PRIMES OF THE FORM $X^2 + NY^2$

SARTH CHAVAN

1. Inroduction

Fermat's first mention of $p = x^2+y^2$ occurs in a 1640 letter to Mersenne while $p = x^2+2y^2$ and $p = x^2+3y^2$ occur later in a 1654 letter to Pascal. Although no proofs for these assertions were given by Fermat in the letters, Fermat states the result as theorems. Fermat stated that

- Every prime number which surpasses by one a multiple of four is composed of two squares.
- Every prime number which surpasses by one a multiple of three is composed of a square and triple of another square.
- Every prime number which surpasses by one or three a multiple of eight is composed of a square and a double of another square.

Later Fermat adds that he has solid proofs for the above assertions. Fermat also studied beyond $p = x^2 + y^2$, $p = x^2 + 2y^2$, $p = x^2 + 3y^2$, his study for $x^2 + Ny^2 = p$ where $N = 5$ was found in a letter to Digby in the year 1658 quoting that

- If two primes, which end in 3 or 7 and surpass by three a multiple of four, are multiplied, then their product will be composed of a square and a quintuple of another square. But Fermat stated that he conjectured it and admitted that he can't prove it! After Fermat, Euler studied the question Characterizing all the primes p which can be written in the form $p = x^2 + Ny^2$ for more than 40 years of his life and achieved remarkable proofs for the same.

In this paper, we will develop the theory of binary quadratic forms and elementary genus theory, which together give an interesting and surprisingly powerful elementary technique in algebraic number theory. But due to some Limitations to binary quadratic forms and elementary genus theory, we will see the theory of Cubic reciprocity and Biquadratic (quartic) reciprocity to prove some interesting results.This is all motivated by a problem in number theory that dates back at least to Fermat: for a given positive integer n, characterizing all the primes which can be written $p = x^2 + ny^2$ for some integers x, y. Euler studied the problem extensively, and was able to solve it for $N = 1, 2, 3, 4$. However after Euler, Gauss and Langrange made a great contribution to this field by Class field theory and binary quadratic forms. However Euler solved the four theorems of Fermat using Reciprocity method and Fermat solved them using descent method. At the end of the Binary quadratic forms section

we will prove the following four theorems of Fermat along with $n = 7$.

1) $p = x^2 + y^2$, for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$ or $p = 2$
2) $p = x^2 + 2y^2$, for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 3 \pmod 8$, or $p = 2$
3) $p = x^2 + 3y^2$, for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$, or $p = 3$
4) $p = x^2 + 4y^2$, for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$

As we will see near the end of the paper, the techniques are not enough for us to characterize primes of the form $p = x^2 + ny^2$ for arbitrary n, but what they are able to achieve is remarkable in its own right. This paper will assume knowledge of basic field theory and group theory and the most important, Reader should have knowledge of quadratic reciprocity because quadratic reciprocity is the core of this paper.

At the end of the binary quadratic forms section, we will be able to use the theory of reduced forms to characterize primes of the form $p = x^2 + ny^2$ for $N = 1, 2, 3, 4, 7$. This theory is elementary but quite powerful, and to develop it, we first must define some concepts which will serve as the foundation for the rest of our discuss. But before that we have to get familiar with some concepts, definitions, and theorems in binary quadratic forms so that at the end we can use them all for our basic question of this paper to solve $x^2 + ny^2 = p$ where $n = 1, 2, 3, 4, 6, 7$.

2. Binary Quadratic Forms

The study of integral binary quadratic forms in two variablesthat is $f(x) = ax^2 + bxy + cy^2$ began with Langrange who introduced the concept of Discriminants, equivalence and reduced forms. When these theories of Langrange are combined with Gauss notion of proper equivalence, one has all the ingredients to develop the theory of binary quadratic forms.Most of the terminologies are due Gauss, though many of the terms he introduced refer to the concepts used implicitly by Langrange. We have the following definitions and theorems:

Definition 2.1. A *binary quadratic form* is a function in two variables $f(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$.

Remark 2.2. We say that a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$ is primitive if a, b, c are relatively prime.

Now a question comes that can an integer be represented by a binary quadratic form and if yes, then what's the condition which implies the same. For this question we have the following definitions and theorems.

Definition 2.3. An integer m is represented by a Binary quadratic form f if there exists $x, y \in \mathbb{Z}$ such that $f(x, y) = ax^2 + bxy + cy^2 = m$. Further if those x, y are prime then it is said that integer m is properly represented in f.

Definition 2.4. A binary quadratic form is said to be positive semidefinite if it only represents non-negative integers, and it is said to be negative semidefinite if it only represents non-positive integers. It is said to be indefinite if it represents both positive and negative integers. A (positive or negative) semidefinite binary quadratic form f is said to be (positive or negative) definite if, whenever $f(x, y) = 0$, then $x, y = 0$

We got some great definitons so far and now we should define some relation between two binary quadratic forms. Which brings us the following definition and theorem.

Definition 2.5. Two binary quadratic forms $f(x, y)$ and $g(x, y)$ are equivalent if there exist $p, q, r, s \in \mathbb{Z}$ such that $f(x, y) = g(px+qy, rx+sy)$ and $ps-qr = \pm 1$ Moreover if $ps-qr = 1$ then $f(x, y)$ and $g(x, y)$ are said to be properly equivalent and if $ps - qr = -1$ then $f(x, y)$ and $g(x, y)$ are said to be improperly equivalent (Note that it is possible for two forms to be both properly equivalent and improperly equivalent)

Theorem 2.6. *A binary quadratic form $f(x, y)$ properly represents an Integer m if and only if $f(x, y)$ is properly equivalent $mx^2 + bxy + cy^2$ for some $b, c \in \mathbb{Z}$ (This is nothing but a result of Definition 2.3)*

Proof. It implies that, Consider for a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, suppose $f(p, r) = m$ where p, r are relatively prime. Since p, r are relatively prime there exist integers q and s such that $ps - qr = 1$ (properly equivalent).Then

$$f(px+qy, rx+sy) = f(p, r)x^2 = (2apq+bps+brq+2crs)xy+f(q, s)y^2 = mx^2+b'xy+c'y^2$$

$f(px + qy, rx + sy) = mx^2 + bxy + cy^2$ for some $p, q, r, s \in \mathbb{Z}$ such that $ps - qr = 1$, then $f(p, r) = m$ where p, r are relatively prime. ■

Now we define Discriminant of the binary quadratic forms which plays the most important role in proving our basic question to characterize primes that can be represented as x^2+Ny^2

Definition 2.7. Discriminant of a binary quadratic form $f(x, y) = ax^2+bxy+cy^2$ is defined as $D = b^2 - 4ac$ (proof for this theorem is for the reader)

Theorem 2.8. *If the discriminant D of $f(x, y) = ax^2 + bxy + cy^2$ is negative and $a > 0$ (respectively $a < 0$), then $f(x, y)$ is positive definite (respectively, negative definite). If D is positive then we say $f(x, y)$ is indefinite.*

We get these terms because if $f(x, y)$ is positive definite,$f(x, y)$ only represents positive integers (the analogous statement holds for negative definite forms), and if $f(x, y)$ is indefinite, it represents both positive and negative integers. We will leave these facts to the reader to verify.

