CSI 2101 Lecture Notes

Mohamed Shakir

February 27, 2023

Contents

Definitions, Theorems, Lemmas, and Corollaries

Definition 4.1.1. *Let a and b be two integers such that $a \neq 0$. We say that a divides b if there exists c such that $b = ac$. If a divides be we say a is a factor or divisor of b. We also can say b is a multiple of a.*

Theorem 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$.*

1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$*
2. *If $a \mid b$, then $a \mid bc$ for every integer*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$*

Corollary 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$ and $a \mid c$, $a \mid (mb + nc)$ for all integers m and n*

Theorem 4.1.2 (The Division Algorithm)**.** *Let $a, d \in \mathbb{Z}$ with $d > 0$. There exists a unique q and r such that*

$$0 \leq r \leq d$$

and

$$a = dq + r$$

We write

$$q = a \ div \ d$$

$$r = a \ mod \ a$$

Definition 4.1.2. *Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. We say a is congruent to b modulo m if $m \mid (a - b)$. We write $a \equiv b \ (mod \ m)$*

Theorem 4.1.3. *Let $a, b, c, d, m \in \mathbb{Z}$ with $m \geq 2$. If $a \equiv b \ (mod \ m)$ and $c \equiv d \ (mod \ m)$, then*

1. *$a + c \equiv b + d \ (mod \ m)$*
2. *$ac \equiv bd \ (mod \ m)$*

Definition 5.1.1. *A positive integer p is prime if it admits exactly two divisors.*

Theorem 5.1.1 (Fundamental Theorem of Arithmetic)**.** *All integers greater than 1 can be written as a product of prime numbers. This representation is unique if we write the prime numbers in non-decreasing order.*

Theorem 5.1.2. *Let $n > 1$ be an integer. If n is not prime, then n has a prime divisor p such that $p \leq \sqrt{n}$.*

Corollary 6.0.1. *Let*

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

$$a = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_k^{b_k}$$

Where p_i is prime, $a_i \geq 0$ and $b_i \geq 0$, $1 \leq i \leq k$. Then

$$gcd(a, b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)}$$

$$lcm(a, b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)}$$

$$gcd(a, b) \cdot lcm(a, b) = ab$$

Lemma 6.0.1. *Let a, b, q, r be integers such that*

$$a = b \cdot q + r$$

Then

$$gcd(a, b) = gcd(b, r)$$

Definition 6.0.1 (Euclidean Algorithm)**.**

$$x = a$$

$$y = b$$

while $y \neq 0$

$$r = x \mod y$$

$$x = y$$

$$y = r$$

return x

Theorem 6.0.1 (Bézout)**.** *Let $a, b \in \mathbb{Z}$ be positive integers. There exists $s, t \in \mathbb{Z}$ such that*

$$s \cdot a + t \cdot b = gcd(a, b)$$

Lemma 6.0.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $gcd(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$.*

Lemma 8.0.1. *Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. If $gcd(a, b) = 1$, and $a \mid (bc)$, then $a|c$.*

Theorem 8.0.1. *Let $a, b, c, m \in \mathbb{Z}$, with $m \geq 2$. Assume $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$. Then $a \equiv b \pmod{m}$.*

Lemma 8.0.2. *Let p be a prime number and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 \cdot a_2 \cdot \cdots \cdot a_n)$, then there exists $1 \leq i \leq n$ such that $p \mid a_i$.*

Theorem 8.0.2. *Let $m \in \mathbb{Z}$ with $m \geq 2$ and let $a \in \mathbb{Z}_m$. The multiplicative inverse of $a \pmod{n}$ exists if and only if $gcd(a, m) = 1$. When it exists, the inverse of $a \pmod{n}$ is unique.*

Lecture 1

Logic and Proof Techniques

TBC.

Lecture 2

Proof Examples

TBC.

Lecture 3

Proof by Induction and More Examples

Lecture 4

Intro to Number Theory

4.1 Divisibility

Definition 4.1.1. *Let a and b be two integers such that $a \neq 0$. We say that a divides b if there exists c such that $b = ac$. If a divides be we say a is a factor or divisor of b. We also can say b is a multiple of a.*

Theorem 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$.*

1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$*
2. *If $a \mid b$, then $a \mid bc$ for every integer*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$*

Proof.

