Math 153: Sample Proofs

Rich Schwartz

December 23, 2013

Here is a result which is pretty obvious.

Lemma 0.1 *If A and B and C are all sets, then*

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

Proof: There are two halves to this result. First we must show that

$$A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$$

and then we must show that

$$(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C.$$

For the first equation, choose an element $x \in (A \cap B) \cup C$. Then either $x \in A \cap B$ or else $x \in C$ (or both). In the first case $x \in A$ and $x \in B$. Therefore $x \in A \cup C$ and $x \in B \cup C$. Therefore $x \in (A \cup C) \cap (B \cup C)$. In the second case, $x \in C$. But then $x \in A \cup C$ and $x \in B \cup C$. Therefore $x \in (A \cup C) \cap (B \cup C)$. In either case we see that $x \in (A \cup C) \cap (B \cup C)$. This shows that any element of our first set belongs to our second set, and therefore establishes the first equation we had wanted to prove.

Now suppose that $x \in (A \cup C) \cap (B \cup C)$. Then $x \in A \cup C$ and $x \in B \cup C$. There are two cases. If $x \in C$ then certainly $x \in (A \cap B) \cup C$. On the other hand, if $x \notin C$ then $x \in A$ and $x \in B$. But then $x \in A \cap B$. Therefore $x \in (A \cap B) \cup C$. This shows that any element of our second set belongs to our first set and therefore establishes the second equation we had wanted to prove. ♠

A positive integer $P > 1$ is prime if it is impossible to write $P = ab$ where a and b are both positive integers greater than 1. Another way to say this is that a prime number is one whose only divisors are 1 and itself. The following proof really uses the *well-ordering* principle, which says that any nonempty set of positive integers has a smallest element. This principle is really quite close to the principle of *induction*. Anyway, here is the next sample proof:

Lemma 0.2 *Any positive integer (greater than* 1*) can be factored into a product of positive primes.*

Proof: We will argue by contradiction. If not all positive integers greater than 1 can be factored into primes then there is some smallest positive integer $N > 1$ that cannot be factored into primes. (We just used the well-ordering principle.) If N is prime then we have an immediate contradiction. So, we must have $N = ab$ where both a and b are positive integers greater than 1. But then both a and b are smaller than N. Since a and b are smaller than the smallest "unfactorable integer", a and b can both be factored into primes. That is

$$a = p_1 \times ... \times p_r; \qquad b = q_1 \times ... \times q_s,$$

where all the ps and qs are understood to be primes. But then

$$N = ab = p_1 \times ... \times p_r \times q_1 \times ... \times q_s$$

and we have successfully factored N into primes. This contradicts the existence of N. The contradiction forces us to acknowledge that all positive integers can be factored into primes. ♠

Our next proof is the classic proof, due to Euclid, that there are infinitely many prime numbers. Our proof uses the previous result about factoring in an essential way.

Theorem 0.3 *There are infinitely many primes.*

Proof: Suppose, for the sake of contradiction, that there are only finitely many prime numbers. Then let $P_1, ..., P_n$ be the complete list of prime numbers. Consider the new number

$$N = P_1 \times ... \times P_n + 1.$$

Notice that N is larger than each of $P_1, ..., P_n$. So, N cannot be prime. On the other hand, we can factor N into primes, like any other positive integer greater than 1. So, there must be some prime on our list that divides N. (any one of the prime factors will do the job.) Let's say that we have ordered our primes so that P_1 divides N. This means that we can write

$$N = aP_1$$

for some other integer a. However, from the very definition of N, we have

$$N = bP_1 + 1,$$

where $b = P_2 \times ... \times P_n$ is some integer. We now know that

$$bP_1 + 1 = aP_1.$$

But then

$$1 = P_1(a - b).$$

Since P_1 is an integer bigger than 1, and $a - b$ is an integer, it is impossible for $P_1(a - b)$ to equal 1. This contradiction shows that there is no largest prime. ♠

The next proof is similar in spirit to the last one, and just uses standard facts about arithmetic that most people would take as axioms. Recall that integers a and b are *relatively prime* if there only common positive divisor is 1. That is, if $k > 0$ divides both a and b then $k = 1$. For instance 3 and 25 are relatively prime.

