

products with a single term (for prime numbers). Every composite number has a factorization into primes which contains more than one term. Examples might be $6 = 2 \cdot 3$, $525 = 3 \cdot 5 \cdot 5 \cdot 7$, etc. If we list primes in increasing order, then we can ignore the statement above about the order of the terms. It is also customary to collect products of the same prime together as an exponent as in $24 = 2^3 \cdot 3$, $525 = 3 \cdot 5^2 \cdot 7$, etc. With these conventions, the theorem can be restated as follows: **Each positive integer can be expressed as a product of primes in Exactly One Way.** That is:

Theorem. (Still the Fundamental Theorem of Arithmetic) If $n > 0$, then there is an integer k such that $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $p_1 < p_2 < \cdots < p_k$ and the p 's are all primes. More over, the p 's and a 's are uniquely determined by n . That is, if $n = q_1^{b_1} q_2^{b_2} \cdots q_i^{b_i}$ where the q 's are primes with $q_1 < q_2 < \cdots < q_i$, then $i = k$, $p_1 = q_1, p_2 = q_2, \cdots, p_k = q_k$, and $a_1 = b_1, \cdots, a_k = b_k$.

Intuitively, this theorem says the following: if two different people are given the same number to factor, and each uses a different **legitimate** method, then they are guaranteed to get the same answer. It is worth noting that this is not obvious, and in fact, it is not true in all number systems. Gauss appears to have been the first person to concretely state and prove this theorem. We will prove the theorem in a bit. But first, we will give several examples of its usefulness.

Theorem. If two positive integers are relatively prime and their product is a square, then both integers are squares.

Proof: Let $uv = y^2$. By the Fundamental Theorem, $y = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, so $y^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k}$. Since $uv = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k}$, the only prime divisors u and v can have are the primes p_1, \cdots, p_k . Since u and v are relatively prime, any prime which divides one of them does not divide the other. So if p_i is a divisor of u , then it is not a divisor of v . Thus, it must be that $p_i^{2a_i}$ occurs in the prime factorization of u . That is, every prime divisor of u occurs to an even power. Now a prime raised to an even power is a square (for example, $5^{18} = (5^9)^2$.) This means that u is a product of squares. But any product of squares is a

square ($x^2y^2 = (xy)^2$.) Thus, u is a square, and by the same reasoning, v is a square.

Theorem. If $\frac{x}{y} = \frac{a}{b}$ where x, y, a, b are positive integers with x and y relatively prime and a and b relatively prime, then $x = a$ and $y = b$.

Proof: If $\frac{x}{y} = \frac{a}{b}$ then $bx = ay$. If p^m is part of the prime factorization of a and p^n is part of the factorization of y , then p^{m+n} will be part of the prime factorization of ay . Since $ay = bx$, p^{m+n} must occur in the prime factorization of bx . But a and b are relatively prime, so p is not a divisor of b . This means that p^{m+n} occurs in the prime factorization of x . Since x and y are relatively prime, p is not a divisor of y , so $n = 0$. Consequently, if p^m is a factor of a , then p^m is also a factor of x . From this we can conclude that a and x have identical factorizations, so $a = x$. Since $bx = ay$, it now follows that $b = y$.

Theorem. $\sqrt{2}$ is irrational. That is, there are no integers m and n with $n \neq 0$ such that $\sqrt{2} = \frac{m}{n}$.

Proof. Suppose, by way of contradiction, that there were such integers m and n . Certainly, we can make them both positive integers. Multiplying by n and squaring gives $2n^2 = m^2$. If two numbers are equal, they must have the same prime factorization, so consider the prime factorizations of m^2 and $2n^2$. In particular, consider the power of 2 which divides each side. If $m = 2^a \cdots$, then $m^2 = 2^{2a} \cdots$, so the prime factorization of m^2 has 2 raised to an even power. On the other hand, if $n = 2^b \cdots$, then $2n^2 = 2^{2b+1} \cdots$, so the prime factorization of $2n^2$ has 2 raised to an odd power. Thus, the factorizations of m^2 and $2n^2$ can not be the same contradicting unique factorization.

We can, of course, give countless additional applications of unique factorization. But let us concede that unique factorization is important, and try to prove it. A proof can be given using Mathematical Induction. We will do something equivalent, but with more historical import. We introduce a proof

technique used by the Greeks, but popularized by Fermat. It is called a **proof by infinite descent**. A proof by infinite descent is actually a proof that something **does not** exist. It goes like this: you are given the problem of showing that no positive integer has some property. You start by assuming that some positive integer **does** have that property. From this, you show that there is a **smaller** positive integer which also has that property. This cannot happen: there are only finitely many positive integers less than any given number, but the above would imply the existence of infinitely many positive integers smaller than some bound.

Before proving the Fundamental Theorem, we give some examples of proofs by infinite descent.

