SUMS OF 2 AND 4 SQUARES

NEIL MAKUR

Abstract. We prove results stating what numbers can be expressed as the sum of two integer squares and the sum of four integer squares. We provide standard proofs of both results, along with investigating Zagier's One-Sentence Proof, which contributes to the former result, and using quaternions to provide an alternative proof of the latter result.

1. Sums of Two Squares

We start by looking at what numbers can be written as the sum of two squares.

1.1. Number-Theoretic Proof.

Proposition 1.1. *Suppose that m and n are both sums of two squares. Then mn is the sum of two squares.*

Proof. Suppose that $m = a^2 + b^2$ and $n = c^2 + d^2$. We present a way of deriving the proof of the theorem, rather than just a single equation. We have that $m = (a + bi)(a - bi)$ and $n = (c + di)(c - di)$. Thus,

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

■

The above result inspires us to look at which primes can be represented as the sum of two squares, and use the results to figure out what composite numbers can be written as the sum of two squares.

1.1.1. *Prime Numbers.* The prime 2 can be written as $1^2 + 1^2$, so we will only consider odd primes. First, consider the squares modulo 4:

n	0	1	2	3
n^2	0	1	0	1

This table means that, if a number is the sum of two squares, it must be 0, 1 or 2 modulo 4. In particular, any prime $p \equiv 3 \pmod 4$ cannot be written as the sum of two squares. Thus, we only have to look at primes $p \equiv 1 \pmod 4$.

Lemma 1.2. *If $p \equiv 1 \pmod 4$, then there is some x such that $p | x^2 + 1$. If $p \equiv 3 \pmod 4$, there is no such x.*

Proof. Consider the set $\{1, 2, \ldots, p-1\}$. Partition it into sets of the form $\{x, -x, x^{-1}, -x^{-1}\}$, where x^{-1} denotes the inverse of x modulo p. These have size 4, except for the following cases.

Date: February 2022.

$x \equiv -x$ In this case, $2x \equiv 0 \pmod{p}$, so $x \equiv 0 \pmod{p}$, since p is odd. This cannot happen by assumption.

$x \equiv x^{-1}$ In this case, $x^2 \equiv 1 \pmod{p}$, so $x \equiv 1 \pmod{p}$ or $x \equiv p-1 \pmod{p}$. This gives the set $\{1, p-1\}$, which has size 2.

$x \equiv -x^{-1}$ In this case, $x^2 \equiv -1 \pmod{p}$. If this happens, $x \equiv -x^{-1} \pmod{p}$ and $-x \equiv x^{-1} \pmod{p}$, so the set becomes $\{x, -x\}$, with size 2.

Most subsets have size 4, except for $\{1, p-1\}$, and possibly one more subset if there is an x with $x^2 \equiv -1 \pmod{p}$. If there is this extra subset, then $p - 1 \equiv 0 \pmod{4}$, and if there is not, $p - 1 \equiv 2 \pmod{4}$. The reverse direction is also clearly necessary. The theorem follows. ■

Using the above lemma, we can figure out what primes we can express as the sum of two squares.

Theorem 1.3. *If $p \equiv 1 \pmod{4}$ is prime, then there are integers x and y with $x^2 + y^2 = p$.*

Proof. Define the set

$$X = \left\{(x', y') : 0 \leq x', y' \leq \lfloor \sqrt{p} \rfloor\right\}.$$

We have that $|X| = (1 + \lfloor \sqrt{p} \rfloor)^2 > p$. Given any s, we can find distinct $(x', y'), (x'', y'') \in X$ with $x' - sy' \equiv x'' - sy'' \pmod{p}$ by the Pigeonhole Principle. Thus, we have that $x' - x'' \equiv s(y' - y'') \pmod{p}$. Letting $x = |x' - x''|$ and $y = |y' - y''|$, we have that $x \equiv \pm sy \pmod{p}$. By assumption, (x', y') and (x'', y'') are distinct, so at least one of x and y is nonzero. Squaring, $x^2 \equiv s^2 y^2 \pmod{p}$. By our lemma, there is some s with $s^2 \equiv -1 \pmod{p}$. Picking this s, we have that $x^2 + y^2 \equiv 0 \pmod{p}$. Now, $0 \leq x, y \leq \lfloor \sqrt{p} \rfloor$, so $0 \leq x^2, y^2 < p$. Hence, $0 \leq x^2 + y^2 < 2p$. Since at least one of x and y is nonzero, $x^2 + y^2 \neq 0$, so we must have $x^2 + y^2 = p$. ■

1.1.2. *Composite Numbers.* Now that we know what primes can be written as the sum of two squares, we can figure out which numbers can be written as such.

