13.1 Congruences

Without carrying out any ‘long multiplication’ show that

(i) $1234567 \times 90123 \equiv 1 \pmod{10}$,
(ii) $2468 \times 13579 \equiv -3 \pmod{25}$.

Solution  This exercise relies on the second part of Theorem 13.1. Note that, in part (i), working modulo 10 is equivalent to taking the final digit.

(i) $1234567 \times 90123 \equiv 7 \times 3 = 21 \equiv 1$,
(ii) $2468 \times 13579 \equiv 18 \times 4 = 72 \equiv -3$. 
Solutions to Chapter 13 Exercises
in Discrete Mathematics by Norman L. Biggs;
2nd Edition 2002

13.1.2

Use the method of casting out nines to show that two of the following equations are false. What can be said about the other equation?

(i) \( 5783 \times 40162 = 233256846 \),
(ii) \( 9787 \times 1258 = 12342046 \),
(iii) \( 8901 \times 5743 = 52018443 \).

Solution  The method is to take the sum of the digits in each number, and repeat if necessary, until we have a statement that is easy to check. If the final statement is false, the original one must also be false. If the final statement is true, the original statement may be true, but it could be false.

(i)
\[
\begin{array}{c}
5783 \times 40162 = 233256846 \\
23 \times 13 = 39 \\
5 \times 4 \neq 12
\end{array}
\]

The original statement must be false.

(ii)
\[
\begin{array}{c}
9787 \times 1258 = 12342046 \\
31 \times 16 = 22 \\
4 \times 7 \neq 4
\end{array}
\]

The original statement must be false.

(iii)
\[
\begin{array}{c}
8901 \times 5743 = 52018443 \\
18 \times 19 = 27 \\
9 \times 10 \equiv 9
\end{array}
\]

The original statement could be true. But in fact it is false, as can be verified by explicit calculation.
13.1.3

Suppose we are given \( m \geq 2 \) and an integer \( x \). The remainder \( r \) when \( x \) is divided by \( m \) satisfies

\[
x \equiv r \pmod{m}, \quad 0 \leq r \leq m - 1,
\]

and is sometimes called the least non-negative residue of \( x \pmod{m} \). Find the least non-negative residue of \( 3^{15} \pmod{17} \) and \( 15^{81} \pmod{13} \).

Solution  Working mod 17,

\[
3^3 = 10, \quad 3^4 = 13, \quad 3^5 = 5
\]

\[
\therefore \quad 3^{15} = 3^5 \times 3^5 \times 3^5 = 125 = 6.
\]

Working mod 13, we have 15 = 2 so \( 15^{81} = 2^{81} \). Now

\[
2^4 = 3, \quad 2^{12} = (2^4)^3 = 3^3 = 1, \quad 2^{72} = (2^{12})^6 = 1;
\]

\[
2^{81} = 2^{72} \times 2^9 = 1 \times 3 \times 3 \times 2 = 18 = 5.
\]
13.2 \( \mathbb{Z}_m \) and its arithmetic

13.2.1

Complete Tables 13.2.1(a, b), the addition and multiplication tables for \( \mathbb{Z}_6 \).

**Solution**

\[
\begin{array}{c|ccccc}
\oplus & 0 & 1 & 2 & 3 & 4 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 \\
3 & 3 & 4 & 5 & 0 & 1 \\
4 & 4 & 5 & 0 & 1 & 2 \\
5 & 5 & 0 & 1 & 2 & 3
\end{array}
\]

\[
\begin{array}{c|ccccc}
\otimes & 0 & 1 & 2 & 3 & 4 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 \\
2 & 0 & 2 & 4 & 0 & 2 \\
3 & 0 & 3 & 0 & 3 & 0 \\
4 & 0 & 4 & 2 & 0 & 4 \\
5 & 0 & 5 & 4 & 3 & 2
\end{array}
\]
13.2.2

Deduce from Theorem 7.5.2 that if $x$ and $y$ are integers such that $xy = 0$ and $x \neq 0$, then $y = 0$. Show by counter-examples that this axiom does not hold in $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{15}$. Is there a counter-example in $\mathbb{Z}_7$?

