CHAPTER 5

Sums of Integer Squares

5.1. Sums of Two Squares

In this section, we characterize all natural numbers which are representable as the sum of two integer squares. In other words, we determine all numbers $n \in \mathbb{N}$ such that the equation

$$n = x_1^2 + x_2^2$$

is soluble in $x_1, x_2 \in \mathbb{Z}$.

The first step in our argument is provided by the following result on the special case when n is a prime congruent to 1 modulo 4.

THEOREM 5.1 (Fermat). *Suppose that $p \in \mathbb{N}$ is prime and $p \equiv 1 \bmod 4$. Then p is representable as the sum of two integer squares; in other words, there exist $x_1, x_2 \in \mathbb{Z}$ such that $p = x_1^2 + x_2^2$.*

We first give the original proof by Fermat using his method of descent. In the next section, we give an alternative proof by Thue which contains ideas that we can develop further to study the number of representations of a natural number as a sum of two integer squares.

PROOF OF THEOREM 5.1. Since $p \equiv 1 \bmod 4$, it follows from Theorem 4.3 that $(-1/p)_L = 1$, and so -1 is a quadratic residue modulo p. The numbers

$$-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}$$

form a complete set of residues modulo p. It follows that one of the elements, x_0 say, satisfies $x_0^2 + 1 \equiv 0 \bmod p$. Since $|x_0| < p/2$, we must have

$$p \leqslant x_0^2 + 1 < \left(\frac{p}{2}\right)^2 + 1 < p^2.$$

In particular, there exists $m \in \mathbb{N}$ satisfying $1 \leqslant m < p$ such that mp can be expressed as a sum of two integer squares. It now suffices to show that the least positive multiple of p which can be expressed as a sum of two integer squares must be p itself.

We prove this by showing that if mp, where $1 < m < p$, is a sum of two integer squares, then there exists $m_0 \in \mathbb{N}$ satisfying $1 \leqslant m_0 < m$ such that $m_0 p$ is also a sum of two integer squares. Suppose now that $1 < m < p$ and

$$mp = x_1^2 + x_2^2, \tag{5.1}$$

where $x_1, x_2 \in \mathbb{Z}$. We define $y_1, y_2 \in \mathbb{Z}$ by writing

$$-\frac{m}{2} < y_1 < \frac{m}{2} \quad \text{and} \quad y_1 \equiv x_1 \bmod m, \tag{5.2}$$

and

$$-\frac{m}{2} < y_2 < \frac{m}{2} \quad \text{and} \quad y_2 \equiv x_2 \bmod m. \tag{5.3}$$

In view of (5.1), we have $y_1^2 + y_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \bmod m$, so there exists $m_0 \in \mathbb{Z}$ such that

$$y_1^2 + y_2^2 = mm_0. \tag{5.4}$$

Combining (5.2)–(5.4), we have

$$mm_0 \leqslant \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = \frac{m^2}{2},$$

so that $m_0 < m$. On the other hand, we must have $m_0 \neq 0$, for otherwise $y_1 = y_2 = 0$, so that $x_1 \equiv x_2 \equiv 0 \bmod m$, and so $m^2 \mid (x_1^2 + x_2^2)$, whence $m \mid p$, contradicting that $1 < m < p$. We therefore must have $1 \leqslant m_0 < m$. Combining (5.1) and (5.4), we now have

$$m_0 p m^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2. \tag{5.5}$$

By (5.1)–(5.3), we have

$$x_1y_1 + x_2y_2 \equiv x_1^2 + x_2^2 \equiv 0 \bmod m,$$

and

$$x_1y_2 - x_2y_1 \equiv x_1x_2 - x_2x_1 \equiv 0 \bmod m.$$

It follows that each term on the right-hand side of (5.5) is divisible by m^2, so that

$$m_0 p = \left(\frac{x_1y_1 + x_2y_2}{m}\right)^2 + \left(\frac{x_1y_2 - x_2y_1}{m}\right)^2,$$

and the proof is complete. ◯

We now determine all the natural numbers which are sums of two integer squares.