1. We have to prove if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Assume that $a \mid b$ and $a \mid c$, then for some $k, l \in \mathbb{Z}$

$$b = k \cdot a$$

$$c = l \cdot a$$

Thus, we have

$$b + c = k \cdot a + l \cdot a = a(k + l)$$

So $a \mid (b + c)$

2. We have to prove if $a \mid b$, $a \mid bc$ for every c. Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Assume that $a \mid b$. Then for some $k \in \mathbb{Z}$,

$$b = k \cdot a$$

Let $c \in \mathbb{Z}$, so

$$bc = k \cdot a \cdot c = a \cdot (kc)$$

Therefore, $a \mid bc$

3. We have to prove if $a \mid b$ and $b \mid c$, then $a \mid c$. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Assume $a \mid b$ and $b \mid c$. Then we have for some $k, l \in \mathbb{Z}$

$$b = k \cdot a$$

$$c = l \cdot b$$

So,

$$c = l \cdot b = l \cdot (k \cdot a) = (lk)a$$

Therefore $a \mid c$

$\square$

Corollary 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$ and $a \mid c$, $a \mid (mb + nc)$ for all integers m and n*

Proof. Let $a, bc \in \mathbb{Z}$ with $a \neq 0$. Assume $a \mid b$ $a \mid c$. By the previous theorem (part 2), we have $a \mid mb$ and $a \mid nc$. Therefore, by the previous theorem (part 1), $a \mid (mb + nc)$ $\square$

Theorem 4.1.2 (The Division Algorithm)**.** *Let $a, d \in \mathbb{Z}$ with $d > 0$. There exists a unique q and r such that*

$$0 \leq r \leq d$$

and

$$a = dq + r$$

We write

$$q = a \ div \ d$$

$$r = a \ mod \ a$$

Definition 4.1.2. *Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. We say a is congruent to b modulo m if $m \mid (a - b)$. We write $a \equiv b$ $(mod \ m)$*

Example: Prove or disprove. We have $a \equiv b$ $(mod \ m)$ if and only if $b \equiv a$ $(mod \ m)$

$$\begin{aligned}
& a \equiv b \ (mod \ m) \\
\iff & m \mid (a - b) && \text{(by definition)} \\
\iff & a - b = km && (k \in \mathbb{Z}) \\
\iff & b - a = -km \\
\iff & m \mid (b - a) \\
\iff & b \equiv a \ (mod \ b) && \text{(by definition)}
\end{aligned}$$

Theorem 4.1.3. *Let $a, b, c, d, m \in \mathbb{Z}$ with $m \geq 2$. If $a \equiv b$ $(mod \ m)$ and $c \equiv d$ $(mod \ m)$, then*

1. $a + c \equiv b + d$ $(mod \ m)$

2. $ac \equiv bd \ (mod\ m)$

Proof. 1. We have to prove $a + c \equiv b + d \ (mod\ m)$. Since $a \equiv b$ and $c \equiv d$, we have

$$m \mid (a - b)$$

$$m \mid (c - c)$$

By theorem 4.1.1 (part 1),we have

$$m \mid ((a - b) + (c - d)$$

$$m \mid ((a + c) - (b + d))$$

Therefore,

$$a + c \equiv b + d \ (mod\ m)$$

2. We have to prove $ac \equiv cd \ (mod\ m)$

Since $a \equiv b$ and $c \equiv d$, we have $m \mid (a - b)$ and $m \mid (c - d)$. By Corollary 4.1.1, we have

$$m \mid (c(a - b) + b(c - d)$$

$$m \mid (ac - bc + bc - bd)$$

$$m \mid (ac - bd)$$

Therefore $ac \equiv bd$.

□

4.2 Arithmetic Modulo m

Let $m \geq 2$ be an integer and

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$$

We define

$$a +_m b = (a + b) \ (mod\ m)$$

$$a \cdot_m b = (a \cdot b) \ (mod\ m)$$

in $\mathbb{Z}_m$, this is arithmetic modulo m. TBC

Lecture 5

Prime Numbers and GCD

5.1 Prime Numbers

Definition 5.1.1. *A positive integer p is prime if it admits exactly two divisors.*

Theorem 5.1.1 (Fundamental Theorem of Arithmetic)**.** *All integers greater than 1 can be written as a product of prime numbers. This representation is unique if we write the prime numbers in non-decreasing order.*

Proof. **(Existence)** By induction,

- **Base Case:** Take $n = 2$. We have $2 = 2$, the product of 1 prime number.
- **Induction Hypothesis:** Let $k \geq 2$ be an integer. Suppose that all numbers $2, 3, 4, \ldots, k-1, k$ can be written as a product of primes.
- **Induction Step:** Consider $k + 1$. If $k + 1$ is prime, then we're done. If not, then $K + 1 = d \cdot e$ for integers $1 < d < k + 1$ and $1 < e < k + 1$ By the induction hypothesis, d and e can be written as products of prime. So $k + 1 = d \cdot e$ can be written as a product of primes.

