Math 55 First Midterm Exam, Prof. Srivastava
February 18, 2016, 3:40pm–5:00pm, F295 Haas Auditorium.

Name: ______________________________

SID: ______________________________

Instructions: Write all answers in the provided space. Please write carefully and clearly, in complete English sentences. This exam includes three pages of scratch paper at the end, which must be submitted, but will not be graded. Do not under any circumstances unstaple the exam.

You are not allowed to use any notes, books, electronic devices, or your own scratch paper.

UC Berkeley Honor Code: *As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.*

Question	Points
1	12
2	8
3	7
4	8
5	7
6	8
Total:	50

Do not turn over this page until your instructor tells you to do so.

1. Circle true (**T**) or false (**F**) for each of the following. There is no need to provide an explanation.

   (a) (3 points) The compound propositions

   $$(p \leftrightarrow q) \to r \qquad \text{and} \qquad r \vee (\neg p \leftrightarrow \neg q)$$

   are logically equivalent. **T** **F**

   > **Solution:** False. Consider the case p true and q and r false. Then the first expression is true (because the conditional is satisfied) and the second is false.

   (b) (3 points) The proposition

   $$(\exists x P(x)) \wedge (\forall y \forall z (P(y) \wedge P(z) \to y = z))$$

   means that there is exactly one element x in the domain such that $P(x)$ is true. **T** **F**

   > **Solution:** True. The first part of the proposition says that there exists an element with the property, and the second part says that if there are two elements with the property then they must be the same.

   (c) (3 points) If A and B are sets such that $A \subseteq \mathbb{Z}$ and $B \subseteq \mathbb{Z}$ then $A \times B = B \times A$. **T** **F**

   > **Solution:** False. Consider $A = \{1\}$ and $B = \{2\}$. Then $A \times B = \{(1,2)\}$ but $B \times A = \{(2,1)\}$. The point of this question is that the order matters when you take the Cartesian product of sets.

   (d) (3 points) The set

   $$S = \{x \in \mathbb{Z} : \quad 5x \equiv 3 \pmod 7\}$$

   is countably infinite. **T** **F**

   > **Solution:** True. Since 5 has an inverse modulo 7, we can solve the congruence by multiplying by 5^{-1}. If x is one solution, then all of the integers $x + 7k$ with $k \in \mathbb{Z}$ are also solutions since $7k \equiv 0 \pmod 7$. Thus the set has the same cardinality as $\mathbb{Z}$, by the bijection $f(k) = x + 7k$, so it is countable.

2. Prove that the following statements are **false** (i.e., prove their negations). Recall that $\mathbb{Z}^+ = \{1, 2, \ldots\}$ denotes the set of positive integers.

(a) (4 points)

$$\forall a, b \in \mathbb{Z}^+ \quad \exists k \in \mathbb{Z}^+ \quad (a + bk \text{ is prime}).$$

Solution: Since the negation of "$a + bk$ is prime" is "$a + bk$ is composite", the negation of the above statement is:

$$\exists a, b \in \mathbb{Z}^+ \quad \forall k \in \mathbb{Z}^+ \quad (a + bk \text{ is composite}).$$

To prove this latter statement, we need to produce an a and b such that for every $k \in \mathbb{Z}^+$ the integer $a + bk$ is composite. Consider $a = b = 2$. Assume k is an arbitrary positive integer. Observe that

$$a + bk = 2(k + 1)$$

is composite since $k + 1 \neq 1$. Since k was arbitrary, we conclude that for every $k \in \mathbb{Z}^+$ the expression $a + bk$ is composite, as desired.

A lot of people asked me whether it is "ok to provide a counterexample". It is, because disproving a statement of type $\forall a, b P(a, b)$ is the same thing as proving a statement of type $\exists a, b \neg P(a, b)$, and the proof is just an example (by existential generalization). This is called a counterexample to the original statement.

(b) (4 points)

$$\exists a, b \in \mathbb{Z}^+ \quad \forall k \in \mathbb{Z}^+ \quad (a + bk \text{ is prime}).$$

Solution: The negation is:

$$\forall a, b \in \mathbb{Z}^+ \quad \exists k \in \mathbb{Z}^+ \quad (a + bk \text{ is composite}).$$

Assume $a, b \in \mathbb{Z}^+$. We need to produce a $k \in \mathbb{Z}^+$ such that $a + bk$ is composite. There are two cases. If $a \neq 1$ then let $k = a$ and observe that

$$a + bk = a + ab = a(b + 1),$$

which is composite since both a and $b + 1$ are not equal to one. If $a = 1$, then let $k = b + 2$ and observe that

$$a + bk = 1 + b(b + 2) = b^2 + 2b + 1 = (b + 1)^2,$$

which is composite since $b + 1 > 1$. Thus, in all cases there exists a k such that $a + bk$ is composite, as desired.

This was by far the hardest question on the exam. Note that there are several different ways to produce the necessary k, and the above is just a suggestion.

3. (7 points) Prove or disprove: if A and B are arbitrary sets, then

$$\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B),$$

where $\mathcal{P}(A) = \{S : S \subseteq A\}$ denotes the power set of A.

