# Math From Scratch Lesson 15:
# The Fundamental Theorem of Arithmetic

W. Blaine Dowler

November 13, 2011

## Contents



## 1 Preliminaries

To this point, we have dealt with division by integers. However, as division by 0 is impossible within the integers, and as divisibility by $d$ implies divisibility by $-d$, we will take a bit of a shorthand here which will help us simplify our discussion. For the duration of this lesson, our divisors will be taken exclusively from the set of natural numbers. Thus, if we say a number has two factors, we really mean it has two natural number factors, and two *more* negative number factors. Similarly, we only consider cases of "dividing into" positive numbers, meaning positive dividends. This means we will only explicitly examine cases such as $6 \div 3$, and allow the subsequent findings for $-6 \div 3$, $6 \div -3$ and $-6 \div -3$ to follow logically without specific examination.

To save time when writing this lesson, the word "number" will be used in an extraordinarily sloppy manner to mean "natural number" unless otherwise specified. Similarly, this will start to use juxtaposition to imply multiplication, meaning $ab$ should be read as $a \cdot b$.

# 2 Classifying Numbers

## 2.1 Even Numbers

An *even number* is an integer which is a multiple of 2.

## 2.2 Odd Numbers

An *odd number* is an integer which is not a multiple of 2.

## 2.3 Prime Numbers

We know that every number $a$ has at least one factor. If $a = 1$, then this is its only factor. If $a \neq 1$, then $a$ has at least two factors, namely 1 and $a$.

**Definition** A number $a$ is a *prime number* if and only if it has *exactly* two factors.

Thus, 1 is not prime as it has less than two factors. 9 is not prime as it has three factors. This seemingly innocuous and arbitrary idea turns out to be important in a myriad of bizarre places.[1] They will resurface time and time again in the course of these lessons.

[1] Don't take my word for it: check out the "Prime Pages" with your favorite search engine.

### 2.4 Composite Numbers

**Definition** A number $a$ is a *composite number* if it has *more than* two factors.

Thus, 1 is neither prime nor composite. Although nothing can be divided by 0, 0 itself is divisible by anything (with quotient and remainder both 0), and thus 0 is a composite number. Also, as 1 is the only number with only a single factor, and any number $a$ has at most $a$ factors (i.e. it can only be divisible by numbers $n$ such that $1 \leq n \leq a$) we know that the number of possible factors of $a$ can be counted. Thus, every number is either prime, composite, or 1.[2]

### 2.5 Perfect Squares

**Definition** A number $a$ is a *perfect square* if it has an *odd number* of factors.

### 2.6 Relatively Prime Numbers

**Definition** Two numbers $a$ and $b$ are said to be *relatively prime* if they have no prime factors in common.

For example, although 4 and 9 are not prime numbers, they are relatively prime as $4 = 2^2$ and $9 = 3^2$ have no prime factors in common. Note that the definition depends entirely on which two numbers have been chosen; 4 and 9 are relatively prime, but 9 and 15 are not, as both are divisible by 3.

Relatively prime numbers open the doorway for the linear diophantine equation, a critical piece of groundwork for the Fundamental Theorem of Algebra.

## 3 The Linear Diophantine Equation

A diophantine equation is an equation of the form

$$ax + by = c$$

in which $a$, $b$, $c$, $x$ and $y$ are all integers. An equation of this form can be solved if and only if the greatest common factor of $a$ and $b$ is a factor of $c$.

[2]Note that, although 0 has infinitely many factors, and is the only number with an infinite number of factors, we will later learn that the number of factors of 0 is a *countably infinite* number, so the statement here still applies.

## 3.1 Greatest Common Factors

The greatest common factor, or greatest common divisor, of two numbers $a$ and $b$, denoted $\gcd(a, b)$, is the greatest number which can divide into both $a$ and $b$ with no remainder. This number exists and is unique for any given pair of numbers $a$ and $b$.

