CS 201: Discrete Math for Computer Science
2020 Spring Semester Midterm Exam

16:00 – 18:00, Apr. 10th, 2020
Total number of questions: 9
Total points: 100

Note: The Midterm exam is **closed book**. Please do *NOT* refer to the textbook or any other references. Any misbehavior will be dealt with severely according to our plagiarism regulation. Please upload your solutions to **Blackboard before 18:30** (You have half an hour to upload!) **No extended submission will be accepted!** Good luck!

Q.1 (11 points) Consider the proposition $((p \to q) \to p) \to q)$.

(1) Construct the truth table for this proposition.

(2) Show that this proposition is *not* logically equivalent to $p \to (q \to (p \to q))$.

Solution:

(1) The truth table is:

p	q	$p \to q$	$(p \to q) \to p$	$((p \to q) \to p) \to q)$
F	F	T	F	T
F	T	T	F	T
T	F	F	T	F
T	T	T	T	T

(2) There are two ways to do this:

- Using a truth table:

p	q	$p \to q$	$q \to (p \to q)$	$p \to (q \to (p \to q))$
F	F	T	T	T
F	T	T	T	T
T	F	F	T	T
T	T	T	T	T

We now can see that the rightmost column does *not* match the rightmost column in the truth table for $((p \to q) \to p) \to q$.

– Using logical equivalences:

$$\begin{aligned} p \to (q \to (p \to q)) &\equiv \neg p \vee (\neg q \vee (\neg p \vee q)) \\ &\equiv (\neg p \vee \vee p) \vee (\neg q \vee q) \\ &\equiv \neg p \vee T \\ &\equiv T. \end{aligned}$$

By the truth table for $((p \to q) \to p) \to q$, they are *not* logically equivalent.

Q.2 (12 points) For the following argument, explain which rules of inference are used for each step.

"All students are hard-working. There is a student who will go to CMU. Therefore, there is a hard-working student who will go to CMU." The universe is "all members in CSE department".

Solution: Let $s(x)$ be "x is a student" let $c(x)$ be "x will go to CMU", and let $h(x)$ be "x is hard-working". we are given premises $\forall x(s(x) \to h(x))$ and $\exists x(s(x) \wedge c(x))$, and we want to conclude $\exists x(c(x) \wedge h(x))$.

step	**reason**
1. $\exists x(s(x) \wedge c(x))$	hypothesis
2. $s(y) \wedge c(y)$	existential instantiation using 1.
3. $s(y)$	simplification using 2.
4. $\forall x(s(x) \to h(x))$	hypothesis
5. $s(y) \to h(y)$	universal instantiation using 4.
6. $h(y)$	modus ponens using 3. and 5.
7. $c(y)$	simplification using 2.
8. $s(y) \wedge h(y) \wedge c(y)$	conjunction using 3, 6 and 7.
9. $\exists x(s(x) \wedge c(x) \wedge h(x))$	existential generalization using 8.

Q.3 (9 points) If two sets A and B are both *uncountable sets*, then what kind of sets can $A \cap B$ be, *finite*, *countably infinite* or *uncountable*? Give examples to explain your answer.

Solution: $A \cap B$ can be finite, e.g., $A = \{x \in \mathbb{R} | x \geq 0\}$, and $B = \{x \in \mathbb{R} | x \leq 0\}$;

$A \cap B$ can be countably infinite, e.g., $A = \{x \in \mathbb{R} | 0 < x < 1\} \cup \mathbb{N}$, and $B = \{x \in \mathbb{R} | 1 < x < 2\} \cup \mathbb{N}$;

$A \cap B$ can be uncountable, e.g., $A = \{x \in \mathbb{R} | 0 < x < 1\}$, and $B = \{x \in \mathbb{R} | 0 < x < 2\}$.

Q.4 (10 points) Consider the function $f : \mathbb{R}^2 \to \mathbb{R}^2$ defined as $(x, y) \mapsto (2x - y, -x + 2y)$. Prove or disprove that f is a bijective function.

