugate of q. Theorem 3.5 and Theorem 3.8 also rely on the fact that the group of units is $\{\pm 1\}$. If we change the group of units to be $\{\pm 1, \pm i\}$, then the arguments will hold if we change $z = \pm \zeta_{p_1}^{\pm \alpha_1} \cdots \zeta_{p_k}^{\pm \alpha_k}$ to $z = \pm i^r \zeta_{p_1}^{\pm \alpha_1} \cdots \zeta_{p_k}^{\pm \alpha_k}$ where $r \in \{0,1\}$. Therefore, we will still have the factorization $G_1(\mathbb{Q}) = U \times F$ where U is the group of units of $\mathbb{Z}[i]$ and F is the free abelian group with generators $\{\zeta_p\}$. Finally, Theorem 4.1 will change as follows. Given a solution (a,b,c) we have 8 distinct solutions corresponding to the integers a, b. That is if we can multiply $\frac{a+bi}{c}$ by ± 1, $\pm i$ or take complex conjugation to get another distinct solution. Therefore, we define Γ to be the group generated by multiplication of -1, i and complex conjugation. We also define

$$T_2 := \left\{ \pm i^r \zeta_{p_1}^{\varepsilon_1 n_1} \cdots \zeta_{p_k}^{\varepsilon_k n_k} : \varepsilon_i \in \{\pm 1\}, r \in \{0,1\} \right\}.$$

With these changes, the same argument will give us the result of Theorem 4.1.

5. Examples and Future Work

5.1. ***Examples.*** We give a few examples of our results.

- Theorem 4.1 holds when the class group $C(-4D)$ has order ≤ 2 and $-D \equiv 2, 3 \bmod 4$. This only occurs when $D = 1,\ 2,\ 5,\ 6,\ 10,\ 13,\ 22,\ 37,\ 58$.

- For our results to be true, we need the class group to be a $\mathbb{Z}/2\mathbb{Z}$ module. Otherwise Theorem 4.1 might not be true. For example take $D = 26$ and $c = 5$. One can prove that the class group $C(-104)$ is not a $\mathbb{Z}/2\mathbb{Z}$ module. Also,

$$\left(\frac{-26}{5}\right) = 1,$$

  but $x^2 + 26y^2 = 5^2$ has no normalized solution.

5.2. ***Future Work.*** Here are some possible avenues for extending the work of this paper.

- This paper does not have full results for the case $-D \equiv 1 \pmod 4$. As stated in Remark 4.2, the problem with this case is that for a normalized solution (a,b,c), c can be even. Many of our results rely on the fact that certain primes are odd. What can be said about the solutions to $x^2 + Dy^2 = c^2$ when c is even?

- Another restriction in this paper for the results to hold is that $C(-4D) \cong (\mathbb{Z}/2\mathbb{Z})^n$. This is necessary in our method, because we use that every element of $C(-4D)$ has order at most 2 when determining if there exists a normalized solution (a,b,c) for a given c. With more advanced tools

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.

is there a way to extend these results for a broader range of integers D?

- What can be said about other Diophantine equations? Can we count the number of normalized solutions to $x^2+y^2+z^2=w^2$, or even more generally $x^2+D_1y^2+D_2z^2=w^2$ for example? For $x_1^2+x_2^2+x_3^2+x_4^2=z^2$ what are the consequences of the multiplicativity of the quaternion norm?

References

[Cox] D. A. Cox, *Primes of the form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, second edition, 2013. Available at: http://www.math.toronto.edu/~ila/Cox-Primes_of_the_form_x2+ny2.pdf.

[Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[Maz1] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

[Maz2] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Met] T. Metsänkylä, *Catalan's Conjecture: Another Old Diophantine Problem Solved*, Bull. Amer. Math. Soc. **41** (2003), 43–57.

[Mih1] P. Mihailescu, *A Class Number Free Criterion for Catalan's Conjecture*, J. Number Th. **99** (2003), 225–231.

[Mih2] P. Mihailescu, *Primary Cyclotomic Units and a Proof of Catalan's Conjecture*, J. reine angew. Math. **572** (2004), 167–195.

[MT-B] S. J. Miller and R. Takloo-Bighash, *An Invitation to Modern Number Theory*, Princeton University Press, 2006.

[PPVW] J. Park, B. Poonen, J. Voight, and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903.

[Si] J. Silverman, *An Introduction to the Theory of Elliptic Curves*, to appear in the Summer School on *Computational Number Theory and Applications to Cryptography* at University of Wyoming in July 2006. https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf.

[ST] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.

[Wa] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907–938.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443–551.

[Ye] A. Yekutieli, *Pythagorean Triples, Complex Numbers, Abelian Groups and Prime Numbers*, to appear in the American Mathematical Monthly (2021), https://arxiv.org/pdf/2101.12166.pdf.

Email address: gvs3ka@virginia.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIRGINIA, CHARLOTTESVILLE, VA 22903

Email address: tmartinez@math.ucla.edu

DEPARTMENT OF MATHEMATICS, UC LOS ANGELES, LOS ANGELES, CA 90095

Email address: sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

Email address: mukhe136@umn.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MINNESOTA, TWIN CITIES, MN 55455

8 Jul 2023 08:00:12 PDT
220602-Miller Version 3 - Submitted to Rocky Mountain J. Math.