A Guide to Arithmetic

Robin Chapman

August 5, 1994

These notes give a very brief resumé of my number theory course. Proofs and examples are omitted. Any suggestions for improvements will be gratefully received. I am grateful to Jasmine Arscott for pointing out some errors in an earlier version.

1 Basic notions

In number theory we deal with the set of *natural numbers*

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

and the set of *integers*

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Probably the most fundamental notion of number theory is that of divisibility. We say that an integer m *divides* an integer n, or that n is divisible by m, or that m is a *factor* or *divisor* of n, if there exists an integer r with $n = rm$. If $m \neq 0$ this means that $n/m \in \mathbb{Z}$. We write $m \mid n$ if m divides n and $m \nmid n$ if m doesn't divide n.

Proposition
(i) If $m \mid n$ and $m \mid r$, then $m \mid n + r$ and $m \mid n - r$,
(ii) if $m \mid n$ and $r \in \mathbb{Z}$, then $m \mid rn$,
(iii) $n \mid 0$ for all $n \in \mathbb{Z}$ but $0 \mid n$ only if $n = 0$,
(iv) $n \mid 1$ if and only if $n = \pm 1$,
(v) if $m \mid n$ and m, $n \in \mathbb{N}$, then $m \leq n$,
(vi) $m \mid n$ if and only if $m \mid -n$ if and only if $-m \mid n$,
(vii) if r, m, $n \in \mathbb{Z}$ and $r \neq 0$ then $m \mid n$ if and only if $rm \mid rn$,
(viii) if $m \mid n$ and $n \mid r$ then $m \mid r$. □

Once we have the concept of divisibility we can define the notion of primality. We say a natural number p is *prime* if $p > 1$, and the only natural numbers dividing p are 1 and p. If $n > 1$ and n isn't prime then we say n is *composite*.

Proposition If $n > 1$ is a natural number, then $n = p_1 p_2 \cdots p_r$ where p_1, $p_2, \ldots, p_r$ are primes. □

Theorem (Euclid) The set of primes is infinite. □

2 Congruences

2.1 Definitions

The most important tool in number theory is the notion of congruence. If a, b and m are integers, we say that a is *congruent* to b modulo m or write

$$a \equiv b \pmod{m}$$

if $m \mid (b-a)$. (If we are lazy we sometimes write $a \equiv b\ (m)$.)

For a fixed number m the relation of congruence is an equivalence relation.

Proposition

(i) $a \equiv a \pmod{m}$ for all a.

(ii) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$. □

Also congruence respects addition, subtraction and multiplication.

Proposition If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

(i) $a + b \equiv a' + b' \pmod{m}$,

(ii) $a - b \equiv a' - b' \pmod{m}$, and

(iii) $ab \equiv a'b' \pmod{m}$. □

Division in general **not** respected. We do, however, have this useful result about going between congruences to different moduli.

Proposition

(i) If $a \equiv b \pmod{m}$ and $d \mid m$ then $a \equiv b \pmod{d}$.

(ii) Suppose $s \neq 0$. Then $a \equiv b \pmod{m}$ if and only if $as \equiv bs \pmod{ms}$. □

If m is fixed then an equivalence class for the relation of congruence modulo m is called a *residue class* modulo m. We sometimes denote the residue class containing a by $\overline{a}$ so that

$$\overline{a} = \{a + rm : r \in \mathbb{Z}\} = \{\ldots, a - m, a, a + m, a + 2m, \ldots\}.$$

If $m > 0$ then there are exactly m residue classes modulo m. If S is a set containing exactly one element of each residue class modulo m, we say that S is a *complete system of residues* modulo m. In particular if $m > 0$ then the set $S = \{0, 1, \ldots, m-1\}$ is a complete system of residues modulo m. Another important example when $m > 0$ is

$$S' = \{a : -m/2 < a \leq m/2\}.$$

If $m = 2n + 1$ is odd then $S' = \{-n, -n+1, \ldots, n-1, n\}$ and if $m = 2n$ is even then $S' = \{-n+1, -n+2, \ldots, n-1, n\}$.

