CSI 2101 Lecture Notes

Last updated:

April 13, 2023

Contents

List 1

List 2

List 3

List 4

Prime Numbers, GCD, and Euclid

4.1 Question 1

Skipping question 1-7

4.8 Question 8

Let $n > 1$ be an integer. If n is not prime, then n has a prime divisor p such that $p \leq \sqrt{n}$. **Answer:** $P(x)$ says "x is prime".

$$\forall n((\neg P(n) \wedge n > 1) \implies \exists p(p \mid n \wedge p \leq \sqrt{n}))$$

True, theorem seen in class.

4.9 Question 9

Let $n > 1$ be an integer. If n has a prime divisor p such that $p \leq \sqrt{n}$, then n is not prime. **Answer:** $P(x)$ says "x is prime".

$$\forall n(\exists p(P(p) \wedge p \leq \sqrt{n}) \implies \neg P(n))$$

True, if n has a prime divisor p, then either n is not prime or $n = p$, if $n = p$, then it contradicts that $p \leq \sqrt{n}$ since $\sqrt{n} < n \forall n > 1$, so n is not prime.

4.10 Question 10

Let a, b, q, r be integers such that $\gcd(a, b) = \gcd(b, r)$. Then $a = bq + r$. **Answer:**

$$\forall a \forall b \forall q \forall r((\gcd(a, b) = \gcd(b, r)) \implies (a = bq + r))$$

Suppose $\gcd(a, b) = \gcd(b, r)$, then let $d = \gcd(a, b) = \gcd(b, r)$. So $d \mid a$, $d \mid b$, and $d \mid r$. Then we have

4.11 Question 11

Let a, b, q, r be integers such that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.
Answer: Lemma seen in class.

4.12 Question 12

Let $a, b, c \in \mathbb{Z}$ with $a = bq + 1$

List 5

Exercises on Euclid, Bézout, Fermat's Theorem, and the Chinese Remainder Theorem

5.1 Question 1

Find the inverse of $a \pmod{m}$ for each of the following pairs of integers through Euclid and Bézout.

(a) $a = 4$, $m = 9$

(b) $a = 19$, $m = 141$

(c) $a = 89$, $m = 232$

(d) $a = 189$, $m = 1231$

(e) $a = 189$, $m = 1232$

(f) $a = 14$, $m = 31$

(g) $a = 200$, $m = 800$

(h) $a = 111$, $m = 511$

(i) $a = 109$, $m = 781$

(j) $a = 208$, $m = 781$

Answer:

(a) $a = 4$, $m = 9$

$$\begin{aligned} 9 &= 2 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \\ 1 &= 9 - 2 \cdot 4 \equiv 7 \cdot 4 \mod 7 \end{aligned}$$

Therefore the inverse of $4 \mod 9$ is 7.

(b) $a = 19$, $m = 141$

$$\begin{aligned} 141 &= 7 \cdot 19 + 8 \\ 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 3 - 2 \\ 1 &= 3 - (8 - 2 \cdot 3) \\ 1 &= -8 + 3 \cdot 3 \\ 1 &= -8 + 3 \cdot (19 - 2 \cdot 8) \\ 1 &= -8 + 3 \cdot 19 - 6 \cdot 8 \\ 1 &= 3 \cdot 19 - 7 \cdot 8 \\ 1 &= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) \\ 1 &= 3 \cdot 19 - 7 \cdot 141 + 49 \cdot 19 \\ 1 &= 52 \cdot 19 - 7 \cdot 141 \equiv 52 \cdot 19 \mod 141 \end{aligned}$$

Therefore the inverse of $19 \mod 141$ is 52.

5.2 Question 2

Solve the following congruences

(a) $4x \equiv 2 \pmod 9$

(b) $19x \equiv 12 \pmod{141}$

(c) $89x \equiv 22 \pmod{232}$

(d) $189x \equiv 32 \pmod{1231}$

(e) $189x \equiv 42 \pmod{1232}$

(f) $14x \equiv 2 \pmod{31}$

(g) $200x \equiv 400 \pmod{800}$

(h) $111x \equiv 111 \pmod{511}$

(i) $109x \equiv 142 \pmod{781}$

(j) $208x \equiv 3 \pmod{781}$

Answer:

(a) $4x \equiv 2 \pmod 9$ We know that 4 has an inverse mod 9 of 7. So $4 \cdot 7 \equiv 1 \implies 4 \cdot 14 \equiv 4 \pmod 9$

(b) $19x \equiv 12 \pmod{141}$ Similarly, $19 \cdot 52 \equiv 1 \implies 19 \cdot 104 \equiv 19 \pmod{141}$

(c) $89x \equiv 22 \pmod{232}$

(d) $189x \equiv 32 \pmod{1231}$

(e) $189x \equiv 42 \pmod{1232}$

(f) $14x \equiv 2 \pmod{31}$

(g) $200x \equiv 400 \pmod{800}$

(h) $111x \equiv 111 \pmod{511}$

(i) $109x \equiv 142 \pmod{781}$

(j) $208x \equiv 3 \pmod{781}$

5.3 Question 3

Solve the following systems of congruences by using the substitution method.

