# MISCELLANEOUS TOPICS IN FIRST YEAR MATHEMATICS 

W W L CHEN

(C) W W L Chen, 1999, 2008.

This chapter is available free to all individuals, on the understanding that it is not to be used for financial gain, and may be downloaded and/or photocopied, with or without permission from the author.

However, this document may not be kept on any information storage and retrieval system without permission from the author, unless such system is not accessible to any individuals other than its owners.

## Chapter 3

## CONGRUENCES

### 3.1. Introduction

Example 3.1.1. We all know that the sum of two even integers is even, the sum of two odd integers is even, and the sum of an even integer and an odd integer is odd. Here we do not need to know the precise values of the numbers involved. Suppose that the number 0 is chosen to represent all even integers, and that the number 1 is chosen to represent all odd integers. Then the information above can be represented in the form $0+0=0,1+1=0$ and $0+1=1$. Of course, the + sign does not represent ordinary addition as we know it. In fact, it represents addition modulo 2 . Integer multiples of 2 are ignored.

Example 3.1.2. Alfred always deposits money into and withdraws money from his bank account in integer multiples of 99 dollars. On the other hand, he always keeps less than 99 dollars with him. He currently has 53 dollars. Now he sells his car for 5250 dollars and buys a computer for 2579 dollars. After visiting the bank, how much money does he have with him? To solve this problem, note that before he visits the bank, he must have $53+5250-2579=2724$ dollars. Suppose that after visiting the bank, he has $r$ dollars left. Then the integer $r$ must satisfy $0 \leq r<99$ and $r=2724-99 q$ for some integer $q$. Note that the difference between $r$ and 2724 is an integer multiple of 99 . One can check that it is possible to take $q=27$ and $r=51$. This is an example of arithmetic modulo 99. Integer multiples of 99 are ignored.

Example 3.1.3. In decimal representation for an integer, we know that if the right most digit is equal to 5 or 0 , then the integer is divisible by 5 , irrespective of any of the other digits. The contribution of the other digits gives rise to an integer which is a multiple of 5 , which we then choose to ignore. This is an example of arithmetic modulo 5 .

Example 3.1.4. In decimal representation for an integer, it is well known that the integer is divisible by 3 precisely when the sum of the digits is divisible by 3 . We shall study later this example of arithmetic modulo 3.

Let us now investigate questions like these in greater detail.
Definition. Suppose that $m, c \in \mathbb{Z}$ and $m \neq 0$. Then we say that $m$ divides $c$, denoted by $m \mid c$, if there exists $q \in \mathbb{Z}$ such that $c=m q$. In this case, we also say that $m$ is a divisor of $c$, or that $c$ is a multiple of $m$.

Example 3.1.5. For every $m \in \mathbb{Z} \backslash\{0\}, m \mid m$ and $m \mid-m$.
Example 3.1.6. For every $c \in \mathbb{Z}, 1 \mid c$ and $-1 \mid c$.
Example 3.1.7. If $m \mid c$ and $c \mid k$, then $m \mid k$. To see this, note that if $m \mid c$ and $c \mid k$, then there exist $q, s \in \mathbb{Z}$ such that $c=m q$ and $k=c s$, so that $k=m q s$. Clearly $q s \in \mathbb{Z}$.

Example 3.1.8. If $m \mid c$ and $m \mid k$, then for every $x, y \in \mathbb{Z}, m \mid(c x+k y)$. To see this, note that if $m \mid c$ and $m \mid k$, then there exist $q, s \in \mathbb{Z}$ such that $c=m q$ and $k=m s$, so that $c x+k y=m q x+m s y=$ $m(q x+s y)$. Clearly $q x+s y \in \mathbb{Z}$.

Definition. Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then we say that $a$ is congruent to $b$ modulo $m$, denoted by $a \equiv b(\bmod m)$, if $m \mid(a-b)$.

Example 3.1 .9 . We have $1999 \equiv 135(\bmod 8)$, since $1999-135=1864$ is divisible by 8 .
Example 3.1.10. Every even integer is congruent to every other even integer modulo 2.
Example 3.1.11. The square of every odd integer is congruent to 1 modulo 8 . To see this, note that every odd integer $n$ can be written in the form $n=2 k+1$, where $k \in \mathbb{Z}$. Then $n^{2}=(2 k+1)^{2}=4 k^{2}+4 k+1$, so that $n^{2}-1=4 k^{2}+4 k=4 k(k+1)$ is a multiple of 8 , since $k(k+1)$ is clearly even.

Example 3.1.12. Let us return to Example 3.1.2 concerning Alfred. We need to find an integer $r$ such that $0 \leq r<99$ and $2724 \equiv r(\bmod 99)$. A naive way to do this is to keep on subtracting 99 from 2724 until we arrive at such an integer; in other words,

$$
2724 \underbrace{-99-99-\ldots-99}_{\text {how many times? }}=r .
$$

To understand this, let us introduce the integer part function. For every $x \in \mathbb{R}$, let $[x] \in \mathbb{Z}$ be defined by $[x] \leq x<[x]+1$. It is not difficult to see that the integer $[x]$ is uniquely defined; in fact, it is the greatest integer not exceeding $x$. Now let $x=2724 / 99$. Then

$$
\left[\frac{2724}{99}\right] \leq \frac{2724}{99}<\left[\frac{2724}{99}\right]+1
$$

so that

$$
0 \leq \frac{2724}{99}-\left[\frac{2724}{99}\right]<1
$$

Multiplying throughout by 99, we obtain

$$
0 \leq 2724-99\left[\frac{2724}{99}\right]<99 .
$$

Now let

$$
r=2724-99\left[\frac{2724}{99}\right] .
$$

Clearly $2724-r$ is a multiple of 99 , so that $2724 \equiv r(\bmod 99)$. Simple calculation gives $r=51$. Note also that $[2724 / 99]=27=q$.

To formalize the calculation described in our last example, we have the following result.
PROPOSITION 3A. Suppose that $m \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $c=m q+r$ and $0 \leq r<m$.

