HW2 — Number Theory

RYSP

July 25, 2025

1. Find the gcd of 621 and 483.

2. Find a solution of

$$621\,m + 483\,n \;=\; k,$$

where $k = \gcd(621, 483)$.

3. Calculate 3^{64} modulo 67 by repeated squaring.

4. Calculate 3^{64} modulo 67 using Fermat's Little Theorem.

5. Compute $\phi(576)$.

6. Find all the solutions of

$$x^3 - x + 1 \;\equiv\; 0 \pmod{25}.$$

7. Find all solutions of

$$x^3 - x + 1 \;\equiv\; 0 \pmod{35}.$$

8. Find the smallest integer N such that $\phi(n) \geq 5$ for all $n \geq N$.

9. Find two positive integers m, n such that

$$\phi(mn) \;=\; \phi(m)\,\phi(n).$$

10. True or false: two positive integers m, n are coprime if and only if

$$\phi(mn) \;=\; \phi(m)\,\phi(n).$$

Give a proof or counterexample.

11. Give the definition of a *reduced residue system* modulo n.

12. State and prove the Chinese Remainder Theorem.

13. Show that

$$(n-1)! \;\equiv\; 0 \pmod{n}$$

for composite n. *Hint: Make sure your proof works for the case $n = p^2$, where p is a prime.*

14. Solve the system of congruences

$$\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}. \end{cases}$$

15. Let n be a positive integer. Show the identity

$$\sum_{i=1}^{n} i \binom{n}{i} = n\,2^{n-1}.$$

Hint: Differentiate both sides of the Binomial Theorem, or manipulate the binomial coefficients.

16. Calculate the order of 3 modulo 301.

17. Solve the congruence $3x^2 + 5x - 2 \equiv 0 \pmod{35}$ by reducing to prime-power moduli and then recombining via CRT.

18. Determine the number of solutions of $x^4 + 2x + 1 \equiv 0 \pmod{72}$.

19. Show that the congruence $x^3 \equiv 1 \pmod{27}$ has exactly three solutions, and find them.

20. Let $n = 2^3 \cdot 7$. Compute the total number of solutions to $5x + 1 \equiv 0 \pmod{n}$.

21. For each prime power divisor p^e of 1001, find the solutions to $x^2 \equiv 8 \pmod{p^e}$, then reconstruct all solutions mod 1001.

22. Prove that any linear congruence $ax + b \equiv 0 \pmod{n}$ has either zero or exactly $\gcd(a, n)$ solutions.

23. Let $n = 2^2 \cdot 3^2$. Show that the polynomial congruence $x^2 + x + 1 \equiv 0 \pmod{n}$ has no solutions.

24. Find all integer solutions $x \pmod{105}$ to the system

$$x \equiv 2 \pmod{3}, \quad x \equiv 4 \pmod{5}, \quad x \equiv 1 \pmod{7}.$$

25. Determine the number of solutions to

$$x^3 - 2x + 1 \equiv 0 \pmod{2^3 \cdot 11}.$$

26. Prove in general that for any polynomial $f(x)$ of degree k, the number of solutions to $f(x) \equiv 0 \pmod{n}$ equals the product of the numbers of solutions mod each $p_i^{e_i}$.

27. Use Fermat's Little Theorem to show that 561 is composite by finding an explicit base a for which $a^{560} \not\equiv 1 \pmod{561}$.

28. Verify that $2^{16} \bmod 17 = 1$ and conclude what Fermat's test says about 17.

29. Find all bases a with $1 < a < 20$ for which the Fermat test falsely declares the Carmichael number $n = 341$ prime.

30. Prove that if $a^{n-1} \equiv 1 \pmod{n}$ for more than half of the $a \in (\mathbb{Z}/n)^\times$, then n is either prime or a Carmichael number.

31. Show by computation that $2^{10} \not\equiv 1 \pmod{1021}$. What does this say about 1021?

32. Describe one advantage and one disadvantage of the Fermat test versus deterministic trial division.

33. Implement (by hand) one iteration of the Miller–Rabin witness test on $n = 561$ with base $a = 2$; determine whether 2 is a strong witness.

34. Prove that if n is prime then for any $a \not\equiv 0 \pmod{n}$, the order of a divides $n - 1$.

35. Carry out Pollard's rho algorithm by hand (up to finding a nontrivial gcd) on $n = 8051$ using $f(x) = x^2 + 1$ and starting value $x_0 = 2$.

36. Use trial division to fully factor $n = 2\,477\,843$.

37. Show that if n is prime then the Pollard rho iteration will never yield a nontrivial factor.

38. For primes $p = 47$, $q = 59$, compute N, $\phi(N)$, and find a valid public exponent $e = 13$. Then compute the private exponent d.

39. Encrypt the message $m = 2025$ under the public key (N, e) found in the previous problem.

40. Decrypt the ciphertext $c = 4182$ using the private key d from above.

41. Show that RSA decryption indeed recovers m by proving $m^{ed} \equiv m \pmod{N}$.

42. Describe one attack that exploits small e or small d in RSA, and explain the condition under which it succeeds.

43. Compute $\phi(n)$ for $n = 360$ and verify the product formula.

44. List all $n \leq 30$ for which $\phi(n) = \phi(n + 1)$.

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

46. Show that $\sum_{d|100} \phi(d) = 100$.