COL 351: Analysis and Design of Algorithms

Lecture 19

Example of a different Number System

$A = \{0, 1, 2, 3, 4, 5, 6\}$

$p = 7$

$\{0, 1, \ldots p-1\}$

addition "$\oplus$" : $a \oplus b = (a + b) \bmod 7$

product "$\otimes$" : $a \otimes b = (a \times b) \bmod 7$

$\oplus$ inv

$1 \oplus 6 = 0$
$2 \oplus 5 = 0$
$3 \oplus 4 = 0$
$4 \oplus 3 = 0$
$5 \oplus 2 = 0$
$6 \oplus 1 = 0$

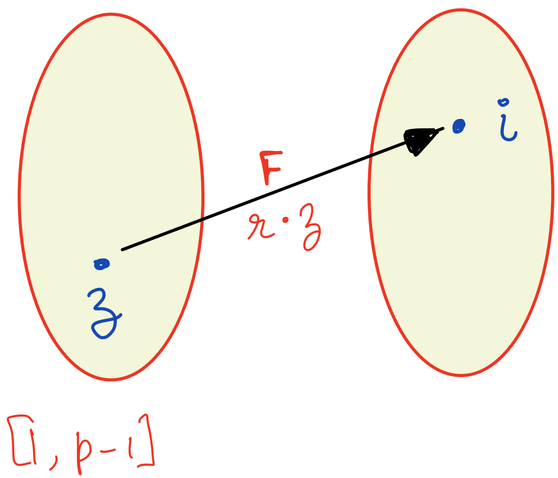
$\otimes$ inv

$1 \otimes 1 = 1$
$2 \otimes 4 = 1$
$3 \otimes 5 = 1$
$4 \otimes 2 = 1$
$5 \otimes 3 = 1$
$6 \otimes 6 = 1$

Modular Arithmetics

$$F(z) = (r \cdot z) \mod p \qquad \text{(Here, } p \text{ is a prime).}$$

$1 \leq r \leq p-1$



* Invertible

* If r is unif random
$\Rightarrow$ output of F is also unif random.

Modular Arithmetics

$${}^{p}C_i = \frac{p \, \lfloor p-1}{\underbrace{\lfloor i \; \lfloor p-i}_{\text{integer}}}$$

$F(z) = (r \cdot z) \mod p$ (Here, p is a prime).

Claim 1: For any $r \in [1, p-1]$, we have $r^{p-1} = 1 \mod p$

Proof:

Hypothesis: Claim holds for $r \leq p-2$.

$$(r+1)^p = \underbrace{r^p}_{= r} + \underbrace{\sum_{i=1}^{p-1} {}^{p}C_i \, r^i}_{= 0} + 1^p \pmod p = r+1 \pmod p$$

$$\Rightarrow \frac{(r+1)^p - (r+1)}{p} \text{ is integer} = (r+1) \frac{\left((r+1)^{p-1} - 1\right)}{p} \text{ is integer}$$

$$\Rightarrow (r+1)^{p-1} = 1 \pmod p$$

Modular Arithmetics

$$F(z) = (r \cdot z) \mod p \qquad \text{(Here, } p \text{ is a prime).}$$

<u>Claim 2</u>: $F(z)$ is invertible, and its inverse is given by $F^{-1}(y) := (r^{p-2}\, y) \mod p$

Proof:

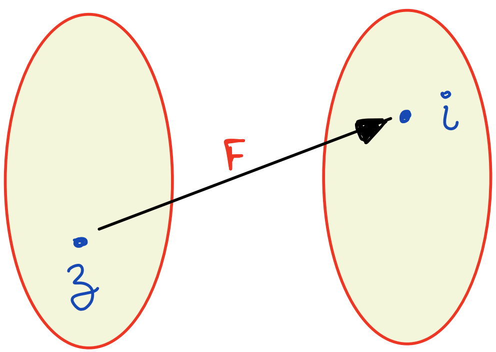
$$z \xrightarrow[F]{\cdot r} rz \pmod p \xrightarrow[F^{-1}]{\cdot r^{p-2}} \underbrace{r^{p-2} \cdot r}_{=1} \cdot z \pmod p$$

Modular Arithmetics

$F(z) \;=\; (r \cdot z) \mod p$ (Here, p is a prime).

Claim 3: If $r \in [1, p-1]$ was random, then for any $z, i \in [1, p-1]$, we have

$$\text{Prob}\big(F(z) = i\big) = \frac{1}{p-1}.$$



Modular Arithmetics

$$F(z) \;=\; (r \cdot z) \;\bmod p \qquad \text{(Here, } p \text{ is a prime).}$$

Claim 3: If $r \in [1, p-1]$ was random, then for any $z, i \in [1, p-1]$, we have

$$\text{Prob}\big(F(z) = i\big) = \frac{1}{p-1}.$$

Proof:

Note: z, i are fixed, but r is random.

$F(z) = i \iff rz \pmod p = i \iff r = z^{p-2}\, i \pmod p$

$\text{Prob}_r\big(F(z) = i\big)$

$\text{Prob}_r\big(r = z^{p-2} \cdot i \pmod p\big)$

$= \dfrac{1}{p-1}$

New hash function

$U = [1, M]$ $\qquad$ $S \subseteq U$ of size n

Let p be a prime in range $[M+1, 2M]$

and r be a random value in set $[1, p-1]$.

Then new hash function is

$$H(z) = \left(r \cdot z \ (\text{mod } p) \right) \text{ mod } n$$

Next Lecture: We will see collision probability under new hash function is small.