Fundamental Theorem Of Arithmetic

Meaning, the U.P.F. Theorem

All letters will denote the naturals : 1 , 2 , 3 , 4 , . .
If $a = bc$ then the b , c numbers are called dividers of a.
Every $a = 1 \cdot a$ and these two, the 1 and a dividers are called the trivial dividers of a.
If $a = bc$ with non trivial dividers, that is both b , c above 1 and under a then such product form is called a decomposition of a and a itself a composite.
The first few composites 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 above 1. So the non composites above 1 became called as primes.
The first few primes are: 2 , 3 , 5 , 7 , 11 , 13 , 17 , 19 , . .
Most amazingly, these decompositions are unique!
Meaning, 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 is the Unique Prime Factorization Theorem or Fundamental Theorem Of Arithmetic.
The reason for the first name comes from a useful generalization.
The non 1 dividers of a number are called as its factors.
Obviously, primes have only one factor, themselves. The prime factorization of a number is its decomposition if it is composite or just itself if it is a prime.

Two nuances, The role of definitions, An example of media stupidity and the Big Lies.

The fact that all composites break down to primes is not the U.P.F. because the U is missing. Above too, we just accepted it as trivial. It could be called as P.F. Theorem or Basic Theorem Of Arithmetic. But mathematicians are obsessed with proofs and so such easily provable facts don't deserve special names. An actual proof relies on two facts.
Firstly, that factors of a factor are again factors and secondly that if some break down still contains composites then those by their definition as composites break down again into factors. Thus the further breakdowns means decreasing factors, that must stop at non composite factors. A factor can not be 1 so we end up with non 1 non composites which are the primes.
This was due to the smart parallel definition of primes and factors. The locking out of 1 from both was a crucial nuance since otherwise we could have arbitrary many 1-s included.
The deep part of the claim of course has nothing to do with this little nuance.
Indeed, regarding other special numbers say the squares it's not true that all numbers can be even decomposed from squares. So we see the not just crucial but deep nuance again between possible or unique decomposition. The bigger picture of these two nuances is that definitions allow to establish claims that are not evident from the definitions themselves. They have to be smart, namely very simple but hiding further surprising consequences. Thus, definitions are the real but hidden motors of mathematics. Hidden, because they are never analyzed due to the mentioned obsession with proofs. This is a fundamental inner stupidity of formalist math.
But the section title refers to a much simpler stupidity too. Indeed, the tricky role of definitions only coming out by their consequences implies that merely to repeat a definition in itself is totally useless and ignores the essence of math.

Yet aside from this, a smart definition in itself is a sign of intelligence. So very wisely, it was decided that to search extraterrestrial intelligence, we should emit radio signals of the primes.
In the film “Contact”, Jodie Foster plays a mathematician who in a TV interview “explains” the primes by regurgitating its definition. This reflects the stupidity of both the Media where indeed such could happen and Hollywood where they “reflect” with the same stupidity.
Nobody in the audience asked “why the primes?”. And indeed, just because the primes are only dividable by 1 and themselves is not a reason to send them into the Universe.
Especially, without seeing that those two are trivial dividers. Verbal garbage was spread.
Telling that all numbers can be decomposed from primes is the absolute beginning of any reasonable importance of the primes. But revealing the second and more amazing level that these decompositions are unique is also a must. In fact, this must be told already in Elementary School because this lies behind the Unique Total Simplifications of fractions. Indeed, when we simplify fractions by crossing out common factors from the numerator and denominator, we never ask a simple but logical question. Is this simplification process unique?
Is it giving a unique further non simplifiable fraction regardless how we simplify?
Imagining the numerator and denominator in prime factorization, the uniqueness of these gives the uniqueness of the total simplifications too. But we shouldn’t prove the U.P.F. and then serve this as proof for the U.T.S. It is much more educational to raise the question of this U.T.S. prior to even mentioning primes. Firstly, because we simplify with whatever we can, not only primes and secondly because the U.T.S. can be continued to prove the U.P.F.
A proof of the U.T.S. itself starts with recognizing a consequence which in fact is the basic idea of all later proofs too and which was not apparent in Elementary School at all.
Namely, that if the total simplifications of a fraction are all identical then it has to be the “minimal” simplification of that fraction!
Here “minimal” means the one with the smallest numerator and denominator among all possible simplifications of our fraction. This is meaningful because these decrease in tandem.
If the minimal simplification were not total, so could be further simplified then that further simplification were a smaller simplification.
So it is enough to show that all simplifications can be continued to the minimal.
In fact, realizing that an s simplifying value is nothing more than a common divider of the numerator and denominator, we can express the U.T.S. also as:

Greatest Common Divider Superiority:
All s common dividers of a , b divide the $< a , b >$ greatest common divider of a , b.

