THUE-VINOGRADOV AND INTEGERS OF THE FORM $x^2 + Dy^2$

PETE L. CLARK

Contents

Introduction – Study of an Elementary Proof

Perhaps the first nontrivial, nonfoundational result in number theory is Fermat's **Two Squares Theorem**: an odd prime number is a sum of two integer squares iff it is congruent to one modulo four.[1]

Fermat claimed a proof of the Two Squares Theorem (Christmas day, 1640) but

Date: November 23, 2011.

[1]Whether or not this vague claim is accurate in a historical sense, it is certainly accurate as a personal statement about the author. For me, number theory began in a three week course taught in the summer of 1992 by Tim Marks and Jamie Pommersheim, and if number theory was the queen of mathematics, the Two Squares Theorem was the jewel in her crown. Almost twenty years later, my fascination with this result shows no signs of abatement.

(as usual) never published it, describing it only as an application of his method of Infinite Descent. The first "public" proof, also using Infinite Descent, was given by Euler in 1747. By now many proofs have been given: the most currently popular one exploits the fact that $x^2 + y^2$ is the norm form of $\mathbb{Z}[\sqrt{-1}]$.

The text [AZ], which compiles "book proofs" in the sense made popular by P. Erdős, gives two proofs of the Two Squares Theorem. One is an involutory proof by Heath-Brown and Zagier. The other exploits a combinatorial lemma of A. Thue.

One may ask why there is so much interest in giving new proofs of very old theorems like the Two Squares Theorem. There are many possible answers, including the thrill that comes with finding one's own proof of a classic result. But there is another reason, and one which provides a test of the worth of a "new proof": what other theorems can be proved by the same or similar arguments?

Thus one has the natural question "What *else* can be proved via Thue's Lemma?" Although a substantial minority of introductory number theory texts include the Thue's Lemma proof of the Two Squares Theorem – e.g. [O, Thm. 11-7], [Sho, Thm. 2.33], [L] – very few put Thue's Lemma to the test by investigating what other results – especially, what other representation theorems for binary quadratic forms – can be proved using it. The only significant exception I know is T. Nagell's classic text [N], which uses Thue's Lemma to determine the primes represented by the forms $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$, $x^2 + 7y^2$, $2x^2 + 3y^2$ [N, Thm. 100] and sets as exercises the determination of primes represented by $x^2 + xy + y^2$, $x^2 + 6y^2$, $2x^2 + 3y^2$, $x^2 + xy + 3y^2$ [N, pp. 265-266].[2] Why Nagell (a student of Thue) chose these particular forms and not others is not explained.

I began thinking seriously about the method of Thue's Lemma when M. Hamel brought a similar argument to my attention in early 2010. I had recently taught a course from Cox's text [C] on the quadratic forms $x^2 + Dy^2$, so it occurred to me to wonder which further such forms could be handled by Thue's Lemma. It is well known – and well described in [C] – that sufficient congruential conditions for a prime p to be of the form $x^2 + Dy^2$ exist only for finitely many values of D called **idoneal numbers** (more on them below). In the summer of 2010 I showed that Thue's Lemma can be used to determine which primes are represented by any *squarefree* idoneal number D. (There are 37 known squarefree idoneal numbers, the largest being $D = 1365$, and at most one further such number, whose existence would contradict the Generalized Riemann Hypothesis.) Unfortunately these arguments required substantial calculations: not every value of D was included in the writeup, but for instance $D = 1365$ was and that case alone filled nearly three pages.

Later in 2010 I showed the results to A. Granville, who quickly suggested that replacing the appeal to Thue's Lemma by a mild "rectangular" generalization – Vinogradov's Lemma – would result in a quantitative improvement in the main result (Theorem 9) which should significantly reduce the amount of calculation. I have followed Granville's suggestion and substantially rewritten the present paper along these lines. By replacing Thue's Lemma with Vinogradov's Lemma (and improving the organization), I have been able to treat all 65 known idoneal numbers as well as give complete proofs, all within a smaller amount of space.

[2]Nagell's text has the following organizational idiosyncrasy: Theorem 100 appears in Chapter VI, but the aforementioned exercises appear at the end of Chapter VII and are thus easy to miss.

There are two other works which are closely related to this one. In 2010 T. Hagedorn gave a new proof of the representation theorem for primes by $x^2 + Dy^2$ for idoneal D using Minkowski's Convex Body Theorem (this generalizes yet another standard proof of the Two Squares Theorem). Hagedorn's argument and mine follow the same basic strategy: we show that for an odd prime number p with $(\frac{-D}{p}) = 1$, there are $x, y \in \mathbb{Z}^+$ and a positive integer k bounded in terms of D such that $x^2 + y^2 = kp$, and then we analyze all cases of $k > 1$ using elementary congruence considerations to either deduce a contradiction or deduce a representation of p as X^2+DY^2. However, the methods lead to different upper bounds on k:

- Using Thue's Lemma gives $k \leq D$.
- Using Vinogradov's Lemma gives $k < 2\sqrt{D}$.
- Using Minkowski's Theorem gives $k \leq \frac{4}{\pi}\sqrt{D}$.

(• Using a sharper Geometry of Numbers bound [HW, Thm. 253] gives $k \leq \frac{2}{\sqrt{3}}\sqrt{D}$.)

Thus Vinogradov's Lemma is a big improvement over Thue's Lemma but is slightly worse than Geometry of Numbers methods. On the other hand, our main result (Theorem 9) applies to *any* binary quadratic form, not just to diagonal positive definite forms. Nevertheless, we believe Hagedorn's approach is "the right one": there are other (especially, non-diagonal) positive definite binary forms $q(x, y)$ for which the primes of the form $q(x, y)$ are determined by congruence conditions, and to prove the representation theorem by the above methods, the improvement offered by Geometry of Numbers bounds seems essential.

Finally, just I was completing this paper I found [Mo66]. Mordell studies prime numbers represented by diagonal forms. Moreover he uses Vinogradov's Lemma to derive Theorem 9 when $B = 0$ and n is prime and applies this to study representations of certain quadratic forms by primes. The only other significant difference is that Mordell's paper is six pages so treats matters in less detail. For instance he writes "I notice that this method [i.e., via Thue-Vinogradov] can be extended apparently to all the cases included in the classical theory when the class number of the genus is one, and gives the results with a minimum of effort." Note "apparently": here we show that these results indeed hold for all idoneal forms $x^2 + Dy^2$.

At the end of [Mo66] is an addendum acknowledging prior similar work of Venkoff (in a Russian textbook from the 1930's) and Nagell (in [N]), and writes "Neither author seems to have realized the full possibilities of the method." This seems ironic: although Mordell came closer to realizing the full possibilities of the method (again, there is more to be said about non-diagonal forms), he did not write much of it down, and 45 years later his work seems to have been nearly forgotten.[3] We hope that this semi-expository paper as well as the work of Hagedorn [Ha10] will revive some interest in this elementary but powerful approach to quadratic forms.

Acknowledgments: I thank Mariah Hamel for introducing me to Thue's Lemma and the "book proof" of the Two Squares Theorem, Jonathan P. Hanke for several helpful conversations, Thomas Hagedorn for cociting me in [Ha10], and Lee Goswick for finding some typographical errors. I am especially grateful to Andrew Granville

[3][Mo66] has zero MathSciNet citations as of October 2011.

for suggesting the replacement of Thue's Lemma with Vinogradov's Lemma and the corresponding improvement from Theorem 8 to Theorem 9.

1. The Lemmas of Thue and Vinogradov

The following remarkably simple and useful result was apparently first proved by A. Thue [Th02] (and published in what seems to be a very obscure journal) and later, but independently, by the brilliant amateur mathematician L. Aubry [Au13].

Theorem 1. *(Thue's Lemma) Let $n > 1$ be an integer, and let b be an integer which is relatively prime to n. There are integers x, y, not both zero, such that (i) $0 \leq |x| < \sqrt{n}$, $0 \leq |y| \leq \sqrt{n}$, and (ii) $x \equiv by \pmod{n}$.*

Although well known in certain circles – e.g. [N], [AZ] – we maintain that Thue's Lemma is not nearly as famous as it should be. Its extreme innocuousness notwithstanding, Theorem 1 is a powerful tool in many number-theoretic endeavors, including the study of integers represented by binary quadratic forms.

We will find useful a generalization of Theorem 1 due to I.M. Vinogradov [Vi27] (and later, but presumably independently, to A. Scholz [Sch]).

Theorem 2. *(Vinogradov's Lemma) Let $a, b, n \in \mathbb{Z}^+$ with $n > 1$ and $\gcd(ab, n) = 1$, and let $\alpha \in \mathbb{R}^{>0}$. There are integers x, y, not both zero, such that:*
(i) $ax \equiv by \pmod{n}$,
(ii) $|x| < \alpha$, $|y| \leq \frac{n}{\alpha}$.

Proof. Step 1: Consider $\{S = (i,j) \in \mathbb{Z}^2 \mid 0 \leq i \leq \lfloor \alpha \rfloor,\ 0 \leq j \leq \lfloor \frac{n}{\alpha} \rfloor\}$. Since $\#S = (\lfloor \alpha \rfloor + 1)\left(\lfloor \frac{n}{\alpha} \rfloor + 1\right) > \alpha \cdot \frac{n}{\alpha} = n$, by the Pigeonhole Principle there are distinct elements $(i_1, j_1),\ (i_2, j_2) \in S$ such that

$$ai_1 - bj_1 \equiv ai_2 - bj_2 \pmod{n}.$$

Put $x = i_1 - i_2$ and $y = j_1 - j_2$. Then x and y are not both zero, $ax \equiv by \pmod{n}$, $|x| \leq \lfloor \alpha \rfloor$ and $|y| \leq \lfloor \frac{n}{\alpha} \rfloor$.
Step 2: If $\alpha \notin \mathbb{Z}$, then $|x| \leq \alpha \iff |x| < \alpha$, and we are done. If $\alpha \in \mathbb{Z}$, then take $0 < \epsilon < \alpha$ and apply the result of Step 1 with $\alpha - \epsilon$ in place of α: there exist integers x and y, not both zero, so that $|x| \leq \alpha - \epsilon < \alpha$ and $|y| \leq \frac{n}{\alpha - \epsilon}$. But for sufficiently small ϵ we have $\lfloor \frac{n}{\alpha - \epsilon} \rfloor = \lfloor \frac{n}{\alpha} \rfloor$ and thus $|y| \leq \lfloor \frac{n}{\alpha} \rfloor \leq \frac{n}{\alpha}$. □

Remark 1.1: Vinogradov's Lemma implies Thue's Lemma: take $\alpha = \sqrt{n}$.

