CHAPTER 0

Preliminaries

1. $\{1, 2, 3, 4\}$; $\{1, 3, 5, 7\}$; $\{1, 5, 7, 11\}$; $\{1, 3, 7, 9, 11, 13, 17, 19\}$; $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

2. **a.** 2; 10 **b.** 4; 40 **c.** 4: 120; **d.** 1; 1050 **e.** $pq^2; p^2q^3$

3. 12, 2, 2, 10, 1, 0, 4, 5.

4. $s = -3$, $t = 2$; $s = 8$, $t = -5$

5. By using 0 as an exponent if necessary, we may write $a = p_1^{m_1} \cdots p_k^{m_k}$ and $b = p_1^{n_1} \cdots p_k^{n_k}$, where the p's are distinct primes and the m's and n's are nonnegative. Then $\mathrm{lcm}(a, b) = p_1^{s_1} \cdots p_k^{s_k}$, where $s_i = \max(m_i, n_i)$ and $\gcd(a, b) = p_1^{t_1} \cdots p_k^{t_k}$, where $t_i = \min(m_i, n_i)$ Then $\mathrm{lcm}(a, b) \cdot \gcd(a, b) = p_1^{m_1+n_1} \cdots p_k^{m_k+n_k} = ab$.

6. The first part follows from the Fundamental Theorem of Arithmetic; for the second part, take $a = 4$, $b = 6$, $c = 12$.

7. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where $0 \leq r_1, r_2 < n$. We may assume that $r_1 \geq r_2$. Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$, where $r_1 - r_2 \geq 0$. If a mod $n = b$ mod n, then $r_1 = r_2$ and n divides $a - b$. If n divides $a - b$, then by the uniqueness of the remainder, we then have $r_1 - r_2 = 0$. Thus, $r_1 = r_2$ and therefore a mod $n = b$ mod n.

8. Write $as + bt = d$. Then $a's + b't = (a/d)s + (b/d)t = 1$.

9. By Exercise 7, to prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$ it suffices to show that n divides $(a + b) - (a' + b')$ and $ab - a'b'$. Since n divides both $a - a'$ and n divides $b - b'$, it divides their difference. Because $a = a' \bmod n$ and $b = b' \bmod n$ there are integers s and t such that $a = a' + ns$ and $b = b' + nt$. Thus $ab = (a' + ns)(b' + nt) = a'b' + nsb' + a'nt + nsnt$. Thus, $ab - a'b'$ is divisible by n.

10. Write $d = au + bv$. Since t divides both a and b, it divides d. Write $s = mq + r$ where $0 \leq r < m$. Then $r = s - mq$ is a common multiple of both a and b so $r = 0$.

11. Suppose that there is an integer n such that $ab \bmod n = 1$. Then there is an integer q such that $ab - nq = 1$. Since d divides both a and n, d also divides 1. So, $d = 1$. On the other hand, if $d = 1$, then by the corollary of Theorem 0.2, there are integers s and t such that $as + nt = 1$. Thus, modulo n, $as = 1$.

12. $7(5n+3) - 5(7n+4) = 1$

13. By the GCD Theorem there are integers s and t such that $ms + nt = 1$. Then $m(sr) + n(tr) = r$.

14. It suffices to show that $(p^2 + q^2 + r^2) \bmod 3 = 0$. Notice that for any integer a not divisible by 3, $a \bmod 3$ is 1 or 2 and therefore $a^2 \bmod 3 = 1$. So, $(p^2 + q^2 + r^2) \bmod 3 = p^2 \bmod 3 + q^2 \bmod 3 + r^2 \bmod 3 = 3 \bmod 3 = 0$.

15. Let p be a prime greater than 3. By the Division Algorithm, we can write p in the form $6n + r$, where r satisfies $0 \leq r < 6$. Now observe that $6n, 6n+2, 6n+3$, and $6n+4$ are not prime.