First Proof. We shall first of all show the existence of such numbers $q, r \in \mathbb{Z}$. Let $q=[c / m]$. Then clearly $q \in \mathbb{Z}$ and

$$
\left[\frac{c}{m}\right] \leq \frac{c}{m}<\left[\frac{c}{m}\right]+1
$$

It follows that

$$
0 \leq \frac{c}{m}-\left[\frac{c}{m}\right]<1
$$

multiplying by $m$, we obtain $0 \leq c-m q<m$. Write $r=c-m q$. Clearly $r \in \mathbb{Z}$ and $0 \leq r<m$. Next we show that such numbers $q, r \in \mathbb{Z}$ are unique. Suppose that $c=m q_{1}+r_{1}=m q_{2}+r_{2}$ with $0 \leq r_{1}<m$ and $0 \leq r_{2}<m$. Then $m\left|q_{1}-q_{2}\right|=\left|r_{2}-r_{1}\right|<m$. Since $\left|q_{1}-q_{2}\right| \in \mathbb{N} \cup\{0\}$, we must have $\left|q_{1}-q_{2}\right|=0$, so that $q_{1}=q_{2}$ and so $r_{1}=r_{2}$ also.

Second Proof. To show the existence of such numbers $q, r \in \mathbb{Z}$, consider the set

$$
S=\{c-m s \geq 0: s \in \mathbb{Z}\}
$$

Then it is easy to see that $S$ is a non-empty subset of $\mathbb{N} \cup\{0\}$. It follows from the Principle of induction that $S$ has a smallest element. Let $r$ be the smallest element of $S$, and let $q \in \mathbb{Z}$ such that $c-m q=r$. Clearly $r \geq 0$, so it remains to show that $r<m$. Suppose on the contrary that $r \geq m$. Then

$$
c-m(q+1)=(c-m q)-m=r-m \geq 0
$$

so that $c-m(q+1) \in S$. Clearly $c-m(q+1)<r$, contradicting that $r$ is the smallest element of $S$. Uniqueness can be established similarly as before.

Definition. Suppose that $m \in \mathbb{N}$ and $c \in \mathbb{Z}$. The unique integer $r$ satisfying

$$
0 \leq r<m \quad \text { and } \quad c \equiv r(\bmod m)
$$

is called the residue of $c$ modulo $m$.
Remark. By Proposition 3A, the residue of $c$ modulo $m$ is the remainder when we divide $c$ by $m$.
A simple consequence of our definition is the following result.
PROPOSITION 3B. Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then $a \equiv b(\bmod m)$ if and only if $a$ and $b$ have the same residue modulo $m$.

Proof. $(\Rightarrow)$ Suppose that $r \in \mathbb{Z}$ and $0 \leq r<m$, and that $a$ has residue $r$ modulo $m$. Then there exists $q_{1} \in \mathbb{Z}$ such that $a=m q_{1}+r$. Since $a \equiv b(\bmod m)$, there exists $q \in \mathbb{Z}$ such that $b=a+m q$. It follows that $b=m\left(q_{1}+q\right)+r$, so that $b$ also has residue $r$ modulo $m$.
$(\Leftarrow)$ Suppose that both $a$ and $b$ have the same residue $r$ modulo $m$. Then $0 \leq r<m$. Furthermore, there exist $q_{1}, q_{2} \in \mathbb{Z}$ such that $a=m q_{1}+r$ and $b=m q_{2}+r$. It follows that $a-b=m\left(q_{1}-q_{2}\right)$, and so $m \mid(a-b)$.

### 3.2. Arithmetic of Congruences

Example 3.2.1. We can check that $76 \equiv 122(\bmod 23)$ and $29 \equiv 98(\bmod 23)$. We can also check that

$$
76+29 \equiv 122+98(\bmod 23) \quad \text { and } \quad 76 \times 29 \equiv 122 \times 98(\bmod 23)
$$

In other words, congruence modulo 23 is preserved by addition and multiplication.
Formally, we have the following result.
PROPOSITION 3C. Suppose that $m \in \mathbb{N}$, and that $a_{1}, a_{2}, b_{1}, b_{2} \in \mathbb{Z}$. Suppose further that $a_{1} \equiv b_{1}$ $(\bmod m)$ and $a_{2} \equiv b_{2}(\bmod m)$. Then
(a) $a_{1}+a_{2} \equiv b_{1}+b_{2}(\bmod m)$; and
(b) $a_{1} a_{2} \equiv b_{1} b_{2}(\bmod m)$.

Proof. Clearly $m \mid\left(a_{1}-b_{1}\right)$ and $m \mid\left(a_{2}-b_{2}\right)$. Hence $m \mid\left(\left(a_{1}-b_{1}\right)+\left(a_{2}-b_{2}\right)\right)=\left(a_{1}+a_{2}\right)-\left(b_{1}+b_{2}\right)$ and $m \mid\left(\left(a_{1}-b_{1}\right) a_{2}+b_{1}\left(a_{2}-b_{2}\right)\right)=a_{1} a_{2}-b_{1} b_{2}$.

Example 3.2.2. Suppose that $m, r \in \mathbb{Z}$ and $0<r<m$. It is easy to see that $0<m-r<m$ and $r+(m-r) \equiv 0(\bmod m)$. In other words, $m-r$ is the additive inverse of $r$ modulo $m$. Also, we have $0+0 \equiv 0(\bmod m)$, so that 0 is its own additive inverse modulo $m$.

Example 3.2.3. To find a multiplicative inverse of 5 modulo 7, we need to find an integer $x$ which satisfies $5 x \equiv 1(\bmod 7)$. We can do this by exhaustion, since we can impose the restriction $0 \leq x<7$ in view of Proposition $3 \mathrm{C}(\mathrm{b})$. It is easy to check that $x=3$ is the only solution under our restriction.

Example 3.2.4. To find a multiplicative inverse of 4 modulo 8, we need to find an integer $x$ which satisfies $4 x \equiv 1(\bmod 8)$. This is impossible, since for every $x \in \mathbb{Z}$, the integer $4 x-1$ is odd, and so never a multiple of 8 . Hence 4 has no multiplicative inverse modulo 8 .

