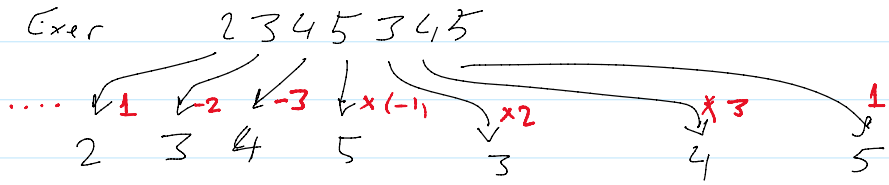
Linear Congruences

Wednesday, February 2, 2022 12:47 PM

Missing: #1, 6

Recall : Modular Arithmetic

Exer $2\,3\,4\,5\,3\,4\,5$



$\equiv 2\,3\,4\,5\,3\,4\,5 \pmod 7$

$\equiv 2 \pmod 7$

1) Modular Exponentiation

Objective:

To compute : $b^n \pmod m$

ModExp : $(b, m, n = (a_{k-1}\, a_{k-2} \cdots a_0)_2)$

$x = 1$; $p \equiv b \pmod m$

for $i = 0$ to $k-1$

if $a_i == 1$ then

$x = x * p \pmod m$.

$p = (p * p) \bmod m$.

return x;

$b^4 = b \cdot b \cdots b$

e.g. $n = 19 = (10011)_2$ (R ← L)

3^{19}

3	1	3^1 ← x
3^2	1	3^2
3^4	0	
3^8	0	
3^{16}	→	3^{16}
↑ p		$= 3^{19}$

e.g. $3^{19} \bmod 11$, $n = (10011)_2$ ← a_i

a_i	$x = 1$	$p = 3$
1	3	9
1	$27 \equiv 5$	$81 \equiv 4$
0	5	$16 \equiv 5$
0	5	$25 \equiv 3$
1	$15 \equiv 4$	9

$\therefore 3^{19} \equiv 4 \pmod{11}$

2] Linear Congruences

Objective: To solve for x in $a \cdot x \equiv b \pmod{m}$

e.g. $2 \cdot x \equiv 6 \pmod{11}$

div by 2 $\Rightarrow x = \frac{6}{2}$ ✗ $\pmod{11}$

$\therefore x \equiv 3$

3] Def^{n}. the inverse of a in (mod m) is $\bar{a}$ (or $\bar{a}^{-1}$)

s.t. $a \cdot \bar{a}^{-1} \equiv 1 \pmod{m}$

e.g. $2^{-1} \equiv 3 \pmod{5}$

$3^{-1} \equiv 5 \pmod{7}$

$2^{-1} \equiv 4 \pmod{7}$

$4^{-1} \equiv ? \pmod{10}$ } has no inverse

$2^{-1} \equiv ? \pmod{8}$ }

$6^{-1} \equiv \pmod{15}$ }

4] Thrm:

if a and m are relatively prime, then

$\exists\ \bar{a}^{-1}$ s.t. $a \cdot \bar{a}^{-1} \equiv 1 \pmod{m}$

and $\bar{a}^{-1}$ is unique in (mod m)

proof:

$\gcd(a, m) = 1$

by EEA, $\gcd(a, b) = x \cdot a + y \cdot m = 1$

apply (mod m): $x \cdot a + 0 \equiv 1 \pmod{m}$

$\therefore \bar{a}^{-1} \equiv x \pmod{m}$

e.g.

find the 4^{-1} in mod 13

$$13 = 3 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0 \quad \leftarrow \text{gcd}$$

$\therefore \quad 1 = 13 - 3 \cdot 4$

$\therefore \quad 4^{-1} = (-3) \equiv 10 \pmod{13}$

5] Solving Linear congruences

$$a \cdot x \equiv b \pmod{m}$$

$$\Longrightarrow \quad x \equiv b \cdot a^{-1} \pmod{m}$$

e.g. $\quad 21x \equiv 3 \pmod{13}$

$$x \equiv 3 \cdot (4^{-1})$$
$$\equiv 3 \cdot 10$$
$$\equiv 30 \equiv 4 \pmod{13}$$