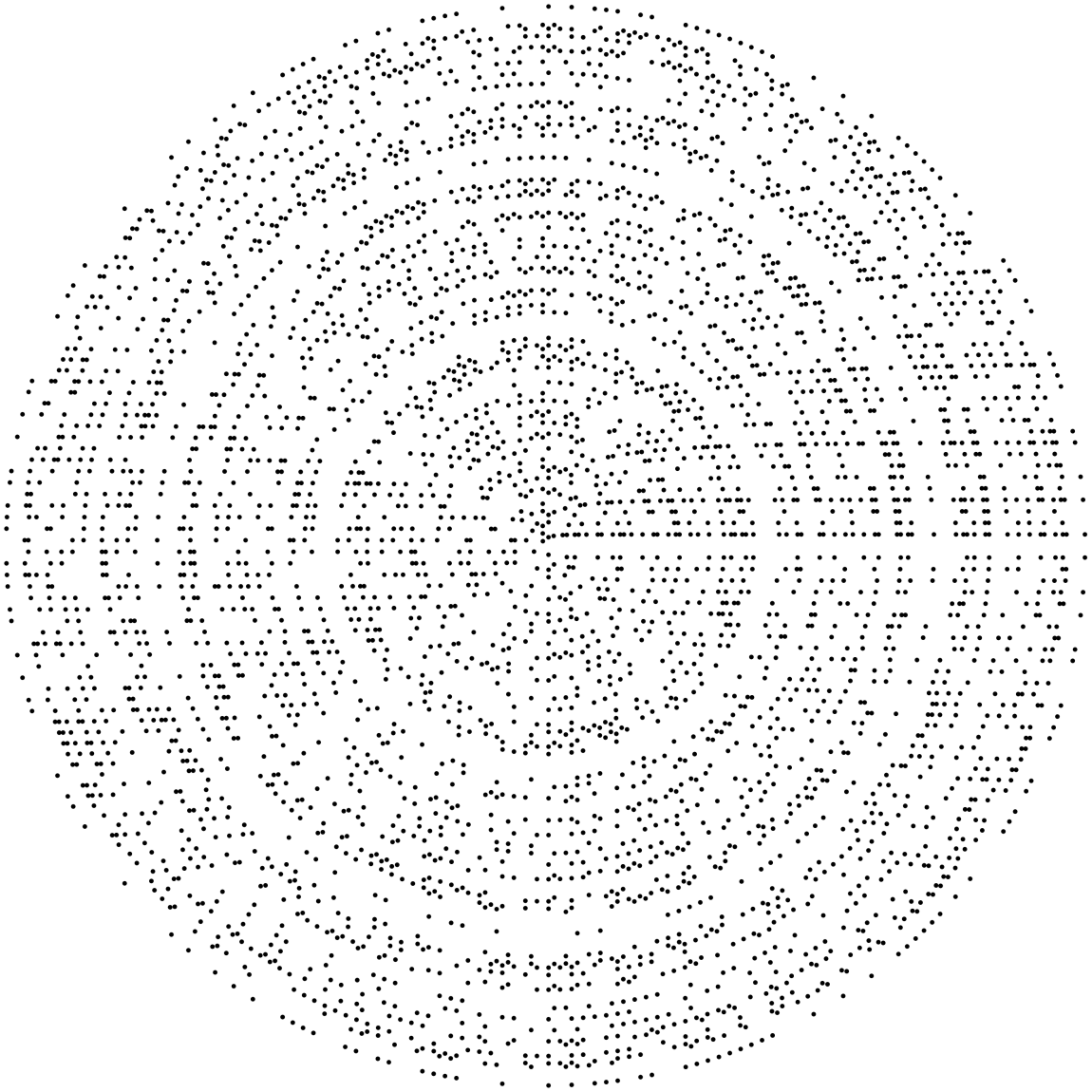
Manchester
Metropolitan
University

6G5Z0048 Number Theory and Abstract Algebra
Department of Computing and Mathematics
Faculty of Science and Engineering
2025/26

Number Theory

Lecture Notes



Dr Killian O'Brien

Contents

Chapter 1

The integers

In this chapter we consider a set of axioms that defines the integers. We can view these axioms as providing a rigorous foundation on top of which we can build the body of number theory. We shall not be focused on these axioms themselves in these number theory notes – they are studied in detail in the fields of *logic* and the *foundations of mathematics*. But we will want to dwell on the concept of induction as it is of central importance to the study of the integers.

❦

We are already have some familiarity with the set of integers,

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}, \tag{1.1}$$

and the operations of addition and multiplication of integers. However we need a rigorous foundation for our study of them. This foundation comes in the form of a list of axioms – statements that describe the fundamental properties that the integers have with regard to addition, multiplication, the order relation etc, and from which all the other properties of the integers can be derived. This list of axioms should *aim to be* complete[1] , in the sense that any property of the integers should be derivable from the axioms. The list should also be minimal in the sense that each axiom should be logically independent of the others.

The need to take such care at his initial stage can be appreciated by considering all the other mathematical systems that have addition-like and multiplication-like operations, such as the natural numbers ($\mathbb{N}$), the rationals ($\mathbb{Q}$), the real numbers ($\mathbb{R}$), the complex numbers ($\mathbb{C}$), matrices, functions, ..., to name but a few.

1.1 Axioms for the integers

Here we present a system of 11 axioms that suffice to uniquely define the integers $\mathbb{Z}$, in that any other system satisfying all these axioms will be essentially the same as the integers.

We will speak of a non-empty set S which has two operations, addition ($+$) and multiplication ($\cdot$) defined on it. These can be thought of as functions

$$+ : S \times S \to S, \tag{1.2}$$

$$\cdot : S \times S \to S. \tag{1.3}$$

[1] In fact we know that it is impossible do this. Kurt Gödel's First Incompleteness Theorem effectively says that any set of axioms for the integers cannot be both consistent and complete. This means that either there will be true statements about the integers that cannot be derived from the axioms, or the system will be inconsistent, i.e. it will contain contradictions and so any statement at all (be it true or false) can be deduced from the axioms.

The first set of axioms concern the addition operation.

1. (*Assosiativity of addition*) For all $x, y, z \in S$, $(x + y) + z = x + (y + z)$.
2. (*Existense of additive identity*) There exists $0 \in S$ with the property that for all $x \in S$, $x + 0 = 0 + x = x$.
3. (*Existence of additive inverses*) For all $x \in S$, there exists $-x \in S$ such that $x + (-x) = (-x) + x = 0$.
4. (*Commutativity of addition*) For all $x, y \in S$, $x + y = y + x$.

These axioms characterise such a system $(S, +)$ as a *commutative group*. The next set of axioms concern the multiplication operation.

5. (*Associativity of multiplication*) For all $x, y, z \in S$, $x(yz) = (xy)z$.
6. (*Existence of multiplicative identity*) There exists $1 \in S$ with the property that for all $x \in S$, $1x = x1 = x$.
7. (*Commutativity of multiplication*) For all $x, y \in S$, $xy = yx$.
8. (*Distributivity between addition and multiplication*) For all $x, y, z \in S$, $(x + y)z = xz + yz$.

These eight axioms characterise the system $(S, +, \cdot)$ as a *commutative ring with identity*.

The next set of axioms concern the concept of the ordering of the elements of S. The ordering $>$ is defined in terms of a set of *positive* elements P. We will write $x > 0$ to mean that $x \in P$, and write $x > y$ to mean that $x - y \in P$.

The system $(S, +, \cdot)$ is an *ordered* ring if there exists a subset $P \subset S$, (think of P as containing all the 'positive' elements) satisfying the following three axioms.

9. (*Trichotomy*) S is a disjoint union

$$S = -P \cup \{0\} \cup P, \tag{1.4}$$

   where $-P = \{-x : x \in P\}$.

10. (*Positivity preserved by sums and products*) For all $x, y \in P$ we have $x + y \in P$ and $xy \in P$.

A system $(S, +, \cdot, >)$ satisfying the above axioms is called a *commutative ordered ring*. All other properties of the order relation can be derived from the above axioms. $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are all examples of commutative ordered rings.

The final step in characterizing the integers, the one that discriminates them from other commutative ordered rings is the notion that the elements 1, $1 + 1$, $1 + 1 + 1$, ...etc are *all* of the positive integers. This notion is captured by either of the following two logically equivalent axioms.

11a. (*Induction axiom*) If J is a subset of the positive elements of S, i.e. $J \subset P \subset S$, and J has the properties

- $1 \in J$,
- $j \in J \Rightarrow j + 1 \in J$,

then $J = P$.

11b. (*Well-ordered axiom*) Every non empty subset of P has a least element, i.e. if $Q \subset P$ is non-empty then there exists $q_{\min} \in Q$ such that for all $q \in Q$ we have $q_{\min} \leq q$.

Moreover the least element $q_{\min}$ referred to in axiom (11b.) is unique, this following from the trichotomy axiom.

It can be shown that there is a unique algebraic system satisfying all the axioms 1 - 11, though we will not go into the details of this proof here. This system is called the integers $\mathbb{Z}$ and the set P of positive integers is more commonly referred to as the natural numbers $\mathbb{N}$. Any other algebraic system which is constructed in such a way as to satisfy axioms 1 - 11 will be essentially a re-labelling of $\mathbb{Z}$ (the technical term is *isomorphic*).

1.2 Consequences of the axioms

As we have said it should be possible to derive other basic properties of the integers from the axioms. Here is a list of some basic consequences that can all be derived from the axioms. Some of the proofs can be tricky and awkward to find. You can find the proofs in the accompanying solutions. As we said above, we shall not dwell on these matters here, instead preferring to get on with the number theory.

Exercise 1.1.

1. The zero element is unique, i.e. if $0'$ is any other integer satisfying $z+0' = z = 0'+z$ for every z then $0' = 0$.
2. Additive inverses are unique, i.e. let $z \in \mathbb{Z}$, if x and x' satisfy $z + x = 0 = z + x'$ then $x = x'$.
3. The multiplicative element 1 is unique.
4. For any $z \in \mathbb{Z}$ we have $-(-z) = z$.
5. For all $z \in \mathbb{Z}$ we have $0z = 0$.
6. For all $z \in \mathbb{Z}$ we have $-z = (-1)z$.
7. $(-1)^2 = 1$.
8. For all $x, y \in \mathbb{Z}$ we have
$$x(-y) = (-x)y = -(xy). \tag{1.5}$$
9. For all $x, y \in \mathbb{Z}$ we have $(-x)(-y) = xy$.
10. (*Cancellation in +*). For all $x, y, z \in \mathbb{Z}$
$$x + z = y + z \;\; \Rightarrow \;\; x = y. \tag{1.6}$$
11. (*Trichotomy*). For any $z \in \mathbb{Z}$ exactly one of the following is true: $z = 0$, $z > 0$ or $0 > z$. Or more generally, for all $x, y \in \mathbb{Z}$ exactly one of the following is true: $x = y$, $x > y$ or $y > x$.
12. (*Transitivity of >*). If $x > y$ and $y > z$ then $x > z$.
13. For integers x, y, if $x > 0$ and $y > 0$ then $x + y > 0$ and $xy > 0$.
14. For integers x, y, if $x > y$ then for all $z \in \mathbb{Z}$ we have $x + z > y + z$.
15. $1 > 0$.

16. For all integers z, if $z \neq 0$ then $z^2 > 0$.
17. For integers x, y, z where $x > y$, if $z > 0$ then $xz > yz$. If $z < 0$ then $xz < yz$.
18. (*Zero-divisors law*). For integers x, y, if $xy = 0$ then $x = 0$ or $y = 0$.
19. (*Cancellation in* $\cdot$). For integers x, y, if $z \neq 0$ and $xz = yz$, then $x = y$.
20. (*More general well-orderedness*). Consider a non-empty subset $A \subset \mathbb{Z}$. If A is bounded above then A contains a greatest element. Similarly, if A is bounded below then A contains a least element.

It is a worthwhile experience to construct proofs for results like this where each step is explicitly justified with reference to the axioms (or previously established results). However it becomes a bit tedious if we always have to take such trouble over relatively straightforward algebraic manipulations. So in future we will not reference the axioms in such detail, except for the induction (or well-ordered) axiom since this provides a key proof method for many results and is the axiom that differentiates the integers from the other number systems.

1.3 Proofs by induction

Many important results in number theory are proved using the induction axiom (or the well-ordered axiom). The induction axiom was expressed in terms of elements of a set. However proofs by induction are more usually presented by associating a statement with each positive integer and making use of the following version of the axiom.

> **Usual phrasing of induction principle**
> Suppose that we have a statement $P(n)$ associated to every integer $n \geq 1$. If the following two statements hold:
>
> - $P(1)$ is true,
> - for all $k \geq 1$, $P(k) \Rightarrow P(k+1)$,
>
> then we can conclude that $P(n)$ holds for every integer $n \geq 1$.

The following exercises show typical basic uses of induction where we prove a straightforward equation or inequality featuring the single variable n. More sophisticated uses of induction will feature in later chapters where we for example we prove a statement for all integers by inducting over the number of primes featuring in the prime factorization of an integer or we prove a statement for all polynomials of a certain kind by inducting over the degree of a polynomial. Look out for these uses when they arise.

Exercise 1.2. Provide proofs for the following results using induction.

1. $\forall\, n \geq 1 \ \displaystyle\sum_{j=1}^{n} j = \frac{1}{2}n(n+1)$.
2. $\forall\, n \geq 1 \ \displaystyle\sum_{j=1}^{n} j^2 = \frac{1}{6}n(n+1)(2n+1)$.
3. $\forall\, n \geq 1 \ \displaystyle\sum_{j=1}^{n} (2j-1) = n^2$.

4. $\forall\, n \geq 1 \;\; \displaystyle\sum_{j=1}^{n} j^3 = \left(\sum_{j=1}^{n} j\right)^2 = \frac{1}{4}n^2(n+1)^2.$

5. $\forall\, n \geq 1 \;\; \displaystyle\sum_{j=1}^{n}(3j-1) = \frac{1}{2}n(3n+1).$

6. $\forall\, n \geq 1 \;\; \left(1+\frac{1}{2}\right)^n \geq 1+\frac{n}{2},$

7. $\forall\, n \geq 1 \; 2^n \leq \frac{(2n)!}{n!n!}.$

Sometimes we make use of what is known as *strong induction*. Again this is just a rephrasing of the induction principle, it is logically equivalent to those we have already met. In strong induction the induction step is proved with the aid of the assumption that the result holds for all integers less than the current integer in question.

Strong induction principle
Suppose that we have a statement $P(n)$ associated to every integer $n \geq 1$. If the following statement holds for all integers $k \geq 1$,

$$\Big(P(1) \wedge P(2) \wedge \cdots \wedge P(k-1)\Big) \Rightarrow P(k), \tag{1.7}$$

then we can conclude that $P(n)$ holds for every integer $n \geq 1$.

Where's the base case? In strong induction we do not need to prove a separate base case as long as we genuinely prove the statement in (1.7) for all $k \geq 1$. Notice that in the case $k = 1$ the left-hand side of the implication is actually an empty conjunction. So the proof of (1.7) for $k = 1$ is actually a proof of the base case $P(1)$!

Equivalence of induction and well ordering

Theorem 1.1. *The induction and well ordered axioms are logically equivalent, i.e.*

$$(11a) \Leftrightarrow (11b).$$

Proof. Left as an exercise for lectures or tutorials. □

Chapter 2

Integer divisibility

In this chapter we introduce the divisibility relation on the integers and look at its basic properties and related concepts. The relation of divisibility accords exactly with our primary-school notions of one number *evenly dividing* into another.

❦

2.1 Divisibility

Definition 2.1 (Divisibility)**.** Let $a, b \in \mathbb{Z}$. We say that b *divides* a if and only if there exists an integer $c \in \mathbb{Z}$ such that

$$a = bc.$$

If this is so then b and c can be referred to as *factors* or *divisors* of a, and a can be referred to as a (integer) multiple of b and c.

We write $b|a$ to denote that b divides a and $b \nmid a$ to denote that it does not.

Warning about the notation

The notation $a|b$ for "a *divides* b" is quite standard and used throughout the mathematical literature. However there is scope for confusion if one does not remember clearly which of the two numbers is the *divisor* or *factor* (a in this case) and which is the *divisee*, i.e. the number being divided up, (b in this case). I have noticed students making such mistakes before so you need to take care, especially if you have not come across this notation before. And if you are someone who is prone to such mistakes then be warned and take appropriate steps to ensure you do not commit such errors. Perhaps this confusion is caused by the similarity of this notation to one of the ways of writing fractions, e.g. x/y, where x is being divided by y. **You have been warned!**

Example 2.1. The integers 1, 3, 5 and 15 all divide 15, whereas 10 is not divisible by 3.

Divisibility is a relation amongst integers, i.e. it is a two-place predicate, providing values for a and b in the predicate $a|b$ produces a statement, which may be true or false depending on the values. An important type of relation is one that behaves like the relation of equality, so called equivalence relations. These are relations that are reflexive, symmetric and transitive. Divisibility is **not** an equivalence relation. It is reflexive and transitive but it is not symmetric. Other important properties are outlined in the following theorem.

Theorem 2.1 (Basic properties of divisibility)**.** *The divisibility relation enjoys the following properties:*

1. (*Reflexivity*) For all $a \in \mathbb{Z}$, $a|a$.
2. (*Transitivity*) For all $a, b, c \in \mathbb{Z}$, if $a|b$ and $b|c$ then $a|c$.
3. (*Divisibility of linear combinations*) For all $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then for all $n, m \in \mathbb{Z}$, $a|\,(nb + mc)$.
4. (1 *divides everything*) For all $a \in \mathbb{Z}$, $1|a$.
5. (*everything divides* 0) For all $a \in \mathbb{Z}$, $a|0$.
6. (0 *divides only itself*) For all $a \in \mathbb{Z}$, if $0|a$ then $a = 0$.
7. For all $a, b, c \in \mathbb{Z}$, if $c \neq 0$ then $a|b$ if and only if $ac|bc$.

The proofs of these properties all follow from one or more applications of the definition of divisibility and properties of the integers. The proofs are left as exercises.

Note that an integer z has exactly the same divisors as its negative $-z$. In order to avoid duplication we normally confine our attention to the divisibility properties of the positive integers.

2.2 Primes

We shall have a lot more to say about prime numbers later, but for now we give the definition and state a fundamental theorem concerning primes in the integers.