Example 1. $\sqrt{2}$ is irrational.

Proof: We already proved this once, assuming the Fundamental theorem. This will be an alternative proof using infinite descent. We want a property related to numbers being rational, and we wish to show that there are no positive integers with that property with respect to $\sqrt{2}$. Here is the property: **If a is a rational number, then there is a positive integer n with the property that na is an integer.** (Can you prove that this is true?)

We claim that there is no positive integer n such that $n\sqrt{2}$ is an integer. Suppose there were such an integer. Consider $n_1 = n\sqrt{2} - n$. We study this new number n_1 . First, $1 < \sqrt{2} < 2 \Rightarrow 0 < \sqrt{2} - 1 < 1$, so $0 < n\sqrt{2} - n < n$, or $0 < n_1 < n$. Now n_1 must be an integer if n has the stated property. And since $0 < n_1 < n$, n_1 is a strictly smaller positive integer. Finally, if we multiply n_1 by $\sqrt{2}$, we have $n_1\sqrt{2} = (n\sqrt{2} - n)\sqrt{2} = 2n - n\sqrt{2}$, which is the difference of two integers. Thus, n_1 is a strictly smaller positive integer than n which has the same property. By infinite descent, there can be no such n and so $\sqrt{2}$ must be irrational.

Example 2. There are no positive integers x, y, z such that $x^2 + y^2 = 3z^2$.

In this case, we will perform an infinite descent on z . Suppose that z is part of a triple of positive integers (x, y, z) with $x^2 + y^2 = 3z^2$. We need the following

fact: When a square is divided by 3, the remainder is either 0 or 1. To see this, consider a number m and its square m^2 . There are three possibilities when m is divided by 3: the remainder is 0 or 1 or 2. This means that $m = 3q + r$, where $r = 0, 1, \text{ or } 2$. Now $m^2 = 9q^2 + 6qr + r^2$. So if $r = 0$ or 1 , when m^2 is divided by 3, the remainder is also 0 or 1. When $r = 2$, $r^2 = 4 = 3 + 1$, so $m^2 = 3(3q^2 + 4q + 1) + 1$, and in this case the remainder is also 1.

Now, when $x^2 + y^2$ is divided by 3, the remainder will be $r_1 + r_2$ where r_1 and r_2 are the remainders when x^2 and y^2 are divided by 3. This remainder must be 0, and the only combination of 1's and 0's which is divisible by 3 is 0 and 0, so both x^2 and y^2 must be divisible by 3. Consequently x and y are divisible by 3, so let $x = 3x_1$ and $y = 3y_1$. Then, $x^2 + y^2 = 9x_1^2 + 9y_1^2 = 3z^2$. Hence, $z^2 = 3x_1^2 + 3y_1^2$ which means that z is divisible by 3. Letting $z = 3z_1$, we have $9x_1^2 + 9y_1^2 = 27z_1^2$, or $x_1^2 + y_1^2 = 3z_1^2$. Thus, if (x, y, z) satisfies $x^2 + y^2 = 3z^2$, then x, y and z must all be divisible by 3, and $(x/3, y/3, z/3)$ will also satisfy the equation. Said differently, if z is part of such a triple, then z is a multiple of 3 and $z/3$ (a smaller positive integer) will also be part of such a triple. By infinite descent, this cannot happen, so there can't be any solutions.

We need one more thing to prove the fundamental theorem:

Lemma. If p is a prime and ab is divisible by p , then a is divisible by p or b is divisible by p .

(It is important that p be a prime: 300 is divisible by 6 even though $300 = 15 \cdot 20$ and neither 15 nor 20 is divisible by 6.)

A proof of the Fundamental Theorem of Arithmetic:

We proceed by infinite descent on numbers not obeying the fundamental theorem. That is, we show that if n is a positive integer which does not have unique factorization, then there is a smaller positive integer which also does not have unique factorization. So suppose that n does not have a unique factorization. Then n must possess two different factorizations:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad n = q_1^{b_1} q_2^{b_2} \cdots q_i^{b_i}.$$

From the first factorization, we have that p_1 is a divisor of n . By the second factorization, we have that p_1 is a divisor of $q_1^{b_1} q_2^{b_2} \cdots q_i^{b_i}$. By the lemma, p_1 must be a divisor of one of the terms q^k . But since the q 's are primes, this can only happen if one of the q 's is equal to p_1 . Say, for example that $q_1 = p_1$. Then dividing both factorizations by p_1 gives

$$n/p_1 = p_1^{a_1-1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad n/p_1 = p_1^{b_1-1} q_2^{b_2} \cdots q_i^{b_i}.$$

If the two factorizations for n are different, then the two factorizations for n/p_1 must also be different, so we have produced a smaller number which also fails to have unique factorization. By infinite descent, no such n can exist.