HW2 Recitation

SI120, Spring 2022; TA: 陈昱聪

Q1

1. (20 points) Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}^+$. Show that $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \lfloor \frac{x}{n} \rfloor$.

   (Hint: division algorithm)

- By using Division Algorithm

Proof:

From **Division Algorithm**,

$\lfloor x \rfloor = qn + r$, where $q, r \in \mathbb{Z}$ and $0 \leqslant r < n$. Further, it is $0 \leqslant r \leqslant n-1$ since r is an integer.

$\frac{\lfloor x \rfloor}{n} = q + \frac{r}{n}$, where $0 \leqslant \frac{r}{n} < 1$, so we have: $\lfloor \frac{\lfloor x \rfloor}{n} \rfloor = \lfloor q + \frac{r}{n} \rfloor = q$.

Since $x = \lfloor x \rfloor + o$, where $o \in (0 , 1)$, so that $0 + o \leqslant r + o \leqslant n - 1 + o$, which is $0 \leqslant r + o < n$, that is $0 \leqslant \frac{r+o}{n} < 1$.

So that $\lfloor \frac{x}{n} \rfloor = \lfloor \frac{\lfloor x \rfloor + o}{n} \rfloor = \lfloor \frac{qn+r+o}{n} \rfloor = \lfloor q + \frac{r+o}{n} \rfloor = q$

Now we have $\lfloor \frac{\lfloor x \rfloor}{n} \rfloor = \lfloor \frac{x}{n} \rfloor = q$.

$\square$

Q1

1. (20 points) Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}^+$. Show that $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$.

   (Hint: division algorithm)

- By using Inequalities

$$\left\lfloor \frac{x}{n} \right\rfloor < \frac{x}{n}$$

$$n\left\lfloor \frac{x}{n} \right\rfloor < x = \lfloor x \rfloor + \{x\}$$

$$n\left\lfloor \frac{x}{n} \right\rfloor \leqslant \lfloor x \rfloor \quad (\text{both side} \in \mathbb{Z})$$

$$\left\lfloor \frac{x}{n} \right\rfloor \leqslant \frac{\lfloor x \rfloor}{n}$$

$$\left\lfloor \frac{x}{n} \right\rfloor \leqslant \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$$

$$\lfloor x \rfloor \leqslant x$$

$$\frac{\lfloor x \rfloor}{n} \leqslant \frac{x}{n}$$

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor \leqslant \left\lfloor \frac{x}{n} \right\rfloor$$

$$\Longrightarrow \quad \Downarrow$$

$$\underline{\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor}$$

Q2

2. (20 points) Let $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$ and $a \equiv b \pmod{n}$. Let $c_0, c_1, \ldots, c_k \in \mathbb{Z}$, where $k \in \mathbb{Z}^+$. Show that $c_0 + c_1 a + \cdots + c_k a^k \equiv c_0 + c_1 b + \cdots + c_k b^k \pmod{n}$.

(Hint: show that $a^i - b^i$ is a multiple of n)

Proof:

$a \equiv b \ (\mathrm{mod}\ n) \Rightarrow n|(a-b) \Rightarrow a-b = qn \Rightarrow a = qn + b$, where $q \in \mathbb{Z}$.

$a^i - b^i = (qn+b)^i - b^i = \sum_{r=0}^{i} C_i^r (qn)^r b^{i-r} - b^i$

Since $C_i^0 (qn)^0 b^i = b^i$, so we have $a^i - b^i = \sum_{r=1}^{i} C_i^r (qn)^r b^{i-r}$.

Then $\frac{a^i - b^i}{n} = \frac{\sum_{r=1}^{i} C_i^r (qn)^r b^{i-r}}{n} = \sum_{r=1}^{i} C_i^r q^r n^{r-1} b^{i-r}$ which is an integer.

Then we have $n|(a^i - b^i)$. Further, $n|c_i(a^i - b^i)$ for any $c_i \in \mathbb{Z}$.

So that $n|(c_0(a^0 - b^0) + c_1(a-b) + c_2(a-b)^2 + \ldots c^k(a-b)^k)$, that is:

$$n|((c_0 + c_1 a + \ldots + c_k a^k) - (c_0 + c_1 b + \ldots + c_k b^k))$$

Which is:

$$c_0 + c_1 a + \ldots + c_k a^k \equiv c_0 + c_1 b + \ldots + c_k b^k \ (\mathrm{mod}\ n)$$

$\square$

Q3

3. (20 points) Let x, y, z be integers such that $x^2 + y^2 = 3z^2$. Show that x, y, z must be all even. Based on this result, show that the equation $x^2 + y^2 = 3z^2$ has no other integer solutions except $(x, y, z) = (0, 0, 0)$.

(1)

Suppose $x = 2m_1 + n_1, y = 2m_2 + n_2, z = 2m_3 + n_3$, where $m_1, m_2, m_3 \in \mathbb{Z},\ n_1, n_2, n_3 \in \{0, 1\}$.

$$[x^2]_p + [y^2]_p = [3z^2]_p$$

$$[4m_1^2 + 4m_1n_1 + n_1^2]_p + [4m_2^2 + 4m_2n_2 + n_2^2]_p = [12m_3^2 + 12m_3n_3 + 3n_3^2]$$

$$[n_1^2 + n_2^2]_p = [3n^3]_p$$

Since $[n_1^2 + n_2^2]_p \in \{[0]_p, [1]_p, [2]_P\}$ while $[3n_3^2]_p \in \{[0]_p, [3]_p\}$, so that we have $[n_1^2 + n_2^2]_p = [3n_3^2]_p = [0]_p$ which means $n_1 = n_2 = n_3 = 0$. So we have x, y, z are all even.

