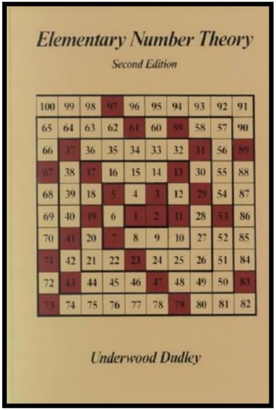
Elementary Number Theory

Section 19. Sums of Four Squares—Proofs of Theorems



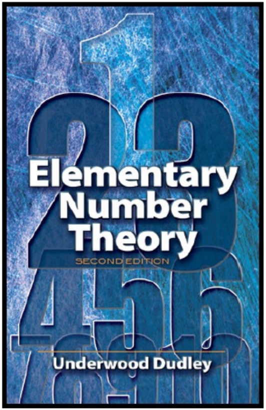


Table of contents

Lemma 19.2

Lemma 19.2. If p is an odd prime, then the equation $1 + x^2 + y^2 \equiv 0 \pmod{p}$ has a solution with $0 \leq x < p/2$ and $0 \leq y < p/2$.

Proof. The elements of $S_1 = \{0^2, 1^2, 2^2, \ldots, ((p-1)/2)^2\}$ are distinct (mod p) because by Lemma 11.1 the equation $x^2 \equiv a$ (mod$p$) (where $p \nmid a$) has exactly two (least residue) solutions or no solution (so as a ranges over the nonzero values of S_1, the two solutions are 1 and $p-1$, 2 and $p-2$, ..., $(p-1)/2$ and $(p_1)/2$, respectively). Hence, the elements in the set $S_2 = \{-1-0^2, -1-2^2, \ldots, -1-((p-1)/2)^2\}$ are distinct (mod p).

Lemma 19.2

Lemma 19.2. If p is an odd prime, then the equation $1 + x^2 + y^2 \equiv 0 \pmod{p}$ has a solution with $0 \leq x < p/2$ and $0 \leq y < p/2$.

Proof. The elements of $S_1 = \{0^2, 1^2, 2^2, \ldots, ((p-1)/2)^2\}$ are distinct (mod p) because by Lemma 11.1 the equation $x^2 \equiv a$ (mod$p$) (where $p \nmid a$) has exactly two (least residue) solutions or no solution (so as a ranges over the nonzero values of S_1, the two solutions are 1 and $p-1$, 2 and $p-2$, ..., $(p-1)/2$ and $(p_1)/2$, respectively). Hence, the elements in the set $S_2 = \{-1-0^2, -1-2^2, \ldots, -1-((p-1)/2)^2\}$ are distinct (mod p). Now the number of elements in S_1 plus the number of elements in S_2 is $((p+1)/2+1)+((p-1)/2+1) = p+1$. Since there are only p least residues modulo p, we must have (by the Pigeonhole Principle) that one of the numbers in S_1 is congruent to one of the numbers in S_2, say $x^2 \in S_1$ and $-1-y^2 \in S_2$ where $x^2 \equiv -1-y^2 \pmod{p}$ and $0 \leq x \leq (p-1)/2$, $0 \leq y \leq (p-1)/2$, as desired. □

Lemma 19.2

Lemma 19.2. If p is an odd prime, then the equation $1 + x^2 + y^2 \equiv 0 \pmod{p}$ has a solution with $0 \leq x < p/2$ and $0 \leq y < p/2$.

Proof. The elements of $S_1 = \{0^2, 1^2, 2^2, \ldots, ((p-1)/2)^2\}$ are distinct (mod p) because by Lemma 11.1 the equation $x^2 \equiv a$ (mod$p$) (where $p \nmid a$) has exactly two (least residue) solutions or no solution (so as a ranges over the nonzero values of S_1, the two solutions are 1 and $p-1$, 2 and $p-2$, ..., $(p-1)/2$ and $(p_1)/2$, respectively). Hence, the elements in the set $S_2 = \{-1-0^2, -1-2^2, \ldots, -1-((p-1)/2)^2\}$ are distinct (mod p). Now the number of elements in S_1 plus the number of elements in S_2 is $((p+1)/2+1) + ((p-1)/2+1) = p+1$. Since there are only p least residues modulo p, we must have (by the Pigeonhole Principle) that one of the numbers in S_1 is congruent to one of the numbers in S_2, say $x^2 \in S_1$ and $-1-y^2 \in S_2$ where $x^2 \equiv -1-y^2 \pmod{p}$ and $0 \leq x \leq (p-1)/2$, $0 \leq y \leq (p-1)/2$, as desired. □

Lemma 19.3

Lemma 19.3. For every odd prime p, there is a positive integer m, $m < p$, such that the equation $mp = x^2 + y^2 + z^2 + w^2$ has a solution.

Proof. By Lemma 19.2, there are x and y, with $0 \leq x \leq p/2$ and $0 \leq y \leq p/2$, such that $mp = x^2 + y^2 + 1^2 + 0^2$ for some positive m. Then we have

$$mp = x^2 + y^2 + 1 < p^2/4 + p^2/4 + 1 < p^2,$$

so that $m < p$, as claimed. □

Lemma 19.3

Lemma 19.3. For every odd prime p, there is a positive integer m, $m < p$, such that the equation $mp = x^2 + y^2 + z^2 + w^2$ has a solution.