Solution  Theorem 7.5.2 says that if $xz = yz$ and $z \neq 0$ then $x = y$. Here we have $xy = 0$ and $x \neq 0$, and we can rearrange this as

$$yx = 0x, \quad x \neq 0,$$

which implies that $y = 0$, as required.

For the second part, we have, for example:

- $3 \times 2 = 0$ in $\mathbb{Z}_6$,
- $4 \times 2 = 0$ in $\mathbb{Z}_8$,
- $3 \times 5 = 0$ in $\mathbb{Z}_{15}$.

There is no such example in $\mathbb{Z}_7$. You can check this by looking at the multiplication table. The general theory is discussed in the next section (Section 13.3).
13.2.3

Solve the simultaneous equations

\[ x + 2y = 4, \]
\[ 4x + 3y = 4 \]

in \( \mathbb{Z}_7 \). Is there a solution in \( \mathbb{Z}_5 \)?

**Solution** In \( \mathbb{Z}_7 \), the solution is \( x = 2, y = 1 \). This can be obtained by multiplying the first equation by 4 (and reducing the coefficients mod 7), which gives

\[ 4x + 8y = 16, \]  
that is \( 4x + y = 2 \).

Subtracting this from the second equation gives \( 2y = 2, y = 1 \).

In \( \mathbb{Z}_5 \) there is no solution. There are many ways to see this: for example, adding the equations gives \( 0(x + y) = 3 \), which is impossible.
13.3 Invertible elements of $\mathbb{Z}_m$

13.3.1

Find the invertible elements of $\mathbb{Z}_6$, $\mathbb{Z}_7$, and $\mathbb{Z}_8$.

**Solution**  By ‘trial and error’, the invertible elements are:

- $\mathbb{Z}_6 : 1, 5$;
- $\mathbb{Z}_7 : 1, 2, 3, 4, 5, 6$;
- $\mathbb{Z}_8 : 1, 3, 5, 7$.

A general rule will be found in Theorem 13.3.1.
13.3.2
Show that $0$ is not invertible in any $\mathbb{Z}_m$, but $1$ is always invertible.

Solution  For any $x$, we have $0 \times x = 0$, and $0 \neq 1$. So no $x$ can be the inverse of $0$.

On the other hand $1 \times 1 = 1$, so $1$ is its own inverse.
13.3.4

Find the inverses of

(i) 2 in \( \mathbb{Z}_{11} \),
(ii) 7 in \( \mathbb{Z}_{15} \),
(iii) 7 in \( \mathbb{Z}_{16} \),
(iv) 5 in \( \mathbb{Z}_{13} \).

Solution  
In these examples, the inverses are easily found by trial and error.

(i) 6,
(ii) 13,
(iii) 7,
(iv) 8.
Solutions to Chapter 13 Exercises

in Discrete Mathematics by Norman L. Biggs;
2nd Edition 2002

13.3.5

Use Fermat’s Theorem to calculate the remainder when $3^{47}$ is divided by 23.

Solution  By Fermat’s Theorem, $3^{22} \equiv 1 \mod 23$. Thus

$$3^{47} = 3^{22} \times 3^{22} \times 3^3 \equiv 1 \times 1 \times 3^3 = 4 \mod 23.$$
13.4 Cyclic constructions for designs

13.4.1
Which of the following are difference sets?

(i) \{2, 3, 5, 11\} in \(\mathbb{Z}_{13}\),
(ii) \{0, 1, 3, 5\} in \(\mathbb{Z}_{13}\),
(iii) \{3, 6, 7, 12, 14\} in \(\mathbb{Z}_{21}\).

Solution We construct the difference tables, as in Table 13.4.1 on p.151.

(i)

\[
\begin{array}{c|cccc}
   & 2 & 3 & 5 & 11 \\
\hline
  2 & - & 12 & 10 & 4 \\
  3 & 1 & - & 11 & 5 \\
  5 & 3 & 2 & - & 7 \\
 11 & 9 & 8 & 6 & - \\
\end{array}
\]

This is a difference set, because every value occurs exactly once.