Solution: First, let's show that f is one-to-one. Let (x, y) and (u, v) be two elements of $\mathbb{R}^2$ satisfying $f(x,y) = f(u,v)$. By definition of f, we have

$$(2x - y, -x + 2y) = (2u - v, -u + 2v).$$

This means that their coordinates are the same, i.e.,

$$\begin{array}{ll} (1) & 2x - y = 2u - v \\ (2) & -x + 2y = -u + 2v. \end{array}$$

Multiplying Eq. (2) by 2 and adding to Eq. (1), we have

$$(2x - y) + 2(-x + 2y) = (2u - v) + 2(-u + 2y).$$

Then we have $y = v$. It then follows that $x = u$ and further $(x,y) = (u,v)$. This proves that f is indeed one-to-one.

Next, let's show that f is onto. For any element $(u,v) \in \mathbb{R}^2$, we want to find an element (x,y) satisfying $f(x,y) = (u,v)$, i.e., $(2x - y, -x + 2y) = (u,v)$. By solving this system of linear equations, we have $(x,y) = (\frac{2}{3}u + \frac{1}{3}v, \frac{1}{3}u + \frac{2}{3}v)$. This prove that f is onto.

Q.5 (12 points)

(1) Derive a formula in terms of n for the summation $\sum_{i=1}^{n} i \cdot 2^{-i}$.

(2) Give a formula for $\sum_{i \geq 1} i \cdot 2^{-i}$.

Solution:

(1) We start from the summation of the first n terms in the geometric progression.

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

Taking the discrete derivative for both sides, we have

$$\begin{aligned} \sum_{i=1}^{n} i \cdot x^{i-1} &= \frac{(x - x^{n+1})'(1 - x) - (x - x^{n+1})(1 - x)'}{(1 - x)^2} \\ &= \frac{nx^{n+1} - (n+1)x^n + 1}{(1 - x)^2}. \end{aligned}$$

Thus, we have

$$\sum_{i=1}^{n} i \cdot x^i = \frac{nx^{n+2} - (n+1)x^{n+1} + x}{(1 - x)^2}.$$

Replacing x by $1/2$, we have

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

(2) We have

$$
\begin{aligned}
\sum_{i\geq 1} i\cdot 2^{-i} &= \lim_{n\to\infty}\sum_{i=1}^{n} i\cdot 2^{-i} \\
&= \lim_{n\to\infty}\left(2-(n+2)\cdot 2^{-n}\right) \\
&= 2.
\end{aligned}
$$

Q.6 (10 points) For three positive integers a, b and k, prove or disprove that

$$\gcd(ka, kb) = k\gcd(a, b).$$

Solution: Let $d = \gcd(a, b)$ and let $d' = \gcd(ka, kb)$. We want to prove that $d' = kd$. Since $d = \gcd(a, b)$, by Bezout's identity, there exist integers s and t such that $d = sa + tb$. Then we have $kd = s(ka) + t(kb)$. Thus, kd is a linear combination of ka and kb. This means $d'|kd$.

On the other hand, since $d|a$ and $d|b$, we have $kd|ka$ and $kd|kb$. Then kd is a common divisor of ka and kb. However, $d' = \gcd(ka, kb)$ is the largest one of the common divisors. It follows that $kd \leq d'$.

Therefore, we have $d' = kd$, i.e., $\gcd(ka, kb) = k\gcd(a, b)$.

Q.7 (12 points) Consider the numbers of the form $n^{13} - 2n^7 + n$, where n is an integer. Determine for which values of n, the number $n^{13} - 2n^7 + n$ is divisible by 98.

Solution: Since $98 = 2\cdot 7^2$ and $\gcd(2, 49) = 1$, we need show that $n^{13} - 2n^7 + n$ is divisible by 2 and 49. Note that $-2n^7$ is even, and n^{13}, n always have the same parity. Thus, $n^{13} - 2n^7 + n$ is always even. It remains to prove that $n^{13} - 2n^7 + n$ is also divisible by 49. We factor this polynomial and have

$$n^{13} - 2n^7 + n = n\cdot(n^6 - 1)^2.$$

If n is not a multiple of 7, then $n^6 - 1$ is divisible by 7 by Fermat's little theorem, and as there are two such factors, $n^{13} - 2n^7 + n$ is indeed divisible by 49. If n is a multiple of 7, then $n^6 - 1$ is not divisible by 7, and since we only have one such factor n, it follows that n is divisible by 49.

