2. NUMBERS AND DIVISIBILITY

§2.1. Number Theory in Mathematics and Computing Science

The earliest numbers to be "invented" were the positive whole numbers, and indeed these were the first numbers we encounter as children. Many early societies, but particularly the Greeks, developed the theory of numbers in quite a sophisticated way. Fundamental to this study is the notion of prime numbers, roughly speaking numbers that have only 1 and themselves as factors.

For many, many centuries number theory was considered the purest of all parts of mathematics – purest in the sense of having no practical applications. The early 20^{th} century number-theorist Hardy was proud that his subject had no practical applications. But then came the computer age with its digital foundations. The need for security in data transmission gave rise to the need for secure codes and the techniques for this were discovered to be lying dormant in the theory of prime numbers.

Throughout the history of mathematics this story has been repeated many times. Mathematics, rather than being created "on demand", often arises out of natural curiosity as mathematicians have developed their subject purely as an academic enquiry. Then, often decades or even centuries later, someone has found an important application. If mathematicians had been too concerned about their research being useful much useful mathematics might never have arisen.

Zero and negative numbers came onto the scene long after their positive counterparts. We include these and operate within the system of integers. Including the negative numbers does not greatly alter the theory, but it does make the theory a little easier in places. With negative numbers included we must modify our definition of prime number – we must allow a prime number p is divisible by –1 and –p as well as 1 and p. But they have no other divisors.

§2.2. The System of Integers

The system that we are studying in this chapter is the system of integers:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

We denote the set of integers by **Z** (from the German word "zahlen" which means "numbers"). Since these are the only numbers we will be considering in this chapter we will often use the more informal word "number" instead of "whole number" or "integer".

The system **Z** has two basic operations of addition and multiplication and these operations satisfy the following properties.

(1) (Closure Law for Addition): For all $a, b \in Z$, $a + b \in Z$.
(2) (Associative Law for Addition): For all $a, b, c \in Z$, $(a + b) + c = a + (b + c)$.
(3) (Commutative Law for Addition): For all $a, b \in Z$, $a + b = b + a$.
(4) (Identity for Addition): There exists $0 \in Z$ such that for all $a \in Z$, $0 + a = a$.
(5) (Inverses under Addition): For all $a \in Z$ there exists $-a \in Z$ such that $a + (-a) = 0$.
(6) (Closure Law for Multiplication): For all $a, b \in Z$, $ab \in Z$.
(7) (Associative Law for Multiplication): For all $a, b, c \in Z$, $(ab)c = a(bc)$.
(8) (Commutative Law for Multiplication): For all $a, b \in Z$, $ab = ba$.
(9) (Identity for Multiplication): There exists $1 \in Z$ such that $1 \neq 0$ and for all $a \in Z$, $1a = a$.

The properties for multiplication mirror those for addition, except that Z does not have inverses under multiplication. Although there exists a number b such that $2b = 1$, it is not an integer.

Tying the additive structure to the multiplicative structure we have the following property.

(10) (Distributive Law): For all $a, b, c \in Z$, $a(b + c) = ab + ac$.

In the system of real numbers we can cancel by a non-zero number. That is, if ab = ac and $a \neq 0$ then we can multiply both sides by a^{-1} to conclude that b = c. In the system Z we do not have inverses a^{-1}. However cancellation is still valid.

(11) (Cancellation Law): For all a, b, c ∈ Z, ab = ac implies that b = c.

Any system that has two operations of addition and multiplication that satisfies all 11 properties is called an "integral domain". We say that these are the axioms for an integral domain. There are other integral domains that you have already met, such as the system of polynomials in one variable with real coefficients.

In addition to the two binary operations the system **Z** has a subset **N** satisfying the following properties. This is the set {0, 1, 2, 3, …} and it is called the set of **natural numbers**.

(12) For all a, b ∈ N, ab ∈ N.
(13) For all a ∈ Z, exactly one of a, –a belongs to N.
(14) For all a ∈ N, a + 1 ∈ N.
(15) If S is a subset of N and:
(i) 0 ∈ S and
(ii) a ∈ S implies that a + 1 ∈ S
then S = N.

We call the non-zero elements of N positive. All other numbers, except for zero, are called **negative**. So there are three basic sets of numbers according to this classification.

negative numbers	**0**	**positive numbers**

§2.3. Induction

When a scientist carries out certain experiments he or she assumes that if a certain outcome occurs under certain circumstances this outcome will always occur under those circumstances. In most cases this turns out to be the case, but from time to time some unknown factor occurs that was not allowed for in the experiment and the scientific theory has to be modified. All scientific truth is tentative in this sense. Light travels in a straight line. No, it bends when travelling in strong magnetic fields. Atoms are the smallest particles. No, they are not – they are made up of electrons, neutrons and protons.

In mathematics we prove theorems that state that certain things will always hold. We do not simply test it in certain cases and, like a scientist, infer that it will always hold. Unless our logic is faulty we will never have to revise our theory – just add to it.

There is a statement that for all numbers n, $n^2 + n + 41$ is a prime number. The first 10 values are 41, 43, 47, 53, 61, 71, 83, 97, 113, 131. They are all prime. Clearly they will continue to be prime for ever. Certainly it remains prime up to n = 39. But when n = 40, $n^2 + n + 41$ will be $40^2 + 40 + 41 = 40(40 + 1) + 41$, quite clearly divisible by 41. And even more clearly it will not be prime for n = 41. Are these isolated examples? Not at all. From n = 42, $n^2 + n + 41$ is often prime and often not.

But how can we prove that something will always work? We cannot check every instance! The answer is that we can often use an argument that works in every case. But sometimes we can only do it by climbing up a ladder, going from one instance to another. This is the Principle of Induction. We prove that if it is true for n, it is true for n + 1, by some argument. If it is true for n = 1 then it is true for n = 2. But then, being true for n = 2 it is true for n = 3, and then n = 4 and so on. What we would have done is to provide a method of getting from each n to the next. It is like some giant infinite ladder. But, like a real ladder, it is not much use if the ladder is not resting on the

ground. With induction we must check the statement for n = 0 or n = 1, or whatever value we want to begin with.

Theorem 1: (Principle of Induction)
Suppose S(n) is a statement depending on some parameter $n \in \mathbf{N}$.
If S(0) is true and
for all n, S(n) implies S(n + 1)
then S(n) is true for all n.
Proof: Let $S = \{n \in N \mid S(n) \text{ is true}\}$. The assumptions show that $0 \in N$ and if $n \in N$ then $n + 1 \in N$. So by property (15) above S = N, in other words S(n) is true for all n.

Example 1: Prove that $\sum_{r=1}^{n} n^3 = \frac{1}{4} n^2(n + 1)^2$.
Solution: For n = 1, LHS = 1 = RHS.
Suppose $\sum_{r=1}^{n} n^3 = \frac{1}{4} n^2(n + 1)^2$.
Then $\sum_{r=1}^{n+1} n^3 = \frac{1}{4} n^2(n + 1)^2 + (n + 1)^3$

$$= \frac{1}{4} (n + 1)^2 [n^2 + 4(n + 1)]$$

$$= \frac{1}{4} (n + 1)^2 [n^2 + 4n + 1]$$

$$= \frac{1}{4} (n + 1)^2 (n + 2)^2.$$

So the result is true for n + 1. Hence by induction it holds for all n.

Sometimes it is not feasible to go from n to n + 1. A stronger form of the Induction Principle is the following.

Theorem 2: (Strong Induction Principle)
Suppose S(n) is a statement depending on some parameter $n \in \mathbf{N}$.
If for all n, S(m) is true for all m < n implies that S(n) is true then S(n) is true for all n.
Proof: Let T(n) be the statement S(m) is true for all m < n.
In symbols T(n) is $\forall m[m < n \rightarrow S(m)]$.
T(0) holds vacuously because m < 0 is always false. Remember here our universe is the set of natural numbers and $p \rightarrow q$ is true whenever p is false.
Suppose T(n) holds. Hence S(m) holds for all m < n. By the assumption in the statement of the theorem this implies that S(n) is true. Hence S(m) holds for all $m \leq n$, in other words, for all m < n + 1. Thus T(n + 1) holds and so by Theorem 1, T(n), and hence S(n) holds for all $n \in \mathbf{N}$.

Example 2: Prove by induction that for all n > 1, n is a product of prime numbers.
Solution: We allow the notion of a "product" of one prime, so prime numbers are automatically covered. Suppose all numbers less than n are products of prime numbers. (This is called the **induction hypothesis**.) If n is prime it is a product of primes. If it is not then n = ab for some numbers a, b with 1 < a, b < n. By the induction hypothesis a, b are each a product of primes, so n = ab is a product of primes. Notice that we could not go from n to n + 1, or n – 1 to n here. The factors a, b will be much smaller than n.

§2.4. Greatest Common Divisors

A fundamental property of the integers is the fact that we can divide one number by another, getting a quotient and a remainder.

Theorem 3: If m, n are integers, where $m \neq 0$, then $n = mq + r$ for some r with $0 \leq r < |m|$.
Proof: Let r be the smallest non-negative integer in the set $S = \{n - mq \mid q \in \mathbf{Z}\}$.
Suppose $r = n - mq \geq |m|$.
If $m > 0$ then this means that $r \geq m$. But $0 \leq r - m = n - m(q + 1) \in S$, contradicting the fact that r is the least.

If $m < 0$ then $|m| = -m$ and so $r \geq -m$. But $0 \leq r + m = n - m(q - 1) \in S$, again contradicting the fact that r is the least.

