CLASS NUMBERS AND PELL’S EQUATION $x^2 + 105y^2 = z^2$

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. In [JMMM] we generalized 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 free $\mathbb{Z}_2$ module, which always happens if the class number is at most 2. In this paper we discuss the main results of [JMMM] using some concrete examples in the case of $D = 105$.

CONTENTS

1. Introduction 1
   1.1. Background 1
   1.2. Results of Yekutieli 4
   1.3. Main results Jaklitsch et. al. 5

2. Proof of the Main Results 7

References 14

1. INTRODUCTION

1.1. Background. A Diophantine equation is a polynomial of finite degree with integer coefficients, where we often are interested in the integer or rational solutions. These problems have fascinated mathematicians for millenia. Perhaps the most famous equation and solutions are the Pythagorean triples, triples of integers $(a, b, c)$ that satisfy

$$f(x, y, z) = x^2 + y^2 - z^2 = 0.$$  

(1.1)

These triples can be represented in multiple forms, and a particularly useful one is to convert to points on the unit circle: $(a/c, b/c)$.

In studying Diophantine equations, there are several natural questions.

Date: April 1, 2022.
2020 Mathematics Subject Classification. 11D09, 11R29.
Key words and phrases. Class numbers, Pythagorean Triples, Pell Equation, Diophantine Equations, Group Structure.

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.
• Are there any solutions? Answering this is often non-trivial, as the analysis of Fermat’s Last Theorem showed: If \(x, y, z\) are positive integers then there are no solutions to \(x^n + y^n = z^n\) if \(n\) is an integer at least three, see [TW, Wi]. Related problems, such as the Beal conjecture \((x^a + y^b = z^c\) with certain constraints) are still open.

• If there are solutions, are there finitely many or infinitely many? For example, Mihăilescu [Mef, Mih1, Mih2] proved Catalan’s Conjecture: the only two consecutive positive powers are 8 and 9, explicitly, if \(x, y > 0\) and \(a, b > 1\) then the only integer solution to \(x^a - y^b = 1\) is \(3^2 - 2^3 = 1\).

• If there are infinitely many solutions, is it possible to parameterize them, and if so is there a structure on the set of solutions?

The answers to these questions are well-known for Pythagorean triples. We can generate all solutions by utilizing Euclid’s formula: \(a = m^2 - n^2, b = 2mn, c = m^2 + n^2\). A common way to find this parameterization is shown in Figure 1. We start with one known solution to the corresponding problem on the unit circle: \((-1)^2 + 0^2 = 1\). Given any rational pair \((x, y)\) on the unit circle, the slope of the line from \((-1, 0)\) to \((x, y)\) is rational, and conversely given any line with rational slope emanating from \((-1, 0)\) it intersects the unit circle at a rational point, see for example [MT-B] for details.

![Figure 1. A rational parametrization of the circle \(x^2 + y^2 = 1\).](image)

What can we say about the structure of the solutions to the Pythagorean equation? It is trivial to see that given a solution \((a, b, c)\) we can multiply each component by any integer \(k > 1\) to obtain a new solution, we thus call triples that are relatively prime primitive solutions. Are there other ways to generate new solutions from existing ones?

The answer is yes, and the motivation comes from an important generalization: elliptic curves (see [Kn, Si, ST]). An elliptic curve in standard (or Weierstrass) form is the set of points \((x, y)\) satisfying the cubic equation
\[
y^2 = x^3 + ax + b,
\]

where \(a, b \in \mathbb{Q}\) and the discriminant \(4a^3 + 27b^2\) is not zero (we need the discriminant to be non-zero to avoid degenerate cases such as lines and parabolas). Mordell proved that the set of rational points forms a group, and the points of infinite order are isomorphic to \(r\) copies of \(\mathbb{Z}\).
Theorem 1.1 (Mordell’s theorem). Let $E(\mathbb{Q})$ be the set of rational points on an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group of the form $\mathbb{Z}^r \oplus \mathbb{T}$, where $r$ is the geometric rank and $\mathbb{T}$ is a finite set of points of finite order.\footnote{Mazur [Maz1, Maz2] proved that there are only 15 possibilities for $\mathbb{T}$: $\mathbb{Z}/NZ$ for $N \in \{1, \ldots, 10, 12\}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}/2NZ$ with $N \in \{1, \ldots, 4\}$. The possible values of the rank are still a mystery. In 1938, Billing found an elliptic curve with rank 3. The largest known rank increased slowly over the years, with the current record due to Elkies in 2006, and is rank at least 28 (see [Du] for a more comprehensive historical data on elliptic curve records). While originally it was conjectured that the rank can be arbitrarily large, now some models (see [PPVW]) suggest that there may only be finitely many curves with rank exceeding 28.}

We demonstrate the group law on the set of rational solutions of an elliptic curve in Figure 2. Thus given two points with rational coordinates, or even taking the same point twice, we can generate additional rational solutions.

