1. Find all integer solutions (x, y) to the equation $9x + 23y = 2$.
2. Prove that if $b, n \in \mathbb{Z}$ have gcd of 1, then the row of the multiplication table for $\mathbb{Z}/n\mathbb{Z}$ corresponding to $b \pmod{n}$ must have n distinct entries.
3. Find all integer solutions to the following congruences.
   (a) $66x \equiv 100 \pmod{244}$
   (b) $66x \equiv 100 \pmod{246}$
4. Find the remainder when 5^{1491} is divided by 7.
5. Find the last two digits of 123^{562}.
6. Let p be a prime. State the definition of a *primitive root of* p, and the definition of the *order* of a unit modulo p. Using these definitions, prove that any primitive root must have order $p - 1$.
7. Let ϕ denote the Euler totient function, and let p and q be distinct primes.
   (a) What is $\phi(pq)$? Prove your answer.
   (b) What is $\phi(p^3)$? Prove your answer.
8. Suppose that $n = pq$ is the product of two distinct primes p and q. Show that if Eve knows both n and $\phi(n)$, then she can factor n.
9. Find all integer solutions x to $x^2 \equiv 4 \pmod{77}$.
10. Find all integer solutions to the equation $x^2 + 17x + 4 \equiv 0 \pmod{42}$.
11. Find all integers x such that:
$$x \equiv 2 \pmod{3}, \qquad x \equiv 3 \pmod{5}, \qquad x \equiv 4 \pmod{7}.$$
12. Noting that 2003 is prime, find all integers x such that
   (a) $x^2 \equiv 7 \pmod{2003}$.
   (b) $x^2 \equiv 3 \pmod{2003}$.
13. For each of the following: State the number of congruence classes x modulo n (for an appropriately chosen n) that are solutions to the equation. Justify your answer.
   (a) $x^{40} \equiv 1 \pmod{41}$
   (b) $5x + 3 \equiv 13 \pmod{55}$
   (c) $x \equiv 3 \pmod{17}$ and $x \equiv 5 \pmod{11}$
   (d) $x^2 \equiv 1 \pmod{35}$
   (e) $x^2 \equiv -1 \pmod{11}$
14. Suppose that $\beta \equiv \alpha^3 \pmod{23}$, and that β has a square root. Prove that α cannot be a primitive root of 23.
15. Let $L_\alpha(\beta)$ denote the discrete log of β with respect to the base α modulo some base p. Let $\mathrm{ord}_p(\alpha)$ denote the multiplicative order of α modulo p. Prove that
$$L_\alpha(\beta\gamma) \equiv L_\alpha(\beta) + L_\alpha(\gamma) \pmod{\mathrm{ord}_p(\alpha)}.$$
16. Explain what Fermat's Little Theorem tells us about whether $n = 91$ is prime,
   (a) using the base $b = 3$.
   (b) using the base $b = 2$.

17. A certain affine cipher is found to map the letter $b = [1]$ to $G = [6]$ and map $h = [7]$ to $K = [10]$ modulo 26. Find the functional equation for the affine cipher.

18. Evaluate the following Jacobi symbols.
    (a) $\left(\frac{2601}{7385}\right)$
    (b) $\left(\frac{1222}{45125}\right)$

19. (a) Does $x^2 = 1093$ have any solutions modulo the prime 65537?
    (b) Does $x^2 = 5$ have any solutions modulo $143 = (11)(13)$?

20. Show that for a prime $p > 3$ that the Legendre symbol $\left(\frac{3}{p}\right)$ is given by

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \text{ is 1 or 11 (mod 12)} \\ -1 & \text{if } p \text{ is 5 or 7 (mod 12).} \end{cases}$$

21. Explain how we can use Jacobi symbols for primality testing. Include a description of the Solovay–Strassen test, and explain why it is computationally more efficient than the brute force trial-division approach to primality testing.

