Math 150: Discrete Mathematics

Midterm Exam 2

Tuesday, November 5, 2024

NAME (please print legibly): Solutions

Your University ID Number: _____

Your University email _____

Indicate your instructor with a check in the appropriate box:

Dannenberg	MW 2:00-3:15pm	
Dannenberg	MW 12:30-1:45pm	
Almomani	TR 2:00-3:15pm	
Nathan	MW 4:50-6:05pm	
Dannenberg	**Math 150A**	

- You are responsible for checking that this exam has all 8 pages.
- No calculators, phones, electronic devices, books, notes are allowed during the exam.
- Show all work and justify all answers.

PLEASE COPY THE HONOR PLEDGE AND SIGN:

I affirm that I will not give or receive any unauthorized help on this exam, and all work will be my own.

_____

_____

_____

YOUR SIGNATURE:_____

1. (20 points) The following are a number of True or False statements related to modular arithmetic. For each, if you believe the answer is True, you do not need to justify your answer. If you believe the answer is False, give a counterexample/justification of your answer.

1. If $x \equiv 2 \pmod 8$ and $y \equiv 7 \pmod 8$, then $x + y \equiv 1 \pmod 8$.

T

2. If $x \equiv 5 \pmod 8$ and $y \equiv -6 \pmod 8$, then $xy \equiv 2 \pmod 8$.

T

3. If $x \equiv 4 \pmod 8$ and $y \equiv 4 \pmod 8$, then $\frac{x}{y} \equiv 1 \pmod 8$.

$\frac{x}{y}$ is not necessarily defined - may not be an integer

$6 \times = 4$
$y = 12$

F

4. If a, b and $m > 1$ are integers such that $ab \equiv 0 \pmod m$, then $a \equiv 0 \pmod m$ or $b \equiv 0 \pmod m$.

$m = 6, \quad a = 2, \quad b = 3$

$ab = 6 \equiv 0 \pmod 6$
$a, b \not\equiv 0 \pmod 6$

F

2. (20 points) Consider the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n, m) = n + m$$

1. Is f injective (one-to-one)? Give a proof or show why not.

f is not injective.

Consider (0,1) and (1,0)'s images under f.

$f(0,1) = 0+1 = 1 = 1+0 = f(1,0)$

Thus, f is not injective.

2. Is f surjective (onto)? Give a proof or show why not.

Let $k \in \mathbb{Z}$. Note that $f(k,0) = k$.

Since $(k,0) \in \mathbb{Z} \times \mathbb{Z}$ as desired, we see that f is surjective.

3. Is f a bijection? Justify your answer.

f is not injective, so is not a bijection

3. (20 points)

1. Given functions $f, g : \mathbb{R} \to \mathbb{R}$, give a precise definition of what it means for f to be in $\Theta(g)$.

① $\exists C_1, C_2, k > 0$ s.t. $C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|$

② $f \in \mathcal{O}(g)$ and $f \in \Omega(g)$

2. Give an example of a function $f : \mathbb{N} \to \mathbb{R}$ which is not in $\mathcal{O}(x^a)$ for any $a \in \mathbb{R}$. You do not need to prove your answer.

$f(x) = 2^x$ increases faster than any polynomial.

$f(x) = x!$ or $f(x) = x^x$ also works.

3. Let $f : \mathbb{N} \to \mathbb{N}$ be defined by the sum

$$f(n) = 1^{13} + 2^{13} + 3^{13} + \cdots + n^{13}.$$

Find the smallest integer a such that $f(n) \in \mathcal{O}(n^a)$. Find witnesses to prove this claim. **Show your work clearly so that it can be understood how you are justifying your claim.**

$a = 14$

Observe that every term in the summation is less than the last term, so

$$f(n) = 1^{13} + 2^{13} + 3^{13} + \ldots + n^{13}$$

$$\leq \underbrace{n^{13} + n^{13} + n^{13} + \ldots + n^{13}}_{n \text{ terms}}$$

$$= n^{14}$$

n is arbitrary, so let $k = 1$ and $C = 1$ be our witnesses.

4. (20 points) Consider the number $N = (561)_8$.

1. Write N in binary. For this part of the question, you **must** convert N into a decimal number first, and then convert that decimal number into binary. Show all of your work.

octal to decimal

$$(561)_8 = 5 \cdot 8^2 + 6 \cdot 8 + 1$$
$$= 320 + 48 + 1 = 369$$

decimal to binary

$$369 = 2 \cdot 184 + 1$$
$$184 = 2 \cdot 92 + 0$$
$$92 = 2 \cdot 46 + 0$$
$$46 = 2 \cdot 23 + 0$$
$$23 = 2 \cdot 11 + 1$$
$$11 = 2 \cdot 5 + 1$$

$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$
$$1 = 2 \cdot 0 + 1$$

Thus, $369 = (101110001)_2$

2. Write N in binary. For this part of the question, you **must** convert N directly from octal into binary. Explain your process.

