An investigation into sums of squares

Daniel Coble

December 11, 2023

Abstract

Here I provide the proof of the sums of two squares statement. I wrote this as part of my Number Theory final project. The proof provided here is by-and-large based on the proof given by Dudley. I reorganized his proof in a way that made it easier (for me) to understand, elaborated and filled in areas which Dudley left to the reader.

Theorem 0.1. *n cannot be written as the sum of two squares if and only if the prime-power decomposition of n contains a prime congruent to $3 \pmod 4$ to an odd power.*

Before beginning the proof, we will start with five lemmas.

Lemma 0.2. *2 is representable.*

Proof. $2 = 1^2 + 1^2$ □

Lemma 0.3. *The product of two representable numbers is representable.*

Proof. $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$ for any integers a, b, c, and d. □

Lemma 0.4. *If n is representable, then so is $k^2 n$ for any k*

Proof. If $n = a^2 + b^2$, then $k^2 n = (ka)^2 + (kb)^2$ □

Lemma 0.5. *Any integer n can be written in the form*

$$n = k^2 p_1 p_2 \cdots p_r, \tag{0.1}$$

where each p_i is a distinct prime and k is unique.

Proof. Let the prime factorization of n be

$$n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \tag{0.2}$$

Define the index sets $I = \{i | 1 \le i \le n,\ e_i \text{ is even}\}$ and $J = \{i | 1 \le i \le n,\ e_i \text{ is odd}\}$. The decomposition is

$$n = \left(\prod_{i \in I} p_i^{e_i}\right)\left(\prod_{i \in J} p_i^{e_i}\right) \tag{0.3}$$

For e_i even, say $e_i = 2f_i$ ($f_i \ge 1$) and if e_i is odd, say $e_i = 2f_i + 1$ ($f_i \ge 0$). Then by rearranging we can produce

$$= \left(\prod_{i \in I} p_i^{2f_i}\right)\left(\prod_{i \in J} p_i^{2f_i+1}\right) \tag{0.4}$$

$$= \left(\prod_{i=1}^{n} p_i^{2f_i}\right)\left(\prod_{i \in J} p_i\right) \tag{0.5}$$

$$= \left(\prod_{i=1}^{n} p_i^{f_i}\right)^2 \left(\prod_{i \in J} p_i\right) \tag{0.6}$$

Then we can relabel the first product as k and the second project $p_1 \cdots p_r$. To show uniqueness, let there be two decompositions:

$$n = k_1^2 p_1 p_2 \cdots p_r = k_2^2 q_1 q_2 \cdots q_s \tag{0.7}$$

with p_i, q_i prime. $k_1^2 | n$ but $k_1 \not| q_1 q_2 \cdots q_s$, since no square divides $q_1 q_2 \cdots q_s$. Therefore $k_1 | k_2$. By the same logic, $k_2 | k_1$, so $k_1 = k_2$. □

Lemma 0.6. *If is an odd prime, then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4. \end{cases} \tag{0.8}$$

Proof. Euler's criterion states

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{0.9}$$

If $p \equiv 1 \pmod 4$ then $(p-1)/2$ is even and $\left(\frac{-1}{p}\right) = 1$. If $p \equiv 3 \pmod 4$ then $(p-1)/2$ is odd and $\left(\frac{-1}{p}\right) = -1$. □

Using the above lemmas, we can decompose the forward and backward directions of 0.1 into two statements.

Theorem 0.7. *(Equivalent to the forward direction of Theorem 0.1.) Suppose $n = k^2 p_1 p_2 \cdots p_r$. If any of $p_1 \dots p_r \equiv 3 \pmod 4$, then n is not representable.*

Remark 1. *(On Theorem 0.7's equivalence to the forward direction.) If $n = k^2 p_1 p_2 \cdots p_r$, and some $p_i \equiv 3 \pmod 4$, then either $p_i | k$ or $p_i \not| k$. If $p_i \not| k$ then the conditions for Theorem 0.7 with the prime power being one. If $p_i | k$, then say $p_i^f || k$, then the conditions for Theorem 0.7 are satisfied with the prime power being $2f+1$. So Theorem 0.7 implies the forward direction of Theorem 0.1.*

Theorem 0.8. *(Equivalent to the backward direction of Theorem 0.1.) For prime p, p is representable if $p = 2$ or $p \equiv 1 \pmod 4$.*

Remark 2. *(On Theorem 0.8's equivalence to the backward direction.) If $n = k^2 p_1 p_2 \cdots p_r$ with all $p_1 ... p_r = 2$ or $\equiv 1 \pmod 4$, then by 0.8, each p_i is representable. By 0.3, $p_1 p_2 \cdots p_r$ is representable and by 0.4, n is representable. Therefore Theorem 0.8 implies (the contrapositive of) the backwards direction of Theorem 0.1.*

Now all we have to do is prove Theorems 0.7 and 0.8

Proof. (of Theorem 0.7). Let $n = k^2 p_1 p_2 \cdots p_r$ and suppose without loss of generality that $p_1 = 3 \pmod 4$. Suppose for a contradiction that $n = x^2 + y^2$. Then define $d = (x, y)$, $x_1 = x/d$, $y_1 = y/d$, and $n_1 = n/d^2$. Then $n_1 = x_1^2 + y_1^2$. If $d \neq 1$, then $d^2 \not| p_i$ for any p_i (since d^2 is a square, its prime factorization must contain a square), so d^2 must divide k^2, so $(k/d)^2$ is an integer, $n_1 = (k/d)^2 p_1 p_2 \cdots p_r$.

