M 2 4 6

Number Theory

Workbook 2 (without solutions)

Euler's ϕ-Function and the Chinese Remainder Theorem

Summer 2013

(originally written and devised by
Trevor Hawkes and Alyson Stibbard;
revised in 2010 by John Cremona)

Aims of these workbooks:

(a) To encourage you to teach yourself mathematics from written material,

(b) To help you develop the art of independent study — working either alone, or co-operatively with other students,

(c) To help you learn a mathematical topic, in this case Number Theory, through calculation and problem-solving.

Copies of this workbook, both with and without solutions, can be found on Mathstuff.

Icons in this Workbook

The 'Section Targets' box contains an idea of what you should aim to get out of the current section. Perhaps you might return to this at the end to evaluate your progress.

Reaching this icon in your journey through the workbook is an indication that an idea should be starting to emerge from the various examples you have seen.

Material here includes reference either to earlier workbooks, or to previous courses such as foundations/Sets and Groups.

A caution. Watch your step over issues involved here.

Are You Ready?

To understand the material and do the problems in each section of this workbook, you will need to be on good terms with:

Section 1: • Basic definitions of Groups and Rings
Section 3: • The Fundamental Theorem of Arithmetic

Note: You will need a pocket calculator for some of the questions in the workbooks, and are encouraged to use one for this purpose and to experiment with results and ideas in the course. Calculators are NOT needed and are NOT allowed in tests or in the examination.

These workbooks were orginally written and devised by *Trevor Hawkes and and Alyson Stibbard*. *Ben Carr* designed the LaTeX template and *Rob Reid* converted their drafts into elegant print. Over the years, other lecturers and students have corrected a number of typos, mistakes and other infelicities. In 2010 *John Cremona* made some substantial revisions.

Send corrections, ask questions or make comments at the module forum. You can join the MA246 forum by going to `http://forums.warwick.ac.uk/wf/misc/welcome.jsp` and signing in, clicking the *browse* tab, and then following the path: Departments > Maths > Modules > MA2xx modules > MA246 Number Theory.

1 Moving the action to $\mathbb{Z}/n\mathbb{Z}$

Section Targets

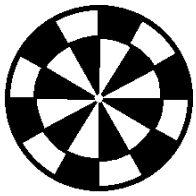
(a) To translate the work of the previous workbook to the ring[a]

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}.$$

(b) To discuss

- the concept of a *unit* in $\mathbb{Z}/n\mathbb{Z}$;
- the fact that these units form a group, $\mathbb{U}_n$;
- Euler's phi-function ϕ, which gives the order of this group;
- Euler's Theorem; and a special case,
- *Fermat's Little Theorem.*

[a] A *ring* is a set R with 2 binary operations: addition $(+)$ and multiplication (juxtaposition). $(R, +)$ has to be a commutative group, and the distributive laws must hold. Keep in mind $\mathbb{Z}$ as a prototype of a ring.



The congruence,

$$ax \equiv b \pmod{n} \tag{1.a}$$

means that ax and b belong to the same congruence class and so $n\mathbb{Z} + ax = n\mathbb{Z} + b$. The rule for multiplying congruence classes (see (1.9) of WB1) gives $n\mathbb{Z}+ax = (n\mathbb{Z}+a)(n\mathbb{Z}+x)$, and if we suppose WLOG that a, x and b lie between 0 and $n-1$ and then use the label a for the class $n\mathbb{Z} + a$, etc. the congruence (1.a) can be rewritten

$$a \times_n x = b \tag{1.b}$$

with $a, x, b \in \{0, 1, \ldots, n-1\}$.

Change of notation Let's now agree to abandon the fastidious notation $+_n$ and $\times_n$ and revert to the more familiar $+$ (for addition in $\mathbb{Z}/n\mathbb{Z}$ as well as in $\mathbb{Z}$) and juxtaposition (for multiplication in $\mathbb{Z}/n\mathbb{Z}$ as well as in $\mathbb{Z}$). It will introduce ambiguity, but we will usually be able to see from the context whether we are working in $\mathbb{Z}/n\mathbb{Z}$ or in $\mathbb{Z}$. In this section, the emphasis will be on $\mathbb{Z}/n\mathbb{Z}$ for some fixed $n \in \mathbb{N}$. The above translation from 'congruences in $\mathbb{Z}$' to 'equations in $\mathbb{Z}/n\mathbb{Z}$' means we can rewrite Theorem 2.11 of WB1 as follows.

(1.1) Theorem *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}/n\mathbb{Z}$. Then the equation,*

$$ax = b \tag{1.c}$$

has a solution $x \in \mathbb{Z}/n\mathbb{Z}$ if and only if (now regarding a and b as integers) $\mathrm{hcf}\{a, n\}$ *divides b.*

Definition: The elements $u \in \mathbb{Z}/n\mathbb{Z}$ such that $uv = 1$ for some $v \in \mathbb{Z}/n\mathbb{Z}$ are called the *units* of $\mathbb{Z}/n\mathbb{Z}$.