If the remainder is zero we say that "m" divides "n".

An integer m **divides** and integer n if $n = mq$ for some integer q. We write this as **m | n**. Equivalently we can say that n is a **multiple** of n.

Example 3: 3 divides 12, –17 divides 34, both 1 and –1 divide every number. Despite the maxim "you can't divide by 0" it is true that 0 divides 0, because $0 = 0q$ for all integers q. So $0 \mid 0$, even though $0 \div 0$ is undefined. Make sure you do not confuse $m \mid n$ with m/n or $m \div n$. The symbol $m \mid n$ is a statement. It can only be true or false. But m/n (equivalently $m \div n$) is a number.

We denote the set of divisors of n by D(n) and the set of multiples of n by n**Z**.

Example 4:
$D(12) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$, $12\mathbf{Z} = \{0, \pm12, \pm24, \pm36, \ldots\}$.
$D(1) = \{\pm1\}$, $1\mathbf{Z} = \mathbf{Z}$.
$D(0) = \mathbf{Z}$ (because $n = n.0$ for all n).
$0Z = \{0\}$.
D(n) is finite for all n, except where n = 0.
n**Z** is infinte for all n, except where n = 0.

The set of **common divisors** of m, n is simply $D(m) \cap D(n)$. Associated with this is mZ + nZ which is the set of all numbers of the form mh + nk where $h, k \in \mathbf{Z}$.

Theorem 4: For all integers m, n $m\mathbf{Z} + n\mathbf{Z} = d\mathbf{Z}$ for some $d \in \mathbf{Z}$.
Proof: Let d be the smallest positive element of m**Z** + n**Z**. Then $d = mh + nk$ for some $h, k \in \mathbf{Z}$.
Clearly any multiple of d will belong to m**Z** + n**Z**.
Now let $N = ma + nb \in m\mathbf{Z} + n\mathbf{Z}$. Let r be the remainder on dividing N by d.
That is, $N = ma + nb = dq + r$ for some $q \in Z$ and $0 \leq r < d$.
Now $r = ma + nb - (mh + nk)q = m(a - hq) + n(b - kq) \in m\mathbf{Z} + n\mathbf{Z}$. But d is the smallest positive element of m**Z** + n**Z**, so it must be that r = 0. Hence $N = dq \in d\mathbf{Z}$ and so m**Z** + n**Z** is a subset of d**Z**.

Suppose m, n are non-zero integers. Then $D(m) \cap D(n)$ is finite. An element of this set of largest absolute value is called a **greatest common divisor** of m, n.

Example 5: $D(15) = \{\pm1, \pm3, \pm5, \pm 15\}$ and $D(51) = \{\pm1, \pm3, \pm17, \pm51\}$ so
$D(m) \cap D(n) = \{\pm1, \pm3\}$. The elements with largest absolute value are ±3, so these are both greatest common divisors of 15 and 51.

Theorem 5: If m**Z** + n**Z** = d**Z** then d is a greatest common divisor.
Proof: Let d = mh + nk. If e is a common divisor of m, n then e | d and so d is a greatest common divisor.
Corollary: A GCD of m, n can be expressed in the form mh + nk.

Clearly every pair of non-zero integers has exactly 2 greatest common divisors, ±d.. However, when we refer to **the greatest common divisor** we mean the positive one. We denote this by **GCD(m, n)**. By Theorem 5 GCD(m, n) = mh + nk for

Example 6: GCD(91, 230) = 13, GCD(56, 27) = 1.

Two non-zero numbers m, n are defined to be **coprime** if GCD(m, n) = 1. Loosely speaking we might say that they have "no common factors", but we would really mean is that the only common factors are ±1.

If we divide two numbers by their GCD the quotients will be coprime because we have removed all common factors.

Theorem 6: If d = GCD(a, b) then a/d and b/d are coprime.
Proof: Let $a = a_0 d$ and $b = b_0 d$ and let $e = GCD(a_0, b_0)$. Let $a_0 = a_1 e$ and $b_0 = b_1 e$.
Then $a = a_1 ed$ and $b = b_1 ed$ and so ed is a common divisor of a, b. Since d is the greatest common divisor it must be that e = 1.

There most obvious way of finding the greatest common divisor of two numbers is to factorise each of them. This, however is highly inefficient. Factorising numbers is extremely time consuming, even with the help of a computer, unless the numbers are small. But long before computer the ancient Greeks had devised a very efficient method of finding GCDs.

Euclid's Algorithm:
To find the GCD of two positive numbers:
(1) Divide the smaller into the larger getting a quotient and remainder.
(2) Replace the larger number by this remainder.
(3) While the smaller number is positive go to step (1) and continue.
(4) When the smaller number becomes zero, the larger is the required GCD.

Example 7: Find GCD(1131, 2977).
Solution: You will probably need to use your calculator to check this.
Dividing 1131 into 2977 we get a quotient of 2 and a remainder of 715.
Our two numbers are now 715 and 1131.
Dividing 715 into 1131 we get a quotient of 1 and a remainder of 416.
Our two numbers are now 416 and 715.
Dividing 416 into 715 we get a quotient of 1 and a remainder of 299.
Our two numbers are now 299 and 416.
Dividing 299 into 416 we get a quotient of 1 and a remainder of 117.
Our two numbers are now 117 and 299.
Dividing 117 into 299 we get a quotient of 2 and a remainder of 65.
Dividing 65 into 117 we get a quotient of 1 and a remainder of 52.
Dividing 52 into 65 we get a quotient of 1 and a remainder of 13.
Dividing 13 into 52 we get a quotient of 4 and a remainder of 0.
The last non-zero remainder is 13 and so GCD(1131, 2977).

By the Corollary to Theorem 5 we can express 13 in the form 1131h + 2977k for some numbers h, k.

Example 8: Find integers h, k such that 13 = 1131h + 2977k.
Solution: We work back through the above calculations.
13 = 65 – 52
= 65 – (117 – 65) = 65.2 – 117
= (299 – 117.2).2 – 117 = 299.2 – 117.5
= 299.2 – (416 – 299).5 = 299.7 – 416.5 m
= (715 – 416).7 – 416.5 = 715.7 – 416.12
= 715.7 – (1131 – 715).12 = 715.19 – 1131.12 m
= (2977 – 1131.2).19 – 1131.12 = 2977.19 – 1131.50
So h = –50, k = 19 is one solution.
You must resist the temptation to simplify, except as a check. Keep the two current numbers intact at all times. However at the end you should check that the expression simplifies to the GCD.

Theorem 7: If m|ab and GCD(a, m) = 1 then m|b.
Proof: By Theorem 5, 1 = ah + mk for some h, k ∈ Z and so b = abh + mkb.
Since m|ab, m|b.

§2.5. Prime Numbers

We define a number to be **prime** if it has exactly 2 positive divisors. Note that this rules out ±1. The usual definition of "prime" says that "p is prime if p ≠ ±1 and the only divisors of p are ±1 and ±p", which is equivalent.

Why do we not allow 1 or –1 to be called prime? There is no logical reason why they could not be included. It is just a matter of convenience. The numbers ±1 have special properties and if we included them as primes we would often have to often say "prime number bigger than 1" in our theorems.

Example 7: The prime numbers are ±2, ±3, ±5, ±7, ±11, ±13, ±17, ±19, ±23, ±31, …

Numbers that are not prime, other than the three special numbers –1, 0, and 1, are called **composite**. There are four basic sets of numbers according to this classification.

0	**±1**	**prime numbers**	**composite numbers**

The reason for classifying ±1 in separately to 0 is because they are the only integers that have integer inverses under multiplication.

Theorem 8: If p is prime and p | ab then p|a or p|b.
Proof: Suppose that p is prime and suppose that p dies not divide a. Then GCD(a, p) = 1 and so, by Theorem 6, p|b.

It is a very useful fact that every number can be factorised uniquely into primes. Well, that is not strictly true. Zero cannot be factorised into primes. The number 1 could be factorised into primes if we allowed products with no factors evaluating to 1. But then this would not work for –1. Let us keep to numbers whose absolute value is bigger than 1. Is it true that "every number whose absolute value is bigger than 1 can be factorised uniquely into primes"?. That depends on what we would consider to be a different factorisation.

Example 8: There are 4 factorisations of 6 into primes:
6 = 2.3 = 3.2 = (–2)(–3). We consider all four factorisations to be the one factorisation.

If we allowed 1 and −1 to be primes we would have infinitely many prime factorisations of 6. For example $6 = (-2).3.(-1).1.1.1.(-1)(-1)$.

Theorem 9: (Fundamental Theorem of Arithmetic)
If $|n| > 1$ then $n = p_1p_2 \dots p_h$ for some h and some primes $p_1, p_2, \dots, p_h$.
Moreover if $n = p_1p_2 \dots p_h = q_1q_2 \dots q_k$ then $h = k$ and after suitable rearrangement of the factors $p_i = \pm q_i$ for each i.
Proof: We prove the first part by induction on |n|. Suppose that numbers whose absolute value is smaller than |n| can be factorised into primes.
If n is prime then $h = 1$ and $p_1 = n$.
If n is composite then $n = ab$ for some numbers a, b where |a| and |b| are bigger than 1.
Since |a| and |b| are smaller than |n| it follows by induction that each of a, b can be factorised into primes and hence so can n.