Remark 1.2: Vinogradov had $a = 1$ in Theorem 2, as in fact will be the case in all of our applications. But it costs nothing extra to state and prove the result in this more general way, and doing so identifies Theorem 2 as a (very) special case of a theorem of Brauer-Reynolds on small solutions to systems of linear congruences [BrRe51]. The Brauer-Reynolds Theorem should also be better known – the lone example I know of an elementary number theory text which makes use of it is [L] – but this is an axe to be ground elsewhere.

2. Preliminaries on Quadratic Reciprocity and Quadratic Forms

2.1. Quadratic reciprocity law.

Recall that for an integer n and an odd prime p, the **Legendre symbol** $(\frac{n}{p})$ 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 3. *(Quadratic Reciprocity) Let ℓ and p be distinct odd primes. Put $\ell^* = (-1)^{\frac{\ell-1}{2}}\ell$. Then:*
a) $(\frac{-1}{p}) = 1 \iff p \equiv 1 \pmod 4$.
b) $(\frac{2}{p}) = 1 \iff p \equiv \pm 1 \pmod 8$.
c) $(\frac{\ell^*}{p}) = (\frac{p}{\ell})$.

Proof. See e.g. [HW] or [IR, §5.2, Thm. 1]. □

2.2. **Binary quadratic forms.**

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

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

with $A, B, C \in \mathbb{Z}$.

We say that an integer m is **represented** by q – or, less formally, "of the form $q(x, y)$" – if there are $x, y \in \mathbb{Z}$ such that $q(x, y) = m$. An integer n is **primitively represented** by q if there are $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$ such that $q(x, y) = n$.

A quadratic form $q(x, y)$ is **primitive** if $\gcd(A, B, C) = 1$. When considering integer reperesentations, it is no loss of generality to restrict to the primitive case.

A quadratic form q is **anisotropic** if for all $(x, y) \in \mathbb{Z}^2$, $q(x, y) = 0 \implies (x, y) = (0, 0)$. We will only be interested in anisotropic forms here. In fact, we will almost entirely be concerned with forms satisfying the stronger property that for all $x, y \in \mathbb{R}$, $q(x, y) \geq 0$, with equality iff $(x, y) = (0, 0)$. Such forms are called **positive definite**.[4] A quadratic form is **indefinite** if there exist $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ such that $q(x_1, y_1) > 0$ and $q(x_2, y_2) < 0$.

The **discriminant** of $q(x, y)$ is defined as $\Delta = B^2 - 4AC$.

Remark 2.1: The binary quadratic form $q(x, y)$ is anisotropic iff Δ is not a square.

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

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

has discriminant $-4D = \Delta$; whereas if $\Delta \equiv 1 \pmod 4$ and $E = \frac{1-\Delta}{4}$, then

$$q_\Delta(x, y) = x^2 + xy + Ey^2$$

has discriminant $1 - 4E = \Delta$. The forms q_Δ are called **principal**.

Proposition 4. *Let $Q(x, y)$ be a quadratic form of discriminant Δ; 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 Δ is a square modulo n.

[4] Negative definite forms are defined in the obvious way but not usually studied, since replacing q with $-q$ we get back to the positive definite case.

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 Δ' of the quadratic form $Q'(x,y) = Q(px+qy, rx+sy)$ is equal to Δ. 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

$$\Delta = \Delta' = (2apr + bps + brq + 2cqs)^2 - 4nQ(r,s), \tag{1}$$

so Δ is a square modulo n. □

Next we record some simple multiplicative identities.

Proposition 5. *Let $D, A, B, x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Then:*

$$\left(x_1^2 + Dy_1^2\right)\left(x_2^2 + Dy_2^2\right) = \left(x_1x_2 - Dy_1y_2\right)^2 + D\left(x_1y_2 + x_2y_1\right)^2,$$

$$\left(Ax_1^2 + By_1^2\right)\left(x_2^2 + ABy_2^2\right) = A\left(x_1x_2 - By_1y_2\right)^2 + B\left(x_2y_1 + Ax_1y_2\right)^2,$$

$$\left(Ax_1^2 + By_1^2\right)\left(Ax_2^2 + By_2^2\right) = \left(Ax_1x_2 - By_1y_2\right)^2 + AB\left(x_1y_2 + x_2y_1\right)^2.$$

Corollary 6. *For any $\Delta \equiv 0 \pmod 4$, the set of integers represented by the principal form q_Δ is closed under multiplication.*

Remark 2.2: There are analogous multiplicative identities which show that the set of integers represented by a principal form of discriminant $\Delta \equiv 1 \pmod 4$ is also closed under multiplication. We will be mainly interested in diagonal forms, so we do not give the identities here. (In fact, it is a pleasant exercise to discover them.)

Theorem 7. *Let $q(x,y) = Ax^2 + Bxy + Cy^2$ be a primitive anisotropic quadratic form of discriminant Δ, and let p be an odd prime such that $(\frac{\Delta}{p}) = -1$.*
a) Suppose that $x, y \in \mathbb{Z}$ are such that $p \mid q(x,y)$. Then $p \mid x$ and $p \mid y$.
b) It follows that for all $(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, $\mathrm{ord}_p(q(x,y))$ is even.

Proof. Step 0: Put $P(t) = At^2 + Bt + C \in \mathbb{Z}[t]$. Since Δ is not a square modulo p, *a fortiori* it is not a square in $\mathbb{Z}$ – or equivalently, in $\mathbb{Q}$ – so that $p(t) \in \mathbb{Q}[t]$ is an irreducible quadratic. Our assumption $\gcd(A,B,C) = 1$ ensures that $p(t) \in \mathbb{Z}[t]$ is *primitive*, so by Gauss's Lemma $p(t)$ is an irreducible element of the UFD $\mathbb{Z}[t]$. Hence it is also prime, so that $R = \mathbb{Z}[t]/(p(t))$ is an integral domain.

On the other hand, let α be the complex number $\frac{-B+\sqrt{\Delta}}{2A}$. Then the homomorphism $\mathbb{Z}[t] \to \mathbb{Z}[\alpha]$ which sends t to α induces an isomorphism of rings $R \xrightarrow{\sim} \mathbb{Z}[\alpha]$.
Step 1: Let p be an odd prime number such that $(\frac{\Delta}{p}) = -1$. We claim that pR is a prime ideal; equivalently, we claim that the quotient ring $R/pR \cong \mathbb{Z}/p\mathbb{Z}[t]/(At^2 + Bt + C)$ is an integral domain. But in turn this is equivalent to the (natural image in $\mathbb{Z}/p\mathbb{Z}[t]$ of the) polynomial $p(t)$ being irreducible in $\mathbb{Z}/p\mathbb{Z}[t]$, which follows from our assumption that the discriminant Δ is not a square in the field $\mathbb{Z}/p\mathbb{Z}$. By Step 0, we also have that $p\mathbb{Z}[\alpha]$ is a prime ideal of $\mathbb{Z}[\alpha]$.
Step 2: Put $\overline{\alpha} = \frac{-B-\sqrt{\Delta}}{2A}$. Note that $\mathbb{Z}[\alpha] = \mathbb{Z}[\overline{\alpha}]$. For integers x and y, not both zero, we have in $\mathbb{Z}[\alpha]$ a factorization

$$q(x,y) = (x + \alpha y)(x + \overline{\alpha} y).$$

Therefore if $p \mid q(x,y)$, then since $p\mathbb{Z}[\alpha]$ is a prime ideal, we must have either $p \mid x + \alpha y$ or $p \mid x + \overline{\alpha} y$. Without loss of generality we consider the first case: we have that $\frac{x}{p} + \frac{y}{p}\alpha \in \mathbb{Z}[\alpha]$, i.e., there exist integers X and Y such that

$$\left(\frac{x}{p}\right) + \left(\frac{y}{p}\right)\alpha = X + Y\alpha.$$

Thus $X = \frac{x}{p}$ and $Y = \frac{y}{p}$, so that $p \mid x$ and $p \mid y$, establishing part a).
Step 3: By Step 2, if $p \mid q(x,y)$, then $\frac{x}{p}, \frac{y}{p} \in \mathbb{Z}$ and thus $\mathrm{ord}_p(q(\frac{x}{p}, \frac{y}{p})) = 2 + \mathrm{ord}_p(q(x,y))$. An evident induction finishes the proof. □

In light of Theorem 7, it is useful to give a name to odd prime numbers p bearing the property $(\frac{\Delta}{p}) = -1$ with respect to a fixed discriminant Δ. We call such primes **anisotropic primes** for Δ.

3. Thue-Vinogradov Applied to Binary Quadratic Forms

Let's apply Theorems 1 and 2 to the representation of integers by quadratic forms.

Theorem 8. *Let $q(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y]$ be an anisotropic quadratic form of discriminant $\Delta = B^2 - 4AC$. 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 $A > 0$, $B = 0$, $C < 0$, then $C < k < A$.
d) If $AC < 0$, then $|k| < \max(|A| + |B|, |C| + |B|)$.

