MISCELLANEOUS TOPICS IN FIRST YEAR MATHEMATICS

W W L CHEN

© 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 $0 \le r < 99$ and r = 2724 - 99q 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 = mq. 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 $m \in \mathbb{Z} \setminus \{0\}, m \mid m \text{ and } m \mid -m$.

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 = mq and k = cs, so that k = mqs. Clearly $qs \in \mathbb{Z}$.

EXAMPLE 3.1.8. If $m \mid c$ and $m \mid k$, then for every $x, y \in \mathbb{Z}$, $m \mid (cx + ky)$. To see this, note that if $m \mid c$ and $m \mid k$, then there exist $q, s \in \mathbb{Z}$ such that c = mq and k = ms, so that cx + ky = mqx + msy = m(qx + sy). Clearly $qx + sy \in \mathbb{Z}$.

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 $a \equiv b \pmod{m}$, if $m \mid (a - b)$.

EXAMPLE 3.1.9. We have $1999 \equiv 135 \pmod{8}$, 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 = 2k + 1, where $k \in \mathbb{Z}$. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$, so that $n^2 - 1 = 4k^2 + 4k = 4k(k + 1)$ 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 $0 \le r < 99$ and $2724 \equiv r \pmod{99}$. 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

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

so that

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

Multiplying throughout by 99, we obtain

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

Now let

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

 $Chapter \ 3 \ : \ Congruences$

Clearly 2724 - r is a multiple of 99, so that $2724 \equiv r \pmod{99}$. 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 = mq + 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

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

multiplying by m, we obtain $0 \le c - mq < m$. Write r = c - mq. Clearly $r \in \mathbb{Z}$ and $0 \le r < m$. Next we show that such numbers $q, r \in \mathbb{Z}$ are unique. Suppose that $c = mq_1 + r_1 = mq_2 + r_2$ with $0 \le r_1 < m$ and $0 \le r_2 < m$. Then $m|q_1 - q_2| = |r_2 - r_1| < m$. Since $|q_1 - q_2| \in \mathbb{N} \cup \{0\}$, we must have $|q_1 - q_2| = 0$, so that $q_1 = q_2$ and so $r_1 = r_2$ also. \bigcirc

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

$$S = \{c - ms \ge 0 : s \in \mathbb{Z}\}.$$

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 - mq = r. Clearly $r \geq 0$, so it remains to show that r < m. Suppose on the contrary that $r \geq m$. Then

$$c - m(q+1) = (c - mq) - m = r - m \ge 0,$$

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. \bigcirc

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

$$0 \le r < m$$
 and $c \equiv r \pmod{m}$

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 $a \equiv b \pmod{m}$ if and only if a and b have the same residue modulo m.

PROOF. (\Rightarrow) Suppose that $r \in \mathbb{Z}$ and $0 \le r < m$, and that *a* has residue *r* modulo *m*. Then there exists $q_1 \in \mathbb{Z}$ such that $a = mq_1 + r$. Since $a \equiv b \pmod{m}$, there exists $q \in \mathbb{Z}$ such that b = a + mq. It follows that $b = m(q_1 + q) + r$, so that *b* also has residue *r* modulo *m*.

(⇐) Suppose that both a and b have the same residue r modulo m. Then $0 \le r < m$. Furthermore, there exist $q_1, q_2 \in \mathbb{Z}$ such that $a = mq_1 + r$ and $b = mq_2 + r$. It follows that $a - b = m(q_1 - q_2)$, and so $m \mid (a - b)$. \bigcirc

3.2. Arithmetic of Congruences

EXAMPLE 3.2.1. We can check that $76 \equiv 122 \pmod{23}$ and $29 \equiv 98 \pmod{23}$. We can also check that

 $76 + 29 \equiv 122 + 98 \pmod{23}$ and $76 \times 29 \equiv 122 \times 98 \pmod{23}$.

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 $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$. Then (a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$; and (b) $a_1a_2 \equiv b_1b_2 \pmod{m}$.

