Final Exam Solution Guide

MAT 200

There are ten questions.
Each question is worth 10 points.

1. Let $(\star)$ denote the following statement about integers n:

If n is divisible by 10, then it is divisible by 2 or divisible by 5.

(a) Is $(\star)$ a true statement? (That is, is it **universally** true?)

Yes, $(\star)$ is a true statement.

(b) What is the *contrapositive* of $(\star)$? Is it a true statement?

If n is not divisible by 2 **and** not divisible by 5, it is not divisible by 10.

This is equivalent to $(\star)$, and thus also true.

(c) What is the *converse* of $(\star)$? Is it a true statement?

If n is divisible by 2 or divisible by 5, it is divisible by 10.

This is false. For example, 4 is divisible by 2, but not divisible by 10.

Remark. Consider the statement $(\dagger)$ given by

If n is divisible by 10, then it is divisible by 2 **and** divisible by 5.

Then $(\dagger)$ is also true, and $(\dagger) \implies (\star)$.

However, the distinction between **and** and **or** is important for part (c). Namely, the converse of $(\dagger)$ is true, while the converse of $(\star)$ is false!

2. Let $f : X \to Y$ and $g : Y \to X$ be functions, and suppose that

$$f \circ g = I_Y \ ,$$

where I_Y is the identity function on Y. Prove that f is a surjection.

Proof. Let y be any element of Y. If we set $x = g(y)$, then

$$\begin{aligned} f(x) &= f(g(y)) \\ &= (f \circ g)(y) \\ &= I_Y(y) \\ &= y. \end{aligned}$$

Thus, for every $y \in Y$, there exists an $x \in X$ such that $f(x) = y$. But this precisely says that f is surjective. QED

3. Recall that $\mathbb{Z}$ denotes the set of integers, $\mathbb{Z}^+$ the set of positive integers, and $\mathbb{Q}$ the set of rational numbers. Define a function $f : \mathbb{Z} \times \mathbb{Z}^+ \to \mathbb{Q}$ by

$$f(p, q) = \frac{p}{q} .$$

(a) Is f an injection? Why?

No. There are many different choices of $(p, q) \in \mathbb{Z} \times \mathbb{Z}^+$ which are assigned the same value by f. For example, $f(1, 1) = 1 = f(2, 2)$.

(b) Is f a surjection? Why?

Yes. Every rational number is, by definition, a quotient of integers, and we can always arrange for the denominator to be positive.

(c) Is f a bijection? Why?

No. To be a bijection, a function must be both an injection and a surjection. Since f is not an injection by part (a), it is not a bijection, either.

4. Let X be a **finite** set, and suppose that $f : X \to X$ is an injection. Does it follow that f is a bijection? Justify your answer with a proof or a counter-example.

Yes, f is necessarily a bijection. Since we are told it is an injection, it suffices to show that it is a surjection. This is proved as follows:

Proof. We proceed via proof by contradiction.

Suppose that f is not a surjection. Then there is some $x_0 \in X$ which is not in the image of f. Setting $Y = X - \{x_0\}$, we can therefore view f as defining a function $g : X \to Y$. (This change of pont-of-view is an example of "restriction of codomain".) Since f is injective, and since g is really just f by another name, g is injective, too. However, if $|X| = m$, then $|Y| = m - 1$. In particular, $|Y| < |X|$. By the **pigeon-hole principle**, a function $g : X \to Y$ therefore cannot be injective. But this is a contradiction!

It follows that the injective function f must be surjective, too. QED

5. Now let X instead be a **denumerable** set, and suppose that $f : X \to X$ is an injection. Does it follow that f is a bijection? Justify your answer with a proof or a counter-example.

No, f is not necessarily a bijection.

Here is a counter-example: let $X = \mathbb{Z}^+$ be the set of positive integers, and to let $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ be the function $f(n) = n + 1$. Then f is injective, but not surjective.

6. Let P be the Euclidean plane. Recall that P is a set, and that its elements are called *points*. Show that the axioms for Euclidean geometry, as given in the geometry notes, imply that P is an uncountable set.

Hint: How many points are there on a line?