Proof. a) 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. Thus there exist $b, l \in \mathbb{Z}$ such that $Ab^2 + Bb + C = ln$. If a prime p divides b and n, it also divides C, contradicting our assumption; thus we must have $\gcd(b,n) = 1$. We apply Thue's Lemma (Theorem 1) to get $x, y \in \mathbb{Z}$, not both zero, such that $0 \leq |x| < \sqrt{n}$, $0 \leq |y| \leq \sqrt{n}$ and $x \equiv by \pmod{n}$. On the one hand

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

and on the other,

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

proving part a).
b) If q is positive definite, then $k = \frac{q(x,y)}{n} > 0$.
c) Suppose $q(x,y) = Ax^2 + Cy^2$ with $A > 0$, $C < 0$. Then

$$C < \frac{q(x,y)}{n} < A.$$

d) If $AC < 0$, then

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

□

Theorem 9. *Let $q(x,y) = Ax^2 + Bxy + Cy^2 \in \mathbb{Z}[x,y]$ be an anisotropic. Let $n \in \mathbb{Z}^+$ be such that $\gcd(n, 2AC) = 1$ and $B^2 - 4AC$ is a square modulo n.*
a) There are nonzero integers x, y, k with $|k| < |B| + 2\sqrt{|A||C|}$ and $q(x,y) = kn$.
b) In addition to the hypotheses of part a), suppose moreover that $AC < 0$. Then there are nonzero integers x, y, k with $0 < |k| < |B| + \sqrt{|A||C|}$.

Proof. By interchanging x and y if necessary, we may assume $|A| \leq |C|$.
a) As in the proof of Theorem 8, there are $b, l \in \mathbb{Z}$ with $\gcd(b,n) = 1$ and $Ab^2 + Bb + C = ln$. Now apply Vinogradov's Lemma (Theorem 2) with $a = 1$ and $\alpha = |\frac{C}{A}|^{\frac{1}{4}}\sqrt{n}$ to get $x, y \in \mathbb{Z}$, not both zero, such that $x \equiv by \pmod{n}$ and

$$0 \leq |x| < |\frac{C}{A}|^{\frac{1}{4}}\sqrt{n},\ 0 \leq |y| \leq |\frac{A}{C}|^{\frac{1}{4}}\sqrt{n}.$$

Thus we have

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

$$0 < |q(x,y)| \leq |A||x|^2 + |B||x||y| + |C||y|^2 < (|B| + 2\sqrt{|A||C|})n.$$

b) If $AC < 0$, then

$$0 < |q(x,y)| \leq |Bxy| + ||A|x^2 - |C|y^2| < (|B| + \sqrt{|A||C|})n.$$

□

Remark 3.1: By the arithmetic-geometric mean inequality, if $|A| \neq |C|$, the bound $|k| < |B| + 2\sqrt{|A||C|}$ of Theorem 9 is an improvement of the bound $|k| < |A| + |B| + |C|$ of Theorem 8. When $|A|$ and $|C|$ are approximately equal in size the gain is modest, but when one is much larger than the other it is a significant improvement. When applied to *principal forms*, Theorem 9 gives a considerably more useful result.

Corollary 10. *a) Let D be an integer such that $-D$ is not a square. Suppose $n \in \mathbb{Z}^+$ is a nonsquare such that $\gcd(n, 2D) = 1$ and $-D$ is a square modulo n. Then there exist integers x, y, k such that*

$$x^2 + Dy^2 = kn,\ 0 < |k| < 2\sqrt{|D|}.$$

b) Let E be an integer such that $1 - 4E$ is not a square. Suppose $n \in \mathbb{Z}^+$ is a nonsquare such that $\gcd(n, 2E) = 1$ and $1 - 4E$ is a square modulo n. Then there exist integers x, y, k such that

$$x^2 + xy + Ey^2 = kn,\ 0 < |k| < 1 + 2\sqrt{|E|}.$$

4. First Applications of Theorem 9

In this section we give some especially simple applications of Theorem 9, of a sort that we feel would be suitable for a first undergraduate course in number theory in which quadratic reciprocity has been introduced.

4.1. **Indefinite forms.**

Theorem 11. *Let n be an odd integer such that 2 is a square modulo n. Then there exist integers x, y such that $n = x^2 - 2y^2$.*

Proof. By Theorem 8c), there are integers x, y, not both zero, such that $x^2 - 2y^2 = kp$ for $-2 < k < 1$. Thus $k = -1$, so that $x^2 - 2y^2 = -n$. This is just the opposite of what we wanted to show, but take heart. The form $q(x, y) = x^2 - 2y^2$ is the principal form of discriminant -8, so that by Proposition 5 the set of nonzero integers it represents is closed under multiplication. Moreover, $1^2 - 2 \cdot 1^2 = -1$. Therefore Proposition 5 implies that q represents n iff it represents $-n$. □

Corollary 12. *A nonzero integer is of the form $q(x, y) = x^2 - 2y^2$ iff for every prime $p \equiv 3, 5 \pmod 8$, $\mathrm{ord}_p(n)$ is even.*

Proof. By Proposition 5, the set of nonzero integers of the form $x^2 - 2y^2$ is closed under multiplication. It certainly includes all squares, $2 = 2^2 - 2 \cdot 1^2$, and by Theorem 11 all primes $p \equiv \pm 1 \pmod 8$. Therefore the conditions given in the statement of the corollary are sufficient for n to be of the form $x^2 - 2y^2$. Conversely, the primes $p \equiv 3, 5 \pmod 8$ are precisely those for which $(\frac{\Delta(q)}{p}) = (\frac{8}{p}) = (\frac{2}{p}) = -1$ – i.e., are anisotropic primes – so by Theorem 7, it is necessary that $\mathrm{ord}_p(n)$ be even at all such primes. □

Theorem 13. *Let $p > 3$ be a prime number such that $(\frac{3}{p}) = 1$. Then there exist integers x, y such that $x^2 - 3y^2 = (-1)^{\frac{p-1}{2}} p$.*

Proof. Applying Theorem 9c), we get nonzero integers x, y, k with $x^2 - 3y^2 = kp$ and $-3 < k < 1$, i.e., $k = -2$ or $k = -1$.
Case 1: $p \equiv 1 \pmod 4$. Together with $(\frac{3}{p}) = 1$, this implies $p \equiv 1 \pmod 3$. Reducing $x^2 - 3y^2 = kp$ modulo 3 shows $k \equiv 1 \pmod 3$, so $k = -2$. Thus $-2p$ is of the form $x^2 - 3y^2$, which is not the answer that we want. But we can get there: $-2 = 1^2 - 3 \cdot 1^2$ is also represented, so by Proposition 4 also $(-2p)(-2) = 4p$ is of the form $x^2 - 3y^2$. Reducing $x^2 - 3y^2 = 4p$ modulo 4 shows that x and y are both even, so $(\frac{x}{2})^2 - 3(\frac{y}{2})^2 = p = (-1)^{\frac{p-1}{2}} p$.
Case 2: $p \equiv 3 \pmod 4$. Together with $(\frac{3}{p}) = 1$, this implies $p \equiv 2 \pmod 3$. Reducing $x^2 - 3y^2 = kp$ modulo 3 shows $k = -1$, so $x^2 - 3y^2 = -p = (-1)^{\frac{p-1}{2}} p$. □

Corollary 14. *Let n be a nonzero integer.*
a) If $\mathrm{ord}_3(n)$ is even, then n is of the form $x^2 - 3y^2$ iff:
(i) For all odd primes p with $(\frac{3}{p}) = -1$, $\mathrm{ord}_p(n)$ is even; and
(ii) n is positive iff the number of prime divisors p of n such that 3 is a square modulo p and $p \equiv 2 \pmod 3$, counted with multiplicity, is even.
b) Suppose that $\mathrm{ord}_3(n)$ is odd. Then n is of the form $x^2 - 3y^2$ iff both of the following hold:
(i) For all odd primes p with $(\frac{3}{p}) = -1$, $\mathrm{ord}_p(n)$ is even;
(ii) n is positive iff the number of prime divisors p of n such that 3 is a square modulo p and $p \equiv 2 \pmod 3$, counted with multiplicity, is odd.

Proof. Step 0: Suppose $n = 3^a N$ with $\gcd(3, N) = 1$ and $x^2 - 3y^2 = 3^a N$. Then $3 \mid x$ so we may put $x = 3X$ and substitute, getting $3X^2 - y^2 = 3^{a-1} N$. If $a > 1$, then $3 \mid y$ so we may put $y = 3Y$ and substitute, getting $X^2 - 3Y^2 = 3^{a-2} N$. So we see: if a is even, $n = 3^a N$ is of the form $x^2 - 3y^2$ iff N is of that form; and if n is odd, $n = 3^a N$ is of the form $x^2 - 3y^2$ iff $-N$ is of that form.
Step 1: Taking Step 0 into account, it suffices to find necessary and sufficient conditions for an integer n with $\gcd(3, n) = 1$ to be of the form $x^2 - 3y^2$. Since

every square is of the form $x^2 - 3y^2$ and for every prime p with $(\frac{3}{p}) = 1$, Theorem 13 shows that $\pm p$ is of the form $x^2 - 3y^2$, if n satisfies conditions (i) and (ii) in the statement of the corollary, then $\pm n = x^2 - 3y^2$. Reducing modulo 3, we see that the sign is determined by the parity condition in (ii).
Conversely, suppose $n = x^2 - 3y^2$. The primes p with $(\frac{3}{p}) = -1$ are precisely those for which $(\frac{\Delta(q)}{p}) = -1$ – i.e., are anisotropic primes – so by Theorem 7, it is necessary that $\text{ord}_p(n)$ be even at all such primes, so (i) is necessary. Again, reduction modulo 3 shows that (ii) is necessary. □

Several more indefinite forms can be treated in this manner. In fact – unlike the case of positive definite forms – it seems likely that representation theorems can be proven for *infinitely many* indefinite binary quadratic forms. So we had better leave this aside for now and turn to the definite case.

4.2. **Positive definite forms.**

If $D = 1$, then Corollary 10a) immediately yields:

Theorem 15. *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 16. *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, $(\frac{-1}{p}) = 1$ if $p \equiv 1 \pmod 4$ and $(\frac{-1}{p}) = -1$ if $p \equiv 3 \pmod 4$. Therefore the conditions on the p-order at primes congruent to 3 modulo 4 are necessary by Theorem 7b). 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 15, p is of the form $x^2 + y^2$. By Proposition 5a), if

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

then n is of the form $x^2 + y^2$. □

Theorem 17. *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. By Corollary 10a), there are 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 18. *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, $(\frac{-2}{p}) = 1$ if $p \equiv 1, 3 \pmod 8$ and $(\frac{-2}{p}) = -1$ if $p \equiv 5, 7 \pmod 8$. The remainder of the proof is very similar to that of Corollary 16. Details left to the reader. □

Theorem 19. *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 Corollary 10a), there exist integers $x, y \in \mathbb{Z}$ such that $x^2+3y^2 = kn$ for some k, $1 \leq k \leq 3$. If $k = 1$, we're done.

