For example, let $p = 557$. We have $2^{139} \equiv 118 \pmod{557}$, and $118^2 \equiv -1 \pmod{557}$, so we let $u = 118$. The Euclidean algorithm is

$$\begin{aligned} 557 &= 4 \cdot 118 + 85 \\ 118 &= 1 \cdot 85 + 33 \\ 85 &= 2 \cdot 33 + 19 \\ 33 &= 1 \cdot 19 + 14 \\ 19 &= 1 \cdot 14 + 5 \\ 14 &= 2 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

The first two remainders less than $\sqrt{557}$ are 19 and 14. We have $19^2 + 14^2 = 557$.

This algorithm is essentially due to Charles Hermite and Joseph Serret (independently) in 1848. Improvements were made by Henry Smith and John Brillhart. For the proof that the algorithm works, see F. W. Clarke, W. N. Everitt, L. L. Littlejohn, and S. J. R. Vorster, "H. J. S. Smith and the Fermat two squares theorem," *Amer. Math. Monthly* 106 (1999), no. 7, 652-665.

CHECK YOUR UNDERSTANDING:

1. Using the fact that $22^2 \equiv -1 \pmod{97}$, write 97 as a sum of two squares.

12.2 Sums of Four Squares

The amazing fact that every positive integer is a sum of four squares was probably known to Diophantus, but the first proof is due to Lagrange in 1770. As in the case of sums of two squares, the key case is that of primes.

Theorem 12.5. *(Lagrange) Every positive integer is a sum of four squares.*

Proof. To start, we prove the theorem when $n = p$ is prime. We need an analogue of Lemma 12.2.

Lemma 12.6. *Let p be prime. Then there are integers u, v such that $u^2 + v^2 + 1 \equiv 0 \pmod{p}$.*

Proof. The case $p = 2$ is trivial (let $u = 1$ and $v = 0$), so assume p is odd. There are $(p-1)/2$ nonzero squares mod p by Exercise 24 in Chapter 5, or by Exercise 31 in Chapter 8. Since 0 is also a square, there are $1 + (p-1)/2 = (p+1)/2$ squares mod p. If we take each square and subtract it from -1, we get $(p+1)/2$ numbers of the form $-1-v^2 \pmod{p}$. We have two sets: the squares with $(p+1)/2$ elements and the numbers $-1 - v^2$ with $(p+1)/2$ elements. There are only p congruence classes mod p, and $(p+1)/2 + (p+1)/2 > p$. Therefore, the two sets must overlap. This means that $u^2 \equiv -1 - v^2 \pmod{p}$ for some u, v, which says that $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. □

Example. As an example of the lemma, let $p = 11$. The squares mod 11 are

$$\{0, 1, 4, 9, 5, 3\}$$

and the numbers of the form $-1 - v^2$ are

$$\{-1, -2, -5, -10, -6, -4\} \equiv \{10, 9, 6, 1, 5, 7\} \pmod{11}.$$

Note that 1 is in both sets, which means that $1^2 \equiv -1 - 3^2$, or $1^2 + 3^2 + 1 \equiv 0 \pmod{11}$.

We now use a two-dimensional analogue of Thue's Lemma.

Lemma 12.7. *Let $n \geq 2$ and let a, b, c, d be integers. There exist w, x, y, z with at least one of y, z nonzero such that*

$$0 \leq |w| \leq \sqrt{n}, \quad 0 \leq |x| \leq \sqrt{n}, \quad 0 \leq |y| \leq \sqrt{n}, \quad 0 \leq |z| \leq \sqrt{n}$$

and

$$w \equiv ay + bz \pmod{n}, \quad x \equiv cy + dz \pmod{n}.$$

Proof. Make a list of all pairs $(i - ak - b\ell, j - ck - d\ell)$ with $0 \leq i, j, k, \ell \leq \sqrt{n}$. Since we are including 0, there are $\lfloor \sqrt{n} \rfloor + 1 > \sqrt{n}$ values of each of i, j, k, ℓ. Therefore, there are more than $(\sqrt{n})^4 = n^2$ pairs. There are

only n^2 pairs of congruence classes mod n, so we must have two pairs that are congruent mod n:

$$i_1 - ak_1 - b\ell_1 \equiv i_2 - ak_2 - b\ell_2 \pmod{n},$$
$$j_1 - ck_1 - d\ell_1 \equiv j_2 - ck_2 - d\ell_2 \pmod{n},$$

where $(i_1, j_1, k_1, \ell_1) \neq (i_2, j_2, k_2, \ell_2)$. Let

$$w = i_1 - i_2, \quad x = j_1 - j_2, \quad y = k_1 - k_2, \quad z = \ell_1 - \ell_2.$$

Then w, x, y, z satisfy the inequalities and the congruences of the lemma. It remains to show that at least one of y, z is nonzero.