(a)

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

(b)

$$\begin{aligned} 5x &\equiv 3 \pmod 6 \\ 4x &\equiv 4 \pmod 7 \end{aligned}$$

(c)

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

(d)

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 3 \end{aligned}$$

(e)

$$\begin{aligned} 3x &\equiv 4 \pmod 5 \\ 2x &\equiv 2 \pmod 4 \\ x &\equiv 1 \pmod 3 \end{aligned}$$

Answer:

(a)

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

$x \equiv 3 \pmod 6 \implies x = 6s+3$ for some $s \in \mathbb{Z}$. Then $x \equiv 4 \pmod 7 \implies 6s+3 \equiv 4 \pmod 7 \implies 6s \equiv 1 \pmod 7$. Now taking the multiplicative inverse of 6 in $\mod 7$, we get $s = 6$. So $x = 6 \cdot 6 + 3 = 39$.

(b)

$$\begin{aligned} 5x &\equiv 3 \pmod 6 \\ 4x &\equiv 4 \pmod 7 \end{aligned}$$

We can start by simplifying the equations, so $5x \equiv 3 \pmod 6$ becomes

$$5 \cdot 5x \equiv x \equiv 5 \cdot 3 \equiv 3 \pmod 6$$

Similarly, $4x \equiv 4 \pmod 7$ becomes

$$2 \times 4x \equiv x \equiv 1 \pmod 7$$

So $x = 6a + 3$ for some $a \in \mathbb{Z}$.

$$\begin{aligned} 6a + 3 &\equiv 1 \pmod 7 \\ 6a &\equiv -2 \pmod 7 \\ 6a &\equiv 5 \pmod 7 \\ a &\equiv 5 \cdot 5 \equiv 4 \pmod 7 \end{aligned}$$

So $x = 6a + 3 = 27$.

(c)

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

$x \equiv 0 \pmod 3$, so $x = 3s$ for some $s \in \mathbb{Z}$.

$$\begin{aligned} 3s &\equiv 3 \pmod 4 \\ 3 \cdot 3s &\equiv 3 \cdot 3 \pmod 3 \\ s &\equiv 1 \pmod 4 \end{aligned}$$

So $s = 4t + 1$ for some $t \in \mathbb{Z}$, then $x = 3s = 12t + 3$

$$\begin{aligned} 12t + 3 &\equiv 4 \pmod 5 \\ 12t &\equiv 1 \pmod 5 \\ 2t &\equiv 1 \pmod 5 \\ t &\equiv 3 \pmod 5 \end{aligned}$$

So $x = 12t + 3 = 36 + 3 = 39$

(d)

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 3 \end{aligned}$$

$x \equiv 1 \pmod 5$, so $x = 5s + 1$ for some $s \in \mathbb{Z}$. Then

$$\begin{aligned} 5s + 1 &\equiv 1 \pmod 4 \\ 5s &\equiv 0 \pmod 4 \\ s &\equiv 0 \pmod 4 \end{aligned}$$

Then $s = 4t$ for some $t \in \mathbb{Z}$, so $x = 5s + 1 = 5(4t) + 1 = 20t + 1$.

$$\begin{aligned} 20t + 1 &\equiv 1 \pmod 3 \\ 20t &\equiv 0 \pmod 3 \\ t &\equiv 0 \pmod 3 \end{aligned}$$

Therefore, $x = 20t + 1 = 1$.

5.4 Question 4

There was no question 4.

5.5 Question 5

Solve the following systems of congruences.

(a)

$$\begin{aligned} x &\equiv 0 \pmod{101} \\ x &\equiv 0 \pmod{103} \\ x &\equiv 0 \pmod{107} \end{aligned}$$

(b)

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 3x &\equiv 2 \pmod 4 \\ 4x &\equiv 3 \pmod 5 \end{aligned}$$

(c)

$$\begin{aligned} 2x &\equiv 1 \pmod 5 \\ 2x &\equiv 4 \pmod 6 \\ 2x &\equiv 1 \pmod 7 \end{aligned}$$

5.6 Question 6

Simplify the following expressions as much as possible.

(a) $7^{121} \pmod{13}$

(b) $23^{1002} \pmod{41}$

Answer:

(a) $7^{121} \pmod{13}$ Using Fermat's theorem, we can rearrange the expression to get

$$\begin{aligned} 7^{121} &= 7^{9\cdot 13+4} \\ &= 7^{9\cdot 13}7^4 \\ &= (7^{13})^9 \cdot 7^4 \\ &\equiv 7^9 \cdot 7^4 \pmod{13} \\ &\equiv 7^{13} \equiv 7 \pmod{13} \end{aligned}$$

Therefore, $7^{121} \equiv 7 \pmod{13}$.