Theorem 2.9. *Show that Discriminant of 2 equivalent binary quadratic forms is equal*

Proof. Let's consider two binary quadratic forms suppose $f(x, y) = ax^2 + bxy + cy^2$ and $F(X, Y) = AX^2 + BXY + CY^2$ are equivalent with $F(X, Y) = f(\alpha X + \beta Y + \gamma X + \delta Y)$ for some Integers $\alpha, \beta, \gamma, \delta$ satisfying the condition $\alpha\delta - \beta\gamma = \pm 1$ (as they are equivalent),

$$A = f(\alpha, \gamma) = a\alpha^2 + b\alpha\gamma + c\gamma^2$$

$$B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta$$

$$C = f(\beta, \delta) = \alpha\beta^2 + b\beta\delta + c\delta^2$$

and now we can easily compute $b^2-4ac = (\alpha\delta-\beta\gamma)^2$ and we know that $\alpha\delta-\beta\gamma = \pm 1$ hence $(\alpha\delta - \beta\gamma)^2 = 1$ and hence it follows that determinants of both of the forms is equal. ■

Theorem 2.10. *Let D be an integer congruent to 0 modulo 4, and m be an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m.*

Proof. Suppose that primitive Binary quadratic form $f(x, y)$ properly represents m. Then we know that $f(x, y)$ is properly equivalent to $mx^2 + bxy + cy^2$ by Theorem 1.8 and hence discriminant $(D) = b^2 - 4ac$ for some $b, c \in \mathbb{Z}$. Therefore $b^2 \equiv D \pmod{m}$. Let

$$b' = \begin{cases} b, \text{ when b is even} \\ b + m, \text{ if not} \end{cases}$$

Then $D = b'^2$ mod m and since m is odd and $D \equiv 0 \pmod 4$, D and b' both are even. Which implies that $D \equiv b'^2 \pmod{m}$ (since 4 divides both D and b'^2, and thus from earlier we get $D \equiv b'^2 - 4mc$ for some $c \in \mathbb{Z}$. hence we have the binary quadratic form $f(x, y) = mx^2 + bxy + cy^2$ which has discriminant D, properly representing m (since $f(1, 0) = m$),and is primitive since m is prime to D, which finishes proof of our Theorem. ■

Theorem 2.11. *Let n be an integer and p be an odd prime that does not divide n. Then p is represented by a primitive form of discriminant $-4n$ if and only if $\left(\frac{-n}{p}\right) = 1$*

Proof. We know that a primitive Binary quadratic form represents a prime p if and only if it properly represents p. Hence the theorem is an immediate consequence of theorem 1.12 and Legendre symbol property, since $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)\left(\frac{2}{p}\right)^2 = \left(\frac{-n}{p}\right)$ ■

Theorem 2.12. *A primitive positive definite Binary quadratic form $ax^2 + bxy + cy^2$ where all a, b, c are relatively prime, is reduced if and only if*

$$1. \mid b \mid \leq a \leq c, \ 2. \mid b \mid \geq 0 \iff b = a \text{ or } b = c$$

Primitive positive definite forms have a very important property, illustrated in the following theorem.

Theorem 2.13. *Every primitive, positive definite form is properly equivalent to a unique reduced form.*

Proof. The proof is a bit longer but is elementary to understand. Let's consider a primitive positive definite binary quadratic form $f(x, y)$ we have to prove that it is properly equivalent to another binary quadratic form satisfying the condition $\mid b \mid \leq a \leq c$, and out of all the other binary quadratic forms equivalent to $f(x, y)$, Let $g(x, y)$ be a binary quadratic form such that the minimal $\mid b \mid$ is minimal.We already know that for any integer m, $g(x + my, y) = ax^2 + (2am + b)xy + c'y^2$ is always properly equivalent to $g(x, y)$, so if $a <\mid b \mid$, we can choose m such that $\mid 2am + b \mid <\mid b \mid$, which contradicts our choice of b. Thus as a result of contradiction we get $a \geq \mid b \mid$. Similarly it can be proved that $c \geq \mid b \mid$. If $a > c$, we simply need to exchange the outer coefficients, which is done in the properly equivalent form $g(-y, x)$ and the resulting Binary quadratic form $ax^2 + bxy + cy^2$ also satisfies the condition $\mid b \mid \leq a \leq c$

This form will already be reduced if $b < 0$ and either $a = -b$ or $a = c$. If $ax^2 + bxy + cy^2$ isn't reduced, $ax^2 - bxy + cy^2$ will be reduced always, so we just need to prove that the two Binary quadratic forms are equivalent if and onlyy if $a = -b$ or $a = c$ Suppose if $a = -b$ then $(x, y) \longmapsto (x + y, y)$ takes $ax^2 - axy + cy^2$ to $ax^2 + axy + cy^2$. Suppose $a = c$ then $(x, y) \longmapsto (-y, x)$ takes $ax^2 - bxy + ay^2$ to $ax^2 + bxy + ay^2$ Hence we have proved that $f(x, y)$ is properly equivalent to a Reduced form. Now all we have to do is that the reduced form is Unique, which we will prove by showing that different reduced forms cannot be properly equivalent. The part to prove that it's unique is left to the reader. ■

Definition 2.14. Two forms are said to be in the same class if they are properly equivalent.

Theorem 2.15. *Let $D < 0$ be fixed. Then the number $h(D)$ of equivalence classes of primitive positive definite forms of discriminant D is finite, and $h(D)$ is equal to the number of reduced forms of discriminant D.*

Proof. So in this theorem we just need to prove that the number of reduced forms of a discriminant D is finite and the rest of the part will easily follow from theorem 1.15

We know that discriminant of a binary quadratic form $ax^2 + bxy + cy^2$ is $b^2 - 4ac$. We also know that for any reduced binary quadratic form $ax^2 + bxy + cy^2$, we have $b^2 \leq a^2$ and $a \leq c$. Hence we obtain that

$$-D = -(b^2 - 4ac) = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \implies \mid b \mid \leq a \leq \sqrt{-D/3}$$

$\implies$ We have finite number of possible values for a, b. The concept of discriminant implies that given values for a, b and D have only one possible value for c and hence this finishes our proof. ■

Another consequence of Theorem 3.13 is that we have the following improvement to Theorem 3.11

Theorem 2.16. *Let n be a positive integer and p an odd prime not dividing n. Then $\left(\frac{-n}{p}\right) = 1$ if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$*

Proof. By theorem 3.11 we get that $\left(\frac{-n}{p}\right) = 1$ if and only if p is properly represented by a primitive form of discriminant $-4n$. Moreover, the proof of Lemma 3.10 shows that we can find such a quadratic form whose coefficient in front of x^2 is p. Hence, by (3.9), the form properly representing p is primitive positive definite, and by Theorem 3.15, this occurs if and only if p is represented by one of the $h(-4n)$ reduced forms of discriminant $-4n$ ■

This theorem tells us something very interesting: whether a prime p is represented by a reduced form of discriminant $-4n$ is simply a matter of whether there is a solution to the congruence $x^2 \equiv -n \pmod{p}$. In fact, we can obtain a more general result (although the discriminant $-4n$ is what interests us).