THEOREM 5.2. *Suppose that $n \in \mathbb{N}$ and $n > 1$, and the canonical decomposition of n is given by*

$$n = 2^r p_1^{r_1} \dots p_k^{r_k} q_1^{s_1} \dots q_\ell^{s_\ell},$$

where the integer $r \geqslant 0$ and $r_1, \dots, r_k, s_1, \dots, s_\ell \in \mathbb{N}$, and $p_1, \dots, p_k, q_1, \dots, q_\ell \in \mathbb{N}$ are primes satisfying $p_1 \equiv \dots \equiv p_k \equiv 1 \bmod 4$ and $q_1 \equiv \dots \equiv q_\ell \equiv 3 \bmod 4$. Then n is a sum of two integer squares if and only if $s_1, \dots, s_\ell$ are all even.

PROOF. Suppose first of all that $n = x_1^2 + x_2^2$, where $x_1, x_2 \in \mathbb{Z}$. Then

$$x_1^2 + x_2^2 \equiv 0 \bmod q_1. \tag{5.6}$$

Suppose on the contrary that s_1 is odd. If $q_1 \nmid x_2$, then it follows from Theorem 3.8 that there exists $x \in \mathbb{Z}$ such that $x_2 x \equiv 1 \bmod q_1$. Multiplying (5.6) by x^2 gives $(x_1x)^2 \equiv -1 \bmod q_1$, impossible since -1 is a quadratic non-residue modulo q_1. It follows that $q_1 \mid x_2$, and so $q_1 \mid x_1$ also. Writing $x_1 = q_1y_1$ and $x_2 = q_1y_2$, we have $n = q_1^2(y_1^2 + y_2^2)$. Hence $s_1 \geqslant 3$. Repeating the argument on n/q_1^2 yields $s_1 - 2 \geqslant 3$. Repeating the argument a sufficient number of times leads eventually to a contradiction. It follows that s_1 must be even. A similar argument shows that $s_2, \dots, s_\ell$ are all even.

The converse follows from the identity

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2, \tag{5.7}$$

on noting that we can apply Theorem 5.1 to each of the primes $p_1, \dots, p_k$, that 2 is a sum of two integer squares, and that $q_j^2 = q_j^2 + 0^2$ is a sum of two integer squares for every $j = 1, \dots, \ell$. ◯

5.2. Number of Representations

A natural question that arises concerns the number of ways any given $n \in \mathbb{N}$ can be represented as a sum of two integer squares. Our starting point is the following alternative proof of Fermat's theorem by Thue.

SECOND PROOF OF THEOREM 5.1. Let $x = (\frac{p-1}{2})!$. Since $4 \mid (p-1)$, it follows that $\frac{p-1}{2}$ is an even integer, and so

$$x^2 = (-1)^{\frac{p-1}{2}} \prod_{r=1}^{\frac{p-1}{2}} r^2 = \prod_{r=1}^{\frac{p-1}{2}} r(-r) \equiv \prod_{r=1}^{\frac{p-1}{2}} r(p-r) = (p-1)! \equiv -1 \bmod p$$

by Wilson's theorem. Hence the congruence

$$x^2 + 1 \equiv 0 \bmod p \tag{5.8}$$

is soluble. We now show that if $x \in \mathbb{Z}$ is a solution of (5.8), then there exist $a, b \in \mathbb{Z}$ such that

$$|a| < p^{\frac{1}{2}}, \quad |b| < p^{\frac{1}{2}}, \quad ab \neq 0 \quad \text{and} \quad ax \equiv b \bmod p. \tag{5.9}$$

