Midterm 2 coverage: ##=

Section 4.4:
- Solving linear congruences.
  ex: $3x \equiv 4 \mod 7$

- Chinese Remainder Theorem
- Fermat's Little Theorem
- Skip 4.5

Section 4.6: Encryption/Decryption
- Caesar cipher, shift cipher
- Cryptanalysis
- transposition cipher
- RSA

Training problems 3 and 4

Chapter 1 of coding the matrix:
- Complex numbers
- conjugate
- Plot
- resizing
- absolute value
- shifting
- comprehensions using Plot

ex: using RSA, encrypt BIG BEN

$n = 1709 \cdot 1721 = 2941189$

$e = 9$

Solution:

$252525 < 2941189$

BIG BEN
01,08,06 01,04,13

↑
block size
is 6 digits

$C_1 = m_1^e \bmod n = \boxed{010806^9 \bmod 2941189}$

$C_2 = m_2^e \bmod n = \boxed{010413^9 \bmod 2941189}$

$C_1 = 799649$

$C_2 = 489205$

ex: RSA decrypt 799649 489205 with

$n = 1709 \cdot 1721 = 2941189$

$e = 9$

Solution:

Need to solve for d. $252525 < 2941189$

d is the inverse of $e \bmod (p-1)(q-1)$ < 6 digits

$= 9 \bmod (1708 \cdot 1720) = 9 \bmod 2937760$

Euclidean Algorithm

$2937760 = 9 \cdot 326417 + 7$

$9 = 7 \cdot 1 + 2$

$7 = 2 \cdot 3 + 1$

$2 = 1 \cdot 2$

$1 = 7 - 2 \cdot 3$

$2 = 9 - 7$

$7 = 2937760 - 9 \cdot 326417$

$1 = 7 - 2 \cdot 3 = 7 - (9-7) \cdot 3 = 7 - 3 \cdot 9 + 3 \cdot 7 = 4 \cdot 7 - 3 \cdot 9$

$= 4 \cdot (2937760 - 9 \cdot 326417) - 3 \cdot 9$

$= 4 \cdot 2937760 - 9 \cdot 1305668 - 3 \cdot 9$

$= 4 \cdot 2937760 - 9 \cdot 1305671$

$= 4 \cdot 2937760 - 1305671 \cdot 9$

$d = 2937760 - 1305671 = 1632089$

$m_1 = c_1^d \bmod n = 799649^{1632089} \bmod 2941189 = 10806 = 010806$

$m_2 = c_2^d \bmod n = 489205^{1632089} \bmod 2941189 = 10413 = 010413$

BIG BEN