Example 3.2.5. To find a multiplicative inverse of 71 modulo 113 , we need to find an integer $x$ which satisfies $71 x \equiv 1(\bmod 113)$. We may impose the restriction $0 \leq x<113$. However, trying to find a solution by exhaustion is still a very unpleasant task.

Clearly, we have two problems. The first is to decide whether a multiplicative inverse exists. The second is to develop a technique for finding it systematically.

To address the first problem, we introduce the idea of the greatest common divisor of two natural numbers, and state here without proof the following result concerning its existence and uniqueness. The interested reader may refer to Section 3.5 for a proof and further discussion.

PROPOSITION 3D. Suppose that $a, m \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ such that
(a) $d \mid a$ and $d \mid m$; and
(b) if $x \in \mathbb{N}$ satisfies $x \mid a$ and $x \mid m$, then $x \mid d$.

Definition. The number $d$ is called the greatest common divisor (GCD) of $a$ and $m$, and is denoted by $d=(a, m)$.

The answer to our first problem is given by the following result.
PROPOSITION 3E. Suppose that $a, m \in \mathbb{N}$. Then there exists a unique $x \in \mathbb{Z}$ satisfying $0 \leq x<m$ and $a x \equiv 1(\bmod m)$, if and only if the greatest common divisor $(a, m)=1$.

Proposition 3E is a special case of Proposition 3G which we shall study in the next section.

A simple way of determining the greatest common divisor $(a, m)$ is given by Euclid's algorithm. In the case when $(a, m)=1$, Euclid's algorithm also provides a systematic way of finding the multiplicative inverse of $a$ modulo $m$. We state below Euclid's algorithm without proof. Again, the interested reader may refer to Section 3.5 for a proof and further discussion.

PROPOSITION 3F. (EUCLID'S ALGORITHM) Suppose that $a, m \in \mathbb{N}$ and $a<m$. Suppose further that $q_{1}, \ldots, q_{n+1} \in \mathbb{Z}$ and $r_{1}, \ldots, r_{n} \in \mathbb{N}$ satisfy $0<r_{n}<r_{n-1}<\ldots<r_{1}<a$ and

$$
\begin{aligned}
m & =a q_{1}+r_{1}, \\
a & =r_{1} q_{2}+r_{2}, \\
r_{1} & =r_{2} q_{3}+r_{3}, \\
& \vdots \\
r_{n-2} & =r_{n-1} q_{n}+r_{n}, \\
r_{n-1} & =r_{n} q_{n+1} .
\end{aligned}
$$

Then $(a, m)=r_{n}$.
Example 3.2.6. Consider the congruence $589 x \equiv 1(\bmod 5111)$. In the notation of Euclid's algorithm, we have $a=589$ and $m=5111$. Then

$$
\begin{aligned}
5111 & =589 \times 8+399 \\
589 & =399 \times 1+190 \\
399 & =190 \times 2+19 \\
190 & =19 \times 10
\end{aligned}
$$

It follows that $(589,5111)=19$, and so 589 does not have a multiplicative inverse modulo 5111 .
Example 3.2.7. Consider the congruence $71 x \equiv 1(\bmod 113)$. In the notation of Euclid's algorithm, we have $a=71$ and $m=113$. Then

$$
\begin{aligned}
113 & =71 \times 1+42 \\
71 & =42 \times 1+29 \\
42 & =29 \times 1+13 \\
29 & =13 \times 2+3 \\
13 & =3 \times 4+1 \\
3 & =1 \times 3
\end{aligned}
$$

It follows that $(71,113)=1$, and so 71 has a multiplicative inverse modulo 113. To find the multiplicative inverse, we work backwards from the second last line to get

$$
\begin{aligned}
1 & =13+3 \times(-4) \\
& =13+(29+13 \times(-2)) \times(-4)=29 \times(-4)+13 \times 9 \\
& =29 \times(-4)+(42+29 \times(-1)) \times 9=42 \times 9+29 \times(-13) \\
& =42 \times 9+(71+42 \times(-1)) \times(-13)=71 \times(-13)+42 \times 22 \\
& =71 \times(-13)+(113+71 \times(-1)) \times 22=113 \times 22+71 \times(-35) .
\end{aligned}
$$

It follows that $71(-35) \equiv 1(\bmod 113)$. Next, the residue of -35 modulo 113 is equal to

$$
-35-113\left[-\frac{35}{113}\right]=78
$$

Hence $x=78$.

### 3.3. Linear Congruences

Example 3.3.1. Consider the congruence $5 x \equiv 2(\bmod 7)$. This can be solved by exhaustion, since we can impose the restriction $0 \leq x<7$. It is easy to check that $x=6$ is the only solution under our restriction.

Example 3.3.2. Consider the congruence $2 x \equiv 4(\bmod 8)$. Again, this can be solved by exhaustion, since we can impose the restriction $0 \leq x<8$. It is easy to check that $x=2$ and $x=6$ are the two solutions under our restriction.

Example 3.3.3. Consider the congruence $2 x \equiv 3(\bmod 8)$. Again, this can be solved by exhaustion, since we can impose the restriction $0 \leq x<8$. It is easy to check that the congruence has no solutions under our restriction. Indeed, for every $x \in \mathbb{Z}$, the integer $2 x-3$ is odd, and so never a multiple of 8 .

Example 3.3.4. Consider the congruence $71 x \equiv 19(\bmod 113)$. We may try to impose the restriction $0 \leq x<113$. However, trying to find a solution by exhaustion is still a very unpleasant task.

As in the case of finding multiplicative inverses, we again have two problems. The first is to decide whether a solution exists. The second is to develop a technique for finding all the solutions systematically.

We shall show that our task is a simple generalization of the task of determining multiplicative inverses. The first problem is answered by the following generalization of Proposition 3E. Then we shall extend the use of Euclid's algorithm to find an effective technique for solving the second problem.

