THE FUNDAMENTAL THEOREM OF ARITHMETIC

BY JAMES D. NICKEL

Introduction

In mathematics, there are three theorems that are significant enough to be called "fundamental." The first theorem, of which this essay expounds, concerns arithmetic, or more properly number theory. The second fundamental theorem concerns algebra or more properly the solutions of polynomial equations, and the third concerns calculus.

Fundamental Theorems		
Arithmetic	*Algebra*	*Calculus*
Unique Prime Factorization Theorem: every composite number can be rewritten as a *unique* product of prime numbers.	Every polynomial equation over the field of complex numbers of degree higher than 1 has a complex number solution where a complex number is of the form a + bi, where a, b ∈ ℝ (set of real numbers) and i = $\sqrt{-1}$.	An indefinite integral can be reversed by differentiation.

Prime Numbers

There are *some* numbers that are *not* divisible by any other number except itself and 1. The ancient Greeks called these numbers *linear* numbers. Today we call them prime numbers.[1] For example, 2, 3, 5, 7, and 11 are prime numbers.[2]

What makes prime numbers special is that they form the "building blocks" of every other number. That is, every number that is not a prime number can be "built" out of prime numbers. Therefore, these numbers are called composite numbers.[3]

The table following provides some examples of prime numbers as building blocks of composite numbers. Notice the *unique* arrangement of the prime factors.

Composite Number	Prime Factorization	Composite Number	Prime Factorization
4	2^2	55	5×11
6	2×3	56	2^3×7
8	2^3	57	3×19
9	3^2	58	2×29
10	2×5	60	2^2×3×5
12	2^2×3	62	2×31
14	2×7	63	3^2×7

Note: This essay is extracted from a Lesson from the forthcoming textbook *Mathematics: Building on Foundations*.

[1] The Ancient Greeks could not picture linear numbers as an array of either square or rectangular dots (one dot was always left over). Prime means "first in excellence, degree, or rank."

[2] The number 1 is not considered to be prime because its only factor is 1. By definition, a prime number must have two *distinct* factors, i.e., itself and 1.

[3] Composite means "made up of distinct components."

THE FUNDAMENTAL THEOREM OF ARITHMETIC

BY JAMES D. NICKEL

Composite Number	Prime Factorization	Composite Number	Prime Factorization
15	3×5	64	2^6
16	2^4	65	5×13
18	2×3^2	66	$2\times3\times11$
20	$2^2\times5$	68	$2^2\times17$
21	3×7	69	3×23
22	2×11	70	$2\times5\times7$
24	$2^3\times3$	72	$2^3\times3^2$
25	5^2	74	2×37
26	2×13	75	3×5^2
27	3^3	76	$2^2\times19$
28	$2^2\times7$	77	7×11
30	$2\times3\times5$	78	$2\times3\times13$
32	2^5	80	$2^4\times5$
33	3×11	81	3^4
34	2×17	82	2×41
35	5×7	84	$2^2\times3\times7$
36	$2^2\times3^2$	85	5×17
38	2×19	86	2×43
39	3×13	87	3×29
40	$2^3\times5$	88	$2^3\times23$
42	$2\times3\times7$	90	$2\times3^2\times5$
44	$2^2\times11$	91	7×13
45	$3^2\times5$	92	$2^2\times23$
46	2×23	93	3×31
48	$2^4\times3$	94	2×47
49	7^2	95	5×19
50	2×5^2	96	$2^5\times3$
51	3×17	98	2×7^2
52	$2^2\times13$	99	$3^2\times11$
54	2×3^3	100	$2^2\times5^2$

To establish that this unique prime factorization exists for all composite numbers would require us to make an infinite list, a task that is impossible. So, we need to turn to a mathematical argument. We need to prove the unique prime factorization of all composite numbers as a theorem. This theorem, the *Fundamental Theorem of Arithmetic*, was practically proved by Euclid (ca. 300 BC), but the first full and correct proof is found in the *Disquisitiones Arithmeticae*, a textbook on number theory (first published in 1801), written by the prince of mathematicians, the German Carl Friedrich Gauss (1777-1855).

