MATHEMATICS 300 — FALL 2002

Introduction to Mathematical Reasoning — H. J. Sussmann

December 9, 2002

This note has two parts.

First, I give you the proof of the binomial theorem, as it was done in class.

Second, I discuss cardinality and finite sets. The book does not tell you what a "finite set" is. Since in the book there is no precise defintion of finite set, the proofs of the basic properties of finite sets (for example, that if A, B are disjoint finite sets then $|A \cup B| = |A| + |B|$) are not proved, or proved with a lot of cheating.

In this handout, I do everything rigorously.

---

1. THE BINOMIAL THEOREM

THEOREM. Let a, b be real numbers. Let n be a natural number. Then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\,.$$

PROOF. We let S be the set of all natural numbers n for which the formula is not true. We want to prove that S is empty.

Assume S is not empty. Then, by the Well Ordering Principle, S has a smallest member. Call it q. Then q is a natural number,

$$(a+b)^q \neq \sum_{k=0}^{q} \binom{q}{k} a^k b^{q-k}\,,$$

and q is the smallest natural number for which this happens.

For $n = 0$, the formula says that $1 = 1$ (because $(a+b)^0 = 1$, since $x^0 = 1$ for every x, and $\sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1$). So q cannot be 0, because the formula is true for $n = 0$, so $0 \notin S$.

Therefore $q > 0$, so $q-1$ is a natural number, and $q - 1 \notin S$. This means that

$$(a+b)^{q-1} = \sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-1-k}\,.$$

Then

$$\begin{aligned}
(a+b)^q &= (a+b)(a+b)^{q-1} \\
&= (a+b) \sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-1-k} \\
&= a\left(\sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-1-k}\right) + b\left(\sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-1-k}\right) \\
&= \left(\sum_{k=0}^{q-1} \binom{q-1}{k} a^{k+1} b^{q-1-k}\right) + \left(\sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-k}\right).
\end{aligned}$$

We now observe that

$$\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k}=\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}\,.$$

(REASON: in the sum $\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k}$, relabel the indices by using "j" for $k+1$. Then, as k ranges from 0 to $q-1$, $k+1$ ranges from 1 to q, so j ranges from 1 to q. Also, $\binom{q-1}{k}a^{k+1}b^{q-1-k}$ becomes $\binom{q-1}{j-1}a^j b^{q-j}$, because $k=j-1$. So

$$\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k}=\sum_{j=1}^{q}\binom{q-1}{j-1}a^j b^{q-j}\,.$$

But the variable of summation is a dummy variable, so we can call it anything we like, and in particular we can substitute k for j, obtaining:

$$\sum_{j=1}^{q}\binom{q-1}{j-1}a^j b^{q-j}=\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}\,.$$

Therefore

$$\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k}=\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}\,,$$

as stated.)

It follows that

$$(a+b)^q \;=\; \left(\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}\right)+\left(\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-k}\right).$$

But

$$\begin{aligned}\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k} &= \binom{q-1}{q-1}a^q b^{q-q}+\sum_{k=1}^{q-1}\binom{q-1}{k-1}a^k b^{q-k}\\ &= a^q+\sum_{k=1}^{q-1}\binom{q-1}{k-1}a^k b^{q-k}\,,\end{aligned}$$

and

$$\begin{aligned}\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-k} &= \binom{q-1}{0}a^0 b^{q-0}+\sum_{k=1}^{q-1}\binom{q-1}{k}a^k b^{q-k}\\ &= b^q+\sum_{k=1}^{q-1}\binom{q-1}{k}a^k b^{q-k}\,.\end{aligned}$$

Therefore

$$(a+b)^q \;=\; a^q+\left(\sum_{k=1}^{q-1}\binom{q-1}{k-1}a^k b^{q-k}\right)+b^q+\left(\sum_{k=1}^{q-1}\binom{q-1}{k}a^k b^{q-k}\right).$$

