MA132 Foundations 2012-2013

Solutions for Test 2

NOTE

1. These solutions are not necessarily in the order of your particular test paper. It should be straightforward matching your question order with the order of the paper you answered.

2. If you got a question wrong, understand why you got it wrong.

3. If you're not sure about a question, discuss it in your supervision group or with your tutor. If you're still not sure, have a word with your lecturer.

1. Which of the following statements is true?
a) Any subgroup of $\mathbb{Z}$ which contains 55 and 99 also contains 11.
b) Any subgroup of $\mathbb{Z}$ which contains 28 and 42 also contains 7.
c) The smallest subgroup of $\mathbb{Z}$ containing 48, 100, and 76 is the set of even numbers.
d) Any subgroup of $\mathbb{Z}$ which contains 24 also contains 76.

Answer: (a). Any subgroup of $\mathbb{Z}$ which contains m and n must contain $\text{hcf}(m, n)$, so if a subgroup contains 55 and 99 it must contain 11, so (a) is true. However, $14\mathbb{Z}$ contains 28 and 42 but not 7, so (b) is false; $4\mathbb{Z}$ contains 48, 100 and 76, so (c) is false; and $24\mathbb{Z}$ obviously contains 24 but does not contain 76 as 76 is not a multiple of 24, so (d) is false.

2. What is $25^6 \mod 7$? (a) 0; (b) 1; (c) 3; (d) 5.

Answer: (b). By Fermat's Little Theorem, $a^{p-1} \equiv 1 \mod p$ provided that a is not divisible by p, so it suffices to observe that 25 is not divisible by 7. Alternatively, one could compute the answer by doing

$$25^6 \equiv (-3)^6 \equiv ((-3)^2)^3 \equiv 9^3 \equiv 2^3 \equiv 1 \mod 7.$$

3. Let A be a subgroup of $\mathbb{Z}$, and let $m, n \in A$. Consider the following statements:
(i) A must contain the product mn.
(ii) A must contain the quotient m/n whenever m/n is an integer.
(iii) A must contain the power m^n.
(iv) A must contain every divisor of m and every divisor of n.
(v) A must contain the highest common factor $\text{hcf}(m, n)$.
(vi) A must contain the lowest common multiple $\text{lcm}(m, n)$.
How many of these statements are true? (a) 2 are true and 4 are false; (b) 3 are true and 3 are false; (c) 4 are true and 2 are false; (d) 5 are true and 1 is false.

Answer: (c). Four are true, namely (i), (iii), (v) and (vi), and two are false, namely (ii) and (iv). A subgroup which contains m and n must contain every multiple of m and every multiple of n: in particular, it must contain mn, so (i) is true; it must contain m^n, so (iii) is true, and it must contain $\text{lcm}(m, n)$, so (vi) is true. Furthermore, by the Euclidean algorithm we can write $\text{hcf}(m, n) = am + bn$ for some $a, b \in \mathbb{Z}$, so (v) is true. However, (ii) is false: even when m/n is an integer, it need not belong to a subgroup which contains m and n (for example, $4\mathbb{Z}$ contains 4 and 8 but not $8/4 = 2$). Finally, (iv) is false as the subgroup need not contain any divisors of m or n except m and n themselves (again, $4\mathbb{Z}$ does not contain 2, which divides every element of $4\mathbb{Z}$).

4. Two positive integers m and n satisfy $\text{hcf}(m, n) = 6$ and $\text{lcm}(m, n) = 210$. What is mn?
(a) 420; (b) 630; (c) 1260; (d) there is insufficient information to determine the product uniquely.

Answer: (c). By corollary 2.13 of the lecture notes, $mn = \text{hcf}(m, n) \times \text{lcm}(m, n) = 6 \times 210 = 1260$. (You didn't need to work out that $m = 30$ and $n = 42$.)

5. Let n be any integer such that $n \equiv 1 \mod 2$ and $n \equiv 2 \mod 5$. What is $n \mod 10$? (a) 1; (b) 2; (c) 6; (d) 7.

Answer (d). If $n \equiv 1 \mod 2$ then n is odd. If $n \equiv 2 \mod 5$, then the last digit of n must be either 2 or 7. Combining the two forces the last digit to be 7, and thus $n \equiv 7 \mod 10$.

