# 6. Representation of integers as sums of two squares

Which $n \in \mathbb{Z}$ can be represented as a sum $n = x^2 + y^2$ for $x, y \in \mathbb{Z}$? Obviously need $n \geq 0$. Can clearly assume that $x$ and $y$ are nonnegative. We have $0 = 0^2 + 0^2$, $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, but no such representation for $n = 3$, 6 or 7.

**Important note:** $(2k)^2 \equiv 0 \pmod 4$, and $(2k+1)^2 = 8\binom{k+1}{2} + 1 \equiv 1 \pmod 8$ (and so certainly $\equiv 1 \pmod 4$).

## 6.1. The case $n = p$, prime.

Which primes are the sum of two squares?

**Theorem 6.1.** *An odd prime $p$ is a sum of two squares (of integers) iff $p \equiv 1 \pmod 4$.*

*Proof.* As $x^2, y^2 \equiv 0$ or $1 \pmod 4$, so $x^2 + y^2 \equiv 0$ or 1 or $2 \pmod 4$. Assuming $p = x^2 + y^2$, then as $p$ is odd, we have $p \equiv 1 \pmod 4$.

Conversely, assume $p \equiv 1 \pmod 4$, and, knowing that then $\left(\frac{-1}{p}\right) = 1$, take $r \in \mathbb{N}$ with $r^2 \equiv -1 \pmod p$. Define $f(u, v) = u + rv$ and $K = \lfloor \sqrt{p} \rfloor$. Note that

$$K < \sqrt{p} < K + 1, \tag{1}$$

as $\sqrt{p} \notin \mathbb{Z}$. Consider all pairs $(u, v)$ with $0 \leq u \leq K$ and $0 \leq v \leq K$. There are $(K+1)^2 > p$ such pairs, and so the multiset of all $f(u, v)$ for such $u, v$ has, by the Pigeonhole Principle, two such pairs $(u_1, v_1) \neq (u_2, v_2)$ for which $f(u_1, v_1) \equiv f(u_2, v_2) \pmod p$. Hence

$$\begin{aligned} u_1 + rv_1 &\equiv u_2 + rv_2 \pmod p \\ u_1 - u_2 &\equiv -r(v_1 - v_2) \pmod p \\ a &\equiv -rb \pmod p, \end{aligned}$$

say, where $a = u_1 - v_1$ and $b = v_1 - v_2$ are not both 0. Hence $a^2 \equiv -b^2 \pmod p$ as $r^2 \equiv -1 \pmod p$, so that $p \mid (a^2 + b^2)$. But $|a| \leq K$, $|b| \leq K$, giving

$$0 < a^2 + b^2 \leq 2K^2 < 2p.$$

So $a^2 + b^2 = p$. □

## 6.2. The general case.

We now look at what happens if a prime $\equiv -1 \pmod 4$ *divides* a sum of two squares.

**Proposition 6.2.** *Let $q \equiv 3 \pmod 4$ be prime, and $q \mid (x^2 + y^2)$. Then $q \mid x$ and $q \mid y$, so that $q^2 \mid (x^2 + y^2)$.*

*Proof.* Assume that it is not the case that both $x$ and $y$ are divisible by $q$, say $q \nmid x$. Then from $x^2 + y^2 \equiv 0 \pmod q$ we get $(yx^{-1})^2 \equiv -1 \pmod q$, contradicting $\left(\frac{-1}{q}\right) = -1$. □

**Proposition 6.3.** *If $n$ is a sum of two squares and $m$ is a sum of two squares then so is $nm$.*

*Proof.* If $n = a^2 + b^2$ and $m = c^2 + d^2$ then

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

□

(This identity comes from complex numbers:

$$(a + ib)(c + id) = ac - bd + i(ad + bc)$$

gives

$$|a + ib|^2 \cdot |c + id|^2 = |ac - bd + i(ad + bc)|^2$$

and hence the identity.)

**Corollary 6.4.** *If $n = A^2 \prod_i n_i$ where $A, n_i \in \mathbb{Z}$ and each $n_i$ is a sum of two squares, then so is $n$.*

*Proof.* Use induction on $i$ to get $n/A^2 = \prod_i n_i = a^2 + b^2$ say. Then $n = (Aa)^2 + (Ab)^2$. □

We can now state and prove our main result.

**Theorem 6.5** ( Fermat)**.** *Write $n$ in factorised form as*

$$n = 2^{f_2} \prod_{p \equiv 1 \pmod 4} p^{f_p} \prod_{q \equiv -1 \pmod 4} q^{g_q},$$

*where (of course) all the $p$'s and $q$'s are prime. Then $n$ can be written as the sum of two squares of integers iff all the $g_q$'s are even.*

*Proof.* If all the $g_q$ are even then $n = A^2 \times$(product of some $p$'s) and also $\times 2$ if $f_2$ is odd. So we have $n = A^2 \times \prod_i (a_i^2 + b_i^2)$ by Theorem 6.1 (using also $2 = 1^2 + 1^2$ if $f_2$ odd). Hence, by Corollary 6.4, $n$ is the sum of two squares.

