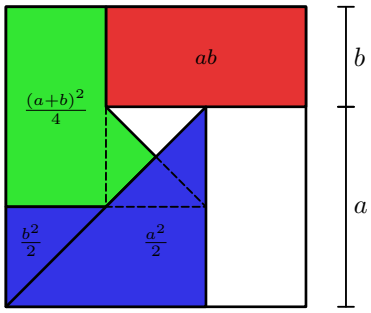
USA(J)MO Handout

Proofs in Pre-USA(J)MO

Author:
Jai Sharma

For:
AoPS

Date:
May 13, 2020



A Proof Without Words of the RMS-AM-GM Inequality: $ab \leq \frac{(a+b)^2}{4} \leq \frac{a^2+b^2}{2}$.

"If only I had the theorems! Then I should find the proofs easily enough." - Georg Bernhard Riemann.

Contents

§0 Acknowledgements

This was made for the Art of Problem Solving Community out there! We would like to thank Evan Chen for his evan.sty code. Thanks to Simon Rubistein-Salzedo for introducing me to mathematical proofs! Made possible by AoPS User naman12. Appendices and title added by AoPS User freeman66.

Art of Problem Solving Community

Evan Chen's Personal Sty File

NAMAN12's Website: Say hi!

FREEMAN66's Website: Say hi!
Note: This is a painting by Richard Feynman, who I admire a lot.

And Evan says he would like this here for evan.sty:

```
Boost Software License - Version 1.0 - August 17th, 2003
Copyright (c) 2020 Evan Chen [evan at evanchen.cc]
https://web.evanchen.cc/ || github.com/vEnhance
```

He also helped with the hint formatting. Evan is a LaTeXgod!
And finally, please do not make any copies of this document without referencing this original one. At least cite us when you are using this document.

§1 Proof by Contradiction

We'll start with an example:

Conjecture 1.1 (Hippasus)
$\sqrt{2}$ is irrational.

Of course, we know that $\sqrt{2} \approx 1.4142...$. That doesn't seem to have much of a pattern, so it must be irrational. But can we find a mathematical proof for this to be completely sure? In order to proceed to the proof, we must introduce the following definitions which you have most likely already learned:

Definition 1.2 (Rational Number) — A **rational number** is a number which can be written as $\frac{x}{y}$, where x and y are integers. Real numbers that are not rational are called irrational.

Definition 1.3 (Greatest Common Divisor) — The **greatest common divisor** of two numbers x and y is written as $\gcd(x, y)$ and is defined as the largest number that divides both x and y.

Definition 1.4 (Lowest Terms) — A rational number $\frac{x}{y}$ is said to be in **lowest terms** if $\gcd(x, y) = 1$ (x and y do not have any common factors greater than 1).

Remark 1.5. If a rational number is not in lowest terms, both x and y can be divided by $\gcd(x, y)$ and the rational number will be in lowest terms because $\gcd(x, y)$ will become 1.

Proof. Assume that $\sqrt{2}$ is a rational number in the form $\frac{a}{b}$ when written in lowest terms. Then

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides, we get

$$2 = \frac{a^2}{b^2}$$

Rearranging this, we get

$$a^2 = 2b^2$$

If a is odd, then a^2 (the left side) becomes odd. However, the right side is even, so a must be even. If we check, squaring an even number a indeed does yield another even number, so a is actually even. We can write an even number x as $x = 2y$ for some integer y. Then, we can also write a as $a = 2c$ for some c. Then our equation from before, $a^2 = 2b^2$ becomes

$$(2c)^2 = 2b^2$$

Expanding the left side, we get

$$4c^2 = 2b^2$$

and dividing by 2, the equation becomes

$$2c^2 = b^2$$

By the same logic as before, b must be even. If both a and b are even, they are both divisible by 2. Then, this contradicts our assumption that $\frac{a}{b}$ is in lowest form. Therefore, our original assumption that $\sqrt{2}$ is rational must be false. If $\sqrt{2}$ is not rational, it must be irrational. Therefore, $\sqrt{2}$ is irrational. □

Theorem 1.6 (Proof by Contradiction)

To show that a statement is true, we sometimes start by assuming that the given statement is false. Then, we show that this cannot be the case because we arrive at an impossible solution. Therefore, the original statement that we assumed to be false must have been true. This is **Proof by Contradiction**.