Theorem 1.4. *A positive integer n can be written as the sum of two squares if and only if, for every prime $p \equiv 3 \pmod{4}$ dividing n, the highest power of p dividing n is even.*

Proof. Let us first show that our condition is sufficient. Write out the prime factorization of n

$$2^a p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{2f_2} q_2^{2f_2} \cdots q_\ell^{2f_\ell},$$

where the p_i are $1 \pmod{4}$, and the q_i are $3 \pmod{4}$. We can write the p_i as $a_i^2 + b_i^2$. Thus,

$$n = (1^2 + 1^2)^a (a_1^2 + b_1^2)^{e_1} (a_2^2 + b_2^2)^{e_2} \cdots (a_k^2 + b_k^2)^{e_k} (q_1^2 + 0^2)^{f_1} (q_2^2 + 0^2)^{f_2} \cdots (q_\ell^2 + 0^2)^{f_\ell}$$

is the product of terms that are each the sum of two squares, and so is the sum of two squares itself.

Now, we show that the condition is necessary by induction on n (this is true with $n = 2$). Suppose that we can write $n = x^2 + y^2$. We show that, if $p \equiv 3 \pmod{4}$ divides n, then p divides both x and y. This suffices, as it means that $p^2 | n$, and we can use the result on $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ by induction. Suppose, for the sake of contradiction, that $p \nmid x$. Then x has a multiplicative inverse modulo p. Thus, we have that $nx^{-2} = (xx^{-1})^2 + (yx^{-1})^2$. Reducing modulo p, $0 \equiv 1 + (yx^{-1})^2 \pmod{p}$, contradicting our earlier lemma. ■

1.2. **The 1-Sentence Proof.** Zagier's One Sentence Proof provides an alternative way of showing that all primes congruent to 1 modulo 4 can be expressed as the sum of two squares. The proof is as follows.

Zagier's One Sentence Proof. The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2+4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & x < y - z \\ (2y - x, y, x - y + z) & y - z < x < 2y \\ (x - 2y, x - y + z, y) & x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd, and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. ∎

This proof is quite dense, so we break it down term by term. We start with defining an involution.

Definition 1.5. For a set X, a function $f : X \to X$ is said to be an *involution on* X if $f \circ f = \mathrm{id}_X$.

Given a set X and an involution f on X, we write $\mathrm{Fix}_f(X)$ for the set of elements fixed by f. In other words, $\mathrm{Fix}_f(X) = \{x \in X : f(x) = x\}$. With this definition, we find the following result, which motivates the use of involutions in existence proofs.

Proposition 1.6. *Given a finite set X and an involution f on X, $|X| \equiv |\mathrm{Fix}_f(X)| \pmod 2$.*

Proof. We partition X into sets of the form $P_x = \{x, f(x)\}$. Notice that $P_{f(x)} = P_x$ by the assumption that f is an involution. If x is not a fixed point, then $|P_x| = 2$, while if x is a fixed point, $|P_x| = 1$. Since $|X| = \sum |P_x|$, the only terms that contribute modulo 2 are the fixed points, so $|X| \equiv |\mathrm{Fix}_f(X)| \pmod 2$. ∎

Thus, if we can show that $|X|$ is odd, there must be an odd number of fixed points for each involution, and so at least one. This is in fact the approach that Zagier uses: he finds an involution that has exactly one fixed point, meaning that $|S|$ is odd, and so a different involution also has a fixed point. Let us investigate the involution given, which we will call f.

