Massachusetts Institute of Technology
6.042J/18.062J, Fall '13: Mathematics for Computer Science
Prof. Albert R Meyer

September 25
revised Tuesday 24th September, 2013, 15:37

Problem Set 4

Due: October 4

Reading: Chapter 6. *Recursive Data Types*; Chapter 7. *Infinite Sets*; Chapter 8. *Number Theory* through 8.4. *The Fundamental Theorem of Arithmetic*

Problem 1.
Ben Bitdiddle is building an online system to process orders for a restaurant. Ben's brilliant idea is to have customers enter their orders online ahead of time so their food is ready when they arrive. Ben would like his online system to validate user input so that customers are immediately aware of any problems with their orders.

Ben wants to make his system as user-friendly as possible. In addition to specifying the items they want to order, customers should be able to input how many of each item they want—in plain English! For example, a customer should be able to order "five factorial" french fries and "positive square root of four" hamburgers. However, a customer should not be able to order "George Washington" slices of pizza (because "George Washington" does not describe a quantity). Ben is faced with a challenge—how can a computer program determine whether an English phrase describes a number?

ASCII is a 256-character alphabet that is often used in computer software. Let ASCII* be the set of (finite) strings of ASCII characters, as described in Section 7.2 of the textbook. Let ASCII_NUM* be the subset of ASCII* which are English descriptions of nonnegative real numbers (not necessarily integers).

(a) Describe a bijection between $\mathbb{N}$ and ASCII_NUM*.

Solution. One way to enumerate the strings in ASCII_NUM* is to sort them first by length and then alphabetically. ■

(b) Consider the numbers S identified by the strings in ASCII_NUM*. In plain English, describe a number which is different from all of them.

Solution. We use diagonalization. Order the numbers in S according to the bijection from part (a). Construct a new number q according to the following: the integer part of q is 1, and the n^{th} digit in the decimal part of q is 2 if the corresponding digit in the n^{th} member of S is not 2, and 1 otherwise. q differs from every number in S at some digit, so $q \notin S$. ■

(c) Conclude that ASCII_NUM* is not a valid set, and that Ben's efforts are futile.

Solution. The solution to part (b) is an English description of a number, so it must be in ASCII_NUM*. That number q must therefore be in S, but we have just shown otherwise—a contradiction. So our assumption that ASCII_NUM* is a valid set is false, and there is no algorithm which determines whether a string is a description of a number. ■

Problem 2.
Fractals are an example of mathematical objects that can be defined recursively. In this problem, we consider the Koch snowflake. Any Koch snowflake can be constructed by the following recursive definition.

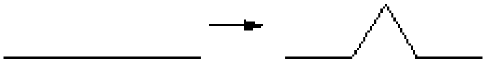

Figure 1 Constructing the Koch Snowflake.

- **base case**: An equilateral triangle with a positive integer side length is a Koch snowflake.
- **constructor case**: Let K be a Koch snowflake, and let l be a line segment on the snowflake. Remove the middle third of l, and replace it with two line segments of the same length as is done in Figure 1

  The resulting figure is also a Koch snowflake.

Prove by structural induction that the area inside any Koch snowflake is of the form $q\sqrt{3}$, where q is a rational number.

Solution. We first show that the side length of any Koch snowflake is rational, and prove it in the lemma below.

Lemma. *Every side length of a Koch snowflake is rational.*

Proof. For the base case, every side length is the same positive integer. For the inductive case, let K be a Koch snowflake. Then K was constructed by modifying a Koch snowflake K' as in the recursive case. By the induction hypothesis, each side length of K' is rational. Let l be the line segment of K' modified via the recursive case. The two new line segments are of length $\frac{l}{3}$, which is rational since l is rational. ■

Now, we prove the main theorem.

Proof. We prove the claim by structural induction.

For the base case, the area of an equilateral triangle with side length l is $q\sqrt{3}$, where $q = \frac{l}{2}$.

For the inductive case, let K be a Koch snowflake. K was constructed by modifying a Koch snowflake K' as in the recursive case above. By the induction hypothesis, the area of K' is $q\sqrt{3}$ for some rational q. Let l' be the length of the line segment of K' that was modified according to the recursive case. The area added by the modification is $q'\sqrt{3}$, where $q' = \frac{l'}{6}$. By the above lemma, l' is rational, so q' is rational. Thus, the area of K is $(q' + q) \cdot \sqrt{3}$, and $q' + q$ is rational, so we have proved our claim. ■

Problem 3.

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.

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

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`... and `099999`... maps both sequences to the same real number, namely, $1/10$. ■

(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 3.1. *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 4.

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 $0 < s_0m + t_0n < g$. But $s_0m + t_0n \in L$, 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.

■