PROOF. Clearly $m \mid (a_1 - b_1)$ and $m \mid (a_2 - b_2)$. Hence $m \mid ((a_1 - b_1) + (a_2 - b_2)) = (a_1 + a_2) - (b_1 + b_2)$ and $m \mid ((a_1 - b_1)a_2 + b_1(a_2 - b_2)) = a_1a_2 - b_1b_2$. \bigcirc

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 $r + (m - r) \equiv 0 \pmod{m}$. In other words, m - r is the additive inverse of r modulo m. Also, we have $0 + 0 \equiv 0 \pmod{m}$, 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 $5x \equiv 1 \pmod{7}$. We can do this by exhaustion, since we can impose the restriction $0 \le x < 7$ in view of Proposition 3C(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 $4x \equiv 1 \pmod{8}$. This is impossible, since for every $x \in \mathbb{Z}$, the integer 4x - 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 $71x \equiv 1 \pmod{113}$. We may impose the restriction $0 \le x < 113$. 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) $d \mid a \text{ and } d \mid m$; and
- (b) if $x \in \mathbb{N}$ satisfies $x \mid a \text{ and } x \mid m$, 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 $0 \le x < m$ and $ax \equiv 1 \pmod{m}$, 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

```
m = aq_1 + r_1,

a = r_1q_2 + r_2,

r_1 = r_2q_3 + r_3,

\vdots

r_{n-2} = r_{n-1}q_n + r_n,

r_{n-1} = r_nq_{n+1}.
```

Then $(a,m) = r_n$.

EXAMPLE 3.2.6. Consider the congruence $589x \equiv 1 \pmod{5111}$. In the notation of Euclid's algorithm, we have a = 589 and m = 5111. Then

$$5111 = 589 \times 8 + 399,$$

$$589 = 399 \times 1 + 190,$$

$$399 = 190 \times 2 + 19,$$

$$190 = 19 \times 10.$$

It follows that (589, 5111) = 19, and so 589 does not have a multiplicative inverse modulo 5111.

EXAMPLE 3.2.7. Consider the congruence $71x \equiv 1 \pmod{113}$. In the notation of Euclid's algorithm, we have a = 71 and m = 113. Then

```
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.
```

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

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

It follows that $71(-35) \equiv 1 \pmod{113}$. Next, the residue of $-35 \pmod{113}$ 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 $5x \equiv 2 \pmod{7}$. This can be solved by exhaustion, since we can impose the restriction $0 \le x < 7$. It is easy to check that x = 6 is the only solution under our restriction.

EXAMPLE 3.3.2. Consider the congruence $2x \equiv 4 \pmod{8}$. 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 $2x \equiv 3 \pmod{8}$. Again, this can be solved by exhaustion, since we can impose the restriction $0 \le x < 8$. It is easy to check that the congruence has no solutions under our restriction. Indeed, for every $x \in \mathbb{Z}$, the integer 2x - 3 is odd, and so never a multiple of 8.

EXAMPLE 3.3.4. Consider the congruence $71x \equiv 19 \pmod{113}$. 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

$$ax \equiv b \pmod{m} \tag{1}$$

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

$$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \left(\mod \frac{m}{(a,m)} \right)$$
(2)

which is satisfied by precisely one value $x = x_0$ in the range $0 \le x < m/(a,m)$. Furthermore, the congruence (1) is satisfied by precisely all the integers $x \equiv x_0 \pmod{m/(a,m)}$.

The interested reader may refer to Section 3.5 for a proof of this result.

REMARKS. (1) By Proposition 3E, the congruence

$$\frac{a}{(a,m)}y \equiv 1 \pmod{\frac{m}{(a,m)}}$$
(3)

has a unique solution satisfying $0 \le y < m/(a, m)$. Clearly the residue x_0 of by/(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 $0 \le x < m/(a, m)$. Note that

$$x_0 = \frac{by}{(a,m)} - \frac{m}{(a,m)} \left[\frac{by}{(a,m)} \middle/ \frac{m}{(a,m)} \right] = \frac{by}{(a,m)} - \frac{m}{(a,m)} \left[\frac{by}{m} \right].$$
(4)

(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) | 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 $71x \equiv 19 \pmod{113}$. 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 $0 \le x < 113$. Recall also that y = 78 is the unique solution to the congruence $71y \equiv 1 \pmod{113}$. Hence

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

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

EXAMPLE 3.3.6. Consider the congruence $96x \equiv 36 \pmod{324}$. Using Euclid's algorithm, we have

$$324 = 96 \times 3 + 36,$$

$$96 = 36 \times 2 + 24,$$

$$36 = 24 \times 1 + 12,$$

$$24 = 12 \times 2.$$

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

$$27 = 8 \times 3 + 3, 8 = 3 \times 2 + 2, 3 = 2 \times 1 + 1, 2 = 1 \times 2.$$

Working backwards, we obtain

$$1 = 3 + 2 \times (-1)$$

= 3 + (8 + 3 × (-2)) × (-1) = 8 × (-1) + 3 × 3
= 8 × (-1) + (27 + 8 × (-3)) × 3 = 27 × 3 + 8 × (-10).