If $p_1 | x_1$, then $p_1^2 | x_1^2$. Since $p_1 | n_1$, that implies $p_1 | y_1^2$, which could only be true if $p_1^2 | y_1^2$. But that would imply $p_1^2 | n_1$, which is not true. Therefore $p_1 \not| x_1$. That means there is a solution u to the congruence

$$x_1 u = y_1 \pmod{p_1}. \tag{0.10}$$

Thus,

$$0 \equiv n_1 \equiv x_1^2 + y_1^2 \equiv x_1^2 + (u x_1)^2 \equiv x_1^2 (1 + u^2) \pmod{p_1} \tag{0.11}$$

And since $p_1 \not| x_1$, we can cancel out x_1^2.

$$1 + u^2 \equiv 0 \pmod{p_1} \tag{0.12}$$

$$u^2 \equiv -1 \pmod{p_1} \tag{0.13}$$

But this is a contradiction, as by Lemma 0.6, -1 does not have a quadratic residue mod p. □

Proof. (of Theorem 0.8). The case $p = 2$ was shown in Lemma 0.2. Let p be a prime with $p \equiv 1 \pmod 4$. The proof works by infinite descent. We first show that there is a solution an equation of the form

$$x^2 + y^2 = kp, \tag{0.14}$$

$k \geq 1$. Then we will show that if $k > 1$, we can find some $k_1 < k$ and solution x_1, y_1 with

$$x_1^2 + y_1^2 = k_1 p. \tag{0.15}$$

Therefore a chain of k_i's could be constructed until arriving at $k_r = 1$, creating a solution.

Step 1. By 0.6, -1 has a quadratic residue and there is a solution u to

$$u^2 \equiv -1 \pmod p \tag{0.16}$$
$$u^2 + 1 \equiv 0 \pmod p \tag{0.17}$$
$$u^2 + 1^2 = kp \tag{0.18}$$

for some k. Take u to be the least residue, $0 \leq u \leq p-1$. Then $u^2 + 1 \leq p^2 - 2p$, so $kp \leq p^2 - 2p$, and we get the inequality

$$1 \leq k \leq p - 2 \tag{0.19}$$

This equation will be important later and it is important to note that since k decreases with each step, it holds with every step.

Step 2. Now we construct x_1 and y_1. First define r, s by the unique solutions to

$$r \equiv x \pmod k \qquad -\frac{k}{2} < r \leq \frac{k}{2} \tag{0.20}$$
$$s \equiv y \pmod k \qquad -\frac{k}{2} < s \leq \frac{k}{2} \tag{0.21}$$

Therefore,

$$r^2 + s^2 \equiv x^2 + y^2 \equiv 0 \pmod k. \tag{0.22}$$

Or

$$r^2 + s^2 = k_1 k \tag{0.23}$$

Now we can combine this with equation (0.14) to produce

$$\left(r^2 + s^2\right)\left(x^2 + y^2\right) = (k_1 k)(kp) = k_1 k^2 p. \tag{0.24}$$

By rearrangement similar to Lemma 0.3,

$$(rx + sy)^2 + (ry - sx)^2 = k_1 k^2 p \tag{0.25}$$

Notice that from (0.20),

$$rx + sy \equiv r^2 + s^2 \equiv 0 \pmod k \tag{0.26}$$
$$ry - sx \equiv rs - sr \equiv 0 \pmod k \tag{0.27}$$

k^2 divides each term. We can produce the integer equation

$$\left(\frac{rx + sy}{k}\right)^2 + \left(\frac{ry - sx}{k}\right)^2 = k_1 p. \tag{0.28}$$

We have produced values

$$x_1 = \frac{rx + sy}{k} \tag{0.29}$$
$$y_1 = \frac{ry - sx}{k} \tag{0.30}$$

We now need to show that $k_1 < k$ and $k_1 \neq 0$. (0.23) and the inequalities from (0.20) show that

$$k_1 k = r^2 + s^2 \leq \left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}\right)^2 = \frac{k^2}{2} \tag{0.31}$$

$$k_1 \leq \frac{k}{2} \tag{0.32}$$

If $k_1 = 0$, then from (0.23), $r = s = 0$. Then we would have from (0.20) that $k|x$ and $k|y$. Then from (0.14) we would get that $k^2|kp$, $k|p$. Either $k = 1$ (in which case we have reached a solution), or $k = p$, but this is explicitly ruled out (0.19). This completes the proof. □

Remark 3. *The proof of Theorem 0.8, and of Lemmas 0.3 and 0.4 are constructive, so provide a method to find any solution $x^2 + y^2 = n$, if n is representable.*

References

[1] U. Dudley, *Elementary number theory*, Courier Corporation, 2012.