THE FUNDAMENTAL THEOREM OF ARITHMETIC

BY JAMES D. NICKEL

A Sketch of the Proof

The proof involves the consideration of two possibilities: Either (1) our list in the table above can be extended indefinitely so that there is a unique factorization of every composite number, or (2) at some place in this list the unique factorization property breaks down. Either Statement 1 or Statement 2 is true. Both cannot be true at the same time.[4]

We want to prove the first statement. We do so by assuming that the second statement is true and then reasoning to a contradiction. Hence, the first statement is true.

Let's now sketch our argument.[5] We assume that C is the first or *smallest* number that can be factored into primes in more than one way. Hence, we shall write two different prime factorizations for C. In the first part of our proof, we will show that none of the primes in one factorization of C occurs in the other. Once we have established this, if C indeed has two different prime factorizations, all the primes in one would be *different* from all the primes in the other. In the second part of our proof, we will construct a number D such that D < C which also has two different factorizations into primes. By doing so, we have contradicted our assumption that C is the *smallest* number that can be factored into primes in more than one way. This contraction shows that Statement 2 is false. Hence, Statement 1 must be true; i.e., every composite number has a unique prime factorization. QED!

Carl Friedrich Gauss (Public Domain)

The Proof: Part 1

We assume that C is the first or *smallest* number that can be factored into primes in more than one way. Hence, we shall write two different prime factorizations for C:

$$C = p_1p_2p_3 \cdots p_n \text{ (First list)}$$
$$C = q_1q_2q_3 \cdots q_m \text{ (Second list)}$$

What do we mean by this notation? It means that C can be factored into primes p_1, p_2, …, p_n. and that there is also another way of factoring C into the primes q_1, q_2, …, q_m. We cannot assume that the number of primes in both lists are the same; i.e., n = m. Also, p_1 does not stand for the first prime number, i.e., 2, and p_2 does not stand for the second prime number; i.e., 3. p_1 stand for some prime number. p_2 stands for another prime number. It may be true that $p_2 = p_1$, but it is not necessarily true; i.e., it may be that $p_2 \neq p_1$.

We now have to show that list of primes p_1, p_2, …, p_n are entirely different from q_1, q_2, …, q_m. This means, for example, if the prime number 11 is in the first list it *cannot* be in the second list. Let's now suppose that the two lists had a prime number in common. We could then rearrange the ordering of each list so that the prime number in common would be the first one in each; i.e., $p_1 = q_1$. Since $p_1 = q_1$, we can conclude:

$$C = p_1p_2p_3 \cdots p_n$$
$$C = p_1q_2q_3 \cdots q_m$$

Dividing both equations by p_1, we get:

---

[4] In logic, this conclusion results from the Law of the Excluded Middle, a transcendental law that states that a formal proposition is either true or false.

[5] There is more than one way to prove this theorem. I am following the logic of Ivan Niven, *Numbers: Rational and Irrational* (New York: Random House, 1961), pp. 117-121.

THE FUNDAMENTAL THEOREM OF ARITHMETIC

BY JAMES D. NICKEL

$$\frac{C}{p_1} = p_2 p_3 \cdots p_n$$
$$\frac{C}{p_1} = q_2 q_3 \cdots q_m$$

This means that we have two *different* prime factorizations of the number $\frac{C}{p_1}$ because we began with two different prime factorizations of C. Do you see why this is impossible? We choose C as the *smallest* number having more than one prime factorization, but $\frac{C}{p_1} < C$!

We have now established that none of the primes in one factorization of C, $p_1, p_2, \ldots, p_n$, occurs in the other, $q_1, q_2, \ldots, q_m$.

The Proof: Part 2

Since none of the primes in one factorization of C, $p_1, p_2, \ldots, p_n$, occurs in the other, $q_1, q_2, \ldots, q_m$, we know that $p_1 \neq q_1$. Since $p_1 \neq q_1$, either $p_1 < q_1$ or $p_1 > q_1$. We will assume that $p_1 < q_1$ and argue to our conclusion realizing that we could also start with $p_1 > q_1$ and come to the same conclusion with the same argument.