Definition 2.2 (Prime, Composite)**.** An integer $p > 1$ is *prime* if it has no positive divisors other than itself and 1. An integer $n > 1$ which is not prime is called *composite*.

It is conventional to reserve the letter p to denote primes, so when writing mathematics in the context of number theory one should not use p to denote a composite number. Note that the integer 1 is considered neither prime nor composite. As we shall see as important aspect of primes is how every integer factors uniquely into a product of prime factors. Allowing 1 as one of these prime factors would destroy this uniqueness.

The list of prime numbers begins

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots \tag{2.1}$$

As the name suggests, an important result concerning primes is the *Fundamental Theorem of Arithmetic*. This will be proved later but it is worth stating it now.

Fundamental Theorem of Arithmetic
Every positive integer n factors into a product of primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \quad p_i \text{ prime}, \alpha_i \in \mathbb{Z}^+ \tag{2.2}$$

and this factorisation is unique up to the order in which the primes are written down.

Most people's intuition about the integers agrees with this result and the existence of such prime factorisations can be proved now and follows by recursively applying the definition of prime/composite to n and using the transitivity of divisibility. But the proof of the uniqueness of these factorisations requires some more theory to be developed.

2.3 Common divisors

Relationships between the divisibility of different integers is investigated using the concept of common divisors.

Definition 2.3 (Common divisor)**.** Let $a, b \in \mathbb{Z}$. An integer c is a *common divisor* of a and b if and only if c divides a and c divides b.

Definition 2.4 (Greatest common divisor)**.** By the well-orderedness of $\mathbb{Z}$ there exists a *greatest common divisor* of a and b. This is denoted $\gcd(a, b)$. Note that some authors use a minimalist notation of (a, b) to denote the greatest common divisor, but we will stick with the more informative $\gcd(a, b)$ in these notes.

Example 2.2. For simple small or simple arguments we can decide the gcd value by inspection, e.g. $\gcd(2, 4) = 2$, $\gcd(30, 42) = 6$, etc. How to get the value of $\gcd(23458972348957, 2348579823475897342)$ is maybe not so clear at the moment!

Definition 2.5 (Coprime)**.** A pair of integers $a, b \in \mathbb{Z}$ are *coprime* (or *relatively prime*) if and only if $\gcd(a, b) = 1$.

This is an important concept which will be used in many places through the notes. A coprime pair is a pair of integers with no non-trivial common divisors. Of course every pair always has at least the common divisor of 1 as 1 divides all integers. As such 1 is often referred to as a trivial common divisor.

Example 2.3. The pair 10, 21 are coprime as they have no positive common divisors apart from 1, so $\gcd(10, 21) = 1$.

Note that as long as a, b are not both zero then $\gcd(a, b)$ exists. This follows since all common divisors of a and b are bounded above by $\max(|a|, |b|)$ in this case, and so a greatest one exists by the well-orderedness of $\mathbb{Z}$.

What we seek now is a method or algorithm to obtain the greatest common divisor of two given integers a and b. We can describe $\gcd(a, b)$ in terms of the overlap in the prime factorisations of a and b. But we have not yet proved the Fundamental Theorem of Arithmetic so this path is not available to us yet. In addition, obtaining the prime factorisations of large integers is computationally hard, whereas the Euclidean algorithm is not so much.

The method for obtaining greatest common divisors is known as Euclid's Algorithm. It consists of repeatedly applying the process of *integer division with remainder*. Again, while we give a rigorous formal treatment of this process here, the concept should be very familiar to you from your schoolwork with integer numbers.

Theorem 2.2 (Integer division with remainder)**.** *Let $a, b \in \mathbb{Z}$, $b \neq 0$. There exists a unique pair $q, r \in \mathbb{Z}$ such that*

$$a = qb + r, \qquad 0 \leq r < |b|. \tag{2.3}$$

Proof. First we prove the existence of such a pair q, r. Consider the set S of non-negative integers of the form $a - qb$, i.e.

$$S = \{a - tb \,:\, t \in \mathbb{Z},\, a - tb \geq 0\}\,. \tag{2.4}$$

Since $b \neq 0$ adding or subtracting sufficient multiples of b from a will eventually produce positive integers, so S is non-empty. By the well-ordered axiom S contains a least element $r = a - qb \geq 0$.

We claim that $r < |b|$. If this were not true then we would have

$$r = a - qb \geq |b| \tag{2.5}$$
$$\Rightarrow\ r - |b| = a - (q \pm 1)b \geq 0. \tag{2.6}$$

This last line shows that we would have $0 \leq r - |b| < r$ and $r - |b| \in S$. But this contradicts the fact that r is the least element in S. So we can conclude that indeed $0 \leq r < |b|$ as required and so we know that the required pair (q, r) exists.

The fact that the pair q, r is unique follows from the uniqueness of r as being the least element in S. For if there were two pairs q_1, r_1 and q_2, r_2 satisfying the conditions of the theorem then we would have:

$$r_1 = r_2, \text{ by uniqueness of least element of } S \tag{2.7}$$
$$\Rightarrow r_1 - r_2 = (q_1 - q_2)b = 0, \tag{2.8}$$
$$\Rightarrow q_1 - q_2 = 0, \text{ by the zero-divisors law, since } b \neq 0 \tag{2.9}$$

and so the pair q, r is indeed unique. □

Before describing the Euclidean Algorithm we give a characterisation of $\gcd(a, b)$ in terms of linear combinations of a and b. The proof of this uses a similar method to the proof of the integer division theorem.

Theorem 2.3 (Characterisation of greatest common divisor)**.** *Suppose that $a, b \in \mathbb{Z}$ are not both zero and that $d = \gcd(a, b)$. Then there exists $n, m \in \mathbb{Z}$ such that*

$$d = ma + nb, \tag{2.10}$$

and moreover any common divisor of a and b divides d.

Proof. Let S be the set of all positive linear combinations of a and b, i.e.

$$S = \{\alpha a + \beta b \,:\, \alpha, \beta \in \mathbb{Z},\ \alpha a + \beta b > 0\}. \tag{2.11}$$

By the well-ordered axiom S has a least element d, which we can write as

$$0 < d = ma + nb, \tag{2.12}$$

for some pair of integers m, n. We claim that d is a common divisor of a and b.

Suppose that d did not divide a. Then by the integer division theorem we could write

$$a = qd + r, \quad 0 < r < d, \tag{2.13}$$
$$\Rightarrow r = a - qd, \tag{2.14}$$
$$= a - q(ma + nb), \text{ (from (2.12) above)} \tag{2.15}$$
$$= (1 - qm)a - qnb. \tag{2.16}$$

So we see that r would be a linear combination of a and b, i.e. $r \in S$. But then this would contradict the fact that d is the least element of S, since we have $r < d$ above. So we conclude that d does indeed divide a. An argument along similar lines will show that d also divides b. So we can conclude that d is a common divisor of a and b.

Next we see that if e is any other common divisor of a and b then $e|d$ by property 3 of theorem 2.1. Hence d is the greatest common divisor and all other common divisors divide d. □

Exercise 2.1. The following are consequences of the recently introduced definitions and results along with previous results on divisibility.

1. Let $a, b \in \mathbb{Z}$ be not both zero. Consider the sets A and B defined by

$$A = \{\, ma + nb \,:\, m, n \in \mathbb{Z} \}\,, \tag{2.17}$$

$$B = \{\, m \gcd(a, b) \,:\, m \in \mathbb{Z} \}\,. \tag{2.18}$$

   Show that $A = B$, i.e. linear combinations of a and b correspond exactly with multiples of $\gcd(a, b)$.

2. Prove that a and b are coprime if and only if there exists $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

3. Suppose that $d = \gcd(a, b)$ and that $a = \alpha d$ and $b = \beta d$. Prove that $\gcd(\alpha, \beta) = 1$.

4. Prove that if $\gcd(a, b) = d$ then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

5. Suppose that $a|c$ and $b|c$ and $\gcd(a, b) = 1$. Prove that $ab|c$.

6. (Euclid's Lemma). Suppose that $c|ab$ and that $\gcd(c, a) = 1$. Prove that $c|b$.

2.4 The Euclidean algorithm and Bezout's identity

We start with a lemma that describes how integer division with remainder relates to greatest common divisors of the divisee, divisor and remainder.

Lemma 2.4. *If $a = qb + r$ then the common divisors of a and b are exactly the common divisors of b and r, in particular*

$$\gcd(a, b) = \gcd(b, r). \tag{2.19}$$

The Euclidean Algorithm works by exploiting this lemma. If we are trying to find $\gcd(a, b)$ (assume that $a \geq b$) then we can perform the integer division step and then we know that $\gcd(a, b) = \gcd(b, r)$ and moreover the pair b, r is *smaller* than the pair a, b. By repeating this procedure we will eventually reach a pair of integers, small enough so that their gcd is obvious. Before describing the algorithm in general we will give an example which shows all the details.

Example 2.4. Find $\gcd(525, 90)$.

Solution.

$$525 = 5 \times 90 + 75, \quad \Rightarrow \quad \gcd(525, 90) = \gcd(90, 75), \tag{2.20}$$

$$90 = 1 \times 75 + \underline{15}, \quad \Rightarrow \quad \gcd(90, 75) = \gcd(75, 15), \tag{2.21}$$

$$75 = 5 \times 15 + 0, \quad \Rightarrow \quad \gcd(75, 15) = \gcd(15, 0) = 15. \tag{2.22}$$

Combining the gcd equations shows that $\gcd(525, 90) = 15$. We notice that we repeat the integer divisions until we reach a remainder of zero. The last non-zero remainder obtained is the greatest common divisor of the original pair a, b.

Bezout's identity

In addition to finding the gcd, the algorithm also provides an instance of the linear combination referred to in theorem 2.3. This linear combination of a and b, equal to their greatest common divisor, theat we get from the Euclidean algorithm is called Bezout's identity. It is found by working through the integer division equations backwards, starting with the second-last one, i.e. the one featuring the gcd as the remainder. We then work our way back through the equations until we have the gcd d expressed as a linear combination of the initial a and b.

$$\begin{aligned} \underline{15} &= 90 - 1 \times 75, \text{ from eq. (2.21)} && (2.23)\\ &= 90 - (525 - 5 \times 90), \text{ from eq. (2.20)} && (2.24)\\ &= -1 \times 525 + 6 \times 90. && (2.25) \end{aligned}$$

□

We give another, slightly longer example, before describing the process in general.

Example 2.5. Find $\gcd(12378, 3054)$.

Solution.

$$\begin{aligned} 12378 &= 4 \times 3054 + 162, && (2.26)\\ 3054 &= 18 \times 162 + 138, && (2.27)\\ 162 &= 1 \times 138 + 24, && (2.28)\\ 138 &= 5 \times 24 + 18, && (2.29)\\ 24 &= 1 \times 18 + \underline{6}, && (2.30)\\ 18 &= 3 \times 6 + 0. && (2.31) \end{aligned}$$

So $\gcd(12378, 3054) = 6$. Working backwards, as described in the previous example, will eventually produce 6 as a linear combination of 12378 and 3054.

$$\begin{aligned} 6 &= 24 - 18, \text{ from eq. (2.30)} && (2.32)\\ &= 24 - (138 - 5 \times 24), \text{ from eq. (2.29)} && (2.33)\\ &= 6 \times 24 - 138, && (2.34)\\ &= 6 \times (162 - 138) - 138, && (2.35)\\ &= 6 \times 162 - 7 \times 138, && (2.36)\\ &\vdots && (2.37)\\ &= 132 \times 12378 - 535 \times 3054, && (2.38) \end{aligned}$$

which is the desired linear combination. □

Algorithm 2.1 (Euclidean Algorithm)**.** *The following procedure is an algorithm for determining* $\gcd(a, b)$ *and obtaining the integer coefficients* m, n *for an expression*

$$\gcd(a, b) = ma + nb. \tag{2.39}$$

We assume that $a \geq b > 0$ (this is sufficient for the general case by earlier comments). Consider the sequence of integer divisions that are carried out until a remainder of zero is obtained:

$$a = q_1 b + r_1, \quad 0 < r_1 < b \tag{2.40}$$
$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \tag{2.41}$$
$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \tag{2.42}$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \tag{2.43}$$
$$r_{n-1} = q_{n+1} r_n. \tag{2.44}$$

The last non-zero remainder r_n obtained in these equations is the required greatest common divisor $r_n = gcd(a, b)$.

From eq (2.43) we get an expression for r_n as a linear combination of r_{n-1} and r_{n-2},

$$r_n = r_{n-2} - q_n r_{n-1}. \tag{2.45}$$

Working backwards through these equations we replace each intermediate remainder r_j ($1 \leq j < n$) with linear combinations of earlier remainders until we arrive at a linear combination for r_n in terms of a and b, as required.

The justification for the conclusions of the algorithm follow from theorem 2.2 and lemma 2.4. The fact that the algorithm will terminate (i.e. stop after a finite number of steps) follows from the fact that the remainders r_i constitute a strictly decreasing sequence of non-negative integers and hence this sequence must arrive at zero after a finite number of steps.

An immediate application of the Euclidean Algorithm gives a proof of the following result.

Theorem 2.5. *If m is a positive integer then*

$$\gcd(ma, mb) = m \gcd(a, b), \tag{2.46}$$

(where a, b are not both zero).

Proof. This follows immediately from observing that the sequence of integer divisions that come about from applying the Euclidean Algorithm to the pair ma, mb are simply the equations from applying the algorithm to the pair a, b, but multiplied through by m. For instance,

$$\Big[a = q_1 b + r_1, \ (0 \leq r_1 < b)\Big] \Leftrightarrow \Big[ma = q_1 mb + mr_1, \ (0 \leq mr_1 < mb)\Big]. \tag{2.47}$$

So if $\gcd(a, b) = r_n$, the final non-zero remainder, then $\gcd(ma, mb) = mr_n$, as required. □

Related to the concept of the greatest common divisor is that of the least common multiple.

Definition 2.6 (Least common multiple)**.** Let $a, b \in \mathbb{Z}$ be both non-zero. The *least common multiple*, $\operatorname{lcm}(a, b)$, is the smallest positive integer that is a both a multiple of a and a multiple of b.

There is a direct relationship between the greatest common divisor and the least common multiple of a pair of integers.

Theorem 2.6. *If $a, b \in \mathbb{Z}$ are both positive then*

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab. \tag{2.48}$$

Proof. Let $d = \gcd(a, b)$. We prove the result directly by showing that the quantity $\frac{ab}{d}$ is equal to $\text{lcm}(a, b)$.

Since d divides a and b there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$a = \alpha d, \ b = \beta d, \tag{2.49}$$

and so

$$\frac{ab}{d} = \alpha b = \beta a. \tag{2.50}$$

This shows that $\frac{ab}{d}$ is a positive common multiple of a and b. Now we show it is the least such one. Suppose that c is another common multiple of a and b, say

$$c = \lambda a = \mu b, \ (\lambda, \mu \in \mathbb{Z}). \tag{2.51}$$

Now since $d = \gcd(a, b)$ we know there are $m, n \in \mathbb{Z}$ such that

$$d = ma + nb. \tag{2.52}$$

Now we examine the quantity c divided by the integer $\frac{ab}{d}$,

$$\frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(ma + nb)}{ab} = \frac{c}{b}m + \frac{c}{a}n = \mu m + \lambda n. \tag{2.53}$$

This last expression shows that c divided by the integer $\frac{ab}{d}$, is an integer, or in other words, $\frac{ab}{d}$ divides c and hence $\frac{ab}{d} \leq c$ as required. □

Exercise 2.2. Here are some questions to help you practice using the Euclidean Algorithm. You should complete these and others until you are confident in using it to find both the gcd and a linear combination for the gcd. It is good practice to make a few notes as you go emphasizing how the pairs we apply the integer division process to all have the same gcd, by lemma 2.4.

1. Use the Euclidean algorithm to find $\gcd(143, 227)$, $\gcd(306, 657)$ and $\gcd(272, 1479)$.
2. Find integers m, n that satisfy the following equations,
   a) $\gcd(56, 72) = 56m + 72n$,
   b) $\gcd(24, 138) = 24m + 138n$,
   c) $\gcd(119, 272) = 119m + 272n$,
   d) $\gcd(1769, 2378) = 1769m + 2378n$.

Exercise 2.3. These exercises develop some more general results as consequences of the definitions and results we have seen so far.

1. Prove or disprove the following statement: if $a|(b + c)$ then $a|b$ or $a|c$.
2. Use the process of integer division with remainder to prove that if $a \in \mathbb{Z}$, one of the integers a, $a + 2$ or $a + 4$ is divisible by 3.
3. Prove that for all $a \in \mathbb{Z}$, $4 \nmid (a^2 + 2)$.
4. Prove the following
   a) $\forall\, n \geq 1 \ 7|(2^{3n} - 1)$,

b) $\forall\, n \geq 1\ 8|(3^{2n}+7)$,

c) $\forall\, n \geq 1\ 3|(2^n+(-1)^{n+1})$.

5. Prove that if an integer a is not divisible by 2 nor by 3, then 24 does divide a^2-1.

6. Prove that in the linear combination

$$\gcd(a,b) = ma + nb,$$

the coefficients m and n are coprime.

7. Prove that if a is odd then $24|a(a^2-1)$.

8. Prove that if a and b are both odd then $8|(a^2-b^2)$.

9. Prove that for all $a \in \mathbb{Z}$, $360|\big(a^2(a^2-1)(a^2-4)\big)$.

10. Prove the following properties of the gcd,

a) If $\gcd(a,b) = \gcd(a,c) = 1$ then $\gcd(a,bc) = 1$.

b) If $\gcd(a,b) = 1$ and $c|a$ then $\gcd(c,b) = 1$.

c) If $\gcd(a,b) = 1$ then $\gcd(ac,b) = \gcd(c,b)$.

d) If $\gcd(a,b) = 1$ and $c|(a+b)$ then $\gcd(a,c) = \gcd(b,c) = 1$.

11. Suppose that a and b are coprime, show that for all $n \geq 1$, a^n and b^n are coprime.

12. Prove that for all $n \geq 1$, if $a^n|b^n$ then $a|b$.

13. Suppose that c is a common multiple of a and b. Prove that $\operatorname{lcm}(a,b)|c$.

GCD of three or more integers

The concept of greatest common divisors extends to sets of three or more integers without difficulty. The Euclidean Algorithm can still be applied to find the gcd in these cases. This is done by finding the gcd of pairs of integers at a time and using results like the following (quoted for the triple of integers case).

