Fundamental Theorem of Arithmetic

Even though this is one of the most important results in all of Number Theory, it is rarely included in most high school syllabi (in the US) formally. Interestingly enough, almost everyone has an intuitive notion of this result and it is almost always informally covered in middle school mathematics classes in the United States.

The Fundamental Theorem of Arithmetic simply states that each positive integer has a unique prime factorization. What this means is that it is impossible to come up with two distinct multisets of prime integers that both multiply to a given positive integer.

To prove this, we must show two things:

1) Each positive integer can be prime factorized.
2) Each prime factorization is unique.

To see the first fact, let $m>1$ be the smallest positive integer which does NOT have a prime factorization. Since m is not a prime number, we can write m as a product of two factors, m_1 and m_2. But, since both of these are smaller than m, they DO have prime factorizations. Thus, m can be expressed as the product of these two factorizations, which creates a prime factorization contradicting the assumption that m does not have one.

Before I continue with the second part of this proof, I want to introduce pi notation, which is very similar to sigma notation:

$$\prod_{i=1}^{n} f(i) = f(1) * f(2) * f(3) * \ldots * f(n-1) * f(n)$$

The only difference between pi notation and sigma notation is that each designated term is multiplied instead of added.

Also, I want to prove the two following lemmas:

1) If p is prime and a and b are positive integers and p | ab, then either p | a or p | b.

2) If p is prime and a_i for $1 \leq i \leq n$, are positive integers, and if $p \mid a_1 a_2 \ldots a_n$ then $p \mid a_i$ for some $1 \leq i \leq n$.

Proof of #1:

If p | a, we are done. Now consider the situation where p does NOT divide evenly into a. In this case, we must have that gcd(p, a) = 1. (This gcd can not be p, and p has no other possible factors, so the gcd must be 1.) Thus, there exist integers x and y such that px + ay = 1. Thus, b = b(px+ay). We can rewrite this as b = (bx)p + (ab)y. Since we know that p | p and p | ab, it follows that p | b, since b is expressed as a linear combination of p and ab.

Proof of #2

Use induction on n. We know the statement is true for n=1 and n=2. So, this takes care of the base case. Assume for n=k, we have that

If p is prime and a_i for $1 \leq i \leq k$, are positive integers, and if $p \mid a_1a_2 \ldots a_k$ then $p \mid a_i$ for some $1 \leq i \leq k$.

Now, we must prove for n= k+1 that

If p is prime and a_i for $1 \leq i \leq k+1$, are positive integers, and if $p \mid a_1a_2 \ldots a_{k+1}$ then $p \mid a_i$ for some $1 \leq i \leq k+1$.

If we have that $p \mid a_1a_2 \ldots a_k$, then using the inductive hypothesis, we can conclude that $p \mid a_i$ for some $1 \leq i \leq k$.

Otherwise, we have that p doesn't divide evenly into $a_1a_2 \ldots a_k$, so we then have that $\gcd(p, a_1a_2 \ldots a_k) = 1$.

Thus, there exists integers x and y such that

$$px + a_1a_2 \ldots a_k y = 1 \text{ so,}$$

$$a_{k+1}(px + a_1a_2 \ldots a_k y) = a_{k+1}$$

$$(a_{k+1}x)p + (a_1a_2 \ldots a_{k+1})y = a_{k+1}$$

Since we have that $p \mid p$ and that $p \mid (a_1a_2 \ldots a_{k+1})$, it follows that $p \mid a_{k+1}$ as desired.

