Quadratic Forms

Yifeng Huang

September 22, 2017

1 Real Quadratic Forms

A **(real) quadratic form** (in two variables) is a polynomial $f(x, y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{R}$. In this lecture, we shall always think of x, y as integers, but a, b, c need or need not be. The **discriminant** is defined as $D = b^2 - 4ac$. A number m is said to be **represented** by the quadratic form $f(x, y)$ if $f(x, y) = m$ for some integers x, y. If x, y can furthermore be chosen to be coprime, then m is said to be **properly represented** by f.

Given a quadratic form $f(x, y)$, we can change variable by matrix $U = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ and consider

$$g(x, y) = f(U(x, y)) = f(\alpha x + \beta y, \gamma x + \delta y)$$

If $U(x, y)$ can run over all $\mathbb{Z} \times \mathbb{Z}$, i.e. $U \in \mathrm{GL}(2, \mathbb{Z})$, then f, g represent the same set of numbers, and we should view them as more or less the same. We say g is f transformed by U. Two quadratic forms are called **(Legendre) equivalent** if they are related by $U \in \mathrm{GL}(2, \mathbb{Z})$. They are called **(Gauss) properly equivalent** if they are related by $U \in \mathrm{SL}(2, \mathbb{Z})$. Proper equivalence will prove to be the "correct" notion later on.

The matrix of a quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $M = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$ and is related by

$$f(x, y) = v^T M v$$

where v is the column vector $[x\ y]^T$.

Given $U \in \mathrm{GL}_2(\mathbb{Z})$, we have

$$f(Uv) = v^T U^T M U v$$

so the matrix of the new quadratic form is $U^T M U$.

Note that the discriminant of a quadratic form is related to its matrix by

$$D = -4 \det(M)$$

Hence discriminant is invariant under equivalence.

If a, b, c are integer, the quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is called **integral** and if further $\gcd(a, b, c) = 1$ then f is called **primitive**. Note that integrality and primitivity are both invariant under equivalence: for primitivity, note that in general,

$$\mathbb{Z}\{a, b, c\} = \mathbb{Z}\{\text{numbers represented by } f\}$$

For a proof, clearly RHS is contained in LHS; also $a = f(1,0), c = f(0,1)$ are both represented, and so is $f(1,1) = a+b+c$, thus $b = (a+b+c) - a - c$ is generated by representable numbers.

We also note that the set of properly representable numbers is invariant under equivalence. The reason is $\gcd(x,y)$ is unchanged if we apply $U \in \mathrm{GL}_2(\mathbb{Z})$. For a quick proof, note that $\gcd(x,y)\mathbb{Z}$ is the image of the map $v^T = [x\ y] : \mathbb{Z}^2 \to \mathbb{Z}$, and

$$\mathrm{im}((Uv)^T) = \mathrm{im}(v^T U^T) = \mathrm{im}(v^T)$$

as U^T is invertible over $\mathbb{Z}$.

In summary, all the bold-faced concepts mentioned above are invariant under equivalence.

Example 1.1. Let $f(x,y) = ax^2 + bxy + cy^2$, then the following form is properly equivalent to f:

$$f(y,-x) = cx^2 - bxy + ay^2$$

The form is equivalent to f:

$$g(x,y) = f(x,-y) = ax^2 - bxy + cy^2$$

We call g the **opposite** of f. Then when is g properly equivalent to f? It turns out that $3x^2+2xy+3y^2$ and $x^2+xy+3y^2$ are properly equivalent to their opposite, but $2x^2+xy+3y^2$ is not. This question will be addressed in the section about reduction.

2 Positive Definite Forms and Lattices

A quadratic form is **positive definite** if the discriminant D is negative. This is equivalent to saying $f(x,y) > 0$ for any $(x,y) \in \mathbb{R}^2 - 0$. From now on, all quadratic forms are assumed to be positive definite.

Given a lattice Λ (which always means full lattice here) in $\mathbb{R}^2$ with an ordered basis $\{v,w\}$, we define the **norm form** associated to $\{v,w\}$ to be

$$f(x,y) = N(xv+yw),$$

where $N(\cdot) = ||\cdot||^2$ is the Euclidean norm squared. Note that the numbers represented by f are precisely $N(\lambda)$ of lattice points $\lambda \in \Lambda$.