If we have a congruence modulo m involving an indeterminate x we can ask if this congruence is soluble, and if so what the solutions are. It clearly suffices to substitute each element of a complete system of residues modulo m for x, and see for which values the congruence is satisfied. This approach is only efficient when m is small, and we shall seek better methods which are practical for large m.

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 $0 \le a_{t+1} = a_{t-1} - qa_t < a_t$ 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 $mn \mid a$. □

Corollary Suppose that m and n are coprime. If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ then $a \equiv b \pmod{mn}$. $\Box$

If p is a prime number then "most" numbers will be coprime to p.

Proposition If p is a prime and $a \in \mathbb{Z}$ then either $p \mid a$ or a is coprime to p. $\Box$

Corollary Let p be a prime. If $p \mid ab$ then either $p \mid a$ or $p \mid b$. $\Box$

We can extend this by induction to products of more than two numbers.

Corollary Let p be a prime. If $p \mid a_1 a_2 \cdots a_k$ then $p \mid a_k$ for some j. $\Box$

This result is used in a crucial manner in the proof of the unique factorization property of integers.

Theorem (The Fundamental Theorem of Arithmetic) If $n > 1$ is a natural number and

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

where the p_is and q_js are all prime, then $r = s$ and we can re-order the q_js such that $p_i = q_i$ for all i. $\Box$

Hence every integer $n > 1$ can be factored into primes in a unique manner. If we collect together occurrences of the same prime we can write

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = \prod_{j=1}^{k} p_j^{r_j} \tag{4}$$

where the p_js are *distinct* primes and each $r_j \geq 1$. From now on if we write an expression such as (4) we assume these conditions hold.

2.3 Simultaneous congruences and the Chinese remainder theorem

We now investigate pairs of simultaneous congruences such as

$$\left.\begin{array}{rcll} x & \equiv & a & \pmod{m} \\ x & \equiv & b & \pmod{n}. \end{array}\right\} \tag{5}$$

The first congruence is equivalent to $x = a + my$ so substituting in the second gives

$$my \equiv b - a \pmod{n}.$$

By the theory of linear congruences this is soluble if and only if $g \mid (b - a)$ where $g = \gcd(m, n)$. If $g \mid (b - a)$ then this congruence has a unique solution for y modulo n/g which translates into a unique solution for x modulo mn/g. In other words we have the theorem.

Theorem The pair of congruences (5) have a simultaneous solution for x if and only if $g \mid (b - a)$ where $g = \gcd(m, n)$. In this case the solution is unique modulo mn/g. $\Box$

Corollary (The Chinese Remainder Theorem) If m and n are coprime then the pair of congruences (5) has a unique solution modulo mn for any integers a and b. $\Box$

We can use the Chinese remainder theorem in the solution of congruences. If $f(x) \equiv 0 \pmod{mn}$ is a congruence with m and n coprime we can solve the same congruence modulo m and modulo n and then put the results together to get the solution modulo mn.

2.4 Euler's φ-function

When p is prime then all numbers not divisible by p are coprime to p. If we look at a non-prime number $n \in \mathbb{N}$ we can ask "how many" numbers are coprime to n. We thus define $\varphi(n)$ to be the number of a with $1 \leq a \leq n$ which are coprime to n. In symbols

$$\varphi(n) = |\{a \in \mathbb{N} : 1 \leq a \leq n, \gcd(a, n) = 1\}|.$$

The function φ is called *Euler's phi-function*. It's clear that $\varphi(1) = 1$ and $\varphi(p) = p - 1$ when p is prime. In fact we can easily generalize this result.
Lemma Let p be prime and let $r \geq 1$. A number a is coprime to p^r if and only if a is coprime to p. □
Corollary Let p be prime and let $r \geq 1$. Then $\varphi(p^r) = p^{r-1}(p-1)$. □