If (5.9) holds, then $0 < a^2 + b^2 < 2p$ and

$$a^2 + b^2 \equiv a^2 + (ax)^2 = a^2(1 + x^2) \equiv 0 \bmod p,$$

so that $a^2 + b^2 = p$. To prove (5.9), consider the numbers of the form $ux - v$, where $u, v \in \mathbb{Z}$ satisfy $0 \leqslant u \leqslant p^{\frac{1}{2}}$ and $0 \leqslant v \leqslant p^{\frac{1}{2}}$. There are $([p^{\frac{1}{2}}] + 1)^2 > p$ choices of such numbers u and v, and only p residue classes modulo p. It follows from Dirichlet's box principle that there exist two such pairs u', v' and u'', v'' such that $u'x - v'$ and $u''x - v''$ belong to the same residue class modulo p and so are congruent to each other modulo p. Now let $a = u' - u''$ and $b = v' - v''$. Then

$$ax - b = (u' - u'')x - (v' - v'') \equiv 0 \bmod p.$$

Clearly we have $|a| < p^{\frac{1}{2}}$ and $|b| < p^{\frac{1}{2}}$. Finally, if $b = 0$, then we must have $a \equiv 0 \bmod p$, and so $a = 0$, a contradiction. Hence $b \neq 0$. Similarly $a \neq 0$. ◯

Our first step towards finding a formula for the number of representations of a natural number as a sum of two integer squares is the following generalization of the above proof of Fermat's theorem.

THEOREM 5.3. *Suppose that $n \in \mathbb{N}$ and $n > 1$. For every solution $x \in \mathbb{Z}$ of the congruence $x^2 + 1 \equiv 0 \bmod n$, there exist unique positive integers $a, b \in \mathbb{N}$ such that*

$$(a, b) = 1, \quad a^2 + b^2 = n \quad \textit{and} \quad ax \equiv b \bmod n. \tag{5.10}$$

PROOF. By considering numbers of the form $ux - v$, where $u, v \in \mathbb{Z}$ satisfy $0 \leqslant u \leqslant n^{\frac{1}{2}}$ and $0 \leqslant v \leqslant n^{\frac{1}{2}}$, we can show as before that there exist non-zero numbers $\alpha, \beta \in \mathbb{Z}$ such that

$$\alpha^2 + \beta^2 = n \quad \text{and} \quad \alpha x \equiv \beta \bmod n.$$

Clearly, we may assume without loss of generality that $\alpha > 0$.

If $\beta > 0$, then we let $a = \alpha$ and $b = \beta$. Clearly $a^2 + b^2 = n$ and $ax \equiv b \bmod n$.

If $\beta < 0$, then we let $a = -\beta$ and $b = \alpha$. Again we have $a^2 + b^2 = n$. On the other hand, we have $bx \equiv -a \bmod n$, so that $bx^2 \equiv -ax \bmod n$. It now follows from the assumption $x^2 \equiv -1 \bmod n$ that $ax \equiv b \bmod n$.

To show that $(a, b) = 1$, note that there exist $k, \ell \in \mathbb{Z}$ such that

$$x^2 + 1 = kn \quad \text{and} \quad b = ax + \ell n.$$

It follows that

$$\begin{aligned} n = a^2 + b^2 &= a^2 + (ax + \ell n)^2 = a^2(1 + x^2) + ax\ell n + (ax + \ell n)\ell n \\ &= a^2 kn + ax\ell n + b\ell n = (a(ak + x\ell) + b\ell)n, \end{aligned}$$

and so $a(ak + x\ell) + b\ell = 1$, whence $(a, b) = 1$.

Finally, to show uniqueness, suppose that the conclusion holds also for the pair $A, B \in \mathbb{N}$. Then

$$n^2 = (a^2 + b^2)(A^2 + B^2) = (aA + bB)^2 + (aB - bA)^2.$$

It follows that $0 < aA + bB \leqslant n$. On the other hand, note that

$$aA + bB \equiv aA + aAx^2 = aA(1 + x^2) \equiv 0 \bmod n.$$

We therefore must have $aA + bB = n$, and so $aB - bA = 0$. Since $(a, b) = (A, B) = 1$, we must therefore have $a = A$ and $b = B$. ◯

THEOREM 5.4. *Suppose that $n \in \mathbb{N}$, and $T(n)$ is equal to the number of solutions of the congruence $x^2 + 1 \equiv 0 \bmod n$. Then the number of solutions of the equation $n = a^2 + b^2$ with $(a, b) = 1$ is equal to $4T(n)$.*

PROOF. Suppose first of all that $n = 1$. Clearly $T(1) = 1$ and the equation $1 = a^2 + b^2$ has four solutions, namely $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$.