Exercise 1.7. If you have time at home, try to show that $\sqrt{3}$ is irrational. What about $\sqrt{5}$? $\sqrt{6}$? Can you generalize to $\sqrt{n}$, with n not a perfect square $(1, 4, 9, \ldots)$.

Exercise 1.8. Show that for any **positive integers** a, b, c with $ab = c^2$, then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.

§2 Proof by Induction

The basic idea behind induction is hidden in the following gem: prove the statement for some $n = a$. Then, prove that if the statement holds for $n = k$, then it must hold for $n = k + 1$. Therefore, since the statement holds for $n = a$, it must hold for $n = a + 1$,$a + 2$,$a + 3$, and so on. This is why induction is typically used when we wish to prove a statement for all integers.

Theorem 2.1 (Principle of Induction)

To show a statement is true for **all positive integers**, we can do it through induction by the following steps:

- Show it is true for some starting values (known as the **base case**), most likely $n = 0$ or $n = 1$.
- Then, we show that if it is true for $n = k$, the statement is true for $n = k + 1$.

So why does this work? We can imagine a sequence of dominoes:

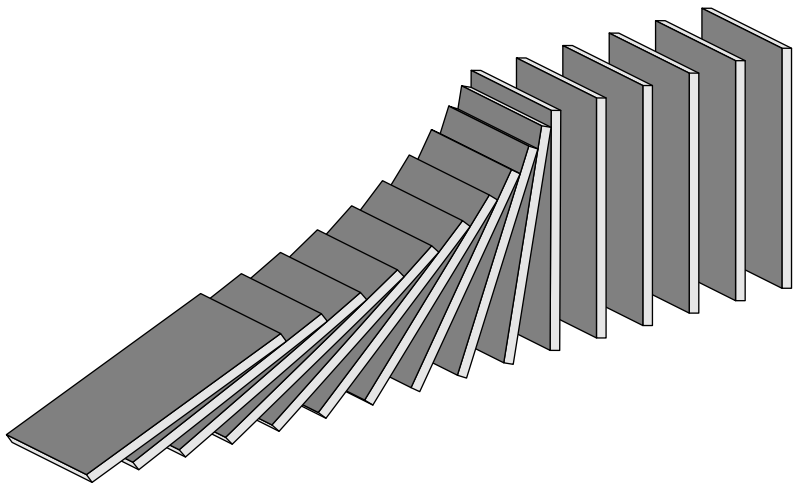


Figure 1: A row of dominoes, falling and knocking the next one over, the process repeating infinitely.

We can use this figure to explain induction. Imagine the first domino is our base case $n = 0$ (a similar argument can be repeated for other starting values such as $n = 1$). We show that it is true, so we knock that

domino over. Then, this knocks the next domino over ($n = 1$), which knocks the next domino over ($n = 2$), and the process continues infinitely. Let's see an example:

Conjecture 2.2 (Faulhaber)
Show that the sum

$$1 + 2 + \cdots + n$$

has value equal to

$$\frac{n(n+1)}{2},$$

where n is any positive integer.

Remark 2.3. In induction, we are often given formulas and asked to prove them. How we got those formulas is another story called derivation.

Proof. We are given the formula $\frac{n(n+1)}{2}$ and are trying to prove this for all positive integers starting with 1, then $2, 3, 4$, and so on. We shall use our induction (or domino principle, whichever you fancy) to show this. We first need to show the statement is true for our base case.

Base Case

We start by proving the base case of $n = 1$ because 1 is the smallest positive integer. This is a fairly simple sum because the sum of the first integer is simply 1. We can verify that the given formula holds by plugging 1 for n. We get

$$\frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = \frac{2}{2} = 1.$$

Now we know that the given formula works for n = 1.

