The Sum of Two Squares Problem

Number Theory and Geometry by Álvaro Lozano-Robledo

Giancarlo Stabler

University of Connecticut

Fall 2024

Context

This semester, I worked through a couple of the later chapters in *Number Theory and Geometry* by Álvaro Lozano-Robledo.

This presentation will focus on content from "Chapter 12: Circles, Ellipses, and The Sum of Two Squares Problem".

Main Question

When can an integer be written as the sum of two squares?

Motivation

There are plenty of reasons we may want to know when an integer is a sum of two squares. This problem has applications relating to finding Pythagorean triples and lattice points on a plane.

Motivation

There are plenty of reasons we may want to know when an integer is a sum of two squares. This problem has applications relating to finding Pythagorean triples and lattice points on a plane.

The problem of determining if an integer is a sum of two squares is equivalent to determining if a circle with integer radius has integral points.

Motivation

There are plenty of reasons we may want to know when an integer is a sum of two squares. This problem has applications relating to finding Pythagorean triples and lattice points on a plane.

The problem of determining if an integer is a sum of two squares is equivalent to determining if a circle with integer radius has integral points.

Less obviously, this turns out to be equivalent to determining if a circle has rational points.

An explanation of some useful notation and terminology.

Integral and Rational Points

Integral and Rational Points

An integral or rational point on a curve C is a point $(x, y) \in C$ such that $x, y \in \mathbb{Z}$ or $x, y \in \mathbb{Q}$, respectively.

Integral and Rational Points

An integral or rational point on a curve C is a point $(x, y) \in C$ such that $x, y \in \mathbb{Z}$ or $x, y \in \mathbb{Q}$, respectively.

Example of an Integral Point

The circle $C_{25} : x^2 + y^2 = 25$ has an integral point at $(3, 4)$.

Integer Congruence

Integer Congruence

Two integers a, b are congruent mod n (denoted $a \equiv b \bmod n$) if $a - b = nm$ for some integer n.

Integers that are congruent mod n have the same remainder when divided by n.

Integer Congruence

Integer Congruence

Two integers a, b are congruent mod n (denoted $a \equiv b \bmod n$) if $a - b = nm$ for some integer n.

Integers that are congruent mod n have the same remainder when divided by n.

Example

We can see that $13 \equiv 5 \bmod 8$ and $9 \equiv 2 \bmod 7$.

Quadratic Residue

Quadratic Residue

An integer q is a quadratic residue mod n if $q \equiv x^2 \bmod n$ for some integer x.

Quadratic Residue

Quadratic Residue

An integer q is a quadratic residue mod n if $q \equiv x^2 \bmod n$ for some integer x.

Example

The numbers 0, 1, and 4 are the quadratic residues mod 5, since $0 \equiv 0^2 \bmod 5$, $1 \equiv 1^2 \equiv 4^2 \bmod 5$ and $4 \equiv 2^2 \equiv 8^2 \bmod 5$.

The numbers 2, 3 are quadratic non-residues mod 5, because there do not exist $x \in \mathbb{Z}$ such that $x^2 \equiv 2, 3 \bmod 5$.

Legendre Symbol

Legendre Symbol

Let $p > 2$ be an odd prime and let a be an integer. The *Legendre Symbol* is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Legendre Symbol

Legendre Symbol

Let $p > 2$ be an odd prime and let a be an integer. The *Legendre Symbol* is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

Example

From the previous example, since 4 is a quadratic residue mod 5, it follows that $\left(\frac{4}{5}\right) = 1$.
Since 2 is a quadratic non-residue mod 5, it follows that $\left(\frac{2}{5}\right) = -1$.

Preliminary Results

We will need to see some lemmas and preliminary results that will be used in main result.

Lemma (10.3.4)

Let $p > 2$ be a prime and let $a, b \in \mathbb{Z}$ relatively prime to p. Then

1. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$. *In particular* $\left(\frac{b^2}{p}\right) = 1$.
2. *If* $a \equiv b \bmod p$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Lemma 12.1.7

Lemma (12.1.7)

Let m, n be integers such that $m = a^2 + b^2$ and $n = c^2 + d^2$, for some $a, b, c, d \in \mathbb{Z}$. Then we have,

$$mn = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2.$$

Lemma 12.1.7

Lemma (12.1.7)

Let m, n be integers such that $m = a^2 + b^2$ and $n = c^2 + d^2$, for some $a, b, c, d \in \mathbb{Z}$. Then we have,

$$mn = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2.$$

Numerical Example

Take $25 = 3^2 + 4^2$ and $13 = 2^2 + 3^2$, then

$$325 = (25)(13) = (3 \cdot 2 + 4 \cdot 3)^2 + (3 \cdot 3 - 4 \cdot 2)^2 = 18^2 + 1^2.$$

Lemma (12.1.9)

Let n be an integer such that $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, and suppose q is a prime such that $q \equiv 3 \bmod 4$.

