Math 55 - Midterm 1, Summer 2017 - Solutions

1 State whether each of the following statements are True or False. There is no need to provide an explanation, and no credit will be given for explanations!

a **(3 points)** If $|A| = |B|$ and $|C| = |D|$, then $|A \times B| = |C \times D|$.

A **False**: There are many counterexamples. Choose non-negative integers n, m such that $n \neq m$ and sets such that $|A| = |B| = n$ and $|C| = |D| = m$. Then $|A \times B| = n^2$ while $|C \times D| = m^2$. In particular, if you choose $A = B = \{1\}$ and $C = D = \emptyset$ we have $|A \times B| = |\{1, 1\}| = 1$ and $|C \times D| = |\emptyset \times \emptyset| = |\emptyset| = 0$.

b **(3 points)** $(\neg q \wedge (p \to q)) \to \neg p$ is a tautology.

A **True**: Directly verify this via a truth table or argue as follows: If $\neg q \wedge (p \to q)$ is true, then $\neg q$ is true and $p \to q$ is true. This forces p to be false i.e. $\neg p$ is true. Thus, $(\neg q \wedge (p \to q)) \to \neg p \equiv \text{True} \to \text{True} \equiv \text{True}$.

c **(3 points)** $\mathbf{R} - \mathbf{Q}$ is countable.

A **False**: If $\mathbf{R} - \mathbf{Q}$ was countable, then $(\mathbf{R} - \mathbf{Q}) \cup \mathbf{Q} = \mathbf{R}$ would be countable; this is a contradiction.

d **(3 points)** The function $f : \mathbf{Z} \times \mathbf{Z} \longrightarrow \mathbf{Z}$ given by $f(m, n) = 9n - 12m$ is onto.

A **False**: Since $3|(9n - 12m)$, the image of f lies inside the set of integers divisible by 3.

e **(3 points)** If $\forall x \exists y P(x, y)$ is True, then $\exists x \forall y P(x, y)$ is True.

A **False**: Let $P(x, y)$ be the statement "$x + y = 0$" with domain $\mathbf{R} \times \mathbf{R}$. Then $\forall x \exists y\ (x + y = 0)$ is true, while $\exists x \forall y\ (x + y = 0)$ is false.

2a **(8 points)** Use the Euclidean algorithm to solve the congruence $9x \equiv 1 \bmod 16$

A Applying the Euclidean algorithm we obtain,

$$\begin{aligned} 16 &= 9 \cdot 1 + 7 \\ 9 &= 7 \cdot 1 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

Using this we obtain,

$$1 = 7 - 2 \cdot 3 = 7 - (9 - 7) \cdot 3 = 4 \cdot 7 - 9 \cdot 3 = 4 \cdot (16 - 9) - 9 \cdot 3 = 4 \cdot 16 - 7 \cdot 9.$$

Thus, $1 \equiv 4 \cdot 16 - 7 \cdot 9 \equiv -7 \cdot 9 \bmod 16$ i.e. -7 is a solution modulo 16.

2b **(2 points)** Solve the congruence $9x \equiv 3 \mod 16$.

A Notice that $x \equiv 1 \cdot x \equiv (-7) \cdot 9x \equiv (-7) \cdot 3 \equiv -21 \equiv 11 \bmod 16$. ■

---

3 The goal of this exercise is to compute $11^{10^5} \bmod 13$.

a (**3 points**) Prove that if r is an integer such that $10^5 \equiv r \bmod 12$ then $11^{10^5} \equiv 11^r \bmod 13$

A By the division algorithm, $10^5 = 12q + r$ with $0 \leq r < 12$ i.e. $10^5 \equiv r \bmod 12$. By Fermat's little theorem we have $11^{12} \equiv 1 \bmod 13$. Thus,

$$11^{10^5} \equiv 11^{12q+r} \equiv (11^{12})^q \cdot 11^r \equiv 11^r \bmod 12.$$

b (**2 points**) Find a suitable r and use it to compute $11^{10^5} \bmod 13$.

A Well, $10^5 \equiv (-2)^5 \equiv -32 \equiv 4 \bmod 12$ and we can take $r = 4$. Thus,

$$11^{10^5} \equiv 11^4 \equiv (-2)^4 \equiv 16 \equiv 3 \bmod 13. \blacksquare$$

---

4 (**5 points**) Determine whether $\forall x(P(x) \longrightarrow Q(x))$ and $\forall x P(x) \longrightarrow \forall x Q(x)$ are logically equivalent.

A They are not logically equivalent: Consider $P(x) =$ "$x > 0$" and $Q(x) =$ "$x < 0$" and the domain to be $\mathbf{R}$ (real numbers). Then $\forall x(P(x) \to Q(x))$ is False as $P(2) \to Q(2)$ is False. On the other hand, $\forall x P(x) \to \forall x P(x)$ is True! [This is 1.4.43 from Homework 1]. ■

5

a (**5 points**) Let A, B be finite sets. Prove that a function $f : A \longrightarrow B$ is one-to-one iff $|f(S)| = |S|$ for all subsets S of A.

A If $f : A \longrightarrow B$ was one-to-one, then for all $x \neq y$ we have $f(x) \neq f(y)$. In particular, if $s_1, \ldots, s_n$ are distinct elements of S, then $f(s_1), \ldots, f(s_n)$ are all distinct elements of $f(S)$ i.e. $|S| = |f(S)|$.

