

# ELEMENTARY NUMBER THEORY

W W L CHEN

© W W L Chen, 1981, 2003.

This chapter originates from material used by the author at Imperial College, University of London, between 1981 and 1990.

It is available free to all individuals, on the understanding that it is not to be used for financial gains,  
and may be downloaded and/or photocopied, with or without permission from the author.

However, this document may not be kept on any information storage and retrieval system without permission  
from the author, unless such system is not accessible to any individuals other than its owners.

## Chapter 5

### SUMS OF INTEGER SQUARES

#### 5.1. Sums of Two Squares

In this section, we shall characterize all natural numbers which are representable as the sum of two integer squares. In other words, we shall 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 5A.** (FERMAT) *Suppose that  $p$  is prime and  $p \equiv 1 \pmod{4}$ . 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 shall first give the original proof by Fermat using his method of descent. In the next section, we shall 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 5A.** Since  $p \equiv 1 \pmod{4}$ , it follows from Theorem 4C that  $(-1/p)_L = 1$ , and so  $-1$  is a quadratic residue modulo  $p$ . The numbers

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

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

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

In particular, there exists  $m \in \mathbb{N}$  satisfying  $1 \leq m < p$  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 shall 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  $1 \leq m_0 < m$  such that  $m_0p$  is also a sum of two integer squares. Suppose now that  $1 < m < p$  and

$$(1) \quad mp = x_1^2 + x_2^2,$$

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

$$(2) \quad -\frac{m}{2} < y_1 < \frac{m}{2} \quad \text{and} \quad y_1 \equiv x_1 \pmod{m}$$

and

$$(3) \quad -\frac{m}{2} < y_2 < \frac{m}{2} \quad \text{and} \quad y_2 \equiv x_2 \pmod{m}.$$

In view of (1), we have  $y_1^2 + y_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{m}$ , so there exists  $m_0 \in \mathbb{Z}$  such that

$$(4) \quad y_1^2 + y_2^2 = mm_0.$$

Combining (2)–(4), we have

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

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  $x_1 \equiv x_2 \equiv 0 \pmod{m}$ , and so  $m^2 \mid (x_1^2 + x_2^2)$ , whence  $m \mid p$ , contradicting that  $1 < m < p$ . We therefore must have  $1 \leq m_0 < m$ . Combining (1) and (4), we now have

$$(5) \quad m_0pm^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2.$$

By (1)–(3), we have

$$x_1y_1 + x_2y_2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{m}$$

and

$$x_1y_2 - x_2y_1 \equiv x_1x_2 - x_2x_1 \equiv 0 \pmod{m}.$$

It follows that each term on the right hand side of (5) is divisible by  $m^2$ , so that

$$m_0p = \left(\frac{x_1y_1 + x_2y_2}{m}\right)^2 + \left(\frac{x_1y_2 - x_2y_1}{m}\right)^2,$$

and the proof is complete.  $\circ$

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

**THEOREM 5B.** *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  $r \geq 0$  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  $p_1 \equiv \dots \equiv p_k \equiv 1 \pmod{4}$  and  $q_1 \equiv \dots \equiv q_\ell \equiv 3 \pmod{4}$ . 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

$$(6) \quad x_1^2 + x_2^2 \equiv 0 \pmod{q_1}.$$

Suppose on the contrary that  $s_1$  is odd. If  $q_1 \nmid x_2$ , then it follows from Theorem 3H that there exists  $x \in \mathbb{Z}$  such that  $x_2 x \equiv 1 \pmod{q_1}$ . Multiplying (6) by  $x^2$  gives  $(x_1 x)^2 \equiv -1 \pmod{q_1}$ , 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  $x_1 = q_1 y_1$  and  $x_2 = q_1 y_2$ , we have  $n = q_1^2 (y_1^2 + y_2^2)$ . Hence  $s_1 \geq 3$ . Repeating the argument on  $n/q_1^2$  yields  $s_1 - 2 \geq 3$ . 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

$$(7) \quad (x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 + x_2 y_2)^2 + (x_1 y_2 - x_2 y_1)^2$$

on noting that we can apply Theorem 5A 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  $j = 1, \dots, \ell$ .  $\circ$

