11. INTEGERS MOD m

§ 11.1. Days of the Week

When we do calculations with days of the week we use a system that's called the system of integers modulo 7, or $\mathbb{Z}_7$ 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. 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 are 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 $\mathbb{Z}_7$. 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 $\mathbb{Z}_7$ 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 $\mathbb{Z}_7$ 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're doing a lot of calculations in $\mathbb{Z}_7$ we can simply

announce that we're working in that system and simply write 5 + 4 = 2.

The system $\mathbb{Z}_7$ is. in many ways. a miniature version of the system of integers. We can add and multiply any two numbers in the system and our answer will be one of the 7 numbers.

§ 11.2. The system $\mathbb{Z}_7$

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 $\mathbb{Z}_7$:
$x + y = y + x$ 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're 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 $\mathbb{Z}_7$:
$0 + x = x = x + 0$ and $1x = x = x1$.

Something that you wouldn't notice just by casual observation, are the associative laws:

For any x, y and z in the system $\mathbb{Z}_7$:
$x + (y + z) = (x + y) + z$ 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 $\mathbb{Z}_7$.

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 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 $\mathbb{Z}_7$.

x	1	2	3	4	5	6
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
x^2	1	4	2	2	4	1
x^3	1	1	6	1	6	6
x^4	1	2	4	4	2	1
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
x^6	1	1	1	1	1	1

So $x^6 \equiv 1 \pmod 7$ 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 have done for 7 can be done for any modulus.

§ 11.3. The system $\mathbb{Z}_m$

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 $\mathbb{Z}_1$ 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 $\mathbb{Z}_2$, 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 “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 $\mathbb{Z}_2$ 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.

Let's try $\mathbb{Z}_8$, the system of integers modulo 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 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 $\mathbb{Z}_8$. In $\mathbb{Z}_7$ the cancellation law:

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

is valid. In $\mathbb{Z}_8$ it's 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 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
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 $x = y$.

[Remember that $ax = ay$ 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 $\mathbb{Z}$ a is not divisible by p. Since p is prime this means that a and p are coprime.

Hence $1 = ah + pk$ for some integers h, k. Multiplying both sides by b we get
$b = (ab)h + p(bk)$. In $\mathbb{Z}_p$ this gives $b = 0$. So if $ab = 0$ in $\mathbb{Z}_p$ either $a = 0$ or $b = 0$.

If we're using the same modulus, m, in a piece of work we simply announce at the beginning that we are working in $\mathbb{Z}_m$. But if we need to change the modulus we use a different notation that constantly reminds us of which modulus we are using at any given time.

We say that ***a* is congruent to *b* modulo *m*** if a and b have the same remainders on division by m. We write this as $\boldsymbol{a \equiv b \pmod{m}}$. In $\mathbb{Z}_m$ this simply means that $a = b$. In $\mathbb{Z}$ it means that m divides $a - b$ or that $a = b + mq$ for some integer q.

Example 2: $27 \equiv 13 \pmod 7$ since 7 divides $27 - 13 = 14$, or equivalently, $27 = 13 + 7.2$.
In $\mathbb{Z}_7$, $27 = 13$. They are just alternative ways of writing 6.

§ 11.4. Inverses in $\mathbb{Z}_m$

For many applications it is important to be able to find an 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 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 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 Euclidean algorithm and then working backwards to express 1 in the form $ab + mc$.

Example 3: Find the inverse of 35 modulo 143.
Solution:

$$\begin{array}{rrr} \quad 4 & \quad 11 & \quad 1 \\ 35\overline{)\,143} & 3\overline{)\,35} & 2\overline{)\,3} \\ \underline{140} & \underline{33} & \underline{2} \\ \quad 3 & \quad 2 & \quad 1 \end{array}$$

So $1 = 3 - 2$
$= 3 - (35 - 3.11) = 3.12 - 35$
$= (143 - 35.4).12 - 35 = 143.12 - 35.49.$
Hence $35(-49) \equiv 1 (\text{mod } 143)$. So the inverse of 35 modulo 143 is $-49 = 94$.

Theorem 5: Let a, m be positive integers and let $\{a_n\}$, $\{q_n\}$, $\{b_n\}$ be sequences of integers defined recursively for $n \geq 0$ (until $a_n = 1$) by:

$a_0 = m$, $b_0 = 0$,
$a_1 = a$, $b_1 = 1$ and, for $n \geq 2$:
$q_n = \text{INT}(a_{n-2}/a_n)$,
$a_n = a_{n-2} - a_{n-1}q_{n-1}$,
$b_n = b_{n-2} - b_{n-1}q_{n-1}$ for $n \geq 2$.

