CS1800
Discrete Structures
Fall 2017

Lecture 9
9/25/17

Last time

- Modular arithmetic
- Division algorithm
- Formal definition of mod
- Properties of mod
  - addition
  - multiplication
  - exponentiation

- Proof

Today

- Finish properties of mod
  - exponentiation
  - add. & mult. identities
  - add. & mult. inverses
- Solving equations mod n
  - inverses & linear decryption
- divides, division, primes

- proof

Next time

- GCD, LCM
- Euclid's alg.

$$13^1 \bmod 11 = 2$$

$$\begin{aligned}13^2 \bmod 11 &= \big((13 \bmod 11) \times (13 \bmod 11)\big) \bmod 11 \\ &= (2 \times 2) \bmod 11 \\ &= 4 \bmod 11 \\ &= 4\end{aligned}$$

$$\begin{aligned}13^4 \bmod 11 &= \big((13^2 \bmod 11) \times (13^2 \bmod 11)\big) \bmod 11 \\ &= (4 \times 4) \bmod 11 \\ &= 5\end{aligned}$$

$$\begin{aligned}13^8 \bmod 11 &= (5 \times 5) \bmod 11 \\ &= 3\end{aligned}$$

$\vdots$

What about $13^{14} \bmod 11$?

Answer: represent 14 in <u>binary</u>

	16	8	4	2	1
14		1	1	1	0

$14 = 8 + 4 + 2$

$\Rightarrow 13^{14} = 13^{8} \cdot 13^{4} \cdot 13^{2}$

so...

$$\begin{aligned} 13^{14} \bmod 11 &= (13^{8} \cdot 13^{4} \cdot 13^{2}) \bmod 11 \\ &= (3 \times 5 \times 4) \bmod 11 \\ &= 60 \bmod 11 \\ &= 5 \end{aligned}$$

$13^{14} = 3{,}937{,}376{,}385{,}639{,}289 \bmod 11$

Real crypto:
- use 1024 bit numbers, 309 decimal digits
- exponents ≥ 65537

$\rightarrow$ intermediate result 20,202,080 digits

$13^{11} \bmod 11$

$= (13^8 \cdot 13^2 \cdot 13^1) \bmod 11$

$= (3 \times 4 \times 2) \bmod 11$

$= 24 \bmod 11$

$= 2$

	8	4	2	1
11:	1	0	1	1

$11 = 8 + 2 + 1$

$13^{11} = 13^8 \cdot 13^2 \cdot 13^1$

Addition & Multiplication tables, mod n

$x \to a \cdot x \mod 3$

① mod 3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

a

② mod 4

x

×	0	1	2	3	
0	0	0	0	0	← bad
1	0	1	2	3	
2	0	2	0	2	← bad
3	0	3	2	1	

a

$x \to a \cdot x \mod 4$

Decrypting Linear Encryption :

$$y = 5\cdot x + 11$$

$$5x + 11 = y$$

-11 is the additive inverse of 11

$$5x + 11 - 11 = y - 11$$

$$5x = y - 11$$

$1/5$ is the mult. inv. of 5

$$\frac{1}{5}\cdot 5x = \frac{1}{5}(y-11)$$

$$x = \frac{1}{5}(y-11)$$

$$y = 5\cdot x + 11 \mod 26$$

$$5x + 11 = y \pmod{26}$$

$$5x + 11 + 15 = y + 15 \pmod{26}$$

$$5x = y + 15 \pmod{26}$$

need mult. inv. of 5

- need mult. inv. of 5, mod 26
- let i be the mult. inv. of 5, mod 26

$$\Rightarrow \quad 5\cdot i = 1 \mod 26$$

$$\Rightarrow \quad 5\cdot i = q\cdot 26 + 1$$

where q & i are <u>integers</u>

$$i = q\cdot(5 + 1/5) + 1/5 \qquad q = 4$$

$$\Rightarrow \quad i = 4(5 + 1/5) + 1/5$$

$$= 21$$

$$y = 4x + 3 \mod 26$$

$$4 \cdot i = q \cdot 26 + 1$$

$$i = q\left(6 + \tfrac{1}{2}\right) + \tfrac{1}{4}$$