- Suppose that (x, y, z) falls into the first case. Then, we have that $f(x', y', z') = (x+2z, z, y-x-z)$. It is clear that $x' > 2y'$, so this falls into the third case. Applying f again gives $(x'', y'', z'') = (x'-2y', x'-y'+z', y') = (x+2z-2z, x+2z-z+y-x-z, z) = (x, y, z)$. Thus, f is an involution in this case.
- Suppose that (x, y, z) falls into the second case. Then, we have that $(x', y', z') = (2y - x, y, x - y + z)$. We can see that $y' - z' = 2y - x - z < 2y - x = x' < 2y = 2y'$, so this falls again into the second case. Applying f again gives that $(x'', y'', z'') = (2y' - x', y', x' - y' + z') = (2y - (2y - x), y, 2y - x - y + x - y + z) = (x, y, z)$, so f is an involution in this case.
- Suppose that (x, y, z) falls into the last case. Then, we have that $(x', y', z') = (x - 2y, x-y+z, y)$. We can see that $x' < y'-z'$, so this falls into the first case. Applying f again gives $(x'', y'', z'') = (x'+2z', z', y'-x'-z') = (x-2y+2y, y, x-y+z-x+2y-y) = (x, y, z)$, so f is an involution in this final case.

It is clear that, if f has a fixed point, it must be in the second case. For this to happen, we must have $2y-x = x$, $y = y$, and $x-y+z = z$. The second is given, and the first two imply

that $x = y$. Plugging this back into the defining equation of S gives that $x(x + 4z) = p$. Because p is prime, we must have either $x = 1$ or $x + 4z = 1$. The latter is impossible, so we have $x = 1$ and $1 + 4z = p$. This means that the only fixed point is $\left(1, 1, \frac{p-1}{4}\right)$.

Now, since f has exactly one fixed point, $|S|$ is odd, so the involution $g(x, y, z) = (x, z, y)$ has a fixed point. Thus, there is some $(x, y, z) \in S$ with $y = z$. This means that $p = x^2 + 4yz = x^2 + 4y^2 = x^2 + (2y)^2$ is the sum of two squares.

2. Sums of Four Squares

2.1. **Quaternions.** Before proving our main theorem of this section, that every integer can be expressed as the sum of four squares, we will introduce the quaternions.

Definition 2.1. A quaternion is a number of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$, and i, j, and k satisfy the equation $i^2 = j^2 = k^2 = ijk = -1$. Addition and multiplication of quaternions are defined as outlined below, with multiplication distributing over addition.

We denote the quaternions as $\mathbb{H}$. Addition is done term-by-term, similar to complex numbers. Numerically,

$$(a_1 + a_2i + a_3j + a_4k) + (b_1 + b_2i + b_3k + b_4k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k.$$

Defining multiplication is a bit harder. To do this, firstly notice that $\frac{1}{i}, \frac{1}{j}, \frac{1}{k}$ are equal to $-i, -j, -k$ respectively. It is also worth noting that real numbers commute with quaternions in multiplication. However, when trying to figure out quaternion multiplication, we must not make the assumption that they commute, as it turns out that they do not.

If we look at the equation $i^2 = ijk$, we can see that $jk = i$. We can also see that

$$jk = i \Rightarrow jki = i^2 = j^2 \Rightarrow ki = j.$$

If we consider the equation $k^2 = ijk$, we can see that $ij = k$.

We can also show that that quaternions do not commute. Multiplying the equations $ij = k$, $jk = i$ and $ki = j$ by i, j, and k on the left respectively, we get that $ik = -j$, $ji = -k$ and $kj = -i$. Putting this all together, we get the following table.

