We show that (14) has no integral solution with $xyz \neq 0$, $z > 0$. Assuming that (14) has such an integral solution we construct another solution with smaller *positive* $z$. This is clearly impossible as it leads to an infinite sequence of decreasing positive integers. The details are as follows.

We may assume that $(x, y, z) = 1, z > 0$. Next $x$ and $y$ cannot both be odd since otherwise reduction modulo 4 would give $z^2 \equiv 2\ (4)$ which is impossible. Let then $x$ be odd, $y$ even so that $z$ is odd. Write $y^4 = (z - x^2)(z + x^2)$ and observe that, since any prime $p$ dividing the two factors on the right must also divide $2z$ and $2x^2$, one must have $(z - x^2, z + x^2) = 2$. But the product of the two factors is a fourth power. The possibilities are therefore

$$\begin{aligned} z - x^2 &= 2a^4, \qquad a > 0, \\ z + x^2 &= 8b^4, \\ a &\text{ odd}, \quad (a, b) = 1, \end{aligned} \tag{15}$$

or

$$\begin{aligned} z - x^2 &= 8b^4, \\ z + x^2 &= 2a^4, \qquad a > 0 \\ a &\text{ odd}, \quad (a, b) = 1. \end{aligned} \tag{16}$$

The first case implies $x^2 = -a^4 + 4b^4$ which is impossible since otherwise $1 \equiv -1\ (4)$. Thus (16) holds and $z = a^4 + 4b^4$. Note that $0 < a < z$. Also eliminating $z$ in (16) shows that $4b^4 = (a^2 - x)(a^2 + x)$. Since $(a, b) = 1$ it follows that $(a, x) = 1$ and arguing as earlier one sees that $(a^2 - x, a^2 + x) = 2$. Writing $a^2 - x = 2c^4$ and $a^2 + x = 2d^4$ one obtains

$$a^2 = c^4 + d^4.$$

Thus we have found a solution to (14) with smaller positive value for $z$ and the proof is complete. □

In particular $x^4 + y^4 = z^4$ has no solution, $xyz \neq 0$. This is a special case of Fermat's Last Theorem.

## §3 Legendre's Theorem

In this section we consider the Diophantine equation

$$ax^2 + by^2 + cz^2 = 0, \tag{17}$$

where $a, b, c$ are square free, pairwise relatively prime integers. We would like to have necessary and sufficient conditions in order that (17) have a nontrivial integral solution. In order that a solution exist it is of course necessary to assume that $a$, $b$ and $c$ are neither all positive nor all negative.

If $m$ and $n$ are nonzero integers let $m\,R\,n$ denote the fact that $m$ is a square modulo $n$. In other words there is an integer $x$ with $x^2 \equiv m\ (n)$. Legendre discovered the following beautiful theorem.

**Proposition 17.3.1.** *Let $a$, $b$, $c$ be nonzero integers, square free, pairwise relatively prime and not all positive nor all negative. Then (17) has a nontrivial integral solution iff the following conditions are satisfied*

(i) $-ab\,R\,c$.
(ii) $-ac\,R\,b$.
(iii) $-bc\,R\,a$.

It is convenient to prove this result in the following equivalent form.

**Proposition 17.3.2.** *Let $a$ and $b$ be positive square free integers. Then*

$$ax^2 + by^2 = z^2 \tag{18}$$

*has a nontrivial solution iff the following three conditions are satisfied*

(i) $a\,R\,b$.
(ii) $b\,R\,a$.
(iii) $-(ab/d^2)\,R\,d$, *where* $d = (a, b)$.

In order to see that Proposition 17.3.2 implies Proposition 17.3.1 consider $ax^2 + by^2 + cz^2 = 0$ as in Proposition 17.3.1 and assume that $a$ and $b$ are positive while $c$ is negative. Then $-acx^2 - bcy^2 - z^2 = 0$ is easily seen to satisfy the conditions of Proposition 17.3.2. If $(x, y, z)$ is a solution then since $c$ is square free $c \mid z$. Putting $z = cz'$ and cancelling we arrive at a solution to (17). That Proposition 17.3.1 implies Proposition 17.3.2 is left as an exercise.

We now proceed to the proof of Proposition 17.3.2. If $a = 1$ the proposition is obvious. Furthermore we may assume $a > b$. For if $b > a$ just interchange $x$ and $y$. If $a = b$ then by (iii) $-1$ is a square modulo $b$. By Exercise 25 at the end of this chapter one can find integers $r$ and $s$ such that $b = r^2 + s^2$. A solution is then given by $x = r$, $y = s$, $z = r^2 + s^2$.

With these preliminaries we proceed to construct a new form $Ax^2 + by^2 = z^2$ satisfying the same hypotheses as (18), $0 < A < a$, and such that if it has a nontrivial solution then so does (18). After a finite number of steps, interchanging $A$ and $b$ in case $A$ is less than $b$ we arrive at one of the cases $A = 1$ or $A = b$, each of which has been settled. Now for the details.

By (ii) there exist, $T$ and $c$ such that

$$c^2 - b = aT = aAm^2; \qquad A, m \in \mathbb{Z} \tag{19}$$

where $A$ is square-free, and $|c| \leq a/2$. First of all we show that $0 < A < a$. This follows from (19) since first of all one has $0 \leq c^2 = aAm^2 + b < a(Am^2 + 1)$. Thus $A \geq 0$. But since $b$ is square-free $A > 0$ by (19). Furthermore by (19) $aAm^2 < c^2 \leq a^2/4$ so that $A \leq Am^2 < a/4 < a$.