So far we have gathered the concept of binary quadratic forms in a simpler way! Now we are ready to solve the most awaited problem of this paper that is $P = x^2 + ny^2$ for $N = 1, 2, 3, 5, 7$

3. Primes of the form $x^2 + ny^2$ for $n = 1, 2, 3, 4, 7, k^2$

Let's summarise all theorems of Binary quadratic forms so far; Theorem 1.13 tells us that a prime p is represented by a Primitive Binary quadratic form of the discriminant $-4n$ if and only if $\left(\frac{-n}{p}\right) = 1$, Since a form with a negative discriminant representing positive integers must be positive definite, we can combine this with Theorem 1.15 to get that a prime p is represented by a reduced form of discriminant $-4n$ if and only if $\left(\frac{n}{p}\right) = 1$, Finally, Theorem 1.16 tells us that the reduced forms of a given discriminant are finite, and actually gives us an explicit bound on the coefficients. Noting that $x^2 + ny^2$ is a reduced form, it is now clear just how useful these results could be to us. And, in fact, we now have all that we need to characterize primes of the form $p = x^2 + ny^2$, for a few values of n. To demonstrate the

power of these theorems and as reward for our efforts so far, we will now prove the four theorems of Fermat, and also characterize primes of the form x^2+7y^2 Amazingly, the proofs now require nothing more than some easy computation.

Theorem 3.1. *For a Prime p,* $p = x^2+y^2$, *for some* $x, y \in \mathbb{Z}$ *if and only if* $p \equiv 1 \pmod 4$ *or* $p = 2$

Proof. We require an odd prime so we will deal with the case $p = 2$ separately.Theorem 1.13 implies that for an odd prime p , p is represented by a reduced form of discriminant -4 if and only if $\left(\frac{-1}{p}\right) = 1$. But first we have to determine all the reduced forms of discriminant -4. From theorem 1.16 we know that $\mid b \mid \leq a \leq \sqrt{4/3} < 2$, $if a = b = 0$, then $D = 0$ resulting $a = 1$. $1 - 4c = -4$ which gives no solution and hence $b = 0$ and hence the only reduced form of the discriminant -4 is $x^2 + y^2$. Now we only need to find p in general for $\left(\frac{-1}{p}\right) = 1$, which is a well known that is $p \equiv 1 \pmod 4$, which proves our Theorem. ■

Theorem 3.2. *For a Prime p,* $p = x^2 + 4y^2$, *for some* $x, y \in \mathbb{Z}$ *if and only if* $\iff p \equiv 1 \pmod 4$

Proof. The Proof goes similar as last theorem's as we can write $4y^2$ as $(2y)^2$ which becomes our new y' and hence proceeding similar way as in the last proof we obtain that $p \equiv 1 \pmod 4$, which proves our Theorem. Next Theorem is generalisation of this theorem. ■

Theorem 3.3. *For a Prime p,* $p = x^2+Ny^2$, *for some* $x, y, z \in \mathbb{Z}, N = z^2$ *if and only if* $p \equiv 1 \pmod 4$

Proof. This is a generalised form of last theorem where we take $N = z^2, z \in \mathbb{Z}$. We just substitute Ny^2 by $z^2y^2 = (zy)^2$ and we get new $y" = (zy)^2$ and then proceeding the similar way as in Last theorem we obtain $p \equiv 1 \pmod 4$, which proves our Theorem. We have proved for every square integer N. ■

Theorem 3.4. $p = x^2 + 2y^2$, *for some* $x, y \in \mathbb{Z}$ *if and only if* $p \equiv 1, 3 \pmod 8$, *or* $p = 2$

Proof. We require an odd prime so we will deal with the case $p = 2$ separately. Theorem 1.13 implies that for an odd prime p , p is represented by a reduced form of discriminant -8 if and only if $\left(\frac{-2}{p}\right) = 1$. But first we have to determine all the reduced forms of discriminant -4. From theorem 1.16 we know that $\mid b \mid \leq a \leq \sqrt{8/3} < 2$, Thus $a = 1$ and as $1 - 4c = 8$ has no integer solutions so $x^2 + 2y^2$ is the only reduced form of the discriminant -8. Now we only need to find p in general for $\left(\frac{-2}{p}\right) = 1$. We know that now we only need to find p in general for $\left(\frac{2}{p}\right) = 1$ only and only when $p \equiv 1, 7 \pmod 8$, Hence we obtain Now we only need to find p in general for $\left(\frac{-2}{p}\right) = 1$, so $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) \implies p \equiv 1, 3 \pmod 8$ which proves our theorem. ■

Theorem 3.5. $p = x^2 + 3y^2$, *for some* $x, y \in \mathbb{Z}$ *if and only if* $p \equiv 1 \pmod 3$, *or* $p = 3$

Proof. We know that theorem 1.13 implies that p should not divide n and hence we handle the case $p = 3$ separately. For $p > 3$ p is represented by a reduced form of discriminant -12 if and only if $\left(\frac{-3}{p}\right) = 1$. But first we have to determine all the reduced forms of discriminant

-4. From theorem 1.16 we know that $\mid b \mid \leq a \leq \sqrt{12/3} = 2$, now showing again that there exist no solution we conclude again that $x^2 + 3y^2$ is the only reduced Binary quadratic form of the discriminant -12, the numerator is no longer congruent to 1 modulo 4 and hence by law of quadratic reciprocity we obtain that we have $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{p}{3}\right)$ By some basic knowledge of field theory and squares in a group we get $\mathbb{F}_3^{*2} = 1 \implies p \equiv 1 \pmod 3$ which proves our theorem. ■

Theorem 3.6. *$p = x^2 + 7y^2$, for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 2, 4 \pmod 7$, or $p = 7$*

Proof. Note that we don't always need to show that there exists no solution for bounds as we know that $h(-4N) = 1$ only if $N = 1, 2, 3, 4, 7$. We know that theorem 1.13 implies that p should not divide n and hence we handle the case $p = 7$ separately. p is represented by a reduced form of discriminant -28 if and only if $\left(\frac{-7}{p}\right) = 1$. This time we don't need to show that $x^2 + 7y^2$ is the only reduced Binary quadratic form of the discriminant -28 as we have already given that in the note! 28. By the same logic as in the previous proof, we get $\left(\frac{-7}{p}\right) = \left(\frac{7}{p}\right)\ \left(\frac{-1}{p}\right) = \left(\frac{p}{7}\right)$. By some basic knowledge of field theory and squares in a group we get $\mathbb{F}_7^{*2} = 1, 2, 4 \implies p \equiv 1, 2, 4 \pmod 7$ which proves our theorem ■