(b) $23^{1002} \pmod{41}$

$$\begin{aligned} 23^{1002} &= 23^{1000+2} \\ &= 23^{1000}23^2 \\ &= 23^{25\cdot 40}23^2 \\ &= (23^{40})^{25}23^2 \\ &\equiv 1^2 5 \cdot 23^2 \pmod{41} \\ &\equiv 23^2 \pmod{41} \\ &\equiv (-18)^2 \pmod{41} \\ &\equiv 4 \cdot 81 \pmod{41} \\ &\equiv 4 \cdot 40 \pmod{41} \\ &\equiv 4 \cdot -1 \pmod{41} \\ &\equiv -4 \equiv 37 \pmod{41} \end{aligned}$$

5.7 Question 7

Simplify the following expressions as much as possible.

(a) $28^{1000000} \pmod{27}$

(b) $6^{778} \pmod{7}$

Answer:

(a) $28^{1000000} \pmod{7}$ $28 \equiv 0 \pmod{7}$, so $28^{1000000} \equiv 0 \pmod{7}$

(b) $6^{778} \pmod{7}$ $6 \equiv -1 \pmod{7}$, so $6^{778} \equiv -1^{778} \pmod{7}$. 778 is even so $6^{778} \equiv 1 \pmod{7}$.

5.8 Question 8

Let $a, m \in \mathbb{Z}$ with $m \geq 2$ and $0 < a < m$. Suppose that $\gcd(a, m) = d > 1$. Find two solutions $x \in \mathbb{Z}_m$ to the following linear congruence

$$a \cdot x \equiv a \pmod{m}$$

5.9 Question 9

Find all primes p and all $x \in \mathbb{Z}_p$ such that

$$x^{p-1} + 7x \equiv 1 \pmod{p}$$

Answer: From Fermat's theorem $x^{p-1} \equiv 1 \pmod{p}$. So,

$$\begin{aligned} x^{p-1} + 7x &\equiv 1 \pmod{p} \\ 1 + 7x &\equiv 1 \pmod{p} \\ 7x &\equiv 0 \pmod{p} \end{aligned}$$

So, we must have that $p = 7$. Then

$$x^6 + 7x \equiv 1 \pmod{7} \implies x^6 \equiv 1 \pmod{6}$$

We can take any value in $\mathbb{Z}_7$ for x and it will satisfy the equation except $x = 0$.

5.10 Question 10

Let $m_1, m_2, \ldots, m_r, a_1, a_2, \ldots, a_r \in \mathbb{Z}$ be positive integers with $m_i \geq 2$ $(1 \leq i \leq r)$. Suppose there exists integers i and j with $1 \leq i \leq j \leq r$ such that m_i and m_j are not co-prime. Then the system

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

does not have a solution.

Answer: False, consider the following system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{m_1} \\ x &\equiv 1 \pmod{m_2} \\ &\vdots \\ x &\equiv 1 \pmod{m_r} \end{aligned}$$

5.11 Question 11

Let $a, m \in \mathbb{Z}$, where $m \geq 2$. If $\gcd(a, m) \neq 1$, then the inverse of a modulo m does not exist.

Answer:

$$\forall a \forall m((\gcd(a, m) \neq 1) \implies \nexists a^{-1}(a^{-1}a \equiv 1 \pmod{m}))$$

True, theorem seen in class.

5.12 Question 12

Let $a, m \in \mathbb{Z}$ such that $m \geq 2$ and $\gcd(a, m) = 1$. If m is not prime, then $a^{m-1} \not\equiv 1 \pmod{m}$.

Answer: $P(x)$ says "x is prime".

$$\forall a \forall m((\gcd(a, m) = 1 \wedge \neg P(m)) \implies a^{m-1} \not\equiv 1)$$

False, take $m = 4$, $a = 5$, then $\gcd(5, 4) = 1$, 4 is not prime. But,

$$5^{4-1} = 5^3 = 125 \equiv 1 \pmod{4}$$

5.13 Question 13

Let $p \in \mathbb{Z}$ and $a \in \mathbb{Z}$ be such that $\gcd(a, p) \neq 1$. Then $a^{p-1} \neq 1 \pmod{p}$.

Answer: $P(x)$ says "x is prime".

$$\forall p \forall a((P(p) \wedge \gcd(a, p) \neq 1) \implies a^{p-1} \not\equiv 1 \pmod{p})$$

True, if $\gcd(a, p) \neq 1$, then $p \mid a$, so

$$a^{p-1} \equiv 0^{p-1} \equiv 0 \pmod{p}$$

5.14 Question 14

Let $a \in \mathbb{Z}$. If there exists $b \in \mathbb{Z}$ such that $a - b^{16} \equiv 3 \pmod{17}$, then $17 \mid (a - 3)(a - 4)$.

Answer:

$$\forall a(\exists b(a - b^{16} \equiv 3 \pmod{17}) \implies 17 \mid (a - 3)(a - 4))$$

Suppose there exists $b \in \mathbb{Z}$ such that $a - b^{16} \equiv 3 \pmod{17}$. Then

$$b^{16} \equiv 1 \pmod{16}$$

by Fermat's Theorem, so

$$a - 1 \equiv 3 \implies a \equiv 4 \pmod{17} \implies 17 \mid (a-4)$$

Then

$$17 \mid (a-4) \implies 17 \mid (a-4)(a-3)$$

5.15 Question 15

Let p be a prime number such that $p \geq 5$. Then $p^2 + 2$ is not prime.