Building on this success for elliptic curves, we revisit Pythagorean triples and see there is a similar structure. An excellent account of this was done recently by Yekutieli [Ye], who sets out a framework amenable to generalization by presenting Pythagorean triples as complex numbers. Thus operations on complex numbers (multiplication, complex conjugation) provide ways of creating new, different solutions from existing ones.

Explicitly, given a Pythagorean triple $(a, b, c)$ we associate the complex number

$$\zeta_{a,b,c} = x + iy = \frac{a}{c} + \frac{b}{c}i.$$  \hfill (1.3)

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 $\zeta$ where both $a$ and $b$ are non-zero. We cannot have $a = b$, as that would lead to $\sqrt{2}$ being rational.\footnote{We would have $2a^2 = c^2$ and thus $\sqrt{2} = c/a \in \mathbb{Q}$.} A straightforward calculation shows that given such a solution $\zeta$ there are 7 other distinct conjugate solutions, we can multiply $\zeta$ by $i, i^2$ and $i^3$ (the units of $\mathbb{Z}[i]$ other than 1) and then we can take the complex conjugates of these four solutions. We illustrate this in Figure 3 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).

Identifying Pythagorean triples with complex numbers yields a commutative group (if $z$ and $w$ are two complex numbers on the unit circle, the multiplicativity of the norm immediately implies
Figure 3. The four trivial solutions \((1, i, -1, -i)\) and the seven conjugates to a non-trivial solution \(\zeta\), which can be taken to lie in the second octant. Image from [Ye].

\(zw\) is also of norm 1 and hence on the unit circle). While rescaling a Pythagorean triple by \(k\) does not change the complex number associated to it, multiplying the associated complex numbers generates new solutions. For example, the triple \((3, 4, 5)\) yields \(\zeta_{3,4,5} = 3/5 + i4/5\), and

\[
\zeta_{3,4,5}^2 = \left(\frac{3}{4} + \frac{4}{5}i\right) \left(\frac{3}{4} + \frac{4}{5}i\right) = -\frac{7}{25} + \frac{24}{25}i, \quad (1.4)
\]

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

\[
\zeta_{3,4,5} \cdot \zeta_{5,12,13} = \left(\frac{3}{5} + \frac{4}{5}i\right) \left(\frac{5}{13} + \frac{12}{13}i\right) = -\frac{33}{65} + \frac{56}{65}i, \quad (1.5)
\]

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

1.2. Results of Yekutieli. Yekutieli [Ye] proved several results about the structure of the group of rational solutions to the unit circle version of the Pythagorean equation. We are interested in the structure of positive integral solutions to the Diophantine equation

\[
x^2 + y^2 = z^2. \quad (1.6)
\]

To understand the main objective of [Ye] first we need to introduce the normalized solutions.

**Definition 1.2.** A solution \((x_0, y_0, z_0)\) to (1.6) is defined to be normalized if \(\gcd(x_0, y_0, z_0) = 1\) and \(x_0 \leq y_0\).
Now, the main objective of [Ye] is to find the number of normalized solutions\(^3\) to (1.6) of the form \((a, b, c)\) for a given positive integer \(c\).

In order to find the above, first he observed that every normalized solution \((a, b, c)\) to (1.6) can be encoded as the rational coordinate point \(\zeta := \frac{a}{\sqrt{c}} + \frac{b}{c}i\) on the 2nd octant of the unit circle and vice-versa. Thus rational coordinate points on the 2nd octant of the unit circle is bijective to the set of normalized solution. Also, one can observe that up to sign the eight points (see\(^5\))

\[
\pm \zeta, \pm i\zeta, \pm i^2\zeta
\]

also correspond to the normalized solution \((a, b, c)\). Thus Yekutieli established a surjection, defined as \(pt\) from the set of rational coordinate points on unit circle onto the set of normalized solutions to (1.6), by which he sends a rational coordinate point on the unit circle to the corresponding normalized solution, for example each of the above 8 points are mapped to \((a, b, c)\) via \(pt\). So it is sufficient to focus on the rational coordinate points on the unit circle.

Next, Yekutieli considered the rational coordinate points on the unit circle algebraically as \(G(Q)\), where

\[
G(Q) := \{a + ib: a, b \in Q, a^2 + b^2 = 1\}.
\]

Note that \(G(Q)\) is a group under complex multiplication. Yekutieli went one step further by proving that \(G(Q) = U \times F\) where \(U := \{1, -1, i, -i\}\) and \(F\) is a free group generated by \(\zeta_p\)\(^4\)

\[
\{\zeta_p := \frac{x_0 + y_0\sqrt{-1}}{x_0 - y_0\sqrt{-1}}: \text{where } p \equiv 1 \pmod{4} \text{ and } x_0^2 + y_0^2 = p^2, x_0, y_0 > 0\}\.
\]

Thus we obtain a factorization of each of the elements of \(G(Q)\). Using this factorization he proved the main result of his paper.

**Theorem 1.3** (Theorem 5.3 of [Ye]). Let \(c > 1\) have prime factorization in \(\mathbb{Z}\) as follows:

\[
c = p_1^{n_1}p_2^{n_2} \cdots p_k^{n_k}
\]

where the \(p_i\)'s are distinct primes and the \(n_i\)'s are positive integers.

