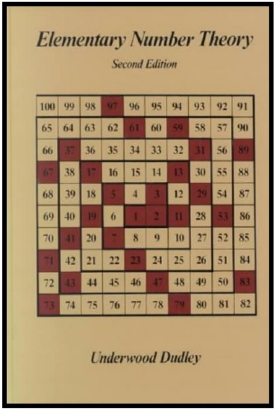
Elementary Number Theory

Section 18. Sums of Two Squares—Proofs of Theorems



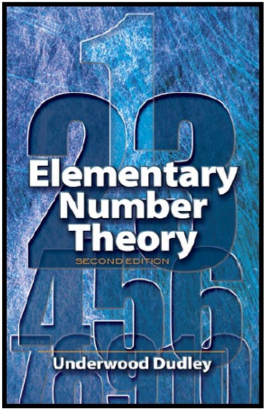


Table of contents

Lemma 18.A

Lemma 18.A. If the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares.

Proof. Suppose p is prime, where $p \equiv 3 \pmod 4$, which appears in the prime-power decomposition of n to an odd power. That is, for some integer $e \geq 0$ we have $p^{2e+1} \mid n$ and $2^{2e+2} \nmid n$. ASSUME that $n = x^2 + y^2$ for some integers x and y. Let $d = (x, y)$, $x_1 = x/d$, $y_1 y/d$, and $n_1 = n/d^2$. Then $x_1^2 + y_1^2 = n_1$ and $(x_1, y_1) = 1$. If p^f is the highest power of p that divides d, then n_1 is divisible by $p^{2e-2f+1}$. Since the exponent $2e - 2f + 1$ is nonnegative, then it is at least 1. Thus $p \mid n_1$.

Lemma 18.A

Lemma 18.A. If the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares.

Proof. Suppose p is prime, where $p \equiv 3 \pmod 4$, which appears in the prime-power decomposition of n to an odd power. That is, for some integer $e \geq 0$ we have $p^{2e+1} \mid n$ and $2^{2e+2} \nmid n$. ASSUME that $n = x^2 + y^2$ for some integers x and y. Let $d = (x, y)$, $x_1 = x/d$, $y_1 y/d$, and $n_1 = n/d^2$. Then $x_1^2 + y_1^2 = n_1$ and $(x_1, y_1) = 1$. If p^f is the highest power of p that divides d, then n_1 is divisible by $p^{2e-2f+1}$. Since the exponent $2e - 2f + 1$ is nonnegative, then it is at least 1. Thus $p \mid n_1$. If $p \mid x_1$ then (since $x_1^2 + y_1^2 = n_1$) $p \mid y_1$; but $(x_1, y_1) = 1$ so we must have that $p \nmid x_1$ and hence $(x_1, p) = 1$. Hence, by Lemma 5.2, there is (unique) u such that $x_1 u \equiv y_1 \pmod p$.

Lemma 18.A

Lemma 18.A. If the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares.

Proof. Suppose p is prime, where $p \equiv 3 \pmod 4$, which appears in the prime-power decomposition of n to an odd power. That is, for some integer $e \geq 0$ we have $p^{2e+1} \mid n$ and $2^{2e+2} \nmid n$. ASSUME that $n = x^2 + y^2$ for some integers x and y. Let $d = (x, y)$, $x_1 = x/d$, $y_1 y/d$, and $n_1 = n/d^2$. Then $x_1^2 + y_1^2 = n_1$ and $(x_1, y_1) = 1$. If p^f is the highest power of p that divides d, then n_1 is divisible by $p^{2e-2f+1}$. Since the exponent $2e - 2f + 1$ is nonnegative, then it is at least 1. Thus $p \mid n_1$. If $p \mid x_1$ then (since $x_1^2 + y_1^2 = n_1$) $p \mid y_1$; but $(x_1, y_1) = 1$ so we must have that $p \nmid x_1$ and hence $(x_1, p) = 1$. Hence, by Lemma 5.2, there is (unique) u such that $x_1 u \equiv y_1 \pmod p$.

Lemma 18.A (continued)

Lemma 18.A. If the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares.