$\times$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

This allows us to multiply quaternions using the regular properties of multiplication distributing over addition, and using the fact that the general form of a quaternion is $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$. After computation, the result is that

$$\begin{aligned}(a_1 + a_2i + a_3j + a_4k)(b_1 + b_2i + b_3j + b_4k) = &(a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)\\ &+ (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)i\\ &+ (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)j\\ &+ (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)k\end{aligned}$$

Along with addition and multiplication, there are other operations that can be done on quaternions. The first operation is conjugation. The conjugate of a quaternion, q is denoted $\bar{q}$, and is defined as $\overline{a + bi + cj + dk} = a - bi - cj - dk$. Notice that a quaternions commutes

with its conjugate: $q\bar{q} = \bar{q}q$, and that $\overline{q_1 q_2} = \bar{q}_2\bar{q}_1$. We can also take the norm of a quaternion using the formula

$$|a + bi + cj + dk| = \sqrt{a^2 + b^2 + c^2 + d^2},$$

or the formula

$$|q| = \sqrt{q\bar{q}}.$$

With these, we can define the multiplicative inverse of a nonzero quaternion as

$$q^{-1} = \frac{\bar{q}}{q\bar{q}} = \frac{\bar{q}}{|q|^2}.$$

As $|q|^2$ is a real number, this makes sense to define. We also have that $q^{-1}q = qq^{-1} = 1$.

2.2. **Hurwitz Quaternions.** When proving the four-square theorem, we use Hurwitz quaternions.

Definition 2.2. The Hurwitz quaternions are quaternions with either all integer or all half-integer coefficients. They take the form

$$\frac{E_0}{2}(1 + i + j + k) + E_1 i + E_2 j + E_3 k,$$

where $E_0, E_1, E_2, E_3 \in \mathbb{Z}$.

Example. The quaternion $\frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$ is a Hurwitz quaternion, using $E_0 = 1$ and $E_{1,2,3} = 0$. The quaternion $3 + i + 4j + k$ is a Hurwitz quaternion with $E_0 = 6$, $E_1 = -2$, $E_2 = 1$ and $E_3 = -2$. We also have that i is a Hurwitz quaternion, with $E_{0,2,3} = 0$ and $E_1 = 1$. However, $\frac{1}{2} + 5i + \frac{7}{2}j + 4k$ is not a Hurwitz quaternion.

In a Hurwitz quaternion, all coefficients are either integers or half-integers. Thus, we can also write Hurwitz quaternions as

$$\alpha = a_1 + a_2 i + a_3 j + a_4 k \quad \text{or} \quad \alpha = \frac{2a_1 + 1}{2} + \frac{2a_2 + 1}{2}i + \frac{2a_3 + 1}{2}j + \frac{2a_4 + 1}{2}k.$$

This gives us

$$|\alpha|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

or

$$|\alpha|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_1 + a_2 + a_3 + a_4 + 1,$$

which is an integer.

We will need to break primes into Hurwitz quaternions in our proof. To prove that this is possible, we have to establish a few lemma.s

Lemma 2.3. *Any odd prime p divides at least one number of the form $1 + x^2 + y^2$.*

Proof. Let

$$X = \{x^2 : 0 \le x \le \lfloor p/2 \rfloor\} \qquad Y = -1 - X.$$

These both contain $\lfloor p/2 \rfloor + 1$ residues modulo p. Since there are a total of p residues, there must be some intersection. This means that there are x and y with $x^2 \equiv -1 - y^2 \pmod{p}$, so that $p|1 + x^2 + y^2$. ■

Lemma 2.4. *For any quaternion $q = a_1 + a_2 i + a_3 j + a_4 k$, where $a_1, a_2, a_3, a_4 \in \mathbb{Q}$, there is a Hurwitz quaternion α with $|q - \alpha|^2 < 1$.*

Proof. Let b_1 be an integer or half-integer with $|a_1 - b_1| \leq \frac{1}{4}$. Pick b_2, b_3, b_4 to be integers of half-integers (the same as b_1) with $|a_\ell - b_\ell| \leq \frac{1}{2}$ for $\ell = 2, 3, 4$. Let $\alpha = b_1 + b_2 i + b_3 j + b_4 k$. Then,

$$|q-\alpha|^2 = (a_1-b_1)^2+(a_2-b_2)^2+(a_3-b_3)^2+(a_4-b_4)^2 \leq \left(\frac{1}{4}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2 = \frac{13}{16} < 1.$$

■

We can now show that we can break primes into Hurwitz quaternions.

