Definition
An integer $n$ is a sum of two squares if $n = x^2 + y^2$ for two non-negative integers $x, y$.

Recall, a Jacobian pair:
Then, let $p$ be a prime in $\mathbb{Z}$. Then the prime factorization of $p$ in $\mathbb{Z}[i]$ is as follows:
- If $p = 2$, then $2 = (1+i)(1-i)$
- If $p = 1 \pmod{4}$, then $p = (m+n) \cdot (m-n) \cdot (m-n)i$ for irreducibles $m, n \in \mathbb{Z}$
- If $p = 3 \pmod{4}$, then $p$ is irreducible in $\mathbb{Z}[i]$. 

In particular:

**Corollary**

Any prime $p$ satisfying $p = 1 \pmod{4}$ is a sum of two squares.

$p = (m+n i)(m-n i)$ in $\mathbb{Z}[i]$ for integers $m,n$

$p = m^2 + n^2$.

What about the reverse direction?

Prop Let $n$ be an odd integer and assume $n$ is a sum of two squares.

If we have $n = x^2 + y^2, \quad 1 \leq x, y \leq 2$

Reduce mod 4:

$x \equiv 2 \pmod{4}$

$n = x^2 + y^2 \equiv 4 \pmod{4}$

$xy \in \{0, 1, 2, 3\}$

$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 0 \pmod{4}, \quad 3^2 = 1 \pmod{4}$
So \( x^2 + y^2 \leq 30.13 \)

\[ x, y \in \mathbb{Z} \]

\[ x^2 + y^2 \leq 30.13 \]

\[ \Rightarrow x \in \mathbb{R} \cap \sqrt{30.13} \]

\[ \bar{n} = \sqrt{30.13} \]

\[ \bar{n} = 5.47 \]

\[ \bar{n} = 5.47 \]

\[ \Rightarrow n, k \text{ even} \]

Since \( n \) is odd, \( n \equiv 1 \mod 4 \).

Putting these facts together.

**Theorem (Fermat's Sum of Two Squares)**

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

In fact, we can relive the above theorem to give a criterion for when an integer is a sum of squares. Any integer is a sum of squares.

**Definition** The integer \( n \in \mathbb{Z} \) is called a Gaussian prime if \( n \) is prime.
Lemma

Let \( \pi \) be a Gaussian prime. Then \( \pi \) is a Gaussian prime.

If \( \pi \in \mathbb{Z} + \mathbb{Z}i \) and suppose \( \pi \mid \alpha \beta \). Then \( \pi \mid \alpha \) or \( \pi \mid \beta \).

\( \Rightarrow \pi \mid \alpha \) or \( \pi \mid \beta \).

Thus, \( \pi \mid \alpha \) or \( \pi \mid \beta \).

Characterization of all Gaussian Primes

Up to associates, the only Gaussian primes are the following:

1. \( \pm 1 \), \( \pm i \),
2. For each prime \( p = 1 \pmod{4} \) there are two Gaussian primes \( \pi \) and \( \overline{\pi} \) of norm \( p \),
3. Each prime \( q = 3 \pmod{4} \) is a
Gaussian prime of norm $a^2$.

By the prop proved by Jonathan (prime factorization of integers in $\mathbb{Z}[i]$) we know the (at 2 care) are prime. Since $N(\pm i) = 2$ is prime so $\pm i$ is a prime. So everything in the above list is a Gaussian prime.

Now let $\alpha$ be a Gaussian prime. Then $N(\alpha)$ is not a unit $\Rightarrow N(\alpha) \neq 1$ so there is a prime $p | N(\alpha)$ ($p \in \mathbb{Z}$).

By what we know about prime factorization of the integer $p$ in $\mathbb{Z}[i]$, there exists a Gaussian prime $\alpha_1 p$ where $\alpha_1$ is a prime factor of an integer in $\mathbb{Z}$, and $\alpha_1$ is in the above list.

But $\pi | N(\alpha)$ so $\pi(\alpha)$ or $\overline{\pi}(\alpha)$
i.e. \( \pi \mid x \) or \( \overline{\pi} \mid x \) so \( x \) is associate to something in \( \mathbb{E} \).

Definition

A positive integer \( n \) is \underline{square-free} if no prime factor \( p \) in the prime factorization of \( n \) occurs with exponent larger than 1 in the prime factorization of \( n \).

It follows from the prime factorization that if \( n = a b^2 \) for \( a, b \in \mathbb{Z} \) we can write \( n \) with a square-free factorization.

Theorem

Let \( n \) be a positive integer and let \( n = a b^2 \) with a square-free factorization and a sum of two squares if and only if no prime \( q \) divides \( q \).
Suppose no prime \( q \) with \( q \equiv 3 \pmod{8} \) divides \( a \). Then for any prime \( p \) of \( \mathcal{O} \), there exists a Gaussian prime \( \pi_p \) of norm \( p \) (by the factorization of Gaussian primes).

Consider \( b \prod_{p|\alpha} \pi_p \) the product of all such primes.

Then \( N(b \prod_{p|\alpha} \pi_p) = N(b) \prod_{p|\alpha} N(\pi_p) \)

(norm is multiplicative)

\[ = b^2 \prod_{p|\alpha} p \]

\[ = b^2 a \]

\[ = n \]

Thus if we write the Gaussian integer

\[ b \prod_{p|\alpha} \pi_p = x + iy \]

then \( N(x + iy) = x^2 + y^2 \) so \( n \) is a sum of two squares.
For the other direction, suppose

\[ n = x^2 + y^2 \] is a sum of two squares

\[ n = (x + iy)(x - iy) \]

Suppose \( q \equiv 3 \pmod{4} \) is an integer prime dividing \( n \). From what we have seen \( q \) is a Gaussian prime \( \Rightarrow q \mid (x + iy) \) or \( q \mid (x - iy) \Rightarrow q \mid x \) and \( q \mid y \).

So \( n = x^2 + y^2 \) \( \Rightarrow q^2 \mid n \)

i.e., if \( n = a b^2 \), a square free, then \( q \mid b \).

Further \( q \mid x \) and \( q \mid y \) so

\[
\frac{n^2}{q^2} = a \left( \frac{b}{q} \right)^2 = \left( \frac{x}{q} + \frac{iy}{q} \right) \left( \frac{x}{q} - \frac{iy}{q} \right)
\]

is a sum of two squares.
The claim thus follows by induction on \( p \).

How many ways can you represent an odd number as a sum of squares? As a warm-up,

**Lemma.** Let \( a, b \in \mathbb{Z} \) with \( a \geq 0, b \geq 0 \). Suppose \( a \) and \( b \) can be written as a sum of squares. Then \( ab \) can be written as a sum of squares in at least two ways.

If
\[
\begin{align*}
a &= x^2 + y^2 \\
b &= z^2 + w^2
\end{align*}
\]

then
\[
ab = (x^2 + y^2)(z^2 + w^2) = x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2.
\]

Also,
\[
ab = x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 = (x^2z^2 + 2xyzw + y^2w^2).
\]
\[ + (k^2 \omega^2 - 2kxy \omega + y^2 \omega^2) \]

or
\[ + (k^2 \omega^2 - 2kxy \omega + y^2 \omega^2) \]

\[ + (k^2 \omega^2 + 2kxy \omega + y^2 \omega^2) \]

\[ = \{(x^2 + y^2 \omega)^2 + (x\omega - y\omega)^2 \}
+ (x\omega + y\omega)^2 \]