Pythagorean Triples mod p

Zoe Shleifer and Elena Su

June 22, 2020

1 Introduction

A Pythagorean triple modulo a prime p is a solution to the equation $x^2 + y^2 \equiv z^2 \pmod{p}$. Using only introductory number theory, we will find surprising results about the distribution of triples across values modulo p. We find that the triples are equally distributed among non-zero values of $z \pmod{p}$ and that the probability that randomly chosen x, y, and z form a Pythagorean is exactly $1/p$. Our eventual goal will be to count the number of Pythagorean triples modulo p.

In Section 2, we will introduce primitive roots and build up their basic properties. These tools will lead us to the important facts about squares modulo p and the Legendre symbol in Section 3. Ultimately, these findings will inform our approach to Pythagorean triples. In Section 4, we will finally compute the total number of triples (Corollary 4.7).

2 Preliminaries

We will begin by providing a few definitions and conventions that will assist us in later proofs. Throughout the paper, p will be an odd prime, and all other variables (a, b, k, g, α ect.) will be integers. Much of our work will take place modulo p, but we generally specify these instances.

Definition 2.1. We use $a \mid b$ to denote that a *divides* b.

Definition 2.2. The *greatest common divisor* of two integers, denoted $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$.

Definition 2.3. We say that a has *order* k modulo p if k is the smallest integer such that $a^k \equiv 1 \pmod{p}$.

Definition 2.4. We call g a *primitive root* mod p if for all $a \pmod{p}$ there exists k such that $g^k = a$.

For example, in the small case of $p = 5$, we find that 2 is a primitive root. If we check each power of 2, we see that all values modulo 5 are covered.
$2^0 = 1$, $2^1 = 2$, $2^3 = 3$, and $2^2 = 4$. We are interested in primitive roots because they are a powerful tool that can help us prove more difficult theorems.

Lemma 2.5. *Let g be a primitive root mod p. The first $p-1$ powers of g — that is, $g^0, g^1, \ldots, g^{p-2}$ — are unique mod p.*

Proof. Assume to the contrary that there are two distinct powers α, α' less than $p-1$ such that $g^\alpha \equiv g^{\alpha'} \pmod{p}$. Without loss of generality, assume $\alpha > \alpha'$. Then $g^{\alpha-\alpha'} \equiv 1 \pmod{p}$. This is a contradiction because g has order $p-1$ by the definition of a primitive root. □

It follows from Definition 2.4 that every value $a \pmod{p}$ can be represented as a power of a primitive root: since there are $p-1$ distinct values and $p-1$ distinct powers. It follows that the order of a primitive root is exactly $p-1$.

The following is a key lemma that will assist us in many later proofs. We will not prove this lemma in this paper, but a full proof can be found in any introductory number theory text.

Lemma 2.6. *For a prime p, there is a primitive root mod p.*

Although we won't prove it here, Lemma 2.6 is a key fact in number theory whose proof can be found in any introductory book on the subject. The following lemma is one of many examples why primitive roots are useful. Additionally, as only prime numbers are guaranteed to have primitive roots, we cannot generalize our results to all composite numbers.

Lemma 2.7. *For all nonzero a mod p, there is a unique x such that $ax \equiv 1 \pmod{p}$. We call x the* inverse *of a mod p, denoted a^{-1}.*

Proof. Consider a primitive root g modulo p. By Lemma 2.5 we know that there exists a power k such that $g^k \equiv a \pmod{p}$. Since k is strictly between 1 and $p-1$, this implies that $(p-1)-k$ is positive. Therefore, by the definition of a primitive root, we know that $g^{p-1} \equiv 1$, so $g^{(p-1)-k}a \equiv 1 \pmod{p}$. By Lemma 2.5, a has an inverse modulo p.

We assume that this inverse is non-unique and take x and x' to be inverses of a then

$$a(x-x') = ax - ax' \equiv 1 - 1 \equiv 0 \pmod{p}.$$

This contradicts the definition of a. So our inverses must be unique. □

3 Legendre Symbols

The Legendre symbol is a powerful tool that will ultimately assist us in counting the number of Pythagorean triples mod p. In this section, our goal is to define the Legendre symbol and to demonstrate some of its properties. For this section, it is important to remember that p is odd.

Definition 3.1. For all a such that $\gcd(a, m) = 1$, we call a is called a *quadratic residue* modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution. If it has no solution, then a is called a *quadratic nonresidue* mod p.

Definition 3.2. If p denotes an odd prime, then the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue, -1 if a is a quadratic nonresidue, and 0 if $p \mid a$.

In this section, our goal is to develop the properties of the Legendre symbol, with the end goal of proving that it is multiplicative.