Notice that unless $n = 1$, the element 0 can never be a unit, which is why we look for units in the multiplication table of $(\mathbb{Z}/n\mathbb{Z})^*$, rather than in that of $\mathbb{Z}/n\mathbb{Z}$

(1.2) Question about addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$

(a) Complete the multiplication table for $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$ when $n = 4$ and $n = 6$ (you did $n = 5$ in WB 1).

(b) Using the multiplication tables, list all the elements u in $\mathbb{Z}/n\mathbb{Z}$ for which $uv = 1$ for some v in $\mathbb{Z}/n\mathbb{Z}$ when $n = 4, 5$ and 6.

Observe that in the multiplication table of $(\mathbb{Z}/n\mathbb{Z})^*$, every row and every column contains either a 1 or a 0 *but not both*. Why do you think this is?

Answers to (1.2)

(a)(i)

$\times_4$	1	2	3
1			
2			
3			

(ii)

$\times_6$	1	2	3	4	5
1					
2					
3					
4					
5					

continued. . .

(b)

(i)

(ii)

(iii)

An element u in $\mathbb{Z}/n\mathbb{Z}$ is a unit iff the equation $ux = 1$ has a solution. By Theorem 1.1 this happens if and only if $\text{hcf}\{u, n\} = 1$; the solution is then *unique* (in $\mathbb{Z}/n\mathbb{Z}$), and is called the *inverse* of u. So we know exactly what the units of $\mathbb{Z}/n\mathbb{Z}$ are.

(1.3) Proposition *The units of* $\mathbb{Z}/n\mathbb{Z}$ *are those elements* $u \in \{1, 2, \ldots, n-1\}$ *such that* $\text{hcf}\{u, n\} = 1$.

(1.4) Notation For $n \geq 2$, we will denote the set of units of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{U}_n$. Thus

$$\mathbb{U}_n = \{u \mid 1 \leq u < n \quad \text{and} \quad \text{hcf}(u, n) = 1\};$$

$$u \in \mathbb{U}_n \quad \text{if and only if} \quad \text{hcf}\{u, n\} = 1.$$

(1.5)

(a) Show that $\mathbb{U}_n \neq \emptyset$ for $n \geq 2$

(b) Write down the units of

(i) $\mathbb{Z}/8\mathbb{Z}$ (ii) $\mathbb{Z}/9\mathbb{Z}$ (iii) $\mathbb{Z}/10\mathbb{Z}$.

(c) Use the empty tables in the answer box below to fill in multiplication tables for $\mathbb{U}_8, \mathbb{U}_9, \mathbb{U}_{10}$. Hence find the inverse of each unit in each case.

(d) For each unit u in $\mathbb{U}_8$, work out the smallest $m \geq 1$ such that $u^m = 1$ (the *order* of u).

(e) Now do the same for $\mathbb{U}_{10}$.

In $\mathbb{Z}/1\mathbb{Z}$ we find that $1 = 0$, so the concept of a unit gets a bit silly. Notice that the entries in these tables all belong to $\mathbb{U}_n$ ($n = 8, 9, 10$). Thus multiplication is a binary operation on $\mathbb{U}_n$. Why?

Answers to (1.5)

(a)

(b)(i)

(ii)

(iii)

(c)

$\times_8$							

$\times_{10}$									

$\times_9$										

(d)

(e)

In the previous question we saw that the product of two units in $\mathbb{Z}/n\mathbb{Z}, (n = 8, 9, 10)$ is another unit. The reason is not hard to find. Let u_1 and u_2 be units in $\mathbb{Z}/n\mathbb{Z}$. Then $u_1v_1 = 1 = u_2v_2$ for suitable v_1, v_2 in $\mathbb{Z}/n\mathbb{Z}$. Hence

$$(u_1u_2)(v_1v_2) = u_1v_1u_2v_2 = 1,$$

and it follows that u_1u_2 is also a unit in $\mathbb{Z}/n\mathbb{Z}$, with inverse v_1v_2. We have therefore justified the following.

(1.6) Proposition *Multiplication on $\mathbb{U}_n$ is a binary operation; in other words, $\mathbb{U}_n$ is closed under multiplication.*

Note that when $uv = 1$ then *both* u and v are in $\mathbb{U}_n$.