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 $(\frac{-3}{p}) = 1$. By quadratic reciprocity, this implies $p \equiv 1 \pmod 3$. That is, to say, n divisible only by primes of the form 1 (mod 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.
Consider the case $x^2 + 3y^2 = 3n$. Then $x = 3X$ for $X \in \mathbb{Z}$: substituting and simplifying gives $3X^2 + y^2 = n$, so n is of the form $x^2 + 3y^2$. □

Corollary 20. *A positive integer n is of the form $x^2 + 3y^2$ iff $\mathrm{ord}_2(n)$ is even and for every prime $p \equiv -1 \pmod 3$, $\mathrm{ord}_p(n)$ is even.*

Proof. The method of proof of Corollaries 16 and 18 establishes this result for all odd n. It follows by Proposition 6 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. □

Theorem 21. *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. Writing $x^2 + 4y^2$ as $x^2 + (2y)^2$, the result becomes equivalent to the claim that in the conclusion of Theorem 15, 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. □

Corollary 22. *A positive integer n is of the form $x^2 + 4y^2$ iff $\mathrm{ord}_2(n) \neq 1$ and for every prime $p \equiv -1 \pmod 4$, $\mathrm{ord}_p(n)$ is even.*

Proof. Again the arguments for odd n are similar to those given above. If $\mathrm{ord}_2(n) = 1$, 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. □

Theorem 23. *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 Corollary 10a), there exist integers $x, y \in \mathbb{Z}$ such that $x^2+7y^2 = kn$ for some k, $1 \leq k \leq 5$. 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 $(\frac{-7}{p}) = 1$, 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 $X^2 + 7Y^2 = p$. □

Corollary 24. *A positive integer is of the form $x^2 + 7y^2$ iff $\mathrm{ord}_2(n) \neq 1$ and for every prime $p \equiv 3, 5, 6 \pmod 7$, $\mathrm{ord}_p(n)$ is even.*

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

5. Primes of the form $x^2 + Dy^2$ for idoneal D

5.1. Auxiliary Congruence Conditions and Small Examples.

The reader may have wondered why, in §4.2, the values $D = 5$ and $D = 6$ were skipped. The answer is that, for these values, the converse of Proposition 4 is false: the necessary condition $(\frac{-D}{p}) = 1$ is no longer sufficient for a prime p to be of the form $x^2 + Dy^2$.

Example 5.1: Let $D = 5$ and $p = 3$. Then $(\frac{-5}{3}) = 1$, but the equation $3 = x^2 + 5y^2$ has no solutions.

Example 5.2: Let $D = 6$ and $p = 5$. Then $(\frac{-6}{5}) = 1$, but the Diophantine equation $5 = x^2 + 6y^2$ has no solutions.

The reasons for this are not so mysterious: for these values of D – as well as infinitely many others – there are *auxiliary congruence conditions* to take into account. Indeed we have the following result.

Proposition 25. *(Auxiliary Congruences) Let $D \in \mathbb{Z}^+$, and let p be a prime with $\gcd(p, 2D) = 1$. Suppose that there exist $x, y \in \mathbb{Z}$ such that $x^2 + Dy^2 = p$. Then:*
a) For each odd prime ℓ dividing D, $(\frac{p}{\ell}) = 1$.
b) If $D \equiv 0 \pmod 8$, then $p \equiv 1 \pmod 8$.
c) If $D \equiv 1, 4, 5 \pmod 8$, then $p \equiv 1 \pmod 4$.
d) If $D \equiv 2 \pmod 8$, then $p \equiv 1, 3 \pmod 8$.
e) If $D \equiv 6 \pmod 8$, then $p \equiv 1, 7 \pmod 8$.

Proof. For part a) we reduce modulo ℓ to get $x^2 \equiv p \pmod \ell$. Since $\gcd(p, D) = 1$, $\gcd(p, \ell) = 1$ and thus $(\frac{p}{\ell}) = 1$. The other cases involve reducing modulo 8 and considering the various possibilities for $p \pmod 8$: details are left to the reader. □

Theorem 26. *Let p be a prime number with $\gcd(10, p) = 1$. Suppose that $p \equiv 1 \pmod 4$ and $(\frac{-5}{p}) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 5y^2$.*

Proof. By Corollary 10a), there are integers $x, y \in \mathbb{Z}$ such that $x^2 + 5y^2 = kp$ for some k, $1 \leq k \leq 4$. Reducing modulo 5, we get $x^2 \equiv kp \pmod 5$, i.e., kp is a nonzero square modulo 5. Our hypotheses imply that p is a square modulo 5, and hence so is k: i.e., $k = 1$ or $k = 4$. If $x^2 + 5y^2 = 4p$, then by Lemma 31, x and y are even, so $p = (\frac{x}{2})^2 + 5(\frac{y}{2})^2$. □

Theorem 27. *A prime p is of the form x^2+6y^2 iff $(\frac{-6}{p}) = 1$ and $p \equiv \pm 1 \pmod 8$.*

Proof. We may assume $\gcd(p, 10) = 1$. The given conditions are necessary by Proposition 25. Conversely, assume they hold. By Corollary 10a), there are $x, y \in \mathbb{Z}$ such that $x^2 + 6y^2 = kp$ for some k, $1 \leq k \leq 4$. Reducing modulo 3, we get $x^2 \equiv kp \pmod 3$, so that $kp \equiv 0, 1 \pmod 3$. Our hypotheses imply $p \equiv 1 \pmod 3$, so $k = 1, 3, 4$. By Lemma 31, if $4p$ is of the form $x^2 + 6y^2$, so is p.

It remains to consider the case $k = 3$: $x^2+6y = 3p$. Write $x = 3X$ and substitute, getting $3x^2 + 2y^2 = p$. Certainly 3 is not of the form $x^2 + 6y^2$, so we may assume $p > 3$. Reducing modulo 3 then gives $p \equiv 2y^2 \equiv 2 \pmod 3$, a contradiction. □

The following result applies the method to a nonprincipal form.

Theorem 28. *A prime p different from 2 and 5 is of the form $2x^2 + 5y^2$ iff $(\frac{-10}{p}) = 1$ and $p \equiv 2, 3 \pmod 5$ iff $p \equiv 7, 13, 23, 27 \pmod{40}$.*

Proof. Necessity: Suppose $p = 2x^2 + 5y^2$. Reducing modulo p gives $2x^2 + 5y^2 \equiv 0 \pmod p$. If $x \equiv 0 \pmod p$, then $p = 2x^2 + 5y^2$ shows $y \equiv 0 \pmod p$ and thus $p = 2x^2+5y^2$ is divisible by p^2, a contradiction. Therefore $2, 5, x, y$ are all invertible modulo p, and $2x^2 + 5y^2 \equiv 0 \implies \frac{-5}{2} \equiv X^2 \pmod p$, which holds iff $-10 \equiv X^2 \pmod p$, i.e., iff $(\frac{-10}{p}) = 1$. Similarly, reducing modulo 5 gives $p \equiv 2x^2 \pmod 5$, so p is not a square modulo 5 and hence $p \equiv 2, 3 \pmod 5$. Thus

$$1 = (\frac{-10}{p}) = (\frac{-2}{p})(\frac{5}{p}) = -(\frac{-2}{p}),$$

so $\frac{-2}{p} = -1$, and thus $p \equiv 5, 7 \pmod 8$. A Chinese Remainder Theorem calculation gives $p \equiv 2, 3 \pmod 5$ and $p \equiv 5, 7 \pmod 8 \iff p \equiv 7, 13, 23, 27 \pmod{40}$.
Sufficiency: Suppose $p > 5$ satisfies the necessary congruence conditions. In particular p is prime to 10 and such that $(\frac{-10}{p}) = 1$, so by Theorem 9 there are $x, y, k \in \mathbb{Z}$ with $2x^2 + 5y^2 = kp$ and $1 \leq k < 2\sqrt{10}$, i.e., $1 \leq k \leq 5$. If $k = 1$, we're done.
• Suppose $2x^2+5y^2 = 2p$. Reducing modulo 5 gives $p \equiv x^2 \pmod 5$, contradiction.
• Suppose $2x^2+5y^2 = 3p$. Reducing modulo 5 gives $p \equiv x^2 \pmod 5$, contradiction.
• Suppose $2x^2 + 5y^2 = 4p$. Then y is even, and reducing modulo 4 shows x is even. So we may put $x = 2X$, $y = 2Y$ to get $2X^2 + 5Y^2 = p$.
• Suppose $2x^2 + 5y^2 = 5p$. Put $x = 5X$ to get $10X^2 + y^2 = p$. Reducing mod 5 shows $(\frac{p}{5}) = 1$, contradiction.

□

5.2. **The representation theorem.**

Example 5.3: Consider the quadratic form $q(x, y) = x^2 + 11y^2$. In this case, the congruence conditions $(\frac{-11}{p}) = 1$ togther with the auxiliary congruence conditions of Proposition 25 are *not* sufficient for a prime p to be of the form x^2+11y^2. Indeed, take $p = 353$; it is congruent to 1 modulo 44, so satisfies all congruence conditions, but is easily seen not to be of the given form. In fact, with a bit more work it can be shown that the congruence $x^2 + 11y^2 \equiv 353 \pmod n$ has solutions for every $n \in \mathbb{Z}^+$. That is, the set of primes represented by $x^2 + 11y^2$ is not characterized by any set of congruence conditions whatsoever. In fact, the following is true.

