Abstract Algebra Chapter 0

—— —— (-)

December 27, 2022

Important Statements:

Well Ordering Principle:

Every nonempty set of positive integers contains a smallest member

Division Algorithm:

Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

GCD is a Linear Combination:

For any nonzero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Corollary:

If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.

Euclid's Lemma:

If p is a prime that divides ab, then p divides a or p divides b.

Fundemental Theorem of Arithmetic:

Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1 p_2 ... p_r$ and $n = q_1 q_2 ... q_s$ where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.

First Principle of Mathematical Induction:

Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n+1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Second Principle of Mathematical Induction:

Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

Equivalence Relations:

1. $a \sim a \; \forall \; a \in S$ (Reflexive Property)
2. $a \sim b \Rightarrow b \sim a$ (Symmetric Property)
3. $a \sim b \wedge b \sim c \Rightarrow a \sim c$ (Transitive Property)

Equivalence Classes Partition:

The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

Properties of Functions:

For $\alpha : \mathrm{A} \rightarrow \mathrm{B}, \beta : \mathrm{B} \rightarrow \mathrm{C}$, and $\gamma : \mathrm{C} \rightarrow \mathrm{D}$

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$.
2. α, β are one-to-one $\Rightarrow \beta\alpha$ is one-to-one.
3. α, β are onto $\Rightarrow \beta\alpha$ is onto.
4. α is one-to-one and onto $\Rightarrow \exists \; \alpha^{-1} : \mathrm{B} \rightarrow \mathrm{A} \mid (\alpha^{-1}\alpha)(a) = a \; \forall \; a \in \mathrm{A}$ and $(\alpha\alpha^{-1})(b) = b \; \forall \; b \in \mathrm{B}$

End of Chapter Exercises

Question 1.

For $n = 5, 8, 12, 20$, and 25, find all positive integers less than n and relatively prime to n.

(a) $n = 5$, $\{1, 2, 3, 4\}$

(b) $n = 8$, $\{1, 3, 5, 7\}$

(c) $n = 12$, $\{1, 5, 7, 11\}$

(d) $n = 20$, $\{1, 3, 7, 9, 11, 13, 17, 19\}$

(e) $n = 25$, $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

Question 2.

Determine:

(a) $\gcd(2^4 \cdot 3^2 \cdot 7^2, 2 \cdot 3^3 \cdot 7 \cdot 11) = 2 \cdot 3^2 \cdot 7$

(b) $\text{lcm}(2^3 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7 \cdot 11) = 2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$

Question 3.

Determine:

(a) $51 \bmod 13 = 3 \cdot 13 + 12 \bmod 13 = 12$

(b) $342 \bmod 85 = 4 \cdot 85 + 2 \bmod 85 = 2$

(c) $62 \bmod 15 = 4 \cdot 15 + 2 \bmod 15 = 2$

(d) $10 \bmod 15 = 0 \cdot 15 + 10 \bmod 15 = 10$

(e) $82 \cdot 73 \bmod 7$

$$\begin{aligned} 82 \cdot 73 \bmod 7 &= (11 \cdot 7 + 5) \cdot (10 \cdot 7 + 3) \bmod 7 \\ &= 5 \cdot 3 \bmod 7 \\ &= 15 \bmod 7 \\ &= 1 \end{aligned}$$

(f) $51 + 68 \bmod 7$

$$\begin{aligned} 51 + 68 \bmod 7 &= (7 \cdot 7 + 2) + (9 \cdot 7 + 5) \bmod 7 \\ &= 2 + 5 \bmod 7 \\ &= 0 \end{aligned}$$

(g) $35 \cdot 24 \bmod 11$

$$\begin{aligned} 35 \cdot 24 \bmod 11 &= (3 \cdot 11 + 2) \cdot (2 \cdot 11 + 2) \bmod 11 \\ &= 3 \cdot 2 \bmod 11 \\ &= 12 \bmod 11 \\ &= 1 \end{aligned}$$

(h) $47 + 68 \bmod 11$

$$\begin{aligned} 47 + 68 \bmod 11 &= (4 \cdot 11 + 3) + (6 \cdot 11 + 2) \bmod 11 \\ &= 3 + 2 \bmod 11 \\ &= 5 \end{aligned}$$

Question 4.

Find integers s and t such that $1 = 7 \cdot s + 11 \cdot t$. Show that s and t are not unique.

We see that, $1 = 7 \cdot (-3) + 11 \cdot (2)$.