Hence the value of $\varphi(n)$ is easily computed whenever n is a power of a prime. To find the value in general we need to know how $\varphi(mn)$ depends on $\varphi(m)$ and $\varphi(n)$ whenever m and n are coprime. We need this preliminary result.
Proposition Let m and n be coprime natural numbers. Then a is coprime to mn if and only if a is coprime to m and a is coprime to n. □

Using this result and the Chinese Remainder Theorem we can now prove the following theorem.
Theorem Let m and n be coprime natural numbers. Then $\varphi(mn) = \varphi(m)\varphi(n)$. □
Corollary If $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ then

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi(p_k^{r_k}) \\
&= p_1^{r_1-1}(p_1-1)p_2^{r_2-1}(p_2-1)\cdots p_k^{r_k-1}(p_k-1) \\
&= n\prod_{j=1}^{k}\left(1 - \frac{1}{p_j}\right).
\end{aligned}$$

□

The main application of the phi-function is to the following result.
Theorem (Fermat-Euler) Let n be a natural number and suppose that a is coprime to n. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

Corollary (Fermat's Theorem) (a) If p is prime and $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(b) If p is prime and $a \in \mathbb{Z}$ then

$$a^p \equiv a \pmod{b}.$$

□

The Fermat-Euler theorem says that if we take a coprime to n, and consider the sequence of powers a, a^2, $a^3, \ldots$ then eventually we reach one, viz., $a^{\varphi(n)}$ which is congruent to 1 modulo n. However we may find that we reach a power a^h with $a^h \equiv 1 \pmod{n}$ earlier. If h is the smallest natural number such that $a^h \equiv 1 \pmod{n}$ we call h the *order* of a modulo n. It is clear that $h \le \varphi(n)$, but in fact more is true.

Lemma Suppose that a has order h modulo n. Then $a^r \equiv a^s \pmod{n}$ if and only if $r \equiv s \pmod{h}$. □

Corollary Suppose that a has order h modulo n. Then $h \mid \varphi(n)$. □

If a has order $\varphi(n)$ modulo n then we call a a *primitive root* modulo n. This is equivalent to saying that every b which is coprime to n is congruent to a power of a modulo n. Not all numbers have primitive roots, but we shall later see that all primes have.

2.5 Primality testing

Fermat's theorem has an important application to primality testing. This is the problem of determining whether a specified number n is prime. As it's easy to see that every composite number n is divisible by a prime $p \le \sqrt{n}$ then a small number n can be tested by primality by dividing by all such primes. However as n gets bigger this method becomes impractical. For an n with 20 digits one would need over 10^8 trial divisions so we need more subtle methods.

Fermat's theorem implies that if $n \nmid a$ and $a^{n-1} \not\equiv 1 \pmod{n}$ then n cannot be prime. Hence if for a given n we can find such an a then we know n isn't prime. So as a basic primality test we pick a number a (usually $a = 2$ will work) and compute a^{n-1} modulo n. If $a^{n-1} \not\equiv 1 \pmod{n}$ then n is not prime, but if $a^{n-1} \equiv 1 \pmod{n}$ then the test is alas inconclusive.

This test avoids a vast amount of trial division but instead seems to rely on the computation of a^{n-1} which may be a really vast number! This difficulty is more apparent than real, as we only need to find the value of this modulo n. Again this seems intractable as the obvious method relies on multiplying a by itself $n-1$ times and at each stage reducing modulo n. This requires about n operations which is worse than trial division. But again this can be circumvented by means of the "binary trick".