Each octal digit becomes 3 bits.

$$(5)_8 = (101)_2$$
$$(6)_8 = (110)_2$$
$$(1)_8 = (001)_2$$

$$(561)_8 = (101\ 110\ 001)_2$$

3. Use modular exponentiation to compute $7^N \mod 13$.

We already have $N = (10111\,0001)_2$

① Tabular method

	$X = 1$	power $= 7$
1	$1 \cdot 7 \equiv 7$	$7^2 \equiv 49 \equiv 10$
0	7	$10^2 \equiv 100 \equiv 9$
0	7	$9^2 \equiv 81 \equiv 3$
0	7	$3^2 \equiv 9$
1	$7 \cdot 9 = 63 \equiv 11$	$9^2 \equiv 3$
1	$11 \cdot 3 \equiv 33 \equiv 7$	$3^2 \equiv 9$
1	$7 \cdot 9 \equiv 63 \equiv 11$	$9^2 \equiv 3$
0	11	$3^2 \equiv 9$
1	$11 \cdot 9 \equiv 99 \equiv \boxed{8}$	

$7^N \mod 13 = \boxed{8}$

② "Symbolic" use of algorithm

$7^N = 7^{(2^0)} \cdot 7^{(2^4)} \cdot 7^{(2^5)} \cdot 7^{(2^6)} \cdot 7^{(2^8)}$

$= 7^1 \cdot 7^{16} \cdot 7^{32} \cdot 7^{64} \cdot 7^{256}$

$7^1 \mod 13 \equiv 7$

$7^2 \mod 13 \equiv 10$

$7^4 \mod 13 \equiv 9$

$7^8 \mod 13 = 3$

$7^{16} \mod 13 = 9$

$7^{32} \mod 13 = 3$

$7^{64} \mod 13 = 9$

$7^{128} \mod 13 = 3$

$7^{256} \mod 13 \equiv 9$

$7^N \mod 13 = (7 \cdot 9 \cdot 3 \cdot 9 \cdot 9) \mod 13$

$= (63 \cdot 27 \cdot 9) \mod 13$

$= (11 \cdot 1 \cdot 9) \mod 13$

$= (99) \mod 13$

$= \boxed{8}$

5. (20 points)

1. Let a, m be integers with $m > 1$ and $\gcd(a, m) = 1$. Give a definition of the **inverse of a modulo m.**

The inverse of a modulo m is the integer $\bar{a}$ such that $\bar{a} \cdot a \equiv 1 \pmod{m}$.

($\bar{a}$ is unique mod m)

2. Find the inverse of 65 modulo 233. Your answer should be the smallest possible non-negative integer satisfying this condition.

Euclidean Algorithm:

$233 = 3 \cdot 65 + 38$
$65 = 1 \cdot 38 + 27$
$38 = 1 \cdot 27 + 11$
$27 = 2 \cdot 11 + 5$
$11 = 2 \cdot 5 + 1$ ← $\gcd(65, 233) = 1$
$5 = 5 \cdot 1 + 0$

Bezout coefficients

$1 = 11 - 2 \cdot 5$
$= 11 - 2 \cdot (27 - 2 \cdot 11)$
$= 5 \cdot 11 - 2 \cdot 27$
$= 5 \cdot (38 - 1 \cdot 27) - 2 \cdot 27$
$= 5 \cdot 38 - 7 \cdot 27$
$= 5 \cdot 38 - 7 \cdot (65 - 1 \cdot 38)$
$= 12 \cdot 38 - 7 \cdot 65$
$= 12 \cdot (233 - 3 \cdot 65) - 7 \cdot 65$
$= 12 \cdot 233 - 43 \cdot 65$

→ Our answer should be non-negative so inverse is **190**

3. Solve the following equation for x.

$$65x \equiv 3 \pmod{233}.$$

We multiply both sides by the inverse of 65 mod 233

$190 \cdot 65x \equiv 190 \cdot 3 \pmod{233}$

$12350x \equiv 570 \pmod{233}$

$1 \cdot x \equiv 104 \pmod{233}$

$x \equiv 104 \pmod{233}$

104

190×65: $950 + 11400 = 12350$

$12350 \div 233 = 53$ remainder -1165, 700

$570 \div 233 = 2$ remainder 104 (-466)

$233 \times 2 = 466$, $233 \times 4 = 932$

This page intentionally left blank.