Q3

3. (20 points) Let x, y, z be integers such that $x^2 + y^2 = 3z^2$. Show that x, y, z must be all even. Based on this result, show that the equation $x^2 + y^2 = 3z^2$ has no other integer solutions except $(x, y, z) = (0, 0, 0)$.

(2)

If $x^2 + y^2 \equiv 3z^2$, then $x^2 + y^2 \equiv 3z^2 \pmod 4$, so that x, y, z are all even. Then let $x = 2i, y = 2j, z = 2k$, where $i, j, k \in \mathbb{Z}$.

Assume that there is a set of non-0 integer z such that $x^2 + y^2 \equiv 3z^2$. Then absolutely, among these non-0 z, there is a smallest z^2 called z_0^2.

$$x^2 + y^2 \equiv 3z_0^2 \Rightarrow 4i^2 + 4j^2 = 3 \cdot 4k^2 \Rightarrow i^2 + j^2 = 3k^2$$

It is clear that $x_1 = i, y_1 = j, z_1 = k$ is set of solutions to this equation. However, $z_1^2 < z_0^2$ where both of them are positive. So z_0^2 is not the smallest. **Contradiction!**

So there isn't any non-0 z to the solution. Since we only have $x = y = 0$ for $x^2 + y^2 \equiv 0$, so there is only one solution, i.e. $x = y = z = 0$.

☐

Q4

4. (20 points) Let p be an odd prime and let $\mathbb{Z}_p^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$.

(1) Show that $([a]_p)^2 = [1]_p$ if and only if $[a]_p \in \{[1]_p, [p-1]_p\}$.

(2) Show that $[1]_p \cdot [2]_p \cdots [p-1]_p = [-1]_p$ and thus conclude that $(p-1)! \equiv -1 (\bmod\ p)$. (This is called **Wilson's Theorem**.)

(Hint: partition the elements of $\mathbb{Z}_p^*$ as $(p+1)/2$ subsets of the form $\{\alpha, \alpha^{-1}\}$)

Solution

4.1

$\Leftarrow$: $1^2 \equiv 1 \pmod p$, $(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod p$

$\Rightarrow$: $p|(a^2-1) = (a+1)(a-1)$, $\because$ p prime $\therefore p|a+1$ or $p|a-1$ $\therefore a = 1$ or $p-1$

4.2

First we prove the uniqueness of inverse.

Assume $\forall a \in \mathbb{Z}_p^*$, $\exists\ m \neq n$ s.t. $am \equiv an \equiv 1 \pmod p$. Then $amn \equiv m \equiv n \pmod p$, so $m = n$, contradiction.

Next we prove $(p-1)! \equiv -1 \pmod p$.

By (1), we know for $a \in \mathbb{Z}_p^*$, if $a^{-1} = a$, $a = 1$ or $p-1$. Since a's inverse is unique, $\mathbb{Z}_p^* \backslash \{1, p-1\}$ can be partitioned as $\bigcup_{i=1}^{\frac{p-3}{2}} \{a_i, a_i^{-1}\}$ where a_i^{-1} is the inverse of a_i and $\forall i \neq j$, $a_i \neq a_j$.

So $(p-1)! \equiv 1 \cdot (p-1) \cdot \prod_{i=1}^{\frac{p-3}{2}} a_i a_i^{-1} \equiv p-1 \equiv -1 \pmod p$.

Q5

5. (20 points) Let p be a prime and $p \notin \{2,5\}$. Show that p divides infinitely many elements of the set $\{9, 99, 999, 9999, 99999, \ldots\}$.

(Hint: consider $([10]_p)^{p-1}$)

Proof:

Since $p \notin \{2,5\}$, $gcd(p,10) = 1$.

From **Fermat's Little Theorem**, we know:

$([10]_p)^p = [10]_p$, that is $([10]_p)^{p-1} = [1]_p$

Again, from **Fermat's Little Theorem**, we have:

$(([10]_p)^p)^p = ([10]_p)^p = [10]_p$

From induction, for any $n \in \mathbb{Z}^+$ we can say that:

$([10]_p)^{p^n} = ([10]_p)^p = [10]_p$,

that is $([10]_p)^{p^n-1} = [1]_p$,

also shown as $[10^{p^n-1}]_p = [1]_p$

In that case, it is clear that $p|(10^{p^n-1} - 1)$.

Let $A = \{a_1, a_2, a_3, \ldots a_n, \ldots\}$, where $a_1 = 10^{p-1} - 1, \ldots a_n = 10^{p^n-1} - 1, \ldots$

Then for every $n \in \mathbb{Z}^+$, $p|a_n$.

Since all 'a's in A could be written as several 9 (e.g. if $p = 7$, then $a_1 = 10^6 - 1 = 999999$), it is clear that $A \subset \{9, 99, 999, 9999, \ldots\}$

Since there are infinite n in $\mathbb{Z}^+$, A is an infinite set.

Now we know that for any prime number such that $p \notin \{2,5\}$, p divides infinitely many elements of the set $\{9, 99, 999, 9999, 99999, \ldots\}$.

□