Indeed, then the U.T.S. is a consequence as follows:
The minimal simplification is obviously the one by the $< a , b >$ greatest simplifying value.
This is a total simplification otherwise it could be continued and weren’t the minimal.
Also, every simplification by an s can be continued to the minimal by using the $\frac{< a , b >}{s}$ simplification. Thus only the minimal is total.
We would think that then leaving the fractions and proving theorems like the one above we get to the Unique Prime Factorization. I thought so too, for quite a long time.
When I came back from Australia to Hungary to retire I went to the Pedagogical Library to go through all current text books in math and physics. It was very depressing! The best high school math book was written by Lajos Posa who I knew from my own high school years. In fact, I had an ugly exchange of letters with Erdös where his name came up. Erdös thought that it was a waste that such a talent got involved in education. I won’t even tell how I reacted.
Anyway, in this book Posa says that “The Fundamental Theorem Of Arithmetic is beyond the scope of this book”. That started me up to go into it again and I wrote about twenty versions.
I knew that I am the best didactical mind at present in this God Forsaken Planet and I succeeded again. A “success” is an exposition of something that arrives to a goal with clearly showing why a claim is true and after such “spine” presents a wider body of all relating details too.
The big lie is that proof is all that counts and the even bigger lie is Wikipedia’s proofless jungle.

Common Multiples, The Basic Approach

Amazingly, the simple concept of the common multiples paves also the simplest road to our goal of proving the U.P.F.T. And though the common multiples are thought in all elementary schools, none of the basic four formulas are ever mentioned.
But the fourth crowning one is completely missing even from all text books of Number Theory.

The definition of an m common multiple of a , b is simply that $m = ia = jb$ for some i , j.

Common Multiples Formula: $m = k[a , b]$.

Where $[a , b]$ is the smallest common multiple and the precise meaning is that:
1. All $k[a , b]$ are common multiples.
2. All common multiples of a , b are $k[a , b]$.
To see 1. observe that if $[a , b] = ia = jb$ then $k[a , b] = (ki)\, a = (kj)\, b$.
To see 2. observe that:
Any non $k[a , b]$ number is either under $[a , b]$ or between $k[a , b]$ and $(k+1)[a , b]$.
The first is impossible for an m common multiple because $[a , b]$ is the first.
In the second case, that is if $k[a , b] < m < (k+1)[a , b]$ were then we would have that $m - k[a , b] < [a , b]$. This $m - k[a , b]$ would be a common multiple since both members are.
So we would again get an impossible common multiple under $[a , b]$.

Common Dividers Formula: $s = \frac{ab}{m}$. The precise meaning now is that:

1. All common dividers of a , b are $\frac{ab}{m}$ with some m common multiple.

2. For all m common multiple that divides ab, $\frac{ab}{m}$ is a common divider.

To see 1: If s is a common divider then $\frac{b}{s}a = \frac{a}{s}b = \frac{ab}{s}$, so $\frac{ab}{s} = m$ and $s = \frac{ab}{m}$.

To see 2: Suppose that for an m common multiple $\frac{ab}{m}$ is a whole.

Then $\frac{a}{\frac{ab}{m}} = \frac{am}{ab} = \frac{m}{b} =$ whole and $\frac{b}{\frac{ab}{m}} = \frac{mb}{ab} = \frac{m}{a} =$ whole.

And these two together mean exactly that $\frac{ab}{m}$ is a common divider of a and b.