Theorem 29. *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 at most two further values of D. Any further values of D which exist are at least 10^8.
*A positive integer D satisfying the above equivalent conditions is said to be **idoneal**.*

Proof. This is a classical, but not easy, result. The most accessible reference for the nonspecialist is probably [C]. □

Remark 5.2: It has been shown that assuming the Generalized Riemann Hypothesis (GRH), $D = 1848$ is indeed the largest idoneal number. It is known unconditionally that if there are any idoneal numbers $D > 1848$, there is exactly one such squarefree number D_{big}. Depending upon certain congruence properties of D_{big}, there may also be one further nonsquarefree idoneal number of the form $N^2 D_{\text{big}}$.[5]

In other words, we need only try out our elementary methods on idoneal numbers D. Conversely, we will now show that (at least) for all squarefree idoneal numbers D appearing on the above list, our elementary methods succeed in determining all primes represented by $x^2 + Dy^2$.

Theorem 30. *(Representation Theorem) Let D be one of the 65 idoneal numbers listed in Theorem 29. Then an odd prime p is of the form $x^2 + Dy^2$ iff $p = D$ or all of the following hold:*
(i) $(\frac{-D}{p}) = 1$,
(ii) For all odd primes $\ell \mid D$, $(\frac{p}{\ell}) = 1$,
(iii) If $D \equiv 0 \pmod 8$, then $p \equiv 1 \pmod 8$,
(iv) If $D \equiv 1, 4, 5 \pmod 8$, then $p \equiv 1 \pmod 4$,
(v) If $D \equiv 2 \pmod 8$, then $p \equiv 1, 3 \pmod 8$,
(vi) If $D \equiv 6 \pmod 8$, then $p \equiv 1, 7 \pmod 8$.

Of course Theorem 30 is really 65 different results, of which we have already proved the first (and easiest!) seven, corresponding to $1 \leq D \leq 7$. I don't know how to prove any 65 theorems without taking some time and space, but I have tried to organize cognate cases and describe various routine calculations in a uniform, high level way so as to make the proof reasonably palatable. We give two easy preparatory lemmas and then begin the proof proper. In view of the of the Auxiliary Congruences (iii) through (vi), it is natural to group together the values of D lying in the same congruence class modulo 8, and this is what we do.

5.3. **Preparatory Lemmas.**

Lemma 31. *Suppose $A, B, x, y \in \mathbb{Z}$ are such that $4n = Ax^2 + By^2$. Suppose moreover that one of the following holds:*
(i) A is odd and $B \equiv 2 \pmod 4$ (or conversely).

[5]It is very common the find in the literature the statement that there is at most one further idoneal value of D, but in [Ka09], E. Kani argues convincingly that this must be a mistake.

(ii) A and B are both odd and $A \equiv B \pmod 4$.
Then x and y are both even, hence $n = A(\frac{x}{2})^2 + B(\frac{y}{2})^2$.

Proof. We need only reduce $4n = Ax^2 + By^2$ modulo 4 and note that under either hypothesis, $Ax^2 + By^2 \equiv 0 \pmod 4$ forces x and y to be even. □

Lemma 32. *Let q be a prime number with $\gcd(q, n) = 1$. Suppose that $\mathrm{ord}_q(D) = 1$ and $\mathrm{ord}_q(kn) \geq 2$. Then if $x^2 + Dy^2 = kn$, then $x = qX$ and $y = qY$ so that $X^2 + Dy^2 = \frac{k}{q^2}n$.*

Proof. Since $q \mid D$ and $q \mid k$, $q \mid x^2$. Since q is prime, by Euclid's Lemma $q \mid x$ and we may take $x = qX$. Substituting and simplifying gives $qX^2 + \frac{D}{q}y^2 = \frac{k}{q}n$. Since $q \mid qX^2$ and $q \mid \frac{k}{q}n$, $q \mid \frac{D}{q}y^2$. Since q is prime and $q \nmid \frac{D}{q}$, $q \mid y^2$ and then $q \mid y$. Taking $y = qY$ and simplifying, we get $X^2 + Dy^2 = \frac{k}{q^2}n$. □

5.4. **Proof of the Representation Theorem: $D \equiv 1, 5 \pmod 8$.**

Suppose $D \in$

$$\{5, 9, 13, 21, 25, 33, 37, 45, 57, 85, 93, 105, 133, 165, 177, 253, 273, 345, 357, 385, 1365\}.$$

We have $x, y, k \in \mathbb{Z}$ with $x^2 + Dy^2 = kp$ and $1 \leq k \leq 2\sqrt{D}$.
Step 0: If $k = 1$, we are done.
Step 1: We claim first that we cannot have $k = 2$: indeed, each of the above values of D is divisible by some $q \in \{3, 5, 11, 13, 19, 37\}$, hence by an odd prime q with $(\frac{2}{q}) = -1$. Therefore reducing $x^2 + Dy^2 = 2p$ modulo q gives a contradiction. Moreover, suppose $4 \mid k$. Put $k = 4K$. By Lemma 31 $x^2 + Dy^2 = 4K$ implies $x = 2X$, $y = 2Y$ and thus $X^2 + DY^2 = k$. So we may assume k is odd.
Step 2: Since $p, D \equiv 1 \pmod 4$, reducing modulo 4 shows $k \not\equiv 3 \pmod 4$.
Step 3: If q is an odd prime dividing D, then reducing (2) modulo q shows $(\frac{k}{q}) \neq -1$.
Step 4: If q is an odd prime exactly dividing D, then by Lemma 32 we need not consider any values of k with $\mathrm{ord}_q(k) \geq 2$.
Step 5: We compile the list of *anisotropic primes*, i.e., primes $\ell \leq 2\sqrt{D}$ with $\gcd(\ell, 2D) = 1$ and $(\frac{-D}{\ell}) = -1$. For each of these primes, if $\ell \mid k$ then $\ell \mid x$, $\ell \mid y$, so $(\frac{x}{\ell})^2 + D(\frac{y}{\ell})^2 = \frac{k}{\ell^2}p$. Thus we need not consider values of k which are divisible by any anistropic prime. It turns out that in all cases every prime $\ell < \sqrt{D}$ with $\gcd(\ell, 2D) = 1$ is anisotropic, but there may be "isotropic primes" ℓ with $\sqrt{D} \leq \ell < 2\sqrt{D}$ with $(\frac{-D}{\ell}) = 1$. Thus the values of k we need to consider are those for which every odd prime divisor is istotropic or divides D; are exactly divisible by q if $\mathrm{ord}_q(D) = 1$; are either odd or exactly divisible by 2; and are not congruent to 3 modulo 4. Happily, in all cases this leaves us with a short (possibly empty) list of values of k to consider. In fact, it turns out that the above considerations complete the proof for each of the following values of D:

$$D \in \{9, 13, 21, 33, 37, 85, 93, 105, 133, 165, 177, 253, 273\}.$$

Step 6: We consider the remaining cases.
D = 25: We are left to consider $k = 5$, and reducing modulo 5 gives a contradiction.
D = 45: We are left to consider $k = 6, 9, 10$. If $k = 6$, take $x = 3X$ to get $3X^2 + 9y^2 = 6p$ and reduce modulo 3 to get a contradiction. If $k = 9$, take $x = 9X$ to get $9X^2 + 5y^2 = p$, and reduce modulo 3 to get a contradiction. If $k = 10$, take $x = 5X$ to get $5X^2 + 9y^2 = 2p$, and reduce modulo 5 to get a contradiction.

D = 57: We are left to consider $k = 6$. Take $x = 3X$ to get $3X^2 + 19y^2 = 2p$, and reduce modulo 3 to get a contradiction.
D = 345: We are left to consider $k = 30$. Take $x = 5X$ to get $5X^2 + 69y^2 = 6p$, and reduce modulo 23 to get a contradiction.
D = 357: We are left to consider $k = 21$. Take $x = 21X$ to get $21X^2 + 17y^2 = p$, and reduce modulo 3 to get a contradiction.
D = 385: We are left to consider $k = 14$. Take $x = 7X$ to get $7X^2 + 55y^2 = 2p$, and reduce modulo 7 to get a contradiction.
D = 1365: We are left to consider $k = 30$. Take $x = 15X$ to get $15X^2+91y^2 = 2p$, and reduce modulo 5 to get a contradiction.

5.5. **Proof of the Representation Theorem: $D \equiv 2, 6 \pmod 8$.**

Suppose $D \in \{2, 4, 6, 10, 18, 22, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462\}$.

Let $p > D$ be a prime satisfying the necessary congruences of the Representation Theorem. We wish to show that there are $x, y \in \mathbb{Z}$ such that $x^2 + Dy^2 = p$. By Corollary 10a) there exist $x, y, k \in \mathbb{Z}$ such that

$$x^2 + Dy^2 = kp \tag{2}$$

with $1 \leq k \leq 2\sqrt{D} = \sqrt{4D}$.
Step 0: If $k = 1$, we're done.
Step 1: Suppose $k = 2$. Then for any odd prime $\ell \mid D$, reducing $x^2 + Dy^2 = 2p$ modulo ℓ yields $1 = (\frac{2p}{\ell}) = (\frac{2}{\ell})(\frac{p}{\ell})$. Since one of our auxiliary congruences is $(\frac{p}{\ell}) = 1$, we conclude $(\frac{2}{\ell}) = 1$, i.e., every odd prime divisor of D is congruent to $\pm 1 \pmod 8$. But this is not the case for any of our D's, a contradiction.
Step 2: If $4 \mid k$, then since $D \equiv 2 \pmod 4$, reducing $x^2 + Dy^2 \equiv 4k'p$ modulo 4 gives a contradiction.
Step 3: Suppose k is divisible by a prime ℓ with $\gcd(\ell, D) = 1$. Then (one computes) in all cases we have $(\frac{\Delta}{\ell}) = -1$, so ℓ is an anisotropic prime for q, so $x^2 + Dy^2 = kp$ implies x and y are both divisible by ℓ and thus $(\frac{x}{\ell})^2 + D(\frac{y}{\ell})^2 = (\frac{k}{\ell^2})p$. Continuing in this way, we may assume that k is not divisible by any anisotopic primes.
Case 4: Suppose k is divisible by an odd prime $q \mid D$.
D = 10: Then $q = k = 5$. If $x^2 + 10y^2 = 5p$, then we may put $x = 5X$ to get $5X^2 + 2y^2 = p$, and reducing modulo 5 gives a contradiction.
D = 18: Then $q = 3$. Since $\lfloor 2\sqrt{18} \rfloor = 8$, we must then have that $\mathrm{ord}_3(kp) = 1$. Thus $x^2+18y^2 = 3Kp$ yields $3X^2+6y^2 = Kp$ with $\gcd(Kp, 3) = 1$, a contradiction.
D = 22 or 58: Then there is no odd prime $q \mid D$ with $q \leq 2\sqrt{D}$.
D = 30: Then $q = 3$ or 5 and $k = 6$ or 9. If $k = 6$, take $x = 6X$ to get $6X^2 + 5y^2 = p$, and reduce modulo 3 to get a contradiction. If $k = 9$, take $x = 3X$ to get $3X^2 + 10y^2 = 3p$ and then $y = 3Y$ to get $X^2 + 30y^2 = p$.
D = 42: Then $q = 3$ or $q = 7$. Suppose first that $q = 3$, so $k = 3$ or $k = 6$. Since $(\frac{p}{7}) = 1$ and $(\frac{3}{7}) = (\frac{6}{7}) = -1$, reducing $x^2 + 42y^2 = kp$ modulo 7 gives a contradiction. Now suppose $q = 7$, so $k = 7$: put $x = 7X$ to get $7X^2 + 6y^2 = p$; reducing modulo 7 gives a contradiction.
D = 70: Reducing (2) modulo 5 and 7 gives $(\frac{k}{5}), (\frac{k}{7}) \neq -1$. Moreover $q = 5$ or $q = 7$. If $q = 5$, then we need consider only $k = 15$: take $x = 5X$ to get $5X^2 + 14y^2 = 3p$; reducing modulo 5 gives a contradiction. If $q = 7$, we need consider only $k = 14$: take $x = 14X$ to get $14X^2 + 5y^2 = 2p$; reducing modulo 5

