

Homework

Q) Let f be a polynomial with integer coefficients.
 Show that $(a-b) \mid (f(a)-f(b))$ for any integers a, b which is same as saying $f(a+d) \equiv f(a) \pmod{d}$

Ans:- $f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 \dots c_i \in \mathbb{Z}$

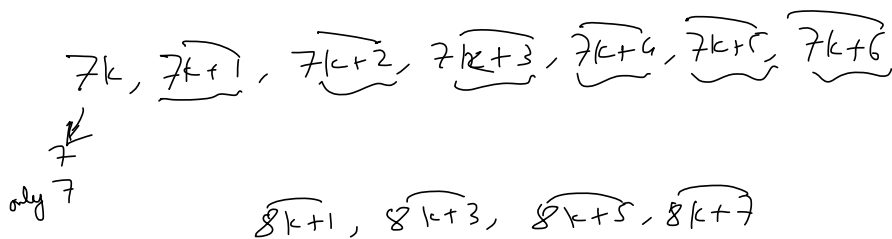
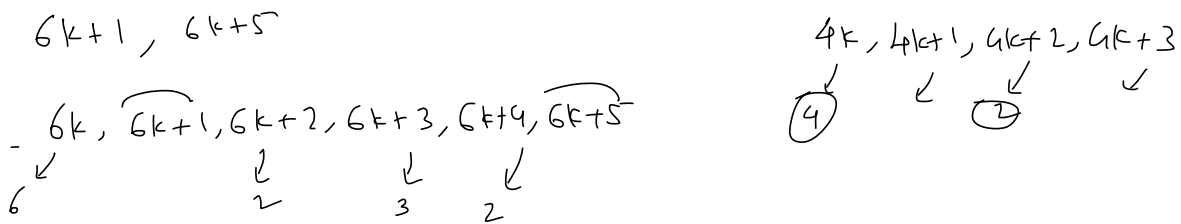
$f(a) = c_n a^n + c_{n-1} a^{n-1} + \dots + c_1 a + c_0$

$f(b) = c_n b^n + c_{n-1} b^{n-1} + \dots + c_1 b + c_0$

$f(a) - f(b) = c_n (a^n - b^n) + c_{n-1} (a^{n-1} - b^{n-1}) + \dots + c_1 (a - b)$

$\Rightarrow (a-b) \mid (f(a) - f(b)) \dots$ as $c_i \in \mathbb{Z}$ and $(a-b) \mid (a^j - b^j) \forall j \geq 1$

$d \mid (f(a+d) - f(a)) \Rightarrow f(a+d) - f(a) \equiv 0 \pmod{d}$
 $\Rightarrow f(a+d) \equiv f(a) \pmod{d}$



$\underbrace{0, 1, \dots, p-1}_p \pmod{p}$

0 → has no inverse

$p-1$ → has $p-1$ as its own inverse

1 → has inverse as 1

$$a^{-1} \equiv \frac{1}{a} \pmod{p} \Rightarrow ax \equiv 1 \pmod{p} \quad a \in \{1, \dots, p-1\}$$

Suppose $\exists b \neq a$ and $b \in \{1, \dots, p-1\}$ and $bx \equiv 1 \pmod{p}$

$$ax - bx \equiv 0 \pmod{p}$$

$$\Rightarrow x(a-b) \equiv 0 \pmod{p}$$

→ 0 or $ix \pmod{p}$ → not possible

* So inverse mod prime is unique

$$a \equiv b^{-1} \pmod{p} \Rightarrow b \equiv a^{-1} \pmod{p}$$

$$a^2 \equiv 1 \pmod{p}$$

$$\Rightarrow a^2 - 1 \equiv 0 \pmod{p}$$

$$\Rightarrow (a-1)(a+1) \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid (a-1)(a+1) \Rightarrow p \mid (a-1) \text{ or } p \mid (a+1)$$

$$\text{So, } a \equiv 1 \pmod{p} \text{ or } a \equiv -1 \pmod{p}$$

$$\text{Only in these cases } a^{-1} \equiv a \pmod{p}$$

$$(p-1)! = 1 \times 2 \times 3 \times \dots \times p-1 \pmod{p} \quad \rightarrow \text{odd } p$$

$$\equiv -(2 \times 3 \times \dots \times p-2) \pmod{p}$$

↓
So we can pair the inverses with each other and get that product as $1 \times 1 \times \dots \times 1 \pmod{p}$

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

$$(p-1)^{-1} \equiv (p-1) \pmod{p}$$

for 2 to $p-2$ every element has inverse in 2 to $p-2$ which are distinct.

$$= -1 \pmod{p} \quad \text{for } p=2 \Rightarrow 1! = 1 \pmod{2} = -1 \pmod{2}$$

Wilson's Theorem:-

Let p be a prime. Then $(p-1)! = -1 \pmod{p}$

→ Another Version of this theorem:-

For any integer n we have

$$(n-1)! = -1 \pmod{n}$$

if and only if n is a prime.

$$n = ab \Rightarrow a \in \{1, \dots, n-1\}$$

for $a, b \in \mathbb{Z}$

$$b \in \{1, \dots, n-1\}$$

$$\Rightarrow ab \mid (n-1)! \quad \text{if } a \neq b$$

$$\Rightarrow (n-1)! = 0 \pmod{a}$$

For $n=4$ we get,

$$(n-1)! = 2 \pmod{n}$$

Now if $a=b$ then

$$n = a^2$$

$$a \leq \sqrt{n}$$

$$a \in \{1, \dots, n-1\}$$

$$2a \in \{1, \dots, n-1\}$$

↳ if $\sqrt{n} > 2$

so for $n=4$ case it's not possible.

$$\Rightarrow a^2 \mid (n-1)!$$

Q) Let p be a prime. Show that the remainder when $(p-1)!$ is divided by $p(p-1)$ is $p-1$.

Q) Find the value of $\gcd(n!+1, (n+1)!)$