The power of our quadratic form theorems should be quite evident now. However, without adding any further theory, this approach suffers from some very serious limitations. All four of the previous proofs were similar in that there was only one reduced form of the given determinant. However, this is not true in the general case. In fact, there are no other values of n where $x^2 + Ny^2$ is the only reduced form of discriminant $-4n$, Trying the same approach on $p = x^2 + 5y^2$ for instance, we get $\left(\frac{-5}{p}\right) = 1$ if and only if p is of the form $x^2 + 5y^2$ or of the form $2x^2 + 2xy + 3y^2$. In order to distinguish between these two cases, we will need some elementary genus theory

4. Elementary Genus Theory

Let's have a look at some definitions, concept and Theorems in Elementary genus theory and use them to solve for $x^2 + Ny^2$ for $N = 5, 6$.

There is a very natural homomorphism related to the Legendre symbol that we will use extensively in this section. Its usefulness to us will become almost immediately apparent, so we will begin this section simply by constructing it. So let's go through some concepts and definitions in Elementary Genus Theory!

Theorem 4.1. *Let D (Discriminant) $= 4n$ for some $n \in \mathbb{Z}$. Then always there is a unique $\chi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \pm 1$ such that $\chi([p]) = \left(\frac{D}{p}\right)$ for all primes p that do not divide D*

Of course, that gives us the following for primes p that do not divide $-4n$ p is represented by a binary quadratic form of discriminant $-4n \iff \left(\frac{N}{p}\right) = 1$ if and only if $[p] \in \ker \chi$

This seems like it might be useful as $\ker \chi$ is a group, and so we might hope to use the algebraic properties of this group to learn more about the forms of a given discriminant. As we will soon demonstrate, there is a useful relationship between a certain subgroup of $\ker \chi$ and the different reduced forms of discriminant $4n$. In fact, for quite a few values of n, we get the best result possible: all the different reduced forms of discriminant $4n$ represent disjoint subsets of $\ker \chi$, and they represent a prime p if and only if $[p]$ is in the corresponding

subset. This all falls under genus theory, which, for our purposes, is the characterization of how different forms do or don't intersect in the values that they represent. We really only need one more theorem to be able to characterize primes of the form $p = x^2 + Ny^2$ for about 50 more values of N. In this section we will prove the following theorems

1) $p = x^2 + 6y^2 \iff p \equiv 1, 7 \pmod{24}$
2) $p = x^2 + 10y^2 \iff p \equiv 1, 9, 11, 19 \pmod{40}$
3) $p = x^2 + 13y^2 \iff p \equiv 1, 9, 17, 25, 29, 49 \pmod{52}$
4) $p = x^2 + 15y^2 \iff p \equiv 1, 9, 31, 49 \pmod{60}$
5) $p = x^2 + 21y^2 \iff p \equiv 1, 25, 37 \pmod{84}$
6) $p = x^2 + 22y^2 \iff p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \pmod{88}$
7) $p = x^2 + 30y^2 \iff p \equiv 1, 31, 49, 79 \pmod{120}$

although it will require a few lemmas and definitions. Now Let's have a look at the required definitions and lemmas.

Definition 4.2. Suppose that $D < 0$ satisfying the condition $D \equiv 0, 1 \pmod 4$ then we define the Principal form of the Discriminant D to be $x^2 - \frac{D}{4}y^2$ if $D \equiv 0 \pmod 4$ and $x^2 + xy + \frac{1-D}{4}y^2$ if $D \equiv 1 \pmod 4$

Question 4.3. *The principal form of discriminant D actually has discriminant D.*

The part of verifying that the principal form of discriminant D actually has discriminant D is now left to the reader.

Theorem 4.4. *If $f(x, y)$ represents an integer m, then m can be written as d^2m', where $f(x, y)$ properly represents m'.*

Proof. We choose x, y such that $f(x, y) = m$ where $x, y \in \mathbb{Z}$. Let $d = gcd(x, y)$, then we get $x = dx'$ and $y = dy'$ where x', y' are relatively prime.Thus we get

$$f(x, y) = f(dx', dy') = m = a(dx')^2 + b(dx')(dy') + c(dy')^2$$
$$a(dx')^2 + b(dx')(dy') + c(dy')^2 = d^2(ax'^2 + bx'y' + cy'^2) = d^2(f(x', y')) = d^2m'$$

which proves our Theorem. ■

Lemma 4.5. *For any prmitive Binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ and Integer M, then $f(x, y) = ax^2 + bxy + cy^2$ properly represents infinitely many integers relatively prime to M*

Proposition 4.6. *Let $D = -4N$ for some positive integer N and let $f(x, y)$ be a primitive binary quadratic form of Discriminant D, then,*

- *1) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by principal form of Discriminant D forms a subgroup H of* $\ker\chi$
- 2*) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the Principal form of discriminant D forms a coset of H in* $\ker\chi$

This preposition plays an important role in proving our question of primes of the form $x^2 + Ny^2$. Now we will have couple of more definitions and a theorem and then we are ready.

Definition 4.7. Let $D = -4n$ for positive n, and let H be as in Preposition 4.6. For any coset H of H, the genus of H' is the set of all quadratic forms of discriminant D that represent H' modulo D.

Theorem 4.8. *Let $D = -4n$ for some positive integer n, and let H be as in Preposition 4.6. If H' is a coset of H in $\ker\chi$ and p is an odd prime not dividing D, then p is represented by a reduced form of discriminant D in the genus of H' if and only if $[p]$ is in H'*

Proof. As we have seen various lemmas and definitions in Elementary Genus Theory so proving this theorem goes a lot easy. The only thing we need to note that distinct cosets of H must be disjoint and then the proof of this theorem easily or we can say immediately follows from lemma 4.5 and the theorem 2.3 from the binary quadratic forms section! The part of proving is left to the reader using the Hint given above. ■

This theorem allows us (in many cases, at least) to make a distinction between the values represented by some of the different reduced forms of the same discriminant. With it, we are now ready to prove the conjecture of Euler's which we gave in the introduction (we chose $n = 6$ to avoid filling the paper with many more Legendre symbol calculations, which at this point should feel trivial to the reader). So let's start!

