CMSC-37110 Discrete Mathematics
MIDTERM Tuesday, November 2, 2017

This version includes the correction to Problem 6(b) distributed in class on a separate sheet, and a typo in Problem 15 ("$1, 2, 3$" instead of "$1, 2, \ldots n$") announced on the blackboard.

Name (print): ______________________________
Email:

This exam contributes 20% to your course grade.

Do **not** *use book, notes, scrap paper.* NO ELECTRONIC DEVICES. Use the space provided on the exam sheets; you may continue on the **back of each sheet. Show all your work.** If you are not sure of the meaning of a problem, **ask the instructor.** The XC ("extra credit") problems are underrated, work on them after having done your best on the non-XC problems.

READ THIS!

If a problem speaks about a random element of a given set and does not specify a distribution, the distribution is assumed to be uniform.

You may use results proved in class except if the question is essentially the same as the result proved in clas; in the latter case you are asked to reproduce the proof.

In addition, you may use the following result, stated but not proved in class.

- (Prime Number Theorem) $\pi(x) \sim \dfrac{x}{\ln x}$ where $\pi(x)$ denotes the number of primes $\leq x$.

---

1. (9 points) Let $k \geq 1$. Find the multiplicative inverse of $k^2 + k + 1$ modulo $k^3 + k^2 + k + 1$. Your answer should be a number between 0 and $k^3 + k^2 + k$. Prove your answer.

2. (7 points) Define the concept of a *relation* on a set. Your answer should be a mathematically accurate English sentence that gives a complete definition. Begin your sentence with these words: "A relation on a set A is ...." As primitives you may use the concepts of sets, functions, and Cartesian products of sets.

3. (7 points) Let $a_1, a_2, \ldots$ be a sequence of real numbers. Define the statement "$\lim_{n\to\infty} a_n = \infty$". Your answer should be a well-quantified expression with no English words.

4. (9 points) Let (Ω, P) be a probability space where P is the uniform distribution and $|\Omega| = p$, a prime number. Prove: there are no nontrivial independent events in this space. Explicitly use the prime property.

5. (9+14 points)

(a) Count the strictly increasing k-term sequences of integers between 1 and n, i.e., the sequences of the form $1 \le x_1 < x_2 < \cdots < x_k \le n$.

(b) Count the (not necessarily strictly) increasing k-term sequences of integers between 1 and n, i.e., the sequences of the form $1 \le y_1 \le y_2 \le \cdots \le y_k \le n$.

Your answers should be simple closed-form expressions (no summation sign, product sign, or dot-dot-dot) involving binomial coefficients in terms of n and k. Prove your answers.

6. (4+7+15 points)

(a) Let us consider a random function $f : [k] \to [n]$ (chosen uniformly form among all such functions). What is the size of the sample space for this experiment?

(b) Let $p(n, k)$ denote the probability that f is injective, i.e., that there are no collisions: $f(x) = f(y) \implies x = y$. Give a simple formula for $p(n, k)$. The formula should be a closed-form expression in terms of factorials (no summation or product signs or dot-dot-dots, but you are allowed to use factorials in addition to ordinary arithmetic and exponentials, like, for example, $k^2 \cdot (n!)^k$).

(c) Prove: if $k = k_n = \omega(\sqrt{n})$ then $\lim_{n\to\infty} p(n, k_n) = 0$. (Recall that $f = \omega(g)$ means $g = o(f)$.)

7. (5+XC15+10 points)

(a) Count the relations on a given set of n elements.

(b) (XC) Let $T(n)$ denote the number of transitive relations on a given set of n elements. Prove: $\log_2 T(n) = \Theta(n^2)$. — In other words, you have to show that there exist positive constants c_1, c_2 such that $c_1 n^2 \leq \log_2 T(n) \leq c_2 n^2$ for all sufficiently large n. Specify your constants. The closer they are to each other, the better. ("$\log_2$" denotes the base-2 logarithm.)

(c) Let $B(n)$ denote the number of equivalence relations on a given set of n elements. Prove that the following statement is false:

. $\log_2 B(n) = \Theta(n^2)$.