gives a contradiction.
D = 78: Reducing (2) modulo 3 and 13 gives $(\frac{k}{3}), (\frac{k}{13}) \neq -1$. Moreover $q = 3$ or $q = 13$. If $q = 3$, we need consider only $k = 3$: take $x = 3X$ to get $3X^2 + 26y^2 = p$; reducing modulo 3 gives a contradiction. If $q = 13$, we need consider only $k = 13$: take $x = 13X$ to get $13X^2 + 6y^2 = p$; reducing modulo 13 gives a contradiction.
D = 102: Reducing (2) modulo 3 and 17 gives $(\frac{k}{3}), (\frac{k}{17}) \neq -1$. Moreover $q = 3$ or $q = 17$. If $q = 3$, we need consider only $k = 15$: take $x = 3X$ to get $3X^2+34y^2 = 5p$; reducing modulo 3 gives a contradiction. If $q = 17$ then $k = 17$ and $(\frac{17}{3}) = -1$.
D = 130: Reducing (2) modulo 5 and 13 gives $(\frac{k}{5}), (\frac{k}{13}) \neq -1$. Moreover $q = 5$ or $q = 13$. If $q = 5$ we need consider only $k = 10$: take $x = 5X$ to get $5X^2+26y^2 = 2p$; reducing modulo 5 gives a contradiction. If $q = 13$ then $k = 13$ and $(\frac{13}{5}) = -1$.
D = 190: Reducing (2) modulo 5 and 19 gives $(\frac{k}{5}), (\frac{k}{19}) \neq -1$. Moreover $q = 5$ or $q = 19$. If $q = 5$ we need only consider $k = 5$: take $x = 5X$ to get $5X^2 + 38y^2 = p$; reducing modulo 5 gives a contradiction. If $q = 19$ then $k = 19$: take $x = 19X$ to get $19X^2 + 10y^2 = p$; reducing modulo 19 gives a contradiction.
D = 210: Reducing (2) modulo 3, 5 and 7 gives $(\frac{k}{3})$, $(\frac{k}{5}), (\frac{k}{7}) \neq -1$. Moreover $q = 3, 5, 7$. If $q = 3$ then $k = 15$ or 21. In the former case, take $x = 15X$ to get $15X^2 + 14y^2 = p$; reducing modulo 3 gives a contradiction. In the latter case, take $x = 21X$ to get $21X^2+10y^2 = p$; reducing modulo 7 gives a contradiction. If $q = 5$, then $k = 15$: take $x = 15X$ to get $15X^2 + 14y^2 = p$; reducing modulo 3 gives a contradiction. If $q = 7$, then $k = 21$, which we have already ruled out.
D = 330: Reducing (2) modulo 3, 5 and 11 gives $(\frac{k}{3})$, $(\frac{k}{5}), (\frac{k}{11}) \neq -1$. Morever, $q = 3, 5, 11$. From these values of q we need consider only $k = 15$. Take $x = 15X$ to get $15X^2 + 22y^2 = p$, and reduce modulo 5 to get a contradiction.
D = 462: Reducing (2) modulo 3, 7 and 11 gives $(\frac{k}{3})$, $(\frac{k}{7}), (\frac{k}{11}) \neq -1$. Moreover $q = 3, 7, 11$ and from these values of q we must consider $k = 15, 22, 42$. If $k = 15$, take $x = 3X$ to get $3X^2 + 154y^2 = 5p$; reducing modulo 3 gives a contradiction. If $k = 22$, take $x = 22X$ to get $22X^2 + 21y^2 = p$; reducing modulo 11 gives a contradiction. If $k = 42$, take $x = 42X$ to get $42X^2 + 11y^2 = p$; reducing modulo 3 gives a contradiction.

5.6. **Proof of the Representation Theorem: $D \equiv 3, 7 \pmod 8$.**

Suppose $D \in \{3, 7, 15\}$.

We have already considered $D = 3$ and $D = 7$, so suppose $D = 15$. Reducing (2) modulo 3 and 5 gives $(\frac{k}{3}), (\frac{k}{5}) \neq -1$, so we are left to consider $k = 4$ and $k = 6$. Reducing $x^2 + 15y^2 = 4p$ modulo 8 shows that both x and y are even, so taking $x = 2X$, $y = 2Y$ gives $X^2 + 15Y^2 = p$. If $k = 6$, we may take $x = 3X$, getting $3X^2 + 5y^2 = 2p$, and reducing modulo 4 gives a contradiction.

5.7. **Proof of the Representation Theorem: $D \equiv 4 \pmod 8$.**

Suppose $D \in \{4, 12, 28, 60\}$.

$D = 4$ has already been considered (Theorem 21); otherwise $D = 4D'$ with $D' \equiv 3 \pmod 4$ and D' idoneal. Suppose p satisfies the necessary congruences of the Representation Theorem. These congruences conditions together with the theorem for

D' imply that p is of the form $x^2 + D'y^2 = p$. Reducing modulo 4 shows that y is even, so $p = x^2 + D'(2Y)^2 = x^2 + DY^2$.

5.8. **Proof of the Representation Theorem:** $D \equiv 0 \pmod 8$**.**

Suppose $D = 8D' \in$

$$\{8, 16, 40, 48, 72, 88, 120, 168, 232, 240, 280, 312, 408, 520, 760, 840, 1320, 1848\}.$$

Let p be an odd prime satisfying the Congruence Conditions of the Representation Theorem. By Corollary 10a), there are $x, y, k \in \mathbb{Z}^+$ with

$$x^2 + Dy^2 = kp,\ 1 \leq k < 2\sqrt{D}.$$

Step 0: If $k = 1$, we are done.
Step 1: Reducing $x^2 + 8D'y^2 = kp$ modulo 8 gives $k \equiv 0, 1, 4 \pmod 8$.
Step 2: Suppose $k = 4$: if $x^2 + 8D'y^2 = 4p$, then we may take $x = 2X$ to get $X^2 + 2D'y^2 = p$. Reducing modulo 8 gives $X^2 + 2D'y^2 \equiv 1 \pmod 8$. Now observe that for all the values of D above we have $\mathrm{ord}_2(D') \in \{1, 2\}$, so if y were odd $X^2 \equiv 5, 7 \pmod 8$, a contradiction. Therefore we may put $y = 2Y$ to get $X^2 + DY^2 = p$.
Step 3: Suppose that $16 \nmid D$ and $x^2 + Dy^2 = 16p$. Then we may take $x = 4X$ to get $2X^2 + D'y^2 = 2p$. Since D' is odd, we may take $y = 2Y$ to get $X^2 + 2D'y^2 = p$. Since $p \equiv 1 \pmod 4$ and $2D' \equiv 2 \pmod 4$, y must be even. Putting $y = 2\mathcal{Y}$ we get $X^2 + 8D'\mathcal{Y}^2 = X^2 + D\mathcal{Y}^2 = p$. Further, we cannot have $x^2 + Dy^2 = 32p$, since $\mathrm{ord}_2(x^2 + 8D'y^2)$ is either even or equal to 3 and $\mathrm{ord}_2(32p) = 5$.
Step 5: Suppose that $16 \mid D$. Then reducing modulo 16 shows $k \not\equiv 8 \pmod{16}$.
Step 6: As usual, we need not consider any values of k which are divisible by any odd anisotropic primes, and we may make use of Lemma 32 to eliminate certain values of k. Again, we are left with short lists to eliminate by more explicit analysis.
D = 8: There are no further values of k to consider.
D = 16: There are no further values of k to consider.
D = 40: We are left to consider $k = 8, 20$. If $k = 8$, then take $x = 4X$ to get $2X^2 + 5y^2 = p$, and reduce modulo 5 to get a contradiction. If $k = 20$, take $x = 5X$ to get $5X^2 + 8y^2 = 4p$, and reduce modulo 5 to get a contradiction.
D = 48: We are left to consider $k = 12$. We may take $x = 6X$ to get $3X^2 + 4y^2 = p$ and then reduce modulo 4 to get a contradiction.
D = 72: We are left to consider $k = 8, 9, 12$. If $k = 8$, take $x = 4X$ to get $2X^2 + 9y^2 = p$, and reduce modulo 3 to get a contradiction. If $k = 9$, take $x = 3X$ to get $X^2 + 8y^2 = p$. We may take $y = 3Y$, so $X^2 + 72Y^2 = p$. If $k = 12$, take $x = 6X$ to get $3X^2 + 6y^2 = 2p$, and reduce modulo 3 to get a contradiction.
D = 88: We are left to consider $k = 8$. We may take $x = 4X$ to get $2X^2 + 11y^2 = p$, and reduce modulo 11 to get a contradiction.
D = 120: We are left to consider $k = 8$. We may take $x = 4X$ to get $2X^2 + 15y^2 = p$ and reduce modulo 3 to get a contradiction.
D = 168: We are left to consider $k = 8$. We may take $x = 4X$ to get $2X^2 + 21y^2 = p$ and reduce modulo 3 to get a contradiction. If $k = 16$ we may take $x = 4X$ to get $2X^2 + 21y^2 = 2p$ and then $y = 2Y$ to get $X^2 + 42Y^2 = p$. Reducing modulo 4 shows that Y is even, so we may put $Y = 2\mathcal{Y}$ and get $X^2 + 168\mathcal{Y}^2 = p$.
D = 232: We are left to consider $k = 8, 16$. If $k = 8$ then we may take $x = 4X$ to get $2X^2 + 29y^2 = p$ and reduce modulo 29 to get a contradiction.