Now we can perform our two induction steps.

Inductive Hypothesis

Assume that the formula $\frac{n(n+1)}{2}$ calculates the sum of the first k positive integers when $n = k$.

Now, we finish off with the last part, which is the inductive step.

Inductive Step

Assume that the given formula holds for $n = k$ for some k. Then we must prove that it also holds for $n = k + 1$. Let us now try to calculate

$$1 + 2 + 3 + \cdots + k + (k + 1)$$

Because of the Inductive Hypothesis, we know that we can use our formula to calculate the value of

$$1 + 2 + 3 + \cdots + k$$

by computing $\frac{k(k+1)}{2}$. We can replace the $1 + 2 + 3 + \cdots + k$ part of our sum with this. Then,

$$1 + 2 + 3 + \cdots + k + (k + 1) = \frac{k(k + 1)}{2} + (k + 1)$$

Factoring out $k+1$ from the right side, we get $(k+1)\left(\frac{k}{2}+1\right)$. Writing the term $\frac{k}{2}+1$ as a single fraction with 2 as the denominator, this term becomes

$$\frac{k}{2}+1=\frac{k}{2}+\frac{2}{2}=\frac{k+2}{2}$$

Substituting this last expression for $\frac{k}{2}+1$ in $(k+1)\left(\frac{k}{2}+1\right)$, we have $(k+1)\cdot\frac{(k+2)}{2}$ or $\frac{(k+1)(k+2)}{2}$. This cannot be simplified further, so we confirm that when $k+1$ is substituted into our formula, the same result is yielded. Indeed, substituting n with $k+1$ in our formula, we get

$$\frac{(k+1)(k+1+1)}{2}=\frac{(k+1)(k+2)}{2}.$$

These two are the same! Therefore, we can conclude that if our formula works for $n=k$, then it must work for $n=k+1$. Remember that we established that this formula works for $n=1$ in our base case. Now that we know that it works for $n=1$, we can use our recently proven conclusion to find that the formula works for $n=1+1=2$, so $n=1$ implies $n=2$. Similarly, our formula works for $n=3,4,5,\ldots$, and therefore, we have proven this formula for all positive integers n.

□

Exercise 2.4. Try to show that the sum of the first n odd integers is n^2 by the Principle of Induction.

Exercise 2.5. Try to show that the sum

$$1^2+2^2+3^2+\cdots+n^2$$

is equal to

$$\frac{n(n+1)(2n+1)}{6}$$

by the Principle of Induction.

§3 Pigeonhole Principle

This next theorem is not a proofs strategy, but merely a concept. This concept is so trivial that no one thought it to be significant for a long time. In this concept, we assume that we have pigeons that live in holes. We put these pigeons into their holes by choosing one hole for each pigeon. This is the same as putting toy balls into different buckets, where the pigeons are the balls and the holes are the buckets.

Conjecture 3.1 (Pigeonhole Principle)

If we have $n+1$ pigeons and only n holes to place them in, we must have at least 2 pigeons in one of the holes.

Proof. The proof for this observation is simple. We can use the method of Proof by Contradiction. We assume that we can place the pigeons into their holes such that there is no more than one pigeon per hole. Suppose we are now placing our pigeons into their holes. If we place more than one pigeon per hole, we have at least 2 pigeons per hole. Therefore, we must place one pigeon per hole. By the time we have place a single pigeon in each of the n holes, we have one pigeon remaining. No matter where we place this pigeon, it will end up in a hole with two pigeons in it. Therefore, it is unavoidable to have at least two pigeons in one of the pigeonholes. □

This conjecture is so trivial, you probably did not need to read the proof in order to assure yourself that it was true. The next conjecture that we prove is a generalization of this previous one.

Conjecture 3.2 (Generalized Pigeonhole Principle)

If we have $n \cdot k + 1$ pigeons and must place them into n different holes, we must have at least $k + 1$ pigeons in one of the n holes.