Answer: $P(x)$ says "x is prime".

$$\forall p((P(p) \wedge p \geq 5) \implies \neg P(p^2+2))$$

If we prove that p^2+2 is divisible by 3, then p^2+2 is certainly not prime. $p \geq 5$, so $\gcd(p,3) = 1$. Then, by Fermat's Theorem, $p^2 \equiv 1 \pmod{p}$, so

$$p^2 + 2 \equiv 1 + 2 \equiv 0 \pmod{3}$$

So, $3 \mid p^2 + 2$, thus $p^2 + 2$ is not prime.

5.16 Question 16

Let p be a prime number such that $p \geq 2$. Then $p^2 + 2$ is not prime.

Answer: $P(x)$ says "x is prime".

$$\forall p((P(p) \wedge p \geq 2) \implies \neg P(p^2+2))$$

False, counterexample: $p = 3$. Then $p^2 + 2 = 9 + 2 = 11$ which is prime.

5.17 Question 17

Let $n \geq 1$ be an integer. Then

$$\sum_{i=1}^{n} i! \equiv 9 \pmod{12}$$

Answer:

$$\forall n((n \geq 1) \implies \sum_{i=1}^{n} i! \equiv 9 \pmod{12})$$

False, take $n = 1$, then $\sum_{i=1}^{n} i! = 1 \not\equiv 9 \pmod{12}$.

5.18 Question 18

Let $n \geq 3$ be an integer. Then

$$\sum_{i=1}^{n} i! \equiv 9 \pmod{12}$$

Answer:

$$\forall n((n \geq 3) \implies \sum_{i=1}^{n} i! \equiv 9 \pmod{12})$$

Proof by induction, the base case when $n = 3$ is true since $3!+2!+1! = 6+2+1 = 9 \equiv 9 \pmod{12}$. Now, suppose the statement is true for k, then to prove it for $k+1$, we have

$$\begin{aligned}
\sum_{i=1}^{k+1} i! &= (k+1)! + \sum_{i=1}^{k} i! \\
&= (k+1) \cdot k \cdot \ldots \cdot 4 \cdot 3 \cdot 2 \cdot 1 + \sum_{i=1}^{k} i! \\
&= 12 \cdot 2(k+1)k + \sum_{i=1}^{k} i! \\
&\equiv \sum_{i=1}^{k} i! \pmod{12} \\
&\equiv 9 \pmod{12} && \text{(By the IH)}
\end{aligned}$$

5.19 Question 19

A prime triplet is a triplet of numbers $(p, p+2, p+4)$ where $p, p+2, p+4$ are prime numbers. There is no prime triplet other than $3, 5, 7$.

Answer: $P(x)$ says "x is prime".

$$\forall p((P(p) \wedge p \neq 3) \implies (\neg P(p+2) \vee P(p+4)))$$

We want to show that $p+2$ or $p+4$ is divisible by 3. We have $p \neq 3$, so $p \pmod 3$ is either 1, or 2. If $p \equiv 1 \pmod 3$, then $p+2 \equiv 3 \equiv 3 \pmod 3$ so $p+2$ is divisible by 3 and thus not prime. If $p \equiv 2 \pmod 3$, then $p+4 \equiv 6 \equiv 0 \pmod 3$ so $p+4$ is divisible by 3 and thus not prime. So in either case, when $p \neq 3$, $(p, p+2, p+4)$ is not a prime triplet.

5.20 Question 20

Let $n \geq 1$ be an odd integer. Then

$$\sum_{i=0}^{n-1} i \equiv 0 \pmod{n}$$

Answer: $P(x)$ says "x is even".

$$\forall n((\neg P(n) \wedge n \geq 1) \implies \left(\sum_{i=0}^{n-1} i \equiv 0 \pmod{n}\right))$$

Consider the equation for the sum

$$\sum_{i=0}^{n-1} i = \frac{(n-1)n}{2}$$

n is odd, so $n = 2l + 1$ for some integer l. Then

$$\begin{aligned} \frac{(2l+1-1)(2l+1)}{2} &= \frac{4l^2+2l}{2} \\ &= 2l^2 + l \\ &= l(2l+1) \\ nl &\equiv 0 \pmod{n} \end{aligned}$$

5.21 Question 21

Let $n \geq 1$ be an even integer. Then

$$\sum_{i=0}^{n-1} i \equiv 0 \pmod{n}$$

Answer: $P(x)$ says "x is even".

$$\forall n((P(n) \wedge n \geq 1) \implies \left(\sum_{i=0}^{n-1} i \equiv 0 \pmod{n}\right))$$