Now,

$$\begin{aligned}\left(\sum_{k=1}^{q-1}\binom{q-1}{k-1}a^k b^{q-k}\right)+\left(\sum_{k=1}^{q-1}\binom{q-1}{k}a^k b^{q-k}\right) &= \sum_{k=1}^{q-1}\left(\binom{q-1}{k-1}+\binom{q-1}{k}\right)a^k b^{q-k}\\ &= \sum_{k=1}^{q-1}\binom{q}{k}a^k b^{q-k}\,,\end{aligned}$$

using the identity

$$\binom{q-1}{k-1} + \binom{q-1}{k} = \binom{q}{k}\,.$$

It follows that

$$(a+b)^q \;=\; a^q + b^q + \Big(\sum_{k=1}^{q-1}\binom{q}{k}a^k b^{q-k}\Big)\,.$$

On the other hand,

$$\begin{aligned}\sum_{k=0}^{q}\binom{q}{k}a^k b^{q-k} &= \binom{q}{0}a^0 b^{q-0} + \Big(\sum_{k=1}^{q-1}\binom{q}{k}a^k b^{q-k}\Big) + \binom{q}{q}a^q b^{q-q} \\ &= b^q + \Big(\sum_{k=1}^{q-1}\binom{q}{k}a^k b^{q-k}\Big) + a^q\,.\end{aligned}$$

Then

$$(a+b)^q \;=\; \sum_{k=0}^{q}\binom{q}{k}a^k b^{q-k}\,.$$

But we established before that

$$(a+b)^q \;\neq\; \sum_{k=0}^{q}\binom{q}{k}a^k b^{q-k}\,.$$

So we have reached a contradiction, and our proof is complete.

---

2. CARDINALITY

What do we mean by the "size" (also called "cardinality") of a set? And what does it mean for two sets to have "the same cardinality." (From now on, we use "cardinality" rather than "size," because "cardinality" is the word most commonly used in mathematics. For finite sets, we will go on using "size.")

If a set A is finite, we can count its members, and find out how many members it has. Then we can tell that two finite sets A, B "have the same cardinality" if they have the same number of members. This approach, however has the drawback that it only amakes sense for finite sets. So, for example, if we look at sets such as $\mathbb{N}$, or $\mathbb{Z}$, or $2^{\mathbb{N}}$, or $2^{\mathbb{Z}}$, or $\mathbb{N}\times\mathbb{N}$, we cannot use this method to decide if, for example, $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality, or $\mathbb{N}$ and $2^{\mathbb{N}}$ have the same cardinality.

There is something else we can do, which is much better. We can often tell that two sets have the same "size" without having to count their members, by finding a way to **match** them.

EXAMPLE 1. Let A be the set of all married men. Let B be the set of all married women. Suppose we are dealing with a monogamous society, in which every married man is married to one and only one woman,and every married woman is married to one and only one man. Then **we can tell, without counting, that A and B have the same size.** How can we do that? We just observe that there is a way to match the members of A with those of B, that is, to construct a *bijection* $f : A \mapsto B$. The definition of B is very simple: if $x \in A$ (that is, if x is a married man) we let $f(x)$ be x's wife. In symbols:

$$f(x) = x\text{'s wife, whenever } x \in A\,.$$

This function is one-to-one, because if x and x' are two different married man, then their wives $f(x)$ and $f(x')$ are different (because no woman can be married to two man). Furthermore, f is onto, because for every member y of B there exists $x \in A$ such that $f(x) = y$ (that is, every married woman is the wife of some man). So f is a bijection from A to B. ♢

