Modular Arithmetic — Instructor Solution Manual

Covers Student Worksheet 'Guided Examples' and 'You Try' problems

> Pronunciation guide: Carl Friedrich Gauss (sounds like 'GOWSS'—rhymes with 'house'); congruent ('kun-GROO-uhnt'); modulo ('MOD-yoo-loh'); modulus ('MOD-yuh-luss').

Summary of key results

Definition (congruence modulo m). For a positive integer m, integers a and b are said to be congruent modulo m if m divides $(a - b)$. We write $a \equiv b \pmod{m}$. Equivalently, a and b have the same remainder upon division by m.

Notation. The number m is the modulus. The set of possible remainders is $\{0,1,\ldots,m-1\}$.

Theorem 4. Let $m>0$. Integers a and b are congruent modulo m iff there exists an integer k such that $a = b + k\cdot m$.

Proof (short). If $a \equiv b \pmod{m}$, then $m \mid (a-b)$, so $a-b = k\cdot m$ for some integer k, i.e., $a = b + k\cdot m$. Conversely, if $a = b + k\cdot m$, then $a-b = k\cdot m$ is a multiple of m, hence $a \equiv b \pmod{m}$. ■

Theorem 5 (Arithmetic with congruences). If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a\cdot c \equiv b\cdot d \pmod{m}$.

Proof idea. From $a = b + k\cdot m$ and $c = d + \ell\cdot m$ (Theorem 4), add to get $a + c = (b + d) + (k + \ell)\cdot m$, so $a + c \equiv b + d \pmod{m}$. Multiply to get $a\cdot c = (b + k\cdot m)(d + \ell\cdot m) = b\cdot d + m(b\ell + dk + k\ell\cdot m)$, which is $b\cdot d$ plus a multiple of m; thus $a\cdot c \equiv b\cdot d \pmod{m}$. ■

Solutions & Commentary — Section A (like Example 5)

Guided Example A (like Example 5). Decide (i) whether 17 is congruent to 5 modulo 6, and (ii) whether 24 and 14 are congruent modulo 6.

Step 1: Use the definition: numbers are congruent mod 6 iff their difference is a multiple of 6.

- (i) $17 - 5 = 12 = 2 \cdot 6$ ⇒ a multiple of 6 ⇒ Yes, $17 \equiv 5 \pmod 6$.
- (ii) $24 - 14 = 10$, which is not a multiple of 6 ⇒ No, $24 \not\equiv 14 \pmod 6$.

Check (remainders): 17 mod 6 = 5; 24 mod 6 = 0 and 14 mod 6 = 2 ⇒ remainders differ ⇒ not congruent.

Solutions for You Try 1.

(a) $10 - 1 = 9 = 3 \cdot 3$ ⇒ Yes, $10 \equiv 1 \pmod 3$. (b) 7 mod 3 = 1 and 13 mod 3 = 1 ⇒ remainders match ⇒ Yes, $7 \equiv 13 \pmod 3$.

Solutions for You Try 2.

(a) $-41 - 7 = -48 = (-4) \cdot 12$ ⇒ multiple of 12 ⇒ Yes, $-41 \equiv 7 \pmod{12}$. (b) $123 - 567 = -444$. Because $9 \cdot (-49) = -441$ and $9 \cdot (-50) = -450$, -444 is not a multiple of 9 ⇒ Not congruent. Alternatively: 123 mod 9 = 6, 567 mod 9 = 0 ⇒ remainders differ.

Solutions & Commentary — Section B (like Example 6)

Guided Example B (like Example 6). Use Theorem 5 with $m = 5$. Given $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, find (i) $(7 + 11) \bmod 5$ and (ii) $(7 \cdot 11) \bmod 5$.

Step 1: Replace each number by a convenient congruent value modulo 5.

- $7 \equiv 2 \pmod{5}$ because $7 = 5 + 2$. $11 \equiv 1 \pmod{5}$ because $11 = 2 \cdot 5 + 1$.

Step 2 (sum): $7 + 11 \equiv 2 + 1 = 3 \pmod{5}$. So $(7 + 11) \bmod 5 = 3$.

Step 3 (product): $7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$. So $(7 \cdot 11) \bmod 5 = 2$.

Solutions for You Try 3.

Modulo 7, $8 \equiv 1$ and $15 \equiv 1$. (a) $8 + 15 \equiv 1 + 1 = 2 \Rightarrow$ answer 2. (b) $8 \cdot 15 \equiv 1 \cdot 1 = 1 \Rightarrow$ answer 1.

Solutions for You Try 4.

Modulo 9, $68 \equiv 68 - 63 = 5$; $101 \equiv 101 - 99 = 2$. (a) Sum: $5 + 2 = 7 \Rightarrow$ answer 7. (b) Product: $5 \cdot 2 = 10 \equiv 1$ (since $10 - 9 = 1$).

Solutions & Commentary — Section C (like Example 7)

Guided Example C (like Example 7). Find the value of $(19^3 \bmod 31)^4 \bmod 23$.

Step 1 (first modulus): Compute $19^3 \bmod 31$. $19^2 = 361$; $19^3 = 361 \cdot 19 = 6859$. Now divide by 31: $31 \cdot 221 = 6851$, leaving remainder 8 $\Rightarrow 19^3 \bmod 31 = 8$.

Step 2 (raise and reduce): We need $8^4 \bmod 23$. First $8^2 = 64 \equiv 64 - 2 \cdot 23 = 18 \pmod{23}$. Then $8^4 = (8^2)^2 \equiv 18^2 = 324 \equiv 324 - 14 \cdot 23 = 324 - 322 = 2 \pmod{23}$.

Conclusion: $(19^3 \bmod 31)^4 \bmod 23 = 2$.

Solutions for You Try 5.

$13^2 \bmod 5$: $13 \equiv 3 \pmod 5$, so $13^2 \equiv 3^2 = 9 \equiv 4$. Now $4^3 = 64$; modulo 7 we have $64 - 56 = 8 \equiv 1$. Final answer: 1.

Solutions for You Try 6.

$37 \equiv -4 \pmod{41}$. $(-4)^5 = -1024$. Since $41 \cdot 25 = 1025$, $-1024 \equiv 1 \pmod{41}$. Then $(37^5 \bmod 41) = 1$. Now $1^6 \bmod 29 = 1$. Final answer: 1.

Teaching notes.

- Encourage students to check congruence both ways: difference-as-multiple (Theorem 4) and remainder comparison.
- In product/sum problems (Theorem 5), reduce early and often. Replace large numbers with small congruent residues.
- For exponent problems, look for smart rewrites (e.g., $37 \equiv -4$) and use repeated squaring. Emphasize that you can reduce after each step.
- Common pitfall: assuming (a mod m)·(b mod m) equals (ab) without explicitly applying Theorem 5. Make them justify the step.