Behind The Fundamental Theorem Of Arithmetic

We call a c a common multiple of a , b if there are m , n so that $c = m a = n b$ and we call m , n as the multipliers in c. The k-th common multiple of a , b will be denoted as c_k and the multipliers in it as m_k and n_k. So $c_k = m_k a = n_k b$.

In particular, $c_1 = m_1 a = n_1 b$ is the first or smallest common multiple.

The basic fact we prove is : $c_k = k\ c_1$. This then obviously implies:

$$m_k = \frac{c_k}{a} = \frac{k c_1}{a} = \frac{k m_1 a}{a} = k\ m_1 \quad \text{and} \quad n_k = \frac{c_k}{b} = \frac{k c_1}{b} = \frac{k n_1 b}{b} = k\ n_1 .$$

Any u number under c_1 gives a positive remainder to a or b because by definition there is no common multiple under c_1. Also trivially $k\ c_1$ is a common multiple.

So for this to be the k-th means that there are no common multiples between any $k\ c_1$ and $(k + 1)\ c_1$. That is, $k\ c_1 + u$ can not be a common multiple with u being under c_1.

And indeed, the remainders of this to a and b are the same as of u for which we saw that at least one of them is positive. Now we get a special consequence of this basic fact.

For any d common divider of a and b , $\frac{a\,b}{d}$ is a common multiple with $\frac{b}{d}$ and $\frac{a}{d}$ as multipliers in it because $\frac{b}{d}\ a = \frac{a}{d}\ b = \frac{a\,b}{d}$. Thus $\frac{a\,b}{d} = c_{k_d}$ and then by our result :

$\frac{b}{d} = k_d\ m_1$ and $\frac{a}{d} = k_d\ n_1$. So $b = d\,k_d\ m_1$, $a = d\,k_d\ n_1$ so $d\,k_d$ is a common divider too.

Thus for the g greatest common divider k_g has to be 1. And so $\frac{a\,b}{g} = c_1$.

If $g = 1$ then $c_1 = a\,b$ so $m_1 = b$, $n_1 = a$ and $m_k = k\,b$, $n_k = k\,a$.

Thus we proved the following:

If a , b are numbers that have only 1 as common divider and $m\,a = n\,b$ then there is a k that $m = k\,b$ and $n = k\,a$. This is enough to prove our title theorem.

An a number is undividable if it only has the trivial dividers 1 and itself a.

Such numbers are : 1 , 2 , 3 , 5 , 7 , 11 , . . . The rest of the numbers: 4 , 6 , 9 , 10 , 12 , . . . are called composites. They can be divided by smaller numbers and so indeed “decomposed”.

For example $4 = 2 \cdot 2$, $6 = 2 \cdot 3$. The earlier $m\,a = n\,b$ can also be said as a divides $n\,b$.

If a is undividable, we can use our results for $m\,a = b_1\,b_2\ .\ .\ b_N$, that is when a divides a product in general. Then quite simply: a must divide one of the b-s. The logic is simple:

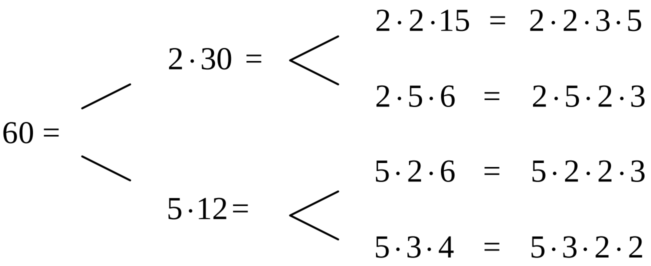
If a doesn’t divide b_1 then a and b_1 can not have any common divider beside 1 because a has no other option. So then $b_2\ .\ .\ .\ b_N$ can be regarded as n in our last result and so it must be $k\,a$. So a divides $b_2\ .\ .\ .\ b_N$. Now again if a doesn’t divide b_2 we get that it must divide $b_3\ .\ .\ .\ b_N$. And so on, eventually a must divide one of them.