Theorem 4.9. $p = x^2 + 6y^2$, *for some $x, y \in \mathbb{Z}$ if and only if* $p \equiv 1, 7 \pmod{24}$

Proof. So let's begin with the proof! Let's consider a prime $p > 3$. Now consider a reduced binary quadratic form say $f(x, y) = ax^2 + bxy + cy^2$ with Discriminant -24 and satisfying the condition $\mid b \mid \leq a \leq \sqrt{-24/3} < 3$ Now if a $= 1$ then $1 - 4c = -24$ has no integer solutions, Hence $b = 0$ and binary quadratic form $f(x, y) = x^2 + 6y^2$. Now if a $= 2$ then $1 - 8c = -24$ and $4 - 8c = -24$ have no integer solutions, and hence binary quadratic form $f(x, y) = 2x^2 + 3y^2$. By properties of Legendre symbol we get that

$$\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) = 1$$

where we know that $\left(\frac{2}{p}\right) = 1 \iff p \equiv 1, 3 \pmod{8}$ and we have already proved in theorem 3.5 that $\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod{8}$ which gives us the below result

$$\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1, 5, 7, 11 \pmod{24}$$

Which obviously implies that $\ker\chi = 1, 5, 7, 11$. Now We can see quite easily that of those values, $x^2 + 6y^2$ represents only 1 and 7 that is nothing but $H = 1, 7$ which implies that $2x^2 + 3y^2$ represents 5 and 11 and hence it can't be in the Genus of H. The genus of H is nothing but simply $x^2 + 6y^2$ and the forms properly equivalent to it. Therefore if p is a prime of the form $x^2 + 6y^2 \iff p \equiv 1, 7 \pmod{24}$ or $p = 2, 3$ which proves our theorem! ■

The Elementary Genus theory works only when the Principal genus consists of only one class, for then we get the congruence conditions that characterize $p = x^2 + Ny^2$. This is what happened when we proved for $n = 6$. Similarly as we proved for $n = 6$ we can prove

that

$$2)\ p = x^2 + 10y^2 \iff p \equiv 1, 9, 11, 19 \pmod{40}$$
$$3)\ p = x^2 + 13y^2 \iff p \equiv 1, 9, 17, 25, 29, 49 \pmod{52}$$
$$4)\ p = x^2 + 15y^2 \iff p \equiv 1, 9, 31, 49 \pmod{60}$$
$$5)\ p = x^2 + 21y^2 \iff p \equiv 1, 25, 37 \pmod{84}$$
$$6)\ p = x^2 + 22y^2 \iff p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \pmod{88}$$
$$7)\ p = x^2 + 30y^2 \iff p \equiv 1, 31, 49, 79 \pmod{120}$$

We can prove above assertions easily as we proved for $n = 6$. Because for $n = 6, 10, 13, 15, 21$, 22, 30 the Principal genus consists of only 1 class, and hence the part of proving those assertions is left to the reader.

Again, this technique allows us to prove a quite impressive result in number theory very easily, needing only a simple, very procedural proof. We encourage the reader to try with $p = x^2 + 5y^2$ to get a further feel of genus theory; as in Theorem 4.9, the proof amounts to little more than basic computations. The power of this technique is fairly remarkable. But while the addition of elementary genus theory let us characterize primes of the form $p = x^2 + Ny^2$ for a lot of values n that the theory of reduced forms alone fell short on, it too has serious limitations. It should be clear that our proof of Theorem 4.9 depended on the fact that the principal form of discriminant -24 was the only reduced form in its genus. From a probabilistic standpoint, though, this is almost never the case. The Genus Theory cannot solve our basic question for all n. For instance let's consider a reduced binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ with determinant $D = -108$, here the Genus theory is completely useless as all reduced binary quadratic forms $x^2 + 27y^2, 4x^2 + 2xy + 7y^2, 4x^2 - 2xy + 7y^2$ lie in the same genus and hence we cannot distinguish them! And so, to finish our paper, we will use genus theory to prove one last conjecture of Euler's, which is about primes of the form $p = x^2 + 14y^2$ This is a noteworthy achievement in its own right, but will also clearly illustrate some of the limitations of the technique we've developed. If we want a better characterization, we would need some further theory that falls outside the scope of this paper. I encourage the interested reader to study class field theory in order to learn more about this problem.

Theorem 4.10. *For a prime p where $p \neq 2, 7$, either p or $2p$ is of the form $x^2 + 14y^2 \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$, and $3p$ is of the form $x^2 + 14y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$*

Proof.

$$p = \begin{Bmatrix} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{Bmatrix} \text{ if and only if } p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$
$$3p = x^2 + 14y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$$

Similarly as we did in the last theorem, we find that only reduced forms of the discriminant $D = -56$ are $x^2 + 14y^2, 2x^2 + 3y^2, 3x^2 + 2xy + y^2, 3x^2 - 2xy + y^2$, and now we need to find when

$$\left(\frac{-14}{p}\right) = 1$$

By properties of Legendre symbol we get that

$$\left(\frac{-14}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{7}{p}\right)\left(\frac{-1}{p}\right) = 1$$

where we know that $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 3 \pmod 8$ which gives us the below result

$$\left(\frac{-14}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-7}{p}\right) = 1$$

if and only if $p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 27, 39, 45 \pmod{56}$, Now it's easy to see that among the set $\{1, 3, 5, 9, 13, 15, 19, 23, 27, 39, 45\}$ the reduced binary quadratic form $x^2 + 14y^2$ only represents $1, 9, 15, 19, 23, 39$ but reduced binary quadratic form $2x^2+7y^2$ obviously represents 9 and it must be in the same genus as the principal form and hence we cannot distinguish between both of them! Similarly we also see that reduced binary quadratic form $3x^2 \pm 2xy + 5y^2$ represents the numbers $3, 5, 13, 19, 27, 45$, and hence share their own genus! It's quite clear that p is of the form $2x^2+14y^2$ if and only if $2p$ is of the form x^2+14y^2, so all it remains to prove is that $3p$ is of the form $x^2 + 14y^2$ if and only if $p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$. as we know that reduced binary quadratic form $3x^2 \pm 2xy + 5y^2$ represents the numbers $3, 5, 13, 19, 27, 45$, and thus it suffices to prove that $3p$ is of the form x^2+14y^2 if and only if p is either of the form $3x^2 + 2xy + 5y^2$ or $3x^2 - 2xy - 5y^2$. Now if we take $p = 3x^2 \pm 2xy - 5y^2$ then we get $3p = 9x^2 \pm 6xy + 15y^2 = (3x \pm y)^2 + 14y^2$. Conversely suppose $3p = x^2 + 14y^2$, if y was a multiple of 3 then y^2 and x^2 would obviously be multiples of 9, which would imply p to be a multiple of 3 which can't be possible as p is a prime and hence a contradiction! Thus contradiction implies that we can express y in the form $3k \pm 1$ where $k \in \mathbb{Z}$. Either way $14y^2 \equiv 2 \pmod 3$ resulting to $x^2 \equiv 1 \pmod 3$ which means that we can express x as $3t \pm (3k \pm 1)$ where $k \in \mathbb{Z}$ and hence we get that

$$p = 3t^2 \pm 2t(3k \pm 1) + 5(3k \pm 1)^2$$

which completes our proof. ■

In the previous section, we noted that there are only finitely many cases when the number of reduced forms $h(-4n)$ of discriminant $-4n$ is equal to 1. This prompts the following similar question: Are there finitely many discriminants of the form $-4n$ for which the principal genus consists of only the principal form? The answer to this question is yes; there are indeed only finitely many such discriminants. It turns out that all genera of forms of discriminant $-4n$ consist of the same number of classes. So, if the principal genus is to contain only the principal form, then all genera must consist of only one class. This is related to the study of convenient numbers, which we have not discussed. There are only finitely many convenient numbers, and a positive integer n is a convenient number if and only if the genera of forms of discriminant $-4n$ consist only of a single class. For a more thorough treatment of this topic, reference sections $3.B$ and $3.C$ of Cox [1].

