7. Diophantine Equations

We start with a very interesting result due to Legendre.

Theorem 7.1. *Suppose that a, b, $c \in \mathbb{Z}$ are nonzero, pairwise coprime, square-free. Then the equation*

$$f(x, y, z) = ax^2 + by^2 + cz^2 = 0$$

has a non-trivial integral solution (so x, y and z are integers, not all zero) if and only if a, b and c do not all have the same sign and $-ab$, $-bc$ and $-ca$ are quadratic residues of $|c|$, $|a|$ and $|b|$, respectively.

The hypotheses might seem restrictive but in fact they are not. Suppose that we start with $Ax^2 + By^2 + Cz^2$, $ABC \neq 0$. If A, B and C have a common factor then we can obviously divide it out. At the other extreme, if one of A, B and C have a square factor then we can absorb this factor into x^2, y^2 and z^2. Suppose that $d = (A, B) > 1$. Then we can multiply by d, to get coefficients d^2A', d^2B' and dC and absorb d^2 into x^2 and y^2. If we repeat this process it is clear that we end up with coefficients that satisfy the hypotheses of (7.1) and we have not changed the sign of the coefficients.

Proof of (7.1). We first check necessity. It is clear that if we can find a nonzero real solution, let alone a nonzero integral solution, then a, b and c cannot have the same sign. If there is a non-trivial solution then there is clearly a non-trivial solution for which the greatest common divisor of x, y and z is one.

In this case $(x, c) = (y, c) = 1$. Indeed, if $p|x$ and $p|c$ then $p|by^2$ so that $p|y$ as $(b, c) = 1$. But then p does not divide z and $p^2|(ax^2 + by^2)$, so that $p^2|c$, a contradiction. Thus $(x, c) = (y, c) = 1$. As

$$ax^2 + by^2 \equiv 0 \mod c,$$

it follows that

$$(axy^{-1})^2 \equiv -ab \mod c.$$

Therefore $-ab$ is a quadratic residue of $|c|$. By symmetry all of the other conditions hold as well.

Now we check sufficiency. Suppose that $|c| > 1$ and that $-ab$ is a quadratic residue of c. The we can find z such that

$$z^2 \equiv -ab \mod c.$$

Then

$$az^2 + ba^2 \equiv 0 \mod c,$$

so that we can find a solution (x_c, y_c) of

$$ax^2 + by^2 \equiv 0 \mod c,$$

where $(c, x_c) = (c, y_c) = 1$. Let $t = x/y$. As the division algorithm holds for monic polynomials over $\mathbb{Z}_c$, it follows that $at^2 + b$ factors, so that $ax^2 + by^2$ factors into a product of linear polynomials

$$ax^2 + by^2 = (a_1x + b_1y)(a_2x + b_2y)$$

in the ring $\mathbb{Z}_c[x, y]$. It follows that we can factor

$$\begin{aligned} f(x, y, z) &\equiv (r_1x + r_2y + r_3z)(s_1x + s_2y + s_3z) \mod c \\ &\equiv g_c(x, y, z)h_c(x, y, z) \mod c. \end{aligned}$$

Similarly, if $|a| > 1$ and $|b| > 1$ we can also factor

$$\begin{aligned} f(x, y, z) &\equiv g_a(x, y, z)h_a(x, y, z) \mod a \\ &\equiv g_b(x, y, z)h_b(x, y, z) \mod b. \end{aligned}$$

By the Chinese Remainder Theorem, we can find polynomials $g(x, y, z)$ and $h(x, y, z)$ whose reductions modulo a, b and c are the given polynomials. It follows that

$$f(x, y, z) = g(x, y, z)h(x, y, z) \mod |abc|.$$

We have proved this if all three of $|a|$, $|b|$ and $|c| > 1$, but it obviously also holds if at least one is not equal to 1.

Now if $|a| = |b| = |c| = 1$ then the result is easy. Otherwise, since $|abc| > 1$ and abc is square-free, at least one of

$$\lambda_1 = \sqrt{|bc|} \qquad \lambda_2 = \sqrt{|ac|} \qquad \text{and} \qquad \lambda_3 = \sqrt{|ab|}$$

is not an integer. Increase this one very slightly and apply (1.1) to get x, y and z such that

$$g(x, y, z) \equiv 0 \mod |abc| \qquad |x| < \lambda_1 \qquad |y| < \lambda_2 \qquad \text{and} \qquad |z| < \lambda_3.$$

We may assume that $a > 0$, $b > 0$ and $c < 0$. It follows that

$$\begin{aligned} f(x, y, z) &< a|bc| + b|ca| + c \cdot 0 \\ &= 2|abc|. \end{aligned}$$

On the other hand,

$$\begin{aligned} f(x, y, z) &> a \cdot 0 + b \cdot 0 + c|ab| \\ &= -|abc|. \end{aligned}$$

As $f(x, y, z) \equiv 0 \mod |abc|$ it follows that

$$f(x, y, z) = 0 \qquad \text{or} \qquad |abc| = -abc.$$

We may assume that we have the latter case, otherwise we are done. It follows that

$$ax^2 + by^2 + c(z^2 + ab) = 0.$$

Thus
$$(ax^2 + by^2)(z^2 + ab) + c(z^2 + ab)^2 = 0.$$
This implies that
$$a(xz + by)^2 + b(yz - ax)^2 + c(z^2 + ab)^2 = 0.$$
Note that $z^2 + ab$ is not zero, as it is positive. $\square$

One very interesting feature of trying to find solutions to an equation of the form
$$ax^2 + by^2 + cz^2 = 0,$$
is that not only does (7.1) furnish a way to decide if there is a solution, in fact it is not hard to show that one can find a non-trivial solution such that
$$\max(|x|, |y|, |z|) < 2 \max(a^2, b^2, c^2),$$
so that there is also an algorithm to find solutions, not only determine whether or not they exist.