

**Tutorial 4 (Week 4)**

**Preparatory question  
(attempt before the tutorial)**

- (a) Write out the addition and multiplication tables for  $\mathbb{Z}_5$ .  
(b) What is  $3^{1000}$  in  $\mathbb{Z}_5$ ?

**Tutorial exercises**

*(Starred exercises are more difficult. Do not be concerned if you are unable to do them.)*

2. Find  $\mathbf{u} + \mathbf{v}$  and  $\mathbf{u} \cdot \mathbf{v}$  if  $\mathbf{u}$  and  $\mathbf{v}$  are the binary vectors  $\mathbf{u} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$  and  $\mathbf{v} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$ .

3. What is the parity check code vector for each of the following binary vectors?

(a)  $[0, 1, 0]$     (b)  $[0, 1, 0, 1, 1, 1]$

4. The following parity check code vectors are received. Has there been an error in transmission?

(a)  $[1, 0, 0, 1, 1]$     (b)  $[1, 0, 0, 0, 0]$     (c)  $[1, 0, 1, 0]$

5. In  $\mathbb{Z}_3$  calculate

(a)  $2 + 2 + 2 + 1$     (c)  $2 \times (2 + 2 + 2 + 1)$

(b)  $2 + 2 + 2 + 2 + 1$     (d)  $2^{10}$

6. Perform the following calculations:

(a)  $3 \times 4 + 6 \times 5$  in  $\mathbb{Z}_7$

(b)  $(8 + 7) \times (9 + 4)$  in  $\mathbb{Z}_{10}$

(c)  $\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3 \\ 3 \end{bmatrix}$  in  $\mathbb{Z}_4^3$

(d)  $\begin{bmatrix} 3 \\ 4 \\ 1 \\ 2 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3 \\ 4 \\ 4 \end{bmatrix}$  in  $\mathbb{Z}_5^4$

7. Solve the following equations in  $\mathbb{Z}_6$ :
- (a)  $x + 4 = 1$    (b)  $2x + 2 = 0$    (c)  $x^2 + x = 0$
8. The barcode used on products in Australia is generally a 13-digit Global Trade Item Number, known as a GTIN-13. Each digit is a number between 0 and 9 (that is, an element of  $\mathbb{Z}_{10}$ ). The first 12 digits give information about the product, and the 13th digit is a check digit. The check vector is  $\mathbf{c} = [1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1]$ . The check digit is chosen so that the dot product of  $\mathbf{c}$  and the barcode vector is 0 in  $\mathbb{Z}_{10}$ .
- (a) Determine whether or not 8 712000 075302 is a valid GTIN-13.
- (b) Determine whether or not 40 07817 31056 4 is a valid GTIN-13.
- (c) Find the check digit,  $d$ , for the GTIN-13: 9 312345 67890  $d$ .
- (d) Given that there is an error in the 8th digit (counting from the left) in the following GTIN-13, and that all other digits are correct, determine the correct GTIN-13: 9 310088 801846.
- (e) \*\* Prove that if two adjacent entries in a GTIN-13 differ by 5, and are mistakenly transposed, the error will not be detected.
9. Before 2007, ISBN numbers contained 10 digits, with the tenth digit being a check digit. For 10-digit ISBNs, the check vector is  $\mathbf{c} = [10, 9, 8, 7, 6, 5, 4, 3, 2, 1]$ , and the check digit is chosen so that the dot product of  $\mathbf{c}$  and the ISBN is 0 in  $\mathbb{Z}_{11}$ .
- (a) Determine whether or not the following is a valid ISBN: 0-13-087304-7
- (b) Find the check digit,  $d$ , in the ISBN: 0-471-16362- $d$
- (c) Find the check digit,  $d$ , in the ISBN: 1-86451-323- $d$
- (d) (i) Show that 0-8044-9257-X is not a valid ISBN.
- (ii) \*\* Given that the only error in the number in part (i) is the transposition of an adjacent pair of entries, is it possible to find the correct ISBN?

