2.2 Linear congruences

The most basic class of congruences are *linear* congruences, viz., congruences of the form

$$ax \equiv b \pmod{m} \tag{1}$$

to be solved for x. By definition (1) is soluble if and only if $m|(b-ax)$ for some x, and this is true if and only if $b - ax = my$ for some x and y. Hence (1) is soluble if and only if

$$ax + my = b \tag{2}$$

for some $x, y \in \mathbb{Z}$. To investigate the solubility of linear congruences we must answer the question: given integers a and m, which integers can be written in the form $ax + my$ with $x, y \in \mathbb{Z}$? To solve this problem we need to recall the notion of the gcd.

Theorem (a) If a, $b \in \mathbb{Z}$ there exists a unique non-negative integer g such that

(i) $g \mid a$ and $g \mid b$, and

(ii) if $h \mid a$ and $h \mid b$ then $h \mid g$.

(b) If g is the integer from part (a) then $g = ar + bs$ for some r, $s \in \mathbb{Z}$. □

We call g the *greatest common divisor* or *gcd* of a and b and write $g = \gcd(a, b)$. It also follows that a number m has the form $ax + by$ if and only if $g \mid m$.

To calculate g, r and s we use the Euclidean algorithm. We may suppose that a and b are both positive. Let $a_1 = a$, $a_2 = b$, $r_1 = s_2 = 1$ and $r_2 = s_1 = 0$. We repeat the following procedure until we get $a_{k+1} = 0$. If we know a_t choose q such that $0 \leq a_{t+1} = a_{t-1} - qa_t < a_t$ and put $r_{t+1} = r_{t-1} - qr_t$ and $s_{t+1} = s_{t-1} - qs_t$. When $a_{k+1} = 0$ then put $g = a_k$, $r = r_k$ and $s = s_k$. As we can easily prove $a_t = ar_t + bs_t$ for each t we have $g = ar + bs$.

Returning to congruence (1), or equivalently equation (2), we see that it is insoluble if $g = \gcd(a, m) \nmid b$. Otherwise if $g \mid b$ write $a = ga'$, $b = gb'$ and $m = gm'$ and note that (1) is equivalent to

$$a'x \equiv b' \pmod{m'}. \tag{3}$$

Now if $g = ar + ms$ then $1 = a'r + m's \equiv a'r \pmod{m}$. Multiplying (3) by r gives

$$x \equiv b'r \pmod{m'}$$

as the general solution of (1). Note that in general we get a solution modulo m', and this is equivalent to g different solutions modulo m.

We note that if $g = \gcd(a, m) = 1$ then the congruence (1) has a unique solution modulo m. As this is quite a desirable state of affairs then we introduce a piece of terminology; integers a and b are said to be *coprime*, or a is *coprime* to b, if $\gcd(a, b) = 1$. The condition of a and b being coprime is equivalent to the solubility of the congruence $ax \equiv 1 \pmod{b}$ for x. It easily follows that if a is coprime to b and $a \equiv a' \pmod{b}$ then a' is coprime to b. Also if a is coprime to c and b is coprime to c, then ab is coprime to c.

A useful property of coprime numbers is that their "least common multiple" is their product.

Proposition If m and n are coprime, and if $m \mid a$ and $n \mid a$ then $mn \mid a$. □

□

With a little more effort one can get similar results giving the value of $\left(\frac{\pm 3}{p}\right)$, then $\left(\frac{\pm 5}{p}\right)$ and so on. Alas the work involved steadily increases. There is however a general result which subsumes all these cases. This result, conjectured by Legendre, and proved by Gauss is the celebrated Law of Quadratic Reciprocity. It can be proved by an ingenious argument using Gauss's Lemma.

Theorem (Law of Quadratic Reciprocity) Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless $p \equiv q \equiv 3 \pmod 4$ when

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

□

Using this result the practical computation of Legendre symbols is now straightforward.

4 Diophantine equations

4.1 Sums of squares

We now turn to the subject of sums of squares. The basic problem is how to express a given number $n \in \mathbb{N}$ as the sum of integer squares using as few squares as possible. Note that we admit $0 = 0^2$ as a square. Putting the question another way we ask which numbers are sums of two squares, sums of three squares and so on. If we consider the numbers from 1 to 100 we find 10 of them are squares, 43 are sums of two squares, 86 are sums of three squares, and all are sums of four squares. We may surmise that all natural numbers are sums of four squares, and this turns out to be true.

It is easy to see that if $n \equiv 3 \pmod 4$ then n is not the sum of two squares, and if $n \equiv 7 \pmod 8$ then n is not the sum of three squares. Hence there are infinitely many numbers which are not sums of three squares. The following result gives a further restriction on which numbers are sums of two squares.

Lemma If p is a prime number with $p \equiv 3 \pmod 4$ and $p \mid x^2 + y^2$ where x, $y \in \mathbb{Z}$, then $p \mid x$ and $p \mid y$, and so $p^2 \mid x^2 + y^2$. □

Corollary If $n = x^2 + y^2$ then $n = r^2 m$ where m is a sum of two squares which is divisible by no prime p satisfying $p \equiv 3 \pmod 4$. □

This corollary says that if n is the sum of two squares and

$$n = \prod_j p_j^{r_j}$$

is the prime factorization of n, then r_j is even whenever $p_j \equiv 3 \pmod 4$. If we consider the numbers n up to 100 we find that if n satisfies this condition, then n is the sum of two squares. We now ask for any n whether this condition