Lemma 0.4 *Suppose that a and b are positive integers that are relatively prime. Then there are integers m and n such that $am + bn = 1$.*

Proof: Let D be the set of all numbers of the form $am + bn$, where m and n range over all possible integers. Note that all elements of D are integers, some of which are positive.. Let δ be the smallest positive integer in D. We would like to show that $\delta = 1$. Since a and b are relatively prime, it suffices to show that δ divides both a and b. We will show that δ divides a. The proof that δ divides b is the same.

We can write

$$\delta = am + bn$$

for some particular choice of m and n. Our argument works like this. We're going to assume that δ does not divide a and then we will produce another pair of integers m' and n' such that the combination $am' + bn'$ is positive and less than δ. This will contradict the choice of δ as the minimum positive element of D.

Here is the argument: When we divide a by δ we get some nonzero remainder, since a doesn't divide δ. This means that there is some integer k such that

$$a = k\delta + r; \qquad ,$$

where $r > 0$ and $r < \delta$. Here r is the remainder. We can write

$$r = a - k\delta = a - k(am + bn) = am' + bn'$$

for some other integers m' and n'. But then r is positive, belongs to D, and is less than δ. This is a contradiction. The only way out of the contradiction is that δ divides a.

Once again, the argument that δ divides b is the same. Since δ divides both a and b we must have $\delta = 1$. But then we have solved the equation $am + bn = 1$. ♠

Here is a proof of the Pythagorean theorem which relies somewhat on modern notions of area.

Theorem 0.5 *Let T be a right triangle. Let a and b be the lengths of the short sides of T and let c be the length of the long side. Then $a^2 + b^2 = c^2$.*

Proof: Let $\mathcal{X}$ denote the set of all triangles which are similar to T. So, the members of $\mathcal{X}$ are rotated and/or dilated and/or shrunk versions of T. There is some particular member T_0 of $\mathcal{X}$ whose long side has length 1. Let λ be the area of T_0. If r is the long side of some other triangle T in $\mathcal{X}$ then the area of T is λr^2. The idea is that we dilate T by r units to create T, and this increases the area by a factor of r^2. We want to emphasize that this principle works for any choice of r. We're going to apply it using 3 different choices of r.

Here's the main construction: Draw the line segment from the right angle of T to the long side, so that this segment makes a right angle with the long side, as shown in Figure 1.

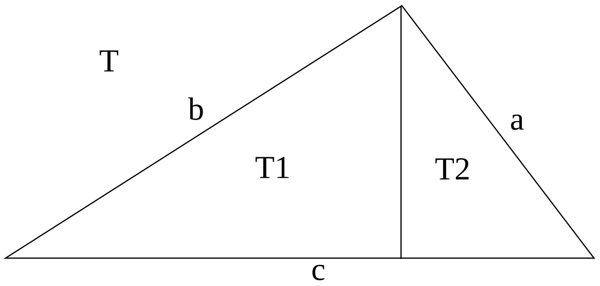

Figure 1

One can see easily, using the fact that T is a right triangle, that the angles of T_1 are the same as the angles of T. Hence T_1 belongs to $\mathcal{X}$. The long side of T_1 is b and hence the area of T_1 is λb^2. Our argument using the dummy variable r above works for any choice of r, as we already mentioned.

The same argument shows that the area of T_2 is λa^2. But T is just the union of T_1 and T_2, and there is no overlap between these two smaller triangles. Therefore

$$\lambda c^2 = \text{area}(T) = \text{area}(T_1) + \text{area}(T_2) = \lambda b^2 + \lambda a^2.$$

Cancelling λ gives $a^2 + b^2 = c^2$. ♠

Here is a classic result from graph theory.

Lemma 0.6 *Let K_6 denote the complete graph on 6 vertices: one has an edge connecting every pair of vertices. Suppose that the edges have been colored red and blue. Then there either exists a red triangle or a blue triangle.*

Proof: Let v_0 be one of the vertices. Of the 5 edges emanating out of v_0, at least three of them have the same color. Without loss of generality, we can assume that there are at least 3 red edges, and that these edges connect v_0 to v_j for $j = 1, 2, 3$. If the edge connecting v_1 to v_2 is red, then $v_0v_1v_2$ is a red triangle. So, if we want to avoid a red triangle, then the edge v_1v_2 is blue. The same argument goes for the edge v_2v_3 and the edge v_3v_1. So, if there is no red triangle, then $v_1v_2v_3$ is a blue triangle. ♠

Here is a generalization of this result, known as the Ramsey theorem for graphs.

