MATH 271 – Winter 2013
Final Exam – Solutions

1. (a) Use the Euclidean algorithm to find $\gcd(77, 62)$. Also use the algorithm to find integers x and y such that $\gcd(77, 62) = 77x + 62y$.

   Solution. Use the Euclidean algorithm to find that $\gcd(77, 62) = 1$ and $1 = 77 \cdot (29) + 62 \cdot (-36)$.

   (b) Use part (a) to find an inverse a for 62 modulo 77 so that $0 \leq a \leq 76$; that is, find an integer $a \in \{0, 1, \ldots, 76\}$ so that $62a \equiv 1 \pmod{77}$.

   Solution. From part (a), we see that -36 is an inverse of 62 modulo 77, because

$$62 \cdot (-36) = 1 + y \cdot 77 \equiv 1 \pmod{77}.$$

   Then 41 is another inverse of 62 modulo 77, because

$$62 \cdot (41) = 62 \cdot (-36) + 62 \cdot 77 \equiv 62 \cdot (-36) \equiv 1 \pmod{77}.$$

2. Let S be the statement:

$$\text{for all positive integers } a \text{ and } b, \text{ if } a \mid b \text{ then } (5a) \mid (5b).$$

   (a) Prove that $\mathcal{S}$ is true. Use the definition of "|" ("divides into").

   Solution. *Proof.* Let a and b be arbitrary positive integers. Assume that $a \mid b$. Then there exists an integer k so that $ak = b$. Multiplying this equation by 5 gives us that $(5a)k = 5b$. Thus $(5a) \mid (5b)$. □

   (b) Write out the *converse* of statement S. Is it true or false? Give a proof or counterexample.

   Solution. The converse is "For all integers a and b, if $(5a) \mid (5b)$ then $a \mid b$." This statement is true.

   Proof (*of the negation*). Let a and b be arbitrary positive integers. Assume that $(5a) \mid (5b)$. Then there exists an integer k so that $(5a)k = 5b$. Dividing this equation by 5 gives us that $ak = b$. Thus $a \mid b$. □

   (c) Write out the *contrapositive* of statement $\mathcal{S}$. Is it true or false? Explain.

   Solution. The contrapositive is "For all integers a and b, if $(5a) \nmid (5b)$ then $a \nmid b$." This statement is true, since the contrapositive is always logically equivalent to the original statement, which is true.

3. Let $\mathcal{S}$ be the power set $\mathscr{P}(\{1, 2, \ldots, 10\})$; that is, $\mathcal{S}$ is the set of all subsets of $\{1, 2, \ldots, 10\}$. Define the relation $\mathscr{R}$ on $\mathcal{S}$ by:

$$\text{for all subsets } A, B \text{ of } \{1, 2, \ldots, 10\}, \quad A \mathrel{\mathscr{R}} B \text{ if and only if } A \cup B \text{ has exactly 3 elements.}$$

   (a) Is $\mathscr{R}$ reflexive? Symmetric? Transitive? Give reasons.

   Solution. The relation R is symmetric, but neither reflexive nor transitive.

   Proof (*that R is symmetric*). Let A and B be subsets of $\{1, 2, \ldots, 10\}$ and suppose that $A \mathrel{\mathscr{R}} B$. Then $A \cup B$ has exactly three elements. Thus $B \cup A$ also has exactly three elements, since $B \cup A = A \cup B$. Therefore $B \mathrel{\mathscr{R}} A$, so $\mathscr{R}$ is symmetric. □

   Proof (*that R is not reflexive*). Let $A = \{1, 2, \ldots, 10\}$. Then $A \cup A = \{1, 2, \ldots, 10\}$, which has 10 elements, so $A \not\mathrel{\mathscr{R}} A$. Hence $\mathscr{R}$ is not reflexive. □

Proof (*that R is not transitive*). Let $A = \{1\}$, $B = \{2,3\}$, and $C = \{1\}$. Then $A \mathscr{R} B$ since $A \cup B = \{1,2,3\}$, which has exactly three elements, and $B \mathscr{R} C$, since $B \cup C = \{1,2,3\}$ which has exactly three elements. But $A \cup C = \{1\}$ has only one elements, so $A \not\mathscr{R} C$. Therefore $\mathscr{R}$ is not transitive. $\square$

(b) Find and simplify the *number* of subsets $A \subseteq \{1,2,\ldots,10\}$ so that $A \mathscr{R} \{1,2,7\}$. Explain.