Next we verify that $A\,R\,b$. Put $b = b_1 d$, $a = a_1 d$ with $(a_1, b_1) = 1$ and note that $(a_1, d) = (b_1, d) = 1$ since $a$ and $b$ are square-free. Then (19) becomes

$$c^2 - b_1 d = a_1 d A m^2 \tag{20}$$

and since $d$ is square-free $d|c$. Put $c = c_1 d$ and cancel to obtain

$$d c_1^2 - b_1 = a_1 A m^2. \tag{21}$$

Thus $A a_1 m^2 \equiv -b_1\ (d)$ or $A a_1^2 m^2 \equiv -a_1 b_1\ (d)$. But $(m, d) = 1$ since by (21) a common factor would divide $b_1$ and $d$ and thus $b$ would not be square-free. Using (iii) and the fact that $m$ is a unit modulo $d$ we conclude that $A\,R\,d$. Furthermore $c^2 \equiv A m^2\ (b_1)$. Since $a\,R\,b$ one has $a\,R\,b_1$. Also $(a, b_1) = 1$ since a common divisor would divide $d$ and $b_1$ contradicting the fact that $b = b_1 d$ is square-free. Similarly $(m, b_1) = 1$ which shows that $A\,R\,b_1$. By Exercise 26, $A\,R\,d b_1$ or $A\,R\,b$.

Next write $A = r A_1, b = r b_2, (A_1, b_2) = 1$. We must verify that $-A_1 b_2\,R\,r$. From (19) we conclude that

$$c^2 - r b_2 = a r A_1 m^2. \tag{22}$$

But $r$ is square-free so $r|c$. If $c = r c_1$ then

$$a A_1 m^2 \equiv -b_2\ (r).$$

Since $a\,R\,b$ we have $a\,R\,r$. Finally writing

$$-a A_1 b_2 m^2 \equiv b_2^2\ (r)$$

and observing that $(a, r) = (m, r) = 1$ we conclude $-A_1 b_2\,R\,r$.

Assume now that $AX^2 + bY^2 = Z^2$ has a nontrivial solution. Then

$$AX^2 = Z^2 - bY^2. \tag{23}$$

Multiplying (23) by (19) one has

$$\begin{aligned} a(AXm)^2 &= (Z^2 - bY^2)(c^2 - b) \\ &= (Zc + bY)^2 - b(cY + Z)^2. \end{aligned}$$

(Note the use of the multiplicativity of the norm map on $\mathbb{Q}(\sqrt{b})$!). Thus (18) has a solution with

$$\begin{aligned} x &= AXm, \\ y &= cY + Z, \\ z &= Zc + bY. \end{aligned}$$

This completes the proof since $X \neq 0$; and $m \neq 0$ as follows from the fact that $b$ is square-free. □

An important corollary of Proposition 17.3.1 is a special case of the so called "Hasse Principle." This principle states roughly that local solvability

implies global solvability. Here local solvability means that the equation under consideration has a nontrivial solution modulo $p^m$ for all primes $p$ and all positive integers $m$, as well as a real solution while global solvability refers to a solution in integers. For quadratic forms this principle is true but it fails for equations of higher degree. For example, the equation $x^4 - 17y^4 = 2z^4$ has a nontrivial solution modulo $p^m$ for all $p$ and $m$, and a real solution, but it has no nontrivial solution in integers [205].

**Corollary.** *Let $a, b, c$ be square-free, pairwise relatively prime integers not all of the same sign. If for each prime power $p^m$ the congruence*

$$ax^2 + by^2 + cz^2 \equiv 0 \ (p^m)$$

*has a solution in integers $(x, y, z)$ not all divisible by $p$ then $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution.*

PROOF. Let $m = 2$ and suppose $p|a$. Then if $(x, y, z)$ is a solution as in the corollary we show that $p \nmid yz$. For if $p|y$, say, then $p|cz^2$ which implies, since $(a, c) = 1$, that $p|z$. Thus $p^2|ax^2$ and since $p \nmid x$ we obtain the contradiction $p^2|a$. Similarly $p \nmid z$. Thus $by^2 + cz^2 \equiv 0 \ (p)$ and division (mod $p$) shows that $-bc \ R \ p$. This being the case for every $p|a$ it follows that $-bc \ R \ a$ (Exercise 26). Similarly $-ab \ R \ c$ and $-ac \ R \ b$ and the corollary now follows by Proposition 17.3.1. □

## §4 Sophie Germain's Theorem

In Chapter 14 we proved that if Fermat's equation for an odd prime $p$

$$x^p + y^p + z^p = 0 \tag{24}$$

had a solution with $p \nmid xyz$ then a very strong congruence held, namely

$$2^{p-1} \equiv 1 \ (p^2).$$

In 1823 Sophie Germain proved the following remarkable result by completely elementary considerations.

**Proposition 17.4.1.** *If $p$ is an odd prime such that $2p + 1 = q$ is also prime then (24) has no integral solution with $p \nmid xyz$,*

PROOF. Assume on the contrary that such a solution exists and suppose that $(x, y, z) = 1$. Write

$$-x^p = (y + z)(z^{p-1} - z^{p-2}y + \cdots + y^{p-1}). \tag{25}$$

The two factors on the right are relatively prime. For clearly $p \nmid y + z$ and if $r \neq p$ is a prime dividing both factors then since $y \equiv -z \ (r)$ one has

$$0 \equiv z^{p-1} - z^{p-2}y + \cdots + y^{p-1} \equiv py^{p-1} \ (r),$$