The smaller an m common multiple is with $s = \frac{ab}{m}$ whole, the bigger this common divider is.
For the smallest possible $m = [a , b]$ we definitely get a whole s and thus a common divider because ab is a common multiple so by the Common Multiples Formula $[a , b]$ divides it.
And then this s must be the greatest common divider that we denote as $< a , b >$ so:

Greatest Common Divider Formula: $< a , b > = \frac{ab}{[a , b]}$.

This combined with the common multiples formula gives a crucial new fourth one.
A didactical masterstroke missing from all text books!

Subdivision Formula: Let $s \mid n$ abbreviate that s divides n. Then: $a \mid bc \rightarrow \frac{a}{< a , b >} \mid c$.

This makes "perfect sense" by a naïve argument that of course proves nothing:
Namely, $< a , b >$ is the maximal "part of a" that divides b.

So everything else that remains in a, that is $\frac{a}{< a , b >}$, should divide the c member.

Let's see the actual proof:
$a \mid bc$ means that bc is a multiple of a but bc is trivally a multiple of b.
So bc is actually a common multiple of a , b and so $bc = k[a , b] = k\frac{ab}{< a , b >}$.

Thus $c = k\frac{a}{< a , b >}$ which means exactly that $\frac{a}{< a , b >} \mid c$.

Relative Primes
The usual name for those a , b that have only 1 as common divider is "relative primes".
A formal definition can also be : $< a , b > = 1$.
A prime and an other number that is not dividable by the prime are relative primes.
But if the other number is dividable by the prime then they are not.
For example, $7 , 14$ are not relative primes because 7 is a non 1 common divider.
Also observe the seemingly strange fact that 1 is relative prime with any number.
Indeed, 1 and any other number obviously can only have 1 as common divider.
The most important fact however is that two different primes are always relative prime.
Indeed, since they are different the only common divider can be 1.

Euclid's Lemma:
$a \mid bc$ and a , b are relative primes $\rightarrow$ $a \mid c$.

The Subdivision Formula with the $< a , b > = 1$ definition of being relative primes means this.

Euclid's Prime Lemma:
If p is a prime , $p \mid bc$ $\rightarrow$ $p \mid b$ or $p \mid c$ maybe both.

The consequence could also be said that if p doesn't divide b then it must divide c.
And observe that if p doesn't divide b then p , b are relative primes and so Euclid's Lemma gives that $p \mid c$. This lemma could also be called as the External Atomness Of Primes.
Indeed, the p prime divider "must be inside" one of the members.
The internal atomness of course means the definition of the primes that they don't decompose.
The crucial more practical point why this specialization from relative primes to primes was important is that there is a new directional generalization from a prime divider.
Namely, to a product of more than two members:
Generalized Prime Lemma:
p is a prime and $p \mid b_1 b_2 \ . \ . \ . \ b_n$ $\rightarrow$ p divides some b member.

Let b_i be the first member so that $b_1 \ . \ . \ . \ b_i$ is already dividable by p.
We claim that $p \mid b_i$. If $i = 1$ then of course we only have b_1 as member and so $p \mid b_1$.
If $i > 1$ then $b_1 \ . \ . \ . \ b_{i-1} = b$ is not dividable by p but $b\, b_i = bc$ is and so
Euclid's Prime Lemma implies that $p \mid c = b_i$.

There is an extra feature about primes that will make this generalization useful.
At the beginning I mentioned that the mere existence of a prime factorization could be called as the Basic Theorem Of Arithmetic but it is so trivial that they gave no name for this.
Well this claim is even simpler, the mere existence of a prime divider. Amazingly, for this we can avoid going into an arbitrary factorization because there is a simpler proof.

Prime Divider Lemma: Every number above 1 has prime divider.

Being above 1 means that it must have divider above 1 since itself is such.
Thus it must have a smallest non 1 divider and we claim that it is a prime.
Indeed, if this were not a prime then it had some smaller non 1 divider.

Products Common Divider Theorem:
If two $a_1 . . . a_m$, $b_1 . . . b_n$ products have an $s \neq 1$ common divider then they must have some a_i , b_j members that also have already some non 1 common divider.