1. If \(p_i \equiv 1 \pmod{4}\) for all \(i\), then the function \(pt\) restricts to a bijection

\[
pt: \{\zeta_{p_1}^{n_1}\zeta_{p_2}^{n_2} \cdots \zeta_{p_k}^{n_k}\} \to PT_c,
\]

where \(PT_c\) denotes the set of normalized solution of the form \((a, b, c)\). Thus there are \(2^{k-1}\) distinct normalized solutions of the form \((a, b, c)\).

2. If \(p_i \not\equiv 1 \pmod{4}\) for some \(i\) then \(PT_c\) is empty i.e., there is no normalized solution of the form \((a, b, c)\).

1.3. **Main results** Jaklitsch et. al. In [JMMM] we generalized the approach of Yekutieli to inspect the structure of integral solutions to

\[
x^2 + Dy^2 = z^2
\]

for \(D > 1\). The goal is the same as that of [Ye], i.e., finding the number of normalized solutions to (1.7) of the form \((a, b, c)\) for a given positive integer \(c\). However, we had to update the definition of normalized solutions for \(D > 1\).

\(^3\)Note that given any solution \((x_0, y_0, z_0)\) to (1.6) we can generate infinitely many solutions out of this particular solutions, for example \((dx_0, dy_0, dz_0), (ey_0, ex_0, ez_0)\) for any arbitrary integer \(d\) and \(e\). Thus by introducing this notion of normalized solution we are just considering the non-trivial generators of the solution space of (1.6).

\(^4\)Note that such \(x_0\) and \(y_0\) always exist for every prime \(p\) satisfying \(p \equiv 1\pmod{4}\). In fact this choice of \(x_0\) and \(y_0\) is unique.
Definition 1.4. A solution \((x_0, y_0, z_0)\) to (1.7) is defined to be normalized if \(\gcd(x_0, y_0, z_0) = 1\).

Note that this definition is slightly different that Definition 1.2 as in case of \(D > 1\) if we swap \((x_0, y_0, z_0)\) to \((y_0, x_0, z_0)\) then it will no longer be a solution to (1.7).

In order to achieve our goal, we generalized the arguments of Yekutieli and focused on rational coordinate points on the ellipse \(x^2 + Dy^2 = 1\), which we can algebraically visualise as the following:

\[ G_D(\mathbb{Q}) := \{ a + b\sqrt{-D} : a, b \in \mathbb{Q} \text{ and } a^2 + Db^2 = 1 \}. \]

Note that this is also a group under the complex multiplication. One of the most important result of our paper is proving that \(G_D(\mathbb{Q}) = U \times F\) where \(U = \{1, -1\}\) and \(F\) is a free group generated over the following set\(^5\):

\[
\left\{ \zeta_p := \frac{x_0 + y_0\sqrt{-D}}{p} ; \text{ where } \left( \frac{-D}{p} \right) = 1 \text{ and } x_0^2 + Dy_0^2 = p^2, x_0, y_0 > 0 \right\}
\]

however we had to impose an extra condition of the class group \(C(-4D)\) being a free \(\mathbb{Z}_2\)-module.

If we assume this extra condition, then due to Lemmas 3.3, 3.4 and 3.5 of [JMMM], such \(\zeta_p\)'s are well defined. We provide the statement of Lemma 3.5 of [JMMM], which uses Lemmas 3.3 and 3.4 of [JMMM] and gives us that the \(\zeta_p\)'s are well defined.

Lemma 1.5 (Lemma 3.5 of [JMMM]). Let \(p\) be an odd prime. Then the equation \(x^2 + Dy^2 = z^2\) has a unique normalized solution of the form \((a, b, p)\).

Using Theorem 3.6 and Theorem 3.9 of [JMMM], we proved that \(G_D(\mathbb{Q}) = U \times F\). We now state these important theorems.

Theorem 1.6 (Theorem 3.6 of [JMMM]). 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

\[ z = \pm \zeta_{p_1}^{\pm \alpha_1} \cdots \zeta_{p_k}^{\pm \alpha_k}. \]

Theorem 1.7 (Theorem 3.9 of [JMMM]). 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 \(c = p_1^{\alpha_1} \cdots p_k^{\alpha_k}\).

Using these results we proved Theorem 4.1 of [JMMM] which states the following and was the main result of that work.

Theorem 1.8 (Theorem 4.1 of [JMMM]). Given an integer \(c > 0\) with prime factorization \(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\) there are normalized solution of the form \((a, b, c)\) if and only if \(\left( \frac{-D}{p_i} \right) = 1\) for all \(i \leq k\). In fact if \(\left( \frac{-D}{p_i} \right) = 1\) for all \(i \leq k\) then there are exactly \(2^{k-1}\) normalized solutions to (1.7) of the form \((a, b, c)\).