**Definition** The *greatest common factor* or *greatest common divisor* of $a$ and $b$ is the number $\gcd(a, b)$ which satisfies three properties:

1. $gcd(a, b) > 0$
2. $gcd(a, b)$ divides both $a$ and $b$
3. $gcd(a, b)$ is divisible by every common factor $f$ of $a$ and $b$

We know this number exists because $a$ and $b$ are always divisible by 1. Thus, they are guaranteed to have at least one common factor. As we also know any other factors would be natural numbers, and that natural numbers are subject to the axiom of inequality. Thus, any common factors are either 1 or different from 1, and may be sorted sequentially. If the $n$ common factors of $a$ and $b$ are denoted by $d_1$ through $d_n$, then the greatest common divisor is the divisor $d_i$ such that $d_i \geq d_j$ for all values of $j$ from 1 to $n$. Thus, the factor exists.

To show that the greatest common factor is unique, we use the third component of its formal definition. Note that this is equivalent to stating that it is the largest common factor. We prove the uniqueness by contradiction: assume that $gcd(a, b)$ is not unique, and show that this leads to a contradiction. Assume $f$ and $g$ are distinct greatest common factors of $a$ and $b$. By the third point of the definition, if $f$ is a greatest common factor of $a$ and $b$, then $f$ is divisible by every other common factor, including $g$. Thus, $f = mg$ for some integer $m$. Similarly, if $g$ is a greatest common factor, then $g = nf$ as $g$ is divisible by $f$. Thus, $f = mg = mnf$, so $mn = 1$. With that, either $m = n = 1$ or $m = n = -1$. As we know from the first part of the definition that both $f$ and $g$ are positive, then $m = n = 1$ must be the case. Thus, $f = g$, and the greatest common factor must be unique.

## 3.2 Implications of Diophantine Equations

Every equation of the form

$$ax + by = c$$

in which $a$, $b$, $c$, $x$ and $y$ are all integers requires that $c$ is divisible by the greatest common factor of $a$ and $b$. If $a$ and $b$ are relatively prime, then their greatest common factor is 1, and $c$ can then be any possible integer. Moreover, the solutions are not unique. If $x_0$ and $y_0$ are values which satisfy this equation for a given, fixed set of $a$, $b$ and $c$, then the set of values $x_n = x_0 + n\frac{b}{\gcd(a,b)}$ and $y_n = y_0 - n\frac{a}{\gcd(a,b)}$ is also a solution:

$$\begin{aligned} a\left(x_0 + n\frac{b}{\gcd(a,b)}\right) + b\left(y_0 - n\frac{a}{\gcd(a,b)}\right) &= ax_0 + by_0 + \frac{ab}{\gcd(a,b)} - \frac{ab}{\gcd(a,b)} \\ &= ax_0 + by_0 \\ &= = c \end{aligned}$$

The diophantine equation has remarkable power for developing proofs. For example, if $a$ and $c$ are relatively prime, and $c$ divides evenly into the product $ab$, then $c$ must divide into $b$. To show this, we start by noting that it is possible to create the diophantine equation

$$ax + cy = 1$$

as $a$ and $c$ are relatively prime, and thus $\gcd(a, c) = 1$. We multiply this equation by $b$ to produce

$$abx + cby = b$$

As $c$ divides into $ab$ evenly, we must have $ab = cz$ for some $z$. Thus, our equation becomes

$$czx + cby = c(zx + by) = b$$

and $c$ must divide evenly into $b$.

# 4 The Fundamental Theorem of Arithmetic

**Theorem 4.1 (Fundamental Theorem of Arithmetic)** *For every number $a$, there is a list of prime numbers $p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_N$ such that $a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_N$. This list of prime numbers is unique.*

To prove that this is the case, we must first create a framework for the methodology of this proof. This method is known as *proof by induction.*

## 4.1 Proof by Induction

The "proof by induction" methodology can be applied any time we have a statement which depends on a natural number $n$. The concept involves two basic steps:

1. Prove that the statement is true for the case $n = 1$ (or some other finite value of $n$.)
2. Prove that, if the statement is ever true for one value of $n$, it will also be true for the value $n + 1$.