EXAMPLE 2. Suppose a large lecture room is full of people, and you see that every person is seated, and every chair is occupied. Then you can conclude, **without counting**, that there are exactly as many chairs as there are people. In other words, if X is the set of all people who are in the room, and Y is the set of all chairs, then you can tell that X and Y have the same number of members. Again, the reason is that you can construct a bijection $b : X \mapsto Y$ by letting $b(x)$ be, for each person $x \in X$, the chair where x is sitting. In symbols:

$$h(x) = \text{the chair where } x \text{ is sittting, whenever } x \in X\,.$$

This function is one-to-one, because if x and x' are two different people, then their chairs $hx)$ and $h(x')$ are different (because two different people cannot occupy the same chair). Furthermore, g is onto, because for every member y of Y there exists $x \in X$ such that $h(x) = y$ (that is, every chair is occupied). So g is a bijection from X to Y. $\diamondsuit$

Drawing inspiration from these two examples, we give the following

DEFINITION 1. Let A, B be sets. We say that B **has the same cardinality as** A if there exists a bijection $f : A \mapsto B$.

IMPORTANT REMARK. This definition make sense for **infinite sets** as well as for finite ones.

EXAMPLE 3. Let $\mathbb{E}$ be the set of all even integers, that is,

$$\mathbb{E} = \{n \in \mathbb{Z} : \exists m \in \mathbb{Z}, n = 2.m\}\,.$$

Then $\mathbb{E}$ has the same cardinality as $\mathbb{Z}$.

PROOF. Define $f(n) = 2.n$ for $n \in \mathbb{Z}$. Then $f : \mathbb{Z} \mapsto \mathbb{E}$. Furthermore, f is one-to-one, because if $n \in \mathbb{Z}$, $n' \in \mathbb{Z}$, and $f(n) = f(n')$, then $2.n = 2.n'$, so $n = n'$. In addition, f is onto $\mathbb{E}$, because if $n \in \mathbb{E}$ then n is an even integer, so there exists $m \in \mathbb{Z}$ such that $2.m = n$, i.e., such that $f(m) = n$. So f is a bijection, and then Definition 1 implies that $\mathbb{E}$ has the same cardinality as $\mathbb{Z}$. $\diamondsuit$

EXAMPLE 4. The set $\mathbb{N}$ has the same cardinality as $\mathbb{N} \times \mathbb{N}$.

PROOF. We have to exhibit a bijection $f : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$. If $u \in \mathbb{N} \times \mathbb{N}$, then u is an ordered pair (m, n) of integers. Define

$$f(u) = 2^m(2n + 1) - 1\,.$$

Then

1. f is indeed a function from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, because if $u = (m, n) \in \mathbb{N} \times \mathbb{N}$, then $2^m \in \mathbb{N}$, $2n+1 \in \mathbb{N}$, $2^m \geq 1$, and $2n+1 \geq 1$, so $2^m(2n+1) \in \mathbb{N}$ and $2^m(2n+1) \geq 1$, from which it follows that $f(u) = 2^m(2n + 1) - 1 \in \mathbb{N}$.
2. f is one-to-one, because if $u = (m, n) \in \mathbb{N} \times \mathbb{N}$ and $u' = (m', n') \in \mathbb{N} \times \mathbb{N}$ are such that $f(u) = f(u')$, then $2^m(2n + 1) - 1 = 2^{m'}(2n' + 1) - 1$, so $2^m(2n + 1) = 2^{m'}(2n' + 1)$; then m is the largest of all exponents μ such that 2^μ divides $f(u)$, and m' is the largest of all exponents μ such that 2^μ divides $f(u')$; since $f(u) = f(u')$, the exponents m, m' are equal; since $m = m'$, the equality $2^m(2n + 1) = 2^{m'}(2n' + 1)$ implies $2n + 1 = 2n' + 1$, so $n = n'$.
3. f is onto, because if $q \in \mathbb{N}$ then $q + 1$ is a positive integer, so we can write $q + 1$ as $2^m.r$ for some $m \in \mathbb{N}$ and some odd $r \in \mathbb{N}$; then $r = 2n + 1$ for some integer n, and n has to be ≥ 0 because $r \geq 0$. Then $q = 2^m.(2n + 1) - 1$, so we have found $u = (m, n) \in \mathbb{N} \times \mathbb{N}$ such that $f(u) = q$. $\diamondsuit$

EXAMPLE 5. The set $\mathbb{N}$ has the same cardinality as $\mathbb{Z}$.

