We are now ready to describe Fermat's Descent Procedure for writing any prime

$$p \equiv 1 \pmod 4$$

as a sum of two squares. As explained above, the idea is to begin with some multiple $Mp$ which is a sum of two squares and, by some clever manipulations, find a smaller multiple which is also a sum of two squares. To help you understand the various steps, we will do an example side-by-side with the general procedure. The Descent Procedure, in all its glory, is on display in the following table. Be sure to go over the procedure step-by-step before proceeding with the text.

To complete the task of writing 881 as a sum of two squares, we repeat the descent procedure starting with the equation

$$107^2 + 2^2 = 13 \cdot 881.$$

This gives

| $p = 881$ | $p$ any prime $\equiv 1 \pmod p$ |
|---|---|
| $107^2 + 2^2 = 13 \cdot 881$<br>$3 \equiv 107 \pmod{13}$<br>$2 \equiv 2 \pmod{13}$ | $A^2 + B^2 = Mp$<br>$u \equiv A \pmod M$<br>$v \equiv B \pmod M$ |
| $3^2 + 2^2 = 13 \cdot 1$ | $u^2 + v^2 = Mr$ |
| $(3^2 + 2^2)(107^2 + 2^2) = 13^2 \cdot 1 \cdot 881$ | $(u^2 + v^2)(A^2 + B^2) = M^2rp$ |
| Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$. | |
| $(3 \cdot 107 + 2 \cdot 2)^2 + (2 \cdot 107 - 3 \cdot 2)^2 = 13^2 \cdot 881$<br>$325^2 + 208^2 = 13^2 \cdot 881$ | $(uA + vB)^2 + (vA - uB)^2 = M^2rp$ |
| Divide by $13^2$.<br>$25^2 + 16^2 = 881$ | Divide by $M^2$.<br>$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp$ |

This second application of the descent procedure has given us the solution to our original problem,

$$881 = 25^2 + 16^2.$$

Of course, for a small number such as 881 it might have been easier to solve $881 = a^2 + b^2$ by trial-and-error, but as soon as $p$ becomes large, the descent procedure is definitely more efficient. In fact, each time the descent procedure is applied, the multiple of $p$ is at least cut in half.

**Descent Procedure**

| $p = 881$ | $p$ any prime $\equiv 1 \pmod p$ |
|---|---|
| Write<br>$387^2 + 1^2 = 170 \cdot 881$<br>with $170 < 881$ | Write<br>$A^2 + B^2 = Mp$<br>with $M < p$ |
| Choose numbers with<br>$47 \equiv 387 \pmod{170}$<br>$1 \equiv 1 \pmod{170}$<br>$-\frac{170}{2} \le 47, 1 \le \frac{170}{2}$ | Choose numbers $u$ and $v$ with<br>$u \equiv A \pmod M$<br>$v \equiv B \pmod M$<br>$-\frac{1}{2}M \le u, v \le \frac{1}{2}M$ |
| Observe that<br>$47^2 + 1^2 \equiv 387^2 + 1^2$<br>$\equiv 0 \pmod{170}$ | Observe that<br>$u^2 + v^2 \equiv A^2 + B^2$<br>$\equiv 0 \pmod M$ |
| So we can write<br>$47^2 + 1^2 = 170 \cdot 13$<br>$387^2 + 1^2 = 170 \cdot 881$ | So we can write<br>$u^2 + v^2 = Mr$<br>$A^2 + B^2 = Mp$<br>(for some $1 \le r < M$) |
| Multiply to get<br>$(47^2 + 1^2)(387^2 + 1^2)$<br>$= 170^2 \cdot 13 \cdot 881$ | Multiply to get<br>$(u^2 + v^2)(A^2 + B^2) = M^2rp$ |
| Use the identity $(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$. | |
| $(47 \cdot 387 + 1 \cdot 1)^2 + (1 \cdot 387 - 47 \cdot 1)^2 = 170^2 \cdot 13 \cdot 881$<br>$\underbrace{18190}_{\text{each divisible by } 170}^2 + \underbrace{340}_{\text{each divisible by } 170}^2 = 170^2 \cdot 13 \cdot 881$ | $\underbrace{(uA + vB)}_{\text{each divisible by } M}^2 + \underbrace{(vA - uB)}_{\text{each divisible by } M}^2 = M^2rp$ |
| Divide by $170^2$.<br>$\left(\frac{18190}{170}\right)^2 + \left(\frac{340}{170}\right)^2 = 13 \cdot 881$<br>$107^2 + 2^2 = 13 \cdot 881$<br>This gives a smaller multiple of 881 written as a sum of two squares. | Divide by $M^2$.<br>$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp$<br>This gives a smaller multiple of $p$ written as a sum of two squares. |
| Repeat the process until $p$ itself is written as a sum of two squares. | |