Proof. We do this proof by the method of Proof by Contradiction as well. Suppose that all of the holes have less than $k + 1$ pigeons. We can therefore place up to k pigeons per hole. Armed with a strategy, we start to confidently place k pigeons in each hole. However, when we reach the last hole and place the k pigeons, we realize that we have only used

$$n \text{ holes} \times k \text{ pigeons per hole} = n \cdot k \text{ pigeons},$$

and that we still have one pigeon left to place in one of the holes (because we started with $n \cdot k + 1$ pigeons). Similar to the last proof, no matter where we place our last pigeon, it will end up in a hole which has $k + 1$ pigeons in it (because we had originally put k pigeons in every hole). Therefore, it is unavoidable to have $k + 1$ pigeons in one of the n holes. □

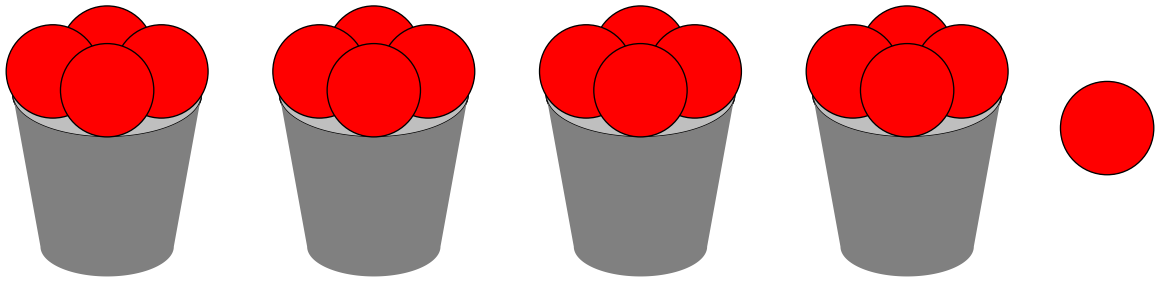


Figure 2: This diagram shows this principle visually if we have $4 \cdot 4 + 1 = 17$ balls. By placing 4 balls in each of the 4 buckets, we use 4 buckets $\times$ 4 balls per bucket $= 16$ balls. However, we have one ball remaining. This ball must be kept in a bucket which will end up having $4 + 1 = 5$ balls.

Remark 3.3. In the image above, we used the analogy of balls and buckets. Note that this is exactly the same as using pigeons and pigeonholes, respectively. There are many analogies for the pigeonhole principle, but you will start to recognize them with enough practice.

This generalization is fairly harder to grasp, but it still comes intuitively to the mind. While this generalization has applications of its own (such as in basic competition math problems), it can also be used to prove more advanced theorems. Let us simply establish our results for now:

Theorem 3.4 (Pigeonhole Principle)

If we have at least $n \cdot k + 1$ pigeons and must place them into n different holes, we must have at least $k + 1$ pigeons in one of the n holes.

Exercise 3.5 (Art of Problem Solving)**.** Use the Pigeonhole Principle to attempt the following problem: If a Martian has an infinite number of red, blue, yellow, and black socks in a drawer, how many socks must the Martian pull out of the drawer to guarantee he has a pair?

§4 Examples

§4.1 Prime Numbers

Note 4.1 — When we say, "Statement A is true if and only if statement B is true," we mean, "Statement A is true if statement B is true and statement A can only be true if statement B is true." Think about this for a minute. For example, statement A can be

"A number is even,"

and statement B can be

"The number is divisible by 2."

Putting these two statements together with an "if and only if", we get

"A number is even if and only if the number is divisible by 2.

This means that "A number is even if it is divisible by 2," which is obviously true because this is the definition of an even number: it is divisible by 2. However, this also means that "A number is even only if it is divisible by 2." This latter statement means that if a number is not divisible by 2, then it must not be even as well. "If and only if" is a very common phrase found in math texts and is often written in shorthand by writing "iff." So, if you see this written somewhere, do not think of it as a typo!

