Pythagorean triples and sums of squares

Robin Chapman

16 January 2004

1 Pythagorean triples

A Pythagorean triple (x, y, z) is a triple of positive integers satisfying $z^2 + y^2 = z^2$. If $g = \gcd(x, y, z)$ then $(x/g, y/g, z/g)$ is also a Pythagorean triple. It follows that if $g > 1$, (x, y, z) can be obtained from the "smaller" Pythagorean triple $(x/g, y/g, z/g)$ by multiplying each entry by g. It is natural then to focus on Pythagorean triples (x, y, z) with $\gcd(x, y, z) = 1$ — these are called primitive Pythagorean triples.

It will be useful to note a basic fact about primitive Pythagorean triples.

Theorem 1 *Let (x, y, z) be a primitive Pythagorean triple. Then* $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Proof Suppose $\gcd(x, y) > 1$. Then there is a prime p with $p \mid x$ and $p \mid y$. Then $z^2 = x^2 + y^2 \equiv 0 \pmod{p}$. As $p \mid z^2$ then $p \mid z$ and so $p \mid \gcd(x, y, z)$, contradicting (x, y, z) being a primitive Pythagorean triple. Thus $\gcd(x, y) = 1$.

The proofs that $\gcd(x, z) = 1$ and $\gcd(y, z) = 1$ are similar. $\square$

Considering things modulo 4 we can determine the parities of the numbers in a primitive Pythagorean triple.

Theorem 2 *If (x, y, z) is a primitive Pythagorean triple, then one of x and y is even, and the other odd. (Equivalently, $x + y$ is odd.) Also z is odd.*

Proof Note that if x is even then $x^2 \equiv 0 \pmod{4}$ and if x is odd then $x^2 \equiv 1 \pmod{4}$. If x and y are both odd then $x^2 \equiv y^2 \equiv 1 \pmod{4}$. Hence $z^2 \equiv x^2 + y^2 \equiv 2 \pmod{4}$, which is impossible. If x and y are both even, then $\gcd(x, y) \geq 2$ contradicting Theorem 1. We conclude that one of x and y is even, and the other is odd.

In any case, $z \equiv z^2 = x^2 + y^2 \equiv x + y \pmod{2}$, so z is odd. $\square$

As the rôles of x and y in Pythagorean triples are symmetric, it makes little loss in generality in studying only primitive Pythagorean triples with x odd and y even.

We can now prove a theorem characterizing primitive Pythagorean triples

Theorem 3 *Let (x, y, z) be a primitive Pythagorean triple with x odd. Then there are r, $s \in \mathbf{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd, such that $x = r^2 - s^2$, $y = 2rs$ and $z = r^2 + s^2$.*

Conversely, if r, $s \in \mathbf{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd, then $(r^2 - s^2, 2rs, r^2 + s^2)$ is a primitive Pythagorean triple.

Proof Let (x, y, z) be a primitive Pythagorean triple with x odd. Then y is even and z is odd. Let $a = \frac{1}{2}(z - x)$, $b = \frac{1}{2}(z + x)$ and $c = y/2$. Then a, b, $c \in \mathbf{N}$. Also

$$ab = \frac{(z - x)(z + x)}{4} = \frac{z^2 - x^2}{4} = \frac{y^2}{4} = c^2.$$

Let $g = \gcd(a, b)$. Then $g \mid (a + b)$ and $g \mid (b - a)$; that is $g \mid z$ and $g \mid x$. As $\gcd(x, z)$, by Theorem 1, then $g = 1$, that is $\gcd(a, b) = 1$.

Let p be a prime factor of a. Then $p \nmid b$, so $v_p(b) = 0$. Hence

$$v_p(a) = v_p(a) + v_p(b) = v_p(ab) = v_p(c^2) = 2v_p(c)$$

is even. Thus a is a square. Similarly b is a square. Write $a = s^2$ and $b = r^2$ where r, $s \in \mathbf{N}$. Then $\gcd(r, s) \mid a$ and $\gcd(r, s) \mid b$; as a and b are coprime, $\gcd(r, s) = 1$. Now $x = b - a = r^2 - s^2$; therefore $r > s$. Also $z = a + b = r^2 + s^2$. As $c^2 = ab = r^2 s^2$, $c = rs$ and so $y = 2rs$. Finally as x is odd, then $1 \equiv x = r^2 + s^2 \equiv r + s$; that is $r + s$ is odd. This proves the first half of the theorem.