## 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 5A. Let  $x = \left(\frac{p-1}{2}\right)!$ . Since  $4 \mid (p-1)$ , it follows that  $(p-1)/2$  is an even integer, and so

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

by Wilson's theorem. Hence the congruence

$$(8) \quad x^2 + 1 \equiv 0 \pmod{p}$$

is soluble. We shall now show that if  $x \in \mathbb{Z}$  is a solution of (8), then there exist  $a, b \in \mathbb{Z}$  such that

$$(9) \quad |a| < p^{1/2}, \quad |b| < p^{1/2}, \quad ab \neq 0 \quad \text{and} \quad ax \equiv b \pmod{p}.$$

If (9) holds, then  $0 < a^2 + b^2 < 2p$  and

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

so that  $a^2 + b^2 = p$ . To prove (9), consider the numbers of the form  $ux - v$ , where  $u, v \in \mathbb{Z}$  satisfy  $0 \leq u, v \leq p^{1/2}$ . There are  $([p^{1/2}] + 1)^2 > p$  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  $ax - b = (u' - u'')x - (v' - v'') \equiv 0 \pmod{p}$ . Clearly we have  $|a| < p^{1/2}$  and  $|b| < p^{1/2}$ . Finally, if  $b = 0$ , then we must have  $a \equiv 0 \pmod{p}$ , and so  $a = 0$ , a contradiction. Hence  $b \neq 0$ . Similarly  $a \neq 0$ .  $\circ$

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 5C.** *Suppose that  $n \in \mathbb{N}$  and  $n > 1$ . For every solution  $x \in \mathbb{Z}$  of the congruence  $x^2 + 1 \equiv 0 \pmod{n}$ , there exist unique positive integers  $a, b \in \mathbb{N}$  such that*

$$(a, b) = 1, \quad a^2 + b^2 = n \quad \text{and} \quad ax \equiv b \pmod{n}.$$

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

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

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  $ax \equiv b \pmod{n}$ .

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  $bx \equiv -a \pmod{n}$ , so that  $bx^2 \equiv -ax \pmod{n}$ . It now follows from the assumption  $x^2 \equiv -1 \pmod{n}$  that  $ax \equiv b \pmod{n}$ .

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

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

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

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

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  $b = B$ .  $\square$

**THEOREM 5D.** *Suppose that  $n \in \mathbb{N}$ , and  $T(n)$  is equal to the number of solutions of the congruence  $x^2 + 1 \equiv 0 \pmod{n}$ . 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 for every solution  $x \in \mathbb{Z}$  of the congruence  $x^2 + 1 \equiv 0 \pmod{n}$ , there exist unique positive integers  $a, b \in \mathbb{N}$  such that

$$(a, b) = 1, \quad a^2 + b^2 = n \quad \text{and} \quad ax \equiv b \pmod{n}.$$

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  $ax \equiv b \pmod{n}$  has unique solution.

The above establishes a one-to-one correspondence between the solutions of the congruence  $x^2 + 1 \equiv 0 \pmod{n}$  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  $b$ .  $\circ$

**THEOREM 5E.** *Suppose that  $n \in \mathbb{N}$ , and  $T(n)$  is equal to the number of solutions of the congruence  $x^2 + 1 \equiv 0 \pmod{n}$ . Then  $T(n) = 0$  if  $4 \mid n$  or if  $n$  is divisible by a prime  $q \equiv 3 \pmod{4}$ . 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 shall assume that  $n > 1$ . Using the Chinese remainder theorem, one can show that  $T(n)$  is a multiplicative function. It follows that if the canonical decomposition of  $n$  is given by

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

where the integer  $r \geq 0$  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  $p_1 \equiv \dots \equiv p_k \equiv 1 \pmod{4}$  and  $q_1 \equiv \dots \equiv q_\ell \equiv 3 \pmod{4}$ , then

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

It is easy to check that  $T(2) = 1$ . On the other hand, the congruence  $x^2 \equiv -1 \pmod{4}$  has no solutions, and so the congruence  $x^2 \equiv -1 \pmod{2^r}$  has no solutions for any  $r \geq 2$ . Hence  $T(2^r) = 0$  for every  $r \geq 2$ , and so  $T(n) = 0$  if  $4 \mid n$ .

