Solutions to Midterm I. Discrete Mathematics 55

Instructor: Zvezdelina Stankova

Problem 1 (20pts). True or False?
To discourage guessing, the problem will be graded as follows:

- 2 pts for each correct answer.
- 0 pts for a blank.
- -2 pts for each incorrect answer.
- If anything else but "True" or "False" is written, more than one answer is written, or the answer is hard to read, you will get -2 points .

(1) If A is a proper subset of B, then $|A| < |B|$.

Answer: False. Counterexample: $A = \mathbb{Z}^+$ and $B = \mathbb{N}$. We have that $\mathbb{Z}^+ \subsetneq \mathbb{N}$, but both are infinitely countable and hence $|\mathbb{Z}^+| = |\mathbb{N}|$.

(2) If $C = A \cup B$, and A is infinitely countable but C is uncountable, then B is uncountable.

Answer: True. If B were countable, then $A \cup B$ would be countable too, as the union of two countable sets, making C countable, a contradiction.

(3) To prove by contradiction a theorem of the form "$p \to q$", we start by assuming $\neg q$.

Answer: True. A proof by contradiction starts with assuming $\neg q$ (and p).

(4) The method of mathematical induction is necessary to prove some theorems that we studied so far in this course.

Answer: True. We have mentioned that induction is necessary for the rigorous proof of some theorems (e.g. Division Algorithm, Euclid's Algorithm, and the Fundamental Theorem of Arithmetic), but we haven't yet studied induction.

(5) Euclidean algorithm is not useful in expressing the GCD of two integers as a linear combination of them with integer coefficients.

Answer: False. After one runs the Euclidean algorithm to find GCD of two integers, then one runs it backwards to find the desired linear combination.

(6) Fermat's Little Theorem applies to a modulo p that is prime but not to a modulo p that is composite.

Answer: True. Counterexample with a composite n: let $n = 10$, $a = 3$. Then 3 and 10 are relatively prime, but $3^{10-1} \not\equiv 1 \pmod{10}$. Indeed, $3^4 = 81 \equiv 1 \pmod{10}$ so that $3^9 = (3^4)^2 \cdot 3^1 \equiv 1^2 \cdot 3 \equiv 3 \not\equiv 1 \pmod{10}$

(7) The set of all infinite sequences of 0s and 1s is uncountable.

Answer: True. One can prove this by modifying Cantor's Diagonalization argument for uncountability of $\mathbb{R}$.

(8) The sequence $\{4k+3\}$ where $k \in \mathbb{N}$ contains infinitely many primes, but the sequence $\{4k+2\}$ does not.

Answer: True. We showed in class that $\{4k+3\}$ contains infinitely many primes. On the other hand, $\{4k+2\}$ does not since it consists of even numbers, only one of which will be prime, namely, 2.

(9) Every non-zero element of $\mathbb{Z}_p$ (where p is prime) has an additive inverse but not necessarily a multiplicative inverse.

Answer: False. Every non-zero element of $\mathbb{Z}_p$ (where p is prime) has an additive inverse and a multiplicative inverse.

(10) The ceiling function from $\mathbb{R} \to \mathbb{Z}$ is neither injective nor surjective.

Answer: False. The ceiling function is not injective, e.g., $\lceil 2.2 \rceil = 3 = \lceil 3 \rceil$, but it is surjective onto $\mathbb{Z}$ since $\lceil n \rceil = n$ for any integer n.

Problem 2 (20pts)

(a) Express the negation of the statement

$$\forall x(\exists y \forall z P(x,y,z) \wedge \exists z \forall y P(x,y,z))$$

so that negations appear only directly in front of predicates (that is, so that no negation is outside a quantifier or an expression involving logical connectives).

Answer:

$$\begin{aligned} & \neg\forall x(\exists y \forall z P(x,y,z) \wedge \exists z \forall y P(x,y,z)) \\ = \; & \exists x \neg(\exists y \forall z P(x,y,z) \wedge \exists z \forall y P(x,y,z)) \\ = \; & \exists x(\neg(\exists y \forall z P(x,y,z)) \vee \neg(\exists z \forall y P(x,y,z))) \\ = \; & \exists x(\forall y \exists z \neg P(x,y,z) \vee \forall z \exists y \neg P(x,y,z)) \end{aligned}$$

(b) Show that $(p \vee q) \wedge (\neg p \vee r) \to (q \vee r)$ is a tautology.

