

QUADRATIC RECIPROCITY, THUE'S LEMMA, AND PRIMES OF THE FORM $x^2 + ny^2$

Alikhan Serik

Abstract

In 1640, Pierre de Fermat posed the question: which primes can be expressed as sums of two squares, that is, in the form $x^2 + y^2$ for some nonnegative integers x and y ? He hypothesized that any prime number of the form $4k + 1$ can be written this way — a statement that was first proved by Euler in two letters to Goldbach (1747, 1749). This theorem revealed a link between prime numbers and quadratic forms, uncovering their deeper properties.

Later, mathematicians generalized Fermat's question, asking which primes can be represented as $x^2 + ny^2$, where n , x , and y are natural numbers. (Even Fermat did this for $n = 2$ and $n = 3$.) Naturally, this question turns out to be more complex, as the answer depends on the value of n . Establishing the conditions under which a prime can be represented in this form often requires methods from algebraic number theory.

In this work, we use Thue's lemma, quadratic reciprocity law, and some other well-known facts, to determine the conditions under which prime numbers can be expressed in the form $x^2 + ny^2$ for some values of n . Thue's lemma allows us finding integer solutions to certain congruences—which plays a key role in determining the representability of a prime in the desired form. The law of quadratic reciprocity helps identifying quadratic residues, which are useful when we explore the existence of integer solutions x, y of the equation $x^2 + ny^2 = p$ for given n , and various primes p .

We begin by presenting a proof of Thue's lemma, and then we review the basic results related to quadratic residues, and prove the quadratic reciprocity law. We apply these fundamental concepts to proving Fermat's theorem on representing primes as sums of two squares. Next, we analyze the cases when n is one of 2, 3, 4, 5, and 13, establishing the conditions for representing primes in the corresponding forms. Each case has its own criteria, showing how the possibility of writing primes in the form $x^2 + ny^2$ depends on n in ways that seem hardly to be related, and thus showing the complexity of the general problem. Our research contributes to the study of the representability of prime numbers in the mentioned form, demonstrating how classical tools help solve difficult problems in number theory.

Background information

Let us begin by proving the following (more or less) elementary and well-known theorems.

Fermat's Little Theorem. If p is a prime number and a is an integer not divisible by p , then the congruence

$$a^{p-1} \equiv 1 \pmod{p}$$

holds.

Proof. For an integer a that is not divisible by p consider the set of integers

$$S = \{a, 2a, \dots, (p-1)a\}.$$

Any two elements of S are distinct modulo p ; indeed, if there exist $i \neq j$ in the set $\{1, 2, \dots, p-1\}$ such that

$$ia \equiv ja \pmod{p},$$

then (because a is not divisible by p) it follows that $i \equiv j \pmod{p}$, which is not possible for distinct $i, j \in \{1, 2, \dots, p-1\}$.

Since S contains $p-1$ distinct elements (and all are nonzero modulo p), and there are $p-1$ nonzero residues modulo p , the elements of the set S taken modulo p form a permutation of the set $\{1, 2, \dots, p-1\}$, thus we have

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}.$$

Consequently we get

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Since $(p-1)!$ is not divisible by p (as p is a prime), we can divide both sides by $(p-1)!$, obtaining

$$a^{p-1} \equiv 1 \pmod{p},$$

as desired.

Thue's Lemma. Let $n > 1$ be a natural number, and let a be an integer. Then there exist natural numbers x and y not exceeding $\sqrt{n}$, not both equal to 0, and such that either

$$ay \equiv x \pmod{n} \quad \text{or} \quad ay \equiv -x \pmod{n}.$$

Proof. There are $(\lfloor \sqrt{n} \rfloor + 1)^2$ expressions of the form $ai - j$ with i and j running through the set $\{0, 1, \dots, \lfloor \sqrt{n} \rfloor\}$. However,

$$(\lfloor \sqrt{n} \rfloor + 1)^2 > n,$$

which means that the number of these expressions is greater than the number of all the residues modulo n , hence (by the pigeonhole principle) there exist numbers $i_1, j_1, i_2, j_2 \in \{0, 1, \dots, \lfloor \sqrt{n} \rfloor\}$ satisfying $(i_1, j_1) \neq (i_2, j_2)$ and

$$ai_1 - j_1 \equiv ai_2 - j_2 \pmod{n},$$

which yields

$$a|i_1 - i_2| \equiv |j_1 - j_2| \pmod{n} \quad \text{or} \quad a|i_1 - i_2| \equiv -|j_1 - j_2| \pmod{n}.$$