Proposition 3.3. *For any odd prime p, the number of nonzero quadratic residues and nonzero nonresidues modulo p are equal.*

Proof. By Lemma 2.5, we can express every $x < p$ in the form $g^k \pmod{p}$, where g is a primitive root modulo p. By Lemma 2.6, know that such a g exists.

First, assume that a is a quadratic residue. Then by Definition 3.1, we know that the equation $a \equiv x^2 \pmod{p}$ has solutions. Substituting in g^k for x yields $g^{2k} \equiv a \pmod{p}$. Therefore, a is only a quadratic residue when g is raised to an even power.

Since the order of $g \pmod{p}$ is $p-1$, there are exactly $\frac{p-1}{2}$ even k, $k < p$, each of which yields a unique nonzero quadratic residue modulo p. The same approach can be used to determine that there are also exactly $\frac{p-1}{2}$ odd k, implying that there are $\frac{p-1}{2}$ nonzero quadratic nonresidues modulo p. □

Proposition 3.4. *For all odd primes p, we have that,*

$$\sum_{k=0}^{p-1} \left(\frac{k}{p}\right) = 0.$$

Proof. There are the same number of nonzero quadratic residues and nonresidues modulo p, by Proposition 3.3. This implies that there are $\frac{p-1}{2}$ values of k such that $\left(\frac{k}{p}\right) = 1$, and that there are also $\frac{p-1}{2}$ values of k such that $\left(\frac{k}{p}\right) = -1$. Additionally, the last value, $k = 0$, has $\left(\frac{k}{p}\right) = 0$. Therefore, by the definition of the Legendre symbol, $\sum_{k=0}^{p-1} \left(\frac{k}{p}\right) = 0$. □

Proposition 3.5. *The number of solutions to $x^2 \equiv a \pmod{p}$ is $1 + \left(\frac{a}{p}\right)$.*

Proof. Consider three cases: when $\left(\frac{a}{p}\right) = 1$, when $\left(\frac{a}{p}\right) = -1$, and finally when $\left(\frac{a}{p}\right) = 0$.
Case 1: $\left(\frac{a}{p}\right) = 1$. Then $1 + \left(\frac{a}{p}\right) = 1 + 1 = 2$, which is indeed the correct number of solutions. Indeed, we can see that if $\sqrt{a}$ is a solution to the equivalence $x^2 \equiv a \pmod{p}$, then $-\sqrt{a}$ is a solution as well.
Case 2: $\left(\frac{a}{p}\right) = -1$, so no solutions exist. This means that $1 + \left(\frac{a}{p}\right) = 1 - 1 = 0$, which is also correct.
Case 3: $\left(\frac{a}{p}\right) = 0$, which implies that $a = 0$ because p is prime. $x \equiv 0 \pmod{p}$ is the only solution to the equation $x^2 \equiv 0 \pmod{p}$, which aligns itself with the proposition. □

Proposition 3.5 allows us to prove Euler's Criterion, which gives an alternate method of computing the Legendre Symbol for a given a and p.

Theorem 3.6 (Euler's Criterion)**.** *If p is an odd prime, then $x^2 \equiv a \pmod{p}$ has two solutions if $a^{(p-1)/2} \equiv 1 \pmod{p}$ and no solutions if $a^{(p-1)/2} \equiv -1 \pmod{p}$. In other words,*

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

Proof. By Lemma 2.6 we know that there exists a primitive root $g \bmod p$. Additionally, by Lemma 2.5, for any k, we can write $k \equiv g^i \pmod{p}$.

Case 1: a is a quadratic residue.
In this case, we can write $a \equiv b^2 \pmod{p}$. Set $b \equiv g^n \pmod{p}$. Evidently, this directly implies that $a^2 \equiv g^{2n} \pmod{p}$. If we raise a to the power of $\frac{p-1}{2}$, then we see that

$$a^{(p-1)/2} \equiv g^{n\cdot(p-1)} \equiv 1 \pmod{p}.$$

Case 2: a is a quadratic nonresidue.
In this case, write $a \equiv g^n$, where n is odd. When we raise a to the power of $\frac{p-1}{2}$, we obtain

$$a^{(p-1)/2} \equiv g^{n\cdot(p-1)/2} \pmod{p}.$$

We can rewrite $n \cdot \frac{p-1}{2}$ as

$$\frac{n-1}{2} \cdot (p-1) + \frac{p-1}{2},$$

meaning that

$$g^{n\cdot(p-1)/2} = g^{(n-1)/2\cdot(p-1)+(p-1)/2}.$$

Since $\frac{n-1}{2} \cdot (p-1)$ is a multiple of $p-1$, we obtain that

$$a^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}.$$

Because g is a primitive root, its order is $p-1$. This directly implies that $g^{(p-1)/2} \equiv -1 \pmod{p}$, as desired.