PROOF. We have to exhibit a bijection $f : \mathbb{Z} \mapsto \mathbb{N}$. If $n \in \mathbb{Z}$, then we define $f(n) = 2.n$ if $n \geq 0$, and $f(n) = -2n-1$ if $n < 0$. (Notice what this does: $f(0) = 0$, $f(-1) = 1$, $f(1) = 2$, $f(-2) = 3$, $f(2) = 4$, $f(-3) = 5$, $f(3) = 6$, ... In other words, we are listing the integers as follows

$$0, -1, 1, -2, 2, -3, 3, -4, 4, -5, 5 \ldots$$

and then we let $f(n) = k - 1$ if n is k-th in the list; for example, $f(3) = 6$ because 3 is seventh in the list.)

Then it is easy to prove that f is a bijection. (You should do it.) $\diamondsuit$

THEOREM 1. *Let A be a set. Then A has the same cardinality as A.*

PROOF. We have to exhibit a bijection $f : A \mapsto A$. We define f by letting $f(x) = x$ for $x \in A$. Then it is easy to prove that f is a bijection, and we are done. $\diamondsuit$

THEOREM 2. *Let A, B be sets, and suppose that B has the same cardinality as A. Then A has the same cardinality as B.*

PROOF. Since B has the same cardinality as A, we can pick a bijection $f : A \mapsto B$. Then $f^{-1} : B \mapsto A$, and f^{-1} is a bijection from B to A. $\diamondsuit$

THEOREM 3. *Let A, B, C be sets, and suppose that B has the same cardinality as A and C has the same cardinality as B. Then C has the same cardinality as A.*

PROOF. Since B has the same cardinality as A, we can pick a bijection $f : A \mapsto B$. Since C has the same cardinality as B, we can pick a bijection $g : B \mapsto C$. Then $g \circ f : A \mapsto C$, and $g \circ f$ is a bijection from A to C. $\diamondsuit$

THEOREM 4. *Let A, B, C, D be sets, and suppose that C has the same cardinality as A and D has the same cardinality as B. Then $A \times B$ has the same cardinality as $C \times D$.*

PROOF. Since C has the same cardinality as A, we can pick a bijection $f : A \mapsto C$. Since D has the same cardinality as B, we can pick a bijection $g : B \mapsto D$. Define a function $h : A \times B \mapsto C \times D$ by letting

$$h(a, b) = (f(a), g(b)) \text{ if } a \in A,\, b \in B\,.$$

Then h is a bijection from $A \times B$ to $C \times D$. (This is easy to prove. You should do it.) $\diamondsuit$

EXAMPLE 6. The set $\mathbb{Z}$ has the same cardinality as $\mathbb{Z} \times \mathbb{Z}$.

PROOF. We know from Example 5 that $\mathbb{N}$ has the same cardinality as $\mathbb{Z}$. Then $\mathbb{N} \times \mathbb{N}$ has the same cardinality as $\mathbb{Z} \times \mathbb{Z}$ by Theorem 4. Also, $\mathbb{N}$ has the same cardinality as $\mathbb{N} \times \mathbb{N}$ (Example 4). So $\mathbb{N}$ has the same cardinality as $\mathbb{Z} \times \mathbb{Z}$ by Theorem 3. Since $\mathbb{N}$ has the same cardinality as $\mathbb{Z}$, it follows from Theorem 2 that $\mathbb{Z}$ has the same cardinality as $\mathbb{N}$. Since $\mathbb{N}$ has the same cardinality as $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}$ has the same cardinality as $\mathbb{N}$, Theorem 3 implies that $\mathbb{Z}$ has the same cardinality as $\mathbb{Z} \times \mathbb{Z}$. $\diamondsuit$

CANTOR'S THEOREM . *Let A be a set. Then there does not exist an onto function $f : A \mapsto 2^A$.*

PROOF. Suppose an onto function $f : A \mapsto 2^A$ exists. Pick one and call it φ. Let

$$S = \{a \in A : a \notin \varphi(a)\}\,.$$

Then $S \subseteq A$, so $S \in 2^A$. Since φ is onto, we can pick $s \in A$ such that $\varphi(s) = S$.