Theorem 2.7 (Greatest common divisor of three integers)**.** *Let $d = \gcd(a,b,c)$ have the obvious definition. Then*

$$d = \gcd\big(\gcd(a,b),c\big) = \gcd\big(\gcd(a,c),b\big) = \gcd\big(\gcd(b,c),a\big). \tag{2.54}$$

Proof. Exercise. □

Example 2.6. Determine $d = \gcd(198, 288, 512)$ and find coefficients for a linear combination

$$d = 198\alpha + 288\beta + 512\gamma. \tag{2.55}$$

Chapter 3

Infinitely many primes and the Fundamental Theorem of Arithmetic

In this chapter we present the formal definition of a prime number and look at some of the immediate properties of prime numbers. Two results stand out in this chapter: there are an infinite number of primes, and any positive integer factorizes uniquely into a product of primes.

❦

Definition 3.1 (Prime, Composite)**.** An integer $p > 1$ is *prime* if it has no positive divisors other than itself and 1. An integer $n > 1$ which is not prime is called *composite*.

As we said in chapter 2 the sequence of prime numbers begins

$$2, 3, 5, 7, 11, \ldots$$

Prime numbers are important as they are the *building blocks* of all the integers, as the following results makes clear.

Theorem 3.1. *Every integer $n \geq 2$ is a prime number, or can be written as a product of primes.*

Proof. This proof neatly illustrates the use of strong induction. Assume that the result holds true for all integers m satisfying $2 \leq m < k$. Then if k is prime we are done. If k is not prime then it has a positive divisor $k_1 \neq 1$, k. But then we have

$$k = k_1 k_2, \quad 1 < k_1, k_2 < k. \tag{3.1}$$

By the induction hypothesis both k_1 and k_2 are either primes or products of primes. Hence k can be written as a product of primes.

Therefore by the principle of strong induction the theorem is true for all $n \geq 2$. □

3.1 An infinite number of primes

A fundamental question concerning the sequence of primes given above is whether it terminates at some point, or indeed goes on without end. The following theorem settles the matter. The proof given here is

Theorem 3.2 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. Suppose there are only a finite number of prime numbers. We could denote them

$$p_1, p_2, p_3, \ldots, p_N.$$

Consider the integer M, given by

$$M = p_1 p_2 \ldots p_N + 1. \tag{3.2}$$

By theorem 3.1 M is either prime or has a prime factor. Now for each $i = 1, 2, \ldots N$, $M > p_i$, so we conclude that M is not prime. Therefore it has a prime divisor, p_j say, for some $1 \leq j \leq N$. However rewriting the definition of M we see that

$$1 = M - p_1 p_2 \ldots p_N. \tag{3.3}$$

But then $p_j|1$, since $p_j|p_1 \ldots p_N$ and $p_j|M$, i.e. $p_j = 1$. However this is a contradiction since p_j is a prime.

So our assumption at the beginning of this proof is false, i.e. there are infinitely many primes as required. □

3.2 The Fundamental Theorem of Arithmetic (FTA)

Theorem 3.1 told us that every integer is a product of primes. This is the sense in which we regard the primes as the building blocks of all integers. However that theorem made no claim on whether such representations are unique. For example, the integer 495 can be expressed as

$$495 = 3^2 \times 5 \times 11. \tag{3.4}$$

But can 495 be expressed as a product of primes in a *different* way? Trivially we could write is as, say,

$$495 = 3 \times 11 \times 3 \times 5, \tag{3.5}$$

but we regard this factorization as equivalent to the first since the primes appearing in it are exactly the same and we have just written them down in a different order. But the question remains can we find a *different* set of primes which multiply together to give 495. Now for any particular number we can simply determine all the primes less than it and check all possible combinations. Such experimentation will always show that these factorizations are unique. But no amount of this experimentation will ever constitute a proof, as there are an infinite number of integers and an infinite number of primes. So we seek a rigorous proof of this fact in order to establish the FTA.

Theorem 3.3 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ factors into a product of primes*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \quad p_i \text{ prime}, \alpha_i \in \mathbb{Z}^+ \tag{3.6}$$

and this factorisation is unique up to the order in which the primes are written down.

While we may feel that this result is intuitively *true* we still need a proof of it. More so when we discover the fact that there exits other number-like systems where the equivalent property does not hold as in the following example (exploring such issues further is beyond the scope of this unit).

Example 3.1 (Non-unique factorisation)**.** Consider the ring

$$\mathbb{Z}[i\sqrt{5}] = \left\{ a + ib\sqrt{5} \,:\, a, b \in \mathbb{Z} \right\}, \tag{3.7}$$

which is a sub-ring of the field $\mathbb{C}$ of complex numbers. Unique factorization does not hold in $\mathbb{Z}[i\sqrt{5}]$ due to examples like

$$6 = 2 \times 3 = \left(1 + i\sqrt{5}\right)\left(1 - i\sqrt{5}\right). \tag{3.8}$$

In such rings where unique factorization does not hold there are the two related properties of *irreducible* and *prime*.

Before presenting the proof of the FTA we record a preliminary lemma, though important in its own right.

Lemma 3.4 (Euclid's lemma)**.** *Let $a, b, p \in \mathbb{Z}$ with p a prime. If $p|ab$ then $p|a$ or $p|b$.*

Proof. Suppose that $p|ab$. If $p|a$ we are done. So suppose further that $p \nmid a$. Since the only divisors of p are 1 and p we must have $\gcd(a, p) = 1$. By Euclid's algorithm there exist integers n and m such that

$$1 = np + ma, \tag{3.9}$$

from which we get

$$b = nbp + mab. \tag{3.10}$$

Both terms on the right of this equation are divisible by p and so by property 3 of theorem 2.1 we have $p|b$. □

By using the extended Euclidean algorithm (for three or more arguments) we can generalise Euclid's lemma as follows.

Corollary. *Let $a_1, \ldots, a_n, p \in \mathbb{Z}$ with p a prime. If $p|a_1 a_2 \ldots a_n$ then there exists $1 \leq i \leq n$ such that $p|a_i$.*

Now we can present the proof of the FTA.

Proof. (Fundamental Theorem of Arithmetic) From theorem 3.1 we already know that n can be factorized into primes. We will use strong induction to prove that this factorization is unique.

Let $n > 1$ and assume that the result is true for all integers $1 < k < n$, i.e. every such integer k has a prime factorization that is unique up to reordering the prime factors. By theorem 3.1 n has a factorization into a product of primes. Suppose there are two such factorizations

$$n = p_1 \ldots p_r = q_1 \ldots q_s, \tag{3.11}$$

where the ps and qs are primes.

Consider p_1. From equation (3.11) we have $p_1|n$, and so $p_1|q_1 \ldots q_s$. Then by the corollary to lemma 3.4 we know that p_1 divides one of the qs. Now by relabelling if necessary we can assume that $p_1|q_1$. But q_1 is prime, therefore $p_1 = q_1$. If $n = p_1 = q_1$ we are done, other wise consider the integer n',

$$n' = \frac{n}{p_1} = p_2 \ldots p_r = q_2 \ldots q_s, \tag{3.12}$$

and note that $1 < \frac{n}{p_1} < n$. So by the induction hypothesis n' has a unique prime factorization (i.e. $r = s$ and $p_2, \ldots, p_r$ are just a relabelling of $q_2, \ldots, q_s$). Therefore so does $n = p_1 n' = q_1 n'$.

So by induction the result holds for all positive integers n. □

Definition 3.2 (Canonical form)**.** The *canonical form* for a positive integer n is the factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i} \tag{3.13}$$

where the p_i are distinct primes, satisfy $p_1 < p_2 < \cdots < p_r$ and the integer α_i is the largest power of p_i dividing n.

This removes the ambiguity of reordering the prime factors of a number. Every positive integer $n > 1$ has a unique canonical form. We can use the canonical form to characterise the greatest common divisor and least common multiple of two integers a and b.

Exercise 3.1. Suppose the canonical forms of integers a and b are

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{s} q_i^{\beta_i}. \tag{3.14}$$

Can you write down the canonical form of $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of this information?

Solution. ... □

3.3 Existence of irrationals

The FTA can be used to demonstrate the existence of irrational quantities.

Theorem 3.5 (Pythagorean)**.** $\sqrt{2}$ *is irrational.*

Proof. Suppose on the contrary that it is rational, and we have

$$\sqrt{2} = \frac{a}{b}, \tag{3.15}$$

where $a, b \in \mathbb{Z}$, $a, b > 0$ and $\gcd(a, b) = 1$, i.e. the fraction is in reduced form. This leads to

$$b^2 2 = a^2. \tag{3.16}$$

This shows that $b|a^2$. We now consider the two cases $b > 1$ and $b = 1$ separately. If $b > 1$ then the FTA guarantees the existence of a prime p such that $p|b$, and so $p|a^2$, by transitivity of divisibility. By lemma 3.4 we then get $p|a$. So now we have $p|b$ and $p|a$ which implies that $\gcd(a, b) \geq p$. But this is a contradiction since we have arranged that $\gcd(a, b) = 1$.

On the other hand if $b = 1$ then we have $a^2 = 2$ which is also a contradiction. Therefore we conclude that $\sqrt{2}$ is irrational. □

This argument can be generalised to the following, the proof of which is left as an exercise.

Theorem 3.6. *Given any integer n, $\sqrt{n}$ is either an integer or irrational.*

Proof. Exercise. □

3.4 Established results and conjectures concerning primes

Part of the fascination of number theory is that there have been great successes in establishing strong results describing aspects of the primes. But there remain a number of famous open problems (i.e. problems that have not been solved yet) which are easy to comprehend on one level but have resisted solution up to now. Not that this is a bad thing. It is the desire to solve these open problems that has driven much of the development of modern number theory in the 19th & 20th centuries and today.

Definition 3.3 ($\pi(x)$)**.** The *prime counting function* $\pi : \mathbb{R} \to \mathbb{R}$ is defined by

$$\pi(x) = \#\text{ primes } p \text{ satisfying } p \leq x\ . \tag{3.17}$$

The function π counts the number of primes up to the value x. The long-term behaviour of π will tell us about the relative density of primes in the integers.

By considering the beginning of the sequence of primes both Gauss (in 1849) and Legendre (in 1798) noticed that $\pi(x)$ grew like the quantity $\frac{x}{\log x}$ and they conjectured that the behaviour of $\pi(x)$ would converge to that of $\frac{x}{\log x}$, but were unable to prove this. In 1859 Riemann, building on earlier work by Euler, found a way to link the behaviour of the *zeta* function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{3.18}$$

to the distribution of primes. In 1896 Hadamard and de la Vallée Poussin both settled the matter by proving the Prime Number Theorem.

Theorem 3.7 (Prime Number Theorem)**.** [1]

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1. \tag{3.19}$$

This and related work was the beginning of *Analytic Number Theory*, i.e. using the tools of real and complex analysis to prove results about the integers (which is a striking connection between the matters continuous (analysis) and discrete (the integers)). An important open problem in analytic number theory concerns the behaviour of the zeta function. A proof of it would have great implications for number theory

Conjecture 3.1 (Riemann Hypothesis)**.** The non-trivial zeroes of the of the zeta function $\zeta : \mathbb{C} \to \mathbb{C}$ are all of the form $\frac{1}{2} + ib$, for some $b \in \mathbb{R}$.

This problem is one of the Clay Mathematics Institute's Millenium Problems[2] and a prize of $1 million awaits the one who solves it.

Conjecture 3.2 (Goldbach)**.** Every even integer greater than 2 can be written as the sum of two primes.

Conjecture 3.3 (Twin primes)**.** There are an infinite number of *twin primes*, i.e. prime pairs of the form n, $n+2$.

[1] This is known as *asymptotic equivalence* and can be written as $\pi(x) \sim \frac{x}{\log x}$.

[2] http://www.claymath.org/millennium/

And the list goes on. For further reading and references on these and related matters you could consult the historical introduction in Apostol (1976)[3]. A classic study of the subject and its history is Dickson (1919)[4]

Exercise 3.2. 1. Practice obtaining canonical forms (prime-power factorizations), for example of the following numbers

$$111;\ 1234;\ 2345;\ 111,111;\ 999,999,999.$$

2. Find some counter-examples to the claim:

$$\forall\, a,b,c \in \mathbb{Z} \quad a|bc \Rightarrow \big(a|b \text{ or } a|c\big). \tag{3.20}$$

Can you explain how these counter-examples work in terms of the canonical forms of a, b, c?

3. Consider the canonical form

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Prove that n is a square if and only if each α_i is even, $i = 1, \ldots r$.

4. Formulate, and prove, the corresponding result for the mth root of n.

5. Show that the only prime number of the form $n^3 - 1$ is 7.

6. Consider the possible outcomes from performing integer division of a prime p with 6, i.e. $p = 6q+?$. Use the results of this analysis to prove that p^2+2 is never prime, for any prime $p \geq 5$.

7. Prove that for p a prime, if $p|a^n$ then $p^n|a^n$.

8. Suppose that $p, q \geq 5$ are prime. Prove that $p^2 - q^2$ is divisible by 24.

9. Is $n^4 + 4$ ever a prime, where $n > 1$?

10. Prove that if $2^n - 1$ is prime then so is n.

11. Prove that if $2^n + 1$ is prime then n is a power of 2.

12. Recall the Fibonacci sequence $\{f_n\}_{n=1}^{\infty}$ defined by

$$f_1 = f_2 = 1, \quad f_{n+1} = f_n + f_{n-1}.$$

Prove that $\gcd(f_n, f_{n+1}) = 1$ for every $n \geq 1$.

---

[3] Apostol, T. M. (1976) *Introduction to analytic number theory.* New York: Springer-Verlag.

[4] Dickson, L. E. (1919) *History of the theory of numbers* (3 volumes). Washington D.C.: Carnegie Institution of Washington. Online and download version available from The Internet Archive http://archive.org/details/historyoftheoryo01dick.

Chapter 4

The congruence relation

The concept of congruence is a way to study to systematically study the properties of the integers under integer division with remainder. By proving some basic properties of it we can quickly detect many patterns of the integers in this regard.

❦

4.1 Congruence

We start with the formal definition of, and notation for, the relation.

Definition 4.1 (Congruence relation)**.** Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say that a is *congruent* to b modulo n if and only if $n|a - b$. The notation used when a is congruent to b is

$$a \equiv b \pmod{n}, \tag{4.1}$$

and if a is not congruent to b we can write

$$a \not\equiv b \pmod{n}. \tag{4.2}$$

One should also think of the congruence relation in terms of the process of integer division with remainder as described in theorem 2.2.

Theorem 4.1 (Congruence and integer division with remainder)**.** *For any given modulus n, a is congruent to b modulo n if and only if a and b leave the same remainder when divided by n.*

Proof. Let the integer divisions of a and b by n be given by

$$a = q_1 n + r_1 \text{ and } b = q_2 n + r_2, \text{ where } 0 \leq r_1, r_2 < n. \tag{4.3}$$

Suppose now that $a \equiv b \pmod{n}$, i.e. that $n|a - b$. Therefore

$$n|(q_1 - q_2)n + (r_1 - r_2) \tag{4.4}$$

and so by theorem 2.1 (part 3) we get

$$n|r_1 - r_2. \tag{4.5}$$

But note that $-n < r_1 - r_2 < n$ and moreover 0 is the only multiple of n in this interval $(-n, n)$. Therefore

$$r_1 - r_2 = 0 \tag{4.6}$$

and so $r_1 = r_2$ as required.

Conversely, suppose now that $r_1 = r_2$ in the integer divisions of a and b by n. Then $a - b = (q_1 - q_2)n$ and so $n|a - b$ as required. □

Equivalence relations

The congruence relation enjoys a number of important properties, which all come from associated properties of the divisibility relation. Of fundamental importance is the fact that the congruence relation is an equivalence relation.

Definition 4.2 (Equivalence relation)**.** A relation $\sim$ on a set X is an equivalence relation if and only if it is reflexive, symmetric and transitive, i.e.

- (*reflexive*) $\forall x \in X \; x \sim x$,
- (*symmetric*) $\forall x, y \in X \; x \sim y \Rightarrow y \sim x$,
- (*transitive*) $\forall x, y, z \in X \quad [x \sim y \,\&\, y \sim z] \Rightarrow x \sim z$.

Definition 4.3 (Equivalence class)**.** The *equivalence class*, $[x]$, of an element x, is simply the set of all elements in X that are equivalent to x, i.e.

$$[x] = \{y \in X \, : \, x \sim y\}. \tag{4.7}$$

A related concept to an equivalence relation on a set X is a partition of a set X.

Definition 4.4 (Partition)**.** Let X be a non-empty set. A *partition* of X is a family, P, of subsets of X, with the following properties

- (P *covers* X)
$$\bigcup_{S \in P} S = X, \tag{4.8}$$
- (P *consists of disjoint sets*)
$$\forall S, T \in P, \quad S = T \text{ or } S \cap T = \emptyset. \tag{4.9}$$

Theorem 4.2 (Congruence is an equivalence)**.** *The congruence relation is an equivalence relation on $\mathbb{Z}$, i.e. it is reflexive, symmetric and transitive.*

Proof. Let n be a positive integer. Recall that $n|0$ and so for any $a \in \mathbb{Z}$ we have $n|a - a$, i.e. $a \equiv a \pmod{n}$, and so congruence is reflexive.

Suppose that $a \equiv b \pmod{n}$, i.e. $n|a-b$. But then by theorem 2.1 (part 3) we have $n|-(a-b)$, i.e. $n|b - a$. Therefore $b \equiv a \pmod{n}$, and so congruence is symmetric.

Suppose now that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, i.e. $n|a-b$ and $n|b-c$. Using the linear combination $a-c = (a-b)+(b-c)$ and theorem 2.1 (part 3) we get $n|a-c$, i.e. $a \equiv c \pmod{n}$, and so congruence is transitive. □

Since congruence is an equivalence relation, the equivalence classes of congruence modulo n form a partition of $\mathbb{Z}$. We use special terminology for these equivalence classes.

Definition 4.5 (Congruence class / reside class, residue)**.** When talking of the equivalence class of an integer a for the congruence relation modulo n we use the terms *congruence class* of a, or *residue class* of a and denote it by $[a]$.