Case 3: a is a multiple of p.
In this case, clearly $a \equiv 0 \pmod{p}$. Since $\frac{p-1}{2}$ is an integer, this implies that $a^{(p-1)/2} \equiv 0 \pmod{p}$. □

Euler's Criterion is useful because it allows us to very easily prove that the Legendre symbol is multiplicative.

Theorem 3.7. *We have $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.*

Proof. If $\left(\frac{a}{p}\right)$ or $\left(\frac{b}{p}\right) = 0$, then this implies that $p \mid a$ or $p \mid b$. However, if this is true, then $p \mid ab$ as well. Therefore, $\left(\frac{ab}{p}\right) = 0$, and so $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ in this case.

Now assume that neither $\left(\frac{a}{p}\right)$ nor $\left(\frac{b}{p}\right) = 0$. By Euler's Criterion [Theorem 3.6],

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

Therefore, we have that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$ when both Legendre symbols are nonzero as well. □

4 Pythagorean Triples

Definition 4.1. A *Pythagorean triple mod p* is a tuple of three nonnegative integers (x, y, z) such that $x^2 + y^2 \equiv z^2 \pmod{p}$ and x, y, and z are all less than p.

In this section, we will count the number of Pythagorean triples modulo p. We will begin by enumerating triples in the case $z = 0$, and then consider the general case. Using these computations, we derive insights about how Pythagorean triples are distributed.

Proposition 4.2. *We have*

$$p + (p-1)\left(\frac{-1}{p}\right)$$

solutions to the equation $x^2 + y^2 \equiv 0 \pmod{p}$.

Proof. Since $x^2 + y^2 \equiv 0 \pmod{p}$, this means that $y^2 \equiv -x^2 \pmod{p}$. From Proposition 3.5, we see that there are $1 + \left(\frac{-x^2}{p}\right)$ solutions to the equation $y^2 \equiv -x^2 \pmod{p}$ for a given x. Additionally, by Theorem 3.7, we can simplify $\left(\frac{-x^2}{p}\right)$ as follows:

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

Moreover, x^2 is always a quadratic residue mod p, so $\left(\frac{x^2}{p}\right) = 1$ when x is nonzero. Therefore,

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

So for any nonzero x, the number of solutions to this equation is

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

As x ranges from 1 to $p-1$, the total number of solutions for nonzero x to the equation $x^2 + y^2 \equiv 0 \pmod{p}$ is given by

$$(p-1) \times \left(1 + \left(\frac{-1}{p}\right)\right).$$

However, we have failed to account for the solution $(0, 0, 0)$. Therefore, there are actually

$$1 + (p-1) \times \left(1 + \left(\frac{-1}{p}\right)\right)$$

Pythagorean triples mod p with $z = 0$. This simplifies to

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

which is equivalent to

$$p + (p-1) \times \left(\frac{-1}{p}\right).$$

□

Lemma 4.3. *For a prime p and an integer a relatively prime to p, we have that*

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right).$$

Proof. For each x, by Lemma 2.7 we know that a must have an inverse modulo p, so we can find $y = a^{-1}x$. This means that $ay \equiv x \pmod{p}$ so we can rewrite the original sum,

$$\sum_{x} \left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right) = \sum_{y} \left(\frac{ay}{p}\right)\left(\frac{ay+a}{p}\right).$$

We know that the Legendre symbol is multiplicative by Theorem 3.7, so we can take out the $\left(\frac{a}{p}\right)$ from both Legendre symbols to get

$$\sum_{y} \left(\frac{a}{p}\right)^2 \left(\frac{y}{p}\right)\left(\frac{y+1}{p}\right).$$

We know $\left(\frac{a}{p}\right)$ is nonzero so $\left(\frac{a}{p}\right)^2 = 1$. Therefore,

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right).$$

□

While the following two propositions may seem arbitrary, a very similar expression will appear when counting triples. The mechanism of substituting 1 for an arbitrary a will be the crux of our final computation. Proposition 4.4 will simplify this substitution even further.

