SQUARES MODULO p, I

KEITH CONRAD

1. Euler's congruence and the Legendre symbol

Let p be a prime number. A numerical study of squares modulo primes has led us to observations like the following:

$$\begin{aligned} -1 \equiv \square \bmod p &\iff p = 2 \text{ or } p \equiv 1 \bmod 4, \\ 2 \equiv \square \bmod p &\iff p = 2 \text{ or } p \equiv 1, 7 \bmod 8, \\ -2 \equiv \square \bmod p &\iff p = 2 \text{ or } p \equiv 1, 3 \bmod 8, \\ 3 \equiv \square \bmod p &\iff p = 2, 3 \text{ or } p \equiv 1, 11 \bmod 12, \\ 5 \equiv \square \bmod p &\iff p = 2, 5 \text{ or } p \equiv 1, 4 \bmod 5. \end{aligned}$$

Now we will introduce tools that will help us eventually prove these equivalences. From now on, $p \neq 2$, so p denotes an *odd* prime.

Lemma 1.1. *The number of nonzero squares modulo p is $(p-1)/2$.*

Proof. Since $a^2 \equiv (-a)^2 \bmod p$, the nonzero integer squares modulo p lie among the squares of the first half of the nonzero integers modulo p:

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p.$$

Moreover, these $(p-1)/2$ squares mod p are different from each other, since

$$\begin{aligned} a^2 \equiv b^2 \bmod p &\iff p|(a-b)(a+b) \\ &\iff p|(a-b) \text{ or } p|(a+b) \\ &\iff a \equiv b \bmod p \text{ or } a \equiv -b \bmod p \end{aligned}$$

and the numbers $1, 2, \ldots, (p-1)/2$ are not $\pm$ each other modulo p. □

Example 1.2. The square modulo 7 are $1^2 = 1$, $2^2 = 4$, and $3^3 = 9 \equiv 2 \bmod 7$.

We can detect squares using a refinement of Fermat's little theorem. For all $a \not\equiv 0 \bmod p$, $a^{(p-1)/2} \bmod p$ is a square root of 1, since

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \bmod p$$

by Fermat. Thus

$$a^{(p-1)/2} \equiv \pm 1 \bmod p. \tag{1.1}$$

Euler found that the value of $a^{(p-1)/2} \bmod p$ distinguishes squares from non-squares.

Theorem 1.3 (Euler)**.** *Let p be an odd prime. For $a \not\equiv 0 \bmod p$,*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \bmod p, & \text{if } a \equiv \square \bmod p, \\ -1 \bmod p, & \text{if } a \not\equiv \square \bmod p. \end{cases}$$

Proof. Suppose $a \equiv b^2 \bmod p$ for some b. Then $b \not\equiv 0 \bmod p$, so

$$a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \bmod p$$

by Fermat.

We now show the converse:

$$a^{(p-1)/2} \equiv 1 \bmod p \Longrightarrow a \equiv \square \bmod p. \tag{1.2}$$

The congruence on the left says a is a root in $\mathbf{Z}/(p)$ of $X^{(p-1)/2} - 1$. A polynomial with coefficients in a field has no more roots in the field than its degree, so there are at most $(p-1)/2$ roots of $X^{(p-1)/2} - 1$ in $\mathbf{Z}/(p)$. The nonzero squares in $\mathbf{Z}/(p)$ are roots, and Lemma 1.1 tells us there are $(p-1)/2$ nonzero squares, so the nonzero squares exhaust all solutions in $\mathbf{Z}/(p)$.

Since, by (1.1), we already know $a^{(p-1)/2} \equiv \pm 1 \bmod p$ for all $a \not\equiv 0 \bmod p$, (1.2) implies that $a^{(p-1)/2} \equiv -1 \bmod p$ for non-squares $a \bmod p$. □

Example 1.4. Is 3 a square modulo 11? Here $p = 11$ and

$$3^{(p-1)/2} = 3^{(10-1)/2} = 3^5 = 243 \equiv 1 \bmod 11,$$

so 3 is a square modulo 11. This does *not* tell us a square root. More generally, the following table illustrates the distinction between squares and non-squares in $\mathbf{Z}/(11)$ through their 5-th powers ($5 = \frac{11-1}{2}$):

a	1	2	3	4	5	6	7	8	9	10
$a^5 \bmod 11$	1	−1	1	1	1	−1	−1	−1	1	−1

Corollary 1.5. *For $p \neq 2$, $-1 \equiv \square \bmod p$ if and only if $p \equiv 1 \bmod 4$.*