Now, to prove the second part of the Fundamental Theorem of arithmetic. Assume to the contrary and let n be the smallest positive integer for which there are two disctinct prime factorizations. Thus we have the following:

$$n = \prod_{i=1}^{\infty} p_i^{a_i} = \prod_{i=1}^{\infty} p_i^{b_i}$$

Now, let k be the smallest value for which $a_k > 0$. Then we must have that $p_k \mid n$. Since this is the case, and we know that p_k does not divide into ANY of the other primes listed thus, it follows that $b_k > 0$. But if this is the case, then we can divide both prime factorizations by p_k which leads to the following:

$$\frac{n}{p_k} = (\prod_{i=1}^{\infty} p_i^{a_i}) / p_k = (\prod_{i=1}^{\infty} p_i^{b_i}) / p_k$$

But, we know that the integer n/p_k has an unique prime factorization since we had assumed that n was the smallest integer without one. Thus it follows that the two prime factorizations above are identical. If that is the case, then it follows that our two distinct prime factorizations for n were not distinct at all.

Here are a couple more classic proofs from Number Theory:

The square root of 2 is irrational.

We will use proof by contradiction here.

Assume that $\sqrt{2}$ is a rational number. Then we can express $\sqrt{2}$ as a fraction of integers in lowest terms. Let $\sqrt{2} = a/b$, where gcd(a,b) = 1. (We can do this because if we pick a and b such that their gcd is NOT 1, we can divde both integers by their gcd.)

$\sqrt{2} = a/b$

$2 = (a/b)^2$, from squaring both sides.
$2a^2 = b^2$, since 2 is prime, we must have that 2 | b

Let b = 2b':

$2a^2 = (2b')^2$
$2a^2 = 4b'^2$
$a^2 = 2b'^2$, once again since 2 is prime, we must have that 2 | a.

But wait, there's a problem with that deduction. If, 2 | a and 2 | b, then the gcd(a,b) > 1. This contradicts the given information, so our initial assumption, that $\sqrt{2}$ is a rational number, is incorrect. Thus, $\sqrt{2}$ must be an irrational number.

Now we will prove that there are an infinite number of prime numbers.

Use proof by contradiction: Assume the contrary, that there are a finite number of prime numbers. In that case, they can all be listed in increasing order. Let this list be: $p_1, p_2, \ldots, p_n$.

But, consider the number $(\prod_{i=1}^{n} p_i) + 1$. None of the listed prime numbers divide into it. So, there are only two possible conclusions:

1) The number itself is prime.
2) The number can be written as a product of multiple numbers that are prime.

But either way, the prime numbers we obtain from this number CAN NOT be on our original list, which contradicts the fact that our original list contained ALL the prime numbers.

As an example, consider the list of prime numbers 2, 3, 5, 7. Now consider the number (2)(3)(5)(7) +1 = 211. This number turns out to be prime. Even if it didn't, it would have prime factors, but those factors could not be any of the numbers on the list.

Least Common Multiple

The least common multiple of two integers is the smallest integer that is a multiple of both integers. Consider the following examples:

lcm(12, 18) =36, since 12 | 36, 18 | 36 and 36 is the smallest integer to satisfy these constraints. (To see this, notice that the only smaller multiple of 18 is 18, which is NOT divisible by 12.)

lcm(15, 35) = 105 and
lcm(17, 19) = 323

Although there is no common algorithm typically taught similar to Euclid's algorithm to find the LCM of two integers, this can also be determined via Euclid's algorithm and one fact that we will prove about the relationship between the LCM of two integers and the GCD of two integers.

Given the prime factorization of two integers a and b, we can determine the LCM of the two integers as follows. Let

$$a = \prod_{i=1}^{\infty} p_i^{a_i} \qquad \textbf{and} \qquad b = \prod_{i=1}^{\infty} p_i^{b_i}$$

Then we have that the lcm(a,b) is

$$\prod_{i=1}^{\infty} p_i^{\max(a_i, b_i)}$$

To prove this is we need to verify two things:

1) That the value above is a common multiple
2) That it is the smallest possible common multiple.'

Clearly it is a common multiple because each prime number appears in the number above at least as many times as it does in either a or b.

But, we can also show that no smaller number is possible because the minimum number of times a particular prime number must appear in the prime factorization of the lcm of a and b is precisely the maximum of the number of times it appears in either. The reasoning is as follows:

If a | b and b | c then a | c.

