

INTEGERS REPRESENTED BY IDONEAL QUADRATIC FORMS

PETE L. CLARK

ABSTRACT. There are 65 known positive integers n for which a prime number p prime to D is of the form $x^2 + ny^2$ iff p lies in certain congruence classes modulo $4n$: these are the **idoneal numbers**. (It is known that there is at most one further such number and if such a 66th idoneal number exists, then the Generalized Riemann Hypothesis is false.) For $n = 1$ this is Fermat's Two Squares Theorem: an odd prime is of the form $x^2 + y^2$ iff $p \equiv 1 \pmod{4}$. In this case, it is also well known exactly which composite integers are sums of two squares, but I have not been able to find in the literature analogous characterizations of all positive integers of the form $x^2 + ny^2$ for all idoneal n . In this note (a work in progress!) I attempt to solve this problem using only tools familiar to the student of elementary number theory. Especially, I do not assume any prior familiarity with quadratic forms, and all needed concepts and results on quadratic forms are developed from scratch.

INTRODUCTION

Recently I learned (from Mariah Hamel) about **Thue's Lemma**, an elementary result on congruences due to the Norwegian mathematician Axel Thue (1863-1922). I was able to track the result down in several texts – [3, Thm. 11-7], [1, Prop., Ch. 4], [4, Thm. 2.33] – but I believe it is not “well-known”. These texts use Thue's Lemma (only) to prove Fermat's Two Squares Theorem, or more precisely to deduce it from the fact that if $p \equiv 1 \pmod{4}$, then -1 is a square mod p (“Fermat's Lemma”). To be sure, there are many other nice proofs of Fermat's Two Squares Theorem, so if this were the only use of Thue's Lemma then perhaps its relative obscurity would be well-deserved.

The purpose of this note is to show that in fact Thue's Lemma can be used to prove many other results on the representation of integers by binary quadratic forms. None of the results that we present here are new – although some are difficult (or impossible?) to find in the contemporary literature – and many of them are theorems of Fermat, Euler or Lagrange, hence very old indeed. However, the more traditional proofs require some rudiments of the theory of binary quadratic forms or the arithmetic of quadratic rings, including some technicalities when $\mathbb{Z}[\sqrt{-D}]$ is not the full ring of integers of $\mathbb{Q}(\sqrt{-D})$. The proofs that I present here use only quadratic reciprocity, and seem distinctly more graceful than the traditional ones. Thus I submit to you that Thue's Lemma should appear more prominently in elementary texts and courses.

Date: June 17, 2010.
© Pete L. Clark, 2010.

1. THUE'S LEMMA

Theorem 1. (*Thue's Lemma*) Let $n > 1$ be an integer, and let c be an integer which is relatively prime to n . Then there exist integers x and y such that

- (i) $0 < |x|, |y| \leq \sqrt{n}$ and
- (ii) $x \equiv cy \pmod{n}$.

Proof. For $1 \leq i, j \leq \lfloor \sqrt{n} \rfloor + 1$, consider the integers $M(i, j) = i - cj$. We get a matrix with $(\lfloor \sqrt{n} \rfloor + 1)^2 > n$ entries, so there exist $(i_1, j_1) \neq (i_2, j_2)$ such that

$$i_1 - cj_1 \equiv i_2 - cj_2 \pmod{n}.$$

Put $x = i_1 - i_2$ and $y = j_1 - j_2$; then (ii) holds. Moreover, $0 \leq |x|, |y| \leq \sqrt{n} < n$, so x (resp. y) is 0 iff it is zero modulo n . By construction x and y are not both 0, and by (ii) if one is zero modulo n so is the other. So both x and y are nonzero. \square

2. SOME PRELIMINARIES

2.1. Quadratic reciprocity law.

Recall that for an integer n and an odd prime p , the **Legendre symbol** $\left(\frac{n}{p}\right)$ is defined to be 0 if $p \mid n$, 1 if $\gcd(p, n) = 1$ and n is a square modulo p and -1 if n is not a square modulo p .

Theorem 2. (*Quadratic Reciprocity*) Let ℓ and p be distinct odd primes. Put $\ell^* = (-1)^{\frac{\ell-1}{2}} \ell$. Then:

- a) $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$.
- b) $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}$.
- c) $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$.

2.2. Binary quadratic forms.

By a **binary quadratic form** we mean a polynomial

$$Q(x, y) = Ax^2 + Bxy + Cy^2$$

with $A, B, C \in \mathbb{Z}$. The **discriminant** of $Q(x, y)$ is defined as

$$\Delta = B^2 - 4AC.$$

Evidently $\Delta \equiv 0, 1 \pmod{4}$. Conversely, given any integer $\Delta \equiv 0, 1 \pmod{4}$, there exists a binary quadratic form of discriminant Δ . Indeed, if $\Delta = 4D$ then the quadratic form

$$q_\Delta(x, y) = x^2 - Dy^2$$

has discriminant $4D$; whereas if $\Delta \equiv 1 \pmod{4}$, the quadratic form

$$q_\Delta(x, y) = x^2 + xy + \frac{1 - \Delta}{4}y^2$$

has discriminant Δ . The forms q_Δ are called **principal**. An integer n is **represented by the form** Q if there exist $x, y \in \mathbb{Z}$ such that $Q(x, y) = n$. An integer n is **primitively represented** by Q if there exist $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$ such that $Q(x, y) = n$.

Proposition 3. *Let $Q(x, y)$ be a quadratic form of discriminant D ; let $n \in \mathbb{Z} \setminus \{0\}$.*

a) If n is squarefree, then all representations of n by $Q(x, y)$ are primitive.

b) If $Q(x, y)$ primitively represents n , then D is a square mod n .

Proof. a) Suppose $n = Q(x, y)$ and $e = \gcd(x, y)$. Then $e^2 \mid n$.

b) Suppose there exist $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$ such that $Q(p, q) = n$. Then there exist integers r and s such that $ps - rq = 1$. Then the matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ has determinant 1, so that the discriminant D' of the quadratic form $Q'(x, y) = Q(px + qy, rx + sy)$ is equal to D . On the other hand, we compute

$$Q'(x, y) = Q(px + qy, rx + sy) = nx^2 + (2apr + bps + brq + 2cqs)xy + Q(r, s)y^2.$$

Thus

$$D = D' = (2apr + bps + brq + 2cqs)^2 - 4nQ(r, s),$$

showing that D is a square modulo n . □

For nonsquarefree values of n , we must continue to make a distinction between primitive representations by $x^2 + Dy^2$ and arbitrary representations by $x^2 + Dy^2$. The following simple result, known already to Euler, is helpful in this regard.