False, counter example: take $n = 2$, then

$$\sum_{i=0}^{n-1} i = 1 \not\equiv 0 \pmod{2}$$

5.22 Question 22

Let $p > 2$ be a prime number. There exists two different integers a and b such that

$$\frac{2}{p} = \frac{1}{a} + \frac{1}{b}$$

Answer: $P(x)$ says "x is prime".

$$\forall p((P(p) \wedge p > 2) \implies \exists a \exists b \left(\frac{2}{p} = \frac{1}{a} + \frac{1}{b}\right))$$

Proof by contradiction. Suppose that for all primes $p > 2$, there exists two different integers a and b such that

$$\frac{2}{p} = \frac{1}{a} + \frac{1}{b}$$

then

$$\begin{aligned}
\frac{2}{p} &= \frac{1}{a} + \frac{1}{b} \\
\frac{2}{p} &= \frac{a+b}{ab} \\
p &= 2\left(\frac{a+b}{ab}\right)
\end{aligned}$$

So this means that p is divisible by 2, but p is prime so it must be that $p = 2$, but this contradicts that $p > 2$. Thus, the statement is false.

List 6

RSA

List 7

Asympotic Notation

7.1 Question 1

Prove or disprove.

$$x \log(x) = O(x^2)$$

Answer:

$$\log(x) < x \implies x \log(x) < x \cdot x < x^2$$

So $x \log(x) = O(x^2)$.

7.2 Question 2

Prove or disprove.

$$x^2 = O(x \log(x))$$

Answer: We want to find $c > 0$ and x_0 such that $x^2 \leq c \cdot x \cdot \log(x)$ for all $x \geq x_0$. But, $\log(x) < x$ for all $x > 0$, so there is no such constant c such that

$$x^2 \leq c \cdot x \cdot \log(x)$$

So $x^2 = O(x \log(x))$ is false.

7.3 Question 3

Prove or disprove.

$$0 = O(1)$$

Answer:

$$0 < 1$$

Take $c = 1$, $x_0 = 1$. Then $0 < c \cdot 1 \ \forall x > x_0$, so $0 = O(1)$ is true.

7.4 Question 4

Prove or disprove.

$$1 = O(0)$$

Answer: Since $c \cdot 0 = 0$ for all c, and $0 < 1$, there is no such c to satisfy $1 < c \cdot 0$, so $1 = O(0)$ is false.

7.5 Question 5

Prove or disprove.

$$1 = O\left(\sin\left(\frac{\pi}{4}n\right)\right)$$

What about $1 = O(\sin(n))$?

Answer: Since $-1 \leq \sin\left(\frac{\pi}{4}n\right) \leq 1 \ \forall n$, there is no c such that

$$1 < c \cdot \sin\left(\frac{\pi}{4}n\right)$$

Similarly for $\sin(n)$. So $1 = O\left(\sin\left(\frac{\pi}{4}n\right)\right)$ and $1 = O(\sin(n))$ are both false.

7.6 Question 6

Prove or disprove.

$$\sin(n) = O(1)$$

Answer: True, since $-1 \leq \sin(n) \leq 1 \ \forall n$, take $c = 2$, then $\sin(n) < c \cdot 1 \ \forall n$, so $\sin(n) = O(1)$.

7.7 Question 7

Prove or disprove.

$$x = O\left(\frac{x}{\log(x)}\right)$$

Answer: False, since $\lim_{x \to \infty} \log(x) = \infty$, $\frac{x}{\log(x)}$ becomes arbitrarly small so there is no c such that $x < c \cdot \frac{x}{\log(x)}$.

7.8 Question 8

Prove or disprove.

$$\frac{x}{\log(x)} = O\left(\frac{x}{\log(x)}\right)$$

Answer: True, since $\log(x) > 1$ for all $x > 10$, then $\frac{x}{\log(x)} < x \ \forall x > 10$, so there is a c such that $\frac{x}{\log(x)} < c \cdot \frac{x}{\log(x)}$. Take $c = 1$ and $x_0 = 10$.

7.9 Question 9

Prove or disprove.

$$2^n = \Theta(3^n)$$

Answer: False, 2^n cannot be $\Omega(3^n)$ because 3^n approaches ∞ as n approaches ∞, so there is no c such that.

$$c \cdot 3^n < 2^n$$

7.10 Question 10

Prove or disprove.

$$x^3 - x = \Omega(1000x^2)$$

Answer: True, we can find $c > \frac{1}{1000}$, then

$$x^3 - x = x^2(x-1) > x^2$$

for all $x > 3$.

7.11 Question 11

Prove or disprove.

$$\log(x) = \Omega(\log(\log(x)))$$

Answer: True, since

$$x > \log(x) \implies \log(x) > \log(\log(x))$$

for all x.

7.12 Question 12

Prove or disprove.

$$\log(\log(x)) = \Omega(\log(x))$$

Answer: False, we cannot find $c > 0$,

$$\log(\log(x)) > c\log(x)$$
$$\frac{\log(\log(x))}{\log(x)} > c$$

Since $x > \log(x)$, it follows that $\log(x) > \log(\log(x))$, so as x increases, $\frac{\log(\log(x))}{\log(x)}$ becomes arbitrarly small, so we cannot find a constant $c > 0$ such that $\log(\log(x)) > c\log(x)$.