Proposition 2.5. *Let p be an odd prime. Then, there are Hurwitz quaternions α and β with $p = \alpha\beta$, such that α^{-1} and β^{-1} are not Hurwitz quaternions.*

Proof. Let

$$p|1 + x^2 + y^2 = (1 + xi + yj)(1 - xi - yj).$$

For any Hurwitz quaternions α and β, let γ be a Hurwitz quaternion with $\left|\frac{\beta}{\alpha} - \gamma\right|^2 < 1$. Then,

$$|\beta - \alpha\gamma|^2 < |\alpha|^2.$$

Consider the set

$$p\mathcal{H} + (1 - \ell i - mj)\mathcal{H},$$

where $\mathcal{H}$ denotes the set of Hurwitz quaternions. This is clearly closed under addition and multiplication on the right by Hurwitz quaternions. If α is a nonzero element of this set of minimal norm, we claim that this set is equal to $\alpha\mathcal{H}$. For any β in the set, there is a Hurwitz quaternion γ with $|\beta - \alpha\gamma|^2 < |\alpha|^2$, and so $|\beta - \alpha\gamma|$ must be 0 by the definition of α. This establishes that $p\mathcal{H} + (1 - \ell i - mj)\mathcal{H} \subseteq \alpha\mathcal{H}$, and the reverse inclusion follows from the closure under multiplication on the right. In particular, we can write $p = \alpha\beta$ for some Hurwitz quaternion β. If β^{-1} were a Hurwitz quaternion, we would be able to write $1 - \ell i - mj$ as a Hurwitz-quaternion-multiple of p. However, $\frac{1}{p} - \frac{\ell}{p}i - \frac{m}{p}j$ is not a Hurwitz quaternion for odd p. If α^{-1} were a Hurwitz quaternion, we would have that $\alpha\mathcal{H} = \mathcal{H}$, so that

$$(1 + \ell i + mj)\mathcal{H} = (1 + \ell i + mj)p\mathcal{H} + (1 + \ell i + mj)(1 - \ell i - mj)\mathcal{H} \subseteq p\mathcal{H},$$

meaning that p divides $1 + \ell i + mj$, creating the same contradiction as before. Thus, we can write $p = \alpha\beta$, where α and β are Hurwitz quaternions whose inverses are not Hurwitz quaternions. ■

Lemma 2.6. *Let α be a Hurwitz quaternion. Then α^{-1} is a Hurwitz quaternion if and only if $|\alpha|^2 = 1$.*

Proof. Suppose that α^{-1} is a Hurwitz quaternion. Then $|\alpha|^2$ and $|\alpha^{-1}|^2$ are positive integers whose product is 1. Thus, they are both 1. If $|\alpha|^2 = 1$, then $\alpha^{-1} = \bar{\alpha}$ is a Hurwitz quaternion. ■

2.3. **A Quaternionic Proof.** We have a similar result to the two-squares case.

Lemma 2.7. *Suppose that m and n are both sums of four squares. Then mn is the sum of four squares.*

Proof. We have that

$$|q_1q_2|^2 = q_1q_2\overline{q_1q_2} = q_1q_2\bar{q}_2\bar{q}_1 = q_1|q_2|\bar{q}_1 = |q_1| \cdot |q_2|.$$

Now, if m is the sum of four squares, we can write $m = |q_1|$, where q_1 is a quaternion with integer coefficients. Similarly, we can write $n = |q_2|$ for a quaternion q_2 with integer coefficients. We have that

$$mn = |q_1| \cdot |q_2| = |q_1q_2|,$$

which is the norm of a quaternion with integer coefficients. Thus, mn is the sum of four squares as well. ■

We can now prove that any integer is the sum of four squares.