Proof. By Theorem 1.3, $-1 \equiv \square \bmod p$ if and only if $(-1)^{(p-1)/2} \equiv 1 \bmod p$. If $p \equiv 1 \bmod 4$ then $(p-1)/2$ is even and the desired congruence holds. If $p \equiv 3 \bmod 4$, then $(p-1)/2$ is odd, so $(-1)^{(p-1)/2} = -1$, and this is $\not\equiv 1 \bmod p$ since $p \neq 2$. □

We can't get a result like Corollary 1.5 so easily for numbers other than -1. For example, Theorem 1.3 says $2 \equiv \square \bmod p \iff 2^{(p-1)/2} \equiv 1 \bmod p$, but it is not easy to see how to compute $2^{(p-1)/2} \bmod p$ for general p, only for individual p on a case-by-case basis.

Definition 1.6. Let p be an odd prime in $\mathbf{Z}^+$. For $a \in \mathbf{Z}$, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

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

In other words, when $a \not\equiv 0 \bmod p$, we know $a^{(p-1)/2} \equiv \pm 1 \bmod p$ by (1.1), and the Legendre symbol $\left(\frac{a}{p}\right)$ is simply the integer 1 or -1 which occurs on the right side. Since $1 \not\equiv -1 \bmod p$, only one of these signs is possible.

Don't confuse the notation $\left(\frac{a}{p}\right)$ with the fraction $\frac{a}{p}$. In any case, the parentheses in the Legendre symbol is always part of the notation of that symbol. The Legendre symbol was

introduced by Legendre in 1798. In books, when the Legendre symbol is on a line of text rather than in a displayed equation, it often typeset like this: $(a|p)$ or (a/p).

Example 1.7. Since $2 \not\equiv \square \bmod 3$, $(\frac{2}{3}) = -1$. Also, since $-7 \equiv 2 \bmod 3$, we have $(\frac{-7}{3}) = -1$ too. The Legendre symbol $(\frac{6}{3})$ is 0.

Example 1.8. Since $6 \equiv 5^2 \bmod 19$, $(\frac{6}{19}) = 1$.

The following theorem summarizes some basic algebraic properties of the Legendre symbol.

Theorem 1.9. *Let p be an odd prime. For a and b in $\mathbf{Z}$,*

(1) $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$,
(2) *if $a \equiv b \bmod p$, then $(\frac{a}{p}) = (\frac{b}{p})$,*
(3) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$,
(4) *the number of solutions to $x^2 \equiv a \bmod p$ is $1 + (\frac{a}{p})$.*

Proof. The first property is an immediate consequence of Theorem 1.3 and the definition of the Legendre symbol. (In fact, Theorem 1.3 motivated that definition.)

The second property reflects the fact that $(\frac{a}{p})$ is determined by the behavior of a modulo p, which is clear from its definition.

For the third property, note $(\frac{ab}{p})$ and $(\frac{a}{p})(\frac{b}{p})$ are 0, 1, or -1, and these three values are distinct modulo p. Therefore we can check $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ in $\mathbf{Z}$ by checking instead that $(\frac{ab}{p}) \equiv (\frac{a}{p})(\frac{b}{p}) \bmod p$. Working modulo p, the two sides become powers:

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \bmod p, \\ \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) &\equiv a^{(p-1)/2} b^{(p-1)/2} \bmod p. \end{aligned}$$

The right sides of both congruences are congruent modulo p, so the left sides are as well (and thus, being 0, 1, or -1, they are equal in $\mathbf{Z}$).