In layperson's terms, this amounts to proving that a statement is true in the first case, and then proving that it will always be true in the "next" case if it's already true in one case. While our intuition says this will work, formal mathematical work needs to prove that with rigour. That proof is not particularly short, nor is it particularly illuminating. The crux of the proof is to create a set of all possible variations of the statement under scrutiny, and then create a function which maps each iteration of the statement onto the set of natural numbers in an isomorphic fashion (to use the terminology introduced in lesson eight.) This forms the formal logical backbone justifying proof by induction.

As an example, let us prove that if $p$ is prime, if $p$ divides into the product $a_1a_2a_3...a_n$ without remainder, and if $a_1, a_2, \ldots, a_n$ are integers, then there exists at least one $i$ for which $p$ divides $a_i$.

If $n = 1$, then the result is trivial. If $p$ divides $a_1$, then $p$ must divide $a_1$. This is the first step of the inductive proof. For the second part, we assume the case is true for case $n$ and show that it must be true for case $n + 1$.

For the case $n + 1$, we have that $p$ divides evenly into $a_1a_2a_3...a_na_{n+1} = (a_1a_2a_3...a_n)\,a_{n+1}$. Thus, either $p$ divides $(a_1a_2a_3...a_n)$ or it does not. If it does, the result follows from the assumption of the $n$ case. If it does not divide $(a_1a_2a_3...a_n)$, then $p$ and $(a_1a_2a_3...a_n)$ are relatively prime. We can then use the earlier result from diophantine equations to show that $p$ must divide $a_{n+1}$.

## 4.2 Proving the Fundamental Theorem of Arithmetic

In our situation, proving the Fundamental Theorem of Arithmetic, we start with the case of $a = 2$. In this case, 2 is prime, so the entire factorization is $2 = 2$. Similarly, $3 = 3$, $4 = 2^2$, $5 = 5$, $6 = 2 \cdot 3$, $7 = 7$, $8 = 2^3$, $9 = 3^2$ and $10 = 2 \cdot 5$. Thus, we have shown that the first few numbers greater than

1 all have prime factorizations. We now must show two things. First, we must complete the second half of the proof by induction to show that this will be true for all numbers higher than 10 as well. Second, we must show that this factorization is unique.

We now show that every number has at least one prime factorization. In this case, we start with number $a$. Part of the proof by induction framework is that all prior cases are assumed to be true; thus, we may assume that all numbers less than $a$ have prime factorizations. Let $a > 2$ be the number we are concerned about. If $a$ is prime, then our prime factorization is $a = a$, and our work is complete. If not, then $a$ can be written as $a = m \cdot n$. This means $a$ is divisible by both $m$ and $n$, which also means $a > m$ and $a > n$. Thus, $m$ and $n$ have prime factorizations, which we can write as $m = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ and $n = p_{r+1} \cdot p_{r+1} \cdot \ldots \cdot p_{r+k}$. Thus, we can create a prime factorization of $a$ with the simple substitution

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_r \cdot p_{r+1} \cdot p_{r+1} \cdot \ldots \cdot p_{r+k}$$

This completes the first portion of the proof: we must now prove the uniqueness of such a representation.[3] This works through a combination of proof by induction and proof by contradiction: assume that the opposite of your intended result is true, and show that this cannot be the case because of some logical contradiction. We assume at first that our number $a$ has two distinct prime factorizations:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_n$$

If we can show that $p_i = q_i$, regardless of $i$, then we can show that these values are not distinct, the lists are identical, and the factorization is unique. There is no harm in sorting these lists, so we shall assume $p_1 \leq p_2 \leq \ldots \leq p_r$ and $q_1 \leq q_2 \leq \ldots \leq q_n$.