We conclude that $ay \equiv x \pmod{n}$ or $ay \equiv -x \pmod{n}$ for $y = |i_1 - i_2| \in \{0, 1, \dots, \lfloor \sqrt{n} \rfloor\}$ and $x = |j_1 - j_2| \in \{0, 1, \dots, \lfloor \sqrt{n} \rfloor\}$, which are natural numbers not both equal to 0 since the pairs (i_1, j_1) and (i_2, j_2) differ. Note that for such x and y we have anyway $a^2 y^2 \equiv x^2 \pmod{n}$.

We remind that an integer $a \in \{0, 1, \dots, p-1\}$ is a *quadratic residue* modulo some prime p if and only if the congruence $x^2 \equiv a \pmod{p}$ has solutions. Otherwise, a is a *quadratic non-residue* modulo p . For instance, 2 is a quadratic residue modulo 7, since $3^2 \equiv 2 \pmod{7}$, while 3 is not, because no integer x exists such that $x^2 \equiv 3 \pmod{7}$. (Actually, all the quadratic residues modulo 7 are 0, 1, 2, and 4.) By extension we can use the same terminology for any integer a . For example, 11 is a quadratic residue modulo 7 (as $11 \equiv 2^2 \pmod{7}$). One immediately sees that all integers are quadratic residues modulo 2, so we further consider that p is an odd prime.

Definition. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ for some $a \in \mathbb{Z}$ and an odd prime p as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1, & \text{if } a \text{ is not a quadratic residue modulo } p, \\ 0, & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

For example, we have

$$\left(\frac{3}{7}\right) = -1, \quad \left(\frac{-21}{7}\right) = 0, \quad \text{and} \quad \left(\frac{11}{7}\right) = 1.$$

Euler's Criterion. If p is an odd prime and a is relatively prime to p , then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Proof. Consider two cases: when a is a quadratic residue, and when it is not.

Case 1. Suppose that a is a quadratic residue modulo p .

By definition, there exists an integer x such that

$$a \equiv x^2 \pmod{p}.$$

Then we have

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p},$$

by Fermat's Little Theorem. So,

$$a^{\frac{p-1}{2}} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p},$$

since a is a quadratic residue.

Case 2. Assume now that a is not a quadratic residue modulo p . Fermat's Little Theorem implies that any integer a (which is relatively prime to p) verifies either $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Then (due to case 1) we infer that, for any a that is not a quadratic residue modulo p , we get

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Since in this case a is a quadratic non-residue, we have

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

thus the desired conclusion

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

follows in this second case, too, finishing the proof.

Note that it is well-known that the number of nonzero quadratic residues modulo p is $\frac{p-1}{2}$, and the same holds for non-residues. So, the congruence

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

has $\frac{p-1}{2}$ solutions in $\{1, 2, \dots, p-1\}$ (namely all the quadratic residues modulo p), and the congruence

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

has also $\frac{p-1}{2}$ solutions (the quadratic non-residues). Also note the following important consequences of Euler's criterion, whose proofs are left to the reader.

Corollary. For any odd prime p and any integers a and b , we have

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Corollary. We have

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

for any odd prime p . In other words, -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$ (and it is not for $p \equiv 3 \pmod{4}$).