1. *If $q \mid n$, then $q \mid a$ and $q \mid b$. In particular, $q^2 \mid n$.*
2. *If $q \mid n$, then q appears to an even power in the prime factorization of n.*

Theorem 12.1.5

Theorem (12.1.5)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \mod 4$.

Theorem 12.1.5

Theorem (12.1.5)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \bmod 4$.

Proof ($\Rightarrow$): Suppose p is an odd prime such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Theorem 12.1.5

Theorem (12.1.5)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \bmod 4$.

Proof ($\Rightarrow$): Suppose p is an odd prime such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Notice that $\gcd(ab, p) = 1$. If $p \mid a$, then $p \mid (p - a^2) = b^2$, so $p \mid b$ which would imply $p^2 \mid (a^2 + b^2) = p$ a contradiction.

Theorem (12.1.5)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \bmod 4$.

Proof ($\Rightarrow$): Suppose p is an odd prime such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Notice that $\gcd(ab, p) = 1$. If $p \mid a$, then $p \mid (p - a^2) = b^2$, so $p \mid b$ which would imply $p^2 \mid (a^2 + b^2) = p$ a contradiction.

We have that a and b are units mod p, and therefore invertible.

Theorem (12.1.5)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \bmod 4$.

Proof ($\Rightarrow$): Suppose p is an odd prime such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Notice that $\gcd(ab, p) = 1$. If $p \mid a$, then $p \mid (p - a^2) = b^2$, so $p \mid b$ which would imply $p^2 \mid (a^2 + b^2) = p$ a contradiction.

We have that a and b are units mod p, and therefore invertible.

Recall that $a^2 + b^2 \equiv 0 \bmod p$, so $a^2 \equiv -b^2 \bmod p$. It follows then that $(ab^{-1})^2 \equiv -1 \bmod p$.

Therefore, -1 is a square mod p, and by Lemma 10.3.4, we know $(p-1)/2$ is even. Thus, $p \equiv 1 \bmod 4$.

$\square$

Proof of Theorem 12.1.5 Continued...

Proof ($\Leftarrow$): Assume that $p \equiv 1 \bmod 4$, so Lemma 10.3.4 shows -1 is a square mod p for some $s \in \mathbb{Z}$ such that $s^2 \equiv -1 \bmod p$.

Proof of Theorem 12.1.5 Continued...

Proof ($\Leftarrow$): Assume that $p \equiv 1 \bmod 4$, so Lemma 10.3.4 shows -1 is a square mod p for some $s \in \mathbb{Z}$ such that $s^2 \equiv -1 \bmod p$.

Let $\lfloor \sqrt{p} \rfloor$ be the *floor* of $\sqrt{p}$, and consider the set of integers

$$S = \{(x, y) : 0 \leq x, y < \lfloor \sqrt{p} \rfloor\}.$$

We claim that there are two distinct pairs (x_1, y_1) and (x_2, y_2) in S such that $sx_1 - y_1 \equiv sx_2 - y_2 \bmod p$.

Proof of Theorem 12.1.5 Continued...

Proof ($\Leftarrow$): Assume that $p \equiv 1 \bmod 4$, so Lemma 10.3.4 shows -1 is a square mod p for some $s \in \mathbb{Z}$ such that $s^2 \equiv -1 \bmod p$.

Let $\lfloor \sqrt{p} \rfloor$ be the *floor* of $\sqrt{p}$, and consider the set of integers

$$S = \{(x, y) : 0 \leq x, y < \lfloor \sqrt{p} \rfloor\}.$$

We claim that there are two distinct pairs (x_1, y_1) and (x_2, y_2) in S such that $sx_1 - y_1 \equiv sx_2 - y_2 \bmod p$.

If all possible values of $sx - y$ for $(x, y) \in S$ were distinct mod p, then there would be $(\lfloor \sqrt{p} \rfloor + 1)^2$ distinct values mod p in S, but

$$(\lfloor \sqrt{p} \rfloor + 1)^2 > (\sqrt{p})^2 = p.$$

Proof of Theorem 12.1.5 Continued...

Proof continued: Since there are exactly p distinct values in the set of representatives mod p, this is a contradiction.

Therefore, there must be two distinct pairs (x_1, y_1) and (x_2, y_2) such that $sx_1 - y_1 \equiv sx_2 - y_2$.

Equivalently, we can say that $sx_0 \equiv y_0$ mod p where $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$. Since $(x_1, y_1) \neq (x_2, y_2)$, we know that at most one of x_0 or y_0 must be non-zero.

It follows from $sx_0 \equiv y_0$ that $s^2x_0^2 \equiv y_0^2$, and therefore we have

$$-x_0^2 \equiv y_0^2 \text{ mod } p \quad \Rightarrow \quad x_0^2 + y_0^2 \equiv 0 \text{ mod } p.$$

Proof of Theorem 12.1.5 Continued...