5. Cubic and Biquadratic Reciprocity

5.1. **Cubic Reciprocity.** In the previous two sections, we have made significant progress on the question of when a prime p can be represented by the quadratic form $x^2 + Ny^2$. In doing this, we formulated necessary and sufficient conditions for numerous values of n. Besides developing some theory on quadratic forms and genera, the most advanced number theoretic tool we have used has been quadratic reciprocity.

As the discussion in the previous section highlighted, only certain cases can be solved with these methods. For other values of n, cubic and biquadratic reciprocity, which are in a sense generalizations of quadratic reciprocity, need to be utilized. Just as quadratic reciprocity tells us when the congruence $x^2 \equiv a \pmod{p}$ has a solution, cubic and biquadratic reciprocity determine when the respective congruences $x^3 \equiv a \pmod{p}$ and $x^4 \equiv a \pmod{p}$ have solutions. In this section, we will answer these questions to show when a prime can be represented by the forms $x^2 + 27y^2$ and $x^2 + 64y^2$. Before we can formulate the Law of Cubic Reciprocity, we need to investigate some of the properties of the ring $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega = \frac{-1+\sqrt{-3}}{2}$ is one of the cube roots of unity. We now review some basic definitions of abstract algebra.

Using Cubic Reciprocity, we will show that a prime p can be represented by the form $x^2 + 27y^2$ if and only if $p \equiv 1 \pmod{3}$ and 2 is a cubic residue of p.

Definition 5.1. Let R be an integral domain

- An element u in R is called a *unit* if u divides 1
- Two elements a and b in R are called *associates* if $a = bu$ for some unit u
- An element p in R is said to be irreducible if $a \mid p$ implies that a is either *a unit* or an *associate* of p
- A non-unit p in R is called a *prime* if $p \neq 0$ and $p \mid ab$ implies that a is either a unit or an associate of p.

Definition 5.2. The ring R is said to be a unique factorization domain (UFD) if every non-zero element r in R, which is a non-unit, has the following properties:

- r can be written as a finite product of (not necessarily distinct) irreducibles p_i of R. That is $r = p_1 p_2 p_3 \cdots p_n$
- if $r = q_1 q_2 \cdots q_n$ is another factorization of r into irreducibles, then $m = n$, and there is some numbering such that p_i and q_i are associates for $i = 1, 2, ..., n$.

A very important property of the ring $\mathbb{Z}[\omega]$ is that it is closed under complex conjugation. Indeed, let $\alpha = a + b\omega$ be an element in $\mathbb{Z}[\omega]$ then,

$$\overline{\alpha} = \overline{a + b\omega} = a + b\omega^2 = a + b(-1 - \omega) = (a - b) - b\omega \in \mathbb{Z}[\omega]$$

This allows us to make the following definition.

Definition 5.3. Let $\alpha = a + b\omega$ be an element of $\mathbb{Z}[\omega]$, We define norm of α, $N(\alpha)$, by the formula

$$N(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$$

Lemma 5.4. *An element α contained in $\mathbb{Z}[\omega]$ is a unit if and only if $N(\alpha) = 1$, the units of $\mathbb{Z}[\omega]$ are therefore $\pm 1, \pm\omega, \pm\omega^2$.*

Proof. If $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$ which implies that α is a unit. If α is a unit, then there exists an element β of $\mathbb{Z}[\omega]$ such that $\alpha\beta = 1$, which again implies that $N(\alpha)N(\beta) = 1$. Therefore $N(\alpha) = 1$, since both $N(\alpha)$ and $N(\beta)$ both are positive integers.

Now suppose we take $\alpha = a + b\omega$ is a unit, Then,

$$a^2 - ab + b^2 = 1 \text{ which is same as } 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$$

There we get two possibilities:

$$2a - b = \pm 1 \text{ and } b = \pm 1 \text{ or } 2a - b = \pm 2 \text{ and } b = 0$$

Solving these six equations we obtain that the units are $\pm 1, \pm\omega, \pm(1+\omega)$. we know that

$$1 + \omega + \omega^2 = 0$$

and hence we get that $\pm 1, \pm\omega, \pm(1+\omega)$ are the same as $\pm 1, \pm\omega, \pm\omega^2$ ■

Lemma 5.5. *If π is a prime in $\mathbb{Z}[\omega]$, then there is a rational prime p such that $N(\pi) = p$ or p^2. If $N(\pi) = p$ then π is not associated to a rational prime, whereas if $N(\pi) = p$ then π^2 then it is an associated to a rational prime*

Proof. We know that $N(\pi) = \pi\overline{\pi} > 1$ is some integer, it is a product of rational primes. Hence $\pi \mid p$ for some rational prime p in the factorization of $N(\pi)$. Thus suppose we have $p = \pi\gamma$ for some $\gamma \in \mathbb{Z}[\omega]$. By the multiplicativity of the norm, we have

$$N(p) = N(\pi)N(\gamma) = p^2.$$

Thus either $N(\pi) = p^2$ and $N(\gamma) = 1$ or $N(\pi) = p$, since π is by definition not a unit. In the former case, γ is a unit and so π is associated to p. In the latter, suppose $\pi = uq$ where q is a rational prime and u is a unit. Then

$$p = N(\pi) = N(u)N(q) = N(q) = q^2$$

which is clearly impossible, Thus π is not associated to a prime. ■

Lemma 5.6. *Suppose an element π in $\mathbb{Z}[\omega]$ is such that $N(\pi) = p$ is a rational prime. Then, π is a prime in $\mathbb{Z}[\omega]$*

Proof. Let's prove this by Contradiction. Suppose that π is not a prime, then we know that π is also not irreducible and hence $\pi = \delta\gamma$ with $N(\delta), N(\gamma) > 1$, Thus we obtain

$$p = N(\pi) = N(\delta)N(\gamma)$$

which is impossible as we know that p is a rational prime and hence we obtain a contradiction proving our theorem that is p is a prime. ■

We now have the necessary information to classify the primes in $\mathbb{Z}[\omega]$

