Problem Set 4

Due: October 4

Reading: Chapter 7. *Infinite Sets*; Chapter 8. *Number Theory* through 8.9. *Multiplicative Inverses and Cancelling*

Problem 1. (a) Define sets A and B such that $\mathbb{N}$ strict A strict B.

Solution. $A = \text{pow}(\mathbb{N})$ and $B = \text{pow}(A)$, for example. ■

(b) Prove or disprove the following claim: *The set of computer programs is uncountable.*

Hint: Refer to the definitions of *ASCII** and *string procedures* from Section 7.2 of the textbook.

Solution. *False.*

Consider a numeral system where the available digits are exactly the set of ASCII characters (the numeric value of each character is inconsequential). Counting in this numeral system equates to enumerating the elements of ASCII*, so ASCII* bij $\mathbb{N}$. Let P be the set of string procedures. For every string procedure $P_s \in P$ there exists at least one string $s \in$ ASCII* which describes it, so ASCII* surj P, and therefore $\mathbb{N}$ surj P. We can define a bijection between $\mathbb{N}$ and P by skipping over repeated string procedures when pairing elements of P with elements of $\mathbb{N}$. Therefore, P is countable. ■

(c) Compute $\text{rem}((2498754270^{184638463})(9234673466^{844759364}), 22)$.

Hint: $18^9 \equiv 8 \mod 22$

Solution. First, we replace the bases of the exponents with their remainders.

$$\text{rem}((12^{184638463})(18^{844759364}), 22)$$

Now, let's examine the remainders of the first few powers of 12.

$$\begin{aligned} \text{rem}(12, 22) &= 12 \\ \text{rem}(12^2, 22) &= 12 \\ \text{rem}(12^3, 22) &= 12 \\ &\cdots \end{aligned}$$

The remainder is always 12. So we can now write

$$\text{rem}((12)(18^{844759364}), 22).$$

Now let's look at the remainders of powers of 18.

$$\begin{aligned}
\text{rem}(18, 22) &= 18\\
\text{rem}(18^2, 22) &= 16\\
\text{rem}(18^3, 22) &= 2\\
\text{rem}(18^4, 22) &= 14\\
\text{rem}(18^5, 22) &= 10\\
\text{rem}(18^6, 22) &= 4\\
\text{rem}(18^7, 22) &= 6\\
\text{rem}(18^8, 22) &= 20\\
\text{rem}(18^9, 22) &= 8\\
\text{rem}(18^{10}, 22) &= 12\\
\text{rem}(18^{11}, 22) &= 18\\
&\cdots
\end{aligned}$$

So it repeats after 11 steps. This means we can keep subtracting 11 from the exponent until the computation becomes feasable. In other words, we can replace the exponent with its remainder mod 11.

$$\begin{aligned}
\text{rem}((12)(18^9), 22) &= \text{rem}((12)(8), 22)\\
&= 8
\end{aligned}$$

■

Problem 2.
In this problem you will prove a fact that may surprise you—or make you even more convinced that set theory is nonsense: the half-open unit interval is actually the "*same size*" as the nonnegative quadrant of the real plane![1] Namely, there is a bijection from $(0, 1]$ to $[0, \infty) \times [0, \infty)$.

(a) Describe a bijection from $(0, 1]$ to $[0, \infty)$.

Hint: $1/x$ almost works.

Solution. $f(x) ::= 1/x$ defines a bijection from $(0, 1]$ to $[1, \infty)$, so $g(x) ::= f(x) - 1$ does the job. ■

(b) An infinite sequence of the decimal digits $\{0, 1, \ldots, 9\}$ will be called *long* if it does not end with all 0's. An equivalent way to say this is that a long sequence is one that has infinitely many occurrences of nonzero digits. Let L be the set of all such long sequences. Describe a bijection from L to the half-open real interval $(0, 1]$.

Hint: Put a decimal point at the beginning of the sequence.

