

Additional Practice: Algebra Weeks 1–4

MA180/MA185/MA190

Contents

1	Divisibility and remainders	1
2	Euclid's algorithm and Bézout identities	2
3	Linear Diophantine equations	3
4	Congruences and modular arithmetic	3
5	Modular inverses and division	4
6	Applications (Checksums)	5

This sheet provides additional practice problems. This is not marked, nor is it part of the tutorials. Although the solutions are available, try to get the point where you can write a complete answer without looking at them.

1 Divisibility and remainders

- For each statement, determine whether it is true or false. If true, give an integer quotient.
 - $8 \mid 104$;
 - $7 \mid 100$;
 - $-6 \mid 42$;
 - $15 \mid 0$;
 - $0 \mid 15$.
- Use the remainder theorem to write $a = bq + r$, where $0 \leq r < b$.
 - $a = 157$, $b = 12$;
 - $a = 2025$, $b = 37$;
 - $a = -64$, $b = 9$;
 - $a = -103$, $b = 11$.
- List all positive common divisors of each pair, and hence find the gcd.

- (a) 24 and 36;
 - (b) 45 and 70;
 - (c) 84 and 126.
4. Determine whether each pair is coprime. Justify the answer.
- (a) 25 and 36;
 - (b) 33 and 55;
 - (c) 143 and 120;
 - (d) 221 and 26.
5. Suppose $d \mid a$ and $d \mid b$. Prove that $d \mid (5a - 3b)$. Generalise the argument to prove that $d \mid (ra + sb)$ for all $r, s \in \mathbb{Z}$.

2 Euclid's algorithm and Bézout identities

6. Use Euclid's algorithm to calculate:
- (a) $\gcd(252, 198)$;
 - (b) $\gcd(391, 299)$;
 - (c) $\gcd(527, 341)$;
 - (d) $\gcd(1232, 428)$.
7. Use Euclid's algorithm to determine which pairs are coprime:
- (a) 89 and 144;
 - (b) 123 and 202;
 - (c) 187 and 221.
8. Use Euclid's algorithm and back-substitution to find integers x, y such that

$$252x + 198y = \gcd(252, 198).$$

9. Find integers x, y satisfying

$$391x + 299y = \gcd(391, 299).$$

Show the complete Euclidean algorithm and back-substitution, and verify the answer.

10. For each pair (a, b) , find integers (x, y) such that $ax + by = \gcd(a, b)$.
- (a) $(a, b) = (65, 28)$;
 - (b) $(a, b) = (144, 55)$;
 - (c) $(a, b) = (414, 662)$.
11. Suppose $\gcd(a, b) = d$. Explain why every integer of the form $ax + by$ is divisible by d , and why some choice of $x, y \in \mathbb{Z}$ satisfies $ax + by = d$.

3 Linear Diophantine equations

12. Determine whether each equation has an integer solution.

(a) $18x + 30y = 7$;

(b) $18x + 30y = 12$;

(c) $35x + 64y = 17$;

(d) $42x + 70y = 15$;

(e) $84x + 126y = 294$.

13. Find one integer solution to each equation.

(a) $65x + 28y = 3$;

(b) $391x + 299y = 161$;

(c) $144x + 55y = 9$.

14. Find all integer solutions of

$$21x + 15y = 12.$$

Use a parameter $n \in \mathbb{Z}$ and verify the resulting family.

15. Find all integer solutions of

$$132x + 84y = 36.$$

Include the gcd, one particular solution, the complete family, and a check.

16. Find all non-negative integer solutions of

$$7x + 11y = 173.$$

Explain how inequalities restrict the parameter.

17. Apples cost 47 cents and oranges cost 31 cents. A customer spends exactly EUR 4.22. Form a Diophantine equation, find all integer solutions, and determine all solutions with non-negative numbers of fruit.

18. Student tickets cost EUR 8 and standard tickets cost EUR 13. Total revenue is EUR 307. Find all non-negative solutions, count the possible combinations, and identify which combination sells the greatest total number of tickets.

4 Congruences and modular arithmetic

19. Find the standard representative in the stated residue system.

(a) 83 in $\mathbb{Z}_7$;

(b) -41 in $\mathbb{Z}_9$;

(c) 237 in $\mathbb{Z}_{11}$;

(d) -2025 in $\mathbb{Z}_{17}$.

20. Determine whether each congruence is true. Justify using divisibility.

- (a) $47 \equiv 5 \pmod{7}$;
- (b) $-8 \equiv 4 \pmod{6}$;
- (c) $71 \equiv 8 \pmod{9}$;
- (d) $2025 \equiv 1 \pmod{16}$;
- (e) $1001 \equiv 0 \pmod{13}$.

21. Give each answer as a standard representative.

- (a) $37 + 49 \pmod{12}$;
- (b) $37 \cdot 49 \pmod{12}$;
- (c) $5^4 \pmod{7}$;
- (d) $2^8 + 3^5 \pmod{5}$;
- (e) $(-17)(23) \pmod{11}$.

22. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Prove that

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

23. Find non-zero $a, b \in \mathbb{Z}_{12}$ such that $ab \equiv 0 \pmod{12}$. Find several pairs. Explain why this cannot happen in $\mathbb{Z}_p$ when p is prime.

5 Modular inverses and division

24. Determine whether each element has an inverse modulo the stated modulus.

- (a) $5 \pmod{14}$;
- (b) $8 \pmod{15}$;
- (c) $9 \pmod{21}$;
- (d) $17 \pmod{43}$;
- (e) $22 \pmod{35}$.

25. Use Euclid's algorithm and back-substitution to calculate:

- (a) $5^{-1} \pmod{14}$;
- (b) $8^{-1} \pmod{15}$;
- (c) $17^{-1} \pmod{43}$;
- (d) $22^{-1} \pmod{35}$.

Check each answer by multiplication.

26. Evaluate each expression if it is defined. Otherwise explain why it is undefined.

- (a) $\frac{8}{3} \pmod{11}$;

- (b) $\frac{7}{5} \pmod{12}$;
- (c) $\frac{4}{6} \pmod{15}$;
- (d) $\frac{11}{7} \pmod{16}$.

27. List all invertible elements of $\mathbb{Z}_{18}$ and pair each element with its inverse.

6 Applications (Checksums)

28. Apply the Luhn algorithm to determine whether

4539148803436467

passes the check. Show the contribution made by every digit.

29. Find the missing digit in

4929 14?8 5673 1026

so that the number satisfies the Luhn check.

30. Use the Luhn algorithm to find the missing digit in

5412 7534 19?2 8476

so that the number passes the Luhn check. Show the contribution made by every digit and verify your answer.

31. Use the PPS-style convention to find the check character in

7654321?A.

32. Use the PPS-style convention to find the check character in

3141592?B.