Examples of Proofs

Some Preliminary Ideas

1. What do odd and even mean?

   n odd means that n = 2k+1, and n even n = 2k for some integer k.

   Find k for 15, 18.

2. x > y and z > t implies that x+z > y+t.

   Based on properties of real numbers.

3. Another idea: Positives multiplied by positives give positives

   That is, a > 0 and b > 0 implies that ab > 0

4. Still one more idea:

   x > y > 0 and z > t > 0 means that xz > yt. You can change the > signs between x and y to >= signs and it's still true.

Direct Proof

Theorem A: If a and b are two positive numbers, and a > b, then $a^2 > b^2$.

(Wow! I get to show the use of a lemma! 😊 Remember that a lemma is a statement that is used to prove a theorem.)

Lemma: If x is positive and y is positive, the x + y is positive. (This is really just a restatement of Property 2 in the preliminary ideas.)

Proof: Since x is positive, this means x > 0. Since y is positive, then y > 0. Then, by Property 2, x + y > 0 + 0, or x + y > 0. This means that x + y is positive.

Proof of Theorem A: If If a > b, then by subtracting b from both sides, we get a - b > 0. By the lemma, a + b > 0. Then, by Property 3 form the preliminary ideas, (a+b)(a-b) > 0. Multiplying out the left side gives $a^2 – b^2 > 0$. Adding b^2 to both sides gives $a^2 > b^2$.

===

Theorem B. If n is an odd integer then n^2 is also odd.

Proof: Since n is odd, n = 2k + 1 for some integer k. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$.

$$= 2(2k^2 + 2k) + 1.$$

Since k is an integer, so is 2k, and so is k^2, and so is $2k^2$, and so then is $2k^2 + 2k$. This is because a sum of integers is an integer and a product of integers is an integer. I should have probably listed those in the properties. Then, $n^2 = 2(m) + 1$ where m is an integer. This means n^2 is odd. (In the previous line, $m = 2k^2 + 2k$.)

==

Indirect Proof

Theorem C. If n^2 is an even integer then n is also even.

Proof: I try a direct proof. If n^2 is even, then $n^2 = 2k$ for some k. This doesn't help, because I need to get to n. This means taking a square root. This is a serious problem. I am trying to work only inside the integers because I need to show that n = 2m for some integer m. But then

$$n = \sqrt{n^2} = \sqrt{2k} = ?$$

and here I reach a dead end, because the square root of 2 is not an integer and I don't see a way to proceed. So, I have to try another method of proof. Let me try indirect proof. Starting over:

Proof (Indirect) Suppose n^2 is an even integer and also n is not even. (This is what you assume for an indirect proof.) So, if n is not even, and it's an integer, it must be odd. So then, n = 2k + 1 for some integer k. Then then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. So then if k is an integer then 2k is an integer, …, $2k^2 + 2k$ is an integer. So then n^2 is odd. But we started by assuming that n^2 is an even integer. No number can be both odd and even. (For fun, you could try to prove this. Suppose j is an integer that is both even and odd. Then j = 2k for some integer k since it's even and also j = 2i + 1 for some integer i since it's odd. Then 2k = 2i + 1, or, subtracting 2i from both sides, we get 2k - 2i = 1. That's a contradiction; it can't be true. Why? So there is no such number.)

==

Theorem D. The square root of 2 is irrational; that is, it can't be written as a fraction of two integers.

Proof: Again, I start with a direct proof. The problem here is that I don't know anything about irrational numbers, except that the irrational numbers are all real numbers that are not rational. That doesn't help at all. So I need another method of proof. I turn to indirect proof. Starting over:

Proof: (Indirect) Suppose the square root of 2 is rational. The rational numbers are the fractions. So, then

$$\sqrt{2} = \frac{m}{n}$$

for two integers m and n. I will assume the fraction is fully reduced. If not, I will divide out the common factor so it is reduced. Now, square both sides. You get

$$2 = \frac{m^2}{n^2}$$

Multiplying both sides by n^2 gives $2n^2 = m^2$. Since 2 divides into $2n^2$ and $2n^2 = m^2$, 2 must divide into m^2. But $m^2 = m*m$, and since 2 doesn't factor, 2 must divide into m itself. Then actually, 4 divides into m^2. Now, since 2 divides into m, let me write m as 2p. Then $2n^2 = m^2$ is the same as

$2n^2 = (2p)^2 = 4p^2$. This is $2n^2 = 4p^2$. Cancel the common 2 to get $n^2 = 2p^2$. Then by the reasoning I just went through, 2 divides into n. Now, I have that m = 2p, and n = 2*something, and m and n have 2 in common. I started off by assuming there was nothing in common, because I had totally reduced the fraction. This is a contradiction, and I was wrong in assuming that the square root of 2 was rational.