More explicitly, the norm form is given by $f(x,y) = ax^2+bxy+cy^2$ where

$$a = \langle v,v\rangle, b = 2\langle v,w\rangle, c = \langle w,w\rangle$$

and the matrix of f is $[v\ w][v\ w]^T$.

If we change the basis of lattice by a matrix $U \in \mathrm{GL}_2(\mathbb{Z})$, the norm form will be transformed by U^T. If we insist that the ordered basis $\{v,w\}$ must be **oriented**, that is, $\det[v\ w] > 0$, then any change of basis matrix is in $\mathrm{SL}_2(\mathbb{Z})$, so the lattice alone determines the proper equivalence class of norm form.

Define the **covolume** of a lattice Λ to be the area of its fundamental domain, which is computed by $\det[v\ w]$ for an oriented basis $\{v,w\}$, and define its **discriminant** to be $D = -4\,\mathrm{covol}(\Lambda)^2$. This matches the notion of discriminant of number fields.

Theorem 2.1. *There is a natural one-to-one correspondence:*

$$\left\{\text{Lattices in } \mathbb{R}^2 = \mathbb{C}\right\}/\mathrm{SO}(2) \cong \left\{\text{Positive definite real quadratic forms}\right\}/\mathrm{SL}_2(\mathbb{Z})$$

$$\Lambda \mapsto \text{Norm form of } \Lambda$$

$$\frac{1}{\sqrt{a}}\mathbb{Z}\{a, \frac{b+\sqrt{D}}{2}\} \hookleftarrow f(x,y) = ax^2 + bxy + cy^2$$

In particular, lattices of discriminant $D < 0$ up to rotation correspond to real quadratic forms of discriminant D up to proper equivalence.

Proof. Use $a = \langle v, v\rangle, b = 2\langle v, w\rangle, c = \langle w, w\rangle$ to constuct a lattice with given norm form.

For discriminant, note $D(f) = -4\det[v\ w]^2 = -4\,\mathrm{covol}(\Lambda)^2 = D_\Lambda$. □

3 Reduction Theory

The goal is to give a set-theoretic description of the set of proper equivalence classes positive definite real quadratic forms. We shall give a unique representative in each class, called the "reduced form".

Proposition 3.1. *Every positive definite real quadratic form is properly equivalent to a form $f(x,y) = ax^2 + bxy + cy^2$ such that $|b| \le a \le c$, and in this case $a, |b|, c$ are uniquely determined.*

Moreover, if $b \neq 0$, then f is properly equivalent to its opposite iff $a = |b|$ or $a = c$.

Proof. Given a lattice Λ associated to the proper equivalence class of the real quadratic form, consider the basis

$$v = \text{shortest nonzero vector in } \Lambda$$

$$w = \text{shortest vector in } \Lambda - \mathbb{Z}v \text{ such that } \det[v\ w] > 0$$

Then the projection of w onto v cannot exceed $\pm\frac{v}{2}$, so $|b| = 2\langle v, w\rangle \le a = \langle v, v\rangle \le c = \langle w, w\rangle$

Moreover, a, c can be completely recovered from the length of vectors of Λ, and then $|b|$ is determined as well since $b^2 - 4ac = D$ is known.

It remains to study when f is properly equivalent to its opposite. If $b = a$, then the projection of w onto v is $\frac{v}{2}$. Then $w - v$ has the same length as w, and if we replace w by $w - v$, b will be negated.

If $a = c$, then $||v|| = ||w||$, and we can start from $v' = w$ and $w' = -v$ (to kepp the orientation), so b is negated.

In all other case, it is easy to see the construction of v, w is unique except we can negate v, w at the same time, but in this case the norm form is unchanged. □

Definition 3.2. A positive definite real quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is called **reduced** if $|b| \le a \le c$. If $|b| = a$ or $a = c$, b is in addition required to be nonnegative.