The "binary trick" is an efficient algorithm for finding the value of a^r modulo n. We observe that if r were a power of 2 this would be straightforward as we could compute the values of a, a^2, $a^4 = (a^2)^2$, $a^8 = (a^4)^2$ and so on, modulo n, until we reach a^r. Alas nature is not usually kind enough to provide such an r but we can easily get around this. We write r in binary notation and let r_j be the number whose binary representation is given by the first j binary digits of r. Then $r_1 = 1$ and $r_k = r$, if r has k binary digits, and for each j either $r_{j+1} = 2r_j$ or $r_{j+1} = 2r_j + 1$. We compute a^{r_j} modulo n for $j = 1, 2, \ldots, k$ successively as follows; $a^{r_1} = a$, and if $a^{r_j} \equiv b \pmod{n}$ then we compute $a^{r_{j+1}} \equiv b^2$ or $b^2 a \pmod{n}$ according to whether $r_{j+1} = 2r_j$ or $2r_j + 1$.

Again we come to the question of whether our test always works; if $a^{n-1} \equiv 1 \pmod{n}$, does it follow that n is prime? The answer alas is no, we have $2^{340} \equiv 1 \pmod{341}$ but 341 is not prime. If n is composite and $a^{n-1} \equiv 1 \pmod{n}$ we say that n is a *pseudoprime to the base a*. It can be shown that there are infinitely many pseudoprimes to each base. We now ask a more modest question; given a composite number n, is there a base to which it is not a pseudoprime? The following lemma says the answer is affirmative.

Lemma If $\gcd(a, n) > 1$, then n is not a pseudoprime to base a. □

Alas on further reflection we see that this result is very weak. If $n = pq$ is a product of two large primes, then the probability of picking a which is not coprime to n is less than $1/p + 1/q$, which is negligible. We thus ask if n is composite is there an a coprime to n such that n is not a pseudoprime to the base a? The answer is no, for if $n = 561$ we find that $a^{560} \equiv 1 \pmod{561}$ for all a coprime to 561. Numbers n such as 561 which are pseudoprimes to all bases a coprime to n, are called *Carmichael numbers.* There has recently been a major breakthrough in the theory of Carmichael numbers.

Theorem (Alford, Granville, Pomerance, 1992) There are infinitely many Carmichael numbers. □

This result is unfortunate for our primality test, as repeatedly testing a Carmichael number for primality is practically certain to fail.

2.6 General congruences and primitive roots

We now return to the general theory of congruences. Consider a polynomial expression

$$f(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_1 x + a_0$$

with the $a_j \in \mathbb{Z}$, and consider the congruence $f(x) \equiv 0 \pmod{m}$. If m divides all the a_j then the congruence reduces to $0 \equiv 0 \pmod{m}$ and we call the congruence *trivial.* Otherwise there exists d such that $m \nmid a_d$ but $m \mid a_j$ if $j > d$. In this case we can ignore terms of higher degree than x^d and we say that the congruence has *degree d modulo m.* Note that the degree of a congruence depends on the modulus. We know that an equation of degree d over the real or complex numbers has at most d solutions. Alas there are examples of congruences of degree d modulo m which have more than d solutions modulo m. Fortunately this does not happen when m is prime.

Proposition Let p be a prime number, and consider a congruence $f(x) \equiv 0 \pmod{p}$ of degree d modulo p. This congruence cannot have more than d distinct solutions modulo p. □

Corollary If p is an odd prime and $a^2 \equiv 1 \pmod{p}$ then $a \equiv \pm 1 \pmod{p}$. □

As with equations over the real numbers a congruence modulo p may have fewer than d solutions. But there is an important special case where we get a full complement of roots.

Proposition Let p be a prime. If $x^p - x = f(x)g(x)$ where the polynomial f has degree d, then the congruence $f(x) \equiv 0 \pmod{p}$ has exactly d distinct solutions modulo p. □

We draw two corollaries from this which we will use in the quest for a primitive root modulo p.