We can manually verify that the factorization is unique for $a = 2$ in the first step of our proof by induction. Let us assume it is true for the case $a$ and then proof this implies truth of case $a + 1$. Now, if $a + 1 = p_1 \cdot p_2 \cdot \ldots \cdot p_r$, then $a + 1$ is divisible by $p_1$. Thus, by our example of proof by induction, $p_1$ divides into some number in the list $q_1 \cdot q_2 \cdot \ldots \cdot q_n$. As every $p$ and $q$ is prime, we must have the situation that $p_1 = q_i$. The same logic may be used to show that $q_1 = p_j$ for some value of $j$. However, these are sorted lists. Hence,

$$p_1 = q_i \geq q_1 = p_j \geq p_1$$

Looking at the terms on the far left and far right, we see that the $\geq$ signs are extraneous, and can be replaced by $=$ signs instead. Thus, we find that $p_1 = q_1$.

[3]This section of the proof closely follows the framework used by George E. Andrews in *Number Theory*, ISBN 0-486-68252-8.

We can then inductively apply this for each and every possible $p_2$ through $p_r$ until we have shown that $r = n$ and $p_i = q_i$ for every possible $i$. Thus, the prime factorization of any number is unique.

## 4.3 Alternative Definition of Perfect Squares

A *perfect square* is a number which, when expressed in its prime factorization, has an even number of instances of every prime factor. (Note that this number of instances is allowed to be zero.) Thus, a number $a$ is a perfect square if it can be written

$$a = p_1^{2e_1} \cdot p_2^{2e_2} \cdot \ldots \cdot p_r^{2e_r} = (p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}) \cdot (p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r})$$

In this case, the combination $x = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ is called the *square root* of $a$.

## 4.4 Counting Prime Numbers

We know from our last lesson that, if $a$ is divisible by $d$, then $a \geq d$. Thus, to see if $a$ is prime, we can compute $a \div 1$, $a \div 2$, $a \div 3$, $\ldots$, $a \div d$ and check explicitly. Instinct says that, as we reach higher and higher numbers, there are more possible factors that a given $a$ can be divided by. While this turns out to be true (for reasons we aren't even close to examining formally), it does beg a question: is it possible to run out of prime numbers? Is there, perhaps, a large but finite number of prime numbers? There is not. Centuries before the adoption of algebra or even the base ten number system, the ancient Greek mathematician Euclid proved that there are infinitely many prime numbers. His logic will be roughly reproduced here, but we'll use modern representations of the values and variables involved.

The proof is completed using the "proof by contradiction" framework as used to prove the uniqueness of a prime factorization. In this instance, assume that there are a finite number of prime numbers, and represent this finite number as $N$. The first prime can then be written $p_1$, the second as $p_2$, and so forth, until the last prime number is written $p_N$. As we are free to multiply and add our natural numbers in any arrangement we choose, we create the following:

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_N + 1$$

If you divide this $a$ by any given prime, you get remainder 1. Therefore, $a$ is not divisible by any of the existing prime numbers, and must itself be prime.

However, as $a$ is *greater* than any of the primes $p_1$ through $p_N$, we find that it *cannot* be on our list of prime numbers. Thus, our "complete" list of prime numbers must be *incomplete*. There cannot be a finite list of all prime numbers, so there must be infinitely many of them.

Beyond simply stating that there are infinitely many prime numbers, it is possible to specify an upper limit to the number of prime numbers less than or equal to a chosen $n$. However, this upper limit[4] requires the use of the "natural logarithm," and we are many, many, many lessons away from defining that function. For now, we'll have to simply be satisfied with the "infinitely many" bit we already have.