Gauss's Lemma. Let p be an odd prime and let a be an integer relatively prime to p . For every $1 \leq j \leq \frac{p-1}{2}$ let r_j be the least positive remainder of ja modulo p . That is, we have

$$ja \equiv r_j \pmod{p} \text{ and } r_j \in \{1, 2, \dots, p-1\} \text{ for all } 1 \leq j \leq \frac{p-1}{2}.$$

Consider that u of these remainders r_j are lesser than $\frac{p}{2}$, and $v = \frac{p-1}{2} - u$ are greater than $\frac{p}{2}$ (note that none of them is 0). Then we have

$$\left(\frac{a}{p}\right) = (-1)^v.$$

Proof. The proof is similar to that of Fermat's Little Theorem, in the sense that we proceed by evaluating in two ways the product of all the remainders r_j modulo p . First, it is clear that

$$r_1 \cdot r_2 \cdot \dots \cdot r_{\frac{p-1}{2}} \equiv a \cdot 2a \cdot \dots \cdot \frac{p-1}{2}a = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Note that for any distinct $i, j \in \{1, 2, \dots, \frac{p-1}{2}\}$ we have that $(i-j)a$ is not divisible by p (because a is not divisible by p , $i-j$ is nonzero, and its absolute value is at most $\frac{p-1}{2}$), and also, $(i+j)a$ is not divisible by p (as $i+j$ is from the set $\{1, 2, \dots, p-1\}$); for the second affirmation the condition $i \neq j$ is not needed. Now let $r_{k_1}, \dots, r_{k_u}$ be all of the r_j s which are lesser than $\frac{p}{2}$ (or from the set $\{1, 2, \dots, \frac{p-1}{2}\}$), and let $r_{l_1}, \dots, r_{l_v}$ be those among the r_j s which are greater than $\frac{p}{2}$ (or from the set $\{\frac{p+1}{2}, \frac{p+3}{2}, \dots, p-1\}$). Due to the above observation we have that

$$r_{k_1}, \dots, r_{k_u}, p - r_{l_1}, \dots, p - r_{l_v}$$

are mutually distinct. But they are all from the set $\{1, 2, \dots, \frac{p-1}{2}\}$, and their number is $\frac{p-1}{2}$, so they coincide in some order with $1, 2, \dots, \frac{p-1}{2}$, which implies

$$r_{k_1} \cdot \dots \cdot r_{k_u} \cdot (p - r_{l_1}) \cdot \dots \cdot (p - r_{l_v}) = \left(\frac{p-1}{2}\right)!,$$

and further yields the congruence

$$(-1)^v r_{k_1} \cdots r_{k_u} \cdot r_{l_1} \cdots r_{l_v} \equiv \left(\frac{p-1}{2}\right)! \pmod{p},$$

or

$$(-1)^v r_{k_1} \cdots r_{k_u} \cdot r_{l_1} \cdots r_{l_v} \equiv a^{p-1} \left(\frac{p-1}{2}\right)! \pmod{p},$$

if we also use Fermat's Little Theorem. Nevertheless, in the left-hand side of this last congruence we actually have the product of all the r_j s, so we get

$$(-1)^v r_1 \cdot r_2 \cdots r_{\frac{p-1}{2}} \equiv a^{p-1} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Comparing the two congruences in which the product of the remainders r_j appears, and canceling the factor $a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$ (which is nonzero modulo p) basically gives us what we intended to prove, namely

$$(-1)^v \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$$

(the last step is Euler's Criterion). Indeed the congruence between $(-1)^v$ and $\left(\frac{a}{p}\right)$ is in fact an equality, because they are both equal to 1 or -1 , so their difference can only be -2 , 0 , or 2 , and it must be 0 modulo p . Since p is odd, only the value 0 is possible for this difference, leading to the desired equality.