7.13 Question 13

Prove or disprove.

$$\log(\sqrt{x}) = \Omega(\log(x))$$

Answer: True,

$$\log(\sqrt{x}) = \log\left(x^{\frac{1}{2}}\right) = \frac{1}{2}\log(x)$$

So take $c_1 = \frac{1}{4}$, and $c_2 = 2$, then

$$c_1 \log(x) \leq \frac{1}{2}\log(x) = \log(\sqrt{x}) \leq c_2 \log(x)$$

7.14 Question 14

Prove or disprove. Let $f(x)$ and $g(x)$ be two functions.

$$f(x) + g(x) = O(\max\{f(x), g(x)\})$$

Answer: True, assume without loss of generality that $f(x) \geq g(x)$, then

$$f(x) + g(x) \leq f(x) + f(x) \leq 2f(x)$$

and $\max\{f(x) + g(x)\} = f(x)$, so take $c = 3$, then

$$f(x) + g(x) \leq 3f(x)$$

7.15 Question 15

Prove or disprove. Let $f(x)$ and $g(x)$ be two functions.

$$\max\{f(x), g(x)\} = O(f(x) + g(x))$$

Answer: False, take $f(x) = x$ and $g(x) = -x$, then $\max\{f(x), g(x)\} = f(x) = x$, but $f(x) + g(x) = 0$, so there is no c such that $\max\{f(x), g(x)\} < c \cdot (f(x) + g(x)) = 0$.

7.16 Question 16

Prove or disprove. Let $f(x)$ and $g(x)$ be two functions.

$$f(x) + g(x) = \Omega(\min\{f(x), g(x)\})$$

Answer: True, assume without loss of generality that $f(x) \leq g(x)$, then

$$f(x) + g(x) \geq f(x) + f(x) = 2f(x)$$

And $\min\{f(x), g(x)\} = f(x)$, so take $c = 2$, then

$$f(x) + g(x) \geq 2\min\{f(x), g(x)\}$$

7.17 Question 17

Prove or disprove. Let $f(x)$ and $g(x)$ be two functions.

$$\min\{f(x), g(x)\} = \Omega(f(x) + g(x))$$

Answer: False, assume without loss of generality that $f(x) \leq g(x)$, then

$$f(x) \leq f(x) + g(x) \implies 0 \leq g(x)$$

There is no such $c > 0$ that would change this inequality since we would require $0 \geq g(x)$.

7.18 Question 18

Find a function $f(n)$ such that

$$\sum_{i=1}^{n} 1 = \Theta(f(n))$$

Answer:

$$\sum_{i=1}^{n} 1 = n$$

so take $f(n) = n$.

7.19 Question 19

Find a function $f(n)$ such that

$$\sum_{i=1}^{n} i = \Theta(f(n))$$

Answer:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

So take

$$f(n) = \frac{n(n+1)}{2}$$

7.20 Question 20

Find a function $f(n)$ such that

$$\sum_{i=1}^{n} 2^i = \Theta(f(n))$$

Answer:

$$\sum_{i=1}^{n} 2^i = \left(\sum_{i=0}^{n} 2^i\right) - 1 = 2^{n+1} - 2$$

Take $f(n) = 2^{n+1} - 2$.

7.21 Question 21

Find a function $f(n)$ such that

$$\sum_{i=1}^{n} \frac{1}{2^i} = \Theta(f(n))$$

Answer: This is a geometric series, so

$$\sum_{i=1}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$$

Take $f(n) = 2 - \frac{1}{2^n}$.

7.22 Question 22

Find a function $f(n)$ such that

$$\sum_{i=1}^{n} \frac{1}{(i(i+1))} = \Theta(f(n))$$

Answer: If we do a partial fraction decomposition, we see that

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \sum_{i=1}^{n} \frac{1}{i} - \frac{1}{i+1}$$

This sum is telescopic, so we get

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = 1 - \frac{1}{n+1}$$

Take $f(n) = 1 - \frac{1}{n+1}$.

List 8

List 9

Graphs

9.1 Question 1

Questions 1 - 7 are bad questions.

9.8 Question 8

How many vertices and how many edges are there in K_n?

Answer: There are n vertices and each vertex is connected to every other (except itself), so the n vertices have degree $n-$,

$$2|E| = \sum_{v \in V} \deg(v) = n \cdot (n-1)$$

So there are $\frac{n(n-1)}{2}$ edges.

9.9 Question 9

How many vertices and how many edges are there in C_n?

Answer: There are n vertices and each vertex is connected to two other vertices, so

$$2|E| = \sum_{v \in V} \deg(v) = 2n$$

Therefore there are $\frac{2n}{2} = n$ edges.

9.10 Question 10

How many vertices and how many edges are there in $K_{m,n}$?