Proof (continued). Since p divides n_1, then

$$0 \equiv n_1 \equiv x_1^2 + y_1^2 \equiv x_1^2 + (ux_1)^2 \equiv x_1^2(1 + u^2) \pmod{p}.$$

Since $(x_1, p) = 1$, then by Theorem 4.4 we can cancel the factors of x_1 to get $1 + u^2 \equiv 0 \pmod{p}$. That is, $u^2 \equiv -1 \pmod{p}$. But by Theorem 11.5, we have that the Legendre symbol $(-1/p) = -1$ since $p \equiv 3 \pmod{4}$ so that -1 is not a quadratic residue $\pmod{p}$. So no such u exists, a CONTRADICTION. So the assumption that $n = x^2 + y^2$ for some integers x and y is false, as claimed. $\square$

Lemma 18.3

Lemma 18.3. Any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$, were k is an integer and the p's are different primes.

Proof. Let the prime-power decomposition of n be $n = q_1^{e_1} q_2 p^{e_2} \cdots q_\ell^{e_\ell}$. Let set A consist of the powers of q_i's with even exponents: $A = \{q_i^{e_i} \mid e_i \text{ is even}\}$. Let set B consist of the powers of q_i's with exponents 1: $B = \{q_i^{e_i} \mid e_i = 1\}$. Let set C be the following powers of q_i's: $C = \{q_i^{e_i - 1} \mid e_i \geq 3, e_i \text{ is odd}\}$. Define k^2 to be the product of the elements of sets A and C: $k^2 = \prod_{p \in A \cup B} p$.

Lemma 18.3

Lemma 18.3. Any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$, were k is an integer and the p's are different primes.

Proof. Let the prime-power decomposition of n be $n = q_1^{e_1} q_2 p^{e_2} \cdots q_\ell^{e_\ell}$. Let set A consist of the powers of q_i's with even exponents: $A = \{q_i^{e_i} \mid e_i \text{ is even}\}$. Let set B consist of the powers of q_i's with exponents 1: $B = \{q_i^{e_i} \mid e_i = 1\}$. Let set C be the following powers of q_i's: $C = \{q_i^{e_i - 1} \mid e_i \geq 3, e_i \text{ is odd}\}$. Define k^2 to be the product of the elements of sets A and C: $k^2 = \prod_{p \in A \cup B} p$. Then $k = \prod_{p \in A} p^{1/2} \prod_{p \in C} p^{1/2}$ (since e_i is even for each element of A, and $e_i - 1$ is even for each element of C, then $p^{1/2}$ is a positive integer power of p). Let $p_1, p_2, \ldots, p_r$ denote the elements of set B. Then n is the product the elements in $A \cup B \cup C$, so that $n = k^2 p_1 p_2 \cdots p_r$, as claimed. $\square$

Lemma 18.3

Lemma 18.3. Any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$, were k is an integer and the p's are different primes.

Proof. Let the prime-power decomposition of n be $n = q_1^{e_1} q_2 p^{e_2} \cdots q_\ell^{e_\ell}$. Let set A consist of the powers of q_i's with even exponents: $A = \{q_i^{e_i} \mid e_i \text{ is even}\}$. Let set B consist of the powers of q_i's with exponents 1: $B = \{q_i^{e_i} \mid e_i = 1\}$. Let set C be the following powers of q_i's: $C = \{q_i^{e_i - 1} \mid e_i \geq 3, e_i \text{ is odd}\}$. Define k^2 to be the product of the elements of sets A and C: $k^2 = \prod_{p \in A \cup B} p$. Then $k = \prod_{p \in A} p^{1/2} \prod_{p \in C} p^{1/2}$ (since e_i is even for each element of A, and $e_i - 1$ is even for each element of C, then $p^{1/2}$ is a positive integer power of p). Let $p_1, p_2, \ldots, p_r$ denote the elements of set B. Then n is the product the elements in $A \cup B \cup C$, so that $n = k^2 p_1 p_2 \cdots p_r$, as claimed. $\square$

Exercise 18.3

Exercise 18.3. If the prime-power decomposition of n contains no prime p, where $p \equiv 3 \pmod 4$, to an odd power, then $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p is congruent to 1 (mod 4).