Note that v is also the number of those ja with $1 \leq j \leq \frac{p-1}{2}$ that leave a negative remainder when divided by p and this remainder is considered from the set

$$\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, \frac{p-3}{2}, \frac{p-1}{2}\right\}.$$

With the above notations, these remainders are

$$r_{l_1} - p, \dots, r_{l_v} - p.$$

Eisenstein's Lemma. (i) Let p be an odd prime number, and let $a \in \mathbb{Z}$ be odd and not divisible by p . Then the Legendre symbol $\left(\frac{a}{p}\right)$ can be expressed as

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor}.$$

(ii) Now let a be any integer not divisible by p . Then we have

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{2ja}{p} \rfloor}.$$

Proof. (i) With the notations from the proof of Gauss's Lemma, we have

$$ja = p \left\lfloor \frac{ja}{p} \right\rfloor + r_j, \quad \text{for all } 1 \leq j \leq \frac{p-1}{2}.$$

By summing all these equalities we get

$$a \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{\frac{p-1}{2}} r_j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + S + T$$

where (again, with the notations from the previous proof)

$$S = \sum_{s=1}^u r_{k_s} \quad \text{and} \quad T = \sum_{t=1}^v r_{l_t}.$$

Since (as we have just seen above)

$$\left\{ 1, 2, \dots, \frac{p-1}{2} \right\} = \{r_{k_1}, \dots, r_{k_u}, p - r_{l_1}, \dots, p - r_{l_v}\}$$

we also get (by equating the sums of the elements from these sets)

$$\sum_{j=1}^{\frac{p-1}{2}} j = S - T + pv.$$

Adding this equality with

$$a \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + S + T$$

yields

$$(a+1) \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + 2S + pv.$$

Because a and p are odd, by reducing the previous equality modulo 2 we obtain

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \equiv v \pmod{2},$$

hence (by using this congruence and Gauss's Lemma)

$$(-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor} = (-1)^v = \left(\frac{a}{p} \right),$$

which we wanted to prove.

(ii) Note that the equality proved for part (i)

$$(a+1) \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor + 2S + pv$$

is true for any integer a (we used the fact that a is odd only after getting it), so we can replace here a by $2a$ (with a being any integer) in order to get

$$(2a+1) \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ja}{p} \right\rfloor + 2S + pw,$$

where the terms in S are now the remainders of $2ja$ modulo p that are lesser than $\frac{p}{2}$, and w is the number of the remainders of the numbers $2ja$ modulo p that are greater than $\frac{p}{2}$. Reducing modulo 2 yields

$$w \equiv \sum_{j=1}^{\frac{p-1}{2}} j + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ja}{p} \right\rfloor \pmod{2},$$

therefore, by Gauss's lemma, we obtain

$$\left(\frac{2a}{p} \right) = (-1)^w = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} j + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ja}{p} \right\rfloor}.$$

Gauss's lemma also gives us that

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

where z is the number of the remainders of the numbers $2, 4, \dots, p-1$ modulo p that are greater than $\frac{p}{2}$, which number is easily seen to be

$$z = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Moreover, it is not hard to notice that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} = \sum_{j=1}^{\frac{p-1}{2}} j \pmod{2}.$$

Consequently

$$\left(\frac{2}{p} \right) = (-1)^z = (-1)^{\frac{p^2-1}{8}},$$

and, since the above obtained equality for $\left(\frac{2a}{p} \right)$ can also be written in the form

$$\left(\frac{2}{p} \right) \left(\frac{a}{p} \right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} j + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ja}{p} \right\rfloor},$$

or

$$(-1)^{\frac{p^2-1}{8}} \left(\frac{a}{p} \right) = (-1)^{\frac{p^2-1}{8} + \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ja}{p} \right\rfloor},$$

the conclusion follows by canceling $(-1)^{\frac{p^2-1}{8}}$. Note that we also proved the formula for the Legendre symbol of 2 modulo an odd prime, namely we have the following result.

Proposition. For any odd prime p we have

$$\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}.$$

This is also an important part of the quadratic reciprocity law, and it basically says that 2 is a quadratic residue modulo p if and only if either $p \equiv 1 \pmod{8}$, or $p \equiv 7 \pmod{8}$ (and 2 is a quadratic non-residue modulo p when p is congruent to either 3, or 5 modulo 8). Actually, the equality (that we obtained above as a consequence of Euler's criterion)

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

is called the first supplement of the quadratic reciprocity law, while the above expression of $\left(\frac{2}{p}\right)$ is, of course, its second supplement.