Let \(\Gamma\) be the abelian group of order 4 generated by multiplication by \(-1\) and complex conjugation. In order to prove this theorem, we defined the sets

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

\(^5\)Note the similarity of this result with the Mordell-Weil theorem for elliptic curves.
and
\[ T_2 := \{ \pm \zeta_{p_1}^{\epsilon_1 n_1} \zeta_{p_2}^{\epsilon_2 n_2} \cdots \zeta_{p_k}^{\epsilon_k n_k} : \epsilon_i \in \{ \pm 1 \} \}. \] (1.8)

Then we exhibited a bijection between \( T_1 \) and
\[ T_2/\Gamma = \{ \zeta_{p_1}^{n_1} \zeta_{p_2}^{n_2} \cdots \zeta_{p_k}^{n_k} : \epsilon_i \in \{ \pm 1 \} \} \] (1.9)
where \( \Gamma \) is the abelian group of order 4 generated by complex conjugation and multiplication by \(-1\). Note that \( T_2/\Gamma \) has \( 2^{k-1} \) many elements which explains why there are \( 2^{k-1} \) many normalized solutions. However, proving these similar results for \( D > 1 \) was more difficult than the \( D = 1 \) case when \( D = 1 \), Yekutieli heavily relied on the fact that \( \mathbb{Z}[\sqrt{-1}] \) is a PID, which can fail for \( \mathbb{Z}[\sqrt{-D}] \) where \( D > 1 \). That is why we had to impose the extra condition of the class group \( C(-4D) \) being a free \( \mathbb{Z}_2 \)-module.

In this survey article we fix a value of \( D \), and verify the main results of [JMMM] and compute everything explicitly to highlight the key ideas of the method. We choose \( D = 105 \) so that the class group becomes \( C(-420) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \). We then choose certain values of \( c \) and verify Theorem 3.6, Theorem 3.9, and particularly, Theorem 4.1 by explicitly finding the normalized solutions of the form \((a, b, c)\).

2. Proof of the Main Results

We provide examples to illustrate the theory we developed in [JMMM]. Recall Pell’s equation
\[ x^2 + Dy^2 = z^2. \] (2.1)
We are interested in positive integral solutions of this equation. Let us choose \( D = 105 \). We state and prove the following claims.

**Claim 2.1.** The class represented by the reduced form \( ax^2 + bxy + cy^2 \) has order \( \leq 2 \) in the group \( C(-4D) \) if and only if \( b = 0 \), \( a = b \) or \( a = c \).

**Proof.** Recall that a primitive positive definite form \([a, b, c]\) is said to be reduced if \( |b| \leq a \leq c \) and \( b \geq 0 \) whenever \( |b| = a \) or \( a = c \). The proof of this claim is essentially Lemma 3.10 of [Cox]. \( \square \)

**Claim 2.2.** The class group of binary quadratic form with discriminant \(-4D = -420\) is isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \).

**Proof.** In order to prove this claim, we explicitly find the equivalence classes, i.e., elements of the class group \( C(-420) \). The equivalence classes are
\[
\begin{align*}
[1, 0, 105], [3, 0, 35], [5, 0, 21], [7, 0, 15], [2, 2, 53], [6, 6, 19], [11, 8, 11], [10, 10, 13]
\end{align*}
\]
where \([a, b, c]\) denotes the equivalence class represented by \([a, b, c]\). Note that each of these primitive forms are reduced and using Claim 2.1 we can infer that the all of the equivalence classes has order less than or equal to 2. To compute these elements of \( C(-420) \) we used a program which was based on the Algorithm 5.3.5 of [Cohen]. The proof of this algorithm’s correctness is in fact Lemma 5.3.4 of the same book. So the cardinality of the class group \( C(-420) \) is 8 and each element of this group has order \( \leq 2 \). Using the structure theorem of finite abelian groups, we infer that the class group \( C(-420) \) is indeed isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \). \( \square \)

We have that \( C(-420) \) is a free \( \mathbb{Z}_2 \)-module. Now, we choose five different values of \( c \) and for each of those values we exhibit the results we developed in our paper.
(1) $c = 11 \times 13$.
(2) $c = 13 \times 19$.
(3) $c = 11 \times 19$.
(4) $c = 11^2 \times 13^3$.
(5) $c = 11 \times 13 \times 19$.

Note that in each of the above choices of $c$, its prime factors are 11, 13 or 19, which satisfy $(\frac{-105}{11}) = (\frac{-105}{13}) = (\frac{-105}{19}) = 1$. By Lemma 3.3 of the [JMMM], for each such choices of $c$, we will attain normalized solutions of the form $(a, b, c)$. Note that

$$4^2 + 105 \cdot 1^2 = (11)^2,$$
$$8^2 + 105 \cdot 1^2 = (13)^2,$$
$$16^2 + 105 \cdot 1^2 = (19)^2.$$

Then we have

$$\zeta_{11} := \frac{4 + \sqrt{-105}}{11}, \quad \zeta_{13} := \frac{8 + \sqrt{-105}}{13}, \quad \zeta_{19} := \frac{16 + \sqrt{-105}}{19}.$$

Now, observe the following.