But also that, $1 = 7 \cdot (8) + 11 \cdot (-5)$.

We can conject:

$$1 = 7 \cdot (11n - 3) + 11 \cdot (-7n + 2), n \in \mathbb{Z}$$

Question 5.

In Florida, the fourth and fifth digits from the end of a driver's license number give the year of birth. The last three digits for a male with birth month m and a birth date b are represented by $40(m - 1) + b$. For females the digits are $40(m - 1) + b + 500$. Determine the dates of birth of people who have last five digits:

(a) 42218

$$218 = 40(6 - 1) + 18$$

(b) 53953

$$953 = 40(12 - 1) + 13 + 500$$

Question 6.

For driver's license number issued in New York prior to September of 1992, the three digits preceding the last two of the number of a male with birth month m and birth date b are represented by $63m + 2b$. For females the digits are $63m + 2b + 1$. Determine the dates of birth and sex(es) corresponding to the numbers:

(a) 248

$$248 = 63(3) + 2(29) + 1$$

(b) 601

$$601 = 63(9) + 2(17)$$

Question 7.

Show that if a and b are positive integers, then $ab = \text{lcm}(a, b) \cdot \gcd(a, b)$.

By Fundemental Theorem of Arithmetic,

$$a = {p_1}^{n_1}{p_2}^{n_2}...{p_k}^{n_k}$$

$$b = {p_1}^{m_1}{p_2}^{m_2}...{p_k}^{m_k}$$

We have,

$$\gcd(a, b) = {p_1}^{\alpha_1}{p_2}^{\alpha_2}...{p_k}^{\alpha_k}, \quad \alpha_i = \min(n_i, m_i)$$

And,

$$\text{lcm}(a, b) = {p_1}^{\beta_1}{p_2}^{\beta_2}...{p_k}^{\beta_k}, \quad \beta_i = \max(n_i, m_i)$$

So,

$$\begin{aligned} \gcd(a, b) \cdot \text{lcm}(a, b) &= \prod_{i=1}^{k} {p_i}^{\alpha_i} \cdot \prod_{i=1}^{k} {p_i}^{\beta_i} \\ &= \prod_{i=1}^{k} {p_i}^{\alpha_i} \cdot {p_i}^{\beta_i} \\ &= \prod_{i=1}^{k} {p_i}^{\alpha_i + \beta_i} \end{aligned}$$

Because we have $\alpha_i + \beta_i = m_i + n_i$

$$\gcd(a, b) \cdot \text{lcm}(a, b) = \prod_{i=1}^{k} {p_i}^{\alpha_i + \beta_i} = \prod_{i=1}^{k} {p_i}^{m_i + n_i} = ab$$

Question 8.

Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

Let $a|c$ and $b|c$, then there exists integers s and t such that $c = as$ and $c = bt$.

We also have integers f and g such that $1 = af + bg$

We can write,

$$\begin{aligned} c &= caf + cdg \\ &= (bt)af + (as)dg \\ &= ab(tf + sg) \end{aligned}$$

Thus, $ab|c$

Additionally, if $a = 3$, $b = 6$, $c = 12$ then $a|c$ and $b|c$, but $ab \nmid c$

Question 9.

If a and b are integers and n is a positive integer, prove that

$$a \bmod n = b \bmod n \iff n|(a-b)$$

Question 10.

Let a and b be integers and $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

Question 11.

Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$, i.e.

$$a \bmod n = a' \implies a = a' + sn,\ s \in \mathbb{Z}$$

$$b \bmod n = b' \implies b = b' + tn,\ t \in \mathbb{Z}$$

Prove that,

$$(a + b) \bmod n = (a' + b') \bmod n \tag{0.11a}$$

$$\begin{aligned}(a+b) \bmod n &= (a'+sn)+(b'+tn) \bmod n\\ &= (a'+b')+(s+t)n \bmod n\\ &= (a'+b') \bmod n\end{aligned}$$

$$(ab) \bmod n = (a'b') \bmod n \tag{0.11b}$$

$$\begin{aligned}(ab) \bmod n &= (a'+sn)\cdot(b'+tn) \bmod n\\ &= (a'b')+(a't+b's)n+(st)n^2 \bmod n\\ &= (a'b') \bmod n\end{aligned}$$

Question 12.

Let a and b be positive integers and let $d = \gcd(a,b)$ and $m = \operatorname{lcm}(a,b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

First, $a = \alpha t$ and $b = \beta t$ for some $\alpha, \beta \in \mathbb{Z}$.