We claim that $s \in S \longleftrightarrow s \notin S$. To prove this, assume first that $s \in S$. Since $S = \varphi(s)$, s satisfies $s \in \varphi(s)$. So the condition "$a \notin \varphi(a)$" that characterizes membership in S is not true for $a = s$. So $s \notin S$. Next, assume that $s \notin S$. Since $S = \varphi(s)$, s satisfies $s \notin \varphi(s)$. So the condition "$a \notin \varphi(a)$" that characterizes membership in S is true for $a = s$. So $s \in S$.

So we have proved that $s \in S \longleftrightarrow s \notin S$. But this is a contradiction. Hence f cannot exist. $\diamondsuit$

COROLLARY OF CANTOR'S THEOREM . *Let A be a set. Then 2^A does not have the same cardinality as A.*

PROOF. We know that there does not exist an onto function $f : A \mapsto 2^A$. So there does not exist a bijection $f : A \mapsto 2^A$, because s come to get serious and define what a "finite set" is.

First,

FINITE SETS

We have been talking about "finite sets," but we never gave a precise definition of what it means for a set to be "finite." The book does not give you a definition either.

Now the time has come to get serious and give a real definition of "finite set."

First, let us introduce some notation:

If n is a natural number, then $I_n = \{m : m \in \mathbb{N} \wedge 1 \leq m \leq n\}$.

For example:

$$I_0 = \emptyset\,,\ \ I_3 = \{1, 2, 3\}\,,\ \ I_{12} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}\,.$$

We are now ready for the definitions.

DEFINITION 2. A set A is *finite* if there exists a natural number n such that A has the same cardinality as I_n.

DEFINITION 3. A set A is *infinite* if it is not finite.

It is then reasonable to guess that the definition of "size of a finite set" will be as follows:

DEFINITION 4. Let A be a finite set and let $n \in \mathbb{N}$. Then we say that A *is a set of size* n (or a *size* n *set*) if there exists a bijection $f : I_n \mapsto A$.

Notice that in stating this definition there is something we did **not** say. We did not say that, if A is a set of size n, then the number n is *the size of* A. And we did **not** say that we agree to write $|A| = n$ if A is of size n. So, for example, if A is a set of size 15, we are not giving ourselves permission to write $|A| = 15$ and to say that 15 is the size of A.

Eventually, we will allow these things, but we will only do so when we are ready. At this point, we are **not** ready. The reason is as follows: **we do not yet know that, if it exists, then the number n such that A is of size n is unique.** In other words, it could happen, for example, that a set A can be matched both with I_{235} and with I_{346}, in which case we would have to say that "A is of size 235," and also that "A is of size 346." In that case, we would not know which number—235 or 346 is $|A|$.

You don't believe that this can happen, right? I don't believe it either, but in mathematics saying that "I don't believe something" is not a proof. So we have to give a real proof that, if A is a set, and n, m are natural numbers such that A is of size n and A is of size m then $n = m$. Until we prove this, we cannot introduce the "size" notation $|A|$.

LEMMA 1. *Let A be a set, and let $a, b \in A$. Then there exists a bijection $f : A \mapsto A$ such that $f(a) = b$.*

PROOF. Either $a = b$ or $a \neq b$. We consider these two cases separately.

If $a = b$, we define f by letting $f(x) = x$ for every $x \in A$.