The next step is if $m\,a = b_1\ b_2\ .\ .\ .\ b_N$ but the b-s are all undividable too.

Here we encounter an interesting difference. The 1 undividable number divides everything, but all others only divide themselves. So if a , b_1 , b_2 , ... , b_N are non 1 undividables then $m\,a = b_1\ b_2\ .\ .\ .\ b_N$ actually means that a has to be one of the b-s.

Finally, we generalize the left side too, that is regard $a_1\ a_2\ .\ .\ .\ a_M = b_1\ b_2\ .\ .\ .\ b_N$ with all non 1 undividables. Then the two sides must be the same except in order.

Indeed, now again we can step by step use our previous result. So using $a_2\ .\ .\ .\ a_M$ as m and a_1 as a, we get that a_1 has to be one of the b-s. Dividing both sides with this we can use our result again and again. This result means that the non 1 undividables that we call primes are unique final dividers of all numbers. And indeed, watching the different decompositions of numbers, we always end up with same final primes:



The non 1 dividers of a number are also called its factors and so our result is known as the: “Unique Prime Factorization Theorem” or “Fundamental Theorem Of Arithmetic”.

The used fact that for a , b having only 1 as common divider, $m\,a = n\,b$ implies a k so that $m = k\,b$, $n = k\,a$ can be proven by a direct method that avoids the common multiples.
This fact by the way to have only 1 as common divider is called as being relative primes.
And this direct method is called induction. It starts with proving the claim for some initial values and here $a = b =1$ are perfect. Indeed, they are obviously relative primes and our claim is trivial because $m\,a = n\,b$ means $m = n$. So such k is the $m = n = k$ value because: $m = k\cdot 1$ and $n = k\cdot 1$. Our claim inherits from this trivial case to all higher values.
To see this, assume that it already inherited to all possible a , b values under a $v > 1$.
Now we show how it inherits to using v for a or b.
Both a and b can not be used as v because then v would be a common divider > 1.
So only the bigger of them say b is v while $a < b = v$.
The $b - a$ difference is also under v and we want to use our claim for the a , $b - a$ pair.
They being under v is not enough, they have to be relative primes. And indeed, any d common divider of a and $b - a$ divides $a + b - a = b$, so if a and b had only 1 as such d then the same is true for a and $b - a$. So indeed, our claim is true for the a , $b - a$ pair.
That is, $M\,a = N\,(b - a)$ implies a k that $M = k\,(b - a)$ and $N = k\,a$.
Now suppose that for our a , b pair we have $m\,a = n\,b$. Subtracting $n\,a$ from both sides, we get $m\,a - n\,a = n\,b - n\,a$ that is $(m - n)\,a = n\,(b - a)$. So we have our previous M , N with $M = m - n$ and $N = n$. So for a k : $m - n = k\,(b - a) = k\,b - k\,a$ and $n = k\,a$ so $m = k\,b$.
So the k we found for a , $b - a$ is good for a , b too. This proves the inheritance.

We might ask if a direct proof by induction is also possible for the U.P.F.T. itself.

The exact claim seems to be that if we have a number prime factorized in two ways as:
$a_1\ a_2 \ldots a_M = b_1\ b_2 \ldots b_N$ then the a-s and b-s are the same except in order.
But a better version is the negative claim that if two $A = a_1\ a_2 \ldots a_M$ and $B = b_1\ b_2 \ldots b_N$ prime products are not mere rearrangements then they can not be equal, $A \neq B$.
This advantage becomes clear from our inductive proof.
For small values the inequality of non rearranged prime products is an experimental fact, and it should feel as a mere coincidence. For example $2\cdot 5 \neq 3\cdot 3$ but the difference is only 1.
Regrading the primes themselves as their own prime factorization, we can say that all numbers after 1 have a single combination of primes with possible repetitions that produce them:

2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , . . .

$2 = 2$
$3 = 3$
$4 = 2\cdot 2$
$5 = 5$
$6 = 2\cdot 3$
.