To prove the second part, let r, $s \in \mathbf{N}$ with $r > s$, $\gcd(r, s) = 1$ and $r + s$ odd. Set $x = r^2 - s^2$, $y = 2rs$ and $z = r^2 + s^2$. Certainly y, $z \in \mathbf{N}$ and also $x \in \mathbf{N}$ as $r > s > 0$. Also

$$x^2 + y^2 = (r^2 - s^2)^2 + (2rs)^2 = (r^4 - 2r^2 s^2 + s^4) + 4r^2 s^2 = r^4 + 2r^2 s^2 + s^4 = z^2.$$

Hence (x, y, z) is a Pythagorean triple. Certainly y is even, and $x = r^2 - s^2 \equiv r - s \equiv r + s \pmod 2$: x is odd. To show that (x, y, z) is a primitive Pythagorean triple we examine $g = \gcd(x, z)$. As x is odd, g is odd. Also $g \mid (x^2 + z^2)$ and $g \mid (z^2 - x^2)$, that is $g \mid 2s^2$ and $g \mid 2r^2$. As r and s are coprime, then $\gcd(2r^2, 2s^2) = 2$, and so $g \mid 2$. As g is odd $g = 1$. Hence (x, y, z) is a primitive Pythagorean triple. $\square$

We now apply this to the proof of Fermat's last theorem for exponent 4.

Theorem 4 *There do not exist x, y, $z \in \mathbf{N}$ with*

$$x^4 + y^4 = z^4. \tag{1}$$

Proof In fact we prove a stronger result. We claim that there are no x, y, $u \in \mathbf{N}$ with

$$x^4 + y^4 = u^2. \tag{2}$$

A natural number solution (x, y, z) to (1) gives one for (2), namely $(x, y, u) = (x, y, z^2)$. Thus it suffices to prove that (2) is insoluble over $\mathbf{N}$.

We use Fermat's method of descent. Given a solution (x, y, u) of (2) we produce another solution (x', y', u') with $u' < u$. This is a contradiction if we start with the solution of (2) minimizing u.

Let (x, y, u) be a solution of (2) over $\mathbf{N}$ with minimum possible u. We claim first that $\gcd(x, y) = 1$. If not, then $p \mid x$ and $p \mid y$ for some prime p. Then $p^4 \mid (x^4 + y^4)$, that is, $p^4 \mid u^2$. Hence $p^2 \mid u$. Then $(x', y', u') = (x/p, y/p, u/p^2)$ is a solution of (2) in $\mathbf{N}$ with $u' < u$. This is a contradiction. Hence $\gcd(x, y) = 1$.

As $\gcd(x, y) = 1$ then $\gcd(x^2, y^2) = 1$, and so (x^2, y^2, u) is a primitive Pythagorean triple by (2). By the symmetry of x and y we may assume that x^2 is odd and y^2 is even, that is, x is odd and y is even. Hence there are r, $s \in \mathbf{N}$ with $\gcd(r, s) = 1$

$$\begin{aligned} x^2 &= r^2 - s^2, \\ y^2 &= 2rs, \\ u &= r^2 + s^2. \end{aligned}$$

Then $x^2 + s^2 = r^2$, and as $\gcd(r, s) = 1$ then (x, s, r) is a primitive Pythagorean triple. As x is odd, there exist a, $b \in \mathbf{N}$ with $\gcd(a, b) = 1$ and

$$\begin{aligned} x &= a^2 - b^2, \\ s &= 2ab, \\ r &= a^2 + b^2. \end{aligned}$$

Then

$$y^2 = 2rs = 4(a^2 + b^2)ab,$$

equivalently $(y/2)^2 = ab(a^2 + b^2) = abr$. (Recall that y is even.) If p is prime and $p \mid \gcd(a, r)$ then $b^2 = (a^2 + b^2) - a^2 \equiv 0 \pmod{p}$ and so $p \mid b$. This is impossible, as $\gcd(a, b) = 1$. Thus $\gcd(a, r) = 1$. Similarly $\gcd(b, r) = 1$. Now abr is a square. If $p \mid a$, then $p \nmid b$ and $p \nmid r$. Thus $v_p(a) = v_p(abr)$

is even, and so a is a square. Similarly b and r are squares. Write $a = x'^2$, $b = y'^2$ and $r = u'^2$ where x', y', $u' \in \mathbf{N}$. Then

$$u'^2 = a^2 + b^2 = x'^4 + y'^4$$

so (x', y', u') is a solution of (2). Also

$$u' \le u'^2 = a^2 + b^2 = r \le r^2 < r^2 + s^2 = u.$$

This contradicts the minimality of u in the solution (x, y, u) of (2). Hence (2) is insoluble over $\mathbf{N}$. Consequently (1) is insoluble over $\mathbf{N}$. □

2 Sums of squares

For $k \in \mathbf{N}$ we let $S_k = \{a_1^2 + \cdots + a_k^2 : a_1, \ldots, a_k \in \mathbf{Z}\}$ be the set of sums of k squares. Note that we allow zero; for instance $1 = 1^2 + 0^2 \in S_2$.

