Discrete Mathematics: Homework 5

Name ID: Number

2020.4.8

1. Let $a \in \mathbb{Z}, b \in \mathbb{Z}^+$ and $x \in \mathbb{R}$. Show that there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $x \leq r < x + b$.

证明. For $a - \lceil x \rceil = bq + r^{'}$, $q, r^{'}$ is unique and exists. $r^{'} \in [0, b)$. Because r is an integer, $r^{'} \in [0, b-1]$
$a = bq + r^{'} + \lceil x \rceil$, $q, r^{'}$ is unique and exists.$r^{'} \in [0, b-1]$.
Let $r = r^{'} + \lceil x \rceil$, $\lceil x \rceil \in [x, x+1)$
Because $r^{'}$ is unique and exists, $\lceil x \rceil$ is known, r is unique and exists.
$r \in [\lceil x \rceil, b + \lceil x \rceil - 1)$, we have $r \in [x, x+b)$ □

2. Let $a, b > 1$ be relatively prime integers. Show that if $a|n$ and $b|n$, then $ab|n$.

证明. Proof by contradiction:
let $S = \{x | x \in \mathbb{Z}, a|x \ and \ b|x\}$ and n is the smallest elements of S and n exists.
Suppose $n = k(ab) + r, r \in (0, ab)$, $a|n$ and $b|n$
By $a|n$, we have $\frac{n}{a} = kb + \frac{r}{a}, r = aq, q \in \mathbb{Z}^+$
By $b|n$, we have $\frac{n}{b} = ka + \frac{r}{b}, r = bp, p \in \mathbb{Z}^+$
So, $a|r$ and $b|r$.
By surmise, $r \in S$ and $r < ab < n$
So, n doesn't exists as the smallest elements in S.
So, $ab|n$.

□

3. Let $a, b_1, b_2, \dots, b_k \in \mathbb{Z}^+$. Show that $gcd(a, b_1 b_2 \dots b_k) = 1$ iff $gcd(a, b_i) = 1$ for every $i \in k$

证明. By undamental theorem of arithmetic , we have

$a = p_{0_1}^{e_{0_1}} p_{0_2}^{e_{0_2}} \dots p_{0_r}^{e_{0_r}}$

$b_1 = p_{1_1}^{e_{1_1}} p_{1_2}^{e_{1_2}} \dots p_{1_r}^{e_{1_r}}$

...

$b_k = p_{k_1}^{e_{k_1}} p_{k_2}^{e_{k_2}} \dots p_{k_r}^{e_{k_r}}$

where p_{k_i} are primes and $e_{k_i} \geq 1$

Prove **if**:

if $gcd(a, b_i) = 1$ for every $i \in k$

then $\forall m, n \in \mathbb{Z}^+$,$p_{i_m} \neq p_{0_n}$

and $b_1 b_2 \dots b_k = p_{1_1}^{e_{1_1}} p_{1_2}^{e_{1_2}} \dots p_{1_r}^{e_{1_r}} \dots p_{k_1}^{e_{k_1}} p_{k_2}^{e_{k_2}} \dots p_{k_r}^{e_{k_r}}$

doesn't have same divisor p with a except 1.

So $gcd(a, b_1 b_2 \dots b_k) = 1$.

Prove **only if**: if $gcd(a, b_1 b_2 \dots b_k) = 1$

$\forall m, n \in \mathbb{Z}^+, i \in \{k\}$, $p_{0_n} \neq p_{i_m}$

so b_i doesn't have same divisor p_{i_m} with a except 1.

$gcd(a, b_i) = 1$ for every $i \in k$

□

4. Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}^+$. Show that $\lfloor \frac{\lfloor x \rfloor}{n} \rfloor = \lfloor \frac{x}{n} \rfloor$

证明. $\forall x \in \mathbb{R}, \exists a \in \mathbb{Z}, \exists \epsilon \in [0, 1)$, such that $x = a + \epsilon, \lfloor x \rfloor = a$

By division algorithm, there exists unique $p \in \mathbb{Z}, r \in (0, n)$, such that $a = pn + r$

Because $a \in \mathbb{Z}$, so $r \in \mathbb{Z}$, we have $r \in (0, n-1]$

For the left side of the equation, $\lfloor \frac{\lfloor x \rfloor}{n} \rfloor = \lfloor \frac{a}{n} \rfloor = p$

For the right side of the equation, $\lfloor \frac{x}{n} \rfloor = \lfloor \frac{a+\epsilon}{n} \rfloor = \lfloor \frac{a}{n} + \frac{\epsilon}{n} \rfloor = \lfloor p + \frac{r}{n} + \frac{\epsilon}{n} = \lfloor p + \frac{r+\epsilon}{n} \rfloor$

Because $r \leq n-1, \epsilon < 1$, $r + \epsilon < n$, so $\lfloor p + \frac{r+\epsilon}{n} \rfloor = p$

Left side = Right side

□

5. Let $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$ and $a \equiv b \ (mod\ n)$. Let $c_0, c_1, \dots, c_k \in \mathbb{Z}$, where $k \in \mathbb{Z}^+$. Show that $c_0 + c_1 a + \cdots + c_k a^k \equiv c_0 + c_1 b + \cdots + c_k b^k \ (mod\ n)$.

证明. By division algorithm, $a = q_a n + r_a$ and $b = q_b n + r_b$ $r_a, r_b \in \mathbb{Z}, r_a \in [0, n), r_b \in [0, n)$

Because $a \equiv b \ (mod\ n)$, we have $r_a = r_b$

$a^i = (q_a n + r_a)^i = f(q_a, r_a)n + r_a^i \equiv r_a^i \ (mod\ n)$

$b^i = (q_b n + r_b)^i = f(q_b, r_b)n + r_b^i \equiv r_b^i \ (mod\ n)$

where $f(x, y) =$

$$\sum_{j=0}^{j<i} C_i^j x^{i-j} y^j$$

Because $r_a^i \equiv r_b^i (mod\ n)$, so we have $a_i \equiv b_i \ (mod\ n)$

which equals to,

$$c_0 + c_1 a + \cdots + c_k a^k \equiv c_0 + c_1 b + \cdots + c_k b^k \ (mod\ n)$$

□

6. Let p be a prime and $p \notin \{2, 5\}$. Show that p divides infinitely many elements of the set $\{9, 99, 999, 9999, 99999, \dots\}$.

证明. $[10]_p = 10 + np$ and $p \notin \{2, 5\}$, we have $gcd([10]_p, p) = 1$

By Fermat's little theorem, we have ${[10]_p}^{p-1} \equiv 1 \ (mod\ p)$

which is $p | ({[10]_p}^{p-1} - 1) \Rightarrow p | ((10 + np)^{p-1} - 1)$.

$\Rightarrow p | (10^{p-1} + \sum_{i=0}^{i<p-1} C_{p-1}^i 10^i (np)^{p-1-i} - 1)$

$\Rightarrow p | (10^{p-1} - 1)$ □