Suppose now that $n > 1$. We have already shown that for every solution $x \in \mathbb{Z}$ of the congruence $x^2 + 1 \equiv 0 \bmod n$, there exist unique positive integers $a, b \in \mathbb{N}$ such that (5.10) holds. Conversely, suppose that $a, b \in \mathbb{N}$ satisfy $(a, b) = 1$ and $n = a^2 + b^2$. It is easy to see that $(a, n) = 1$, and so the congruence $ax \equiv b \bmod n$ has unique solution.

The above establishes a one-to-one correspondence between the solutions of $x^2 + 1 \equiv 0 \bmod n$ and numbers $a, b \in \mathbb{N}$ such that $(a, b) = 1$ and $n = a^2 + b^2$. The factor 4 occurs if we permit negative values for a and b. ◯

THEOREM 5.5. *Suppose that $n \in \mathbb{N}$, and $T(n)$ is equal to the number of solutions of the congruence $x^2 + 1 \equiv 0 \bmod n$. Then $T(n) = 0$ if $4 \mid n$ or if n is divisible by a prime $q \equiv 3 \bmod 4$. Otherwise we have $T(n) = 2^k$, where k is the number of distinct odd prime factors of n.*

PROOF. Clearly the result is valid if $n = 1$, so we assume that $n > 1$. It is not too difficult to show that $T(n)$ is a multiplicative function. It follows that if the canonical decomposition of n is given by

$$n = 2^r p_1^{r_1} \dots p_k^{r_k} q_1^{s_1} \dots q_\ell^{s_\ell},$$

where the integer $r \geqslant 0$ and $r_1, \dots, r_k, s_1, \dots, s_\ell \in \mathbb{N}$, and $p_1, \dots, p_k, q_1, \dots, q_\ell \in \mathbb{N}$ are primes satisfying $p_1 \equiv \dots \equiv p_k \equiv 1 \bmod 4$ and $q_1 \equiv \dots \equiv q_\ell \equiv 3 \bmod 4$, then

$$T(n) = T(2^r)T(p_1^{r_1}) \dots T(p_k^{r_k})T(q_1^{s_1}) \dots T(q_\ell^{s_\ell}).$$

It is easy to check that $T(2) = 1$. Also, the congruence $x^2 \equiv -1 \bmod 4$ has no solutions, and so the congruence $x^2 \equiv -1 \bmod 2^r$ has no solutions for any $r \geqslant 2$. Hence $T(2^r) = 0$ for every $r \geqslant 2$, and so $T(n) = 0$ if $4 \mid n$.

Suppose next that $q \in \mathbb{N}$ is a prime satisfying $q \equiv 3 \bmod 4$. Since -1 is a quadratic non-residue modulo q, it follows that the congruence $x^2 \equiv -1 \bmod q$ has no solutions, and so the congruence $x^2 \equiv -1 \bmod q^s$ has no solutions for any $s \geqslant 1$. Hence $T(q^s) = 0$ for every $s \geqslant 1$, and so $T(n) = 0$ if $q \mid n$.

To complete the proof, it suffices to show that for every prime $p \in \mathbb{N}$ satisfying $p \equiv 1 \bmod 4$, we have $T(p^r) = 2$ for every $r \geqslant 1$. Suppose that $r \in \mathbb{N}$ is fixed. Any solution of the congruence $x^2 \equiv -1 \bmod p^r$ can be assumed to be an element in the set