===

Proof Using the Contrapositive

Theorem E. If n^2 is an even integer then n is also even.

Proof: As above, I find this too hard to prove directly so I try something else. This time I will try to prove the contrapositive. The contrapositive is: If n is not an even integer, then n^2 is not an even integer. Let me start over:

Proof (Contrapositive): If n is not an even integer, then n^2 is not an even integer. (Usually in a proof using the contrapositive, people don't explicitly say what the contrapositive is, because they assume everybody knows that.)

Suppose n is not even. Then it's odd, and so, n = 2k + 1 for some integer k. Then

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which says that n^2 is odd, or n^2 is not even.

===

Theorem F. If a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Proof: Once again, I try to prove this directly. So, assume x and y are two real numbers and

xy > 100. Now what can I say about x and y themselves? Not really anything. So, let me try the contrapositive. It is: If x and y are two positive real numbers and NOT (at least one of the numbers is greater than 10) then NOT (their product is greater than 100). Starting over:

Proof: (Contrapositive) I need to show: If x and y are two positive real numbers and NOT (at least one of the numbers is greater than 10) then NOT (their product is greater than 100). Cleaning this up gives: If x and y are two real numbers and x is not greater than 10 and also y is not greater than 10, then their product is not greater than 100. Then, since x is positive, x > 0. Also, x <= 10. So I can write

10 >= x > 0 and similarly for y 10 > = y > 0. By Property 4, 10*10 >= xy, which says that the product is not greater than 100.

==

Proof Using Cases

This is also called Proof by Exhaustion. Exhaustion here means that you try (or “exhaust”) all possible cases.

Theorem H. Prove that if n is any integer not divisible by 3, then n^2 leaves a remainder of 1 when it is divided by 3.

Proof (By cases) Look at all possible remainders when dividing by 3. The only possible remainders are 0, 1, and 2. In C++, we write this as n % 3 = 0 or n % 3 = 1 or n % 3 = 2. Also, note that “n^2 leaves a remainder of 1 when it is divided by 3” Is a very long and roundabout way of saying “n^2 % 3 = 1” This was background material. Back to the proof.

n is not divisible by 3. This means that n % 3 =0 is impossible. So, n % 3 = 1 or n % 3 = 2. These are the two cases.

Case 1: n % 3 = 1. This means that if you divide n by 3 you get a remainder of 1. Then n = 3k + 1 for some integer k. (You can also get this formula because n has a remainder of 1. Subtract that remainder, giving n-1. Now this must be divisible by 3. So n – 1 = 3k for some integer k.) So,

n = 3k + 1. Square both sides to get: $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. So n^2 % 3 = 1.

Case 2: n % 3 = 2. Then n = 3k + 2 for some integer k. Square both sides to get

$n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1$. So n^2 % 3 = 1.

In either case, $n^2 \% 3 = 1$.

==

In class, I was asked how I came up with these proofs. I will tell you some of my ideas.

In Theorem A, I started out with the end of the problem. That was $a^2 > b^2$. I wasn't sure what to do, but I noticed that if I subtracted b^2 from both sides I would get --- > 0. (That's three dashes on the left. I use it to stand for some expression.) Preliminary ideas 3 and 4 both involve things being greater than 0, so I tried to use them. This means I have to play with expressions until I find something that matches them closely.

In Theorem B, I didn't do anything special. I wrote down what I was assuming and checked what n^2 was. I was just lucky it worked out. It often does! Many direct proofs occur in this way.

Theorem C uses the same idea as Theorem B. After I changed to an indirect proof, I just kept saying this means that, and that means something else, and something else means… until I arrived at the conclusion. Again, it just happened that I reached the conclusion. But also again, this happens often.

In Theorem D, after I decided to do an indirect proof, I started by squaring both sides. Tat's for exactly the same reason I changed from a direct proof to an indirect proof. I can't work with square roots and still guarantee tat I am working only with integers. Not only might I be working with non-integers, I might be working with irrational numbers. This hurts even more, since I only know about the irrationals as being the complement of the rationals (the leftover parts in the reals). I need to find something better.

Theorem E is essentially the same as Theorem B.

Theorem F looks like Property 4, so I tried that.

Theorem H involved something not being divisible by 3. I wasn't sure what that meant, so I investigated division by 3. I then realized there were only three possible remainders. After ruling out one of the possibilities, I just tried each of the others. Again, like in Theorem B, I just wrote things down one after another and the answer popped out.

I hope these ideas help.