In order to show that the descent procedure actually works, there are five assertions which we need to verify. At the first step we need to find numbers $A$ and $B$ with

(i) $A^2 + B^2 = Mp$ and $M < p$.

To do this, we take a solution to the congruence

$$x^2 \equiv -1 \pmod{p}$$

with $1 \le x < p$. Quadratic Reciprocity tells us that there is a solution, since we are assuming the $p \equiv 1 \pmod 4$, and then $A = x$ and $B = 1$ will have the property that $A^2 + B^2$ is divisible by $p$. Further,

$$M = \frac{A^2 + B^2}{p} \le \frac{(p-1)^2 + 1^2}{p} = p - \frac{p-2}{p} < p.$$

In the second step of the descent procedure we chose numbers $u$ and $v$ satisfying

$$u \equiv A \pmod{M}, \quad v \equiv B \pmod{M}, \quad \text{and} \quad -\frac{1}{2} \le u, v \le \frac{1}{2}M.$$

We then observed that

$$u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \pmod{M},$$

so $u^2 + v^2$ is divisible by $M$, say $u^2 + v^2 = Mr$. The remaining four statements we need to check are:

(ii) $r \ge 1$.
(iii) $r < M$.
(iv) $uA + vB$ is divisible by $M$.
(v) $vA - uB$ is divisible by $M$.

We will check them in reverse order. To verify (v) we compute

$$vA - uB \equiv B \cdot A - A \cdot B \equiv 0 \pmod{M}.$$

Similarly, for (iv) we have

$$uA + vB \equiv A \cdot A + B \cdot B \equiv Mp \equiv 0 \pmod{M}.$$

For (iii) we use the fact that $u$ and $v$ are between $-M/2$ and $M/2$ to estimate

$$r = \frac{u^2 + v^2}{M} \le \frac{(M/2)^2 + (M/2)^2}{M} = \frac{M}{2} < M.$$

Notice this actually shows that $r \le M/2$, so every time the descent procedure is used, the multiple of $p$ is at least cut in half.

Finally, to show that (ii) is true, we need to check that $r \neq 0$. So we will assume that $r = 0$ and see what happens. Well, if $r = 0$, then $u^2 + v^2 = 0$, so we must have $u = v = 0$. But $u \equiv A \pmod{M}$ and $v \equiv B \pmod{M}$, so $A$ and $B$ are divisible by $M$. This implies that $A^2 + B^2$ is divisible by $M^2$. But $A^2 + B^2 = Mp$, so we see that $M$ must divide the prime $p$. We also know that $M < p$, so it must be true that $M = 1$. This means that $A^2 + B^2 = p$ and we're already done writing $p$ as a sum of two squares! Thus, either (ii) is true, or else we already had $A^2 + B^2 = p$ and there was no reason to use the descent procedure in the first place.

This completes the verification that the descent procedure always works, so we have now finished proving both parts of the Sum of Two Squares Theorem (For Primes).

**Exercise 25.3.** Use the descent procedure twice, starting from the equation

$$557^2 + 55^2 = 26 \cdot 12049,$$

to write the prime 12049 as a sum of two squares.