We prove the second part by induction on the number of prime factors, h. Suppose that $p_1p_2 \dots p_h = q_1q_2 \dots q_k$. Then p_1 divides $q_1q_2 \dots q_k$ and so p_1 divides q_j for some j, by Theorem 4. Since q_j is prime and $p_1 \neq \pm 1$, this means that $p_1 = \pm q_j$. Rearranging the factors and dividing by p_1 we get $p_2 \dots p_h = (\pm q_1)q_2 \dots q_k$. By induction $h - 1 = k - 1$ and for each $i \geq 2$, $p_i = \pm q_j$ for some $j \geq 2$.

§2.6. Generating Prime Numbers

There is no known formula for the n'th prime number. At least there are formulae that are so impractical to use they are worse than no formula at all. There is virtually no improvement on the simple-minded approach of testing all factors.

One obvious improvement is the fact that we only need to test for factors up to $\sqrt{n}$.

Theorem 10: If p has no factors n for $2 \leq n \leq \sqrt{p}$ then p is prime.
Proof: If $p = ab$ where $1 < a, b < p$ then one of a, b must be less than or equal to $\sqrt{p}$ (If they were both bigger than $\sqrt{p}$ then ab would be bigger than p.

Another improvement is that if we are generating all primes, by the time we got to p we would have a list of all primes less than p. In that case we only need to test for divisibility by primes up to $\sqrt{p}$. In any case we need never test for divisibility by numbers that are obviously composite, such as even numbers and multiples of 5.

It is useful to be able to recognise multiples of 2, 3 and 5.
Multiples of 2are those numbers that end in 0, 2, 4, 6 or 8.
Multiples of 5 are those numbers that end in 0 or 5.
Multiples of 3 are those numbers where the sum of the digits is a multiple of 3.

Example 9: Is 3197 prime?
Solution: $\sqrt{3197} = 56.542\dots$ so we only need to test by numbers up to 56. But 56, 55 and 54 are clearly composite so in fact we need only go up to 53.
3197 is clearly not divisible by 2, 3 or 5. So, using our calculator we test for 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.

We discover that 23 is a factor and that $3197 = 23.139$.

Example 10: Is 5113 prime?
Solution: $\sqrt{5113} = 71.50\dots$ so we only need to test by numbers up to 71.

5113 is clearly not divisible by 2, 3 or 5. So, using our calculator we test for 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71. Since 5113 is not divisible by any of these it must be prime.

An ancient method for generating primes is known as the sieve of Eratosthenes. It is particularly suitable if you happen to live in an ancient civilization without calculators. You write down a list of all numbers, in order from 2 to some large number. You circle the "2" and then cross out every 2^{nd} number after that.

At each stage you circle the first number that has not been crossed out. That will be a prime number. If is p then cross out every p^{th} number after that. Continue until every number has been circled or crossed out. The circled numbers will be prime and the crossed out ones will be composite.

Example 11: Use the sieve of Eratosthenes to find all the primes up to 100.
Solution:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Notice that as numbers get larger, primes become rarer. In successive groups of 10 the percentage of primes is 40%, 40%, 20%, 20%, 30%, 20%, 20%, 30%, 20%, 10%, giving 25% over the first 100. The percentage of primes up to 1000 drops to 16.8%. In the first 10,000 it is only about 12% and in the first million it is less than 8%. Could it be that primes become so rare that they finish altogether? Is there in fact a largest prime?

Of course there are infinitely many numbers altogether, but even if there were only finitely many primes there would still be infinitely many numbers. After all there are infinitely many powers of 2 and that uses just one prime. This question was asked, answered, a long time ago by the ancient Greeks.

Theorem 11: (Euclid) There are infinitely many primes.
Proof: The simple method of showing that there are infinitely many numbers is to say, "if there is a biggest number just add 1 and you get a bigger one". This does not work because adding 1, or even 2 to a prime does not always give a prime. But we can do something a little bit similar.

Suppose there is a largest prime N. Now take $N! = N(N-1)(N-2)\ldots 3.2.1$. Every prime divides N! because every prime will appear as one of its factors. Now take N! + 1. No prime number will divide it because they all divide N! and no number bigger than 1 can divide two successive numbers. But every number bigger than 1 is divisible by a prime number, so we get a contradiction. Hence there are infinitely many prime numbers.

§2.7. Linear Congruences

Example 12: Find a multiple of 123 that is 231 more than a multiple of 312.
Solution: Expressed algebraically, the problem is to find numbers m, n so that

$$123m = 231 + 312n.$$

We could work through various values of n and divide by 123 until we find a value of n for which 231 + 312n is a multiple of 123. But this might take some time, if indeed there is a solution. We need some better technique than trial and error.

When two numbers a, b differ by a multiple of m we write

$$\mathbf{a \equiv b (mod\ m)}.$$

We say that "**a is congruent to b modulo m**" and m is called the **modulus** for this equation. So we have the following equivalent ways of saying the same thing:

$$a \equiv b (mod\ m)$$
$$a = b + mq \text{ for some } q \in Z$$
$$m \mid (a - b)$$
a, b leave the same remainder when divided by m.

A familiar example of this is when doing calculations with days of the week. If the a^{th} day of the year falls on the same day as the b^{th} then $a \equiv b (mod\ 7)$.

Example 13: If today is Tuesday, on what day of the week will it be in 1000 days time?
Solution: Working modulo 7 we can divide 1000 by 7. We throw away the quotient and hang on to the remainder. With a little calculation we see that the remainder is 6.

Alternatively, if we wanted to do the calculation in our head we could reason as follows. Throw away 700 days. That is a whole number of weeks. That leaves 300. Throw away 280 and we are left with 20. Throw away 14 and we are left with 6.

The day of the week in 1000 days time will be the same as in 6 days time. Before we start counting 6 days forward we realise that $6 \equiv -1 (mod\ 7)$ so the day will be the same as yesterday, that is Monday.

The equation $123m = 231 + 312n$ can be written as $123m \equiv 231 (mod\ 312)$, which has the form $ax \equiv b (mod\ m)$. We can work with congruence equations pretty much like ordinary ones.

Every number is congruent to itself.
If $a \equiv b (mod\ m)$ then $b \equiv a (mod\ m)$.
If $a \equiv b (mod\ m)$ and $b \equiv c (mod\ m)$ then $a \equiv c (mod\ m)$.
If $a \equiv b (mod\ m)$ and $c \equiv d (mod\ m)$ then $a + c \equiv b + d (mod\ m)$ and $ac \equiv bd (mod\ m)$.

You should think through why these are so. The very last is the only one that is not very straightforward.

The important difference between the congruence $ax \equiv b (mod\ m)$ and the equation $ax = b$ is that with the equation, provided $a \neq 0$, we can divide and get the solution $x = a/b$. Things are a little trickier with congruence equations. For a start there may be no solutions.

Example 14: Solve the congruence equation $15x \equiv 7 (mod\ 105)$.
Solution: Written as an equation this becomes $15x = 7 + 105y$. Since 15 and 105 are both divisible by 5 and 7 is not there can be no solutions.

Theorem 12: The congruence $ax \equiv b (mod\ m)$ has a solution if and only if $GCD(a, m) \mid b$.
Proof: Let $d = GCD(a, m)$ and suppose that the congruence has a solution x. Then $ax = b + my$ for some y. Since $d|a$ and $d|m$ it must be that $d|b$.
Conversely suppose that $d \mid b$. Let $b = dq$.
By the corollary to Theorem 5 we may write $d = ah + mk$ for some integers h, k.

Then b = dq = ahq + mkq so a(hq) = b + m(–kq). Consequently x = hq is a solution.to the congruence.

Example 12 (continued):
We wish to solve the congruence 123m ≡ 231(mod 312).
Now 123 = 3.41 and 312 = 3.8.13 so GCD(123, 312) = 3. Since 3|231 there is a solution. But what is it?
We calculate GCD(123, 312) by Euclid's Algorithm, even though we know the answer to be 3.
Dividing 312 by 123 we get a quotient of 2 and a remainder of 66.
Dividing 123 by 66 we get a quotient of 1 and a remainder of 57.
Dividing 66 by 57 we get a quotient of 1 and a remainder of 9.
Dividing 57 by 9 we get a quotient of 6 and a remainder of 3.
Dividing 9 by 3 we get a quotient of 3 and a remainder of 0.

Working back through these calculations we get
3 = 57 – 9.6
= 57 – (66 – 57),6 = 57.7 – 66.6
= (123 – 66).7 – 66.6 = 123.7 – 66.13
= 123.7 – (312 – 123.2).13 = 312(–13) + 123.33
Now 231 = 3.77
= 312(–13).77 + 123.33.77.
Hence 123.(33.77) = 231 + 312.(13.77) ≡ 231(mod 312).
So m = 33.77 = 2541 is a solution to the congruence. The corresponding value of n is 13.77 = 1001. This is not the only solution. m = 2541 + 312s and n = 1001 + 123s is a solution for all s. And even this does not represent the complete solution.

Theorem 14: Let d = GCD(a, m) and let a = a_0d and m = m_0d.
If x_0 is a solution to the congruence equation ax ≡ b(mod m) then the complete solution is
x = x_0 + m_0t for some number t.
Proof: Let a = a_0d and m = m_0d.
Suppose ax_0 ≡ b(mod m) and let ax_0 = b + mq. Let x = x_0 + m_0t.
Then ax = ax_0 + am_0t = b + mq + am_0t = mt so ax ≡ b(mod m).
Suppose ax ≡ b(mod m). Then ax ≡ ax_0(mod m) and so x ≡ x_0(mod m_0).