Evidently $(\mathbb{U}_n, \times)$ has a *neutral* (or *identity*) *element* 1, and every element u has an *inverse* v such that $uv = vu = 1$. The *associative law* for $\mathbb{U}_n$ follows from the corresponding law for multiplication in $\mathbb{Z}$. To spell this out in detail,

A similar argument shows that the *commutative law* for $\mathbb{U}_n$ $(uv = vu)$ follows from the corresponding law for multiplication in $\mathbb{Z}$.

$$\begin{aligned}(uv)w &= ((n\mathbb{Z}+u)(n\mathbb{Z}+v))(n\mathbb{Z}+w)\\ &= (n\mathbb{Z}+uv)(n\mathbb{Z}+w)\\ &= n\mathbb{Z}+(uv)w\\ &= n\mathbb{Z}+u(vw)\\ &= (n\mathbb{Z}+u)(n\mathbb{Z}+vw)\\ &= (n\mathbb{Z}+u)((n\mathbb{Z}+v)(n\mathbb{Z}+w))\end{aligned}$$

for all $u, v, w, \in \mathbb{U}_n$. We have therefore justified the following theorem.

(1.7) Theorem *If $n \geq 2$, the set $\mathbb{U}_n$ is a commutative[a] group with respect to the binary operation of multiplication in $\mathbb{Z}/n\mathbb{Z}$.*

[a] Recall that a group satisfying the commutative law is called *abelian* after the Norwegian mathematician, Niels Henrik Abel (1802-1829)

The order $|\mathbb{U}_n|$ of $\mathbb{U}_n$ (i.e. the number of elements in $\mathbb{U}_n$) is given by Euler's so-called *phi-function*,

$$\phi : \mathbb{N} \longrightarrow \mathbb{N}$$

which is defined as follows:

(1.8) Definition

(a) An integer m is said to be *relatively prime* (or *coprime*) to an integer n if $\text{hcf}\{m, n\} = 1$.

(b) For all $n \in \mathbb{N}$, the value of $\phi(n)$ is the number of positive integers not exceeding n that are relatively prime to n. In symbols, we have

$$\phi(n) = |\{m \in \mathbb{N} : m \leq n, \text{hcf}\{m, n\} = 1\}|$$

We note in particular the following consequences of this definition:

(1.9) Corollary

(a) $\phi(1) = 1$, *and*

(b) *for* $n \geq 2$, *the value of* $\phi(n)$ *is equal to* $|\mathbb{U}_n|$, *the order of the group of units of* $\mathbb{Z}/n\mathbb{Z}$.

Two groups G and H are isomorphic if there is a bijection $f : G \to H$ such that $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$. This is equivalent to saying that there is a way of pairing off their elements so that their multiplication tables look the same.

(1.10) Questions on $\phi(n)$

(a) Work out $\phi(n)$ for $1 \leq n \leq 24$.

(b) Write down the values of n in (a) with $\phi(n) = n - 1$.

(c) What do you notice about the answer in (b)?

(d) Work out the orders of each of the elements in $\mathbb{U}_5$ and $\mathbb{U}_{10}$.

(e) We can identify $\mathbb{U}_5$ as a cyclic group by writing:

$$\mathbb{U}_5 = \{1, 2, 3, 4\} = \{2^0, 2^1, 2^2, 2^3\}$$

(since $2^3 = 3$). Write $\mathbb{U}_{10}$ in a similar way and show that the groups $\mathbb{U}_5$ and $\mathbb{U}_{10}$ are isomorphic.

Part (d) of (1.10) is a special case of the fact that two cyclic groups of the same order are isomorphic. If $G = \{g^i : 0 \leq i \leq n-1\}$ and $H = \{h^i : 0 \leq i \leq n-1\}$then the map $f : g^i \to h^i$ is an isomorphism.

Answers to (1.10)

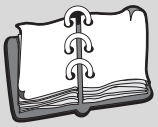
(a)

(b)

(c)

(d)

(e)



Look for *Lagrange's Theorem* in your *Foundations* (*Sets and Groups*) notes.

Recall: The *order* of a group is the number of elements in the group. The *order* of a group element g is the smallest natural number m such that $g^m = 1$. Consequently, the order of g is also the order of

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\},$$

the subgroup generated by g.

If g is an element of order m in a group G (i.e. $g^m = 1$), the powers $1, g, g^2, \ldots, g^{m-1}$ of g form a subgroup of G with m elements. (This is called the *cyclic subgroup generated by* g and is sometimes denoted by $\langle g \rangle$.) Lagrange's Theorem states that the order of a subgroup divides the order of the parent group. Hence $m = |\langle g \rangle|$ divides $|G|$ and so

the order of a group is divisible by the orders of each of its elements.

A special case of this states that if u is a unit in $\mathbb{Z}/n\mathbb{Z}$, then the order m of u divides the order $\phi(n)$ of the group of units $\mathbb{U}_n$, in other words, $\phi(n) = mm'$ for some $m' \in \mathbb{N}$. In particular, $u^{\phi(n)} = u^{mm'} = (u^m)^{m'} = 1^{m'} = 1$. This is the content of our next result.