*Aside on Sums of Squares and Complex Numbers*

The identity

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2$$

which expresses the product of sums of two squares as a sum of two squares has been very useful, and we will find further uses for it in the next chapter. You may well have wondered from whence this identity comes. The answer lies in the realm of complex numbers, that is, numbers of the form

$$z = x + iy,$$

where $i$ is a square root of $-1$. Two complex numbers can be multiplied together in the usual way as long as you remember to replace $i^2$ by $-1$. Thus,

$$\begin{aligned}(x_1 + iy_1)(x_2 + iy_2) &= x_1x_2 + ix_1y_2 + iy_1x_2 + i^2y_1y_2 \\ &= (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).\end{aligned}$$

Complex numbers also have absolute values,

$$|z| = |x + iy| = \sqrt{x^2 + y^2}.$$

This idea is to imagine the number $z = x + iy$ as corresponding to the point $(x, y)$ in the plane, and then $|z|$ is just the distance from $z$ to the origin $(0, 0)$. Now our identity comes from the fact that

"the absolute value of a product is the product of the absolute values."

In other words, $|z_1 z_2| = |z_1| \cdot |z_2|$. Writing this out in terms of $x$'s and $y$'s gives

$$\begin{aligned}
\big|(x_1 + iy_1)(x_2 + iy_2)\big| &= |x_1 + iy_1| \cdot |x_2 + iy_2| \\
\big|(x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2)\big| &= |x_1 + iy_1| \cdot |x_2 + iy_2| \\
\sqrt{(x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2} &= \sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2}.
\end{aligned}$$

If we square both sides of this last equation, we get exactly our identity (where $x_1 = u$, $y_1 = v$, $x_2 = A$, and $y_2 = -B$).

There is a similar identity, involving sums of four squares, which is due to Euler,

$$\begin{aligned}
&(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\
&\quad = (aA + bB + cC + dD)^2 + (aB - bA - cD + dC)^2 \\
&\qquad + (aC + bD - cA - dB)^2 + (aD - bC + cB - dA)^2.
\end{aligned}$$

This complicated identity is related to the theory of quaternions[†] in the same way that our identity is related to complex numbers. It is an unfortunate fact that there is no analogous identity for sums of three squares, and indeed the question of writing numbers as a sum of three squares is much more difficult than the same problem for either two or four squares.

[†] Quaternions are numbers of the form $a + ib + jc + kd$, where $i$, $j$, and $k$ are three different square roots of $-1$ satisfying strange multiplication rules such as $ij = -ji$.

CHAPTER 20

# Which Numbers Are Sums of Two Squares?

In the last chapter we gave a definitive answer to the question of which primes can be written as a sum of two squares. We now take up the same question for arbitrary numbers. Part of our strategy, which can be summed up in three words, has a long and glorious history:

"Divide and Conquer!"

Of course, "Divide" doesn't mean division per se. Rather, it means to break the problem up into pieces of manageable size, and then "Conquer" means we need to solve each piece. But these two steps, which may suffice for warfare, will have to be followed by a third step, namely fitting the pieces back together. This unification step will use the identity from the last chapter which expresses a product of sums of squares as a sum of squares:

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2. \qquad (*)$$

Here, then, is our step-by-step strategy for expressing a number $m$ as a sum of two squares.

| | |
|---|---|
| Divide: | Factor $m$ into a product of primes $p_1 p_2 \cdots p_r$. |
| Conquer: | Write each prime $p_i$ as a sum of two squares. |
| Unify: | Use the identity $(*)$ repeatedly to write $m$ as a sum of two squares. |

We know from the previous chapter exactly when the Conquer step will work, since we know that a prime $p$ is a sum of two squares if and only if either $p = 2$ or $p \equiv 1 \pmod 4$. For example, to write 10 as a sum of two squares, we factor $10 = 2 \cdot 5$, write 2 and 5 as sums of two squares,

$$2 = 1^2 + 1^2 \qquad \text{and} \qquad 5 = 2^2 + 1^2,$$