CS 70 ## 2.13 LECTURE 8

CHINESE REMAINDER THEOREM

$x \equiv a \mod p$ where p & q are coprime ($\gcd(p,q)=1$)
$x \equiv b \mod q$
Hopeless to know anything other than $x \bmod pq$
Think of x as $\begin{bmatrix} a \\ b \end{bmatrix}$; $x = av_p + bv_q$ $\quad v_p = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $v_q = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
$v_p \bmod q = 0 \Rightarrow v_p = k_p q$ ↪ $v_p \bmod p = 1$, $v_p \bmod q = 0$
Need $k_p q = 1 \mod p \longrightarrow k_p = q^{-1} \mod p$. $k_q = p^{-1} \mod q$
Recall: $1 = \_p + \_q \xrightarrow{\text{egcd}} 1 = k_q p + k_p q = v_q + v_p$
$z \equiv a \mod p$
$z \equiv b \mod q$ GOAL: $z \equiv x \mod pq$
Consider $z-x$: $z-x \equiv 0 \mod p$; $z-x \equiv 0 \mod q$ ↪ $z-x \equiv 0 \mod pq$
Because $\gcd(p,q)=1 \Rightarrow \text{lcm}(p,q) = pq \Rightarrow z-x = \ell pq$ ▨

EX How many numbers don't have multiplicative inverses mod pq?
Need numbers that aren't relatively prime to p & q. This is all the multiples of p & q: p multiples of q, q multiples of p minus a double-counted 0. $p+q-1$.

mod 3 \ mod 5	5	11	2	8	14
(10)	1	7	13	4	
0	(6)	12	3	9	

$p=5$
$q=3$

CRT: Multiplication.

THM $x = \begin{bmatrix} a \\ b \end{bmatrix}$ & $y = \begin{bmatrix} c \\ d \end{bmatrix} \Longrightarrow xy = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ take $\begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 100 \overset{\text{mod } 5}{\underset{\text{mod } 3}{}} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

PROOF $x = av_p + bv_q$ $\quad y = cv_p + dv_q \longrightarrow xy = acv_p^2 + bdv_q^2 + cbv_pv_q + adv_pv_q$
$xy = acv_p^2 + bdv_q^2 + 0$ must show $v_p^2 \equiv v_p \mod pq$ ← have pq factor
Know $1 = v_q + v_p$; $1 \cdot v_p \equiv v_p$ $\quad (v_q + v_p)v_p \equiv v_p$ $\quad v_p^2 + v_pv_q \equiv v_p$

GENERAL $m_1, m_2 \ldots m_n$ pairwise coprime. $x \equiv a_i \bmod m_i$ $\quad x = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$ $v_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$
$v_i = k_i \prod_{j \neq i} m_j$ so $v_i \bmod m_j = 0$ for $i \neq j$
$k_i = \left(\prod_{j \neq i} m_j\right)^{-1} \bmod m_i$

⟶
⟶

FERMAT'S LITTLE THEOREM

Try mod 5: $0^0 \equiv ?$ $0^1 \equiv 0$ $0^2 \equiv 0$ ...

$1^0 \equiv 1$ $1^1 \equiv 1$ $1^2 \equiv 1$ ...

$2^0 \equiv 1$ $2^1 \equiv 2$ $2^2 \equiv 4$ $2^3 \equiv 3$ $2^4 \equiv 1$

periodic, but period is 4 or 1 o_O

$3^0 \equiv 1$ $3^1 \equiv 3$ $3^2 \equiv 4$ $3^3 \equiv 2$ $3^4 \equiv 1$

$4^0 \equiv 1$ $4^1 \equiv 4$ $4^2 \equiv 1$

period 2

All of these, however, fit in period 4.

THM Given $a \not\equiv 0$, $a^{p-1} \equiv 1 \bmod p$ if p is prime. Can be written as $a^p \equiv a \bmod p$ if p is prime

PROOF p is prime, and $\gcd(a,p) = 1$. a's times table mod p has everything $0, a, 2a, 3a, \ldots, (p-1)a$ consider $\prod_{i=1}^{p-1} ai = a^{p-1} \prod_{i=1}^{p-1} i = a^{p-1}(p-1)!$

Multiplication commutes.

$a^{p-1}(p-1)! \bmod p = (p-1)! \bmod p$ $\quad a^{p-1}(p-1)! \equiv (p-1)! \bmod p$

$\gcd((p-1)!, p) = 1$ can divide! $\quad a^{p-1} \equiv 1 \bmod p$ ▨