# MATH221-001 200630 Group Work 1 Solutions DRAFT

Edward Doolittle

November 12, 2006

1. (a) The set $S = \{23, 24, 25, \ldots\}$. We would like to define a function $f : S \to \mathbb{N}$ by $f(n) = n - 22$, which would be a bijection, but unfortunately we don't yet have a definition of the subtraction operation. We could define subtraction (which will take almost the entirety of chapter 7, so isn't easy) or we can work in the following roundabout way.

   We define a function $g : \mathbb{N} \to S$ by $g(n) = n + 22$. That function is a surjection because if $m \in S$, then $m \geq 23$ which by the definition of $\geq$ means that either $m = 23$ or $m > 23$. In the first case, $m = g(1)$. In the second case, the definition of $>$ implies that there is a number $n$ such that $m = 23 + n$, in which case $m = g(n + 1)$. In any case, $m = g(n)$ for some $n \in \mathbb{N}$, so the map is surjective. Furthermore, the map is an injection because $g(n_1) = g(n_2)$ implies $n_1 + 22 = n_2 + 22$ which by the cancellation rule for addition implies $n_1 = n_2$. Therefore $g$ is a bijection.

   Since $g$ is a bijection it has an inverse $g^{-1}$ which is also a bijection. Let $f = g^{-1}$. Then $f$ has all the required properties: $f : S \to \mathbb{N}$ and $f$ is a bijection. (What we have done is essentially to define subtraction of the number 22 from another number; the problem with the above definition is that subtraction only works for $n$ large enough, which is messy.)

   (b) As in part (a), we define a function $g(n) = 5n$ and use $g$ to construct a function $f$ with the required properties. I'll leave the details up to you.

   (c) Here the function is a little harder to figure out, but it is quite similar to the previous: $g(n) = 100n$ works. Fill in the details.

   (d) Here the function is $g(n) = n^2$. Fill in the details.

2. Note that, according to the definition, each of the sets $S$ in problem 1 is an example of a countable set.

   (a) We need an example of a bijection from $\mathbb{N}$ to $\mathbb{N}$. The identity function $f(n) = n$ is one example. The function

   $$f(n) = \begin{cases} n + 1, & n \text{ odd} \\ n - 1, & n \text{ even} \end{cases}$$

   from Midterm Test 1 is another example. It's easier to prove that the identity function is a bijection, so I suggest you stick with that example.

   (b) Let $S$ be the subset. If $S$ is finite we are done, so we assume $S$ is infinite. We would like to define a bijection $g : \mathbb{N} \to S$ as in question 1. The function $g$ would be something like "the $n^{\text{th}}$ element of $S$", but we really need something like mathematical induction to get this to work properly. We inductively define the sets $S_i$ in the following manner: $S_0 = \{\}$, the empty set, and $S_{n+1} = (S - S_n) \cup$ the least element of $S - S_n$. For example, if $S$ is the primes, then $S_0 = \{\}$, $S_1 = \{2\}$, $S_2 = \{2, 3\}$, $S_3 = \{2, 3, 5\}$, and so on. Each of those sets (other than $S_0$) is bounded above and non-empty (why?), and so each of those sets has a greatest element. Letting the function $g(n) =$ the greatest element of set $S_n$ gives us the function we need. (Please supply the details, i.e., that $g$ is a bijection.)

   (c) The intersection of countable sets $S$ and $T$ is a subset $V$ of $S$, so by a variation on part (b), $V$ is countable. Fill in the details.

(d) We have two countable sets $S$ and $T$, so there are bijections $f_1 : S \to \mathbb{N}$ and $f_2 : T \to \mathbb{N}$. We define a new function $f : S \cup T \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2f_1(n) - 1, & n \in S \\ 2f_2(n), & n \in T \end{cases}$$

The function $f$ counts the elements of $S \cup T$, zig-zagging from $S$ to $T$. (One from you, one from me, one from you, one from me, etc.) Drawing a picture might help. Now show that this function is a bijection.

Actually, the above solution is not quite right. How can you fix it up if $S$ and $T$ share some elements in common, i.e., if they have a non-empty intersection? For examples, $S$ could be the set of prime numbers and $T$ the set of numbers divisible by 3.

3. (a) To construct an example, take $S = \mathbb{N}$, the simplest example of an infinite set that we have. The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n + 1$ is an injection but not a surjection. (Why? Supply the details.) There are many other examples.

(b) Again take $S = \mathbb{N}$. Define $g : \mathbb{N} \to \mathbb{N}$ by

$$g(n) = \begin{cases} n - 1, & n > 1 \\ 1 & n = 1 \end{cases}$$

Then $g$ is a surjection but not an injection. (Details!)

Note that $g$ is a right inverse for $f$, which is not important, just interesting.

(c) This is essentially the pigeonhole principle. If $f$ is not a surjection, let the set $T$ be the image of all the elements of $S$ under the mapping $f$. If $f$ is not a surjection, then $T$ is smaller than $S$. Then we have an injection $f : S \to T$, impossible by the pigeonhole principle. So our assumption that $f$ is not a surjection is wrong.