After the numbers become huge it’s not easy at all to find these combinations and even to establish if our number is a prime so there won’t be any combination from smaller numbers.

Only with this in mind can we really explain our claim properly and with the help of the above appearing horizontal heading of the primes. By what we just said, that these are hard to tell, this heading should be better regarded as a work in progress, that is continuing as we find new primes downward. The already found smaller primes of course give a lot of opportunities to pick from them especially considering allowed repetitions. We should only search these combinations because a number can have only smaller prime factors unless it's a new prime.
But as triviality it is true that using the bigger yet not "discovered" primes we won't get new prime factorizations for smaller numbers. So we can include these too as true inequalities:

$2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , \ . \ . \ .$

$2 = 2$ and $2 \neq 3$, $2 \neq 2\cdot 2$, $2 \neq 5$, $2 \neq 2\cdot 3$, $2 \neq 7$, $2 \neq 2\cdot 2\cdot 2$, $2 \neq 3\cdot 3$, . . .

$3 = 3$ and $3 \neq 2$, $3 \neq 2\cdot 2$, $3 \neq 5$, $3 \neq 2\cdot 3$, $3 \neq 7$, $3 \neq 2\cdot 2\cdot 2$, $3 \neq 3\cdot 3$, . . .

$4 = 2\cdot 2$ and $2\cdot 2 \neq 2$, $2\cdot 2 \neq 3$, $2\cdot 2 \neq 5$, $2\cdot 2 \neq 2\cdot 3$, $2\cdot 2 \neq 7$, $2\cdot 2 \neq 2\cdot 2\cdot 2$, . . .

$5 = 5$ and $5 \neq 2$, $5 \neq 3$, $5 \neq 2\cdot 2$, . . .

$6 = 2\cdot 3$ and $2\cdot 3 \neq 2$, $2\cdot 3 \neq 3$, . . .

.

These infinite many inequalities already appearing in the first line is the crucial feature that allows our induction to inherit the $A \neq B$ inequalities in our v-th line from earlier $A' \neq B'$.
Observe that we have big values appearing already in our first line and in all the under v lines again we will have infinite many such values. But only on one side! The left or right could be of course exchanged and is irrelevant. Now if we reduce both A and B in an $A \neq B$ inequality then one of them being in the v line will make the new $A' \neq B'$ inequality definitely in an earlier line. So assuming those we can get the new inequality.
But this relies on two crucial facts that our tricky A', B' reductions must obey:
That $A' \neq B' \rightarrow A \neq B$ plus that if A , B were non rearranged then A', B' are such too.
Indeed, then by our assumption of the inequalities under v for non rearranged products, we get that $A' \neq B'$ and so $A \neq B$ is true too by our verified implication.
There will be different cases of such A', B' reductions and if in one we have a sub case that implies $A \neq B$ then we don't have to follow that scenario.
The simplest case is if A and B contain any common $a_i = b_j$ prime members.
Then dividing them with these we at once get the smaller A' and B' and trivially:
$A' \neq B' \rightarrow A \neq B$ and A', B' inherit the non rearrangement too.
The first such inheritance in our lines above is $2\cdot 2 \neq 2\cdot 3$. It follows from the first $2 \neq 3$.
By this reduction method, it's enough to reduce the A , B products that contain no common members at all. For these we get our A', B' in a trickier way.
Since these have no common members, $a_1 \neq b_1$ too and so we can assume that $a_1 < b_1$, by choosing this lettering. We replace this b_1 in B for a_1 but this new $B^* = a_1 b_2 \ldots b_N$ is not our B' yet even though obviously $B^* < B$.
If $B^* < A$ is not true then trivially $A \neq B$ so we don't have to follow this scenario.
If $B^* < A$ is true then we can form our A', B' as the following two differences that are trivially smaller than A , B and get some prime factorizations for them:
$A' = A - B^* = a_1 a_2 \ldots a_M - a_1 b_2 \ldots b_N = a_1 (a_2 \ldots a_M - b_2 \ldots b_N) = a_1 \ p_1 p_2 \ldots p_K$.
$B' = B - B^* = b_1 b_2 \ldots b_N - a_1 b_2 \ldots b_N = b_2 \ldots b_N (b_1 - a_1) = b_2 \ldots b_N \ q_1 q_2 \ldots q_L$.
Obviously $A' \neq B' \rightarrow A \neq B$, so we only must show that A' and B' can not be rearranged.
For this, observe that a_1 appears in A' but it can not appear in B'. Indeed, the b-s are all different from a_1 because A , B had no common members at all. And the q-s are different from a_1 because they divide $b_1 - a_1$ while a_1 can not since b_1 is a different prime.