By the previous lemma s has a p prime divider. This p is also a common divider and so by the Generalized Prime Lemma it must divide some member in both products.
Observe that not having such a_i , b_j members, means that any pair of members from the two products are relative primes. Thus the negative form of our theorem is:

Relative Prime Products Theorem:
If a_1 , . , a_m and b_1 , . , b_n are two sets of numbers that all a_i , b_j are relative primes, then the two products formed from them are relative primes too.
Remember that two different primes are always relative primes and so:

Disjoint Prime Products Theorem:
If p_1 , . , p_m and q_1 , . , q_n are two sets of primes having no common member then the two products formed from them are relative primes. And so finally we arrived to:

U.P.F. or Fundamental Theorem Of Arithmetic

Indirect proof means that we assume the opposite of a claim and refute that by a contradiction.
But usually the advantage in such indirect argument lies in assuming other things too.
For example, here if we assume that there were numbers that have different prime factorizations then we can also assume that there would be an F first such number.
So refuting this F would refute all different prime factorizations.
But a non merely rearranged prime factorizations of F actually would have to be totally different, meaning that they would contain no common member.
Indeed, any common member would imply that we can divide the two versions with that and thus obtain a smaller than F number with two different factorization.
Thus we only have to refute two such totally different prime factorizations.
But by the Disjoint Prime Products Theorem two such prime products are relative primes.
So in particular they can not be equal.
This was the end of our basic road. The shortest but at the same time most general picture.
Such always exists and this is the yet hidden didactical principle of the Universe.
But now come the “gardens”, the sidetrackings. First two alternative proofs will be shown.

1. An amazing “direct” indirect proof of the U.P.F.

This proof will be indirect again and the “direct” merely refers to the fact that this proof does not rely on any earlier results, so it is “direct” in this sense.
So let $F = p_1 p_2 . . . p_m = q_1 q_2 . . . q_n$ be our first non unique prime factorization, that as we explained must be totally different that is having no common member on the two sides.
We can assume $p_1 < q_1$ because otherwise we can rename the two sides.
Replacing q_1 in the right side with p_1, it becomes $p_1 q_2 . . . q_n < F$.
So if we subtract $p_1 q_2 . . . q_n$ from both decompositions we get equal natural numbers:
$p_1 p_2 . . . p_m - p_1 q_2 . . . q_n = q_1 q_2 . . . q_n - p_1 q_2 . . . q_n$. So :

$$p_1 (p_2 . . . p_m - q_2 . . . q_n) = q_2 . . . q_n (q_1 - p_1)$$

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

$$p_1 r_1 . . . r_j = q_2 . . . q_n s_1 . . . s_k$$

These two prime factorizations are of a number under F so should be mere rearrangements.
But this can not be the case. Indeed, p_1 appears on the left but it can not on the right.
Because the q-s were all different from it and the s-s all divide $q_1 - p_1$ while p_1 can not because it doesn't divide q_1. And thus F couldn't exist at all!

2. A less indirect proof

I show a consequence of the Generalized Prime Lemma that can give a bit more constructive proof, though still having some hidden indirect part in it.

Primes Lemma:
If a p prime divides a $q_1 \cdot \cdot \cdot q_n$ product of primes, it is a member in the product, $p = q_i$.

Indeed, by the Generalized Prime Lemma p must divide a q_i but now this can only be if it is that q_i.

U.P.F. the third time:
Let two prime factorizations of a number be: $p_1 \cdot \cdot \cdot p_m = q_1 \cdot \cdot \cdot q_n$.
Every occurring prime on the left divides the left trivially as member but by the equality divides the right too. Thus by our Primes Lemma it must occur there as member too. So we can pick any member of the left and divide both sides with it. The number of members decreased on both sides so repeating this we must end up with a single p on the left "or" a single q on the right.
But this "or" must actually be an "and" because a prime can not be a product of primes.
And so these final remaining two primes are the same by the equality that always inherited.

Greatest Common Divider Superiority, Euclidian Algorithm

We mentioned the first already on page 3 as the way to prove the Unique Total Simplification of fractions. But we didn't mention it in our basic approach. We could have easily. Indeed:
By the Common Dividers Formula, the Common Multiples Formula and the Greatest Common Divider Formula applied in succession:

All common dividers are $s = \frac{ab}{m} = \frac{ab}{k[a\,,b]} = \frac{\frac{ab}{[a\,,b]}}{k} = \frac{<a\,,b>}{k}$. And so:

Greatest Common Divider Superiority: All common dividers divide the greatest one.

