2. LINEAR CONGRUENCES

§2.1. The Ring of Integers Modulo *m*

When we do calculations with days of the week can 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 don't have to 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'd 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.

We define $\mathbb{Z}_m = \{0, 1, 2, ..., m - 1\}$ and add and multiply its elements as we would for integers, except that we take the remainder of our calculations after dividing by m. We call this reducing the answer **modulo m**, or **mod *m*** for short. So modulo 7, $3 + 5 = 8 = 1$ and $4.6 = 24 = 3$.

We will investigate the properties of these systems for various values of m. They behave rather like the integers themselves, though with some important differences. Many of these properties can be summarised by calling them ‘rings’.

We can describe the workings of the system $\mathbb{Z}_7$ 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:

$\mathbb{Z}_7$ 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 $\mathbb{Z}_7$ 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's 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 $y = \mathbf{-x}$. The following table gives the additive inverses of all the elements of $\mathbb{Z}_7$.

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 don't want to divide by zero.

What is 3/5 in $\mathbb{Z}_7$? In other words, what number when multiplied by 5 gives 3? We look along the '5' row until we find a 3. We're guaranteed to find a 3 because every non-zero 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 $y = \boldsymbol{x^{-1}}$. The following table gives the multiplicative inverses of all the non-zero elements of $\mathbb{Z}_7$.

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, $\mathbb{Z}_7$, is that we can describe any function from $\mathbb{Z}_7$ to $\mathbb{Z}_7$ 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 don't 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 $x^6 = 1$ for all non-zero $x \in \mathbb{Z}_7$. You may wonder why we would ever want to raise days of the week to powers. The answer is that we wouldn't. 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's of vital interest to business. But of course 7 is much too small a number for these purposes. What we've done for 7 can be done for any modulus.

The smallest of these rings is $\mathbb{Z}_1$ but as this contains just one number 0 with 0 + 0 = 0 and 0.0 = 0 it isn't of much use. The smallest useful example is $\mathbb{Z}_2$, 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 $\mathbb{Z}_2$.

+	**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 $\mathbb{Z}_2$ is sometimes called "dunce's arithmetic". Apart from having very little to learn by way of one's tables, a dunce could get 50% of the answers correct in an arithmetic test just by guessing!

But surely $\mathbb{Z}_2$ is far too simple a mathematical system to be of any practical use. For cryptography it is, but there's 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 $\mathbb{Z}_2$ is admirably suited because every message transmitted electronically is just a long string of 0's and 1's.

A very simple error-correcting system is to transmit data in bytes, that is, binary strings of length 8. Here the first 7 bits (a bit is simply a 0 or 1) contain the information and the 8^{th} bit is a *check bit*. This is a 0 or 1 that makes the entire byte have an even number of 1's. Then, if one of the bits gets transmitted wrongly, the byte would have an odd number of 1's and the error would be detected. The computer could ask for the byte to be retransmitted. But in many circumstances it isn't feasible to retransmit. There are more sophisticated systems whereby errors are not only detected but can be corrected, provided the errors aren't too frequent. This is discussed in a chapter in my *Languages and Machines* notes.

Let's try $\mathbb{Z}_8$, 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 $\mathbb{Z}_7$. Each row is identical to the one above but moved one place to the left, with the number that falls off the left-hand edge ‘wrapping around’ to the right-hand end. But with multiplication the pattern is very different. With $\mathbb{Z}_7$ the non-zero entries were uniformly distributed with each one appearing once in every row and column in the non-zero part of the table. But with $\mathbb{Z}_8$ 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 $\mathbb{Z}_7$ behaves much more like the arithmetic we're used to than does $\mathbb{Z}_8$. In $\mathbb{Z}_7$ the cancellation law:

$$\text{if } xy = xz \text{ and } x \neq 0 \text{ then } y = z$$

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

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

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

In fact the quadratic $x^2 - 1 = 0$ has as many as *four* solutions in $\mathbb{Z}_8$ 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 $\mathbb{Z}_8$ so different to that of $\mathbb{Z}_7$? The difference is simply due to the fact that 7 is prime and 8 is not.

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 $x = y$.

[Because $ax = ay$ 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 doesn't hold for matrices.

