PRIMES OF THE FORM $x^2 + ny^2$ AND THE GEOMETRY OF (CONVENIENT) NUMBERS

THOMAS R. HAGEDORN

In a 1640 letter to Mersenne, Fermat first stated his theorem that an odd prime p can be written in the form x^2+y^2 precisely when $p \equiv 1 \mod 4$. During the next two decades he discovered similar statements for when a prime p could be written in the forms $x^2 + 2y^2$ and $x^2 + 3y^2$. Namely:

$$\begin{aligned} p = x^2 + 2y^2 &\iff p = 2 \quad \text{or} \quad p \equiv 1, 3 \mod 8, \\ p = x^2 + 3y^2 &\iff p = 3 \quad \text{or} \quad p \equiv 1 \mod 3. \end{aligned}$$

As was his custom, Fermat did not give proofs of these statements, but a century later, Euler used Fermat's method of descent to give the first rigorous proofs of these three results (in 1750, 1774, and 1763 respectively).

For any positive integer n, it is natural to ask whether there are congruence conditions that precisely describe the set of primes p such that $p = x^2 + ny^2$, for some $x, y \in \mathbf{Z}$ (with a finite number of exceptions). We call n a convenient number,[1] or *numerus idoneus* in Latin, if there is a finite set S of primes, an integer N, and congruence classes $c_1, \ldots, c_k \mod N$ such that for all primes $p \notin S$,

$$p = x^2 + ny^2 \iff p \equiv c_1, \ldots, c_k \mod N. \tag{1}$$

The work of Fermat and Euler shows that $n = 1, 2, 3$ are convenient numbers. It follows easily from Fermat's original theorem that $n = 4$ is a convenient number as

$$p = x^2 + 4y^2 \iff p \equiv 1 \mod 4.$$

Is 5 a convenient number? Euler thought so and conjectured that for primes $p \neq 5$:

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \mod 20. \tag{2}$$

Lagrange and Gauss rigorously proved this conjecture using the theory of binary quadratic forms.

Euler was particularly interested in finding convenient numbers as they were a useful tool for finding large prime numbers (in Euler's era). Let n be a convenient number. It can be shown that if the equation $x^2 + ny^2 = m$ has exactly one solution of relatively prime positive integers (x, y), then the integer m is prime. If n is a large convenient number, one can significant reduce the number of calculations needed to check if m is prime as one only needs to consider positive integer values for $y \leq \sqrt{m/n}$. For example, Euler correctly conjectured that $n = 1848$ is a convenient number and

[1]This definition can be shown to be equivalent to the definitions of Euler and Gauss.

Convenient Numbers n	$h(-4n)$
1, 2, 3, 4, 7	1
5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58	2
21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253	4
105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760	8
840, 1320, 1365, 1848	16

TABLE 1. Table of the 65 known convenient numbers and the class numbers $h(-4n)$ of the group of binary quadratic forms with discriminant $-4n$.

used it to prove with minimal calcuations that $m = 18,518,809$ is prime as the only positive solution to the equation

$$18,518,809 = x^2 + 1848y^2,$$

is $x = 197$, $y = 100$.

Thus, if Euler could find large convenient numbers, he could find very large prime numbers. Through numerical calculations, Euler found the 65 convenient numbers listed in Table 1, the largest one being $n = 1848$. Remarkably, even though Euler searched up to $10,000$, he found no more convenient numbers. To quote Weil [9, p. 229], "that such a naturally defined set of numbers should apparently be finite, as [Euler] now came to conjecture, was a novel experience to him." In his *Disquisitiones*, Gauss used his theory of positive definite quadratic forms to rigorously prove:

Theorem 1. *The 65 numbers in Table 1 are convenient numbers.*

It is an open question whether there are any more convenient numbers other than those in Table 1. Weinberger [10] showed that there are at most two more convenient numbers and that there is at most one more squarefree convenient number n. If n exists and is odd, then there are exactly 66 convenient numbers. If n exists and is even, then both n and $4n$ are convenient numbers and there are exactly 67 convenient numbers. If n doesn't exist, the list in Table 1 is complete and there are 65 convenient numbers [4].

The main result of this paper is to give an elementary alternative proof of Theorem 1 by proving explicit propositions of type (1) for the 65 values in Table 1. We use only elementary number theory and Minkowski's geometry of numbers. When $n = 1$, this application is well-known, giving Fermat's theorem on $p = x^2 + y^2$, and is often presented as the first application of Minkowski's theory. For other values of n, however, this application does not seem to be in the literature. Such an omission is curious as the only methods used are Minkowski's theory of numbers and elementary number theory. As an example, for $n = 93$, we can easily show:

Proposition 2. *For a prime p,*

$$p = x^2 + 93y^2 \text{ for some } x, y \in \mathbf{Z} \iff$$
$$p \equiv 1, 25, 49, 97, 109, 121, 133, 157, 169, 193, 205, 253, 289, 349, 361 \mod 372.$$

We can similarly prove statements of type (1) for all 65 numbers in Table 1. In this article's last section, we show that the Geometry of Numbers can also be used to prove similar statements for some non-convenient numbers. For example, $n = 14$ is not a convenient number as one can show (by elementary means [7]) that there is no choice of S, N for which a statement of type (1) is true when $n = 14$. But we can easily prove Euler's conjecture:

Proposition 3. *Let $p \neq 2, 7$ be a prime number. There exists $x, y \in \mathbf{Z}$ such that $p = x^2 + 14y^2$ or $p = 2x^2 + 7y^2 \iff p \equiv 1, 9, 15, 23, 25, 39 \mod 56$.*

Hence, Proposition 3 is the best possible statement for $n = 14$ that uses only congruences. We note that both of the binary forms in Proposition 3 represent primes in each of the specified congruence classes and that no prime can be represented by both forms. For instance, consider the two primes $p = 113, 281$. They both satisfy $p \equiv 1 \mod 56$, but $281 = 15^2 + 14(2)^2$, $113 = 2(5)^2 + 7(3)^2$, and neither prime is represented by the other form.