(1.11) Euler's Theorem

(a) *If u is a unit in $\mathbb{Z}/n\mathbb{Z}$, then $u^{\phi(n)} = 1$.*

(b) *For any integer m relatively prime to n,*

$$m^{\phi(n)} \equiv 1 \pmod{n}$$

Part (b) of (1.11) is simply a restatement of part (a) in the language of congruences. If $m = kn + m_0$, then $\text{hcf}\{m, n\} = \text{hcf}\{m_0, n\}$ (convince yourself of this). Suppose that $\text{hcf}\{m, n\} = 1$ and let m_0 denote the remainder when m is divided by n ($1 \leq m_0 < n$). Then

$$m^{\phi(n)} \equiv m_0^{\phi(n)} \pmod{n} \qquad (1.d)$$

and regarding m_0 as an element of $\mathbb{U}_n$ (since $\text{hcf}\{m_0, n\} = 1$), we have the following equation in $\mathbb{Z}/n\mathbb{Z}$:

$$m_0^{\phi(n)} = 1.$$

This equation can be written in the notation of congruences (with $m_0 \in \mathbb{Z}$) thus:

$$m_0^{\phi(n)} \equiv 1 \pmod{n}. \qquad (1.e)$$

Part (b) is now the conjunction of the congruences (1.d) and (1.e).

The special case when n is prime Now let $n = p$, a prime. If $1 \leq u \leq p - 1$, evidently $\text{hcf}\{u, p\} = 1$ and therefore

$$\mathbb{U}_p = \{1, 2, \ldots, (p-1)\}$$

and $\phi(p) = p-1$. (you may have observed in (1.10)(c) that $\phi(p) = p-1$ in the case when p is a prime). This gives the following special case of Euler's Theorem;

Notation
$p \nmid m$ means 'p does not divide m'.

(1.12) Fermat's Little Theorem *Let p be a prime.*

(a) *If $p \nmid m$, then*

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

(b) *For all integers m*

$$m^p \equiv m \pmod{p}.$$

Example
$2^{16} \equiv 1 \pmod{17}$. Equivalently, $2^{17} \equiv 2 \pmod{17}$, i.e. 17 divides $2^{17} - 2$. Check this on your calculator.

If $p \nmid m$, then $\text{hcf}\{m, p\} = 1$, so part (a) follows directly from Euler's Theorem. Multiplying by m gives part (b) also (when $p \nmid m$). When $p \mid m$ then part (b) holds trivially since both sides $\equiv 0 \pmod{p}$.

Remark There are many proofs of Fermat's Little Theorem. Here are two more in outline.

(a) Prove (1.12)(b) by induction on m. The induction step uses (i) the binomial theorem

$$(m+1)^p - (m+1) = \\ (m^p - m) +_p C_1 m^{p-1} +_p C_2 m^{p-2} + \ldots +_p C_{p-1} m$$

and also the fact that (ii) when p is a prime, the binomial coefficient ${}_pC_r$ is divisible by p when $1 \leq r \leq p-1$.

(b) If $p \nmid m$, then $\text{hcf}\{p, m\} = 1$, and by WB1, $\{m, 2m, \ldots, (p-1)m\}$ is a complete set of residues mod p. Hence

$$m \times \ldots \times (p-1)m \equiv 1 \times 2 \times \ldots \times (p-1) \pmod{p}$$

or

$$m^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

whence p divides $(p-1)!(m^{p-1}-1)$. Since p does not divide $(p-1)!$, we can cancel the factor of $(p-1)!$ to get $m^{p-1} \equiv 1 \pmod{p}$.

(1.13) Question Requiring Fermat's Little Theorem Suppose p is an odd prime. Show that

$$1^p + 2^p + \ldots + p^p \equiv 0 \pmod{p}$$

Answer to (1.13)

Summary of Section 1

- We saw how to switch between congruences in $\mathbb{Z}$ and equations in $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$.
- We investigated the elements u in $\mathbb{Z}/n\mathbb{Z}$ for which $uv = 1$ for some $v \in \mathbb{Z}/n\mathbb{Z}$. These units form a group $\mathbb{U}_n$ with respect to multiplication.
- The order of the group is $\phi(n)$ equals the number of integers m coprime with n in the range $1 \leq m \leq n$.
- Lagrange's Theorem tells us that the multiplicative orders of the units in $\mathbb{Z}/n\mathbb{Z}$ divide the group order $|\mathbb{U}_n| = \phi(n)$, which translated into the language of congruences implies that $m^{\phi(n)} \equiv 1 \pmod{n}$ when $\mathrm{hcf}\{m, n\} = 1$. This is known as Euler's Theorem.
- Fermat's Little Theorem, which states that $m^p \equiv m \pmod{p}$ for all primes p and for all $m \in \mathbb{Z}$, is a special case of Euler's Theorem.

