ID: IT-21024
Name: Md. Shahidul Islam

Modulare Arithmatic :

✓ $(a+b)\%m = (a\%m + b\%m)\%m$

$(a-b)\%m = ((a\%m - b\%m)\%m + m)\%m$

$(a*b)\%m = (a\%m * b\%m)\%m$

~~$-x\%m = (m-x)\%m$~~ ~~$((-x\%m)+m)\%m$~~

✓ $-x\%m = (m-(x\%m))\%m = (-x\%m+m)\%m$

$x\%m = x - \left\lfloor \frac{x}{m} \right\rfloor * m$

✓ Inverse modulo: i) $\frac{1}{a}\%m$ exist করে when $gcd(a,m)=1$.

ii) m modulo তে a র modulo inverse ~~x~~ x হলে $(\frac{1}{a}\%m = x)$

হলে, $(a*x)\%m = 1$

iii) m prime হলে, $a\%m, 2*a\%m, 3*a\%m, \ldots (m-1)*a\%m$

র সব গুলো value distinct হবে। Because

$i*a \equiv j*a \ (\%m)$

$\frac{1}{a} * i*a \equiv \frac{1}{a} * j*a \ (\%m)$; a র modulo inverse exist করে বলেই $\frac{1}{a}$ গুণ করা যায়।

$i \equiv j \ (\%m)$

ID: IT-21024
Name: md. shahidul Islam

iv) Fermatts little theorem: m prime হলে,

$(a * 2a * 3a * \cdots\cdots * (m-1)a) \% m = ((m-1)!) \% m$

$\Rightarrow (a^{m-1} * (m-1)!) \% m = ((m-1)!) \% m$

$\Rightarrow a^{m-1} \% m = 1 \% m$

$\therefore a^{m-1} \equiv 1 (\% m)$ → m always prime

v) From fermatt little theorem,

$a^{m-1} \equiv 1 (\% m)$

$\Rightarrow \frac{a^{m-1}}{a} \equiv \frac{1}{a} (\% m)$

$\Rightarrow a^{m-2} \equiv \frac{1}{a} (\% m)$

that means,

$\frac{1}{a} \% m = a^{m-2} \% m$ → m always prime

i) $a \% m = b \% m$ হলে, $(a*n) \% m = (b*n) \% m$ হবে।

ii) $a \% m = b \% m$ হলে, $\frac{a}{n} \% m = \frac{b}{n} \% m$ হবে যদি n এবং m coprime.

ID: IT-21024
Name: Md. Shahidul Islam

Question-1: $-17 \% 23 = ?$

Soln:

$$(-17 \% 23 + 23) \% 23 = 6 \% 23$$

$$= 6 \quad \text{(Ans.)}$$

সূত্র: $-a \% m = (-a \% m + m) \% m$

Question-2: Find Multiplicative Inverse of -13 upon modulo 23?

Soln: The corresponding value of -13 modulo 23 in modulo field is

$$(-13 \% 23 + 23) \% 23 = 10 \% 23$$

$$= 10$$

We know the fermat's little theorem,

$$\frac{1}{a} \% m = a^{m-2} \% m \; ; \text{where } \gcd(a, m) = 1.$$

$$\therefore \frac{1}{-13} \% 23 = \frac{1}{10} \% 23$$

$$= 10^{23-2} \% 23$$

$$= 7 \quad \text{(Ans.)}$$