22. Give examples of the following, or explain why they cannot exist.
    (a) Integers n and b so that b is a (nonzero) zero divisor in $\mathbb{Z}/n\mathbb{Z}$.
    (b) Integers n and b so that b does not have any square roots modulo n.
    (c) An integer b that has a square root modulo *any* integer n.
    (d) Two odd integers $n < m$ such that $\phi(n) = \phi(m) = 20$
    (e) An affine function (modulo 26) that does not have an inverse.
    (f) A prime number p such that 3 is a square modulo p, but p is not a square modulo 3.
    (g) A composite integer that "passes" the Fermat primality test.
    (h) A prime integer that "fails" the Fermat primality test.
    (i) A composite number that "passes" the Solovay-Strassen test.
    (j) A prime number that "fails" the Solovay-Strassen test.
    (k) A valid encryption / decryption pair of RSA exponents for the modulus $n = (19)(29)$.
    (l) A primitive root in $\mathbb{Z}/5\mathbb{Z}$.
    (m) A code with code rate $\frac{1}{4}$.
    (n) A (3,4,2) code.
    (o) A 5-ary code of length 4 and minimum distance 4.
    (p) A perfect code (ie, a code that realizes the Hamming bound).
    (q) A nonlinear binary code.
    (r) A 2-dimensional subspace of $(\mathbb{F}_2)^4$.
    (s) A degree-4 polynomial in $\mathbb{F}_3[x]$ that is not irreducible.
    (t) A polynomial with integer coefficients that is irreducible in $\mathbb{Z}[x]$ but reducible in $\mathbb{F}_2[x]$.
    (u) A polynomial with integer coefficients that is reducible in $\mathbb{Z}[x]$ but irreducible in $\mathbb{F}_2[x]$.
    (v) A field with 5^2 elements.
    (w) A field of characteristic 7.

(x) A field of characteristic 4.

(y) An elliptic curve over $\mathbb{F}_5$ that contains the point $(1, 0)$.

23. Let p be a positive prime, and $a \in \mathbb{Z}/p\mathbb{Z}$. Prove that a can have at most 2 square roots in $\mathbb{Z}/p\mathbb{Z}$.

24. Arjun and Barack are communicating using the RSA algorithm with modulus $n = 10573 = (97)(109)$. Arjun sends an encrypted message to Barack, which he decrypts with the exponent $d = 2117$ to discover the plaintext $m = 221 \pmod{10573}$. What was the encrypted message that Barack received?

25. Explain how to select a modulus $n = pq$ for use with RSA. Give at least three criteria for the choice of p and q, and explain which factorization method each criterion is intended to safeguard against.

26. The ciphertext 75 was obtained using the RSA algorithm with $n = 437$ and $e = 3$. You know that the plaintext is a positive integer less than 10. Determine which integer this is without factoring n.

27. Akiko and Beth want to establish a shared secret key using the Diffie-Hellman algorithm, using the prime $p = 83$ and primitive root $\alpha = 2$. Akiko chooses the secret exponent 5, and Beth chooses 4. What key do they establish?

28. To run the Diffie–Hellman key exchange modulo the prime p, why is $p - 1$ a poor choice of secret exponent?

29. Suppose that Aditya wishes to send a secret message to Blair, but Evelyn is able to intercept their transmissions and suspects (correctly) that Aditya's message is one of four particular messages. Explain how this would enable Evelyn to discover the message if Aditya and Blair use RSA, but why it would remain computationally difficult for Evelyn if they use the ElGamal system.

30. Prove that in any Diffie-Hellman key exchange (modulo a prime p), an eavesdropper can determine whether the shared secret has a square root mod p.

31. Aubrey is sending encrypted messages to Bai using the ElGamal system with prime $p = 151$ and primitive root $\alpha = 6$.

    (a) On their first exchange, Aubrey receives the number $38 \pmod{151}$. She chooses the secret exponent $k = 3$. What information should she send back to Bai?

    (b) On their second exchange, Bai sends $\beta \equiv 2^{140} \equiv 32 \pmod{151}$. Aubrey returns the numbers $\alpha^k \equiv 105 \pmod{151}$ and $\beta^k m \equiv 22 \pmod{151}$. What is her message m?

32. Explain why knowing four distinct square roots of a congruence class $a \pmod{n}$ enables us to find a nontrivial factor of n.

33. Use the Miller–Rabin test to investigate whether $n = 337$ is prime. What can you conclude?

34. An integer n is called a *strong pseudoprime* to the base b if it passes the Miller-Rabin test to base b.

    (a) Show that 65 is a strong pesudoprime to base 8 and base 18 but not to base 14 (which is the product of 8 and 18 modulo 65).

    (b) **(Challenge)** Let n be an odd composite integer which is either a prime power or divisible by an integer which is congruent to 3 modulo 4. Suppose that n is a strong pseudoprime to the bases b_1 and b_2. Prove that n is a strong pseudoprime to the base $b_1 b_2$.