2 The Chinese Remainder Theorem

Section Targets

(a) To consider solutions to *simultaneous congruences* of the form

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

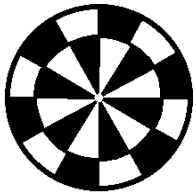
for given $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$:

- •to establish a criterion for solubility;
- •to give a method of solution.

(b) To show that there is a bijection

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

(which is an isomorphism of rings) when m and n are coprime.



Let $m, n \in \mathbb{N}$. We want to see when we can find a single number $x \in \mathbb{Z}$ satisfying simultaneously *both* $x \equiv a \pmod{m}$ *and* $x \equiv b \pmod{n}$, when a, b are given integers.

(2.1) Question about simultaneous congruences

(a) Do $x \equiv 0 \pmod{2}$ and $x \equiv 1 \pmod{2}$ have a simultaneous solution?

(b) Do $x \equiv 6 \pmod{10}$ and $x \equiv 7 \pmod{10}$ have a simultaneous solution?

(c) Do $x \equiv 6 \pmod{10}$ and $x \equiv 7 \pmod{16}$ have a simultaneous solution?

(d) Do $x \equiv 6 \pmod{10}$ and $x \equiv 8 \pmod{16}$ have a simultaneous solution?

(e) Let $c = 6a - 5b$. Show that $c \equiv a \pmod{5}$ and $c \equiv b \pmod{6}$. What does this tell you about the simultaneous congruences $x \equiv a \pmod{5}$, $x \equiv b \pmod{6}$?

Answer to (2.1)

(a)

(b)

(c)

(d)

(e)

These examples show that some condition is necessary for two congruences to have a simultaneous solution. In fact there is a rather obvious necessary condition, which turns out to be sufficient!

(2.2) Chinese Tables

(a) Fill in the table with the integers a, $0 \leq a < 12$ so that a goes in the row labelled $a \pmod 3$ and in the column labelled $a \pmod 4$:

	0	1	2	3	(mod 4)
0			6		
(mod 3) 1			10		
2			2		

(b) Repeat with $a \pmod 3$ and $a \pmod 5$ for $0 \leq a < 15$:

	0	1	2	3	4	(mod 5)
0						
(mod 3) 1						
2						

(c) What happens if you try to put the a with $0 \leq a < 24$ into a 4×6 table in the same way?

	0	1	2	3	4	5	(mod 6)
0							
(mod 4) 1							
2							
3							

Answers to (2.2)

(a)

(b)

(c)

The next question establishes the necessary condition for simultaneous congruences to have a solution.

(2.3) Establishing the necessary condition

(a) Let $h \mid m$. Show that $x \equiv a \pmod{m} \Rightarrow x \equiv a \pmod{h}$.

(b) Let $h = \text{hcf}(m, n)$. Show that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ together imply $a \equiv b \pmod{h}$.

Answers to (2.3)

(a)

(b)

Hence a necessary condition for the simultaneous solubility of $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ is $a \equiv b \pmod{h}$ where $h = \mathrm{hcf}(m, n)$. This condition is vacuous when $h = 1$, i.e. when the moduli m, n are coprime. This case is the simplest.

(2.4) Theorem: Chinese Remainder Theorem Mark I Let $m, n \in \mathbb{N}$ be coprime. Then

(a) For all $a, b \in \mathbb{Z}$ the simultaneous congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

have a solution $x \in \mathbb{Z}$.

(b) If x_1, x_2 are both solutions then $x_1 \equiv x_2 \pmod{mn}$.

Proof

(a) Since $\mathrm{hcf}(m, n) = 1$ there exist $u, v \in \mathbb{Z}$ such that $mu + nv = 1$ (Extended Euclidean Algorithm). Set $x = bmu + anv$. Then x is a solution:

$$x - a = bmu + a(nv - 1) = (b - a)mu \equiv 0 \pmod{m}$$

and similarly $x - b \equiv 0 \pmod{n}$.

(b) $x_1 \equiv a \equiv x_2 \pmod{m}$ and similarly $x_1 \equiv x_2 \pmod{n}$. So $x_1 - x_2$ is divisible both by m and by n. Since m and n are coprime it is also divisible by mn.

Example Let $m = 15$ and $n = 38$, Using the EEA (see WB1) we solve $mu + nv = 1$ to get $u = -5$, $v = 2$: $1 = -5m + 2n = -75 + 76$. Now $x = 76a - 75b$ satisfies

$$\begin{aligned} x - a &= 75(a - b) \equiv 0 \pmod{15}; \\ x - b &= 76(a - b) \equiv 0 \pmod{38}. \end{aligned}$$

For example, if $a = 7$ and $b = 8$ we find $x = 76 \cdot 7 - 75 \cdot 8 = 532 - 600 = -68$, and indeed $-68 \equiv 7 \pmod{15}$ and $-68 \equiv 8 \pmod{38}$. The general solution is $x \equiv -68 \pmod{570}$ (since $15 \cdot 38 = 570$), and the least positive solution is $x = -68 + 570 = 502$, so we may also write the general solution as $x \equiv 502 \pmod{570}$.