Quadratic Reciprocity Law. Let p, q be odd prime numbers. Then

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Proof. Consider in the Cartesian plane the rectangle $ABCD$ with vertices at the points $A(0, 0)$, $B\left(\frac{p}{2}, 0\right)$, $C\left(\frac{p}{2}, \frac{q}{2}\right)$, and $D\left(0, \frac{q}{2}\right)$. We look at the points situated inside $ABCD$, and having integer coordinates—which we call, as usual, lattice points, or integer points. Definitely, no such point lies on the open line segment AC , because p and q are relatively prime, and the equation of (the line) AC is $y = \frac{q}{p}x$. The number of the lattice points that are inside $ABCD$ and under its diagonal AC is

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$$

because each of them has an abscissa $1 \leq j \leq \frac{p-1}{2}$ and an ordinate y that is a positive integer and satisfies $y < \frac{jq}{p}$. Similarly, the number of the lattice points inside $ABCD$ that are above the diagonal AC is

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

On the other hand, it is clear that the number of all the integer points inside $ABCD$ is $\frac{p-1}{2} \cdot \frac{q-1}{2}$, so the double counting we made shows us that

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

(Actually this equality holds for any relatively prime positive integers p and q .) Now, by the first part of Eisenstein's lemma and the previous equality, we get the desired result:

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor} \cdot (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Primes of the Form $x^2 + ny^2$ with $n \in \{1, 2, 3, 4, 5, 13\}$

Fermat's theorem on the representation of a prime as the sum of two squares was proven by Euler, and, since then, it was widely generalized, for example to representations of integers by quadratic forms, among which the representations of positive integers in the form $x^2 + ny^2$ (for various n) have a special place. We will further see some simple proofs of such results (for the above mentioned values of n) using Thue's lemma and the quadratic reciprocity law as main ingredients.

Fermat's Theorem on the Sum of Two Squares

An odd prime $p \equiv 1 \pmod{4}$ can be represented as the sum of two squares if and only if $p \equiv 1 \pmod{4}$.

Proof. The "only if" part follows immediately if we recall that any square is congruent to either 0, or 1 modulo 4 (so, a sum of two squares can only be congruent modulo 4 to 0, 1, or 2). For the other implication, let $p \equiv 1 \pmod{4}$, and note that, by the first supplement of the quadratic reciprocity, we have $\left(\frac{-1}{p}\right) = 1$, hence there exists an integer a such that $a^2 \equiv -1 \pmod{p}$. According to Thue's lemma, we can find natural numbers x and y less than $\sqrt{p}$, not both equal to 0, and such that $a^2y^2 \equiv x^2 \pmod{p}$, yielding

$$x^2 \equiv a^2y^2 \equiv -y^2 \pmod{p} \implies x^2 + y^2 \equiv 0 \pmod{p}.$$

Nevertheless, since x and y are less than $\sqrt{p}$ and not both 0, we get

$$0 < x^2 + y^2 < 2p,$$

therefore the only possibility is $x^2 + y^2 = p$, which finishes the proof of Fermat's theorem. Note that $2 = 1^2 + 1^2$ is clearly a sum of two squares, while the primes congruent to 3 modulo 4 are not, and that, by using all these facts, one can prove that a natural number $N > 1$ can be written as the sum of two squares if and only if in the prime factorization of N all the primes congruent to 3 modulo 4 appear with an even exponent.

Theorem on the Sum of a Square and Twice a Square

An odd prime p can be expressed as the sum of a square and twice a square if and only if $p \equiv 1 \pmod{8}$, or $p \equiv 3 \pmod{8}$.

