HW3 — Number Theory

RYSP

July 25, 2025

1. Compute $\phi(n)$ for each of the following:

- $n = 36$
- $n = 1001$
- $n = 2^5 \cdot 3^2$
- $n = 7 \cdot 11 \cdot 13$
- $n = 2^3 \cdot 5 \cdot 17$

2. Show by direct inclusion–exclusion that if $n = p^e$ then

$$\phi(p^e) = p^e - p^{e-1}.$$

3. Prove the product formula

$$n = \prod_{i=1}^{r} p_i^{e_i} \quad \Longrightarrow \quad \phi(n) = n \prod_{i=1}^{r} \Big(1 - \tfrac{1}{p_i}\Big).$$

4. Verify the product formula by computing $\phi(2310)$ in two ways:

$$2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11.$$

5. Let $a = 18$, $b = 30$, $c = 42$. Compute

$$d = \gcd(a, b, c)$$

by successive Euclidean algorithm steps, and then find explicit integers x, y, z such that

$$18x + 30y + 42z \;=\; d.$$

Give a clear step-by-step derivation of the Bezout coefficients.

6. Prove that

$$\sum_{d \mid n} \phi(d) \;=\; n.$$

7. Use the identity $\sum_{d|n} \phi(d) = n$ to show that

$$\sum_{d|360} \phi(d) = 360.$$

8. Let n be a positive integer. Show that

$$\sum_{\substack{d|n \\ d \text{ odd}}} \phi(d) = \begin{cases} n, & \text{if } n \text{ is odd,} \\ n/2, & \text{if } n \text{ is even.} \end{cases}$$

9. Derive the Möbius-inversion formula for $\phi(n)$:

$$\phi(n) = \sum_{d|n} \mu(d) \, \frac{n}{d}.$$

10. Compute $\phi(n)$ for $n = 840$ by using the Möbius-inversion formula.

11. Prove that

$$n \sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} (p-1).$$

12. Prove that for $n > 2$, $\phi(n)$ is even.

13. Find all $n \leq 20$ for which $\phi(n)$ is odd.

14. Prove that for $n > 1$,

$$\phi(n) \leq n - 1.$$

15. Prove that for $n > 1$,

$$\phi(n) \geq \sqrt{n}.$$

16. Show that equality $\phi(n) = \sqrt{n}$ cannot occur for any integer $n > 1$.

17. Show that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 1, 2, 4, p^e, 2p^e$ for an odd prime p.

18. Solve the system of congruences:

$$x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7, \quad x \equiv 4 \pmod 9.$$

19. How many solutions modulo 1000 does

$$x^2 \equiv 1 \pmod{1000}$$

have? List them.

20. Prove that if $\gcd(a, n) = 1$, then the congruence

$$x \equiv a \pmod{p_i^{e_i}} \quad (i = 1, \ldots, r)$$

has exactly one solution modulo $n = \prod p_i^{e_i}$.

21. Determine all integers x modulo 231 satisfying

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 7, \quad x \equiv 0 \pmod{11}.$$

22. State Fermat's Little Theorem. Use it to test whether 341 is prime.

23. Find a base a with $1 < a < 341$ such that 341 is a pseudoprime to base a.

24. Show that if $a^{n-1} \not\equiv 1 \pmod n$ for some $\gcd(a, n) = 1$, then n is composite.

25. Describe the trial-division method for factoring an integer n and analyze its running time in terms of n.

26. What is the heuristic running time of the Number Field Sieve for factoring a large integer n?

27. In an RSA setup, let $p = 47$, $q = 59$. Compute $N = pq$ and $\phi(N)$.

28. Choose $e = 13$. Compute the decryption exponent d satisfying $ed \equiv 1 \pmod{\phi(N)}$.

29. Encrypt the message $m = 100$ under the public key (N, e) from above.

30. Solve the system of congruences

$$\begin{cases} x \equiv 3 \pmod 5, \\ x \equiv 4 \pmod 7. \end{cases}$$

31. Determine all integers x modulo 231 satisfying

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 7, \\ x \equiv 3 \pmod{11}. \end{cases}$$

32. Let

$$\begin{cases} x \equiv -1 \pmod{13}, \\ x \equiv 5 \pmod{17}, \\ x \equiv 2 \pmod{19}. \end{cases}$$

Find the smallest nonnegative solution.

33. How many solutions modulo 84 does the congruence

$$\begin{cases} x \equiv 2 \pmod 6, \\ x \equiv 5 \pmod{14} \end{cases}$$

have? List them.