(2.5) Practice with CRT Let $m = 20$ and $n = 17$. Write down a formula for the general solution x to the simultaneous congruences $x \equiv a \pmod{20}$ and $x \equiv b \pmod{17}$, in terms of a and b. Hence find the least positive solution when $(a, b) = (5, 2)$ and when $(a, b) = (11, 9)$.

Answer to (2.5)

(2.6) We now turn to the general case, where the moduli are not (necessarily) coprime. We saw above that a necessary condition for a solution to exist is that $a \equiv b \pmod{h}$ where $h = \mathrm{hcf}(m, n)$. This turns out to be also sufficient.

(2.7) Theorem: Chinese Remainder Theorem Mark II Let $m, n \in \mathbb{N}$ and $h = \mathrm{hcf}(m, n)$. Let $a, b \in \mathbb{Z}$. Then the simultaneous congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

have a solution $x \in \mathbb{Z}$ if and only if $a \equiv b \pmod{h}$; any two solutions are congruent modulo $l = \mathrm{lcm}(m, n)$.

Make sure that you can prove the fact used in (b)!

(2.8) Proof of CRT II Prove this by filling in the details of this sketch:

(a) Writing $h = mu + nv$ with $u, v \in \mathbb{Z}$, set $x = (anv + bmu)/h$. Show that $x \in \mathbb{Z}$ and is a solution provided that $h \mid (b - a)$.

(b) For the last part, use the fact that any integer divisible by both m and n is also divisible by their lcm.

Answer to (2.8)

(2.9) Solve the following simultaneous congruences (or show that they have no solutions). In each case express the answer as a single congruence to an appropriate modulus, and give the least positive solution.

(a) $\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 13 \pmod{15} \end{cases}$

(b) $\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 4 \pmod{15} \end{cases}$

(c) $\begin{cases} x \equiv 10 \pmod{60} \\ x \equiv 80 \pmod{350} \end{cases}$

(d) $\begin{cases} x \equiv 2 \pmod{910} \\ x \equiv 93 \pmod{1001} \end{cases}$

To save space the details of the EEA computations have been omitted.

Answers to (2.9)

(a)

(b)

(c)

(d)

(2.10) We complete this section by giving a new view of the Chinese Remainder Theorem which goes far beyond its role so far as a tool for solving congruences: it will enable us to determine the structure of $\mathbb{Z}/n\mathbb{Z}$ (as a ring) and $\mathbb{U}_n$ (as a group), by reducing to the case where n is a prime power.

Look back at Question (2.2). This illustrates the following result.

(2.11) Chinese Remainder Theorem Mark III Let $m, n \in \mathbb{N}$ be coprime. Then there is a bijection

$$\mathbb{Z}/mn\mathbb{Z} \longleftrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

given by $a \pmod{mn} \mapsto (a \pmod{m}, a \pmod{n})$.

(2.12) Proof of (2.11) Check that the map is well-defined. Show that it is surjective and injective using the existence and uniqueness parts of Theorem (2.4) respectively.

Answer to (2.12)

(2.13) Convince yourself that the map in Theorem (2.11) preserves both addition and multiplication in the groups on both sides. (On the right-hand-side the operations are defined component-wise).

Answer to (2.13)

So the bijection between the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ mapping

$$a \pmod{mn} \mapsto (a \pmod{m}, a \pmod{n})$$

preserves both the ring operations of addition and multiplication. Such a map is called a *ring isomorphism*, so a fancier way of stating what we have proved is this:

(2.14) Corollary: Chinese Remainder Theorem Mark IV Let $m, n \in \mathbb{N}$ be coprime. Then

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

as an isomorphism of rings.

By writing n as a product of prime powers, we obtain the following version:

(2.15) Corollary Let $n \in \mathbb{N}$ have prime factorization $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ where $p_1 < p_2 < \dots < p_k$ are prime and all $e_i \geq 1$. Then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}.$$

In the next section we will see how the CRT can also apply to the unit groups $\mathbb{U}_n$. This will help us find a formula for $\phi(n)$, the order of the group $\mathbb{U}_n$.

Projects for further investigation

I. Look at simultaneous solutions to 3 or more congruences $x \equiv a_i \pmod{n_i}$ for $i = 1, 2, \dots$. What conditions on the moduli guarantees a solution for all a_i?

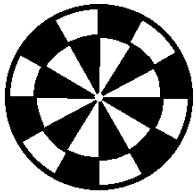
II. Consider natural numbers $n \neq 0, 1$ with at most d digits such that n^2 ends in the same d digits as n. For example, when $d = 1$, only $n = 5$ and $n = 6$ have this property; when $d = 2$, both $n = 25$ (with $n^2 = 625$) and $n = 76$ (with $n^2 = 5776$) do. Are there any others for $d = 2$? How many are there for larger d? Can you find them? Can you spot any patterns?