In our next section, we discuss (arguably) some of the most important numbers: prime numbers. We start off with a definition:

Definition 4.2 (Prime) — A positive integer $n \geq 2$ is **prime** if and only if it is divisible by 1 and n and none of

$$2, 3, 4, \ldots, n-1.$$

A positive integer that is not prime is referred to as composite.

Remark 4.3. Note that any positive integer n that is composite can be written as $n = a \cdot b$, where a and b are both greater than 1.

Remark 4.4. The number 1 is neither prime nor composite. It is special because it is the product of no primes at all! In other words, if we do not multiply any prime numbers together (or any numbers for that matter), we will end up with the number 1.

Why are prime numbers so important? As we will now see, prime numbers are the building blocks of all numbers.

Conjecture 4.5 (Fundamental Theorem of Arithmetic)

Every positive integer greater than 1 has a unique way in which it can be written as the product of multiple prime numbers. Specifically, a number n can be written as the product

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$$

where $p_1, p_2, \ldots, p_m$ are primes and $k_1, k_2, \ldots, k_m$ are positive integers (also known as whole numbers).

Proof. In order to prove this conjecture, we must prove two things:

- Every number has a prime factorization;
- Every number has a unique prime factorization.

Notice how these two parts are in the original conjecture, but we isolated them explicitly. This is a powerful problem solving tool. We perform the following proof for the first part of the conjecture by strong induction, which will be introduced here. Strong induction works similar to normal induction and is founded on the following key ideas:

- Prove a conjecture for some number $n = a$. This is our **Base Case.**
- Prove that if the conjecture is true for

$$n = a, a+1, a+2 \cdots, k-1,$$

where $a < k$ (assuming that this is true is known as the **Inductive Hypothesis**), then it must be true for k.

- This last part is the **Inductive Step**. If the conjecture, as proved in the base case, holds for $n = a$, then it must hold for $n = a+1, a+2, a+3, \ldots$, therefore proving the conjecture for $n = k$ for all integers $k \geq a$.

Now, let's get back to proving the Fundamental Theorem of Arithmetic. We do so with strong induction:

Base Case

Since 1 is neither prime nor composite, we start with our base case of $n = 2$. Since 2 is prime, we can simply write its prime factorization as 2, and we are done with our base case.

Now we proceed to making the:

Induction Hypothesis

We must assume that all the numbers

$$2, 3, 4, \ldots, k-1$$

have a prime factorization. Now, we try to find whether k has a prime factorization.

This last part is done in the

Induction Step

k is either prime or composite. If k is prime, then its prime factorization is simply k. However, if k is composite, then we can write k as $k = x \cdot y$, where x and y are positive integers greater than 1 and are either prime or composite (see remark above). Clearly, x and y must be less than k. By our inductive hypothesis, both x and y must both have prime factorizations. Suppose

$$x = p_1^{j_1} \cdot p_2^{j_2} \cdot p_3^{j_3} \cdots p_m^{j_m}$$

and

$$y = q_1^{i_1} \cdot q_2^{i_2} \cdot q_3^{i_3} \cdots q_l^{i_l}.$$

Multiplying these two, we get

$$k = x \cdot y = p_1^{j_1} \cdot p_2^{j_2} \cdot p_3^{j_3} \cdots p_m^{j_m} \cdot q_1^{i_1} \cdot q_2^{i_2} \cdot q_3^{i_3} \cdots q_l^{i_l}.$$

The simplified version of this is the prime factorization of k.

Therefore, all numbers $k \geq 2$ have a prime factorization.

Now, we must prove that every number k has a **unique** prime factorization. We can do this using Proof by Contradiction. Suppose that a number n has two prime factorizations so that

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$$

and

$$n = q_1 \cdot q_2 \cdot q_3 \cdots q_l$$

where p_i and q_j are distinct primes for all i and j. We need the following

Lemma 4.6 (Euclid)
Every prime number $p \mid ab$ (this means p divides the product of a and b) satisfies $p \mid a$ or $p \mid b$.