We can also establish Euler's conjecture:

Proposition 4. *Let $p \neq 3$ be a prime number. Then $3p = x^2 + 14y^2$ for some $x, y \in \mathbf{Z}$ $\iff p \equiv 3, 5, 13, 19, 27, 45 \mod 56$.*

The subject of convenient numbers and genus theory is a rich one. For more information on these areas and the complete answer to when we can express a prime p in the form $p = x^2 + ny^2$, we encourage the reader to consult [2]. Kani [4] has also written a comprehensive survey on convenient numbers. In addition, Kani [6, 5] has found that convenient numbers play an important role in studying moduli problems for genus 2 curves and has introduced a new generalization of them. Coincidentally, Clark [1] has also recently written an expository article on convenient numbers similar in spirit to this paper. Clark discusses statements of the form (1) using elementary number theory, but uses Thue's lemma instead of our use of Minkowski's Geometry of Numbers.

1. Congruence Conditions and Quadratic Reciprocity

In order to prove the statement in (1), for a given n, we must determine the congruence conditions that an odd prime p must satisfy. We determine the necessary congruence conditions using the law of quadratic reciprocity. Quadratic reciprocity, discovered by Euler and Legendre and first proved by Gauss [3], gives an efficient way to determine the squares mod p, for an odd prime p. The Legendre symbol is defined for an odd prime p and integers a by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a non-zero square mod } p, \\ -1, & \text{if } a \text{ is not a square mod } p, \\ 0, & \text{if } a \equiv 0 \mod p. \end{cases}$$

Thus, $\left(\frac{3}{11}\right) = 1$ as $5^2 \equiv 3 \mod 11$, whereas $\left(\frac{2}{11}\right) = -1$ as none of the squares $1^2, 2^2, \ldots, 10^2$ modulo 11 equals 2. The following properties of the Legendre symbol are easy to prove.

Lemma 5. *Let p be an odd prime. Then*

1. *If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

By part (2) of Lemma 5, $\left(\frac{-1}{11}\right) = -1$ and -1 is not a square mod 11. By part (3) of the lemma, $\left(\frac{-2}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right) = (-1)(-1) = 1$ and -2 is a square mod 11, as $-2 \equiv 9 \equiv 3^2 \mod 11$ demonstrates. The law of quadratic reciprocity makes the calculation of $\left(\frac{a}{p}\right)$ quite easy for large a, p.

Proposition 6 (Law of Quadratic Reciprocity [3])**.** *Let p, q be two odd primes.*

1. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv 1, 7 \mod 8, \\ -1, & \text{if } p \equiv 3, 5 \mod 8, \end{cases}$

Example. We can now easily determine if 2, 31 are squares mod 71. Since $71 \equiv 7 \mod 8$, 2 is a square. Trial and error shows that $12^2 \equiv 2 \mod 71$. Now

$$\left(\frac{31}{71}\right) = (-1)^{\frac{31-1}{2}\frac{71-1}{2}}\left(\frac{71}{31}\right) = -\left(\frac{71}{31}\right) = -\left(\frac{9}{31}\right) = -(+1) = -1,$$

so 31 is not a square mod 71. The first equality follows from part (2) of the proposition and the third equality follows from part (1) of Lemma 5.

Jacobi generalized the Legendre symbol $\left(\frac{P}{Q}\right)$ to all odd integers P, Q. Let $P = \prod_i p_i^{n_i}$, $Q = \prod_j q_j^{m_j}$ be the prime factorizations and define

$$\left(\frac{P}{Q}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right)^{n_i m_j}.$$

As with the Legendre symbol, $\left(\frac{P}{Q}\right) = -1$ implies that P is not a square mod Q. However, the converse is not true. The law of quadratic reciprocity also holds (amazingly) for the Jacobi symbol and is very useful for efficiently calculating the Legendre symbol $\left(\frac{n}{p}\right)$ for an odd integer n and an odd prime p.

We can now state some essential results used in the convenient number problem.

Lemma 7. *Let p be an odd prime and n an integer with $(n, p) = 1$. Then $p|x^2 + ny^2$ for some relatively prime integers $x, y \iff \left(\frac{-n}{p}\right) = 1$.*

Proof. If $\left(\frac{-n}{p}\right) = 1$, then $-n \equiv x^2 \mod p$ for some $x \in \mathbf{Z}$. So $p|x^2 + n = x^2 + n \cdot 1^2$. Conversely, if $p|x^2 + ny^2$, then $x^2 \equiv -ny^2 \mod p$. If $y \equiv 0 \mod p$, then $x \equiv 0 \mod p$, and x, y would not be relatively prime. Thus, $y \not\equiv 0 \mod p$, y is invertible and $(x/y)^2 \equiv -n \mod p$. So $\left(\frac{-n}{p}\right) = 1$. □

Proposition 8. *Let $n \geq 1$, and p be an odd prime relatively prime to n such that $p = x^2 + ny^2$. Then*

1. $\left(\frac{-n}{p}\right) = 1$ *and* $\left(\frac{p}{q}\right) = 1$ *for every odd prime $q|n$.*
2. $p \equiv 1 \mod 4$ *if* $n \equiv 0, 1 \mod 4$.
3. $p \equiv 1 \mod 8$ *if* $8|n$.