We know that a is divisible by p^k, and we are know that lcm(a,b) is divisible by a. Thus it follows that p^k | lcm(a,b).

This reasoning holds for each prime, this we can see that the value above is a divisor of any multiple of a and b, proving its minimality.

Using similar reasoning, we can show that the gcd(a,b) can be expressed as:

$$\prod_{i=1}^{\infty} p_i^{\min(a_i, b_i)}$$

Now, with these two results, we can show the following:

ab = gcd(a,b)*lcm(a,b).

To see this, simply compute the product on the right:

gcd(a,b)*lcm(a,b) =

$$\prod_{i=1}^{\infty} p_i^{\min(a_i,b_i)} * \prod_{i=1}^{\infty} p_i^{\max(a_i,b_i)} =$$

$$\prod_{i=1}^{\infty} p_i^{\min(a_i,b_i)+\max(a_i,b_i)} =$$

$$\prod_{i=1}^{\infty} p_i^{a_i+b_i} =$$

$$\prod_{i=1}^{\infty} p_i^{a_i} p_i^{b_i} =$$

$$\prod_{i=1}^{\infty} p_i^{a_i} * \prod_{i=1}^{\infty} p_i^{b_i} =$$

ab

As an exercise, use this result to compute the LCM(45, 120).

Number of Divisors of an Integer

Using the Fundamental Theorem or arithmetic, every positive integer n can be expressed as follows:

$$n = \prod_{p_i \in Primes} p_i^{a_i}$$

Notice that an arbitrary divisor, d, of n must have the form:

$$d = \prod_{p_i \in Primes} p_i^{d_i}$$

where, for all i, $0 \leq d_i \leq a_i$. This means, that for each d_i, we have precisely a_i+1 choices for what it could be: 0, 1, 2, 3, …, a_i.

It follows that $\tau(n)$, the sum of divisors of n, can be expressed as follows:

$$\tau(n) = \prod_{p_i \in Primes} (a_i + 1)$$

Let's consider a simple example, $n = 2^3 \times 3^4$. All divisors of n take the form 2^a3^b with $0 \leq a \leq 3$ and $0 \leq b \leq 4$. We can make a table of these divisors as follows:

a/b	0	1	2	3	4
0	$2^0 3^0$	$2^0 3^1$	$2^0 3^2$	$2^0 3^3$	$2^0 3^4$
1	$2^1 3^0$	$2^1 3^1$	$2^1 3^2$	$2^1 3^3$	$2^1 3^4$
2	$2^2 3^0$	$2^2 3^1$	$2^2 3^2$	$2^2 3^3$	$2^2 3^4$
3	$2^3 3^0$	$2^3 3^1$	$2^3 3^2$	$2^3 3^3$	$2^3 3^4$

This $n = 8 \times 81 = 648$ has $(3 + 1)(4 + 1) = 4 \times 5 = 20$ divisors.

Parity of the Number of Divisors

If we example the formula for the number of divisors of an integer n: $\prod_{p_i \in Primes}(a_i + 1)$, we see that this product is odd if and only if each of the a_i's is even. Namely, if each of the a_i's is even, the number n is a perfect square. This means that all positive integers that are perfect squares have an odd number of divisors, and all other integers have an even number of divisors.

We can also see this fact by attempting to pair of divisors of an integer.

Let's consider a couple example cases n = 36 and n = 48

36 = 1 x 36	**48 = 1 x 48**
= 2 x 18	**= 2 x 24**
= 3 x 12	**= 3 x 16**
= 4 x 9	**= 4 x 12**
= 6 x 6	**= 6 x 8**

In both cases, we see that we generate divisors in pairs, d and n/d. Thus, the number of divisors will be even, UNLESS, in that last pair, d = n/d. Of course, this occurs if and only if $n = d^2$ for a positive integer d, which means that n is a perfect square!