4 Relationship with Ideal Class Group

The main result of this section is a one-to-one correspondence between the set of all integral primitive quadratic forms of a fixed discriminant $D < 0$ and the ideal class group of an order of imaginary quadratic field. The idea is, given a (suitable) ideal $\mathfrak{a}$ of such an order $\mathcal{O}$, viewed as a lattice, we take its norm form and normalize it to a primitive one.

Definition 4.1. Let Λ be a lattice in $\mathbb{C} = \mathbb{R}^2$. Define the multiplication ring of Λ to be

$$\mathcal{O}_\Lambda = \{z \in \mathbb{C} : z\Lambda \subseteq \Lambda\}$$

If $\mathcal{O}_\Lambda \neq \mathbb{Z}$, then we say Λ to have **complex multiplication** and $\mathcal{O}_\Lambda$ is called the **CM ring** of Λ.

Now let Λ be a lattice with CM. Clearly $\mathcal{O}_\Lambda$ is unchanged if Λ is scaled by some $c \in \mathbb{C}^\times$. So assume $\Lambda = \mathbb{Z}\{1, \tau\}$. Then for all $z \in \mathcal{O}_\Lambda$, we have $z \cdot 1 \in \Lambda$, so $\mathcal{O}_\Lambda \subseteq \Lambda$, thus $\mathcal{O}_\Lambda$ is a free abelian group of rank 2. Hence $K := \mathrm{Frac}(\mathcal{O}_\Lambda)$ is an imaginary quadratic number field and $\mathcal{O}_\Lambda$ is an order of it. In conclusion, the CM ring of a CM lattice must be an order of a quadratic number field.

We also observe that we can make $\Lambda \subseteq K$ after scaling. Again assume $\Lambda = \mathbb{Z}\{1, \tau\}$, and $a \in K - \mathbb{Z}$ satisfies $a\Lambda \in \Lambda$. Then

$$a\tau = b + c\tau \text{ for some } b, c \in \mathbb{Z}$$

Hence $\tau = \frac{b}{a-c} \in K$ since $a \neq c$.

Now we fix $K = \mathbb{Q}(\sqrt{-d})$ and an order $\mathcal{O}$ and study the lattices that have CM ring exactly $\mathcal{O}$. It suffices to study the ones in K, so they are fractional ideals of $\mathcal{O}$. Following Cox's terminology, say a fractional ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is **proper** if its CM ring $\{z \in K : z\mathfrak{a} \subseteq \mathfrak{a}\}$ is no larger than $\mathcal{O}$. Warning: this has nothing to do with "ideals that are proper subsets".

Theorem 4.2. *Let D be the discriminant of the order $\mathcal{O}$ as a lattice. Then there is a one-to-one correspondence*

$$\{\textit{Proper fractional ideals in } K\}/K^\times \cong \left\{ \begin{array}{c} \textit{Positive definite primitive integral} \\ \textit{quadratic forms of discriminant } D \end{array} \right\} /\mathrm{SL}_2(\mathbb{Z})$$

$$\mathfrak{a} \mapsto \textit{Norm form of } \mathfrak{a} \textit{ then normalized}$$

$$\mathbb{Z}\{a, \frac{b+\sqrt{D}}{2}\} \hookleftarrow f(x,y) = ax^2 + bxy + cy^2$$

The key of the proof is the following computation of CM ring:

Theorem 4.3. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic number field, and Λ is a lattice in K. Then its norm form has rational coefficient. Let $f(x,y) = ax^2+bxy+cy^2$ be the unique (up to proper equivalence) positive definite primitive integral quadratic form that is proportional to the norm form of Λ. Then the CM ring $\mathcal{O}_\Lambda$ of Λ is the order of discriminant D, where D is the discriminant of $f(x,y)$.*

Remark. Note that an order of imaginary quadratic field is determined by its discriminant. This is because the only subgroup of $\mathbb{Z}^2$ of index f that contains $\mathbb{Z}\times 0$ is $\mathbb{Z}\times f\mathbb{Z}$. In specific, if $\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\omega$ is the maximal order, and $\mathcal{O}$ is an order of conductor $[\mathcal{O}_K : \mathcal{O}] = f$, then $\mathcal{O} = \mathbb{Z}+\mathbb{Z}f\omega$. Alternatively, we have a formula

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{D+\sqrt{D}}{2}$$

where $\mathcal{O}$ is the order of discriminant D.