## Further exercises

In addition to these exercises, the following exercises from the textbook – *Linear Algebra: A Modern Introduction* by David Poole – are relevant:

**Exercises 1.4:** 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53.

## Solutions

1. (a)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b) We can approach this question by looking for a small power of 3 that is equal to 1 in  $\mathbb{Z}_5$ . From the multiplication table in part (a), we see that  $3^2 = 4$  and  $4^2 = 1$ , so  $3^4 = (3^2)^2 = 4^2 = 1$ .

Hence  $3^{1000} = (3^4)^{250} = 1$ .

2. Remember that the calculations are in  $\mathbb{Z}_2$ , so that  $1 + 1 = 0$ .

$$\mathbf{u} + \mathbf{v} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad \mathbf{u} \cdot \mathbf{v} = 1 + 1 = 0.$$

3. To create the parity check code vector, a check digit is added to the vector. The check digit is either 0 or 1, chosen so that the number of 1s in the parity check code vector is even. (Another way of saying this is that the check digit is chosen so that the sum of the entries in the parity check code vector is 0 in  $\mathbb{Z}_2$ .) So, in part (a), where there is just one 1 in the vector, we add 1 to create the parity check code vector, whereas in part (b), where the vector contains four 1s, we add a 0.

(a)  $[0, 1, 0, 1]$     (b)  $[0, 1, 0, 1, 1, 1, 0]$

4. Parity check code vectors always contain an even number of 1s. Hence, there must be an error in the vectors in (a) and (b).

In part (c) the vector contains two 1s, so no single error has been made.

5. (a)  $2 + 2 + 2 + 1 = 2 \times 3 + 1 = 1$  in  $\mathbb{Z}_3$ .

(b)  $2 + 2 + 2 + 2 + 1 = 3 \times 3 = 0$  in  $\mathbb{Z}_3$ .

(c)  $2 \times (2 + 2 + 2 + 1) = 2 \times 1 = 2$  in  $\mathbb{Z}_3$ .

(d) As in question 1 (b), look for a small power of 2 that is equal to 1 in  $\mathbb{Z}_3$ . Since  $2^2 = 4 = 1$  in  $\mathbb{Z}_3$ , we have  $2^{10} = (2^2)^5 = 1^5 = 1$ .  
(Alternately:  $2^{10} = 1024 = 3 \times 341 + 1 = 1$  in  $\mathbb{Z}_3$ .)

6. (a) Notice that there is more than one way to approach such a calculation.

For example,  $3 \times 4 + 6 \times 5 = 12 + 30 = 42 = 0$  in  $\mathbb{Z}_7$ , since  $42 = 6 \times 7$ . Alternately, since  $12 = 5$  and  $30 = 2$  in  $\mathbb{Z}_7$ , we have  $3 \times 4 + 6 \times 5 = 5 + 2 = 7 = 0$ .

- (b)  $(8 + 7) \times (9 + 4) = 5 \times 3 = 5$  in  $\mathbb{Z}_{10}$ .
- (c) The notation  $\mathbb{Z}_m^n$  means the set of vectors with  $n$  entries, each of which is an element of  $\mathbb{Z}_m$ . So any calculation involving vectors in  $\mathbb{Z}_4^3$  is carried out in  $\mathbb{Z}_4$ . Hence,  $\begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3 \\ 3 \end{bmatrix} (= 9 + 6 + 3) = 1 + 2 + 3 = 2$ .

(d) Here the calculation is done in  $\mathbb{Z}_5$ :  $\begin{bmatrix} 3 \\ 4 \\ 1 \\ 2 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3 \\ 4 \\ 4 \end{bmatrix} = 4 + 2 + 4 + 3 = 3$ .

7. The solution must be an element (or elements) of the set  $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ . One way to solve such equations is simply to try each possibility.

- (a)  $x = 3$ , since  $3 + 4 = 7 = 1$  in  $\mathbb{Z}_6$ .
- (b)  $x = 2$  or  $5$ . ( $2 \times 2 + 2 = 6 = 0$ ;  $2 \times 5 + 2 = 12 = 0$ .)
- (c)  $x = 0, 2, 3, 5$ .

