5. Sums of more than two squares

Theorem 5.1. *The natural number n is a sum of three squares,*

$$n = x^2 + y^2 + z^2$$

if and only if n is not of the form $4^t(8k+7)$.

Proof. We only prove the easy direction. Suppose that n is a sum of three squares.

Note that a square is congruent to 0, 1 or 4, modulo 8. The sum of three squares is then congruent to 0, 1, 2, 3, 4, 5, or 6, modulo 8. Thus no number of the form $8k+7$ is a sum of three squares.

Suppose that n is divisible by 4. Then x, y and z are all even. It follows that $n/4$ is also a sum of three squares. Thus no number of the form $4^t(8k+7)$ is a sum of three squares. □

One reason it is hard to figure out which numbers are the sums of three squares is that there is no easy formula involving products of three squares. Indeed, 3 is a sum of four squares, 5 is a sum of three squares but 15 is not.

We now turn to the problem of four squares. First note that

Lemma 5.2. *If x_1, x_2, x_3, x_4, y_1, y_2, y_3 and y_4 are all real then*

$$\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\
&\quad = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_1 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\
&\quad + (x_1y_2 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x24y_3 - x_3y_2)^2.
\end{aligned}$$

In particular the set of natural numbers which are the sum of four squares is closed under multplication.

Proof. Of course one can simply expand both sides and check we get the same terms (so that the result holds in any commutative ring).

One can also use the quaternions. If

$$\alpha = x_1 + x_2i + x_3j + x_4k$$

then

$$\bar{\alpha} = x_1 - x_2i - x_3j - x_4k$$

and

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = \alpha\bar{\alpha} = N(\alpha).$$

Note that

$$\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}.$$

We have

$$\begin{aligned} N(\alpha\beta) &= \alpha\beta\overline{\alpha\beta} \\ &= \alpha\beta\bar{\beta}\bar{\alpha} \\ &= \alpha N(\beta)\bar{\alpha} \\ &= N(\beta)\alpha\bar{\alpha} \\ &= N(\alpha)N(\beta). \end{aligned}$$ □

Theorem 5.3. *Every natural number is the sum of four squares.*

Proof. As 1 is the sum of four squares, (5.2) implies that it is enough to show that every prime is a sum of four squares.

The idea is to solve the congruence

$$x^2 + y^2 + z^2 + t^2 \equiv 0 \mod p$$

and at the same time place some bounds on x, y, z and t.

The trick is to first find a and b such that

$$a^2 + b^2 \equiv -1 \mod p.$$

In other words, we have to solve the equation

$$x^2 + y^2 + 1 \equiv 0 \mod p.$$

This is easy if $p = 2$. If p is odd then let x and y range independently over the integers 0, 1, 2, ..., $(p-1)/2$. We check that x^2 and $-(1+y^2)$ are distinct. Suppose that $i^2 = j^2 \mod p$. As

$$i^2 - j^2 = (i - j)(j + j)$$

is divisible by p, it follows that either $i - j$ or $i + j$ is divisible by p. As

$$i + j < p,$$

it follows that $i = j$. Thus we get

$$\begin{aligned} \frac{p+1}{2} + \frac{p+1}{2} &= p + 1 \\ &> p, \end{aligned}$$

numbers so that two of them must coincide, modulo p, which is to say we can solve the equations.

Pick a and b such that $a^2 + b^2 \equiv -1 \mod p$. By (1.1) we may solve the equations

$$\begin{aligned} az + bt &\equiv x \mod p \\ bz - at &\equiv y \mod p, \end{aligned}$$

where x, y, z and t not all zero and further

$$\max(|x|, |y|, |z|, |t|) < \sqrt{p} + \epsilon,$$

for any $\epsilon > 0$. Note that there are $r = 2$ equations and $s = 4$ unknowns and so if we take $\lambda_i = \sqrt{p} + \epsilon$ then

$$\lambda_1 \lambda_2 \lambda_3 \lambda_4 > p^2.$$

As $\sqrt{p}$ is not an integer, if we choose $\epsilon > 0$ small enough then we can ensure that

$$\max(|x|, |y|, |z|, |t|) < \sqrt{p}.$$

Note that

$$\begin{aligned} x^2 + y^2 &\equiv (az + bt)^2 + (bz - at)^2 \\ &= (a^2 + b^2)(z^2 + t^2) \\ &\equiv -(z^2 + t^2) \mod p. \end{aligned}$$

On the other hand

$$\begin{aligned} 0 &< x^2 + y^2 + z^2 + t^2 \\ &< p + p + p + p \\ &= 4p. \end{aligned}$$

Thus

$$x^2 + y^2 + z^2 + t^2 = Ap,$$

for some $A = 1$, 2 or 3.

If $A = 1$ then we are done. Suppose that $A = 2$. Possibly rearranging we may assume that $x \equiv y \mod 2$ in which case $z \equiv t \mod 2$. In this case

$$p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2,$$

so that p is a sum of squares.

Finally suppose that $A = 3$. The prime $p = 3$ has a representation

$$3 = 1^2 + 1^2 + 1^2 + 0^2.$$

So we may assume that $p \neq 3$. x^2 is congruent to 0 or 1 modulo 3. On the other hand, as

$$x^2 + y^2 + z^2 + t^2 = 3p,$$

it follows that

$$x^2 + y^2 + z^2 + t^2 \equiv 0 \mod 3.$$

Therefore at least one of x, y, z and t is divisible by 3. Suppose x is divisible by 3. Not all of them are divisible by 3 as otherwise the sum of the squares is divisible by 9, impossible. Thus all three of y, z and t are not divisible by 3, so that they are congruent to ± 1 modulo 3. Thus one of $\pm z$ and one of $\pm t$ are congruent to y modulo 3. Call these numbers z' and t'.

We have

$$p = \left(\frac{y + z' + t'}{3}\right)^2 + \left(\frac{x + z' - t'}{3}\right)^2 + \left(\frac{x - y + t'}{3}\right)^2 + \left(\frac{x + y - z'}{3}\right)^2,$$

so that p is a sum of squares. $\square$