Conversely, if $|f(S)| = |S|$ for all subsets $S$of A, we would have $|\{x, y\}| = |\{f(x), f(y)\}|$ for all $x, y \in S$. If $x \neq y$, this would imply that $f(x) \neq f(y)$ i.e. f is one-to-one. ■

b (**2 points**) Find the number of distinct functions from $\{1, 2\} \longrightarrow \{1, 2\}$.

A There are four functions:

i. f_1 such that $f_1(1) = f_1(2) = 1$

ii. f_2 such that $f_2(1) = f_2(2) = 2$

iii. f_3 such that $f_3(1) = 1$ and $f_3(2) = 2$

iv. f_4 such that $f_4(1) = 2$ and $f_4(2) = 1$.

c (**3 points**) Prove that the set of functions from $\mathbf{Z}^+ \longrightarrow \mathbf{Z}^+$ is uncountable.

A Let S be the set of functions from $\mathbf{Z}^+ \longrightarrow \mathbf{Z}^+$. We mimic the proof of the fact that $(0, 1)$ was uncountable. If S was countable, then we could list the functions as $f_1, f_2, f_3, \ldots$. Now define a new function by $f(n) = f_n(n) + 1$. If f was in the list, then $f = f_m$ for some m and in particular, $f(m) = f_m(m)$. This would imply $f_m(m) + 1 = f_m(m)$, which is a contradiction. Thus, f is not in the list which implies that S must have been uncountable.

Note One can also choose the function $f(n) = \begin{cases} 4 & \text{if } f_n(n) \neq 4 \\ 5 & \text{else} \end{cases}$ and show it's not on the list (now it's very similar to the proof of the fact that $(0, 1)$ is uncountable). ■

---

6 Theorem: For any $n \in \mathbf{Z}$, $49n + 5$ is never a product of **two** consecutive integers; equivalently, $49n + 5 = m(m + 1)$ has no solutions for any $n, m \in \mathbf{Z}$

a (**2 points**) For which $m \in \mathbf{Z}$, is $m(m + 1) \equiv 5 \bmod 7$? Give your answer modulo 7.

A By directly checking $m \equiv 0, 1, 2, 3, 4, 5, 6 \bmod 7$ we see that $m \equiv 3 \bmod 7$ is the only one that satisfies $m(m + 1) \equiv 3 \cdot 4 \equiv 12 \equiv 5 \bmod 7$.

b (**2 points**) Using part a, or otherwise, prove the Theorem.

A By the division algorithm we have $m = 7k + 3$. Thus, $m(m + 1) = (7k + 3)(7k + 4) = 49k^2 + 49k + 12$. Since $49n + 5 = m(m + 1)$, we have $49n + 5 = 49(k^2 + k) + 12$. This is a contradiction; for example looking at the expression mod 49 we obtain $5 \equiv 12 \bmod 49$. ■

Bonus (**3 points**) Show that $49n + 5$ is never a product of two or more consecutive integers.

A I will present a solution that goes through a few cases. Consider a product of $k + 1$ consecutive integers, $m(m + 1) \cdots (m + k)$ and let $S = \{m, m + 1, \ldots, m + k\}$; here $k \geq 1$ by assumption.

i. If $k \geq 6$, then at least one of the elements of S is divisible by 7. Thus, $m(m + 1) \cdots (m + k) \equiv 0 \bmod 7$ while $49n + 5 \equiv 5 \bmod 7$; in particular, these quantities cannot be equal.

The above argument implies that none of the elements of S can be divisible by 7. To finish the proof, we will show that $m(m + 1) \cdots (m + k)$ is **never** congruent to 5 mod 7 for all $1 \leq k \leq 5$.

ii. If $k = 5$, unless $m \equiv 1 \bmod 7$, one of the elements of S is going to be divisible by 7. Thus, $m(m + 1) \cdots (m + 5) \equiv 1 \cdot 2 \cdots 6 \equiv -1 \equiv 6 \bmod 7$.

iii. If $k = 4$, unless $m \equiv 1, 2 \bmod 7$, one of the elements of S is going to be divisible by 7. If $m \equiv 1 \bmod 7$ we obtain a product that's congruent to $5! \equiv 1 \bmod 7$ and if $m \equiv 2 \bmod 7$, the product is congruent to $2 \cdots 6 \equiv -1 \equiv 6 \bmod 7$.

iv. If $k = 3$, we have $m \equiv 1, 2, 3, \bmod 7$. The corresponding products are congruent to $1 \cdot 2 \cdot 3 \cdot 4 \equiv 3 \bmod 7$, , $2 \cdot 3 \cdot 4 \cdot 5 \equiv 1 \bmod 7$ and $3 \cdot 4 \cdot 5 \cdot 6 \equiv 3 \bmod 7$ respectively

iv. If $k = 2$, we have $m \equiv 1, 2, 3, 4 \bmod 7$. The corresponding products are congruent to $1 \cdot 2 \cdot 3 \equiv 6 \bmod 7$, $2 \cdot 3 \cdot 4 \equiv 3 \bmod 7$, $3 \cdot 4 \cdot 5 \equiv 4 \bmod 7$ and $4 \cdot 5 \cdot 6 \equiv 1 \bmod 7$, respectively.

v. The case of $k = 1$ was solved in part b.

Thus, $49n + 5$ is never a product of two or more consecutive integers. ■