PROPOSITION 3G. Suppose that $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then the congruence

$$
\begin{equation*}
a x \equiv b(\bmod m) \tag{1}
\end{equation*}
$$

is soluble if and only if $(a, m) \mid b$. In this case, the congruence (1) is the same as the congruence

$$
\begin{equation*}
\frac{a}{(a, m)} x \equiv \frac{b}{(a, m)}\left(\bmod \frac{m}{(a, m)}\right) \tag{2}
\end{equation*}
$$

which is satisfied by precisely one value $x=x_{0}$ in the range $0 \leq x<m /(a, m)$. Furthermore, the congruence (1) is satisfied by precisely all the integers $x \equiv x_{0}(\bmod m /(a, m))$.

The interested reader may refer to Section 3.5 for a proof of this result.
Remarks. (1) By Proposition 3E, the congruence

$$
\begin{equation*}
\frac{a}{(a, m)} y \equiv 1\left(\bmod \frac{m}{(a, m)}\right) \tag{3}
\end{equation*}
$$

has a unique solution satisfying $0 \leq y<m /(a, m)$. Clearly the residue $x_{0}$ of $b y /(a, m)$ modulo $m /(a, m)$ is a solution of the congruence (2), and hence the unique solution of the congruence (2) in the range $0 \leq x<m /(a, m)$. Note that

$$
\begin{equation*}
x_{0}=\frac{b y}{(a, m)}-\frac{m}{(a, m)}\left[\frac{b y}{(a, m)} / \frac{m}{(a, m)}\right]=\frac{b y}{(a, m)}-\frac{m}{(a, m)}\left[\frac{b y}{m}\right] . \tag{4}
\end{equation*}
$$

(2) In other words, to study a congruence of the type (1), we can first of all calculate the greatest common divisor ( $a, m$ ) by Euclid's algorithm. If $(a, m) \mid b$, then we concentrate on the congruence (2). To find the unique solution of (2), we first solve the congruence (3) and then use the formula (4) to complete our task.

Example 3.3.5. Consider the congruence $71 x \equiv 19(\bmod 113)$. Recall from Example 3.2 .7 that $(71,113)=1$. Hence $(71,113) \mid 19$, and so the congruence has a unique solution in the range $0 \leq x<113$. Recall also that $y=78$ is the unique solution to the congruence $71 y \equiv 1(\bmod 113)$. Hence

$$
x=19 y-113\left[\frac{19 y}{113}\right]=1482-113\left[\frac{1482}{113}\right]=13
$$

is the unique solution of the congruence $71 x \equiv 19(\bmod 113)$ in the range $0 \leq x<113$, and the congruence $71 x \equiv 19(\bmod 113)$ is satisfied by precisely all the integers $x \equiv 13(\bmod 113)$.

Example 3.3.6. Consider the congruence $96 x \equiv 36(\bmod 324)$. Using Euclid's algorithm, we have

$$
\begin{aligned}
324 & =96 \times 3+36 \\
96 & =36 \times 2+24 \\
36 & =24 \times 1+12 \\
24 & =12 \times 2
\end{aligned}
$$

It follows that $(96,324)=12$, a divisor of 36 . We next concentrate on the congruence $8 x \equiv 3(\bmod 27)$, and try to find the unique solution in the range $0 \leq x<27$. To do this, we consider the congruence $8 y \equiv 1(\bmod 27)$. Using Euclid's algorithm, we have

$$
\begin{aligned}
27 & =8 \times 3+3, \\
8 & =3 \times 2+2, \\
3 & =2 \times 1+1, \\
2 & =1 \times 2
\end{aligned}
$$

Working backwards, we obtain

$$
\begin{aligned}
1 & =3+2 \times(-1) \\
& =3+(8+3 \times(-2)) \times(-1)=8 \times(-1)+3 \times 3 \\
& =8 \times(-1)+(27+8 \times(-3)) \times 3=27 \times 3+8 \times(-10)
\end{aligned}
$$

It follows that $8(-10) \equiv 1(\bmod 27)$. Next, the residue of -10 modulo 27 is equal to

$$
-10-27\left[-\frac{10}{27}\right]=17
$$

Hence $y=17$. Since $8(17) \equiv 1(\bmod 27)$, it follows that $8(51) \equiv 3(\bmod 27)$, and the residue of 51 modulo 27 is given by

$$
51-27\left[\frac{51}{27}\right]=24
$$

Hence $x=24$ is the unique solution of the congruence $8 x \equiv 3(\bmod 27)$ in the range $0 \leq x<27$, and the congruence $96 x \equiv 36(\bmod 324)$ is satisfied by precisely all the integers $x \equiv 24(\bmod 27)$.

### 3.4. Special Divisibility Rules

Throughout this section, we shall consider natural numbers with decimal representation

$$
n=x_{k} x_{k-1} \ldots x_{3} x_{2} x_{1}
$$

where $x_{1}, \ldots, x_{k} \in\{0,1,2, \ldots, 9\}$ and $x_{k} \neq 0$, and true value

$$
n=10^{k-1} x_{k}+10^{k-2} x_{k-1}+\ldots+10^{2} x_{3}+10 x_{2}+x_{1}
$$

Remarks. (1) We know that $n$ is a multiple of 5 precisely when $x_{1} \in\{0,5\}$. Indeed,

$$
n-x_{1}=10^{k-1} x_{k}+10^{k-2} x_{k-1}+\ldots+10^{2} x_{3}+10 x_{2}
$$

is always divisible by 5 . In other words, we have $n \equiv x_{1}(\bmod 5)$, and so $n$ is divisible by 5 precisely when $x_{1}$ is divisible by 5 .
(2) We know that $n$ is a multiple of 2 precisely when $x_{1}$ is even. Indeed,

$$
n-x_{1}=10^{k-1} x_{k}+10^{k-2} x_{k-1}+\ldots+10^{2} x_{3}+10 x_{2}
$$

is always divisible by 2 . In other words, we have $n \equiv x_{1}(\bmod 2)$, and so $n$ is divisible by 2 precisely when $x_{1}$ is divisible by 2 .
(3) We know that $n$ is a multiple of 4 precisely when $x_{2} x_{1}$ is a multiple 4. Indeed,

$$
n-x_{2} x_{1}=10^{k-1} x_{k}+10^{k-2} x_{k-1}+\ldots+10^{2} x_{3}
$$

is always divisible by 4 . In other words, we have $n \equiv x_{2} x_{1}(\bmod 4)$, and so $n$ is divisible by 4 precisely when $x_{2} x_{1}$ is divisible by 4 .