(Uniqueness) to be seen later. □

Theorem 5.1.2. *Let $n > 1$ be an integer. If n is not prime, then n has a prime divisor p such that $p \leq \sqrt{n}$.*

Proof. Let $n > 1$, if n is not prime, then $n = a \cdot b$ for two integers $1 < a < n$ and $1 < b < n$. We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ by contradiction. Assume $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. This is a contradiction so $a \leq \sqrt{n}$.

Assume without loss of generality that $a \leq \sqrt{n}$. If a is prime, we're done. If not, then by the fundamental theorem of arithmetic, a is divisible by a prime number p □

Theorem 5.1.3. *There exists an infinite number of prime numbers.*

Proof. By contradiction, suppose there exists a finite number of prime numbers, say k prime numbers, and we order them

$$p_1 < p_2 < p_3 < \cdots < p_k$$

Consider the number

$$Q = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1 \in \mathbb{Z}$$

Since $Q > p_k$, then Q is not prime by our assumption. By Theorem 5.1.2, Q is divisible by a prime number. So $p_i \mid Q$ for some $1 \leq i \leq k$. We also have that

$$p_i \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_i \cdot \ldots \cdot p_k)$$

By Corollary 4.1.1, we get

$$p_i \mid (Q - p_1 \cdot p_2 \cdot \ldots \cdot p_k)$$

$p_i \mid 1$ Therefore $p_i = 1$, this is a contradiction since we assumed p_k is the largest prime but $Q > p_k$ is prime. $\square$

Lecture 6

Euclidean Algoirthm and Bézout's Theorem

Corollary 6.0.1. *Let*

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$
$$a = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_k^{b_k}$$

Where p_i is prime, $a_i \geq 0$ and $b_i \geq 0$, $1 \leq i \leq k$. Then

$$gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)}$$

$$lcm(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)}$$

$$gcd(a,b) \cdot lcm(a,b) = ab$$

Example:

$$24 = 2^3 \cdot 3$$
$$36 = 2^2 \cdot 3^2$$
$$gcd(24,36) = 2^2 \cdot 3^1 = 12$$
$$lcm(24,36) = 2^3 \cdot 3^2 = 72$$
$$12 \cdot 72 = 864 = 24 \cdot 36$$

Lemma 6.0.1. *Let a, b, q, r be integers such that*

$$a = b \cdot q + r$$

Then

$$gcd(a,b) = gcd(b,r)$$

Proof. Let a, b, q, r be integers such that

$$a = bq + r$$

Let $d \in \mathbb{Z}$. We will prove that

$$d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$$

$(\implies)$ Let $d \in \mathbb{Z}$. Assume $d \mid a$ and $d \mid b$. Then $d \mid (1 \cdot a + (-q) \cdot b)$, by Corollary 4.1.1. Then $a = bq + r \implies r = a - bq$, so $d \mid (1 \cdot a + (-q) \cdot b) \implies d \mid r$.

$(\impliedby)$ Let $d \in \mathbb{Z}$. Assume $d \mid b$ and $d \mid r$. Then $d \mid (q \cdot b + 1 \cdot r)$ by Corollary 4.1.1. Then $d \mid a$, therefore $d \mid a$ and $d \mid b$ $\square$

Example: $gcd(414, 662)$, $662 = 1 \cdot 414 + 248$

$$\begin{aligned} 662 &= 1 \cdot 414 + 248 \\ 414 &= 1 \cdot 248 + 166 \\ 248 &= 1 \cdot 166 + 82 \\ 166 &= 2 \cdot 82 + 2 \\ 82 &= 41 \cdot 2 + 0 \end{aligned}$$

The last none-zero remainder of this sequence is the gcd of 414 and 662 by the previous lemma. (can someone find which lemma this is!)

Definition 6.0.1 (Euclidean Algorithm)**.**

$$x = a$$

$$y = b$$

while $y \neq 0$

$$r = x \mod y$$

$$x = y$$

$$y = r$$

return x

This algorithm returns the gcd of a and b.