Euclid was aware of this very much and had a not quite exact proof for it that we modernize.
We'll use sets and the $A \supseteq B$ containment meaning that all members of B are inside A.

Let $D(n)$ denote the set of dividers of n and $D(a,b)$ the set of common dividers of a and b. Since the dividers of $< a\,,\, b >$ are trivially common dividers, that is $D(a,b) \supseteq D(< a\,,\, b >)$, thus our claim is that: $D(a,b) = D(< a\,,\, b >)$.

The fundamental fact on which our proof relies is that:
$D(a,b) = D(a-b,b)$ if $a > b$ and $D(a,b) = D(a,b-a)$ if $b > a$.
Indeed, the common dividers inherit to the differences.
Only if $a = b$ can we not apply one of these "replacements".
So regarding the sequence of these as far as possible:
$D(a,b) = D(a',b') = \cdot \cdot \cdot = D(a^*,b^*) = D(g,g) = D(g)$.
Here a^*,b^* are the last possible replacements and thus they must have the g common value.
The greatest member of $D(g)$ which is obviously g must be the same as of $D(a,b)$.
And so $g = < a\,,\, b >$ and so $D(a,b) = D(< a\,,\, b >)$.

Euclidian Algorithm

Euclid discovered the subtraction trick we used in the proof above but as we said his arguments were not an exact proof. On the other hand, his approach was actually a much more efficient method to get to the g final value as the greatest common divider.

Instead of the D(a,b) = D(a-b,b) if a > b and D(a,b) = D(a,b-a) if b > a replacements we could use D(a,b) = D(a-kb,b) if a > kb and D(a,b) = D(a,b-ka) if b > ka.

Using the maximal k means that a – kb or b – ka are the remainders in each other.
Now, such remainders are also meaningful when we change a larger than 1 fraction into so called "mixed number" form, writing the whole value in front: $\frac{a}{b} = w_1 \frac{a_1}{b}$.
Indeed, then $a = w_1 b + a_1$ and a_1 is the remainder of a on dividing with b.
The reason for the subscript is that we'll continue this. We turn the $\frac{a_1}{b}$ fractional part upside down to get the $\frac{b}{a_1}$ larger than 1 fraction and change it again into the $w_2 \frac{b_1}{a_1}$ mixed form.
Continuing this, we'll get a sequence of whole parts and fractions.
We stop when we get a fraction that is a whole, so the next numerator would become zero.
Here the denominator will be < a,b >. A simple example goes like this:

$\frac{225}{160} = 1\frac{65}{160}$, $\frac{160}{65} = 2\frac{30}{65}$, $\frac{65}{30} = 2\frac{5}{30}$, $\frac{30}{5} = 6$ = whole, so: $< 225 , 160 > = 5$.

The Fractional Variants Approach

From the Euclidian Algorithm the Greatest Common Divider Superiority and the Unique Total Simplification of fractions do not follow directly. But as I said, it can even be continued to the U.P.F. theorem. It is an interesting road but there is an even better one that starts with fractions.
In elementary school the expansions and simplifications of an $\frac{a}{b}$ fraction are introduced but in a sense these hid a more important concept.
Namely, the variants of $\frac{a}{b}$ meaning all those $\frac{c}{d}$ fractions that re equal in value to $\frac{a}{b}$.
In fact, this will correct a wider hidden distinction of fractions being equal or identical.
Equality, so being variants means $\frac{a}{b} = \frac{c}{d}$ which actually means ad = bc while being identical should be denoted as $\frac{a}{b} \equiv \frac{c}{d}$ and meaning that a = c and b = d.

The most important clarification is visualizing all possible variants of an $\frac{a}{b}$ fraction.
The { x ; P(x) } set collection can be introduced. This as all those x for which P(x) is true.

So the variant set of $\frac{a}{b} = \left[\frac{a}{b}\right] = \{ \frac{c}{d} ; \frac{c}{d}$ is variant of $\frac{a}{b} \} = \{ \frac{c}{d} ; \frac{c}{d} = \frac{a}{b} \}$.