To show the number of solutions of $x^2 \equiv a \bmod p$ is $1 + (\frac{a}{p})$, we take cases. If $a \bmod p$ is a nonsquare then the congruence has 0 solutions and $1 + (\frac{a}{p}) = 1 - 1 = 0$. If $a \bmod p$ is a nonzero square then the congruence has 2 solutions (a nonzero square modulo p has two square roots), and $1 + (\frac{a}{p}) = 1 + 1 = 2$. If $a \equiv 0 \bmod p$ then the congruence has 1 solution (namely $x \equiv 0 \bmod p$) and $1 + (\frac{a}{p}) = 1 + (\frac{0}{p}) = 1 + 0 = 1$. □

The third property of Theorem 1.9, the multiplicativity of the Legendre symbol, is fundamental. Be sure you understand the proof. Taking cases according to the two nonzero values of $(\frac{a}{p})$ and $(\frac{b}{p})$, the multiplicativity of the Legendre symbol means the following three facts about *nonzero* numbers modulo p:

- the product of two squares is a square,
- the product of a square and a non-square is a non-square,
- the product of two non-squares is a square.

Example 1.10. In $\mathbf{Z}/(11)$, 2 and 7 are not squares. Their product is 3, which is a square ($3 = 25$ in $\mathbf{Z}/(11)$).

Example 1.11. $(\frac{2}{19}) = -1$, $(\frac{3}{19}) = -1$, so $(\frac{6}{19}) = 1$. In Example 1.8 we saw explicitly why $(\frac{6}{19}) = 1$.

Example 1.12. Is 60 mod 103 a square? Note 103 is prime. We want to compute $(\frac{60}{103})$. Since $60 = 4 \cdot 3 \cdot 5$,

$$\left(\frac{60}{103}\right) = \left(\frac{4}{103}\right)\left(\frac{3}{103}\right)\left(\frac{5}{103}\right) = \left(\frac{3}{103}\right)\left(\frac{5}{103}\right),$$

so we are reduced to computing $(\frac{3}{103})$ and $(\frac{5}{103})$. From the patterns observed for when $3 \equiv \square \bmod p$ and when $5 \equiv \square \bmod p$, the values of $(\frac{3}{p})$ and $(\frac{5}{p})$ should depend on 103 mod 12 and 103 mod 5. Accepting those patterns as generally true, from $103 \equiv 7 \bmod 12$ we get

$$\left(\frac{3}{103}\right) = -1,$$

and since $103 \equiv 3 \bmod 5$,

$$\left(\frac{5}{103}\right) = -1.$$

Thus $(\frac{60}{103}) = (-1)(-1) = 1$, so 60 mod 103 is a square. This method does *not* tell us a square root. Doing a brute force search reveals a square root is 36: $60 \equiv 36^2 \bmod 103$.

Example 1.13. We have $(\frac{6}{p}) = (\frac{2}{p})(\frac{3}{p})$. Therefore, when $p \neq 2$ or 3, deciding whether or not 6 is a square modulo p is "reduced" to whether or not 2 and 3 are squares modulo p. If they are both squares or are both non-squares, then 6 is a square modulo p. If one is a square and the other is not, then 6 mod p is not a square.

For nonzero $a \in \mathbf{Z}$, write

$$a = \varepsilon p_1 p_2 \cdots p_r.$$

where $\varepsilon = \pm 1$ and the p_i's are positive prime numbers. Some of the p_i's may be equal. By multiplicativity of the Legendre symbol,

$$\left(\frac{a}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{p_1}{p}\right)\cdots\left(\frac{p_r}{p}\right).$$

Thus, the computation of a general Legendre symbol $(\frac{a}{p})$ is reduced to the case where $a = -1$ or a is a prime in $\mathbf{Z}^+$. Because of the peculiar nature of the prime 2 in the context of squares, it is useful to consider three cases: $a = -1$, $a = 2$, and $a = q$ is an odd prime.

2. The Quadratic Reciprocity Law: Motivation

Numerical evidence has already suggested that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv 3 \bmod 4, \end{cases} \tag{2.1}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \bmod 8, \\ -1, & \text{if } p \equiv 3, 5 \bmod 8. \end{cases} \tag{2.2}$$