When dealing with a congruence relation modulo n we often like to deal with a set of representatives of the congruence classes. It is usual practice to use the integers $0, 1, 2, \ldots, n-1$ to represent the n congruence classes modulo n. Such a set of representatives is called a complete set of *residues* modulo n. 1

Other important properties of the congruence relation are described in the following exercise problems. They can all be justified by arguing carefully from the definition of congruence and using relevant properties of divisibility.

Exercise 4.1. In the following let $a, b, a', b', c \in \mathbb{Z}$ with $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Prove that each of the following holds:

1. $a + b \equiv a' + b' \pmod{m}$,
2. $ab \equiv a'b' \pmod{m}$,
3. $\forall c \in \mathbb{Z}\ a + c \equiv a' + c \pmod{m}$,
4. $\forall c \in \mathbb{Z}\ ac \equiv a'c \pmod{m}$,
5. $\forall k \in \mathbb{Z}$ such that $k \geq 0,\ a^k \equiv (a')^k \pmod{m}$,
6. $f(a) \equiv f(a') \pmod{m}$, where f is any polynomial with integer coefficients.

Consider item 4 from the above exercises. We might ask ponder whether the converse of this is true, i.e. if $xc \equiv yc \pmod{m}$ can we conclude that $x \equiv y \pmod{m}$? It isn't obvious and we should be wary of jumping to the conclusion that yes we can. Note that there is no number (integer) $\frac{1}{c}$ around, with which we could multiply both sides of the congruence in order to *cancel* the c. Well the answer to this pondering is ... sometimes. Exactly how and when we may cancel factors from a congruence is given by the following result.

Theorem 4.3 (Cancelling factors in a congruence)**.** *If $xc \equiv yc \pmod{m}$ then $x \equiv y \pmod{\frac{m}{d}}$, where $d = \gcd(c, m)$. In particular, if $\gcd(c, m) = 1$ and $xc \equiv yc \pmod{m}$ then $x \equiv y \pmod{m}$.*

Proof. Assume that $xc \equiv yc \pmod{m}$ and that $d = \gcd(c, m)$. This means that $xc - yc = qm$ for some $q \in \mathbb{Z}$, i.e.

$$(x - y)c = qm, \text{ for some } q \in \mathbb{Z}. \tag{4.10}$$

We can factorise c and m as $c = c'd$ and $m = m'd$ for some $c', m' \in \mathbb{Z}$ where $\gcd(c', m') = 1$, (see the question 3 of Exercises 2.1). Using these factorizations to expand equation (4.10) we get

$$(x - y)c'd = qm'd \tag{4.11}$$

$$\Rightarrow (x - y)c' = qm'. \tag{4.12}$$

Note that $m' | (x - y)c'$. But since $\gcd(c', m') = 1$, by Euclid's lemma (question 6 Exercises 2.1), we have $m' | x - y$ which is equivalent to $x \equiv y \pmod{m'}$. This is our required result, since $m' = \frac{m}{d}$. □

Of course we can always cancel a factor from both sides of a congruence, as long as we can cancel it from the modulus as well, as described in the following result.

Theorem 4.4 (Cancelling a factor from all parts of a congruence)**.**

$$x \equiv y \ (mod\ m) \Leftrightarrow xc \equiv yc \ (mod\ mc). \tag{4.13}$$

Proof. In lectures. □

4.2 Dealing with large integers

The power of the congruence idea can been seen in how it can be used to solve problems relating to large integers. Just by exploiting the $a \equiv b \pmod{n}$ notation and some of the basic properties of congruence we can reach conclusions about the divisibility properties of large integers without having to explicitly evaluate the integers themselves.

Example 4.1 (Dealing with large integers)**.** Consider the following problems.

1. Show that $41|2^{20} - 1$.
2. What remainder is left upon dividing $\sum_{n=1}^{100} n!$ by 12?

Solution. In lecture. □

Exercise 4.2. The following exercises describe more properties of the congruence relation as well as other results about dealing with large integers.

1. Prove that if $a \equiv b \pmod{n}$ and $m|n$ then $a \equiv b \pmod{m}$.
2. Prove that if $a \equiv b \pmod{n}$ and $d|a$, $d|b$ and $d|n$ then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.
3. Find some counter-examples to the claim

$$\text{“}a^2 \equiv b^2 \pmod{n} \Rightarrow a \equiv b \pmod{n}\text{”}.$$

4. Prove that if $a \equiv b \pmod{n}$ then $\gcd(a, n) = \gcd(b, n)$.
5. What is the remainder left when 2012^{2012} is divided by 5?
6. What remainders are left when 2^{50} is divided by 7? When 41^{65} is divided by 7?
7. Prove that is a is odd then

$$\forall\, n \geq 1 \ a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

4.3 The modular arithmetic groups

Two of the items in Exercises 4.1 show that the operations of addition and multiplication preserve congruences. Let us consider them again. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then

$$a + b \equiv a' + b' \pmod{m} \text{ and } ab \equiv a'b' \pmod{m}. \tag{4.14}$$

These amount, more or less, to saying that addition and multiplication are well-defined operations on the congruence classes of the integers modulo m. For suppose that $[a]$ and $[b]$ are two congruence classes modulo n. We can define the sum and product of these *congruence classes* by the following:

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

But we ask ourselves: do these definitions make sense? Are they in fact defining genuine operations on the congruence classes? The problem might be that if we chose different representatives for the congruence classes $[a]$ and $[b]$ would we end up with the same sum and product of the congruence classes?

The properties of congruence in (4.14) above assure us that we will always get the same sum or product congruence class no matter which representatives of $[a]$ and $[b]$ we choose. So the operations of addition and multiplication on *congruence classes* are indeed well-defined.

Recall the definition of a group.

Definition 4.6 (Group, group axioms)**.** A *group* $(G, *)$ is a pair consisting of a non-empty set G together with a binary operation $*$ defined on G such that the following axioms hold,

1. (*Closure*) $\forall\, a, b \in G \quad a * b \in G$,
2. (*Associativity*) $\forall\, a, b, c \in G \quad a * (b * c) = (a * b) * c$,
3. (*Existence of identity*) $\exists\, e \in G\ \forall\, a \in G \quad e * a = a * e = a$,
4. (*Existence of inverses*) $\forall\, a \in G\ \exists\, a^{-1} \in G \quad a * a^{-1} = a^{-1} * a = e$.

Note that the group is the pair consisting of the set and the operation that together satisfy the four group axioms. This is an important point as there may be more than one operation that one can define on a given set G such that it forms a group with respect to that operation. However in practice we may relax this formalism and simply refer to 'the group G', as long as what the operation is is understood and no confusion will arise.

So we will investigate what groups we can form using the operations of addition and multiplication on the congruence classes modulo n.

The additive modular arithmetic group

Definition 4.7. ($\mathbb{Z}_n$) We write $\mathbb{Z}_n$ for the set of congruence classes modulo n. We normally use the integers $0, 1, 2, \ldots, n-1$ as a complete residue system, so that

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}\,. \tag{4.15}$$

Theorem 4.5 (Additive modular arithmetic group)**.** *The system* $(\mathbb{Z}_n, +)$ *forms a group.*

Proof. All four group axioms hold for $(\mathbb{Z}_n, +)$. Closure and associativity come from the associated properties of addition on the integers themselves. The identity element is $[0]$, for

$$[a] + [0] = [a + 0] = [a]. \tag{4.16}$$

The inverse of the element $[a]$ is $[-a] = [n - a]$, for

$$[a] + [-a] = [a + (-a)] = [0]. \tag{4.17}$$

□

The structure of these additive modular arithmetic groups is straightforward to describe. We can see that each group $(\mathbb{Z}_n, +)$ is cyclic. The element $[1]$ will be a generator, i.e.

$$\mathbb{Z}_n = \{[1], [1] + [1], [1] + [1] + [1], \ldots\}. \tag{4.18}$$

Recall that Cayley tables are a tool we can use for visualising the structure of a group.

$*$	$\cdots$	g_j	$\cdots$
$\vdots$			
g_i	$\cdots$	$g_i * g_j$	$\cdots$
$\vdots$			

Figure 4.1: A generic Cayley table

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figure 4.2: Cayley table for $(\mathbb{Z}_4, +)$

Definition 4.8 (Cayley table)**.** A *Cayley table* for a finite group $(G, *)$ is a two-dimensional table, whose rows and columns are indexed by the elements of G. The entries in the body of the table show the results of combining the row and column index elements with the operation $*$. See the generic Cayley table in figure 4.1. Take note of the convention regarding the ordering of the factors in the product $g_i * g_j$, the row index element is on the left and the column index element is on the right. It is important to have this convention and to stick to it as not all groups are Abelian.

Example 4.2. The table for the group $(\mathbb{Z}_4, +)$ is shown in figure 4.2.

When laid out in this way, the Cayley tables of the groups $(\mathbb{Z}_n, +)$ all have the same structure — each row is a shift one place to the right of the row above it.

The multiplicative modular arithmetic group

Consider whether we can form a group out of $\mathbb{Z}_n$ and the operation $\times$. The closure, associativity and identity axioms all hold here. Closure and associativity follow from the corresponding properties of $\times$ on $\mathbb{Z}$ and the identity element is clearly [1]. However the existence of inverses axiom is not so clear. The question is: given a congruence class $[a]$ modulo n, is there a congruence class $[b]$ such that

$$[a][b] = [1], \tag{4.19}$$

or in other words

$$ab \equiv 1 \pmod{n}? \tag{4.20}$$

Now we might naturally begin thinking of the quantity $\frac{1}{a}$. But this will not be an integer (unless $a = \pm 1$) and so cannot help us here. A clue to the solution of this quandary is given by the following observations

$$\begin{aligned} \exists b \in \mathbb{Z}\ ab \equiv 1 \pmod{n} &\Leftrightarrow \exists b \in \mathbb{Z}\ n|(ab-1) && (4.21)\\ &\Leftrightarrow \exists b \in \mathbb{Z}\ \exists q \in \mathbb{Z}\ ab - 1 = qn, && (4.22)\\ &\Leftrightarrow \exists b \in \mathbb{Z}\ \exists q \in \mathbb{Z}\ 1 = ab - qn, && (4.23)\\ &\Leftrightarrow \gcd(a, n) = 1, && (4.24) \end{aligned}$$

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Figure 4.3: Cayley table for $(\mathbb{Z}_5^\times, \times)$

this last step being justified by question 2 of Exercises 2.1. These observations form a proof of the following theorem

Theorem 4.6. *The congruence class* $[a]$ *modulo* n *has an inverse with respect to* $\times$ *if and only if* $\gcd(a, n) = 1$.

Proof. Given above. □

These observations also give us a way of actually finding a representative for the multiplicative inverse of a congruence class $[a]$ modulo n. We should apply the Euclidean algorithm to the pair (a, n) to find their gcd. Having confirmed that this is indeed 1, we can obtain from the algorithm a linear combination of a and n that is equal to 1. The coefficient, x, of a in this linear combination will be a representative of the multiplicative inverse of $[a]$, i.e. if $xa + yn = 1$ then $[a]^{-1} = [x]$. Choosing the least positive element in $[x]$ will give us the standard representative (residue) of $[a]^{-1}$. An alternative method for obtaining a representative of $[a]^{-1}$ making use of Euler's ϕ function shall be described later.

Exercise 4.3. Using the Euclidean algorithm described above (or other methods/observations), practice finding multiplicative inverses modulo a modulus n.

So in order to have a multiplicative group of congruence classes modulo n we need to discard those congruence classes of integers that are not coprime to n.

Definition 4.9 (Reduced residue system)**.** A *reduced residue system* modulo n is the set $\mathbb{Z}_n^\times$ defined by

$$\mathbb{Z}_n^\times = \{[a] \,:\, \gcd(a, n) = 1\}. \tag{4.25}$$

The above discussion has established the following result.

Theorem 4.7 (Multiplicative modular arithmetic group)**.** *The system* $(\mathbb{Z}_n^\times, \times)$ *forms a group.*

Proof. Given above. □

Again we can investigate the structure using Cayley tables.

Example 4.3. The table for the group $(\mathbb{Z}_5^\times, \times)$ is shown in figure 4.3.

Example 4.4. The table for the group $(\mathbb{Z}_8^\times, \times)$ is shown in figure 4.4.

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Figure 4.4: Cayley table for $(\mathbb{Z}_8^\times, \times)$

4.4 The Euler totient function

Recall that the order of a group refers to the number of elements in the group.

Definition 4.10 (Euler totient function)**.** The *Euler totient function*, ϕ, is the function that gives the order of the multiplicative modular arithmetic groups, i.e. $\phi(n)$ is the order of $\mathbb{Z}_n^\times$. Expanding this definition says that $\phi(n)$ is the number of integers a such that $1 \leq a \leq n$ and $\gcd(a, n) = 1$.

In the next chapter we shall investigate Euler's ϕ function further. For now we should familiarise ourselves with these groups with the aid of the following exercise.

Exercise 4.4. For a range of reasonably small moduli m, construct Cayley tables for the group $(\mathbb{Z}_m^\times, \times)$ and investigate the subgroups that they possess.

Chapter 5

Euler's totient function

At the end of the last chapter we introduced Euler's totient function ϕ. In this chapter we prove some of its basic properties and in particular establish a product formula for evaluating $\phi(n)$ based on the prime factorisation of n.

❦

Definition. The *Euler totient function*, ϕ, is the function that gives the order of the multiplicative modular arithmetic groups, i.e. $\phi(n)$ is the order of $\mathbb{Z}_n^\times$. Expanding this definition says that $\phi(n)$ is the number of integers a such that $1 \leq a \leq n$ and $\gcd(a, n) = 1$.

We now turn to the problem of actually evaluating the values, $\phi(n)$, of this function. We could proceed from the definition and simply go through all the numbers less than n and test each one to see if it is coprime to n, and if it is, count it! While this is faithful to the definition, it quickly becomes impractical for large n and it feels a little naive. We will establish here a formula for $\phi(n)$ that is based on the prime factorization (canonical form) of n.

Theorem 5.1 (Euler totient function formula)**.** *Let $n = \prod_{i=1}^{r} p_i^{a_i}$ be the canonical form of the integer n. Then*

$$\phi(n) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1). \tag{5.1}$$

Sketch of proof. The argument is long and to make the presentation easier we have split it up between a number of lemmas. The overall argument will be as follows. We shall prove firstly that the value of ϕ on a prime power (lemma 5.2) is

$$\phi\left(p^a\right) = p^{a-1}(p - 1). \tag{5.2}$$

Then we shall prove that ϕ is *multiplicative* (lemma 5.5), i.e. that

$$\gcd(a, b) = 1 \Rightarrow \phi(ab) = \phi(a)\phi(b). \tag{5.3}$$

Then the argument proceeds by induction on the number of distinct primes in the canonical form of n. Lemma 5.2 proves the base case, i.e. when n has just one distinct prime factor. Assuming that the theorem holds when the integer n has k distinct factors we consider an integer m given by the canonical form (with $k + 1$ distinct prime factors)

$$m = \prod_{i=1}^{k+1} p_i^{a_i}. \tag{5.4}$$

We split one of the prime-power factors, say the last, apart from the rest of the factors, i.e.

$$m = \left(\prod_{i=1}^{k} p_i^{a_i} \right) p_{k+1}^{a_{k+1}}. \tag{5.5}$$

Now since the primes p_i are all distinct we can apply lemma 5.5 to get

$$\phi(m) = \phi\left(\prod_{i=1}^{k} p_i^{a_i} \right) \phi\left(p_{k+1}^{a_{k+1}} \right), \tag{5.6}$$

$$= \left(\prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) \right) p_{k+1}^{a_{k+1}-1} \left(p_{k+1} - 1 \right), \tag{5.7}$$

where the last line follows from applying the induction hypothesis made above and lemma 5.2. Therefore the theorem holds when the integer m has $k+1$ distinct prime factors. So by the principle of induction the theorem is true for integers with any number of distinct prime factors, i.e. it is true for all n. □

This proof will be valid once we have established the necessary lemmas that it relies upon. We now establish the value of the Euler totient function at a prime-power.

Lemma 5.2. *If p is a prime and a an integer such that $a \geq 1$ then*

$$\phi\left(p^a\right) = p^{a-1}(p-1). \tag{5.8}$$

Proof. Consider the relevant range of integers

$$1, 2, 3, \ldots, p^a - 1, p^a. \tag{5.9}$$

The value $\phi\left(p^a\right)$ is the number of integers in this range that are coprime to p^a. We will identify how many in the range are *not* coprime to p^a. For any integer z, z is not coprime to p^a if z has a factor of p, i.e. if z is a multiple of p. So how many multiples of p are there in this range of integers. The multiples of p here are

$$p, 2p, 3p, \ldots, p^{a-1}p. \tag{5.10}$$

There are p^{a-1} integers so that are not coprime to p^a. Therefore the required value of the Euler totient function is

$$\phi\left(p^a\right) = p^a - p^{a-1} = p^{a-1}(p-1), \tag{5.11}$$

as claimed. □

We approach the proof that ϕ is multiplicative. We begin with some preparatory lemmas. The first of these is actually question 4 from Exercises 4.2. We repeat it here for convenience.

Lemma 5.3. *If $a \equiv b \pmod{n}$ then $\gcd(a, n) = \gcd(b, n)$.*

Next we have a lemma concerning gcds and products.

Lemma 5.4. *For all integers u, v, w we have*

$$\gcd(u, vw) = 1 \Leftrightarrow \left[\gcd(u, v) = 1 \,\&\, \gcd(u, w) = 1 \right]. \tag{5.12}$$

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & b-1 & b \\ b+1 & b+2 & b+3 & \cdots & 2b-1 & 2b \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ (a-1)b+1 & (a-1)b+2 & (a-1)b+3 & \cdots & ab-1 & ab \end{array}$$

Figure 5.1: The $a \times b$ array of the integers in $[1, ab]$

Proof. One direction of this equivalence, namely,

$$\gcd(u, vw) = 1 \Leftarrow [\gcd(u, v) = 1 \,\&\, \gcd(u, w) = 1], \tag{5.13}$$

is just a restatement of question 10 (a) from Exercises 2.3. The other direction

$$\gcd(u, vw) = 1 \Rightarrow [\gcd(u, v) = 1 \,\&\, \gcd(u, w) = 1], \tag{5.14}$$

can be established as follows. Suppose that $\gcd(u, vw) = 1$, then by question 2, Exercises 2.1, there exists a linear combination of u and vw equal to 1, say

$$\alpha u + \beta vw = 1. \tag{5.15}$$

But the linear combination in equation (5.15) can equally well be considered as a linear combination of u and v equal to 1, and as a linear combination of u and w equal to 1. So applying question 2, Exercises 2.1 again we see that $\gcd(u, v) = \gcd(u, w) = 1$. □

Now finally we can prove that ϕ is multiplicative, which will complete the proof of theorem 5.1.