Example:$gcd(465, 144)$

$$\begin{aligned} 465 &= 3 \cdot 144 + 33 \\ 144 &= 4 \cdot 33 + 12 \\ 33 &= 2 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Therefore $gcd(465, 144) = 3$.

Note: When you show the trace of Euclid's algorithm, you must include the last line with a remainder of 0.

Theorem 6.0.1 (Bézout)**.** *Let $a, b \in \mathbb{Z}$ be positive integers. There exists $s, t \in \mathbb{Z}$ such that*

$$s \cdot a + t \cdot b = gcd(a, b)$$

Proof. Let $a, b \in \mathbb{N} \setminus \{0\}$. Run Euclidian algorithm, and assume without loss of generality $b \leq a$.

$$\begin{aligned}
a &= q \cdot b + r \\
r_0 &= q_1 \cdot r_1 + r_2 \\
r_1 &= q_2 \cdot r^2 + r_3 \\
r_2 &= q_3 \cdot r_3 + r_4 \\
&\vdots \\
r_{n-3} &= q_{n-2} \cdot r_{n-2} + r_{n-1} \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n \\
r_{n-1} &= q_n \cdot r_n + 0
\end{aligned}$$

Then, we have

$$\begin{aligned}
gcd(a, b) &= r_n \\
&= r_{n-2} - q_{n-1} \cdot r_{n-1} \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2}r_{n-2}) \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2}r_{n-2}) \\
&= -q_{n-1} \cdot +(1 + q_{n-2}q_{n-1}) \cdot r_{n-2} \\
&\vdots \\
&= s \cdot r_0 + t \cdot r_1 \\
&= s \cdot a + t \cdot tb
\end{aligned}$$

So we read the trace of Euclid's algorithm backward while keeping $gcd(a, b)$ on the same side of the equality. □

TBC.

Lemma 6.0.2. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $gcd(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$.*

Proof. Assume $gcd(a, b) = 1$ and $a \mid (bc)$. By Bézout, there exist $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot b = gcd(a, b) = 1$$

$$s \cdot a \cdot c + t \cdot b \cdot c = c \qquad (*)$$

Since $a \mid a$ and $a \mid (bc)$, we have

$$a \mid (s \cdot c \cdot a + t \cdot b \cdot c$$

By Corollary 4.1.1. Then from (*), this means

$$a \mid c$$

$\square$

Lecture 7

Applications of Bézout's Theorem

TBC.

Lecture 8

GCD and Modulo n, Multiplicative Inverses in Modulo n

Lemma 8.0.1. *Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. If $gcd(a, b) = 1$, and $a \mid (bc)$, then $a|c$.*

Proof. Seen last week. $\square$

Theorem 8.0.1. *Let $a, b, c, m \in \mathbb{Z}$, with $m \geq 2$. Assume $ac \equiv bc \ (mod\ m)$ and $gcd(c, m) = 1$. Then $a \equiv b \ (mod\ m)$.*

Proof. Let $a, b, c, m \in \mathbb{Z}$ with $m \geq 2$. Assume $ac \equiv bc \ (mod\ m)$ and $gcd(c, m) = 1$.

$$\begin{aligned} m &\mid (ac - bc) && \text{(def of mod)} \\ m &\mid (c(a - b)) && \\ m &\mid (a - b) && \text{(by previous lemma)} \\ a &\equiv b \ (mod\ m) && \text{(def of mod)} \end{aligned}$$

$\square$

Lemma 8.0.2. *Let p be a prime number and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 \cdot a_2 \cdot \cdots \cdot a_n)$, then there exists $1 \leq i \leq n$ such that $p \mid a_i$.*

Proof. By induction on n.

- **Base Case:** $n = 1$. Let p be a prime number, if $p \mid a_1$, then $p \mid a_1$
- **Induction Hypothesis:** Let $k \geq 1$ be an integer. Suppose that for all integers $a_1, a_2, \ldots, a_k$

$$p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_k) \implies \exists 1 \leq i \leq k \ s.t\ p \mid a_i$$

If $p \mid a_{k+1}$, then we're done. If not, then

$$gcd(p, a_{k+1}) = 1$$

So $p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_k)$ by the previous lemma. By the induction hypthesis, ther exists $1 \leq i \leq k$ such that $p \mid a_i$.