The sets S_2 and S_4 are closed under multiplication.

Theorem 5 *1. If m, $n \in S_2$ then $mn \in S_2$.*

2. If m, $n \in S_4$ then $mn \in S_4$.

Proof Let m, $m \in S_2$. Then $m = a^2 + b^2$ and $n = r^2 + s^2$ where a, b, r, $s \in \mathbf{Z}$. By the *two-square* formula,

$$(a^2 + b^2)(r^2 + s^2) = (ar - bs)^2 + (as + br)^2,$$

it is immediate that $mn \in S_2$.

Let m, $m \in S_4$. Then $m = a^2 + b^2 + c^2 + d^2$ and $n = r^2 + s^2 + t^2 + u^2$ where a, b, c, d, r, s, t, $u \in \mathbf{Z}$. By the *four-square* formula,

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + u^2) \\ = \; & (ar - bs - ct - du)^2 + (as + br + cu - dt)^2 \\ & + (at - bu + cr + ds)^2 + (au + bt - cs + dr)^2, \end{aligned}$$

it is immediate that $mn \in S_4$. □

We remark that the two-square theorem comes from complex numbers:

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= |a + bi|^2 |c + di|^2 \\ &= |(a + bi)(c + di)|^2 \\ &= |(ac - bd) + (ad + bc)|^2 \\ &= (ac - bd)^2 + (ad + bc)^2. \end{aligned}$$

Similarly the four-square theorem comes from the theory of quaternions (if you know what they are).

We can restrict the possible factorizations of a sum of two squares. Recall that if p is prime, and n is an integer, then $v_p(n)$ denotes the exponent of the largest power of p dividing n: $p^{v_p(n)} \mid n$ but $p^{v_p(n)+1} \nmid n$.

Theorem 6 *Let p be a prime with $p \equiv 3 \pmod 4$ and let $n \in \mathbf{N}$. If $n \in S_2$ then $v_p(n)$ is even.*

Proof Let $n = a^2 + b^2$ with a, $b \in \mathbf{Z}$ and suppose $p \mid n$. We aim to show that $p \mid a$ and $p \mid b$. Suppose $p \nmid a$. Then there is $c \in \mathbf{Z}$ with $ac \equiv 1 \pmod p$. Then $0 \equiv c^2 n = (ac)^2 + (bc)^2 \equiv 1 + (bc)^2 \pmod p$. This implies that $\left(\frac{-1}{p}\right) = 1$, but we know that $\left(\frac{-1}{p}\right) = 1$ when $p \equiv 3 \pmod 4$. This contradiction proves that $p \mid a$. Similarly $p \mid b$. Thus $p^2 \mid (a^2 + b^2) = n$ and $n/p^2 = (a/p)^2 + (b/p)^2 \in S_2$.

Let $n \in S_2$ and $k = v_p(n)$. We have seen that if $k > 0$ then $k \geq 2$ and $n/p^2 \in S_2$. Note that $v_p(n/p^2) = k - 2$. Similarly if $k - 2 > 0$ (that is if $k > 2$) then $k-2 \geq 2$ (that is $k \geq 4$) and $n/p^4 \in S_2$. Iterating this argument, we find that if $k = 2r + 1$ is odd, then $n/p^{2r} \in S_2$ and $v(n/p^{2r}) = 1$, which is impossible. We conclude that k is even. $\Box$

If $n \in \mathbf{N}$, we can write $n = rm^2$ where m^2 is the largest square dividing n and r is *squarefree*, that is either $r = 1$ or r is a product of distinct primes. If any prime factor p of r is congruent to 3 modulo 4 then $v_p(n) = 1 + 2v_p(m)$ is odd, and $n \notin S_2$. Hence, if $n \in S_2$, the only possible prime factors of r are $p = 2$ and the p congruent to 1 modulo 4. Obviously $2 = 1^2 + 1^2 \in S_2$. It would be nice if all primes congruent to 1 modulo 4 were also in S_2. Fortunately, this is the case.

