Primes Which Are a Sum of Two Squares

Scott Kirila

June 25, 2020

UNIVERSITY OF EXETER

Overview

Question. When can a prime number be written as a sum of two positive squared integers?

We begin with some numerical observations:

✓ $2 = 1^2 + 1^2$

✗ $3 = 1^2 + 2$, but 2 is not a perfect square ($\sqrt{2}$ is irrational!)

✓ $5 = 1^2 + 2^2$

✗ $7 = 1^2 + 6 = 2^2 + 3$

✗ $11 = 1^2 + 10 = 2^2 + 7 = 3^2 + 2$

✓ $13 = 2^2 + 3^2$

✓ $17 = 1^2 + 4^2$

Let's assume that q is an odd prime, so $q \equiv 1 \pmod{2}$.

What about modulo 4?

An odd number is congruent to 1 or 3 modulo 4, so $q = 1 + 4N$ or $q = 3 + 4N$.

From our list, only odd primes congruent to 1 modulo 4 are a sum of squares. **Coincidence?**

Let's look at squares modulo 4:

$$\begin{aligned} 0^2 &\equiv 0 \pmod 4 \\ 1^2 &\equiv 1 \pmod 4 \\ 2^2 &\equiv 0 \pmod 4 \\ 3^2 &\equiv 1 \pmod 4. \end{aligned}$$

So any sum of two squares, $m^2 + n^2$, is

$$m^2 + n^2 \equiv \begin{cases} 0^2 + 0^2 \pmod 4 \\ 0^2 + 1^2 \pmod 4 \\ 1^2 + 1^2 \pmod 4 \end{cases} \equiv \begin{cases} 0 \pmod 4 \\ 1 \pmod 4 \\ 2 \pmod 4 \end{cases}$$

- If $q = m^2 + n^2$, then $q \equiv 0, 1, 2 \pmod 4$.

- Since q is prime, it is not divisible by 4.

- If $q \equiv 2 \pmod 4$, then q is divisible by 2 (since then $p = 2 + 4k$). Hence $q = 2$.

Conclusion? Either $q = 1^2 + 1^2$, or $q \equiv 1 \pmod 4$.

So any odd prime which is a sum of two squares must be congruent to 1 (mod 4).

Is the converse true? If q is an odd prime which is congruent to 1 (mod 4), must it be a sum of two squares?

The quick answer is: YES!

Theorem[1]

An odd prime number is a sum of two squared integers **if and only if** it is congruent to 1 (mod 4).

But first we need a middle step to help bridge the gap.

[1] Attributed to Girard* (1625), Fermat* (1640), and Euler (1750)

Observation. If $q = m^2 + n^2$, then q does not divide n.

- Why not? Otherwise q divides $m^2 = q - n^2$.
- Since q is prime and divides $m^2 = m \cdot m$, it actually divides m.
- This means that q^2 divides $m^2 + n^2 = q$, which is impossible!

So $n \not\equiv 0 \pmod{q}$.

In particular, it has a multiplicative inverse[2], n^*, modulo q:

$$n \cdot n^* \equiv 1 \pmod{q}.$$

[2] Infinity of Primes II, slide 6

Since $q = m^2 + n^2$, we have

$$\begin{aligned} m^2 + n^2 &\equiv 0 \pmod{q} \\ m^2 &\equiv -n^2 \pmod{q} \\ m^2 \cdot (n^*)^2 &\equiv -1 \pmod{q} \\ (m \cdot n^*)^2 &\equiv -1 \pmod{q}, \end{aligned}$$

and so -1 is a square modulo q.

What we know so far:

$$\begin{tikzcd} \boxed{q = m^2 + n^2} \arrow[r] \arrow[dr] & \boxed{-1 \equiv \square \pmod{q}} \arrow[d, dashed] \\ & \boxed{q \equiv 1 \pmod{4}} \end{tikzcd}$$

Regarding that dashed arrow on the previous slide:

- If -1 is a square modulo q, then there is an integer j with $j^2 \equiv -1 \pmod{q}$.
- Squaring both sides, we get $j^4 \equiv 1 \pmod{q}$.
- Alex's *rolling pin* argument[3] can be used here to show that 4 divides $q - 1$.
- But this is the same as saying $q \equiv 1 \pmod{4}$

[3] Infinity of Primes II, Slide 11. Note that 4 is the size of $\{1, j, j^2, j^3\}$

Fun fact: using what we know from the previous slide, we can show that there are infinitely many primes[4] congruent to 1 (mod 4).

- Suppose Q is the largest prime congruent to 1 (mod 4).
- If q is a prime dividing $(2 \cdot 3 \cdot 5 \cdots Q)^2 + 1$, then

$$(2 \cdot 3 \cdot 5 \cdots Q)^2 \equiv -1 \pmod{q}.$$

- This means that $q \equiv 1 \pmod{4}$.
- But q must also be larger than Q, since $q \neq 2, 3, 5, \ldots, Q$. Contradiction!

---

[4] Compare this proof to Infinity of Primes I, Slide 14 (Euclid).