D = 240: We are left to consider $k = 16$. We may take $x = 4X$ to get $X^2 + 15y^2 = p$. Reducing modulo 8 shows y is divisible by 4, so we may take $y = 4Y$ to get $X^2 + 240Y^2 = p$.
D = 280: We are left to consider $k = 8$. If $k = 8$ we may take $x = 4X$ to get $2X^2 + 35y^2 = p$ and reduce modulo 5 to get a contradiction.
D = 312: We are left to consider $k = 8, 12$. If $k = 8$ we may take $x = 4X$ to get $2X^2 + 39y^2 = p$ and reduce modulo 3 to get a contradiction. If $k = 12$ we may take $x = 6X$ to get $3X^2 + 26y^2 = p$ and reduce modulo 3 to get a contradiction.
D = 408: We are left to consider $k = 8$. We may take $x = 4X$ to get $2X^2+51y^2 = p$ and reduce modulo 3 to get a contradiction.
D = 520: We are left to consider $k = 8, 40$. If $k = 8$ we may take $x = 4X$ to get $2X^2 + 65y^2 = p$ and reduce modulo 5 to get a contradiction. If $k = 40$ we may take $x = 20X$ to get $10X^2 + 13y^2 = p$ and reduce modulo 5 to get a contradiction.
D = 760: We are left to consider $k = 8, 20$. If $k = 8$ we may take $x = 4X$ to get $2X^2 + 95y^2 = p$ and reduce modulo 5 to get a contradiction. If $k = 20$ we may take $x = 10X$ to get $5X^2 + 38y^2 = p$ and reduce modulo 5 to get a contradiction.
D = 840: We are left to consider $k = 8$. We may take $x = 4X$ to get $2X^2+105y^2 = p$ and reduce modulo 5 to get a contradiction.
D = 1320: We are left to consider $k = 8, 60, 64$. If $k = 8$ we may take $x = 4X$ to get $2X^2 + 165y^2 = p$ and reduce modulo 5 to get a contradiction. If $k = 60$ we may take $x = 30X$ to get $15X^2+22y^2 = p$ and reduce modulo 5 to get a contradiction. If $k = 64$ we may take $x = 2^2X$ to get $2X^2 + 165y^2 = 2^3p$. Next we may take $y = 2Y$ to get $X^2 + 330Y^2 = 2^2p$. Next we may take $X = 2\mathcal{X}$ to get $2\mathcal{X}^2 + 165Y^2 = 2p$. Next we may take $Y = 2\mathcal{Y}$ to get $\mathcal{X}^2 + 330\mathcal{Y}^2 = p$. Reducing modulo 4 shows $\mathcal{Y}$ is even and thus $\mathcal{Y} = \mathfrak{Y}$ and finally we get $\mathcal{X}^2 + 1320\mathfrak{Y}^2 = p$.
D = 1848: We are left to consider $k = 8, 64$. If $k = 8$ we may take $x = 4X$ to get $2X^2 + 231y^2 = p$ and reduce modulo 3 to get a contradiction. If $k = 64$ we may take $x = 2^2X$ to get $2X^2 + 231y^2 = 2^3p$. Next take $y = 2Y$ to get $X^2 + 462Y^2 = 2^2p$. Next take $X = 2\mathcal{X}$ to get $2\mathcal{X}^2 + 231Y^2 = 2p$. Next take $Y = 2\mathcal{Y}$ to get $\mathcal{X}^2 + 462\mathcal{Y}^2 = p$. Reducing modulo 4 shows $\mathcal{Y}$ is even and thus $\mathcal{Y} = \mathfrak{Y}$ and finally we get $\mathcal{X}^2 + 1848\mathfrak{Y}^2 = p$.

This completes the proof of the Representation Theorem.

6. Some representations of squarefree integers

6.1. **A squarefree representation theorem.**

For some idoneal values of D, we can go beyond Theorem 29 and find all squarefree values of n prime to $2D$ which are represented by $x^2 + Dy^2$. The idea is to apply Theorem 9 to *all* the positive definite diagonal forms of discriminant $-4D$ and exploit the multiplication identities of Proposition 5.

Theorem 33. *Let n be a squarefree positive integer prime to 3. Then:*
a) n is of the form $q_1 = x^2 + 6y^2$ iff -6 is a square modulo n and $n \equiv 1 \pmod 3$.
b) n is of the form $q_2 = 2x^2 + 3y^2$ iff -6 is a square modulo n and $n \equiv -1 \pmod 3$.

Proof. Step 0: In both cases, the given conditions are easily seen to be necessary: that -6 needs to be a square modulo n is a consequence of Proposition 4, and the other conditions come from reducing modulo 3.

Step 1: By Theorem 27, we know that if n is *prime* and satisfies $(\frac{-6}{n}) = 1$ and $n \equiv 1 \pmod 3$, then n is of the form $x^2 + 6y^2$. In the same way, we now establish the analogous result for primes represented by $q_2(x,y)$. Indeed, since $(\frac{-6}{p}) = 1$, there exist $x, y, k \in \mathbb{Z}$, with $1 \leq k \leq 4$, such that $2x^2 + 3y^2 = kn$. Assume first that $\gcd(k,3) = 1$. Then reduction modulo 3 shows $k \equiv 1 \pmod 3$, so $k = 1$ or $k = 4$. If $2x^2 + 3y^2 = 4n$, then by Lemma 31, both x and y are even, so n is of the form q_2. Finally, if $2x^2 + 3y^2 = 3n$, then we may substitute $x = 3X$ to get $6X^2 + y^2 = n$, again a contradiction.
Step 2: Let $n = p_1 \cdots p_r q_1 \cdots q_s$ be a product of distinct primes in which each $p_i \equiv 1 \pmod 3$ and each $q_j \equiv -1 \pmod 3$. The desired conclusion is equivalent to the fact that n is of the form $q_1(x,y)$ if s is even and of the form $q_2(x,y)$ if s is odd. But indeed, the multiplicative identities of Proposition 5 show that if n_1 and n_2 are either both of the form q_1 or both of the form q_2, then $n_1 n_2$ is of the form q_1, whereas if n_1 is of the form q_1 and n_2 is of the form q_2, then $n_1 n_2$ is of the form q_2. The result follows. □

Remark 6.1: A more elegant paraphrase of the last part of the argument is: the mapping χ_3 which takes an integer n prime to 3 to its reduction modulo 3 is a quadratic Dirichlet character on $\mathbb{Z}$. By Step 1, and the multiplicative identity, every squarefree integer prime to 3 is represented by exactly one of q_1 and q_2, and the ones which are represented by q_1 are precisely those in the kernel of χ_3.

More generally:

Theorem 34. *Let $D = 2\ell_1 \cdots \ell_r$ be one of the 12 numbers*

$$6, 10, 22, 30, 42, 70, 102, 130, 190, 210, 330, 462.$$

Then Thue-Vinogradov will show a squarefree positive integer n prime to $\frac{D}{2}$ is of the form $x^2 + Dy^2$ iff $-D$ is a square modulo n and $(\frac{n}{\ell_i}) = 1$ for all $1 \leq i \leq r$.

The proof of Theorem 34 proceeds along the lines of Theorem 33, except that when $r > 1$ we need an analogue of Proposition 5 giving an identity for the product of two distinct nonprincipal diagonal forms of discriminant D.

For $C \mid D$, put $q_C = Cx^2 + \frac{D}{C}y^2$. Now we have the following result.

Proposition 35. *Let D be a squarefree positive integer, and let $A, B \in \mathbb{Z}^+$ be divisors of D. Moreover, put $d = \gcd(A,B)$ and $a = \frac{A}{d}$, $b = \frac{B}{d}$.*
a) For any integers x_1, x_2, y_1, y_2, we have

$$\left(Ax_1^2 + \frac{D}{A}y_1^2\right)\left(Bx_2^2 + \frac{D}{B}y_2^2\right) = ab\left(dx_1x_2 - \frac{D}{dab}y_1y_2\right)^2 + \frac{D}{ab}\left(ax_1y_2 + bx_2y_1\right)^2.$$

b) Thus if we have an integer n of the form q_A and an integer n' of the form q_B, the product nn' is of the form $q_{\frac{AB}{\gcd A, B^2}}$.

Proof. We have a polynomial identity

$$\left(Ax_1^2 + \frac{D}{A}y_1^2\right)\left(Bx_2^2 + \frac{D}{B}y_2^2\right) = AB\left(x_1x_2 - \frac{D}{AB}y_1y_2\right)^2 + \frac{D}{AB}\left(Ax_1y_2 + Bx_2y_1\right)^2.$$

Substituting $A = da$, $B = db$ gives us part a). As for part b), it is enough to note that since D is squarefree, so are A and B, hence $\gcd(a,d) = \gcd(b,d) = \gcd(a,b) = 1$ are pairwise coprime divisors of D, so $\frac{D}{dab}$ and $\frac{D}{ab}$ are integers. □

The proof of Theorem 34 using Thue-Vinogradov is quite similar to that of Theorem 30. However, we are concerned that the reader may not wish to see further explicit calculations along the lines of §5.4 – 5.8, so to change things up a bit we will give a *non-elementary proof* of Theorem 34. Specifically, we will use some classical genus theory and facts about idoneal numbers to *guarantee* that the Thue-Vinogradov method will succeed without looking explicitly at cases. This line of reasoning has the following curious benefit: in the (unlikely, but not provably false given current technology) event that there is a squarefree idoneal number $D_{\text{big}} \equiv 2 \pmod 4$ with $D_{\text{big}} > 462$, then can be sure that the Thue-Vinogradov method will succeed in determining which squarefree numbers are of the form $x^2 + D_{\text{big}}y^2$!