Also, $d = \gcd(a,b) = ax + by$ for some $x, y, \in \mathbb{Z}$.

Thus,

$$\begin{aligned}d &= ax+by\\ &= (\alpha t)x + (\beta t)y\\ &= t(\alpha x + \beta y)\end{aligned}$$

So, t divides d. $\square$

Next, $s = a'a$ and $s = b'b$, for some multiples $a', b' \in \mathbb{Z}$

Question 13.

Let n and a be positive integers and let $d = \gcd(a,n)$. Show that

$$\exists\, x \mid ax \bmod n = 1 \iff d = 1 \tag{0.13}$$

Question 14.

Show that $5n+3$ and $7n+4$ are relatively prime for all n.

We demonstrate through induction:

$n = 1$:

$$5(1) + 3 = 8 \text{ and } 7(1) + 4 = 11$$

Obviously, for $n = 1$, $5n+3$ and $7n+4$ are relatively prime.

$n > 1$:

We assume the statement is true for n and demonstrate that the statement is also true for $n+1$.

$$5(n+1) + 3 = (5n+3) + 5$$
$$7(n+1) + 4 = (7n+4) + 7$$

Since $5n+3$ and $7n+4$ are relatively prime, we can write:

$$1 = s(5n+3) + t(7n+4)$$

Question 15.

Prove that every prime greater than 3 can be written in the form $6n+1$ or $6n+5$.

We can take the contrapositive of the statement as:

$$p \notin \{6n+1, 6n+5\}, n \in \mathbb{N} \Rightarrow p \notin Primes$$

It's easy to see that every natural number can be written as $6n+k$ with $n \in \mathbb{Z}$ and $k \in \{0,1,2,3,4,5\}$. If $k \in \{0,2,4\}$ then the resultant will be divisible by 2 and thus not prime. Similarly, if $k = \{0,3\}$ then the resultant is divisible by 3.

If, by assumption, we take p prime, then it must be that $k \in \{1,5\}$.

Question 16.

Determine

(a) $7^{1000} =$ mod 6

(b) $6^{1001} =$ mod 7

Question 17.

Let a, b, s, and t be integers. If $a \bmod st = b \bmod st$, show that $a \bmod s = b \bmod s$, and $a \bmod t = b \bmod t$. What conditions on s and t is needed to make the converse true?

Question 18.

Determine $8^{402} = 5$.

Question 19.

Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

Question 20.

Let $p_1, p_2, ..., p_n$ be primes. Show that $p_1 p_2 ... p_n + 1$ is divisible by none of these primes.

Question 21.

Prove that there are infinitely many primes. *(Hint: Use Question 20.)*

Question 22.

For every positive integer n, prove that $1 + 2 + ... + n = n(n + 1)/2$.

Question 23.

For every positive integer n, prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set)

Question 24.

For any positive integer n, prove that $2^n 3^{2n} - 1$ is always divisible by 17.

Question 25.

Prove that there is some positive integer n such that $n, n+1, n+2, ..., n+200$ are all composite.

Question 26.

(Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 ... a_n$, prove that p divides a_i for some i.

Question 27.

Use the Generalized Euclid's Lemma to establish the uniqueness portion of the Fundemental Theorem of Arithmetic.

Question 28.

What is the larget bet that cannot be made with chips worth \$7.00 and \$9.00? Verify that your answer is correct with both forms of induction.

Question 29.

Prove that the First Principle of Mathematical Induction is a consequence of the Well Ordering Principle.

Question 30.

The Fibonacci numbers are $1, 1, 2, 3, 5, 8, 13, 21, 34, ...$ In general, the Fibonacci numbers are defined by $f_1 = 1, f_2 = 1$, and for $n \geq 3, f_n = f_{n-1} + f_{n-2}$. Prove that the nth Fibonacci number of f_n satisfies $f_n < 2^n$.

Question 31.

In the cut "As" from *Songs in the Key of Life*, Stevie Wonder mentions the equation $8 \times 8 \times 8 \times 8 = 4$. Find all integers n for which this statement is true, modulo n.

Question 32.

Prove that for every integer $n, n^3 \bmod 6 = n \bmod 6$.