8. (a) Let  $\mathbf{u} = [8, 7, 1, 2, 0, 0, 0, 0, 7, 5, 3, 0, 2]$ . Then  $\mathbf{c} \cdot \mathbf{u} = 3 \neq 0$  in  $\mathbb{Z}_{10}$ . Hence the GTIN-13 is invalid.

(b) Let  $\mathbf{u} = [4, 0, 0, 7, 8, 1, 7, 3, 1, 0, 5, 6, 4]$ . Then  $\mathbf{c} \cdot \mathbf{u} = 0$  in  $\mathbb{Z}_{10}$ . Hence the GTIN-13 is valid.

(c) Let  $\mathbf{v} = [9, 3, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, d]$ . Then  $\mathbf{c} \cdot \mathbf{v} = 3 + d$  in  $\mathbb{Z}_{10}$ , and hence  $d = 7$ .

(d) Let  $\mathbf{w} = [9, 3, 1, 0, 0, 8, 8, x, 0, 1, 8, 4, 6]$ , where we have replaced the incorrect 8th digit by  $x$ . Then  $\mathbf{c} \cdot \mathbf{w} = 3x$  in  $\mathbb{Z}_{10}$  and since we must have  $\mathbf{c} \cdot \mathbf{w} = 3x = 0$ , the only possibility is  $x = 0$ .

The correct GTIN-13 is 9 310088 001846.

(e) Suppose that  $x$  and  $y$  are two adjacent entries in a GTIN-13, and that the correct order is  $x$  followed by  $y$ . The contribution of these two entries to the dot product of  $\mathbf{c}$  and the barcode vector is either  $x + 3y$  or  $3x + y$ . If  $x$  and  $y$  are transposed, then the contribution will be  $y + 3x$  or  $3y + x$ . In either case, the difference between the contributions to the dot product is  $2|x - y|$ , and if  $x$  and  $y$  differ by 5, then  $2|x - y| = 0$  in  $\mathbb{Z}_{10}$ . So the transposition of two adjacent entries that differ by 5 will not alter the dot product, and hence the error will not be detected.

9. (a) Let  $\mathbf{u} = [0, 1, 3, 0, 8, 7, 3, 0, 4, 7]$ . Then  $\mathbf{c} \cdot \mathbf{u} = 0$  in  $\mathbb{Z}_{11}$ , and hence the ISBN is valid.

(b) Let  $\mathbf{u} = [0, 4, 7, 1, 1, 6, 3, 6, 2, d]$ . Then  $\mathbf{c} \cdot \mathbf{u} = 4 + d$  in  $\mathbb{Z}_{11}$ , and so  $d = 7$ .

(c) Let  $\mathbf{u} = [1, 8, 6, 4, 5, 1, 3, 2, 3, d]$ . Then  $\mathbf{c} \cdot \mathbf{u} = 8 + d$  in  $\mathbb{Z}_{11}$ , and so  $d = 3$ .

(d) (i) Let  $\mathbf{v} = [0, 8, 0, 4, 4, 9, 2, 5, 7, 10]$ . (Remember that  $X$  is used as the check digit in an ISBN if the check digit is 10.) Then  $\mathbf{c} \cdot \mathbf{v} = 7 \neq 0$  in  $\mathbb{Z}_{11}$ , and so the ISBN is invalid.

- (ii) Suppose that the transposed entries are  $x$  and  $y$ , and that  $x$  should be in position  $n + 1$ , *counting from the right*, and  $y$  should be in position  $n$ . (Note that if we count positions from the right, then the entry in position  $n$  is multiplied by  $n$  when we calculate the dot product.) So, when  $x$  and  $y$  are in their correct places, the contribution to the dot product is  $(n+1)x+ny$ . When  $x$  and  $y$  are transposed, the contribution is  $(n+1)y+nx$ . The difference,  $|(n+1)x+ny-((n+1)y+nx)| = |x-y|$ , must equal 7 and so we are looking for two adjacent entries that differ by 7.

The adjacent digits 9 and 2 differ by 7, so interchanging those would give a valid ISBN: 0-8044-2957-X. But the adjacent digits 0 and 4 also differ by 7 in  $\mathbb{Z}_{11}$ , so that 0-8404-9257-X is also a valid ISBN. Hence we cannot tell which is the correct ISBN.