Lecture 13: Modular Arithmetic

Date: September 27, 2019.

Recap

- For integers a, b, $a \mid b$ iff there is an integer k such that $b = ak$.
- For integers n, d with $d \neq 0$, there exist unique integers $\mathsf{qcnt}(n,d)$ and $\mathsf{rem}(n,d)$ such that $n = \mathsf{qcnt}(n,d)d + \mathsf{rem}(n,d)$. where $0 \leq \mathsf{rem}(n,d) < |d|$
- $\gcd(m,n)$ is the greatest among the common divisors of m and n. Can be computed efficiently using Euclid's algorithm.
- $a \equiv b \pmod{n}$ iff $n \mid (a-b)$. $a \equiv \mathsf{rem}(a,n) \bmod n$.
- $a \equiv b \pmod{n}$ iff $\mathsf{rem}(a,n) = \mathsf{rem}(b,n)$.

Equivalence Relation. A binary relation R on a set A (i.e., $R \subseteq A \times A$) is an **equivalence relation** iff

Reflexive. $\forall a \in A$, $(a,a) \in R$.

Symmetric. $\forall a, b \in A$, $(a,b) \in R$ IMPLIES $(b,a) \in R$

Transitive. $\forall a, b, c \in A$, $[(a,b) \in R$ AND $(b,c) \in R]$ IMPLIES $(a,c) \in R$.

Question 1. For each of the following relations on $\mathbb{N}$, identify whether they are reflexive, symmetric, and/or transitive. (a) $\emptyset$ ST (b) $\mathsf{id} = \{(n,n) \mid n \in \mathbb{N}\}$ RST (c) $\mathbb{N} \times \mathbb{N}$ RST (d) $\leq = \{(n,m) \mid n \leq m\}$ RT

$[n]_{\mathsf{id}} = \{n\}$ $[n]_{\mathbb{N}\times\mathbb{N}} = \mathbb{N}$

Equivalence Classes. For an equivalence relation R on A, and an element $a \in A$, the **equivalence class** of a (w.r.t. R) is

$$[a]_R = \{b \in A \mid (a,b) \in R\}. \qquad [a]_R = R(\{a\})$$

Proposition 1. *Let A be any set, and let R be an arbitrary equivalence relation on A. For any $a, b \in A$, either $[a]_R \cap [b]_R = \emptyset$ or $[a]_R = [b]_R$.*

$A = B$: $A \subseteq B$ and $B \subseteq A$ iff $\forall x \in A$ iff $x \in B$.

$[a]_R \cap [b]_R \neq \emptyset$ IMPLIES $[a]_R = [b]_R$

$[a]_R \cap [b]_R = \emptyset$ OR $[a]_R = [b]_R$

Let fix R, $a, b \in A$.

Assume $[a]_R \cap [b]_R \neq \emptyset$

$\exists c$. $(a,c) \in R$ and $(b,c) \in R$.

$[a]_R \subseteq [b]_R$: Consider $d \in [a]_R$ i.e $(a,d) \in R$

Since R is symmetric, $(d,a) \in R$

Since R is transitive (d,c)

Since R is symmetric $(c,b) \in R$

Since R is transitive $(d,b) \in R$.

Since R is symmetric $(b,d) \in R$

$\Rightarrow d \in [b]_R$. $[b]_R \subseteq [a]_R$ by the same reason.

Proposition 2. *For any $n \in \mathbb{Z}$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

$\forall a, b, c$.

$a \equiv a \pmod{n}$ | $n \mid a - a$ i.e $n \mid 0$

$a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ | $n \mid a-b$ then $n \mid b-a$

$a \equiv b \pmod{n}$ AND $b \equiv c \pmod{n}$ IMPLIES $a \equiv c \pmod{n}$

$n \mid (a-b)$, $n \mid (b-c)$ then $n \mid (a-b)+(b-c) \Rightarrow n \mid a-c \Rightarrow a \equiv c \pmod{n}$

Proposition 3. *For any integer n, congruence modulo n is a "congruence", i.e. if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then*

$$a + c \equiv b + d \pmod{n}$$
$$ac \equiv bd \pmod{n}$$

$n \mid a-b$, $n \mid c-d$, $(a+c)-(b+d) = (a-b)+(c-d)$

$n \mid (a-b)+(c-d) \Rightarrow n \mid (a+c)-(b+d) \Rightarrow a+c \equiv b+d \pmod{n}$

Remainder Arithmetic. To find the remainder on division by n of the result of a series of additions and multiplications, applied to some integers

- replace each integer operand by its remainder on division by n
- replace the result of each operation, by the remainder on division by n

Question 2. What is the remainder when $((4427)(173000) + 92567 + 3006^{23556})$ is divided by 7?

$\text{rem}(e,7) = (3(2) + 6 + 3^{23556} \bmod 7 = \text{rem}(5 + 3^{23556} \bmod 7, 7) \equiv (5+1) \bmod 7$

$\equiv 6 \bmod 7$

$3^0 \equiv 1 \bmod 7$ $3^1 \equiv 3 \bmod 7$ $3^2 \equiv 2 \bmod 7$ $3^3 \equiv 6 \bmod 7$ $3^4 \equiv 4 \bmod 7$ $3^5 \equiv 5 \bmod 7$ $3^6 \equiv 1 \bmod 7$

Extended GCD Algorithm

Theorem 4 (Bézout). *For any integers a, b, $\gcd(a,b)$ is a linear combination of a and b, i.e., there are integers s, t such that $\gcd(a,b) = sa + tb$.*

To compute $\gcd(a,b)$, we can assume WLOG a, b are positive, and $a \geq b$.

```
gcd(a,b)
    x = a; y = b;


    while (y > 0)

        r = rem(x,y)
        x = y
        y = r



    return x
```