Induction Step: Suppose

$$p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot a_{k+1})$$

$\square$

Theorem 8.0.2. *Let $m \in \mathbb{Z}$ with $m \geq 2$ and let $a \in \mathbb{Z}_m$. The multiplicative inverse of a $(mod\ n)$ exists if and only if $gcd(a, m) = 1$. When it exists, the inverse of a $(mod\ n)$ is unique.*

Proof. Let $m \in \mathbb{Z}$ with $m \geq 2$ and $a \in \mathbb{Z}_m$

($\Longrightarrow$): Assume the multiplicative inverse of a $(mod\ n)$ exists. Let $\bar{a}$ be this inverse. By definition,

$$\begin{aligned} a \cdot \bar{a} &\equiv 1\ (mod\ m) \\ m &\mid (a \cdot \bar{a} - 1) && \text{(def. of modulo)} \end{aligned}$$

Then, $a \cdot \bar{a} - 1 = k \cdot m$ for some $m \in \mathbb{Z}$. Let $d = gcd(a, m)$ Then $d|a$ and $d|m$. By a result seen in class,

$$\begin{aligned} &d \mid (\bar{a} \cdot a + (-k)m) \\ &d \mid 1 \end{aligned}$$

So, $d = 1$

($\Longleftarrow$): Assume $gcd(a, m) = 1$. By Bézout, there exists $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot m = gcd(a, m) = 1$$

$$\begin{aligned} s \cdot a + t \cdot m &\equiv 1\ (mod\ m) \\ s \cdot a + t \cdot 0 &\equiv 1\ (mod\ m) \\ s \cdot a &\equiv 1\ (mod\ m) \end{aligned}$$

So, we can take $\bar{a} \equiv s$ $(mod\ m)$

(Uniqueness): Consider two arbitrary multiplicative inverses of a $(mod\ m)$. Denote them by, $s, s' \in \mathbb{Z}_m$. So by definition

$$sa \equiv 1\ (mod\ m) \text{ and } s'a \equiv 1\ (mod\ m)$$

Then $gcd(a, m) = 1$ by the previous proof, also we have

$$\begin{aligned}
sa &\equiv s'a \ (mod\ m) && \\
m &\mid (sa - s'a) && \text{(def. of modulo)} \\
m &\mid (a(s - s')) && \\
m &\mid (s - s') && \text{(since } gcd(a, m) = 1\text{)} \\
s &\equiv s' \ (mod\ m) && \text{(def. of modulo)}
\end{aligned}$$

Therefore, s and s' are the same in $\mathbb{Z}_m$. □

Example: Find the multiplicative inverse of 101 (mod 4620).

Euclid:

$$\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Bézout:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (23 - 7 \cdot 3) \\
1 &= 3 - 1 \cdot 23 + 7 \cdot 3 \\
1 &= 8 \cdot 3 - 1 \cdot 23 \\
1 &= -1 \cdot 23 + 8 \cdot 3 \\
1 &= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) \\
1 &= -1 \cdot 23 + 8 \cdot 26 - 8 \cdot 23 \\
1 &= -9 \cdot 23 + 8 \cdot 26 \\
1 &= 8 \cdot 26 - 9 \cdot 23 \\
1 &= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) \\
1 &= 8 \cdot 26 - 9 \cdot 75 + 18 \cdot 26 \\
1 &= -9 \cdot 75 + 26 \cdot 26 \\
1 &= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) \\
1 &= -9 \cdot 75 + 26 \cdot 101 - 26 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\
1 &= 26 \cdot 101 - 35 \cdot 4620 + 1575 \cdot 21 \\
1 &= -35 \cdot 4620 + 1601 \cdot 101
\end{aligned}$$

So,

$$
\begin{aligned}
-35 \cdot 4620 + 1601 \cdot 101 &\equiv 1 \ (mod\ 4620) \\
-35 \cdot 0 + 1601 \cdot 101 &\equiv 1 \ (mod\ 4620) \\
1601 \cdot 101 &\equiv 1 \ (mod\ 4620) \\
\overline{101} &\equiv 1601 \ (mod\ 4620)
\end{aligned}
$$

Therefore, the inverse of 101 in $\mathbb{Z}_{4620}$ is 1601.

Example: Find the multiplicative inverses in $\mathbb{Z}_{10}$.