It follows that $8(-10) \equiv 1 \pmod{27}$. Next, the residue of $-10 \mod{27}$ is equal to

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

Hence y = 17. Since $8(17) \equiv 1 \pmod{27}$, it follows that $8(51) \equiv 3 \pmod{27}$, 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 $8x \equiv 3 \pmod{27}$ in the range $0 \le x < 27$, and the congruence $96x \equiv 36 \pmod{324}$ is satisfied by precisely all the integers $x \equiv 24 \pmod{27}$.

3.4. Special Divisibility Rules

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

$$n = x_k x_{k-1} \dots x_3 x_2 x_1,$$

where $x_1, ..., x_k \in \{0, 1, 2, ..., 9\}$ and $x_k \neq 0$, and true value

$$n = 10^{k-1}x_k + 10^{k-2}x_{k-1} + \ldots + 10^2x_3 + 10x_2 + x_1.$$

REMARKS. (1) We know that n is a multiple of 5 precisely when $x_1 \in \{0, 5\}$. Indeed,

$$n - x_1 = 10^{k-1}x_k + 10^{k-2}x_{k-1} + \ldots + 10^2x_3 + 10x_2$$

is always divisible by 5. In other words, we have $n \equiv x_1 \pmod{5}$, 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,

$$n - x_1 = 10^{k-1}x_k + 10^{k-2}x_{k-1} + \ldots + 10^2x_3 + 10x_2$$

is always divisible by 2. In other words, we have $n \equiv x_1 \pmod{2}$, 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_2x_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 $n \equiv x_2 x_1 \pmod{4}$, 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

$$n - (x_k + x_{k-1} + \ldots + x_3 + x_2 + x_1) = (10^{k-1} - 1)x_k + (10^{k-2} - 1)x_{k-1} + \ldots + (10^2 - 1)x_3 + (10 - 1)x_2 + (10^{k-1} - 1)x_k + (10^{k-2} - 1)x_{k-1} + \ldots + (10^{k-1} - 1)x_k + (10^{k-2} - 1)x_{k-1} + \ldots + (10^{k-1} - 1)x_k + (10^{k-2} - 1)x_{k-1} + \ldots + (10^{k-1} - 1)x_k + (10^{k-1} - 1)x_k$$

is always divisible by 3. In other words, we have $n \equiv x_k + x_{k-1} + \ldots + x_3 + x_2 + x_1 \pmod{3}$, 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. \bigcirc

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

$$(x_1 + x_3 + x_5 + \ldots) - (x_2 + x_4 + x_6 + \ldots)$$

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 26348410x278, where $x \in \{0, 1, 2, ..., 9\}$. 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 26348410x278 again, where $x \in \{0, 1, 2, ..., 9\}$. 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 37x2469y2z, where $x, y, z \in \{0, 1, 2, ..., 9\}$. 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 y20 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

$$y \in \{1, 3, 5, 7, 9\},\$$

9 | (33 + x + y),
11 | (y - x - 3).

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 $p \mid ab$, 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

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

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,

$$p \mid ac$$
 and $p \nmid c$.

Since $p \nmid a$, we must have c > 1. On the other hand, we must have c < p; for if $c \ge p$, then c > p, and since $p \mid ac$, 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 = cq + r and $0 \le r < c$. Since p is a prime, we must have $r \ge 1$, so that $1 \le r < c$. However, ar = ap - acq, so that $p \mid ar$. We now have

 $p \mid ar$ and $p \nmid r$.

But r < c and $r \in \mathbb{N}$, contradicting that c is the smallest element of S. \bigcirc

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 3N. We shall first of all show by induction that every integer $n \ge 2$ 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 $2 \le m < n$ 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 $2 \le n_1 < n$ and $2 \le n_2 < n$ such that $n = n_1 n_2$. By our induction hypothesis, both n_1 and n_2 are representable as a products of primes, so that n must be representable as a product of primes.

