CS1800
Discrete Structures
Fall 2017

Lecture 8
9/21/17

Last time

- Finish logic
  - variables, predicates
  - quantifiers : $\exists, \forall$
- Start encryption
  - encoding $a \to 0$, $b \to 1$, $\vdots$
  - encryption

$$x \to (x+b) \bmod n$$

$$x \to (a \cdot x + b) \bmod n$$

$$x \to x^b \bmod n$$

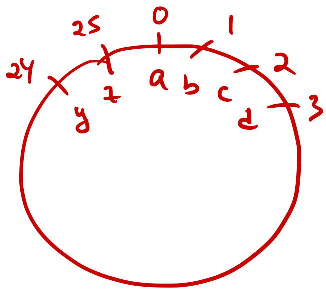
- mod function
  - arithmetic on a circle

Today

- Modular arithmetic & properties
- proof

Next time

- Continue...



Definition of mod

Division Algorithm: Let a be an integer and n a positive integer. Then there are <u>unique</u> integers q & r, $0 \le r < n$, such that

$$a = n \cdot q + r.$$

$$63 \quad 5 \cdot 12 + 3$$

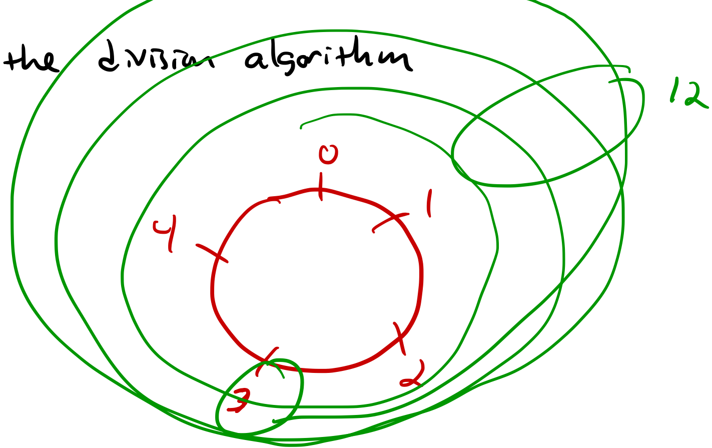
$$\begin{array}{r|l} & 12 \;\; q \\ \hline 5 & 63 \\ & \underline{5} \\ & 13 \\ & \underline{10} \\ & 3 \;\; r \end{array}$$

mod: remainder after division

$a \bmod n$ = "remainder after dividing a by n"

= r in the division algorithm

$63 \bmod 5 = 3$



Properties of modular arithmetic:

① $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

② $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

③ $-a \bmod n = n - (a \bmod n)$

④ If $a \bmod n = b \bmod n$, then $\exists$ integer k such that $a-b = k \cdot n$

$63 \bmod 5 = 3$

$18 \bmod 5 = 3$

45

Proof:

Let $r = a \bmod n = b \bmod n$

By division algorithm, we have

$$a = q_1 \cdot n + r$$
$$- \quad b = q_2 \cdot n + r$$

$$a-b = (q_1 \cdot n + r) - (q_2 \cdot n + r)$$
$$= (q_1 - q_2) \cdot n$$
$$= k \cdot n \quad \text{where } k = q_1 - q_2$$

Examples

① $(40+39) \bmod 11 = 79 \bmod 11 = 2$

$$
\begin{aligned}
&(40+39) \bmod 11 \\
&= [(40 \bmod 11) + (39 \bmod 11)] \bmod 11 \\
&= [7 + 6] \bmod 11 \\
&= 13 \bmod 11 \\
&= 2
\end{aligned}
$$

② $(40 \times 39) \bmod 11 = 1560 \bmod 11 = (141 \times 11 + 9) \bmod 11 = 9$

$$
\begin{aligned}
&(40 \times 39) \bmod 11 \\
&= [(40 \bmod 11) \times (39 \bmod 11)] \bmod 11 \\
&= 7 \times 6 \bmod 11 \\
&= 42 \bmod 11 \\
&= 9
\end{aligned}
$$

③

$$(13 \times 6 + 4) \bmod 11 = 82 \bmod 11 = 5$$

$$\shortparallel$$

$$[\,(13 \times 6) \bmod 11 + 4 \bmod 11\,\} \bmod 11$$

$$\shortparallel$$

$$[\,\{[13 \bmod 11\} \times [6 \bmod 11] \bmod 11\} + [4 \bmod 11]\,\} \bmod 11$$

$$\shortparallel$$

$$[\,[2 \times 6) \bmod 11 + 4\,\} \bmod 11$$

$$\shortparallel$$

$$\{1 + 4\} \bmod 11$$

$$\shortparallel$$

$$5$$

(4) $$13^2 \bmod 11 = 169 \bmod 11 = (15 \times 11 + 4) \bmod 11 = 4$$

$$\parallel$$

$$[(13 \bmod 11) \times (13 \bmod 11)] \bmod 11$$

$$\parallel$$

$$[2 \times 2) \bmod 4$$

$$\parallel$$

$$4$$

(5) $$13^4 \bmod 11 = 28,561 \bmod 11 = (2596 \times 11 + 5) \bmod 11 = 5$$

$$\parallel$$

$$[(13^2 \bmod 11) \times (13^2 \bmod 11)] \bmod 11$$

$$\parallel$$

$$(4 \times 4) \bmod 11$$

$$\parallel$$

$$16 \bmod 11$$

$$\parallel$$

$$5$$

(6) $$13^8 \bmod 11 = \_ = 3$$

$$13^7 = 13^4 \cdot 13^2 \cdot 13^1$$

$$5 \cdot 4 \cdot 2 \Rightarrow 7$$