If $a \neq b$, we define f by letting $f(x) = x$ for every $x \in A$ such that $x \neq a$ and $x \neq b$, and we let $f(a) = b$, $f(b) = a$.

In both cases it is easy to prove that f is a bijection from A to A. (You should do it.) Clearly, $f(a) = b$. ♢

THEOREM 5. *Let m, n be natural numbers and suppose $f : I_n \mapsto I_m$ is a one-to-one function. Then $n \leq m$.*

PROOF. We use induction with respect to n. If $n = 0$ then the conclusion that $m \geq n$ follows, because $m \in \mathbb{N}$, so $m \geq 0$.

Now suppose we have proved that if $\mu \in \mathbb{N}$ and $g : I_{n-1} \mapsto I_\mu$ is one-to-one then $n-1 \leq \mu$. Let $m \in \mathbb{N}$, $f : I_n \mapsto I_m$ be such that f is one-to-one. Using Lemma 1, pick a bijection $h : I_m \mapsto I_m$ such that $h(f(n)) = m$. Let $F = h \circ f$. Then $F : I_n \mapsto I_m$, and F is one-to-one (because f and h are one-to-one). Define $G : I_{n-1} \mapsto I_{m-1}$ by letting $G(x) = F(x)$ for $x \in I_{n-1}$. (The fact that G maps I_{n-1} to I_{m-1} needs proof. Here it is. If $x \in I_{n-1}$ then $G(x) = F(x)$ and $F(x) \in I_m$, so $G(x) \in I_m$, that is, $G(x) \in \mathbb{N}$ and $1 \leq G(x) \leq n$. Furthermore, $F(x) \neq m$—because $x \neq n$, since $x \in I_{n-1}$, so $F(x) \neq F(n) = m$, since F is one-to-one. Therefore $G(x) \in I_{m-1}$.) Then G is one-to-one. (Proof: if $x, x' \in I_{n-1}$ and $x \neq x'$, then $F(x) \neq F(x')$, because F is one-to-one. Therefore $G(x) \neq G(x')$, because $G(x) = F(x)$ and $G(x') = F(x')$.)

By the inductive hypothesis, with $\mu = m - 1$, we can conclude that $n - 1 \leq m - 1$. But then $n \leq m$, and we are done. ♢

THEOREM 6. *Let m, n be natural numbers and suppose $f : I_n \mapsto I_m$ is an onto function. Then $n \geq m$.*

PROOF. We define $g : I_m \mapsto I_n$ as follows. If $y \in I_m$, then there exists $x \in I_n$ such that $f(x) = y$, because f is onto. Then the set $\{x : x \in I_n \wedge f(x) = y\}$ is nonempty, so by the Well Ordering principle it has a smallest member. We choose $g(y)$ to be this smallest member. Then $g(y) \in I_n$ and $f(g(y)) = y$ for every $y \in I_m$. It follows that g is one-to-one. (Proof: if $y, y' \in I_m$ and $y \neq y'$, then $g(y) \neq g(y')$ because if $g(y) = g(y')$ then $f(g(y)) = f(g(y'))$, which is impossible since $f(g(y)) = y$, $f(g(y')) = y'$, and $y \neq y'$.) Therefore Theorem 5 implies that $m \leq n$, and we are done. ♢

THEOREM. *(THE PIGEON-HOLE PRINCIPLE.) Let A, B be finite sets and let $n \in \mathbb{N}$, $m \in \mathbb{N}$, be such that A is of size n and B is of size m. Let $f : A \mapsto B$ be a function. Then*

1. *If f is one-to-one then $n \leq m$.*
2. *If f is onto then $n \geq m$.*

PROOF OF THE PIGEON-HOLE PRINCIPLE. Since A is of size n, we can pick a bijection $g : I_n \mapsto A$. Since B is of size m, we can pick a bijection $h : I_m \mapsto B$. Then h^{-1} is a bijection from B to I_m. Define $F = h^{-1} \circ f \circ g$. Then $f : I_n \mapsto I_m$.