Solution. The answer is $2^3 = 8$. The reasoning is as follows. The only subsets A of $\{1,2,\ldots,10\}$ that can be related to $\{1,2,7\}$ are the subsets of $\{1,2,7\}$. Indeed, ff $A \not\subseteq \{1,2,7\}$, then $|A \cup \{1,2,7\}|$ would be more than three. However, for all subsets A of $\{1,2,7\}$, we have $A \cup \{1,2,7\} = \{1,2,7\}$ and thus $A \mathscr{R} \{1,2,7\}$. The number of subsets of $\{1,2,7\}$ is 2^3, since $\{1,2,7\}$ has three elements.

(c) Find and simplify the *number* of subsets $A \subseteq \{1,2,\ldots,10\}$ so that $A \mathscr{R} \emptyset$. Explain.

Solution. The answer is $\binom{10}{3} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = \frac{720}{6} = 120$. The reasoning is as follows. Given any subset A, the number of elements of $A \cup \emptyset$ is equal to the number of elements of A. Hence a subset A will be related to the empty set if and only if A has exactly three elements. The number of subsets of $\{1,2\ldots,10\}$ that have exactly three elements is $\binom{10}{3}$.

4. (a) Write out the *contrapositive* of the following statement:

$$\text{for all positive real numbers } r, \text{ if } r \text{ is irrational then } \sqrt{r} \text{ is irrational.}$$

Solution. The converse is: "For all positive real numbers r, if $\sqrt{r}$ is rational then r is rational."

(b) Prove the statement from part (a) by using contradiction or the contrapositive. (Use no facts about rationals or irrationals except for the definitions.)

Solution. *Proof* (*by contrapositive*). Let r be an arbitrary positive real number. Assume that $\sqrt{r}$ is rational. Then there exist integers a and b so that $\sqrt{r} = \frac{a}{b}$ and $b \neq 0$. Then $r = (\sqrt{r})^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, where a^2 and b^2 are integers and $b^2 \neq 0$ since $b \neq 0$. Hence r is rational. $\square$

Solution (Alternate)**.** *Proof* (*by contradiction*). Let r be an arbitrary positive real number. Assume that r is irrational. Assume for the sake of getting a contradiction that $\sqrt{r}$ is rational. Then there exist integers a and b so that $\sqrt{r} = \frac{a}{b}$ and $b \neq 0$. Then $r = (\sqrt{r})^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, where a^2 and b^2 are integers and $b^2 \neq 0$ since $b \neq 0$. Hence r is rational. But this is a contradiction, since r is irrational. Thus the assumption that $\sqrt{r}$ is rational is wrong. Therefore $\sqrt{r}$ is irrational. $\square$

5. One of the following statements is true and one is false. Prove the true statement. Write out and prove the *negation* of the false statement.

(a) $\forall A \subseteq \mathbb{Z}$, $\exists B \subseteq \mathbb{Z}$ so that $(1,2) \in A \times B$.

Solution. This statement is false. Its negation is "$\exists A \subseteq \mathbb{Z}$ so that $\forall B \subseteq \mathbb{Z}$, $(1,2) \notin A \times B$."

Proof (of negation). Let $A = \emptyset$. Let B be an arbitrary subset of $\mathbb{Z}$. Then $(1,2) \notin A \times B$ since $1 \notin A$. $\square$

(b) $\forall A \subseteq \mathbb{Z}$, $\exists B \subseteq \mathbb{Z}$ so that $(1,2) \notin A \times B$.

Solution. Let A be an arbitrary subset of $\mathbb{Z}$. Let $B = \emptyset$. Then $(1,2) \notin A \times B$ since $2 \notin B$.

