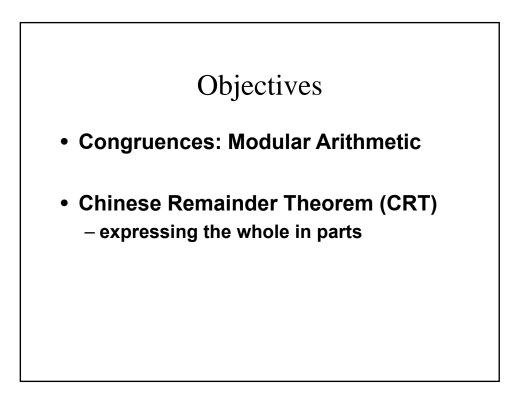
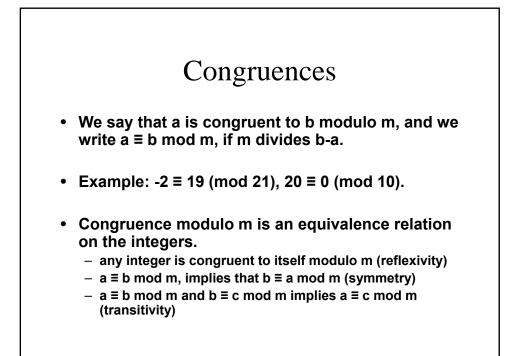
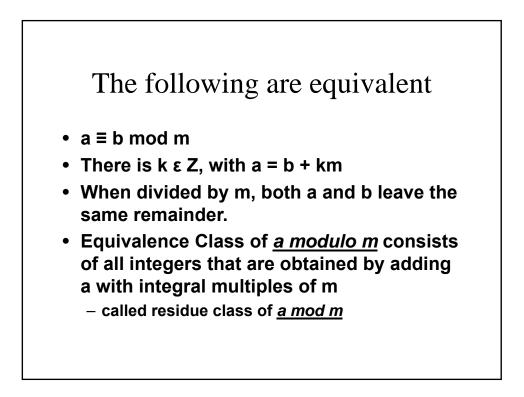
Congruences

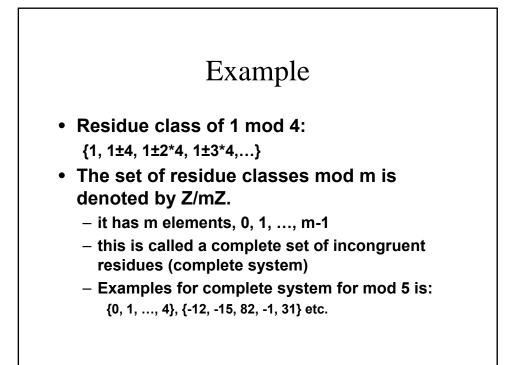
Debdeep Mukhopadhyay

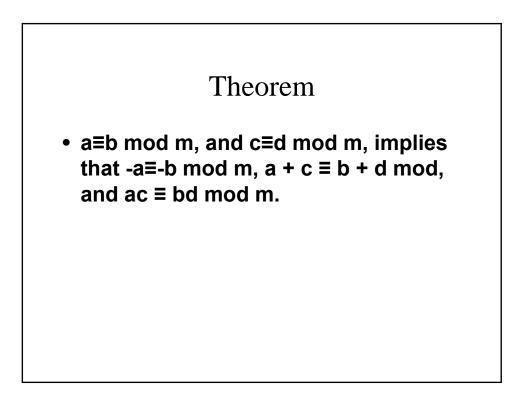
Associate Professor Department of Computer Science and Engineering Indian Institute of Technology Kharagpur INDIA -721302







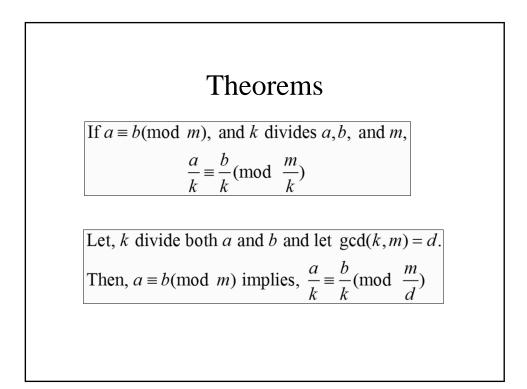


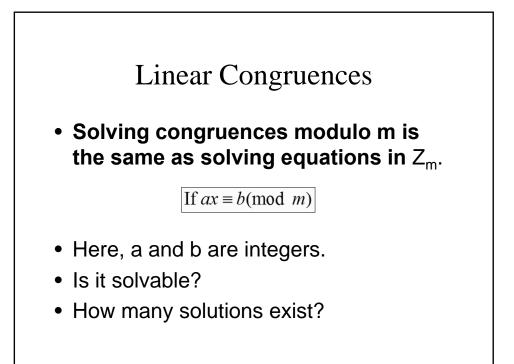


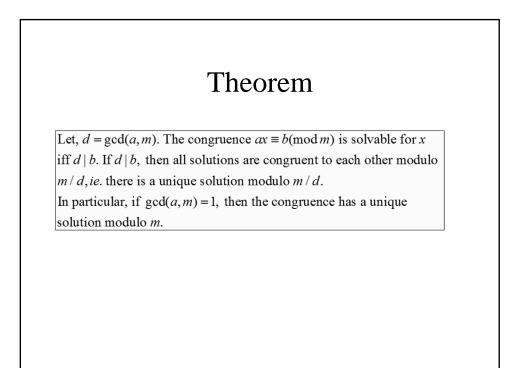
Example

Prove that $2^{2^5} + 1$ is divisible by 641.