Proof. By Lemma 8.3, any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$ where the p's are different. If n is odd, then no p_i is 2 and since no p_i is 3 (mod 4), then each p_i must be 1 (mod 4), as claimed.

Exercise 18.3

Exercise 18.3. If the prime-power decomposition of n contains no prime p, where $p \equiv 3 \pmod 4$, to an odd power, then $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p is congruent to 1 (mod 4).

Proof. By Lemma 8.3, any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$ where the p's are different. If n is odd, then no p_i is 2 and since no p_i is 3 (mod 4), then each p_i must be 1 (mod 4), as claimed. If n is even and one of the p_i is 2, say $p_j = 2$, then we have $n = 2k^2 p_1 p_2 \cdots p_{j-1} p_{j+1} p_{j+2} \cdots p_r$. Since the prime-power decomposition contains no prime which is 3 (mod 4), then none of $p_1, p_2, \ldots, p_{j-1}, p_{j+1}, p_{j+2}, \ldots, p_r$ is 3 (mod 3) (so that each is 1 (mod 4)) and the claim holds.

Exercise 18.3

Exercise 18.3. If the prime-power decomposition of n contains no prime p, where $p \equiv 3 \pmod 4$, to an odd power, then $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p is congruent to 1 (mod 4).

Proof. By Lemma 8.3, any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$ where the p's are different. If n is odd, then no p_i is 2 and since no p_i is 3 (mod 4), then each p_i must be 1 (mod 4), as claimed. If n is even and one of the p_i is 2, say $p_j = 2$, then we have $n = 2k^2 p_1 p_2 \cdots p_{j-1} p_{j+1} p_{j+2} \cdots p_r$. Since the prime-power decomposition contains no prime which is 3 (mod 4), then none of $p_1, p_2, \ldots, p_{j-1}, p_{j+1}, p_{j+2}, \ldots, p_r$ is 3 (mod 3) (so that each is 1 (mod 4)) and the claim holds. If n is even and none of the p_i is 2 then we have $n = k^2 p_1 p_2 \cdots p_r$ where each $p_1, p_2, \ldots, p_r$ is odd and 1 (mod 4), as claimed. □

Exercise 18.3

Exercise 18.3. If the prime-power decomposition of n contains no prime p, where $p \equiv 3 \pmod 4$, to an odd power, then $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p is congruent to 1 (mod 4).

Proof. By Lemma 8.3, any integer n can be written in the form $n = k^2 p_1 p_2 \cdots p_r$ where the p's are different. If n is odd, then no p_i is 2 and since no p_i is 3 (mod 4), then each p_i must be 1 (mod 4), as claimed. If n is even and one of the p_i is 2, say $p_j = 2$, then we have $n = 2k^2 p_1 p_2 \cdots p_{j-1} p_{j+1} p_{j+2} \cdots p_r$. Since the prime-power decomposition contains no prime which is 3 (mod 4), then none of $p_1, p_2, \ldots, p_{j-1}, p_{j+1}, p_{j+2}, \ldots, p_r$ is 3 (mod 3) (so that each is 1 (mod 4)) and the claim holds. If n is even and none of the p_i is 2 then we have $n = k^2 p_1 p_2 \cdots p_r$ where each $p_1, p_2, \ldots, p_r$ is odd and 1 (mod 4), as claimed. □

Lemma 18.4

Lemma 18.4. Every prime congruent to 1 (mod 4) can be written as a sum of two squares.

Proof. Since $p \equiv 1 \pmod 4$, by Theorem 11.5, we have that the Legendre symbol $(-1/p) = 1$ since $p \equiv 1 \pmod 4$ so that -1 is a quadratic residue $\pmod p$. Hence there is u such that $u^2 \equiv -1 \pmod p$. That is $p \mid (u^2 + 1)$, and so $u^2 + 1 = kp$ for some $k \geq 1$. Hence $x^2 + y^2 = kp$ has a solution for some $k \geq 1$.

Lemma 18.4

Lemma 18.4. Every prime congruent to 1 (mod 4) can be written as a sum of two squares.