Proof. Lemma 7 proves the first part of (1). The second part follows immediately from reducing $x^2 + ny^2 = p \bmod q$ as x, y must be relatively prime. (2) If $n \equiv 0, 1 \mod 4$, then since $x^2, y^2 \equiv 0, 1 \mod 4$, we have $p = x^2 + ny^2 \equiv 0, 1, 2 \mod 4$. Since p is odd, $p \equiv 1 \mod 4$. Part (3) follows similarly by working mod 8. □

We now translate the three conditions in Proposition 8 into congruence conditions on p. Let

$$S_n = \{ \text{ prime divisors of } n\}.$$

Given n, define

$$N_n = 2^t \prod_{\substack{q|n \\ q \text{ odd} \\ \text{prime}}} q, \text{ where } t = \begin{cases} 0, & \text{if } n \equiv 3 \mod 4, \\ 2, & \text{if } n \equiv 1 \mod 4, \\ 2, & \text{if } n \equiv 4 \mod 8, \\ 3, & \text{if } n \equiv 0, 2, 6 \mod 8. \end{cases} \tag{3}$$

Define

$$k_n = c \prod_{\substack{q|n \\ q \text{ odd} \\ \text{prime}}} \left(\frac{q-1}{2}\right), \quad \text{with } c = \begin{cases} 1, & \text{if } n \equiv 0, 1, 3 \mod 4 \\ 2, & \text{if } n \equiv 2 \mod 4. \end{cases}$$

By the Chinese Remainder Theorem, there are k_n congruence classes $c = c_1, \ldots, c_{k_n} \in (\mathbf{Z}/N_n\mathbf{Z})^*$ defined by the conditions $\left(\frac{c}{q}\right) = 1$ for every odd prime $q|n$ and

$$\begin{aligned} c &\equiv 1 \mod 4 && \text{if } n \equiv 1 \mod 4, \\ c &\equiv 1, 3 \mod 8 && \text{if } n \equiv 2 \mod 8, \\ c &\equiv 1, 7 \mod 8 && \text{if } n \equiv 6 \mod 8, \\ c &\equiv 1 \mod 4 && \text{if } n \equiv 4 \mod 8, \\ c &\equiv 1 \mod 8 && \text{if } n \equiv 0 \mod 8. \end{aligned} \tag{4}$$

Proposition 9. *Given $n > 1$, the $k = k_n$ congruence classes $c_1, \ldots, c_k$ mod N_n have the property that an odd prime p satisfies $p \equiv c_1, \ldots, c_k \mod N_n$ if and only if p satisfies the three conditions:*

1. $\left(\frac{-n}{p}\right) = 1$ *and* $\left(\frac{p}{q}\right) = 1$ *for every odd prime $q|n$.*
2. $p \equiv 1 \mod 4$ *if* $n \equiv 0, 1 \mod 4$.

3. $p \equiv 1 \mod 8$ *if* $8|n$.

Proof. Let $n = 2^r m$, with m odd, and assume p is an odd prime satisfying the three given conditions. Let $\prod_q q^{n_q}$ be the prime factorization of m. Using Jacobi reciprocity, condition (1) gives

$$\begin{aligned}\left(\frac{-n}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{2^a}{p}\right)\left(\frac{m}{p}\right) = (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2^r}{p}\right)\left(\frac{p}{m}\right)\\ &= (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2^r}{p}\right)\prod_{q|m}\left(\frac{p}{q^{n_q}}\right)\\ &= (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2^r}{p}\right)\prod_{q|m}\left(\frac{p}{q}\right)^{n_q}\\ &= (-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2^r}{p}\right).\end{aligned}$$

Condition (1) thus holds if $\left(\frac{p}{q}\right) = 1$ for all odd prime divisors q of n and

$$(-1)^{\frac{p-1}{2}\frac{m+1}{2}}\left(\frac{2^r}{p}\right) = 1. \tag{5}$$

The three conditions (1), (2), (3) are thus equivalent to $\left(\frac{p}{q}\right) = 1$ for all odd prime divisors q of n and p $(= c)$ satisfying the appropriate congruence condition in (4). We demonstrate case when $n \equiv 2 \mod 8$. Then $r = 1$ and $m \equiv 1 \mod 4$. Then equation (5) holds precisely when $p \equiv 1 \mod 4$ and $\left(\frac{2}{p}\right) = 1$, or $p \equiv 3 \mod 4$ and $\left(\frac{2}{p}\right) = -1$. Hence $p \equiv 1, 3 \mod 8$. Then by the definition of the c_i, $p \equiv c_1, \ldots, c_k \mod N_n$. The other cases are established similarly, and the $(\Leftarrow)$ direction is proved. The $(\Rightarrow)$ implication follows immediately by reversing the logic. □

Combining these theorems, we have shown:

Proposition 10. *Given n, there exists a finite set S_n and $k = k_n$ congruence classes $c_1, \ldots, c_k \mod N_n$ such that if $p = x^2 + ny^2$, for an odd prime $p \notin S_n$, then $p \equiv c_1, \ldots, c_k \mod N_n$.*

We note that the congruence classes c_i were explicitly described in the proof of Proposition 9. Other than the explicit formula for k_n, this proposition is unremarkable. But by proving the converse, we will extend Fermat's theorem.

Proposition 11. *Let n be any of the 65 numbers in Table 1. Then there are $k = k_n$ congruence classes $c_1, \ldots, c_k$, mod N_n such that for odd primes $p \notin S_n$,*

$$p = x^2 + ny^2 \Longleftrightarrow p \equiv c_1, \ldots, c_k \mod N_n. \tag{6}$$

As a result, we obtain Theorem 1 as a corollary. We will prove Proposition 11 directly for each of the integers n in Table 1 using Minkowski's theorem. Unfortunately, while this method gives an elementary proof that these 65 numbers are convenient numbers, it doesn't allow one to prove that other numbers are not convenient numbers. To do this, one needs the power of genus theory in Gauss's theory of binary quadratic forms.

2. Minkowski's Geometry of Numbers

An amazing discovery of 19^{th}-century mathematics was Minkowski's simple use of geometry to prove theorems about numbers. We will apply his methods to reprove Theorem 1. We begin by recalling some geometric definitions.

