Fundamental Theorem Of Arithmetic

If a c number is dividable by a smaller $a \neq 1$ number then the result is a $b \neq 1$ smaller number too. So $c = ab$ and this is called a decomposition of c and c a composite number.
The first few composite numbers are : $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, . . .
One or both members in a decomposition can again be composites and so then we can continue the decomposition. Above, 8 was the first such because it had the 4 composite member.
So the full decomposition of 8 is $2 \cdot 2 \cdot 2$. In such full decompositions we always get non composite final members and they never become 1. So the non composites above 1 became called as primes. The first few primes are: 2 , 3 , 5 , 7 , 11 , 13 , 17 , . . .
Thus, the full decompositions are also called as prime factorizations.
The word "factor" comes from calling in general the non 1 dividers as factors.
This allows a factor to be the number itself and for primes this is the only factor.
For these a prime factorization is thus itself. This way, every number above 1 has a prime factorization and most amazingly the prime factorizations are unique too! This means that regardless in what order we did the decompositions, the final primes are the same:

$$60 = \begin{cases} 2 \cdot 30 = \begin{cases} 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 \\ 2 \cdot 5 \cdot 6 = 2 \cdot 5 \cdot 2 \cdot 3 \end{cases} \\ 5 \cdot 12 = \begin{cases} 5 \cdot 2 \cdot 6 = 5 \cdot 2 \cdot 2 \cdot 3 \\ 5 \cdot 3 \cdot 4 = 5 \cdot 3 \cdot 2 \cdot 2 \end{cases} \end{cases}$$

This claim in general is the Unique Prime Factorization Theorem or Fundamental Theorem Of Arithmetic. Observe that if $P_1 \; P_2 \ldots P_M = Q_1 \; Q_2 \ldots Q_N$ were alternative prime factorizations, that is the P-s could not be rearranged in their order to get the Q-s, then dividing both sides with P_1 if it's not on the other side then with P_2 if it's not there, and so on, we would get the remaining $p_1 \; p_2 \ldots p_m = q_1 \; q_2 \ldots q_n$ that would have no common members at all.
So to prove the U.P.F.T. we only have to refute such totally different prime factorizations.
For this it would be enough to prove that every c number has some p prime factor that remains a prime factor in any ab decomposition in at least one member say a and then p remains again in one of the factors of a, and so on. Indeed, then p would remain as prime factor in any prime factorization and so would contradict totally different decompositions.
Luckily, we don't need to find such mystery p prime factors because Euclid's Lemma says that all p prime factors are such:
If a p divides ab then p must divide at least one of a or b.
The crucial step to prove this easily, is to see an other way what it says:
For any p prime, the set of those ab products where p divides neither a nor b but p divides ab, is an empty set. It is empty because if we form the same sets of ab products for general d numbers instead of p, then a claim is true about d that can not be true for primes.
This claim is that, the minimal ab products in the sets are such that both a and b divide d.
Indeed, then since neither a nor b can be d or 1, already one dividing d means that d is composite.
We prove our claim about the minimal ab in two steps. First we show that if either member say b were bigger than d then we had a smaller b' so that the new smaller ab' is similar as ab. Then that if b is smaller than d but it wouldn't divide d then again we had a smaller b'.
For the first case our b' is quite simply $b - d$. Indeed, $ab' = a(b - d) = ab - ad$ is again dividable by d. But b' is still not. In the second case it's not enough to subtract b from d because the result wouldn't necessarily be smaller than b. We have to subtract it as many m times it is possible, in other words we must form the $d - mb = b'$ remainder.
Then $ab' = a(d - mb) = ad - amb$ so is again dividable by d. But b' itself is not.

For the smallest prime 2, Euclid's Lemma simply says that if ab is even then at least one of a or b must be even too. Or in negative form, if both a , b are odd then ab is odd too.

This can be seen simply by $ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2M + 1$.
For the next prime 3, the non triple numbers can be $3m + 1$ or $3m + 2$ and the four product combinations will show again quite easily that two non triples' product remains non triple.
This could be continued for 5 , 7 , 11 , . . observing the 16 , 36 , 100 , . . many combinations empirically. In general, we must prove that $ab = (pm + r)(pn + s) = pM + rs$ can not be dividable by p for any r , s under p. Which again means that rs is not dividable.
So a prime can not divide a product made from smaller numbers.
Our simple proof showed exactly this in its second step.
Surprisingly, we can avoid Euclid's Lemma and refute totally different prime factorizations directly by refuting the first such $F = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$.
Changing sides we can assume $p_1 < q_1$. Then replacing q_1 in the right side with p_1, it becomes $p_1 q_2 \ldots q_n < F$, so we can subtract it from both decompositions:

$p_1 p_2 \ldots p_m - p_1 q_2 \ldots q_n = q_1 q_2 \ldots q_n - p_1 q_2 \ldots q_n$. So :

$p_1 (p_2 \ldots p_m - q_2 \ldots q_n) = q_2 \ldots q_n (q_1 - p_1)$

Decomposing the bracketed numbers into primes too, we get prime factorizations of both sides:

$$p_1 r_1 \ldots r_j = q_2 \ldots q_n s_1 \ldots s_k$$

These two prime factorizations are of a smaller than F number so should be mere rearrangements. We show that this is not the case, proving that F couldn't exist at all!
Indeed, p_1 appears on the left but it can not on the right. Because the q-s were all different by assumption and the s-s all divide $q_1 - p_1$ while p_1 can not because it doesn't divide q_1.

