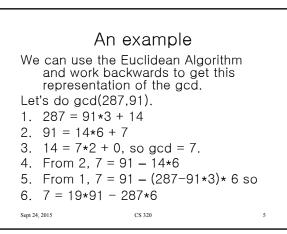
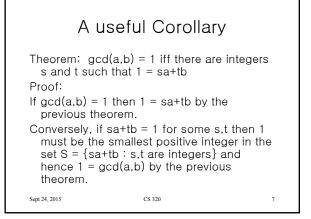


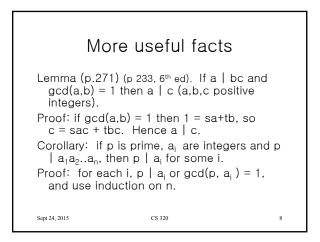
Proof. Let  $S = \{sa + tb : s, t \text{ are integers}\}\)$  a = 1a + 0b, b = 0a + 1b are in S.Note that the sum of any two elements of S is also in S, and any multiple of an element of S is in S. Thus, if x,y are in S and we divide y into x, x = qy + r, 0 \le r < y, then r = x-qy is in S. Sept24,2015

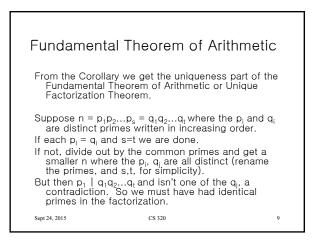
= {sa+tb : s,t are i Then for any x in S, x = qd + r, $0 \le r <$ so r must be 0 by Thus d is a common But every common d	d   x, because if d, then r is in S, definition of d. divisor of a and b. livisor u of a and b ent of S, and hence e $u \le d$ . (a,b), the greatest	5
Sept 24, 2015	CS 320	4

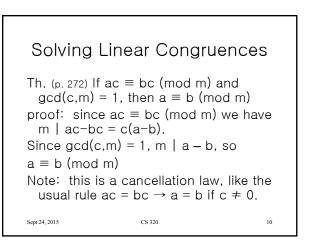


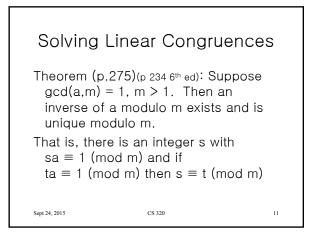
Note that this representation of gcd(a,b) as sa + tb isn't unique. We have 7 = 19\*91 - 287\*6, but also 7 = (19-287)\*91+(-6+91)\*287, so 7 = (-268)\*91+(85)\*287For another algorithm, see p 273, 41-45 (6<sup>th</sup> ed. p. 246, 48-51)

