CUNY Queens College
CSCI 220 - 11
Instructor: Xinying Chyn

EXAM # 1

Department of Computer Science
Spring 2022
March 8, 2022

10:45 AM – 12:00PM, Tuesday, March 8, 2022 (Total of 75 minutes)

Complete all of the following information.

STUDENT **LAST** NAME (PRINT): ____

STUDENT **FIRST** NAME (PRINT):____

CUNY ID #: ______________________________________

THIS IS A CLOSED BOOK TEST.
NO BOOKS, NOTES, COMPUTERS, CELL PHONES, OR OTHER ELECTRONICS

THE CALCULATOR IS <u>NOT</u> ALLOWED IN THIS EXAM.

It is the Department policy to give a grade of F to any student who helps or receives help from any other student during an exam.

The exam has 9 questions out of 100 points in total.

If your printed exam is missing any problem, please notify the proctor as soon as possible.

ANSWER THE QUESTIONS IN THE SPACES PROVIDED.
SHOW ALL WORK TO RECEIVE FULL CREDIT.

Question:	1	2	3	4	5	6	7	8	9	Grade
Points:										

Problem 1: [20 points]
Reduce the following modulus to the LNR form
Show all your calculation.

a) $-220 \pmod{23}$

$-220 + 230 = 10$

$\boxed{10 \pmod{23}}$

b) $123 * 321 \pmod{23}$

$23 \times 5 = 115 \qquad 23 \times 4 = 92$

$$\begin{array}{r} 123 \\ -115 \\ \hline 8 \end{array} \qquad \begin{array}{r} 321 \\ -230 \\ \hline 91 \\ -92 \\ \hline -1 \end{array}$$

$123 * 321 \equiv 8 * -1 \equiv -8 \equiv \boxed{15 \pmod{23}}$

c) $25! \pmod{23}$

$25! \equiv 25 \cdot 24 \cdot 23 \cdot 22 \cdot \cdots \cdot 2 \cdot 1$

$\equiv 25 \cdot 24 \cdot 0 \cdot 22 \cdot \cdots \cdot 2 \cdot 1$

$\equiv 0 \pmod{23}$

d) $3^{222} \pmod{23}$

23 is prime, FLT: $3^{22} \equiv 1 \pmod{23}$

$3^{222} \equiv (3^{22})^{10} \cdot 3^2 \equiv 1^{10} \cdot 3^2 \equiv 1 \cdot 9 \equiv \boxed{9 \pmod{23}}$

e) $11^{-1} \pmod{23}$, find the inverse of 11 (mod 23)

$11x \equiv 1 \pmod{23} \Rightarrow 11x + 23k = 1$

$23 = 11(2) + 1 \longrightarrow 1 = 23(1) + 11(-2)$

$11(-2) \equiv -22 \equiv 1 \pmod{23}$

$+23$

$11^{-1} \equiv -2 \underset{+23}{} \equiv \boxed{21 \pmod{23}}$

Problem 2: [8 points] CRT

Find all integers (in modular form) x such that when x divided by 5, the remainder is 3; when x divided by 7, the remainder is 4; when x divided by 8, the remainder is 6.

Show all your calculation and explain how you got all the solution (why is your modular covered all solution).

$x \equiv 3 \pmod 5 \equiv 8 \equiv 13 \equiv 18$

$x \equiv 4 \pmod 7 \equiv 18$

$x \equiv 6 \pmod 8 \equiv 158$

$x \equiv 18 \pmod{35}$

$\equiv 53 \leftarrow \equiv 13 \equiv 5 \pmod 8$

$\equiv 88 \leftarrow \equiv 0 \pmod 8$

$\equiv 123 \leftarrow \equiv 3 \pmod 8$

$\equiv 158 \leftarrow \equiv -2 \equiv 6 \pmod 8$

$x \equiv 158 \pmod{280}$

5, 7, 8 are pairwise relatively prime.

by CRT, there is an unique solution (mod $5 \times 7 \times 8$).

Therefor 158 (mod 280) are the only solution.

Problem 3: [8 points]

Checking primality

a) Is 109 a prime? If so, prove it. If not, find the prime factors.

$\sqrt{109} = 10....$ Primes $\leq \sqrt{109}$: 2, 3, 5, 7,

$2 \nmid 109$

$3 \nmid 109$

$5 \nmid 109$

$7 \nmid 109$

$$\begin{array}{r} 109 \\ -70 \\ \hline 39 \\ -35 \\ \hline 4 \end{array}$$

109 is a prime.

b) Is 119 a prime? If so, prove it. If not, find the prime factors.

$\sqrt{119} = 10....$ Primes $\leq \sqrt{119} = 2, 3, 5, 7$

119 is not a prime.

$2 \nmid 119$

$3 \nmid 119$

$5 \nmid 119$

$7 \mid 119$

$$\begin{array}{rl} 119 & \\ -70 & \cdot 10 \cdot 7 \\ \hline 49 & \\ -49 & 7 \cdot 7 \\ \hline 0 & \end{array}$$

$119 = 7 \cdot 17$

$\boxed{\{7, 17\}}$

Problem 4: [10 points]
Base conversion. Show all your calculation.
a) Find the base 3 expansion of $(333)_{10}$.

$333 = 3(111) + 0$
$111 = 3(37) + 0$
$37 = 3(12) + 1$
$12 = 3(4) + 0$
$4 = 3(1) + 1$
$1 = 3(0) + 1$ STOP.