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

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

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

Now any  $x \in \mathcal{R}$  must satisfy the congruence  $x^2 \equiv m \pmod{p^r}$  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  $x^2 \equiv y^2 \pmod{p^r}$  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  $x \equiv \pm y \pmod{p^r}$ . 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  $x^2 \equiv m \pmod{p^r}$ . 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  $x^2 \equiv m \pmod{p^r}$ . Note now that  $-1$  is a quadratic residue modulo  $p$ . It follows that there are precisely two numbers  $x \in \mathcal{R}$  such that  $x^2 \equiv -1 \pmod{p^r}$ , and so  $T(p^r) = 2$ .  $\circ$

**THEOREM 5F.** *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  $x^2 + 1 \equiv 0 \pmod{n}$ .

PROOF. Suppose that  $a, b \in \mathbb{Z}$  satisfy  $n = a^2 + b^2$ . Write  $d = (a, b)$ . Then  $d^2 \mid n$ . If we write  $a_1 = a/d$  and  $b_1 = b/d$ , then the pair  $a_1, b_1$  satisfy

$$(10) \quad \frac{n}{d^2} = a_1^2 + b_1^2 \quad \text{and} \quad (a_1, b_1) = 1.$$

On the other hand, suppose that  $d^2 \mid n$ , and that  $a_1, b_1 \in \mathbb{Z}$  satisfy (10). If we write  $a = da_1$  and  $b = db_1$ , then  $(a, b) = d$  and  $n = a^2 + b^2$ . We can therefore identify any pair  $a, b \in \mathbb{Z}$  satisfying  $n = a^2 + b^2$  with the pair  $a_1, b_1 \in \mathbb{Z}$  satisfying (10), where  $d = (a, b)$ . The result now follows on noting Theorem 5D.  $\circ$

**THEOREM 5G.** *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*

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

where  $\chi : \mathbb{N} \rightarrow \mathbb{R}$  is the non-principal character modulo 4, defined for every  $m \in \mathbb{N}$  by

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

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

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

It is easy to show that the function  $\chi(n)$  is multiplicative, so it follows from Theorem 2A that the function  $W(n)$  is also multiplicative. On the other hand, recall that the function  $T(n)$  is multiplicative. It follows from Theorem 5F, in a way similar to the proof of Theorem 2A, 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  $p$  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

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

If  $r$  is even, then

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

If  $r$  is odd, then

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

Hence

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

Consider next

$$W(p^r) = \chi(p^r) + \dots + \chi(p) + 1.$$

It is easy to show that  $\chi(p^u) = (\chi(p))^u$  for every  $u \in \mathbb{N}$ . Hence

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

This completes the proof.  $\circ$

### 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 5H.** (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

$$(11) \quad \begin{aligned} & (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & \quad + (x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)^2, \end{aligned}$$

it suffices to show that every prime can be expressed as a sum of four integer squares. Clearly we have  $2 = 1^2 + 1^2 + 0^2 + 0^2$ . Also, it follows from Theorem 5A that every prime  $p \equiv 1 \pmod{4}$  is a sum of four integer squares. It therefore remains to prove that every prime  $q \equiv 3 \pmod{4}$  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  $1 \leq a \leq q - 2$  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  $q \equiv 3 \pmod{4}$ , it follows from Theorem 4C 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