Proposition 4. *Let D, x_1, x_2, y_1, y_2 be positive integers. Then:*

a) $(x_1x_2 - Dy_1y_2)^2 + D(x_1y_2 + x_2y_1)^2 = (x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2)$.

b) (ANALOGUE FOR FORMS OF ODD DISCRIMINANT).

Proof. Direct calculation verifies part a). For part b) □

Corollary 5. *For any $\Delta \equiv 0, 1 \pmod{4}$, the set of integers represented by the principal form q_Δ is closed under multiplication.*

Theorem 6. *Let $D \in \mathbb{Z}^+$ and let p be a prime with $\left(\frac{-D}{p}\right) = -1$.*

a) Suppose $x, y \in \mathbb{Z}$ are such that $p \mid x^2 + Dy^2$. Then $p \mid x$ and $p \mid y$.

b) For all $x, y \in \mathbb{Z}^+$, $\text{ord}_p(x^2 + Dy^2)$ is even.

Proof. Let $R = \mathbb{Z}[\sqrt{-D}]$ be the integral domain $\mathbb{Z}[t]/(t^2 + D)$. Any element of R may be expressed as $x + y\sqrt{-D}$ for unique $x, y \in \mathbb{Z}$.

Step 1: We claim that for a prime p such that $-D$ is not a square modulo p , the ideal $(p) = pR$ is a prime ideal of R . Equivalently, the quotient ring R/pR is an integral domain. Now $R/pR = \mathbb{Z}[t]/(t^2 + D, p) = \mathbb{Z}/p\mathbb{Z}[t]/(t^2 + D)$, and that $-D$ is not a square modulo p means precisely that the polynomial $(t^2 + D)$ over the finite field $\mathbb{Z}/p\mathbb{Z}$ is irreducible. Hence $(t^2 + D)$ is a prime ideal of $\mathbb{Z}/p\mathbb{Z}[t]$, so R/pR is a domain.

Step 2: In the ring R we have the factorization

$$x^2 + Dy^2 = (x + \sqrt{-D}y)(x - \sqrt{-D}y).$$

Then $p \mid x^2 + Dy^2$, meaning $(x + \sqrt{-D}y)(x - \sqrt{-D}y) \in pR$. Since pR is prime, one of $x \pm \sqrt{-D}y$ lies in pR . That is, $\frac{x}{p} \pm \sqrt{-D}\left(\frac{y}{p}\right) \in \mathbb{Z}[\sqrt{-D}]$, so $p \mid x$ and $p \mid y$. This establishes part a).

Step 3: Put $N = x^2 + Dy^2$. Indeed 0 is even, so assume $p \mid N$. By part a), there are $X, Y \in \mathbb{Z}$ such that $x = pX$, $y = pY$ and thus $\frac{N}{p^2} = X^2 + DY^2$. An evident inductive argument finishes the proof. □

3. THE MAIN THEOREM AND ITS CONSEQUENCES

Theorem 7. Let $q(x, y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x, y]$ be an anisotropic quadratic form. Put $\Delta = B^2 - 4AC$. Let $n \in \mathbb{Z}^+$ be a nonsquare such that $\gcd(n, 2C) = 1$ and Δ is a square modulo n .

a) There exist $k, y, z \in \mathbb{Z}$ with $0 < |x|, |y| < \sqrt{n}$, $0 < |k| < |A| + |B| + |C|$, such that

$$q(x, y) = kn.$$

b) If q is positive definite, then $k > 0$.

c) If $AC < 0$, then $|k| < \max(|A| + |B|, |C| + |B|)$.

Proof. Since n is odd, $\frac{1}{2} \in \mathbb{Z}/n\mathbb{Z}$ and thus the quadratic formula is valid: since the discriminant Δ of the quadratic $Ax^2 + Bx + C$ is a square modulo n , there is a rational root: i.e., there exists $c, l \in \mathbb{Z}$ such that $Ac^2 + Bc + C = ln$. If a prime p divides c and n , it also divides C , contradicting our assumption; thus we must have $\gcd(c, n) = 1$. We may therefore apply Theorem 1 to n and c to get $x, y \in \mathbb{Z}$, $x \equiv cy \pmod{n}$ and $0 < |x|, |y| \leq \sqrt{n}$. Since n is not a perfect square, we have $|x|, |y| < \sqrt{n}$. We have on the one hand

$$q(x, y) = Ax^2 + Bxy + y^2 = y^2(Ac^2 + Bc + C) \equiv 0 \pmod{n}$$

and on the other,

$$0 < |q(x, y)| \leq |Ax^2 + Bxy + Cy^2| < (|A| + |B| + |C|)n,$$

proving part a). If q is positive definite, then $k = \frac{q(x, y)}{n} > 0$. If $AC < 0$ (which implies that q is indefinite), then

$$\frac{|q(x, y)|}{n} \leq |B| + |Ax^2 + Cy^2| < |B| + \max(|A|, |C|) = \max(|A| + |B|, |C| + |B|).$$

□

The following simple “supplement” to Theorem 7 will be useful.

Proposition 8. Let n be a positive integer and D a squarefree integer. Suppose that Dn is of the form $x^2 + Dy^2$. Then also n is of the form $x^2 + Dy^2$.

Proof. If $x^2 + Dy^2 = Dn$, then $D \mid x^2$. Since D is squarefree, $D \mid x$, so we may put $x = DX$ with $X \in \mathbb{Z}$. Then $D^2X^2 + Dy^2 = Dn$, so $n = y^2 + DX^2$. □

4. FORMS $q_{-4D} = x^2 + Dy^2$

Theorem 9. For a positive integer D , the following are equivalent:

(i) There exist coprime positive integers a and N such that every prime number $p \equiv a \pmod{N}$ is of the form $x^2 + Dy^2$.

(ii) Every prime number $p \equiv 1 \pmod{4D}$ is of the form $x^2 + Dy^2$.

(iii) There is a nonempty subset $S \subset (\mathbb{Z}/4D\mathbb{Z})^\times$ such that for a prime number p with $\gcd(p, D) = 1$, p is of the form $x^2 + Dy^2$ iff $p \equiv s \pmod{4D}$ for some $s \in S$.

(iv) $D = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848$, plus possibly one further value of D . If this other value exists, it is at least 10^8 .