To sum up, $n^{13} - 2n^7 + n$ is divisible by 98 if and only if n is either divisible by 49 or not divisible by 7.

Q.8 (14 points) For a collection of balls, the number is not known. If we count them by 2's, we have 1 left over; by 3, we have nothing left; by 4, we have 1 left over; by 5, we have 4 left over; by 6, we have 3 left over; by 7, we have nothing left; by 8, we have 1 left over; by 9, nothing is left. How many balls are there? Give the details of your calculation.

Solution:

This is equivalent to solve the following system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 6 \\ x &\equiv 0 \pmod 7 \\ x &\equiv 1 \pmod 8 \\ x &\equiv 0 \pmod 9 \end{aligned}$$

Since $x \equiv 3 \pmod 6$, we have $x = 6k + 3$ and further have $x \equiv 1 \pmod 2$ and $x \equiv 0 \pmod 3$. Thus, $x \equiv 3 \pmod 6$ is redundant in the system and can be ignored. Note that $x \equiv 1 \pmod 8$ implies both $x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 4$, and $x \equiv 0 \pmod 9$ implies $x \equiv 0 \pmod 3$. We thus have an equivalent but refreshed system of congruences as:

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 0 \pmod 7 \\ x &\equiv 1 \pmod 8 \\ x &\equiv 0 \pmod 9 \end{aligned}$$

All the m_i's are pairwise relatively prime, and we are able to use Chinese Remainder Theorem or back substitution to solve this system of congruences. Note that $m = 5 \cdot 7 \cdot 8 \cdot 9 = 2520$, $M_1 = 7 \cdot 8 \cdot 9 = 504$, $M_2 = 5 \cdot 8 \cdot 9 = 360$, $M_3 = 5 \cdot 7 \cdot 9 = 315$, and $M_4 = 5 \cdot 7 \cdot 8 = 280$. By extended Euclidean algorithm, we have $y_1 = 4$, $y_2 = 5$, $y_3 = 3$, and $y_4 = 1$. Then by Chinese Remainder Theorem, we have the solution is

$$x \equiv 4 * 504 * 4 + 0 + 1 * 315 * 3 + 0 \pmod{2520} \equiv 1449 \pmod{2520}.$$

Q.9 (10 points) Recall the RSA public key cryptosystem: Bob posts a public key (n, e) and keeps a secret key d, where n is the product of two prime numbers. When Alice wants to send a message $0 < M < n$ to Bob, she calculates $C = M^e \pmod n$ and sends C to Bob. Bob then decrypts this by calculating $C^d \pmod n$. Given the value of $\phi(n) = (7070)_8$ in *octal expansion* for $n = (7263)_8$ also in *octal expansion*. Can you factorize n, i.e., to find the values of p and q? Explain your answer.

Solution: Yes. We first convert the two values to decimal numbers: by computing the values of the two numbers, we have

$$\begin{aligned} (7070)_8 &= 7 \cdot 8^3 + 7 \cdot 8^1 = 3640 \\ (7263)_8 &= 7 \cdot 8^3 + 2 \cdot 8^2 + 6 \cdot 8^1 + 3 = 3763. \end{aligned}$$

By the equation $\phi(n) = (p-1)(q-1) = (n+1) - (p+q)$, we know that $pq = n = 3763$ and $p + q = (n+1) - \phi(n) = 124$. Thus, p and q are the two root of the equation

$$x^2 - 124x + 3763 = 0.$$

By the well-known quadratic formula, we have

$$\begin{aligned} p,\ q &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \\ &= \frac{124 \pm \sqrt{124^2 - 4 * 3763}}{2} \\ &= \frac{124 \pm 18}{2} \\ &= 53,\ 71. \end{aligned}$$