PROPOSITION 3H. The natural number $n$ is a multiple of 3 precisely when the sum of its digits in decimal representation is a multiple of 3 .

Proof. Note that
$n-\left(x_{k}+x_{k-1}+\ldots+x_{3}+x_{2}+x_{1}\right)=\left(10^{k-1}-1\right) x_{k}+\left(10^{k-2}-1\right) x_{k-1}+\ldots+\left(10^{2}-1\right) x_{3}+(10-1) x_{2}$
is always divisible by 3 . In other words, we have $n \equiv x_{k}+x_{k-1}+\ldots+x_{3}+x_{2}+x_{1}(\bmod 3)$, and so $n$ is divisible by 3 precisely when $x_{k}+x_{k-1}+\ldots+x_{3}+x_{2}+x_{1}$ is divisible by 3 .

The proof of the following result is almost identical.
PROPOSITION 3J. The natural number $n$ is a multiple of 9 precisely when the sum of its digits in decimal representation is a multiple of 9 .

We state without proof the following result concerning divisibility by 11 .

PROPOSITION 3K. The natural number $n$ is a multiple of 11 precisely when the number

$$
\left(x_{1}+x_{3}+x_{5}+\ldots\right)-\left(x_{2}+x_{4}+x_{6}+\ldots\right)
$$

is a multiple of 11 .

Example 3.4.1. The number 38562907 is not a multiple of 3 , since the sum of its digits is equal to 40 , not a multiple of 3 .

Example 3.4.2. Consider the number $26348410 x 278$, where $x \in\{0,1,2, \ldots, 9\}$. The sum of its digits is equal to $45+x$. It follows that the number is divisible by 9 precisely when $x=0$ or $x=9$.

Example 3.4.3. Consider the number $26348410 x 278$ again, where $x \in\{0,1,2, \ldots, 9\}$. For the number to be divisible by 11 , the number

$$
(8+2+0+4+4+6)-(7+x+1+8+3+2)=3-x
$$

must be a multiple of 11 . This is satisfied precisely when $x=3$.
Example 3.4.4. Consider the number $37 x 2469 y 2 z$, where $x, y, z \in\{0,1,2, \ldots, 9\}$. We wish to determine all values of $x, y$ and $z$ such that the number is a multiple of $5,8,9$ and 11 simultaneously. For the number to be a multiple of 5 , we must have $z \in\{0,5\}$. For the number to be a multiple of 8 , we must have $z \neq 5$, and so $z=0$ is the only possibility. In this case, the number $y 20$ must be a multiple of 8 . This is satisfied precisely when $y \in\{1,3,5,7,9\}$. For the number to be a multiple of 9 , the number

$$
3+7+x+2+4+6+9+y+2+z=33+x+y+z=33+x+y
$$

must be a multiple of 9 . For the number to be a multiple of 11 , the number

$$
(z+y+6+2+7)-(2+9+4+x+3)=z+y-x-3=y-x-3
$$

must be a multiple of 11 . To summarize, we must have $z=0$ and

$$
\begin{aligned}
& y \in\{1,3,5,7,9\}, \\
& 9 \mid(33+x+y), \\
& 11 \mid(y-x-3)
\end{aligned}
$$

The only solution is $(x, y, z)=(0,3,0)$.

### 3.5. Further Discussion

In this section, we shall first establish the existence and uniqueness of the greatest common divisor of two given natural numbers, and prove Euclid's algorithm. We first need some results on primes.

Definition. Suppose that $a \in \mathbb{N}$ and $a>1$. Then we say that $a$ is prime if it has exactly two positive divisors, namely 1 and $a$. We also say that $a$ is composite if it is not prime.

Remark. Note that 1 is neither prime nor composite. There is a good reason for not including 1 as a prime. See the remark following Proposition 3N.

Throughout this section, the symbol $p$, with or without suffices, denotes a prime.
PROPOSITION 3L. Suppose that $a, b \in \mathbb{Z}$, and that $p \in \mathbb{N}$ is a prime. If $p \mid a b$, then $p \mid a$ or $p \mid b$.
Proof. If $a=0$ or $b=0$, then the result is trivial. We may also assume, without loss of generality, that $a>0$ and $b>0$. Suppose that $p \nmid a$. Let

$$
S=\{b \in \mathbb{N}: p \mid a b \text { and } p \nmid b\} .
$$

Clearly it is sufficient to show that $S=\emptyset$. Suppose, on the contrary, that $S \neq \emptyset$. Then since $S \subseteq \mathbb{N}$, it follows from the Principle of induction that $S$ has a smallest element. Let $c \in \mathbb{N}$ be the smallest element of $S$. Then in particular,

$$
p \mid a c \quad \text { and } \quad p \nmid c
$$

Since $p \nmid a$, we must have $c>1$. On the other hand, we must have $c<p$; for if $c \geq p$, then $c>p$, and since $p \mid a c$, we must have $p \mid a(c-p)$, so that $c-p \in S$, a contradiction. Hence $1<c<p$. By Proposition 3A, there exist $q, r \in \mathbb{Z}$ such that $p=c q+r$ and $0 \leq r<c$. Since $p$ is a prime, we must have $r \geq 1$, so that $1 \leq r<c$. However, $a r=a p-a c q$, so that $p \mid a r$. We now have

$$
p \mid a r \quad \text { and } \quad p \nmid r .
$$

But $r<c$ and $r \in \mathbb{N}$, contradicting that $c$ is the smallest element of $S$.
Using Proposition 3L a finite number of times, we have the following extension.
PROPOSITION 3M. Suppose that $a_{1}, \ldots, a_{k} \in \mathbb{Z}$, and that $p \in \mathbb{N}$ is a prime. If $p \mid a_{1} \ldots a_{k}$, then $p \mid a_{j}$ for some $j=1, \ldots, k$.

We remarked earlier that we do not include 1 as a prime. The following result is one justification.
PROPOSITION 3N. (FUNDAMENTAL THEOREM OF ARITHMETIC) Suppose that $n \in \mathbb{N}$ and $n>1$. Then $n$ is representable as a product of primes, uniquely up to the order of factors.