Next we shall show uniqueness. Suppose that

$$n = p_1 \dots p_r = p'_1 \dots p'_s,\tag{5}$$

where $p_1 \leq \ldots \leq p_r$ and $p'_1 \leq \ldots \leq p'_s$ are primes. Now $p_1 \mid p'_1 \ldots p'_s$, so it follows from Proposition 3M that $p_1 \mid p'_j$ for some $j = 1, \ldots, s$. Since p_1 and p'_j are both primes, we must then have $p_1 = p'_j$. On the other hand, $p'_1 \mid p_1 \ldots p_r$, so again it follows from Proposition 3M that $p'_1 \mid p_i$ for some $i = 1, \ldots, r$, so again we must have $p'_1 = p_i$. It now follows that $p_1 = p'_j \geq p'_1 = p_i \geq p_1$, so that $p_1 = p'_1$. It now follows from (5) that

$$p_2 \dots p_r = p'_2 \dots p'_s.$$

Repeating this argument a finite number of times, we conclude that r = s and $p_i = p'_i$ for every $i = 1, \ldots, r$. \bigcirc

Grouping together equal primes, we can reformulate Proposition 3N as follows.

PROPOSITION 3P. Suppose that $n \in \mathbb{N}$ and n > 1. Then n is representable uniquely in the form

$$n = p_1^{m_1} \dots p_r^{m_r},\tag{6}$$

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

$$a = p_1^{u_1} \dots p_r^{u_r}$$
 and $m = p_1^{v_1} \dots p_r^{v_r}$, (7)

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

$$d = \prod_{j=1}^{r} p_j^{\min\{u_j, v_j\}}$$

Clearly $d \mid a$ and $d \mid m$. Suppose now that $x \in \mathbb{N}$ and $x \mid a$ and $x \mid m$. Then $x = p_1^{w_1} \dots p_r^{w_r}$, where $0 \leq w_j \leq u_j$ and $0 \leq w_j \leq v_j$ for every $j = 1, \dots, r$. Clearly $x \mid d$. Finally, note that the representations (7) are unique in view of Proposition 3P, so that d is uniquely defined. \bigcirc

PROOF OF PROPOSITION 3F. We shall first of all prove that

$$(a,m) = (a,r_1).$$
 (8)

Note that (a,m) | a and $(a,m) | (m - aq_1) = r_1$, so that $(a,m) | (a,r_1)$. On the other hand, $(a,r_1) | a$ and $(a,r_1) | (aq_1 + r_1) = m$, so that $(a,r_1) | (a,m)$. (8) follows. Similarly

$$(a, r_1) = (r_1, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n).$$
(9)

Note now that

$$(r_{n-1}, r_n) = (r_n q_{n+1}, r_n) = r_n.$$
(10)

The result follows on combining (8)–(10). \bigcirc

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 $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/(c,m)}$, where (c,m) denotes the greatest common divisor of c and m.
- (b) Furthermore, if (c, m) = 1, then $a \equiv b \pmod{m}$.

SKETCH OF PROOF. We have (a - b)c = ac - bc = mq 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 ± 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). \bigcirc

EXAMPLE 3.5.1. Note that $18 \equiv 14 \pmod{4}$ implies $9 \equiv 7 \pmod{2}$ and not $9 \equiv 7 \pmod{4}$.

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 $a \in M = \{0, 1, 2, ..., m - 1\}$, there exists a unique element $x \in S$ such that $x \equiv a \pmod{m}$.

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 $x \not\equiv y \pmod{m}$.

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 $k \in \mathbb{Z} \setminus \{0\}$, and that (k, m) = 1. As x runs through a complete set of residues modulo m, kx runs through a complete set of residues modulo m.

PROOF. By Proposition 3Q(b), if $x \not\equiv y \pmod{m}$, then $kx \not\equiv ky \pmod{m}$. The result follows from the Remark above. \bigcirc

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 $ax_0 + my_0 = b$, 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

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

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

$$\frac{a}{(a,m)}x_0 \equiv \frac{b}{(a,m)} \left(\mod \frac{m}{(a,m)} \right), \tag{11}$$

whence

$$ax_0 \equiv b \pmod{m},\tag{12}$$

and so (1) is soluble. Furthermore, if $x \equiv x_0 \pmod{m/(a,m)}$, then (11) and hence also (12) hold with x_0 replaced by x. To show that the residue class $x_0 \mod m/(a,m)$ gives all the solutions, let x be any solution of (1). Then $a(x - x_0) \equiv 0 \pmod{m}$. By Proposition 3Q, we have $x - x_0 \equiv 0 \pmod{m/(a,m)}$.

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, $(m_i, m_j) = 1$ whenever $1 \leq i < j \leq n$. Suppose further that $a_1, \ldots, a_n \in \mathbb{Z}$. Then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

are satisfied by precisely the members of a unique residue class modulo $m_1 \dots m_n$.