Factorization table: There are precisely 37 known squarefree idoneal numbers D . We group them according to the shape of their prime factorization: here we let ℓ_1, \dots, ℓ_n stand for distinct odd primes.

$$D = 1.$$

$$D = 2.$$

$$D = \ell: 3, 5, 7, 13, 37.$$

$$D = 2\ell: 6 = 2 \cdot 3, 10 = 2 \cdot 5, 22 = 2 \cdot 11, 58 = 2 \cdot 29.$$

$$D = \ell_1\ell_2: 15 = 3 \cdot 5, 21 = 3 \cdot 7, 33 = 3 \cdot 11, 57 = 3 \cdot 19, 85 = 5 \cdot 17, 93 = 3 \cdot 31, 133 = 7 \cdot 19, 177 = 3 \cdot 59, 253 = 11 \cdot 23.$$

$$D = 2\ell_1\ell_2: 30 = 2 \cdot 3 \cdot 5, 42 = 2 \cdot 3 \cdot 7, 70 = 2 \cdot 5 \cdot 7, 78 = 2 \cdot 3 \cdot 13, 102 = 2 \cdot 3 \cdot 17, 130 = 2 \cdot 5 \cdot 13, 190 = 2 \cdot 5 \cdot 19.$$

$$D = \ell_1\ell_2\ell_3: 105 = 3 \cdot 5 \cdot 7, 165 = 3 \cdot 5 \cdot 11, 273 = 3 \cdot 7 \cdot 13, 345 = 3 \cdot 5 \cdot 23, 357 = 3 \cdot 7 \cdot 17, 385 = 5 \cdot 7 \cdot 11.$$

$$D = 2\ell_1\ell_2\ell_3: 210 = 2 \cdot 3 \cdot 5 \cdot 7, 330 = 2 \cdot 3 \cdot 5 \cdot 11, 462 = 2 \cdot 3 \cdot 7 \cdot 11.$$

$D = \ell_1\ell_2\ell_3\ell_4: 1365 = 3 \cdot 5 \cdot 7 \cdot 13$. Remark: The 65 values listed in Theorem 9(iv) were discovered by Euler, who called them **numeri idonei**. In English they are called “convenient” or “idoneal” numbers, and they have many other characterizations. Of all things, Euler used them to find large primes, like 1,000,003.

If $D = 1$, then applying Theorem 7 immediately yields:

Theorem 10. *Let n be a positive integer such that -1 is a square modulo n . Then there exist integers x and y such that $n = x^2 + y^2$.*

Corollary 11. *A positive integer n is of the form $x^2 + y^2$ iff for every prime $p \equiv 3 \pmod{4}$, $\text{ord}_p(n)$ is even.*

Proof. By quadratic reciprocity, for an odd prime p , $\left(\frac{-1}{p}\right) = 1$ if $p \equiv 1 \pmod{4}$ and $\left(\frac{-1}{p}\right) = -1$ if $p \equiv 3 \pmod{4}$. Therefore the conditions on the p -order at primes congruent to 3 modulo 4 are necessary by Theorem 6b). Conversely, $2 = 1^2 + 1^2$ and for any n , $n^2 = n^2 + 0^2$. Also, if $p \equiv 1 \pmod{4}$, then -1 is a square modulo p , so by Theorem 10, p is of the form $x^2 + y^2$. By Proposition 4a), if

$$(1) \quad n = 2^a p_1^{b_1} \cdots p_r^{b_r} q_1^{2c_1} \cdots q_s^{2c_s}, \quad p_1, \dots, p_r \equiv 1 \pmod{4}, \quad q_1, \dots, q_s \equiv 3 \pmod{4},$$

then n is of the form $x^2 + y^2$. □

Let $D = 2$. Applying Theorem 7 and Lemma 8 gives:

Theorem 12. *Let n be an odd positive integer such that -2 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 2y^2$.*

Proof. We apply Theorem 7 with $N = 2$, getting that there exist integers $x, y \in \mathbb{Z}$ such that either $x^2 + 2y^2 = n$ or $x^2 + 2y^2 = 2n$. In the former case we are done, so assume that $x^2 + 2y^2 = 2n$. Then $2 \mid x$, so we may write $x = 2X$ and obtain $2n = x^2 + 2y^2 = 4X^2 + 2y^2$, so $n = y^2 + 2X^2$. □

Corollary 13. *A positive integer n is of the form $x^2 + 2y^2$ iff for every prime $p \equiv 5, 7 \pmod{8}$, $\text{ord}_p(n)$ is even.*

Proof. By quadratic reciprocity, for an odd prime p , $\left(\frac{-2}{p}\right) = 1$ if $p \equiv 1, 3 \pmod{8}$ and $\left(\frac{-2}{p}\right) = -1$ if $p \equiv 5, 7 \pmod{8}$. The remainder of the proof is very similar to that of Corollary 11. Details left to the reader. \square

Remark: The common strategy of deduction of Corollary 11 (resp. Corollary 13) from Theorem 10 (resp. Theorem 12) persists in the proofs of Corollaries 15, 17 and 19. The proofs of these corollaries will therefore be omitted.

Theorem 14. *Let n be a positive integer such that $\gcd(12, n) = 1$ and -3 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 3y^2$.*

Proof. Applying Theorem 7 and Lemma 8, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 3y^2 = kn$ for some k , $1 \leq k < 3$. If $k = 1$, we're done, so we consider the case $x^2 + 3y^2 = 2n$. Reducing modulo 3 we get $x^2 \equiv 2n \pmod{3}$. Let p be any (odd, by hypothesis) prime divisor of n . Then, since -3 is a square mod n , *a fortiori* we have $\left(\frac{-3}{p}\right) = 1$. By quadratic reciprocity, this implies $p \equiv 1 \pmod{3}$. That is, to say, n divisible only by primes of the form $1 \pmod{3}$, from which it follows that $n \equiv 1 \pmod{3}$, and thus $2n \equiv 2 \pmod{3}$. But then $x^2 \equiv 2 \pmod{3}$, a contradiction. \square

Corollary 15. *A positive integer n is of the form $x^2 + 3y^2$ iff $\text{ord}_2(n)$ is even and for every prime $p \equiv -1 \pmod{3}$, $\text{ord}_p(n)$ is even.*

Proof. The method of proof of Corollaries 11 and 13 establishes this result for all odd n . It follows by Proposition 5 that the given conditions are sufficient for representability of n . Now suppose that $n = 2^a m$ with m and a both odd. We must show that n is not of the form $x^2 + 3y^2$.

Case 1: $a = 1$. Then reducing $x^2 + 3y^2 = 2m$ modulo 4 gives a contradiction.