- $\bar{0}$ does not exist since $gcd(0, 10) = 10 \neq 1$
- $\bar{1} \equiv 1 \ (mod\ 10)$
- $\bar{2}$ does not exist since $gcd(2, 10) = 2 \neq 1$
- $\bar{3} \equiv 7 \ (mod\ 10)$
- $\bar{4}$ does not exist since $gcd(4, 10) = 2 \neq 1$
- $\bar{5}$ does not exist since $gcd(5, 10) = 5 \neq 1$
- $\bar{6}$ does not exist since $gcd(6, 10) = 2 \neq 1$
- $\bar{7} \equiv 3 \ (mod\ 10)$
- $\bar{8}$ does not exist since $gcd(8, 10) = 2 \neq 1$
- $\bar{9} \equiv 9 \ (mod\ 10)$

This concludes the material for midterm 1.

Lecture 9

Solving Congruences

Definition 9.0.1 (Linear Congruence)**.** *$ax \equiv b$ (mod m)*

Example:

$$3x \equiv 5 \ (mod\ 7)$$
$$x \equiv 0 \ (mod\ 7)$$
$$x - 0 = 7k$$

Question: What is the multiplicative inverse of 3 (mod 7) So we have $3x \equiv 5$ (mod 7).

$$15x \equiv 25 \ (mod\ 7)$$
$$x \equiv 4 \ (mod\ 7)$$
$$3 \cdot 4 = 12 \equiv 5 \ (mod\ 7)$$

9.1 Linear Congruence System

Find x such that

$$x \equiv a_1 \ (mod\ m_1)$$
$$x \equiv a_2 \ (mod\ m_n)$$
$$\vdots$$
$$x \equiv a_n \ (mod\ m_n)$$

Example:

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 5 \ (mod\ 7)$$

Try $x = 68$

$$68 \equiv 2 \ (mod\ 3)$$

$$68 \equiv 3 \ (mod\ 5)$$
$$68 \equiv 5 \ (mod\ 7)$$

So, $x = 68$ is a solution to the system.

9.1.1 Substitution Method

$$x \equiv 2 \ (mod\ 3)$$
$$x = 3 \cdot t + 2$$

For some $t \in \mathbb{Z}$

$$x \equiv \ (mod\ 5)$$
$$3t + 2 \equiv 3 \ (mod\ 5)$$
$$3t \equiv 1 \ (mod\ 5)$$

Multiply $3x$ by the multiplicative inverse of 3 in $\mathbb{Z}_5$.

$$2 \cdot 3t \equiv 2 \cdot 1 \ (mod\ 5)$$
$$t \equiv 2 \ (mod\ 5)$$
$$t = 5u + 2 \ (mod\ 5)$$

For an $u \in \mathbb{Z}$

$$\left.\begin{aligned} x &= 3t + 2 \\ t &= 5u + 2 \end{aligned}\right\}$$
$$\implies x = ?$$
$$x = 3(5u + 2) + 2 = 15u + 8$$

$$\begin{aligned} 15u + 8 &\equiv 5 \ (mod\ 7) \\ 15u &\equiv -3 \ (mod\ 7) \\ 15u &\equiv 4 \ (mod\ 7) \\ 15u - 14u &\equiv 4 \ (mod\ 7) \\ u &\equiv 4 \ (mod\ 7) \end{aligned}$$

So $u = 7v + 4$ for some $v \in \mathbb{Z}$. Thus,

$$\begin{aligned} x &= 15u + 8 \\ &= 15(7v + 4) + 8 \\ &= 105v + 68 \end{aligned}$$

So,

$$105v + 68 \equiv 2 \ (mod\ 3)$$
$$105v + 68 \equiv 3 \ (mod\ 5)$$
$$105v + 68 \equiv 5 \ (mod\ 7)$$

Example:

$$x \equiv 1 \ (mod\ 4)$$
$$x \equiv 3 \ (mod\ 5)$$

Then $x = 4t + 1$ for some $t \in \mathbb{Z}$. Then from the second equation, we get

$$\begin{aligned} 4t + 1 &\equiv 3 \ (mod\ 5) \\ 4t + 1 - 1 &\equiv 3 - 1 \ (mod\ 5) \\ 4t &\equiv 2 \ (mod\ 5) \\ 4 \cdot 4t &\equiv 4 \cdot 2 \ (mod\ 5) \\ 16t &\equiv 8 \ (mod\ 5) \\ 16t &\equiv 8 \ (mod\ 5) \\ 16t - 15t &\equiv 8 - 5 \ (mod\ 5) \\ t &\equiv 3 \ (mod\ 5) \end{aligned}$$

Thus, $t = 5u + 3$ for some $u \in \mathbb{Z}$. So $x = 20u + 13$ is a solution to the system.

$$20u + 13 \equiv 1 \ (mod\ 4)$$
$$20u + 13 \equiv 3 \ (mod\ 5)$$

Question: Are there systems that admit no solution? Consider

$$x \equiv 2 \ (mod\ 4)$$

$$x \equiv 3 \ (mod\ 6)$$

So $x = 4t + 2$ for some $t \in \mathbb{Z}$

$$4t + 2 \equiv 3 \ (mod\ 6)$$

$$4t \equiv 1 \ (mod\ 6)$$

But, 4 does not have a multiplicative inverse in $\mathbb{Z}_6$ since $gcd(4, 6) \neq 1$.