Example 12 (continued):
The complete solution is m = 2541 + 104t and n = 1001 + 41t.

Theorem 15: ax ≡ ay(mod m) if and only if $x \equiv y \left(\mathrm{mod}\ \frac{m}{GCD(a,m)}\right)$.

Proof: Let d = GCD(a. m) and let a = a_0d and m = m_0d.
Suppose ax ≡ ay(mod m). Then ax = ay + mq for some number q.
Hence $a_0$dx = $a_0$dx + $m_0$dq. Dividing by d we get a_0x = a_0y + m_0q. That is m_0 divides a_0(x – y).
Since GCD(a_0, m_0) = 1, m_0 divides x – y and so x ≡ y(mod m_0).
Conversely if x ≡ y(mod m_0) then m_0 divides x – y and so m = m_0d divides d(x – y) and hence it divides a_0d(x – y) = ax – ay.

The moral of the story is that we are permitted to divide both sides of a congruence by a common factor provided we divide the modulus by the GCD of the modulus and the common factor.

Example 12 (again):
We wish find integers m, n such that 123m = 231 + 312n.
Instead of writing this as 123m ≡ 231(mod 312), we can write it as 312n ≡ −231(mod 123). Clearly we can reduce the numbers 312 and 231 modulo 123, giving 66n ≡ −108(mod 123).
But −108 ≡ 15(mod 123) so we can write the equation as 66n ≡ 15(mod 123).
Dividing by 3 this becomes 22n ≡ 5(mod 41) ≡ 46(mod 41).
Dividing by 2 (this time the modulus does not change since 2 and 41 are coprime) we get
11n ≡ 23(mod 41) ≡ 64(mod 41) ≡ 105(mod 41) ≡ 146(mod 41).
We are continuing to add the modulus until we get a multiple of 11.
11n ≡ 146(mod 41) ≡ 187(mod 41) so n ≡ 17(mod 41).
If we take n = 17 we get 123m = 231 + 312.17 = 5535 so m = 45. This agrees with the previous solution if we take t = −24.
The complete solution is n = 17 + 41t, giving 123m = 231 + 312(17 + 41t) = 5535 + 12792t
so m = 45 + 104t.

This technique of dividing by factors of the coefficient can be quite useful if the coefficient has small factors. But if the coefficient is a large prime it would be very inefficient.

§2.8. The Peano Axioms

The 15 properties given in §2.2 were not proved. They represent facts about the integers and the natural numbers that "everyone knows". Now we cannot prove everything out of nothing. In mathematics we must start with some fundamental axioms. But it would be nice to assume as little as possible.

The following four axioms define the system of natural numbers **N**.

Peano Axioms: N is a set, together with a function S:**N**→**N**. The value of S(n) is called the **successor**. The following axioms are assumed.

(P0) 0 ∈ N.
(P1) There is no n ∈ N for which S(n) = 0.
(P2) S(m) = S(n) implies that m = n.
(P3) If S is a subset of N with the properties:
(i) 0 ∈ S and
(ii) ∀n[n ∈ S → S(n) ∈ S]
then S = N.

Of course we may think of S(n) as being n + 1, but as yet there is no such operation as addition. We must define it. Firstly we can define individual numbers. For example we define 1 as S(0), 2 = S(S(0)), 3 = S(S(S(0))) and so on.

We define addition inductively as follows. For simplicity we write S(n) as n^+.

Addition:
(A0) n + 0 = n.
(A1) n + m^+ = (n + m)$^+$.

Example 15: Prove that 2 + 2 = 4.
Solution: 1 is defined as 0^+, 2 = 1^+, 3 = 2^+ and 4 = 3^+.
2 + 0 = 2 by definition.
2 + 1 = 2 + 0^+ = (2 + 0)$^+$ = 2^+ = 3.
Hence 2 + 2 = 2 + 1^+ = (2 + 1)$^+$ = 3^+ = 4.

Make sure you check that every step follows from the definitions.

For all n, n + 0 = n by (A0). It is natural to expect that 0 + n = n. After all, the addition of numbers is commutative. But we have not yet proved this. So we must prove that 0 behaves as we expect on the left as well as on the right.

Theorem 16: 0 + n = n for all n ∈ **N**.
Proof: We prove this by induction on n. Let S = {n | 0 + n = n}.
0 + 0 = 0 by (A0) so 0 ∈ S.

Suppose that n ∈ S. Then 0 + n = n.
$0 + n^+ = (0 + n)^+$ by A1
$= n^+$ by the induction hypothesis.
Hence $n^+ \in S$. By P3, S = **N**.

Theorem 17: $m + n^+ = m^+ + n$ for all m, n ∈ **N**.
Proof: Induction on n. Let S = {n | $m + n^+ = m^+ + n$ for all m}.
For all m ∈ **N**, $m + 0^+ = (m + 0)^+$ by A1
$= m^+$ by A0
$= m^+ + 0$ by A0. Hence 0 ∈ S.

Suppose that n ∈ S, that is, $m + n^+ = m^+ + n$ for all m.
Then for all m, $m + n^{++} = (m + n^+)^+$ by A1
$= (m^+ + n)^+$ by the induction hypothesis
$= m^+ + n^+$ by A1.
Hence $n^+ \in S$. By P3, S = **N**.

At last we are in a position to prove the commutative law for addition.

Theorem 18: m + n = n + m for all m, n ∈ **N**..
Proof: Induction on n. Let S = {n | m + n = n + m for all m, n ∈ **N**.
For all m ∈ **N**, m + 0 = 0 by A0
= 0 + m by Theorem 16.

Suppose that n ∈ S, that is, m + n = n + m for all m.
Then for all m, $m + n^+ = (m + n)^+$ by A1
$= (n + m)^+$ by the induction hypothesis
$= n + m^+$ by A1
$= n^+ + m$ by Theorem 17.
Hence $n^+ \in S$. By P3, S = **N**.

In a similar way we can prove the associative law for addition, but let us move on to multiplication.

Multiplication:
(M0) n0 = 0.
(M1) $nm^+ = nm + n$.

(M1) makes sense if you remember that ultimately we will recognise nm^+ as n(m + 1).

Theorem 19: $0n = 0$ for all $n \in N$.
Proof: Induction on n. Let $S = \{n \mid 0n = 0\}$.
$00 = 0$ by M0 so $0 \in S$.
Suppose that $n \in S$. Then $0n = 0$.
$0n^+ = 0n + 0$ by M1
$= 0 + 0$ by the induction hypothesis
$= 0$ by A0.
Hence $n^+ \in S$. By P3, $S = \mathbf{N}$.

Theorem 20: $m^+n = mn + n$ for all $m, n \in \mathbf{N}$.
Proof: Induction on n. Let $S = \{n \mid m^+n = mn + n \text{ for all } m\}$.
For all m, $m^+0 = 0$ by M0
$= 0 + 0$ by A0
$= m0 + 0$ by M0 so $0 \in S$.
Suppose that $n \in S$. Then for all m, $m^+n = mn + n$.
For all m, $m^+n^+ = m^+n + m^+$ by M1
$= (mn + n) + m^+$ by the induction hypothesis
$= mn + (n + m^+)$ by the associative law for addition whose proof we omitted
$= mn + (n^+ + m)$ by Theorem 17
$= mn + (m + n^+)$ by Theorem 18
$= (mn + m) + n^+$ by the associative law again
$= mn^+ + n^+$ by M1
Hence $n^+ \in S$. By (P3) $S = \mathbf{N}$.

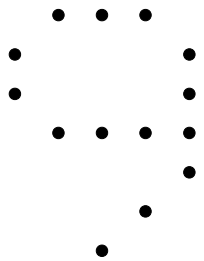
Theorem 21: $mn = nm$ for all $n \in \mathbf{N}$.
Proof: Induction on n. Let $S = \{n \mid mn = nm \text{ for all } m\}$.
For all m, $m0 = 0$ by M0
$= 0m$ by Theorem 19 so $0 \in S$.
Suppose that $n \in S$. Then for all m, $mn = nm$.
For all m, $mn^+ = mn + m$ by M1
$= nm + m$ by the induction hypothesis
$= n^+m$ by Theorem 20.
Hence $n^+ \in S$. By P3, $S = \mathbf{N}$.

By similar methods we can prove the associative law for multiplication, the distributive law and so on. We can define exponentiation inductively and prove the standard properties. Then we can extend our system to include the negative integers and so form the system of integers, with **N** as a subset. We can define subtraction and then we can define $\leq$ by defining $m \leq n$ if $n - m \in \mathbf{N}$. The usual properties of $\leq$ can then be proved. It is a lot of work to develop it fully. But the important point of all this is that we can start by assuming just 4 axioms.

§2.9. Binary Arithmetic

The only place in a computer where you will find the number 9 is on the keyboard. Inside the computer you will only find 0's and 1's. All computer memory consists of electronic "switches" that can be either ON or OFF. We usually represent 0 by a switch being OFF and a 1 by the switch being ON.

All digits, as they are entered, are immediately converted to binary strings. All of the arithmetic performed by a computer is carried out in binary. Only when a final answer is displayed would you again see a "9". And even this is binary, in the sense that the shape of the "9" symbol is displayed by an array of "pixels", tiny dots that can be either ON or OFF.



With the base 10 arithmetic we are used to we use the 10 digits 0 to 9. With base 2 arithmetic, or binary, we only use 0 and 1. We cannot call them digits, because that word suggests our fingers. Instead they are called **bits**.