PROOF. For every j = 1, ..., n, write $q_j = m_1 ... m_{j-1} m_{j+1} ... m_n$. Then $(q_j, m_j) = 1$. By Proposition 3G, there exists $k_j \in \mathbb{Z}$ such that $q_j k_j \equiv a_j \pmod{m_j}$. Now let

$$x_0 = \sum_{j=1}^n q_j k_j.$$

If $x \equiv x_0 \pmod{m_1 \dots m_n}$, then $x \equiv x_0 \equiv q_i k_i \equiv a_i \pmod{m_i}$ for every $i = 1, \dots, n$. On the other hand, if x is a solution to the simultaneous congruences, then $x \equiv a_i \equiv x_0 \pmod{m_i}$ for every $i = 1, \dots, n$. Hence $x \equiv x_0 \pmod{m_1 \dots m_n}$.

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 = mq + 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 $0 \le x < 10$:
- a) $3x \equiv 1 \pmod{10}$ b) $2x \equiv 4 \pmod{10}$
- c) $5x \equiv 2 \pmod{10}$
- 4. For each of the following linear congruences, find by exhaustion all the solutions, if any:
 - a) $6x \equiv 1 \pmod{7}$ b) $6x \equiv 2 \pmod{7}$ c) $6x \equiv 1 \pmod{8}$ d) $6x \equiv 2 \pmod{8}$
- 5. Solve the congruence $6x \equiv 7 \pmod{13}$.
- 6. Solve the congruence $z^2 + 3z + 2 \equiv 0 \pmod{5}$.
- 7. Solve each of the following congruences modulo 5 and modulo 6: a) $x^2 + 2x + 2 \equiv 0$ b) $x^2 + 2x + 3 \equiv 0$
- 8. Solve each of the following congruences: a) $x^{75} + 6x^{49} + 3x^2 + 1 \equiv 0 \pmod{7}$

b) $x^{47} + 3x^{22} + 4x^7 + 3x^2 + 1 \equiv 0 \pmod{5}$

- 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 × 5123456789 × 7123456789 × 11123456789 × 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 $a \equiv b \pmod{2n}$, then $a^2 \equiv b^2 \pmod{4n}$.
 - b) Suppose that $k \in \mathbb{N}$. Show that if $a \equiv b \pmod{kn}$, then $a^k \equiv b^k \pmod{k^2n}$.
- 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 (mod 29) b) 74 (mod 111) c) 113 (mod 549) d) 279 (mod 303)
- 14. You are given that $4 \times 79 9 \times 35 = 1$.
 - a) Find the inverse of 35 (mod 79).
 - b) Use part (a) to solve the congruence $35x \equiv 3 \pmod{79}$.

- 15. a) Show that $28^{-1} \equiv 4 \pmod{37}$.
 - b) Hence solve the congruence $28x \equiv 19 \pmod{37}$.
- 16.a) Use Euclid's algorithm to show that (136, 311) = 1.
 - b) Find an integer y satisfying $0 \le y < 311$ and $136y \equiv 1 \pmod{311}$.
 - c) Find an integer x satisfying $0 \le x < 311$ and $136x \equiv 2 \pmod{311}$.
- 17.a) Use Euclid's algorithm to show that (219, 313) = 1.
 - b) Find a positive integer y < 313 which satisfies $219y \equiv 1 \pmod{313}$.
 - c) Use part (b) to find a positive integer x < 313 which satisfies $219x \equiv 4 \pmod{313}$.
 - 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 $121y \equiv 1 \pmod{391}$.
 - c) Use part (b) to find a positive integer x < 391 which satisfies $121x \equiv 3 \pmod{391}$.
 - 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 $152y \equiv 1 \pmod{333}$.
 - c) Use part (b) to find a positive integer x < 333 which satisfies $152x \equiv 3 \pmod{333}$.
 - 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) 377x ≡ 53 (mod 481)
 b) 377x ≡ 58 (mod 464)
- 21. Find $n \in \mathbb{N}$ for which $2^n \equiv 1 \pmod{5}$. Deduce the remainder when $2^{50} + 1$ is divided by 5.
- 22. Find $n \in \mathbb{N}$ for which $2^n \equiv 1 \pmod{31}$. 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 1x31y56 in decimal notation is a multiple of both 3 and 11:
 - a) Show that the integer is a multiple of 11 precisely when $x y \equiv 4 \pmod{11}$.
 - 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 $x + y \equiv 2 \pmod{3}$.
 - 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 1974x17y940z 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).