Thus actually we collect all those $\frac{c}{d}$ fractions that ad = bc.

A big problem is that obviously we must collect infinite many fractions since all the expansions must be collected. A crucial help is to realize that we can talk about smaller or bigger variants because if $\frac{c}{d} = \frac{a}{b}$ and c < a then also d < b while if c > a then also d > b.

So for equal fractions the numerator and denominator must decrease or increase in tandem.

And so we can regard merely the smaller variants of an $\frac{a}{b}$ fraction which is a finite set.

The incorrectness of the naïve assumption that variants must be the same as simplifications or expansions then can be made quite explicit as actually collecting by trials all fractions that are the smaller variants of a fraction say $\frac{48}{36}$. So we don't jump into this fraction and try to simplify it rather list all fractions with smaller numerators and denominators and actually check if they are equal to $\frac{48}{36}$. This exercise will then show that it is not obvious at all why this set should be the set of all simplifications of $\frac{48}{36}$. Of course it will be but this must be proven and our road will do this. The tool for this is to visualize the $\left[\frac{a}{b}\right]$ variant set in increasing order.

Which of course is not meant in actual values since they are all equal, rather by the numerator and denominator values that as we said increase in tandem. So we shouldn't even use $<$ for this ordering rather $\frac{c'}{d'} \prec \frac{c}{d}$ meaning that $c' < c$ and $d' < d$. And finally, the most important part in this ordered variant set vision is that we can introduce $\frac{\eta(a,b)}{\delta(a,b)}$ as the smallest variant.

If we only regard a fix $\frac{a}{b}$ fraction's variant set then this can be abbreviated as $\frac{\eta}{\delta}$.

And then our first formula that actually corresponds to the common multiples formula is:

Variants Formula: $\left[\frac{a}{b}\right] = \frac{\eta}{\delta} \prec \frac{2\eta}{2\delta} \prec \frac{3\eta}{3\delta} \prec \ldots$

In words: All variants of an $\frac{a}{b}$ fraction are expansions of the smallest variant $\frac{\eta}{\delta}$.

Or in shortest way: $\frac{c}{d} = \frac{a}{b} \rightarrow \frac{c}{d} \equiv \frac{k\eta}{k\delta}$.

Enough to show that all $\frac{k\eta}{k\delta}$ are in $\left[\frac{a}{b}\right]$ but no $\frac{c}{d}$ members are "in-between" two $\frac{k\eta}{k\delta}$ and $\frac{(k+1)\eta}{(k+1)\delta}$ consecutive expansions.

The first is trivial more generally as: $\frac{c}{d} \in \left[\frac{a}{b}\right] \rightarrow \frac{kc}{kd} \in \left[\frac{a}{b}\right]$.

Indeed: $\frac{c}{d} = \frac{a}{b} \rightarrow cb = da \rightarrow cbk = dak \rightarrow \frac{kc}{kd} = \frac{a}{b}$.

For the second, first we show that: $\frac{c'}{d'} \prec \frac{c}{d} \in \left[\frac{a}{b}\right] \rightarrow \frac{c-c'}{d-d'} \in \left[\frac{a}{b}\right]$. This is true because:

$\frac{c}{d} = \frac{a}{b}, \frac{c'}{d'} = \frac{a}{b} \rightarrow cb = da, c'b = d'a \rightarrow cb - c'b = da - d'a \rightarrow (c - c')b = (d - d')a$

$\rightarrow \frac{c-c'}{d-d'} = \frac{a}{b}$. And now to see how this implies the no in-betweenness:

Suppose a $\frac{c}{d}$ were in-between $\frac{k\eta}{k\delta}$ and $\frac{(k+1)\eta}{(k+1)\delta}$.

Using our last result with $\frac{c'}{d'} \equiv \frac{k\eta}{k\delta}$ we get that $\frac{c-k\eta}{d-k\delta} \in \left[\frac{a}{b}\right]$.

Also, by the in-betweenness: $k\eta < c < (k+1)\eta \rightarrow c - k\eta < (k+1)\eta - k\eta = \eta$.

So these two together are impossible because the smallest numerator in $\left[\frac{a}{b}\right]$ is η.

