Summary Midterm 1

February 12, 2023 13:08

4.1 Divisibility

$a \mid b \leftrightarrow \exists c$ such that $b = ac$

+ Theorems

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$:

- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
  - We also have $a \mid (mb + nc)\ \forall m, n \in \mathbb{Z}$
- If $a \mid b$, then $a \mid bc \quad \forall c \in \mathbb{Z}$
- If $a \mid b$ and $b \mid c$, then $a \mid c$

4.2 Division Algorithm

Let $a, d \in \mathbb{Z}$ with $d > 0$
$\exists!\, q, r \in \mathbb{Z}$ such that $a = dq + r$ for $0 \leq r < d$

<u>Notation:</u> If $a = dq + r$ for $0 \leq r < d$, we write:

- $q = a \text{ div } d$
- $r = a \bmod d$

4.3 Modulo

Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. a is congruent to b modulo m if $m \mid (a - b)$, and we denote it as $a \equiv b \pmod{m}$

Note: $a \equiv b \pmod{m} \leftrightarrow b \equiv a \pmod{m}$

+ Theorems

- Let $a, b, c, d, m \in \mathbb{Z}$ with $m \geq 2$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$

- $a + c \equiv b + c \pmod{m} \rightarrow a \equiv b \pmod{m}$
- $c \not\equiv 0 \pmod{m}, ac \equiv bc \pmod{m} \nrightarrow a \equiv b \pmod{m}$

4.4 Arithmetic Modulo

For $m \geq 2$, define $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$
$a +_m b = (a + b) \pmod{m}$
$a \cdot_m b = (a \cdot b) \pmod{m}$

5.1 Prime Numbers

$p \in \mathbb{Z}$ is prime if it has exactly two divisors, 1 and itself

5.2 Fundamental Theorem of Arithmetic

All integers greater than 1 can be written as a unique product of prime numbers

+ Theorems

- For $n \in \mathbb{Z}$ such that $n > 1$. If n is not prime, then n has a prime divisor p such that $p \leq \sqrt{n}$
- There exists an infinite number of prime numbers

5.3 Greatest Common Divisor

For $a, b \in \mathbb{Z}$ such that $a \neq 0$ or $b \neq 0$
The greatest integer d such that $d \mid a$ and $d \mid b$ is the GCD of a and b

a, b are coprime if $\text{GCD}(a, b) = 1$

5.4 Least Common Divisor

For $a, b \in \mathbb{Z}$ such that $a \neq 0$ and $b \neq 0$
The least integer m such that $a \mid m$ and $b \mid m$ is the LCM of a and b

+ Theorems

- For $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ where p_i are prime numbers and $a_i > 0$ are integers and for $d \in \mathbb{Z}$
  Then $d \mid n \leftrightarrow d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ where $0 \leq b_i \leq a_i$

- For $\begin{cases} a = p_1^{a_1} \dots p_k^{a_k} \\ b = p_1^{b_1} \dots p_k^{b_k} \end{cases}$ with p_i primes and $a_i, b_i \geq 0$:
  - $\text{GCD}(a, b) = p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)}$
  - $\text{LCM}(a, b) = p_1^{\max(a_1, b_1)} \dots p_k^{\max(a_k, b_k)}$

- $\text{GCD}(a, b) \times \text{LCM}(a, b) = a \times b$

- For $a, b, q, r \in \mathbb{Z}$ such that $a = bq + r$, then $\text{GCD}(a, b) = \text{GCD}(b, r)$

6.1 Euclid's Algorithm

$$
\begin{aligned}
a &= q_1 \times b + r_1 \\
b &= q_2 \times r_1 + r_2 \\
r_1 &= q_3 \times r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + r_{n+1}
\end{aligned}
$$

And $\text{GCD}(a, b) = r_n$ when $r_{n+1} = 0$

6.2 Bezout's Algorithm

For $a, b \in \mathbb{Z}$ and $a, b > 0$, then there exists $s, t \in \mathbb{Z}$ such that $sa + tb = \text{GCD}(a, b)$

We run Euclid's algorithm backwards:
$\text{GCD}(a, b) = r_n = r_{n-2} - q_{n-1} \times r_{n-2} = \dots = sa + tb$

+ Example of Euclid and Bezout

Run Euclid first for GCD(662,414)
a: $662 = 1 \times 414 + 248$
b: $414 = 1 \times 248 + 166$
c: $248 = 1 \times 166 + 82$
d: $166 = 2 \times 82 + 2$
e: $82 = 41 \times 2 + 0$

So $\mathrm{GCD}(662, 414) = 2$

Run Bezout now:
$2 = 166 - 2 \times 82$ from d
$= 166 - 2(248 - 1 \times 166)$ from c
$= -2 \times 248 + 3 \times 166$ simple rearranging
$= -2 \times 248 + 3(414 - 1 \times 248)$ from b
$= 3 \times 414 - 5 \times 248$ simple rearranging
$= 3 \times 414 - 5(662 - 1 \times 414)$ from a
$= 8 \times 414 - 5 \times 662$ simple rearranging
$= -5 \times 662 + 8 \times 414$

So $-5 \times 662 + 8 \times 414 = 2 = \mathrm{GCD}(662, 414)$

+ Theorems

- For $a, b, c \in \mathbb{Z}$ with $a \neq 0$
  If $\mathrm{GCD}(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$

- For $a, b, m \in \mathbb{Z}$ with $a > 0$ and $b > 0$
  There exists $s, t \in \mathbb{Z}$ such that $sa + tb = m \leftrightarrow \mathrm{GCD}(a, b) \mid m$

- For $a, b, c, m \in \mathbb{Z}$ with $m \geq 2$
  If $ac \equiv bc \pmod{m}$ and $\mathrm{GCD}(c, m) = 1$, then $a \equiv b \pmod{m}$

- For p, a prime number and $a_1, \dots, a_n \in \mathbb{Z}$
  If $p \mid (a_1 \times \cdots \times a_n)$, then $\exists\ 1 \leq i \leq n$ such that $p \mid a_i$

- For $m \in \mathbb{Z}$ with $m \geq 2$ and $a \in \mathbb{Z}_m$
  The multiplicative inverse of $a \pmod{m}$ exists if and only if $\mathrm{GCD}(a, m) = 1$. It's unique when it exists