35. The integer $n = 416021$ is the product of two primes. Use Fermat factorization to factor n.

36. Use the $(p - 1)$ algorithm with bound $B = 6$ to factor $n = 361$.

37. Factor $n = 899$ given that you know that $a^{840} \equiv 1 \pmod{n}$ for any unit a modulo n.

38. The integer $n = 12707$ is the product of two primes. Use the following information to factor n:

$$437^2 \equiv (2^2)(7)(13) \pmod{12707}$$
$$813^2 \equiv (5)(41) \pmod{12707}$$
$$1193^2 \equiv (5)(13) \pmod{12707}$$
$$4911^2 \equiv (5)(7) \pmod{12707}$$

39. **(Challenge)** Explain why we should not run the Pollard rho algorithm using a function of the form $f(x) = ax + b$ for some $a, b \in \mathbb{Z}$.

40. Use Pollard's rho algorithm to factor $n = 1757$ with the function $f(x) = x^2 + 2$.

41. Describe the Pohlig-Hellman algorithm.

42. Use the Baby Step, Giant Step method to solve $11^x \equiv 13 \pmod{31}$.

43. The class 3 is a primitive root of the prime 89. Consider the following:

$$3^9 \equiv 14 \pmod{89}$$
$$3^{14} \equiv 20 \pmod{89}$$
$$3^{17} \equiv 6 \pmod{89}$$
$$3^{28} \equiv 44 \pmod{89}$$

Compute $L_3(2), L_3(3), L_3(5), L_3(7), L_3(11)$, and use the Index Calculus to compute $L_3(13)$.

44. Define the *Hamming distance* on the set of q-ary length n words, and explain why it satisfies the triangle inequality.

45. Let C be the code
$$\{(a, b, c, d) \in (\mathbb{Z}/7\mathbb{Z})^4 \mid a + 3b + 2c + 5d \equiv 0 \pmod{7}\}.$$
Determine q, determine whether the code is linear, determine n, M, d, and compute the code rate of C.

46. What is the largest possible number of words in a code with length 6 and minimum distance 3?

47. Let C be the linear ternary code
$$\{(a, b, c) \in (\mathbb{Z}/3\mathbb{Z})^3 \mid a + b + c \equiv 0 \pmod{3}\}.$$
Compute a generator matrix for C, and determine n, M, d and the code rate.

48. A certain ternary linear code has generator matrix
$$G = \begin{pmatrix} 1 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 \end{pmatrix}$$
A codeword is transmitted over a noisy channel, and the recipient receives the word 12011. Determine whether this is a codeword, and, if not, determine its nearest neighbour codeword.

49. Define the weight function $wt(u)$ on $\mathbb{F}_p^n$ and prove that it satisfies the triangle inequality:
$$wt(u + v) \leq wt(u) + wt(v).$$

50. (a) Let $\mathbb{F}$ be a field of q elements, and consider $\mathbb{F}^n$ as a vector space over $\mathbb{F}$. Let V be a k-dimensional subspace of n. Compute the number of vectors in V. In particular, show that this number does not depend on n.

    (b) Suppose that G is a $k \times n$ generator matrix over the field $\mathbb{F}$ of q elements. Determine the rank of G, and the dimension of the row span of G, and explain your answer. How many vectors are there in the row span of G?

    (c) Suppose that H is a parity check matrix for the code generated by G. What is the relationship between H and G? What is the relationship between the row span of G and the kernel of the linear map $v \mapsto vH^T$?

51. For this question, refer to your Field Axioms handout. Let $\mathbb{F}$ be field, and a any element of $\mathbb{F}$. Let $-a$ denote the additive inverse of a, and -1 the additive inverse of the multiplicative identity element 1. Let $\dfrac{1}{b}$ denote the multiplicative inverse of b for any $b \in \mathbb{F}$. Using the field axioms and the definitions of additive and multiplicative inverse, prove the following.

    (a) $(-1) \cdot a = -a$

    (b) $-\left(\dfrac{1}{a}\right) = \dfrac{1}{-a}$.

52. Let $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, and let $P(x)$ be the irreducible polynomial $P(x) = x^3 + x + 1 \in \mathbb{F}_5[x]$. Compute an inverse of $(x + 1)$ modulo $P(x)$.

53. Let E be an elliptic curve over a field $\mathbb{F}$, and P be a point on E with (additive) order k. For any $m \in \mathbb{Z}$, show that

$$mP = \infty \qquad \text{if and only if} \qquad m \equiv 0 \pmod{k}.$$

    (Compare to Problem 20 in Trappe–Washington Chapter 3.)

54. Show that if $P = (x, 0)$ is a point on an elliptic curve E, then P is a point of order 2.

55. Count the number of points on the elliptic curve $y^2 = x^3 + x + 3$ over $\mathbb{Z}/5\mathbb{Z}$.

56. Factor $n = 35$ using the elliptic curve $y^2 = x^3 + 5x + 8$ and the point $(1, 28)$.