$$\mathcal{R} = \{x \in \mathbb{N} : 0 < x < p^r,\ p \nmid x\}.$$

Now any $x \in \mathcal{R}$ must satisfy the congruence $x^2 \equiv m \bmod p^r$ for some number $m \in \mathbb{N}$ satisfying $0 < m < p^r$ and $(m/p)_L = 1$. There are $\frac{1}{2}(p-1)$ numbers $m \in \mathbb{N}$ satisfying $0 < m < p$ and $(m/p)_L = 1$, and so there are $\frac{1}{2}(p-1)p^{r-1} = \frac{1}{2}\phi(p^r)$ numbers $m \in \mathbb{N}$ satisfying $0 < m < p^r$ and $(m/p)_L = 1$. Suppose now that $x^2 \equiv y^2 \bmod p^r$ and $p \nmid x$. Then $p^r \mid (x+y)(x-y)$, so that $p \mid (x+y)$ or $p \mid (x-y)$; but not both, for otherwise p must divide their sum $2x$, a contradiction. It follows that $p^r \mid (x+y)$ or $p^r \mid (x-y)$, and so $x \equiv \pm y \bmod p^r$. Hence for each of the $\frac{1}{2}\phi(p^r)$ numbers $m \in \mathbb{N}$ satisfying $0 < m < p^r$ and $(m/p)_L = 1$, there are at most two numbers $x \in \mathcal{R}$ such that $x^2 \equiv m \bmod p^r$. Since $\mathcal{R}$ contains precisely $\phi(p^r)$ elements, it follows that for each of the $\frac{1}{2}\phi(p^r)$ numbers $m \in \mathbb{N}$ satisfying $0 < m < p^r$ and $(m/p)_L = 1$, there are precisely two numbers $x \in \mathcal{R}$ such that $x^2 \equiv m \bmod p^r$. Note now that -1 is a quadratic residue modulo p. It follows that there are precisely two numbers $x \in \mathcal{R}$ such that $x^2 \equiv -1 \bmod p^r$, and so $T(p^r) = 2$. ◯

THEOREM 5.6. *Suppose that $n \in \mathbb{N}$, and $S(n)$ is equal to the number of solutions of the equation $n = a^2 + b^2$ in numbers $a, b \in \mathbb{Z}$. Then*

$$S(n) = 4 \sum_{d^2 \mid n} T\left(\frac{n}{d^2}\right),$$

where for every $n \in \mathbb{N}$, the number $T(n)$ is equal to the number of solutions of the congruence $x^2 + 1 \equiv 0 \bmod n$.

PROOF. Suppose that $a, b \in \mathbb{Z}$ satisfy $d = (a, b)$. Clearly $d^2 \mid n$. Now write $a_1 = a/d$ and $b_1 = b/d$, and identify the pair a, b with the pair a_1, b_1, where clearly

$$\frac{n}{d^2} = a_1^2 + b_1^2 \quad \text{and} \quad (a_1, b_1) = 1.$$

The result now follows on noting Theorem 5.4. ◯

By the non-principal character modulo 4, we mean the function $\chi : \mathbb{N} \to \mathbb{R}$, defined for every $m \in \mathbb{N}$ by

$$\chi(m) = \begin{cases} 0, & \text{if } m \equiv 0 \bmod 2, \\ 1, & \text{if } m \equiv 1 \bmod 4, \\ -1, & \text{if } m \equiv 3 \bmod 4. \end{cases}$$

THEOREM 5.7. *Suppose that $n \in \mathbb{N}$, and $S(n)$ is equal to the number of solutions of the equation $n = a^2 + b^2$ in numbers $a, b \in \mathbb{Z}$. Then*

$$S(n) = 4 \sum_{m|n} \chi(m),$$

where $\chi : \mathbb{N} \to \mathbb{R}$ is the non-principal character modulo 4.

PROOF. For every $n \in \mathbb{N}$, write

$$\sum_{m|n} \chi(m) = W(n).$$

It is not difficult to show that the function $\chi(n)$ is multiplicative, and so it follows from Theorem 2.1 that the function $W(n)$ is also multiplicative. On the other hand, recall that the function $T(n)$ is multiplicative. It follows from Theorem 5.6, in a way similar to the proof of Theorem 2.1, that if $(n_1, n_2) = 1$, then

$$\frac{S(n_1 n_2)}{4} = \frac{S(n_1)}{4} \frac{S(n_2)}{4}.$$

To complete the proof, it therefore suffices to show that for any prime $p \in \mathbb{N}$ and any $r \in \mathbb{N}$, we have

$$\frac{S(p^r)}{4} = W(p^r),$$

since the result is obvious for $n = 1$.