A *symmetric* subset R of $\mathbf{R}^2$ is a subset R with the property that $-x \in R$ whenever $x \in R$. R is *convex* if for all points $x, y \in R$, the line segment l connecting x, y is contained in R. Lastly, a *lattice* L in $\mathbf{R}^2$ is the set of integral linear combinations $av + bw$, $a, b \in \mathbf{Z}$, for two linearly independent vectors $v, w \in \mathbf{R}^2$. A *fundamental domain* for L is the region of $\mathbf{R}^2$ defined by

$$\mathcal{F} = \{\, rv + sw |\, 0 \leq r, s < 1,\, r, s \in \mathbf{R}\}.$$

$\mathcal{F}$ has the property that one can translate every point x in the plane by an element of the lattice L to a point in $\mathcal{F}$. In other words, $x = l + y$, for some $l \in L$, $y \in \mathcal{F}$. From linear algebra, the area of $\mathcal{F}$ equals $|\det M|$, where M is the matrix whose rows are the vectors v, w. If $v, w \in \mathbf{Z}^2$, then L is a subgroup of $\mathbf{Z}^2$, and the area of $\mathcal{F}$ equals the index $[\mathbf{Z}^2 : L]$ of L in $\mathbf{Z}^2$.

The following simple geometric proposition is the foundation for Minkowski's Geometry of Numbers.

Proposition 12 (Minkowski)**.** *Let L be a lattice in $\mathbf{R}^2$ whose fundamental domain has area V. If R is a convex, symmetric subset of $\mathbf{R}^2$ with $\mathrm{Area}(R) > 4V$, then R contains a non-zero point of L.*

Proof. Consider the lattice $2L$. Since $2L$ has index 4 in L, its fundamental domain has area $4V$. Now translate every point of R by a vector in $2L$ into the fundamental domain for $2L$. Since $\mathrm{Area}(R) > 4V$, there must be two points $x, y \in R$ whose translates coincide. Hence $x = y + 2z$, for some non-zero element $z \in L$. Now if $y \in R$, then $-y \in R$ since R is symmetric. And if $-y, y + 2z \in R$, then the midpoint of the line connecting them $[-y + (y + 2z)]/2 = z$ must be in R since R is convex. Hence R contains a non-zero point of L. □

3. Convenient Numbers

Fermat's theorem on the sum of squares shows that $n = 1$ is a convenient number. Its proof via Minkowski's Geometry of Numbers is well-known and is often the first example of Minkowski's theory in elementary number theory texts [8]. We begin our proof of Theorem 1 by proving Euler's conjecture that $n = 5$ is a convenient number.

Proposition 13. *Let p be an odd prime. Then $p = x^2 + 5y^2$ for some integers x, y if and only if $p \equiv 1, 9 \mod 20$.*

Proof. ($\Rightarrow$) By Proposition 8, we know $\left(\frac{p}{5}\right) = 1$ and $p \equiv 1 \mod 4$, or equivalently $p \equiv 1, 9 \mod 20$. ($\Leftarrow$) The hypothesis $p \equiv 1, 9 \mod 20$ is exactly the congruence condition on p specified by Proposition 9 for $n = 5$. Thus, by Proposition 9, $\left(\frac{-5}{p}\right) = 1$ and there exists an integer u such that $u^2 \equiv -5 \mod p$. Now consider the lattice $L \subset \mathbf{R}^2$ defined by

$$L = \{(a, b) \in \mathbf{Z}^2 | a \equiv ub \mod p\}.$$

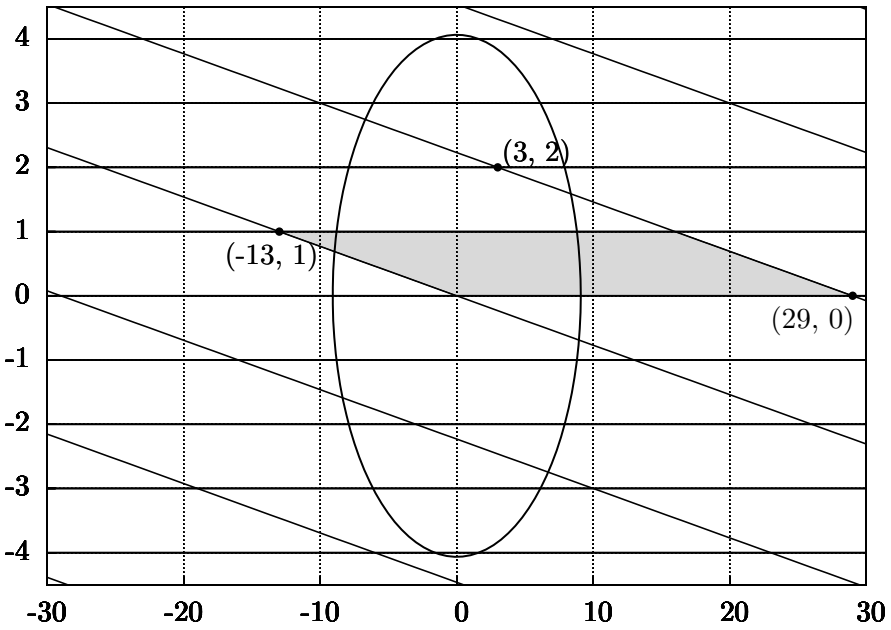

FIGURE 1. The lattice L generated by $(-13, 1)$ and $(29, 0)$ has the fundamental domain shaded above. The domain has area 29 and the ellipse $x^2 + 5y^2 = B_5 \cdot 29$ has area $4 \cdot 29$. By the Geometry of Numbers, the ellipse must contain a non-zero integral lattice point in L. The only such points are $\pm(3, 2)$.

L is generated by the vectors $v = (p, 0)$, $w = (u, 1)$ and has index $\begin{vmatrix} p & 0 \\ u & 1 \end{vmatrix} = p$ in $\mathbf{Z}^2$. Consequently, the area of its fundamental domain has area p. Let R_k be the ellipse defined by $x^2 + 5y^2 = k$. Then R_k has area $\pi k/\sqrt{5} > 1.4k$. Choose $k = 2.84p$. Then Area $R_k > 4p$, and $R_k \cap L$ contains a non-zero point (a, b). Now

$$a^2 + 5b^2 \equiv (ub)^2 + 5b^2 \equiv -5b^2 + 5b^2 \equiv 0 \mod p,$$

so $p|a^2 + 5b^2$. Now since $(a, b) \in R_k$, we have $a^2 + 5b^2 \leq 2.84p$, so $a^2 + 5b^2 = p$ or $2p$. We now show that the latter case cannot occur. Suppose $a^2 + 5b^2 = 2p$. Then $a^2 \equiv 2p \equiv 2 \mod 5$, which gives a contradiction as 2 is not a square mod 5. Hence $a^2 + 5b^2 = p$ and ($\Leftarrow$) is proved. □