Proof. By Lemma 19.2, there are x and y, with $0 \leq x \leq p/2$ and $0 \leq y \leq p/2$, such that $mp = x^2 + y^2 + 1^2 + 0^2$ for some positive m. Then we have

$$mp = x^2 + y^2 + 1 < p^2/4 + p^2/4 + 1 < p^2,$$

so that $m < p$, as claimed. □

Lemma 19.4

Lemma 19.4. If m and p are odd, with $1 < m < p$, and $mp = x^2 + y^2 + z^2 + w^2$, then there is a positive integer k_1 with $1 \leq k_1 < m$ such that $k_1 p = x_1^2 + y_1^2 + z_1^2 + w_z^2$ for some integers x_1, y_1, z_1, w_1.

Proof. First, let m and p be odd, with $1 < m < p$, and $mp = x^2 + y^2 + z^2 + w^2$. If m is even, then x, y, z, w are either all odd, or all even, or two are odd and two are even. In each case, $x \equiv y \pmod 2$ and $z \equiv w \pmod 2$. Hence, as can be verified by multiplying out,

$$\frac{mp}{2} = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2.$$

If $m/2$ is even, we can repeat the process and express $(m/4)p$ as a sum of four squares. Then, if $m/4$ is even then we can repeat the process and express $(m/8)p$ as a sum of four squares. This process can be repeated until we have an odd multiple of p written as a sum of four squares.

Lemma 19.4

Lemma 19.4. If m and p are odd, with $1 < m < p$, and $mp = x^2 + y^2 + z^2 + w^2$, then there is a positive integer k_1 with $1 \leq k_1 < m$ such that $k_1 p = x_1^2 + y_1^2 + z_1^2 + w_z^2$ for some integers x_1, y_1, z_1, w_1.

Proof. First, let m and p be odd, with $1 < m < p$, and $mp = x^2 + y^2 + z^2 + w^2$. If m is even, then x, y, z, w are either all odd, or all even, or two are odd and two are even. In each case, $x \equiv y \pmod 2$ and $z \equiv w \pmod 2$. Hence, as can be verified by multiplying out,

$$\frac{mp}{2} = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2.$$

If $m/2$ is even, we can repeat the process and express $(m/4)p$ as a sum of four squares. Then, if $m/4$ is even then we can repeat the process and express $(m/8)p$ as a sum of four squares. This process can be repeated until we have an odd multiple of p written as a sum of four squares.

Lemma 19.4 (continued 1)

Proof (continued). So, without loss of generality, we can assume from the beginning that m is odd. Now choose A, B, C, D such that

$$A \equiv x \pmod{m}, \;\; B \equiv y \pmod{m}, \;\; C \equiv z \pmod{m}, \;\; D \equiv w \pmod{m}$$

and $-m/2 < A, B, C, D < m/2$ (which can be done since m is odd). We then have $A^2 + B^2 + C^2 + D^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod{m}$, or $A^2 + B^2 + C^2 + D^2 = km$ for some k. Since

$$km = A^2 + B^2 + C^2 + D^2 < m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2,$$

then we must have $0 < k < m$.

Lemma 19.4 (continued 1)

Proof (continued). So, without loss of generality, we can assume from the beginning that m is odd. Now choose A, B, C, D such that

$$A \equiv x \pmod{m},\ \ B \equiv y \pmod{m},\ \ C \equiv z \pmod{m},\ \ D \equiv w \pmod{m}$$

and $-m/2 < A, B, C, D < m/2$ (which can be done since m is odd). We then have $A^2 + B^2 + C^2 + D^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod{m}$, or $A^2 + B^2 + C^2 + D^2 = km$ for some k. Since

$$km = A^2 + B^2 + C^2 + D^2 < m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2,$$

then we must have $0 < k < m$. (If $k = 0$, then $A = B = C = D = 0$ and $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$, so $m^2 \mid x^2 + y^2 + z^2 + w^2$ and, since $x^2 + y^2 + z^2 + w^2 = mp$ by hypothesis, then $m^2 \mid mp$. But this implies $m \mid p$ in contradiction to the hypothesis that $1 < m < p$.)

Lemma 19.4 (continued 1)

Proof (continued). So, without loss of generality, we can assume from the beginning that m is odd. Now choose A, B, C, D such that

$$A \equiv x \pmod{m},\;\; B \equiv y \pmod{m},\;\; C \equiv z \pmod{m},\;\; D \equiv w \pmod{m}$$

and $-m/2 < A, B, C, D < m/2$ (which can be done since m is odd). We then have $A^2 + B^2 + C^2 + D^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod{m}$, or $A^2 + B^2 + C^2 + D^2 = km$ for some k. Since

$$km = A^2 + B^2 + C^2 + D^2 < m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2,$$

then we must have $0 < k < m$. (If $k = 0$, then $A = B = C = D = 0$ and $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$, so $m^2 \mid x^2 + y^2 + z^2 + w^2$ and, since $x^2 + y^2 + z^2 + w^2 = mp$ by hypothesis, then $m^2 \mid mp$. But this implies $m \mid p$ in contradiction to the hypothesis that $1 < m < p$.)