Consider first of all

$$\frac{S(p^r)}{4} = \sum_{d^2|p^r} T\left(\frac{p^r}{d^2}\right).$$

If r is even, then

$$\frac{S(p^r)}{4} = T(p^r) + T(p^{r-2}) + \ldots + T(p^2) + T(1) = \begin{cases} 1, & \text{if } p = 2, \\ 1, & \text{if } p \equiv 3 \bmod 4, \\ r+1, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

If r is odd, then

$$\frac{S(p^r)}{4} = T(p^r) + T(p^{r-2}) + \ldots + T(p^3) + T(p) = \begin{cases} 1, & \text{if } p = 2, \\ 0, & \text{if } p \equiv 3 \bmod 4, \\ r+1, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Hence

$$\frac{S(p^r)}{4} = \begin{cases} 1, & \text{if } p = 2, \\ 1, & \text{if } p \equiv 3 \bmod 4 \text{ and } r \text{ is even}, \\ 0, & \text{if } p \equiv 3 \bmod 4 \text{ and } r \text{ is odd}, \\ r+1, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Consider next $W(p^r) = \chi(p^r) + \ldots + \chi(p) + 1$. We can show that $\chi(p^u) = (\chi(p))^u$ for every $u \in \mathbb{N}$. Hence

$$W(p^r) = (\chi(p))^r + \ldots + \chi(p) + 1 = \begin{cases} 1, & \text{if } p = 2, \\ 1, & \text{if } p \equiv 3 \bmod 4 \text{ and } r \text{ is even}, \\ 0, & \text{if } p \equiv 3 \bmod 4 \text{ and } r \text{ is odd}, \\ r+1, & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

This completes the proof. ◯

REMARK. The above treatment is due to Landau (1927) and is likely to have been influenced by Dirichlet's work concerning primes in arithmetic progressions.

5.3. Sums of Four Squares

We now study the problem of representing natural numbers as sums of four integer squares, and show that this is always possible.

THEOREM 5.8 (Lagrange). *Every $n \in \mathbb{N}$ is representable as the sum of four integer squares; in other words, for every $n \in \mathbb{N}$, there exist $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.*

PROOF. In view of the identity

$$\begin{aligned}(5.11)\qquad &(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ &\quad + (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)^2,\end{aligned}$$

it suffices to show that every prime can be expressed as a sum of four integer squares. Clearly $2 = 1^2 + 1^2 + 0^2 + 0^2$. On the other hand, it follows from Theorem 5.1 that every prime $p \equiv 1 \bmod 4$ is a sum of four integer squares. It therefore remains to prove that every prime $q \equiv 3 \bmod 4$ is a sum of four integer squares.

Naturally the number 1 is a quadratic residue modulo q. Let $a \in \mathbb{N}$ be the smallest number in the range $1 \leqslant a \leqslant q-2$ such that $a+1$ is a quadratic non-residue modulo q, so that

$$\left(\frac{a+1}{q}\right)_L = -1 \quad \text{and} \quad \left(\frac{a}{q}\right)_L = 1.$$

Since $q \equiv 3 \bmod 4$, it follows from Theorem 4.3 that $(-1/q)_L = -1$, and so

$$\left(\frac{-a-1}{q}\right)_L = \left(\frac{-1}{q}\right)_L \left(\frac{a+1}{q}\right)_L = 1.$$

In other words, there exist integers x_1 and x_2 in the complete set

$$-\frac{q-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-1}{2}$$

of residues modulo q such that $x_1^2 \equiv a \bmod q$ and $x_2^2 \equiv -a-1 \bmod q$. Hence

$$x_1^2 + x_2^2 + 1^2 + 0^2 \equiv 0 \bmod q$$

and

$$q \leqslant x_1^2 + x_2^2 + 1 < 2\left(\frac{q}{2}\right)^2 + 1 < q^2.$$

In particular, there exists $m \in \mathbb{N}$ satisfying $1 \leqslant m < q$ such that mq can be expressed as a sum of four integer squares. It now suffices to show that the least positive multiple of q which can be expressed as a sum of four integer squares must be q itself.