If f is one-to-one, then F is one-to-one, because $F = h^{-1} \circ f \circ g$ and g, h^{-1} are bijections. Therefore Theorem 5 implies that $n \leq m$.

If f is onto, then F is onto, because $F = h^{-1} \circ f \circ g$ and g, h^{-1} are bijections. Therefore Theorem 6 implies that $n \geq m$. ♢

THEOREM. *(IMPORTANT COROLLARY OF THE PIGEON-HOLE PRINCIPLE.) Let A, B be finite sets and let $n \in \mathbb{N}$, $m \in \mathbb{N}$, be such that A is of size n and B is of size m. Let $f : A \mapsto B$ be a bijection. Then $m = n$.*

PROOF OF THE IMPORTANT COROLLARY. Since f is one-to-one, $n \leq m$. Since f is onto, $n \geq m$. Therefore $n = m$. $\diamondsuit$

It follows from the corollary that, if A is a finite set then there is one **and only one** $n \in \mathbb{N}$ such that A is of size n. So now, finally, we have the right to define *the* size $|A|$ of a finite set A.

DEFINITION 5. Let A be a finite set. *The size* of A is the unique natural number n such that A is of size n. $\diamondsuit$

NOTATION. We use $|A|$ to denote the size of A. $\diamondsuit$

THEOREM 7. *Let A, B be finite sets such that $A \cap B = \emptyset$. Then $A \cup B$ is a finite set and*

$$|A \cup B| = |A| \cup |B| .$$

PROOF. Let $n = |A|$, $m = |B|$. Pick bijections $f : I_n \mapsto A$, $g : I_m \mapsto B$. Define $F : I_{n+m} \mapsto A \cup B$ by letting $F(x) = f(x)$ if $x \in I_n$, $F(x) = g(x - n)$ if $x \in I_{n+m}$ but $x \notin I_n$. Then F is a bijection. **(This is the key point. Make sure you know how to prove it. The fact that $A \cap B = \emptyset$ should play a crucial role in your proof.)** Therefore $|A \cup B| = n + m$. $\diamondsuit$

THEOREM 8. *Let $n \in \mathbb{N}$. Then the set I_n is finite and $|I_n| = n$.*
PROOF. $I_0 = \emptyset$, and $\emptyset$ is a bijection from I_0 to $\emptyset$. $\diamondsuit$

PROOF. Define a bijection $f : I_n \mapsto I_n$ by letting $f(x) = x$ for $x \in I_n$. $\diamondsuit$

COROLLARY OF THEOREM 8. *The empty set $\emptyset$ is finite and $|\emptyset| = 0$.*
PROOF. $\emptyset = I_0$. $\diamondsuit$

THEOREM 9. *For every a, the set $\{a\}$ is finite and $|\{a\}| = 1$.*
PROOF. Define a bijection $f : I_1 \mapsto \{a\}$ by letting $f(1) = a$. $\diamondsuit$

THEOREM 10. *Let A, B be sets such that A is finite and $B \subseteq A$. Then B is finite.*

PROOF. We first prove that if $n \in \mathbb{N}$ then every subset of I_n is finite. We use induction with respect to n. If $n = 0$ then $I_n = \emptyset$. Therefore, if $S \subseteq I_n$, then $S = \emptyset$, so S is finite by the corollary of Theorem 8. Now suppose we have proved that every subset of I_{n-1} is finite. Let $S \subseteq I_n$. Then either $n \in S$ or $n \notin S$. If $n \notin S$ then $S \subseteq I_{n-1}$, so S is finite by the inductive hypothesis. If $n \in S$, then $S = S' \cup \{n\}$, where $S' = \{k \in S : k < n\}$. The set S' is finite by the inductive hypothesis. The set $\{n\}$ is finite by Theorem 9. The sets S', n obviously satisfy $S \cap \{n\} = \emptyset$. Therefore $S' \cup \{n\}$ is finite by Theorem 7.