What can be said about $(\frac{q}{p})$ when p and q are distinct (positive) odd prime numbers? The following experimentally discovered properties of $\pm q \equiv \square \bmod p$, where $p \neq q$, suggest a connection between $(\frac{q}{p})$ and $(\frac{p}{q})$:

$$\begin{aligned}
3 \equiv \square \bmod p &\iff p \equiv 1, 11 \bmod 12,\\
-3 \equiv \square \bmod p &\iff p \equiv 1 \bmod 3,\\
5 \equiv \square \bmod p &\iff p \equiv 1, 4 \bmod 5,\\
-5 \equiv \square \bmod p &\iff p \equiv 1, 3, 7, 9 \bmod 20,\\
7 \equiv \square \bmod p &\iff p \equiv 1, 3, 9, 19, 25, 27 \bmod 28,\\
-7 \equiv \square \bmod p &\iff p \equiv 1, 2, 4 \bmod 7,\\
11 \equiv \square \bmod p &\iff p \equiv 1, 5, 7, 9, 10, 25, 35, 37, 39 \bmod 44,\\
-11 \equiv \square \bmod p &\iff p \equiv 1, 3, 4, 5, 9 \bmod 11,\\
13 \equiv \square \bmod p &\iff p \equiv 1, 3, 4, 9, 10, 12 \bmod 13,\\
-13 \equiv \square \bmod p &\iff p \equiv 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \bmod 52.
\end{aligned}$$

Writing the (signed) prime on the left as $\pm q$, the modulus on the right is q or $4q$. The modulus is q for $-3, 5, -7, -11$, and 13, while it is $4q$ for $3, -5, 7, 11$, and -13. What separates $3, 7$, and 11 from 5 and 13 is the value mod 4: $3, 7, 11 \equiv 3 \bmod 4$ and $5, 13 \equiv 1 \bmod 4$. This leads us to the formulation of the above conjectures as: for $q \equiv 1 \bmod 4$, $q \equiv \square \bmod p$ if and only if $p \equiv \square \bmod q$, while for $q \equiv 3 \bmod 4$, $-q \equiv \square \bmod p$ if and only if $p \equiv \square \bmod q$. We combine these both into

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{if } p \text{ or } q \equiv 1 \bmod 4,\\ -\left(\frac{p}{q}\right), & \text{if } p \text{ and } q \equiv 3 \bmod 4. \end{cases} \tag{2.3}$$

This equation and the formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ in (2.1) and (2.2) are collectively referred to as the quadratic reciprocity law.

Theorem 2.1 (Quadratic Reciprocity)**.** *Let p and q be distinct odd positive primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \tag{2.4}$$

Furthermore, for any positive prime p,

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

Equation (2.4) is called the *main law* of quadratic reciprocity and the formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ are called the *supplementary laws*. In the main law, the sign $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ is 1 if p *or* q is $\equiv 1 \bmod 4$ and is -1 if p *and* $q \equiv 3 \bmod 4$. Therefore the main law is the same as (2.3). The supplementary laws are just another way of writing (2.1) and (2.2) (check!).

Quadratic reciprocity was first conjectured by Euler in 1742. Legendre claimed to have a proof in 1785, but there was a gap. The first proof is due to Gauss in 1796, just shy of his 19th birthday. (Before the year was over, he found two more proofs!) He called it the *aureum theorema* ("golden theorem"). For a list of more than 200 proofs, see `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`.

Example 2.2. Let's use quadratic reciprocity to calculate $(\frac{30}{79})$:

$$\left(\frac{30}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{3}{79}\right)\left(\frac{5}{79}\right), \tag{2.5}$$

so computing $(\frac{30}{79})$ is reduced to computing $(\frac{q}{79})$ for $q = 2$, 3, and 5.

Since $79 \equiv 7 \bmod 8$, the supplementary law tells us

$$\left(\frac{2}{79}\right) = 1.$$

Using the main law (and noting $79 \equiv 3 \bmod 4$),

$$\left(\frac{3}{79}\right) = -\left(\frac{79}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

and (since $5 \equiv 1 \bmod 4$)

$$\left(\frac{5}{79}\right) = \left(\frac{79}{5}\right) = \left(\frac{4}{5}\right) = 1$$

Thus $(\frac{30}{79}) = 1 \cdot (-1) \cdot 1 = -1$, so 30 is not a square modulo 79.

Example 2.3. We will use quadratic reciprocity to show for $p \neq 2$ that $(\frac{-2}{p}) = 1$ if and only if $p \equiv 1, 3 \bmod 8$. Then $(\frac{-2}{p}) = -1$ in the complementary case, which is $p \equiv 5, 7 \bmod 8$ (odd numbers that are not 1 or 3 mod 8 are 5 or 7 mod 8).