In base 10 arithmetic, when we reach 9 the next number is written "10". This indicates 1 times 10 plus 0. We then use 2-digits numbers, such as 37. This represents $3 \times 10 + 7$. Finally we reach 99 and if we want to go higher we must use a third digit.

In binary we need to use 2 digits very quickly. The next number after 1 is 10. In binary notation this represents 1 times 2 plus 0. The following number is 11, representing 2 + 1.

The following table displays the first 20 integers in both decimal (base 10) notation and binary (base 2). Examine it carefully.

decimal	**binary**
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011
20	10100

Example 16: Convert 1097 to binary.
Solution: We proceed from right to left.
The last bit, the right-hand bit, is 1 because 1097 is odd.
Subtract this bit and divide by 2. This gives 548. This is even so the next bit is 0.
Subtract this bit and divide by 2. This gives 274. This is even so the next bit is 0.
Subtract this bit and divide by 2. This gives 137. This is odd so the next bit is 1.
Subtract this bit and divide by 2. This gives 68. This is even so the next bit is 0.
So far our binary number is … 01001.

Subtract this bit and divide by 2. This gives 34. This is even so the next bit is 0.
Subtract this bit and divide by 2. This gives 17. This is odd so the next bit is 1.
Subtract this bit and divide by 2. This gives 8. This is even so the next bit is 0.
Subtract this bit and divide by 2. This gives 4. This is even so the next bit is 0.
Subtract this bit and divide by 2. This gives 2. This is even so the next bit is 0.
Subtract this bit and divide by 2. This gives 1. This is odd so the next bit is 1.

This is where we stop. We assemble the sequence of 0's and 1's in reverse order, giving 10001001001.

Example 17: Convert the binary number 10111001011 to decimal.
Solution: Prepare a table with 3 columns. In the left-hand column write down the bits, starting with the right-hand end. In the first row and 2nd column write down 1. Then, going down this row, double each number to get the number in the next row. In the 3rd column copy these powers of 2, but only where there is a 1 in the 1st column. The required number is the sum of all of these numbers.

1	1	1
1	2	2
0	4	
1	8	8
0	16	
0	32	
1	64	64
1	128	128
1	256	256
0	512	
1	1024	1024
TOTAL		**1483**

Addition of numbers in binary is very easy. It follows the same process as addition of numbers. You start with the right hand bits and add. If the sum is 0 or 1 you simply write that down as the right-hand bit of the answer and proceed to the 2nd column (from the right). But if both numbers have a 1 in that column the sum is 2. You must convert this to 10, write down the 0 and "carry" the 1, as you would if you were working in base 10 arithmetic and the sum exceeded 9. This carried bit has to be added to the sum of the bits in the next column.

In the 2nd column you add the two bits and add the carry bit. This time the answer could be 0, 1, 2 or 3. It would be 3 if there were 1's in that column for both numbers and the carry bit was also 1. But you write these as 00, 01, 10 or 11. You put down the right-hand bit of these in your answer and carry the left-hand bit.

Example 18: Calculate 100111 + 11110 in binary.
Solution: We could convert these to decimal and add in the usual way but this is not how a computer would do it.

1	0	0	1	1	1
	1	1	1	1	0

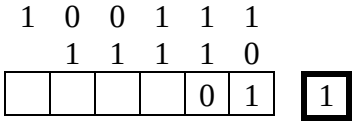
0

The small box to the right contains the carry bit. At the start it is 0.
1 + 0 + 0 = 01. Put down the 0 and carry the 1.

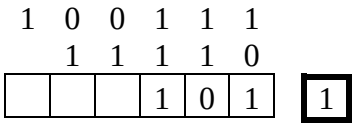
1	0	0	1	1	1
	1	1	1	1	0
					1

0

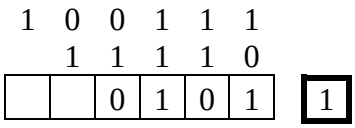
1 + 1 + 0 = 10. Put down the 0 and carry the 1.



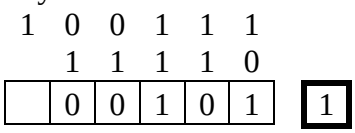
1 + 1 + 1 = 11. Put down the 1 and carry the other 1.



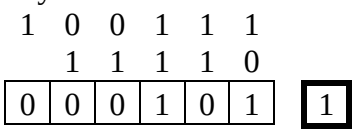
0 + 1 + 1 = 10. Put down the 0 and carry the 1.



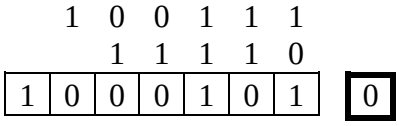
0 + 1 + 1 = 10. Put down the 0 and carry the 1.



1 + 0 + 1 = 10. Put down the 0 and carry the 1.



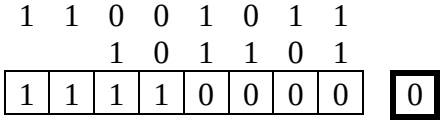
If we had enough memory set aside for these numbers that we could use a 7^{th} column we would continue. 0 + 0 + 1 = 01. Put down the 1 and carry the 0. The process will terminate with the sum in the bottom row.



On the other hand, if we only allowed 6-bit numbers we would have terminated at the previous stage. Because our numbers overflowed the available space the wrong answer will be given, but the fact the carry bit is 1 at the end can be used to trigger an error message.

In practice 16 bits are usually set aside for an integer, allowing for numbers from 0 to 65535 to be represented, but more space can be allocated when larger numbers are used.

Example 19: Calculate 11001011 + 101101 in binary. (Use 8 bits of memory for each integer.)
Solution:



The great thing about binary arithmetic is that it is very easy to learn our multiplication tables. All we need to know is that $0 \times 0 = 0 \times 1 = 0$ and $1 \times 1 = 1$.

Usually with "long multiplication" we accumulate various numbers and we add them at the end.

```
    3 5 7
    2 8 4 ×
  ---------
    1 4 2 8
  2 8 5 6 0
  7 1 4 0 0
---------
1 0 1 3 8 8
```

But on a computer, using binary notation, it is easier to keep a running total. We use three memory registers, one for each of the factors, one for the final answer. We multiply the first number by shifting it to the left in response to reading the bits of the second number.

Example 20: Calculate 1101 × 10011.
Solution: Let us call the three memory registers A, B and C.
At the start A will contain 1101 and B will contain 10011. We show these in a table with 4 rows. In what follows we will show some bits as blank. These will actually contain 0's. It is just that it is easier to follow if cells that are not relevant at a given stage are shown as blank.

```
      1  1  0  1
1  0  0  1  1
```

Because the 1st bit (from the right) of A is 1 we add B to C.

```
      1  1  0  1
1  0  0  1  1
1  0  0  1  1
```

Now we shift B to the left.

```
         1  1  0  1
   1  0  0  1  1
      1  0  0  1  1
```

Since the 2nd bit (from the right) of A is 0 we do NOT add B to C. We shift B to the left.

```
            1  1  0  1
1  0  0  1  1
         1  0  0  1  1
```

Since the 3rd bit (from the right) of A is 1 we add B to C.

```
            1  1  0  1
1  0  0  1  1
1  0  1  1  1  1  1
```

We shift B to the left.

```
               1  1  0  1
1  0  0  1  1
   1  0  1  1  1  1  1
```

Since the 4th bit (from the right) of A is 1 we add B to C.

```
               1  1  0  1
1  0  0  1  1
1  1  1  1  0  1  1  1
```

We have finished. The answer, in C, is 11110001. Let us check this by performing the multiplication in decimal: $13 \times 19 = 247$. The binary equivalent of 247 is 11110111.

§2.10. Applications of Binary Arithmetic

The main application of binary numbers is to computing science, though they do have some applications within mathematics. They also underlie some interesting magic tricks and games.

Guess which number I chose.

There are 7 cards on each of which there are 64 numbers. The magician shows the cards to a volunteer. "Think of a number between 1 and 127. Don't tell me what it is. Now go through these cards and give me those cards where your number appears."

These are the cards:

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
65	67	69	71	73	75	77	79	81	83	85	87	89	91	93	95
97	99	101	103	105	107	109	111	113	115	117	119	121	123	125	127

2	3	6	7	10	11	14	15	18	19	22	23	26	27	30	31
34	35	38	39	42	43	46	47	50	51	54	55	58	59	62	63
66	67	70	71	74	75	78	79	82	83	86	87	90	91	94	95
98	99	102	103	106	107	110	111	114	115	118	119	122	123	126	127

4	5	6	7	12	13	14	15	20	21	22	23	28	29	30	31
36	37	38	39	44	45	46	47	52	53	54	55	60	61	62	63
68	69	70	71	76	77	78	79	84	85	86	87	92	93	94	95
100	101	102	103	108	109	110	111	116	117	118	119	124	125	126	127

8	9	10	11	12	13	14	15	24	25	26	27	28	29	30	31
40	41	42	43	44	45	46	47	56	57	58	59	60	61	62	63
72	73	74	75	76	77	78	79	88	89	90	91	92	93	94	95
104	105	106	107	108	109	110	111	120	121	122	123	124	125	126	127

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

Having collected the cards that contain the chosen number from the volunteer, the magician merely adds the numbers in the top-left corner to reveal the chosen number. For example, if the

volunteer chose 77she would choose the cards with 1, 4, 8 and 64 at the top left. The magician adds these: 1 + 4 + 8 + 64 = 77.