## 4.5 Identifying Prime Numbers: Sieve of Eratosthenes

Another ancient Greek mathematician names Eratosthenes is credited with developing a highly efficient means of identifying which numbers are prime, up to some highest number of interest $n$. Let us work an example with the value $n = 100$ as the highest point of interest for us. We begin by making a list of all 100 interesting numbers, which I will write in a grid format:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

Now, we eliminate 1, as it is not prime:

[4]Number $N$ of primes less than $n$: $N \leq n \ln n$

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

The next smallest number is the number 2. This is prime. Now, any number divisible by 2 cannot possibly be prime, so we delete them from the list:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | | 5 | | 7 | | 9 | |
| 11 | | 13 | | 15 | | 17 | | 19 | |
| 21 | | 23 | | 25 | | 27 | | 29 | |
| 31 | | 33 | | 35 | | 37 | | 39 | |
| 41 | | 43 | | 45 | | 47 | | 49 | |
| 51 | | 53 | | 55 | | 57 | | 59 | |
| 61 | | 63 | | 65 | | 67 | | 69 | |
| 71 | | 73 | | 75 | | 77 | | 79 | |
| 81 | | 83 | | 85 | | 87 | | 89 | |
| 91 | | 93 | | 95 | | 97 | | 99 | |

The next smallest number on our list is 3. As we have eliminated the multiples of all prime numbers which are less than 3, and 3 persists, 3 itself must be prime. We eliminate the multiples of 3 from the list:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | | 5 | | 7 | | | |
| 11 | | 13 | | | | 17 | | 19 | |
| | | 23 | | 25 | | | | 29 | |
| 31 | | | | 35 | | 37 | | | |
| 41 | | 43 | | | | 47 | | 49 | |
| | | 53 | | 55 | | | | 59 | |
| 61 | | | | 65 | | 67 | | | |
| 71 | | 73 | | | | 77 | | 79 | |
| | | 83 | | 85 | | | | 89 | |
| 91 | | | | 95 | | 97 | | | |

In doing so, we notice something odd. Half of our multiples of 3 were already eliminated. (Specifically, 6, 12, 18, and so forth.) This is because they were *also* multiples of 2, and were removed in that step. In fact, the multiples of 3 we had to remove were $3 \cdot 3$, $3 \cdot 5$, $3 \cdot 7$, $3 \cdot 9$, and so forth. In other words, we only had to eliminate numbers that were the product of 3 and numbers that were still on our list *after* eliminating the multiples of 2. Our next prime is the next smallest remaining number, which is 5. Here, multiples of 5 which are already multiples of 2 or 3 have been eliminated. Of the 19 multiples of 5 we started with, only 6 remain! The smallest one which needs to be eliminated is 25, the product of $5 \cdot 5$. This is another reason the method is so efficient: many numbers are eliminated for us with each step, making subsequent steps faster. After eliminating the multiples of 5, we have

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | | 5 | | 7 | | | |
| 11 | | 13 | | | | 17 | | 19 | |
| | | 23 | | | | | | 29 | |
| 31 | | | | | | 37 | | | |
| 41 | | 43 | | | | 47 | | 49 | |
| | | 53 | | | | | | 59 | |
| 61 | | | | | | 67 | | | |
| 71 | | 73 | | | | 77 | | 79 | |
| | | 83 | | | | | | 89 | |
| 91 | | | | | | 97 | | | |

We now eliminate the multiples of our next prime number, 7, with only three eliminations: $7 \cdot 7 = 49$, $7 \cdot 11 = 77$ and $7 \cdot 13 = 91$. This leaves:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | | 5 | | 7 | | | |
| 11 | | 13 | | | | 17 | | 19 | |
| | | 23 | | | | | | 29 | |
| 31 | | | | | | 37 | | | |
| 41 | | 43 | | | | 47 | | | |
| | | 53 | | | | | | 59 | |
| 61 | | | | | | 67 | | | |
| 71 | | 73 | | | | | | 79 | |
| | | 83 | | | | | | 89 | |
| | | | | | | 97 | | | |

Our next prime is 11. The first multiple of 11 to examine is $11 \cdot 11 = 121$, which is higher than the highest number of interest on our chart. This will be true of all numbers remaining on our chart: our highest number, 100, is a perfect square. Once we reach primes higher than 10 (as $10^2 = 100$) our list is complete. All 25 remaining numbers on this list are prime.

## 5 Upcoming Lessons

We now have division and factoring established. The next few lessons will be spent exploring algebraic rings and remainders, before eventually defining the rational numbers and algebraic fields.