Proof of Theorem. If we multiply Λ by $r \in K^\times$, the norm form will be multiplied by $N(r)$, a rational number, so $f(x,y)$ is unchanged. We may assume WLOG that $\Lambda = \mathbb{Z}\{1, \tau\}$, $Im(\tau) > 0$. Then $\mathcal{O}_\Lambda$ is a sublattice of Λ that contains 1, so $\mathcal{O}_\Lambda$ must be of the form $\mathbb{Z}\{1, n\tau\}$, where n is the smallest positive integer such that $n\tau \in \mathcal{O}_\Lambda$.

Now $n\tau\Lambda \subseteq \Lambda$ iff $n\tau^2 \in \Lambda$. Observe that:

Lemma 4.4. *Let $\Lambda = \mathbb{Z}\{1, \tau\}$ with $Im(\tau) > 0$ and $f(x, y) = ax^2 + bxy + cy^2$ be any quadratic form proportional to the norm form of Λ on basis $\{1, \tau\}$. Then τ satisfies the equation $ax^2 - bx + c = f(x, -1) = 0$*

Proof. The norm form must be $x^2 + \frac{b}{a}xy + \frac{c}{a}y^2$, so

$$\frac{b}{a} = 2\langle 1, \tau\rangle = 2Re(\tau) = \tau + \overline{\tau}$$

$$\frac{c}{a} = \langle \tau, \tau\rangle = \tau + \overline{\tau}$$

Thus $\tau, \overline{\tau}$ are two solutions of $x^2 - \frac{b}{a}x + \frac{c}{a} = 0$, i.e. $ax^2 - bx + c = 0$. □

Continue to proof. We then have $n\tau^2 = \frac{n}{a}(b\tau - c)$, so $n\tau^2 \in \Lambda$ iff $\frac{nb}{a}, \frac{nc}{a} \in \mathbb{Z}$. This is equivalent to $a|n \gcd(b, c)$. But a is coprime to $\gcd(b, c)$ by primitivity, so this is again equivalent to $a|n$. Hence a is the smallest choice for n, and $\mathcal{O}_\Lambda = \mathbb{Z}\{1, a\tau\}$.

It remains to calculate the discriminant of $\mathcal{O}_\Lambda$. The covolume of $\mathcal{O}_\Lambda$ is $a\, Im(\tau) = \sqrt{-D}/2$ (by applying quadratic formula on $a\tau^2 - b\tau + c = 0$), so

$$D_{\mathcal{O}_\Lambda} = -4 \operatorname{covol}(\mathcal{O}_\Lambda)^2 = -4(-D)/4 = D$$

□

Proof of Theorem 4.2. If we mod out both sides of the correspondence in Theorem 2.1 by $\mathbb{R}_+$ scaling, then both sides of Theorem 4.2 are subsets of the corresponding object. So it suffices to check that a fractional ideal $\mathfrak{a}$ of K is proper iff its associated primitive form $f(x, y)$ has discriminant D. But this is now obvious since $\mathfrak{a}$ is proper iff the CM ring of $\mathfrak{a}$ is $\mathcal{O}$ iff $D_{\mathcal{O}_\mathfrak{a}} = D$, but $D_{\mathcal{O}_\mathfrak{a}} = D_{f(x,y)}$ by Theorem 4.3. □

It is a surprising fact that for imaginary quadratic fields, proper ideals are precisely the invertible ones, so that proper ideals here are closed under multiplication.

Lemma 4.5. *A fractional ideal $\mathfrak{a}$ of an order $\mathcal{O}$ of an imaginary quadratic field K is proper if and only if $\mathfrak{a}$ is invertible, i.e. there is fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$.*

Proof. "if" (true for any field): we want to show that for $z \in K$, $z\mathfrak{a} \subseteq \mathfrak{a}$ implies $z \in \mathcal{O}$. Indeed let $\mathfrak{b}$ be an inverse of $\mathfrak{a}$, then $z\mathfrak{ab} \subseteq \mathfrak{ab}$, i.e. $z\mathcal{O} \subseteq \mathcal{O}$. But $1 \in \mathcal{O}$, so $z \in \mathcal{O}$.