Theorem 9.1.1 (Chinese Remainder Theorem)**.** *Let* $m_1, m_2, \ldots, m_r \in \mathbb{Z}$ *be pairwise co-prime integers such that* $m_i \geq 2$ *for* $1 \leq i \leq r$

Definition 9.1.1 (Pairwise Co-prime)**.** $gcd(m_i, m_j) = 1$

Let $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, then the system

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_r \ (mod\ m_r) \end{aligned}$$

admits a unique solution $(mod\ m_1 \cdot m_2 \cdots m_r)$.In other words, the solution exists and is unique in $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_r}$

Consider the system

$$\begin{aligned} x &\equiv 2 \ (mod\ 3) \\ x &\equiv 3 \ (mod\ 5) \\ x &\equiv 5 \ (mod\ 7) \end{aligned}$$

So we have $\mathbb{Z}_{3 \cdot 5 \cdot 7} = \mathbb{Z}_{105}$, $68 \in \mathbb{Z}_{105}$ and $x = 105u + 68$.

Lecture 10

Fermat's Theorem

Theorem 10.0.1 (Fermat's Theorem)**.** *Let $p, a \in \mathbb{Z}$ such that p is prime, then*

1. $$a^p \equiv a \ (mod\ p)$$

2. *If $gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \ (mod\ p)$*

Example:

$$1534^{2016} \ (mod\ 2017)$$

2017 is prime and $1534 < 2017$, so $gcd(1534, 2017) = 1$ and $1534^2016 \equiv 1$ (mod 2017)

Proof. For (2) $1 \cdot a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$ are all different $(mod\ p)$.

- $a = 12$ and $p = 7$
- $1 \cdot a \equiv 5 \ (mod\ 7)$
- $2 \cdot a \equiv 3 \ (mod\ 7)$
- $3 \cdot a \equiv 1 \ (mod\ 7)$
- $4 \cdot a \equiv 6 \ (mod\ 7)$
- $5 \cdot a \equiv 4 \ (mod\ 7)$
- $6 \cdot a \equiv 2 \ (mod\ 7)$

- $a = 9$ and $p = 5$
- $1 \cdot a \equiv 4 \ (mod\ 5)$
- $2 \cdot a \equiv 4 \ (mod\ 5)$
- $3 \cdot a \equiv 4 \ (mod\ 5)$
- $4 \cdot a \equiv 4 \ (mod\ 5)$

$\square$

Lecture 11

Intro to Cryptography

Lecture 12

Asympotic Notation

12.1 Big-O Notation

The *O-notation* describes an asympotic upper bound.

Definition 12.1.1. *Let*

$$f : \mathbb{N} \to \mathbb{R}^+$$
$$g : \mathbb{N} \to \mathbb{R}^+$$

be two functions. We say that f is O(g) *if there exists a real number $c > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$,*

$$f(n) \leq c \cdot g(n)$$

Notation:

$$f(n) \leq c \cdot g(n)$$
$$f = O(g)$$
$$\exists c \exists k \forall n (n \geq k \implies f(n) \leq c \cdot g(n))$$

Domain: $k, n \in \mathbb{N}$, $c \in \mathbb{R}^+ \setminus \{0\}$

Example: $13x^3 + 12x^2 + 5 = O(x^3)$. We have

$$13x^3 + 12x^2 + 5 \leq 13x^3 + 12x^3 + 5x^2 = 30x^3$$

Take $c = 30$ and $k = 1$. So

$$13x^3 + 12x^2 + 5 \leq 30 \cdot x^3$$

for all $x \geq 1$. Therefore $13x^3 + 12x^2 + 5 = O(x^3)$.