REmark. If 1 were to be included as a prime, then we would have to rephrase the Fundamental theorem of arithmetic to allow for different representations like $6=2 \times 3=1 \times 2 \times 3$. Note also then that the number of prime factors of 6 would not be unique.

Proof of Proposition 3 N . We shall first of all show by induction that every integer $n \geq 2$ is representable as a product of primes. Clearly 2 is a product of primes. Assume now that $n>2$ and that every $m \in \mathbb{N}$ satisfying $2 \leq m<n$ is representable as a product of primes. If $n$ is a prime, then it is obviously representable as a product of primes. If $n$ is not a prime, then there exist $n_{1}, n_{2} \in \mathbb{N}$ satisfying $2 \leq n_{1}<n$ and $2 \leq n_{2}<n$ such that $n=n_{1} n_{2}$. By our induction hypothesis, both $n_{1}$ and $n_{2}$ are representable as products of primes, so that $n$ must be representable as a product of primes.

Next we shall show uniqueness. Suppose that

$$
\begin{equation*}
n=p_{1} \ldots p_{r}=p_{1}^{\prime} \ldots p_{s}^{\prime} \tag{5}
\end{equation*}
$$

where $p_{1} \leq \ldots \leq p_{r}$ and $p_{1}^{\prime} \leq \ldots \leq p_{s}^{\prime}$ are primes. Now $p_{1} \mid p_{1}^{\prime} \ldots p_{s}^{\prime}$, so it follows from Proposition 3M that $p_{1} \mid p_{j}^{\prime}$ for some $j=1, \ldots, s$. Since $p_{1}$ and $p_{j}^{\prime}$ are both primes, we must then have $p_{1}=p_{j}^{\prime}$. On the other hand, $p_{1}^{\prime} \mid p_{1} \ldots p_{r}$, so again it follows from Proposition 3 M that $p_{1}^{\prime} \mid p_{i}$ for some $i=1, \ldots, r$, so again we must have $p_{1}^{\prime}=p_{i}$. It now follows that $p_{1}=p_{j}^{\prime} \geq p_{1}^{\prime}=p_{i} \geq p_{1}$, so that $p_{1}=p_{1}^{\prime}$. It now follows from (5) that

$$
p_{2} \ldots p_{r}=p_{2}^{\prime} \ldots p_{s}^{\prime}
$$

Repeating this argument a finite number of times, we conclude that $r=s$ and $p_{i}=p_{i}^{\prime}$ for every $i=1, \ldots, r$. $\bigcirc$

Grouping together equal primes, we can reformulate Proposition 3 N as follows.
PROPOSITION 3P. Suppose that $n \in \mathbb{N}$ and $n>1$. Then $n$ is representable uniquely in the form

$$
\begin{equation*}
n=p_{1}^{m_{1}} \ldots p_{r}^{m_{r}} \tag{6}
\end{equation*}
$$

where $p_{1}<\ldots<p_{r}$ are primes, and where $m_{j} \in \mathbb{N}$ for every $j=1, \ldots, r$.
Definition. The representation (6) is called the canonical decomposition of $n$.

Proof of Proposition 3D. If $a=1$ or $m=1$, then take $d=1$. Suppose now that $a>1$ and $m>1$. Let $p_{1}<\ldots<p_{r}$ be all the distinct prime factors of $a$ and $m$. Then by Proposition 3P, we can write

$$
\begin{equation*}
a=p_{1}^{u_{1}} \ldots p_{r}^{u_{r}} \quad \text { and } \quad m=p_{1}^{v_{1}} \ldots p_{r}^{v_{r}} \tag{7}
\end{equation*}
$$

where $u_{1}, \ldots, u_{r}, v_{1}, \ldots, v_{r} \in \mathbb{N} \cup\{0\}$. Note that in the representations (7), when $p_{j}$ is not a prime factor of $a$ (resp. $m$ ), then the corresponding exponent $u_{j}$ (resp. $v_{j}$ ) is zero. Now write

$$
d=\prod_{j=1}^{r} p_{j}^{\min \left\{u_{j}, v_{j}\right\}}
$$

Clearly $d \mid a$ and $d \mid m$. Suppose now that $x \in \mathbb{N}$ and $x \mid a$ and $x \mid m$. Then $x=p_{1}^{w_{1}} \ldots p_{r}^{w_{r}}$, where $0 \leq w_{j} \leq u_{j}$ and $0 \leq w_{j} \leq v_{j}$ for every $j=1, \ldots, r$. Clearly $x \mid d$. Finally, note that the representations (7) are unique in view of Proposition 3P, so that $d$ is uniquely defined.

Proof of Proposition 3F. We shall first of all prove that

$$
\begin{equation*}
(a, m)=\left(a, r_{1}\right) \tag{8}
\end{equation*}
$$

Note that $(a, m) \mid a$ and $(a, m) \mid\left(m-a q_{1}\right)=r_{1}$, so that $(a, m) \mid\left(a, r_{1}\right)$. On the other hand, $\left(a, r_{1}\right) \mid a$ and $\left(a, r_{1}\right) \mid\left(a q_{1}+r_{1}\right)=m$, so that $\left(a, r_{1}\right) \mid(a, m)$. (8) follows. Similarly

$$
\begin{equation*}
\left(a, r_{1}\right)=\left(r_{1}, r_{2}\right)=\left(r_{2}, r_{3}\right)=\ldots=\left(r_{n-1}, r_{n}\right) \tag{9}
\end{equation*}
$$

Note now that

$$
\begin{equation*}
\left(r_{n-1}, r_{n}\right)=\left(r_{n} q_{n+1}, r_{n}\right)=r_{n} \tag{10}
\end{equation*}
$$

The result follows on combining (8)-(10).
We next establish Proposition 3G concerning the solution of linear congruences. We begin by making a couple of simple observations.