(d) Again, this is essentially the pigeonhole principle. If $g$ is not an injection, then there are two elements $n_1$ and $n_2$ in $S$ such that $g(n_1) = g(n_2)$. We take the element $n_2$ out of $S$ to form the set $T$. Then $g : T \to S$ is still a surjection. It has a right inverse $h : S \to T$ which is an injection (why? draw a picture), but the size of $T$ is less than the size of $S$, so the pigeonhole principle applies to show that $h$ is not an injection. The assumption that $g$ is not an injection leads to a contradiction, so $g$ must be an injection.

4. (a) See p. 52 of the textbook.

(b) Suppose the set of upper primes is finite; write the set as $\{p_1, p_2, \ldots, p_k\}$. Form the number $N = 4p_1p_2 \cdots p_k - 1$. The number $N$ is of the form $4n + 3$, so $N$ must have a prime factor which is an upper prime (it can't have 2 as a prime factor because $N$ isn't even, and if it had all lower prime factors it would be of the form $4n + 1$, which it isn't). That prime factor can't be one in the list already (why?), so our assumption that the set of upper primes is finite must be false.

Let's try the procedure to see how it keeps generating new upper primes. Let's start with the given list of upper primes, 3, 7, and 11. Suppose someone claimed that was all the upper primes. I say, no, we can generate another one this way: multiply $4 \times 3 \times 7 \times 11$ and then subtract 1 to get 923. The prime factors of 923 are 13 and 71. One of them must be of the form $4n + 3$; in fact, 71 is of that form, so our assumption that $\{3, 7, 11\}$ is a list of all the upper primes was incorrect. If we did the procedure over again with $\{3, 7, 11, 71\}$ we would get a prime factorization of $17^2 \times 227$, which gives us another new prime factor of the form $4n + 3$, namely 227. Guess what happens if we do it again with the list $\{3, 7, 11, 71, 227\}$?

(c) The argument is similar to that in (b). Suppose the set of all primes of the form $6n + 5$ is finite. Multiply them together, then multiply by 6, then subtract 1 to get $N = 6p_1p_2 \cdots p_k - 1$ which is again of the form $6n + 5$. The number $N$ cannot have a factor of the form $6n$ or $6n + 2$ or $6n + 4$ because those numbers are all even, and $N$ is odd. Furthermore $N$ cannot have a factor of the form $6n+3$, because then $N$ would be divisible by 3, but it's not. If all the factors of $N$ are of the form $6n+1$, then $N$ would be of the form $6n+1$, but it's not, so $N$ must have a prime factor of the form $6n+5$. That factor can't be on our list, so our assumption that we had a list of all the prime factors of the form $6n+5$ must have been wrong.

Try it a few times; you can get started with the list $\{5\}$ and see how to generate new primes of the form $6n+5$ from that list, then repeat the procedure.

(d) The proof for numbers of the form $4n+1$ breaks down because $N = 4p_1p_2\cdots p_k+1$ doesn't necessarily have any factors of the form $4n+1$; it may have just an even number of factors of the form $4n+3$. For example, if our list is $\{5\}$, $N = 4\times 5+1 = 21 = 3\times 7$ which has two factors of the form $4n+3$ but none of the form $4n+1$. In fact, all attempts to prove that there is an infinite number of primes of the form $4n+1$ failed until the $19^{\text{th}}$ century, when Dirichlet proved the result using sophisticated methods from calculus.

5. (a) Tell each guest currently in the hotel in room $n$ to move to room $f(n) = n+1$.

(b) Tell each guest currently in the hotel in room $n$ to move to room $f(n) = n+100$.

(c) Tell each guest currently in the hotel in room $n$ to move to room $f(n) = 2n$, then tell each guest in the other hotel in room $n$ to move to room $2n-1$ in the new hotel. (Or to room $2n+1$ if we don't do subtraction and if we don't mind having one empty room.)

(d) Following the system I devised in the lectures, label each occupant of room $n$ in hotel $m$, and think of them as "lattice points" (i.e., points with integer coordinates) in the first quadrant of the plane. There are a series of lines of slope $-1$ passing through the lattice points; the lines have the equations $m+n=k$ where $k$ is a natural number. For example, the guest in room 7 of hotel 12 is on the line $m+n=19$. If we have already accommodated all guests on lower-numbered lines, we would have to have made room for guests on the triangle of lattice points below $m+n=19$; the number of such guests is the triangular number $17\times 18/2 = 153$. So we can safely put the guest in room 7 of hotel 12 into room $153+7=160$ of the new hotel. in general, we put the guest in room $n$ of hotel $m$ into room

$$f(m,n) = \frac{(m+n-2)(m+n-1)}{2} + m$$

of the new hotel. (Try it for a few values, and then prove that that function is an injection, which means no two guests get the same hotel room, and a surjection, which means I'm using every room in the new hotel so my manager is happy.) There are certainly many other possible ways to answer this question.

(e) First we put every guest of room $n$ of every hotel $m$ in a given city $c$ into one hotel using the procedure in part (d). Then we apply part (d) again to the infinite number of guests in an infinite number of cities to put them into a single hotel. For an exact formula, the function $f(c, f(m,n))$ works very nicely. You can do a little algebra, if you like, to write down the formula in explicit form for less mathematically talented bellhops.