Lemma 5.5. *The Euler totient function ϕ is multiplicative, i.e. if $\gcd(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.*

Proof. We shall establish this result directly – evaluating the left-hand side by counting the number of integers in the range $[1, ab]$ that are co-prime to ab, but doing so in such a way that shows this number is equal to the product $\phi(a)\phi(b)$. We consider the integers $1, 2, 3, \ldots, ab-1, ab$ laid out in the $a \times b$ array as shown in figure 5.1.

So our task now is to consider the integers in this array and count how many of them are coprime to ab. Applying lemma 5.4 this is equivalent to counting how many of the integers in this array are coprime to both a and b.

This array consists of b columns. Notice that all the integers in a given column are all congruent to each other modulo b, since any two integers in the same column differ by a multiple of b. These columns are indexed by their first entries $r = 1, \ldots, b$. Note that by lemma 5.3, r is coprime to b if and only if every other integer of the form $qb + r$ (i.e. all those in the same column as r) are coprime to b. Therefore, of the b columns, $\phi(b)$ of them consist of integers all of whom are coprime to b, and all the integers in the array that are coprime to b are contained in these $\phi(b)$ columns.

Our task now becomes to decide how many integers in these 'coprime' columns are coprime to a. Consider any column from the array, say the one headed by the integer r. This column contains the a integers

$$r, b + r, 2b + r, \ldots (a-1)b + r. \tag{5.16}$$

We claim that these a integers are all incongruent to each other modulo a. For suppose that two were not, i.e. suppose that $vb + r \equiv wb + r \pmod{a}$. Therefore $a|(v - w)b$ and hence $a|v - w$, since a and b are coprime (Euclid's Lemma, Question 6, Exercises 2.1). But this is a contradiction unless $v = w$, since v and w are both positive integers less than a and so the only way a can divide their difference is if their difference is zero! So now we know that all the a integers in this column are incongruent modulo a, i.e. they represent each and every one of the a congruence classes modulo a. These congruence classes are the congruence classes of the integers $0, 1, 2, 3, \ldots, a - 1$. Now there are $\phi(a)$ of these integers that are coprime to a. Therefore, by lemma 5.3, there are $\phi(a)$ integers in the array column headed by r that are coprime to a.

We have now established the required result in the lemma. Let us summarize. We set out the array in figure 5.1 and tasked ourselves with counting how many of the integers in this array were coprime to both a and b. We argued that all the integers coprime to b in the array were contained in just $\phi(b)$ of the columns, and every integer in these $\phi(b)$ columns was coprime to b. Then we argued that in any given column, there were $\phi(a)$ integers coprime to a. So this means that in total, there are $\phi(b)\phi(a)$ integers in the array that are coprime to both a and b, as required. □

5.1 Some properties of the totient function

Example 5.1. The following examples show some ways of reasoning out properties of ϕ.

1. Prove that $\phi(n) = \phi(2n)$ if and only if n is odd.
2. Find all integers such that $\phi(n) = 12$.

5.2 Euler's theorem

Recall Lagrange's theorem concerning finite groups which we encountered Mathematics Fundamentals. Note that the order of a group refers simply to the number of elements in the group.

Theorem 5.6 (Lagrange)**.** *If G is a finite group and H is a subgroup of G then the order of H divides the order of G.*

Corollary. *If G is a finite group of order n and $a \in G$ then $a^n = e$, where e is the identity element.*

Proof. This follows from considering $\langle a \rangle$, the cyclic subgroup of G generated by a, where

$$\langle a \rangle = \{a^m \, : \, m \in \mathbb{Z}\}. \tag{5.17}$$

Since G is finite, so will $\langle a \rangle$ be. The order of $\langle a \rangle$ is the smallest integer $r \geq 1$ such that $a^r = e$. By Lagrange's theorem $r|n$, i.e. $n = qr$ so that

$$a^n = a^{qr} = (a^r)^q = e^q = e. \tag{5.18}$$

□

Applying this to our present context gives us the following important result in number theory.

Theorem 5.7 (Euler)**.** *Let n be a positive integer and suppose that* $\gcd(a, n) = 1$*, then*

$$a^{\phi(n)} \equiv 1 \ \textit{(mod } n\textit{)}. \tag{5.19}$$

Proof. This is simply the corollary to Lagrange's theorem applied to the group $\mathbb{Z}_n^\times$. □

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

$$a^{p-1} \equiv 1 \pmod{p} \tag{5.20}$$

Both Euler's theorem and Fermat's Little theorem can be proved without the aid of group theory by carefully arguing about the relevant congruence classes and using properties of divisibility. However since we have the concept of groups at our disposal it makes sense to exploit the powerful general principle of Lagrange's theorem.

Exercise 5.1. These exercises will help you to become familiar with ϕ and working with its product formula.

1. Become confident in using the product formula of theorem 5.1 – for instance, evaluate the first 30 values, $\phi(1), \phi(2), \ldots, \phi(30)$.
2. What is $\phi(p)$, where p is a prime?
3. Show that $\phi(n) = \frac{n}{2}$ if and only if $n = 2^k$ for some $k \geq 1$. To do this, write n in the form $n = 2^k m$, where $2 \nmid m$, and then show that $\phi(n) = \frac{n}{2}$ implies that $m = 1$.
4. In the group $\mathbb{Z}_{15}^\times$, simplify the product $a^{24}b^{15}$.
5. In the group $\mathbb{Z}_{42}^\times$, simplify the product $a^{25}b^{23}$
6. Find the units digit of 3^{100}.

Chapter 6

Polynomial congruences I: linear congruences and the Chinese Remainder Theorem

Polynomials have been studied extensively in mathematics, indeed it was the search for simple formulae to solve polynomials that led Galois to lay the foundations of group theory and abstract algebra.

Question 6 of Exercises 4.1 established that if f is a polynomial with integer coefficients and $x \equiv y \pmod{n}$ then

$$f(x) \equiv f(y) \pmod{n}. \tag{6.1}$$

This result shows that polynomials with integer coefficients *fit well* with congruences. They take congruent arguments to congruent values. Throughout this chapter (in fact probably throughout this unit) we only consider polynomials with integer coefficients, so for brevity's sake we will understand the term **polynomial** to refer one with **integer coefficients** unless explicitly stated otherwise.

In this and the following chapter we will develop the theory needed to find solutions (if they exist) of a polynomial congruence. We will follow the approach given by Apostol (1976)[1].

❦

Definition 6.1 (Polynomial congruence)**.** A *polynomial congruence* is a congruence of the form

$$f(x) \equiv 0 \pmod{m}, \tag{6.2}$$

where f is a polynomial.

Comparison with polynomial equations

Recall the Fundamental Theorem of Algebra which asserts if f is a polynomial (with real coefficients) of degree n then f has n complex roots (when counted with multiplicities). Might such a situation hold for polynomial congruences? A little investigation throws some light on this.

[1] Apostol, T. M. (1976) *Introduction to analytic number theory.* New York: Springer-Verlag.

Some initial investigations

Firstly, since our main focus is the integers we will seek only integer solutions for (6.2). Secondly, question 6 from Exercises 4.1 shows that if any solution exists at all for (6.2) then it will have an infinite number of integer solutions, since we can take any other integer congruent to the first one, and this will also be a solution. So the appropriate objects to search for are the *congruence classes* of solutions to (6.2), i.e. we will regard two integer solutions of (6.2) as being essentially the same if they belong to the same congruence class modulo m.

So might we hope that a polynomial congruence of degree n would have n solutions? Considering some simple examples shows that we cannot expect any simple results like this to hold true in general.

Example 6.1. Solve the linear congruence

$$2x \equiv 3 \pmod 4. \tag{6.3}$$

Solution. This has no solutions at all. The integer $2x - 3$ is odd for every x, and so can not be divisible by 4. □

Example 6.2. Solve the congruence

$$x^2 - 1 \equiv 0 \pmod 8. \tag{6.4}$$

Solution. Considering each of the eight congruence classes modulo 8 we see that this has four solutions, given by $x \equiv 1,\ 3,\ 5,\ 7 \pmod 8$. □

So sometimes congruences have no solutions, and sometimes there are more solutions than the degree of the polynomial. It looks like this problem will require careful detailed study to describe the general behaviour. We will start by examining polynomial congruences of degree 1 and giving a complete description of the solutions of these. The general problem of polynomial congruences of any degree and with respect to any modulus, shall be studied in the next chapter. The approach is based on the canonical form, $n = \prod_i p_i^{\alpha_i}$, of the modulus and makes use of the other main result of this chapter, the Chinese Remainder Theorem.

6.1 Linear congruences

Definition 6.2. A *linear congruence* is a polynomial congruence where the polynomial has degree 1, i.e. something of the form

$$ax \equiv b \pmod n. \tag{6.5}$$

The solution(s) of a linear congruence can be completely described in terms of a, b and n as the following results show.

Theorem 6.1. *If* $\gcd(a, n) = 1$ *then the linear congruence*

$$ax \equiv b \ \textit{(mod } n\textit{)} \tag{6.6}$$

has a unique solution, which is given by

$$x \equiv a^{\phi(n)-1}b \ \textit{(mod } n\textit{)}. \tag{6.7}$$

Proof. Assume that $\gcd(a, n) = 1$. Then a has a multiplicative inverse modulo n, by theorem 4.6. By remarks following Euler's theorem (theorem 5.7) $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$. So multiplying both sides of $ax \equiv b \pmod{n}$ by $a^{\phi(n)-1}$ we get the required result, namely $x \equiv a^{\phi(n)-1}b \pmod{n}$. □

But what if $\gcd(a, n) \neq 1$, do solutions exist then?

Theorem 6.2. *If* $\gcd(a, n) = d$ *then the linear congruence*

$$ax \equiv b \pmod{n} \tag{6.8}$$

has a solution if and only if $d|b$.

Proof. We prove both directions of the equivalence separately. Assume that $ax \equiv b \pmod{n}$, i.e. $n|(ax - b)$. This in turn means that there exists $q \in \mathbb{Z}$ such that

$$ax - b = qn, \tag{6.9}$$

which reorganises to

$$b = ax - qn. \tag{6.10}$$

This last equation shows b to be a linear combination of a and n. Therefore any common divisor of a and n will also divide b. So in particular $d|b$. This proves the 'only if' direction of the equivalence.

To prove the 'if' direction, assume that $d|b$, i.e. $b = b'd$ for some $b' \in \mathbb{Z}$. Now we know from the Euclidean algorithm (or theorem 2.3) that there exists $r, s \in \mathbb{Z}$ such that

$$d = ar + ns. \tag{6.11}$$

Multiplying both sides by b' gives

$$b = b'd = a(rb') + n(sb'), \tag{6.12}$$

which reorganises to

$$a(rb') - b = n(-sb'), \tag{6.13}$$

or in other words, $n|a(rb') - b$, which in turn means that $a(rb') \equiv b \pmod{n}$. So a solution to the original congruence exists and is given by $x \equiv rb' \pmod{n}$. □

Notice that theorem 6.2 does not imply that the solution of the original congruence is unique (for there are many choices for the coefficients r, s in the linear combination for d). This point is resolved by the following result.

Theorem 6.3. *Suppose that* $\gcd(a, n) = d$ *and* $d|b$. *Then the linear congruence*

$$ax \equiv b \pmod{n}, \tag{6.14}$$

has exactly d *solutions modulo* n. *These are the congruence classes, modulo* n, *of*

$$t + i\frac{n}{d}, \quad \big(i = 0, 1, 2, \ldots, (d-1)\big), \tag{6.15}$$

where t *is the unique solution (modulo* $\frac{n}{d}$*) of the congruence*

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}. \tag{6.16}$$

Proof. By theorem 4.4 the congruences

$$ax \equiv b \pmod{n} \text{ and } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}} \tag{6.17}$$

have exactly the same (integer) solutions. Now the integers referred to in 6.15 are all solutions of $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, and hence of $ax \equiv b \pmod{n}$ also.

These solutions are all incongruent modulo n. For suppose that this was not the case, then we would have

$$t + r\frac{n}{d} \equiv t + s\frac{n}{d} \pmod{n}, \tag{6.18}$$

for some $0 \leq r, s \leq d-1$. Cancelling the t from both sides gives

$$r\frac{n}{d} \equiv s\frac{n}{d} \pmod{n}, \tag{6.19}$$

and applying theorem 4.3 to this allows us to cancel the $\frac{n}{d}$ to produce the congruence

$$r \equiv s \pmod{d}. \tag{6.20}$$

But since $0 \leq r, s \leq d-1$, the difference $|r-s|$ must also satisfy $0 \leq |r-s| \leq d-1$, and so the only way it can be divisible by d is if $r - s = 0$, i.e. $r = s$. This shows that the solutions in equation 6.15 are distinct modulo n.

The final part of the proof is to show that the solutions in equation 6.15 are *all* of the solutions of the original congruence $ax \equiv b \pmod{n}$. Suppose that s is any solution of $ax \equiv b \pmod{n}$. Then $at \equiv as \pmod{n}$, since they are both congruent to b modulo n. Then cancelling the a from this (using theorem 4.3), we get

$$t \equiv y \pmod{\frac{n}{d}}. \tag{6.21}$$

This means that $\frac{n}{d} | t - y$, or equivalently,

$$y = t + q\frac{n}{d}, \tag{6.22}$$

for some $q \in \mathbb{Z}$. But of course, $q \equiv i \pmod{d}$ for some $0 \leq i \leq d-1$ and so

$$q\frac{n}{d} \equiv i\frac{n}{d} \pmod{n}, \tag{6.23}$$

(where this last congruence follows by applying theorem 4.3 to $q \equiv i \pmod{d}$). Putting congruence 6.23 together with equation 6.22, give us

$$y \equiv t + i\frac{n}{d} \pmod{d}, \tag{6.24}$$

which says exactly that the solution y is one that has already been identified in 6.15 above. This completes the proof. □

Example 6.3. Solve the linear congruences

1. $5x \equiv 3 \pmod{24}$,
2. $25x \equiv 15 \pmod{120}$.

Exercise 6.1. Here are some more linear congruences for you to solve.

1. $18x \equiv 30 \pmod{42}$
2. $9x \equiv 21 \pmod{30}$
3. $25x \equiv 15 \pmod{29}$
4. $5x \equiv 2 \pmod{26}$
5. $6x \equiv 15 \pmod{21}$
6. $36x \equiv 8 \pmod{102}$
7. $34x \equiv 60 \pmod{98}$
8. $140x \equiv 133 \pmod{301}$
9. $25x \equiv 15 \pmod{125}$

6.2 Chinese Remainder Theorem

The previous section has described completely the techniques needed to solve any linear congruence (or to decide if it has no solutions). Before moving to the case of polynomials of degree higher than 1 we shall have a look at the Chinese Remainder Theorem – a tool for solving simultaneous congruences.

This theorem is so named because examples of the type of problem to which it can be applied occur in early Chinese literature (first century AD). The writer Sun-Tsu posed the problem

> Find a number which leaves the remainders 2, 3 and 2 when divided by 3, 5, and 7 respectively.

Theorem 6.4 (Chinese Remainder Theorem)**.** *Assume that the moduli $m_1, \ldots, m_k$ are pairwise coprime, i.e. if $r \neq s$ then* $\gcd(m_r, m_s) = 1$*. Then the system of congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned} \tag{6.25}$$

has a unique solution modulo the product $m_1 m_2 \ldots m_k$.

Proof. We will form the simultaneous solution x as a sum of various products of the moduli and the b_i.

We let M denote the product of the moduli, i.e. $M = m_1 m_2 \ldots m_k$. For each each $i = 1, \ldots, k$ we let $M_i = \frac{M}{m_i}$. Note that as a consequence of this definition, $M_i \equiv 0 \pmod{m_j}$ for any $i \neq j$. Also, $\gcd(M_i, m_i) = 1$ and so for each $i = 0, \ldots, k$, the integer M_i has a multiplicative inverse modulo m_i, we denote this by M_i', i.e.

$$M_i' M_i \equiv 1 \pmod{m_i}. \tag{6.26}$$

The simultaneous solution x is formed as follows,

$$x = \sum_{i=1}^{k} b_i M_i M_i' = b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots + b_k M_k M_k'. \tag{6.27}$$

Consider the congruence class of this x modulo one of the m_i. Since $M_i \equiv 0 \pmod{m_j}$ for any $i \neq j$, this reduces to

$$x \equiv b_i M_i M_i' \pmod{m_i}, \tag{6.28}$$

but M_i' is the inverse of M_i modulo m_i, so this gives us

$$x \equiv b_i \pmod{m_i}. \tag{6.29}$$

So now we know that x is a simultaneous solutions of the congruences in 6.25.

What remains to be shown is that the solution in 6.27 is unique modulo M. Suppose that y is any other simultaneous solution of 6.25. Then $x \equiv y \pmod{m_i}$ for each $i = 1, \ldots, k$, i.e. $m_i | x - y$. But the m_i are all pairwise-coprime so this implies that $M | x - y$ (this is proved in Question 5 of Exercises 2.1), i.e. $x \equiv y \pmod{M}$. □

The earlier problem of Sun-Tsu is equivalent to the first of the following examples

Example 6.4. Solve the following systems of simultaneous linear congruences in

1.

$$x \equiv 2 \pmod{3} \tag{6.30}$$
$$x \equiv 3 \pmod{5} \tag{6.31}$$
$$x \equiv 2 \pmod{7}. \tag{6.32}$$

2.

$$x \equiv 0 \pmod{3} \tag{6.33}$$
$$x \equiv 1 \pmod{4} \tag{6.34}$$
$$x \equiv 10 \pmod{23}. \tag{6.35}$$

Exercise 6.2. Use the method of the Chinese Remainder Theorem to solve the systems in questions 1 – 3.