"only if" (only true for imaginary quadratic field): let $\overline{\mathfrak{a}}$ be the complex conjugate of $\mathfrak{a}$, and claim that $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$, where $N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$ is the ideal norm of $\mathfrak{a}$ in $\mathcal{O}$. If this is true, $\overline{\mathfrak{a}}/N(\mathfrak{a})$ provides an inverse of $\mathfrak{a}$.

If I replace $\mathfrak{a}$ by $r\mathfrak{a}$, $r \in K^\times$, then both sides of the equality will be multiplied by $||r||^2$. So we may scale $\mathfrak{a}$ and assume $\mathfrak{a} = \mathbb{Z}\{1, \tau\}$. Being proper means the primitive form $f(x, y) = ax^2 + bxy + cy^2$ associated to $\mathfrak{a}$ has discriminant D. Recall $f(\tau, -1) = 0$. We have

$$\mathfrak{a}\overline{\mathfrak{a}} = \mathbb{Z}\{1, \tau, \overline{\tau}, \tau\overline{\tau}\} = \mathbb{Z}\{1, \tau, \frac{b}{a} - \tau, \frac{c}{a}\} = \mathbb{Z}\{1, \frac{b}{a}, \frac{c}{a}, \tau\}$$

Since $\gcd(a, b, c) = 1$, $\mathfrak{a}\overline{\mathfrak{a}} = \dfrac{1}{a}\mathbb{Z}\{1, a\tau\}$. By the proof of Theorem 4.3, we saw $\mathcal{O} = \mathcal{O}_\mathfrak{a} = \mathbb{Z}\{1, a\tau\}$. So it remains to show $N(\mathfrak{a}) = \dfrac{1}{a}$. But this is easy by looking at the covolumes of $\mathcal{O}$ and $\mathfrak{a}$. □

Corollary 4.6. *As an upshot of the last claim, we see that the ideal norm is multiplicative on proper ideals, because $N(\mathfrak{a})\mathcal{O} = \mathfrak{a}\overline{\mathfrak{a}}$ and RHS is multiplicative in $\mathfrak{a}$.*

5 Composition of Primitive Quadratic Forms

Now in theorem 4.2, the LHS is the ideal class group of $\mathcal{O}$, denoted $\mathrm{Cl}(\mathcal{O})$. Via the bijection, we can push the group structure to RHS, and we shall call it the **form class group** $\mathrm{Cl}(D)$ of discriminant $D < 0$. The group operation is called **composition**, and I denote by symbol *. Note that for forms f and g, the composition $f * g$ is only determined up to proper equivalence.

As the main question, what is the group structure of $\mathrm{Cl}(D)$ explicitly? What does the composition look like and how to compute it?

The identity and inverse of the group is easy to compute:

Proposition 5.1. *The inverse of a form $f(x,y) = ax^2 + bxy + cy^2$ is its opposite $ax^2 - bxy + cy^2$. The identity element of $\mathrm{Cl}(D)$ is given by*

$$\begin{cases} x^2 + ny^2, & D = -4n \\ x^2 + xy + ny^2, & D = -4n+1 \end{cases}$$

The composition is much more complicated. I postpone any concrete example until I finish the general computation and draw some observation.

Let $D, K, \mathcal{O}$ be as before, and suppose primitive quadratic forms f, g are given by proper ideals $\mathfrak{a} = \mathbb{Z}\{a, b\}, \mathfrak{b} = \mathbb{Z}\{c, d\}$. The norm form of $\mathfrak{a}$ is $N(ax+by)$, and its discriminant is the discriminant $D_\mathfrak{a}$ of lattice $\mathfrak{a}$. It is proportional to $f(x,y)$, but the discriminant of f is D, so

$$f(x,y) = \sqrt{\frac{D}{D_\mathfrak{a}}} N(ax+by) = \frac{N(ax+by)}{N(\mathfrak{a})}$$

In particular, the set of numbers represented by f is precisely $\{\frac{N(\alpha)}{N(\mathfrak{a})} : \alpha \in \mathfrak{a}\}$.

