MAT-CSC A67: Discrete Mathematics — Summer 2024

Assignmnet 4: Sets, Cardinality of Sets, Modular Arithmetic

Due Date: Sunday, July 14, 11:59 PM, on Crowdmark

[**NOTE:** Bonus points earned in the assignments will only contribute to your total assignment grade and will not be applied to your quiz, term test, or final exam grades. We will be extra strict with grading bonus questions.]

Q1. **(4 pts, Set Basics)** Let A, B, C and D be arbitrary sets.

1.a. Prove that $A \subseteq \emptyset$ if and only if $A = \emptyset$.

1.b. Suppose that $A \cup B \subseteq C \cup D$ and $A \cap B = \emptyset$. If $C \subseteq A$, prove that $B \subseteq D$.

Q2. **(8 pts, Solving Congruences)** Let a, b, d, and $n > 1$ be arbitrary integers.

2.a. Prove that if $ad \equiv bd \pmod{n}$, then $a \equiv b \pmod{\frac{n}{\gcd(d,n)}}$.

2.b. Solve $7x \equiv 12 \pmod{13}$ for $x \in \{0, 1, 2, \ldots, 12\}$.

2.c. Solve $84x - 38 \equiv 79 \pmod{15}$ for $x \in \{0, 1, 2, \ldots, 14\}$.

2.d. Solve $2x \equiv 3 \pmod{14}$ for $x \in \{0, 1, 2, \ldots, 13\}$.

Q3. **(6 pts, Fermat's Little Theorem)** The french mathematician Pierre de Fermat, one of the leading mathematicians of the first half of the seventeenth century, made many important discoveries in number theory. One of the most useful of these states that if p is prime and p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$. This result is known as Fermat's Little Theorem. Use this theorem to answer the following questions.

3.a. Prove that there does not exists any two integers a and b, neither of which is divisible by 17, such that $a^{16} \not\equiv b^{16} \pmod{17}$.

3.b. Find an integer d such that $(M^{11})^d \equiv M \pmod{55}$ for all M prime to 55.
[**HINT:** You may find using the following theorem that you proved in Quiz 7 helpful. Let $m_1, m_2, m_3, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. If $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m_1 m_2 \ldots m_n}$.]

3.c. Use Fermat's little theorem to find $5^{2003} \mod 1001$.
[**NOTE:** $1001 = 7 \cdot 11 \cdot 13$.]
[**HINT:** You may find using the following theorem that you proved in Quiz 7 helpful. Let $m_1, m_2, m_3, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. If $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m_1 m_2 \ldots m_n}$.]

Q4. **(4 pts, Set of Finite Binary Strings)** Consider the following definition of binary strings:

> The set of finite binary strings, denoted by $\{0,1\}^*$ which we read as "zero one star", is defined (recursively) by:
>
> **Basis Step:** $\lambda \in \{0,1\}^*$
> **Recursive Step:** If $s \in \{0,1\}^*$, then $s0 \in \{0,1\}^*$ and $s1 \in \{0,1\}^*$
>
> where $s0$ and $s1$ are the results of string concatenation. The symbol λ, pronounced "lambda" is used to denote the empty string and has the property that $\lambda x = x\lambda = x$ for each string x.

Determine and justify whether the set $\{0,1\}^*$ is finite, countably infinite, or uncountable.

Q5. **(4 pts)** Consider the function redun3 : $\{0,1\}^* \to \{0,1\}^*$ where the output of the function is computed by the algorithm below.

Listing 1: Create redundancy by repeating each bit three times

```
procedure redun3($a_{k-1} \cdots a_0$)
for $i$ := 0 to $k-1$
$c_{3i}$ := $a_i$
$c_{3i+1}$ := $a_i$
$c_{3i+2}$ := $a_i$
return $c_{3k-1} \cdots c_0$
```

1. Determine and briefly justify whether redun3 is one-to-one.
2. Determine and briefly justify whether redun3 is onto.

Q6. (8 pts) Find explicit bijections to prove the following.

6.a. The set of even positive integers has the same cardinality as the set of odd positive integers.

6.b. The sets $\mathbb{R}$ and $(0, 1)$ have the same cardinality.
[**HINT:** You may find the function $\arctan x$ useful.]

6.c. The sets $\{x : \exists a \in \mathbb{Z}_{>1} x = \frac{1}{a}\}$ and $\{x : \exists a \in \mathbb{Z}_{\geq 1} x = \frac{1}{a}\}$ have the same cardinality.