Theorem 0.7 *Let n be any integer. Let $N = 2^{2n}$. Let K_N be the complete graph on N vertices. If every edge of K_N colored either red or blue, then there is either a red copy of K_n in the graph or a blue copy of K_n in the graph.*

Proof: Let $\Gamma_0 = K_N$, the whole graph. Choose any vertex v_0. At least half of the edges emanating from v_0 have the same color. Call this color C_0. We are going to choose $2n - 2$ vertices inductively. Assume that vertices $v_0, ..., v_k$ have been chosen, with associated colors $C_0, .., C_k$, and an associated sequence $\Gamma_k \subset ... \subset \Gamma_0$ such that Γ_k is a complete graph on $2^{2n}/2^k$ vertices for each k. Let v_{k+1} be any vertex of Γ_k. At least $2^{2n}/2^{k+1}$ of the edges connecting v_{k+1} to other vertices of Γ_k have the same color C_{k+1}. Let $\Gamma_{k+1} \subset \Gamma_k$ be a complete graph of size $2^{2n}/2^{k+1}$ such that every edge connecting v_{k+1} to a vertex of Γ_{k+1} has color C_{k+1}. We make this construction for each $k = 0, ..., 2n-4$, getting vertices $v_0, ..., v_{2n-3}$ such that the edge connecting v_i to v_j has color C_i as long as $j > i$. From amongst the first $2n - 3$ of these vertices, there are at least $n - 1$ of them such that the associated color, say C, is the same. Call these vertices $v_{i_1}, ..., v_{i_{n-1}}$. Let $i_n = 2n - 3$, the index of the last vertex constructed. By construction all the edges connecting vertices in the set $\{v_{i_0}, ..., v_{i_n}\}$ have the same color, C. ♠

Here is a classic result from combinatorics:

Lemma 0.8 *Suppose that every point in the plane is colored one of three colors. Then there are two points on the plane, exactly one unit apart, which have the same color.*

Proof: Let the colors be red, white, and blue. We can suppose without loss of generality that the origin, x_0, is colored white. Let C be the circle of radius 1 centered on the origin. If some point of C is colored white then obviously there are two white points that are exactly one unit apart and we are done. So, we can suppose that all points of C are colored red and blue.

Suppose that x_1 and x_2 are any two points on C that are one unit apart from each other. Then the points x_0, x_1, x_2 form an equilateral triangle whose sides are one unit apart. This is shown in Figure 2. If these three points do not have all different colors, then we are done. So, suppose they have all different colors.

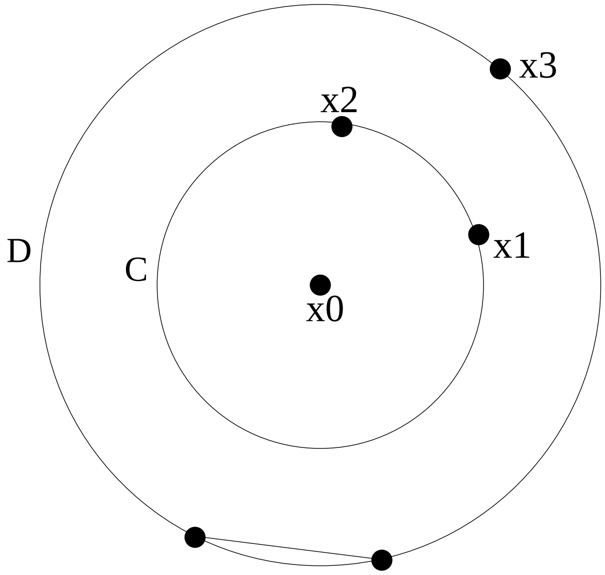

Figure 2

Consider the point x_3, which makes the *other* equilateral triangle with x_1 and x_2. Recall that x_1 and x_2 are red and blue (or else blue and red). If x_3 is not white then we are done. So, suppose that every configuration like the one above gives rise to a white x_3. But then the entire circle D is colored white. But then any chord of D having length 1, such as the one shown at the bottom of Figure 2, connects two white points. ♠

The logic of the last result merits some further discussion. We are trying to prove that some particular statement is true. Our strategy is to assume the worst case at each stage and show that even the worst case leads to the truth of the lemma. It is important to notice e.g. that we are not asserting that any particular 3-coloring of the plane leads to the circle D being colored completely white. Rather, we are asserting that any coloring of the plane either has the desired two-point property or else has the white circle—and then the white circle gives us the two-point property anyhow.