

## Applied Algebra: Solutions to selected practice problems.

### Number theory.

3. Does there exist an integer  $x$  such that  $x \equiv 5 \pmod{15}$  and  $x \equiv 3 \pmod{10}$ ? Explain why or why not.

**Solution:** No, such  $x$  does not exist. Indeed, if  $x \equiv 5 \pmod{15}$ , then  $x = 5 + 15k = 5(1 + 3k)$ , so  $x$  is a multiple of 5. If  $x \equiv 3 \pmod{10}$ , then  $x - 3 = 10l = 5 \cdot 2l$ , so  $x - 3$  is a multiple of 5. But  $x$  and  $x - 3$  can not be divisible by 5 simultaneously, since 3 is not divisible by 5.

*For the rest of the number theory practice problems see the solutions to Homework 7 where similar problems are discussed.*

### Symmetric groups.

5. Write the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 7 & 2 & 8 & 4 & 11 & 3 & 9 & 5 & 1 & 6 & 10 \end{pmatrix}$$

- 1) as a product of disjoint cycles;
- 2) as a product of 3-cycles (not necessarily disjoint).

**Solution:** 1) (i) The permutation  $\sigma$  maps 1 to 12, 12 to 10, 10 to 1. Hence we get 3-cycle (1 12 10).

(ii) Similarly,  $2 \mapsto 7 \mapsto 3 \mapsto 2$  providing 3-cycle (2 7 3).

(iii) Since 3 has already been served, start with  $4 \mapsto 8 \mapsto 9 \mapsto 5 \mapsto 4$ . We get 4-cycle (4 8 9 5)

(iv) Finally,  $6 \mapsto 11 \mapsto 6$  providing the transposition (6 11).

Hence,  $\sigma = (1\ 12\ 10)(2\ 7\ 3)(4\ 8\ 9\ 5)(6\ 11)$

2) We do not touch the first two cycles, since they already have length 3. Replace (4 8 9 5)(6 11) with (4 11 6)(4 5 6)(4 8 9).

6. Is it possible to write the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 7 & 2 & 8 & 4 & 6 & 3 & 9 & 5 & 1 & 11 & 10 \end{pmatrix}$$

as a product of 3-cycles (not necessarily disjoint)? Explain why or why not.

**Solution:** It is impossible. The cycle decomposition of  $\sigma$  is (1 12 10)(2 7 3)(4 8 9 5). Hence,  $\text{sgn}(\sigma) = (-1)^2(-1)^2(-1)^3 = -1$ , so  $\sigma$  is odd. However, a 3-cycle is an even permutation, thus any product of 3-cycles must be an even permutation.

**Group theory.**

**7.** Let  $k > 1$  be any integer. Show that  $\varphi(k^3 - 1)$  is divisible by 3.

**Solution:** Note that  $k$  is an element of order 3 in  $G_n$  (=the group of invertible congruence classes modulo  $n$ ) for  $n = k^3 - 1$ . Indeed,  $k^3 \equiv 1 \pmod{n}$ , and  $k \not\equiv 1 \pmod{n}$ , since  $1 < k < k^3 = n + 1$ . By the Lagrange theorem, the order of  $G_n$ , which is equal to  $\varphi(n)$ , is divisible by the order of  $k$ . Hence,  $\varphi(k^3 - 1)$  is divisible by 3.

**8.** Let  $G$  be the group  $G_{23}$ . Find  $a \in G_{23}$  such that every element of  $G_{23}$  is a power of  $a$ : that is, show that  $G$  is a cyclic group by finding a generator for it. Similarly show that  $G_{26}$  is cyclic by finding a generator for it. Is every group of the form  $G_n$  cyclic?

**Solution:** Find  $a$  by trial and error method. Note that the order of  $a$  must be equal to the order of the whole group  $G_{26}$ , which is  $\varphi(26) = 12$ . First, try  $a = 3$  (this is the smallest  $a \neq 1$  in  $G_{26}$ ).

$a$	$a^2$	$a^3$
3	9	1

So 3 has order 3, not 12. Try 5.

$a$	$a^2$
5	-1

The order of 5 is 4, since  $5^4 = (5^2)^2 = (-1)^2 = 1$ . Try 7.

$a$	$a^2$	$a^3$	$a^4$	$a^5$	$a^6$	$a^7$	$a^8$	$a^9$	$a^{10}$	$a^{11}$	$a^{12}$
7	23	5	9	11	25	19	3	21	17	15	1

Only  $a^{12} = 1$ , and all elements of  $G_{26}$  are present in this table. Hence,  $a = 7$  is the generator of  $G_{26}$ .

Note that the group  $G_8$  of order  $\varphi(8) = 4$  is not cyclic, since it does not have an element of order 4 (element 1 has order 1 and elements 3, 5, 7 have order 2).

*For Problems 9 and 10, see their solutions in the textbook.*

**11.** Give an example of a group of order 8, that is not cyclic.

**Solution:** One example is the group  $G_{16}$ . Its order is  $\varphi(16) = 8$ , but it does not have any elements of order 8. It is easy to check that every element  $a \in G_{16}$  satisfies the equation  $a^4 = 1$ . Indeed, all elements of  $G_{16}$  are odd, and every odd number can be written as  $4k \pm 1$ . Then  $(4k \pm 1)^4 = (16k^2 \pm 8k + 1)^2 \equiv (8k \pm 1)^2 \equiv (64k^2 + 16k + 1) \equiv 1 \pmod{16}$ .

Another example is the dihedral group  $D_4$  — the group of symmetries of a square. It consists of eight elements — four rotations and four reflections. It is not cyclic, because it is not even Abelian.

**Error-correcting/detecting codes:**

**12.** Let the code function  $f : B^4 \rightarrow B^7$  be given by the generating matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

- 1) Find the number of the codewords of  $f$ . Find the minimal distance between the codewords.
- 2) How many errors does  $f$  detect and how many errors does it correct?
- 3) Find the parity-check matrix of  $f$ . Use it to write down the two-column decoding table for  $f$ .
- 4) Use this table to correct the message

1100111 1011000 1010110 0011001 1101010 1111111 1010101.

**Solution:** 1) The minimal distance is two, since the minimal weight of a nonzero codeword is two (in this case the codeword of minimal weight is the last row of  $G$ ).

2) This code detects one error and corrects none (in general). However, some “not too bad” errors can be corrected as we see below.

3) The parity-check matrix is

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The two-column decoding table has  $2^7/2^4 = 8$  rows.

0000000	000
1000000	111
0100000	110
0001000	100
0000010	010
0000001	001
1001000	011
1000010	101

Note that the third row (with the coset leader 0100000) has an alternative coset leader 0010000 of the same weight (and of course with the same syndrome 110). Hence, all words in  $B^7$  with syndrome 110 can be corrected (using the maximum likelihood decoding method) in two different ways. So we can not correct such words with certainty even if we are sure that they have only one error. The same thing happens with the fourth row (with syndrome 100). However, we can correct with certainty one error in any word in  $B^7$  whose syndrome is 111, 010 or 001.

4) Compute the syndromes of the words in the message

1100111	110
1011000	101
1010110	111
0011001	011
1101010	111
1111111	100
1010101	100

We can correct the third and the fifth words. The correct decoded words are 0010 and 0101, respectively. We know for sure that the second and fourth words have at least two errors but we can not correct them with 100% accuracy. As for the first and the last two words, we can only say that they have at least one error but we can not correct them.

We must conclude that the code given by  $f$  is not a good one, since we were able to correct only two words out of seven.