Example 1: The Cancellation Law doesn't hold in $\mathbb{Z}_{100}$ since $10.10 = 0$ in $\mathbb{Z}_{100}$ while $10 \neq 0$ in that system.

Theorem 1: If $p > 1$, the Cancellation Law holds in $\mathbb{Z}_p$ 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 $\mathbb{Z}_p$, $ab = 0$ while $a \neq 0$ and $b \neq 0$ and so the cancellation law fails. In other words if the cancellation law holds in $\mathbb{Z}_p$ then p must be prime.

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

§ 2.2. Inverses in $\mathbb{Z}_m$

For many applications it's important to be able to find a multiplicative inverse in $\mathbb{Z}_m$ where one exists. The elements that have inverses are called 'units'. A **unit** of $\mathbb{Z}_m$ is any element of $\mathbb{Z}_m$ that has an inverse under multiplication.

Theorem 2: Any product of units is a unit.
Proof: It's sufficient to prove this for a product of two units.
Since $(b^{-1}a^{-1})(ab) = 1$ it's clear that ab has an inverse.

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

Theorem 3: If a is a unit of $\mathbb{Z}_m$ 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 4: $a \in \mathbb{Z}_m$ is a unit if and only if
$$\text{GCD}(a, m) = 1.$$
Proof: Suppose that a is a unit of $\mathbb{Z}_m$.
Then for some $b \in \mathbb{Z}_m$, $ab = 1$.
In $\mathbb{Z}$ this becomes $ab = 1 + mq$ for some $q \in \mathbb{Z}$.
Let $d = \text{GCD}(a, m)$. Then, since d divides both a and m it follows that d divides 1.

Suppose now that $\text{GCD}(a, m) = 1$.
Then $1 = ah + mk$ for some $h, k \in \mathbb{Z}$.

In $\mathbb{Z}_m$ 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 One-Way Euclidean Algorithm.

INVERSE OF a in $\mathbb{Z}_m$		
A	**Q**	**B**
m		0
a		1
…	…	…
A′	…….	B′
A	q = INT(A′/A)	B
A′ – Aq		B′ – qB
…	…	…
1	q	$\mathbf{a^{-1}}$

Example 2: Find the inverse of 137 in $\mathbb{Z}_{577}$.

A	**Q**	**B**
577		0
137	4	1
29	4	–4
21	1	17
8	2	–21
5	1	59
3	1	–80
2	1	139
1		–219

So the inverse of 137 in $\mathbb{Z}_{577}$ is $-219 = 358$.

§ 2.3. Powers in $\mathbb{Z}_m$

Consider the geometric progression 1, x, x^2, x^3, ... for some $x \in \mathbb{Z}_m$. Since $\mathbb{Z}_m$ 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 $\mathbb{Z}_{10}$, 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 3: 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 $\mathbb{Z}_{10}$, $7^4 = 1$ then 7 to any multiple of 4 will give 1 in $\mathbb{Z}_{10}$. 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 $\mathbb{Z}_{10}$. 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".) We'll give three separate proofs.

Theorem 5 (FERMAT): If p is prime and $0 \neq a \in \mathbb{Z}_p$, then $a^{p-1} = 1$.

Proof: #1: Suppose that a is a minimal counter-example to the statement that $a^p = a$. Clearly $a > 1$. Let $b = a - 1$.
Then $a^{p-1} = (b + 1)^p = b^p + pb^{p-1} + \frac{1}{2}p(p-1)b^{p-2} + ... + 1$.
Since p is prime, all the binomial coefficients, except the first and the last, are multiples of p.
So in $\mathbb{Z}_p$: $a^p = (b + 1)^p = b^p + 1 = b + 1 = a$. This contradicts the fact that a is a minimal counter-example, so $a^p = a$ for all a.
If $a \neq 0$ we can use the cancellation Law to get $a^{p-1} = 1$.

Proof #2: (For those who know a little group theory) Since p is prime the non-zero elements of $\mathbb{Z}_p$ form a group of order $p - 1$ 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 $a \in \mathbb{Z}_p$.

Proof #3: Let $N = 1.2.3 \ldots (p-1)$. Clearly p doesn't divide N and so in $\mathbb{Z}_p$, $N \neq 0$.
In the remainder of the proof we interpret everything as elements of $\mathbb{Z}_p$.

