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)

According to Division Algorithm
there are unique $q, r \in Z$ such that
$0 \le r < n$ and $x = qn + r$

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

$$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{qn+r}{n} \right\rfloor = \left\lfloor q + \frac{r}{n} \right\rfloor$$

since $0 \le r < n$ and $n \in Z^+$

then $\frac{r}{n} < 1$, so $\left\lfloor q + \frac{r}{n} \right\rfloor = q$

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

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)

Suppose that $a > b$

since $a \equiv b \pmod{n}$ then there exists $k \in Z$ such that $a-b = kn$ which means $a-b$ is a multiple of n.

since $a^i - b^i = (a-b)(a^{i-1} + a^{i-2}b + \cdots + ab^{i-2} + b^{i-1})$

then $a^i - b^i$ is also a multitipe of n.

So $(c_0 + c_1 a + \cdots + c_k a^k) - (c_0 + c_1 b + \cdots + c_k b^k)$

$= (c_0 - c_0) + c_1(a-b) + \cdots + c_k(a^k - b^k)$

$= c_1 r_1 n + c_2 r_2 n + \cdots + c_k r_k n$

$(r_1, r_2, \cdots, r_k \in Z)$

it is a multiple of n

So $c_0 + c_1 a + \cdots + c_k a^k \equiv c_0 + c_1 b + \cdots + c_k b^k \pmod{n}$

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) if z is even and x, y are odd

then $(x^2+y^2) \bmod 4 = 2$ while $3z^2 \bmod 4 = 0$, so it contradicts

so if z is even, x, y are also even

(2) if z is odd, then x is odd and y is even (*)

or y is odd and x is even.

take (*) as an example, $x^2 \bmod 3 = 1$ or 0, $y^2 \bmod 3 = 1$

so $(x^2+y^2) \bmod 3 = 1$ or 2 while $3z^2 \bmod 3 = 0$, it contradicts

Conclusion: x, y, z must be all even.

---

if there exists an integer solution such that $x, y, z \in \mathbb{Z}^+$

then there exists an integer solution (x', y', z') where

x', y', z' are relatively prime.

however, we know that x, y, z must be all even.

so they have common divisor 2

so the assumption is not true

Conclusion: the equation $x^2+y^2=3z^2$ has no other integer solutions except $(x,y,z)=(0,0,0)$

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 $\{\alpha, \alpha^{-1}\}$)

(1) $\Leftarrow$ It's obvious that $([a]_p)^2 = [1]_p$ holds when $[a]_p = [1]_p$

if $[a]_p = [p-1]_p$ since $[p-1]_p = \{p-1+px, x \in \mathbb{Z}\} = \{-1+pt, t \in \mathbb{Z}\} = [-1]_p$.

so $([a]_p)^2 = ([p-1]_p)^2 = ([-1]_p)^2 = [1]_p$.

$\Rightarrow$ since $([a]_p)^2 = [1]_p$ then $[a]_p = [1]_p$ or $[-1]_p$

$[-1]_p = \{-1+px, x \in \mathbb{Z}\} = \{p-1+pt, t \in \mathbb{Z}\} = [p-1]_p$

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

---

(2) It's obvious that the theorem holds if $p = 2$ and 3

if $p > 3$: since $p-1 \equiv -1 \pmod p$, $1 \equiv 1 \pmod p$

we just need to prove $2 \times 3 \times \cdots \times (p-2) \equiv 1 \pmod p$

for any a in $[2, p-2]$. since $\gcd(a, p) = 1$

$ax \equiv 1 \pmod p$ $x \in [1, p-1]$

if $x = 1$, then $a = 1$, since $a \in [2, p-2]$, $a \neq 1$

if $x = p-1$. then $a = p-1$, since $a \in [2, p-2)$. $a \neq p-1$

so $x \in [2, p-2]$

we can always find $a \cdot b \in [2, p-2]$ $a \neq b$ which meets $a \times b \equiv 1 \pmod p$ since the number of elements in $[2, p-2]$ is even. So $2 \times 3 \times \cdots \times (p-2) \equiv 1 \pmod p$

Conclusion. Wilson's Theorem holds.

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

Since p is a prime and $p \notin \{2,5\}$

then $p \nmid 10$

According to Fermat's Little Theorem.

p is a prime, $p \nmid 10$

So $10^{p-1} \equiv 1 \pmod{p}$

It means $p \mid 10^{p-1} - 1$

$\{10^{p-1} - 1\} = \{9, 99, 999, \cdots\}$

Conclusion: p divides infinitely many elements of the set $\{9, 99, 999, 9999, \cdots\}$