Conversely, suppose $q \mid n = a^2 + b^2$, where $q \equiv -1 \pmod 4$ is prime. Let $q^k$ be the highest power of $q$ dividing both $a$ and $b$, so say $a = q^k a_1$, $b = q^k b_1$. Then

$$\frac{n}{q^{2k}} = a_1^2 + b_1^2.$$

Now $q \nmid \frac{n}{q^{2k}}$, as otherwise $q$ would divide both $a_1$ and $b_1$, by Prop. 6.2. Hence $q^{2k}$ is the highest power of $q$ dividing $n$, i.e., $g_q = 2k$ is even. Hence all the $g_q$'s are even. □

### 6.3. **Related results.**

**Proposition 6.6.** *If an integer $n$ is the sum of two squares of rationals then it's the sum of two squares of integers.*

*Proof.* Suppose that

$$n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

for some rational numbers $a/b$ and $c/d$. Then

$$n(bd)^2 = (da)^2 + (bc)^2.$$

Hence, by Thm 6.5, for every prime $q \equiv -1 \pmod 4$ with $q^i || n(bd)^2$, $i$ must be even. But then if $q^\ell || bd$ then $q^{i-2\ell} || n$, with $i - 2\ell$ even. Hence, by Thm 6.5 (in the other direction), $n$ is the sum of two squares of integers. □

**Corollary 6.7.** *A rational number $n/m$ is the sum of two squares of rationals iff $nm$ is the sum of two squares of integers.*

*Proof.* If $nm = a^2 + b^2$ for $a, b \in \mathbb{Z}$ then

$$\frac{n}{m} = \left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2.$$

Conversely, if

$$\frac{n}{m} = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$$

then

$$nm = \left(\frac{am}{b}\right)^2 + \left(\frac{cm}{d}\right)^2.$$

Hence, by Prop. 6.6, $nm$ is the sum of two squares of integers. □

6.4. **Finding all ways of expressing a rational as a sum of two rational squares.** Now let $h$ be a rational number that can be written as the sum of two squares of rationals. We can then describe *all* such ways of writing $h$.

**Theorem 6.8.** *Suppose that $h \in \mathbb{Q}$ is the sum of two rational squares: $h = s^2 + t^2$, where $s, t \in \mathbb{Q}$. Then the general solution of $h = x^2 + y^2$ in rationals $x, y$ is*

$$x = \frac{s(u^2 - v^2) - 2uvt}{u^2 + v^2} \qquad y = -\left(\frac{t(u^2 - v^2) + 2uvs}{u^2 + v^2}\right), \tag{2}$$

*where $u, v \in \mathbb{Z}$ not both zero.*

*Proof.* We are looking for all points $(x, y) \in \mathbb{Q}^2$ on the circle $x^2 + y^2 = h$. If $(x, y)$ is such a point, then for $x \neq s$ the chord through $(s, t)$ and $(x, y)$ has rational slope $(t - y)/(s - x)$.

Conversely, take a chord through $(s, t)$ of rational slope $r$, which has equation $y = r(x - s) + t$. Then for the intersection point $(x, y)$ of the chord and the circle we have

$$x^2 + (r(x - s) + t)^2 = h,$$

which simplifies to

$$x^2(1 + r^2) + 2rx(t - rs) + (r^2 - 1)s^2 - 2rst = 0,$$

using the fact that $t^2 - h = -s^2$. This factorises as

$$(x - s)((1 + r^2)x + 2rt + s(1 - r^2)) = 0.$$

For $x \neq s$ we have

$$x = \frac{s(r^2 - 1) - 2rt}{1 + r^2}$$

and

$$\begin{aligned} y &= t + r(x - s) \\ &= -\left(\frac{t(r^2-1)+2sr}{1+r^2}\right), \end{aligned}$$

on simplification. Finally, substituting $r = u/v$ gives (2). Note that $v = 0$ in (2) (i.e., $r = \infty$) gives the point $(r, -s)$. $\square$

**Corollary 6.9.** *The general integer solution $x, y, z$ of the equation $x^2 + y^2 = nz^2$ is*

$$(x, y, z) = (a(u^2 - v^2) - 2uvb, b(u^2 - v^2) + 2uva, u^2 + v^2),$$

*where $n = a^2 + b^2$, with $a, b, u, v \in \mathbb{Z}$, and $u, v$ arbitrary.*

(If $n$ is not the sum of two squares, then the equation has no nonzero solution, by Prop. 6.6.)

In particular, for $n = 1 = 1^2 + 0^2$, we see that the general integer solution to Pythagoras' equation $x^2 + y^2 = z^2$ is

$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2).$$

For a socalled *primitive* solution — one with $\gcd(x, y) = 1$ – choose $u, v$ with $\gcd(u, v) = 1$ and not both odd.