Now let us go back to our general situation. Suppose A is a finite set and $B \subseteq A$. Let $n = |A|$. Pick a bijection $f : I_n \mapsto A$. Let $S = \{x \in I_n : f(x) \in B\}$. Then $S \subseteq I_n$, so S is finite. Define a function $g : S \mapsto B$ by letting $g(x) = f(x)$ for $x \in S$. Then g is a bijection. (*Make sure you know how to prove this!*) Let $m = |S|$. Pick a bijection $h : I_m \mapsto S$. Let $G : I_m \mapsto B$ be defined by $G = g \circ h$. Then G is a bijection. Therefore B is finite. $\diamondsuit$

THEOREM 11. *Let A, B be finite sets. . Then $A \cup B$ is a finite set and*

$$|A \cup B| + |A \cap B| = |A| \cup |B|\,.$$

PROOF. By Theorem 10, the sets $A \cap B$, $A - B$, $B - A$ are finite, because they are subsets of A or of B. Let $n = |A|$, $m = |B|$, $\nu = |A - B|$, $\mu = |B - A|$, $\theta = |A \cap B|$. Then $A = (A - B) \cup (A \cap B)$, and $(A - B) \cap (A \cap B) = \emptyset$. So Theorem 7 tells us that $n = \nu + \theta$. Also, $B = (B - A) \cup (A \cap B)$, and $(B - A) \cap (A \cap B) = \emptyset$. So Theorem 7 tells us that $m = \mu + \theta$. Furthermore, $A \cup B = (A - B) \cup B$ and $(A - B) \cap B = \emptyset$, so Theorem 7 tells us that $A \cup B$ is finite and $|A \cup B| = \nu + m$. Therefore $|A \cup B| + |A \cap B| = \nu + m + \theta - n + m$. ♢

THEOREM 12. *Let A, B be sets such that A is finite and $B \subseteq A$. Then B is finite and $|B| \leq |A|$.*

PROOF. We already know that B is finite. Furthermore, $A = (A - B) \cup B$, and $(A - B) \cap B = \emptyset$, and the set $A - B$ is finite by Theorem 10. Therefore $|A| = |A - B| + |B|$ by Theorem 7. Since $|A - B| \geq 0$, the conclusion that $|B| \leq |A|$ follows. ♢

THEOREM 13. *The set $\mathbb{N}$ is infinite.*

PROOF. Suppose $\mathbb{N}$ was finite. Let $n = |\mathbb{N}|$. The set I_{n+1} is a subset of $\mathbb{N}$, so Theorem 13 implies that $|I_{n+1}| \leq n$. But $|I_{n+1}| = n + 1$. So $n + 1 \leq n$, which is not true. Therefore $\mathbb{N}$ is not finite. ♢

THEOREM 14. *Let A, B be sets such that A is infinite, and suppose $f : A \subseteq B$ is a one-to-one function. Then B is infinite.*

PROOF. Suppose B was finite. Let $S = \operatorname{im} f$. Then $S \subseteq B$, so S is finite. Let $n = |S|$. Pick a bijection $g : I_n \mapsto S$. Let Let $h = g^{-1} \circ f$. Then $h : A \mapsto I_n$ and h is a bijection. Therefore A is finite, which contradicts our hypothesis. ♢

THEOREM 15. *The sets $\mathbb{N}$, $2^{\mathbb{N}}$ are infinite and do not have the same cardinality.*

PROOF. We already now that $\mathbb{N}$ is infinite. The function $f : \mathbb{N} \mapsto 2^{\mathbb{N}}$ given by $f(x) = \{x\}$ is one-to-one. Therefore Theorem 14 implies that $2^{\mathbb{N}}$ is infinite. Finally, Cantor's Theorem implies that $\mathbb{N}$ and $2^{\mathbb{N}}$ do not have the same cardinality. ♢