

Additional Practice: Algebra Weeks 1–4 Solutions

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	4
5	Modular inverses and division	4
6	Applications (Checksums)	5

1 Divisibility and remainders

- True: $104 = 8(13)$.
 - False: $100 = 7(14) + 2$.
 - True: $42 = (-6)(-7)$.
 - True: $0 = 15(0)$.
 - False: $0q = 0 \neq 15$ for every integer q .
- $157 = 12(13) + 1$.
 - $2025 = 37(54) + 27$.
 - $-64 = 9(-8) + 8$.
 - $-103 = 11(-10) + 7$.
- The positive common divisors and gcds are:
 - 1, 2, 3, 4, 6, 12; gcd 12.
 - 1, 5; gcd 5.
 - 1, 2, 3, 6, 7, 14, 21, 42; gcd 42.
- Coprime: $25 = 5^2$ and $36 = 2^2 3^2$ have no common prime factor.
 - Not coprime: $\gcd(33, 55) = 11$.

(c) Coprime: $143 = 11 \cdot 13$ and $120 = 2^3 \cdot 3 \cdot 5$.

(d) Not coprime: $221 = 13 \cdot 17$ and $26 = 2 \cdot 13$, so the gcd is 13.

5. Write $a = du$ and $b = dv$, where $u, v \in \mathbb{Z}$. Then

$$5a - 3b = d(5u - 3v), \quad ra + sb = d(ru + sv).$$

Both bracketed expressions are integers, proving both claims.

2 Euclid's algorithm and Bézout identities

6. (a) $252 = 198 + 54$, $198 = 3(54) + 36$, $54 = 36 + 18$, $36 = 2(18)$. Thus the gcd is 18.

(b) $391 = 299 + 92$, $299 = 3(92) + 23$, $92 = 4(23)$. Thus the gcd is 23.

(c) $527 = 341 + 186$, $341 = 186 + 155$, $186 = 155 + 31$, $155 = 5(31)$. Thus the gcd is 31.

(d) $1232 = 2(428) + 376$, $428 = 376 + 52$, $376 = 7(52) + 12$, $52 = 4(12) + 4$, $12 = 3(4)$. Thus the gcd is 4.

7. The successive Euclidean remainders (including the final zero) are:

(a) For $(144, 89)$: 55, 34, 21, 13, 8, 5, 3, 2, 1, 0. The gcd is 1: coprime.

(b) For $(202, 123)$: 79, 44, 35, 9, 8, 1, 0. The gcd is 1: coprime.

(c) For $(221, 187)$: 34, 17, 0. The gcd is 17: not coprime.

8. Using the divisions in Question 6(a),

$$18 = 54 - 36 = 54 - (198 - 3 \cdot 54) = 4(252 - 198) - 198 = 4 \cdot 252 - 5 \cdot 198.$$

Thus $(x, y) = (4, -5)$; indeed $1008 - 990 = 18$.

9. Euclid's algorithm gives

$$391 = 299 + 92, \quad 299 = 3 \cdot 92 + 23, \quad 92 = 4 \cdot 23.$$

Back-substitution gives

$$23 = 299 - 3 \cdot 92 = 299 - 3(391 - 299) = -3 \cdot 391 + 4 \cdot 299.$$

Thus $(x, y) = (-3, 4)$; indeed $-1173 + 1196 = 23$.

10. Suitable identities are:

(a) $65(-3) + 28(7) = 1$, so $(x, y) = (-3, 7)$.

(b) $144(-21) + 55(55) = 1$, so $(x, y) = (-21, 55)$.

(c) $414(8) + 662(-5) = 2$, so $(x, y) = (8, -5)$.

In (a) and (b), the identity forces the gcd to be 1. In (c), both numbers are even and the identity forces the gcd to be 2.

11. Since $d \mid a$ and $d \mid b$, we have $d \mid ax + by$ for all integers x, y . Bézout's identity (obtained by back-substitution in Euclid's algorithm) gives some x, y with $ax + by = d$.

3 Linear Diophantine equations

12. An integer solution exists exactly when $\gcd(a, b) \mid c$.

(a) No: $\gcd(18, 30) = 6 \nmid 7$.

(b) Yes: $6 \mid 12$.

(c) Yes: $\gcd(35, 64) = 1 \mid 17$.

(d) No: $\gcd(42, 70) = 14 \nmid 15$.

