# Prime factorization

We will prove that every integer has a unique *prime factorization*. This is also called *the fundamental theorem of arithmetic*.

$$n = p_1 \cdot p_2 \ldots p_k$$

In the list of the prime factors of $n$, a factor may be repeated.

Example:

$$12 = 2 \cdot 2 \cdot 3$$

To compare two factorizations for uniqueness, we suppose they are sorted (say, from smallest to greatest).

More examples for relatively small numbers:

```
 39  = 3.13
144  = 2.2.2.2.3.3
210  = 2.3.5.7
2310 = 2.3.5.7.11
```

Sometimes the factors can be hard to find.

Example:

Let's try 123456789. By using the digit addition trick, we can tell that this number is divisible by 9 (I get $9 + 9 + 9 + 9 + 9$).

At first it seems easy. I found two factors of 3, leaving 13717421.

Then my luck ran out. The smallest prime factor was too large for me to find by hand. So I used Python.

`https://gist.github.com/telliott99/3043a0d9ddc44f8503c83c848b2f8382`

3607 and 3803 are the two prime factors of that number, which once found, are easily confirmed. Factoring is a hard problem.

### background

We will prove the unique prime factorization theorem.

But before starting on that, when we say that one integer *evenly divides* another one, written as $a|n$ or $a$ is a factor of $n$, we mean there exists another integer $k$ such that

$$a \cdot k = n$$

$a$ times $k$ is exactly equal to $n$ with no remainder.

Take care to distinguish $a|b$ ($a$ divides $b$) from $a/b$ ($a$ divided by $b$).

If there is also a number $m$ where $a$ evenly divides $m$, we write $a|m$ and mean that

$$a \cdot j = m$$

Addition or subtraction of $m + n$ gives

$$m + n = a \cdot j + a \cdot k = a(k + j)$$

$$m - n = a \cdot j - a \cdot k = a(k - j)$$

- If $a|m$ and $a|n$, $a$ also divides their sum or difference.

We rely on this fact below.

Also, we can manually check all the numbers up to some reasonable lower limit, like 100. They all have unique prime factorizations. Therefore, if there is a number with two such factorizations, it is larger than 100, and there must be a smallest such number.

### abnormal numbers

Hardy and Wright (*Theory of Numbers*, sect. 2:11) have a proof of prime factorization which I find quite elegant.

*Proof.*

By contradiction.

Hardy:

> Let us call numbers which can be factored into primes in more than one way, *abnormal*, and let $n$ be the smallest abnormal number.

Start by supposing that there are two different factorizations of $n$:

$$n = p_1 \cdot p_2 \ldots p_k$$

and

$$n = q_1 \cdot q_2 \ldots q_j$$

where the $p$'s and $q$'s are all primes.

### Different factorizations

As a preliminary result, consider the possibility that some factor appears in both factorizations, that some $p$ is equal to a $q$.

Let us rearrange if necessary so the shared factor is listed first: let $p_1 = q_1$ and

$$n = p_1 \cdot p_2 \ldots p_k$$

$$n = p_1 \cdot q_2 \ldots q_j$$

But now, $n/p_1$ ($n$ divided by $p_1$) is abnormal, because it has two different prime factorizations.

That is impossible, because $n$ is the smallest abnormal number.

Therefore, no $p$ is a $q$ and no $q$ is a $p$. If there exist abnormal numbers with two factorizations, those factorizations must be completely different.

### inequality

We may take $p_1$ to be the least $p$ and $q_1$ to be the least $q$. In this part, we establish that $p_1 \cdot q_1 < n$.

Since $n$ is composite, either

- $p_1 \cdot p_1 = n$, or
- $p_1$ times some number larger than $p_1$ is equal to $n$.

In the second case, $p_1 \cdot p_1 < n$.

A similar result holds for $q_1$.

But, since $p_1 \neq q_1$, only one of $p_1$ or $q_1$ at most, can be squared to give $n$. Either $p_1 \cdot p_1 < n$ or $q_1 \cdot q_1 < n$ or perhaps both are true.

From this it follows that

$$p_1 \cdot q_1 < n$$

**the contradiction**

Let

$$N = n - p_1 q_1$$

We know that $0 < p_1 q_1 < n$ because of the last section, and because neither is equal to zero.

Therefore $0 < N < n$ also.

We know that $N$ is not abnormal (because $n$ is the smallest abnormal number).

We're given that $p_1 | n$ and so, from the above equality

$$N = n - p_1 q_1$$

and our preliminary result about what factorization means, it must be that $p_1 | N$. The same is true for $q_1$, namely $q_1 | N$.

Hence both $p_1$ and $q_1$ appear in the unique factorization of $N$, so $p_1 q_1 | N$.

Certainly, $p_1 q_1$ divides itself, so it follows that $p_1 q_1 | n$, using our preliminary result about factorization.

Hence, $q_1 | (n/p_1)$.

But $n/p_1$ is less than $n$ and has the unique prime factorization $p_2 \cdot p_3 \ldots p_k$.

Since $q_1$ is not a $p$, this is impossible.

Hence there cannot be any abnormal numbers.

□

As we said, this is *fundamental theorem of arithmetic*, so it's worth a bit of effort for the proof.