Proof continued: Since there are exactly p distinct values in the set of representatives mod p, this is a contradiction.

Therefore, there must be two distinct pairs (x_1, y_1) and (x_2, y_2) such that $sx_1 - y_1 \equiv sx_2 - y_2$.

Equivalently, we can say that $sx_0 \equiv y_0$ mod p where $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$. Since $(x_1, y_1) \neq (x_2, y_2)$, we know that at most one of x_0 or y_0 must be non-zero.

It follows from $sx_0 \equiv y_0$ that $s^2 x_0^2 \equiv y_0^2$, and therefore we have

$$-x_0^2 \equiv y_0^2 \bmod p \quad \Rightarrow \quad x_0^2 + y_0^2 \equiv 0 \bmod p.$$

Thus, $x_0^2 + y_0^2$ is some non-zero integer multiple of p, and

$$0 < x_0^2 + y_0^2 \leq (\lfloor\sqrt{p}\rfloor)^2 + (\lfloor\sqrt{p}\rfloor)^2 = 2(\lfloor\sqrt{p}\rfloor)^2 < 2(\sqrt{p})^2 = 2p.$$

Proof of Theorem 12.1.5 Continued...

Proof continued: Since there are exactly p distinct values in the set of representatives mod p, this is a contradiction.

Therefore, there must be two distinct pairs (x_1, y_1) and (x_2, y_2) such that $sx_1 - y_1 \equiv sx_2 - y_2$.

Equivalently, we can say that $sx_0 \equiv y_0 \bmod p$ where $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$. Since $(x_1, y_1) \neq (x_2, y_2)$, we know that at most one of x_0 or y_0 must be non-zero.

It follows from $sx_0 \equiv y_0$ that $s^2 x_0^2 \equiv y_0^2$, and therefore we have

$$-x_0^2 \equiv y_0^2 \bmod p \quad \Rightarrow \quad x_0^2 + y_0^2 \equiv 0 \bmod p.$$

Thus, $x_0^2 + y_0^2$ is some non-zero integer multiple of p, and

$$0 < x_0^2 + y_0^2 \leq (\lfloor\sqrt{p}\rfloor)^2 + (\lfloor\sqrt{p}\rfloor)^2 = 2(\lfloor\sqrt{p}\rfloor)^2 < 2(\sqrt{p})^2 = 2p.$$

There is one multiple of p strictly between 0 and $2p$. Therefore, $x_0^2 + y_0^2 = p$, so p is a sum of two squares.

$\square$

Main Result

Main Result

Theorem (12.1.10)

Let $n > 1$ be a natural number. The circle $C_n : x^2 + y^2 = n$ has an integral point if and only if every prime divisor p of n with $p \equiv 3 \bmod 4$ appears to an even power in the prime factorization of n.

Equivalently, n can be be written as a sum of two squares if and only if the square-free part of n is not divisible by any prime p of the form $p \equiv 3 \bmod 4$.

Proof of Main Result

We will begin by showing that if the circle $C_n : x^2 + y^2 = n$ has an integral point, then any prime factors $q \equiv 3 \bmod 4$ of n appear to an even power in the prime factorization of n.

Proof (⇒): Suppose first that C_n has an integral point, i.e.,

$$n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}.$$

Also suppose that n has a prime divisor $q \equiv 3 \bmod 4$.

Then, by Lemma 12.1.9, the prime q appears to an even power in the prime factorization of n.

□

Proof of Main Result Continued...

Now we will show that if all prime $p \equiv 3 \bmod 4$ show up with even power in the prime factorization of n, then C_n has an integral point.

Proof ($\Leftarrow$): Assume that for all primes $p \equiv 3 \bmod 4$, p shows up in an even power in the prime factorization of n.

We can split n such that $n = n'm^2$, where n' is square-free, and we can assume that n' is not divisible by any prime p. Then

$$n' = 2^{\ell} p_1 p_2 \cdots p_t,$$

where ℓ is 0 or 1, and $p_i \equiv 1 \bmod 4$ are prime for $0 \leq i \leq t$.

Note that $2 = 1^2 + 1^2$, and so by Theorem 12.1.5, it follows that $p_i = a_i^2 + b_i^2$ for $a_i, b_i \in \mathbb{Z}$.

Proof of Main Result Continued...

Proof continued: Since we have shown that the factors of n' are individually sums of two squares, we can repeatedly apply Lemma 12.1.7, which lets us find that $n' = a'^2 + b'^2$ for some $a', b' \in \mathbb{Z}$. Thus,

$$n = n'm^2 = (a'^2 + b'^2)m^2 = (a'm)^2 + (b'm)^2.$$

Therefore, n is a sum of two squares.

Since $n = (a'm)^2 + (b'm)^2$, the circle C_n has integral point, namely $(a'm, b'm)$.

$\square$

Thank you!

Questions?