We suppose that in the representations of n, we suppose that one of the p_i's is not any of the q_j's. Then, we have that

$$p_i \mid n = q_1^{i_1} \cdot q_2^{i_2} \cdot q_3^{i_3} \cdots q_l^{i_l},$$

so p_i divides one of the q_j, a contradiction. Thus, the two primes are the same. We are only concerned about the exponents now. Let $p_m = q_n$ for some m and n and that these are raised to the powers j_m and i_m, respectively. Assume that for contradiction, $i_m < j_m$ (if not, then we can reverse the roles of the two). Then, considering the number

$$\frac{n}{q_n^{i_n}},$$

we see that two prime factorizations are

$$p_1^{j_1} \cdots p_{m-1}^{j_{m-1}} p_m^{j_m - i_n} p_{m+1}^{j_{m+1}} \cdots p_k^{j_k} = q_1^{i_1} \cdots q_{n-1}^{i_{n-1}} q_{n+1}^{i_{n+1}} \cdots q_l^{i_l}.$$

Notice how there is no $q_n^{i_n}$ on the right hand side because we divided by it. This leads to a contradiction as p_m appears on the left hand side and not on the right hand side (because no other q_x is divisible by p_m). Thus, our original assumption that n has 2 prime factorizations was false, so we know that every positive number greater than one must have a unique prime factorization. □

Let us establish our new proof technique:

Theorem 4.7 (Strong Induction)
Strong induction is a proofs strategy that works similar to induction. There are 3 parts to a strong induction proof:

- Prove a conjecture for some number $n = a$. This is our **Base Case.**
- Assume that the conjecture holds for

  $$n = a, a+1, a+2 \cdots, k-1,$$

  where $a < k$. This is called the **Inductive Hypothesis**.
- Prove that this conjecture must also hold for k. This last part is the **Inductive Step**.

If the conjecture, as proved in the base case, holds for $n = a$, then it must hold for $n = a+1, a+2, a+3, \ldots$, therefore proving the conjecture for $n = k$ for all integers $k \geq a$.

Because of Fundamental Theorem of Arithmetic, we can define the following:

Definition 4.8 (Prime Factorization) — Every positive integer n greater that 1 can be expressed in the form

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$$

and this is called the **prime factorization** of n.

Try your hands at the following exercises:

Exercise 4.9. Write the prime factorization of the following numbers: 24, 35, 360. What about 5,040? See the definition of a prime factorization for the writing structure (above).

Exercise 4.10. Find the prime factorization of 10. What about 100? 1,000? Try 1,000,000. What about 10^n for some integer n?

Conjecture 4.11 (Infinitude of Primes)
There are an infinite number of primes.

Proof. We can perform this simple proof using Proof by Contradiction. Assume that there is only a finite number of primes $p_1, p_2, p_3, \cdots, p_n$. Now, if we multiply all of these primes together and add one, we get

$$p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1.$$

Let us now find the prime factorization of this number. Uh-oh, we find that our number is not divisible by $p_1, p_2, p_3, \cdots, p_n$. If our new number is prime, then we have found another prime that is not on our finite list of all the primes and therefore we have reached a contradiction. On the other hand, if our number is composite, then it must be divisible by some prime number because it must have a prime factorization. However, it is not divisible by any of the prime numbers in this finite list (it leaves a remainder of when when divided by each of $p_1, p_2, p_3, \cdots, p_n$. In either scenario (whether our number is prime or composite), we have reached a contradiction. Therefore, our original assumption that there is a finite number of primes must have been false. Because of our contradiction, we know that there must be an infinite number of prime numbers. □

From this proof, we conclude that

Theorem 4.12 (Infinitude of Primes)
There are an infinite number of prime numbers.