Proof. Since $p \equiv 1 \pmod 4$, by Theorem 11.5, we have that the Legendre symbol $(-1/p) = 1$ since $p \equiv 1 \pmod 4$ so that -1 is a quadratic residue $\pmod p$. Hence there is u such that $u^2 \equiv -1 \pmod p$. That is $p \mid (u^2 + 1)$, and so $u^2 + 1 = kp$ for some $k \geq 1$. Hence $x^2 + y^2 = kp$ has a solution for some $k \geq 1$. In fact, we can take $y = 1$ and $u = ((p-1)/2)!$ because

$$\begin{aligned}\left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv \left(\frac{p-1}{2}\frac{p-3}{2}\cdots(3)(2)(1)\right)^2 \\ &\equiv \left((-1)^{(p-1)/2}\frac{-(p-1)}{2}\frac{-(p-3)}{2}\cdots(-3)(-2)(-1)\right) \\ &\quad\times\left(\frac{p-1}{2}\frac{p-3}{2}\cdots(3)(2)(1)\right)\ldots\end{aligned}$$

Lemma 18.4

Lemma 18.4. Every prime congruent to 1 (mod 4) can be written as a sum of two squares.

Proof. Since $p \equiv 1 \pmod 4$, by Theorem 11.5, we have that the Legendre symbol $(-1/p) = 1$ since $p \equiv 1 \pmod 4$ so that -1 is a quadratic residue $\pmod p$. Hence there is u such that $u^2 \equiv -1 \pmod p$. That is $p \mid (u^2+1)$, and so $u^2 + 1 = kp$ for some $k \geq 1$. Hence $x^2 + y^2 = kp$ has a solution for some $k \geq 1$. In fact, we can take $y = 1$ and $u = ((p-1)/2)!$ because

$$\begin{aligned} \left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv \left(\frac{p-1}{2}\frac{p-3}{2}\cdots(3)(2)(1)\right)^2 \\ &\equiv \left((-1)^{(p-1)/2}\frac{-(p-1)}{2}\frac{-(p-3)}{2}\cdots(-3)(-2)(-1)\right) \\ &\quad \times\left(\frac{p-1}{2}\frac{p-3}{2}\cdots(3)(2)(1)\right)\ldots \end{aligned}$$

Lemma 18.4 (continued 1)

Proof (continued). ...

$$\begin{aligned}\left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv \left(\frac{(p+1)}{2}\frac{p(p+3)}{2}\cdots(p-3)(p-2)(p-1)\right)\\ &\quad\times\left(\frac{p-1}{2}\frac{p-3}{2}\cdots(3)(2)(1)\right) \text{ since } (p-1)/2 \text{ is even}\\ &\equiv (p-1)! \equiv -1 \pmod{p} \text{ by Theorem 10.B.}\end{aligned}$$

Let k be the least positive integer such that $x^2+y^2=kp$ has some integer solution x and y. If we can show that $k=1$, then we have $x^2+y^2=p$, as desired. For $x^2+y^2=kp$, define integers r and s by:

$$r \equiv x \pmod{k},\ s \equiv y \pmod{k},\quad \text{where } -\frac{k}{2} < r \le \frac{k}{2},\ -\frac{k}{2} < s \le \frac{k}{2}.$$

By Lemma 4.1 we have $r^2+s^2 \equiv x^2+y^2 \pmod{k}$.

Lemma 18.4 (continued 1)

Proof (continued). ...

$$\begin{aligned}\left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv \left(\frac{(p+1)}{2}\frac{p(p+3)}{2}\cdots(p-3)(p-2)(p-1)\right)\\ &\quad\times\left(\frac{p-1}{2}\frac{p-3}{2}\cdots(3)(2)(1)\right) \text{ since } (p-1)/2 \text{ is even}\\ &\equiv (p-1)! \equiv -1 \pmod{p} \text{ by Theorem 10.B.}\end{aligned}$$

Let k be the least positive integer such that $x^2+y^2=kp$ has some integer solution x and y. If we can show that $k=1$, then we have $x^2+y^2=p$, as desired. For $x^2+y^2=kp$, define integers r and s by:

$$r \equiv x \pmod{k},\ s \equiv y \pmod{k}, \text{ where } -\frac{k}{2} < r \le \frac{k}{2},\ -\frac{k}{2} < s \le \frac{k}{2}.$$

By Lemma 4.1 we have $r^2+s^2 \equiv x^2+y^2 \pmod{k}$.