Theorem 7 *Let p be a prime with $p \equiv 1 \pmod 4$. Then $p \in S_2$.*

Proof As $p \equiv 1 \pmod 4$ then $\left(\frac{-1}{p}\right) = 1$ and so there is $u \in \mathbf{Z}$ with $u^2 \equiv -1 \pmod p$. Let

$$A = \{(m_1, m_2) : m_1, m_2 \in \mathbf{Z}, 0 \leq m_1, m_2 < \sqrt{p}\}.$$

Then A has $(1 + s)^2$ elements, where s is the integer part of $\sqrt{p}$, that is, $s \leq \sqrt{p} < s + 1$. Hence $|A| > p$. For $\mathbf{m} = (m_1, m_2) \in \mathbf{R}^2$ define $\phi(\mathbf{m}) = um_1 + m_2$. Then ϕ is a linear map from $\mathbf{R}^2$ to $\mathbf{R}$, and if $\mathbf{m} \in \mathbf{Z}^2$ then $\phi(\mathbf{m}) \in \mathbf{Z}$.

As $|A| > p$, the $\phi(\mathbf{m})$ for $\mathbf{m} \in A$ can't all be distinct modulo p. Hence there are distinct $\mathbf{m}$, $\mathbf{n} \in A$ with $\phi(\mathbf{m}) \equiv \phi(\mathbf{n}) \pmod p$. Let $\mathbf{a} = \mathbf{m} - \mathbf{n}$. Then

$\phi(\mathbf{a}) = \phi(\mathbf{m}) - \phi(\mathbf{n}) \equiv 0 \pmod p$. Let $\mathbf{a} = (a, b)$. Then $a = m_1 - n_1$ where $0 \le m_1, n_1 < \sqrt{p}$ so that $|a| < \sqrt{p}$. Similarly $|b| < \sqrt{p}$. Then $a^2 + b^2 < 2p$. As $\mathbf{m} \ne \mathbf{n}$ then $\mathbf{a} \ne (0,0)$ and so $a^2+b^2 > 0$. But $0 \equiv \phi(\mathbf{a}) = ua+b \pmod p$. Hence $b \equiv -ua \pmod p$ and so $a^2 + b^2 \equiv a^2 + (-ua)^2 \equiv a^2(1 + u^2) \equiv 0 \pmod p$. As a^2+b^2 is a multiple of p, and $0 < a^2+b^2 < 2p$, then $a^2+b^2 = p$. We conclude that $p \in S_2$. $\square$

We can now characterize the elements of S_2.

Theorem 8 (Two-square theorem) *Let $n \in \mathbf{N}$. Then $n \in S_2$ if and only if $v_p(n)$ is even whenever p is a prime congruent to 3 modulo 4.*

Proof If $n \in S_2$, p is prime and $p \equiv 3 \pmod 4$ then $v_p(n)$ is even by Theorem 7.

If $v_p(n)$ is even whenever p is a prime congruent to 3 modulo 4 then $p = rm^2$ where each prime factor p of r is either 2 or congruent to 1 modulo 4. By Theorem 7 all such p lie in S_2. Hence By Theorem 5 $r \in S_2$. Hence $r = a^2 + b^2$ where a, $b \in \mathbf{Z}$ and so $n = rm^2 = (am)^2 + (bm)^2 \in S_2$. $\square$

The representation of a prime as a sum of two squares is essentially unique.

Theorem 9 *Let p be a prime. If $p = a^2 + b^2 = c^2 + d^2$ with a, b, c, $d \in \mathbf{N}$ then either $a = c$ and $b = d$ or $a = d$ and $b = c$.*

Proof Consider

$$\begin{aligned}(ac + bd)(ad + bc) &= a^2cd + abc^2 + abd^2 + b^2cd \\ &= (a^2 + b^2)cd + ab(c^2 + d^2) \\ &= pcd + pab = p(ab + cd).\end{aligned}$$

As $p \mid (ac + bd)(ad + bc)$ then either $p \mid (ac + bd)$ or $p \mid (ad + bc)$. Assume the former — the latter case can be treated by reversing the rôles of c and d. Now $ac + bd > 0$ so that $ac + bd \ge p$. Also

$$\begin{aligned}(ac + bd)^2 + (ad - bc)^2 &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= (a^2 + b^2)(c^2 + d^2) = p^2.\end{aligned}$$

As $ac+bd \ge p$, the only way this is possible is if $ac+bd = p$ and $ad-bc = 0$. Then $ac^2 + bcd = cp$ and $ad^2 - bcd = 0$, so adding gives $a(c^2 + d^2) = cp$, that is $ap = cp$, so that $a = c$. Then $c^2 + bd = p = c^2 + d^2$ so that $bd = d^2$, so that $b = d$. $\square$

We wish to prove the theorem of Lagrange to the effect that all natural numbers are sums of four squares. It is crucial to establish this for primes.