A consequence of this observation, that divisors of an integer come in pairs is that if an integer, n, is composite (not prime and greater than 1), then it must have a divisor greater than 1 and less than or equal to the square root of n. We can prove this fact as follows, via contradiction:

Assume to the contrary that some integer n is composite, but has no integer divisor less than or equal to $\sqrt{n}$. Since n is composite, there exist two integers (neither equal to 1 or n), a and b, such that

$$n = ab > \sqrt{n}\sqrt{n} = n$$

Clearly, n being greater than n is a contradiction. It follows that our assumption is incorrect and that n must have at least one divisor less than or equal to its square root.

In the previous example, intuitively, when we list pairs of divisors, one is less than or equal to the square root and the other one is greater than or equation to the square root.

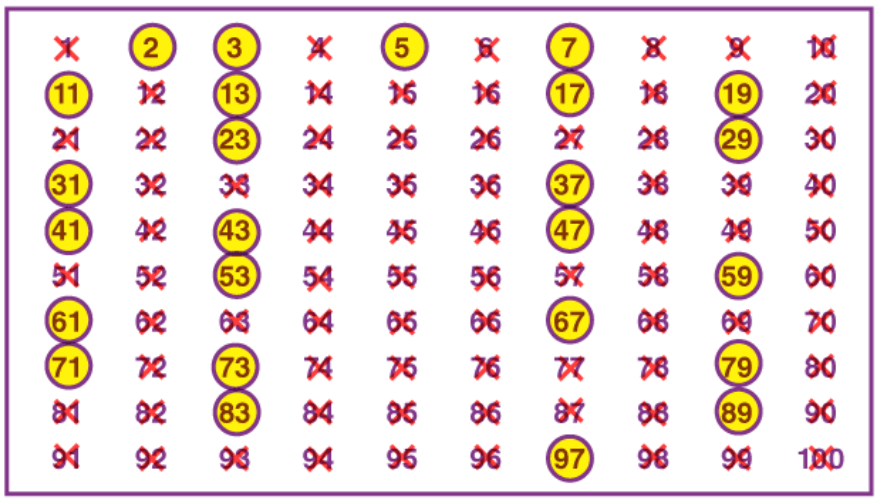
Primality Test

This means, that if we want to test to see if an integer is prime or not, we just need to try to divide it by primes (if we happen to know these already) until the square root of the number. If none divide in evenly, then the number is prime. Consider determining if 239 is prime:

239 is not divisible by 2 (remainder 1)
239 is not divisible by 3 (remainder 2)
239 is not divisible by 5 (remainder 4)
239 is not divisible by 7 (remainder 1)
239 is not divisible by 11 (remainder 8)
239 is not divisible by 13 (remainder 5)

We can stop because the next prime, 17 is greater than the square root of 239.

If we want to generate all of the primes up to a given integer n, we can run the Sieve of Eratosthenes. We write down all the integers from 1 to n. Then we go to 2, circle it (it's prime), then cross off all of its multiples greater than 2 (all other evens). Then, we go to the next uncrossed number (3), and circle it. Followed by crossing off all of its multiples. We continue in this fashion circling each future uncrossed number, followed by crossing off its larger multiples.



Sum of Divisors of an Integer

Continue using the notation as before, and let's build off of the previous example, $n = 2^3 \times 3^4$. Let's look at the table of divisors:

a/b	0	1	2	3	4
0	$2^0 3^0$	$2^0 3^1$	$2^0 3^2$	$2^0 3^3$	$2^0 3^4$
1	$2^1 3^0$	$2^1 3^1$	$2^1 3^2$	$2^1 3^3$	$2^1 3^4$
2	$2^2 3^0$	$2^2 3^1$	$2^2 3^2$	$2^2 3^3$	$2^2 3^4$
3	$2^3 3^0$	$2^3 3^1$	$2^3 3^2$	$2^3 3^3$	$2^3 3^4$

Now, let's consider adding these divisors (in the center of the table).