Lemma 18.4 (continued 2)

Proof (continued). Since $x^2 + y^2 = kp$ and $r^2 + s^2 \equiv x^2 + y^2 \pmod{k}$, then $r^2 + s^2 \equiv 0 \pmod{k}$, or $r^2 + s^2 = k_1 k$ for some k_1. It follows that $(r^2 + s^2)(x^2 + y^2) = (k_1 k)(kp) = k_1 k^2 p$. By Lemma 18.1, $(r^2 + s^2)(x^2 + y^2) = (rx + sy)^2 + (ry - sx)^2$. Thus

$$k_1 k^2 p = (rx + sy)^2 + (ry - sx)^2. \qquad (*)$$

Since $r \equiv x \pmod{k}$ and $s \equiv y \pmod{k}$ then we have $rx + sy \equiv r^2 + s^2 \equiv 0 \pmod{k}$, and $ry - sx \equiv rs - sr \equiv 0 \pmod{k}$. Thus k^2 divides $(rx + sy)^2$ and $(ry - sx)^2$, and so from $(*)$ we have

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

an equation in integers. Let $x_1 = (rx + sy)/k$ and $y_1 = (ry - sx)/k$, so that $x_1^2 + y_1^2 = k_1 p$.

Lemma 18.4 (continued 2)

Proof (continued). Since $x^2 + y^2 = kp$ and $r^2 + s^2 \equiv x^2 + y^2 \pmod{k}$, then $r^2 + s^2 \equiv 0 \pmod{k}$, or $r^2 + s^2 = k_1 k$ for some k_1. It follows that $(r^2 + s^2)(x^2 + y^2) = (k_1 k)(kp) = k_1 k^2 p$. By Lemma 18.1, $(r^2 + s^2)(x^2 + y^2) = (rx + sy)^2 + (ry - sx)^2$. Thus

$$k_1 k^2 p = (rx + sy)^2 + (ry - sx)^2. \qquad (*)$$

Since $r \equiv x \pmod{k}$ and $s \equiv y \pmod{k}$ then we have $rx + sy \equiv r^2 + s^2 \equiv 0 \pmod{k}$, and $ry - sx \equiv rs - sr \equiv 0 \pmod{k}$. Thus k^2 divides $(rx + sy)^2$ and $(ry - sx)^2$, and so from $(*)$ we have

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

an equation in integers. Let $x_1 = (rx + sy)/k$ and $y_1 = (ry - sx)/k$, so that $x_1^2 + y_1^2 = k_1 p$.

Lemma 18.4 (continued 3)

Lemma 18.4. Every prime congruent to 1 (mod 4) can be written as a sum of two squares.

Proof (continued). Since we chose r and s such that $-k/2 < r \leq k/2$ and $-k/2 < s \leq k/2$., then we have $r^2 + s^2 \leq (k/2)^2 + (k/2)^2 = k^2/2$. But $r^2 + s^2 = k_1 k$ as shown above, so $k_1 k \leq k^2/2$ or $k_1 \leq k/2$. Hence $k_1 < k$.

If $k_1 \geq 1$, then we have $1 \leq k_1 < k$ and that $x^2 + y^2 = k_1 p$ has a solution for $x = x_1$ and $y = y_1$. But this contradicts the fact that k is a minimal value for which $x^2 + y^2 = kp$ has a solution for some x and y. So we must have $k_1 = 0$. Then we have $r = s = 0$. Since $r \equiv x \pmod{k}$ and $s \equiv y \pmod{k}$, we have $k \mid x$ and $k \mid y$. So $k^2 \mid (x^2 + y^2)$ and, since $x^2 + y^2 = kp$, then $k \mid p$. Hence $k = 1$ or $k = p$. If $k = p$, then $u^2 + 1 = p^2$, a contradiction because there are no consecutive positive square numbers. Therefore $k = 1$ and $x^2 + y^2 = kp = p$ has a solution, as claimed. □

Lemma 18.4 (continued 3)

Lemma 18.4. Every prime congruent to 1 (mod 4) can be written as a sum of two squares.