Solution. Putting a decimal point in front of a long sequence defines a bijection from L to $(0, 1]$. This follows because every real number in $(0, 1]$ has a unique long decimal expansion. Note that if we didn't exclude the non-long sequences, namely, those sequences ending with all zeroes, this wouldn't be a bijection. For example, putting a decimal point in front of the sequences $1000\ldots$ and $099999\ldots$ maps both sequences to the same real number, namely, $1/10$. ■

[1] The half open unit interval, $(0, 1]$, is $\{r \in \mathbb{R} \mid 0 < r \leq 1\}$. Similarly, $[0, \infty) ::= \{r \in \mathbb{R} \mid r \geq 0\}$.

(c) Describe a surjective function from L to L^2 that involves alternating digits from two long sequences. *Hint:* The surjection need not be total.

Solution. Given any long sequence $s = x_0, x_1, x_2, \ldots$, let

$$h_0(s) ::= x_0, x_2, x_4, \ldots$$

be the sequence of digits in even positions. Similarly, let

$$h_1(s) ::= x_1, x_3, x_5, \ldots$$

be the sequence of digits in odd positions. Then h is a surjective function from L to L^2, where

$$h(s) ::= \begin{cases} (h_1(s), h_2(s)), & \text{if } h_1(s) \in L \text{ and } h_2(s) \in L, \\ \text{undefined}, & \text{otherwise.} \end{cases} \tag{1}$$

■

(d) Prove the following lemma and use it to conclude that there is a bijection from L^2 to $(0, 1]^2$.

Lemma 2.1. *Let A and B be nonempty sets. If there is a bijection from A to B, then there is also a bijection from $A \times A$ to $B \times B$.*

Solution. *Proof.* Suppose $f : A \to B$ is a bijection. Let $g : A^2 \to B^2$ be the function defined by the rule $g(x, y) = (f(x), f(y))$. It is easy to show that g is a bijection:

- g **is total**: Since f is total, $f(a_1)$ and $f(a_2)$ exist $\forall a_1, a_2 \in A$ and so $g(a_1, a_2) = (f(a_1), f(a_2))$ also exists.
- g **is surjective**: Since f is surjective, for any $b_i \in B$ there exists $a_i \in A$ such that $b_i = f(a_i)$. So for any (b_1, b_2) in B^2, there is a pair $(a_1, a_2) \in A^2$ such that $g(a_1, a_2) ::= (f(a_1), f(a_2)) = (b_1, b_2)$. This shows that g is a surjection.
- g **is injective**:

$$\begin{aligned} g(a_1, a_2) = g(a_3, a_4) \quad &\text{iff} \quad (f(a_1), f(a_2)) = (f(a_3), f(a_4)) && \text{(by def of } g\text{)} \\ &\text{iff} \quad f(a_1) = f(a_3) \text{ AND } f(a_2) = f(a_4) \\ &\text{iff} \quad a_1 = a_3 \text{ AND } a_2 = a_4 \text{(since } f \text{ is injective)} \\ &(a_1, a_2) = (a_3, a_4), \end{aligned}$$

  which confirms that g is injective.

■

Since it was shown in part (b) that there is a bijection from L to $(0, 1]$, an immediate corollary of the Lemma is that there is a bijection from L^2 to $(0, 1]^2$. ■

(e) Conclude from the previous parts that there is a surjection from $(0, 1]$ and $(0, 1]^2$. Then appeal to the Schröder-Bernstein Theorem to show that there is actually a bijection from $(0, 1]$ and $(0, 1]^2$.

Solution. There is a bijection between $(0, 1]$ and L by part (b), a surjective function from L to L^2 by part (c), and a bijection from from L^2 to $(0, 1]^2$ by part (d). These surjections compose to yield a surjection from $(0, 1]$ to $(0, 1]^2$.

Conversely, there is obviously a surjective function $f : (0, 1]^2 \to (0, 1]$, namely

$$f(\langle x, y \rangle) ::= x.$$

The Schröder-Bernstein Theorem now implies that there is a bijection from $(0, 1]$ to $(0, 1]^2$. ■

(f) Complete the proof that there is a bijection from $(0, 1]$ to $[0, \infty)^2$.