We can prove Proposition 11 for all 65 convenient numbers in Table 1 by modifying this argument. Proposition 10 proves the ($\Rightarrow$) direction in general and establishes the explicit congruence conditions on p. It only remains to prove the ($\Leftarrow$) direction. Define

$$B_n = [4\sqrt{n}/\pi]$$

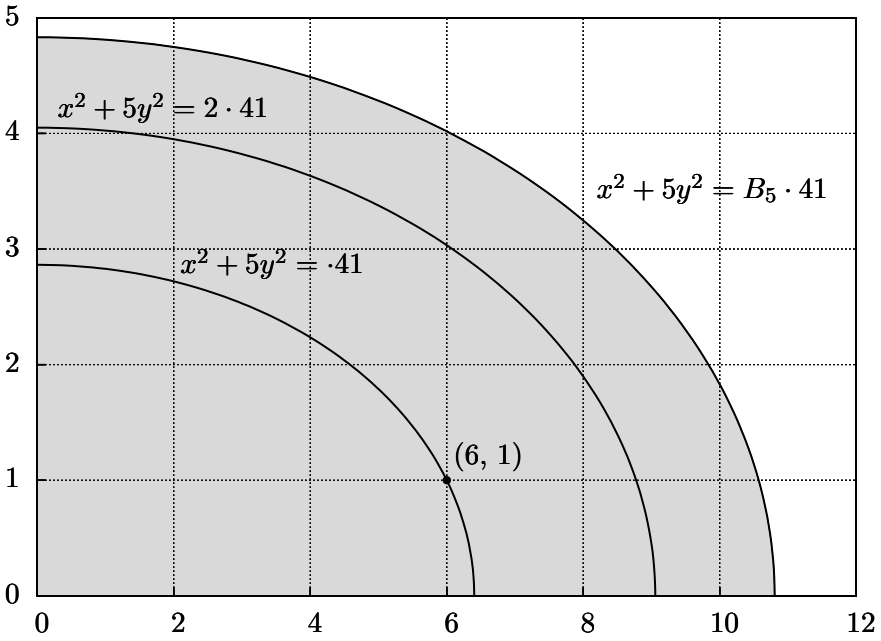

FIGURE 2. An illustration of the Geometry of Numbers argument for $x^2 + 5y^2 = p$, for $p = 41$. Since $B_5 \approx 2.84$, there must be an integral point lying on one of the two ellipses $x^2 + 5y^2 = 41$, $x^2 + 5y^2 = 2 \cdot 41$.

The proof of Proposition 13($\Leftarrow$) consisted of three main steps. First, the congruence $p \equiv 1, 9 \mod 20$ implied $\left(\frac{-5}{p}\right) = 1$. Second, Geometry of Numbers showed that the equation $x^2 + 5y^2 = dp$ has a solution for some $d \leq 2 = B_5$. Lastly, we showed that the equation $x^2 + 5y^2 = 2p$ did not have a solution. Hence the equation $x^2 + 5y^2 = p$ must have a solution when $p \equiv 1, 9 \mod 20$. Hence, for a general n, our strategy would be:

1. The congruence conditions on p specified by Proposition 9 imply $\left(\frac{-n}{p}\right) = 1$.
2. (Geometry of Numbers) By Minkowski's theory, $\left(\frac{-n}{p}\right) = 1$ implies that the equation $x^2 + ny^2 = dp$ has a solution (a, b) for some positive integer $d \leq B_n$.
3.* For each integer d with $1 < d \leq B_n$, show that the equation $x^2 + ny^2 = dp$ has no solution.

While the first two steps are valid for all values of n, the third step becomes more difficult. As n and B_n become larger, there are more cases of d to consider. To tackle these additional cases, the following lemma proves useful.

Lemma 14. *Let p, q be distinct odd primes. Assume $\left(\frac{p}{q}\right) = 1$, $q|n$, and $q \nmid d$. If $\left(\frac{d}{q}\right) = -1$, then the equation $x^2 + ny^2 = dp$ has no integral solutions.*

Proof. Assume that $x^2 + ny^2 = dp$ for some x, y. Then $x^2 \equiv dp \not\equiv 0 \mod q$. So $\left(\frac{dp}{q}\right) = 1$, but this contradicts the hypothesis that $\left(\frac{dp}{q}\right) = -1$. Hence, the equation has no solution. □

We will now try to prove Proposition 2 using the above method. We will run into one new situation.

Proof of Proposition 2. The direction ($\Rightarrow$) was already proved in Proposition 10. ($\Leftarrow$) Using the above framework, Geometry of Numbers shows that there are is a positive integer $d \leq B_{93} = 12$ such that the equation $x^2 + 93y^2 = dp$ has a solution. To finish the proof we need to show that $d = 1$ has this property.

By the given congruence conditions for p, $\left(\frac{p}{3}\right) = \left(\frac{p}{31}\right) = 1$. By Lemma 14, the choices $d = 2, 3, 5, 6, 7, 8, 11$ can be eliminated as $\left(\frac{d}{3}\right) = -1$ or $\left(\frac{d}{31}\right) = -1$. That leaves the choices $d = 4, 9, 10, 12$. We now show that there is no solution when $d = 12$. For if $x^2 + 93y^2 = 12p$, then $x^2 + y^2 \equiv 0 \mod 4$. Then both x, y must be even and $(x/2)^2 + 93(y/2)^2 = 3p$. But this gives a contradiction as the equation $x^2 + 93y^2 = dp$ has no solution when $d = 3$. Hence, there cannot be a solution when $d = 12$.

