1. let $x = nq + r$ $|r| < |n|$ $\left|\frac{r}{n}\right| < 1$, $q \in \mathbb{Z}$

① $x \geq 0$ $\frac{x}{n} > 0$

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

$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{\lfloor nq + r \rfloor}{n} \right\rfloor = \lfloor q + \frac{\lfloor r \rfloor}{n} \rfloor$ $(0 < \lfloor r \rfloor < r)$

$0 < \frac{\lfloor r \rfloor}{n} < \frac{r}{n} < 1$

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

② $x < 0$. $\frac{x}{n} < 0$ $\frac{r}{n} < 0$ $0 > \frac{r}{n} > \frac{\lfloor r \rfloor}{n} \geq -1$

$\lfloor \frac{x}{n} \rfloor = \lfloor q + \frac{r}{n} \rfloor = q - 1$

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

$= q - 1$

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

$\Rightarrow$ In sum, $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \lfloor \frac{x}{n} \rfloor$

2.

① $b = 0$. $a \equiv b \pmod n \Rightarrow n \mid a$

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

$= c_1 a + \cdots c_k a^k$ $(*)$

$\xrightarrow{n \mid a} n \mid (*) \Rightarrow c_0 + c_1 a + \cdots + c_k a^k \equiv c_0 + c_1 b + \cdots c_k b^k \pmod n$

② $b \neq 0$. $a^i - b^i = b^i[(\frac{a}{b})^i - 1]_{i-1}$; $\Rightarrow$ from $a \equiv b \pmod n \Rightarrow n \mid (a-b)$

$= b^i \frac{(a-b)}{b} \cdot \sum_{j=0} (\frac{a}{b})^j$ $\Rightarrow$ $n \mid a^i - b^i$

$= \frac{(a-b)}{b} \sum_{i=0}^{n-1} a^i b^{n-i}$

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

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

and $n \mid (a^i - b^i)$

$\Rightarrow n \mid (**)$ $\Rightarrow$ In sum:

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

proof:

$a^n - 1 = (a-1)\sum_{i=0}^{n-1} a^i$

$= a\sum_{i=0}^{n-1} a^i - \sum_{i=0}^{n-1} a^i$

$= \sum_{i=1}^{n} a^i - \sum_{i=0}^{n-1} a^i$

Discrete Mathematics: Homework 2

(Deadline: 8:00am, March 4, 2022)

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)

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)

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 $(x, y, z) = (0, 0, 0)$.

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 $(p-1)! \equiv -1 (\text{mod } p)$. (This is called **Wilson's Theorem**.)

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

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

lemma: $a, b \in \mathbb{R}$. $m \in \mathbb{Z}$

$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$

proof: $a^0 = b^0 = 1$. $a \equiv b \pmod m$ are true

hypothesis: $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$

$\Rightarrow a^n a \equiv b^n b \pmod m$.

induction: $\Rightarrow a^{k+1} \equiv b^{k+1} \pmod m \Rightarrow$ proved.

3. proof:

Lemma: square of integer is congruent to 1 or 0 mod 3

① $x \in [0]_3 \Rightarrow x^2 \in [0^2] \bmod 3 = [0]_3$

② $x \in [1]_3 \Rightarrow x^2 \in [1^2] \bmod 3 = [1]_3$ ← (used)

③ $x \in [2]_3 \Rightarrow x^2 \in [2^2] \bmod 3 = [1]_3$

$(n \in \mathbb{Z}^+)$ by least integer therem, wlog we can choose a minimum z satisfies.

$x^2 + y^2 = 3z^2 \Rightarrow x^2 + y^2 \equiv 0 \pmod 3$ (principle)

$x^2 \equiv y^2 \equiv 0 \equiv x \equiv y \equiv 0 \pmod 3$

$x = 3a$ $y = 3b$

$\Rightarrow 9a^2 + 9b^2 = 3z^2$.

$3(a^2 + b^2) = z^2$

$3 \mid z^2 \Rightarrow 3 \mid z$

so let $z = 3c$

$\Rightarrow a^2 + b^2 = 3c^2 \Rightarrow c = \frac{z}{3} < z$

$\Rightarrow$ Contradict to 'z is minimum'

by this, only solution is $x = y = z = 0$, x, y, z are even

4.(1) if: if $[a]_p \in \{[1]_p, [p-1]_p\}$

$([1]_p)^2 = [1^2]_p = [1]_p$. correct.