If $y = z = 0$, then $w \equiv x \equiv 0 \pmod{n}$. Since $|w|, |x| \leq \sqrt{n}$, we must have $x = w = 0$. But $w = x = y = z = 0$ implies that $(i_1, j_1, k_1, \ell_1) = (i_2, j_2, k_2, \ell_2)$, contrary to the choice of these 4-tuples. This completes the proof of the lemma. □

We now return to the proof of Lagrange's theorem. We start by showing that if p is a prime number then p is a sum of four squares. Let u, v be as in Lemma 12.6. By Lemma 12.7, there exist w, x, y, z, with at least one nonzero and with all less than $\sqrt{p}$ (they cannot equal $\sqrt{p}$ because $\sqrt{p}$ is not an integer) such that

$$w \equiv uy + vz \pmod{p}, \quad x \equiv vy - uz \pmod{p}.$$

Then

$$\begin{aligned} w^2 + x^2 + y^2 + z^2 &\equiv (uy + vz)^2 + (vy - uz)^2 + y^2 + z^2 \\ &\equiv (u^2 + v^2 + 1)y^2 + (v^2 + u^2 + 1)z^2 \\ &\equiv 0 + 0 \equiv 0 \pmod{p} \end{aligned}$$

(the cross terms with yz cancel). Moreover,

$$0 < w^2 + x^2 + y^2 + z^2 < (\sqrt{p})^2 + (\sqrt{p})^2 + (\sqrt{p})^2 + (\sqrt{p})^2 = 4p.$$

The only multiples of p between 0 and $4p$ are p, $2p$, and $3p$, so

$$w^2 + x^2 + y^2 + z^2 = p, 2p, \text{ or } 3p.$$

If $w^2 + x^2 + y^2 + z^2 = p$, we're done. We need to treat the cases where the sum equals $2p$ or $3p$.

Suppose that $w^2+x^2+y^2+z^2 = 2p$. Then either all of w, x, y, z are odd, or two of them are odd, or all are even (if one of them is odd or three of them are odd, then $w^2+x^2+y^2+z^2$ is odd, so does not equal $2p$). By rearranging the order, we can assume that

$$w \equiv x \pmod 2, \quad y \equiv z \pmod 2.$$

Then $(w \pm x)/2$ and $(y \pm z)/2$ are integers, and

$$\begin{aligned}\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 \\ = \frac{w^2+x^2+y^2+z^2}{2} = p\end{aligned}$$

(expand it out; a lot of cross terms cancel), so we obtain p as the sum of four squares.

Now suppose that $w^2+x^2+y^2+z^2 = 3p$. As in the case $2p$, we want to manipulate this to get p as a sum of four squares. If $p = 3$, then $3 = 1^2+1^2+1^2+0^2$, so we know 3 is a sum of four squares. Therefore, we assume that $p \neq 3$. If $w \equiv x \equiv y \equiv z \equiv 0 \pmod 3$, then $w^2+x^2+y^2+z^2 \equiv 0 \pmod 9$, while $3p \not\equiv 0 \pmod 9$, contradiction. Therefore, at least one of w, x, y, z is nonzero mod 3. Since $0^2 \equiv 0 \pmod 3$ and $(\pm 1)^2 \equiv 1 \pmod 3$, it is easy to see that the only way for $w^2+x^2+y^2+z^2$ to add up to $3p$ is for three of w, x, y, z to be $\pm 1 \pmod 3$ and one of them to be $0 \pmod 3$. By rearranging the order, if necessary, we can assume that $z \equiv 0 \pmod 3$. By changing the signs of w, x, y, if necessary, we may assume that $w \equiv x \equiv y \equiv 1 \pmod 3$. Let

$$\begin{aligned}x_1 = (w+x+y)/3, \quad x_2 = (w-x+z)/3, \\ x_3 = (-w+y-z)/3, \quad x_4 = (x-y+z)/3.\end{aligned}$$

Then x_1, x_2, x_3, x_4 are integers. A straightforward but lengthy calculation shows that

$$x_1^2+x_2^2+x_3^2+x_4^2 = (w^2+x^2+y^2+z^2)/3 = p.$$

Therefore, p is a sum of four squares in all cases.

To prove that every positive integer is a sum of four squares, we need

to extend Equation(12.1) to four squares. Here's the relevant identity:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)&\\ = (ae-bf-cg-dh)^2+(af+be+ch-dg)^2&\\ +(ag+ce+df-bh)^2+(ah+de+bg-cf)^2.&\quad (12.2)\end{aligned}$$

If you don't believe this, multiply it out and check it. To see how it can be deduced using quaternions, see Exercise 4. However, this identity was discovered before quaternions were discovered!

Every prime is a sum of four squares, and Equation (12.2) says that products of sums of four squares are sums of four squares. Since every integer $n \geq 2$ is a product of primes, each such n is a sum of four squares. Finally, $1 = 1^2+0^2+0^2+0^2$, so 1 is also a sum of four squares. This completes the proof. □

In 1834, Carl Gustav Jacobi gave a formula for the number of ways of writing n as a sum of four squares. Let $S(n)$ be the sum of all the divisors d of n that are not multiples of 4. For example, when $n = 20$ we have

$$S(20) = 1 + 2 + 5 + 10 = 18.$$

Then there are exactly $8S(n)$ ways of writing n as a sum of four squares, where different orders of the summands are regarded as different and the squares can be squares of positive or negative numbers. So, for example, we can write

$$\begin{aligned}1 &= 0^2+0^2+0^2+1^2\\ &= 0^2+0^2+0^2+(-1)^2\\ &= 0^2+0^2+1^2+0^2\\ &= 0^2+0^2+(-1)^2+0^2\\ &= 0^2+1^2+0^2+0^2\\ &= 0^2+(-1)^2+0^2+0^2\\ &= 1^2+0^2+0^2+0^2\\ &= (-1)^2+0^2+0^2+0^2.\end{aligned}$$

Note that $8S(1) = 8$, which is the number of ways we've written 1 as a sum of four squares.