We now analyze the case $d = 10$. From the congruence criteria, $p \equiv 1 \mod 4$ and $2p \equiv 2 \mod 8$. If $x^2 + 93y^2 = 10p$, then reducing modulo 4, $x^2 + y^2 \equiv 2 \mod 4$ and both x, y must be odd. So $x^2, y^2 \equiv 1 \mod 8$ and $x^2 + 93y^2 \equiv x^2 + 5y^2 \equiv 6 \mod 8$. But as $10p \equiv 2p \equiv 2 \mod 8$, $x^2 + 93y^2 \not\equiv 10p \mod 8$ and $x^2 + 93y^2 = 10p$ cannot have a solution.

The remaining cases $d = 4, 9$ are handled differently. We first consider $d = 4$. If $x^2 + 93y^3 = 4p$ has a solution, then $x^2 + y^2 \equiv 0 \mod 4$, which forces x, y to both be even. Thus $(x/2)^2 + 93(y/2)^2 = p$ and the original equation $x^2 + 93y^2 = p$ has a solution. So $x^2 + 93y^2 = 4p$ has a solution precisely when $x^2 + 93y^2 = p$ has a solution. When $d = 9$, a similar situation occurs. If the equation $x^2 + 93y^2 = 9p$ has a solution, then so does the equation $x^2 + 93y^2 = p$.

Summarizing, we have seen that for every choice of d with $1 < d \leq B_{93}$, that either the equation $x^2 + 93y^2 = dp$ has no solution or if it has a solution, then so does the equation $x^2 + 93y^2 = p$. Thus, the equation $x^2 + 93y^2 = p$ has a solution. □

In light of the new wrinkle caused by the cases $d = 4, 9$ in the above proof, we need to revise step 3*. We introduce the following terminology:

Definition 15. Fix n and let $c_1, \ldots, c_k \mod N_n$ be the congruence classes defined in Proposition 9. We say d is *regular* for n if p is a prime satisfying $p \equiv c_1, \ldots, c_k \mod N_n$ and if the equation $x^2 + ny^2 = dp$ has an integral solution, then the equation $x^2 + ny^2 = d'p$ has an integral solution for some positive integer $d' < d$.

We note that if the equation $x^2 + ny^2 = dp$ never has an integral solution for primes p satisfying $p \equiv c_1, \ldots, c_k \mod N_n$, then d is regular for n. Thus, to prove Proposition 11, we replace Step (3*) in the strategy above with:

3. (Descent) For each d satisfying $1 < d \leq B_n$, show that d is regular for n.

Using this terminology, Lemma 14 can be rewritten as follows:

Lemma 16. *Let q be an odd prime divisor of n. If $q \nmid d$ and $\left(\frac{d}{q}\right) = -1$, then d is regular for n.*

The case $d = 10$ in the proof for $n = 93$ follows from a similar lemma.

Lemma 17. *Let q be an odd prime divisor of d with $(q, n) = 1$ and $\left(\frac{-n}{q}\right) = -1$. Then d is regular for n.*

Proof. Let p be a prime satisfying the congruence conditions in Proposition 9. As a result $\left(\frac{-n}{p}\right) = 1$. Thus $q \neq p$. Suppose $x^2 + ny^2 = dp$ for some integers x, y, d. Then $x^2 \equiv -ny^2 \mod q$. Since $\left(\frac{-n}{q}\right) = -1$, $x \equiv y \equiv 0 \mod q$. Letting $x = qx_0, y = qy_0$, one has $q^2(x_0^2 + ny_0^2) = dp$. Since $q \neq p$, $q^2|d$ and the equation $x^2 + ny^2 = d'p$ has a solution for $d' = d/q^2$. Thus, d is regular for n. □

Similarly the cases $d = 4, 9$ follows from:

Lemma 18. *(a) If $n \equiv 1 \mod 4$ and $4|d$, then d is regular for n. (b) Let q be prime and let l be an odd integer such that $q^l|(n, d)$. If $\left(\frac{n/q^l}{q}\right) \neq \left(\frac{d/q^l}{q}\right)$, then d is regular for n.*

Proof. (a) Assume $x^2 + ny^2 = dp$. Then $x^2 + y^2 \equiv 0 \mod 4$. Hence both x, y are even and $(x/2)^2 + n(y/2)^2 = (d/4)p$. Since $d/4 < d$, d is regular for n. (b) Let $l = 2m + 1$, $n = q^l n_0$, $d = q^l d_0$. Assume $x^2 + q^l n_0 y^2 = q^l d_0 p$. Then $x^2 \equiv 0 \mod q^l$ and $x = q^{m+1}x_0$. Since $qx_0^2 + n_0y^2 = d_0p$, $n_0y^2 \equiv d_0p \mod q$. Suppose $y \not\equiv 0 \mod q$. Since $\left(\frac{y^2}{q}\right) = \left(\frac{p}{q}\right) = 1$, one has $\left(\frac{n_0}{q}\right) = \left(\frac{d_0}{q}\right)$, contradicting the hypothesis. Hence, $y \equiv 0 \mod q$. Then $(x/q)^2 + n(y/q)^2 = (d/q^2)p$ and d is regular. □

Unfortunately, when either n or d is even, there appears to be no single method for showing that d is regular for n. Instead, one needs several lemmas to cover all the cases that arise. We summarize Lemmas 16, 17, 18 and the additional congruence lemmas in the following proposition.

Proposition 19. *Given n, d, if one of the following conditions is satisfied then d is regular for n.*

a. There exists an odd prime divisor q of n with $q \nmid d$ and $\left(\frac{d}{q}\right) = -1$.
b. There exists an odd prime divisor q of d with $(q, n) = 1$ and $\left(\frac{-n}{q}\right) = -1$.
c. $n \equiv 1 \mod 4$ and $4|d$.
d. There exists an odd prime q and an odd integer l such that q^l is the highest power of q dividing (n, d) and $\left(\frac{n/q^l}{q}\right) \neq \left(\frac{d/q^l}{q}\right)$.
e. There is an odd integer k such that 2^k is the highest power of 2 dividing (n, d) and either $2^{k+1}|n$ or $2^{k+1}|d$.
f. $n \equiv 3 \mod 4$ and $d = 2$.
g. $d = 4$ and $n \equiv 7 \mod 8$, $n \equiv 8, 12 \mod 16$, or $n \equiv 16 \mod 32$.
h. $4|n$ and $d \equiv 3 \mod 4$.
i. $8|n$ and $d \equiv 5 \mod 8$.
j. $(n, d) \equiv (3 \cdot 4^a, 4^a) \mod 4^{a+1}$ for some $a \geq 1$.
k. $(n, d) \equiv (2 \cdot 9^a, 9^a) \mod 3^{2a+1}$ for some $a \geq 1$.

