HW4 — Number Theory

RYSP

July 25, 2025

1. Solve the linear congruence
$$14x \equiv 30 \pmod{100}.$$

2. Determine if the congruence
$$21x \equiv 35 \pmod{49}$$
has a solution, and if so, find all solutions modulo 49.

3. Show that the congruence
$$6x \equiv 15 \pmod{9}$$
has no solution.

4. Solve
$$25x \equiv 10 \pmod{35}.$$

5. Given $a = 18$, $m = 30$, and $b = 12$, find all solutions to
$$ax \equiv b \pmod{m}.$$

6. Prove that if $\gcd(a, m) = 1$, then the linear congruence
$$ax \equiv b \pmod{m}$$
has a unique solution modulo m.

7. For which values of b does
$$15x \equiv b \pmod{45}$$
have a solution?

8. Find all solutions to
$$x^2 \equiv 1 \pmod{7}.$$

9. Prove that the congruence
$$x^3 \equiv 2 \pmod{5}$$
has at most 3 solutions.

10. Given the polynomial

$$f(x) = x^2 + 1,$$

show that it has no solution modulo 3.

11. Solve

$$x^2 + x + 1 \equiv 0 \pmod{5}.$$

12. Show that the polynomial

$$x^4 - 1 \equiv 0 \pmod{7}$$

has at most 4 solutions.

13. Let $p = 11$. Prove that

$$x^5 - 1 \equiv 0 \pmod{p}$$

has exactly 5 solutions.

14. Find all roots of

$$x^3 + 2x + 1 \equiv 0 \pmod{7}.$$

15. Verify Wilson's theorem for $p = 7$, i.e., show that

$$6! \equiv -1 \pmod{7}.$$

16. Solve the system

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

17. Solve the system

$$\begin{cases} x^2 \equiv 1 \pmod{8}, \\ x \equiv 3 \pmod{5}. \end{cases}$$

18. Let $m = 12 = 2^2 \cdot 3$. Find all solutions to

$$x^2 \equiv 4 \pmod{12}.$$

19. Prove that the number of solutions modulo

$$m = p_1^{e_1} p_2^{e_2}$$

equals the product of the number of solutions modulo each prime power.

20. Given

$$x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{9},$$

find $x \pmod{36}$.

21. Find the order of 2 modulo 7.

22. Show that if $\mathrm{ord}_p(a) = h$, then

$$a^k \equiv 1 \pmod{p}$$

if and only if $h \mid k$.

23. Compute the order of $3^4 \pmod{7}$ given that $\mathrm{ord}_7(3) = 6$.

24. Let $p = 11$. Find a primitive root modulo 11.

25. Prove that if $\gcd(h, k) = 1$, and $\mathrm{ord}_m(a) = h$, $\mathrm{ord}_m(b) = k$, then

$$\mathrm{ord}_m(ab) = hk.$$

26. Show that the number of primitive roots modulo a prime p is

$$\phi(p - 1).$$

27. Find all primitive roots modulo 13.

28. Given $p = 17$ and primitive root $g = 3$, find the discrete logarithm of 13 base 3 modulo 17.

29. Solve

$$x^4 \equiv 1 \pmod{13}$$

using the index calculus method.

30. For $p = 19$, $g = 2$ primitive root, find all solutions to

$$x^6 \equiv 8 \pmod{19}.$$

31. Explain why solving discrete logarithms modulo a large prime is computationally difficult.

32. Given

$$x \equiv g^k \pmod{p} \quad \text{and} \quad a \equiv g^\ell \pmod{p},$$

write the congruence

$$x^d \equiv a \pmod{p}$$

in terms of k, ℓ, and d.

33. Prove that the polynomial

$$f(x) = x^p - x$$

in $\mathbb{F}_p[x]$ factors into linear factors corresponding to all elements of $\mathbb{F}_p$.

34. Prove that

$$(p - 1)! \equiv -1 \pmod{p}$$

using polynomial factorization.

35. For $m = 35$, find the smallest positive integer N such that

$$a^N \equiv 1 \pmod{35}$$

for all a with $\gcd(a, 35) = 1$.

36. Show that a primitive root modulo p exists for every prime p.

37. Given

$$m = 2p^e,$$

where p is an odd prime and $e \geq 1$, prove that m admits a primitive root.

38. State and explain Artin's conjecture on primitive roots.

39. Show that if

$$f(x) \mid (x^p - x) \quad \text{in} \quad \mathbb{F}_p[x],$$

then

$$f(x) \equiv 0 \pmod{p}$$

has exactly $\deg f$ distinct solutions.

40. Let $p = 29$. Find a primitive root modulo 29 and compute its order.