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 4: $p = 7$
$N = 1.2.3.4.5.6$
$2^6N = 2.4.6.1.3.5 = N$
Hence $2^6 = 1$ in $\mathbb{Z}_7$.

Theorem 6: (FERMAT'S LAST THEOREM): For all integers $n \geq 3$ 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 weren't developed until the late 20th century, the consensus seems to be that he only *thought* he had a proof.

§ 2.4. Congruences

Using the ring of integers modulo m is very useful when the modulus remains the same throughout. But often we need to change the modulus. In this case we use the concept of congruence.

When two numbers a, b differ by a multiple of m we write $\boldsymbol{a \equiv b \pmod{m}}$. 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:

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

The relation of equivalence is indeed an equivalence relation. That is, it is reflexive, symmetric and transitive. It shares other properties with equality.

Theorem 6: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
Proof: Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Then $m \mid (a - b)$ and $m \mid (c - d)$.
Since $(a + c) - (b + \mathrm{d}) = (a - b) + (c - d)$ and
$ac - bd = a(c - d) + d(a - b)$, these are multiples of m.

Changing the modulus we get other results that are not mirrored by mere equality. For example it's obvious that if $a \equiv b \pmod{m}$ and $n \mid m$ then $a \equiv b \pmod{n}$. This is a case of going from a larger modulus to a smaller. The following theorem allows us to proceed, in certain circumstances, from smaller moduli to larger ones.

Theorem 7: If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ and m, n are coprime then $a \equiv b \pmod{mn}$.
Proof: Suppose $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$.
Then $a - b = mk$ for some integer k.
Since $n \mid a - b$ we can conclude that $n \mid mk$.
But since m, n are coprime this means that $n \mid k$.
Hence $mn \mid mk = a - b$ and so $a \equiv b \pmod{mn}$.

§ 2.5. The One-Way Euclidean Algorithm Revisited

Having introduced the concept of congruence we can now easily prove that the One-Way Algorithm works.

Theorem 8: Let a, b be positive integers and let $\{a_k\}$, $\{q_k\}$, $\{b_k\}$ be sequences of integers defined recursively by:

$a_0 = a, \quad b_0 = 0;$

$a_1 = b, \quad b_1 = 1;$ and for $k \geq 0$

$a_r = a_{r-2} - a_{r-1}q_{r-1};$

$q_{r+1} = \text{INT}(a_r/a_{r+1});$

$b_r = b_{r-2} - b_{r-1}q_{r-1}.$

Then $bb_r \equiv a_r \pmod{a}$ for all r.

[Of course once we obtain $a_r = 0$ we can't obtain q_r and the process terminates.]

Proof: Let r be a minimal counter-example.

Then $bb_0 = 0$ so $r > 0$.

$bb_1 = b\ a_1\ r > 1.$

Now $bb_{r-1} \equiv a_{r-1}$ and $bb_{r-2} \equiv a_{r-2}$.

Then $bb_r = \text{b}(\text{b}_{r-2} - b_{r-1}q_{r-1})$

$\equiv a_{r-2} - a_{r-1}q_{r-1}$

$\equiv a_r$, contradicting the fact that r is a minimal counter-example.

Corollary: When $a_r = 0$, $a_{r-1} = \text{GCD}(a, b) = ha + kb$ for some k, where $k = b_{r-1}$.

Proof: The successive a_i's are the remainders that arise in the Euclidean algorithm and we have shown that the GCD, d, is the last non-zero remainder, a_{r-1}.

Since $bb_{r-1} \equiv a_{r-1} \equiv d \pmod{a}$ then $d = bk + ah$ for some integer h.

§ 2.6. Solving Linear Congruences

If we have to solve the equation $ax = b$ we simply divide both sides by a to get $x = b/a$. Of course if $a = 0$ we couldn't do that but we'd soon realise if we were trying to solve an equation that has no solution.

Consider the equation $ax \equiv b \pmod{p}$ where p is prime. If p doesn't divide a we could still divide by a to get $x = b/a$, but in this case we haven't finished. We must find a^{-1} and then multiply by b to get an answer in the range 0 to $p - 1$.