6. Define the relation R on the set $\mathbb{Z}^+$ of all positive integers by:

$$\text{for all } a, b \in \mathbb{Z}^+, \quad a \, R \, b \text{ if and only if the largest digit of } a \text{ is equal to the largest digit of } b.$$

For example, $271 \, R \, 770$ because the largest digit of 271 is 7, which is also the largest digit of 770.

(a) Prove that R is an equivalence relation on $\mathbb{Z}^+$.

Solution. *Proof.* We prove that R is reflexive, symmetric, and transitive.

- (Reflexive) Let $a \in \mathbb{Z}^+$. The largest digit of a is equal to itself. Thus $a\,R\,a$. Hence R is reflexive.
- (Symmetric) Let $a, b \in \mathbb{Z}^+$ and assume that $a\,R\,b$. Then the largest digit of a is equal to the largest digit of b. Hence the largest digit of b is equal to the largest digit of a. So $b\,R\,a$. Therefore R is symmetric.
- (Transitive) Let $a, b, c \in \mathbb{Z}^+$. Assume that $a\,R\,b$ and $b\,R\,c$. Then the largest digit of a is equal to the largest digit of c, which is equal to the largest digit of c. Hence $a\,R\,c$ and thus R is transitive.

Thus R is an equivalence relation because it is reflexive, symmetric, and transitive. □

(b) Find the *number* of equivalence classes of R. Explain.

Solution. There are 9 equivalence classes. For any positive integer, its largest digit must be one of 1, 2, 3, 4, 5, 6, 7, 8, or 9. So there are 9 possibilities.

(c) Find the *number* of positive integers between 100 and 1000 which are in the equivalence class [271]. Explain

Solution. The answer is $7 \cdot 8^2 - 6 \cdot 7^2 = 154$. The reasoning is as follows. Note that 1000 is not related to 271. The integers between 100 and 999 (inclusively) are all of the three-digit positive integers. The three-digit integers that are related to 271 have 7 as their largest digit. Hence we must find the number of three-digit positive integers that have a 7, but don't have an 8 or a 9.

Let A be the set of three-digit positive integers that have no 7's, no 8's, and no 9's. Then $|A| = 6{\cdot}7{\cdot}7$. The recipe for A is as follows:

1. Pick the first digit. It can't be 0, 7, 8, or 9. There are 6 choices.
2. Pick the second digit. It can't be 7, 8, or 9. There are 7 choices.
3. Pick the last digit. It can't be 7, 8, or 9. There are 7 choices.

Let B be the set of three-digit positive integers that have no 8's and no 9's. Then $|B| = 7 \cdot 8 \cdot 8$. The recipe for B is as follows:

1. Pick the first digit. It can't be 0, 8, or 9. There are 7 choices.
2. Pick the second digit. It can't be 8 or 9. There are 8 choices.
3. Pick the last digit. It can't be 8 or 9. There are 8 choices.

The number of three-digit positive integers that have a 7 but have no 8's or 9's is $|B - A|$. Since $A \subseteq B$, this is

$$|B - A| = |B| - |A| = 7 \cdot 8 \cdot 8 - 6 \cdot 7 \cdot 7 = 7 \cdot (8 \cdot 8 - 6 \cdot 7) = 7 \cdot (64 - 42) = 7 \cdot 22 = 154.$$

7. (a) Suppose that $f\colon \mathbb{Z} \to \mathbb{Z}$ is a one-to-one function. Define a function $g\colon \mathbb{Z} \to \mathbb{Z}$ by: for all $x \in \mathbb{Z}$, $g(x) = -f(x)$. Prove that g is also one-to-one.

Solution. *Proof.* Let x_1 and x_2 be arbitrary integers. Assume that $g(x_1) = g(x_2)$. Then $-f(x_1) = -f(x_2)$. Multiplying by -1 gives us $f(x_1) = f(x_2)$. Then $x_1 = x_2$, since f is one-to-one. Hence g is one-to-one. □

(b) Suppose that $f\colon \mathbb{Z} \to \mathbb{Z}$ is an onto function. Define a function $g\colon \mathbb{Z} \to \mathbb{Z}$ by: for all $x \in \mathbb{Z}$, $g(x) = f(x) + 4$. Prove that g is also onto.