PROPOSITION 3Q. Suppose that $m \in \mathbb{N}$, and that $a, b, c \in \mathbb{Z}$ with $c \neq 0$.
(a) If $a c \equiv b c(\bmod m)$, then $a \equiv b(\bmod m /(c, m))$, where $(c, m)$ denotes the greatest common divisor of $c$ and $m$.
(b) Furthermore, if $(c, m)=1$, then $a \equiv b(\bmod m)$.

Sketch of Proof. We have $(a-b) c=a c-b c=m q$ for some $q \in \mathbb{Z}$, so that

$$
(a-b) \frac{c}{(c, m)}=\frac{m}{(c, m)} q .
$$

The integers $c /(c, m)$ and $m /(c, m)$ have no common factors apart from $\pm 1$. It follows that $m /(c, m)$ cannot divide into $c /(c, m)$ and so must divide $a-b$, proving part (a). Part (b) is clearly obvious from part (a).

Example 3.5.1. Note that $18 \equiv 14(\bmod 4)$ implies $9 \equiv 7(\bmod 2)$ and not $9 \equiv 7(\bmod 4)$.
Definition. Suppose that $m \in \mathbb{N}$. A set $S$ of $m$ integers is said to be a complete set of residues modulo $m$ if for every integer $a \in M=\{0,1,2, \ldots, m-1\}$, there exists a unique element $x \in S$ such that $x \equiv a$ $(\bmod m)$.

Remark. Suppose that $S$ is a set of $m$ integers. Then $S$ is a complete set of residues modulo $m$ if and only if for any distinct $x, y \in S$, we have $x \not \equiv y(\bmod m)$.

Example 3.5.2. The set $\{1,12,8,19,-15\}$ is a complete set of residues modulo 5 .
PROPOSITION 3R. Suppose that $m \in \mathbb{N}$ and $k \in \mathbb{Z} \backslash\{0\}$, and that $(k, m)=1$. As $x$ runs through $a$ complete set of residues modulo $m, k x$ runs through a complete set of residues modulo $m$.

Proof. By Proposition $3 \mathrm{Q}(\mathrm{b})$, if $x \not \equiv y(\bmod m)$, then $k x \not \equiv k y(\bmod m)$. The result follows from the Remark above.

Proof of Proposition 3G. The result is trivial if $a=0$, so we assume without loss of generality that $a \neq 0$. Suppose that (1) is soluble. Then there exist $x_{0}, y_{0} \in \mathbb{Z}$ such that $a x_{0}+m y_{0}=b$, and so $(a, m) \mid b$. On the other hand, suppose that $(a, m) \mid b$. Since $(a /(a, m), m /(a, m))=1$, it follows from Proposition 3R that

$$
0, \frac{a}{(a, m)}, \frac{2 a}{(a, m)}, \ldots,\left(\frac{m}{(a, m)}-1\right) \frac{a}{(a, m)}
$$

form a complete set of residues modulo $m /(a, m)$. Hence one of the numbers $x_{0}$ in the set

$$
\left\{0,1, \ldots, \frac{m}{(a, m)}-1\right\}
$$

satisfies

$$
\begin{equation*}
\frac{a}{(a, m)} x_{0} \equiv \frac{b}{(a, m)}\left(\bmod \frac{m}{(a, m)}\right), \tag{11}
\end{equation*}
$$

whence

$$
\begin{equation*}
a x_{0} \equiv b(\bmod m) \tag{12}
\end{equation*}
$$

and so (1) is soluble. Furthermore, if $x \equiv x_{0}(\bmod m /(a, m))$, then (11) and hence also (12) hold with $x_{0}$ replaced by $x$. To show that the residue class $x_{0}$ modulo $m /(a, m)$ gives all the solutions, let $x$ be any solution of $(1)$. Then $a\left(x-x_{0}\right) \equiv 0(\bmod m)$. By Proposition 3Q, we have $x-x_{0} \equiv 0(\bmod m /(a, m))$.

We complete this chapter by establishing the following famous result concerning simultaneous linear congruences.

PROPOSITION 3S. (CHINESE REMAINDER THEOREM) Suppose that $n>1$, and that the numbers $m_{1}, \ldots, m_{n} \in \mathbb{N}$ are pairwise coprime; in other words, $\left(m_{i}, m_{j}\right)=1$ whenever $1 \leq i<j \leq n$. Suppose further that $a_{1}, \ldots, a_{n} \in \mathbb{Z}$. Then the simultaneous congruences

$$
\begin{aligned}
x & \equiv a_{1}\left(\bmod m_{1}\right) \\
& \vdots \\
x & \equiv a_{n}\left(\bmod m_{n}\right)
\end{aligned}
$$

are satisfied by precisely the members of a unique residue class modulo $m_{1} \ldots m_{n}$.
Proof. For every $j=1, \ldots, n$, write $q_{j}=m_{1} \ldots m_{j-1} m_{j+1} \ldots m_{n}$. Then $\left(q_{j}, m_{j}\right)=1$. By Proposition 3G, there exists $k_{j} \in \mathbb{Z}$ such that $q_{j} k_{j} \equiv a_{j}\left(\bmod m_{j}\right)$. Now let

$$
x_{0}=\sum_{j=1}^{n} q_{j} k_{j} .
$$

If $x \equiv x_{0}\left(\bmod m_{1} \ldots m_{n}\right)$, then $x \equiv x_{0} \equiv q_{i} k_{i} \equiv a_{i}\left(\bmod m_{i}\right)$ for every $i=1, \ldots, n$. On the other hand, if $x$ is a solution to the simultaneous congruences, then $x \equiv a_{i} \equiv x_{0}\left(\bmod m_{i}\right)$ for every $i=1, \ldots, n$. Hence $x \equiv x_{0}\left(\bmod m_{1} \ldots m_{n}\right)$.