6. What is $(314 \times 159) \mod 5$? (a) 1; (b) 2; (c) 3; (d) 4.

Answer: (a). Note that $314 \times 159 \equiv (314 \mod 5) \times (159 \mod 5) \equiv 4 \times 4 \equiv 16 \equiv 1 \mod 5$. (You didn't need to work out that $314 \times 159 = 49926$.)

7. Consider the following statements:
(i) If m and n are integers then $m\mathbb{Z} \cup n\mathbb{Z}$ is closed under addition but not subtraction.
(ii) The set of odd integers is a subgroup of $\mathbb{Z}$.
(iii) $100\mathbb{Z} + 103\mathbb{Z}$ contains $15\mathbb{Z}$.
(iv) If p and q are distinct prime numbers then $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$.
(v) Given two subgroups of $\mathbb{Z}$, one subgroup must contain the other.
How many of these statements are true? (a) 1 is true and 4 are false; (b) 2 are true and 3 are false; (c) 3 are true and 2 are false; (d) 4 are true and 1 is false.

Answer: (b). Two are true, namely (iii) and (iv), and three are false, namely (i), (ii) and (v). (i) is false; $2\mathbb{Z} \cup 3\mathbb{Z}$ does not contain $2 + 3 = 5$. (ii) is false; the set is not closed under addition (or subtraction). (iii) is true, since $15 = 5 \times 3 = 5(103 - 100) \in 100\mathbb{Z} + 103\mathbb{Z}$, so this contains $15\mathbb{Z}$ (indeed, as 100 and 103 are coprime, the sum is just $\mathbb{Z}$). (iv) is true, since distinct primes are coprime. (v) is clearly false ($\mathbb{Z}$ itself is a subgroup for example).

8. Let A be a nonempty subset of $\mathbb{Z}$ which is closed under addition (i.e. if $x, y \in A$ then $x + y \in A$); and let B be a nonempty subset of $\mathbb{Z}$ which is closed under subtraction (i.e. if $x, y \in B$ then $x - y \in B$). Which of the following statements is true?
(a) Both A and B must be subgroups of $\mathbb{Z}$.
(b) A must be a subgroup of $\mathbb{Z}$, but B need not be a subgroup of $\mathbb{Z}$.
(c) B must be a subgroup of $\mathbb{Z}$, but A need not be a subgroup of $\mathbb{Z}$.
(d) Neither A nor B need be a subgroup of $\mathbb{Z}$.

Answer: (c). A subset of $\mathbb{Z}$ which is closed under addition need not be a subgroup of $\mathbb{Z}$: for example, take $A = \mathbb{N} \cup \{0\}$, which is closed under addition but is not closed under subtraction. However, if a nonempty subset B of $\mathbb{Z}$ is closed under subtraction, then B *is* a subgroup of $\mathbb{Z}$. First, note that as B is nonempty, there is some element $b \in B$; thus $0 = b - b \in B$. Thus, if $y \in B$, then $-y = 0 - y \in B$ as it is closed under subtraction. Then for any $x, y \in B$, we have $x + y = x - (-y) \in B$, and so B is also closed under addition.

9. What is $6^7 \mod 8$? (a) 0; (b) 2; (c) 4; (d) 6.

Answer (a). Simply notice that $6^7 \equiv (-2)^7 \equiv -2^7 \equiv -2 \times 8 \times 8 \equiv 0 \mod 8$.

10. Precisely how many subgroups of $\mathbb{Z}$ include the number 30? (a) 4; (b) 6; (c) 8; (d) infinitely many.

Answer (c). Eight subgroups include 30, namely $\mathbb{Z}$, $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$, $6\mathbb{Z}$, $10\mathbb{Z}$, $15\mathbb{Z}$, and $30\mathbb{Z}$.

11. Let p and q be distinct primes, and let n be any integer such that $n \equiv 1 \mod p$ and $n \equiv 1 \mod q$. What is $n \mod pq$? (a) 0; (b) 1; (c) p; (d) q.

Answer (b). If $n \equiv 1 \mod p$ and $n \equiv 1 \mod q$, then $n - 1$ is divisible by both p and q, and hence $n - 1$ is divisible by pq, so $n \equiv 1 \mod pq$.