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 $n = \mathsf{qcnt}(n, d)d + \mathsf{rem}(n, d)$.
- $\gcd(m, n)$ 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 $n \mid (a - b)$.
- $a \equiv b \pmod{n}$ 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) $\emptyset$ (b) $\mathsf{id} = \{(n, n) \mid n \in \mathbb{N}\}$ (c) $\mathbb{N} \times \mathbb{N}$ (d) $\leq = \{(n, m) \mid n \leq m\}$

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

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

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 $[a]_R = [b]_R$.*

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

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*

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

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?

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
```