We prove this by showing that if mq, where $1 < m < q$, is a sum of four integer squares, then there exists $m_0 \in \mathbb{N}$ satisfying $1 \leqslant m_0 < m$ such that $m_0 q$ is also a sum of four integer squares. Suppose now that $1 < m < q$ and

$$(5.12)\qquad mq = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

where $x_1, x_2, x_3, x_4 \in \mathbb{Z}$. Suppose that m is even. Then the right hand side of (5.12) must be even. It follows that an even number of the four terms x_1, x_2, x_3, x_4 must be even, so we may assume without loss of generality that $x_1 \equiv x_2 \bmod 2$ and $x_3 \equiv x_4 \bmod 2$. It follows that

$$\frac{m}{2}q = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2.$$

We can therefore assume that m is odd. For $i = 1, 2, 3, 4$, let $y_i \in \mathbb{Z}$ satisfy

$$(5.13)\qquad -\frac{m}{2} < y_i < \frac{m}{2} \quad \text{and} \quad y_i \equiv x_i \bmod m.$$

In view of (5.12) and (5.13), we have

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod m,$$

so there exists $m_0 \in \mathbb{Z}$ such that

$$(5.14)\qquad y_1^2 + y_2^2 + y_3^2 + y_4^2 = mm_0.$$

Combining (5.13) and (5.14), we have

$$mm_0 < 4\Big(\frac{m}{2}\Big)^2 = m^2,$$

so that $m_0 < m$. On the other hand, we must have $m_0 \neq 0$, for otherwise $y_i = 0$ for every $i = 1, \ldots, 4$, so that $x_i \equiv 0 \bmod m$, and so $m^2 \mid (x_1^2 + x_2^2 + x_3^2 + x_4^2)$, whence $m \mid q$, contradicting that $1 < m < q$. We therefore must have $1 \leqslant m_0 < m$. Combining (5.11), (5.12) and (5.14), we now have

$$\begin{aligned} m_0 q m^2 = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & + (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)^2. \end{aligned} \tag{5.15}$$

By (5.12) and (5.13), we have

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod m.$$

Also each of the terms

$$x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \quad x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2, \quad x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3$$

is congruent to 0 modulo q. It follows that each term on the right hand side of (5.15) is divisible by m^2, so that m_0q is a sum of four integer squares. ◯

5.4. Sums of Three Squares

The situation is very different in the case of three integer squares. The main reason is that there is no analogue of (5.7) and (5.11) in this case. We only concern ourselves with the following simple theorem.

THEOREM 5.9. *No integer of the form $4^k(8m + 7)$, where $k, m \in \mathbb{N} \cup \{0\}$, can be represented as a sum of three squares.*

PROOF. Note first of all that every integer square is congruent to $0, 1, 4$ modulo 8, so that $(8m+7)$ is never a sum of three squares for any $m \in \mathbb{Z}$. Hence the conclusion of Theorem 5.9 is true for $k = 0$.

We now proceed by induction on k. Suppose that $4^s(8m + 7)$ is never a sum of three squares for any $m \in \mathbb{Z}$. We show that $4^{s+1}(8m + 7)$ is never a sum of three squares for any $m \in \mathbb{Z}$. Suppose on the contrary that

$$4^{s+1}(8m + 7) = x_1^2 + x_2^2 + x_3^2,$$

where $x_1, x_2, x_3 \in \mathbb{Z}$. Since $x^2 \equiv 0 \bmod 4$ if x is even and $x^2 \equiv 1 \bmod 4$ if x is odd, it follows that each of x_1, x_2, x_3 must be even, so that

$$4^s(8m + 7) = \Big(\frac{x_1}{2}\Big)^2 + \Big(\frac{x_2}{2}\Big)^2 + \Big(\frac{x_3}{2}\Big)^2,$$

a contradiction. ◯

A result of Legendre in 1798 says that every other natural number can be written as a sum of three integer squares. The main idea involves binary and ternary quadratic forms, and we do not develop these ideas here.