Simplifications

The $s > 1$ common dividers of a, b are important for the $\frac{a}{b}$ fractions.

Because, then the $\frac{\frac{a}{s}}{\frac{b}{s}}$ simplification of $\frac{a}{b}$ is a variant of $\frac{a}{b}$.

Indeed, $\frac{ab}{s} = \frac{a}{s}b = \frac{b}{s}a \rightarrow \frac{\frac{a}{s}}{\frac{b}{s}} = \frac{a}{b}$.

The minimal simplification is obviously the one with the $< a , b >$ greatest common divider of a and b and so:

Smallest Variant Formula: The smallest variant $\frac{\eta}{\delta}$ is the minimal simplification of $\frac{a}{b}$.

That is: $\eta = \frac{a}{< a , b >}$ and $\delta = \frac{b}{< a , b >}$. Or in reverse:

$\frac{a}{b}$ is the $< a , b >$ expansion of the smallest variant, that is: $\frac{a}{b} \equiv \frac{< a , b > \eta}{< a , b > \delta}$.

So this answers our original question: Where is $\frac{a}{b}$ in $\left[\frac{a}{b}\right]$? It is the $< a , b >$-th member.

The proof is trivial: By the Variants Formula $\frac{\eta}{\delta}$ is not only a variant of $\frac{a}{b}$ but a simplification of $\frac{a}{b}$ too. So since all simplifications of $\frac{a}{b}$ are variants too, $\frac{\eta}{\delta}$ being the smallest variant, it is the smallest or as we called it the minimal simplification too.

Total simplifications:

An $\frac{a}{b}$ fraction's $\frac{\frac{a}{s}}{\frac{b}{s}}$ simplification is total if it can not be simplified anymore.

That is, $\frac{a}{s}$ and $\frac{b}{s}$ have no other common divider than 1. That is $< \frac{a}{s} , \frac{b}{s} > = 1$.

This is what we always tried to achieve in Elementary School by crossing out common dividers from the numerator and denominator. But we never asked, whether this method is unique. It is! And the explanation now is easy. Only the minimal simplification is total.

Indeed, first of all it is total because it is $\frac{\eta}{\delta}$ and so every other variant is expansion of it and none is a simplification. But also in reverse, only $\frac{\eta}{\delta}$ is a total simplification among all variants and thus among all simplification too.

An even wider missed question was if $\frac{a}{b} = \frac{c}{d}$ implies same total simplifications too? Indeed:

$$\frac{a}{b} = \frac{c}{d} \rightarrow \left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \rightarrow \frac{\eta(a,b)}{\delta(a,b)} \equiv \frac{\eta(c,d)}{\delta(c,d)} \rightarrow \eta(a,b) = \eta(c,d) , \delta(a,b) = \delta(c,d).$$

That is: $\frac{a}{< a, b >} = \frac{c}{< c, d >}$ and $\frac{b}{< a, b >} = \frac{d}{< c, d >}$. This result has a simpler special case:

Greatest Common Divider Distributivity: $< ae , be > = < a , b > e$.

$$\left[\frac{a}{b}\right] = \left[\frac{ae}{be}\right] \rightarrow \frac{\eta(a,b)}{\delta(a,b)} \equiv \frac{\eta(ae,be)}{\delta(ae,be)} \rightarrow \eta(a,b) = \eta(ae,be) \rightarrow \frac{a}{<a,b>} = \frac{ae}{<ae,be>}.$$

The heuristic argument on page 3 showed how the Greatest Common Divider Superiority implies the Unique Total Simplification but now we already showed this without.
So now we just prove the first and Euclid's Lemma again to finish this approach:

Greatest Common Divider Superiority: $s \mid a$ and $s \mid b \rightarrow s \mid <a,b>$.

$$\frac{\frac{a}{s}}{\frac{b}{s}} \in \left[\frac{a}{b}\right] \rightarrow \frac{\frac{a}{s}}{\frac{b}{s}} \equiv \frac{k\eta}{k\delta} \rightarrow \frac{a}{s} = k\eta = k\frac{a}{<a,b>} \rightarrow <a,b> = ks \rightarrow s \mid <a,b>.$$