Then for all n, $ab_n \equiv a_n (\text{mod } m)$.

Proof: For $n = 0$ this merely says that $0 \equiv m \pmod{m}$, which is certainly true.
For $n = 1$ this says that $a \equiv a \pmod{m}$, which is also true.
Suppose now that $n \geq 2$ and suppose that:

$$ab_n \equiv a_n \pmod{m}.$$

Then $ab_{n+1} = a(b_{n-1} - b_n q_n)$
$\equiv ab_{n-1} - ab_n q_n$
$\equiv a_{n-1} - a_n q_n \pmod{m}$
$\equiv a_{n+1} \pmod{m}$.

Corollary: If a, m are coprime, ultimately $a_n = 1$ and so

$$b_n \equiv a^{-1} \pmod{m}.$$

So by computing the sequence $\{b_n\}$ in parallel with the $\{a_n\}$ we can find the inverse of a modulo m. We set our working in three columns. The first column contains the successive values of q. The second column contains the values of a_n and the third column contains the values of b_n.

To begin with we set down the following values in the second and third columns. The first column remains blank at this stage.

q_n	a_n	b_n
	m	0
	a	1

These rows correspond to $n = 0$ and $n = 1$.

We compute each of the remaining rows from the two rows above it as follows:

	a_{n-2}	b_{n-2}
q_{n-1}	a_{n-1}	b_{n-1}
INT(a_{n-2} /a_{n-1})	$a_{n-2} - a_{n-1}q_{n-1}$	$b_{n-2} - b_{n-1}q_{n-1}$

We continue until we obtain a '1' in the middle column. The required inverse will now appear in the third column. The table will have the form:

$\boldsymbol{q_n}$	$\boldsymbol{a_n}$	$\boldsymbol{b_n}$
	m	0
	a	1
…	…	…
	a_{n-2}	b_{n-2}
q_{n-1}	a_{n-1}	b_{n-1}
INT(a_{n-2} /a_{n-1})	$a_{n-2} - a_{n-1}q_{n-1}$	$b_{n-2} - b_{n-1}q_{n-1}$
…	…	…
	1	inverse

Each item in the first column is obtained by finding the quotient on dividing the two most recent two entries in the middle column and the quotient goes in the middle column.

	Δ	
	□	
quotient	remainder	

For the third column we do the remainder calculation on the two most recent entries in the third column, but using the same quotient as before.

	A	B
	a	b
q	A – $a.q$	B – $b.q$

Example 4: Find the inverse of 35 mod 143.
Solution: We begin with:

q_n	a_n	b_n
	143	0
	35	1

For the next row we find INT(143/35) = 4, 143 – 35.4 = 3and 0 – 1.4 = –4.

q_n	a_n	b_n
	143	0
	35	1
4	3	– 4

The table is completed in the same way:

q_n	a_n	b_n
	143	0
	35	1
4	3	– 4
11	2	45
1	1	–49

So the inverse of 35 modulo 143 is – 49 = 94.

§ 11.5. 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 5: 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
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".

Fermat's Last Theorem states that 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 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. There are now

numerous proofs of this theorem – here are three of them.

Theorem 6 (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:

$$(a + 1)^p = a^p + pa^{p-1} + \tfrac{1}{2}p(p - 1)a^{p-2} + ... + 1.$$

Since p is prime, all the binomial coefficients, except the first and the last, are multiples of p so, modulo 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 $\mathbb{Z}_p$ 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 $a \in \mathbb{Z}_p$.

Proof #3: Let $N = (p - 1)! = 1.2.3 \ldots (p - 1)$.

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 $a^{p-1}\mathrm{N} = a.2a.3a. \ldots .(p-1)$.
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 $a^{p-1}\mathrm{N} = \mathrm{N}$ and, since $\mathrm{N} \neq 0$ in $\mathbb{Z}_p$, it follows by the Cancellation Law that $a^{p-1} = 1$.

Example 6: $p = 7$
$\mathrm{N} = 1.2.3.4.5.6$
Now modulo 7, {2, 4, 6, 8, 10, 12} = {2, 4, 1, 3, 5}. Both sets therefore have the same product,
$2^6\mathrm{N} = 2.4.6.1.3.5 = \mathrm{N}$
$\therefore\ 2^6 = 1$ in $\mathbb{Z}_7$.
Note that in this example $\mathrm{N} = 720 \equiv -1 (\mathrm{mod}\ 7)$. This holds for all primes p.

Theorem 7: If p is prime then $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.
Proof: Now $(p-1)! = 1.2.3 \ldots (p-1)$. Each one of these factors has an inverse in $\mathbb{Z}_p$ and it will cancel its inverse, provided that inverse is a different element of $\mathbb{Z}_p$. So N is the product of all those elements of $\mathbb{Z}_p$ that are equal to their own inverse.
But if $x = x^{-1}$ then $x^2 = 1$ and so $(x-1)(x+1) = 0$. Since the cancellation law holds in $\mathbb{Z}_p$ (for prime p) we must have $x = 1$ or $x = -1$. The product of these is -1.

§ 11.6. Euler's φ-Function

We define **φ(*n*)** to be the number of units of $\mathbb{Z}_m$. In other words, it is the number of integers from 1 to *m* that are coprime with *m*.

Example 7: φ(10) = 4 since the units of Z_{10} are 1, 3, 7 and 9.
φ(21) = 12 since the units of $\mathbb{Z}_{21}$ are 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19 and 20.

Theorem 8: If *p* is prime and $n \geq 1$, $\varphi(p^n) = p^{n-1}(p-1)$.
Proof: Of the numbers from 1 to p^n, the ones that are not coprime to p^n are the multiples of *p*. There are p^{n-1} of these and so $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.
Corollary: $\varphi(p) = p - 1$.

Theorem 9: If *p*, *q* are distinct primes then:

$$\varphi(p^m q^n) = p^{m-1}(p-1)q^{m-1}(q-1).$$

Proof: Of the numbers from 1 to $p^m q^n$ the ones that are not coprime to $p^m q^n$ are the multiples of *p* and the multiples of *q*.

Now there are $p^{m-1}q^n$ multiples of *p* in this range, and $p^m q^{n-1}$ multiples of *q*. But don't forget that the $p^{m-1}q^{n-1}$ multiples of *pq* will get counted both times, and so by the Principle of Inclusion-Exclusion we have:

$$\varphi(p^m q^n) = p^m q^n - p^{m-1}q^n - p^m q^{n-1} + p^{m-1}q^{n-1}$$
$$= p^{m-1}(p-1)q^{m-1}(q-1).$$

Corollary: $\varphi(pq) = (p-1)(q-1)$.

The general case is as follows. We omit the proof.

Theorem 10: $\varphi(p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k})$
$= p_1^{n_1-1}(p_1 - 1)\, p_2^{n_2-1}(p_2 - 1) \ldots p_k^{n_k-1}(p_k - 1)$.

An alternative formulation of this theorem is as follows. If the distinct prime divisors of N are $p_1, p_2, \ldots, p_k$ then $\varphi(N) = \dfrac{N}{(p_1 - 1)...(p_k - 1)}$.

Leonard Euler gave the following generalisation of Fermat's Little Theorem.

Theorem 11 (EULER): If a is coprime with n then:

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

Proof #1: This proof is adapted from Proof #3 of Fermat's Little Theorem.
Let N be the product of all the units of $\mathbb{Z}_n$.
Clearly $N \neq 0$ in $\mathbb{Z}_n$.
Multiply each of the factors of N by a.
Hence $a^{\varphi(n)}N$ is the product of each of the units after being multiplied by a.
By the cancellation law, no two of these factors are equal, so they must be all the units in some order. Hence $a^{\varphi(n)}N = N$. Now the product of any collection of units is a unit so N is a unit.
By the Cancellation Law $a^{\varphi(n)} = 1$.

Proof #2: However the simplest proof is by group theory. The elements of $\mathbb{Z}_n$ that are coprime with n are precisely the units. They form a group, often denoted by $\mathbb{Z}_n^{\#}$, under multiplication. The order (size) of this group is $\varphi(n)$. By Lagrange's Theorem the order of each element divides the order of the group and so if a is one of these units, $a^{\varphi(n)} = 1$ in $\mathbb{Z}_n$.

Example 8: $\varphi(20) = \varphi(2^2.5) = 2^1(2-1)5^0(5-1)$
$= 2.4 = 8.$
$\varphi(7000) = \varphi(2^3.5^3.7) = 2^2.5^2.4.6 = 2400.$

In computing powers modulo n, we can use Euler's theorem to break down the power to a much smaller one.

Example 9: Find 69^{4803} modulo 7000.
Solution: $\varphi(7000) = 2400$ so
$69^{2400} \equiv 1$ and hence
$69^{4800} \equiv 1$ so $69^{4803} \equiv 69^3 \equiv 328509 \equiv 6509.$

If the modulus is large, even breaking down a power to a smaller one may still result in a large power, too large to compute with the computing device available. The trick here is to break the power up as a sum of powers of 2. The number to be raised is then squared repeatedly. But at each stage the answer is reduced modulo the modulus, so that the numbers

involved in the calculation are never bigger than the square of the modulus.

Example 10: Find 69^{4900} modulo 7000.
Solution: As above, $69^{4800} \equiv 1 \pmod{7000}$ so $69^{4900} \equiv 69^{100}$.
$69^2 \equiv 4761$
$69^4 \equiv 4761^2 \equiv 22667121 \equiv 1121$
$69^8 \equiv 3641$
$69^{16} \equiv 5881$
$69^{32} \equiv 6161$
$69^{64} \equiv 3921$
Now $100 = 64 + 32 + 4$ so
$69^{100} = 69^{64}.69^{32}.69^4$
$\equiv 3921.6161.1121$
$\equiv 24157281.1121$
$\equiv 281.1121$
$\equiv 315001$
$\equiv 1$
Hence $69^{5000} \equiv 1$

EXERCISES FOR CHAPTER 11

EXERCISES 11A (Arithmetic Mod m)

Ex 11A1: If $x = 7$ and $y = 6$, compute $x^3 + y^3 \pmod{11}$.

Ex 11A2:
Find the inverses of the non-zero elements of $\mathbb{Z}_{11}$.

Ex 11A3: Which elements of $\mathbb{Z}_{15}$ have inverses under multiplication?

Ex 11A4: Find the remainder on dividing 13^{31967} by 31.

Ex 11A5: Calculate $\varphi(2600)$. Hence find 3^{1000} in $\mathbb{Z}_{2600}$.

Ex 11A6: In $\mathbb{Z}_{1271}$ find $1037^{1234567}$.

Ex 11A7: Find the remainder on dividing 11^{1603} by 600.

Ex 11A8: Find the inverse of 125 modulo 2592. (This obtains the decoding number for user A in example 13.)

Ex 11A9: (i) Solve the equation $143x \equiv 1 \pmod{300}$.
(ii) Find $\varphi(78200)$.

SOLUTIONS FOR CHAPTER 11

Ex 11A1: 9

Ex 11A2:

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

Ex 11A3: 1, 2, 4, 7, 8, 11, 13, 14.

Ex 11A4: 17.

Ex 11A5: $\varphi(2600) = 960$; $3^{1000} = 601$

Ex 11A6: 872

Ex 11A7: $\varphi(600) = \varphi(2^3.3.5^2) = 2^2.2.5.4 = 160$.
Thus $11^{160} = 1$ in $\mathbb{Z}_{600}$.
Hence $11^{1603} = 11^3 = 1331 = 131$.
Thus the remainder is 131.

Ex 11A8:

20	1	1	1
125) 2592	92) 125	33) 92	26) 33
250	92	66	26
92	33	26	7

etc.

Hence $1 = 5 - 2.2$

$= 5 - 2(7 - 5) = 3.5 - 2.7$

$= 3(26 - 3.7) - 2.7 = 3.26 - 11.7$

$= 3.26 - 11(33 - 26) = 14.26 - 11.33$

$= 14(92 - 33.2) - 11.33 = 14.92 - 39.33$

$= 14.92 - 39(125 - 92) = 53.92 - 39.125$

$= 53(2592 - 125.20) - 39.125$

$= 53.2592 - 1099.125.$

Hence $1 \equiv (-1099).125 \pmod{2592}$.

The inverse of 125 modulo 2592 is therefore:

$-1099 \equiv 1493.$

Ex 11A9:

$300 = 143.2 + 14$

$143 = 14.10 + 3$

$14 = 3.4 + 2$

$3 = 2.1 + 1$

$\therefore 1 = 3 - 2$

$= 3 - (14 - 3.4)$

$= 3.5 - 14$

$= (143 - 14.10).5 - 14$

$= 143.5 - 14.51$

$= 143.5 - (300 - 2.143).51$

$= 143.107 - 300.51$

$\equiv 143.107 \pmod{300}$.

$\therefore x \equiv 107 \pmod{300}$.

(ii) $\varphi(78200) = \varphi(2^3.5^2.17.23) = 2^2.5.4.16.22 = 28160.$