The beauty of this proof to me is that it actually shows how the inequality of non rearranged prime products inherits. But the new Formalists who only care about the shortness of a "proof" would prefer the following indirect version that completely hides the inheritance:

Suppose there were numbers that have non rearrangable prime factorizations.
Let the first be: $F = a_1\ a_2\ .\ .\ .\ a_M = b_1\ b_2 \ldots b_N$
If these two had common $a_i = b_j$ members then dividing with this we would get equal non rearrangable two sides again contradicting that F was the smallest value for such.
So $a_1 \neq b_1$ too and we can assume that $a_1 < b_1$.
We replace this b_1 in the right, getting the smaller $a_1\ b_2 \ldots b_N$.
Subtracting this from both original sides we get:

$a_1\ (a_2 \ldots a_M - b_2 \ldots b_N) \quad = \quad b_2 \ldots b_N\ (b_1 - a_1)$ Prime factorizing these fully:

$a_1\ p_1\, p_2 \ldots p_K \quad = \quad b_2 \ldots b_N\ q_1\, q_2 \ldots q_L$

These are smaller than our first non rearrangable equality so they should be rearrangable.
If we can show that this is not the case, we got a contradiction.
And indeed, a_1 can not appear on the right because $b_2 \ldots b_N$ were different by assumption and $q_1\, q_2 \ldots q_L$ all divide $b_1 - a_1$ while a_1 can't.

A distorted, over complicated and faulty version of this proof was published by Courant in his "What Is Mathematics", seventy years ago!
There is a deep problem with this and even my preferred longer proof and it is common with the original non inductive and also with the inductive one for the relative prime multiples.
They all used ad hoc or out of the blue tricks.
The first proof used the introduction of the g greatest common divider.
The second inductive used the smart a , $b - a$ smaller pairs.
And of course these last proofs used the heaviest trick by creating the $a_1\ b_2 \ldots b_N$ number.
But the U.P.F.T. itself followed from the relative primes without any tricks very logically.
It's also historically the way things progressed because the claim that primes divide separately is also called as Euclid's Lemma because he already used that to get the U.P.F.T.
But the relative prime fact was not so clearly proven. He also ventured into the fact that the common dividers dived the greatest.
I want to show now a perfectly straightforward proof for our relative prime fact that is a bit longer but avoids the ad hoc detour to the greatest common divider. So we must show that:
For relative prime a , b : $m\,a = n\,b \rightarrow$ there is a k that $m = k\,b$ and $n = k\,a$.
Again we use $c_1 = m_1\,a = n_1\,b$ as the first common multiple and we can prove as before that any other $c = m\,a = n\,b = k\,c_1 = k\ m_1\,a = k\ n_1\,b$.
Now observe that m_1, n_1 are relative prime multipliers because if they had a d common divider we could divide them with this and get smaller multipliers. Plus, these are the only relative prime multipliers because the others have the $k > 1$ as common divider.
Now again we realize that a , b reversed as b , a are multipliers simply because $b\,a = a\,b$.
Now regard relative prime a , b and then b , a are relative primes too and so are relative prime multipliers and so must be m_1, n_1. Then any other $m = k\ m_1 = k\,b$ and $n = k\ n_1 = k\,a$.
Check the details and think about which one you regard as best proofs.