Theorem 2.8. *Any integer can be written as the sum of four integer squares.*

Proof. It suffices to prove this for primes, and since $2 = 1^2+1^2+0^2+0^2$, we only consider odd primes. Let p be an odd prime, and write $p = \alpha\beta$ for Hurwitz quaternions with $|\alpha|^2, |\beta|^2 \neq 1$. We then have that $p^2 = |p|^2 = |\alpha\beta|^2 = |\alpha|^2|\beta^2|$. These are both integers greater than 1, and so $|\alpha|^2 = |\beta|^2 = p$. If α has integer coefficients, we are done, so suppose that α has half-integer coefficients. Let

$$\omega = \frac{\pm 1 \pm i \pm j \pm k}{2}$$

be chosen such that $\gamma = \omega + \alpha$ has even integer coefficients. Then,

$$p = |\alpha|^2 = |\gamma - \omega|^2 = (\gamma - \omega)\overline{(\gamma - \omega)}.$$

Since $|\omega| = 1$, we can multiply by $\bar{\omega}$ on the left and ω on the right to obtain that

$$p = \bar{\omega}p\omega = \bar{\omega}(\gamma - \omega)\overline{(\gamma - \omega)}\omega = \bar{\omega}(\gamma - \omega)(\bar{\gamma} - \bar{\omega})\omega = (\bar{\omega}\gamma - 1)(\bar{\gamma}\omega - 1).$$

Since γ has even integer coefficients and ω has half-integer coefficients, $\bar{\omega}\gamma - 1$ has integer coefficients. Let $\alpha' = \bar{\omega}\gamma - 1$. We have that

$$|\alpha'|^2 = |\bar{\omega}\gamma - 1|^2 = |\bar{\omega}|^2|\gamma - \omega|^2 = 1 \cdot |\alpha|^2 = p.$$

Thus, we have found a way to write p as the sum of four squares. ■

2.4. **A Number-Theoretic Proof.** Recall that an odd prime p divides at least one number of the form $1 + x^2 + y^2$. Recall further that, from the proof of this statement, we can take $0 \leq x, y \leq \lfloor p/2 \rfloor$. Then,

$$1 \leq 1 + x^2 + y^2 \leq \frac{2p^2 - 4p + 6}{4} < \frac{p^2}{2}.$$

Thus, we can write

$$0 < x^2 + y^2 + 1^2 + 0^2 = mp < \frac{p^2}{2}$$

for some integer m. Thus, there are a, b, c, d with

$$0 < a^2 + b^2 + c^2 + d^2 = mp < \frac{p^2}{2}.$$

We will use this result in an alternate number-theoretic proof that any integer is the sum of four squares.

Lemma 2.9. *If n is even and is a sum of four squares, then $\frac{n}{2}$ is also a sum of four squares.*

Proof. Suppose that $n = a^2 + b^2 + c^2 + d^2$. Then, an even number of a, b, c, d are even. Thus, we can assume that a and b have the same parity, and c and d have the same parity. We have that

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

■

Altenate Proof of Theorem 2.8. We once again only have to show this for odd primes ($2 = 1^2 + 1^2 + 0^2 + 0^2$). Suppose that p is an odd prime. There is some $m < \frac{p}{2}$ with $a^2 + b^2 + c^2 + d^2 = mp$. Take m to be minimal with this property. If m were even, then $\frac{m}{2}p$ could be expressed as the sum of four squares, so m is odd. If $m = 1$, we are done, so suppose that $m > 1$. If $m|a, b, c, d$, we could divide by m^2 to get a representation of p as the sum of four squares, so suppose that m does not divide at least one of these. Take w, x, y, z such that $w \equiv a \pmod{m}$, $x \equiv -b \pmod{m}$, $y \equiv -c \pmod{m}$ and $z \equiv -d \pmod{m}$, and $|w|, |x|, |y|, |z| \leq \frac{m-1}{2}$. We have that

$$0 < w^2 + x^2 + y^2 + z^2 = mk < 4\left(\frac{m-1}{2}\right)^2 = (m-1)^2$$

for some integer $0 < k < m$. Now,

$$\begin{aligned} m^2kp = &(aw - bx - cy - dz)^2 + (ax + bw + cz - dy)^2 \\ &+ (ay + cw + dx - bz)^2 + (az + dw + by - cx)^2, \end{aligned}$$

and all of these squares are divisible by m^2. Thus, we can divide out by m^2 to show that kp is a sum of four squares, contradicting m's minimality. We therefore have that $m = 1$. ■