(e) Yes: $\gcd(84, 126) = 42 \mid 294$.

13. (a) $(x, y) = (-9, 21)$: $-585 + 588 = 3$.

(b) $(x, y) = (-21, 28)$: $-8211 + 8372 = 161$.

(c) $(x, y) = (31, -81)$: $4464 - 4455 = 9$.

14. The gcd is 3, and $(2, -2)$ is a particular solution. All solutions are

$$x = 2 + 5n, \quad y = -2 - 7n \quad (n \in \mathbb{Z}).$$

Indeed $21(2+5n)+15(-2-7n) = 12$. Completeness follows from $7(x-2) = -5(y+2)$ and $\gcd(7, 5) = 1$.

15. Euclid gives $132 = 84 + 48$, $84 = 48 + 36$, $48 = 36 + 12$, $36 = 3(12)$, so the gcd is 12. A particular solution is $(-1, 2)$. All solutions are

$$x = -1 + 7n, \quad y = 2 - 11n \quad (n \in \mathbb{Z}).$$

Check: $132(-1 + 7n) + 84(2 - 11n) = 36$. These are all solutions since the reduced coefficients 11 and 7 are coprime.

16. A particular solution is $(9, 10)$; since $\gcd(7, 11) = 1$, all integer solutions are

$$x = 9 + 11n, \quad y = 10 - 7n.$$

Non-negativity requires $-9/11 \leq n \leq 10/7$, hence $n = 0, 1$. The solutions are $(9, 10), (20, 3)$.

17. With x apples and y oranges, $47x + 31y = 422$. Since $\gcd(47, 31) = 1$ and $(7, 3)$ is a solution, all integer solutions are

$$x = 7 + 31n, \quad y = 3 - 47n.$$

Non-negativity gives $-7/31 \leq n \leq 3/47$, hence $n = 0$. Thus the only purchase is 7 apples and 3 oranges.

18. With x student tickets and y standard tickets, $8x + 13y = 307$. All integer solutions are

$$x = 1 + 13n, \quad y = 23 - 8n.$$

Non-negativity requires $-1/13 \leq n \leq 23/8$, so $n = 0, 1, 2$. The three combinations are $(1, 23), (14, 15), (27, 7)$. Since $x + y = 24 + 5n$, the greatest total is 34 tickets: 27 student and 7 standard.

4 Congruences and modular arithmetic

19. (a) 6, since $83 = 7(11) + 6$.
(b) 4, since $-41 = 9(-5) + 4$.
(c) 6, since $237 = 11(21) + 6$.
(d) 15, since $-2025 = 17(-120) + 15$.
20. (a) True: $47 - 5 = 42 = 7(6)$.
(b) True: $-8 - 4 = -12 = 6(-2)$.
(c) True: $71 - 8 = 63 = 9(7)$.
(d) False: $2025 - 1 = 2024 = 16(126) + 8$.
(e) True: $1001 = 13(77)$.
21. (a) $86 \equiv 2 \pmod{12}$.
(b) $37 \cdot 49 \equiv 1 \cdot 1 = 1 \pmod{12}$.
(c) $5^4 = 625 \equiv 2 \pmod{7}$.
(d) $2^8 + 3^5 = 499 \equiv 4 \pmod{5}$.
(e) $(-17)(23) = -391 \equiv 5 \pmod{11}$.

22. Write $a - b = mr$ and $c - d = ms$, with $r, s \in \mathbb{Z}$. Then

$$(a + c) - (b + d) = m(r + s), \quad ac - bd = c(a - b) + b(c - d) = m(cr + bs).$$

Thus m divides both differences, proving the two congruences.

23. Examples in $\mathbb{Z}_{12}$ are $(a, b) = (2, 6), (3, 4), (4, 6), (6, 8)$. Each product is divisible by 12. If a product ab is divisible by p , then a and b are divisors of p . Since p is prime, at least one of them must be divisible by p . (See Euclid's lemma.)

5 Modular inverses and division

24. An inverse exists exactly when the element and modulus are coprime.
- (a) Yes: $\gcd(5, 14) = 1$.
(b) Yes: $\gcd(8, 15) = 1$.
(c) No: $\gcd(9, 21) = 3$.
(d) Yes: $\gcd(17, 43) = 1$.
(e) Yes: $\gcd(22, 35) = 1$.
25. (a) $14 = 2(5) + 4$, $5 = 4 + 1$, $4 = 4(1)$. Hence

$$1 = 5 - (14 - 2 \cdot 5) = 3 \cdot 5 - 14.$$

Thus $5^{-1} \equiv 3 \pmod{14}$.

