

CHINESE REMAINDER THEOREM

$x \equiv a \pmod p$
 $x \equiv b \pmod q$ where $p \& q$ are coprime ($\gcd(p, q) = 1$)

Hopeless to know anything other than $x \pmod{pq}$
 Think of x as $\begin{bmatrix} a \\ b \end{bmatrix}$; $x = av_p + bv_q$
 $v_p \pmod q = 0 \implies v_p = k_p q$ $\leftarrow v_p = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, v_q = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
 $v_p \pmod p = 1, v_p \pmod q = 0$

Need $k_p q = 1 \pmod p \implies k_p = q^{-1} \pmod p$. $k_q = p^{-1} \pmod q$
 Recall: $1 = _p + _q \xrightarrow{\text{egcd}} 1 = k_q p + k_p q = v_q + v_p$

$z \equiv a \pmod p$
 $z \equiv b \pmod q$ GOAL: $z \equiv x \pmod{pq}$
 Consider $z - x$: $z - x \equiv 0 \pmod p$; $z - x \equiv 0 \pmod q$
 Because $\gcd(p, q) = 1 \implies \text{lcm}(p, q) = pq \implies z - x = l pq$ $\leftarrow z - x \equiv 0 \pmod{pq}$

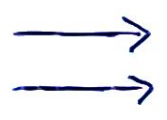
EX How many numbers don't have multiplicative inverses mod pq ?
 Need numbers that aren't relatively prime to $p \& q$. This is all the multiples of $p \& q$: p multiples of q , q multiples of p minus a double-counted 0. $p+q-1$.

	5	11	2	8	14	$p=5$
$\pmod{10}$	10	1	7	13	4	$q=3$
	0	6	12	3	9	
	mod 5					

CRT: Multiplication.

THM $x = \begin{bmatrix} a \\ b \end{bmatrix} \& y = \begin{bmatrix} c \\ d \end{bmatrix} \implies xy = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ take $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 100 \pmod{5} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
PROOF $x = av_p + bv_q$ $y = cv_p + dv_q \implies xy = acv_p^2 + bdv_q^2 + cbv_p v_q + adv_p v_q$
 $xy = acv_p^2 + bdv_q^2 + 0$ must show $v_p^2 \equiv v_p \pmod{pq}$ \leftarrow have pq factor
 know $1 = v_q + v_p$; $1 \cdot v_p \equiv v_p$ $(v_q + v_p)v_p \equiv v_p$ $v_p^2 + v_p v_q \equiv v_p$

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



FERMAT'S LITTLE THEOREM

Try mod 5:

$0^0 \equiv ?$	$0^1 \equiv 0$	$0^2 \equiv 0$...
$1^0 \equiv 1$	$1^1 \equiv 1$	$1^2 \equiv 1$...
$2^0 \equiv 1$	$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 3$ $2^4 \equiv 1$
<u>periodic, but period is 4 or 1</u> $0-0$			
$3^0 \equiv 1$	$3^1 \equiv 3$	$3^2 \equiv 4$	$3^3 \equiv 2$ $3^4 \equiv 1$
$4^0 \equiv 1$	$4^1 \equiv 4$	$4^2 \equiv 1$	
period 2			

All of these, however, fit in period 4.

THM Given $a \neq 0$, $a^{p-1} \equiv 1 \pmod p$ if p is prime. Can be written as $a^p \equiv a \pmod p$ if p is prime

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

$a^{p-1} (p-1)! \pmod p = (p-1)! \pmod p$
 $\gcd((p-1)!, p) = 1$ can divide!

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