Homework Assignment 2 U27565203 JaeHongLee

Problem 1.21, 1.34, 2.11, 2.12

Problem 1 (1.21)
Show that for all integer a, b we have (a) $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = |ab|$,
(b) $\gcd(a,b) = 1 \Rightarrow \mathrm{lcm}(a,b) = |ab|$.

(a) for all positive integers $a, b \in \mathbb{Z}$, let's say $\gcd(a,b) = d$. d is an arbitrary integer $d \in \mathbb{Z}$. Let's say $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ and $a_1, b_1 \in \mathbb{Z}$ a_1 and b_1 are relatively prime. so we can say $\mathrm{lcm}(a,b) = a_1 \times b_1 \times d$ so $\gcd(a,b) \times \mathrm{lcm}(a,b) = d \times a_1 \times b_1 \times d$ $= ab$. This works for all positive integer a, b.

When a, b are both 0, gcd of (a, b) are 0, and lcm(a, b) are also 0 so $|ab| = 0$ so this works. when a, b are all negative integer it is the same process with $a = a' \times -1$, $b = b' \times -1$ for positive integers a' and b'. multiple of of two negative integers. is positive integer, so $\gcd(a,b) \times \mathrm{lcm}(a,b) = ab = |ab|$.
When a and b have different sign (ex a is negative, b is positive integers), Let's say a is a negative, b is a positive integers. $\gcd(a,b) = d$ which d is a positive greatest common divisor of a and b. $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. $\mathrm{lcm}(a,b)$ is a non-negative so $\mathrm{lcm}(a,b) = a_1 \times b_1 \times d \times -1$. so $\gcd(a,b) \times \mathrm{lcm}(a,b)$ $= d \times a_1 \times b_1 \times d \times -1 = -ab$ which has the same value $|ab|$.

(b) for all integer $a, b \in \mathbb{Z}$ we have $\gcd(a,b) = 1$ and we need to show $\mathrm{lcm}(a,b) = |ab|$. When $\gcd(a,b) = 1$, a and b are relatively prime. a and b are relatively prime so a and b's least common multiple is $a \times b$.

When a, b ∈ all positive integers $\mathrm{lcm}(a,b) = ab$ so $|ab| = ab$. this is correct when a, b either one is zero then $\mathrm{lcm}(a,b) = 0$ so $|ab| = ab = 0$ this is correct. when a, b are all negative integers $\mathrm{lcm}(a,b) = ab$ which is positive $ab = |ab|$. when a, b either one is negative integers $\mathrm{lcm}(a,b) = ab$ which is a negative number However $|ab| = ab \times -1$ (when either one of a, b are negative) so this is also correct.

Problem 2. (1.34)
This exercise develops a characterization of least common multiples in terms of ideals.

a) Arguing directly from the definition of an ideal, show that if I and J are ideal of $\mathbb{Z}$, Then so is $I \cap J$.

$I, J \in I \Rightarrow I \cap J \in I$

we have I and J are ideals of $\mathbb{Z}$. we need to show $I \cap J$ are ideals of $\mathbb{Z}$

There are two sets I and J which are ideals of $\mathbb{Z}$, By the definition of ideal, "for all $z \in \mathbb{Z}$, there have to have $\alpha + \beta \in I$, $\alpha z \in$ Ideal set.

Let's say any arbitrary elements $\alpha, \beta \in I \cap J$ which means $\alpha \in I$, $\alpha \in J$, $\beta \in I$, $\beta \in J$. so $\alpha \in I, \beta \in I$ means $\alpha + \beta \in I$, $\alpha \in J, \beta \in J$ means $\alpha + \beta \in J$ so $\alpha + \beta \in I \cap J$, similarly for arbitrary integer $z \in \mathbb{Z}$, $\alpha z \in I$, $\alpha z \in J$, $\beta z \in I$, $\beta z \in J$ so $I \cap J$ are ideal of $\mathbb{Z}$

b) Let $a, b \in \mathbb{Z}$, and consider the ideal $I := a\mathbb{Z}$ and $J := b\mathbb{Z}$ by part (a), we know that $I \cap J$ is an ideal. By Theorem 1.6 we know that $I \cap J = m\mathbb{Z}$ for some uniquely determined non-negative integer m. show that $m = \operatorname{lcm}(a, b)$