Note that: $641 = 640 + 1 = 5*2^7 + 1$. Thus, $5*2^7 \equiv -1 \mod 641$. $\Rightarrow (5*2^7)^4 \equiv (-1)^4 \mod 641$ $\Rightarrow 5^4*2^{28} \equiv 1 \mod 641$ $\Rightarrow (625 \mod 641)*2^{28} \equiv 1 \mod 641$ $\Rightarrow (-2^4)*2^{28} \equiv 1 \mod 641$ $\Rightarrow 2^{32} \equiv -1 \mod 641$



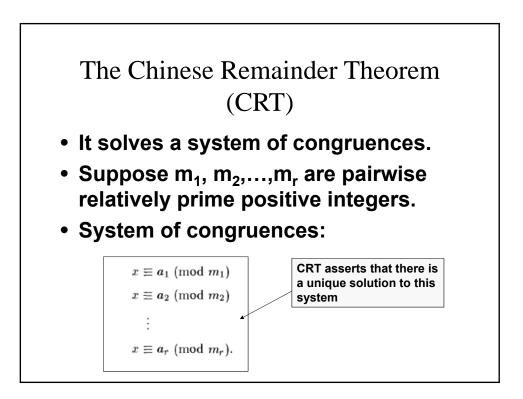


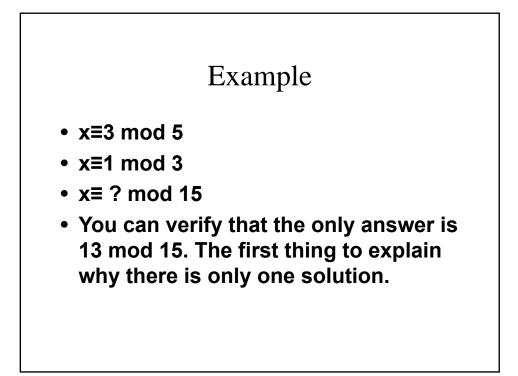


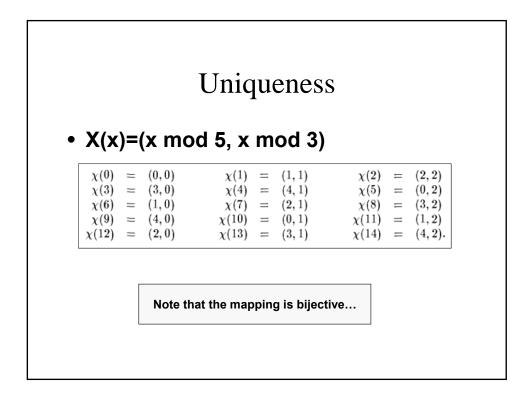
Example

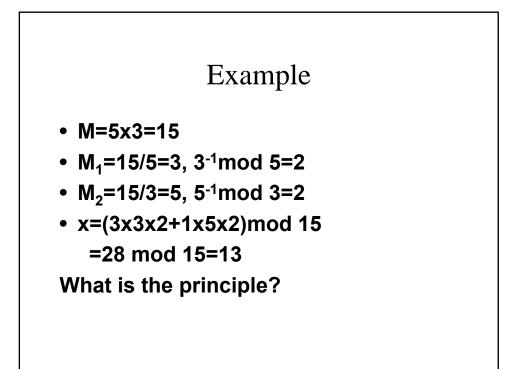
 $21x \equiv 9 \pmod{15}$ is solvable and has 3 solutions modulo 15.

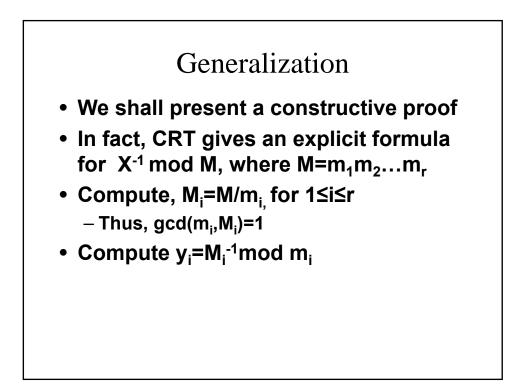
 $21x \equiv 8 \pmod{15}$ is not solvable.











- Thus, M_iy_i≡1 (mod m_i), for 1≤i≤r
- Define,

$$\rho(a_1,\ldots,a_r) = \sum_{i=1}^r a_i M_i y_i \mod M.$$

- Compute, ρ mod m_i≡a_i [This is because M_iy_i≡1 (mod m_i) and M_iy_i≡0 (mod m_j)]
- Since, the domain and range have the same cardinality and the function X() is onto, by our previous discussion the function is bijective. Thus the solution is unique modulo M.