Example 5: Solve $3x \equiv 2 \pmod{11}$.
Solution 1: $x \equiv 2.3^{-1}$ [We usually write it this way rather than as a fraction.]
To find 3^{-1} we can simply multiply 1, 2, 3, ..., 10 by 3 until we get 1.
We soon discover that $3.4 = 12 = 1 \bmod 11$
and so $3^{-1} = 4$.
Hence $x \equiv 2.4 \equiv 8$.

Solution 2: Clearly the above method is much more time consuming if the prime is large.
Another method is to write $3x \equiv 2 \equiv 13 \equiv 24 (\text{mod } 11)$ and this gives $x \equiv 8$.

Solution 3: The above method is good if the coefficient is small, or factorises into small factors. The following method is the default method if the other methods appear to be unsuitable.
We observe that GCD(3, 11) = 1, but nevertheless we compute it by The One-Way Euclidean algorithm.

A	**Q**	**B**
11		0
3	3	1
2	1	–3
1		**4**

So 3^{-1} mod 11 is 4, giving $x \equiv 8$ as the solution.

Example 6: Solve the congruence $293x \equiv 5 (\text{mod } 1093)$.
Solution: Here both 293 and 1093 are prime. Methods 1 and 2 are totally inappropriate. They would take far too long. Let's use the One-Way Euclidean algorithm.

	Q	**B**
1093		0
293	3	1
214	1	– 3
79	2	4

56	1	–11
23	2	15
10	2	–41
3	3	97
1		**–332**

So modulo 1093, $293^{-1} = -332$ and so the solution is

$$x \equiv -332*5 \equiv -1660 \equiv 526.$$

When the modulus is composite, solving congruences is rather more difficult because only some non-zero numbers have inverses and many equations have no solutions.

Example 7: Solve the congruence equation

$$15x \equiv 7 (\text{mod } 105).$$

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 9: The congruence $ax \equiv b (\text{mod } m)$ has a solution if and only if GCD(a, m) divides b.

Proof: Let d = GCD(a, m) and suppose that the congruence has a solution x.

Then $ax = b + my$ for some y.

Since $d \mid a$ and $d \mid m$ it must be that $d \mid b$.

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.

Theorem 10: Let $d = \text{GCD}(a, m)$ and let $a = a_0 d$ and $m = m_0 d$.
If x_0 is a solution to the congruence equation

$$ax \equiv b (\text{mod } m)$$

then the complete solution is

$$x = x_0 + m_0 t \text{ for some number } t.$$

Proof: Let $a = a_0 d$ and $m = m_0 d$.
Suppose $ax_0 \equiv b (\text{mod } m)$ and let $ax_0 = b + mq$.
Let $x = x_0 + m_0 t$.
Then $ax = ax_0 + am_0 t$
$= b + mq + am_0 t$
$= mt$ so $ax \equiv b (\text{mod } m)$.
Suppose $ax \equiv b (\text{mod } m)$.
Then $ax \equiv ax_0 (\text{mod } m)$ and so $x \equiv x_0 (\text{mod } m_0)$.

Theorem 11: $ax \equiv ay (\text{mod } m)$ if and only if $x \equiv y \left(\text{mod } \frac{m}{\text{GCD}(a,m)}\right)$.

Proof: Let $d = \text{GCD}(a, m)$ and let $a = a_0 d$ and $m = m_0 d$.
Suppose $ax \equiv ay (\text{mod } m)$.
Then $ax = ay + mq$ for some number q.
Hence $a_0 dx = a_0 dy + m_0 dq$.
Dividing by d we get $a_0 x = a_0 y + m_0 q$.
That is m_0 divides $a_0(x - y)$.

Since GCD(a_0, m_0) = 1, m_0 divides $x - y$ and so

$$x \equiv y (\text{mod } m_0).$$

Conversely if $x \equiv y (\text{mod } m_0)$ then m_0 divides $x - y$ and so

$$m = m_0 d \text{ divides } d(x - y)$$

and hence it divides $a_0 d(x - y) = ax - ay$.

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.

§ 2.7. The Chinese Remainder Theorem

Theorem 12 (Chinese Remainder Theorem):

Suppose a_1, a_2, ..., a_k, m_1, m_2, ..., m_k are integers and suppose that the m_i are pairwise coprime.

