University of Toronto Scarborough
Final Exam Sample, MATA67 and CSCA67: Discrete Mathematics, Summer 2024
Section: LEC01, Erfan Meskar
Duration: 3 hours
Aids: No aid-sheet is permitted. No electronic or mechanical computing devices are permitted.

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

- The University of Toronto Scarborough and you, as a student, share a commitment to academic integrity. You are reminded that you may be charged with an academic offence for possessing any unauthorized aids during the writing of an exam. Clear, sealable, plastic bags have been provided for all electronic devices with storage, including but not limited to: cell phones, smart watches, SMART devices, tablets, laptops, and calculators. Please turn off all devices, seal them in the bag provided, and place the bag under your desk for the duration of the examination. You will not be able to touch the bag or its contents until the exam is over. If, during an exam, any of these items are found on your person or in the area of your desk other than in the clear, sealable, plastic bag, you may be charged with an academic offence. A typical penalty for an academic offence may cause you to fail the course.
- There are 9 questions and 12 pages in this exam, including this one. When you receive the signal to start, please make sure that your copy of the examination is complete.
- Answer each question directly on the examination paper, in the space provided. **Please write carefully and clearly, in complete English sentences.**
- Do not under any circumstances unstaple the exam.

Q1 **(True or False)** Choose the correct answer by checking the appropriate box.

1.a (1 point) The compound propositions $(p \leftrightarrow q) \rightarrow r$ and $r \vee (\neg p \leftrightarrow \neg q)$ are logically equivalent.

□ TRUE □ FALSE

1.b (1.5 point) Consider the claim "for any integers a and b, if ab is an even, then a or b is even." Which of the following proofs is a valid proof of this claim?

□ Assume arbitrary integers a and b. Assume that a or b is even - say it is a (the case where b is even will be identical, with roles of a and b reversed). Choose k such that $a = 2k$. Observe that $ab = (2k)b = 2(kb)$. Thus, ab is even.

□ Assume arbitrary integers a and b. Assume a and b are odd. Choose k and m such that $a = 2k + 1$ and $b = 2m + 1$. Then $ab = 4km + 2k + 2m + 1 = 2(2km + k + m) + 1$. Observe that $(2km + k + m)$ is an integer. Therefore, ab is odd.

□ Assume arbitrary integers a and b. By way of contradiction, assume a or b is even but ab is odd. Assume a is even (the case where b is even will be identical, with roles of a and b reversed). Choose k such that $a = 2k$. Observe that $ab = (2k)b = 2(kb)$. Thus, ab is even, which is a contradiction.

1.c (1 point) Consider the statement "for any non-empty set A, if $\{x\} \in \mathcal{P}(A)$ then $x \in A$. The next paragraph claims to prove this statement. Is this proof correct?

> Assume A is an arbitrary non-empty set. Suppose x is an arbitrary element of A. Then, by definition of the power set, there will be a singleton set containing x in $\mathcal{P}(A)$, that is, $\{x\} \in \mathcal{P}(A)$, as desired.

[**RECALL:** $\mathcal{P}(A)$ denotes the power set of A.]

□ The proof is correct.

□ The proof is incorrect.

1.d (1 points) Assume arbitrary events A and B defined over the same probability space. Assume that $0 < \mathbb{P}(A) < 1$ and $0 < \mathbb{P}(B) < 1$. Determine which of the following statements are true.

1.d. i $\mathbb{P}(A \cup B) \geq \mathbb{P}(A) + \mathbb{P}(B)$ □ TRUE □ FALSE

1.d. ii $\mathbb{P}(A \cap \overline{B}) = \mathbb{P}(\overline{B}) - \mathbb{P}(\overline{A} \cap \overline{B})$ □ TRUE □ FALSE

1.e (1 point) The set containing all infinite binary strings is uncountable.

□ TRUE □ FALSE

Q2 **(Short answer)** No explanation is needed for questions **2.a** to **2.e**.

2.a **(4 points)** Consider the following statement.

> "There are exactly two math major students who are neither computer science major nor engineering major students."

Translate this statement from English to predicate logic with existential (*i.e.*, $\exists$) and universal (*i.e.*, $\forall$) quantifiers. Let the domain be the set of all students at UTSC and let

- $M(x)$ be x is a math major.
- $C(x)$ be x is a computer science major.
- $E(x)$ be x is an engineering major.

[**NOTE:** You are **not allowed** to use uniqueness quantifier (*i.e.*, $\exists!$).]

[**Write your answer here.**]

2.b **(1 points)** Fill in the blanks with the proper function properties "injective", "not injective", "surjective", and "not surjective."
[**RECALL:** Injective is another word for a one-to-one function. Surjective is another word for an onto function.]

1. Assume arbitrary sets A and B. Suppose that $f : A \to B$ is arbitrary. To show that f is ________________, show that if $f(x) = f(y)$ for arbitrary $x, y \in A$, then $x = y$.

2. Assume arbitrary sets A and B. Suppose that $f : A \to B$ is arbitrary. To show that f is ________________, find a particular elements $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

2.c **(1 points)** Clearly state the Fundamental Theorem of Arithmetic (FTA).

[**Write your answer here.**]

2.d In class, we studied the binomial theorem, in which we studied $(x+y)^n$. For instance, Consider $(x+y)^2 = (x+y)(x+y)$. before grouping, this polynomial looks like $xx+xy+yx+yy$. Thus, the number of terms in this polynomial before grouping is 4. After grouping, it looks like $x^2+2xy+y^2$. Hence, the number of terms in this polynomial after grouping is 3. Furthermore, the number of times xy appears before grouping (*i.e.*, the coefficient of xy after grouping) is 2.