Proof. For the "only if" part notice that $p = x^2 + 2y^2$ implies that x is odd, hence $x^2 \equiv 1 \pmod{8}$. When y is even this gives $x^2 + 2y^2 \equiv 1 \pmod{8}$, while for odd y we must have $x^2 + 2y^2 \equiv 3 \pmod{8}$.

Now, for the converse, let p be a prime congruent to 1, or to 3 modulo 8. Due to the supplements of the quadratic reciprocity law, we know that

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{-1}{p}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}} = (-1)^{\frac{p^2+4p-5}{8}},$$

and it is easy to check that if $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$, then $p^2 + 4p - 5 \equiv 0 \pmod{16}$, and if $p \equiv 5 \pmod{8}$ or $p \equiv 7 \pmod{8}$, then $p^2 + 4p - 5 \equiv 8 \pmod{16}$. Thus, $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$. Consequently, we can choose a such that $-2 \equiv a^2 \pmod{p}$, and by Thue's lemma we can choose natural numbers x and y less than $\sqrt{p}$, not both 0 and such that $a^2y^2 \equiv x^2 \pmod{p}$. Then we have

$$x^2 \equiv a^2y^2 \equiv -2y^2 \pmod{p} \implies x^2 + 2y^2 \equiv 0 \pmod{p}.$$

Using bounds on x and y , we get

$$0 < x^2 + 2y^2 < 3p,$$

which implies that $x^2 + 2y^2$ can be either p , or $2p$. In the first case we are done, otherwise, if $x^2 + 2y^2 = 2p$, then x is even, say $x = 2k$, meaning that

$$4k^2 + 2y^2 = 2p \implies 2k^2 + y^2 = p,$$

that is, p is again the sum of a square and twice a square, finishing the proof.

Theorem on the Sum of a Square and Three Times a Square

A prime $p > 3$ can be expressed as the sum of a square and three times a square if and only if $p \equiv 1 \pmod{3}$.

Proof. In the representation of a prime $p > 3$ in the form $x^2 + 3y^2$ we must have $x \not\equiv 0 \pmod{3}$, which leads to $x^2 \equiv 1 \pmod{3}$, and then to $p = x^2 + 3y^2 \equiv 1 \pmod{3}$, which proves the "only if" part.

Further, for $p \equiv 1 \pmod{3}$, we have $\left(\frac{-3}{p}\right) = 1$, because

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

and, by the quadratic reciprocity law, we have

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

This shows that there exists an integer a such that $a^2 \equiv -3 \pmod{p}$. For this a , there exist, by Thue's lemma, natural numbers x, y less than $\sqrt{p}$, not both 0, and satisfying $a^2 y^2 \equiv x^2 \pmod{p}$. Thus we have $-3y^2 \equiv a^2 y^2 \equiv x^2 \pmod{p}$, whence $x^2 + 3y^2 \equiv 0 \pmod{p}$. Because we also have $0 < x^2 + 3y^2 < 4p$, $x^2 + 3y^2$ could only equal one of p , $2p$, or $3p$. If $x^2 + 3y^2 = p$, then the required representation is obtained. The equality $x^2 + 3y^2 = 2p$ is impossible modulo 3, so this case is excluded. Finally, if $x^2 + 3y^2 = 3p$, then $x = 3k$, and the equation becomes $3k^2 + y^2 = p$, which gives again the desired representation.

Note that 2 is not representable in the form $x^2 + 3y^2$, while $3 = 0^2 + 3 \cdot 1^2$ evidently (and trivially) is.

Remark. The case $n = 4$ can be skipped, since the possibility of representing an odd prime p as $x^2 + 4y^2$ is clearly equivalent to that of representing p as a sum of two squares. (If $p = x^2 + y^2$ is odd, then one of x and y must be even.) So, the primes of the form $x^2 + 4y^2$ are precisely those congruent to 1 modulo 4.

Theorem on the Sum of a Square and Five Times a Square

An odd prime $p \neq 5$ can be expressed as the sum of a square and five times a square if and only if $p \equiv 1 \pmod{20}$ or $p \equiv 9 \pmod{20}$.