$(333)_{10} = \boxed{(110100)_3}$

b) Find the decimal (base 10) expansion of $(110100)_2$.

$$\begin{array}{cccccc} 32 & 16 & 8 & 4 & 2 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 5 & 4 & 3 & 2 & 1 & 0 \end{array}$$

$(110100)_2$

$1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 0$
$= 32 + 16 + 0 + 4 + 0 + 0 = \boxed{(52)_{10}}$

Problem 5: [14 points]
Given a, b, and c are positive integers. Determine whether the following statements are true or false. State TRUE or FALSE! If true, prove it. If false, provide a counterexample.
a) If $ab|c$, then $a|c$ and $b|c$.

True

$ab | c \rightarrow \exists k \in \mathbb{Z} : \quad c = ab \cdot k$
$c \equiv 0 \pmod{ab}$ $\quad c = a(bk) \rightarrow a|c$
$c \equiv 0 \pmod{a}$ $\quad c \equiv 0 \pmod{b}$ $\quad c = b(ak) \rightarrow b|c$ ✓

b) If $a|c$ and $b|c$, then $ab|c$.

False.

$2|2, \; 2|2 \rightarrow 2 \cdot 2 \nmid 2$
$4|12, \; 6|12 \rightarrow \underbrace{4 \cdot 6}_{24} \nmid 12$

c) If $c|ab$, then $c|a$ and $c|b$.

False

$12 | 3 \cdot 4 \rightarrow 12 \nmid 3$ and $12 \nmid 4$.

Problem 6: [10 points]
Solve for all values of x where $51x \equiv 15\ (mod\ 72)$ using the method from lecture.
Make sure your answer is in the least non-negative residue form.
Show all your work and the calculations.

$51x \equiv 15 \pmod{72} \rightarrow 51x + 72k = 15$

$\gcd(51, 72) = 3 \qquad 3 \mid 15\ \checkmark$

$72 = 51(1) + 21$

$51 = 21(2) + 9$

$21 = 9(2) + 3$

$9 = 3(3) + 0$

$3 = 21(1) + 9(-2)$

$= 21(1) + [51(1) + 21(-2)](-2)$

$= 21(5) + 51(-2)$

$= (72(1) + 51(-1))(5) + 51(-2)$

$3 = 51(-7) + 72(5)$

$5\times$ $\downarrow\times 5$ $\downarrow\times 5$

$15 = 51(-35) + 72(25)$

x

$x \equiv -35 \left(\mod \frac{72}{3}\right)$

$x \equiv -35 \pmod{24}$

$+48$

$$\boxed{x \equiv 13 \pmod{24}}$$

Problem 7: [10 points]
Using mathematical induction to show that $1 + 2 + 3 + \cdots + \overset{2(1)}{\overset{\downarrow}{2n}} = 2n^2 + n$ for positive integer n.
Show all your steps.

Basis step: $n = 1$ $\quad 1+2 = 2(1)^2 + 1$

$3 = 3$ ✓

Inductive step: IH: Assume $1+2+3+\cdots+2k = 2k^2+k$, for $k \geq 1$.

Want to show $1+2+3+\cdots+2(k+1) = 2(k+1)^2+(k+1)$.

$\underbrace{1+2+3+\cdots+2k}+(2k+1)+(2k+2) = 2(k^2+2k+1)+(k+1)$

by IH, $2k^2+k+(2k+1)+(2k+2) = 2k^2+4k+2+k+1$

$2k^2+5k+3 = 2k^2+5k+3$ ✓

Problem 8: [10 points]

a) Determine whether $\log(x^3)$ is $O(\log x)$. Explain your answer.

$$\log(x^3) = 3\log x \leq 3\log x \quad \text{for } x > 1, \quad \boxed{\begin{array}{l} C=3 \\ k=1 \end{array}}$$

$$\lim_{x\to\infty} \frac{\log(x^3)}{\log(x)} = 3 \text{ is bounded}$$

$$\log(x^3) = O(\log x)$$

b) Determine whether $220x^{220}$ is $o\left(\frac{x^{222}}{222}\right)$. Explain your answer.

$$\lim_{x\to\infty} \frac{220x^{220} \cdot 222}{\frac{x^{222}}{\cancel{222}} \cdot \cancel{222}} = \lim_{x\to\infty} \frac{220 \cdot 222 \cdot \cancel{x^{220}}}{x^{\cancel{222}\,2}} = 0$$

$$220x^{220} = o\left(\frac{x^{222}}{222}\right)$$

Problem 9: [10 points]

a) Find example of $f(x)$ such that $f(x) = O(x^2)$ and $x = o(f(x))$.
If it's not possible, explain why that's the case.

$$\lim_{x\to\infty} \frac{f(x)}{x^2} \neq \infty \qquad \lim_{x\to\infty} \frac{x}{f(x)} = 0$$

$$f(x) = x^2$$

$$f(x) = x \cdot \sqrt{x} \qquad f(x) = x\log(x)$$

b) Find example of $f(x)$ such that $f(x) = O(x^2)$ and $x^2 = o(f(x))$.
If it's not possible, explain why that's the case.

$$\lim_{x\to\infty} \frac{f(x)}{x^2} \neq \infty, \quad \lim_{x\to\infty} \frac{x^2}{f(x)} = 0$$

cannot satisfy at the same time.

It's impossible.