1. $x \equiv 1 \pmod{3}$, $x \equiv 4 \pmod{5}$, $x \equiv 3 \pmod{7}$.
2. $x \equiv 5 \pmod{13}$, $x \equiv 11 \pmod{23}$, $x \equiv 15 \pmod{31}$.
3. $x \equiv 5 \pmod{6}$, $x \equiv 7 \pmod{11}$, $x \equiv 3 \pmod{5}$.
4. *A problem of Brahmagupta, India, 7th century AD.* There is a basket of eggs. If the eggs are removed 2 at a time there remains 1 egg in the basket. If they are removed 3 at a time there remains 2 eggs in the basket. If removed by 4 there remains 3. If removed by 5 there remains 4. If removed by 6 there remains 5. But if the eggs are removed 7 at a time there remain no eggs in the basket.

   What is the smallest number of eggs that could be in the basket?
5. The Chinese Remainder Theorem applies to systems where the moduli are pairwise-coprime. But there can still be simultaneous solutions when this is not so. Prove the following result:

   > A simultaneous solution x exists for $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ iff $d | a - b$, where $d = \gcd(n, m)$. In addition, show that this solution is unique modulo $\operatorname{lcm}(n, m)$.

Chapter 7

Polynomial congruences II

In this chapter we continue from the last chapter and build to the general case of polynomial congruences, i.e. polynomials of any degree and modulo any modulus n.

7.1 Polynomial congruences modulo a prime

Recall that in the previous chapter we looked at a quadratic congruence (Example 6.2) $x^2 - 1 \equiv 0 \pmod 8$, which had *four* solutions. We also looked at a linear congruence in example 6.1 which had *no* solutions at all. These examples, and others like them, show that there is no relationship in general between the degree of the congruence and the number of solutions it possesses. This stands in contrast to the situation of polynomial *equations* where we have the Fundamental Theorem of Algebra.

However for polynomial congruences modulo a prime p, we do have a result similar in some senses to the Fundamental Theorem of Algebra.

Theorem 7.1 (Lagrange)**.** *Let f be a polynomial of degree n, say*

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad (a_i \in \mathbb{Z}). \tag{7.1}$$

If $a_n \not\equiv 0 \pmod p$ (i.e. $p \nmid a_n$) then the polynomial congruence

$$f(x) \equiv 0 \pmod p \tag{7.2}$$

has at most n solutions.

Proof. *This proof is a particularly nice example of the use of induction together with proof by contradiction. It appears long, though I have gone to some lengths to give a detailed description of the argument.*

This result is proved by induction of the degree n of the congruence. When $n = 1$ we are considering a linear congruence, one of the form

$$a_1 x + a_0 \equiv 0 \pmod p,$$

where $a_1 \not\equiv 0 \pmod p$, i.e. $p \nmid a_1$. So $\gcd(a_1, p) = 1$ and so there exists a unique solution, by theorem 6.1. This solution is given by

$$x \equiv -a_1' a_0 \pmod p,$$

where a_1' is the multiplicative inverse of a_1 modulo p. So our polynomial congruence of degree 1 has one solution and so the result holds true for $n = 1$.

Now we assume that the result holds true for some value $n = k \geq 1$. So we are assuming that every polynomial congruence of degree k,

$$f(x) = \sum_{i=0}^{k} a_i x^i \equiv 0 \pmod{p},$$

where $a_k \not\equiv 0 \pmod{p}$, has at most k solutions (modulo p).

To prove the induction step we have to prove that the same thing holds true for polynomial congruences of degree $k + 1$. We shall achieve this using the proof by contradiction technique. So we shall suppose that we have a congruence of degree $k + 1$ that has $k + 2$ distinct solutions modulo p. What we will do is show that this supposition contradicts the induction hypothesis that is in force at the moment. In this way we will have achieved the induction step, i.e. showed that if the result holds true for $n = k$ then it must hold true for $n = k + 1$.

So we suppose that we have a congruence

$$g(x) = \sum_{i=0}^{k+1} b_i x^i \equiv 0 \pmod{p},$$

where $b_{k+1} \not\equiv 0 \pmod{p}$, which has $k + 2$ distinct solutions modulo p denoted by

$$x \equiv x_0, x_1, \ldots, x_{k+1} \pmod{p}. \tag{7.3}$$

In order to reach a contradiction we will need to construct a related polynomial congruence of degree k which also has *too many* solutions, thus contradicting the induction hypothesis. This related polynomial is constructed in turn from the polynomial G which we get subtracting a particular constant from g as follows,

$$G(x) = g(x) - g(x_0) = \sum_{i=1}^{k+1} b_i \left(x^i - x_0^i\right).$$

(Note that the $i = 0$ term has been omitted from the summation as it is equal to zero.) Next we observe that $x = x_0$ is a solution of the polynomial equation $G(x) = 0$ and so $(x - x_0)$ must be a factor of $G(x)$. So there must exist a polynomial $h(x)$ with integer coefficients satisfying

$$G(x) = g(x) - g(x_0) = (x - x_0)h(x).$$

We now make some additional observations about this new polynomial $h(x)$. It has degree k and has leading coefficient b_{k+1} (which remember satisfies $b_{k+1} \not\equiv 0 \pmod{p}$).

Note also that for any $j = 1, 2, \ldots, k + 1$,

$$G(x_j) = g(x_j) - g(x_0) = (x_j - x_0)h(x_j) \equiv 0 \pmod{p}, \tag{7.4}$$

where the final congruence relation holds true since $g(x_j)$ and $g(x_0)$ are both congruent to 0 modulo p (from above). But the solutions $x_0, x_1, \ldots, x_{k+1}$ introduced in (7.3) above are incongruent modulo p, or in other words for $j = 1, 2, \ldots, k + 1$,

$$p \nmid (x_j - x_0).$$

This, together with the congruence at the end of (7.4) implies that for $j = 1, 2, \ldots, k+1$ we have $h(x_j) \equiv 0 \pmod{p}$. We have finally reached the contradiction we said we would. To summarize, we have constructed a polynomial congruence

$$h(x) \equiv 0 \pmod{p},$$

of degree k whose leading coefficient is not divisible by p and which has $k+1$ distinct solutions modulo p. This contradicts the induction assumption we made earlier. Where did this polynomial $h(x)$ come from? It came from the polynomial $g(x)$. So we can conclude now that no such polynomial $g(x)$ can exist, or in other words, the result of the theorem holds true for $n = k+1$.

Thus we have proved the induction step. So by the principle of mathematical induction we can conclude that the result in the theorem holds true for all $n \geq 1$, i.e. it holds true for all polynomial congruences satisfying the given conditions. □

Corollary. *Let f be a polynomial of degree n, say*

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad (a_i \in \mathbb{Z}). \tag{7.5}$$

If f has more than n solutions (modulo p) then every coefficient of f is divisible by p, i.e.

$$a_i \equiv 0 \pmod{p}, \tag{7.6}$$

for each $i = 0, \ldots, n$.

Proof. This is a proof by contradiction. Suppose on the contrary that there is some coefficient that is not divisible by p. Let a_N be the one with largest index. So we have $N \leq n$ and the congruence

$$\sum_{i=0}^{N} a_i x^i \equiv 0 \pmod{p}$$

has leading coefficient not divisible by p but has more than N solutions. This contradicts Lagrange's theorem 7.1. So we conclude that all the coefficients of $f(x)$ are divisible by p as required. □

In general finding solutions to polynomial congruences modulo p requires a combination of approaches. One can attempt to factorise the original polynomial (into polynomial factors with *integer* coefficients), apply techniques likes *completing the square*, testing each congruence class in turn, ... But at least Lagrange's theorem 7.1 gives an upper bound on the number of solutions, which will serve as something of a guide in solving any particular polynomial congruence.

7.2 Polynomial congruences modulo a prime power

We now turn to the task of finding the solutions to a polynomial congruence where the modulus is a prime power, i.e.

$$f(x) \equiv 0 \pmod{p^a}. \tag{7.7}$$

This will involve a procedure for *lifting* any given solution of the congruence $f(x) \equiv 0 \pmod{p^{k-1}}$, to a solution(s) of the congruence $f(x) \equiv 0 \pmod{p^k}$. Applying this procedure repeatedly will allow us to *lift* solutions of $f(x) \equiv 0 \pmod{p}$ all the way up to solutions of $f(x) \equiv 0 \pmod{p^a}$.

In the theorem below the notation $f'(x)$ denotes the derivative of the polynomial $f(x)$.

Theorem 7.2 (Congruences with prime-power moduli)**.** *Consider the polynomial congruence*

$$f(x) \equiv 0 \pmod{p^{a-1}}. \tag{7.8}$$

Suppose this has a solution r, i.e. $f(r) \equiv 0 \pmod{p^{a-1}}$, with $0 \leq r < p^{a-1}$.

- *If $f'(r) \not\equiv 0 \pmod{p}$ then r can be lifted to a solution s, unique modulo p^a, of the congruence*

$$f(x) \equiv 0 \pmod{p^a}, \tag{7.9}$$

  such that $s \equiv r \pmod{p^{a-1}}$. In this case the new solution is given by

$$s = r + tp^{a-1}, \tag{7.10}$$

  where t is the (unique) solution of the congruence

$$tf'(r) + \frac{f(r)}{p^{a-1}} \equiv 0 \pmod{p}, \tag{7.11}$$

  chosen in the range $0 \leq t < p$.

- *If $f'(r) \equiv 0 \pmod{p}$ then:*
  - *if $f(r) \equiv 0 \pmod{p^a}$ then r can be lifted to solutions of the congruence $f(x) \equiv 0 \pmod{p^a}$ in p distinct ways, modulo p^a. In this case the new solutions $s_0, s_2, \ldots, s_{p-1}$ are given by*

$$s_i = r + ip^{a-1},$$

    for $i = 0, 1, \ldots, p-1$.
  - *if $f(r) \not\equiv 0 \pmod{p^a}$ then r cannot be lifted to a solution of the congruence $f(x) \equiv 0 \pmod{p^a}$.*

Proof. Omitted. □

We shall not deal with the proof of this theorem. It can be found in the book by Apostol[1].

Example 7.1. Find some solutions of the congruence

$$x^2 + 3x - 16 \equiv 0 \pmod{81}. \tag{7.12}$$

Solution. In lectures. □

7.3 Procedure for solving a polynomial congruence

We can now outline a strategy for finding all the solutions (if any exist) to any given polynomial congruence

$$f(x) \equiv 0 \pmod{n}. \tag{7.13}$$

Keep in mind the remarks made near the beginning of chapter 6. We are seeking to find which congruence classes modulo n solve this congruence. We need to apply the following steps.

[1] Apostol, T. M. (1976) *Introduction to analytic number theory.* New York: Springer-Verlag.

1. Find the canonical form of the modulus n, i.e.
$$n = \prod_{i=1}^{r} p_i^{a_i}. \tag{7.14}$$

2. Consider the system of congruences
$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \quad (i = 1, \ldots, r). \tag{7.15}$$
Taking each of these congruences in turn, use the method of theorem 7.2 to find all its solutions.

3. Any solution of the original congruence in (7.13) is obtained by applying the Chinese Remainder Theorem to a set of solutions for the system in (7.15).
If any of the congruences in (7.15) has no solutions then there are no solutions of the original congruence in (7.13).
Providing that solutions exist for each of the congruences in (7.15), take all possible combinations of these, and for each combination use the Chinese Remainder Theorem to find the corresponding solution of the original congruence in (7.13).

Exercise 7.1. Questions 1 through 7 concern finding solutions to polynomial congruences. Question 8 is a divisibility test which can be proved using some of the basic properties of the congruence relation covered to date.

1. Show how the method of theorem 7.2 works to generate all of the solutions of the previously considered polynomial congruence
$$x^2 - 1 \equiv 0 \pmod{8}. \tag{7.16}$$

2. Solve completely the polynomial congruence
$$x^2 - 90x + 96 \equiv 0 \pmod{125}. \tag{7.17}$$

3. Solve completely the polynomial congruence
$$3x^2 - 40x + 223 \equiv 0 \pmod{49}. \tag{7.18}$$

4. Solve completely the polynomial congruence
$$4x^2 + 86x + 68 \equiv 0 \pmod{121}. \tag{7.19}$$

5. Solve completely the polynomial congruence
$$4x^2 - 86x + 79 \equiv 0 \pmod{121}. \tag{7.20}$$

6. Solve completely the polynomial congruence
$$n^{13} \equiv n \pmod{1365}. \tag{7.21}$$

7. Solve completely the polynomial congruence
$$n^{17} \equiv n \pmod{4080}. \tag{7.22}$$

8. Suppose that a four-digit integer is written as $abcd$ in its usual decimal notation. Define the function f by
$$f(n) = a + 7b + 3c - 2d. \tag{7.23}$$
Show that $23|n$ iff $23|f(n)$.

Chapter 8

Quadratic Residues

This chapter explores the solutions of quadratic congruences modulo a prime p. This turns out to depend on the existence of elements with square roots (or *quadratic residues*) in the multiplicative modular groups $\mathbb{Z}_p$.

8.1 Reflecting on quadratic *equations* and the quadratic formula

Recall the well known formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \tag{8.1}$$

for obtaining the solutions to a quadratic equation,

$$ax^2 + bx + c = 0, \quad (a \neq 0). \tag{8.2}$$

The equation in 8.1 gives the solutions of 8.2, provided of course, that such solutions exists. When one restricts x to be an element of the real numbers then solution(s) only exist when the *discriminant* $b^2 - 4ac$ is non-negative, as then the discriminant has a (real) square root. If one allows x to be an element of the complex numbers then the solutions always exist as the discriminant will always have a square root.

It is helpful to see again the reasoning that leads to the quadratic solution formula. In order to simplify the following algebra we begin by multiplying both sides of the equation by $4a$,

$$ax^2 + bx + c = 0 \Leftrightarrow 4a^2x^2 + 4abx + 4ac = 0, \tag{8.3}$$

which has the effect of making the x^2 term a nice square. We continue by recasting the left hand side of this new equation by *completing the square*

$$\ldots \Leftrightarrow (2ax + b)^2 - b^2 + 4ac = 0 \tag{8.4}$$

$$\Leftrightarrow (2ax + b)^2 = b^2 - 4ac, \tag{8.5}$$

and we can now take the square root of both sides to get

$$\cdots \Leftrightarrow 2ax + b = \pm\sqrt{b^2 - 4ac}, \tag{8.6}$$

(provided of course that this is allowed – it will not be if $x \in \mathbb{R}$ and $b^2 - 4ac < 0$). Finally, tidying up leads to the quadratic formula

$$\cdots \Leftrightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{8.7}$$

Notice the need for the $a \neq 0$ condition to allow division by a.

Exercise 8.1. Obtain the quadratic formula using a similar 'completing the square' technique but *without* first multiplying across by $4a$. You should reach the same formula at the end.

So we can say that we have a complete understanding of the solutions of quadratic equations, in that we can say exactly when solutions will exist, and when they do we know how to obtain them. The aim in this chapter is to reach a similar position with regard to quadratic *congruences*.

8.2 Quadratic congruences - initial investigation

Let p be an odd prime and consider the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{8.8}$$

For this to be a genuine quadratic we would require that the x^2 term is actually present, i.e. that $a \not\equiv 0 \pmod{p}$ or $p \nmid a$. But since p is a prime this condition is equivalent to saying that $\gcd(a, p) = 1$. So let us try and repeat the reasoning that lead to the solution in the case of quadratic equations. We will be working with congruences so we should understand the coefficients a, b, c as representing their respective congruence classes modulo p.

$$ax^2 + bx + c \equiv 0 \pmod{p} \Leftrightarrow 4a(ax^2 + bx + x) \equiv 0 \pmod{p}, \tag{8.9}$$

$$\Leftrightarrow 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}, \tag{8.10}$$

$$\Leftrightarrow (2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{p}. \tag{8.11}$$

So far, so good. Next, we would be tempted to make the step

$$\cdots \Leftrightarrow 2ax + b \equiv \sqrt{b^2 - 4ac} \pmod{p}. \tag{8.12}$$

But can we do this? We haven't discussed square roots in a congruence context up to now in any detail. It is clear what a modular square root is. If $u \equiv v^2 \pmod{p}$ then we could say that v is a square root of u modulo p. But do square roots always exist? Is there a corresponding notion of positive and negative for congruence classes modulo p? These and other questions are what we explore in this chapter.

8.3 Definition and some initial results

In the congruence context we tend not to use the term *square root* so as to avoid confusion with its normal meaning. Instead we use the term *quadratic residue*.

Definition 8.1 (Quadratic residues)**.** Let p be an odd prime and consider the quadratic congruence

$$x^2 \equiv n \pmod{p}, \tag{8.13}$$

where $n \not\equiv 0 \pmod{p}$. If this has a solution $x \in \mathbb{Z}$ then we say that n is a *quadratic residue* modulo p, otherwise we say that n is a *quadratic non-residue* modulo p.

As with solutions of polynomial congruences, it should be understood that the concept of a quadratic residue is one that applies to the *congruence classes* modulo p. That is, if $n \equiv m \pmod{p}$ then n is a quadratic residue if and only if m is a quadratic residue.

Example 8.1. For the prime $p = 5$ the congruence classes of 1 and 4 are both quadratic residues, and the congruence classes of 2 and 3 are quadratic non-residues.

For the prime $p = 7$ the quadratic residues are $1, 2, 4$ while $3, 5, 6$ are quadratic non-resides. To verify this we can check the congruence class of each of $1^2, 2^2, 3^3, 4^2, 5^2$ and 6^2.

Once we have the concept of a quadratic residue there are two different, though related, types of questions that come to mind. Firstly, for a given prime p we might be interested in determining which of the congruence classes modulo p are quadratic residues and which are quadratic non-residues. Secondly, for a given integer n, we might be interested in determining for which primes p is n a quadratic residue and for which p is n a non-residue.

Exercise 8.2. Without any deeper systematic understanding of quadratic residues the best we can do to answer these questions is to check all possibilities.

1. Classify the congruence classes modulo 11 as quadratic residues / non-residues.
2. Consider all the odd primes $p \leq 20$. For which p is 2 a quadratic residue / non-residue?
3. Consider all the odd primes $p \leq 20$. For which p is -1 a quadratic residue / non-residue?
4. Consider all the odd primes $p \leq 20$. For which p is 5 a quadratic residue / non-residue?
5. Do the answers to these questions (and other numerical investigation) reveal any pattern or systematic behaviour?