Corollary Let p be a prime and suppose that $m \mid (p-1)$. Then there are exactly m distinct solutions of $x^m \equiv 1 \pmod{p}$ modulo p. □

Corollary Let p and q be primes and suppose that $q^r \mid (p-1)$ for some $r \geq 1$. Then there are exactly $q^{r-1}(q-1)$ distinct numbers of order q^r modulo p. □

Putting this result together with the next lemma establishes the existence of primitive roots modulo p.

Lemma If a and b have orders h and k respectively modulo m, and h and k are coprime, then ab has order hk modulo m. □

Theorem If p is a prime then there exists a primitive root g modulo p, i.e., g has order $p-1$ modulo p. □

We can use the existence of a primitive root g modulo a prime p to simplify many arguments. Note that if $p \nmid a$ then $a \equiv g^r \pmod{p}$ for some r. There is also a nice procedure for recognizing primitive roots. If $p-1$ has the distinct prime factors q_1, $q_2, \ldots, q_r$, then g is a primitive root modulo p if and only if $q^{(p-1)/q_j} \not\equiv 1 \pmod{p}$ for each j.

As all numbers not congruent to zero modulo the prime p are congruent to powers of a given primitive root g of p, then we can introduce an analogue of the logarithm. If g is a primitive root of the prime p and $a \equiv g^r \pmod{p}$ then we call r the *discrete logarithm* of a to the base g modulo p, and denote $r = \log_{p,g}(a)$. As $g^r \equiv g^s$ if and only if $r \equiv s \pmod{p-1}$ then the discrete logarithm is only defined modulo $p-1$. We have the important formula

$$\log_{p,g}(ab) \equiv \log_{p,g}(a) + \log_{p,g}(b) \pmod{p-1}.$$

2.7 The Miller-Rabin test

We have observed that if p is prime then the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1 \pmod{p}$. Hence if $x \not\equiv \pm 1 \pmod{n}$ but $x^2 \equiv 1 \pmod{n}$, then n cannot be prime. We can apply this result to primality testing. If n is an odd number (there's no point in testing even numbers for primality!) write $n-1 = 2^r s$ where s is odd. If the basic primality test fails on n for some base a, i.e., $a^{n-1} \equiv 1 \pmod{n}$ we consider the values of a^s, a^{2s}, $a^{4s}, \ldots, a^{2^r s} = a^{n-1}$ modulo n (note that computing $a^{n-1} \pmod{n}$ by the binary trick will give all these values on the way) and check to see whether for some j we have $a^{2^j s} \not\equiv \pm 1 \pmod{m}$ but $a^{2^{j+1} s} \equiv 1 \pmod{m}$. If this happens we conclude that n is composite.

This test is called the *Miller-Rabin* test and is a crucial improvement over the basic primality test. One can show (but we won't) the following result.

Theorem If n is an odd composite number, then the proportion of numbers a with $1 < a < n$, such that the Miller-Rabin test applied to n and a shows that n is composite, is at least $3/4$. □

This result shows that there is no analogue for the Miller-Rabin test of Carmichael numbers. Given an odd composite number n and taking a random number a in the range $1 < a < n$ the probability is at most $1/4$ that the Miller-Rabin test is inconclusive. Repeating this k times one has at most a $1/4^k$ chance of failure. Hence one can be as confident as one likes that a given large number is prime (but never quite certain).

2.8 Applications to cryptography

The difficulty of factorizing large integers has resulted in an important application to cryptography. The *RSA cryptosystem* (Rivest, Shamir, Adleman,

1978) is the most famous example. This is a so-called *public key* system, where one publishes the encoding algorithm, so anyone can send you coded messages, but one keeps the decoding algorithm secret. One takes large primes p and q (usually large, 100+ digits) and selects a number r coprime to $\varphi(pq) = (p-1)(q-1)$. One then finds s such that $rs \equiv 1 \pmod{\varphi(n)}$. One publishes $n = pq$ and r, but keeps p, q and s secret. To code a message one represents it as a number m with $0 < m < n$ and the coded message is the number m' in the same range satisfying $m' \equiv m^r \pmod{n}$. Now it's easy to show that $m'^s \equiv m^{rs} \equiv m \pmod{n}$, so that possession of the key s enables one to decode the message. But the only known way to find s given $n = pq$ and r is to factorize n into its prime factors, and then solve $rs \equiv 1 \pmod{\varphi(n)}$. As factorizing large numbers into primes is still an intractable problem (but one on which progress is being made) the RSA system is secure.