(1) By Theorem [1.8], we expect to have 2 normalized solutions. Since $11 \cdot 13$ has two prime factors, the theorem tells us we will have $2^1$ many normalized solutions. One can check that there are only two normalized solutions of the form $(a, b, c)$: $(73, 12, 11 \cdot 13)$ and $(137, 4, 11 \cdot 13)$. The solution $(73, 12, 11 \cdot 13)$ corresponds to $\frac{73 + 12\sqrt{-105}}{11 \cdot 13} \in G_D(\mathbb{Q})$ and $(137, 4, 11 \cdot 13)$ corresponds to $\frac{137 + 4\sqrt{-105}}{11 \cdot 13} \in G_D(\mathbb{Q})$ up to sign. Also, the following equalities hold:

$$\frac{-73 + 12\sqrt{-105}}{11 \cdot 13} = \zeta_{11}\zeta_{13},$$
$$\frac{137 - 4\sqrt{-105}}{11 \cdot 13} = \zeta_{11}^{-1}\zeta_{13},$$
$$\frac{137 + 4\sqrt{-105}}{11 \cdot 13} = \zeta_{11}\zeta_{13}^{-1},$$
$$\frac{-73 - 12\sqrt{-105}}{11 \cdot 13} = \zeta_{11}^{-1}\zeta_{13}^{-1}.$$

Each of the normalized solutions $(a, b, 11 \cdot 13)$ corresponds to an element of the form $\pm \zeta_{11}^{\pm1}\zeta_{13}^{\pm1}$ in $G_D(\mathbb{Q})$. However, since we are considering positive integral solutions only, there only 2 positive integral solutions to (2.1) where $D = 105$. This observation supports the claim of Theorem [1.8]. In the case of this example, the bijection between $T_2/\Gamma$ and the set of normalized solutions is as follows:

$$-\zeta_{11}^{-1}\zeta_{13}^{-1} \mapsto (73, 12, 11 \cdot 13),$$
$$\zeta_{11}\zeta_{13}^{-1} \mapsto (137, 4, 11 \cdot 13),$$

hence there are only 2 normalized solutions. We present the above information in the table below.
| Expected number of solutions | $2^1 = 2$ |
|------------------------------|------------|
| Actual solutions            | $(73, 12, 11 \cdot 13), (137, 4, 11 \cdot 13)$ |
| Solutions as elements of $G_D(\mathbb{Q})$ | $\frac{73+12\sqrt{-105}}{11 \cdot 13}, \frac{137+4\sqrt{-105}}{11 \cdot 13}$ |
| Factorization of elements   | $\frac{-73+12\sqrt{-105}}{11 \cdot 13} = \zeta_{11} \zeta_{13}$ |
|                             | $\frac{137-4\sqrt{-105}}{11 \cdot 13} = \zeta_{11}^{-1} \zeta_{13}$ |
|                             | $\frac{137+4\sqrt{-105}}{11 \cdot 13} = \zeta_{11} \zeta_{13}^{-1}$ |
|                             | $\frac{-73-12\sqrt{-105}}{11 \cdot 13} = \zeta_{11}^{-1} \zeta_{13}^{-1}$ |
| Bijection between $T_2/\Gamma$ and normalized solutions | $\frac{-\zeta_{11}}{\zeta_{11} \zeta_{13}^{-1}} \mapsto (73, 12, 11 \cdot 13)$ |
|                             | $\frac{\zeta_{11}}{\zeta_{11} \zeta_{13}^{-1}} \mapsto (137, 4, 11 \cdot 13)$ |

**Table 1.** $D = 11 \cdot 13$.

(2) Again, we have two prime factors, so [1.8] states that there should be 2 normalized solutions. The two normalized solutions of the form $(a, b, 13 \times 19)$ are $(23, 24, 13 \cdot 19)$ and $(233, 8, 13 \cdot 19)$. Writing these solutions as elements of $G_D(\mathbb{Q})$, we get $\frac{23+24\sqrt{-105}}{13 \cdot 19}$ and $\frac{233+8\sqrt{-105}}{13 \cdot 19}$. We can then represent the elements of $G_D(\mathbb{Q})$ as products of $\zeta_p$ terms:

$$\frac{23 + 24\sqrt{-105}}{13 \cdot 19} = \zeta_{13} \zeta_{19}$$

$$\frac{233 - 8\sqrt{-105}}{13 \cdot 19} = \zeta_{13}^{-1} \zeta_{19}$$

$$\frac{233 + 8\sqrt{-105}}{13 \cdot 19} = \zeta_{13} \zeta_{19}^{-1}$$

$$\frac{23 - 24\sqrt{-105}}{13 \cdot 19} = \zeta_{13}^{-1} \zeta_{19}^{-1}.$$

Therefore, each solution of (2.1) corresponds to an element of the form $\pm \zeta_{13} \pm \zeta_{19}$ in $G_D(\mathbb{Q})$. We only consider positive integral solutions, which correspond to the elements $\zeta_{13} \zeta_{19}$. Therefore, the bijection between $T_2/\Gamma$ and the set of normalized solutions is given by

$$\zeta_{13} \zeta_{19} \mapsto (23, 24, 13 \cdot 19)$$

$$\zeta_{13}^{-1} \zeta_{19}^{-1} \mapsto (233, 8, 13 \cdot 19).$$

(3) This example follows a very similar format to the two preceding it. We get 2 normalized solutions of the form $(a, b, 11 \times 19)$: $(41, 20, 11 \cdot 19)$ and $(169, 12, 11 \cdot 19)$, which is what [1.8] predicts. If we write these as solutions as elements of $G_D(\mathbb{Q})$ we get $\frac{41+20\sqrt{-105}}{11 \cdot 19}$. We write the factorization of solutions of the form $(a, b, 11 \times 19)$:

$$\frac{-41 + 20\sqrt{-105}}{11 \cdot 19} = \zeta_{11} \zeta_{19}.$$
| Expected number of solutions | $2^1 = 2$ |
| Actual solutions | $(23, 24, 13 \cdot 19), (233, 8, 13 \cdot 19)$ |
| Solutions as elements of $G_D(\mathbb{Q})$ | $\frac{23+24\sqrt{-105}}{13 \cdot 19}, \frac{233+8\sqrt{-105}}{13 \cdot 19}$ |
| Factorization of elements | $\frac{23+24\sqrt{-105}}{13 \cdot 19} = \zeta_{13} \zeta_{19}$, $\frac{233+8\sqrt{-105}}{13 \cdot 19} = \zeta_{13}^{-1} \zeta_{19}$ |
| Bijection between $T_2/\Gamma$ and normalized solutions | $\zeta_{13} \zeta_{19} \mapsto (23, 24, 13 \cdot 19)$, $\zeta_{13}^{-1} \zeta_{19} \mapsto (233, 8, 13 \cdot 19)$ |

Table 2. $D = 13 \cdot 19$.

| Expected number of solutions | $2^1 = 2$ |
| Actual solutions | $(41, 20, 11 \cdot 19), (169, 12, 11 \cdot 19)$ |
| Solutions as elements of $G_D(\mathbb{Q})$ | $\frac{41+20\sqrt{-105}}{11 \cdot 19}, \frac{169+12\sqrt{-105}}{11 \cdot 19}$ |
| Factorization of elements | $\frac{41+20\sqrt{-105}}{11 \cdot 19} = \zeta_{11} \zeta_{19}$, $\frac{169+12\sqrt{-105}}{11 \cdot 19} = \zeta_{11}^{-1} \zeta_{19}$ |
| Bijection between $T_2/\Gamma$ and normalized solutions | $\zeta_{11}^{-1} \zeta_{19}^{-1} \mapsto (41, 20, 11 \cdot 19)$, $\zeta_{11} \zeta_{19} \mapsto (169, 12, 11 \cdot 19)$ |

Table 3. $D = 11 \cdot 19$. 

\[
\begin{align*}
169 - 12\sqrt{-105} & = \zeta_{11}^{-1} \zeta_{19} \\
169 + 12\sqrt{-105} & = \zeta_{11} \zeta_{19}^{-1} \\
-41 - 20\sqrt{-105} & = \zeta_{11}^{-1} \zeta_{19}^{-1}.
\end{align*}
\] 

The positive solutions then correspond to the elements $\zeta_{13} \zeta_{19}$ and $\zeta_{13}^{-1} \zeta_{19}$, so the bijection between $T_2/\Gamma$ and the set of normalized solutions is given by

$\zeta_{11}^{-1} \zeta_{19}^{-1} \mapsto (41, 20, 11 \cdot 19)$, $\zeta_{11} \zeta_{19} \mapsto (169, 12, 11 \cdot 19)$. 

10
(4) In this example, the number \(11^2 \cdot 13^3\) still only has 2 distinct prime factors, so \([1.8]\) states that there will 2 normalized solutions of the form \((a, b, 11^2 \times 13^3)\). One can check that these solutions are \((251792, 8321, 11^2 \cdot 13^3)\) and \((105632, 23807, 11^2 \cdot 13^3)\). Writing these solutions as elements of \(G_D(\mathbb{Q})\) we get \(\frac{251792 + 8321\sqrt{-105}}{11^2 \cdot 13^3}\) and \(\frac{105632 + 23807\sqrt{-105}}{11^2 \cdot 13^3}\). We factor these elements into products of \(\zeta_p\) by:

\[
\frac{251792 + 8321\sqrt{-105}}{11^2 \cdot 13^3} = (\zeta_{11})^{-2} (\zeta_{13})^3
\]

\[
\frac{251792 - 8321\sqrt{-105}}{11^2 \cdot 13^3} = (\zeta_{11})^2 (\zeta_{13})^{-3}
\]

\[
\frac{105632 - 23807\sqrt{-105}}{11^2 \cdot 13^3} = (\zeta_{11})^2 (\zeta_{13})^3
\]

\[
\frac{105632 + 23807\sqrt{-105}}{11^2 \cdot 13^3} = (\zeta_{11})^{-2} (\zeta_{13})^{-3}.
\]

The positive normalized solutions are \(\frac{251792 + 8321\sqrt{-105}}{11^2 \cdot 13^3}\) and \(\frac{105632 + 23807\sqrt{-105}}{11^2 \cdot 13^3}\), which correspond to the elements \((\zeta_{11})^{-2} (\zeta_{13})^3\) and \((\zeta_{11})^{-2} (\zeta_{13})^{-3}\) respectively. Therefore, the bijection between \(T_2/\Gamma\) and the set of normalized solutions is as follows:

\[
(\zeta_{11})^{-2}(\zeta_{13})^3 \mapsto (251792, 8321, 11^213^3)
\]

\[
(\zeta_{11})^{-2}(\zeta_{13})^{-3} \mapsto (105632, 23807, 11^213^3).
\]

| Expected number of solutions | 2^1 = 2 |
|------------------------------|---------|
| Actual solutions            | (251792, 8321, 11^2 \cdot 13^3),
                            | (105632, 23807, 11^2 \cdot 13^3) |
| Solutions as elements of G_D(\mathbb{Q}) | \begin{align*}
\frac{251792 + 8321\sqrt{-105}}{11^2 \cdot 13^3},
\frac{105632 + 23807\sqrt{-105}}{11^2 \cdot 13^3}
\end{align*} |
| Factorization of elements   | \begin{align*}
\frac{251792 - 8321\sqrt{-105}}{11^2 \cdot 13^3} &= \zeta_{11}^2 \zeta_{13}^3 \\
\frac{105632 - 23807\sqrt{-105}}{11^2 \cdot 13^3} &= \zeta_{11}^{-2} \zeta_{13}^{-3}
\end{align*} |
| Bijection between T_2/\Gamma and normalized solutions | \begin{align*}
-\zeta_{11}^2 \zeta_{13}^3 &\mapsto (251792, 8321, 11^2 \cdot 13^3) \\
\zeta_{11}^{-2} \zeta_{13}^{-3} &\mapsto (105632, 23807, 11^2 \cdot 13^3)
\end{align*} |

**Table 4.** \(D = 11^2 \cdot 13^3\).
(5) This example differs from the previous ones, because there are 3 prime factors of $11 \cdot 13 \cdot 19$ rather than 2. Therefore, Theorem 1.8 states that there will be $2^2 = 4$ normalized solutions. One can check that these solutions are $(2612, 73, 11 \cdot 13 \cdot 19)$, $(2428, 119, 11 \cdot 13 \cdot 19)$, $(1772, 201, 11 \cdot 13 \cdot 19)$, and $(92, 265, 11 \cdot 13 \cdot 19)$. We factor these solutions, written as elements of $G_D(\mathbb{Q})$ as follows:

\[
\frac{-2428 + 119\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}\zeta_{13}\zeta_{19}, \quad \frac{2612 + 73\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}^{-1}\zeta_{13}\zeta_{19}
\]

\[
\frac{1772 + 201\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}\zeta_{13}^{-1}\zeta_{19}, \quad \frac{92 - 265\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}^{-1}\zeta_{13}^{-1}\zeta_{19}
\]

\[
\frac{92 + 265\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}\zeta_{13}^{-1}\zeta_{19}, \quad \frac{1772 - 201\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}^{-1}\zeta_{13}^{-1}\zeta_{19}
\]

\[
\frac{2612 - 73\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}\zeta_{13}^{-1}\zeta_{19}, \quad \frac{-2428 - 119\sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}^{-1}\zeta_{13}^{-1}\zeta_{19}^{-1}
\]

So, each of the normalized solutions of the form $(a, b, 11 \cdot 13 \cdot 19)$ corresponds to the elements of the form $\pm \zeta_{11}^{\pm 1}\zeta_{13}^{\pm 1}\zeta_{19}^{\pm 1}$ in $G_D(\mathbb{Q})$. The positive solutions are given by $\zeta_{11}\zeta_{13}\zeta_{19}$, $-\zeta_{11}\zeta_{13}^{-1}\zeta_{19}^{-1}$, $\zeta_{11}\zeta_{13}^{-1}\zeta_{19}$, and $\zeta_{11}\zeta_{13}\zeta_{19}^{-1}$. Therefore, the bijection between $T_2/\Gamma$ and the set of normalized solutions is as follows:

\[
\zeta_{11}^{-1}\zeta_{13}\zeta_{19}^{-1} \mapsto (2612, 73, 11 \cdot 13 \cdot 19)
\]

\[
-\zeta_{11}^{-1}\zeta_{13}^{-1}\zeta_{19}^{-1} \mapsto (2428, 119, 11 \cdot 13 \cdot 19)
\]

\[
\zeta_{11}\zeta_{13}^{-1}\zeta_{19} \mapsto (1772, 201, 11 \cdot 13 \cdot 19)
\]