$\Rightarrow [(p-1)_p]^2 = [p^2-2p+1]_p$, $[p^2]_p = [0]_p$, $[-2p]_p = 0_p$.

$\Rightarrow ([p-1]_p)^2 = [1]_p$.

only if:

since p is an odd prime. if $([a]_p)^2 = [1]_p$

$\underbrace{[1]_p}_{\cap \mathbb{R}^+} = \{1, p+1 \cdots\}$ $\qquad [a]_p = [\pm 1]_p$.

$\underbrace{[-1]_p}_{\cap \mathbb{R}^+} = \{p-1, 2p-1 \cdots\}$

since $\mathbb{Z}_p^* = \{[1]_p, [2]_p \cdots [p-1]_p$.

only $1, p-1 \leq p-1$

$\Rightarrow$ To sum up. if and only if.

(2). to prove: $(p-1)! \equiv -1 \pmod p$ $\quad$ p is prime

① when $p=2$ $\qquad [1]_2 = [-1]_2$ is trivial

② $p \neq 2$ $(p \geq 3)$

consider

$g(x) = (x-1)(x-2)\cdots(x-(p-1))$ $\qquad h(x) = x^{p-1}-1$

$m(x) = h(x) - g(x)$

$= x^{p-1} - 1 - (x-1)(x-2)\cdots(x-(p-1))$

substitute $x=a$ for $a \in \{1, 2, \cdots p-1\}$.

$f(a) = a^{p-1} - 1 \equiv 1 - 1 \equiv 0 \bmod p$

since p prime, by Fermat's little theorem.

degree of f less than $(p-1)$ $\quad x^{p-1}$ is coefficient $= 1-1 = 0$.

p-1 solutions for $f(a) \equiv 0 \bmod p$. in $\{1, 2 \ldots p-1\}$.

$\Rightarrow$ So all coefficient of f is divisible by p.

$\Rightarrow$ So $f(0) \equiv 0 \pmod p$

$\Rightarrow 0 \equiv -1 - \prod_{k=1}^{p-1}(-k) = -1 - (p-1)!$

(p is odd, $(-1)! = 1$).

$\Rightarrow (p-1)! \equiv -1 \bmod p$.

~~5. $9 \ldots 9 = 10^k - 1$ consider $p \notin \{2, 5\}$, since then $p \nmid 10$, $p \nmid (10+pn)$~~

~~let $l = m(p-1)$, m is integer~~

~~$10^l \equiv (10^{p-1})^m \equiv 1^m \equiv 1 \bmod p$.~~

~~$(10^{p-1} \equiv 1 \pmod p)$~~ $\quad$ ~~proof: p is prime, Euler's phi: $\phi(p) = p-1$~~

~~Euler's Theorem: $(10+pn)^{p-1} = [1]_n$~~

~~$\Rightarrow ([10]_p)^{p-1} = [1]_n$.~~

~~$99 \ldots 99 = 10^k - 1$~~

5. $[10]_p = \{10 + pn, n \in \mathbb{Z}\}$ $\qquad 9 \cdots 9 = 10^k - 1$

$p \notin \{2, 5\}$ $\; p \nmid 10$ $\; p \nmid (10+pn)$ $\; \gcd(10, p) = 1$ $\; \gcd(p, 10+pn) = 1$ $\; \angle$ $[10]_p \in \mathbb{Z}_n$, $\gcd(10, p) = 1$

p is a prime $\Rightarrow$ Euler's phi: $\phi(p) = (p-1)p^{1-1} = p-1$ $\qquad [10]_p \in \mathbb{Z}_n^*$.

Euler's theorem: $([10])^{p-1} = [1]_p$

let $l = m(p-1)$ $\quad m \geq 1$, $m \in \mathbb{Z}$

$10^l = 10^{m(p-1)} = (10^{p-1})^m = [1^m]_p = [1]_p \Rightarrow 10^l - 1 = [0]_p$.

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

it covers infinite items in $\{9, 99 \cdots 999\}$

$\Rightarrow$ p divides $\{9, 99, 999 \cdots\}$

infinitely elements in.

method 2

proof ②:

if p is prime. $1 \cdots p-1$ relative prime to p

for $a \in \{1, 2, \ldots p-1\}$. $\exists b$: $ab \equiv 1 \bmod p$.

b is prime. $a \equiv b$ iff $a = 1$ $b = p-1$

$a = 2$ $b = p-2$

$\vdots$

for $2 \cdot 3 \cdots (p-2) \equiv 1 \bmod p$

$1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) = (p-1) \bmod p$

$= -1 \bmod p$.