16. By properties of modular arithmetic we have $(7^{1000}) \bmod 6 = (7 \bmod 6)^{1000} = 1^{1000} = 1$. Similarly, $(6^{1001}) \bmod 7 = (6 \bmod 7)^{1001} = -1^{1001} \bmod 7 = -1 = 6 \bmod 7$.

17. Since st divides $a - b$, both s and t divide $a - b$. The converse is true when $\gcd(s, t) = 1$.

18. Observe that $8^{402} \bmod 5 = 3^{402} \bmod 5$ and $3^4 \bmod 5 = 1$. Thus, $8^{402} \bmod 5 = (3^4)^{100} 3^2 \bmod 5 = 4$.

19. If $\gcd(a, bc) = 1$, then there is no prime that divides both a and bc. By Euclid's Lemma and unique factorization, this means that there is no prime that divides both a and b or both a and c. Conversely, if no prime divides both a and b or both a and c, then by Euclid's Lemma, no prime divides both a and bc.

20. If one of the primes did divide $k = p_1 p_2 \cdots p_n + 1$, it would also divide 1.

21. Suppose that there are only a finite number of primes $p_1, p_2, \ldots, p_n$. Then, by Exercise 20, $p_1 p_2 \ldots p_n + 1$ is not divisible by any prime. This means that $p_1 p_2 \ldots p_n + 1$, which is larger than any of $p_1, p_2, \ldots, p_n$, is itself prime. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ is the list of all primes.

22. $\frac{-7}{58} + \frac{3}{58} i$

23. $\frac{-5+2i}{4-5i} = \frac{-5+2i}{4-5i} \frac{4+5i}{4+5i} = \frac{-30}{41} + \frac{-17}{41} i$

24. Let $z_1 = a + bi$ and $z_2 = c + di$. Then $z_1 z_2 = (ac - bd) + (ad + bc)$; $|z_1| = \sqrt{a^2 + b^2}, |z_2| = \sqrt{c^2 + d^2}, |z_1 z_2| = \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} = |z_1||z_2|$.

25. x NAND y is 1 if and only if both inputs are 0; x XNOR y is 1 if and only if both inputs are the same.

26. If $x = 1$, the output is y, else it is z.

27. Let S be a set with $n+1$ elements and pick some a in S. By induction, S has 2^n subsets that do not contain a. But there is one-to-one correspondence between the subsets of S that do not contain a and those that do. So, there are $2 \cdot 2^n = 2^{n+1}$ subsets in all.

28. Use induction and note that $2^{n+1}3^{2n+2} - 1 = 18(2^n 3^{2n}) - 1 = 18(2^n 3^{3n} - 1) + 17$.

29. Consider $n = 200! + 2$. Then 2 divides n, 3 divides $n+1$, 4 divides $n+2, \ldots$, and 202 divides $n+200$.

30. Use induction on n.

31. Say $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where the p's and the q's are primes. By the Generalized Euclid's Lemma, p_1 divides some q_i, say q_1 (we may relabel the q's if necessary). Then $p_1 = q_1$ and $p_2 \cdots p_r = q_2 \cdots q_s$. Repeating this argument at each step we obtain $p_2 = q_2, \cdots, p_r = q_r$ and $r = s$.

32. 47. Mimic Example 12.

33. Suppose that S is a set that contains a and whenever $n \geq a$ belongs to S, then $n+1 \in S$. We must prove that S contains all integers greater than or equal to a. Let T be the set of all integers greater than a that are not in S and suppose that T is not empty. Let b be the smallest integer in T (if T has no negative integers, b exists because of the Well Ordering Principle; if T has negative integers, it can have only a finite number of them so that there is a smallest one). Then $b-1 \in S$, and therefore $b = (b-1)+1 \in S$. This contradicts our assumption that b is not in S.

34. By the Second Principle of Mathematical Induction, $f_n = f_{n-1} + f_{n-2} < 2^{n-1} + 2^{n-2} = 2^{n-2}(2+1) < 2^n$.