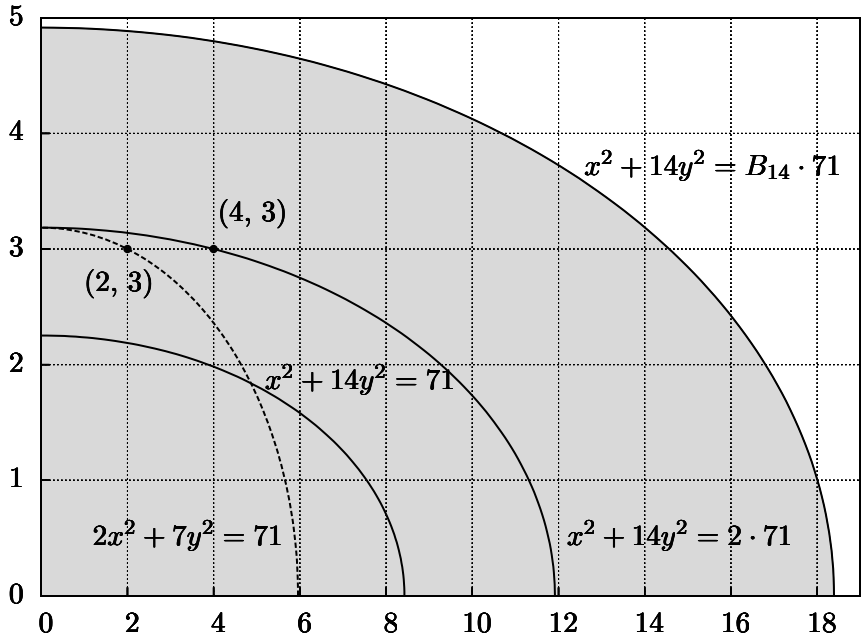

FIGURE 3. If $n = 14$ were a convenient number, then since $p = 71$ satisfies the necessary congruence criteria, the equation $x^2 + 14y^2 = 71$ would have an integral solution. However, 14 is not a convenient number. The solution guaranteed by the Geometry of Numbers argument lies on the ellipse $x^2 + 14y^2 = 2 \cdot 71$. The prime 71 is represented by another quadratic form, $2x^2 + 7y^2$, which lies in the same genus as $x^2 + 14y^2$.

We note that criteria (e) is the analogue of criteria (d) for the prime $q = 2$ and criteria (f)-(j) cover special cases when either d or n is divisible by a power of 2. We omit the proofs of criteria (e)-(k) as they are proved in the same manner as Lemmas 16, 17, and 18 above. Using the proposition, one can carry out Step (3) above and show that for every value n in Table 1, every $d \leq B_n$, $d \neq 1$ is regular for n. Hence, all 65 values in Table 1 are convenient numbers and Theorem 1 is proved.

Of the 11 criteria listed in Proposition 19 that are used in the proof of Theorem 1, four of them are used for only a single pair (n, d). Criteria (f) is only needed for $(n, d) = (7, 2)$; criteria (i) for $(16, 5)$; criteria (j) for $(240, 16)$; and criteria (k) for $(72, 9)$.

4. Applications to $x^2 + ny^2 = pq$ and Non-Convenient Numbers

Minkowski's Geometry of Numbers can be used in a similar way as in the previous section to prove theorems about the expressibility of specific composite numbers by a quadratic form.

Proposition 20. *Let $p, q \equiv 3, 7 \pmod{20}$ be odd primes. Then $pq = x^2 + 5y^2$ for some integers x, y.*

Proof. The congruence conditions give $\left(\frac{-5}{p}\right) = \left(\frac{-5}{q}\right) = 1$. So there exists solutions to the equations $x^2 \equiv -5 \pmod{p}$, $x^2 \equiv -5 \pmod{q}$. By the Chinese Remainder Theorem, there is an integer u such that $u^2 \equiv -5 \mod pq$. Now consider the lattice $L \subset \mathbf{R}^2$ defined by

$$L = \{(a, b) \in \mathbf{Z}^2 | \, a \equiv ub \mod pq\}.$$

As L has index pq in $\mathbf{Z}^2$, its fundamental domain has area pq. Let R_k be the ellipse defined by $x^2 + 5y^2 = k$. Then R_k has area $\pi k/\sqrt{5} > 1.4k$. Choose $k = 2.9pq$. Then Area $R_k > 4pq$, and $R_k \cap L$ contains a non-zero point (a, b). Now

$$a^2 + 5b^2 \equiv (ub)^2 + 5b^2 \equiv -5b^2 + 5b^2 \equiv 0 \mod pq,$$

so $pq | a^2 + 5b^2$. Now since $(a, b) \in R_k$, we have $a^2 + 5b^2 < 2.9p$, so $a^2 + 5b^2 = pq$ or $2pq$. Now if $a^2 + 5b^2 = 2pq$, then regarding the equation mod 5 shows that $2pq \equiv \pm 2 \pmod{5}$ is a square, giving a contradiction. Hence $a^2 + 5b^2 = pq$. □

It is straightforward to see that one can prove statements similar to Proposition 20 for any convenient number n. But the usefulness of this method is not limited solely to convenient numbers. It can prove a limited number of similar statements for other numbers. For example, we can prove Euler's conjecture Proposition 3, which is normally proved via genus theory.