Theorem 5.7. *Let p be a rational prime. If $p \equiv 2 \pmod 3$, then p is a prime. If $p \equiv 1 \pmod 3$, then $p = \pi\overline{\pi}$, where π is prime in $\mathbb{Z}[\omega]$. Hence, $3 = -\omega^2(1-\omega)^2$, where $1-\omega$ is a prime in $\mathbb{Z}[\omega]$.*

Proof. Suppose that $p \equiv 2 \pmod 3$, given that p is not a prime. Thus $p = \pi\gamma$ where $N(\pi), N(\gamma) > 1$. So $p^2 = N(\pi)N(\gamma)$, implying that $N(\pi) = p$. Now we write $\pi = a + b\omega$. Then

$$p = N(\pi) = a^2 - ab + b^2 \text{ Hence } 4p = (2a-b)^2 + 3b^2$$

which implies that $p \equiv (2a-b)^2 \pmod 3$. This is impossible since 1 is the only quadratic residue modulo 3, but we have $p \equiv 2 \pmod 3$. Thus p is a prime. Now suppose that $p \equiv 1 \pmod 3$. Thus by quadratic reciprocity we have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{(p-1)(3-1)}{2}}(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$$

So, there exist integers a and b such that $pb = a^2 + 3$. Hence, p divides

$$(a + \sqrt{-3})(a - \sqrt{-3} = (1 + a + 2\omega)(1 - 2 - \omega)$$

If p was a prime in $\mathbb{Z}[\omega]$,it would have to divide one of the factors. So, p would have to divide either $a+1$ or $a-1$, and, in particular,2. But this is impossible since $p \neq 2$ and hence $\frac{2}{p}$ is irreducible. Thus $p = \pi\gamma$. Hence,

$$p^2 = N(\pi)N(\gamma) \implies p = N(\pi) = \pi\overline{\pi}$$

Notice that

$$x^2 + x + 1 = (x - \omega)(x - \omega^2)$$

Taking norms we obtain $N(1-\omega)^2 = 9$, which is the same as $3 = N(1-\omega)$, By the previous lemma, $1 - \omega$ is prime. This completes the proof. ■

We are now in a position to investigate the properties of the ring $\mathbb{Z}[\omega]$ more thoroughly. We split the elements of $\mathbb{Z}$ into the set of equivalence classes $\mathbb{Z}/p\mathbb{Z}$ via the congruence relation $a \equiv b \pmod{p}$. We may similarly introduce a congruence relation on $\mathbb{Z}[\omega]$ given by $\alpha \equiv \beta \pmod{\gamma}$ which once again means $\gamma \mid (\alpha - \beta)$. This forms the ring $\mathbb{Z}[\omega]/\gamma\mathbb{Z}[\omega]$. The first natural question to ask is how many elements comprise this ring.

Theorem 5.8. *Let π be a prime in $\mathbb{Z}[\omega]$. Then $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field with $N(\pi)$ elements.*

Corollary 5.9. *If $\pi \nmid \alpha$ then $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$*

Proof. The previous theorem showed that $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a finite field with $N(\pi)$ elements, and so every nonzero element has an inverse. Since $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ has $N(\pi)$ elements, it follows that $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ has $N(\pi) - 1$ elements. Now the result follows by Langrange's Theorem. ■

Lemma 5.10. *Suppose that π is a prime such that $N(\pi) \neq 3$ and $\pi \nmid \alpha$. Then there exists a unique $m = 0, 1, 2$ such that $\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod{\pi}$*

Proof. Corollary 4.11 shows that $\pi \mid \alpha^{N(\pi)-1} - 1$. But we know that

$$\alpha^{N(\pi)-1} - 1 = (\alpha^{\frac{N(\pi)-1}{3}} - 1)(\alpha^{\frac{N(\pi)-1}{3}} - \omega)(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2)$$

Since π is prime, it must divide one of the factors. In fact, it can only divide one of the factors, since if it divided two it would have to divide their difference, which is impossible as a consequence of the above discussion. ■

Definition 5.11. Let π be a prime in $\mathbb{Z}[\omega]$. If $N(\pi) \neq 3$ then the cubic residue character of α modulo π is given by

$$\left(\frac{\alpha}{\pi}\right)_3 = 0 \text{ if } \pi \mid \alpha$$

$$\left(\frac{\alpha}{\pi}\right)_3 = \omega^m \text{ for } m = 0, 1, 2 \text{ according to } \alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod{\pi} if p \nmid \alpha$$

The cubic residue character is entirely analogous in the theory of cubic residues to the Legendre symbol in the theory of quadratic residues. Consequently, we have many similar results.

Lemma 5.12. *Let π be a prime in $\mathbb{Z}[\omega]$. Let α and β be elements of $\mathbb{Z}[\omega]$, then*

1) $\alpha^{\frac{N(\pi)-1}{3}} = \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$

2) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$

3) *if* $\alpha \equiv \beta \pmod{\pi}$ *then* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

4) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *if and only if* $x^3 \equiv \alpha \pmod{\pi}$ *has a solution in* $\mathbb{Z}[\omega]$

Proof. (1) This follows immediately from the definition.
(2)

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{\frac{N(\pi)-1}{3}} \equiv (\alpha)^{\frac{N(\pi)-1}{3}} (\beta)^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$$

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$$

(3) If $\alpha = \beta \pmod{\pi}$ Then,

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha)^{\frac{N(\pi)-1}{3}} \equiv (\beta)^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi} \implies \left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$$

■

Remark 5.13. Let a be an integer. When $p \equiv 1 \pmod 3$, part (4) of Lemma 6.12 tells us something interesting about the congruence $x^2 \equiv a \pmod p$. By Theorem 6.8 we know that $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ is isomorphic to $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ Consequently $p \nmid a$ we see that

$$x^3 \equiv a \pmod p \text{ is solvable in } \mathbb{Z} \text{ if and only if } \left(\frac{a}{\pi}\right)_3 = 1$$

Before stating the Law of Cubic Reciprocity, we need the following definition:

Definition 5.14. A prime π in $\mathbb{Z}[\omega]$ is said to be primary if $\pi \equiv \pm 1 \pmod 3$

One can quickly check that exactly two of the associates $\pm\pi, \pm\omega\pi, \pm\omega^2\pi$ are primary by writing $\pi = a + b\omega$ and checking explicit cases.

Theorem 5.15 (Law of Cubic Reciprocity)**.** . *Let* π_1 *and* π_2 *be primary primes with* $N(\pi_1), N(\pi_2) \neq 3$ *and* $N(\pi_1) \neq N(\pi_2)$*, Then*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

The proof is not beyond the scope of the paper, but requires the introduction of Gauss and Jacobi sums, in addition to being very long. Now it's a lot of definitions and lemma's and theorems and We now turn our attention to the main problem of this section.