Proof: One way is to reason by contradiction. Suppose that the implication is false for some truth values of p, q and r. This means that the conclusion $q \vee r$ is false and the hypothesis $(p \vee q) \wedge (\neg p \vee r)$ is true. The disjunction $q \vee r$ is false exactly when both q and r are false. If p is false, then $p \vee q$ is false; if p is true, then $\neg p$ is false so that $\neg p \vee r$ is false. In either case, the conjunction $(p \vee q) \wedge (\neg p \vee r)$ is false, so the hypothesis is false. This is a contradiction. We conclude that the implication cannot be false for any truth values of its propositional variables. This means that the implication is a tautology. □

Problem 3 (20pts) Give an example of two uncountable sets A and B such that $A - B$ is

(a) finite. Explain.

Answer: Let $A = B = \mathbb{R}$: uncountable. Then $A - B = \emptyset$, finite.

(b) countably infinite. Explain.

Answer: Let $A = \mathbb{R}$ and $B = \mathbb{R} - \mathbb{Z}$: both uncountable. Then $A - B = \mathbb{Z}$, countably infinite.

(c) uncountable. Explain.

Answer: Let $A = \mathbb{C}$ and $B = \mathbb{R}$: both uncountable. Then $A - B$ is the set of all complex non-real numbers. $A - B$ contains a subset of all purely imaginary numbers $i\mathbb{R} = \{ir \mid r \in \mathbb{R} - \{0\}\}$, which is uncountable (why?) so that $A - B$ is also uncountable.

For another example, take $A = \mathbb{R} \times \mathbb{R}$ and $B = \mathbb{R} \times \{0\}$. Both are uncountable because $\mathbb{R}$ is uncountable. Then $A - B = \mathbb{R} \times (\mathbb{R} - \{0\})$ which contains an uncountable subset, e.g., $\mathbb{R} \times (\{1\})$, whichi is uncountable (why?), making the bigger set $A - B = \mathbb{R} \times (\mathbb{R} - \{0\})$ also uncountable.

Problem 4 (20pts) Include all relevant calculations and explanations:

(a) Find all integers x that satisfy the congruence $54x \equiv 2 \pmod{89}$.

Solution: We find the gcd(89,54) by using the Euclidean algorithm:

$$\begin{aligned} 89 &= 1\cdot 54+35 \\ 54 &= 1\cdot 35+19 \\ 35 &= 1\cdot 19+16 \\ 19 &= 1\cdot 16+3 \\ 16 &= 5\cdot\ 3+1. \end{aligned}$$

Thus, $\gcd(89,54)=1$. We now reverse the Euclidean algorithm to find a linear combination of 54 and 89 that equals 1:

$$\begin{aligned} 1 &= 16-5\cdot 3 = 16-5(19-16) = 6\cdot 16-5\cdot 19 = 6\cdot(35-19)-5\cdot 19 = 6\cdot 35-11\cdot 19 \\ &= 6\cdot 35-11\cdot(54-35) = 17\cdot 35-11\cdot 54 = 17(89-54)-11\cdot 54 = 17\cdot 89-28\cdot 54. \end{aligned}$$

Thus, the multiplicative inverse of 54 modulo 89 is -28. Multplying both sides of the congruence by -28 we get:

$$(-28)\cdot 54x \equiv (-28)\cdot 2 \pmod{89} \;\Rightarrow\; 1\cdot x \equiv -56 \equiv -56+89 = 33.$$

Thus, all integers satisfying the congruence are $x=89k+33$ for $k\in\mathbb{Z}$. □

(b) Find the remainder of $47^{200} \pmod{19}$.

Solution: $47\equiv 9 \pmod{19}$, hence $47^{200}\equiv 9^{200} \pmod{19}$. Since 19 is prime and 9 is relatively prime with 19, by Fermat's Little Theorem, $9^{18}\equiv 1 \pmod{19}$. Dividing 200 by 18, we have $200=18\cdot 11+2$. Therefore,

$$47^{200}\equiv 9^{200} = 9^{18\cdot 11+2} = (9^{18})^{11}\cdot 9^2 \equiv 1^{11}\cdot 81 \equiv 5 \pmod{19}. \quad \square$$

Problem 5 (20pts) Two players take turns removing 1, 2, 3, 4, or 5 cards from a stack of 2014 cards. The player who takes the last card *loses*. Is there a strategy for one of the players to always win? If yes, which player is this and what is his strategy? If not, why not? Explain.

Solution: The first player can always win. Indeed, $2014\equiv 4 \pmod 6$. The first player takes 3 cards on his first turn, and then completes the moves of the second player to 6 each time: if the second player takes k cards, the first player then takes $6-k$ cards, for $k=1,2,3,4,5$. As a result, after each of the first player's moves the number of the remaining cards is always 1 more than a multiple of 6. When there are only 7 cards left, whatever the second player takes, the first player will be able to leave exactly one card, forcing the second player to take the last card. Thus, the first player can always win the game. □