§4.2 Euclidean Algorithm

Finding the gcd of two numbers a and b can be done by comparing the prime factorizations of the two numbers. From the prime factorizations, we can easily see the maximum power of a prime p such that both a and b are divisible by this power of p. Say this power of p is k. Then, p^k divides both a and b. If we find p^k for all such primes and multiply them, we get the $\gcd(a, b)$. However, there is an even better way to find the $\gcd(a, b)$. We start by proving a lemma.

Conjecture 4.13 (Discovering the Euclidean Algorithm)
If a and b are nonzero integers and k is an integer, then $\gcd(a, b) = \gcd(a, b - k \cdot a)$.

Proof. It suffices to show that the $\gcd(a, b)$ divides $b - k \cdot a$. If $d = \gcd(a, b)$, then $a = d \cdot x$ and $b = d \cdot y$ for some x and y. Note that because $d = \gcd(a, b)$, x and y must be **relatively prime**, meaning that $\gcd(x, y) = 1$. Thus,

$$b - k \cdot a = (d \cdot y) - k \cdot (d \cdot x) = d(y - k \cdot x).$$

Therefore, $b - k \cdot a$ is also a multiple of d. Therefore, we must have $\gcd(a, b) = \gcd(a, b - k \cdot a)$. □

How does this help us find the $\gcd(a, b)$ for two integers a and b? Well, this helps us to simplify the problem, as shown in the following example:

Example 4.14 (Euclidean Algorithm Example)
Find the $\gcd(144, 270)$.

Proof. Finding the prime factorization for these two numbers looks like a bit of a pain. However, if we let $a = 144$ and $b = 270$, we know that

$$\gcd(a, b) = \gcd(a, b - k \cdot a) = \gcd(144, 270 - 144) = \gcd(144, 126) = \gcd(126, 144).$$

We have reduced the complexity of this problem. Again, we can take $a = 126$ and $b = 144$. Notice how we always let b, the second number, be the larger of the two numbers (the order of a and b in $\gcd(a, b)$ does not matter). We have

$$\gcd(126, 144) = \gcd(126, 144 - 126) = \gcd(126, 18) = \gcd(18, 126).$$

Wow, this seems to be working really well! Let's try that again!

$$\gcd(18, 126) = \gcd(18, 126 - 7 \cdot 18) = \gcd(18, 0).$$

At this point, it is clear that $\gcd(18, 0) = 18$. Therefore, $\gcd(144, 270) = \boxed{18}$ as well. □

This last example showed us how to use our recently discovered gcd trick to evaluate $\gcd(a, b)$ for some integers a and b. We will define this process, called the **Euclidean Algorithm** generally as follows:

Theorem 4.15 (Euclidean Algorithm)
If we are trying to find $\gcd(a, b)$, rearrange these two numbers so that the second number b is the larger of our two numbers. Now, perform the following four steps:

- If $a = 0$ or $b = 0$, then the final answer is the nonzero number. In this case, we are done.
- If $a \neq 0$ and $b \neq 0$, then consider the number $b - k \cdot a$, where $0 \leq b - k \cdot a \leq a$ and k is an integer. This number is somewhere between 0 and a, which means that we have reduced the complexity of the problem. Replace the current value of b with this number and proceed.
- Switch the order of a and b so that the second number in $\gcd(b, a)$, or a, is greater than the first number, or b.
- Switch the names of a and b to make sure that b is always the second number in the pair. Namely, so that we have $\gcd(a, b)$.

Joke 1 (Question)

Try to unscramble the word "Algorithm" into another math word! (Proceed to find the answer.)

Think over this last theorem, or the Euclidean Algorithm, and see how it applies to the example shown above. Now, we explore an extension of this algorithm.

Conjecture 4.16 (Bézout's Lemma)

The $\gcd(a, b)$, where a and b are positive integers, is the smallest positive integer that can be expressed as $a \cdot x + b \cdot y$, where x and y are integers.