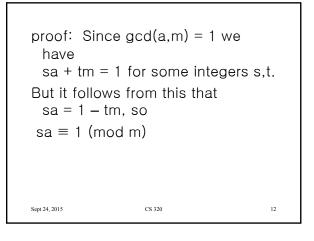


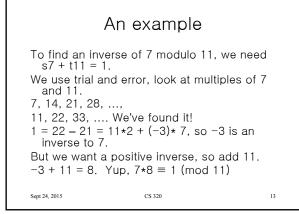


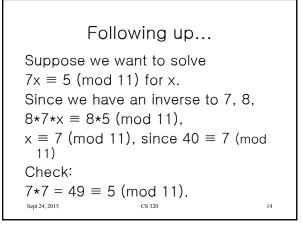


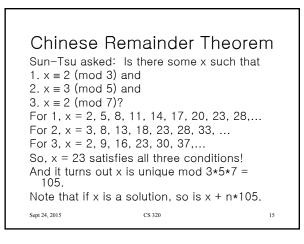


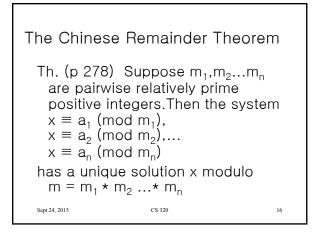




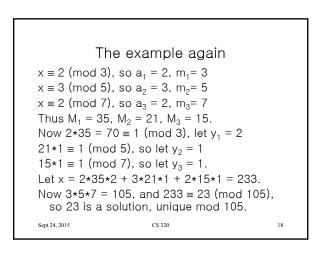


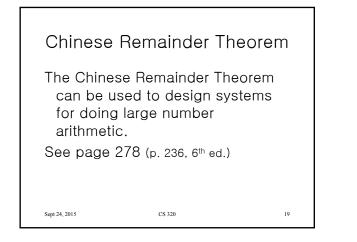


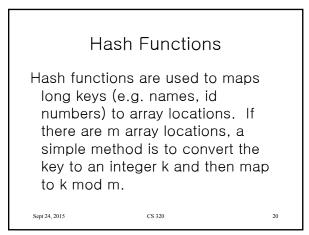




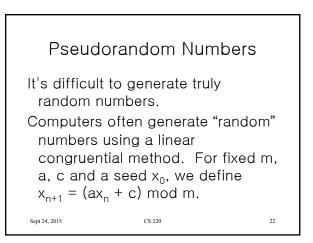
Proof: Let  $M_k = m/m_k = m_1...m_{k-1}m_{k+1}...m_n$ Then  $gcd(M_k,m_k) = 1$  for k = 1,...,n. Hence  $M_k$  has an inverse  $y_k \mod m_k$ ,  $M_k y_k \equiv 1 \pmod{m_k}$ . Let  $x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n$ . Then  $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k} \forall k$ , since  $a_j M_j y_j \equiv 0 \pmod{m_k}$  for  $j \neq k$ . To see uniqueness, if x and y are two solutions then  $x - y \equiv 0 \pmod{m_k} \forall k$ and hence  $m \mid x - y$ , so  $x \equiv y \pmod{m_k}$ .

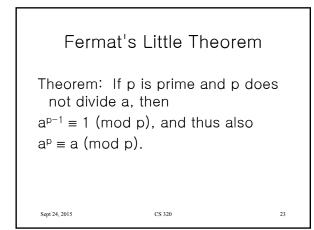






Hashing collisions A collision is when two keys map to the same array location. A perfect hash function is designed to produce no collisions. A collision can be resolved by moving down the array to the next free array location, or by hanging linked lists off the array locations.





Proof: The numbers a, 2a, 3a,, (p-1)a are distinct mod p since their pairwise differences are not 0 mod p.		
Thus they are 1, 2, 3,, p-1 in some order, mod p.		
So a*2a**(p-1)a ≡ 1*2**(p-1) (mod p)		
Dividing both sides by 1*2*3**(p-1), which is relatively prime to p, we get a <sup>p-1</sup> ≡ 1 (mod p), hence a <sup>p</sup> ≡ a (mod p)		
Sept 24, 2015 CS 320 24		

## Cryptology

- A really simple cryptographic method was used by Julius Caesar. This was to shift each letter right a fixed number of places in the alphabet.
- If we encode each letter by its position in the alphabet we can use:
  - $f(x) = (x + k) \mod 26$ , to shift k places.

Sept 24, 2015

CS 320

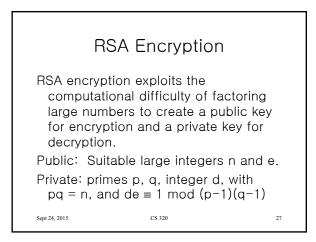
25

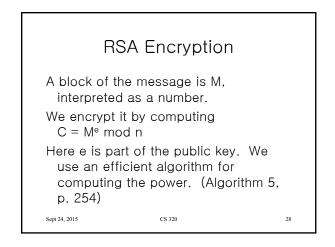
## Cryptology The Caesar cypher is very easy to crack, and any cryptographic method which uses a fixed code for each letter is vulnerable to attacks based on the frequency of occurrence of particular letters.