Proof. If we have $p = x^2 + 5y^2$, then p is clearly a quadratic residue modulo 5, and -5 is also a quadratic residue modulo p (since $x^2 \equiv -5y^2 \pmod{p}$ and y is invertible modulo p). Thus we have

$$\left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) \left(\frac{p}{5}\right) = \left(\frac{-5}{p}\right) \left(\frac{p}{5}\right) = 1,$$

or

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

meaning that $p \equiv 1 \pmod{4}$. Also, the fact that p is a quadratic residue modulo 5 implies $p \equiv 1 \pmod{5}$ or $p \equiv 4 \pmod{5}$. By combining with $p \equiv 1 \pmod{4}$ (and using the Chinese Remainder Theorem), in the first of these cases we get $p \equiv 1 \pmod{20}$, while the second yields $p \equiv 9 \pmod{20}$.

Conversely, suppose that $p \equiv 1 \pmod{20}$ or $p \equiv 9 \pmod{20}$. In both cases we have that -5 is a quadratic residue modulo p , so we can pick an integer a such that $a^2 \equiv -5 \pmod{p}$, then (using

Thue's lemma) we can choose nonnegative integers x and y not both 0, lesser than $\sqrt{p}$, for which $a^2y^2 \equiv x^2 \pmod{p}$. It follows that $0 < x^2 + 5y^2 < 6p$, and $x^2 \equiv ay^2 \equiv -5y^2 \pmod{p}$, hence $x^2 + 5y^2$ can only be equal to one of $p, 2p, 3p, 4p$, or $5p$.

If $x^2 + 5y^2 = p$, then the required representation is obtained.

The case $x^2 + 5y^2 = 2p$ is not possible, which is easily seen by checking the equality modulo 8.

The equality $x^2 + 5y^2 = 3p$ is also impossible, since checking modulo 5 shows that the remainders are incompatible.

If $x^2 + 5y^2 = 4p$, then both $x = 2x'$ and $y = 2y'$ are even, so the equation reduces to $x'^2 + 5y'^2 = p$, and we have a representation of p .

If $x^2 + 5y^2 = 5p$, then x is divisible by 5, i.e., $x = 5k$, and the equation becomes $5k^2 + y^2 = p$, which again represents p as the sum of a square and five times a square.

Finally notice that 2 has not such a representation, while 5 obviously has.

Theorem on the Sum of a Square and Thirteen Times a Square

An odd prime number $p \neq 13$ can be expressed as the sum of a square and thirteen times a square if and only if p is congruent modulo 52 to one of the numbers 1, 9, 17, 25, 29, or 49.

Proof. Assume first that the equation $x^2 + 13y^2 = p$ has integer solutions x, y . Then clearly p is a quadratic residue modulo 13, and, also, -13 is a quadratic residue modulo p (since, as in the previous proof, we have $x^2 \equiv -13y^2 \pmod{p}$, and y is not invertible modulo p), so we need to find those p for which $\left(\frac{-13}{p}\right) = 1$ and $\left(\frac{p}{13}\right) = 1$. By using quadratic reciprocity, we then get

$$1 = \left(\frac{-13}{p}\right) \cdot \left(\frac{p}{13}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{13-1}{2}} \cdot (-1)^{\frac{p-1}{2}} = (-1)^{3(p-1)} \cdot (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

so it follows that $p \equiv 1 \pmod{4}$. Moreover, p is a quadratic residue modulo 13, hence p is congruent modulo 13 to one of the numbers 1, 3, 4, 9, 10, 12. Combining these by the Chinese Remainder Theorem yields that p is congruent modulo 52 to one of 1, 9, 17, 25, 29, or 49.