6.d. The sets $(0, 1)$ and $(0, 1]$ have the same cardinality.
[**HINT:** You may find the bijection in part **6.c.** useful.]

Q7. **(2 Bonus pts, from "Introduction to Higher Mathematics," by Patrick Keef and David Guichard.)** We have now seen infinite sets of two different sizes $\aleph_0$ which denotes the cardinality of $\mathbb{Z}_{>0}$ and c which denotes the cardinality of $\mathbb{R}$. Is there a largest infinite size, *i.e.*, a largest cardinal number?

George Cantor answered this question by studying the power sets. Recall that for any set A, the power set of A, written $\mathcal{P}(A)$, is the collection of all subsets of A. For finite sets, the power set is not just larger than the original set, it is much larger. This makes it natural to hope that the power set of an infinite set will be larger than the base set.

Let $|A| < |B|$ mean that $|A| \leq |B|$, but A and B do not have the same cardinality. The next theorem answers both questions posed above.

> **Cantor's Theorem:** If A is any set, then $|A| < |\mathcal{P}(A)|$.
>
> **Proof:** Assume A is an arbitrary set. First, we need to show that $|A| \leq |P(A)|$. Define an injection $f : A \to \mathcal{P}(A)$ by $f(a) = \{a\}$.
>
> Now we need to show that there is no bijection $g : A \to \mathcal{P}(A)$. For a contradiction, suppose g is such a bijection. Let $S = \{a \in A : a \notin g(a)\} \subseteq A$. Since $S \in \mathcal{P}(A)$, $S = g(x)$, for some $x \in A$, because g is a surjection. There are two possibilities: $x \in S$ and $x \notin S$.
>
> 1. If $x \in S$, then $x \notin g(x) = S$, *i.e.*, $x \notin S$, a contradiction.
> 2. If $x \notin S$, then $x \in g(x) = S$, *i.e.*, $x \in S$, a contradiction.
>
> Therefore, no such bijection is possible.□

Now, it is your turn to use Cantor's Theorem to **prove that there is not a largest set**, *i.e.*, for any set A there is a set B with $|A| < |B|$.

"Are you not entertained?" Wait for what comes next.

Many questions about the cardinal numbers remain. Since we know that $\mathbb{Z}$ and $\mathbb{Q}$ are the same size, and that $\mathbb{R}$ is larger, one very natural question is whether there are any sets *between* $\mathbb{Z}$ and $\mathbb{R}$, that is, strictly bigger than $\mathbb{Z}$ (and $\mathbb{Q}$) but strictly smaller than $\mathbb{R}$. The **continuum hypothesis** says:

> **continuum hypothesis:** There is no set A with $|\mathbb{Z}| < |A| < |\mathbb{R}|$.

That is, the continuum hypothesis asserts that $|\mathbb{R}|$ is the first cardinal number larger than $|\mathbb{Z}|$. Remarkably, the continuum hypothesis cannot be proved to be true and cannot be proved to be false. In the 1920's, Kurt Gödel showed that the continuum hypothesis cannot be disproved, and in the early 1960's, Paul Cohen showed that it cannot be proved either.

Q8. **(10 Bonus pts, An Introduction to Measure Theory)** The length of an interval (a, b) is clear – we define $l(a, b) = b - a$ as expected – but we'd like to generalize length to more sets. Doing this in general is a bit complicated, so we'll restrict ourselves to studying zero length. Given a set $S \subseteq R$ we say S has measure zero if for every $\epsilon > 0$ there is a countable collection of intervals $I_1, I_2, \ldots$ so that both $S \subseteq I_1 \cup I_2 \cup \ldots$ and

$$l(I_1) + l(I_2) + \ldots < \epsilon.$$

8.a. Prove that for any $x \in \mathbb{R}$, the singleton set $\{x\}$ has measure zero.

8.b. Prove that whenever $A \subseteq B$ and B has measure zero, then A also has measure zero.

8.c. Given two sets A and B with measure zero, prove that $A \cup B$ has measure zero.

8.d. Given a countable collection of measure zero sets $A_1, A_2, A_3, \ldots$, prove their union has measure zero. [**HINT:** For each n, cover A_n by intervals with error less than $\frac{\epsilon}{2^n}$.]

8.e. Prove that $\mathbb{Q}$ has measure zero.