By multiplicativity, $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$. So $(\frac{-2}{p}) = 1$ precisely when $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both 1 or when $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both -1. By the supplementary laws of quadratic reciprocity $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both 1 precisely when $p \equiv 1 \bmod 4$ and $p \equiv 1, 7 \bmod 8$. Knowing a number mod 8 tells you what it has to be mod 4. Since $p \equiv 1 \bmod 8$ forces $p \equiv 1 \bmod 4$, we have

$$p \equiv 1 \bmod 4 \text{ and } p \equiv 1 \bmod 8 \iff p \equiv 1 \bmod 8.$$

On the other hand, the two conditions $p \equiv 1 \bmod 4$ and $p \equiv 7 \bmod 8$ are incompatible because the second condition forces $p \equiv 7 \equiv 3 \bmod 4$ rather than $p \equiv 1 \bmod 4$. Therefore $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both 1 precisely when $p \equiv 1 \bmod 8$.

Turning now to the case when $(\frac{-1}{p})$ and $(\frac{2}{p})$ are both -1, the supplementary law of quadratic reciprocity tells us this happens precisely when $p \equiv 3 \bmod 4$ and $p \equiv 3, 5 \bmod 8$. Easily

$$p \equiv 3 \bmod 4 \text{ and } p \equiv 3 \bmod 8 \iff p \equiv 3 \bmod 8,$$

but the conditions $p \equiv 3 \bmod 4$ and $p \equiv 5 \bmod 8$ are inconsistent since the second condition reduces to $p \equiv 5 \equiv 1 \bmod 4$ rather than $p \equiv 3 \bmod 4$.

Collecting what we have done, for odd prime p the value of $(\frac{-2}{p})$ is 1 precisely when $p \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$.

Example 2.4. Let's use quadratic reciprocity to prove one of the patterns from the square-search tables. For which primes $p \neq 2, 3$ is $3 \equiv \square \bmod p$? In terms of the Legendre symbol, we want to describe those p with $(\frac{3}{p}) = 1$. By the main law of quadratic reciprocity,

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

This is 1 when both factors are 1 or both are -1. We have

$$(-1)^{(p-1)/2} = 1 \iff p \equiv 1 \bmod 4$$

and

$$\left(\frac{p}{3}\right) = 1 \Longleftrightarrow p \equiv 1 \bmod 3.$$

By the Chinese remainder theorem, $p \equiv 1 \bmod 4$ and $p \equiv 1 \bmod 3$ if and only if $p \equiv 1 \bmod 12$.

Also,

$$(-1)^{(p-1)/2} = -1 \Longleftrightarrow p \equiv 3 \bmod 4$$

and

$$\left(\frac{p}{3}\right) = -1 \Longleftrightarrow p \equiv 2 \bmod 3.$$

These two congruence conditions on p are the same as the single condition $p \equiv 11 \bmod 12$.

Thus, for $p \neq 2$ or 3, $(\frac{3}{p}) = 1$ if and only if $p \equiv 1, 11 \bmod 12$.

Example 2.5. From quadratic reciprocity we will show for $p \neq 2, 3$ that $-3 \equiv \square \bmod p \Longleftrightarrow p \equiv 1 \bmod 3$. Using the main law and the supplementary law for $(\frac{-1}{p})$,

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

Therefore $(\frac{-3}{p}) = 1$ if and only if $(\frac{p}{3}) = 1$, which means $p \equiv 1 \bmod 3$.

Example 2.6. Our next example is a cautionary note. Is $-1 \equiv \square \bmod 161$? Since $161 \equiv 1 \bmod 4$, $(-1)^{(161-1)/4} = (-1)^{40} = 1$, so $-1 \equiv \square \bmod 161$. However, this reasoning is bogus because 161 is *not prime*: $161 = 7 \cdot 23$. In fact, $-1 \bmod 161$ is not a square: if $-1 \equiv a^2 \bmod 161$ then $-1 \equiv a^2 \bmod 7$, but $-1 \bmod 7$ is not a square. The moral is that to decide whether an integer is a square in some modulus using quadratic reciprocity, one should first check that the modulus is prime.

3. Proving square patterns

We will prove the two supplementary laws for $(\frac{-1}{p})$ and $(\frac{2}{p})$. The main law will be proved in part II, building on the ideas developed below. The approach we use is due to V. A. Lebesgue (1838).