The trick is based on the fact that the first card lists all those numbers whose binary expressions have a 1 in the 1st place (counting from the right), the 2nd card lists all those with a 1 in the 2nd place, and so on. So from the choice of cards we get the binary representation of the chosen number. In our example it would be 1001101. But we do not have to do too much mental arithmetic because the appropriate powers of 2 are listed in the top-left corner of the cards.

To make the trick a little more mystifying one should jumble the numbers. But the powers of 2 should still be in a uniform position, perhaps in the bottom-right corner. Also with the numbers going up to 127 it might give the game away that it has something to do with powers of 2. Instead it would be a good idea to only list numbers up to 99, even though this would mean that some cards would have fewer numbers than others.

The Game of Nim:

This is a game between two players. Place several piles of matches on the table. The piles should contain different numbers of matches to start with. Players alternate their moves. At each move a player must take 1 or more matches from one of the piles (they can take a whole pile if they wish, or as little as 1 match). The player who takes the last match wins.

There is a simple strategy based on binary numbers which give you a very high probability of winning, irrespective of whether you go first or second. You would only lose by a fluke, unless the other player is using the same strategy.

The trick is to record the numbers of matches in the piles in binary, with these binary representations being written one under the other.

For example, suppose we have 5 piles, containing 11, 8, 12, 10 and 4 matches. We write the binary representations of these numbers as follows.

1	0	1	1
1	0	0	0
1	1	0	0
1	0	1	0
0	1	0	0

The strategy is to leave an even number of 1's in each column. If it is your turn you should take 1 match from the 1st pile. This leaves piles of 10, 8, 12, 10 and 4 matches.

1	0	1	0
1	0	0	0
1	1	0	0
1	0	1	0
0	1	0	0

Suppose your opponent takes 5 matches from the 4th pile. The table is now as follows.

1	0	1	1
1	0	0	0
1	1	0	0
0	1	0	1
0	1	0	0

We need to remove a 1 from the left column, so we take matches from one of the first three piles. Suppose we take from the 1st pile. To give an even number of 1st in each column we need to change the 1st row to 0101. That is, we want to leave 5 matches in the 1st pile and so we take 5 matches from the 1st pile.

The table is now:

0	1	0	1
1	0	0	0
1	1	0	0
0	1	0	1
0	1	0	0

Suppose our opponent takes the whole of the 5th pile. The table is now:

1	0	1	1
1	0	0	0
1	1	0	0
1	0	1	0
0	0	0	0

We must change something in the 2nd column, and we cannot change a 0 into a 1 because that would mean adding matches back to a pile – something that is not allowed. So we must remove the 1 from the 3rd row. To fix up the last column we must change the 0 into a 1. So the 3rd pile must be left with 1001 matches (in binary), or 9 matches. We must therefore take 3 matches from the 3rd pile.

If you leave the piles so that this binary table has an even number of 1's in every column then your opponent cannot achieve this since he is required to take at least one match. So no matter what he does he must always leave at least one match. You will be sure of taking the last match and so win.

§2.11. Arithmetic Modulo m

When we do calculations with days of the week we use a system that is called the system of integers modulo 7, or $\mathbf{Z}_7$ for short. This is a system in which we throw away multiples of 7 (whole weeks) and only keep remainders after division by 7.

Today is Thursday. What day of the week will it be in 8 days time? Clearly it will be a Friday. We do not count forward 8 days. We simply recognise that in 7 days time it will still be a Thursday, so 8 days will bring us to a Friday. In 72 days time it will be a Saturday. We can ignore 70 of the 72 days because they represent so many whole weeks. We simply count 2 days forward from today.

What day of the week will it be in 1000 days time? Dividing 1000 by 7 we get a quotient of 142 with a remainder of 6. Actually the quotient is unimportant, only the remainder. So if we were doing the calculation in our head, and we were feeling particularly lazy, we might say something like this. "Throw away 700 to get 300. Now discard 280, leaving 20. Take off 14 and this leaves us with 6." We simply subtract suitable multiples of 7 repeatedly until we get an answer in the range 0 to 6.

Having discovered that it will be the same day of the week in 6 days time as it will be in 1000, what then? Would we count forward 6 days from today? Not if we were particularly lazy. We would realise that in 6 days time it will be the same day of week as it was yesterday. If today is Thursday our answer is Wednesday. In the system of days of the week 6 days forward is the same as one day back.

The mathematical system that underlies all this is the system $\mathbf{Z}_7$. It consists of 7 numbers 0, 1, 2, 3, 4, 5 and 6. These numbers may look like integers but they are not. For if we add the integers 5 and 4 we get 9, but if we add the numbers 5 and 4 in this $\mathbf{Z}_7$ system we get 2. Five days from now plus a further 4 days brings us to the same day of the week as it will be in 2 days time.

You could take the view that 5 + 4 is 9 but in the system $\mathbf{Z}_7$ the symbol 9 is just another name for 2 since they differ by 7. The important thing, however, is that we quote our final answer using the standard names for these numbers, that is one of the symbols 0, 1, 2, 3, 4, 5 or 6.

To avoid confusing calculations in the mod 7 system with those for ordinary integers we often add a note to remind us that our result is valid for the mod 7 system. So we might write $5 + 4 \equiv 2 (\text{mod } 7)$. However if we are doing a lot of calculations in $\mathbf{Z}_7$ we can simply announce that we are working in that system and simply write $5 + 4 = 2$.

The system $\mathbf{Z}_7$ is in many ways a miniature version of the integers. We can add and multiply any two numbers in the system and our answer will be one of the 7 numbers in the system. We can describe the workings of the system $\mathbf{Z}_7$ by setting out its addition and multiplication tables.

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Examine these tables and look for patterns.

Note that the entries in the body of each table are all in the set {0, 1, 2, 3, 4, 5, 6}. We describe this by saying that:

$\mathbf{Z}_7$ is *closed under addition and multiplication*.

Secondly both tables are symmetric about the (top-left to bottom-right) diagonal. We describe this by saying that addition and multiplication in $\mathbf{Z}_7$ are commutative. That is:

for all numbers x and y in the system, $x + y = y + x$ and $xy = yx$.

Note that each table has a row that is identical with the numbers above the table. This reflects the fact that there are numbers in the system that have no effect when they are added to or multiplied by any number. These numbers are called the "identities". The additive identity is the number 0 and the multiplicative identity is the number 1. The special properties of these numbers are described by the statements:

for any x in the system $0 + x = x = x + 0$ and
$1x = x = x1$.

Something that you would not notice just by casual observation, are the associative laws:

for any x, y and z in the system $x + (y + z) = (x + y) + z$ and
$x(yz) = (xy)z$.

In the addition table every one of the 7 numbers appears in each row and column. This allows subtraction to be possible. What is 2 – 5? It should mean "that number which when added to 5 gives 2". We look along the 5 row until we reach a 2. The fact that every number appears in every row and column guarantees that we'll find a 2. There it is in the "4" column. So 5 + 4 = 2 and hence 2 – 5 = 4.

In particular the number 0 appears in each row and column. That is:

for every number x there is a number y such that x + y = 0 = y + x.

We denote this additive inverse of x by y = –x. The following table gives the additive inverses of all the elements of $\mathbf{Z}_7$.

x	0	1	2	3	4	5	6
–x	0	6	5	4	3	2	1

When it comes to multiplication things are just a little different. The first row and column consist entirely of 0's. But if we focus our attention on the non-zero part we get every non-zero number appearing exactly once in each row and column. This allows us to divide in this system, provided we do not want to divide by zero.

What is 3/5 in $\mathbf{Z}_7$? In other words, what number when multiplied by 5 gives 3? We look along the "5" row until we find a 3. We are guaranteed to find a 3 because every number occurs exactly once in the 5 row. There it is, in the "2" column. So 5.2 = 3 and hence 3/5 = 2.

In particular the number 1 appears in each row and column (apart from the 0 one). That is:

for every non-zero number x there is a number y such that xy = 1 = yx.

We denote this multiplicative inverse of x by $y = x^{-1}$. The following table gives the multiplicative inverses of all the non-zero elements of $\mathbf{Z}_7$.

x	1	2	3	4	5	6
$\mathbf{x^{-1}}$	1	4	5	2	3	6

The advantage of having only a finite number of numbers in our mini number system, $\mathbf{Z}_7$, is that we can describe any function from $\mathbf{Z}_7$ to $\mathbf{Z}_7$ by means of a table of values. Above we have the table for $f(x) = x^{-1}$. What about some other powers?

x	1	2	3	4	5	6
$\mathbf{x^2}$	1	4	2	2	4	1
$\mathbf{x^3}$	1	1	6	1	6	6
$\mathbf{x^4}$	1	2	4	4	2	1
$\mathbf{x^5}$	1	4	5	2	3	6

Notice that we do not need a calculator to complete this table. We simply multiply each row by the first to get the next. So there is no need to compute 5^5, for example. We simply multiply 5^4 by 5, that is, 2 times 5 which, mod 7, is 3.

Now something rather remarkable happens when we compute the next power.

x	1	2	3	4	5	6
$\mathbf{x^6}$	1	1	1	1	1	1

So $x^6 \equiv 1 \pmod 7$ for all non-zero $x \in \mathbf{Z}_7$. You may wonder why we would ever want to raise days of the week to powers. The answer is that we would not. Doing calculations with the calendar is just one of the more elementary applications of these finite mathematical systems. A much more important application is to the science of cryptography, the science of secret codes. Transmitting information securely is no longer only of interest to secret agents and the military. It is of vital interest to business. But of course 7 is much too small a number for these purposes. What we have done for 7 can be done for any modulus.