## Problems for Chapter 3

1. Prove the following version of Proposition 3A: Suppose that $m \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $c=m q+r$ and $1 \leq r \leq m$.
2. a) Find the multiplicative inverse of each of the numbers $1,2,3,4,5,6$ modulo 7 , if it exists.
b) Find the multiplicative inverse of each of the numbers $1,2,3,4,5,6,7$ modulo 8 , if it exists.
c) Can you comment on the above?
3. For each of the following congruences, find all solutions $x$ satisfying $0 \leq x<10$ :
a) $3 x \equiv 1(\bmod 10)$
b) $2 x \equiv 4(\bmod 10)$
c) $5 x \equiv 2(\bmod 10)$
4. For each of the following linear congruences, find by exhaustion all the solutions, if any:
a) $6 x \equiv 1(\bmod 7)$
b) $6 x \equiv 2(\bmod 7)$
c) $6 x \equiv 1(\bmod 8)$
d) $6 x \equiv 2(\bmod 8)$
5. Solve the congruence $6 x \equiv 7(\bmod 13)$.
6. Solve the congruence $z^{2}+3 z+2 \equiv 0(\bmod 5)$.
7. Solve each of the following congruences modulo 5 and modulo 6 :
a) $x^{2}+2 x+2 \equiv 0$
b) $x^{2}+2 x+3 \equiv 0$
8. Solve each of the following congruences:
a) $x^{75}+6 x^{49}+3 x^{2}+1 \equiv 0(\bmod 7)$
b) $x^{47}+3 x^{22}+4 x^{7}+3 x^{2}+1 \equiv 0(\bmod 5)$
9. This is one of those rare occasions when you will find a calculator useful in mathematics. So take out your toy and have a go.
a) Find the residue of 274659278 modulo 1687 .
b) Find the residue of -274659287 modulo 1687 .
c) Find the residue of the sum of $289574837,-146827648$ and 127048729 modulo 3.
d) Find the residue of the product of $289574837,-146827648$ and 127048729 modulo 3 .
[Hint: For part (d), it may be a little tricky to find the product of the three numbers, even though you may have a state-of-the-art toy. Try to use some theory instead, with the help of your calculator.]
10. Find the remainder of $2123456789 \times 5123456789 \times 7123456789 \times 11123456789 \times 13123456789$ on division by 3 . Explain your argument carefully, quoting relevant results.
[Hint: The product contains 50 digits, so your calculator is unlikely to cope. Nevertheless, your calculator will be of some help.]
11. Suppose that $a, b, n \in \mathbb{N}$,
a) Show that if $a \equiv b(\bmod 2 n)$, then $a^{2} \equiv b^{2}(\bmod 4 n)$.
b) Suppose that $k \in \mathbb{N}$. Show that if $a \equiv b(\bmod k n)$, then $a^{k} \equiv b^{k}\left(\bmod k^{2} n\right)$.
12. Use Euclid's algorithm to find the gcd of 35 and 79.
13. For each of the following, use Euclid's algorithm to determine whether the multiplicative inverse exists, and if so, determine its value:
a) $13(\bmod 29)$
b) $74(\bmod 111)$
c) $113(\bmod 549)$
d) $279(\bmod 303)$
14. You are given that $4 \times 79-9 \times 35=1$.
a) Find the inverse of $35(\bmod 79)$.
b) Use part (a) to solve the congruence $35 x \equiv 3(\bmod 79)$.
15. a) Show that $28^{-1} \equiv 4(\bmod 37)$.
b) Hence solve the congruence $28 x \equiv 19(\bmod 37)$.
16. a) Use Euclid's algorithm to show that $(136,311)=1$.
b) Find an integer $y$ satisfying $0 \leq y<311$ and $136 y \equiv 1(\bmod 311)$.
c) Find an integer $x$ satisfying $0 \leq x<311$ and $136 x \equiv 2(\bmod 311)$.
17. a) Use Euclid's algorithm to show that $(219,313)=1$.
b) Find a positive integer $y<313$ which satisfies $219 y \equiv 1(\bmod 313)$.
c) Use part (b) to find a positive integer $x<313$ which satisfies $219 x \equiv 4(\bmod 313)$.
d) Are your solutions in parts (b) and (c) unique?
18. a) Use Euclid's algorithm to show that $(121,391)=1$.
b) Find a positive integer $y<391$ which satisfies $121 y \equiv 1(\bmod 391)$.
c) Use part (b) to find a positive integer $x<391$ which satisfies $121 x \equiv 3(\bmod 391)$.
d) Are your solutions in parts (b) and (c) unique?
19. a) Use Euclid's algorithm to show that $(152,333)=1$.
b) Find a positive integer $y<333$ which satisfies $152 y \equiv 1(\bmod 333)$.
c) Use part (b) to find a positive integer $x<333$ which satisfies $152 x \equiv 3(\bmod 333)$.
d) Are your solutions in parts (b) and (c) unique?
20. For each of the following congruences, use Euclid's algorithm to determine whether the congruence is soluble, and if so, determine also the solutions:
a) $377 x \equiv 53(\bmod 481)$
b) $377 x \equiv 58(\bmod 464)$
21. Find $n \in \mathbb{N}$ for which $2^{n} \equiv 1(\bmod 5)$. Deduce the remainder when $2^{50}+1$ is divided by 5 .
22. Find $n \in \mathbb{N}$ for which $2^{n} \equiv 1(\bmod 31)$. Deduce the remainder when $2^{100}$ is divided by 31 .
23. Follow the steps below to find all digit pairs $(x, y)$ such that the integer $1 x 31 y 56$ in decimal notation is a multiple of both 3 and 11:
a) Show that the integer is a multiple of 11 precisely when $x-y \equiv 4(\bmod 11)$.
b) Find all the nine digit pairs $(x, y)$ for which the integer is a multiple of 11 .
c) Show that the integer is a multiple of 3 precisely when $x+y \equiv 2(\bmod 3)$.
d) Show that there are precisely three digit pairs $(x, y)$ in part (b) for which the integer is a multiple of 3 .
24. The number $1974 x 17 y 940 z$ is divisible by both 8 and 11 , and has residue 1 modulo 3 . Follow the steps below to determine all the possible values of the triplet $(x, y, z)$ :
a) Explain why $z=0$ or $z=8$.
b) Consider the case when $z=0$. Use arithmetic modulo 3 and modulo 11 to determine all the possible values of the triplet $(x, y, 0)$.
c) Consider the case when $z=8$. Use arithmetic modulo 3 and modulo 11 to determine all the possible values of the triplet $(x, y, 8)$.