Theorem 3.1. *For any odd prime p in $\mathbf{Z}^+$,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4, \\ -1, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

That is, $-1 \equiv \square \bmod p \Longleftrightarrow p \equiv 1 \bmod 4$.

Proof. That $(\frac{-1}{p})$ is given by the two values depending on $p \bmod 4$ is just a rephrasing of Corollary 1.5. □

To prove the formula for $(\frac{2}{p})$ and (later) the main law of quadratic reciprocity, we will count the number of points on the "mod p circle"

$$x^2 + y^2 \equiv a \bmod p.$$

Lemma 3.2. *For $a \in \mathbf{Z}/(p)$,*

$$\#\{(x, y) : x, y \in \mathbf{Z}/(p), x^2 + y^2 = a\} = \begin{cases} p - (\frac{-1}{p}), & \text{if } a \neq 0, \\ p + (\frac{-1}{p})(p-1), & \text{if } a = 0. \end{cases}$$

In particular, the number of ways of writing a as a sum of two squares in $\mathbf{Z}/(p)$ is the same for all nonzero a.

Proof. Let N_a be the number of solutions. First we will compute N_0 and then we will look at N_a for $a \not\equiv 0 \bmod p$.

Since $N_0 = \#\{(x,y) : x, y \in \mathbf{Z}/(p), x^2 = -y^2\}$, if there is a solution with $y \not\equiv 0 \bmod p$ then we can divide by y to see that $-1 \equiv \square \bmod p$. So contrapositively, if $-1 \not\equiv \square \bmod p$ then we must have $y \equiv 0 \bmod p$, so $x \equiv 0 \bmod p$, which means $N_0 = 1$. If, on the other hand, $-1 \equiv \square \bmod p$, say $-1 \equiv t^2 \bmod p$, then $x^2 \equiv -y^2 \bmod p$ if and only if $x \equiv \pm ty \bmod p$, so to each nonzero y ($p-1$ choices for that) there are 2 choices of x and to $y = 0$ we need $x = 0$. Thus $N_0 = 2(p-1) + 1 = 2p - 1$, so

$$N_0 = \begin{cases} 1, & \text{if } -1 \not\equiv \square \bmod p, \\ 2p-1, & \text{if } -1 \equiv \square \bmod p, \end{cases}$$

which is described in a uniform way by the single formula $p + (\frac{-1}{p})(p-1)$.

Now we compute N_a for $a \not\equiv 0 \bmod p$. We will show N_a is the same for all nonzero $a \bmod p$ and then compute this common value.

Write

$$N_a = \sum_{b+c=a} \#\{x : x^2 \equiv b \bmod p\}\#\{y : y^2 \equiv c \bmod p\},$$

where the sum runs over all b and c in $\mathbf{Z}/(p)$ which add up to a modulo p. Using Theorem 1.9(4),

$$\begin{aligned} N_a &= \sum_{b+c=a} \left(1 + \left(\frac{b}{p}\right)\right)\left(1 + \left(\frac{c}{p}\right)\right) \\ &= \sum_{b+c=a} \left(1 + \left(\frac{b}{p}\right) + \left(\frac{c}{p}\right) + \left(\frac{bc}{p}\right)\right) \\ &= \sum_{b} \left(1 + \left(\frac{b}{p}\right) + \left(\frac{a-b}{p}\right) + \left(\frac{b(a-b)}{p}\right)\right) \\ &= p + \sum_b \left(\frac{b}{p}\right) + \sum_b \left(\frac{a-b}{p}\right) + \sum_b \left(\frac{b(a-b)}{p}\right). \end{aligned}$$

There are as many squares as nonsquares among the nonzero values mod p, so the second and third sums above each contain as many 1's as -1's, so both sums are 0. We are left with

$$N_a = p + \sum_b \left(\frac{b(a-b)}{p}\right).$$

The formula still looks like it depends on a, but now we make the dependence disappear by a clever change of variables: in the sum over all $b \bmod p$, replace b with ab. (This is an invertible change of variables since $a \not\equiv 0 \bmod p$.) Then

$$N_a = p + \sum_b \left(\frac{ab(a-ab)}{p}\right) = p + \sum_b \left(\frac{a^2 b(1-b)}{p}\right) = p + \sum_b \left(\frac{b(1-b)}{p}\right).$$

The last formula does not involve a, so all N_a for $a \not\equiv 0 \bmod p$ are the same. What is this common value?