(ii)

\[
\begin{array}{c|cccc}
   & 0 & 1 & 3 & 5 \\
\hline
  0 & - & 12 & 10 & 8 \\
  1 & 1 & - & 11 & 9 \\
  3 & 3 & 2 & - & 11 \\
  5 & 5 & 4 & 2 & - \\
\end{array}
\]

This is not a difference set because, for example, 11 occurs twice and 6 not at all.

(iii)

\[
\begin{array}{c|cccccc}
   & 3 & 6 & 7 & 12 & 14 \\
\hline
  3 & - & 18 & 17 & 12 & 10 \\
  6 & 3 & - & 20 & 15 & 13 \\
  7 & 4 & 1 & - & 16 & 14 \\
 12 & 9 & 6 & 5 & - & 19 \\
 14 & 11 & 8 & 7 & 2 & - \\
\end{array}
\]

This is a difference set because every value occurs exactly once.
13.4.2

Repeat the Example given on p. 152 with 23 replaced by 11, and with 23 replaced by 31. Make a conjecture about the parameters of the associated design when \( m \) is any prime of the form \( 4n + 3 \).

**Solution**  In \( \mathbb{Z}_{11} \) the squares are 1, 3, 4, 5 and 9, and in the difference table each value occurs twice. In \( \mathbb{Z}_{31} \) the squares are 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25 and 28, and in the difference table each value occurs seven times.

We observe that working in \( \mathbb{Z}_p \) where \( p \) is a prime of the form \( 4n + 3 \), the number of non-zero squares is \( 2n + 1 \). Furthermore, in the cases \( n = 2, 5, 7 \), each value occurs exactly \( n \) times in the difference table. This observation leads to the conjecture that we can always construct a 2-design with parameters

\[
v = 4n + 3, \quad k = 2n + 1, \quad r_2 = n
\]

in this way. (For the proof of a more general result, see Section 23.8.)
13.5 Latin squares

An ordinary pack (deck) of cards contains four Jacks, four Queens, four Kings, and four Aces, one of each denomination from each of the four suits—Hearts, Clubs, Diamonds, and Spades. Explain how to arrange these 16 cards in a $4 \times 4$ square in such a way that each row contains one card from each suit and one card from each denomination. Interpret your result in terms of latin squares.

**Solution** One solution is as follows.

\[
\begin{array}{cccc}
A\text{S} & K\text{H} & Q\text{C} & J\text{D} \\
K\text{C} & A\text{D} & J\text{S} & Q\text{H} \\
Q\text{D} & J\text{C} & A\text{H} & K\text{S} \\
J\text{H} & Q\text{S} & K\text{D} & A\text{C}
\end{array}
\]

If we denote A,K,Q,J by 1,2,3,4 respectively, and H,C,D,S in the same way, we get the arrangement

\[
\begin{array}{cccc}
14 & 21 & 32 & 43 \\
22 & 13 & 44 & 31 \\
33 & 42 & 11 & 24 \\
41 & 34 & 23 & 12
\end{array}
\]

which is a pair of orthogonal latin squares using the symbols 1,2,3,4.
Solutions to Chapter 13 Exercises

in Discrete Mathematics by Norman L. Biggs;
2nd Edition 2002

13.5.2

Use the construction given in Theorem 13.5.2 to obtain four mutually orthogonal
latin squares of order 5.

Solution

\[ L_1: \begin{array}{cccc}
0 & 1 & 2 & 3 \\
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 0 \\
3 & 4 & 0 & 1 \\
4 & 0 & 1 & 2
\end{array} \]

\[ L_2: \begin{array}{cccc}
0 & 1 & 2 & 3 \\
2 & 3 & 4 & 0 \\
4 & 0 & 1 & 2 \\
3 & 4 & 0 & 1 \\
1 & 2 & 3 & 4
\end{array} \]

\[ L_3: \begin{array}{cccc}
0 & 1 & 2 & 3 \\
3 & 4 & 0 & 1 \\
1 & 2 & 3 & 4 \\
4 & 0 & 1 & 2 \\
2 & 3 & 4 & 0
\end{array} \]

\[ L_4: \begin{array}{cccc}
0 & 1 & 2 & 3 \\
4 & 0 & 1 & 2 \\
3 & 4 & 0 & 1 \\
2 & 3 & 4 & 0 \\
1 & 2 & 3 & 4
\end{array} \]