Proof of Proposition 3. The congruence conditions in the ($\Rightarrow$) direction immediately follow from quadratic reciprocity as both equations $x^2 + 14y^2 = p$, $2x^2 + 7y^2 = p$ mod p imply $\left(\frac{-14}{p}\right) = 1$. ($\Leftarrow$) The congruence conditions imply that $-14 \equiv u^2 \mod p$ for some u. Using Geometry of Numbers as in proof of Proposition 20, we find that the equation $x^2 + 14y^2 = dp$ has an integral solution for some $d = 1, 2, 3$, or 4. As $\left(\frac{3}{7}\right) = -1$, $d = 3$ is regular for $n = 14$ by Proposition 19(a) and can be dismissed. Similarly $d = 4$ is regular by Proposition 19(e). If $d = 1$, we are done. If $d = 2$, then x must be even. Letting $x = 2x_0$, one has $2x_0^2 + 7y^2 = p$ and the proposition is proved. □

Similarly, we can establish Euler's conjecture Proposition 4, which is usually proved using Gauss's composition theory for binary forms.

Proof of Proposition 4. (a)($\Rightarrow$) We can assume $p \neq 2, 3, 7$. Then any solution (x, y) must be relatively prime. Then $\left(\frac{-14}{p}\right) = \left(\frac{3p}{7}\right) = 1$ and quadratic reciprocity gives $p \equiv 3, 5 \pmod{8}$, $p \equiv 3, 5, 6 \pmod{7}$, which gives the desired congruences. ($\Leftarrow$) The congruence conditions imply $\left(\frac{-14}{p}\right) = 1$. Hence, as in the proof of Proposition 3, there exists a solution (x, y) with $x^2 + 14y^2 = dp$, for some $d = 1, 2, 3, 4$. If $d = 1, 2, 4$, then $x^2 \equiv dp \pmod{7}$ and $\left(\frac{p}{7}\right) = 1$, contradicting the congruence conditions on p. Thus $d = 3$ and $x^2 + 14y^2 = 3p$. □

Does Proposition 4 have a generalization similar to Proposition 20? Yes, Proposition 4 is but a specific case of the following more general proposition.

Proposition 21. *Let p, q be odd primes with $p, q \equiv 3, 5, 13, 19, 27, 45 \mod 56$. Then $pq = x^2 + 14y^2$ for some integers x, y.*

Unfortunately, the methods of this paper are too weak to prove Proposition 21! In order to prove it, we must use the more powerful methods of Gauss's theory of genera. We now illustrate the problem one encounters when one tries to generalize the proof of Proposition 4 to prove Proposition 21.

Assume p, q are given as in the hypothesis of Propostion 21. Following the proof of Proposition 20, one can show that there exists a solution to $x^2 + 14y^2 = pqd$, for some positive integer $d \leq 4$. If $d = 4$, then x, y would both be even, and there would be a solution to $x^2 + 14y^2 = pq$. If $d = 3$, then $\left(\frac{3pq}{7}\right) = 1$, but $\left(\frac{3}{7}\right) = \left(\frac{p}{7}\right) = \left(\frac{q}{7}\right) = -1$, giving a contradiction. But when we consider the case $d = 2$, we cannot obtain a contradiction as 2 is a square mod 7. As a result, we know that there is a solution to the equation $x^2+14y^2 = pq$ or the equation $x^2+14y^2 = 2pq$, but we cannot definitely say that either equation can be solved!

Using genus theory one can show that the both equations can always be solved. We now sketch a proof of both this claim and Proposition 21, and refer the reader to [2] for background material. The class group of binary quadratic forms with discriminant -56 consists of 4 forms divided up into two genera. The principal genus of forms with discriminant -56 consists of $e = x^2 + 14y^2$, the identity element for the group, and $f = 2x^2 + 7y^2$; the other genus consists of the two forms $g = 3x^2 + 2xy + 5y^2$, $h = 3x^2 - 2xy + 5y^2$. By genus theory, one can show that primes p, q satisfying the hypotheses in Proposition 21 are represented by either g or h. However, as g, h represent exactly the same values in $\mathbf{Z}$ (since one can replace (x, y) by $(x, -y)$), we can assume g represents p and h represents q. Gauss's law of composition for quadratic forms then shows that pq is represented by the composition form $g \circ h$. Since $e = g \circ h$, $x^2+14y^2 = pq$ has an integral solution, proving Proposition 21. Similarly, f represents the number 2, so $h = f \circ g$ represents $2p$. Since g represents q, we have that $2pq$ is represented by $g \circ h = e$, and $x^2 + 14y^2 = 2pq$ has a solution as well.

References

[1] P. Clark, *Integers Represented by Idoneal Quadratic Forms*, www.math.uga.edu/~pete/thuelemmav3.pdf.

[2] D. Cox, *Primes of the Form x^2+ny^2 : Fermat, Class Field Theory, and Complex Multiplication*, Wiley, 1997.

[3] C. F. Gauss, (1801) *Disquisitiones Aritmeticae*, trans. by Arthur A. Clarke, Yale University Press, 1965.

[4] E. Kani, *Idoneal Numbers and some Generalizations*, www.mast.queensu.ca/~kani/papers/idoneal.pdf.

[5] E. Kani, *The existence of Jacobians isomorphic to a product of two elliptic curves*, Preprint.

[6] E. Kani, *The moduli space of Jacobians isomorphic to a product of two elliptic curves,* Preprint.

[7] B. Spearman, K. S. Williams, *Representing Primes by Binary Quadratic Forms,* American Mathematical Monthly, **99**(5) (1992), pp. 423-426

[8] I. Stewart, D. Tall, *Algebraic Number Theory and Fermat's Last Theorem, 3rd Ed.,* A.K. Peters, Natick, MA 2001.

[9] A. Weil, *Number Theory: An Approach Through History,* Birkhäuser, Boston, Basel, and Stuttgart, 1984.

[10] P.J. Weinberger, *Exponents of the class groups of complex quadratic fields,* Acta Arith. **22** (1973), pp. 117–124.

E-mail address: hagedorn@tcnj.edu

Department of Mathematics and Statistics, The College of New Jersey, P.O. Box 7718, Ewing, NJ 08628