We now assume that $p_1 < q_1$ and then show that there exists another number, D, having two different prime number factorizations where D < C. If we can do this, we have contradicted our assumption that C is the *smallest* number with more than one prime factorization proving thereby the *Fundamental Theorem of Arithmetic*. Let's proceed!

We construct D is follows:

$$D = (q_1 - p_1) q_2 q_3 \cdots q_m$$

Note that D is the product of $(q_1 - p_1)$ and the primes $q_2, q_3, \ldots, q_m$. Hence, D can also be written as a difference:

$$D = q_1 q_2 q_3 \cdots q_m - p_1 q_2 q_3 \cdots q_m \Leftrightarrow$$
$$D = C - p_1 q_2 q_3 \cdots q_m \Leftrightarrow$$
$$D + p_1 q_2 q_3 \cdots q_m = C$$

Since $p_1 q_2 q_3 \cdots q_m > 0$, then D < C.

We are rounding third base and heading for home! We have one more relationship to prove; i.e., that D has two different prime number factorizations.

Note again that $D = (q_1 - p_1) q_2 q_3 \cdots q_m$. Each of the factors $q_2, q_3, \ldots, q_m$ is prime but the first factor, $q_1 - p_1$, is not necessarily prime. If $q_1 - p_1$ could be factored into primes, we would have a factoring of D into primes which *would not include the prime p_1 as one of its factors*. Why? First note that p_1 is not in the list $q_2, q_3, \ldots, q_m$ because we established this in Part 1 of our proof. Second, if $q_1 - p_1$ is factored into primes, p_1 would not be one of its factors. Why? If p_1 were a factor in the prime factorization of $q_1 - p_1$, then p_1 would be a divisor of $q_1 - p_1$. In other words, there a number x would exist such that:

$$x = \frac{q_1 - p_1}{p_1} \Leftrightarrow$$

$$q_1 - p_1 = p_1x \Leftrightarrow$$
$$q_1 = p_1 + p_1x \Leftrightarrow$$
$$q_1 = p_1(1 + x)$$

If $q_1 = p_1(1 + x)$, we have a problem. This equation states that p_1 is a divisor of q_1. This is impossible because a prime number cannot be the divisor of another prime number!

Next, we need to show that D can also be factored in another way s*o that p_1 is one of its prime factors*. To do this, we remind ourselves that:

$$D = C - p_1q_2q_3 \cdots q_m$$

Since $C = p_1p_2p_3 \cdots p_n$, then $D = p_1p_2 \cdots p_n - p_1q_2q_3 \cdots q_m = p_1\left(p_2p_3 \cdots p_n - q_2q_3 \cdots q_m\right)$.

The number within the parentheses, $p_2p_3 \cdots p_n - q_2q_3 \cdots q_m$, is not necessarily prime. If we could factor it into primes, we would have a prime factorization of D that *includes* p_1. Thus, we have demonstrated two prime factorizations of D or two ways to obtain such a factorization, one *without* the prime p_1 and one *with* the prime p_1. Another way to state this is that D, where $D < C$, has two *different* prime factorizations.

QED!

You really have to be on your "logical toes" to follow this line of reasoning. Even though this argumentation is challenging, its beauty is revealed in every step of its unfolding.

Conclusion

This logical argument gives you a flavor of how mathematicians develop proofs in number theory. Number theory is a substantial part of mathematics and many mathematicians (particularly university professors) devote all their time to the study of various aspects of this branch of mathematics. If this method of reasoning is intriguing or fascinating to you, then you might prayerfully consider mathematics in terms of your vocational calling under God. Number theory is not just theory; it has some important applications. See the essay entitled *Keeping Secrets* at http://www.biblicalchristianworldview.net/Mathematical-Circles/keepingSecrets.pdf for one example of the application of number theory in the modern computer world.