MATH 160 — Number Theory

numberbender.com

Name: _____ Date: _____ Score: / 10

Learning Objectives

- Find GCD using the Euclidean Algorithm and LCM via the GCD
- Compute modular arithmetic and solve linear congruences
- Apply Fermat's Little Theorem to reduce large exponents
- Use prime factorization to count divisors

For the Euclidean Algorithm: always write each division step. For modular arithmetic: remainders must be in [0, n–1].

1. Find gcd(48, 18) using the Euclidean Algorithm. Show all steps.

$$\gcd(48, 18) = ?$$

Answer: _____

2. Find lcm(12, 18) using the formula lcm(a,b) = ab / gcd(a,b).

$$\text{lcm}(12, 18) = \frac{12 \cdot 18}{\gcd(12, 18)}$$

Answer: _____

3. Find the prime factorization of 360. Use it to find all divisors.

$$360 = ?$$

Answer: _____

4. Compute 17 mod 5 and −7 mod 3. Explain what "mod" means.

$$17 \pmod 5 = ? \quad -7 \pmod 3 = ?$$

Answer: _____

5. Solve the linear congruence: 3x ≡ 7 (mod 11).

$$3x \equiv 7 \pmod{11}$$

Answer: _____

6. Use the Euclidean algorithm to find gcd(252, 105) and express it as a linear combination (Bézout's Identity).

$$\gcd(252, 105) = 252s + 105t \text{ (Bezout)}$$

Answer: _____

7. Apply Fermat's Little Theorem to compute 3■■ mod 23.

$$3^{47} \pmod{23}$$

Answer: _____

Scan to watch

8. Determine if 97 is prime using trial division.

97 prime? $\sqrt{97} \approx 9.8$

Answer: _____

9. Find all solutions to $x^2 \equiv 1 \pmod 8$.

$$x^2 \equiv 1 \pmod 8$$

Answer: _____

10. Two bells ring together at time 0. Bell A rings every 12 minutes; Bell B rings every 18 minutes. When do they next ring together?

$\text{lcm}(12, 18) = ?$

Answer: _____

Problems 1–2: GCD then LCM — always in this order. Problem 5 (linear congruence): requires finding modular inverse. Problem 7 (Fermat): reduce exponent modulo p–1 first.

Solutions

1. Find gcd(48, 18) using the Euclidean Algorithm. Show all steps.

$\gcd(48, 18) = ?$

→ *48 = 2·18 + 12.*
→ *18 = 1·12 + 6.*
→ *12 = 2·6 + 0.*
→ *Remainder is 0 → gcd(48, 18) = 6.*

Answer: $\gcd(48, 18) = 6$

2. Find lcm(12, 18) using the formula lcm(a,b) = ab / gcd(a,b).

$$\text{lcm}(12, 18) = \frac{12 \cdot 18}{\gcd(12, 18)}$$

→ *gcd(12,18): 18=1·12+6, 12=2·6+0 → gcd=6.*
→ *lcm(12,18) = 12·18/6 = 216/6 = 36.*

Answer: $\text{lcm}(12, 18) = 36$

3. Find the prime factorization of 360. Use it to find all divisors.

$360 = ?$

→ *360 ÷ 2 = 180. 180 ÷ 2 = 90. 90 ÷ 2 = 45.*
→ *45 ÷ 3 = 15. 15 ÷ 3 = 5. 5 is prime.*
→ *360 = $2^3 \cdot 3^2 \cdot 5$.*
→ *Number of divisors = (3+1)(2+1)(1+1) = 4·3·2 = 24 divisors.*

Answer: $360 = 2^3 \cdot 3^2 \cdot 5^1$

4. Compute 17 mod 5 and –7 mod 3. Explain what "mod" means.

$17 \pmod 5 = ? \quad -7 \pmod 3 = ?$

→ *17 mod 5: 17 = 3·5 + 2. Remainder = 2.*
→ *–7 mod 3: –7 = (–3)·3 + 2. Remainder = 2. (remainder is always ≥ 0)*
→ *"a mod n" = remainder when a is divided by n (0 ≤ r < n).*

Answer: $17 \pmod 5 = 2, \quad -7 \pmod 3 = 2$

5. Solve the linear congruence: 3x ≡ 7 (mod 11).

$3x \equiv 7 \pmod{11}$

→ *Find 3■¹ mod 11 (the inverse of 3 mod 11).*
→ *3·4=12≡1 (mod 11) → 3■¹=4.*
→ *x ≡ 4·7 = 28 ≡ 6 (mod 11).*

Answer: $x \equiv 6 \pmod{11}$

6. Use the Euclidean algorithm to find gcd(252, 105) and express it as a linear combination (Bézout's Identity).

$\gcd(252, 105) = 252s + 105t$ (Bezout)

→ *252 = 2·105 + 42.*
→ *105 = 2·42 + 21.*
→ *42 = 2·21 + 0. gcd = 21.*
→ *Back-substitute: 21 = 105 – 2·42 = 105 – 2(252–2·105) = 5·105 – 2·252.*
→ *Bézout: 21 = 252(–2) + 105(5).*

Answer: $\gcd(252, 105) = 21 = 5 \cdot 105 + (-2) \cdot 252$ (see steps)

---

7. Apply Fermat's Little Theorem to compute 3■■ mod 23.

$3^{47} \pmod{23}$

→ *Fermat: if p is prime and gcd(a,p)=1, then a^(p-1) ≡ 1 (mod p).*
→ *23 is prime and gcd(3,23)=1 → $3^{22} \equiv 1 \pmod{23}$.*
→ *47 = 2·22 + 3. 3■■ = $(3^{22})^2 \cdot 3^3 \equiv 1 \cdot 27 \equiv 27 \bmod 23 = 4$.*

Answer: $3^{47} \equiv 3^3 \cdot (3^{22})^2 \equiv 27 \cdot 1 \equiv 4 \pmod{23}$

---

8. Determine if 97 is prime using trial division.

97 prime? $\sqrt{97} \approx 9.8$

→ *Check divisibility by primes ≤ √97 ≈ 9.8: test 2, 3, 5, 7.*
→ *97 is odd (not ÷2). 9+7=16 (not ÷3). Ends in 7 (not ÷5). 97÷7=13.8… (not ÷7).*
→ *No prime ≤ 9 divides 97 → 97 is prime.*

Answer: 97 is prime

---

9. Find all solutions to $x^2 \equiv 1 \pmod 8$.

$x^2 \equiv 1 \pmod 8$

→ *Test x = 0,1,2,3,4,5,6,7 (mod 8):*
→ *$1^2=1\equiv1$✓ $2^2=4$ $3^2=9\equiv1$✓ $4^2=16\equiv0$ $5^2=25\equiv1$✓ $6^2=36\equiv4$ $7^2=49\equiv1$✓.*
→ *Solutions: x ≡ 1, 3, 5, 7 (mod 8).*

Answer: $x \equiv 1, 3, 5, 7 \pmod 8$

---

10. Two bells ring together at time 0. Bell A rings every 12 minutes; Bell B rings every 18 minutes. When do they next ring together?

$\text{lcm}(12, 18) = ?$

→ *They ring together again after lcm(12,18) minutes.*
→ *gcd(12,18) = 6. lcm = 12·18/6 = 36.*
→ *They next ring together at t = 36 minutes.*

Answer: $\text{lcm}(12, 18) = 36$ minutes