2.9 Mersenne numbers

There are certain classes of numbers which can be tested for primality by special methods. The most famous of these are the *Mersenne numbers* $M_n = 2^n - 1$. One easily shows that if n is composite then M_n is also, so for M_n to be prime it is necessary that n be prime. However the converse is false, for $M_{11} = 2047 = 23 \times 89$. Nevertheless there is a test for primality of Mersenne numbers which has given a series of numbers each of which has been the highest known prime. The current record holder is M_{756839} which was found on a CRAY computer at the Atomic Energy Research Authority at Harwell in 1992.

Most Mersenne numbers of the form M_p with p prime are alas composite. the following result gives us some information about their prime factors.
Proposition If q is a prime factor of $M_p = 2^p - 1$ where p is prime, then $q \equiv 1 \pmod{p}$. □

3 Quadratic residues

We wish to study the theory of quadratic congruences in detail. We confine ourselves to a prime modulus p, which we shall assume is odd. By the familiar technique of completing the square one can reduce any such congruence to the form

$$x^2 \equiv a \pmod{p}. \tag{†}$$

If $p \mid a$ then (†) is equivalent to $x \equiv 0 \pmod{p}$. Otherwise if $p \nmid a$ and (†) has a solution $x \equiv b \pmod{p}$ then $p \nmid b$ and $x \equiv -b \pmod{p}$ is another, different solution. As (†) cannot have more than two distinct solutions modulo p then these are the only solutions. Such an a where $p \nmid a$ and (†) is soluble is called a *quadratic residue* modulo p. If the congruence (†) is insoluble then a is called a *quadratic non-residue* modulo p.

For convenience we introduce some notation. If p is an odd prime and

$a \in \mathbb{Z}$ we define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ +1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Note that $\left(\frac{a}{p}\right)$ is only defined if p is an odd prime. By our previous remarks we see that the congruence (†) has precisely $1 + \left(\frac{a}{p}\right)$ distinct solutions modulo p.

We now ask how may quadratic residues are there modulo p. If g is a primitive root modulo p then it's easy to see that g^s is a quadratic residue modulo p if and only if s is even. As every non-zero residue is congruent to a power of g modulo p we see that exactly half of the non-zero residues modulo p are quadratic residues. Hence there are $(p-1)/2$ distinct quadratic residues and $(p-1)/2$ distinct quadratic non-residues modulo p. By writing $a \equiv g^s \pmod{p}$ one easily gets the following result.

Proposition (Euler's Criterion) If p is an odd prime and $a \in \mathbb{Z}$ then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

□

Corollary Let p be an odd prime and let a, $b \in \mathbb{Z}$. Then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Corollary If p is an odd prime then

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

□

To calculate further values of the Legendre symbol we use the following result which is derived from Euler's criterion.

Proposition (Gauss's Lemma) Let p be an odd prime and suppose $p \nmid a$. Put $p' = (p-1)/2$ and define $c_1, c_2, \ldots, c_{p'}$ by $c_j \equiv aj \pmod{p}$ and $|c_j| < p/2$. Let μ be the number of negative c_js. Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

□

By turning the handle we get the following important corollary.

Corollary Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}, \end{cases}$$

and

$$\left(\frac{-2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 3 \pmod{8}, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{8}. \end{cases}$$

□

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 does imply that n is the sum of two squares. In order to show that the answer is yes we need the following useful lemma.