We can always answer such questions by simply checking all the possible congruence classes. However for large moduli this becomes impractical and always resorting to brute force like this is not taking advantage of the properties of congruence and residues. We shall see later in this chapter that knowing the residue status of the integers -1 and 2 with respect to all primes p, combined with a result called quadratic reciprocity, gives us a systematic way to answer such questions more efficiently.

The correct algebraic setting for thinking about quadratic residues is the multiplicative group $\left(\mathbb{Z}_p^\times, \times\right)$, also called the reduced residue system modulo p (see definition 4.9). Recall that when p is a prime the elements of this group can be represented by the integers $1, 2, 3, \ldots, p-1$. So the only difference between the sets $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p$, is that $0 \in \mathbb{Z}_p$.

Our first general result about quadratic residues says quite simply that half of the elements in $\mathbb{Z}_p^\times$ are quadratic residues and half of them are not.

Theorem 8.1 (Counting residues modulo a prime p)**.** *Let p be an odd prime. Then the reduced residue system $\mathbb{Z}_p^\times$ contains $\frac{p-1}{2}$ quadratic residues modulo p and $\frac{p-1}{2}$ quadratic non-residues modulo p.*

Proof. It is clear that each of the integers

$$1^2,\, 2^2,\, \ldots,\, \left(\frac{p-1}{2}\right)^2, \tag{8.14}$$

are quadratic residues modulo p since each of these are square integers. In addition, each of these squares represent different congruence classes modulo p. For if this were not the case we could have $x^2 \equiv y^2 \pmod{p}$, where $1 \leq x, y \leq \frac{p-1}{2}$, i.e.

$$p|x^2 - y^2, \quad \left(1 \leq x, y \leq \frac{p-1}{2}\right) \tag{8.15}$$

This is equivalent to

$$p|(x-y)(x+y). \tag{8.16}$$

But $0 < x + y < p$ and so we know that $p \nmid (x+y)$. Now since p is a prime Euclid's lemma tells us that the other factor is divisible by p, i.e. $p|(x-y)$. But $0 \leq |x-y| < p$ so it must be that $x - y = 0$, i.e. $x = y$.

So the congruence classes represented by the squares in (8.14) are distinct. Moreover, these are all the quadratic residues. To show this, consider a quadratic residue y^2 where $\frac{p-1}{2} < y \leq p-1$. Then we have $y = p - x$ for some $1 \leq x \leq \frac{p-1}{2}$ and so $y^2 \equiv x^2 \pmod{p}$. So in other words, the quadratic residue y^2 has already been listed in (8.14).

So we have proved that the $\frac{p-1}{2}$ congruence classes represented by the integers in (8.14) are all of the quadratic residue classes modulo p. Therefore the remaining $\frac{p-1}{2}$ congruence classes in $\mathbb{Z}_p^\times$ are quadratic non-residues. □

8.4 The Legendre symbol

For working with quadratic residues it is helpful to introduce a compact notation for the statement that n is a quadratic residue modulo p.

Definition 8.2 (Legendre symbol)**.** The Legendre symbol $(n \,|\, p)$ is defined for odd primes p when $n \not\equiv 0 \pmod{p}$. It indicates whether n is a quadratic residue as follows ,

$$(n \,|\, p) = \begin{cases} +1 & \text{if } n \text{ is a quad. residue mod. } p \\ -1 & \text{if } n \text{ is not a quad. residue mod. } p \end{cases}. \tag{8.17}$$

For the sake of completeness we can define the Legendre symbol when the argument n is not co-prime to p by

$$(n \,|\, p) = 0 \text{ whenever } n \equiv 0 \pmod{p}. \tag{8.18}$$

Note on the notation: This notation is not universally used. Some authors will write $\left(\frac{n}{p}\right)$ for the Legendre symbol instead. This suffers from the drawback that it can be confused with regular fractions. Of course, our notation also suffers from the drawback that it can be confused with our earlier use of the vertical bar | in the divisibility relation. Either way, this shows the importance of understanding the context of what you are reading and being clear on exactly what the symbols mean!

Example 8.2. Looking back to example 8.1, for the prime $p = 7$ we have

$$(1 \,|\, 7) = (2 \,|\, 7) = (4 \,|\, 7) = +1,$$

and

$$(3 \,|\, 7) = (5 \,|\, 7) = (6 \,|\, 7) = -1.$$

Exercise 8.3. Investigate the quadratic residues with respect to some other small prime moduli and record your results using the Legendre symbol notation.

Remember that the concept of quadratic residues is defined for congruence classes modulo p so we can view the Legendre symbol $(n \,|\, p)$ as a function in the first variable as follows

$$(\cdot \,|\, p) \,:\, \mathbb{Z}_p^{\times} \to \{-1, +1\}\,. \tag{8.19}$$

We shall now be concerned with methods for evaluating $(n \,|\, p)$ and establishing some of its general properties. Of course if the argument n is itself a square integer then we can immediately say that it is a quadratic residue, i.e.

Lemma 8.2. *Consider an odd prime p and an integer m such that $m \not\equiv 0 \pmod{p}$, then*

$$\left(m^2 \,\middle|\, p\right) = +1. \tag{8.20}$$

Proof. This follows immediately from the definition. □

An important property of the Legendre symbol is that it behaves very well with respect to the operation of multiplication, as the following theorem shows.

Theorem 8.3 (Legendre symbol is multiplicative)**.** *The Legendre symbol is completely multiplicative, i.e. for all $n, m \in \mathbb{Z}$ we have*

$$(nm \,|\, p) = (n \,|\, p)\,(m \,|\, p)\,, \tag{8.21}$$

for all odd primes p.

Proof. First we deal with the cases where either side of the equation is zero. If $(mn \,|\, p) = 0$ then $p|mn$, but since p is prime then we know that $p|m$ or $p|n$, in which case at least one of $(m \,|\, p)$ and $(n \,|\, p)$ is zero and so the result holds. Conversely, if $(m \,|\, p)\,(n \,|\, p) = 0$ then one of these factors is zero, i.e. $p|m$ or $p|n$. In both cases we get $p|mn$ and so $(mn \,|\, p) = 0$ and again the result holds.

To settle the remaining cases we make use of the formula of Euler's criterion (theorem 8.4). This gives us the following chain of congruences and equation,

$$(mn \,|\, p) \equiv (mn)^{\frac{p-1}{2}} = (m)^{\frac{p-1}{2}}\,(n)^{\frac{p-1}{2}} \equiv (m \,|\, p)\,(n \,|\, p) \pmod{p}. \tag{8.22}$$

Note that we now know that

$$(mn \,|\, p) \equiv (m \,|\, p)\,(n \,|\, p) \pmod{p}, \tag{8.23}$$

but the result we want is equality between the two, not just congruence. However the congruence is equivalent to

$$p|\,(mn \,|\, p) - (m \,|\, p)\,(n \,|\, p)\,, \tag{8.24}$$

but since Legendre symbols are either ± 1, this difference is equal to -2, 0 or 2. The only one of these divisible by p is of course 0. And so the result follows. □

8.5 Evaluating the Legendre symbol

First we recall the results of Euler's theorem and its corollary *Fermat's Little Theorem* (theorem 5.7). This stated that if $n \not\equiv 0 \pmod{p}$ then

$$n^{p-1} \equiv 1 \pmod{p}. \tag{8.25}$$

So when p is an odd prime (i.e. $p-1$ is even) a consequence of this is that

$$\left(n^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}, \tag{8.26}$$

i.e.

$$n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}. \tag{8.27}$$

So here we have a formula involving n and p which takes the values ± 1. Could this in fact agree with the function $(n \mid p)$? The following result asserts that it does!

Theorem 8.4 (Euler's criterion)**.** *If p is an odd prime then*

$$(n \mid p) \equiv n^{\frac{p-1}{2}} \pmod{p}. \tag{8.28}$$

Proof. We shall show that in all cases the two expressions agree. Fistly, suppose that $(n \mid p) = +1$. In this case we know there exists an integer m such that

$$n \equiv m^2 \pmod{p}. \tag{8.29}$$

But then we have

$$n^{\frac{p-1}{2}} \equiv \left(m^2\right)^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod{p}, \tag{8.30}$$

where the last congruence is true by Fermat's Little Theorem. So the two expressions agree in this case.

Secondly, suppose that $(n \mid p) = -1$. Considering the polynomial congruence

$$f(x) \equiv x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}, \tag{8.31}$$

we see that this has at most $\frac{p-1}{2}$ solutions by Lagrange's theorem (theorem 7.1). However we have already seen that the $\frac{p-1}{2}$ quadratic residues modulo p are solutions to this polynomial congruence, so it can not have any more solutions. So we can conclude in this case that

$$n^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}. \tag{8.32}$$

But we know that $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ and so we conclude in this case that $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and hence the two expressions agree in this case.

Lastly, if $(n \mid p) = 0$ then $p|n$ and so $p|n^{\frac{p-1}{2}}$ also, i.e. $n^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. So in this last case the two expressions also agree. □

So Euler's criterion gives us a formula which we can use to evaluate Legendre symbols. However for large primes p this will need us to calculate large powers of n. So we continue to investigate the properties of the Legendre symbol to find better methods.

Now we characterise the residue status of -1 with regard to the congruence class of the modulus p modulo 4.

Theorem 8.5. *If p is an odd prime then*

$$(-1 \mid p) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}. \tag{8.33}$$

Proof. From Euler's criterion be have

$$(-1\,|\,p) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}. \tag{8.34}$$

But both sides of this congruence are equal to ± 1 and so therefore they are in fact equal, i.e.

$$(-1\,|\,p) = (-1)^{\frac{p-1}{2}}. \tag{8.35}$$

The required result then comes from noting that the value of the right hand side, since it is a power of -1, depends only on whether $\frac{p-1}{2}$ is even or odd. If $p \equiv 1 \pmod 4$ then $\frac{p-1}{2}$ is even whereas if $p \equiv 3 \pmod 4$ then it is odd. □

Now the residue status of the congruence class of 2 is characterised with regard to the congruence class of p modulo 8.

Theorem 8.6. *If p is an odd prime then*

$$(2\,|\,p) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}. \tag{8.36}$$

Proof. Euler's criterion says that

$$(2\,|\,p) \equiv 2^{\frac{p-1}{2}} \pmod{p} \tag{8.37}$$

and this proof works by forming a particular product of congruence classes modulo p and rewriting this product in two ways. The first way will feature the power of 2 from the Euler's criterion expression above, and the second way will feature a power of -1, from which we will get the result of this theorem.

The product we use is the product of all the congruence classes modulo p represented by the even integers between 1 and $p-1$, namely $2 \times 4 \times 6 \times \cdots \times (p-1)$, (remember that p is odd so $p-1$ is even).

Firstly we extract the powers of 2 by simply factoring each of the even numbers as follows

$$2 \times 4 \times 6 \times \cdots \times (p-1) = 2^{\frac{p-1}{2}} \left(1 \times 2 \times \cdots \times \frac{p-1}{2}\right) \tag{8.38}$$

$$= 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \tag{8.39}$$

The second way of rewriting the product will again bring out the $\left(\frac{p-1}{2}\right)!$ term. We reorder the elements $2, 4, 6, \ldots, p-1$ by choosing elements in an alternating fashion from the end and beginning of the list as follows:

$$p - 1 \equiv 1(-1)^1 \pmod{p} \tag{8.40}$$

$$2 \equiv 2(-1)^2 \pmod{p} \tag{8.41}$$

$$p - 3 \equiv 3(-1)^3 \pmod{p} \tag{8.42}$$

$$4 \equiv 4(-1)^4 \pmod{p} \tag{8.43}$$

$$\vdots \tag{8.44}$$

$$s \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod{p}. \tag{8.45}$$

p	p^2-1	$(p^2-1)/8$	parity	$(-1)^{(p^2-1)/8}$
$8q+1$	$64q^2+16q$	$8q^2+2q$	even	$+1$
$8q+3$	$64q^2+48q+8$	$8q^2+6q+1$	odd	-1
$8q+5$	$64q^2+80q+24$	$8q^2+10q+3$	odd	-1
$8q+7$	$64q^2+112q+48$	$8q^2+14q+6$	even	$+1$

Table 8.1: Examining p modulo 8

The final element s will be either $p-\frac{p-1}{2}$ or $\frac{p-1}{2}$, accordingly as $\frac{p-1}{2}$ is odd or even. So now we multiply all these congruences together to obtain

$$2\times 4\times 6\times\cdots\times(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+3+\cdots+(p-1)/2}\pmod p. \tag{8.46}$$

Using the closed form for the arithmetic series in the exponent gives us

$$2\times 4\times 6\times\cdots\times(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8}\pmod p. \tag{8.47}$$

Combining the congruences (8.39) and (8.47) gives

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8}\pmod p. \tag{8.48}$$

The factorial factor can be cancelled without changing the modulus p, since $\left(\frac{p-1}{2}\right)!$ is coprime to p. This gives us

$$2^{\frac{p-1}{2}}\equiv(-1)^{(p^2-1)/8}\pmod p, \tag{8.49}$$

which when combined with Euler's criterion gives us

$$(2\,|\,p)\equiv(-1)^{(p^2-1)/8}\pmod p. \tag{8.50}$$

Since $(2\,|\,p)$ and $(-1)^{(p^2-1)/8}$ are both equal to ±1 the congruence is actually an equation, i.e.

$$(2\,|\,p)=(-1)^{(p^2-1)/8}. \tag{8.51}$$

The result of the theorem follows from evaluating the power of -1 by examining the parity (odd/even) of $(p^2-1)/8$ and how this depends on the congruence class of p modulo 8, as shown in table 8.1. Summarizing the results of the table gives us the required result as

$$(2\,|\,p)=\begin{cases}+1 & \text{if } p\equiv\pm1 \pmod 8\\ -1 & \text{if } p\equiv\pm3 \pmod 8\end{cases}. \tag{8.52}$$

□

The following result of Gauss provides a simpler way to evaluate the Legendre symbol for large inputs.

Theorem 8.7 (Gauss)**.** *Suppose that p is an odd prime and that $n\not\equiv 0 \pmod p$. Consider the least positive residues modulo p of the following numbers,*

$$n, 2n, 3n, \ldots, \frac{p-3}{2}n, \frac{p-1}{2}n. \tag{8.53}$$

If m is the number of these residues which are greater than $\frac{p}{2}$, then

$$(n\,|\,p)=(-1)^m. \tag{8.54}$$

Proof. Multiplying the elements in the list in (8.53) together gives us

$$\prod_{j=1}^{(p-1)/2} jn = n^{(p-1)/2}\left(\frac{p-1}{2}\right)!. \tag{8.55}$$

The first of the terms on the right we recognise from Euler's criterion as being congruent to $(n\,|\,p)$. We will recast the product of elements from the left hand side by assigning to each ± 1 in keeping with the statement of the theorem.

Consider the least positive residue r of a typical element jn. If this residue r does exceed $\frac{p}{2}$ then $(p-1)/2 \leq r \leq p-1$ and we can say

$$jn \equiv r \equiv -s \pmod{p}, \tag{8.56}$$

for some $1 \leq s \leq (p-1)/2$. In this way we can associate to each multiple jn an element $\epsilon_j s_j$ where $\epsilon_j = \pm 1$ and $1 \leq s_j \leq (p-1)/2$ for each $1 \leq j \leq (p-1)/2$. This gives us a 1-1 congruence correspondence between the two sets

$$\left\{n, 2n, 3n, \ldots, \frac{p-3}{2}n, \frac{p-1}{2}n\right\} \tag{8.57}$$

and

$$\left\{\epsilon_1 1, \epsilon_2 2, \epsilon_3 3, \ldots, \epsilon_{\frac{p-3}{2}}\frac{p-3}{2}, \epsilon_{\frac{p-1}{2}}\frac{p-1}{2}.\right\} \tag{8.58}$$

So multiplying all the elements from one of these sets will give something congruent to multiplying all the elements from the other set. Combining this observation with equation (8.55) gives us the congruence

$$n^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv \prod_{j=1}^{(p-1)/2} \epsilon_j j \pmod{p} \tag{8.59}$$

$$\equiv (-1)^m\left(\frac{p-1}{2}\right)! \pmod{p}, \tag{8.60}$$

where m is the count of the number of negative ϵ_j as in the statement of the theorem. Cancelling the factorial (as $(p-1)/2$ is coprime to p) from this and combining with Euler's criterion this gives us the required result,

$$n^{(p-1)/2} \equiv (n\,|\,p) = (-1)^m. \tag{8.61}$$

(*Note that the final relation is equality rather than congruence, as each side is* ± 1.) □

In order to use this new method of evaluating the Legendre symbol we need a way of calculating the value of m, or rather its congruence class modulo 2. This result will be a key ingredient in the proof of the Quadratic Reciprocity Law in the next section. First, recall the notation for 'integer part' and 'fractional part' of a real number x,

$$x = [x] + \{x\}, \tag{8.62}$$

where $[x] \in \mathbb{Z}$ and $0 \leq \{x\} < 1$.

Theorem 8.8. *The congruence class of the number m from Gauss' formula is given by*

$$m \equiv \sum_{j=1}^{(p-1)/2}\left[\frac{jn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod{2}, \tag{8.63}$$

which when n is odd, simplifies to

$$m \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{jn}{p}\right] \pmod 2. \tag{8.64}$$

Proof. Again, we focus on the multiples jn for $1 \leq j \leq \frac{p-1}{2}$ and obtain an expression for their least positive residues r_j, as follows:

$$\frac{jn}{p} = \left[\frac{jn}{p}\right] + \left\{\frac{jn}{p}\right\} \tag{8.65}$$

$$\Leftrightarrow \quad jn = p\left[\frac{jn}{p}\right] + p\left\{\frac{jn}{p}\right\}. \tag{8.66}$$

This last equation shows the integer division of tn by p where the remainder is given by

$$r_j = p\left\{\frac{jn}{p}\right\}, \quad 0 \leq r_j < p \tag{8.67}$$

$$= jn - p\left[\frac{jn}{p}\right]. \tag{8.68}$$

Recall the representation for these residues that we used in the proof of Gauss' lemma

$$\left\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\right\} \equiv \left\{\epsilon_1 1, \epsilon_2 2, \epsilon_3 3, \ldots, \epsilon_{\frac{p-1}{2}} \frac{p-1}{2}\right\} \pmod p. \tag{8.69}$$

Making use of the $\epsilon_j = \pm 1$ classification allows to represent the sum of these residues as [1]

$$\sum_{j=1}^{(p-1)/2} r_j = \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = +1}} j + \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = -1}} (p-j) \tag{8.70}$$

$$\Rightarrow \quad \sum_{j=1}^{(p-1)/2} \left(jn - p\left[\frac{jn}{p}\right]\right) = \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = +1}} j + mp - \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = -1}} j, \quad \text{by (8.68)} \tag{8.71}$$

$$\Rightarrow \quad n \sum_{j=1}^{(p-1)/2} j - p \sum_{j=1}^{(p-1)/2} \left[\frac{jn}{p}\right] = \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = +1}} j + mp - \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = -1}} j. \tag{8.72}$$

Now introduce the equation

$$\sum_{j=1}^{(p-1)/2} j = \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = +1}} j + \sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = -1}} j. \tag{8.73}$$

[1] In the following equations a summation such as

$$\sum_{\substack{1 \leq j \leq \frac{p-1}{2} \\ \epsilon_j = +1}} j$$

denotes the sum of the values j for which $1 \leq j \leq \frac{p-1}{2}$ AND $\epsilon_j = +1$, i.e. both conditions must hold true for j to be included in the sum.