Proof. The incidence axiom implies that P contains a line ℓ. The **ruler axiom** then tells us that there is a bijective "coordinate system"

$$f : \ell \to \mathbb{R}$$

and since f is a bijection, it has an inverse $f^{-1} : \mathbb{R} \to \ell$, which is also a bijection. If $j : \ell \to P$ is the inclusion function, arising from the fact that ℓ is a subset of P, the composition

$$j \circ f^{-1} : \mathbb{R} \to P$$

is therefore necessarily injective, since it is the composition of two injections.

If P were countable, there would be an injection $g : P \to \mathbb{Z}^+$, and the composition

$$g \circ j \circ f^{-1} : \mathbb{R} \to \mathbb{Z}^+$$

would be injective. Since any subset of $\mathbb{Z}^+$ is either finite or denumerable, this gives rise, via restriction of codomain, to a bijection between $\mathbb{R}$ and a countable set — namely, the image of $g \circ j \circ f^{-1}$. It follows that $\mathbb{R}$ is countable. But Cantor's Theorem says that $\mathbb{R}$ is *uncountable*, so this is a contradiction. It follows that P must be uncountable, as claimed. QED

7. Prove by induction that, for any positive integer k, 10^k is congruent to $(-1)^k$ modulo 11. Then use this to show that any positive integer is congruent mod 11 to the alternating sum of its digits.

Let $\mathbf{P}(k)$ be the statement

$$10^k \equiv (-1)^k \bmod 11.$$

Base case. $10 = 11 - 1 \equiv -1 = (-1)^1 \bmod 11$, so $\mathbf{P}(1)$ is true.

Inductive step. We will show that $\mathbf{P}(m) \implies \mathbf{P}(m+1)$.
Suppose that $\mathbf{P}(m)$ is true. Then

$$10^m \equiv (-1)^m \bmod 11.$$

However, we also know that

$$10^1 \equiv (-1)^1 \bmod 11,$$

since we have just checked that the bases case is true. Furthermore, we know that multiplying two valid congruences with the same modulus yields another valid congruence with that modulus. Multiplying the last two congruences above thus yields

$$(10^m)10^1 \equiv (-1)^m(-1)^1 \bmod 11,$$

and on simplification this gives us

$$10^{m+1} \equiv (-1)^{m+1} \bmod 11,$$

which is the statement $\mathbf{P}(m+1)$. Thus $\mathbf{P}(m) \implies \mathbf{P}(m+1)$, as claimed.

Since both the base case and the inductive step are valid, the principle of induction therefore tells us that $\mathbf{P}(k)$ is true for every positive integer k.

In decimal notation, $n_m n_{m-1} \cdots n_1 n_0$ represents the positive integer $\sum_{j=0}^{m} n_j 10^j$. Since 10^0 and $(-1)^0$ are both just fancy notations for 1, the above inductive argument tells us $10^j \equiv (-1)^j \bmod 11$ for every integer $j \geq 0$. Hence

$$\sum_{j=0}^{m} n_j 10^j \equiv \sum_{j=0}^{m} n_j (-1)^j \bmod 11$$

and the right-hand expression is exactly the alternating sum

$$n_0 - n_1 + n_2 - n_3 + \cdots \pm n_m$$

of the digits of the number in question.

8. (a) Carefully state the definition of congruence of triangles, according to our geometry notes.

By definition, $\triangle ABC \cong \triangle A'B'C'$ means the following statements are true:

$$\begin{array}{cc} |AB| = |A'B'| & m\angle A = m\angle A' \\ |AC| = |A'C'| & m\angle B = m\angle B' \\ |BC| = |B'C'| & m\angle C = m\angle C' \end{array}$$

(b) Let T be the set of all triangles $\triangle ABC$ in the plane, where our definition of a triangle is understood to include a listing of its three vertices in a definite order. Show that congruence of triangles is an equivalence relation on T.