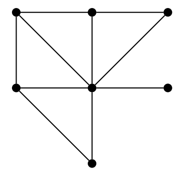
Solution. *Proof.* Let y be an arbitrary integer. Then $y - 4$ is also an integer. Since f is onto, there exists an $x \in \mathbb{Z}$ so that $f(x) = y - 4$. Then $g(x) = f(x) + 4 = y - 4 + 4 = y$, so g is onto. □

(c) Suppose that f and g are one-to-one functions from $\mathbb{Z}$ to $\mathbb{Z}$. Define the function $h\colon \mathbb{Z} \to \mathbb{Z}$ by $h(x) = f(x) + g(x)$ for all $x \in \mathbb{Z}$. Must h be one-to-one? Give a proof or counter example.

Solution. It does not have to be the case that h is one-to-one. Let f be the function defined by $f(x) = x$ for all $x \in \mathbb{Z}$ and let g be the function defined by $g(x) = -f(x)$. Note that f is one-to-one. Furthermore, g is also one-to-one, because of the statement in part (a). However, $h(1) = f(1) + g(1) = 1 - 1 = 0$ and $h(0) = f(0) + g(0) = 0$. Therefore h is not one-to-one.

8. (a) Draw a **simple** graph G with exactly seven vertices and exactly ten edges, and so that some vertex of G has degree 6.

   Solution. One example of such a graph is:

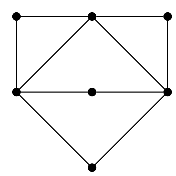


   (b) Answer part (a) again, but so that your graph G does **not** have an Euler circuit. (Be sure to explain why you know that G does not have an Euler circuit.)

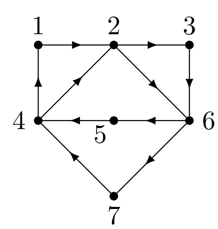
   Solution. The graph given in the solution to part (a) does not have an Euler circuit, because at least one vertex has odd degree.

   (c) Answer part (a) again, but so that your graph G **does** have an Euler circuit. (Be sure to explain why you know that G has an Euler circuit.)

   Solution. One example of such a graph is:



   This graph is simple, since it does not have any loops or parallel edges. This graph also has an Euler circuit. One example of an Euler circuit on this graph would be the circuit labeled here:



   that starts and ends at vertex 1 and goes $1 \to 2 \to 3 \to 6 \to 5 \to 4 \to 2 \to 6 \to 7 \to 4 \to 1$. (Alternatively, we see that it must have an Euler circuit because it is connected and every vertex has even degree.)

9. Define the sequence $a_1, a_2, a_3, \ldots$ by: $a_1 = 1$, and $a_n = 7a_{n-1} + 4$ for all integers $n \geq 2$. Prove by **induction on** n that a_n is odd for all integers $n \geq 1$. (Use no facts about odd integers except the definition.)

   Solution. Let $P(n)$ be the statement: "a_n is odd".

   Proof. We will prove that $P(n)$ is true for all integers $n \geq 1$ by induction on n.

   Base case ($n = 1$): We have $a_1 = 1$ by definition, and 1 is odd. So $P(1)$ is true.

Induction step: Let $k \geq 1$ be an integer. Suppose that a_k is odd (IH). By IH, there exists an integer m so that

$$a_k = 2m + 1. \tag{$*$}$$

(We want to show that a_{k+1} is odd.) Now

$$\begin{aligned}
a_{k+1} &= 7a_k + 4 \\
&= 7(2m+1) + 4 && \text{by } (*) \\
&= 14m + 7 + 4 \\
&= 14m + 10 + 1 \\
&= 2(7m+5) + 1,
\end{aligned}$$

where $7m + 5$ is an integer, so a_{k+1} is odd.

By the principle of induction, a_n is odd for all integers $n \geq 1$. $\square$