Adding equations (8.72) and (8.73) gives

$$(n+1)\sum_{j=1}^{(p-1)/2} j - p\sum_{j=1}^{(p-1)/2}\left[\frac{jn}{p}\right] = mp + 2\sum_{\substack{1\le j\le \frac{p-1}{2}\\ \epsilon_j=+1}} j. \tag{8.74}$$

In order to get the required results from this we will reduce it modulo 2, sum the first arithmetic sequence on the left hand side and note that $p \equiv 1 \pmod 2$ and $n+1 \equiv n-1 \pmod 2$, giving us

$$(n-1)\frac{p^2-1}{8} + \sum_{j=1}^{(p-1)/2}\left[\frac{jn}{p}\right] \equiv m \pmod 2, \tag{8.75}$$

as required. □

8.6 Quadratic reciprocity

We now come to a very important result in number theory. It describes the relationship between the quadratic residue status of a pair of primes modulo each other. We shall look at the statement of the result now and then discuss the way it can be used to help evaluate Legendre symbols.

Theorem 8.9 (Law of Quadratic Reciprocity)**.** *If p, q are distinct odd primes then their Legendre symbols are related by*

$$(q\,|\,p) = \begin{cases} -(p\,|\,q) & \text{if } p \equiv q \equiv 3 \pmod 4 \\ (p\,|\,q) & \text{otherwise} \end{cases} \tag{8.76}$$

In terms of quadratic residues this states that if p and q are not both congruent to 3 modulo 4 thenb p is a quadratic residue modulo q iff q is a quadratic residue modulo p, and when p and q *are* both congruent to 3 modulo 4 then p and q will have opposite quadratic residue status modulo each other.

Strategy for evaluating $(n\,|\,p)$

We can gather together a number of properties of the Legendre symbol to allow us to easily find its value. The method works by repeatedly reducing Legendre symbols to other Legendre symbols featuring *smaller* arguments. In this way we will eventually reach Legendre symbols featuring the arguments -1 and 2, whose values have been settled earlier in theorems 8.5 and 8.6. The results we will use are

- Congruence property: If $n \equiv m \pmod p$ then $(n\,|\,p) = (m\,|\,p)$.
- Multiplicative property: $(nm\,|\,p) = (n\,|\,p)\,(m\,|\,p)$.
- Quadratic Reciprocity: $(q\,|\,p) = (p\,|\,q)$, unless $p \equiv q \equiv 3 \pmod 4$ in which case $(q\,|\,p) = -(p\,|\,q)$.

Example 8.3. Evaluate the Legendre symbol $(219\,|\,383)$.

p mod. 12	p mod. 3	p mod. 4	$(3\,|\,p)$
1	1	1	$+1$
5	2	1	-1
7	1	3	-1
11	2	3	$+1$

Table 8.2: The values of p modulo 12

Solution.

$$\begin{aligned}(219\,|\,383) &= (3\,|\,383)\,(73\,|\,383) && (8.77)\\ &= \Big(-(383\,|\,3)\Big)\,(383\,|\,73) && (8.78)\\ &= \Big(-(2\,|\,3)\Big)\,(18\,|\,73) && (8.79)\\ &= -(-1)\,(2\,|\,73)\,(9\,|\,73) && (8.80)\\ &= (2\,|\,73) && (8.81)\\ &= +1 && (8.82)\end{aligned}$$

Make sure you understand how each step is made using the various properties.

So we can say that solutions do exits for the quadratic congruence $x^2 \equiv 219 \pmod{383}$ as 219 is a quadratic residue modulo 383. □

The following example shows how to use reciprocity to establish a congruence result for the Legendre symbols $(3\,|\,p)$.

Example 8.4. Describe the value of $(3\,|\,p)$ in terms of the congruence class of p modulo a suitable integer.

Solution. By quadratic reciprocity we have

$$(3\,|\,p) = \begin{cases}(p\,|\,3) & \text{if } p \equiv 1 \pmod 4\\ -(p\,|\,3) & \text{if } p \equiv 3 \pmod 4\end{cases}. \tag{8.83}$$

By considering the definition we see that

$$(p\,|\,3) = \begin{cases}+1 & \text{if } p \equiv 1 \pmod 3\\ -1 & \text{if } p \equiv 2 \pmod 3\end{cases}. \tag{8.84}$$

So we now have two congruence conditions on p to consider. The values of p modulo 3 and 4 will be determined by the congruence class of p modulo 12 (this is an example of the Chinese Remainder Theorem). The details are laid out in table 8.2 and give us the final description

$$(3\,|\,p) = \begin{cases}+1 & p \equiv \pm 1 \pmod{12}\\ -1 & p \equiv \pm 5 \pmod{12}\end{cases}. \tag{8.85}$$

And so this gives us a description of exactly when solutions exist for the congruence $x^2 \equiv 3 \pmod p$ in terms of the congruence class of p modulo 12. □

Proof of the Quadratic Reciprocity Law

We now turn to providing a proof for the Quadratic Reciprocity Law. The law was discovered by Euler in the mid 18th Century and then rediscovered by Legendre in 1785. Gauss discovered it for himself independently of Euler and Legendre and provided the first complete proof in 1796. The law is famous for accumulating many proof over the years. The following proof is an example of a *lattice point counting technique* and is based on ideas from Gauss' work. It makes use of the results of the previous section.

Proof of Theorem 8.9. We prove the result by establishing the formula

$$(p\,|\,q)\,(q\,|\,p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{8.86}$$

That this is equivalent to the required result can be seen by considering the parity of the exponent. If p and q are both congruent to 3 modulo 4 then the exponent is odd and so the two Legendre symbols must have opposite signs, otherwise (when at least one of p and q is congruent to 1 modulo 4) the exponent is even and so the Legendre symbols must have the same sign.

As a graphical aid to the proof we consider the integer lattice shown in figure 8.1. For our purposes a lattice consists of all points in the plain with integer coordinates. We consider the rectangle R with corners at the origin and the point $\left(\frac{p}{2}, \frac{q}{2}\right)$ (note that this point is not a lattice point). We wish to count the number, M, of lattice points belonging to the interior of R, i.e. not on its boundary. These points are shown in black in the figure. Of course we can see immediately that

$$M = \frac{p-1}{2}\frac{q-1}{2}. \tag{8.87}$$

We also count these points in another way by counting the points that lie in the triangles T_1 and T_2, that lie either side of the diagonal through R, as shown in figure 8.1. We note that the diagonal of R is the line with slope $\frac{q}{p}$ and there are no lattice points lying on this line between the origin and the point (p, q) (if there were this would imply that p and q have a common divisor greater than 1). Hence the number of points M in R can be expressed as

$$M = M_1 + M_2. \tag{8.88}$$

The number of points, M_1, lying in T_1 is given by the sum

$$M_1 = \sum_{t=1}^{(p-1)/2} \left\lfloor \frac{tq}{p} \right\rfloor.$$

The number of points, M_2, lying in T_2 is given by the sum

$$M_2 = \sum_{s=1}^{(q-1)/2} \left\lfloor \frac{sp}{q} \right\rfloor.$$

Note: You should satisfy yourself that the number of points lying in the column over t in the triangle T_1 is indeed given by $\left\lfloor \frac{tq}{p} \right\rfloor$, and similarly, the number of points in the row across from s in the triangle T_2 is indeed given by $\left\lfloor \frac{sp}{q} \right\rfloor$.

Note that these sums are exactly the expressions occurring in the formula for the Legendre symbol from theorem 8.8. So we can say that

$$(p\,|\,q) = (-1)^{M_2} \text{ and } (q\,|\,p) = (-1)^{M_1}, \tag{8.89}$$

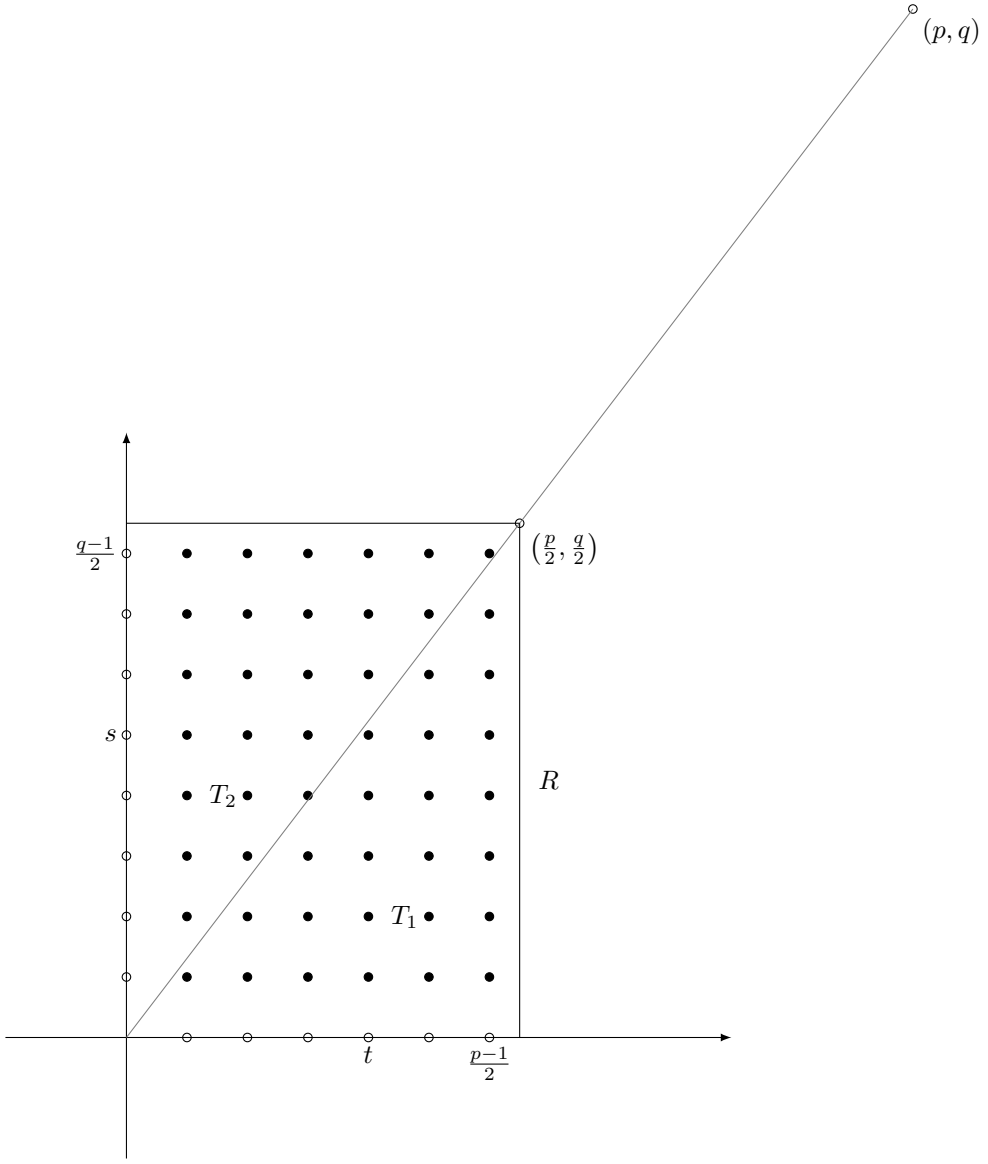


Figure 8.1: Counting the lattice points inside R, (shown for the case $p = 13$, $q = 17$).

and hence

$$(p \,|\, q)\,(q \,|\, p) = (-1)^{M_2+M_1} = (-1)^{M} = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}, \tag{8.90}$$

as required. □

Exercise 8.4. Here are some exercises and problems based on quadratic residues and quadratic reciprocity. These are selected exercises from *Elementary Number Theory* by David Burton, Allyn & Bacon (1980).

1. Find the solutions (if they exist) of the following quadratic congruences.

   a) $x^2 + 7x + 10 \equiv 0 \pmod{11}$,

   b) $3x^2 + 9x + 7 \equiv 0 \pmod{13}$,

   c) $5x^2 + 6x + 1 \equiv 0 \pmod{23}$.

2. Verify that the quadratic residues modulo 17 are (the congruence classes) of 1, 2, 4, 8, 9, 13, 15, 16.

3. Show why 3 is a quadratic residue modulo 23, but a quadratic non-residue modulo 19.

4. Suppose that p is an odd prime and that n is a quadratic residue modulo p. Prove that n cannot be a generator of the group $\mathbb{Z}_p^\times$.

5. Suppose that p is an odd prime of the form $p = 2^k + 1$, for some $k \in \mathbb{Z}$. Prove that if n is a quadratic non-residue modulo p then n is a generator of $\mathbb{Z}_p^\times$.

6. The integer 2 is a generator of $\mathbb{Z}_{19}^\times$. Use this knowledge to find all the quadratic residues modulo 19.

7. Let p be an odd prime and consider the quadratic congruence

   $$ax^2 + bx + c \equiv 0 \pmod{p},$$

   where $\gcd(a, p) = 1$, i.e. $p \nmid a$. Prove that the congruence is solvable if and only if $b^2 - 4ac$ is equal to 0 or is a quadratic residue modulo p. Then use this result to verify that the congruence

   $$5x^2 - 6x + 2 \equiv 0 \pmod{17}$$

   has solutions.

8. Use the Legendre symbol and its properties to prove that the congruence

   $$x^2 \equiv -38 \pmod{13}$$

   is solvable.

9. Use Gauss' lemma to evaluate each of the Legendre symbols: (8|11), (7|13), (5|19), (11|23), (6|31).

10. Use the law of quadratic reciprocity to evaluate the Legendre symbol (29|53). Give an interpretation of the result in terms of the solvability of a particular quadratic congruence.

11. Repeat the previous question for the Legendre symbols (71|73), (−219|383) and (461|773).

Exercise 8.5. Here are some additional exercises and problems based on quadratic residues and quadratic reciprocity. These are selected exercises from *Elementary Number Theory* by David Burton, Allyn & Bacon (1980) and *Introduction to Analytic Number Theory* by Tom M. Apostol.

1. Assume that p is an odd prime, i.e. p is a prime and $p > 2$. Suppose that the integers in the set
$$\mathbb{Z}_p^\times \{1, 2, 3, \ldots, p-1\}$$
can be partitioned into the subsets $S, T \subset \mathbb{Z}_p^\times$ so that S and T are both non-empty, they are disjoint (i.e. $S \cap T = \emptyset$) and they cover $\mathbb{Z}_p^\times$, (i.e. $S \cup T = \mathbb{Z}_p^\times$). Furthermore, suppose that S and T satisfy the following product properties
$$\forall s_1, s_2 \in S,\ s_1 s_2 \in S,$$
$$\forall t_1, t_2 \in T,\ t_1 t_2 \in S,$$
$$\forall s \in S,\ t \in T,\ st \in T.$$
Prove that the only subsets S and T satisfying all these properties are
$$S = \left\{ n \in \mathbb{Z}_p^\times \ :\ (n|p) = +1 \right\},$$
and
$$T = \left\{ n \in \mathbb{Z}_p^\times \ :\ (n|p) = -1 \right\},$$
i.e. S must be the set of quadratic residues and T must be the set of quadratic non-residues, modulo p.

2. Establish the following summation formulae for the Legendre symbol $(\cdot|\cdot)$,

   a)
   $$p \equiv 1 \pmod 4 \Rightarrow \sum_{n=1}^{p-1} n(n|p) = 0,$$

   b)
   $$p \equiv 1 \pmod 4 \Rightarrow \sum_{\substack{n=1 \\ (n|p)=+1}}^{p-1} n \ = \ \frac{p(p-1)}{4}.$$

   Hints: think flexibly about the summation index, e.g. as n runs through the values $1, 2, \ldots, p-1$, so does $p - n$, but in a different order.

3. Recall Euclid's proof of the infinitude of primes. Dirichlet's theorem is a generalisation of this and asserts that if $\gcd(a, b) = 1$ then the arithmetic sequence, $\{an + b\}_{n=1}^{\infty}$, contains an infinite number of primes. The proof of this is quite technical (see Chapter 7 of Apostol's book) however certain special cases can be proved with the aid of the machinery we have studied to date.

   The proofs have the same overall structure as Euclid's proof, i.e. assume there are only a finite number of primes of the given type, examine the divisibility properties of a certain number N defined in terms of the 'finite' list of primes and then deduce that the number N must have a prime factor of the given type which does not appear on the 'finite' list. This is a contradiction and hence there must be an infinite number of primes of the given type.

   So construct proofs for the following cases of Dirichlet's theorem using the guidance given.

a) There are infinitely many primes p of the form $p = 4n - 1$. *Hint: let p be the largest prime of the form $p = 4n - 1$ and consider*

$$N = \left(2^2 \times 3 \times 5 \times 7 \times \cdots \times p\right) - 1.$$

b) There are infinitely many primes p of the form $p = 8k + 3$. *Hint: let $p_1, \ldots, p_s$ be the finite list of primes of the form $8k + 3$, then consider*

$$N = (p_1 p_2 \ldots p_s)^2 + 2.$$

c) There are infinitely many primes p of the form $p = 6k + 1$. There are infinitely many primes p of the form $p = 6k + 1$. *Hint: let $p_1, \ldots, p_s$ be the finite list of primes of the form $6k + 1$, then consider*

$$N = (2p_1 p_2 \ldots p_s)^2 + 3.$$