Since $\sum_{a \bmod p} N_a = p^2$ (because every pair (x, y) in $(\mathbf{Z}/(p))^2$ is counted by one N_a), write N_a for $a \not\equiv 0 \bmod p$ as N_1 to get $N_0 + (p-1)N_1 = p^2$, so

$$N_1 = \frac{p^2 - N_0}{p-1} = \frac{p^2 - p - (\frac{-1}{p})(p-1)}{p-1} = p - \left(\frac{-1}{p}\right).$$

□

Theorem 3.3. *For any odd prime p in $\mathbf{Z}^+$,*

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

That is, $2 \equiv \square \bmod p \iff p \equiv 1, 7 \bmod 8$.

Proof. We will count the number of points on the "mod p unit circle"

$$x^2 + y^2 \equiv 1 \bmod p$$

in two ways. By Lemma 3.2, there are $p - (\frac{-1}{p})$ points. We will now compute the number, as an integer modulo 8, in a different way.

The solutions to $x^2 + y^2 \equiv 1 \bmod p$ come in collections of size 8: given any solution (x, y) we have 8 solutions by changing signs independently:

$$(x, y), \quad (-x, y), \quad (x, -y), \quad (-x, -y), \quad (y, x), \quad (-y, x), \quad (y, -x), \quad (-y, -x).$$

Actually, these 8 solutions are different *provided* $x \not\equiv 0 \bmod p$, $y \not\equiv 0 \bmod p$, and $x \not\equiv \pm y \bmod p$. So the total number of solutions is congruent modulo 8 to the number of solutions with $x \equiv 0 \bmod p$, $y \equiv 0 \bmod p$, or $x \equiv \pm y \bmod p$. The condition $x \equiv 0 \bmod p$ means $(x, y) = (0, \pm 1)$, $y \equiv 0 \bmod p$ means $(x, y) = (\pm 1, 0)$, and $x \equiv \pm y \bmod p$ means $(x, y) = (c, \pm c)$ where $2c^2 \equiv 1 \bmod p$. There are such c precisely when $2 \equiv \square \bmod p$, in which case c has 2 values. So the number of exceptions we have found is $2 + 2 + 4 = 8$ if $2 \equiv \square \bmod p$ and $2 + 2 + 0 = 4$ if $2 \not\equiv \square \bmod p$. Thus

$$p - \left(\frac{-1}{p}\right) \equiv \begin{cases} 0 \bmod 8, & \text{if } 2 \equiv \square \bmod p, \\ 4 \bmod 8, & \text{if } 2 \not\equiv \square \bmod p. \end{cases}$$

We can write this in a uniform way as

$$p - \left(\frac{-1}{p}\right) \equiv 2\left(1 - \left(\frac{2}{p}\right)\right) \bmod 8.$$

Dividing this congruence by 2 (which reduces the modulus to 4) and rearranging terms,

$$\left(\frac{2}{p}\right) \equiv 1 - \frac{p - (\frac{-1}{p})}{2} \bmod 4.$$

Now take cases on $p \bmod 8$. If $p \equiv 1 \bmod 8$, $p - (\frac{-1}{p}) = p - 1 \equiv 0 \bmod 8$, so $1 - \frac{p-(\frac{-1}{p})}{2} \equiv 1 \bmod 4$. If $p \equiv 3 \bmod 8$, $p - (\frac{-1}{p}) = p + 1 \equiv 4 \bmod 8$, so $1 - \frac{p-(\frac{-1}{p})}{2} \equiv -1 \bmod 4$. If $p \equiv 5 \bmod 8$, $p - (\frac{-1}{p}) = p - 1 \equiv 4 \bmod 8$, so $1 - \frac{p-(\frac{-1}{p})}{2} \equiv -1 \bmod 4$. Lastly, if $p \equiv 7 \bmod 8$, $p - (\frac{-1}{p}) = p + 1 \equiv 0 \bmod 8$, so $1 - \frac{p-(\frac{-1}{p})}{2} \equiv 1 \bmod 4$. We have computed $(\frac{2}{p})$ in all cases. □