So we may assume $a \geq 3$ and, seeking a contradiction, that we have integers x and y such that $x^2 + 3y^2 = 2^a m$.

Case 2: x and y are both odd. Then reducing modulo 8 gives a contradiction.

Case 3: x and y have opposite parity. Then reducing modulo 2 gives a contradiction.

Case 4: $x = 2X$, $y = 2Y$. Then $X^2 + 3Y^2 = 2^{a-2}m$ and an inductive argument completes the proof. \square

Theorem 16. *Let n be an odd positive integer such that -4 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 4y^2$.*

Proof. Taking $x^2 + 4y^2$ as $x^2 + (2y)^2$, we see the result is equivalent to the claim that in the conclusion of Theorem 10, we can take one of x or y to be even. This is certainly true, because if they were both odd, then $x^2 + y^2 = n$ would be even. \square

Corollary 17. *A positive integer n is of the form $x^2 + 4y^2$ iff $\text{ord}_2(n) \neq 1$ and for every prime $p \equiv -1 \pmod{4}$, $\text{ord}_p(n)$ is even.*

Proof. Again the arguments for odd n are similar to those given above. If $\text{ord}_2(n) = 1$, then reducing modulo 4 shows that n is not of the form $x^2 + 4y^2$. On the other hand, $4 = 2^2 + 4 \cdot 0^2$ and $8 = 2^2 + 4 \cdot 1^2$ are both of the form $x^2 + 4y^2$, hence so is every $n = 2^k$ with $k > 1$. The result follows. \square

Theorem 18. *Let n be a positive integer such that $\gcd(14, n) = 1$ and -7 is a square modulo n . Then there exist integers x and y such that $n = x^2 + 7y^2$.*

Proof. Applying Theorem 7 and Lemma 8, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 7y^2 = kn$ for some k , $1 \leq k < 7$. If $k = 1$ we are done, so assume $k > 1$.

Step 1: Reducing modulo 7, we get $x^2 \equiv kn \pmod{7}$, i.e., kn is a nonzero square modulo 7. Let p be any (odd, by hypothesis) prime divisor of n . Then our hypothesis implies $\left(\frac{-7}{p}\right) = 1$, so by quadratic reciprocity p is a square modulo 7. Therefore n is a product of nonzero squares modulo 7 so it itself a nonzero square modulo 7. Therefore k , being the quotient of nonzero squares modulo 7, is itself a nonzero square modulo 7: i.e., $k = 1, 2, 4$.

Step 2: Suppose $x^2 + 7y^2 = 2n$. The possible values of the left hand side modulo 8 are 0, 1, 3, 4, 5, 7. The possible values of the right hand side are 2, 6: contradiction.

Step 3: Suppose $x^2 + 7y^2 = 4n$. Since the right hand side is even, x and y must have the same parity. If they are both odd, $x^2 + 7y^2 \equiv 0 \pmod{8}$, contradiction. So x and y are both even: $x = 2X$, $y = 2Y$, $4X^2 + 4 \cdot 7Y^2 = 4p$, and $X^2 + 7Y^2 = p$. \square

Corollary 19. *A positive integer is of the form $x^2 + 7y^2$ iff $\text{ord}_2(n) \neq 1$ and for every prime $p \equiv 3, 5, 6 \pmod{7}$, $\text{ord}_p(n)$ is even.*

Proof. By quadratic reciprocity, for an odd prime p , $\left(\frac{-7}{p}\right) = 1$ if $p \equiv 1, 2, 4 \pmod{7}$ and $\left(\frac{-7}{p}\right) = -1$ if $p \equiv 3, 5, 6 \pmod{7}$. The rest is left to the reader. \square

Why did we skip $D = 5$ and $D = 6$? Because for these values the converse of Proposition 3 is false!

Example 1: Take $D = 5$ and $p = 3$. Then $\left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1$, but the equation $3 = x^2 + 5y^2$ has no solutions. More generally, reducing mod 20 shows:

Proposition 20. *Let p be a prime such that $\text{gcd}(20, p) = 1$. If there exist $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = p$, then $p \equiv 1, 9 \pmod{20}$.*

Example 2: Take $D = 6$ and $p = 5$. Then $\left(\frac{-6}{5}\right) = \left(\frac{4}{5}\right) = 1$, but the Diophantine equation $5 = x^2 + 6y^2$ has no solutions. More generally, reducing mod 24 shows:

Proposition 21. *Let p be a prime such that $\text{gcd}(10, p) = 1$. If there exist $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = p$, then $p \equiv 1, 7 \pmod{24}$.*

Remarkably, simply by taking these auxiliary congruence conditions into account, the above methods can be extended to derive results for these values of D .

Theorem 22. *Let n be a positive integer with $\text{gcd}(10, n) = 1$. Suppose that -1 and -5 are both squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 5y^2$.*

Proof. Applying Theorem 7 and Lemma 8, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = kn$ for some k , $1 \leq k < 5$.

Step 1: Reducing modulo 5, we get $x^2 \equiv kn \pmod{5}$, i.e., kn is a nonzero square modulo 5. Let p be any (odd, by hypothesis) prime divisor of n . Then our hypothesis implies $\left(\frac{-5}{p}\right) = 1$, so by quadratic reciprocity p is a square modulo 5. Therefore n is a product of nonzero squares modulo 5 so it itself a nonzero square modulo 5. Therefore k , being the quotient of nonzero squares modulo 5, is itself a nonzero square modulo 5: i.e., $k = 1, 4$.

Step 2: Suppose that $x^2 + 5y^2 = 4n$. We claim that x and y are both even, hence substituting $x = 2X$, $y = 2Y$ gives $X^2 + 5Y^2 = n$. Indeed, this follows simply by considering $x^2 + 5y^2$ modulo 4. \square

Very similar arguments can be used to show the following “complement”:

Theorem 23. *Let $n \in \mathbb{Z}^+$ with $\gcd(10, n) = 1$. Suppose that for every prime p dividing n , $p \equiv 3, 7 \pmod{20}$. Then there exist $x, y \in \mathbb{Z}$ such that $2n = x^2 + 5y^2$.*

Theorem 24. *Let n be a positive integer with $\gcd(6, n) = 1$. Suppose that every prime divisor of n is congruent to 1 or 3 modulo 24. Then there exist integers x and y such that $n = x^2 + 6y^2$.*

Proof. Applying Theorem 7 and Lemma 8, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 6y^2 = kn$ for some k , $1 \leq k < 6$.