8. (10 points) Recall the little-oh notation: for the functions f, g we say that $f(x) = o(g(x))$ as $x \to L$ if $\lim_{x \to L} f(x)/g(x) = 0$. Recall that $\pi(x)$ denotes the number of primes $\leq x$. Decide which of the following three statements is true. The little-oh statements refer to $x \to \infty$. Circle and prove your answer.

(a) $\pi(x) = o(x^{0.9})$ (b) $x^{0.9} = o(\pi(x))$ (c) neither.

9. (9 points) Determine all pairs (x, y) of integers such that $\text{lcm}(x, y) < \gcd(x, y)$ (no typo here) and $x + y = 2017$.

10. (10 points) Let (Ω, P) be a finite probability space with a sample space of n elements. Determine

$$\sum_{A \subseteq \Omega} P(A).$$

Your answer should be a very simple expression in terms of n. Prove your answer.

11. (7+9 points)

(a) Let A, B, C be nontrivial independent events in a probability space. Prove: $A \cap B$ and $B \cap C$ are positively correlated.

(b) Construct a probability space (Ω, P) and 3 pairwise independent nontrivial events, $A, B, C \subseteq \Omega$, such that $A \cap B$ and $B \cap C$ are negatively correlated. Make your space as small as possible.

12. ((5+2)+3+6+5+9XC) In the island nation of the United States of Bernoullia (USB), there are n residents and k states. Each resident has a unique "home state" and will be called a "resident" of that state. An overseas Ph. D. student arrives by boat at USB Port to perform an urgent study of two related random variables, X and Y, before the islands submerge due to rising seas. Here are some of zir findings in the form of exercises.

    (a) Let X be the number of residents of a random state. (a1) Determine $E(X)$. (a2) What is the sample space for this experiment? (We assume uniform distribution over this sample space.) — Your answer to (a1) should be a simple expression in terms of n and k.

    (b) Let Y be the number of residents in a random resident's home state. (The random resident is chosen uniformly from among all residents of USB.) What is the sample space for this experiment?

    (c) Let c_i be the number of residents of state i. Give a simple formula for $E(Y)$ in terms of the c_i. (This formula involves the summation symbol.)

    (d) Give a closed-form expression of $E(Y)$ in terms of k, n, and $E(X^2)$. (No summation or product symbols or dot-dot-dots.)

    (e) (XC) Prove: $E(Y) \geq E(X)$. (The average resident resides in a greater-than-average state.) Determine, under what condition on the c_i is $E(Y) = E(X)$.

13. (8+8 points points)

    (a) Let $k \in \mathbb{Z}$. Prove: $\gcd(3k+1, 8k-5)$ is either 1 or 23.

    (b) Prove that $\gcd(3k+1, 8k-5) = 23$ for infinitely many values of k.

14. (16 points) Suppose $a^{21} \equiv 1 \pmod{71}$. Prove: $a^7 \equiv 1 \pmod{71}$.

15. (6 points) For every $n \geq 1$, find a system of n simultaneous congruences of the form $x \equiv a_i \pmod{m_i}$ $(i = 1, 2, \ldots, n)$ such that (a) no two of the m_i are relatively prime; (b) no two of the a_i are equal; and (c) the system has a solution. State the value M such that your system has a unique solution modulo M. No proofs necessary.

16. (XC 15 points) Let $A_1, \dots, A_m$ be events such that $(\forall i)(P(A_i) = 1/2)$ and $(\forall i \neq j)(P(A_i \cap A_j) \leq 1/5)$. Prove: $m \leq 6$.

17. (XC 12 points) Prove: If we pick $n+1$ elements from the set $\{1, \dots, 2n\}$ then one of them will divide another one.

18. (XC 8 points) Let p be a prime number and let $f(x) = 1 + x + x^2 + \dots + x^{p-2}$. Prove: $(\forall x)(f(x) \equiv -1, 0 \text{ or } 1 \pmod{p})$.