We use induction,

$n = 1$ is obvious as $1 = 1^3 \bmod 6$

$n > 1$:

We assume that $n^3 \bmod 6 = n \bmod 6$

$$\begin{aligned}(n+1)^3 \bmod 6 &= n^3 + 3n^2 + 3n + 1 \bmod 6\\ &= n + 3n^2 + 3n + 1 \bmod 6\\ &= (n+1) + 3n(n+1) \bmod 6\\ &= (n+1) \bmod 6\end{aligned}$$

Because, either $3n$ or $3(n+1)$ is a multiple of 6.

Question 33.

If it were 2:00A.M. now, what time would it be 3735 hours from now?

We say that 2:00A.M. is 2 mod 24 so the question reduces to

$$2 + 3735 \bmod 24$$

$$\begin{aligned}2 + 3735 \bmod 24 &= 3737 \bmod 24\\ &= 155(24) + 17 \bmod 24\\ &= 17 \bmod 24\end{aligned}$$

Thus the time would be 5:00P.M.

Question 34.

Determine the check digit for a money order with identification number 7234541780.

Question 35.

Suppose that in one of the noncheck positions of a money order number, the digit 0 is substituted for the digit 9 or vice versa. Prove that this error will not be detected by the check digit. Prove that all other errors involving a single position are detected.

Question 36.

Suppose that a money order identification number and check digit of 21720421168 is erroneously copied as 27750421168. Will the check digit detect the error?

Question 37.

A transposition error involving distinct adjacent digits is one of the form $...ab... \to ...ba...$ with $a \neq b$. Prove that the money order check digit scheme will not detect such errors unless the check digit itself is transposed.

Question 38.

Determine the check digit for the Avis rental car with identification number 540047.

Question 39.

Show that a substitution of a digit a_i' for the digit $a_i (a_i' \neq a_i)$ in a noncheck position of a UPS number is detected if and only if $|a_i - a_i'| \neq 7$.

Question 40.

Determine which transposition errors involving adjacent digits are detected by the UPS check digit.

Question 41.

Use the UPC scheme to determine the check digit for the number 07312400508

Question 42.

Explain why the check digit for a money order for the number N is the repeated decimal digit in the real number $N \div 9$.

Question 43.

The 10-digit International Standard Book Number (ISBN-10) $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ has the property

$(a_1, a_2, ..., a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \bmod 11 = 0$. The digit a_{10} is the check digit. When a_{10} is required to be 1- to make the dot product 0, the character X is used as the check digit. Verify the check digit for the ISBN-10 assigned to this book.

Question 44.

Suppose that an ISBN=10 has a smudged entry where the question mark appears in the number 0-716?-2841-9. Determine the missing digit.

Question 45.

Suppose three consectutive digits *abc* of an ISBN-10 are scrambled as *bca*. Which such errors will go undetected?

Question 46.

The ISBN-10 0-669-03925-4 is the result of a transposition of two adjacent digits not involving the first or last digit. Determine the correct ISBN-10.

Question 47.

Suppose the weighting vector for ISBN-10s was changed to (1,2,3,...,10). Explain how this would affect the check digit.

Question 48.

Use the two-check-digit error-correction method described in this chapter to append two check digits to the number 73445860.

Question 49.

Suppose that an eight-digit number has two check digits appended using the error-correction method described in this chapter and it is incorrectly transcribed as 4302511568. If exactly one digit is incorrect, determine the correct number.

Question 50.

The state of Utah appends a ninth digit a_9 to an eight-digit driver's license number $a_1a_2...a_8$ so that $(9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 +$

a_9) mod $10 = 0$. If you know that the license number 149105267 has exactly one digit incorrect, explain why the error cannot be in position 2,4,6, or 8.

Question 51.

Complete the proof of Theorem 0.7

Question 52.

Let S be the set of real numbers. If $a, b \in S$, define $a \sim b$ if $a-b$ is an integer. Show that $\sim$ is an equivalence relation on S. Describe the equivalence classes of S.

Question 53.

Let S be the set of integers. If $a, b \in S$, define aRb if $ab \geq 0$. Is R an equivalence relation on S?

Question 54.

Let S be the set of integers. If $a, b \in S$, define aRb is $a+b$ is even. Prove that R is an equivalence relation and determine the equivalence classes of S.

Question 55.

Complete the proof of Theorem 0.6 by showing that $\sim$ is an equivalence relation on S.

Question 56.

Prove that none of the integers 11, 111, 1111, 11111, ... is a square of an integer.

Question 57.

(Cancellation Property) Suppose $\alpha, \beta,$ and, γ are functions. If $\alpha\gamma = \beta\gamma$ and γ is one-to-one and onto, prove that $\alpha = \beta$.