CS 2051: Honors Discrete Mathematics
Spring 2023 Homework 6 Supplement

Sean Peng*

1. A countable set is a set that has a one-to-one mapping with the set of natural numbers. Prove that the set of positive rational numbers is countable by setting up a function that assigns to a rational number p/q with $\gcd(p, q) = 1$ the base 11 number formed by the decimal representation of p followed by the base 11 digit A, which corresponds to the decimal number 10, followed by the decimal representation of q.

   Solution: By the definition of rational numbers, for all $x \in \mathbb{Q}$, there exists $p, q \in \mathbb{Z}$, such that $x = p/q$ and $\gcd(p, q) = 1$. Let $f : \mathbb{Q}^+ \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A\}^n$, such that $f(p/q) = (pAq)_{11}$, where $\gcd(p, q) = 1$ and $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A\}^n$ is the set of base 11 numbers. We will show that this function is one-to-one.

   Let $x, y \in \mathbb{Q}^+$, where $f(x) = f(y)$. By the definition of rational numbers, we have $x = p/q, y = r/s$, where $p, q, r, s \in \mathbb{Z}^+$ and $\gcd(p, q) = \gcd(r, s) = 1$. By the definition of f, $pAq = rAs$. Since p, q, r, s do not contain the digit A, we have $p = r, q = s$. Then, $p/q = r/s$ and $x = y$. We have shown that if $f(x) = f(y)$, then $x = y$. Therefore, f is one-to-one.

   If $p, q > 0$, then $(pAq)_{11} > 0$. Since every element in the range of f is positive, and each positive base 11 number converts to a different positive decimal number, there is also a one-to-one mapping from $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A\}^n$ to $\mathbb{N}$. Then, there is a one-to-one mapping of $|\mathbb{Q}^+|$ to $\mathbb{N}$. Therefore, we have proven that $\mathbb{Q}^+$ is countable. ■

2. Define a Carmichael number as a composite number n which satisfies the following relation: $b^n \equiv b \pmod{n}$, for all integers b. Show that if $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes that satisfy $p_j - 1 | n - 1$ for $j = 1, 2, \ldots, k$, then n is a Carmichael number.

   Solution: I proceed with a direct proof. We will show that if $n = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes that satisfy $p_j - 1 | n - 1$ for $j = 1, 2, \ldots, k$, then n is a Carmichael number.

   Let $b \in \mathbb{Z}$. WLOG, let p_j be an arbitrary prime factor of n, where $1 \leq j \leq n$. We will consider two cases: $\gcd(b, p_j) = 1$ and $\gcd(b, p_j) > 1$.

   Suppose $\gcd(b, p_j) = 1$. By Fermat's Little Theorem, $b^{p_j - 1} \equiv 1 \pmod{p_j}$. Since $p_j - 1 | n - 1$, there exists a constant c such that $n - 1 = c(p_j - 1)$. Then,

$$
\begin{aligned}
b^{(p_j-1)c} &\equiv 1^c \pmod{p_j} && \text{Raise both sides to the power of } c \\
b^{n-1} &\equiv 1 \pmod{p_j} && \text{Simplify both sides} \\
b^n &\equiv n \pmod{p_j} && \text{Multiply both sides by n}
\end{aligned}
$$

*Solutions were published with the permission of the student.

Suppose $\gcd(b, p_j) > 1$. Then, since p_j is prime, we have $p_j | b$, which leads to:

$$\begin{aligned}
b &\equiv 0 \pmod{p_j} && \text{Definition of mod} \\
b^n &\equiv 0 \pmod{p_j} && \text{Raise both sides to the power of } n \\
b^n &\equiv b \pmod{p_j} && \text{From line 1 and 2}
\end{aligned}$$

We have shown that for all $j, 1 \leq j \leq n$, $b^n \equiv b \pmod{p_j}$, for all $b \in \mathbb{Z}$. Since $n = p_1 p_2 \cdots p_k$ where $p_1, p_2, \ldots, p_k$ are distinct, by the Chinese Remainder Theorem, $b^n \equiv b \pmod{n}$, for all $b \in \mathbb{Z}$. Therefore, with the given conditions, n is a Carmichael number. ■