Lemma If m and n are sums of two squares, then so is mn. □

It now suffices to show that any prime p which is not congruent to 3 modulo 4 is a sum of two squares. This is trivial for $p = 2 = 1^2 + 1^2$ so consider a prime $p \equiv 1 \pmod 4$.

Theorem If p is a prime number with $p \equiv 1 \pmod 4$, then p is a sum of two squares. □

This result finally gives the characterization of sums of two squares.

Theorem Let $n \in \mathbb{N}$ have the prime factorization

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

Then n is the sum of two squares if and only if r_j is even whenever $p_j \equiv 3 \pmod 4$. □

Another nice result is that a prime $p \equiv 1 \pmod 4$ can be expressed as the sum of two squares in a unique fashion.

Proposition If p is a prime number and $p = x^2 + y^2 = u^2 + v^2$, where x, y, u, $v \in \mathbb{N}$ and $x > y$, $u > v$, then $x = u$ and $y = v$. □

In general one can work out a formula giving the number of representations of a number n as the sum of two squares, but we shall not go into this.

When we turn to sums of three squares things become very difficult. It is possible for numbers m and n to be sums of three squares, yet for mn not to be. This makes the approach used for sums of two squares, where we build up from the case where n is prime, fail. We just state the main result.

Theorem (Gauss) A number $n \in \mathbb{N}$ is the sum of three squares if and only if one cannot write $n = 4^a m$ where $m \equiv 7 \pmod 8$. □

The proof of one half of the theorem is easy, namely that a number $n = 4^a m$ with $m \equiv 7 \pmod 8$ is not the sum of three squares. The converse is a very deep theorem indeed.

When we come to sums of four squares life becomes easier again. Every natural number is the sum of four squares. Again we have a product rule.

Lemma If m and n are sums of four squares then so is mn. □

This enables us to reduce the proof of the following theorem to the case where n is prime.

Theorem (Legendre) If $n \in \mathbb{N}$ then n is the sum of four squares. □

4.2 Pell's equation and continued fractions

Given a number $n \in \mathbb{N}$, Pell's equation is

$$x^2 - ny^2 = 1.$$

We wish to find integer solutions to this equation. As $(\pm x, \pm y)$ are solutions if (x, y) is then we need only consider $x, y \geq 0$. We have the obvious solution $(x, y) = (1, 0)$ so it suffices to consider the case where $x, y \in \mathbb{N}$, and such solutions are called *non-trivial.* We can easily rule out solutions for a certain class of n.

Lemma If n is a square then Pell's equation $x^2 - ny^2 = 1$ has no non-trivial solution. $\square$

Numerical investigation for non-square values of n indicate that solutions of Pell's equation do exist, but that they vary unpredictably as n varies. Before showing how to find a solution, we show that given one solution we can find infinitely many others.

Lemma If $x_j^2 - ny_j^2 = 1$ for $j = 1$ and 2, then $x_3^2 - ny_3^2 = 1$ where $x_3 = x_1x_2 + ny_1y_2$ and $y_3 = x_1y_2 + y_1x_2$. $\square$

Corollary If $x^2 - ny^2 = 1$ has a non-trivial solution, then it has infinitely many solutions. $\square$

To solve Pell's equation we notice that it can be written as $(x/y)^2 - n = 1/y^2$. This shows that $(x/y)^2$ is close to n and so the rational number x/y is close to the irrational number $\sqrt{n}$. More precisely it's clear that $x/y > \sqrt{n}$ and so as

$$\begin{aligned}\frac{x}{y} - \sqrt{n} &= \frac{(x/y)^2 - n}{x/y + \sqrt{n}} \\ &= \frac{1}{y^2}\left(\frac{x}{y} + \sqrt{n}\right)^{-1}\end{aligned}$$

then $0 < x/y - \sqrt{n} < 1/(2y^2\sqrt{n})$. It follows that to solve Pell's equation one must find very good rational approximations to $\sqrt{n}$. We shall describe a method for obtaining such approximations to any irrational number, and use them to solve Pell's equation.