Proof (continued). Since we chose r and s such that $-k/2 < r \leq k/2$ and $-k/2 < s \leq k/2$., then we have $r^2 + s^2 \leq (k/2)^2 + (k/2)^2 = k^2/2$. But $r^2 + s^2 = k_1 k$ as shown above, so $k_1 k \leq k^2/2$ or $k_1 \leq k/2$. Hence $k_1 < k$.

If $k_1 \geq 1$, then we have $1 \leq k_1 < k$ and that $x^2 + y^2 = k_1 p$ has a solution for $x = x_1$ and $y = y_1$. But this contradicts the fact that k is a minimal value for which $x^2 + y^2 = kp$ has a solution for some x and y. So we must have $k_1 = 0$. Then we have $r = s = 0$. Since $r \equiv x \pmod{k}$ and $s \equiv y \pmod{k}$, we have $k \mid x$ and $k \mid y$. So $k^2 \mid (x^2 + y^2)$ and, since $x^2 + y^2 = kp$, then $k \mid p$. Hence $k = 1$ or $k = p$. If $k = p$, then $u^2 + 1 = p^2$, a contradiction because there are no consecutive positive square numbers. Therefore $k = 1$ and $x^2 + y^2 = kp = p$ has a solution, as claimed. □

Theorem 18.1

Theorem 18.1. Integer 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 (mod 4) to an odd power.

Proof. By Lemma 18.A, if the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares, as claimed.

Theorem 18.1

Theorem 18.1. Integer 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 (mod 4) to an odd power.

Proof. By Lemma 18.A, if the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares, as claimed.

Now assume the prime-power decomposition of n contains no prime p to an odd power, where $p \equiv 3 \pmod 4$. Then by Exercise 18.3, we have that either $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p_i is congruent to 1 (mod 4).

Theorem 18.1

Theorem 18.1. Integer 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 (mod 4) to an odd power.

Proof. By Lemma 18.A, if the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares, as claimed.

Now assume the prime-power decomposition of n contains no prime p to an odd power, where $p \equiv 3 \pmod 4$. Then by Exercise 18.3, we have that either $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p_i is congruent to 1 (mod 4). Now $2 = 1^2 + 1^2$ and each p_i can be written as a sum of two squares by lemma 18.4. So by Note 18.A, both $p_1 p_2 \cdots p_r$ and $2p_1 p_2 \cdots p_r$, where each p_i is congruent to 1 (mod 4), can be written as a sum of two squares. Lemma 18.3 then implies that for any k, $k^2 p_1 p_2 \cdots p_r$ and $2k^2 p_1 p_2 \cdots p_r$ can be written as a sum of two squares. Since n must be of one of these two forms, then n can be written as a sum of two squares, as claimed. □

Theorem 18.1

Theorem 18.1. Integer 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 (mod 4) to an odd power.

Proof. By Lemma 18.A, if the prime-power decomposition of n contains a prime congruent to 3 (mod 4) which is raised to an odd power, then n cannot be written as the sum of two squares, as claimed.

Now assume the prime-power decomposition of n contains no prime p to an odd power, where $p \equiv 3 \pmod 4$. Then by Exercise 18.3, we have that either $n = k^2 p_1 p_2 \cdots p_r$ or $n = 2k^2 p_1 p_2 \cdots p_r$ for some k and r, where each p_i is congruent to 1 (mod 4). Now $2 = 1^2 + 1^2$ and each p_i can be written as a sum of two squares by lemma 18.4. So by Note 18.A, both $p_1 p_2 \cdots p_r$ and $2p_1 p_2 \cdots p_r$, where each p_i is congruent to 1 (mod 4), can be written as a sum of two squares. Lemma 18.3 then implies that for any k, $k^2 p_1 p_2 \cdots p_r$ and $2k^2 p_1 p_2 \cdots p_r$ can be written as a sum of two squares. Since n must be of one of these two forms, then n can be written as a sum of two squares, as claimed. □