Here's how we'll finish proving the Theorem:

$$\begin{tikzcd}
\boxed{q = m^2 + n^2} \arrow[dr] & \boxed{-1 \equiv \square \pmod{q}} \arrow[l, dashed, swap, "\text{Step 2}"] \\
 & \boxed{q \equiv 1 \pmod{4}} \arrow[u, dashed, swap, "\text{Step 1}"]
\end{tikzcd}$$

From now on, let $G = \{1, 2, \ldots, q-1\}$.

So for any $a \in G$, there is an $a^* \in G$ with

$$a \cdot a^* \equiv 1 \pmod{q}.$$

Step 1

If q is a prime number congruent to $1 \pmod 4$, then -1 is a square modulo q.

Proof. We collect the elements of G into subsets of the form

$$E_a := \{a,\ a^*,\ q-a,\ q-a^*\}.$$

This set has size 4, *unless* some of the elements are repeated.

Take $a = 1$ for example, which is its own multiplicative inverse.

Then $E_1 = \{1, q-1\}$.

Since $q \neq 2$, we see that E_1 has size 2, not 4.

Proof of Step 1

Let's count the size of $E_a = \{a, a^*, q - a, q - a^*\}$ for $a \neq 1$.

First check if $a = a^*$.

- If $a = a^*$, then $a^2 \equiv 1 \pmod{q}$.
- Substract 1 from both sides, so $(a-1)(a+1) \equiv 0 \pmod{q}$.
- Since $a \neq 1$, $a - 1$ has a multiplicative inverse modulo q.
- Multiply both sides by $(a-1)^*$ to get $a + 1 \equiv 0 \pmod{q}$.
- Therefore $a \equiv -1 \pmod{q}$, and so $a = q - 1$.

Proof of Step 1

So $E_1 = E_{q-1}$ has size 2, and this covers the case where $a^* = a$.

Another possibility is $a = q - a$, which means that $q = 2a$.

✗ But q is odd, so this can't happen.

The next case[5] is when $a = q - a^*$

- Rearranging terms, this also means that $a^* = q - a$.
- Since $a \neq 1, q-1$, we see that $a \neq a^*$. And so

  $$E_a = \{a, a^*, q-a, q-a^*\} = \{a, a^*\}$$

  has size 2.
- Most importantly, we also have $a^2 \equiv -1 \pmod{q}$.

[5] Note: in this case, a cannot be 1 or $q-1$.

Proof of Step 1

To summarize:

1. $E_1 = E_{q-1} = \{1, q-1\}$ has size 2.
2. If $a^2 \equiv -1 \pmod{q}$, then $E_a = \{a, a^*\}$ has size 2.
3. For all other a, each element is distinct; so E_a has size 4.

Of course, G doesn't always have elements of the second type. For example:

- ✓ If $q = 101$, then $(10)^2 \equiv -1 \pmod{q}$.
- ✗ If $q = 7$, then $a^2 \equiv 1, 2, 4 \pmod{q}$.

Proof of Step 1

This splits up G into subsets of size 2 and 4:

- If -1 is not a square modulo q, then there is precisely one subset of size 2: $\{1, q-1\}$.
- There are two subsets of size 2 otherwise.
- Everything else is containing in a subset of size 4.

Let c_2 count the number of such subsets of size 2, so $c_2 = 1$ or 2.

Let c_4 be the number of distinct subsets E_a of size 4.

Proof of Step 1

Then we have

$$2c_2 + 4c_4 = q - 1.$$

Reducing modulo 4, we get

$$q \equiv 1 + 2c_2 \pmod 4.$$

From this, we see that

$$c_2 = \begin{cases} 1 & \text{if } q \equiv 3 \pmod 4, \\ 2 & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

This proves Step 1, since $q \equiv 1 \pmod 4$ implies there are two subsets of size 2. $\square$

Proof of Step 2

Step 2

If -1 is a square modulo q, then q is a sum of two squared integers.

Proof. Let $j \in G$ be such that $j^2 \equiv -1 \pmod{q}$.

- Consider $a - jb$ for integers a, b with $0 \leq a, b < \sqrt{q}$.
- **Key point:** there are $> \sqrt{q}$ choices for each of a and b (because we include 0).
- So there are *more than* $(\sqrt{q})^2 = q$ pairs (a, b).

Let's look at $a - jb \pmod{q}$.

There are q possible values for $a - jb \pmod{q}$.

Pigeonhole principle: If you sort $> q$ items[6] into q bins[7], one of the bins must contain (at least) two items.

- So there are two *different* pairs (a, b) and (a', b') with

$$a - jb \equiv a' - jb' \pmod{q}.$$

- Rearranging, we get

$$a - a' \equiv j(b - b') \pmod{q}.$$

- Set $x = a - a'$ and $y = b - b'$, so

$$x \equiv jy \pmod{q}.$$

[6] $a - jb$
[7] its value modulo q

Proof of Step 2

Squaring both sides, we get

$$\begin{aligned} x^2 &\equiv j^2 y^2 \pmod{q} \\ &\equiv -y^2 \pmod{q}. \end{aligned}$$

So q divides $x^2 + y^2$. Almost there!