\[
\zeta_{11}\zeta_{13}\zeta_{19} \mapsto (92, 265, 11 \cdot 13 \cdot 19).
\]
| Expected number of solutions | $2^2 = 4$ |
|-----------------------------|----------|
| Actual solutions            | (2612, 73, 11 · 13 · 19), (2428, 119, 11 · 13 · 19), (1772, 201, 11 · 13 · 19), (92, 265, 11 · 13 · 19) |
| Solutions as elements of $G_D(\mathbb{Q})$ | $\frac{2612 + 73 \sqrt{-105}}{11 \cdot 13 \cdot 19}$, $\frac{2428 + 119 \sqrt{-105}}{11 \cdot 13 \cdot 19}$, $\frac{1772 + 201 \sqrt{-105}}{11 \cdot 13 \cdot 19}$, $\frac{92 + 265 \sqrt{-105}}{11 \cdot 13 \cdot 19}$ |
| Factorization of elements  | $\frac{-2428 + 119 \sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11} \zeta_{13} \zeta_{19}$, $\frac{2612 + 73 \sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}^{-1} \zeta_{13} \zeta_{19}$, $\frac{1772 + 201 \sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11} \zeta_{13}^{-1} \zeta_{19}$, $\frac{92 + 265 \sqrt{-105}}{11 \cdot 13 \cdot 19} = \zeta_{11}^{-1} \zeta_{13}^{-1} \zeta_{19}$ |
| Bijection between $T_2/\Gamma$ and normalized solutions | $\zeta_{11}^{-1} \zeta_{13} \zeta_{19} \mapsto (2612, 73, 11 \cdot 13 \cdot 19)$, $\zeta_{11}^{-1} \zeta_{13}^{-1} \zeta_{19} \mapsto (2428, 119, 11 \cdot 13 \cdot 19)$, $\zeta_{11} \zeta_{13}^{-1} \zeta_{19} \mapsto (1772, 201, 11 \cdot 13 \cdot 19)$, $\zeta_{11} \zeta_{13} \zeta_{19} \mapsto (92, 265, 11 \cdot 13 \cdot 19)$ |

| Table 5. $D = 11 \cdot 13 \cdot 19$. |

From the above set of examples we observe the following.

- From examples (1), (2), (3) we note that the prime factors (other than satisfying $\left( -\frac{420}{p} = 1 \right)$ where $p = 11, 13, 19$) in particular has no contribution to the number of normalized solutions. In each of these examples we have changed the set of prime factors yet the number of distinct normalized solution of the form $(a, b, c)$ is always 2.
- From (4) we observe that the exponent of the prime factors of $c$ has no significance in case of determining the number of distinct normalized solutions. In this particular examples we have raised 11 and 13 to higher exponents yet the number of normalized solutions of the form $(a, b, c)$ is still 2.
- From (5) we note that the number of prime factors takes importance in case of determining the number of distinct normalized solutions. Here the number of primes factors of $c$ is no longer 2 unlike the earlier cases. Consequently we note that the normalized solution of the form $(a, b, c)$ is now 4 instead of 2.

From these above set of examples we have verified the main results of [JMMM], i.e., Theorem 3.6, Theorem 3.9 and Theorem 4.1.
The theorem holds for values of $D$ when when $-D \equiv 2, 3 \mod 4$ and when $C(-4D)$ is a free $\mathbb{Z}_2$ module. There are 65 numbers called Euler's convenient numbers in [Cox]. They are numbers $n$ such that $C(-4n)$ is a free $\mathbb{Z}_2$ module. They are conjectured to be the only numbers $n$ with this property, but there can be at most two more such numbers. Therefore if we take the subset of these numbers that are square free and equivalent to 1 or 2 mod 4 we get the following list, these are the known values of $D$ for which the theorem holds: 1, 2, 5, 6, 8, 10, 13, 21, 22, 30, 33, 37, 42, 57, 58, 70, 78, 85, 93, 102, 105, 130, 133, 165, 177, 190, 210, 253, 273, 330, 345, 357, 385, 462, and 1365.

Our analysis crucially uses the structure of the class group, in particular that each element has order two. A natural next project is to investigate what happens for other structures, and see if similarly comprehensive classifications hold.

REFERENCES

[Cohen] Henri Cohen, A course in computational number theory, Springer, Latest Edition, . Available at: https://tinyurl.com/284d73zx

[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

[Du] A. Dujella, History of elliptic curves rank records, https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html

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

[JMMM] T. Jaklitsch, T. C. Martinez, S. J. Miller and S. Mukherjee, Connections of Class Numbers to the Group Structure of Generalized Pythagorean Triples (preprint), https://arxiv.org/abs/2112.03663

[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. Mihăilescu, A Class Number Free Criterion for Catalan’s Conjecture, J. Number Th. 99 (2003), 225–231.

[Mih2] P. Mihăilescu, 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 the 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: thomasjaklitsch@college.harvard.edu
DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138
Email address: tmartinez@hmc.edu

DEPARTMENT OF MATHEMATICS, HARVEY MUDD COLLEGE, CLAREMONT, CA 90701
Email address: sjml@williams.edu, Steven.Miller.MC.96@aya.yale.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267
Email address: smukherjee@cmi.ac.in

DEPARTMENT OF MATHEMATICS, CHENNAI MATHEMATICAL INSTITUTE, SIRUSERI, CHENNAI, TAMILNADU-603103