M1F Foundations of Analysis Problem Sheet 5

1. Fix $f\colon S \to T$ and suppose there exists $g\colon T \to S$ such that $g \circ f = \mathrm{id}_S$. Is f

   (a) injective ?

   (b) surjective ?

   (c) bijective ?

   Give a proof or counterexample for each.
   (You are strongly advised to try to draw a diagram to answer questions like this.)

   (a) Suppose that $f(x) = f(y)$. Then $g \circ f(x) = g \circ f(y)$. But $g \circ f = \mathrm{id}_S$, so this says that $x = y$. Therefore f is injective.

   (b) and (c) No, eg. $\{1\} \xrightarrow{f} \{1, 2\} \xrightarrow{g} \{1\}$.

2. Suppose that $S \neq \emptyset$ and that $f\colon S \to T$ is injective. Prove that there exists $g\colon T \to S$ such that $g \circ f = \mathrm{id}_S$.

   $S \neq \emptyset$, so $\exists s_0 \in S$.

   Given any $t \in T$, it is either in the image of f or it is not.

   If it is not then set $g(t) = s_0$.

   If it is, then $\exists s_t \in S$ such that $f(s_t) = t$. Also, s_t is unique because f is injective. Define $g(t) = s_t$.

   Fix any $s \in S$, and let $t = f(s)$. Then $s_t = s$ by the definition of s_t, since $f(s) = t$. Therefore $g(f(s)) = g(t) = s_t = s$ for all $s \in S$. Therefore $g \circ f = \mathrm{id}_S$.

3. $*$ Suppose that S, T are finite sets of m, n elements respectively. How many injections are there $S \to T$? How many bijections ?

   If $S \to T$ is an injection then $m = |S| \leq |T| = n$. So if $m > n$ then there are no injections.

   If $m \leq n$ then we want injections $\{s_1, \ldots s_m\} \to \{t_1, \ldots t_n\}$. These are maps f such that the $f(s_i)$ are all distinct.

   For $f(s_1)$ we have n choices. For $f(s_2)$ we can choose any of the t_i except $f(s_1)$, so we have $(n-1)$ choices. Etc. For $f(s_m)$ we have $n - m + 1$ choices left.

   So we have $n.(n-1)\ldots(n-m+1)$ choices, i.e. there are $\frac{n!}{(n-m)!}$ injections.

   For a bijection we must have $n = m$, and then any injection is automatically surjective and so a bijection. So the number of bijections equals the number of injections, equals $n!$.

   (Notice this is the same as the number of ways of reordering n points. Why ?!)

4. You intercept the brief message "2" encoded by RSA with the woeful public key $(N, e) = (143, 11)$.

   Crack the code and so decode the message.

   Crack the code by factorising $N = pq$ as $143 = 11.13$.

   Then $(p-1)(q-1) = 10.12 = 120$ and $e = 11$ is coprime to 120.

   By Euclid (or inspection), $11.11 - 120 = 1$, so $d = 11$.

   Therefore the message is decoded as $y^d = 2^{11}$ mod 143.

   But, working mod 143, $2^7 = 128 = -15$ so $2^{11} = -15.16 = -240 = 46$ so the message was "46".

5. (a) Calculate $(p+1)^2$ mod $p(p+2)$.

   (b) You notice that your internet bank's RSA public key is of the form $(N, e) = (p(p+2), p)$ for some pair of *prime* numbers $p, p+2$. The millionaire Martin Liebeck uses the same bank to save the proceeds from his book, and you intercept the transmission of his PIN number, which has been encoded as "$p+1$". Crack the code to find his PIN number.

   $(p+1)^2 = p^2 + 2p + 1 = p(p+2) + 1 \equiv 1$ mod $p(p+2)$.

p and q are $p, p+2$ (1). So $(p-1)(q-1) = p^2 - 1$ so we can put $d = p$ (and $\lambda = 1$) to solve $de - \lambda(p-1)(q-1) = 1$.

Therefore his PIN number is $(p+1)^d = (p+1)^p$ mod $p(p+2)$.

But $(p+1)^2 \equiv 1$ and $p = 2n+1$ is odd (because both p and $p+2$ are prime), so $(p+1)^p \equiv (p+1)^{2n}(p+1) \equiv 1.(p+1) \equiv p+1$ mod $p(p+2)$. So his PIN number is also $p+1$.

6. How many numbers between 1 and 30,000,000 are divisible by neither 5 nor 6 ?

Those divisible by five are $F = \{5, 10, \ldots, 30000000\}$. So $|F| = 6,000,000$.

Those divisible by six are $S = \{6, 12, \ldots, 30000000\}$. So $|S| = 5,000,000$.

Those divisible by both are those divisible by 30, cos 5 and 6 are coprime. I.e. $F \cap S = \{30, 60, \ldots, 30000000\}$. So $|F \cap S| = 1,000,000$.

Those divisible by one or the other are $F \cup S$, of size $|F| + |S| - |F \cap S| = 6,000,000 + 5,000,000 - 1,000,000 = 10,000,000$. The remaining $30,000,000 - 10,000,000 = 20,000,000$ numbers are divisible by neither.

7. Each week Prof. McCoy eats 10 packs of McCoy's Real McCoy crisps, coyly.

A varied diet is important, so she wonders how many weeks she can eat a different distribution[1] of packs of her 4 favourite flavours "Normal", "Poisson", "Gamma and pineapple" and "Wallenius' noncentral univariate hypergeometric distribution".

Then she has an idea: she will decide what to eat each week by marking off 3 different numbers from the list $\{1, 2, \ldots, 13\}$, leaving 10 numbers. The numbers to the left of the 1st mark will tell her how many packs of Normal to eat, the numbers between the 1st and 2nd mark will represent packs of Poisson, then Gamma between the 2nd and 3rd marks, and finally the numbers after the 3rd mark will denote packets of Wallenius[2].

How many weeks can she carry on with different distributions before she has to start eating her least favourite flavour "Student's tea" ?

† How many ways can you write $n \in \mathbb{N}$ as a sum $n_1 + \ldots + n_k$ of k nonnegative integers, where order *is*[3] important ?

Distributions are the same things as choices of 3 distinct numbers from $\{1, 2, \ldots, 13\}$ by the method described. So the number of possible distributions is $\binom{13}{3}$. After $\binom{13}{3}$ weeks she will have to start eating Student's t.

Similarly splitting $n = n_1 + n_2 + \ldots n_k$ into k nonnegative integers is the same as marking off $k-1$ distinct numbers from $\{1, 2, \ldots, n+k-1\}$, leaving n unmarked numbers. The numbers before the 1st marked number give n_1, those between 1st and 2nd give n_2, etc. Thus there are $\binom{n+k-1}{k-1}$ ways.

[1] For instance last week, she ate 5 packs of Normal, 0 Poisson, 2 Gammas and 3 Wallenius, so the distribution was 5,0,2,3.

[2] So last week the marked numbers were 6,7 and 10.

[3] So, for instance, $n = a + b$ and $n = b + a$ count as *different* ways of expressing n as a sum of two numbers, unless $a = b$.