Lemma 19.4 (continued 2)

Proof (continued). Thus $m^2kp = (mp)(km) = (x^2 + y^2 + z^2 + w^2)(A^2 + B^2 + C^2 + D^2)$, and by Lemma 19.1 we have

$$\begin{aligned} m^2kp &= (xA + yB + zC + wD)^2 + (xB - yA + zD - wC)^2 \\ &\quad +(xC - yD - zA + wB)^2 + (xD + yC - zB - wA)^2. \end{aligned}$$

Since modulo m we have $x \equiv A$, $y \equiv B$, $z \equiv C$, and $w \equiv D$, then each parenthetic term is divisible by m:

$$xA + yB + zC + wD \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m},$$

$$xB - yA + zD - wC \equiv xy - yx + zw - wz \equiv 0 \pmod{m},$$

$$xC - yD - zA + wB \equiv xz - yw - zx + wy \equiv 0 \pmod{m},$$

$$xD + yC - zB - wA \equiv xw + yz - zy - wx \equiv 0 \pmod{m}.$$

Lemma 19.4 (continued 3)

Lemma 19.4. If m and p are odd, with $1 < m < p$, and $mp = x^2 + y^2 + z^2 + w^2$, then there is a positive integer k_1 with $1 \leq k_1 < m$ such that $k_1 p = x_1^2 + y_1^2 + z_1^2 + w_z^2$ for some integers x_1, y_1, z_1, w_1.

Proof (continued). So if we put

$$x_1 = (xA + yB + zC + wD)/m, \;\; y_1 = (xB - yA + zD - wC)/m,$$

$$z_1 = (xC - yD - zA + wB)/m, \;\; w_1 = (xD + yC - zB - wA)/m,$$

then we have $x_1^2 + y_1^2 + z_1^2 + w_1^2 = (m^2 kp)/m^2 = kp$. As shown above we have $0 < k < m$, so with $k_1 = k$ we have $k_1 p = x_1^2 + y_1^2 + z_1^2 + w_z^2$ where $0 < k_1 < m$, as claimed. □

Lemma 19.A

Lemma 19.A. Every prime p can be written as the sum of four integer squares.

Proof. For $p = 2$, we have $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$. So we can assume that p is an odd prime. By Lemma 19.2, there is positive integer $m < p$ such that $mp = x^2 + y^2 + z^2 + w^2$ has a solution. Let m be a minimum such positive integer m.

Lemma 19.A

Lemma 19.A. Every prime p can be written as the sum of four integer squares.

Proof. For $p = 2$, we have $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$. So we can assume that p is an odd prime. By Lemma 19.2, there is positive integer $m < p$ such that $mp = x^2 + y^2 + z^2 + w^2$ has a solution. Let m be a minimum such positive integer m. ASSUME $m > 1$. Then by Lemma 19.4, there is positive $k_1 < m$ such that $k_1 p = x^2 + y^2 + z^2 + w^2$. But this CONTRADICTS the minimality of positive integer m. This contradictions shows that $m = 1$. (Dudley describes this in terms of Fermat's infinite descent.) That is, $p = x^2 + y^2 + z^2 + w^2$ has a solution, and hence p is the some of four integer squares, as claimed. □

Lemma 19.A

Lemma 19.A. Every prime p can be written as the sum of four integer squares.

Proof. For $p = 2$, we have $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$. So we can assume that p is an odd prime. By Lemma 19.2, there is positive integer $m < p$ such that $mp = x^2 + y^2 + z^2 + w^2$ has a solution. Let m be a minimum such positive integer m. ASSUME $m > 1$. Then by Lemma 19.4, there is positive $k_1 < m$ such that $k_1 p = x^2 + y^2 + z^2 + w^2$. But this CONTRADICTS the minimality of positive integer m. This contradictions shows that $m = 1$. (Dudley describes this in terms of Fermat's infinite descent.) That is, $p = x^2 + y^2 + z^2 + w^2$ has a solution, and hence p is the some of four integer squares, as claimed. □

Theorem 19.1

Theorem 19.1. Lagrange's Four-Square Theorem.
Every positive integer can be written as the sum of four integer squares.

Proof. Let n be a positive integer. Suppose that the prime-power decomposition of n is $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. By Lemma 19.A, each p_i can be written as the sum of four integer squares. By Lemma 19.1 (and induction), we then have that the $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ can be written as the sum of four integer squares, as claimed. □

Theorem 19.1

Theorem 19.1. Lagrange's Four-Square Theorem.
Every positive integer can be written as the sum of four integer squares.

Proof. Let n be a positive integer. Suppose that the prime-power decomposition of n is $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. By Lemma 19.A, each p_i can be written as the sum of four integer squares. By Lemma 19.1 (and induction), we then have that the $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ can be written as the sum of four integer squares, as claimed. □