To approximate a real number ξ by rationals we use the technique of continued fractions. A (finite) *continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_{r-1} + \cfrac{1}{a_r}}}}}$$

where $a_0 \in \mathbb{Z}$ and $a_j \in \mathbb{N}$ for each $j > 0$. For convenience we abbreviate this expression by $\langle a_0, a_1, \ldots, a_r\rangle$. We can represent any rational number by a continued fraction, and approximate any irrational number by continued fractions by the following procedure.

Let ξ be any positive real number. Let $[\,\xi\,]$ denote the integer part of ξ, i.e., the integer a such that $a \leq \xi < a + 1$. Put $a_0 = [\,\xi\,]$, and $\eta_0 = \xi - a_0$. If $\eta_0 = 0$ then $\xi = a_0 = \langle a_0\rangle \in \mathbb{Q}$ and we stop, otherwise we put $\xi_1 = 1/\eta_0$, $a_1 = [\,\xi_1\,]$ and $\eta_1 = \xi_1 - a_1$. If $\eta_1 = 0$ then $\xi = \langle a_0, a_1\rangle \in \mathbb{Q}$ and we stop, otherwise we put $\xi_2 = 1/\eta_1$, $a_2 = [\,\xi_2\,]$ and $\eta_2 = \xi_2 - a_2$, and we keep going. If $\xi \in \mathbb{Q}$ we eventually get $\eta_r = 0$ and so $\xi = \langle a_0, a_1, \ldots, a_r\rangle$ (this process is essentially equivalent to the Euclidean algorithm), but if $\xi \notin \mathbb{Q}$ we go on forever getting an *infinite continued fraction* $\xi = \langle a_0, a_1, \ldots, a_r, \ldots\rangle$.

The *convergents* of a (finite or infinite) continued fraction $\langle a_0, a_1, a_2, \ldots, \rangle$. are the numbers c_0, c_1, $c_2, \ldots$ where $c_j = \langle a_0, a_1, \ldots, a_j\rangle$. The convergents of the continued fraction of a number ξ, form a sequence of excellent approximations to ξ. We can obtain the convergents easily by a recurrence relation.

Proposition Let $c_0, c_1, c_2 \ldots$ be the convergents to the continued fraction $\langle a_0, a_1, a_2, \ldots \rangle$. If we write $c_j = h_j/k_j$ in lowest terms, then $h_{r+1} = a_{r+1}h_r + h_{r-1}$ and $k_{r+1} = a_{r+1}k_r + k_{r-1}$. □

If we apply the continued fraction technique to $\sqrt{n}$ we see that we get a recurring continued fraction. In fact more is true.

Theorem Let $n \in \mathbb{N}$ be a non-square. Then there exists a number m such that

$$\sqrt{n} = \langle a_0, a_1, a_2, \ldots, a_{m-1}, 2a_0, a_1, a_2 \ldots \rangle,$$

i.e., $a_m = 2a_0$ and $a_{r+m} = a_r$ for all $r \geq 0$.

Also if the c_j are the convergents of this continued fraction and $c_j = h_j/k_j$ in lowest terms, then

$$h_{sm-1}^2 - nk_{sm-1}^2 = (-1)^{sm}$$

for all $s \in \mathbb{N}$. □

It follows that we can read off infinitely many solutions of Pell's equation from the continued fraction of $\sqrt{n}$. However if m is odd then we get a solution of the *negative Pell equation* $x^2 - ny^2 = -1$ before we get a solution of Pell. We can then exploit the following shortcut to get a solution of Pell.

Lemma If $x^2 - ny^2 = -1$ then $x'^2 - ny'^2 = 1$ where $x' = x^2 + ny^2$ and $y' = 2xy$. □