- Since $0 \leq a, a' < \sqrt{q}$, we have $|x| = |a - a'| < \sqrt{q}$
- So $x^2 < q$, and the same is true for y^2.
- Then $x^2 + y^2 < 2q$ and is divisible by q.
- Hence $x^2 + y^2 = 0$ or q.

Proof of Step 2

If $x^2 + y^2 = 0$, then $x = 0$ and $y = 0$.

- But then $a = a'$ and $b = b'$.
- We used the pigeonhole principle to find *distinct* pairs (a, b) and (a', b'), so this can't happen.

And we're done, because the only possibility left is that $x^2 + y^2 = q$. ∎

Combining Steps 1 and 2 proves the rest of the Theorem.

Lemma[8]

Since q is prime, we have $(q-1)! \equiv -1 \pmod{q}$.

Proof. Recall that 1 and $q-1$ are the only elements of G which are their own inverse.

Write the remaining $2Q := q-3$ elements as $a_1, a_1^*, \dots, a_Q, a_Q^*$.

Then

$$\begin{aligned}(q-1)! &= (q-1)\prod_{k=1}^{Q} a_k a_k^* \\ &\equiv (-1)\prod_{k=1}^{Q} 1 \pmod{q}.\end{aligned}$$

This is $\equiv -1 \pmod{q}$, so we're done. □

[8] Part of Wilson's Theorem

Now note that

$$\begin{aligned}(q-1)! &= 1 \cdots \left(\frac{q-1}{2}\right) \cdot \left(\frac{q+1}{2}\right) \cdots (q-1) \\ &= 1 \cdots \left(\frac{q-1}{2}\right) \cdot \underbrace{\left(q - \frac{q-1}{2}\right) \cdots (q-1)}_{\frac{q-1}{2} \text{ terms}} \\ &\equiv 1^2 \cdots \left(\frac{q-1}{2}\right)^2 \cdot (-1)^{\frac{q-1}{2}} \pmod{q}.\end{aligned}$$

But $\frac{q-1}{2}$ is even. So, after applying the Lemma, we see that

$$-1 \equiv \left[\left(\frac{q-1}{2}\right)!\right]^2 \pmod{q}.$$

■

A 'one-line' proof

Let $\mathbb{N}$ denote the positive integers. Consider the set

$$S := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = q\}.$$

For example, if $q = 1 + 4N$, then $(1, 1, N) \in S$.

- Define a map $f : S \to S$ by $f(x, y, z) = (x, z, y)$.
- Since $x^2 + 4yz = x^2 + 4zy$, this map is well-defined[9].
- If we apply f twice, then we get back our original input:

  $$f(f(x, y, z)) = (x, y, z).$$

  Such a function is called an *involution*.

[9] That is, if $(x, y, z) \in S$, then $f(x, y, z) \in S$

A 'one-line' proof

Remark. A *fixed point* of f is any point for which $f(x, y, z) = (x, y, z)$.

But this means that $y = z$, and so $x^2 + 4y^2 = q$.

That is, $q = x^2 + (2y)^2$, which is exactly what we want!

So it suffices to show that f has at least one fixed point.

To do this, we define another involution[10]:

$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & \text{if } x < y-z, \\ (2y-x, y, x-y+z) & \text{if } y-z < x < 2y, \\ (x-2y, x-y+z, y) & \text{if } x > 2y. \end{cases}$$

Let's find its fixed points, i.e. where $g(x,y,z) = (x,y,z)$

- If $x < y - z$, then

$$\begin{aligned} x + 2z &= x, \\ z &= y, \\ y - x - z &= z. \end{aligned}$$

✗ The only possibility is $x = y = z = 0$, but this doesn't satisfy $x < y - z$.

✗ Similarly for $x > 2y$.

[10] **Exercise.** Check this!

A 'one-line' proof

If $y - z < x < 2y$, then

$$\begin{aligned} 2y - x &= x, \\ y &= y, \\ x - y + z &= z. \end{aligned}$$

So $x = y$, and $x, y, z > 0$.

- Thus $(x, x, z) \in S$ is a fixed point of g.
- But $(x, x, z) \in S$ satisfies

$$q = x^2 + 4xz = x(x + 4z).$$

- Since q is prime, $x = 1$ and hence $z = N$.
- So g has a single fixed point $(1, 1, N)$ when $q = 1 + 4N$.

A 'one-line' proof

We're practically done!

- Since g has exactly one fixed point, S must have an odd number of elements.
- Why? Pair each element $(x, y, z) \in S$ with its buddy $g(x, y, z)$.
- The only element that can't be paired is $(1, 1, N)$.
- $\#S = 2(\text{ number of pairs}) + 1$, so $\#S$ is odd.

A 'one-line' proof

Fact. An involution, f, on a set of odd size must have a fixed point.

- Why? The same reasoning as on the previous slide.
- We pair up each (x, y, z) with $f(x, y, z)$

So f has a fixed point, as desired. $\blacksquare$

This proof is due to Don Zagier (1990), building upon work of Roger Heath-Brown (1984).