Solution. There is a bijection from $(0, 1]$ to $(0, 1]^2$ by part (e), and there is a bijection from $(0, 1]^2$ to $[0, \infty)^2$ by part (a) and the Lemma. These bijections compose to yield a bijection from $(0, 1]$ to $[0, \infty)^2$. ■

Problem 3.
Let m, n be integers, not both zero. Define a set of integers, $L_{m,n}$, recursively as follows:

- **Base cases**: $m, n \in L_{m,n}$.
- **Constructor cases**: If $j, k \in L_{m,n}$, then
  1. $-j \in L_{m,n}$,
  2. $j + k \in L_{m,n}$.

Let L be an abbreviation for $L_{m,n}$ in the rest of this problem.

(a) Prove *by structural induction* that every common divisor of m and n also divides every member of L.

Solution. We proceed by structural induction on the definition of $a \in L$. The induction hypothesis is

$$P(a) ::= \forall q.((q \mid m \text{ AND } q \mid n) \text{ IMPLIES } q \mid a).$$

Base cases: Clearly, any common divisor, q, of m and n will divide m, so $P(m)$ holds. q will also divide n, so $P(n)$ holds. This completes the proof for the base cases.

Constructor cases: Assume that $P(j)$ and $P(k)$. That is, any common divisor, q, of m and n also divides j and k. Since q divides both j and k, therefore it must divide any linear combination of j and k, in particular $-j$ and $j + k$. Thus $P(j)$ and $P(k)$ imply both $P(-j)$ and $P(j + k)$. This completes the proof for the constructor cases.

We conclude by structural induction that $P(a)$ holds for all $a \in L$, as required. ■

(b) Prove that any integer multiple of an element of L is also in L.

Solution. Let a be an element of L and define the predicate

$$P(k) ::= ka \in L.$$

We prove that $P(k)$ holds for all $k \in \mathbb{N}$ by induction on k, with induction hypothesis, P.

Base case ($k = 0$): $0a = 0 = m + (-m) \in L$.

Induction step: Assume $P(k)$, so $ka \in L$. But we are given that $a \in L$, so $(k + 1)a = ka + a \in L$ by the second recursive step in the definition of L. This proves $P(k + 1)$, completing the induction proof.

Now since $ka \in L$ implies $-ka \in L$ by the first recursive step in the definition of L, we conclude that $ka \in L$ for all $k \in \mathbb{Z}$ ■

(c) Show that if $j, k \in L$ and $k \neq 0$, then $\text{rem}(j, k) \in L$.

Solution. Say r is the remainder of j divided by k. That is, $j = qk + r$ for some quotient $q \in \mathbb{Z}$ and remainder, r, where $0 \leq r < |k|$.

Now that $(-q)k \in L$ by part (b), so $j + (-q)k \in L$ the second recursive step in the definition of L. That is, $r \in L$. ■

(d) Show that there is a positive integer $g \in L$ which divides every member of L. *Hint:* The least positive integer in L.

Solution. At least one of the integers $m, -m, n, -n \in L$ must be positive. Hence by the Well Ordering Principle, there is a least positive integer $g \in L$.

Suppose $a \in L$. We must show that $g \mid a$.

We prove this by contradiction: if g does not divide a, then $\text{rem}(a,\ g)$ is a positive integer which is in L by part (c). But $\text{rem}(a,\ g)$ is by definition less than g, contradicting the minimality of g. ■

(e) Conclude that $g = \text{GCD}(m, n)$ for g from part (d).

Solution. Solution 1: We will prove this by contradiction: Let $h = \text{GCD}(m, n)$ and suppose that $h \neq g$. Since $m, n \in L$ and g divides every element of L, therefore g is a common divisor of m and n. Since h is their greatest common divisor and g is not, therefore $h > g$.

Since h is a common divisor of m and n, therefore by part (a), h divides every element of L. But $g \in L$, so $h \mid g$, and therefore $h \leq g$. Contradiction!

Thus our original assumption must have been false, and therefore $g = \text{GCD}(m, n)$, as required.

Solution 2: Since $m, n \in L$, therefore by part (b), $sm, tn \in L$ for all $s, t \in \mathbb{Z}$. By the second constructor case, then, $sm + tn \in L$.

Recall from Corollary 8.2.3 in the Notes that an integer is a linear combination of m and n iff it is a multiple of $\text{GCD}(m, n)$. Since $\text{GCD}(m, n) > 0$, therefore $\text{GCD}(m, n)$ is equal to the smallest positive linear combination of m and n.