Answer: There are $m+n$ vertices and each of the m vertices are connected to each of the m vertices are connected to n vertices, and vice-versa. so

$$2|E| = \sum_{v \in V} \deg(v) = 2mn \implies |E| = mn$$

9.11 Question 11

How many vertices and how many edges are there in an $(m \times n)$-grid?

Answer: There are mn vertices, the equation for the number of edges is

$$|E| = (n-1)m + (m-1)n = 2mn - n - m$$

9.12 Question 12

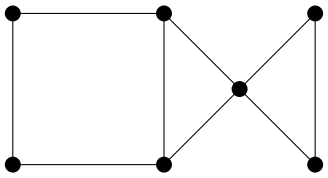
Does there exist a graph with 8 vertices, where the degrees of the vertices are 1, 2, 2, 2, 3, 3, 4 and 4? Prove that your answer is correct.

Answer: No, since there are an odd number of odd vertices, and by a theorem seen in class (Theorem 18.0.2 in my notes), there is no such graph.

9.13 Question 13

Does there exist a graph with 8 vertices, where the degrees of the vertices are 2, 2, 2, 2, 3, 3, 4 and 4? Prove that your answer is correct.

Answer: Yes, we can give an example:



Note, a good strategy for these types of questions is to start with the vertex with the highest degree, and then work your way down.

9.14 Question 14

Prove or disprove. Let $G = (V, E)$ be a graph. If G is a forest, then G is biartite.

Answer:

Proof. By a result seen in class, a graph is bipartite if and only if it has no cycles of odd length (Theorem 22.0.1 in my notes). By definition, a forest has no cycles and therefore no cycles of odd length, so it is bipartite. □

9.15 Question 15

For what values of n is K_n bipartite? Prove that your answer is correct.

Answer: K_n by definition has every vertex connected to every other vertex, so the only cases where we could partition the vertices into two sets such that every edge has an endpoint in each set is if $n = 1$, or $n = 2$. You can also see that for any $n \geq 3$, K_n has a cycle of length 3 so it cannot be bipartite.

Note: In certain textbooks/resources online, graphs with 1 vertex and 0 edges are bipartite (so by extension *all* forests are bipartite). But, in this course the professor treats the case with 1 vertex and 0 edges as *not bipartite*. Which means forests are not bipartite (except for $|V| \geq 2$). Therefore the only possible values of n for K_n to be bipartite is $n = 2$.

9.16 Question 16

For what values of n is C_n bipartite? Prove that your answer is correct.

Answer: Again, using theorem 22.0.1, a graph is bipartite if and only if it has no cycles of odd length. By definition, C_n has 1 cycle of length n, so it is bipartite when n is even, and not bipartite when n is odd.

9.17 Question 17

For what values of m and n is $K_{m,n}$ bipartite? Prove that your answer is correct

By the definition of $K_{m,n}$, is a complete bipartite graph.

9.18 Question 18

For what values of m and n is an $(m \times n)$-grid bipartite? Prove that your answer is correct.

Answer: By the definition of an $(m \times n)$-grid, it does not have any cycles of odd length, so it is bipartite for all values m, n.

Note: Again the professor has a discrepncy here, since a 1×1 grid has 1 vertex and 0 edges, and is not bipartite. So $(m \times n)$ is bipartite for all $(m, n) \neq (1, 1)$.

9.19 Question 19

For all $n \geq 1$, find the size of a maximum matching in K_n. For what values of n do we have a perfect matching. Prove that your answer is correct.

Answer: We'll consider 2 cases where n is even and n is odd.

- **Case 1:** n **is even.** We have the set of vertices

$$V = \{v_0, v_1, v_2, \dots v_{n-1}\}$$

  There exists an edge between each vertex (by definition of K_n), so we can match each of the two vertices to get the matching

$$\{\{v_0, v_1\}, \{v_1, v_2\}, \dots \{v_{n-2}, v_{n-1}\}\}$$

  This matching contains every vertex so it is a perfect matching. The size of the maximum matching is $\frac{n}{2}$.

- **Case 2:** n **is odd.** We have the set of vertices

$$V = \{v_0, v_1, v_2, \dots, v_{n-2}, v_{n-1}\}$$

  n is odd so $n-1$ is even, then using the first case again we can match the $n-1$ vertices

$$\{\{v_0, v_1\}, \{v_1, v_2\}, \dots \{v_{n-3}, v_{n-2}\}\}$$

  Leaving 1 vertex which cannot be matched. The size of the maximum matching is $\frac{n-1}{2}$ and it is not perfect.

So K_n has a maximum matching of size $\left\lfloor \frac{n}{2} \right\rfloor$ for all $n \geq 1$ and it is perfect for all even n.

9.20 Question 20

For all $n \geq 3$, find the size of a maximum matching in C_n. For what values of n do we have a perfect matching? Prove that your answer is correct.

Answer: We'll consider 2 cases where n is even and n is odd.