   This involves looking for solutions of $n^2 \equiv n \pmod{10^d}$ other than $n = 0, 1$. You should first try to solve $n^2 \equiv n \pmod{2^d}$ and $n^2 \equiv n \pmod{5^d}$, and then use CRT to put the solutions together to give solutions modulo 10^d.

Summary of Section 2

- We found a criterion for the solubility of pairs of simultaneous congruences.
- We gave a method (based on the EA) for solving simultaneous congruences, including the general solution.
- We interpreted these results as a ring isomorphism between $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ when m, n are coprime.
- We discovered that the same name (Chinese Remainder Theorem) may be used to label many different, related results.

3 Calculating $\phi(n)$



Section Targets

(a) To show that, when m, n are coprime,

$$\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$$

(isomorphism of groups: see page 6).

(b) To show that $\phi(n)$ has the important property of being multiplicative.

(c) To derive a simple formula for $\phi(n)$ from this property.

(3.1) In the tables of Question (2.2)(a,b), circle the entries a which are coprime to mn (where m and n are the numbers of rows and of columns). Also circle the row labels which are coprime to m and the column labels which are coprime to n. What do you notice?

Answers to (3.1)

(a)

(b)

This suggests the following general result, which is easy to prove.

(3.2) Let $m, n \in \mathbb{N}$ be coprime, let $a, b \in \mathbb{Z}$ and let $x = c$ be any solution to the simultaneous congruences $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$. Show that $\text{hcf}(c, mn) = 1 \iff \text{hcf}(a, m) = 1$ and $\text{hcf}(b, n) = 1$.

Answer to (3.2)

This means that in the bijection $\mathbb{Z}/mn\mathbb{Z} \leftrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, units on the left correspond to pairs of units on the right. In other words, the bijection restricts to a bijection $\mathbb{U}_{mn} \leftrightarrow \mathbb{U}_m \times \mathbb{U}_n$. And since this bijection respects the group operation (multiplcation) on both sides, it is in fact a group isomorphism:

(3.3) Corollary: Chinese Remainder Theorem Mark V Let $m, n \in \mathbb{N}$ be coprime. Then

$$\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$$

as an isomorphism of groups.

(3.4) Theorem: Multiplicativity of ϕ Let $m, n \in \mathbb{N}$ be coprime. Then

$$\phi(mn) = \phi(m)\phi(n).$$

Counting products
Make sure that you understand why

$$|A \times B| = |A| \cdot |B|$$

for all finite sets A, B, and also why

$$|A| = |A'|$$

when there is a bijection from A to A'.

(3.5) Do you see why Theorem 3.4 follows immediately from Theorem 3.3? If not, see the side panel.

(3.6) Theorem 3.4 states that the function $\phi : \mathbb{N} \to \mathbb{N}$ is *multiplicative*. It would be nice if 'being multiplicative' meant that

$$n = ab \Rightarrow \phi(n) = \phi(a)\phi(b)$$

but it does not! It only means that

$$n = ab \quad \text{with } a, b \text{ coprime} \Rightarrow \phi(n) = \phi(a)\phi(b)$$

(3.7) Definition A function $f : \mathbb{N} \to \mathbb{N}$ is said to be *multiplicative* if $f(ab) = f(a)f(b)$ for every pair of coprime numbers a and b.

Pattern?
Note the cases where $\phi(ab)$ really *is* equal to $\phi(a)\phi(b)$, and those where $\phi(ab) \neq \phi(a)\phi(b)$. What is the pattern?

(3.8) Questions on $\phi(ab)$

(a) Work out $\phi(2), \phi(4), \phi(8)$. Is $\phi(2)\phi(4) = \phi(8)$?

(b) Work out $\phi(3), \phi(6), \phi(12)$. which of the following (if any) is equal to $\phi(24)$:
(i) $\phi(2)\phi(12)$, (ii) $\phi(3)\phi(8)$, (iii) $\phi(4)\phi(6)$.

(c) In the following two cases write down all the factorisations, $n = ab$ and decide whether $\phi(ab) = \phi(a)\phi(b)$:
(i) $n = 30$, (ii) $n = 72$

(d) Which of your factorisations $72 = ab$ satisfy $\text{hcf}\{a, b\} = 1$?

Answers to (3.8)

Using the multiplicativity of ϕ we will now derive a formula for it.

Factorisation
The formula for $\phi(n)$ involves knowing all the prime factors of n. On the 1997 Number Theory exam, a number of candidates could not factorise 22500 into prime powers.

(3.9) Question on Prime Factorisation

(a) Factorise each of the following numbers into a product of primes:

$$64, 72, 168, 2419$$

(b) Factorise each of the following numbers into a product of prime powers:

$$96, 168, 22500$$

(c) Which of the following numbers are prime:

$$169, 1231, 28891$$

Recall that n is prime if and only if it fails to be divisible by all primes p satisfying $2 \leq p \leq \sqrt{n}$.

Answers to (3.9)

Primes Even though you only have to check primes up to $\sqrt{n}$, you will have noticed from (c) that it is hard work to check whether a given number n is prime.

By repeated application of this Theorem, we obtain the following:

(3.10) Corollary If the natural number n has a factorisation

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

into powers of distinct primes, then

$$\phi(n) = \phi\left(p_1^{\alpha_1}\right) \phi\left(p_2^{\alpha_2}\right) \dots \phi\left(p_t^{\alpha_t}\right)$$

(3.11) Example

$$\phi(36) = \phi(2^2)\phi(3^2) = \phi(4)\phi(9) = 2 \times 6 = 12\,.$$

To complete our task of finding a formula for $\phi(n)$ we therefore just need to find $\phi(n)$

in the case where n is a *prime power* $n = p^\alpha$.

Warning
A lot of candidates in the 1997 examination very wrongly assumed that

$$\phi(p^\alpha) = \phi(p)^\alpha$$

Since $\phi(2) = 1$ and $\phi(4) = \phi(2^2) = 2$, this cannot be the case!

(3.12) Questions on $\phi(p^\alpha)$

(a) Write down the numbers 1 to 2^4. Cross out the ones that are *not* coprime with 2^4. How many are left. Which ones did you delete?

(b) Now try to work out $\phi(2^5), \phi(3^2), \phi(3^4), \phi(7^3)$. Look for a pattern in the numbers you delete that gives you a shortcut to the answer.

Answers to (3.12)

You may have already noticed that a number is *not* coprime with p^α if and only if it is divisible by p. Thus the following numbers in the range 1 to p^α are *not* coprime with p^α:

$$p, 2p, 3p, \ldots, p^2, p^2 + p, p^2 + 2p, \ldots, p^\alpha$$

One in every p is *not* coprime with p^α; in other words $p^\alpha/p = p^{\alpha-1}$ are *not* coprime with p^α. Hence $p^\alpha - p^{\alpha-1}$ *are* coprime with p^α. You should be convinced, therefore, that

(3.13) Lemma If p is a prime and α a natural number, then

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha\left(1 - \frac{1}{p}\right)$$

We now combine this lemma and the preceding corollary to produce a theorem that enables us to easily calculate $\phi(n)$ for *any* n.

(3.14) Theorem For any natural number n,

$$\phi(n) = n \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right)$$

Proof If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ is the prime power decomposition of n, then

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{\alpha_1}\right) \dots \phi\left(p_t^{\alpha_t}\right) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \dots p_t^{\alpha_t}\left(1 - \frac{1}{p_t}\right) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right) \\
&= n \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

Warning
Do not be fooled by the first formula into thinking that $\phi(n)$ is a multiple of n! It certainly is not, since $\phi(n) < n$ (unless $n = 1$).

(3.15) When $n = \prod_{p|n} p^{\alpha}$ there are several different ways of writing the formula for $\phi(n)$:

$$\begin{aligned}
\phi(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\
&= \prod p^{\alpha}\left(1 - \frac{1}{p}\right) \\
&= \prod p^{\alpha-1}(p-1).
\end{aligned}$$

(3.16) Concluding Questions

(a) Calculate $\phi(288)$, $\phi(22500)$, $\phi(10^6)$.

(b) Write down the divisors of 24 and check that

$$\sum_{d|24} \phi(d) = 24$$

(c) If $\phi(ab) = \phi(a)\phi(b)$, does it follow that a and b are coprime?

(d) $\phi(n)$ is even for all $n \geq 3$. [Can you see any reasons for this apart from looking at the formula?]

(e) $p \mid n \implies (p-1) \mid \phi(n)$, and $p^{\alpha} \mid n \implies p^{\alpha-1} \mid \phi(n)$.

(f) $\phi(pm) = \begin{cases} p\phi(m) & \text{if } p \mid m \\ (p-1)\phi(m) & \text{if } p \nmid m \end{cases}$.

(g) $m \mid n \implies \phi(m) \mid \phi(n)$.

Answers to (3.16)

(a)

(b)

(c)

(d)

(e)

(f)

(g)

Summary of Section 3

- In general $\phi(ab) \neq \phi(a)\phi(b)$.
- The Euler ϕ-function is *multiplicative* in the sense that $\phi(ab) = \phi(a)\phi(b)$ when a and b are coprime.
- If $p_1, p_2, \ldots, p_t$ are the distinct prime divisors of a natural number n, then $\phi(n)$ is the product of n with the rational number

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_t}\right)$$