Now, consider the polynomial $(x+y+z)^n = (x+y+z)(x+y+z)\dots(x+y+z)$.

2.d. i (1 points) What is the number of terms before grouping?

[**Write your answer here.**]

2.d. ii (1 points) What is the number of terms after grouping?

[**Write your answer here.**]

2.d. iii (1 points) What is the number of times $x^{n_1}y^{n_2}z^{n_3}$ appears before grouping (*i.e.*, the coefficient of $x^{n_1}y^{n_2}z^{n_3}$ after grouping)?

[**Write your answer here.**]

2.e (2 points) If n indistinguishable cookies are distributed randomly among 32 distinct children, what is the probability in terms of n that at least one student gets none?

[**Write your answer here.**]

Q3 **(10 points)** A new variation of Covid is spreading across Canada. A Covid test correctly returns a positive among those who have Covid with probability 90% and correctly returns a negative among those who do not have Covid with probability 95%. Suppose that 4% of people in the population have Covid. Let C denotes the event that a person has Covid.

A randomly selected person from the population takes the test and tests positive for Covid. Let T_1 denotes the event that the test result is positive. This person wants to be extra certain that they have Covid, so they take an additional test and get a negative result. Let T_2 denotes the event that the second test result is positive (so $\overline{T_2}$ denotes the event that the second test result is negative).
Find the chance that they have Covid given their first test is positive and their second test is negative.

Assume the test results are independent given the Covid status, *i.e.*, $\mathbb{P}(T_2 \mid C \cap T_1) = \mathbb{P}(T_2 \mid C)$.
[**NOTE:** Answer to the following parts can be left as fractions of sums of products (*e.g.*, as expressions like $\frac{0.9\times0.8+0.7\times0.6}{0.1\times0.2\times0.3+0.4\times0.5}$). Don't simplify your answer any further.]

[**Write your answer here.**]

Q4 **(7 points)** Assume n is an arbitrary positive integer and $k \leq n$ is an arbitrary positive integer. Use a combinatorial argument to establish the identity:

$$\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{n}{k} = \binom{n+1}{k+1}.$$

[**Write your answer here.**]

Q5 **(9 pt)** For positive integers n and N, suppose n draws are made at random with replacement from the values $\{1, \ldots, N\}$. Find the expectation of the maximum value drawn.

[**Write your answer here.**]

Q6 **(9 points)** n gentlemen attend a party, leaving their hats at the door. At the end of the party, they randomly and independently grab hats on their way. What is the probability of none of the gentlemen leaving with his own hat?

[**Write your answer here.**]

Q7 **(8 points)** Use induction to prove the Corollary of Euclid's lemma.

> **Corollary of Euclid's Lemma:** Let $k \geq 1$ be any arbitrary positive integer. For any prime p and any positive integers $a_1, \ldots, a_k$, if $p \mid a_1 a_2 \ldots a_k$, then $p \mid a_j$ for some integer $1 \leq j \leq k$.
> [**NOTE:** Proofs based on prime factorization of p and a_i's **receive** 0 **point**.]

[**Write your answer here.**]

Q8 **(8 points)** Prove that for any non-empty sets A and B, and any function $f : A \to B$, f is surjective if and only if, for any $E \subseteq \mathcal{P}(A)$,

$$B - f(E) \subseteq f(A - E).$$

[**RECALL:** $\mathcal{P}(A)$ denotes the power set of A.]

[**Write your answer here.**]

Q9 An important application of modular arithmetic is to generate a sequence of pseudo-random numbers $x_0, x_1, x_2, \ldots$, defined by the recursion

$$x_n = ax_{n-1} \text{ mod } p, \qquad \text{for } n = 1, 2, 3, \ldots$$

Here p is a prime number, a is a positive integer such that $a \not\equiv 0 \pmod{p}$, and x_0, known as the initialization seed, is a positive integer less than p satisfying $x_0 \not\equiv 0 \pmod{p}$. The *period* d is the smallest positive integer that satisfies $x_d = x_0$; note that the sequence repeats after d numbers have been generated. We want to make d as large as possible. In this problem, you will see how large d can possibly be, using basic facts about modular arithmetic.
[**NOTE:** Proofs based on prime factorization of the parameters defined above **receive** 0 **point**.]

9.a (2 points) For $n \in \mathbb{Z}_{\geq 0}$, find x_n as a function of n, a, and x_0. Write your answer in the box provided; no justification is needed.

[**Write your answer here.**]

9.b (3 points) Prove that $a^d \equiv 1 \pmod{p}$
[**HINT:** for any positive integers a, b, d, and $n > 1$, if $ad \equiv bd \pmod{n}$ and $\gcd(n, d) = 1$, then $a \equiv b \pmod{n}$.]

[**Write your answer here.**]

9.c (5 points) Now let n_0 be the smallest positive integer that satisfies $a^{n_0} \equiv 1 \pmod{p}$. Prove that n_0 divides all positive integers n such that $a^n \equiv 1 \pmod{p}$.

[**Write your answer here.**]

9.d (3 points) Finally, prove that the period d divides $p - 1$.

[**Write your answer here.**]

[**This page is intentionally left blank. You may use it for your scratch notes or extra space for your answers.**]