Theorem 5.16. *Let* p *be a prime. Then,* $p = x^2 + 27y^2$ *if and only if* $p \equiv 1 \pmod 3$ *and 2 is a cubic residue modulo* p*.*

Proof. Suppose that $p = x^2 + 27y^2$. Then, $p \equiv x^2 \equiv 1 \pmod 3$. Now all it remains to show that 2 is a cubic residue modulo p. Let $\pi = x + 3\sqrt{-3}y$ be an element of $\mathbb{Z}[\omega]$ (Notice that $\sqrt{-3} = 1 + 2\omega$). Then $p = \pi\overline{\pi}$ which implies that p is a prime by theorem 6.7.

$$2 \text{ is a cubic residue modulo if and only if } \left(\frac{2}{\pi}\right)_3 = 1$$

We already know that 2 is a primary prime.

$$\pi = x + 3\sqrt{-3}y = x + 3(1 + 2\omega)y = x + 3y + 6\omega y \equiv x \equiv \pm 1 \pmod 3$$

The last congruence holds because if x were divisible by 3, then p would also be divisible by 3. We therefore have that π is primary. By cubic reciprocity, it suffices to show that $\left(\frac{2}{\pi}\right)_3 = 1$

$$\left(\frac{2}{\pi}\right)_3 \equiv (\pi)^{\frac{N(2)-1}{3}} \equiv \pi \pmod 2$$

So, we just need to prove that $\pi \equiv 1 \pmod 2$. But

$$\pi = x + 3y + 6\omega y = x + 3y = x + y \pmod 2$$

since x and y have opposite parity (because $x^2 + 27y^2$ is odd), $\pi \equiv 1 \pmod 2$

Now suppose that $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p, by Theorem 6.8, we can write $p = 4\pi\overline{\pi}$ where π is an element of $\mathbb{Z}[\omega]$. Hence $\pi = a + 3b\omega$ for some integers a and b,

$$4p = 4\pi\overline{\pi} = 4(a^2 - 3ab + 9b^2) = (2a - 3b)^2 + 27b^2$$

Therefore, all we need to do is verify that b is even, since then both sides of the above equation are divisible by four. Since 2 is a cubic residue we have,

$$\left(\frac{2}{\pi}\right)_3 = 1$$

By Cubic reciprocity we know that

$$\left(\frac{\pi}{2}\right)_3 = 1$$

But we know that

$$\left(\frac{\pi}{2}\right)_3 \equiv \pi \equiv 1 \pmod 2$$

Hence, $a + 3b\omega \equiv 1 \pmod 2$, implying that a is odd and b is even. This completes the proof ■

5.2. **Biquadratic Reciprocity.** Similarly to how we were able to use cubic reciprocity to answer the question of when a prime $p = x^2 + 27y^2$, we will use biquadratic reciprocity to show that $p = x^2 + 64y^2$ if and only if $p \equiv 1 \pmod 4$ and 2 is a quadratic residue modulo p. The development of biquadratic reciprocity is almost entirely analogous to that cubic reciprocity. The main difference is that instead of considering the ring $\mathbb{Z}[\omega]$ we consider the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Notice that i is a fourth root of unity, playing the same role as ω, which is a third root of unity. The ring $\mathbb{Z}[i]$ which is also commonly known as Gaussian Integers is an Principal Ideal Domain and hence Unique factorization domain. In gaussian Integers if α is an element of $\mathbb{Z}[i]$ then we define Norm of *alpha* by $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$ and $N(\alpha) = 1$ if and only if α is a unit. Therefore the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. The following results are proved in an entirely similar fashion as the results of the previous section, and so their proofs are omitted.

Lemma 5.17. *Let p be a prime in $\mathbb{Z}$ then,*

- *If $p = 2$ then we can write $2 = i^3(1+i)^2$, where $1+i$ is a prime in $\mathbb{Z}$*
- *If $p \equiv 1 \pmod 4$ then there is a prime $\pi \in \mathbb{Z}[i]$ such that $p = \pi\overline{\pi}$ and primes π and $\overline{\pi}$ are not associated in $\mathbb{Z}[i]$*
- *If $p \equiv 3 \pmod 4$ then p remains prime in $\mathbb{Z}[i]$*

Theorem 5.18. *Let π be an irreducible in $\mathbb{Z}[i]$. Then the ring $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field with $N(\pi)$ elements.*

Corollary 5.19. *if $\pi \nmid \alpha$ then $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$*

Lemma 5.20. *If $\pi \nmid \alpha$ and $N(\pi) \neq 2$ then there exist unique integer m, $0 \leq m \leq 3$ such that*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv i^m \pmod \pi$$

the above lemma allows us to make the following definition.

Definition 5.21. Let π be an irreducible with $N(\pi) \neq 2$. Then the biquadratic residue character of α and π is given by

- $\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$
- If $\alpha \equiv \beta \pmod \pi$ then $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$
- $\left(\frac{\alpha}{\pi}\right)_4 = 1$ if and only if $x^4 \equiv \alpha \pmod \pi$ has a solution in $\mathbb{Z}[\omega]$

Before we state the Law of Biquadratic Reciprocity, we need the following definitions.

Definition 5.22. A non-unit α in $\mathbb{Z}[i]$ is called primary if and only if $\alpha \equiv 1 \pmod{(1+i)^3}$

Theorem 5.23. *(Law of Biquadratic Reciprocity). Let π and λ be relatively prime primary elements of $\mathbb{Z}[i]$, then*

$$\left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{\lambda}{\pi}\right)_4 (-1)^{\frac{N(\pi)-1}{4}\frac{N(\lambda)-1}{4}}$$

The proof is not beyond the scope of the paper, but requires the introduction of Gauss and Jacobi sums, in addition to being very long.

It is very interesting to notice how similar the statement of biquadratic reciprocity is to that of quadratic reciprocity. The relationship between quadratic and biquadratic characters will be used in proving the following theorem, which details the biquadratic character of 2. The reader may also see how the theorem is proven using the supplementary laws of biquadratic reciprocity, by looking at Section $4.B$, of Cox [1].

Theorem 5.24. *If $\pi = a + bi$ is a primary prime in $\mathbb{Z}[i]$ then*

$$\left(\frac{2}{\pi}\right)_4 = i^{\frac{ab}{2}}$$

The proof for this theorem is left for the reader to prove.

Theorem 5.25. *Let p be a prime. Then, $p = x^2 + 64y^2$ if and only if $p \equiv 1 \pmod 4$ and 2 is a cubic residue modulo p*

Proof. Let $p \equiv 1 \pmod 4$ be a prime. By Lemma 6.16 there exists a primary prime $\pi = a+bi$ such that $p = a^2 + b^2 = \pi\overline{\pi}$. Notice that because π is primary, a is odd and b is even. We know that $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is isomorphic to $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Now Theorem 6.23 and definition 6.20 show that

$$\left(\frac{2}{\pi}\right) = i^{\frac{ab}{2}} = 1 \text{ if and only if } x^4 \equiv 2 \pmod p \text{ has a solution in } \mathbb{Z}$$

But this occurs if and only if b is divisible by 8, which immediately implies the result. ■

References

[Cox11] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.