Number Theory:

Modular Exponentiation

02/24

Prof. Forrest

Warm up

① Discuss with your neighbors whether a hot dog is a sandwich.

② what is $2^3 \bmod 3$?

$2^3 \bmod 3$ $\quad 8 \bmod 3 = 2$

$3k + r = 8$

r_2 $\quad r_2$

Logisitics

1. Labs 2 graded
2. Proj 2 on this way
3. Exam 1 is next R Mich 5
   → covg through tomorrow
   → topics and some problems will be completed by E.O.W.
   → Lab office hrs is just time to study and ask questions.

$a \equiv b \mod n$ $\quad nk = a - b$ for some $k \in \mathbb{Z}$

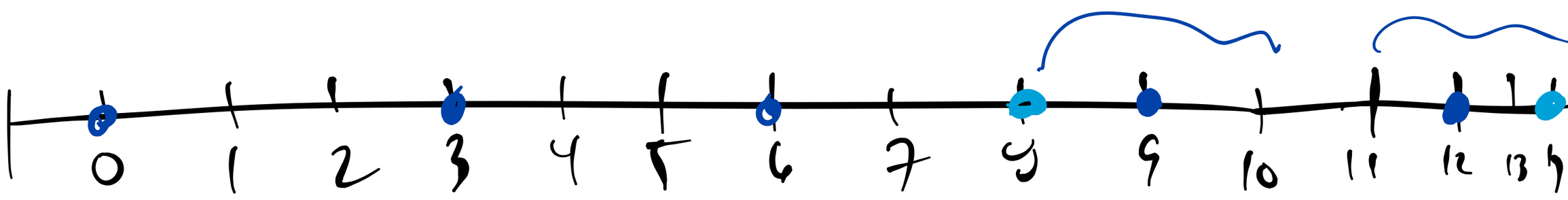
$14 \equiv 2 \mod 3$ $\quad 3k = 14 - 2 = 12$

$k = 4$

$14 \bmod 3 = 2$

$14 \equiv 8 \mod 3$ $\quad 3k = 14 - 8$?

$k = 2$



$$6^{22} \bmod 25 = ?$$

$$ab \bmod m = [a \bmod m \cdot b \bmod m] \bmod m$$

$$6 \cdot 6 \bmod m = [6 \bmod m \cdot 6 \bmod m] \bmod m$$

$$[6^2 \equiv 36] \bmod 25$$

$$36 \equiv 36 \bmod 25$$

$$25 \cdot 1 + r = 36$$

$$[36 \equiv 11] \bmod 25$$

$6^3 \equiv 6^2 \bmod 25 \cdot 6 \bmod 25$

$\equiv 66 \bmod 25$

$216 \equiv 16 \bmod 25$

$25u = 6^2 - 36$

$36 \equiv 36$

$36 - 36 = 0$

$6^{22} \bmod 25$ $[[6, 24]]$

$= 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdot 6 \cdots$

$= 6 \bmod 25 \cdot 6 \bmod 25 \cdot \cdots \bmod 25$

$n = 22$ $O(n)$

$\hat{}$ exponent

$6^{22} \bmod 25 = ?$

$6 \equiv 6 \bmod 25$

$6^2 \equiv 36 \bmod 25$

$\equiv 11 \bmod 25$

$6^4 \equiv 121 \bmod 25$

$\equiv 21 \bmod 25$

$6^8 \equiv 441 \bmod 25$

$\equiv 16 \bmod 25$

$6^{16} \equiv 256 \bmod 25$

$\equiv 6 \bmod 25$

$6^{32} \equiv 36 \bmod 25$

$\equiv 11$

How can we use these values to find 6^{22} easily?

$O(\log n)$

$3^{11} \mod 13$?

$3 \equiv 3 \mod 13$

$3^2 \equiv 9 \mod 13$

$3^4 \equiv 81 \mod 13 \leftarrow 13 \cdot 6 + 3 = 81$

$\equiv 3 \mod 13$

$3^8 \equiv 9 \mod 13$

$3^{11} = 3^{1+2+8} = 3 \cdot 3^2 \cdot 3^9 \equiv 3 \cdot 9 \cdot 9 \equiv 243 \mod 13$

$= 9$

x^{24}

$x^1 \xrightarrow{S} x^2 \xrightarrow{M} x^3 \xrightarrow{S} x^6 \xrightarrow{S} x^{12} \xrightarrow{S} x^{24}$

Square: S multiply: M

24 binary is ? 11000_2

x^{11000_2} x^{24}

Square

if $b_i == 1$:

multiply (m)

Moving from left → right

we square our answer

if the bit is 1 we

multiply by our base

① answer = 1

1^2 = answer

answer = answer * X

X

② X^2 S

X^3 M

③ X^6

④ X^{12}

⑤ X^{24}

algorithm (b : integer, n : integer, m : positive integer)

base ↑ b

exponent ↑ n

mod ↑ m

$3^{29} \mod 13$

output: $b^n \mod m$

answer = 1

for i = 0 to (len(bit(n))):

answer = (answer)^2 mod m

if bit(n)[i] == 1 then

answer = answer * b mod m

① Everytime we square or exponent we add a zero to our bit string

$(x^1)^2 = x^2$ $\quad 1 \to 1_2 \quad 2 \to 10_2$

$(x^n)^2 = x^{2n}$ $\quad 3 \to 11_2 \quad 6 \to 110_2$

② everytime we multiply we add one to our bitstring

$x \cdot x^2 = x^3$ $\quad x \cdot x^4 = x^{4+1}$

$2 \to 10_2 \quad 3 \to 11_2$

$6 \to 110_2 \quad 7 \to 111_2$

Recursive Approach

$6^{22} \mod 25 \equiv (6^{11} \mod 25)^2 \mod 25$

$\equiv (6 \cdot 6^{10} \mod 25)^2 \mod 25$

$(6 \cdot (6^5 \mod 25)^2)^2 \mod 25$

$(6 \cdot (6 \cdot 6^4 \mod 25)^2)^2$

$(6 \cdot (6 \cdot (6^2 \mod 25))^2)^2$

$(6 \cdot 6 \cdot 6 \mod 25)^2$

$6 \cdot (6^0 \mod 25)^2$

1

$5^{15} \mod 13$

$O(\log n)$

$$5^{15} \bmod 13 = 5 \cdot 5^{14} \bmod 13$$

$$\equiv 5 \cdot (5^7 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot 5^6 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5^3 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5 \cdot 5^2 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5 \cdot (5 \bmod 13)^2 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5 \cdot (5 \cdot 5^0 \bmod 13)^2 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5 \cdot (5 \cdot 1)^2 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5 \cdot (5)^2 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (5 \cdot 25 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (125 \bmod 13)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (5 \cdot (8)^2 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (320 \bmod 13)^2 \bmod 13$$

$$= 5 \cdot (8)^2 \bmod 14 = 8$$

notice we generated 5 s and $\log_2(15) \approx 3.91$