

1. (a) State the division algorithm. (b) State the Chinese remainder theorem.

(c) Solve the following system of congruences:  $x \equiv 13 \pmod{25}$        $x \equiv 9 \pmod{18}$

To work with the smaller modulus, start with the equation from the larger one. Write  $x = 13 + 25q$  for some  $q \in \mathbf{Z}$ , and substitute to get  $13 + 25q \equiv 9 \pmod{18}$ , which reduces to  $7q \equiv 14 \pmod{18}$ . Now  $\gcd(7, 18) = 1$ , so we can cancel 7 from both sides. (Or, by trial and error you can see that multiplying both sides by  $-5$  will give you  $-35q \equiv q \pmod{18}$ .) In any case, you should get  $q \equiv 2 \pmod{18}$ . This final answer is  $x \equiv 63 \pmod{25 \cdot 18}$ .

2. (a) Use the Euclidean algorithm to find  $[8]_{27}^{-1}$  (in  $\mathbf{Z}_{27}^\times$ ).

$$\begin{bmatrix} 1 & 0 & 27 \\ 0 & 1 & 8 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -3 & 3 \\ 0 & 1 & 8 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -3 & 3 \\ -2 & 7 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 3 & -10 & 1 \\ -2 & 7 & 2 \end{bmatrix}, \text{ so } [8]_{27}^{-1} = [-10]_{27} = [17]_{27}.$$

(b) Find  $\varphi(27)$  and list all of its positive divisors.       $\varphi(27) = 27 \cdot \frac{2}{3} = 18$  since  $27 = 3^3$ .

The positive divisors of 18 are 1, 2, 3, 6, 9, 18.

(c) Find the order of  $[8]_{27}$  in the group  $\mathbf{Z}_{27}^\times$ .       $8^2 = 64 \equiv 10 \pmod{27}$        $8^3 = 8 \cdot 10 \equiv -1 \pmod{27}$

$8^6 = (8^3)^2 \equiv 1 \pmod{27}$  From part (b) the possible orders are 2, 3, 6, 9, 18, so  $[8]_{27}$  has order 6.

3. Let  $\sigma = (3, 6, 8)(1, 9, 4, 3, 2, 7, 6, 8, 5)(2, 3, 9, 7) \in S_9$ .

(a) Write  $\sigma$  as a product of disjoint cycles.       $\sigma = (1, 9, 8, 5)(3, 4, 6)$

(b) Is  $\sigma$  even or odd?       $\sigma = (1, 9)(9, 8)(8, 5)(3, 4)(4, 6)$  so it is an odd permutation

(c) What is the order of  $\sigma$  in  $S_9$ ?       $\text{lcm}[4, 3] = 12$  (d) Compute  $\sigma^{-1}$  in  $S_9$ .       $\sigma^{-1} = (1, 5, 8, 9)(3, 6, 4)$

4. (a) State the definition of an equivalence relation. (b) State the definition of a subgroup of a group.

(c) Let  $G$  be a group, and let  $H$  be a subgroup of  $G$ . For  $x, y \in G$ , define  $x \sim y$  if  $x^{-1}y \in H$ . Prove that  $\sim$  defines an equivalence relation on  $G$ . Solution: This is similar to the proof of Lemma 3.2.9.

5. (a) State the definition of a one-to-one function. (b) State the definition of an onto function. (c) State the definition of an isomorphism of groups. (d) Let  $G_1, G_2$  be groups and let  $H_2$  be a subgroup of  $G_2$ . Prove that if  $\phi: G_1 \rightarrow G_2$  is an isomorphism, then  $H_1 = \{g \in G_1 \mid \phi(g) \in H_2\}$  is a subgroup of  $G_1$ .

Closure: If  $a, b \in H_1$ , then  $\phi(a), \phi(b) \in H_2$ , so  $ab \in H_1$  since  $\phi(ab) = \phi(a)\phi(b) \in H_2$  (because  $\phi$  is a group isomorphism and  $H_2$  is closed).

Identity: We have  $e \in H_1$  since  $\phi(e) = e \in H_2$  because  $\phi$  is a group isomorphism and any subgroup contains  $e$ .

Inverses: If  $a \in H_1$ , then  $\phi(a) \in H_2$ , so  $(\phi(a))^{-1} \in H_2$  since  $H_2$  contains inverses of its elements. But then  $\phi(a^{-1}) = (\phi(a))^{-1} \in H_2$  since  $\phi$  is a group isomorphism, and so  $a^{-1} \in H_1$ .

6. (a) Let  $H$  and  $K$  be subgroups of the group  $G$ . Prove that  $HK$  is a subgroup of  $G$  if and only if  $KH \subseteq HK$ .

I proved this proposition in class; it should be in your class notes.

(b) Let  $G = \mathbf{Z}_{10}^\times \times \mathbf{Z}_{10}^\times$ , let  $H = \langle (3, 3) \rangle$  and let  $K = \langle (3, 7) \rangle$ . List the elements of  $HK$ .

$$H = \{(1, 1), (3, 3), (9, 9), (7, 7)\} \text{ and } K = \{(1, 1), (3, 7), (9, 9), (7, 3)\}.$$

$$HK = \{(1, 1), (3, 3), (9, 9), (7, 7), (3, 7), (9, 1), (7, 3), (1, 9)\}$$

7. (a) State the definition of a cyclic group. (b) Write out ONE of the following proofs from the text:

I. Any subgroup of a cyclic group is cyclic. II. If  $G$  is a cyclic group of order  $n$ , then  $G$  is isomorphic to  $\mathbf{Z}_n$ .

8. (a) State the definition of the order of an element. (b) Prove or disprove: If  $a, b$  are elements of the group  $G$  with  $o(a) = m$  and  $o(b) = n$ , where  $m, n$  are positive integers, then  $o(ab) \leq \text{lcm}[m, n]$ .

The result is false in general. For example, in  $S_3$ , let  $a = (1, 2)$  and  $b = (2, 3)$ . Then  $m = 2$  and  $n = 2$ , so  $\text{lcm}[m, n] = 2$ , but  $ab = (1, 2)(2, 3) = (1, 2, 3)$ . In this example  $o(ab) = 3 > 2 = \text{lcm}[m, n]$ .

If  $ab = ba$  and  $\text{lcm}[m, n] = k$ , then  $k = mq$  and  $k = np$  for some  $q, p \in \mathbf{Z}$ . Then  $(ab)^k = a^k b^k = a^{mq} b^{np} = (a^m)^q (b^n)^p = e$ , and so  $o(ab) \mid \text{lcm}[m, n]$ . Note: it can be proved that if  $\gcd(m, n) = 1$ , then  $o(ab) = mn$ .