[This means that GDC(m_i, m_j) = 1 whenever $i \neq j$.]

Then there exists an integer x such that

$x \equiv a_i (\text{mod } m_i)$ for i = 1, 2, ..., k.

Proof: Let M = Πm_i and for each i let n_i = M/m_i.

Then n_i is coprime with m_i for each i.

Hence for each j there exists a solution, x_j, to the congruence $n_i x_j \equiv 1 (\text{mod } m_i)$.

Let $x = \Sigma n_i a_i x_i$.

Since m_j divides n_i if $j \neq i$,

$x \equiv n_i a_i x_i \ (\text{mod } m_j)$ for each j

$\equiv a_j (\text{mod } m_j)$.

Example 8: Find an integer x such that $x \equiv 1(\text{mod } 10)$, $x \equiv 2(\text{mod } 21)$ and $x \equiv 3(\text{mod } 29)$.

Solution: This is possible since GCD(10, 21) = GCD(10, 29) = GCD(21, 29) = 1.

Here $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $m_1 = 10$, $m_2 = 21$, $m_3 = 29$.

Then $M = \Pi m_i = 6090$, $n_1 = 609$, $n_2 = 290$, $n_3 = 210$.

The three equations are, respectively:

$$609x \equiv 1(\text{mod } 10),$$
$$290x \equiv 1(\text{mod } 21),$$
$$210x \equiv 1(\text{mod } 29).$$

But we can reduce the coefficients modulo the respective moduli to get:

$$9x \equiv 1(\text{mod } 10),$$
$$17x \equiv 1(\text{mod } 21) \text{ and}$$
$$7x \equiv 1(\text{mod } 29).$$

We could use Euclid's algorithm but it is easier here to use more elementary means.

We can write the above equations as:

$-x \equiv 1(\text{mod } 10)$, giving $x_1 = -1$,

$-4x \equiv 1 \equiv -20(\text{mod } 21)$, giving $x_2 \equiv 5$ and

$7x \equiv -28(\text{mod } 29)$, giving $x_3 = -4$.

So $x = \Sigma n_i a_i x_i = 609.1.(-1) + 290.2.5 + 210.3.(-4)$

$= -229$.

If you want a positive x you only have to add M = 6090 to get $x = 5861$.

EXERCISES FOR CHAPTER 2

Exercise 1: Solve the congruence equation:

$$100x \equiv 26 (\text{mod } 42).$$

Exercise 2: Solve the congruence equation:

$$293x \equiv 7 (\text{mod } 1093).$$

Exercise 3: Solve the congruence equation:

$$2018x \equiv 4 (\text{mod } 5000).$$

Exercise 4: Solve the congruence equation:

$$2407\text{x} \equiv 1079 (\text{mod } 3071).$$

Exercise 5: Find the inverse of 18 in $\mathbb{Z}_{175}$.

Exercise 6: Find the inverse of 31 in $\mathbb{Z}_{1001}$

Exercise 7: Find 5^{127} in $\mathbb{Z}_{13}$.

Exercise 8: Find 17^{1000} in $\mathbb{Z}_{37}$.

SOLUTIONS FOR CHAPTER 2

Exercise 1: Suppose $100x \equiv 26 (\text{mod } 42)$.
Then $16x \equiv 26 (\text{mod } 42)$ (since $100 \equiv 16 (\text{mod } 42)$
Hence $8x \equiv 13 (\text{mod } 21)$ using Theorem 11

$\equiv 34 (\text{mod } 21)$

So $4x \equiv 17 (\text{mod } 21)$

$\equiv 38 (\text{mod } 21)$

$\therefore\ 2x \equiv 19 (\text{mod } 21)$

$\equiv 40 (\text{mod } 21)$

So $x \equiv 20 \text{ (mod } 21)$

Alternately we can use the One Way Algorithm, after reducing the equation to $8x \equiv 13 (\text{mod } 21)$ as above:

	Q	**B**
21		0
8	2	1
5	1	–2
3	1	3
2	1	–5
1	2	8

Hence $1 = 8.8 (\text{mod } 21)$.

$13 = 8.104 (\text{mod } 21) \equiv 8.20 (\text{mod } 21)$,

reducing 104 mod 21.

Hence $x \equiv 20$ is the solution.