Theorem 1.6 "Let I be an ideal of $\mathbb{Z}$. Then there exists a unique non-negative integer d such that $I = d\mathbb{Z}$"

we know $I := a\mathbb{Z}$ and $J := b\mathbb{Z}$ so we can say $I = a\mathbb{Z}$, $J = b\mathbb{Z}$ which mean I contains multiple of a; J contains multiple of b. we need to prove $I \cap J = m\mathbb{Z}$ which means $I \cap J$ are multiple of m and $m = \operatorname{lcm}(a, b)$.

we need to prove $I \cap J = m\mathbb{Z}$, $m \Rightarrow \operatorname{lcm}(a, b)$ and $\operatorname{lcm}(a, b) \Rightarrow m$ which $I \cap J = m\mathbb{Z}$

Let's say there is an element $x \in I \cap J$. so $x \in I$ and $x \in J$ which means $x \in a\mathbb{Z}$, $x \in b\mathbb{Z}$ so $x = as$, $x = bt$ for some integer $s, t \in \mathbb{Z}$. so $a|x$, $b|x$. this show m is a multiple of a, b. common multiple And also $x \in (I \cap J = m\mathbb{Z})$ $x \in m\mathbb{Z}$, so $x = m \cdot q$ for some integer $p \in \mathbb{Z}$. so $m|x$ so m divides all x which means m divides all common multiple of a and b which is a definition of Least common multiple.

Problem 3 (2.11)

Show that there are 14 distinct, possible, yearly (Gregorian) calendars, and that all 14 calendars actually occur

Before we show that there are 14 distinct possible, we need to know there is a leap year and average year. The average year is the normal 365 days (February is until 28th). The leap year is when there is a February 29 which makes a year 366 days. leap year occurs every 4 years.

Each week is 7 days so 365 days are ($365 = 7 \times 52 + 1$ which is 52 weeks and 1 day $365 \equiv 1 \pmod 7$ and 366 days are ($366 = 7 \times 52 + 2$) which is 52 weeks and 2 days $366 \equiv 2 \pmod 7$).

Each normal year starts from mon ~ sun are 7 cases and Each leap year starts from mon ~ sun are 7 cases. Normal years (365 days) $\equiv 1 \pmod 7$ so the start day starts for sure we need to show leap year start day change through mon ~ sun.

Since leap year is every 4 years, lets say 3 normal year and 1 leap year as a set. Let say the first leap year start day is monday. When 1 leap year and 3 normal years end, The summation of modules 7 is $2 \pmod 7 + 1 \pmod 7 + 1 \pmod 7 + 1 \pmod 7 = 5 \pmod 7$.

0 1 2 3 4 5 6
mo t w th F S S

So after 4 years, the start day of leap year is (mon + 5 days), Saturday. the next 4 years it will be $(5+5)-7=3$ $3 \pmod 7$) which is thursday next leap year the start day is $1 \pmod 7$.. follow by $6 \pmod 7$, $4 \pmod 7$, $2 \pmod 7$, $0 \pmod 7$ so. It will rotate one cycle $7 \times 4 = 28$ years.

problem 4. (2.12)
Let $a_1 \dots a_k, b, n$ be integers with $n > 0$, and let $d := \gcd(a_1, \dots a_k, n)$ Show that the congruence

$$a_1 z_1 + \cdots + a_k z_k \equiv b \pmod n$$

has a solution $z_1, \dots, z_k \in \mathbb{Z}$ if and only if $d \mid b$

From Theorem 2.5 " Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$ For every $b \in \mathbb{Z}$, the congruence $az \equiv b \pmod n$ has a solution $z \in \mathbb{Z}$ if and only if $d \mid b$

So from Theorem 2.5 we know $az \equiv b \pmod n$ has a solution z if and only if $d \mid b$.

1) we have $a_1 z_1 + \cdots a_k z_k \equiv b \pmod n$ for some $z_1, \dots, z_k \in \mathbb{Z}$.
so ↓
2) $a_1 z_1 + \cdots a_k z_k \equiv b + nxy$ for some $z_1, z_2 \dots, z_k, y \in \mathbb{Z}$ by definition of congruecence

3) so $a_1 z + \cdots + a_k z_k - ny = b$ for some $z_1, z_2, \dots z_k, y \in \mathbb{Z}$
↓
By definition of of gcd, $a_1 z_1 + \cdots + a_k z_k - ny$, $\gcd(a_1, \dots, a_k) = d$
so $d \mid b$.