Some informal notes on countabiliy.

Definition 0.1 Two sets A, B are said to be *equinumerous* if there exists a bijection $f : A \to B$. We denote this by $A \approx B$ We also say that under these circumstances A and B have the same *cardinality*, and write $|A| = |B|$.

So two sets are equinumerous if their elements can be 'paired off.' This seems reasonable, but it has the consequence that a set can be equinumerous to a proper subset of itself. For example, the succesor function $n \mapsto n + 1$ gives a bijection from $\mathbb{N}$ to $\mathbb{N} \setminus \{0\}$. (Exercise: find bijections between $\mathbb{N}$ and $2\mathbb{N}$, and between $\mathbb{N}$ and $\mathbb{Z}$.) Note however that we do have the following properties:

Lemma 0.2 *For sets A, B, C we have the following:*
(i) if $A \approx B$ then $B \approx A$;
(ii) $A \approx A$;
(iii) if $A \approx B$ and $B \approx C$ then $A \approx C$.

Proof: (i) The inverse of a bijection is a bijection.
(ii) Consider the identity function $A \to A$.
(iii) The composition of two bijections is a bijection. $\square$

Note that a set A is equinumerous with a subset of a set B iff there is an injective function $f : A \to B$.

Definition 0.3 A set is *countably infinite* (or *denumerable*) if it is equinumerous with $\mathbb{N}$. A set is *countable* if it is finite or countably infinite. A set which is not countable is called *uncountable*.

Uncountable sets exist. Thus there are 'different sizes of infinity.' This was first observed by Georg Cantor. Here is an example of an uncountable set: the argument used to show the uncountablilty is called Cantor's diagonal argument.

Example 0.4 Let S be the set of all sequences of zeros and 1's. So formally S is the set of all functions $s : \mathbb{N} \to \{0, 1\}$. Then S is uncountable. For suppose there were a bijection $g : \mathbb{N} \to S$. Then consider the sequence $s \in S$ given by

$$s(n) = \begin{cases} 0 & \text{if } g(n)(n) = 1 \\ 1 & \text{if } g(n)(n) = 0 \end{cases}$$

Note that $g(n)(n)$ is the n-th term in the sequence $g(n)$. So the sequence s differs from the n-th sequence $g(n)$ in the n-th place. In particular, for all $n \in \mathbb{N}$ we have $s \neq g(n)$. Thus g cannot be onto: contradiction.

We can use this to observe that the set of real numbers $\mathbb{R}$ is uncountable. There is an obvious bijection between S and a subset of $\mathbb{R}$. Send the sequence s to the real number with decimal expansion

$$s(0) \cdot s(1)s(2)s(3)\dots.$$

Now applying the fact below that a subset of a countable set has to be countable, we see that $\mathbb{R}$ is uncountable.

Theorem 0.5 *(i) Every subset of $\mathbb{N}$ is countable.*
(ii) Every subset of a countable set is countable.

Proof: Clearly (ii) follows from (i) as a subset of a countable set is equinumerous with a subset of $\mathbb{N}$. To prove (i), suppose S is an infinite subset of $\mathbb{N}$. Then there exists a function $f : \mathbb{N} \to S$ given by:

$f(0)$ is the least element of S;

$f(n+1)$ is the least element of $S \setminus \{f(0), \dots, f(n)\}$.

[We're using things which will only be formally justified later.]

Note also that by definition, f is injective. It is onto, because if $s \in S$ then $f(n) = s$ for some $n \leq s$. $\Box$

Corollary 0.6 *A set S is countable if and only if there exists an injective function $g : S \to \mathbb{N}$.* $\Box$

Theorem 0.7 *(i) Let A, B be countable sets. Then $A \times B$ is countable.*

(ii) Let B be a countable set and let S be the set of all finite sequences of elements of B. Then S is countable.

Proof: Recall that a natural number $n > 1$ is a prime number if the only natural numbers dividing it are 1 and itself. Recall also that any natural number $m > 1$ can be written in a unique way as a product of powers of prime numbers (this is the Fundamental Theorem of Arithmetic: see your first-year notes, or look it up in a basic text).

(i) Let $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$ be bijections (actually, injectivity is enough). Define a function $h : A \times B \to \mathbb{N}$ by

$$h(a, b) = 2^{f(a)} 3^{g(b)}.$$

Then by FTA h is injective and so $A \times B$ is countable.

(ii) This is similar. Let $p_0, p_1, p_2, p_3, \dots$ be the sequence of primes (in some order, usually taken to be increasing). Let $f : B \to \mathbb{N}$ be an injection. Define a function $h : S \to \mathbb{N}$ as follows. Let h send the empty sequnce to 0. For $s = s(0)s(1)\dots s(n) \in S$ let

$$h(s) = p_0^{f(s(0))+1} p_1^{f(s(1))+1} \dots p_n^{f(s(n))+1}.$$

Then FTA implies that h is injective and so S is countable. $\Box$

Theorem 0.8 *(i) A non-empty set S is countable if and only if there exists a surjection $h : \mathbb{N} \to S$.*

(ii) A non-empty set S is countable if and only if there exists a surjection $g : T \to S$ for some countable set T.

(iii) If A is a countable set of countable sets then

$$\bigcup A = \{y : (\exists x \in A)(y \in x)\}$$

is countable.

Proof: (i) One direction is clear. So suppose there exists a surjection $h : \mathbb{N} \to S$. For $s \in S$ let $g(s)$ be the smallest element of $h^{-1}(s) = \{n \in \mathbb{N} : h(n) = s\}$ (this set is non-empty as h is surjective). Then $g = \{(s, g(s)) : s \in S\}$ is an injective function from S to $\mathbb{N}$. So S is countable by Corollary 0.6.

(ii) This follows trivially from (i).

(iii) Let $F : \mathbb{N} \to A$ be a surjection. So for each $n \in \mathbb{N}$, $F(n)$ is a countable set. So there exists a surjection $g_n : \mathbb{N} \to F(n)$. Then $h : \mathbb{N} \times \mathbb{N} \to \bigcup A$ given by

$$h(n, m) = g_n(m)$$

is a surjection. So the result follows from (ii) and countability of $\mathbb{N} \times \mathbb{N}$ (Theorem 0.7). $\square$

(The proof of (iii) used implicitly the Axiom of Choice - we will come back to this.)

EXERCISE: Show that the following sets are countable (you may use any of the above results):

(a) The set of finite subsets of $\mathbb{N}$.

(b) The set of subsets of $\mathbb{N}$ with finite complement.

(c) The set of rational numbers.

(d) The set of real numbers which are roots of non-zero polynomial equations with rational coefficients.

(e) The set of those real numbers which can be described by sentences in English.