Conversely, if p is congruent modulo 52 to one of these numbers, then -13 is a quadratic residue modulo p , hence there exists an integer a such that $a^2 \equiv -13 \pmod{p}$. By Thue's lemma we can find natural numbers less than $\sqrt{p}$, not both 0, and such that $ay^2 \equiv x^2 \pmod{p}$. It follows that $0 < x^2 + y^2 < 14p$ and $x^2 \equiv ay^2 \equiv -13y^2 \pmod{p}$, hence that $x^2 + 13y^2$ is one of the numbers jp with $1 \leq j \leq 13$. We further consider all these cases, and note that some of them are impossible, while the others lead to a representation of p as desired.

When $x^2 + 13y^2 = p$ there is nothing left to prove.

The equality $x^2 + 13y^2 = 2p$ is impossible, since 2 is not a quadratic residue modulo 13 and p is, so $2p$ is not a quadratic residue modulo 13 either.

Next, $x^2 + 13y^2 = 3p$ considered modulo 3 would give that x, y are divisible by 3, and this would lead to $p = 3$, which is excluded by the form of p .

If $x^2 + 13y^2 = 4p$, then $x = 2x', y = 2y'$ must be even (if they are both odd the equality cannot hold modulo 4, and if one is odd and the other is even, the equality is not true modulo 2), so $x'^2 + 13y'^2 = p$, which confirms the statement.

The equality $x^2 + 13y^2 = 5p$ is, again, impossible because 5 is not a quadratic residue by modulo 13, and the same can be said about the equalities $x^2 + 13y^2 = jp$ for $j \in \{6, 7, 8\}$.

If $x^2 + 13y^2 = 9p$, then $x = 3x', y = 3y'$ are divisible by 3, so we get $x'^2 + 13y'^2 = p$, thus p can be represented as the sum of a square and thirteen times a square.

We cannot have $x^2 + 13y^2 = 10p$ because, checking modulo 5, we see that the only possibility is that x, y are divisible by 5, which requires $p = 5$, but this is excluded by the possible forms of p .

The equality $x^2 + 13y^2 = 11p$ is impossible because it cannot hold modulo 4 (or because 11 is not a quadratic residue modulo 13).

If we had $x^2 + 13y^2 = 12p$ then x, y would be even, which would transform the equation into $x'^2 + 13y'^2 = 3p$ for some integers x', y' , but we have already seen that this is impossible modulo 3.

Finally, $x^2 + 13y^2 = 13p$ implies that $x = 13k$ is divisible by 13, yielding $13k^2 + y^2 = p$, hence the theorem follows.

For completeness, we note that 13 is representable as the sum of a square and thirteen times a square, and 2 is not.

We have proved the cases of $n = 1, 2, 3, 4, 5$ to demonstrate the effectiveness of our (simple and elementary) method, then we skipped the cases of n from 6 to 12 not because they cannot be approached in this way, but in order to test the limits of the method for a greater n . For instance, we invite the reader to prove that a prime $p > 3$ is of the form $x^2 + 6y^2$ if and only if p is congruent to either 1, or 7 modulo 24 (while 2 and 3 are, evidently, not representable in this form).

Of course, as n increases, the amount of necessary computations increases, too, although the basic ideas remain the same. Nevertheless, it must be said that there are values of n for which these ideas do not work, and, consequently, much deeper theories are needed to solve those cases. For example, when $n = 27$, Euler conjectured and Gauss proved that $p = x^2 + 27y^2$ is solvable in integers x and y if and only if $p \equiv 1 \pmod{3}$ and the congruence $x^3 \equiv 2 \pmod{p}$ has a solution—that is, 2 is a cubic residue modulo p . (Not to mention the more complicated characterization of the primes of the form $x^2 + 14y^2$.) Nevertheless, the method that we exposed has the merit of being elementary and easy to understand, so we invite the interested reader to try other cases for small values of n .

Acknowledgements. The author is grateful to the editors and the anonymous referee for their valuable comments that considerably improved this paper.

References

1. David A. Cox: *Primes of the Form $x^2 + ny^2$* , John Wiley and Sons, 1989
2. W. Sierpinski: *Elementary Theory of Numbers*, North-Holland Mathematical Library, PWN-Polish Scientific Publishers, 1988