Now proceed by contradiction. Suppose that $g \neq \text{GCD}(m, n)$. Then g is not equal to the smallest positive value of $sm + tn$. That is, there exist $s_0, t_0 \in \mathbb{Z}$ such that $0 < s_0 m + t_0 n < g$. But $s_0 m + t_0 n \in L$, contradicting the fact from part (d) that g is the smallest positive member of L.

Thus it must be that $g = \text{GCD}(m, n)$, as required.

■

Problem 4.

Suppose a, b are relatively prime integers greater than 1. In this problem you will prove that Euler's function is *multiplicative*, that is, that

$$\phi(ab) = \phi(a)\phi(b).$$

The proof is an easy consequence of the Chinese Remainder Theorem.[2]

(a) Conclude from the Chinese Remainder Theorem that the function $f : [0, ab) \to [0, a) \times [0, b)$ defined by

$$f(x) ::= (\text{rem}(x,\ a), \text{rem}(x,\ b))$$

is a bijection.

[2] The *Chinese Remainder Theorem* asserts that if a, b are relatively prime and greater than 1, then for all m, n, there is a *unique* $x \in [0, ab)$ such that

$$x \equiv m \pmod{a},$$
$$x \equiv n \pmod{b}.$$

A proof appears in Problem 8.49.

Solution. By definition, f has the [= 1 out], total function property.

The Chinese Remainder Theorem says that the congruences

$$x \equiv m \pmod{a},$$
$$x \equiv n \pmod{b}.$$

have a solution x, which means that f has the [$\geq$ 1 in], surjective property. Moreover, the solution is unique up to congruence modulo ab, which means that all solutions have the same remainder modulo ab. So in particular, there is a unique solution $x \in [0, ab)$, which means that f has the [$\leq$ 1 in], injective property, and hence f is a bijection, namely, [= 1 out] and [= 1 in]. ■

(b) For any positive integer, k, let $\mathbb{Z}_k^*$ be the integers in $[0, k)$ that are relatively prime to k. Prove that the function f from part (a) also defines a bijection from $\mathbb{Z}_{ab}^*$ to $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$.

Solution. By Unique Factorization, x is relatively prime to ab iff x is relatively prime to a and x is relatively prime to b. But since $\gcd(x, a) = \gcd(a, \text{rem}(x, a))$, it follows that x is relatively prime to a iff $\text{rem}(x, a)$ is relatively prime to a, and likewise for b. That is,

$$x \in \mathbb{Z}_{ab}^* \quad \text{iff} \quad f(x) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^*,$$

which means that f defines a total surjective function from $\mathbb{Z}_{ab}^*$ to $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$. And since $f : [0, ab) \to [0, a) \times [0, b)$ was injective, it remains injective when restricted to the domain $\mathbb{Z}_{ab}^*$, which proves that f defines a bijection from $\mathbb{Z}_{ab}^*$ to $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$. ■

(c) Conclude from the preceding parts of this problem that

$$\phi(ab) = \phi(a)\phi(b). \tag{2}$$

Solution. The mapping f defines a bijection between $\mathbb{Z}_{ab}^*$ and $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$. So

$$\phi(ab) ::= |\mathbb{Z}_{ab}^*| = |\mathbb{Z}_a^* \times \mathbb{Z}_b^*| = |\mathbb{Z}_a^*| \cdot |\mathbb{Z}_b^*| = \phi(a) \cdot \phi(b).$$

■

(d) Prove Corollary 8.10.11: for any number $n > 1$, if $p_1, p_2, \ldots, p_j$ are the (distinct) prime factors of n, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_j}\right).$$

Solution. We know from Theorem 8.10.10 that for all primes, p, and $k > 0$,

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

So if

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_j^{k_j}$$

where all the k's are positive, then repeated applications of (2) give

$$\begin{aligned}
\phi(n) &= \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_j^{k_j}) \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdot p_1^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_1^{k_j}\left(1 - \frac{1}{p_j}\right) \\
&= p_1^{k_1} \cdot p_2^{k_2} \cdots p_j^{k_j} \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_j}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_j}\right).
\end{aligned}$$

■