Exercise 2: Using the One Way Algorithm:

A	**Q**	**B**
1093		0
293	3	1
214	1	– 3
79	2	4
56	1	–11

23	2	15
10	2	–41
3	3	97
1		–332

Hence $1 \equiv 293,(-332) \pmod{1093}$
Hence $7 \equiv 293(-2324) \pmod{1093}$ which gives
$x \equiv -2324 \equiv 955 \pmod{1093}$.

Exercise 3: Suppose $2018x \equiv 4 \pmod{5000}$.

Probably we'd notice that 2 divides all three numbers and we would reduce this equation to $1009x \equiv 2 \pmod{2500}$. But let's see what would happen if we didn't notice this and use the original equation. Using the One Way Algorithm:

A	Q	B
5000		0
2018	2	1
964	2	–2
90	10	5
64	1	–52
26	2	57
12	2	–166
2	6	389
0		

Hence $2 \equiv 2018.389 \pmod{5000}$ and so

$$4 \equiv 2018.778 (\text{mod } 5000).$$

This gives $x \equiv 778 (\text{mod } 5000)$.

Note that this gives only some of the solutions because there are in fact two solutions modulo 5000. This is because the original equation reduces to:

$$1009x \equiv 2 (\text{mod } 2500).$$

Of course $x = 778$ will be a solution to this so the complete solution is $x \equiv 778 (\text{mod } 2500)$.

Now we observed from our table that GCD(2018, 5000) = 2 and there are solutions because 2 divides 4. So if we're solving $ax \equiv b (\text{mod } m)$ we proceed as in the One Way Solution. We get the GCD and observe that it divides b. Then we find h, k as above but we report the solution so obtained modulo m/GCD(a, m).

The moral of the story is: if you notice common factors between a and m check that they divide b and work with the simplified equation, dividing each number by such common factors. However if you don't notice such a common factor, proceed as usual. If you subsequently discover that the GCD is not 1 simply divide the modulus by that GCD.

Exercise 4: There is a common factor but it isn't obvious. Just proceed normally.

A	Q	B
3071		0
2407	1	1
664	3	−1
415	1	4

249	1	–5
166	1	9
83	2	–14
0		

So the GCD is 83.
Hence $2407.(-14) \equiv 83 \pmod{3071}$.
Note that 83 | 1079 and 1079/83 = 13.
Hence $2407.(-14).13 \equiv 83.13 \equiv 1079$, so
one solution is $x \equiv -14.13 \pmod{3071}$
$\equiv -182 \pmod{3071} \equiv 2889 \pmod{3071}$.
However the complete solution is:
$x \equiv 2889 \pmod{3071/83}$, that is
$x \equiv 2889 \pmod{37} \equiv 3 \pmod{37}$.

Exercise 5:

A	Q	B
175		0
18	9	1
13	1	–9
5	2	10
3	1	–29
2	1	39
1		–68

So the inverse is –68 = 107.

Exercise 6:

A	Q	B
1001		0
31	32	1
9	3	–32
4	2	97
1		–226

So the inverse is –226 = 775.

Exercise 7: 13 is prime and 5 is not divisible by 13.
Hence, be Fermat's Little Theorem, $5^{12} = 1$ in $\mathbb{Z}_{13}$.
Hence $5^{120} = 1$ and so $5^{127} = 5^7 = 78125 = 8$.
NOTE: We could have obtained 5^7 (mod 13) without the aid of a calculator as follows:
$5^2 = 25 = 12 = -1$ in $\mathbb{Z}_{13}$.
Hence $5^4 = 1$, and so $5^7 = 5^4.5^2.5 = -5 = 8$.
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 8: In $\mathbb{Z}_{37}$, $17^{36} = 1$.
Now 1000 = 36.27 + 28.
Hence, in $\mathbb{Z}_{37}$ $17^{1000} = 17^{28}$.
$17^2 = 289 = 30$ in $\mathbb{Z}_{37}$.
$17^4 = 30^2 = 900 = 12$.
$17^8 = 12^2 = 144 = 33$.
$17^{16} = 33^2 = 1089 = 16$.
Hence $17^{28} = 17^{16}.17^8.17^4 = 16.33.12 = 6336 = 9$.