Cryptography 1/27

Reagan Shirk

January 27, 2020

Congruent Class

- If $m|a-b$, we say that a is congruent to b modulo m
  - $a \equiv b \pmod{m}$
  - $\forall a,\ a \equiv a \pmod{m}$
  - If $a \geq b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
  - If $a \equiv b \pmod{m}, b \geq c \pmod{m} \Rightarrow a \equiv c \pmod{m}$
  - $\mathbb{Z} = m\mathbb{Z} \cup (1 + m\mathbb{Z}) \cup \cdots \cup (m - 1 + m\mathbb{Z})$
    - $a + m\mathbb{Z} = \{a + mi \mid i \in \mathbb{Z}\}$
- Definition:
  - $(a + m\mathbb{Z} + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z})$
  - $(a + m\mathbb{Z} \times (b + m\mathbb{Z}) = (a \times b) + m\mathbb{Z})$
- Ring of congruent classes
  - $(\frac{\mathbb{Z}}{m\mathbb{Z}}, +, \times)$

Group: $(S, \circ)$

- $\forall a, b, c, (a \circ b) \circ c = a \circ (b \circ c)$
- $\exists e s.t. a \circ e = a$
- $\forall a, \exists b, a \circ b = e$
  - Having the first identity = semigroup, first and second identity = monoid, all identities = group
- Ring: $(S, +, \times)$
  - $(S, +)$ group
  - $(S, \times)$ monoid
  - $a \times (b + c) = a \times b + a \times c$
  - Example: $(\mathbb{Z}, +, \times)$ is a ring of integers
  - A field is a ring such that every nonzero element has a multiplicative inverse

Example

- Semigroup: $(2^+, +)$
  - This is a semigroup because it is not a monoid (it has no 0/identity?)
  - To make it a monoid, you need $(2^+ \cup \{0\}, +)$, not a group
  - To make it a group, you need $(\mathbb{Z}, +)$
    - Doing a multiplication here instead of an addition makes it a monoid because inverses...?

Modular Inverse

- Inverse of $\frac{1}{5} (\text{mod} 12) = 5$
- Inverse of $\frac{1}{5} (\text{mod} 13) = 8$
  - Because $5 \times 8 = 40$ and $40 \bmod 13 = 1$
- What if the mod number is really big?

  - You can't quickly calculate the answer by hand, a loop would give you really bad time complexity
  - Instead you do... something
  - $\frac{\mathbb{Z}}{m\mathbb{Z}}, a$ is invertible iff $\gcd(a, m) = 1$
- If $\gcd(a, m) \neq 1$, then a is not invertible
  - Easy proof
- If $\gcd(a, m) = 1$, then a is invertible
  - Proof by extended Euclidean algorithm
    - In polynomial time, we can find x, y such that $ax + my = 1$