We will complete the proof of Theorem 31.

**Theorem 31** An integer \( n \) is a sum of two squares if and only if \( n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} x^2 \), where \( p_i \equiv 1 \pmod{4} \) are primes in \( \mathbb{Z} \) and \( x \in \mathbb{Z} \).

**Proof:**

Anthony has shown that if \( n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} x^2 \), where \( p_i \equiv 1 \pmod{4} \) are primes in \( \mathbb{Z} \) and \( x \in \mathbb{Z} \) then \( n \) is a sum of two squares.

Conversely suppose that \( p = x^2 + y^2 \) is a sum of two squares. If \( x \) and \( y \) are both odd, then

\[
x^2 + y^2 = 2 \left( \frac{(x + y)^2}{2} + \frac{(x - y)^2}{2} \right)
\]

and so \( x^2 + x^2 \) is twice a sum of two squares. If the two squares involved are both odd, we can repeat the process until we have \( x^2 + y^2 \) in the form \( 2^a \) times an odd number which is a sum of two squares.

Suppose then that we have \( n = x^2 + y^2 \) an odd number.

If \( d = (x, y) \) then \( x = dX \) and \( y = dY \) where \( (X, Y) = 1 \) and \( n = x^2 + y^2 = d^2(X^2 + Y^2) \), and \( X^2 + Y^2 \) is odd, with \( (X, Y) = 1 \).

Now \( X^2 + Y^2 \) is not divisible by any prime \( p \equiv 3 \pmod{4} \). For if \( X^2 + Y^2 \equiv 0 \pmod{p} \), then \( X^2 \equiv -Y^2 \pmod{p} \) and, dividing by \( Y \), modulo \( p \) we have \( (XY^{-1})^2 \equiv -1 \pmod{p} \). But there is no \( \sqrt{-1} \) in \( \mathbb{Z}_p \), when \( p \equiv 3 \pmod{4} \), by Theorem something or other. (You need to check that \( X \) and \( Y \) are not 0 \pmod{p} but this is easy because \( (X, Y) = 1 \).) Hence \( X^2 + Y^2 \) is a product of odd primes \( p \equiv 1 \pmod{4} \) and \( n = 2^a d^2 p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \), where \( p_i \equiv 1 \pmod{4} \). This completes the proof.

**Example**

\[
65 = (1^2 + 2^2)(2^2 + 3^2)
\]

\[
= (1.2 - 2.3)^2 + (1.3 + 2.2)^2
\]

\[
= 4^2 + 7^2 \text{ while also}
\]

\[
65 = (2.2 - 1.3)^2 + (2.3 + 1.2)^2
\]

\[
= 1^2 + 8^2.
\]

**Remark.** In general a prime \( p \equiv (mod \ 4) \) can be written in essentially only one way as a sum of two squares (up to order and signs). This corresponds to the uniqueness of factorisation theorem in \( \mathbb{Z}[i] \). I won’t prove that here.

I want to begin this week of lectures with Pierre de Fermat 1601 - 1665. He wrote in his copy of his book of Diophantus on the solution of equations in integers that he had found a proof of
the fact that \( x^n + y^n = z^n \) has no solutions in non-zero integers \( x, y, z \) if \( n > 2 \), but the margin was not large enough for him to be able to include the proof of this. Then he died! It has since been shown that he was correct by an English mathematician Wiles in Cambridge. It is almost certain that Fermat did not have a proof. It is also almost certain that the proof he thought he had was the so-called Method of Descent. I want to give us two examples of this in action here. The first is the only actual proof we have from Fermat. Though he was a great mathematician he did not publish any of his proofs - indeed there was no opportunity for him to do so because there were no mathematical journals at the time in which he could publish his work.

**Theorem 32 Fermat** There are no non-zero integers \( x, y, y \) such that \( x^4 + y^4 = z^4 \).

**Proof.**

We’ll show that there are no non-zero integers \( x, y, z \) such that \( x^4 + y^4 = z^2 \) ... a stronger assertion obviously. We can obviously change the signs of any of the terms \( x, y, z \) and so we can assume that we are solving the equation in positive integers.

Among all positive triples \( x, y, z \) with \( x^4 + y^4 = z^2 \), choose one with \( z \) minimal. So suppose we have that triple and \( x^4 + y^4 = z^2 \). Clearly \( x, y, z \) are pairwise co-prime and without loss we can assume that \( x \) is odd, \( y \) is even and \( z \) is odd.

Then we can apply the solution of Pythagoras to find integers \( a, b \) such that

\[
\begin{align*}
x^2 &= a^2 - b^2 \\
y^2 &= 2ab \\
z &= a^2 + b^2.
\end{align*}
\]

Note that \( (a, b) = 1 \), because if \( p|a \) and \( p|b \) then \( p|a^2 - b^2 = x^2 \) and \( p|x \) while \( p|y^2 \) and \( p|y \). But \( (x, y) = 1 \). So \( a \) and \( b \) are not both even. But they’re also not both odd, because then \( z = a^2 + b^2 \) is even. Hence one of \( a, b \) is even and one is odd.

Now \( x^2 = a^2 - b^2 \) and so \( x^2 + b^2 = a^2 \) and \( (x, a, b) \) is another basic Pythagorean triple. Since one of \( a \) and \( b \) is even and one is odd, only \( a \) can be odd because \( a^2 = b^2 + x^2 \) is even only if both \( x \) and \( b \) are even. Hence \( a \) is odd and \( b \) is even.

Hence there exists \( \alpha, \beta \) with \( \alpha > \beta > 0 \) and \( (\alpha, \beta) = 1 \) such that

\[
\begin{align*}
x &= \alpha^2 - \beta^2 \\
b &= 2\alpha\beta \\
a &= \alpha^2 + \beta^2.
\end{align*}
\]

The equation \( y^2 = 2ab \) is the killer equation here. We have

\[
y^2 = 2ab = 2(\alpha^2 + \beta^2).2\alpha\beta.
\]

But \( \alpha, 4\beta, (\alpha^2 + \beta^2) \) are pairwise co-prime and so by Lemma 17 they are all squares. So \( \alpha = X^2, \beta = Y^2 \) and \( \alpha^2 + \beta^2 = Z^2 \).

Hence

\[
\alpha^2 + \beta^2 = X^4 + Y^4 = Z^2.
\]
Since clearly $\alpha < b$, $\alpha^2 < b^2$ and $\beta^2 < a$ so $Z^2 = \alpha^2 + \beta^2 < b^2 + a \leq b^2 + a^2 = z \leq z^2$. This contradicts the minimality of $z^2$ and so there is no solution of $x^4 + y^4 = z^2$ in non-zero positive integers.

This completes the proof.

**TRANSFINITE NUMBERS**