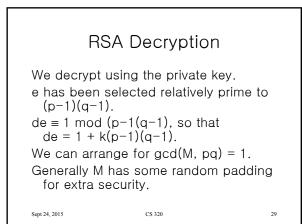
CS 320

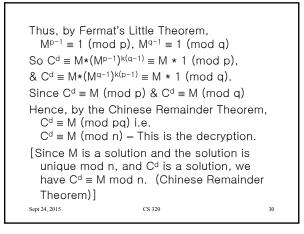
26

Sept 24, 2015

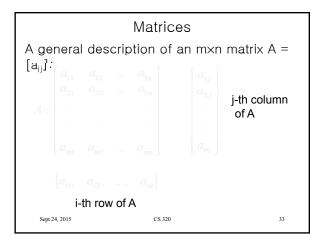


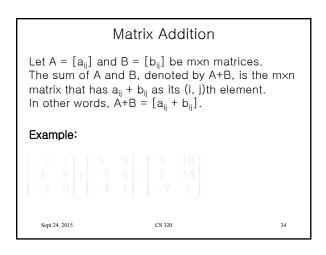




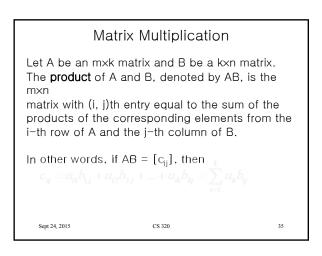


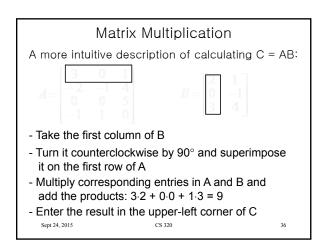
## Matrices A **matrix** is a rectangular array of numbers. Private Key Cryptography A matrix with m rows and n columns is called an m×n matrix. The RSA algorithm uses a fair bit of computation, so in practice it is used is a 3×2 matrix. Example: A not for exchanging large messages, but for a secure exchange of private keys which can then be used to A matrix with the same number of rows and columns exchange large messages efficiently is called square. and securely using DES or AES, Two matrices are equal if they have the same symmetric key algorithms, whose number of rows and columns and the corresponding computational cost is cheap. See entries in every position are equal. Wikipedia for more info. Sept 24, 2015 CS 320 Sept 24, 2015 CS 320 31

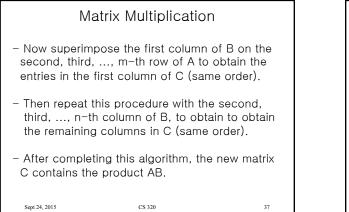


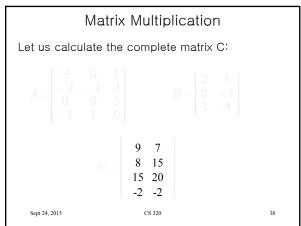


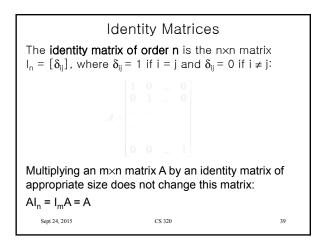
32











Powers and Transposes of Matrices		
The <b>power function</b> can be defined for <b>square</b> matrices. If A is an nxn matrix, we have:		
$A^0 = I_n$ , $A^r = AAAA$ (r times the matrix A)		
The <b>transpose</b> of an m×n matrix $A = [a_{ij}]$ , denoted by $A^t$ , is the n×m matrix obtained by interchanging the rows and columns of A.		
In other words, if $A^t = [b_{ij}]$ , then $b_{ij} = a_{ji}$ for $i = 1, 2,, n$ and $j = 1, 2,, m$ .		
Sept 24, 2015 CS 320	40	