The same method works for $Ax^2 + By^2 + Cz^2 = 0$.

### 6.5. **Sums of three squares, sums of four squares.**

**Proposition 6.10.** *No number of the form $4^a(8k + 7)$, where $a$ is a nonnegative integer, is the sum of three squares (of integers).*

*Proof.* Use induction on $a$. For $a = 0$: Now $n^2 \equiv 0, 1$ or $4 \pmod 8$, so a sum of three squares is $\equiv 1$ or $1$ or $2$ or $3$ or $4$ or $5$ or $6 \pmod 8$, but $\not\equiv 7 \pmod 8$.

Assume result true for some integer $a \geq 0$. If $4^{a+1}(8k + 7) = n_1^2 + n_2^2 + n_3^2$ then all the $n_i$ must be even, and so $= 4(n_1'^2 + n_2'^2 + n_3'^2)$ say. But then $4^a(8k + 7) = n_1'^2 + n_2'^2 + n_3'^2$, contrary to the induction hypothesis. $\square$

In fact (won't prove)

**Theorem 6.11** (Legendre 1798, Gauss)**.** *All positive integers except those of the form $4^a(8k + 7)$ are the sum of three squares.*

Assuming this result, we can show

**Corollary 6.12** (Lagrange 1770)**.** *Every positive integer is the sum of four squares.*

*Proof.* The only case we need to consider is $n = 4^a(8k + 7)$. But then $n - (2^a)^2 = 4^a(8k + 6) = 2^{2k+1}(4k + 3)$, which (being exactly divisible by an odd power of 2) is not of the form $4^{a'}(8k' + 7)$, so is the sum of three squares. $\square$

## 7. Fermat's method of descent

Around 1640, Fermat developed a method for showing that an equation had no integer solutions. In essence, the method is as follows: assume that the equation *does* have a solution. Pick the 'smallest' (suitably defined) one. Use the assumed solution to construct a smaller solution, contradicting the fact that the one you started with was the smallest. This contradiction proves that there is in fact no solution. The technique is called *Fermat's method of descent.* It is, in fact, a form of strong induction. (Why?)

We illustrate the method with one example:

**Theorem 7.1.** *The equation*

$$x^4 + y^4 = z^2 \tag{3}$$

*has no solution in positive integers $x, y, z$.*

**Corollary 7.2** (Fermat's Last Theorem for exponent 4)**.** *The equation $x^4 + y^4 = z^4$ has no solution in positive integers $x, y, z$.*

*Proof of Theorem 7.1.* (From H. Davenport, *The higher arithmetic. An introduction to the theory of numbers*, Longmans 1952, p.162). Suppose that (3) has such a solution. Assume we have a solution with $|z|$ minimal. We can clearly assume that $z$ is positive and $\neq 1$, i.e., that $z > 1$. If $d = \gcd(x, y) > 1$ we can divide by $d^4$, replacing $x$ by $x/d$, $y$ by $y/d$ and $z$ by $z/d^2$ in (3), obtaining a solution with $|z|$ smaller. So we must have $\gcd(x, y) = 1$.

Now from Corollary 6.9 we know that

$$X^2 + Y^2 = Z^2$$

has general solution (with $\gcd(X, Y) = 1$), possibly after interchanging $X$ and $Y$ of

$$X = p^2 - q^2 \qquad Y = 2pq \qquad Z = p^2 + q^2,$$

where $p, q \in \mathbb{N}$ and $\gcd(p, q) = 1$, so

$$x^2 = p^2 - q^2 \qquad y^2 = 2pq \qquad z = p^2 + q^2.$$

As a square is $\equiv 0$ or $1 \pmod 4$, and $x$ is odd (because $\gcd(x, y) = 1$), we see that $p$ is odd and $q$ is even, say $q = 2r$. So

$$x^2 = p^2 - (2r)^2 \qquad \left(\frac{y}{2}\right)^2 = pr.$$

Since $\gcd(p, r) = 1$ and $pr$ is a square, we have $p = v^2$ and $r = w^2$ say, so

$$x^2 + (2w^2)^2 = v^4.$$

Note that, as $\gcd(p, q) = 1$, we have $\gcd(x, q) = 1 = \gcd(x, 2w^2)$. Hence applying Corollary 6.9 again

$$x = p_1^2 - q_1^2 \qquad 2w^2 = 2p_1q_1 \qquad v^2 = p_1^2 + q_1^2,$$

where $\gcd(p_1, q_1) = 1$ and not both are odd. Say $p_1$ odd, $q_1$ even. Thus $w^2 = p_1q_1$, giving $p_1 = v_1^2$, $q_1 = r_1^2$, say. Hence

$$v^2 (= p_1^2 + q_1^2) = v_1^4 + r_1^4,$$

which is another solution of (3)! But

$$v^2 = p = \sqrt{z - q^2} < \sqrt{z},$$

giving $v < z^{1/4}$, so certainly $v < z$ (as $z > 1$), contradicting the minimality of $z$. $\square$