For any positive integer, m, the system of integers mod m is the set {0, 1, 2, ... , m–1} with addition and multiplication carried out **modulo m**, that is, the result of adding or multiplying two of these elements is adjusted to give one of these m numbers by subtracting a suitable multiple of m. More formally we add or multiply in the usual way but then take the remainder on dividing by m.

The smallest of these is $\mathbf{Z}_1$ but as this contains just one number 0 with 0 + 0 = 0 and 0.0 = 0 it is not of much use. The smallest useful example is $\mathbf{Z}_2$, the integers modulo 2. Here we have just two numbers 0 and 1. They combine just as they normally do in integer arithmetic with one exception: 1 + 1 = 0. Here are the full addition and multiplication tables for $\mathbf{Z}_2$.

+	**0**	**1**
0	0	1
1	1	0

×	**0**	**1**
0	0	0
1	0	1

Incidentally, notice that these tables have the same patterns as the addition and multiplication tables for the entities "odd" and "even". If you consider 0 as representing "even" and 1 representing "odd" then 1 + 1 = 0 is simply recording the fact that "odd plus odd is even".

No wonder $\mathbf{Z}_2$ is sometimes called "dunces arithmetic". Apart from having very little to learn by way of one's tables, a dunce could get 50% of the answers in an arithmetic test correct just by guessing!

But surely $\mathbf{Z}_7$ is far too simple a mathematical system to be of any practical use. For cryptography it is, but there is another sort of code – the error-correcting code. Here the goal is not to conceal the message but to compensate for a small number of errors that can creep in when a message is transmitted electronically. Here $\mathbf{Z}_2$ is admirably suited because every message transmitted electronically is just a long string of 0's and 1's.

Let's try $\mathbf{Z}_8$, the system of integers mod 8. Here are its addition and multiplication tables.

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	5	7	0
2	2	3	4	5	5	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Notice that the above addition table is very similar to the one for $\mathbf{Z}_7$. Each row is identical to the one above but moved one place to the left, with the number that falls of the left-hand edge "wrapping around" to the right-hand end. But with multiplication the pattern is very different. With $\mathbf{Z}_7$ the non-zero entries were uniformly distributed with each one appearing in every row and column in the non-zero part of the table. But with $\mathbf{Z}_8$ 2's, 4's and 6's occur more frequently than 1's, 3's, 5's and 7's and 0's creep into the non-zero part of the table (for example $2 \times 4 = 0$ even though neither 2 nor 4 is zero).

The system $\mathbf{Z}_7$ behaves much more like the arithmetic we are used to than it does to $\mathbf{Z}_8$. In $\mathbf{Z}_7$ the cancellation law:

$$\textit{If } xy = 0 \textit{ then } x = 0 \textit{ or } y = 0$$

is valid. In $\mathbf{Z}_8$ it is not.

The lack of the cancellation law in $\mathbf{Z}_8$ turns our normal notions of algebra on their head. Take the solution of quadratic equations. A quadratic cannot have more than two solutions, right? Wrong! At least for $\mathbf{Z}_8$ it is wrong. Take the quadratic equation $x^2 - 1 = 0$.

Solving, we get $(x - 1)(x + 1) = 0$. So far so good, even in $\mathbf{Z}_8$. But as soon as we try to say "hence $x - 1 = 0$ or $x + 1 = 0$" we have transgressed in $\mathbf{Z}_8$ because this last step appeals to the cancellation law which is just not true in $\mathbf{Z}_8$.

In fact the quadratic $x^2 - 1 = 0$ has as many as *four* solutions in $\mathbf{Z}_8$ as is shown by the following table of squares.

x	0	1	2	3	4	5	6	7
$\mathbf{x^2}$	0	1	4	1	0	1	4	1

So why is the arithmetic and algebra of $\mathbf{Z}_8$ so different to that of $\mathbf{Z}_7$? The difference is simply due to the fact that 7 is prime and 8 is not.

Definition: The **Cancellation Law** states that:

If $xy = 0$ then $x = 0$ or $y = 0$.

An equivalent statement is:

If $a \neq 0$ and $ax = ay$ then $x = y$.

[For $ax = ay$ is equivalent to $a(x - y) = 0$.]

While the Cancellation Law holds in ordinary arithmetic it fails to hold in many algebraic systems. For example it does not hold for matrices.

Example 21: The Cancellation Law does not hold in $\mathbf{Z}_{100}$ since $10.10 = 0$ in Z_{100} while $10 \neq 0$ in that system.

Theorem 22: If $p > 1$, the Cancellation Law holds in $\mathbf{Z}_p$ if and only if p is prime.
Proof: Suppose the modulus p is not prime. Then $p = ab$ for some a, b with $0 < a, b < p$. Then in $\mathbf{Z}_p$, $ab = 0$ while $a \neq 0$ and $b \neq 0$ and so the cancellation law fails. In other words if the cancellation law holds in $\mathbf{Z}_p$ then p must be prime.

Now suppose that p is prime and suppose that in $\mathbf{Z}_p$, $ab = 0$ where $a \neq 0$. Hence in $\mathbf{Z}$, ab is divisible by p but a is not. Hence p divides b. In $\mathbf{Z}_p$ this translates to $b = 0$.

§ 2.12. Inverses in Z_m

For many applications it is important to be able to find an inverse in $\mathbf{Z}_m$ where one exists. The elements that have inverses are called "units".

A **unit** of $\mathbf{Z}_m$ is any element of $\mathbf{Z}_m$ that has an inverse under multiplication.

Theorem 23: Any product of units is a unit.
Proof: It is sufficient to prove this for a product of two units.
Since $(b^{-1}a^{-1})(ab) = 1$ it is clear that ab has an inverse.

The special property of units is that it is always possible to cancel them in equations.

Theorem 24: If a is a unit of $\mathbf{Z}_m$ and $ax = ay$ then $x = y$.
Proof: If $ax = ay$ and "a" is a unit then $a^{-1}(ax) = a^{-1}(ay)$ and so $x = y$.

Theorem 25: $a \in \mathbf{Z}_m$ is a **unit** if and only if $(a, m) = 1$.
Proof: Suppose that "a" is a unit of $\mathbf{Z}_m$. Then for some $b \in \mathbf{Z}_m$, $ab = 1$.
In $\mathbf{Z}$ this becomes $ab = 1 + mq$ for some $q \in Z$.
Let $d = (a, m)$. Then, since d divides both a and m it follows that d divides 1.

Suppose now that (a, m) = 1.
Then 1 = ah + mk for some h, k ∈ **Z**.
In $\mathbf{Z}_m$ this becomes 1 = ah, so a has an inverse, namely h.

We can find inverses modulo m by working out the greatest common divisor by the Euclidean algorithm and then working backwards to express 1 in the form ab + mc.

Example 22f: Find the inverse of 35 modulo 143.
Solution:

4	11	1
35) 143	3) 35	2) 3
140	33	2
3	2	1

So 1 = 3 – 2
= 3 – (35 – 3.11) = 3.12 – 35
= (143 – 35.4).12 – 35 = 143.12 – 35.49.
Hence 35(–49) ≡ 1(mod 143). So the inverse of 35 modulo 143 is –49 = 94.

§ 2.13. Powers in $\mathbf{Z}_m$

Consider the geometric progression 1, x, x^2, x^3, ... for some x ∈ $\mathbf{Z}_m$. Since $\mathbf{Z}_m$ is finite we must get repetitions. And once one power is equal to an earlier one the same block of numbers simply repeats.

For example in $\mathbf{Z}_{10}$, the powers of 3 are 1, 3, 9, 7, 1, 3, 9, 7, ... The powers of 2 are 1, 2, 4, 8, 6, 2, 4, 8, 6, ...

This simple fact enables us to answer questions in our head that would appear to require enormous amounts of computation.

Example 23: What is the final digit in 7^{1995}?
Solution: There's no need to compute the complete value of 7^{1995}. In any case to do so would require more than a normal calculator. But computing the first few powers of 7 modulo 10, until we get a repetition, we have:

n	0	1	2	3	4
$\mathbf{7^n}$	1	7	9	3	1

Since in $\mathbf{Z}_{10}$, $7^4 = 1$ then 7 to any multiple of 4 will give 1 in $\mathbf{Z}_{10}$. So we need only find the remainder on dividing 1995 by 4. Now 1995 = 498.4 + 3, so $7^{1995} = (7^4)^{498}.7^3 = 7^3 = 3$ in $\mathbf{Z}_{10}$. Hence 7^{1995} ends in a 3.

The following Theorem is known as Fermat's "Little" Theorem. This is to distinguish it from his celebrated "Last Theorem". Fermat's Last Theorem states that for all integers n ≥ 3 there are no solutions to the equation $x^n + y^n = z^n$ for non-zero integers x, y and z.

We all know that $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. There infinitely many such integer solutions to the equation $x^2 + y^2 = z^2$. But when it comes to n = 3, or any larger value of n, the situation is quite different.

There are, of course, trivial solutions such as $0^n + 1^n = 1^n$ but no non-trivial solutions. It was proved for n = 3 a long time ago, and over the years for larger and larger values of n. But it wasn't until the late 20th century that it was proved that there are no non-trivial solutions for *all* n.

Fermat claimed to have proved this theorem 350 years ago in a note in one of his books but claimed "the margin is too small to contain it". There has been much controversy as to whether he really did have a complete proof, but as it took over 350 years for such a proof to be found, and since this proof required whole tracts of mathematics that were not developed until the late 20th century, the consensus seems to be that he only thought he had a proof.