Proof. Since both a and b are multiples of $d = \gcd(a, b)$, every number in this form will also be a multiple of d. If you do not believe me, try it for yourself! Therefore, the smallest **positive** number that could be in this form is d. Therefore, we only have to show that d itself can be written in this form, and we will be done. We can do this using the Euclidean Algorithm. If we can show that every number produced by the Euclidean Algorithm can be written in this form, then the $\gcd(a, b)$, which is also one of these numbers, can be written in this form and we are done. We can do this by the Principle of Induction.

Base Case.

This will be the first and second numbers "produced" by the Euclidean Algorithm, or a and b themselves. Of course, these can be expressed in the form $a \cdot x + b \cdot y$ by allowing $y = 0$ and $x = 0$, respectively (Think about it!).

Now, we shall proceed with the

Inductive Hypothesis

Let us name each number produced by the Euclidean Algorithm as b_n for some integer n in the sequence that the number was produced. So, $b = b_0$, $a = b_1$, and $b - k \cdot a = b_2$, and so on. Because of our **Base Case**, we can assume that b_{n-1} and b_n can be written in this form. Let $b_{n-1} = ax_{n-1} + by_{n-1}$ and $b_n = ax_n + by_n$. Now we must prove that b_{n+1} can be written in this form as well.

Finally, the backbone of the proof is in the

Inductive Step.

So, how do we get the next term b_{n+1}? Well, by the Euclidean Algorithm, $b_{n+1} = b_{n-1} - k \cdot b_n$. By our definitions of b_{n-1} and b_n, we have

$$b_{n+1} = b_{n-1} - k \cdot b_n = (ax_{n-1} + by_{n-1}) - k \cdot (ax_n + by_n).$$

Rearranging this, we have

$$a(x_{n-1} - kx_n) + b(y_{n-1} - ky_n).$$

If we take $x = x_{n-1} - kx_n$ and $y = y_{n-1} - ky_n$, we have written b_{n+1} in the form $a \cdot x + b \cdot y$.

As mentioned before, this means that we are done with our proof. □

§A Appendix A: List of Theorems, Lemmas, and Conjectures

List of Theorems, Lemmas, and Conjectures

List of Theorems, Lemmas, and Conjectures

§B Appendix B: Other Proof Techniques

§B.1 Proof by Contraposition

Proof by contraposition infers the statement "if p then q" by establishing the logically equivalent contrapositive statement: "if not q then not p".

Example B.1

Prove that if x^2 is even, then x is even.

Solution. Suppose that x is odd. Then $x \cdot x = x^2$ is odd. Thus, x^2 can only be even if x is even. □

§B.2 Proof by Construction

For existence problems, one can construct the solutions. It can also be a **counterexample**, in which you disprove the claim. Some say there are also **nonconstructive** proofs, in which you don't need to actually prove it, but rather give an example. I'd say this is still constructive, as shown below:

Example B.2

Prove there exists an even prime number.

Solution. I claim 2 is this number. The only factors of 2 are 1 and 2, which directly implies it is a prime number. □

§B.3 Proof by Exhaustion

This is more commonly known as **casework**. Given a finite amount of cases, they can all be checked to give a certain result. Of course, you could have an infinite number of cases, but if there exists a way to prove none of them work, you have still exhausted that case. This is a proof commonly used by computer scientists.

§B.4 Combinatorial Argument

A combinatorial proof establishes the equivalence of different expressions by showing that they count the same object in different ways. Often a bijection between two sets is used to show that the expressions for their two sizes are equal. Alternatively, a double counting argument provides two different expressions for the size of a single set, again showing that the two expressions are equal.

§B.5 Proof Without Words

This was presented on the title page. The idea is that the visual proves the claim in some clever way - I recommend you search these up, and see for yourself how they work!

§B.6 Probabilistic Method

This method is too advanced for even the appendix. You can read about it here.

§B.7 Fake Proofs

Sometimes it is fun to "spot the mistake" in the proof. Most of the time, fake proofs arise from **fakesolving** - thinking you solved the problem when you really didn't. I encourage you to not only Google search for fake proofs, but also false proof techniques! One of my favorites is **Proof by Intimidation**.