Notice that for each row, we can factor out a term of the form 2^i. So, the sum of the first row is:

$$2^0(3^0 + 3^1 + 3^2 + 3^3 + 3^4)$$

Similarly, the sums of the second, third and fourth rows are:

$$2^1(3^0 + 3^1 + 3^2 + 3^3 + 3^4)$$
$$2^2(3^0 + 3^1 + 3^2 + 3^3 + 3^4)$$
$$2^3(3^0 + 3^1 + 3^2 + 3^3 + 3^4)$$

When we go to add each of these sums, we can factor out

$$(3^0 + 3^1 + 3^2 + 3^3 + 3^4)$$

yielding the expression:

$$(2^0 + 2^1 + 2^2 + 2^3)(3^0 + 3^1 + 3^2 + 3^3 + 3^4)$$

Both of these are geometric sums, thus we can express this product more succinctly as:

$$\frac{(2^4 - 1)}{(2 - 1)} \times \frac{(3^5 - 1)}{(3 - 1)}$$

In general, even if we have more than two distinct prime factors, we can list the sum of each possible divisor as the product of sums, where each sum is each unique prime factor raised to each power from 0 through a_i, where $p_i^{a_i}$, is the term for prime p_i in the prime factorization of the integer.

It follows that, if

$$n = \prod_{p_i \in Primes} p_i^{a_i}$$

then $\sigma(n)$, the sum of divisors of n is:

$$\sigma(n) = \prod_{p_i \in Primes} \frac{(p_i^{a_i+1} - 1)}{(p_i - 1)}$$

Number of times a prime p divides evenly into n!

Let's try to figure this out for a specific example: How many times does the prime number 2 divide evenly into 12!

n = 12, p = 2

n! = 12! = 1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12

Imagine crossing off each number that has a factor of 2. These show up every other integer.

1 x ~~2~~ x 3 x ~~4~~ x 5 x ~~6~~ x 7 x ~~8~~ x 9 x ~~10~~ x 11 x ~~12~~
1 2 3 4 5 6

So far we've divided 2 into 12! 6 times. This is 12/2 using integer division.

When we did this, we generated new integers that were 1 through 6 which might have new factors of 2. All the numbers we didn't cross off will never generate a factor of 2:

1 x ~~2~~ x 3 x ~~4~~ x 5 x ~~6~~ x 7 x ~~8~~ x 9 x ~~10~~ x 11 x ~~12~~
1 ~~2~~ 3 ~~4~~ 5 ~~6~~
1 2 3

Now I've divided out an addition 3 copies of 2. This is 6/2 using integer division.

1 x ~~2~~ x 3 x ~~4~~ x 5 x ~~6~~ x 7 x ~~8~~ x 9 x ~~10~~ x 11 x ~~12~~
1 ~~2~~ 3 ~~4~~ 5 ~~6~~
1 ~~2~~ 3
1

So, we have now canceled 1 additional copy 2, for a total of 6 + 3 + 1 = 10.

2 | 12
2 | 6 **6 + 3 + 1**
2 | 3
2 | 1
0

So, essentially, we continue this process, crossing off new multiples that might be leftover after a round of cross offs. After each round, the new integers that remain are a smaller range [1..n/p] as compared to [1..n] from the previous round. We continue rounds until our range shrinks to be less than p.

Formally, the following formula is the number of times the prime number p divides evenly into n!:

$$\sum_{i=1}^{n} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Is the number of times a prime number p divides evenly into n!

By hand I did 12/2 + 6/2 + 3/2 (int div)
The formula does 12/2 + 12/4 + 12/8 (int div)
These are equivalent.

To answer the question: how many zeroes are at the end of n!, notice that we need to answer the number of times 2 divides evenly into n! and the number of times 5 divides evenly into n! Whichever is smaller (the latter one) is the answer to the question, how many 0s are at the end of n! Let's try one quick example:

How many 0s are at the end of 800 factorial?

This is the same as the answer to the question, how many times does 5 divide evenly into 800!

5 | 800
5 | 160
5 | 32
5 | 6
1

Answer = 160 + 32 + 6 + 1 = 199