In spite of this simple result, we return to Euclid's Lemma.
For $r , s < p$ rs never being dividable by p, has a wider reality true for any d dividers.
Not surprisingly, this again relates to remainders. Fixing r and stepping in s, we get:
$sr = r , 2r , . . . , (d-1) r$ and we can check the remainders of these to d.
If they never become 0 this means that the sequence members were not dividable by d.
But this is not true for general d divider. What's worse, even the non 0 remainders will seem random if we go through the sr values. Observe that these remainders are $sr - td$, where t denotes the biggest multiple of d still not above sr.
We can regard these sr , td values as two infinite sequence of the repeated r , d distances under each other. Then the r and d distances can be nicely visualized as two types of train carriages with different lengths. The 0 remainders are coincidings of carriage endings while the other remainders are the distances back from an r carriage to the last d carriage.
It's immediately clear that after a first coinciding everything starts again, so it seems stupid to regard the infinite train tracks. On the other hand, for arbitrary r , d carriage lengths we may not even have coinciding at all. We avoid this problem by assuming that r and d are whole numbers, that is full units, say meters. Then coinciding is certain because $dr = rd$ so using the other carriage's length as step number will bring about a coinciding for sure.
The infinity of tracks is useful for the simple reason that this way it's evident that any $sr - td$ remainder's any m multiple is again a remainder if it's still under r and d.
Indeed, $(ms) r - (mt) d = m (sr - td)$, so using the ms and mt steppings, we get our wanted multiple remainder. This is far away but due to our obvious restart after coincidings, we get these multiple remainders already in the section up to the first coinciding. So now we just have to know the g minimal non zero remainder value and then all the positive remainders will be the multiples of this, that is $g , 2g , . . , (d - 1)g$.
But what is this g minimal remainder? Two simple facts help:
Firstly, g must divide both r and d. Indeed, if g had a positive remainder in either than this would mean a smaller remainder as well.
Secondly, any common divider of r and d must divide g, in fact any $sr - td$ remainder.
Thus of course, g must be the greatest common divider of r and d. So as a side result we obtained that any g greatest common divider is dividable by all the other common dividers.

If r and d have no common factor, that is their only common divider is 1, this is called as r and d being relative primes and in this case $g = 1$ and so all $1, 2, \ldots, d-1$ values are remainders up to the $dr = rd$ coinciding.
This means that 0 can not appear, simply because there is no room for it among the remainders and so the trivial $dr = rd$ coinciding is the first.
This can be seen in an other way too, without remainders just from the coincidings:
If s and t have an f common factor then obviously $sr = td$ can not be the first coinciding because $\frac{s}{f}r = \frac{t}{f}d$ is an earlier. So the first coinciding can only be with relative prime s, t.
Also, all other coincidings are multiples so can have no relative prime step numbers.
So there is only one relative prime step numbered coinciding, the first.
Thus, for relative prime r and d, the trivial coinciding $dr = rd$ has to be the first.
If $d = p$ prime and r is not multiple of p then they are relative primes and if $r < d = p$ then obviously this is the case and so we see at once why rs couldn't be a p-number.
It has to produce all positive remainder values up to p, without room for 0.

This big picture of remainders has a very simple practical meaning and alternate vision:

An $sr = td$ coinciding means $\frac{r}{d} = \frac{t}{s}$, that is the equality of two fractions.

If r and d are relative primes, we can not simplify $\frac{r}{d}$ anymore and then:

$t = mr$ and $s = md$, that is the $\frac{t}{s}$ fraction is merely an expansion of $\frac{r}{d}$.
This also means that if we simplify any fraction to the full in any ways by crossing out common factors as we do it in elementary school, then the final simple fraction is always the same regardless how we simplified. Not surprisingly, the U.P.F.T. lies behind this practice.
Indeed, imagining the r numerator and d denominator in prime factorization, the uniqueness of these gives the uniqueness of simplifications too.
But there is an amazing continuation of this fractional application.
In an infinite square grid system we can call as "connector" the line segment between any two grid points. The horizontal and vertical components can be regarded as the fraction members and usually the vertical is the r numerator and the horizontal is the d denominator.

This way the slope of the line on which the connector lies is exactly $\frac{r}{d}$.
It is visually trivial that on a line that contains some grid points, these are all repetitions of a shortest grid distance or connector. Also trivially, if a connector represents a simple fraction then there are no grid points inside, so this is a minimal connector. Thus, all fractions that are equal to such simple one and so have same slope, must be multiples, so indeed expansions.

To simplify a fraction completely in one step, we should divide the numerator and the denominator by their greatest common divider, so to know g is very practical.
Euclid made a very simple algorithm that finds g. It works by turning fractions upside down and should start with $r > d$. Such $\frac{r}{d}$ fractions can be written in a "mixed number" form by placing the W "whole part" in front as a larger number: $W\frac{r'}{d}$. The new r' numerator is the remainder and of course $r' < d$. That's why we have to turn this upside down to $\frac{d}{r'}$.
Then we repeat this till we get a fraction where turning upside down is pointless because it would become a whole. The last numerator is g. For example:

$\frac{72}{28} = 2\frac{16}{28}$, $\frac{28}{16} = 1\frac{12}{16}$, $\frac{16}{12} = 1\frac{4}{12}$ so $g = 4$.