His "Little" Theorem, on the other hand, is one that he is known to have proved. Many other proofs have since appeared. Here are three of them.

Theorem 26: (Fermat) If p is prime and "a" is a not a multiple of p then $a^{p-1} \equiv 1 (\text{mod } p)$.
Proof: #1: We prove by induction on "a" that for all $a \geq 1$, $a^p \equiv a (\text{mod } p)$.
If a = 1 the result is clearly true so suppose now that it is true for "a". Then by the Binomial Theorem, $(a + 1)^p = a^p + pa^{p-1} + \frac{1}{2}p(p - 1)a^{p-2} + ... + 1$. Since p is prime, all the binomial coefficients, except the first and the last, are multiples of p, so mod p:

$$(a + 1)^p \equiv a^p + 1 \equiv a + 1 \text{ (mod p) by the induction hypothesis.}$$

Hence the result holds for a + 1. To get from $a^p = a$ to $a^{p-1} = 1$ we use the Cancellation Law.

Proof #2: (For those who know a little group theory) Since p is prime the non-zero elements of $\mathbf{Z}_p$ form a group under multiplication. By Lagrange's Theorem the order of each element of this group divides p – 1, the order of the group. Hence $a^{p-1} = 1$ for all non-zero $a \in \mathbf{Z}_p$.

Proof #3: Let N = 1.2.3 … (p –1). Clearly p doesn't divide N and so in $\mathbf{Z}_p$, $N \neq 0$.
In the remainder of the proof we interpret everything as elements of $\mathbf{Z}_p$.
Multiply each of the factors of N by "a".

Hence $a^{p-1}N = a.2a.3a. \ldots .(p-1)$.
By the cancellation law, no two of these factors are equal, so they must be all the non-zero elements in some order. Hence the right hand side of the above equation is N.

So $a^{p-1}N = N$ and since $N \neq 0$ it follows by the Cancellation Law that $a^{p-1} = 1$.

Example 24: p = 7
N = 1.2.3.4.5.6
$2^6N = 2.4.6.1.3.5 = N$
$\therefore 2^6 = 1$ in $\mathbf{Z}_7$.
Note that in this example $N = 720 \equiv -1 (\text{mod } 7)$. This holds for all primes p.

EXERCISES FOR CHAPTER 2

Exercise 1: Factorise 2926 into prime factors.

Exercise 2: Factorise 713 into primes.

Exercise 3: Show that 659 is prime.

Exercise 4: Find the first prime after 1000.

Exercise 5: Find the GCD of 11111 and 3403.

Exercise 6: Find the GCD of 10101 and 5019.

Exercise 7: Solve the congruence equation $100x \equiv 26 (\text{mod } 42)$.

Exercise 8: Solve the congruence equation $101x \equiv 26 (\text{mod } 142)$.

Exercise 9: Solve the congruence equation $2018x \equiv 4 (\text{mod } 5000)$.

Exercise 10: Find the inverse of 18 in Z_{175}.

Exercise 11: Find the inverse of 31 in $\mathbf{Z}_{1001}$

Exercise 12: Find 5^{127} in $\mathbf{Z}_{13}$.

Exercise 13: Find 17^{1000} in $\mathbf{Z}_{37}$.

SOLUTIONS FOR CHAPTER 2

Exercise 1: 2926 = 2.1463.
We now try dividing 1463 by 3, 5, 7, 11, …and discover that it is exactly divisible by 7.
So 2926 = 2.7.209 = 2.7.11.19.

Exercise 2: We try dividing by the primes 3, 5, 7, 11, …and eventually discover that
713 = 23.31.

Exercise 3: $\sqrt{659} = 25.6\ldots$ so we only need to check for divisibility by primes up to 23.
Since none of these primes divide 659 we can conclude that 659 is prime.

Exercise 4: $\sqrt{1000} = 31.6$ so we will only need to check for prime divisors up to 31 (unless it turned out that there are no primes between 1000 and $33^2 = 1089$).
1001 = 7.143
1003 = 17.59
1007 = 19.53
1009 is prime.

Exercise 5:

3	3	1	3	2	5
3403)11111	902)3403	697)902	205)697	82)205	41)205
10209	2706	697	615	164	205
902	697	205	82	41	0

The last non-zero remainder is 41. Hence the GCD of 11111 and 3403 is 41.

Exercise 6: 10101 = 5019*2 + 63
5019 = 63*79 + 42
79 = 42 + 37
42 = 37 + 5
37 = 5*7 + 2
5 = 2*2 + 1
So GCD(10101, 5019) = 1.

Exercise 7: Suppose $100x \equiv 26 \pmod{42}$.
$\therefore\ 16x \equiv 26 \pmod{42}$ (since $100 \equiv 16 \pmod{42}$)
$\therefore\ 8x \equiv 13 \pmod{21}$
$\equiv 34 \pmod{21}$
$\therefore\ 4x \equiv 17 \pmod{21}$
$\equiv 38 \pmod{21}$
$\therefore\ 2x \equiv 19 \pmod{21}$
$\equiv 40 \pmod{21}$
$\therefore\ x \equiv 20 \pmod{21}$

Exercise 8: The method used in exercise 2 is not suitable because 101 has no small divisors, in fact it is prime. In this case we use the general method, which is to find GCD(101, 142). Of course, since 101 is prime, it will be 1, but we carry out the calculations anyway because we need the details.

$142 = 101.1 + 41$
$101 = 41.2 + 19$
$41 = 19.2 + 3$
$19 = 3.6 + 1$
$\therefore 1 = 19 - 3.6$
$= 19 - (41 - 19.2).6 = 19.13 - 41.6$
$= (101 - 41.2).13 - 41.6 = 101.13 - 41.32$
$= 101.13 - (142 - 101).32 = 101.45 - 142.32$

Hence $101.45 \equiv 1 \pmod{142}$ and so
$101.(45.26) \equiv 26 \pmod{142}$.
So the solution is $x \equiv 45.26 \pmod{142}$
$\equiv 1170 \pmod{142}$
$\equiv 34 \pmod{142}$.

Exercise 9: Suppose $2018x \equiv 4 \pmod{5000}$.
Then $1009x \equiv 2 \pmod{2500}$.
$2500 = 1009.2 + 482$
$1009 = 482.2 + 45$
$482 = 45.10 + 32$
$45 = 32 + 13$
$32 = 13.2 + 6$
$13 = 6.2 + 1$
$\therefore 1 = 13 - 6.2$
$= 13 - (32 - 13.2).2 = 13.5 - 32.2$
$= (45 - 32).5 - 32.2 = 45.5 - 32.7$
$= 45.5 - (482 - 45.10).7 = 45.75 - 482.7$
$= (1009 - 482.2).75 - 482.7 = 1009.75 - 482.157$
$= 1009.75 - (2500 - 1009.2).157 = 1009.389 - 2500.157$

Hence $1009.389 \equiv 1 \pmod{2500}$ and so $1009.778 \equiv 2 \pmod{2500}$.
The solution to the congruence equation is thus $x \equiv 778 \pmod{2500}$.

Exercise 10:
$175 = 18.9 + 13$
$18 = 13 + 5$
$13 = 5.2 + 3$
$5 = 3 + 2$
$3 = 2 + 1$
$\therefore 1 = 3 - 2$
$= 3 - (5 - 3) = 3.2 - 5$
$= (13 - 5.2).2 - 5 = 13.2 - 5.5$
$= 13.2 - (18 - 13).5 = 13.7 - 18.5$ (Note, we only substitute for one of the 5's.)
$= (175 - 18.9).7 - 18.5 = 175.7 - 18.68$

Hence $18.(-168) = 1 \pmod{175}$.
So the inverse of 18 in Z_{175} is $-168 = 7$.

Exercise 11:
$1001 = 31.32 + 9$
$31 = 9.3 + 4$
$9 = 4.2 + 1$
$\therefore\ 1 = 9 - 4.2$
$= 9 - (31 - 9.3).2 = 9.7 - 31.2$
$= (1001 - 31.32).7 - 31.2 = 1001.7 - 31.\ 226$
Hence $31(-226) = 1$ in $\mathbf{Z}_{1001}$ so the inverse is $-226 = 775$.

Exercise 12: 13 is prime and 5 is not divisible by 13.
Hence, be Fermat's Little Theorem, $5^{12} = 1$ in Z_{13}.
Hence $5^{120} = 1$ and so $5^{127} = 5^7 = 78125 = 8$.
Note: We could have obtained 5^7 without the aid of a calculator as follows:
$5^2 = 25 = 12 = -1$ in Z_{13}.
Hence $5^4 = 1$.
Hence $5^7 = 5^4.5^2.5 = -5 = 8$.
This technique, of breaking up the power into powers of 2, is useful when we have to compute a very large power, too large for our calculator.

Exercise 13: In $\mathbf{Z}_{37}$, $17^{36} = 1$.
Now $1000 = 36.27 + 28$.
Hence, in $\mathbf{Z}_{37}$ $17^{1000} = 17^{28}$.
$17^2 = 289 = 30$ in $\mathbf{Z}_{37}$.
$17^4 = 30^2 = 900 = 12$.
$17^8 = 12^2 = 144 = 33$.
$17^{16} = 33^2 = 1089 = 16$.
Hence $17^{28} = 17^{16}.17^8.17^4$
$= 16.33.12$
$= 6336$
$= 9$.