Solution: This is false. Consider the sets $A = \{1\}$ and $B = \{2\}$, with union $A \cup B = \{1, 2\}$. Let $S = \{1, 2\}$. Notice that $S \subseteq A \cup B$ so $S \in \mathcal{P}(A \cup B)$. However, $S \not\subseteq A$ and $S \not\subseteq B$ so $S \notin \mathcal{P}(A)$ and $S \notin \mathcal{P}(B)$, which implies that $S \notin \mathcal{P}(A) \cup \mathcal{P}(B)$. Thus, we have $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

The intuition behind the above argument is that in general $A \cup B$ may contain subsets S which contain elements from both *A and B, and such subsets may not be contained in either A or B by itself (if each contains an element not contained in the other).*

Note that one of the inclusions, namely $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ is true. Many people proved this and received partial credit.

4. (8 points) Prove that if a and m are positive integers such that $gcd(a, m) = 1$ then the function

$$f : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$$

defined by

$$f(x) = (a \cdot x) \ \mathbf{mod} \ m$$

is a bijection, where **mod** denotes the remainder operation.

Solution: Since $gcd(a, m) = 1$ we know that a has an inverse modulo m (proved in class). Let b be such an inverse, i.e.,

$$ab \equiv 1 \pmod{m}. \tag{1}$$

To show that f is a bijection, we need to show that it is injective (1-1) and surjective (onto). Let $S = \{0, \ldots, m-1\}$ denote the domain (and codomain).

We first show that f is injective. Assume $x, y \in S$ and $f(x) = f(y)$, i.e.

$$ax \ \mathbf{mod} \ m = ay \ \mathbf{mod} \ m.$$

This is equivalent to saying

$$ax \equiv ay \pmod{m}.$$

Multiplying both sides by b, we have

$$bax \equiv bay \pmod{m},$$

which by (1) is just

$$x \equiv y \pmod{m}.$$

Thus, $m|x-y$. Observe that since $0 \le x, y < m$, we have $|x-y| < m$. Thus, this is only possible if $x - y = 0$, or $x = y$ as desired.

To see that f is surjective, let $z \in S$ be some element in the codomain. Let

$$x = bz \ \mathbf{mod} \ m,$$

and observe that $x \in S$ (the domain) and

$$ax \equiv abz \equiv z \pmod{m}.$$

Since $z \in \{0, \ldots, m-1\}$ this means that $ax \ \mathbf{mod} \ m = z$, so $f(x) = z$, as desired.

5. (7 points) Prove that if a and m are positive integers such that $gcd(a, m) \neq 1$ then a does *not* have an inverse modulo m.

Solution: We prove the contrapositive. Assume a has an inverse modulo m, i.e., there exists an integer b such that

$$ab \equiv 1 \pmod{m}.$$

This is equivalent to $m|(ab-1)$, which means there is an integer k such that

$$ab - 1 = mk,$$

which after rearrangement is

$$ba + (-k)m = 1.$$

Suppose d is any common divisor of a and m, i.e., $d|a$ and $d|m$. Since b and k are integers it follows that $d|(ba - km)$, so $d|1$. Thus we must have $d = 1$, so $gcd(a, m) = 1$, as desired.

You can shorten the proof a little by appealing to the the strong version of Bézout's theorem, which says that $gcd(a, m)$ is the smallest positive integer linear combination of a and m. Thus the existence of the linear combination $ba + (-k)m$ immediately implies that $gcd(a, m) = 1$.

6. (a) (4 points) Calculate the remainder $(-9)^{933}$ **mod** 13.

Solution: Observe that $-9 \equiv 4 \pmod{13}$, so it suffices to find 4^{933} **mod** 13. Since 13 is prime and $13 \not| 4$, Fermat's little theorem tells us that

$$4^{12} \equiv 1 \pmod{13}.$$

Thus, we only care about the remainder of 933 modulo 12; dividing, we get

$$933 = 77 \cdot 12 + 9,$$

so

$$4^{933} \equiv (4^{12})^{77} \cdot 4^9 \equiv 4^9 \equiv 2^{18} \pmod{13}.$$

We now observe that $13 \not| 2$ so again by Fermat's little theorem we have $2^{12} \equiv 1 \pmod{13}$, simplifying the above expression to

$$2^{18} \equiv 2^6 \equiv 64 \equiv 12 \pmod{13},$$

since $64 = 4 \cdot 13 + 12$. Thus

$$(-9)^{933} \textbf{ mod } 13 = 12.$$

(b) (4 points) Use the Euclidean Algorithm to find the greatest common divisor of 270 and 63.

Solution: We repeatedly divide the larger number by the smaller one:

$$\begin{aligned} 270 &= 4 \cdot 63 + 18 & &\Rightarrow gcd(270,63) = gcd(63,18) \\ 63 &= 3 \cdot 18 + 9 & &\Rightarrow gcd(63,18) = gcd(18,9) \\ 18 &= 2 \cdot 9 + 0 & &\Rightarrow gcd(18,9) = 9. \end{aligned}$$

We conclude that $gcd(270,63) = 9$.

Name and SID: ____

[Scratch Paper 1]

Name and SID: ____________________

[Scratch Paper 2]

Name and SID: ____

[Scratch Paper 3]