Proposition 4.4. *We have that*

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -1.$$

The align* environment uses & symbols. See the following example of how to use it.

$$\begin{aligned} LHS &= RHS1 \\ &= RHS2. \end{aligned}$$

Proof. Let S equal the sum above. Then, by Lemma 4.3 we have that

$$\begin{aligned} (p-1)S &= \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) \\ &= \sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right) \\ &= \sum_{a=1}^{p-1}\sum_{x=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right). \end{aligned}$$

By Proposition 3.4 we have that

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) = 0.$$

However, our sum does not include $a = 0$. So we can subtract out that term to get,

$$\sum_{x=1}^{p-1} \left(\frac{x}{p}\right)\left(0 - \left(\frac{x}{p}\right)\right) = \sum_{x=1}^{p-1} -\left(\frac{x}{p}\right)^2 = -(p-1).$$

This means that $-(p-1) = S(p-1)$, so $S = -1$. □

Proposition 4.5. *Let N denote the number of solutions (x, y) to $x^2 + y^2 \equiv 1 \pmod{p}$. Given a fixed $k < p$, the number of solutions (x, y) to $x^2 + y^2 = k^2$ will be N.*

Proof. We can write $x^2 + y^2 = 1$ as $y^2 = (1-x)(1+x)$. We know this has N solutions. Similarly, we can write

$$x^2 + y^2 = k^2 \text{ as } y^2 = k^2 - x^2.$$

Dividing by k^2 we find that

$$\frac{y^2}{k^2} = 1 - \frac{x^2}{k^2}.$$

Since we can multiply a Pythagorean triple $(x, y, 1)$ by k to get a solution (kx, ky, k) and likewise, we can multiply a triple (kx, ky, k) by k^{-1} to get another solution $(x, y, 1)$, we find that $(x, y, 1)$ is a triple if and only if (kx, ky, k) is also a triple. Therefore, there must be an equal number of solutions N for all nonzero k. □

It follows that given the number of solutions M of the form (x, y, z) with $z \not\equiv 0$ to $x^2 + y^2 \equiv z^2 \pmod{p}$ every z will have $\frac{M}{p-1}$ solutions (x, y)

The previous proposition gives us a really surprising result about the distribution of Pythagorean triples (x, y, z). We find that they are equally distributed among the nonzero values of z. This fact will be very useful in finding the number of total Pythagorean triples.

Theorem 4.6. *For any $k \not\equiv 0 \pmod{p}$, the number of solutions to $x^2 + y^2 \equiv k^2$ is $p - \left(\frac{-1}{p}\right)$.*

Proof. By Proposition 3.5 we know that the number of solutions to $x^2 \equiv a \pmod{p}$ is $1 + \left(\frac{a}{p}\right)$. This tells us that number of solutions is given by,

$$\sum_{y=0}^{p-1} 1 + \left(\frac{k^2 - y^2}{p}\right).$$

By Theorem 3.7 we expand to find that the previous sum is equal to

$$p + \left(\frac{-1}{p}\right) \sum_{y=0}^{p-1} \left(\frac{y+k}{p}\right) \left(\frac{y-k}{p}\right).$$

Each $(y - k)$ is uniquely represented by a $y' \pmod{p}$, so we can substitute to get that

$$p + \left(\frac{-1}{p}\right) \sum_{y'=0}^{p-1} \left(\frac{y'}{p}\right) \left(\frac{y'+2k}{p}\right).$$

From here we can another substitution of $a = 2k$ because each value modulo p is divisible by 2. Therefore, we obtain

$$p + \left(\frac{-1}{p}\right) \sum_{y'=0}^{p-1} \left(\frac{y'}{p}\right) \left(\frac{y'+a}{p}\right).$$

By Proposition 4.4 we have that

$$p + \left(\frac{-1}{p}\right) \sum_{y'=0}^{p-1} \left(\frac{y'}{p}\right) \left(\frac{y'+a}{p}\right) = p - \left(\frac{-1}{p}\right).$$

□

This means that if we randomly choose x and y mod p, the value of $x^2 + y^2$ is equally likely to be each of the $p - 1$ nonzero values mod p. It follows that $\left(\frac{x^2+y^2}{p}\right)$ is equally likely to be 1 and -1.

Corollary 4.7. *The total number of Pythagorean triples mod p is p^2.*

Proof. We add the number of solutions (x, y) to $x^2 + y^2 \equiv 0$ from Proposition 4.2 to the number of solutions (x, y, z) to $x^2+y^2 \equiv z^2 \pmod{p}$ for each nonzero z from Theorem 4.6. We get

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

□

It follows that a random (x, y, z) have probability $\frac{1}{p}$ of being a Pythagorean triple.

5 Acknowledgements

We used *An Introduction to the Thoery of Numbers* by G.H. Hardy as our number theory reference throughout the program. We would like to thank PRIMES Circle for creating this incredible opportunity, and Peter Haine for proof-reading our work. We'd also like to thank our parents for their support. But most of all, a huge shout-out to our mentor, Maya Sankar, for dealing with our outrageous theorem labels and for her dedication in teaching us number theory with patience and enthusiasm.