Theorem 10 *Let p be a prime. Then $p \in S_4$.*

Proof If $p \equiv 1 \pmod 4$ then there are a, $b \in \mathbf{Z}$ with $p = a^2 + b^2 + 0^2 + 0^2$ (Theorem 7) so that $p \in S_4$. Also $2 = 1^2 + 1^2 + 0^2 + 0^2 \in S_4$ and $3 = 1^2 + 1^2 + 1^2 + 0^2 \in S_4$. We may assume that $p > 3$ and that $p \equiv 3 \pmod 4$. As a consequence $\left(\frac{-1}{p}\right) = -1$.

Let w be the smallest positive integer with $\left(\frac{w}{p}\right) = -1$. Then $\left(\frac{w-1}{p}\right) = 1$ and $\left(\frac{-w}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{w}{p}\right) = 1$. Hence there are u, $v \in \mathbf{Z}$ with $w - 1 \equiv u^2 \pmod p$ and $-w \equiv v^2 \pmod p$. Then $1 + u^2 + v^2 \equiv 1 + (w-1) - w \equiv 0 \pmod p$.

Let

$$B = \{(m_1, m_2, m_3, m_4) : m_1, \ldots, m_4 \in \mathbf{Z}, 0 \le m_1, \ldots, m_4 < \sqrt{p}\}.$$

Then B has $(1+s)^4$ elements, where s is the integer part of $\sqrt{p}$, that is, $s \le \sqrt{p} < s + 1$. Hence $|A| > p^2$. For $\mathbf{m} = (m_1, nm_2, m_3, m_4)$ define $\psi(\mathbf{m}) = (um_1 + vm_2 + m_3, -vm_1 + um_2 + m_4)$. Then ψ is a linear map from $\mathbf{R}^4$ to $\mathbf{R}^2$. If $\mathbf{m} \in \mathbf{Z}^4$ then $\psi(\mathbf{m}) \in \mathbf{Z}^2$. We write $(a, b) \equiv (a', b') \pmod p$ if $a \equiv a' \pmod p$ and $b \equiv b' \pmod p$. If we have a list $(a_1, b_1), \ldots, (a_N, b_N)$ of vectors in $\mathbf{Z}^2$ with $N > p^2$, then there must be some i and j with $(a_i, b_i) \equiv (a_j, b_j) \pmod p$. This happens for the vectors $\psi(\mathbf{m})$ with $\mathbf{m} \in B$ as $|B| > p^2$. There are distinct $\mathbf{m}$, $\mathbf{n} \in B$ with $\psi(\mathbf{m}) \equiv \psi(\mathbf{n}) \pmod p$. Let $\mathbf{a} = \mathbf{m} - \mathbf{n}$. Then $\psi(\mathbf{a}) = \psi(\mathbf{m}) - \psi(\mathbf{n}) \equiv 0 \pmod p$. Let $\mathbf{a} = (a, b, c, d)$. Then $a = m_1 - n_1$ where $0 \le m_1, n_1 < \sqrt{p}$ so that $|a| < \sqrt{p}$. Similarly $|b|$, $|c|$, $|d| < \sqrt{p}$. Then $a^2 + b^2 + c^2 + d^2 < 4p$. As $\mathbf{m} \ne \mathbf{n}$ then $\mathbf{a} \ne (0, 0, 0, 0)$ and so $a^2 + b^2 + c^2 + d^2 > 0$.

Now $(0, 0) \equiv \phi(\mathbf{a}) = (ua + vb + c, -va + ub + d) \pmod p$. Hence $c \equiv -ua - vb \pmod p$ and $d \equiv va - ub \pmod p$. Then

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ua + vb)^2 + (va - ub)^2 \\ &= (1 + u^2 + v^2)(a^2 + b^2) \equiv 0 \pmod p \end{aligned}$$

As $a^2 + b^2 + c^2 + d^2$ is a multiple of p, and $0 < a^2 + b^2 + c^2 + d^2 < 4p$, then $a^2 + b^2 + c^2 + d^2 \in \{p, 2p, 3p\}$.

