Discrete Mathematics

FTA, binary relation, equivalence relation, equivalence class, congruence, mod, floor, ceiling, residue class, $\mathbb{Z}_n$

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

FTA Proof

THEOREM: If $a, b, c \in \mathbb{Z}, c|ab$ and $\gcd(c, a) = 1$, then $c|b$.

- There exist s, t such that $1 = \gcd(a, c) = as + ct$.
  - $b = bas + bct$
  - $c|ab, c|ct \Rightarrow c|(bas + bct) \Rightarrow c|b$

THEOREM: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

- $p|a$: done
- $p \nmid a \Rightarrow \gcd(p, a) = 1$
  - $\gcd(p, a) = 1 \land p|ab \Rightarrow p|b$

Fundamental Theorem of Arithmetic: proof of uniqueness

- Suppose that $n = p_1 \cdots p_r = q_1 \cdots q_s$, where p_i, q_j are all primes
  - $p_1|n \Rightarrow p_1|q_1 \cdots q_s \Rightarrow p_1|q_j$ for some $j \Rightarrow p_1 = q_j$
  - W.l.o.g., we suppose that $j = 1$. Then $p_2 \cdots p_r = q_2 \cdots q_s$
  - The theorem is true by induction.

FTA Applications

THEOREM: Suppose that $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, b = p_1^{\beta_1} \cdots p_r^{\beta_r}$. Then

$$d := p_1^{\min(\{\alpha_1,\beta_1\})} \cdots p_r^{\min(\{\alpha_r,\beta_r\})} = \gcd(a,b)\,.$$

- d is a common divisor of a, b
- d is largest among the common divisors
  - Suppose that d' is a common divisor of a, b
  - $d' = p_1^{e_1} \cdots p_r^{e_r}$
    - $d'|a \Rightarrow e_i \le \alpha_i$ for all $i \in [r]$; $d'|b \Rightarrow e_i \le \beta_i$ for all $i \in [r]$
      - $e_i \le \min\{\alpha_i, \beta_i\}$ for all $i \in [r]$

THEOREM: There are infinitely many primes.

- Suppose there are only n primes: $p_1, \dots, p_n$
- By FTA, $N = p_1 \cdots p_n + 1$ must be a product of primes
- $\exists i \in [n]$ such that $p_i | N$
- But $p_i \nmid N$

Equivalence Relation

DEFINITION: Let A, B be two sets. A **binary relation** from A to B is a subset $R \subseteq A \times B$. // aRb means $(a, b) \in R$

EXAMPLE: $R = \{(a, a): a \in \mathbb{Z}^+\}$ is a binary relation from $\mathbb{Z}^+$ to $\mathbb{Z}^+$

- aRb means that $a = b$; R is "="

DEFINITION: Let A be a set. An **equivalence relation** R on A is a binary relation R from A to A such that

- **Reflexive**: aRa for all $a \in A$
- **Symmetric**: $aRb \Rightarrow bRa$ for all $a, b \in A$
- **Transitive**: $aRb, bRc \Rightarrow aRc$ for all $a, b, c \in A$

DEFINITION: The **equivalence class** of $a \in A$ is the set

$$[a]_R = \{b \in A: aRb\}$$

Equivalence Class

THEOREM: Let R be an equivalence relation on A. For any $a, b \in A$, $[a]_R = [b]_R$ if and only if aRb.

- $\Rightarrow$: $[a]_R = [b]_R \Rightarrow a \in [b]_R \Rightarrow aRb$
- $\Leftarrow$: aRb
  - $\forall x \in [a]_R, xRa$
  - $\forall x \in [a]_R, xRb$
  - $[a]_R \subseteq [b]_R$
  - similarly, $[b]_R \subseteq [a]_R$

THEOREM: Let R be an equivalence relation on A. For any $a, b \in A$, either $[a]_R \cap [b]_R = \emptyset$ or $[a]_R = [b]_R$

- $[a]_R \cap [b]_R = \emptyset$: done
- $[a]_R \cap [b]_R \neq \emptyset$
  - $\exists c \in [a]_R \cap [b]_R$
  - cRa, cRb
  - aRb (i.e., $[a]_R = [b]_R$)

The equivalence classes under R form a partition of A.
Partition: a set $\{A_1, A_2, \dots, A_n\}$ nonempty subsets of A

- $A_i \cap A_j = \emptyset, \forall i \neq j$
- $\cup_{i=1}^{n} A_i = A$

Congruence

THEOREM: Let $n \in \mathbb{Z}^+$. Then $R = \{(a, b) \in \mathbb{Z}^2 : n|(a - b)\}$ is an equivalence relation on $\mathbb{Z}$ (from $\mathbb{Z}$ to $\mathbb{Z}$).

- R is a binary relation from $\mathbb{Z}$ to $\mathbb{Z}$
  - Reflexive: $n|(a - a) \Rightarrow aRa$
  - Symmetric: $aRb \Rightarrow n|(a - b) \Rightarrow n|(b - a) \Rightarrow bRa$
  - Transitive: $aRb, bRc \Rightarrow n|(a - b), n|(b - c) \Rightarrow n|(a - c) \Rightarrow aRc$

DEFINITION: Let $n \in \mathbb{Z}^+$ and $R = \{(a, b) \in \mathbb{Z}^2 : n|(a - b)\}$.