(b) $15 = 8 + 7$, $8 = 7 + 1$, $7 = 7(1)$. Hence

$$1 = 8 - (15 - 8) = 2 \cdot 8 - 15.$$

Thus $8^{-1} \equiv 2 \pmod{15}$.

(c) $43 = 2(17) + 9$, $17 = 9 + 8$, $9 = 8 + 1$, $8 = 8(1)$. Hence

$$1 = 9 - (17 - 9) = 2(43 - 2 \cdot 17) - 17 = 2 \cdot 43 - 5 \cdot 17.$$

Thus $17^{-1} \equiv -5 \equiv 38 \pmod{43}$.

(d) $35 = 22 + 13$, $22 = 13 + 9$, $13 = 9 + 4$, $9 = 2(4) + 1$, $4 = 4(1)$. Hence

$$\begin{aligned} 1 &= 9 - 2(13 - 9) = 3 \cdot 9 - 2 \cdot 13 \\ &= 3(22 - 13) - 2 \cdot 13 = 3 \cdot 22 - 5(35 - 22) \\ &= 8 \cdot 22 - 5 \cdot 35. \end{aligned}$$

Thus $22^{-1} \equiv 8 \pmod{35}$.

26. Division means multiplication by the denominator's inverse.

(a) $3^{-1} \equiv 4 \pmod{11}$, so $8/3 \equiv 32 \equiv 10 \pmod{11}$.

(b) $5^{-1} \equiv 5 \pmod{12}$, so $7/5 \equiv 35 \equiv 11 \pmod{12}$.

(c) Undefined: $\gcd(6, 15) = 3$, so 6 has no inverse modulo 15.

(d) $7^{-1} \equiv 7 \pmod{16}$, so $11/7 \equiv 77 \equiv 13 \pmod{16}$.

27. The invertible elements are $\{1, 5, 7, 11, 13, 17\}$. Their inverse pairings are

$$1 \leftrightarrow 1, \quad 5 \leftrightarrow 11, \quad 7 \leftrightarrow 13, \quad 17 \leftrightarrow 17.$$

Indeed $5 \cdot 11 = 55$, $7 \cdot 13 = 91$ and $17^2 = 289$ are all equivalent to 1 modulo 18.

6 Applications (Checksums)

28. For 4539 1488 0343 6467, the contributions from left to right are

$$8, 5, 6, 9, \quad 2, 4, 7, 8, \quad 0, 3, 8, 3, \quad 3, 4, 3, 7.$$

Their sum is $80 \equiv 0 \pmod{10}$, so the number **passes**.

29. For 4929 14d8 5673 1026, the contributions are

$$8, 9, 4, 9, \quad 2, 4, x, 8, \quad 1, 6, 5, 3, \quad 2, 0, 4, 6.$$

The total is $71 + x$, so $x \equiv 9 \pmod{10}$. Since d is in the tenth position and since x is odd, we need $x = 9 = 1 + 8$, giving $d = 9$.

30. For 5412 7534 19d2 8476, the contributions are

$$1, 4, 2, 2, \quad 5, 5, 6, 4, \quad 2, 9, x, 2, \quad 7, 4, 5, 6.$$

The total is $64 + x$, so $x = 6$ and $d = 3$.

PPS convention. Use $A = 1, \dots, V = 22, W \equiv 0 \pmod{23}$. We require

$$d_8 \equiv 8d_1 + 7d_2 + 6d_3 + 5d_4 + 4d_5 + 3d_6 + 2d_7 + 9d_9 \pmod{23}.$$

31. For 7654321? A , the sum excluding the check character is

$$8(7) + 7(6) + 6(5) + 5(4) + 4(3) + 3(2) + 2(1) + 9(1) = 177.$$

Thus $d_8 \equiv 177 \equiv 16 \pmod{23}$, corresponding to P . The answer is 7654321 PA .

32. For 3141592? B , the sum excluding the check character is

$$8(3) + 7(1) + 6(4) + 5(1) + 4(5) + 3(9) + 2(2) + 9(2) = 129.$$

Thus $d_8 \equiv 129 \equiv 14 \pmod{23}$, corresponding to N . The answer is 3141592 NB .