Modular Arithmetic — Student Worksheet

Number Theory & Cryptography Unit

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

A quick tale: young Carl Friedrich Gauss (1777–1855) once stunned his teacher by summing the numbers 1 through 100 in seconds. He noticed pairs add to 101—(1+100), (2+99), …—which makes 50 pairs, so the total is $50 \times 101 = 5050$. That pattern-spotting is the spirit of number theory and why modular arithmetic is a superpower.

Key ideas

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 $\{0,1,\dots,m-1\}$.

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 $a\cdot c \equiv b\cdot d \pmod{m}$. ■

Working with Congruences (Definition & Theorem 4)

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) $17 - 5 = 12 = 2 \cdot 6 \Rightarrow$ a multiple of 6 $\Rightarrow$ Yes, $17 \equiv 5 \pmod 6$.

• (ii) $24 - 14 = 10$, which is not a multiple of 6 $\Rightarrow$ No, $24 \not\equiv 14 \pmod 6$.

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

You Try 1 (easier). Decide if (a) $10 \equiv 1 \pmod 3$, and (b) 7 and 13 are congruent modulo 3.

Show your work here

You Try 2 (harder). Decide if (a) $-41 \equiv 7 \pmod{12}$, and (b) 123 and 567 are congruent modulo 9.

Show your work here

Arithmetic with Congruences (Theorem 5)

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 $(7 \cdot 11) \bmod 5 = 2$.

You Try 3 (easier). Work modulo 7. Compute (a) $8 + 15$ and (b) $8 \cdot 15$, giving answers as remainders in $\{0,\dots,6\}$.

Show your work here

You Try 4 (harder). Work modulo 9. Compute (a) $(68 + 101) \bmod 9$ and (b) $(68 \cdot 101) \bmod 9$ by first reducing 68 and 101 modulo 9.

Show your work here

Exponent Tricks with Mods (Powering & Reductions)

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

You Try 5 (slightly easier). Compute $(13^2 \bmod 5)^3 \bmod 7$. Show each reduction step.

Show your work here

You Try 6 (harder). Compute $(37^5 \bmod 41)^6 \bmod 29$. Hint: $37 \equiv -4 \pmod{41}$.

Show your work here