35. For $n = 1$, observe that $1^3 + 2^3 + 3^3 = 36$. Assume that $n^3 + (n+1)^3 + (n+2)^3 = 9m$ for some integer m. We must prove that $(n+1)^3 + (n+2)^3 + (n+3)^3$ is a multiple of 9. Using the induction hypothesis we have that $(n+1)^3 + (n+2)^3 + (n+3)^3 = 9m - n^3 + (n+3)^3 = 9m - n^3 + n^3 + 3 \cdot n^2 \cdot 3 + 3 \cdot n \cdot 9 + 3^3 = 9m + 9n^2 + 27n + 27 = 9(m + n^2 + 3n + 3)$.

36. You must verify the cases $n = 1$ and $n = 2$. This situation arises in cases where the arguments that the statement is true for n implies that it is true for $n+2$ is different when n is even and when n is odd.

37. The statement is true for any divisor of $8^3 - 4 = 508$.

38. One need only verify the equation for $n = 0, 1, 2, 3, 4, 5$. Alternatively, observe that $n^3 - n = n(n-1)(n+1)$.

39. Since 3736 mod 24 = 16, it would be 6 p.m.

40. 5

41. Observe that the number with the decimal representation $a_9a_8\ldots a_1a_0$ is $a_9 10^9 + a_8 10^8 + \cdots + a_1 10 + a_0$. From Exercise 9 and the fact that $a_i 10^i \bmod 9 = a_i \bmod 9$ we deduce that the check digit is $(a_9 + a_8 + \cdots + a_1 + a_0) \bmod 9$. So, substituting 0 for 9 or vice versa for any a_i does not change the value of $(a_9 + a_8 + \cdots + a_1 + a_0) \bmod 9$.

42. No

43. For the case in which the check digit is not involved, the argument given Exercise 41 applies to transposition errors. Denote the money order number by $a_9a_8\ldots a_1a_0c$ where c is the check digit. For a transposition involving the check digit $c = (a_9 + a_8 + \cdots + a_0) \bmod 9$ to go undetected, we must have $a_0 = (a_9 + a_8 + \cdots + a_1 + c) \bmod 9$. Substituting for c yields $2(a_9 + a_8 + \cdots + a_0) \bmod 9 = a_0$. Then cancelling the a_0, multiplying by sides by 5, and reducing module 9, we have $10(a_9 + a_8 + \cdots + a_1) = a_9 + a_8 + \cdots + a_1 = 0$. It follows that $c = a_9 + a_8 \cdots + a_1 + a_0 = a_0$. In this case the transposition does not yield an error.

44. 4

45. Say the number is $a_8a_7\ldots a_1a_0 = a_8 10^8 + a_7 10^7 + \cdots + a_1 10 + a_0$. Then the error is undetected if and only if $(a_i 10^i - a_i' 10^i) \bmod 7 = 0$. Multiplying both sides by 5^i and noting that $50 \bmod 7 = 1$, we obtain $(a_i - a_i') \bmod 7 = 0$.

46. All except those involving a and b with $|a - b| = 7$.

47. 4

48. Observe that for any integer k between 0 and 8, $k \div 9 = .kkk\ldots$.

50. 7

51. Say that the weight for a is i. Then an error is undetected if modulo 11, $ai + b(i-1) + c(i-2) = bi + c(i-1) + a(i-2)$. This reduces to the cases where $(2a - b - c) \bmod 11 = 0$.

52. Say the valid number is $a_1a_2\ldots a_{10}$ and a_i and a_{i+1} were transposed. Then, modulo 11, $10a_1 + 9a_2 + \cdots + a_{10} = 0$ and $10a_1 + \cdots + (11-i)a_{i+1} + (11-(i+1))a_i + \cdots + a_{10} = 5$. Thus, $5 = 5 - 0 = (10a_1 + \cdots + (11-i)a_{i+1} + (11-(i+1))a_i + a_{10}) - (10a_1 + 9a_2 + \cdots + a_{10})$. It follows that $(a_{i+1} - a_i) \bmod 11 = 5$. Now look for adjacent digits x and y in the invalid number so that $(x - y) \bmod 11 = 5$. Since the only pair is 39, the correct number is 0-669-09325-4.