Step 1: Reducing modulo 3, we get $x^2 \equiv kn \pmod{3}$, so that $kn \equiv 0, 1 \pmod{3}$. Our hypothesis implies $\left(\frac{-3}{p}\right) = 1$ for all prime divisors of n , so by quadratic reciprocity $p \equiv 1 \pmod{3}$. Thus $n \equiv 1 \pmod{3}$. It follows that $k = 1, 3, 4$.

Step 2: Since -1 is a square modulo 4, quadratic reciprocity implies $n \equiv 1 \pmod{4}$. So if $k = 3$, $3k \equiv 3, 5 \pmod{8}$, which are not values of $x^2 + 6y^2 \pmod{8}$.

Step 3: If $k = 4$, then $4 \mid x^2 + 6y^2$. From this we deduce $2 \mid x$, $4 \mid x^2$ and $2 \mid y$, so we may put $x = 2X$, $y = 2Y$ and then we get $X^2 + 6Y^2 = p$. \square

Theorem 25. *An odd positive integer n is of the form $x^2 + 8y^2$ iff:*

- (i) *For all primes $p \equiv 5, 7 \pmod{8}$, $\text{ord}_p(n)$ is even, and*
- (ii) *$n \equiv 1 \pmod{4}$.*

Proof. Since $x^2 + 8y^2 = x^2 + 2(2y)^2$, a positive integer is of the form $x^2 + 8y^2$ iff it is of the form $x^2 + 2y^2$ with y even. By Theorem X, for n prime to 2, n is of the form $x^2 + 8y^2$ iff for every prime divisor p of n with $p \equiv 5, 7 \pmod{8}$, $\text{ord}_p(n)$ is even. Thus condition (i) is necessary. Moreover, reducing $x^2 + 8y^2 = n$ modulo 4 gives $n \equiv x^2 \pmod{4}$; since n is odd, we conclude $n \equiv 1 \pmod{4}$: condition (ii).

Conversely, suppose n satisfies (i) and (ii), so by Theorem XX we may write $n = x^2 + 2y^2$. If y is odd, then $n \equiv x^2 + 2 \equiv 2, 3 \pmod{4}$, hence we must have y is even, qed. \square

Theorem 26. *A positive integer n prime to 6 is of the form $x^2 + 9y^2$ iff:*

- (i) *For all primes $p \equiv 3 \pmod{4}$, $\text{ord}_p(n)$ is even, and*
- (ii) *$n \equiv 1 \pmod{3}$.*

Proof. Since $x^2 + 9y^2 = x^2 + (3y)^2$, an integer n is of the form $x^2 + 9y^2$ iff it is of the form $x^2 + y^2$ with at least one of x, y divisible by 3. Thus by Corollary 11, condition (i) is necessary. Conversely, reducing $n = x^2 + 9y^2$ modulo 3 gives $n \equiv x^2 \equiv 1 \pmod{3}$: condition (ii).

Conversely, suppose n satisfies (i) and (ii), so by Corollary 11 we may write $n = x^2 + y^2$. If $3 \nmid xy$, then $n \equiv x^2 + y^2 \equiv 2 \pmod{3}$, hence we must have $3 \mid x$ or $3 \mid y$, qed. \square

Theorem 27. *Let n be a positive integer prime to 10. Suppose that for every prime p dividing n , $p \equiv 1, 3 \pmod{8}$ and $p \equiv \pm 1 \pmod{5}$. Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 10y^2$.*

Proof. Since $p \equiv 1, 3 \pmod{8}$ for all primes dividing n , -10 is a square modulo n . Applying Theorem 7 and Lemma 8, there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + 10y^2 = kn$ for some k , $1 \leq k < 10$.

Step 1: Suppose first that $k = 5$, $x^2 + 10y^2 = 5n$. Since every prime divisor

of n is 1 or 3 mod 8, n itself is congruent to 1 or 3 mod 8, so $5n \equiv 5, 7 \pmod{8}$. But the values of $x^2 + 10y^2$ modulo 8 are 0, 1, 2 and 3, contradiction.

Step 2: Assume $k \neq 5$, and reduce modulo 5: $x^2 \equiv kn \pmod{5}$, so $kn \equiv 1, 4 \pmod{5}$. Thus $k = 1, 4, 9$. If $x^2 + 10y^2 = 4n$, then x is even, so $4 \mid x^2$, so $2 \mid y$, so $(x/2)^2 + 10(y/2)^2 = n$. If $x^2 + 10y^2 = 9n$, reduce modulo 3: $x^2 + 10y^2 \equiv x^2 + y^2 \equiv 0 \pmod{3}$ implies x and y are both divisible by 3. Thus $(x/3)^2 + 10(y/3)^2 = n$. \square

Theorem 28. *A positive integer n prime to 6 is of the form $x^2 + 12y^2$ iff:*

- (i) For all primes $p \equiv 2 \pmod{3}$, $\text{ord}_p(n)$ is even, and
- (ii) $n \equiv 1 \pmod{4}$.

Proof. Since $x^2 + 12y^2 = x^2 + 3(2y)^2$, an integer n is of the form $x^2 + 12y^2$ iff it is of the form $x^2 + 3y^2$ with y even. Thus by Corollary 15, condition (i) is necessary. Conversely, reducing $n = x^2 + 12y^2$ modulo 4 gives $n \equiv 1 \pmod{4}$: condition (ii).

Conversely, suppose n satisfies (i) and (ii), so by Corollary 15 we may write $n = x^2 + 3y^2$. If y is odd, then $n = x^2 + 3y^2 \equiv x^2 + 3 \equiv 0, 3 \pmod{4}$, contradiction. Thus y is even, qed. \square

Theorem 29. *Let n be a positive integer with $\gcd(30, n) = 1$. Suppose that -3 and 5 are both squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 15y^2$.*

Proof. The hypotheses imply that -15 is a square modulo n , so that there exists an integer k , with $1 \leq k \leq 14$, such that kn is of the form $x^2 + 15y^2$.

Case 1: Assume that $\gcd(k, 15) = 1$. Then reducing modulo 3 and 5 gives $k \equiv 1 \pmod{3}$ and $k \equiv \pm 1 \pmod{5}$, so $k = 1$ or 4. If $k = 1$, we're done. If $x^2 + 15y^2 = 4n$, then reducing modulo 8 shows that x and y are both even, so $(\frac{x}{2})^2 + 15(\frac{y}{2})^2 = n$.