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

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

$$x_1^2 + x_2^2 + 1^2 + 0^2 \equiv 0 \pmod{q}$$

and

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

In particular, there exists  $m \in \mathbb{N}$  satisfying  $1 \leq m < q$  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 shall 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  $1 \leq m_0 < m$  such that  $m_0q$  is also a sum of four integer squares. Suppose now that  $1 < m < q$  and

$$(12) \quad mq = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

where  $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ . If  $m$  is even, then the right hand side of (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  $x_1 \equiv x_2 \pmod{2}$  and  $x_3 \equiv x_4 \pmod{2}$ . In particular, we have

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

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

$$(13) \quad -\frac{m}{2} < y_i < \frac{m}{2} \quad \text{and} \quad y_i \equiv x_i \pmod{m}.$$

In view of (12) and (13), we have

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

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

$$(14) \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 = mm_0.$$

Combining (13) and (14), we have

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

so that  $m_0 < m$ . On the other hand, we must have  $m_0 \neq 0$ , for otherwise  $y_i = 0$  for every  $i = 1, \dots, 4$ , so that  $x_i \equiv 0 \pmod{m}$ , 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  $1 \leq m_0 < m$ . Combining (11), (12) and (14), we now have

$$(15) \quad m_0qm^2 = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + (x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)^2.$$

By (12) and (13), we have

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

Also each of the terms  $(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)$ ,  $(x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2)$  and  $(x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)$  is congruent to 0 modulo  $q$ . It follows that each term on the right hand side of (15) is divisible by  $m^2$ , so that  $m_0q$  is a sum of four integer squares.  $\circ$

#### 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 (7) and (11) in this case. Here, we shall only concern ourselves with the following simple theorem.

**THEOREM 5J.** *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 5J 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 shall 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  $x^2 \equiv 0 \pmod{4}$  if  $x$  is even and  $x^2 \equiv 1 \pmod{4}$  if  $x$  is odd, it follows that each of  $x_1, x_2, x_3$  must be even, so that

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

a contradiction.  $\circlearrowleft$

It was proved by Legendre in 1798 that all other natural numbers are representable as sums of three integer squares.

#### PROBLEMS FOR CHAPTER 5

- Suppose that the natural number  $n$  has canonical decomposition  $n = 2^r p_1^{r_1} \dots p_k^{r_k} q_1^{s_1} \dots q_\ell^{s_\ell}$ , where the integer  $r \geq 0$  and  $r_1, \dots, r_k, s_1, \dots, s_\ell \in \mathbb{N}$ , and  $p_1, \dots, p_k, q_1, \dots, q_\ell$  are primes satisfying  $p_1 \equiv \dots \equiv p_k \equiv 1 \pmod{4}$  and  $q_1 \equiv \dots \equiv q_\ell \equiv 3 \pmod{4}$ . Suppose further that  $m = p_1^{r_1} \dots p_k^{r_k}$ .
  - Show that the function  $S(n)$  defined in Theorem 5F satisfies

$$S(n) = \begin{cases} 0 & \text{if at least one of } s_1, \dots, s_\ell \text{ is odd,} \\ 4d(m) & \text{otherwise.} \end{cases}$$

- Suppose that  $s_1, \dots, s_\ell$  are all even. Show that the number of solutions of the equation

$$n = x^2 + y^2 \quad \text{in } x, y \in \mathbb{Z} \text{ satisfying } x \geq y \geq 0,$$

is equal to the number of solutions of the equation

$$m = xy \quad \text{in } x, y \in \mathbb{Z} \text{ satisfying } x \geq y > 0.$$

[HINT: Show that both are equal to  $[\frac{1}{2}d(m) + \frac{1}{2}]$ .]

- Suppose that  $n \in \mathbb{N}$ . Show that if the equation  $n = x^2 + y^2$  has more than one solution in  $x, y \in \mathbb{N}$  with  $x$  even, then  $n$  is composite.
- Show that for every real number  $X > 0$ , the function  $S(n)$  defined in Theorem 5F satisfies the inequalities

$$\pi X - 4X^{1/2} - 4 < \sum_{n \leq X} S(n) < \pi X + 4X^{1/2}.$$

- We know that if each of two non-negative integers is a sum of two squares of non-negative integers, then so is their product. Show that the analogous assertion for three squares is false.