6.2. **Further background on quadratic forms.**

We will need to assume some background in quadratic forms: namely Minkowski reduction, Gauss Composition and elementary genus theory. A good reference for all of these is [C, Ch. 1]. In particular we will make use of:

Theorem 36. *(*[C, Lemma 2.5]*) Let $\Delta \equiv 0, 1 \pmod 4$ be a negative integer. Let n be an odd integer relatively prime to Δ. Then TFAE:*
(i) Δ is a square modulo n.
(ii) n is primitively represented by some primitive, positive definite binary quadratic form $q(x, y)$ of discriminant Δ.

Theorem 37. *(*[C, Thm. 2.8]*) Let q be a primitive, positive definite binary quadratic form of discriminant Δ.*
a) There exists a unique primitive positive definite binary quadratic form $q'(x, y) = ax^2 + bxy + cy^2$ of discriminant Δ such that:
(i) q' is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to q,
(ii) $|b| \leq a \leq c$,
(iii) if $|b| = a$ or $a = c$ then $b \geq 0$,
(iv) $a \leq \frac{|\Delta|}{3}$.

A form q' satisfying (i) through (iv) is called **Minkowski reduced**. Note that the principal forms q_Δ are Minkowski reduced. More generally, a primitive diagonal form $Ax^2 + By^2$ is Minkowski-reduced iff $A < B$ (or $A = B = 1$).

6.3. **The proof of Theorem 34.**

Suppose that $D = 2\ell_1 \cdots \ell_r$ is a squarefree even idoneal number.

For each pair of positive integers (a, c) with $a < c$ and $ac = D$, let $q_a = ax^2 + cy^2$. Then each $q_{D,a}$ is a primitive, positive definite Minkowski-reduced form of discriminant $-4D$. This gives 2^r pairwise inequivalent forms of discriminant $-4D$. By [C, Prop. 3.11], the number of genera of discriminant $-4D$ is precisely 2^r. By our assumption that D is idoneal, each genus has a unique class, and therefore $h(-4D) = 2^r$ and the $q_{D,a}$'s represent all the classes of forms of discriminant $-4D$. Therefore, by Theorem 36, if n is squarefree and prime to D, then $-4D$ is a square modulo n iff n is represented by some form $q_{D,a}$, and if so, it is represented by *exactly one* such form.

Step 1: For each odd prime ℓ dividing D, consider the quadratic character $\chi_\ell : n \mapsto$

$(\frac{n}{\ell})$. If $q_a = ax^2+by^2 = n$, then – as we have seen many times! – reduction modulo ℓ gives us a quadratic condition on n. Namely, if $\ell \mid a$, then we get $(\frac{n}{\ell}) = (\frac{b}{\ell})$, whereas if $\ell \mid b$ we get $(\frac{n}{\ell}) = (\frac{a}{\ell})$. We call these the **generic characters** and compile them into a single map $\Theta : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}^r,\ n \mapsto (\chi_1(n), \ldots, \chi_r(n))$. Similarly, for each reduced representative q_a we may define $\Theta(q_a) \in \{\pm 1\}^r$. Then the fundamental fact is that for a positive squarefree integer n prime to D such that $-4D$ is a square modulo n, n is represented by some form in the genus of q_a iff $\Theta(n) = \Theta(q_a)$.

In the case of an idoneal $D \equiv 2 \pmod 4$, this recovers all the results that we have proven by elementary methods! However, our goal here is to use this genus theory to guarantee that the method of Thue-Vinogradov will succeed. We need a classical fact about idoneal numbers.

Proposition 38. *(*[Ka09, Prop. 25]*) If D is an idoneal number, then for all odd primes $\ell < \sqrt{D}$ we have $(\frac{-D}{\ell}) \neq 1$.*

We now begin the proof of Theorem 34. More precisely, we will show that the method of Thue-Vinogradov recovers the above conclusion: namely, that a squarefree n prime to D and such that $-4D$ is a square mod n is represented precisely by the form q_a such that $\Theta(q_a) = \Theta(n)$.

Step 1: Let p be a prime number which is prime to D, and let a be such that $\Theta(q_a) = \Theta(p)$. (Thus *we know* that q_a represents p, but the goal is to show that we can deduce this elementarily from Thue-Vinogradov.) Applying Thue-Vinogradov to q_a and p, we get that there exist k, x, y such that $ax^2+by^2 = kp$ with $1 \leq k < a+b$. We may in fact assume that $k < D$.
Suppose first that $k = \ell$ is an odd prime which is prime to D. If $(\frac{-4D}{\ell}) = -1$, then $ax^2 + by^2 = \ell p$ implies that $\mathrm{ord}_\ell(\ell p) \geq 2$, i.e., that $\ell = p$, a contradiction since $\ell < D < p$. Next suppose $(\frac{-4D}{\ell}) = 1$, so that ℓ is represented by some form of discriminant $-4D$. But the only primes less than $a + b$ which are represented by $q_a = ax^2 + by^2$ are a and or b (if either of these happens to be prime), neither of which is prime to D. So q_a does not represent ℓ, and by idoneality ℓ is then represented by a quadratic form $q_{a'}$ in a different genus. By the identity of Proposition 35a), ℓp is then represented by the product genus $q_{a''} = q_a q_{a'}$. If $q_{a''} = q_a$, then q' lies in the principal genus, which is a contradiction since $x^2 + Dy^2$ does not represent $\ell < a + b < D$. Therefore ℓp is *not* represented by q_a, contradiction.

Next suppose that $k = \ell$ is prime (possibly 2) which divides D. If $\ell \mid a$, then the equation $ax^2 + by^2 = \ell p$ leads to $\frac{a}{\ell}x^2 + b\ell Y^2 = p$, giving a representation of p by the genus $q_{\frac{a}{\ell}}$, a contradiction since we know that p is already represented by q_a. If $\ell \mid b$, then we similarly get $q' = a\ell X^2 + \frac{b}{\ell}y^2 = a'x^2 + b'y^2 = p$. A little thought shows that neither of a', b' is equal to either of a, b, so q' is again in a different genus from q_a but still represents p, contradiction.

If k is divisible by 4, then by Lemma 31 we reduce to the case of $\frac{k}{4}$ instead. The remaining case is that k is odd and composite and therefore divisible by an odd prime $\ell < \sqrt{D}$. But by Proposition 38 we then have that ℓ is an anisotropic prime for $-4D$ and hence by Theorem 7 we reduce to the case $\frac{k}{\ell^2}$. Thus Thue-Vinogradov will succeed in showing that p is represented by q_a.

Step 2: Suppose $n = p_1 \cdots p_s$ is squarefree, prime to D and such that $-4D$ is a square mod n. This implies that $-4D$ is a square mod p_j for each p_j, so that by Step 1 each p_j is represented by the unique form q_{a_j} with $\Theta(q_{a_j}) = \Theta(p_j)$. Using Proposition 35, we see that n is represented by the quadratic form q_a corresponding to the product genus $\prod_{j=1}^{s} q_{a_j}$ – which, as we have seen, is simply q_a where a is the squarefree part of $a_1 \cdots a_s$. In particular, n is represented by the principal form q_1 iff $a_1 \cdots a_s$ is a perfect square iff for all $1 \leq i \leq r$, the generic character $\chi_i(n) = 1$. Moreover, genus theory guarantees that the genus characters will give congruence obstructions to any other squarefree n prime to D being represented by the principal form. Thus our elementary methods will suffice to determine precisely the set of squarefree n prime to D represented by q_1 (or any other diagonal form q_a). This completes the proof of Theorem 34.

References

[AZ] M. Aigner and G.M. Ziegler, *Proofs from The Book*. Including illustrations by Karl H. Hofmann. Third edition. Springer-Verlag, Berlin, 2004.

[Au13] L. Aubry, Un théorème d'arithmétique, Mathesis (4), 1913.

[BrRe51] A. Brauer and R.L. Reynolds, *On a theorem of Aubry-Thue*. Canadian J. Math. 3 (1951), 367–374.

[C] 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.

[Ha10] T.R. Hagedorn, *Primes of the form x^2+ny^2 and the geometry of (convenient) numbers*. Preprint, 2010.

[HW] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*.

[IR] K. Ireland and M. Rosen, *A classical introduction to modern number theory*. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[Ka09] E. Kani, *Idoneal Numbers and some Generalizations*, preprint 2009, available at `http://www.mast.queensu.ca/~kani/papers/idoneal.pdf`

[L] W.J. LeVeque, *Fundamentals of number theory*. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977.

[Mo66] L.J. Mordell, *Solvability of the equation $ax^2 + by^2 = p$*. J. London Math. Soc. 41 (1966), 517-522.

[N] T. Nagell, *Introduction to Number Theory*. John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm, 1951.

[O] O. Ore, *Number theory and its history*. Reprint of the 1948 original. With a supplement. Dover Publications, Inc., New York, 1988.

[Sch] A. Scholz, *Einfuhrung in die Zahlentheorie*, Berlin, 1939.

[Sho] V. Shoup, *A computational introduction to number theory and algebra*. Second edition. Cambridge University Press, Cambridge, 2009.

[Th02] A. Thue, *Et par antydninger ti1 en taltheoretisk metode*, Kra. Vidensk. Selsk. Forh. 7 (1902), 57-75.

[Vi27] I.M. Vinogradov, *On a general theorem concerning the distribution of the residues and non-residues of powers*. Trans. Amer. Math. Soc. 29 (1927), 209–17.

Department of Mathematics, University of Georgia, Athens, GA 30602, USA
E-mail address: `plclark@gmail.com`