Example: $x^2 = O\left(\frac{1}{2}x^2 - 10x\right)$. We have

$$x^2 \leq 2\left(\frac{1}{2}x^2 - 10x\right)$$

Now we want

$$x^2 \geq 40x$$

so that that $x^2 - 40x$ is positive. So

$$x > 40$$

Then,

$$\begin{aligned} x^2 &= 2x^2 - x^2 \\ &\leq 2x^2 - 40x \\ &= 4\left(\frac{1}{2}x^2 - 10x\right) \end{aligned}$$

So take $c = 4$ and $k = 40$. Then $x^2 = O\left(\frac{1}{2}x^2 - 10x\right)$ for all $x \geq 40$.

Proposition 12.1.1. *Let $a > 0$ and $b > 0$. be two rael numbers. We have*

$$log^a(x) = O(x^b)$$

Proof. Let $a > 0$ and $b > 0$ be two real numbers. We'll use that fact that $\forall x \geq 0$, we have $x \leq e^x$. From which, we have $log(x) \leq x$. Let x be an integer. We have, by the previous property,

$$\begin{aligned} \log(x^{\frac{b}{a}}) &\leq x^{\frac{b}{a}} \\ \frac{b}{a}\log(x) &\leq x^{\frac{b}{a}} \\ \left(\frac{b}{a}\right)^a \log^a(x) &\leq x^b \\ \log^a(x) &\leq \left(\frac{a}{b}\right)^a x^b \end{aligned}$$

So we take $c = \left(\frac{a}{b}\right)^a$ and $k = 1$. $\square$

12.2 Big-Omega Notation

The Ω-*notation* describes an asympotic lower bound.

Definition 12.2.1. *Let*

$$f : \mathbb{N} \to \mathbb{R}^+$$

$$g : \mathbb{N} \to \mathbb{R}^+$$

be two functions. We say that f is $\Omega(g)$ if there exists a real number $c > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$,

$$f(n) \geq c \cdot g(n)$$

Notation:

$$f(n) = \Omega(g(n))$$
$$f = \Omega(g)$$
$$\exists c \exists k \forall n (n \geq k \implies f(n) \geq c \cdot g(n))$$

Domain: $k, n \in \mathbb{N}$, $c \in \mathbb{R}^+ \setminus \{0\}$

Example: $13x^3 + 12x^2 + 5 = \Omega(x^3)$.

$$13x^3 + 12x^2 + 5 \geq 13x^3$$

Take $c = 13$ and $k = 0$. So $13x^3 + 12x^2 + 5 = \Omega(x^3)$.

Example: $x^2 = \Omega\left(\frac{1}{2}x^2 - 10x\right)$.

$$\begin{aligned} x^2 &\geq \frac{1}{2}x^2 \\ &\geq \frac{1}{2}x^2 - 10x \\ &= 1 \cdot \left(\frac{1}{2}x^2 - 10x\right) \end{aligned}$$

Take $c = 1$ and $k = 0$. So $x^2 = \Omega\left(\frac{1}{2}x^2 - 10x\right)$ $\forall x \geq k$.

Proposition 12.2.1. *Let $f(n)$ and $g(n)$ be two functions.*

$$f(n) = O(g(n)) \iff g(n) - \Omega(f(n))$$

Proof. ($\implies$) Let $f(n)$ and $g(n)$ be two functions. Assume $f(n) = O(g(n))$. Then there exists $c > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$, we have $f(n) \leq c \cdot g(n)$. So,

$$f(n) \leq c \cdot g(n)$$

given that $n \geq g(n)$, then

$$g(n) \geq \frac{1}{c} f(n)$$

($\impliedby$) The proof follows the same. □

12.3 Big-Theta Notation

The Θ-*notation* describes an asympotic upper and lower bound.

Definition 12.3.1. *Let*

$$f : \mathbb{N} \to \mathbb{R}^+$$
$$g : \mathbb{N} \to \mathbb{R}^+$$

be two functions. We say that f is $\Theta(g)$ if there exists a real number $c_1 > 0$, $c_2 > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$. In otherwords,

$$f(n) = O(g(n)) \text{ and } f(n) = \Omega(g(n))$$

Notation:

$$f(n) = \Theta(g(n))$$

$$f = \Theta(g)$$

Proposition 12.3.1. *Let $f(n)$ and $g(n)$ be two functions. $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $g(n) = \Omega(f(n))$.*

Proof.

$$f(n) = \Theta(g(n)) \iff f(n) = O(g(n)) \text{ and } f(n) = \Omega(g(n))$$

By the definition of theta, so

$$g(n) = \Omega(f(n)) \text{ and } g(n) = O(f(n))$$

From the previous proposition, then

$$g(n) = \Theta(f(n))$$

□