Reflexive: For any triangle $\triangle ABC \in T$, we have $\triangle ABC \cong \triangle ABC$ because

$$\begin{array}{cc} |AB| = |AB| & m\angle A = m\angle A \\ |AC| = |AC| & m\angle B = m\angle B \\ |BC| = |BC| & m\angle C = m\angle C \end{array}$$

Symmetric: $\triangle ABC \cong \triangle A'B'C' \implies \triangle A'B'C' \cong \triangle ABC$ because

$$\left(\begin{array}{cc} |AB| = |A'B'| & m\angle A = m\angle A' \\ |AC| = |A'C'| & m\angle B = m\angle B' \\ |BC| = |B'C'| & m\angle C = m\angle C' \end{array}\right) \implies \left(\begin{array}{cc} |A'B'| = |AB| & m\angle A' = m\angle A \\ |A'C'| = |AC| & m\angle B' = m\angle B \\ |B'C'| = |BC| & m\angle C' = m\angle C \end{array}\right)$$

Transitive: For three triangles $\in T$, we have
$\triangle ABC \cong \triangle A'B'C'$ and $\triangle A'B'C' \cong \triangle A''B''C'' \implies \triangle ABC \cong \triangle A''B''C''$
because

$$\begin{array}{ccccc} |AB| = |A'B'| & \text{and} & |A'B'| = |A''B''| & \implies & |AB| = |A''B''| \\ |AC| = |A'C'| & \text{and} & |A'C'| = |A''C''| & \implies & |AC| = |A''C''| \\ |BC| = |B'C'| & \text{and} & |B'C'| = |B''C''| & \implies & |BC| = |B''C''| \\ m\angle A = m\angle A' & \text{and} & m\angle A' = m\angle A'' & \implies & m\angle A = m\angle A'' \\ m\angle B = m\angle B' & \text{and} & m\angle B' = m\angle B'' & \implies & m\angle B = m\angle B'' \\ m\angle C = m\angle C' & \text{and} & m\angle C' = m\angle C'' & \implies & m\angle C = m\angle C'' \end{array}$$

Since $\cong$ is therefore reflexive, symmetric, and transitive, it is therefore an equivalence relation on T.

9. Recall that $\mathbb{R}$ denotes the set of real numbers, while $\mathbb{Z}$ denotes the set of integers. Define a relation $\sim$ on $\mathbb{R}$ by

$$x \sim y \iff x - y \in \mathbb{Z}$$

for any $x, y \in \mathbb{R}$. Prove that $\sim$ is an equivalence relation.

Reflexive: For any $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Z}$, and hence $x \sim x$. Therefore $\sim$ is reflexive.

Symmetric: Suppose that $x, y \in \mathbb{R}$, and that $x \sim y$. Then $x - y = n$ for some integer $n \in \mathbb{Z}$. Hence $y - x = -(x - y) = -n \in \mathbb{Z}$, so that $y \sim x$. This shows that $x \sim y \implies y \sim x$. Therefore $\sim$ is symmetric.

Transitive: Suppose that $x, y, z \in \mathbb{R}$, that $x \sim y$, and that $y \sim z$. Then $x - y = m$ for some integer n, and $y - z = n$ for some integer n. Hence

$$x - z = (x - y) + (y - z) = m + n \in \mathbb{Z}$$

so that $x \sim z$. This shows that $x \sim y$ and $y \sim z \implies x \sim z$. Therefore $\sim$ is transitive.

We have now shown that $\sim$ is reflexive, symmetric, and transitive. Therefore $\sim$ is an equivalence relation.

10. Let X and Y be finite sets, with $|Y| = 2$ and $|X| = n \geq 2$. Compute the cardinality of

$$\mathrm{Surj}(X, Y) = \{ \text{ functions } f : X \to Y \mid f \text{ is a surjection } \}.$$

Hint: What is the cardinality of its complement in $\mathrm{Fun}(X, Y)$?

Let a and b be the two elements of Y. If $f : X \to Y$ is **not** surjective, then either a is not in the image of f, or else b is not in the image of f. If a is not in the image, we must have $f(x) = b$ for all $x \in X$, since a function must assign a value to every element of its domain, and b is the only possible value that hasn't been excluded; so in this case, f must therefore be the constant function with value b. On the other hand, if b is not in the image, then, by the same reasoning, $f(x) = a$ for all $x \in X$, and f is therefore the constant function with value a. Thus, there are exactly 2 functions $X \to Y$ which **aren't** surjections.

Since $|\mathrm{Fun}(X, Y)| = |Y|^{|X|} = 2^n$, it follows that

$$|\mathrm{Surj}(X, Y)| = 2^n - 2.$$