- **Case 1:** n **is even.** We have the set of vertices

$$V = \{v_0, v_1, v_2, \dots v_{n-1}\}$$

  From the definition of C_n, we have the edges

$$E = \{\{v_0, v_1\}, \{v_1, v_2\}, \dots \{v_{n-2}, v_{n-1}\}\}$$

  This is already a matching that contains every vertex so it is a perfect matching. The size of the maximum matching is $\frac{n}{2}$.

- **Case 2:** n **is odd.** We have the set of vertices

$$V = \{v_0, v_1, v_2, \dots, v_{n-2}, v_{n-1}\}$$

n is odd so $n-1$ is even, then using the first case again we can match the $n-1$ vertices

$$\{\{v_0, v_1\}, \{v_1, v_2\}, \ldots \{v_{n-3}, v_{n-2}\}\}$$

Leaving 1 vertex which cannot be matched. The size of the maximum matching is $\frac{n-1}{2}$ and it is not perfect.

So C_n has a maximum matching of size $\lfloor \frac{n}{2} \rfloor$ for all $n \geq 3$ and it is perfect for all even n.

9.21 Question 21

For all$1 \leq m \leq n$, find the size of a maximum matching in an $(m \times n)$-grid. For what values of m and n do we have a perfect matching? Prove that your answer is correct.

Answer: We'll consider 2 cases where mn is even and mn is odd.

- **Case 1:** mn **is even.** We have the set of vertices

$$V = \{v_{1,1}, v_{1,2}, \ldots, v_{1,n}, v_{2,1}, v_{2,2}, \ldots, v_{2,n}, \ldots, v_{m,n}\}$$

Each vertex is connected to a vertex in an adjacent column and row, so the set of edges is

$$E = \{v_{i,j}, v_{i+1,j}\} \cup \{v_{i,j}, v_{i,j+1}\}$$

for $1 \leq i \leq m$, $1 \leq j \leq n$. Since mn is even, then either m is even or n is even or both. If m is even, then we can match each vertex to the vertex in the adjacent row. So, we have the matching

$$\left\{\{v_{2i-1,j}, v_{2i,j}\} : 1 \leq i \leq \frac{m}{2}\ 1 \leq j \leq n\right\}$$

The same argument applies for when n is even,

$$\left\{\{v_{i,2j-1}, v_{i,2j}\} : 1 \leq i \leq m\ 1 \leq j \leq \frac{n}{2}\right\}$$

So in either case, we have a perfect matching. The size of the maximum matching is $\frac{mn}{2}$.

- **Case 2:** mn **is odd.** Similarly, to the first case, but this time we have both m and n are odd, so there is a row (or column) of vertices that are not being matched to any other vertex. The size of the maximum matching is $\frac{mn-1}{2}$ and it is not perfect.

9.22 Question 22

For all $1 \leq m \leq n$, find the size of a maximum matching in $K_{m,n}$. For what values of m and n do we have a perfect matching? Prove that your answer is correct

Answer: Let $G = (V, E)$, we'll partition V into 2 sets V_1 and V_2 where $|V_1| = m$ and $|V_2| = n$. Since $K_{m,n}$ is bipartite graph, we will use Hall's Theorem. Assume without loss of generality that $m \leq n$. Then we have that there exists a matching for all vertices in V_1 since $|N(S)| \geq |S|$ for all $S \subseteq V_1$ (since in a $K_{m,n}$ graph, each vertex in the set V_1 is mapped to each vertex in the set V_2). So, the size of a maximum matching is m and it is not perfect. In the case where $n \geq m$, we can use the same argument to show that the size of a maximum matching is n and it is not perfect. So the maximum matching size is $\min m, n$. Now when $m = n$, we have a perfect matching since $K_{m,n}$ is a complete bipartite graph, so each vertex in V_1 has an edge to each vertex in V_2.

9.23 Question 23

Prove or disprove.

(a) The graph $G = (V, \{\})$ is bipartite.

(b) The graph $G = (V, \{\})$ is a forest.

Answer:

(a) Since the graph G has no edges, it has no cycles, so by Theorem 22.0.1, it is bipartite.

(b) The graph G has no edges, so it is a forest since it has no cycles.

Note: Again, for part a the prof considers the graph G to *not* be bipartite for $|V| = 1$, so this holds for all V where $|V| \geq 1$.

9.24 Question 24

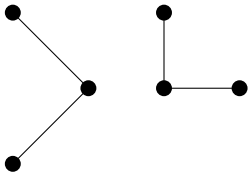
(a) Does there exist a graph with 6 vertices, where the degrees of vertices are 1,1,1,1,2 and 2? Prove your answer is correct.

(b) Same question, but this time, we want a connected graph.

(c) Same question, but this time, we want a bipartite graph.

Answer:

(a) Yes, example:



(b) No, since the highest degree for this graph is 2, we have no cycles. So it is a forest. Then by Theorem 20.0.1, we have $n = |V| = 6$ and $m = |E| = 4$, so $n > m$ and G has $n-m$ connected components. So G has $n-m = 6-4 = 2$ connected components, so it is not connected.

(c) Yes, example: