Proof Methods

Tristan Shin

26 Oct 2016

This lecture and paper serve to assist with the understanding and formulation of basic proof methods. Topics that will be discussed include the methods of contradiction, mathematical induction, and the pigeonhole principle.

1 Contradiction

The method of contradiction is exactly what the name describes: we will attempt to prove a result by showing that the opposite cannot happen. In logical terms: if p is the assertion we are trying to prove, we will show that p is true by showing that $\neg p$ is false.

Example 1: Prove that there exists infinitely many prime numbers.

Proof: **Assume not**, then there are finitely many prime numbers. Note that there exists at least one, because 2 is one. Let all of them be $p_1, p_2, \ldots, p_k$ for some finite k. Consider $n = p_1 p_2 \cdots p_k + 1$. This is clearly larger than 1, so it has a prime factor. But none of the p_i divide it, as otherwise p_i divides 1, so we have arrived at a **contradiction**. Thus, our initial assumption that there are finitely many primes is wrong and there are infinitely many prime numbers. ■

This next example is a bit more complicated.

Example 2: Prove that $\sqrt{2}$ is irrational.

Proof: **Assume not**, then there exist relatively prime positive integers m and n such that $\sqrt{2} = \frac{m}{n}$ (consider a rational number reduced in simplest form). Then $2 = \frac{m^2}{n^2}$, or $m^2 = 2n^2$.

Next, I claim that 2 divides m. **Assume not**, then 2 does not divide m^2 either. But 2 divides $2n^2 = m^2$, **contradiction**. Thus, 2 divides m.

Now, let $m = 2x$ for a positive integer x. Then we get $4x^2 = 2n^2$, or $2x^2 = n^2$. We can repeat the previous argument on n and x in place of m and n to deduce that 2 divides n. But then 2 divides m and n, **contradiction**. Thus, our initial assumption that there are relatively prime positive integers m and n such that $\sqrt{2} = \frac{m}{n}$ is wrong and $\sqrt{2}$ is irrational. ■

This previous example gave an insight to a related proof method which is more advanced — the method of infinite descent. This method essentially assumes a set of positive integers has a minimum. We then deduce that there is a smaller element, which is a contradiction as we will have an infinitely decreasing sequence of positive integers, which cannot exist. This itself lends to a sub-method called Vieta Jumping in which integer roots of quadratics are examined to deduce a contradiction in some statement.

2 Induction

Induction works like falling dominoes: knocking domino 1 results in knocking domino 2, which in turn results in knocking domino 3, and so on such that if domino n is knocked down, domino $n + 1$ is as

well. If we have an infinite number of dominoes lined up in a straight ray with a small enough space in between the dominoes, knocking down the first domino will, by this process, knock down every domino in the line. This is the basic idea behind induction: knowing the truth of a problem statement about n for a "moment" $n = k$ might help us to prove the statement for $n = k + 1$. To perform induction, one needs a **base case** and an **inductive step**. The base case is the first domino: we must manually prove this case in order to set off our chain reaction. The inductive hypothesis is the assumption that domino n has been knocked off, which will set off the inductive step: the action that happens as a result of domino n falling, namely domino $n + 1$ falling.

There is another form of induction called strong induction. In this version, instead of assuming the statement for a single moment $n = k$, we assume it for a range of moments (so say we can assume that the statement is true for all $n = 1, 2, \ldots, k$). This is often helpful when just one moment is too weak to fully prove the next moment of the statement.

Example 1: Prove that $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

Proof: We will do this by induction. **The base case** of $n = 1$ is just $1 = \frac{1 \cdot 2}{2}$, which is true. **Now, assume that this works for some** $n = k$ **with** $k \geq 1$. Then $1+2+3+\ldots+k = \frac{k(k+1)}{2}$. Adding $k+1$ to each side, we get that $1 + 2 + 3 + \ldots + k + (k + 1) = \frac{k(k+1)}{2} + (k + 1) = (k + 1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2}$. **This is the statement for** $n = k + 1$, so by induction, we are done. ■

Next, we will prove Fermat's Little Theorem.

Example 2: Let n be a nonnegative integer and p a prime number. Prove that $n^p - n$ is divisible by p.

Proof: We will do this by induction. **The base case** of $n = 0$ is just p dividing 0. **Now, assume that this works for some** $n = k$ **with** $k \geq 0$. Then $k^p - k$ is divisible by p. Consider $(k + 1)^p - (k + 1)$. We can expand the power by the Binomial Theorem: $(k + 1)^p = \sum_{i=0}^{p} \binom{p}{i} k^i$. For $i = 1, 2, \ldots, p - 1$, note that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is divisible by p because the numerator is but the denominator is not ($i, p - i < p$ and p is a prime). Thus, we can ignore them when considering divisibility by p. It suffices to prove that $k^p + 1 - k - 1 = k^p - k$ is divisible by p. But this is the **inductive hypothesis**, so we have proven the case for $n = k + 1$. By induction, we are done. ■

This next example is a hard problem from a contest.

Example 3: Suppose that a sequence $a_1, a_2, \ldots$ of positive real numbers satisfies

$$a_{k+1} \geq \frac{ka_k}{a_k^2 + (k - 1)}$$

for every positive integer k. Prove that $a_1 + a_2 + \ldots + a_n \geq n$ for every $n \geq 2$.

Proof: First, we prove this for $n = 2$. The problem statement gives that $a_2 \geq \frac{1}{a_1}$. Thus,

$$a_1 + a_2 \geq a_1 + \frac{1}{a_1} \geq 2$$

by AM-GM, so this is true for $n = 2$.

Now, we prove the problem statement by induction on n. **The base case** of $n = 2$ was proven above. Assume that the statement holds for some $n = m \geq 2$.

If $a_{m+1} < 1$, note that the given inequality rearranges to $a_k \geq \frac{k}{a_{k+1}} - \frac{k-1}{a_k}$. Summing this up for

$k = 1, 2, \ldots, m$ gives that

$$a_1 + a_2 + \ldots + a_m \geq \sum_{k=1}^{m} \frac{k}{a_{k+1}} - \sum_{k=0}^{m-1} \frac{k}{a_{k+1}} = \frac{m}{a_{m+1}}.$$

Now, note that $(1 - a_{m+1})(m - a_{m+1}) > 0$, so $\frac{m}{a_{m+1}} + a_{m+1} > m + 1$. Thus,

$$a_1 + a_2 + \ldots + a_m + a_{m+1} > m + 1,$$

and the claim is true for $n = m + 1$.

Otherwise, $a_{m+1} \geq 1$. **Invoke the inductive hypothesis** and we get that

$$a_1 + a_2 + \ldots + a_m + a_{m+1} \geq m + a_{m+1} \geq m + 1,$$

and the claim is true for $n = m + 1$.

Either way, the claim is true for $n = m + 1$, so by induction, we are done. ■

3 Pigeonhole Principle

In the Pigeonhole Principle, we have a pigeons and b pigeonholes which we must put the pigeons into. Given that $a > b$, it is intuitive that there must be a pigeonhole with multiple pigeons in it (prove it by contradiction). A slightly stronger version is that there exists a pigeonhole with at least $\lceil \frac{a}{b} \rceil$ pigeons in it. This has many applications to several problems.

Example 1: Prove that among any group of people with at least two people, there exist two people who are friends with the same number of people (friendship is mutual).

Proof: Assume that there are n people. The number of people whom a certain person is friends with is an integer between 0 and $n - 1$, inclusive. However, there cannot be a person who is friends with $n - 1$ people and a person who is friends with 0 people because the one who has $n - 1$ friends is friend with everyone else in this group, including the one with 0 friends, which is a clear contradiction. Thus, the number of friends a person can have is either an integer between 0 and $n - 2$ or 1 and $n - 1$, inclusive. Either way, there are at maximum $n - 1$ possible values of the number of friends that a certain person has. But there are n people, so by the pigeonhole principle, there must exist a value that is used twice. Thus, there are two people who are friends with the same number of people. ■

This result can also be phrased in terms of graphs: In a graph, there exist two vertices with the same degree.

Example 2: Show that the Fibonacci sequence is eventually periodic modulo any positive integer n.

Consider the pairs of residues (a, b) with $0 \leq a, b \leq n - 1$. There are n^2 of them. We can label each positive integer c with a corresponding pair of residues (a_c, b_c) such that $a_c \equiv F_c \pmod{n}$ and $b_c \equiv F_{c+1} \pmod{n}$. By the pigeonhole principle, there exist two positive integers $c < d$ with the same pair of residues (i.e. $a_c = a_d$ and $b_c = b_d$). Let $t = d - c$. Notice then that $F_c \equiv F_d = F_{c+t} \pmod{n}$ and $F_{c+1} \equiv F_{d+1} = F_{c+1+t} \pmod{n}$. Assume that $F_k \equiv F_{k+t} \pmod{n}$ for a positive integers k and $k + 1$ with $k \geq c$. This is true for $k = c$. Then $F_{k+2} = F_{k+1} + F_k \equiv F_{k+1+t} + F_{k+t} = F_{k+2+t} \pmod{n}$. Thus, by induction, $F_k \equiv F_{k+t} \pmod{n}$ for all positive integers k at least c. This demonstrates the claim. ■

Note that in this solution, we used the pigeonhole principle with an infinite number of pigeons.

4 Problems

Here are some practice problems involving the three techniques discussed. The first three should be fairly accessible upon digesting the information from the lecture, while the last three are harder challenge problems.

1. Prove that there does not exist a smallest positive real number.

2. Let $f(x)$ be a function satisfying $f(x+y) = f(x) + f(y)$ for all x and y in its domain. Show that $f\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} f(x_i)$ for all integers $n \geq 2$.

3. Given any 7 real numbers, prove that there exist two of them, say x and y, such that
$$0 \leq \frac{x-y}{1+xy} \leq \frac{1}{\sqrt{3}}.$$

4. In Lineland there are $n \geq 1$ towns, arranged along a road running from left to right. Each town has a *left bulldozer* (put to the left of the town and facing left) and a *right bulldozer* (put to the right of the town and facing right). The sizes of the $2n$ bulldozers are distinct. Every time when a left and right bulldozer confront each other, the larger bulldozer pushes the smaller one off the road. On the other hand, bulldozers are quite unprotected at their rears; so, if a bulldozer reaches the rear-end of another one, the first one pushes the second one off the road, regardless of their sizes.

   Let A and B be two towns, with B to the right of A. We say that town A can *sweep* town B *away* if the right bulldozer of A can move over to B pushing off all bulldozers it meets. Similarly town B can sweep town A away if the left bulldozer of B can move over to A pushing off all bulldozers of all towns on its way.

   Prove that there is exactly one town that cannot be swept away by any other one.

5. Find, with proof, the smallest possible area of a convex pentagon whose vertices all have integer coordinates.

6. Suppose that n and k are positive integers such that
$$1 = \underbrace{\varphi(\varphi(\cdots\varphi(}_{k \text{ times}} n)\cdots)).$$

   Prove that $n \leq 3^k$.

5 Hints

1. Prove this by contradiction. Assume there is a smallest positive real number x, and find another positive real number smaller than it that is related to x.

2. Whenever we are given a specific case as our problem statement, it is always tempting to try induction. In this case, we would want to induct on n.

3. Remember the tangent difference formula: $\tan(a-b) = \frac{\tan a - \tan b}{1+\tan a \tan b}$? Apply the pigeonhole principle on some differences.

4. Apply strong induction. This problem requires no more thinking past the realization that you can reduce it to the problem for a smaller value of n and apply strong induction.

5. Guess the answer, then try to prove that the next smallest possible area doesn't work. To do this, apply the pigeonhole principle on the parity pair of the coordinates (i.e. reduce the coordinates modulo 2 and see which ones are possible).

6. Consider a function $w(n)$ that counts the number of 2's that are shed off as φ is repeatedly applied. Note that $w(n) \leq k$. Then apply strong induction to finish the problem off.

6 Solutions

1. Assume that there exists a smallest positive real number and let it be x. Now, define $y = \frac{x}{2}$. Note that because x is positive, $x > \frac{x}{2}$ and $0 < \frac{x}{2}$. But then y is a positive real number smaller than x, contradiction.

2. We prove this by induction. The base case of $n = 2$ is just the problem statement. Assume that this statement holds for some $n = k$, where $k \geq 2$. Then

$$f\left(\sum_{i=1}^{k+1} x_i\right) = f\left(\sum_{i=1}^{k} x_i + x_{k+1}\right) = f\left(\sum_{i=1}^{k} x_i\right) + f\left(x_{k+1}\right) = \sum_{i=1}^{k} f\left(x_i\right) + f\left(x_{k+1}\right) = \sum_{i=1}^{k+1} f\left(x_i\right),$$

   and the claim is proven for $n = k + 1$. Thus, by induction, we are done.

3. Let the seven numbers be $x_1, x_2, \ldots, x_7$. Furthermore, let $y_i = \arctan x_i$. Then the expression we are looking at turns into

$$\frac{\tan y_i - \tan y_j}{1 + \tan y_i \tan y_j} = \tan\left(y_i - y_j\right).$$

   The inequality we are concerned with then becomes

$$0 \leq y_i - y_j \leq \frac{\pi}{6}.$$

   Now, look at the intervals $\left[\frac{\pi k}{6}, \frac{\pi(k+1)}{6}\right)$ for $k = 0, 1, \ldots, 5$. There are six of them, and the seven y_i must go into these six intervals. By the pigeonhole principle, there exist two of them that are in the same interval. Let them be y_i and y_j with $y_i \geq y_j$. Then the largest difference that can be obtained is $\frac{\pi}{6}$ (at the endpoints of this interval), so

$$0 \leq y_i - y_j \leq \frac{\pi}{6}.$$

   Thus, we have shown that there exist such y_i and y_j satisfying the inequality, so there are x and y among the 7 numbers such that

$$0 \leq \frac{x - y}{1 + xy} \leq \frac{1}{\sqrt{3}}.$$

4. We prove this by strong induction. The base case of $n = 1$ is trivial, as a single town cannot be swept away by any nonexistent towns. Assume that this statement holds for all $n = 1, 2, \ldots, k$, where $k \geq 1$. Then consider the set-up for $n = k + 1$. Suppose that the towns in order from left to right are $T_1, T_2, \ldots, T_{k+1}$. Note that the left bulldozer of T_1 and the right bulldozer of T_{k+1} are useless, so ignore them. Among the remaining $2k$ bulldozers, there is one of them that is the biggest. WLOG let it be the left bulldozer of town T_m with $m > 1$. It is clear that this bulldozer can sweep away any town to the left of T_m, so any town to the left of T_m cannot sweep away T_i for $i = m, m + 1, \ldots, k + 1$. Now, among towns $T_m, T_{m+1}, \ldots, T_{k+1}$, there exists one, say T_p which cannot be swept away by any other town T_i for $i = m, m + 1, \ldots, k + 1$ (there are $k - m + 2 \leq k$ towns we are considering, so apply the inductive hypothesis). But T_p cannot be swept away by any town to the left of T_m either, so T_p cannot be swept away by any town and we are done by induction.

5. The answer is $\frac{5}{2}$. This is achievable by a pentagon with vertices $(0, 0)$, $(1, 0)$, $(2, 1)$, $(1, 2)$, and $(0, 1)$. Let I be the number of integer points in the interior of the pentagon and B be the number of integer points on the boundary of the pentagon. I claim that there exists an integer point in the interior of the pentagon. Consider the five points as (x_i, y_i) for $i = 1, 2, 3, 4, 5$. Reduce the coordinates modulo 2 to get the coordinates as (x_i', y_i'), where $x_i', y_i' \in \{0, 1\}$. There are a total of 4 distinct pairs (x_i', y_i'), but there are 5 i. Thus, by the pigeonhole principle, there exist two indices i and j such that $(x_i', y_i') = \left(x_j', y_j'\right)$. But then $\left(\frac{x_i + x_j}{2}, \frac{y_i + y_j}{2}\right)$ is an integer point and is on the line segment from (x_i, y_i) to (x_j, y_j). As the pentagon is convex, this point must be in the interior of the pentagon, as it cannot be on the pentagon due to the fact that either $x_i \neq x_j$ or $y_i \neq y_j$. Thus,

there is at least one integer point in the interior of the pentagon, so $I \geq 1$. Now, because there are 5 points, it is clear that $B \geq 5$. But then by Pick's Theorem, $K = I + \frac{B}{2} - 1 \geq 1 + \frac{5}{2} - 1 = \boxed{\frac{5}{2}}$.

6. Let $w : \mathbb{N} \to \mathbb{N}$ satisfy the following: $w(ab) = w(a) + w(b)$ for all $a, b \in \mathbb{N}$, $w(2) = 1$, and $w(p) = w(p-1)$ for all primes p. Note that $w(n)$ counts the number of 2's that are shed off as φ is repeatedly applied. Note then that $w(n) \leq k$. Thus, it suffices to prove that $w(p) \geq \log_3 p$ for every prime p. In fact, I claim that $w(n) \geq \log_3 n$ for every positive integer n. This is true for $n = 1$ and 2. Assume that this statement holds for all $n = 1, 2, \ldots, p-1$, where p is an odd prime. Then

$$w(p) = w(p-1) = w(2) + w\left(\frac{p-1}{2}\right) \geq 1 + \log_3\left(\frac{p-1}{2}\right) = \log_3\left(\frac{3}{2}p - \frac{3}{2}\right) \geq \log_3 p,$$

so the claim is true for $n = p$. Now, let q be the smallest prime greater than p. Consider an integer n such that $p + 1 \leq n \leq q - 1$. Note that n is composite. In particular, it has prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with $p_1, p_2, \ldots, p_k \leq p$. But then

$$w(n) = \sum_{i=1}^{k} e_i w(p_i) \geq \sum_{i=1}^{k} e_i \log_3 p_i = \log_3 p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \log_3 n$$

by the inductive hypothesis and our result. But then we have that the statement is true for all $n = 1, 2, \ldots, q-1$, and we can proceed with our induction. Thus, by induction, we have that

$$\log_3 n \leq w(n) \leq k,$$

so $n \leq 3^k$.