Similarly,

$$g(z,w) = \frac{N(cz+dw)}{N(\mathfrak{b})}$$

Hence

$$f(x,y)g(z,w) = \frac{N((ax+by)(cz+dw))}{N(\mathfrak{ab})}$$

by multiplicativity of ideal norms.

Let $h = f * g$ be the composition of f and g, then it is the form associated to $\mathfrak{ab}$. Note that $(ax+by)(cz+dw) \in \mathfrak{ab}$, we see that

Proposition 5.2. *If an integer m is represented by $f(x,y)$ as above, and n is represented by $g(x,y)$, then mn is represented by $f * g$.*

To be more explicit, let e, f be an oriented basis for $\mathfrak{ab}$, then ac, ad, bc, bd are all of the form $\square e + \square f$ where all the $\square$'s are integers. Then

$$\begin{aligned} f(x,y)g(z,w) &= \frac{N(xzac + xwad + yzbc + ywbd)}{N(\mathfrak{ab})} \\ &= \frac{N(xz(\square e + \square f) + xw(\square e + \square f) + yz(\square e + \square f) + yw(\square e + \square f)}{N(\mathfrak{ab})} \\ &= \frac{N(e(\square xz + \square xw + \square yz + \square yw) + f(\square xz + \square xw + \square yz + \square yw)}{N(\mathfrak{ab})} \\ &= h(\square xz + \square xw + \square yz + \square yw, \square xz + \square xw + \square yz + \square yw) \end{aligned}$$

In other words,

Proposition 5.3. *Let h be a representative in the proper equivalence class of $f * g$. Then*

$$f(x,y)g(z,w) = h(B_1(x,y;z,w), B_2(x,y;z,w))$$

for some bilinear form $B_i(x,y;z,w) = a_{11}xz + a_{12}xw + a_{21}yz + a_{22}yw$ with integer coefficients.

This is exactly Legendre's idea of composition. But there is a flaw if we only use this formula to define composition: the forms h that satisfy this may lie in at worst four proper equivalence classes and two equivalent classes! From Gauss point of view, it is because this identity does not distinguish within equivalence class, so if f, g are not properly equivalent to their opposite, then the proper equivalence class of h could be $f * g, \overline{f} * g, f * \overline{g}$ or $\overline{f} * \overline{g}$.

6 Examples

1. Compute $\mathrm{Cl}(-14)$.
2. Work out $(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2$

7 Primes Represented by Quadratic Forms

Basic questions: what primes can be represented by $x^2 + ny^2$?

$n = 1$: $p = 2$ or $p \equiv 1 \mod 4$.

$n = 2$: $p = 2$ or $p \equiv 1, 3 \mod 8$.

$n = 3$: $p = 3$ or $p \equiv 1 \mod 3$.

All the above can be deduced from the following, since for $n = 1, 2, 3$, $x^2 + ny^2$ is the only reduced quadratic form of discriminant $-4n$.

Theorem 7.1. *Let $n > 0$ be an integer and p a prime not dividing n. Then p is represented by some primitive form of discrimant $-4n$ iff $(-n/p) = 1$.*

Proof. Some Fermat's descent. □

Similar for $n = 7$, $h(-4n) = 1$, so $p \neq 7$ is represented by $x^2 + 7y^2$ iff $(-7/p) = 1$ iff $p \equiv 1, 9, 11, 15, 23, 25 \mod 28$.

How about $n = 5$?

There are two reduced forms of discriminant -20: $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$.

We only have $p = x^2 + 5y^2$ or $2x^2 + 2xy + 3y^2$ iff $p \equiv 1, 3, 7, 9 \mod 20$. However we have a save: by working mod 20, we find that $x^2 + 5y^2 \equiv 1, 9 \mod 20$ while $2x^2 + 2xy + 3y^2 \equiv 3, 7 \mod 20$.

So we conclude that $p = x^2 + 5y^2$ iff $p = 5$ or $p \equiv 1, 9 \mod 20$.