When $a^2 + b^2 + c^2 + d^2 = p$ then certainly $p \in S_4$. Alas, we need to consider the bothersome cases where $a^2 + b^2 + c^2 + d^2 = 2p$ or $3p$.

Suppose that $a^2 + b^2 + c^2 + d^2 = 2p$. Then $a^2 + b^2 + c^2 + d^2 \equiv 2 \pmod 4$ so that two of a, b, c, d are odd and the other two even. Without loss of generality a and b are odd and c and d are even. Then $\frac{1}{2}(a+b)$, $\frac{1}{2}(a-b)$, $\frac{1}{2}(c+d)$ and $\frac{1}{2}(c-d)$ are all integers, and a simple computation gives

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

so that $p \in S_4$.

Finally suppose that $a^2 + b^2 + c^2 + d^2 = 3p$. Then $a^2 + b^2 + c^2 + d^2$ is a multiple of 3 but not 9. As $a^2 \equiv 0$ or $1 \pmod 3$ then either exactly one or all four of a, b, c and d are multiples of 3. But the latter case is impossible (for then $a^2 + b^2 + c^2 + d^2$ would be a multiple of 9), so without loss of generality $3 \mid a$ and b, c, $d \equiv \pm 1 \pmod 3$. By replacing b by $-b$ etc., if necessary, we may assume that $b \equiv c \equiv d \equiv 1 \pmod 3$. Then Then $\frac{1}{3}(b+c+d)$, $\frac{1}{3}(a+b-c)$, $\frac{1}{3}(a+c-d)$,$\frac{1}{3}(a+d-b)$, are all integers, and a simple computation gives

$$\begin{aligned} & \left(\frac{b+c+d}{3}\right)^2 + \left(\frac{a+b-c}{3}\right)^2 + \left(\frac{a+c-d}{3}\right)^2 + \left(\frac{a+d-b}{3}\right)^2 \\ = & \frac{a^2+b^2+c^2+d^2}{3} = p \end{aligned}$$

so that $p \in S_4$. $\square$

We can now prove Lagrange's four-square theorem.

Theorem 11 (Lagrange) *If $n \in \mathbf{N}$ then $n \in S_4$.*

Proof Either $n = 1 = 1^2 + 0^2 + 0^2 + 0^2 \in S_4$, or n is a product of a sequence of primes. By Theorem 10, each prime factor of n lies in S_4. Then by Theorem 5, $n \in S_4$. $\square$

We finish with some remarks about sums of three squares. This is a much harder topic than sums of two and of four squares. One reason for this is that the analogue of Theorem 5 is false. Let $m = 3 = 1^2 + 1^2 + 1^2$ and $n = 5 = 2^2 + 1^2 + 0^2$. Then $m \in S_3$ and $n \in S_3$ but $mn = 15 \notin S_3$. It follows that we cannot reduce the study of sums of three squares to this problem for primes.

Theorem 12 *1. If $m \in S_3$ then $m \not\equiv 7 \pmod 8$.*

2. If $4n \in S_3$ then $n \in S_3$.

Proof Let $m = a_1^2 + a_2^2 + a_3^2$. As $a_j^2 \equiv 0$ or $1 \pmod 4$ then $m \equiv k \pmod 4$ where k is the number of odd a_j. If $m \equiv 7 \pmod 8$ then $m \equiv 3 \pmod 4$ and so all of the a_j are odd. But if a_j is odd, then $a_j^2 \equiv 1 \pmod 8$ and so $m = a_1^2 + a_2^2 + a_3^2 \equiv 3 \pmod 8$, a contradiction.

Let $m = 4n = a_1^2 + a_2^2 + a_3^2$. As $m \equiv 0 \pmod 4$ then all of the a_j are even. Hence $n = (a_1/2)^2 + (a_2/2)^2 + (a_3/2)^2 \in S_3$. $\square$

As a consequence, if $n = 4^k m$ where k is a nonnegative integer and $m \equiv 7 \pmod 8$ then $n \notin S_3$. Gauss proved in his *Disquisitiones Arithmeticae* that if $n \in \mathbf{N}$ is not of this form, then $n \in S_3$. Alas, all known proofs are too difficult to be presented in this course.