Case 2: Assume that $3 \mid k$ and put $k = 3K$ with $1 \leq K \leq 4$. If $x^2 + 15y^2 = 3Kn$, then we may put $3 = 3X$ and get an equation $3X^2 + 5y^2 = Kn$. We now proceed in a similar fashion to the overall proof: namely, reducing modulo 5 rules out $K = 1, 4$. If $K = 2$, then reducing modulo 4 gives a contradiction. If $K = 3$, then we may write $X = 3\mathcal{X}$ and get the equation $\mathcal{X}^2 + 15y^2 = n$, great.

Case 3: Assume that $5 \mid k$ and put $k = 5K$ with $1 \leq K \leq 2$. From the equation $x^2 + 15y^2 = 5Kn$, we may write $x = 5X$, getting $5x^2 + 3y^2 = Kn$, reducing us to Case 2. \square

Theorem 30. *Let n be a positive integer with $\gcd(42, n) = 1$. Suppose that -1 , -3 and -7 are all square modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 21y^2$.*

Proof. The hypotheses imply that -21 is a square modulo n , so that there exists an integer k , with $1 \leq k \leq 20$, such that kn is of the form $x^2 + 21y^2$.

Case 1: Assume that $\gcd(k, 21) = 1$. Then reducing modulo 3 and 7 gives $k \equiv 1 \pmod{3}$, $k \equiv 1, 2, 4 \pmod{7}$, so $k = 1, 4, 16$. If $k = 1$, we're done. If $x^2 + 21y^2 = 4n$, then reduction modulo 4 shows x and y are both even, so $n = (\frac{x}{2})^2 + 21(\frac{y}{2})^2$. If $x^2 + 21y^2 = 16n^2$, then two applications of the above argument shows $n = (\frac{x}{4})^2 + 21(\frac{y}{4})^2$.

Case 2: Suppose $k = 3K$, so $x^2 + 21y^2 = 3Kn$ and thus $3x^2 + 7y^2 = Kn$, with $1 \leq K \leq 6$. Reducing modulo 7 rules out $K = 1, 4$; reducing modulo 3 rules out $K = 2, 5$. Otherwise we may put $K = 3\mathcal{K}$ and get $x^2 + 21y^2 = n$ (okay) or $x^2 + 21y^2 = 2n$, which has already been ruled out.

Case 3: Suppose $k = 7K$, so $x^2 + 21y^2 = 7Kn$ and thus $7x^2 + 3y^2 = Kn$ with $1 \leq K \leq 2$, reducing us to Case 2. \square

Theorem 31. *Let p be a prime number. Then p is of the form $x^2 + 22y^2$ iff $p \equiv \pm 1 \pmod{8}$ and $\left(\frac{p}{11}\right) = 1$.*

Proof. Clearly 2 and 11 are not of the form $x^2 + 22y^2$, so we may assume $\gcd(22, p) = 1$. Reducing a putative equation $x^2 + 22y^2 = p$ modulo p gives $\left(\frac{-22}{p}\right) = 1$; reducing it modulo 11 gives $\left(\frac{p}{11}\right) = 1$. These conditions are equivalent to $p \equiv \pm 1 \pmod{8}$ and $\left(\frac{p}{11}\right) = 1$, demonstrating the necessity. Now suppose they are satisfied. As above, we then have $\left(\frac{-22}{p}\right) = 1$, so that there exists an integer k , with $1 \leq k \leq 21$, such that kp is of the form $x^2 + 22y^2$. We have that

$$\left(\frac{-22}{3}\right) = \left(\frac{-22}{5}\right) = \left(\frac{-22}{7}\right) = \left(\frac{-22}{17}\right) = -1.$$

From this and Theorem 6 it follows that we need not consider the cases in which k is divisible by 3, 5, 7 or 17, since we will either derive a contradiction or reduce to the case of a proper divisor of k . Moreover, reducing $x^2 + 22y^2 = kp$ modulo 11 shows that $\left(\frac{k}{11}\right) \neq -1$, eliminating the cases $k = 13$ and $k = 19$. We are left with $k = 2, 4, 8, 11, 16$.

If $x^2 + 22y^2 = 2p$, then we may put $x = 2X$, getting $2X^2 + 11y^2 = p$. Since $\left(\frac{2}{11}\right) = -1$, reducing modulo 11 gives a contradiction.

If $x^2 + 22y^2 = 4p$, then $2X^2 + 11y^2 = 2p$, so we may put $y = 2Y$, getting $X^2 + 22Y^2 = p$. Similarly the case $k = 8$ reduces to $k = 2$ and the case $k = 16$ reduces to $k = 1$.

If $x^2 + 22y^2 = 11p$, then we may put $x = 11X$, getting $11X^2 + 2y^2 = p$, a case which we have dealt with above. \square

Theorem 32. *Let n be a positive integer with $\gcd(66, n) = 1$. Suppose that -1 , -3 and -11 are all squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 33y^2$.*

Proof. The hypotheses imply that -33 is a square modulo n , so that there exists an integer k , with $1 \leq k \leq 32$, such that kn is of the form $x^2 + 33y^2$.

Case 1: Assume that $\gcd(k, 33) = 1$. Reducing $x^2 + 33y^2 = kn$ modulo 3 and 11, one sees that the possible values of k are $k = 1, 4, 16, 25, 31$. If $k = 1$, we're done. If $x^2 + 33y^2 = 4n$, then reducing modulo 4 shows that x and y are both even, so $n = \left(\frac{x}{2}\right)^2 + 33\left(\frac{y}{2}\right)^2$. If $k = 16$, apply the previous case twice. If $k = 25$, then since $\left(\frac{-33}{5}\right) = -1$, Theorem 6 shows that x and y are both divisible by 5, so $\left(\frac{x}{5}\right)^2 + 33\left(\frac{y}{5}\right)^2 = n$. If $k = 31$, then $-$ since $n \equiv 1 \pmod{4}$ $-$ reducing modulo 4 gives a contradiction.

Case 2: Assume $k = 3K$, leading to the equation $3X^2 + 11y^2 = Kn$ with $1 \leq K \leq 10$. Reducing modulo 3 rules out $K = 1, 4, 7, 10$. Reducing modulo 11 rules out $K = 2$. If $K = 3$, then the obvious cancellation leads to $X^2 + 33Y^2 = n$, okay. If $K = 4$, then reducing modulo 4 shows that both X and y are even, taking us back to the case $K = 1$. If $K = 5$ then reducing modulo 4 gives a contradiction. If $K = 6$, then the obvious cancellation leads to a representation of $2n$ by $x^2 + 33y^2$, which we have seen is impossible. The case $K = 8$ reduces to the case $K = 2$, whereas the case $K = 9$ reduces to the case $K = 1$.

