Honors Discrete Mathematics: Lecture 14 Notes

Gerandy Brito Spring 2022

Sarthak Mohanty

TA Remark. It's only Monday and I'm already tired :(

Division

Definition. We said d is the greatest common divisor of a and b (notation: $d = \gcd(a, b)$) if $d \mid a$, $d \mid b$, and d is the largest integer with these properties.

Lemma. Let $a \geq b > 0$. Then $\gcd(a, b) = gcd(a - b, b)$.

Proof. Set $d = \gcd(a, b)$ and $\hat{d} = \gcd(a - b, b)$

1. We will show first that $d \leq \hat{d}$. $d \mid a$ and $d \mid b$ by definition of d . Then $d \mid a - b$ and d is a common divisor of $a - b$ and b. $d \leq \hat{d}$ by definition of $\hat{d}$.
2. Now we show that $\hat{d} \leq d$. $\hat{d} \mid a - b$ and $\hat{d} \mid b$ by definition. Then $\hat{d} \mid ((a - b) + b)$. $\hat{d}$ is also a common divisor of a and b, implying $d \hat{\leq} d$ by definition.

Note the same proof leads to $\gcd(a, b) = \gcd(a - b, a)$.

$$\begin{aligned}
\gcd(a, b) &= \gcd(a - b, b) \\
&= \gcd(a - 2b, b) \\
&= \gcd(a - 3b, b) \\
&\vdots \\
&= \gcd(a - qb, b)
\end{aligned}$$

Reminder. We said d divides a if $\exists q \in \mathbb{Z}$ such that $a = qd$.

Claim. Let $a, d \in \mathbb{N}$. There exists a unique pair $(q, r) \in \mathbb{N}$ such that:

- $0 \leq r \leq d - 1$
- $a = q \cdot d + r$.

Proof of Claim.

- Existence: Follows from long division.
- Uniqueness: Assume $\exists (q, r)$ and $\exists (q', r')$ such that $a = q \cdot d + r$ and $a = q'd + r'$ and $0 \leq r, r' \leq d - 1$. We have $a = q \cdot d + r = q' \cdot d + r'$. Rearranging, we get $d(q - q') = r' - r < d$ (More precisely: $|r - r'| < d$). Thus, equality only holds if $q - q' = 0$ OR $q = q'$ and $r - r' = 0$ OR $r = r'$.

We now devise a procedure for finding the greatest common divisor, known as the Euclidean algorithm.

Initialization. Set $a_1 = a$ and $b_1 = b$.

Inductive Step. Set $a_i = b_{i-1}$, and set $b_i = a - qb$. Repeat this step, incrementing i in each iteration, until $i = n$ such that b_n is set equal to 0.

Termination. Return $\gcd(a, b)$, given by a_n.

Definition. Consider $\mathcal{R}_m$ to be the equivalence relation over $\mathbb{Z}$:

$a\mathcal{R}_m b$ if the remainder of a when divided by m equals remainder of b when divided by m.

With this equivalence relation, we can partition the elements in $\mathbb{Z}$ int he form $[0], [1], [2], \ldots, [m - 1]$.

TA Remark. . These equivalency classes are known as congruency classes.

Definition. $\mathbb{Z}_m$ is the set of equivalence classes of $\mathcal{R}_m (|\mathbb{Z}_m| = m)$.

Notation:

- Elements in $\mathbb{Z}_m$ are denoted by $\bar{a}$.
- $r = \min\{x \geq 0 \text{ in each equivalence class}\}$ is the representative of the class.
- $a\mathcal{R}_m$ is denoted as $a \equiv b \pmod{m}$.

Examples. $m = 4$.
Then $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ where $\bar{0} = \{-12, -8, -4, 0, 4, 8, 12, \dots\}$ and $\bar{1} = \{-11, -7, -3, 1, 5, 9, 12, 17, \dots\}$.
Operations on $\mathbb{Z}_m$. (Used on homework)

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} + \bar{b} = \overline{a \cdot b}$

In $\mathbb{Z}_4$:

- $\bar{1} + \bar{2} = \bar{3}$
- $\bar{6} + \bar{8} = \bar{1}4 \sim \bar{2} + \bar{0} = \bar{2}$
- $\bar{1} + \bar{3} = \bar{0}$
- $\bar{2} + \bar{3} = \bar{1}$.

Post Lecture

Question 1

Let $m, a_1, b_1, a_2, b_2 \in \mathbb{Z}$. Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

(a) Prove that $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

(b) Prove that $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(c) Prove that $a^k \equiv b^k \pmod{m}$ for any $k \in \mathbb{N}$.

Solution

(a) Since $m \mid b_1 - a_1$ and $m \mid b_2 - a_2$, we know $m \mid (b_1 - a_1) + (b_2 - b_1)$; rearranging, we find that $m \mid (b_1 + b_2) - (a_1 + a_2)$, so $b_1 + b_2 \equiv a_1 + a_2 \pmod{m}$.

(b) Since $m \mid b_1 - a_1$, it follows that $m \mid b_2(b_1 - a_1)$. Since $m \mid b_2 - a_2$, it follows that $m \mid a_1(b_2 - a_2)$. Then $m \mid [b_2(b_1 - a_1) + a_1(b_2 - a_2)]$; simplifying, we find that $m \mid b_1 b_2 - a_1 a_2$, so $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(c) Let $P(n)$ be the sentence

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}.$$

Base Case: $P(1)$ is true, since $a \equiv b \pmod{m} \Rightarrow a^1 \equiv b^1 \pmod{m}$ is always true.
Inductive Step: Now let $n \in \mathbb{N}$ such that $P(n)$ is true. Then since $a \equiv b \pmod{m}$ and $a^n \equiv b^n \pmod{m}$, we know $a(a^n) \equiv b(b^n) \pmod{m}$, or equivalently, $a^{n+1} \equiv b^{n+1} \pmod{m}$. Hence $P(n+1)$ is true as well.
Conclusion: We have proved by induction that for each $n \in \mathbb{N}$, $P(n)$ is true.