- The notation $\boldsymbol{a \equiv b}$ **(mod** $\boldsymbol{n}$**)** means that aRb.
  - $a \equiv b \pmod{n}$ is called a **congruence**
    - Read as: a is **congruent** to b modulo n
    - n is called the **modulus** of the congruence
  - $\boldsymbol{a \not\equiv b}$ **(mod** $\boldsymbol{n}$**)**: $(a, b) \notin R$, or equivalently $n \nmid (a - b)$
    - Read as: a is not congruent to b modulo n

Congruence

THEOREM: Let $n \in \mathbb{Z}^+$. For any $a \in \mathbb{Z}$, there is a unique integer r such that $0 \le r < n$ and $a \equiv r \pmod{n}$.

- **Existence**: by division algorithm, $\exists\, q, r \in \mathbb{Z}$ s.t. $0 \le r < n, a = qn + r$
  - $a \equiv r \pmod{n}$
- **Uniqueness**: suppose that $0 \le r' < n$ and $a \equiv r' \pmod{n}$
  - $|r - r'| < n$ and $r \equiv r' \pmod{n}$
    - $|r - r'| < n$ and $n | (r - r')$
      - $r = r'$

DEFINITION: Let $a, n \in \mathbb{Z}$ and $n > 0$. Then there are unique integers q, r such that $0 \le r < n$ and $a = nq + r$.

- We define $a \bmod n$ as r.

Residue Class

DEFINITION: Let $\alpha \in \mathbb{R}$.

- $\lfloor \alpha \rfloor$: **floor** of α, the largest integer $\leq \alpha$
- $\lceil \alpha \rceil$: **ceiling** of α, the smallest integer $\geq \alpha$
  - If $a = nq + r$, then $q = \lfloor a/n \rfloor$ and $r = a - nq$

DEFINITION: Let $a \in \mathbb{Z}, n \in \mathbb{Z}^+$. We denote the equivalence class of a under the equivalence relation mod n with $[a]_n$ and call it the **residue class of** a mod n.

- $[a]_n = a + n\mathbb{Z} = \{a + nx : x \in \mathbb{Z}\}$
  - any element of $[a]_n$ is a **representative** of $[a]_n$

EXAMPLE: $[0]_6 = \{0, \pm 6, \pm 12, \dots\}$; $[1]_6 = \{\dots, -11, -5, 1, 7, 13, \dots\}$; ...

THEOREM: Let $n \in \mathbb{Z}^+$. For any $a \in \mathbb{Z}$, there is a unique integer r such that $0 \leq r < n$ and $[a]_n = [r]_n$.

- $r = a \bmod n$

$\mathbb{Z}_n$

COROLLARY: $\{[0]_n, [1]_n, \dots, [n-1]_n\}$ is a partition of $\mathbb{Z}$.

- $\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$
- $[a]_n \cap [b]_n = \emptyset$ for all $a, b \in \{0,1,\dots,n-1\}$

DEFINITION: Let n be any positive integer. We define $\mathbb{Z}_n$ to be set of all residue classes modulo n.

- $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
  - $\mathbb{Z}_n = \{0,1,\dots,n-1\}$;
- $\mathbb{Z}_n = \{[1]_n, [2]_n, \dots, [n]_n\}$
  - $\mathbb{Z}_n = \{1,2,\dots,n\}$

EXAMPLE: Two representations of the set $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$
  $= \{0,1,2,3,4,5\}$
- $\mathbb{Z}_6 = \{[-3]_6, [-2]_6, [-1]_6, [0]_6, [1]_6, [2]_6\}$
  $= \{-3,-2,-1,0,1,2\}$

$\mathbb{Z}_n$

DEFINITION: Let $n \in \mathbb{Z}^+$. For all $[a]_n, [b]_n \in \mathbb{Z}_n$, define

- **addition**: $[a]_n + [b]_n = [a+b]_n$
- **subtraction**: $[a]_n - [b]_n = [a-b]_n$
- **multiplication**: $[a]_n \cdot [b]_n = [a \cdot b]_n$

Well-defined? If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$a \pm b \equiv a' \pm b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

- Hence, $[a]_n \pm [b]_n = [a']_n \pm [b']_n$; $[a]_n \cdot [b]_n = [a']_n \cdot [b']_n$
  - $a \equiv a' \pmod{n} \Rightarrow n | (a - a') \Rightarrow \exists x$ such that $a - a' = nx$
  - $b \equiv b' \pmod{n} \Rightarrow n | (b - b') \Rightarrow \exists y$ such that $b - b' = ny$
    - $(a + b) - (a' + b') = nx + ny$
    - $(a - b) - (a' - b') = nx - ny$
    - $ab - a'b' = a(b - b') + b'(a - a') = any + b'nx$