Case 3: Assume $k = 11K$, leading to the equation $11X^2 + 3y^2 = Kn$ with $1 \leq K \leq 2$, reducing us to Case 2. \square

Theorem 33. *Let n be a positive integer with $\gcd(104, n) = 1$. Suppose that -1 , -3 and -19 are all squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 57y^2$.*

Proof. The hypotheses imply that -57 is a square modulo n , so that there exists and integer k , with $1 \leq k \leq 56$, such that kn is of the form $x^2 + 57y^2$.

Case 1: Assume that $\gcd(k, 57) = 1$. Reducing modulo 3, 4 and 19, one sees that the possible values of k are 1, 4, 16, 25, 28. If $k = 1$, we're done. If $x^2 + 57y^2 = 4n$, reducing modulo 4 shows that x and y are both even, so $n = (\frac{x}{2})^2 + 33(\frac{y}{2})^2$. If $x^2 + 57y^2 = 16n$, apply the previous argument twice. If $x^2 + 57y^2 = 25n$, then since $(\frac{-57}{5}) = -1$, Theorem 6 applies to show that $5 \mid x$ and $5 \mid y$, so $n = (\frac{x}{5})^2 + 57(\frac{y}{5})^2$. If $x^2 + 57y^2 = 28n$, then reducing mod 4 shows that x and y are both even, reducing us to a case that we have already eliminated.

Case 2: Suppose that $k = 3K$, with $1 \leq K \leq 18$. Thus $x^2 + 57y^2 = 3Kn$, so $x = 3X$ and $3X^2 + 19y^2 = Kn$. Reducing modulo 4 shows that we cannot have $K \equiv 1 \pmod{4}$. Reducing modulo 3 shows that we cannot have $K \equiv 2 \pmod{3}$. Since $(\frac{3}{19}) = -1$, reducing modulo 19 shows that we must have $(\frac{K}{19}) = -1$. This eliminates all values of K except $K = 3, 9, 10, 12, 15, 18$. If $K = 10$, then reducing modulo 8 gives a contradiction. Otherwise we may put $K = 3\mathcal{K}$ and get $3X^2 + 19y^2 = 3\mathcal{K}n$, $y = 3Y$, $X^2 + 57Y^2 = \mathcal{K}n$, and we are finished by induction.

Case 3: suppose that $k = 19K$ with $K = 1, 2$. So $x^2 + 57y^2 = 19Kn$, $x = 19X$, $19X^2 + 3y^2 = Kn$ and we are reduced to Case 2. \square

Theorem 34. *Let p be a prime number. Then p is of the form $x^2 + 58y^2$ iff $p \equiv \pm 1, 3 \pmod{8}$ and $(\frac{p}{29}) = 1$.*

Proof. Clearly 2 and 29 are not of the form $x^2 + 58y^2$, so we may assume $\gcd(58, p) = 1$. Reducing a putative equation $x^2 + 58y^2 = p$ modulo p gives $(\frac{-58}{p}) = 1$; reducing it modulo 29 gives $(\frac{p}{29}) = 1$. These conditions are equivalent to $p \equiv \pm 1, 3 \pmod{8}$ and $(\frac{p}{29}) = 1$, demonstrating the necessity. Now suppose they are satisfied. As above, we then have $(\frac{-58}{p}) = 1$, so that there exists an integer k , with $1 \leq k \leq 57$, such that kp is of the form $x^2 + 58y^2$. We have that $(\frac{-58}{\ell}) = -1$ for $\ell = 3, 5, 7, 11, 13, 17, 19, 23, 41, 53$. From this and Theorem 6 it follows that we need not consider the cases in which k is divisible by any of these primes, since we will either derive a contradiction or reduce to the case of a proper divisor of k . Moreover, reducing $x^2 + 58y^2 = kp$ modulo 29 shows that $(\frac{k}{29}) \neq -1$, eliminating the cases $k = 31, 37, 43, 47$. We are left with $k = 2, 4, 8, 16, 29, 32$.

If $x^2 + 58y^2 = 2p$, then we may put $x = 2X$, getting $2X^2 + 29y^2 = p$. Since $(\frac{2}{29}) = -1$, reducing modulo 29 gives a contradiction.

If $x^2 + 58y^2 = 4p$, then $2X^2 + 29y^2 = 2p$, so we may put $y = 2Y$, getting $X^2 + 58Y^2 = p$. Similarly the cases $k = 8$ and $k = 32$ reduce to the case $k = 2$ and the case $k = 16$ reduces to the case $k = 1$.

Finally, if $x^2 + 58y^2 = 29p$, then we may put $x = 29X$, getting $29X^2 + 2y^2 = p$, a case which we have dealt with above. \square

Theorem 35. *Let n be a positive integer with $\gcd(170, n) = 1$. Suppose that $-1, 5$ and 17 are all squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 85y^2$.*

Proof. The hypotheses imply that -85 is a square modulo n , so that there exists and integer k , with $1 \leq k \leq 84$, such that kn is of the form $x^2 + 85y^2$.

Case 1: Assume that $\gcd(k, 85) = 1$. Reducing modulo 4, 5 and 17, one sees that the possible values of k are 1, 4, 9, 16, 49, 64. If $k = 1$, we're done. If $x^2 + 85y^2 = 4n$, reducing modulo 4 shows that x and y are both even, so $n = (\frac{x}{2})^2 + 85(\frac{y}{2})^2$. If $x^2 + 85y^2 = 16n$ or $64n$, apply the previous argument several times. If $x^2 + 85y^2 =$

$9n$, then since $(\frac{-85}{3}) = -1$, Theorem 6 applies to show that $3 \mid x$, $3 \mid y$, so that $(\frac{x}{3})^2 + 85(\frac{y}{3})^2 = n$. Similarly for $k = 49$, since $(\frac{-85}{7}) = -1$.

Case 2: Suppose that $k = 5K$, with $1 \leq K \leq 16$. Thus $x^2 + 85y^2 = 5Kn$, so $x = 5X$ and $5X^2 + 17y^2 = Kn$. Reducing modulo 4 shows $K \not\equiv 3 \pmod{4}$; reducing modulo 5 shows $(\frac{K}{17}) \neq 1$, and reducing modulo 17 shows that $(\frac{K}{5}) \neq 1$. This eliminates all values of K except $K = 5, 10, 15$. Thus we may put $K = 5\mathcal{K}$ with $1 \leq \mathcal{K} \leq 3$ and get $X^2 + 85Y^2 = \mathcal{K}n$, reducing ourselves to previously considered cases.

Case 3: Suppose that $k = 17K$, with $1 \leq K \leq 4$. Then we may put $x = 17X$ and get $17X^2 + 5y^2 = Kn$, again reducing ourselves to previously considered cases. \square

4.1. prime D part II.

Let $D \equiv 1 \pmod{4}$ be a prime number. We say that D satisfies **property (I)** if both of the following hold:

(I1) For all primes $q < \frac{D}{2}$, $(\frac{-D}{q}) = -1$, and

(I2) For all primes $q < D$ with $q \equiv 1 \pmod{4}$, $(\frac{q}{D}) = -1$.

Theorem 36. *Suppose $D \equiv 5 \pmod{8}$ is a prime number satisfying property (I).*

Let n be a positive integer prime to $2D$ such that:

(i) Every prime divisor p of n is congruent to $1 \pmod{4}$, and

(ii) Every prime divisor p of n satisfies $(\frac{-D}{p}) = 1$.

Then there exist integers $x, y \in \mathbb{Z}$ such that $n = x^2 + Dy^2$.

Proof. Step 1: Suppose n is a positive integer satisfying (i) and (ii). Then $-D$ is a square modulo n , and we may apply Theorem 7 and Lemma 8 to get $x, y \in \mathbb{Z}$ such that $x^2 + Dy^2 = kn$ for some $1 \leq k < D$. Reducing modulo D , we get that kn is a nonzero square modulo D . The hypotheses imply that every prime divisor of n is a nonzero square modulo D , hence n itself is a nonzero square modulo D , so k is a nonzero square modulo D . Note that since $D \equiv 5 \pmod{8}$, 2 is not a square modulo D .

Step 2: Suppose that $4 \mid k$. Then, since $D \equiv 1 \pmod{4}$, reducing modulo 4 shows that x and y are both even, so $(\frac{x}{2})^2 + (\frac{y}{2})^2 = (\frac{k}{4})n$.

Step 3: Suppose that k is divisible by an odd prime q with $q < \frac{D}{2}$. Reducing $x^2 + Dy^2 = kn$ modulo q , we get that $x^2 + Dy^2 \equiv 0 \pmod{q}$. By property (I), $-D$ is not a square modulo q , so the congruence implies that x and y are both divisible by q . Thus $kn = x^2 + Dy^2$ is divisible by q^2 . If $q^2 \mid k$, then

$$\left(\frac{k}{q^2}\right)n = \left(\frac{x}{q}\right)^2 + D\left(\frac{y}{q}\right)^2.$$

If $q^2 \nmid k$, then $q \mid n$. Then by (i) we have $(\frac{-D}{q}) = 1$, contradicting property (I). It follows that if $x^2 + Dy^2 = kn$, then there exist $X, Y \in \mathbb{Z}$ such that $X^2 + DY^2 = qn$, where q is prime, $q \equiv 3 \pmod{4}$, and $\frac{D}{2} < q < D$.

Step 4: If $(\frac{-D}{q}) = -1$, then as in Step 2, reducing modulo q gives a contradiction. Hence $(\frac{-D}{q}) = 1$, so $(\frac{q}{D}) = (\frac{D}{q}) = -(\frac{-D}{q}) = -1$, contradicting Step 1. \square

Direct computation shows that $D = 5, 13, 37$ satisfy property (I). Thus:

Theorem 37. *Let n be a positive integer prime to 10. Suppose that -1 and -5 are both squares modulo n . Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 5y^2$.*

Theorem 38. *Let n be a positive integer prime to 26. Suppose that*

(i) *Every prime $p \mid n$ is congruent to 1 (mod 4), and*

(ii) *For all primes $p \mid n$, $(\frac{-13}{p}) = 1$.*

Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 13y^2$.

Theorem 39. *Let n be a positive integer prime to 74. Suppose that*

(i) *Every prime $p \mid n$ is congruent to 1 (mod 4), and*

(ii) *For all primes $p \mid n$, $(\frac{-37}{p}) = 1$.*

Then there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + 37y^2$.

Remark: Let $D \equiv 1 \pmod{4}$ is a prime, and let p be a prime number with $\gcd(p, 2D) = 1$. Then the equation $x^2 + Dy^2 = p$ implies $(\frac{-D}{p}) = (\frac{p}{D}) = 1$: equivalently, $(\frac{p}{D}) = 1$ and $p \equiv 1 \pmod{4}$. Thus the density of the set of such primes is at most $\frac{1}{4}$. Let $h(-D)$ be the class number of $\mathbb{Q}(\sqrt{-D})$. By [2] the density of the set of primes represented by $x^2 + Dy^2$ is $\frac{1}{2h(-D)}$. The number of genera of quadratic forms of discriminant $-4D$ is equal to 2. Then the elementary theory of genera gives that the following are equivalent:

(i) Every prime p satisfying $(\frac{D}{p}) = (\frac{-1}{p}) = 1$ is of the form $x^2 + Dy^2$.

(ii) Every genus of primitive quadratic forms modulo $-4D$ has a unique class.

(iii) $h(-D) = 2$.

The list of all imaginary quadratic fields of class number 2 is known (STARK), and among discriminants of the form $-4D$ with $D \equiv 1 \pmod{4}$ prime, the complete list is $D = 5, 13, 37$. Thus our method succeeds for all idoneal quadratic forms in this case.

Remark: A result of A. Gica [3, Thm. 1] shows that in fact the condition (I1) is superfluous: if a prime number p has the property that $q < p$, $q \equiv 1 \pmod{4} \implies (\frac{q}{p}) = -1$, then $p \in \{2, 3, 5, 7, 13, 37\}$.

REFERENCES

- [1] M. Aigner and G.M. Ziegler, *Proofs from The Book*. Including illustrations by Karl H. Hofmann. Third edition. Springer-Verlag, Berlin, 2004.
- [2] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.
- [3] A. Gica, *Quadratic residues of certain types*, Rocky Mountain J. Math. 36 (2006), 1867-1871.
- [3] O. Ore, *Number theory and its history*. Reprint of the 1948 original. With a supplement. Dover Publications, Inc., New York, 1988.
- [4] V. Shoup, *A computational introduction to number theory and algebra*. Second edition. Cambridge University Press, Cambridge, 2009.
- [5] A. Thue, *Et par antydninger ti1 en taltheoretisk metode*, Kra. Vidensk. Selsk. Forh. 7 (1902), 57-75.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GA 30602, USA
 E-mail address: pete@math.uga.edu