Subdivision Formula: $a \mid bc \rightarrow \frac{a}{<a,b>} \mid c.$

The proof uses both the Variants Formula and the Smallest Variant Formula:

$$a \mid bc \rightarrow bc = da \rightarrow \frac{c}{d} = \frac{a}{b} \rightarrow \frac{c}{d} \in \left[\frac{a}{b}\right] \rightarrow c = k\eta = k\frac{a}{<a,b>}.$$

The Linear Combinations Approach

Quite oppositely as Euclid's practical remainder method, here we'll go with abstraction above the subtraction trick and thus make a direct proof of the Greatest Common Divider Superiority even simpler. But actually it becomes a complete third road of obtaining all our previous results. The abstraction is to regard all possible repeated additions and subtractions from the two fix numbers a and b. So we regard all possible $c = \pm\alpha a \pm \beta b$ natural numbers.
We claim that if the set of these is C and the smallest member is c_1 then:
$C = \{c_1, 2c_1, 3c_1, \ldots\}$
It's enough to show that no c combination can be between kc_1 and $(k+1)c_1$.
And indeed, in that case $c - kc_1$ were a combination under c_1.
Now observe that $(b+1)a - ab = a$ and $(a+1)b - ba = b$ are themselves combinations and thus are c_1 multiples too. Or in other words c_1 is a common divider of a and b.
But observe also that any s common divider of a and b divides any combination, in particular c_1 too. Thus all common divider of a, b divides c_1 and so it has to be $<a,b>$.

We can also realize that $c_1 = <a,b>$ is also a linear combination so:
$<a,b> = \pm\alpha a \pm \beta b$ with some α and β numbers. This is also called as Bezout's Identity.
This reveals again that all common dividers of a, b must divide $<a,b>$ but even more importantly, it also gives the Subdivision Formula very easily:
Indeed, multiplying both sides with c we get that:

$<a,b>c = (\pm\alpha a \pm \beta b)c = \pm\alpha ac \pm \beta bc$. So if $a \mid bc$ then a divides the right end.

So it is am and $<a,b>c = am$. Thus $c = \frac{a}{<a,b>} m$. And so indeed $\frac{a}{<a,b>} \mid c$.

To get the fact that equal fractions have same minimal simplification is a bit more involved.

Here we have to multiply Bezout's Identity with a c again and a d too:

$<a,b>c = \pm\alpha ac \pm \beta bc$ and $<a,b>d = \pm\alpha ad \pm \beta bd$ for any c, d.

If $\frac{a}{b} = \frac{c}{d}$, that is $ad = bc$ then:

$< a,b > c = \pm \alpha ac \pm \beta ad = a (\pm \alpha c \pm \beta d)$ and $< a,b > d = \pm \alpha bc \pm \beta bc = b (\pm \alpha c \pm \beta d)$.

Thus $c = \frac{a}{< a , b >} (\pm \alpha c \pm \beta d)$ and $d = \frac{b}{< a , b >} (\pm \alpha c \pm \beta d)$ so $\pm \alpha c \pm \beta d$ divides c , d.

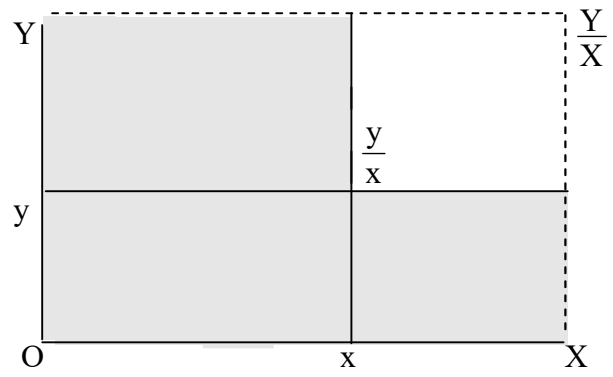
But any s common divider of c , d also divides $\pm \alpha c \pm \beta d$ so this is actually $< c,d >$.

Thus $c = \frac{a}{< a , b >} < c,d >$ and so indeed $\frac{a}{< a, b >} = \frac{c}{< c, d >}$.

Connectors, Alterations

This should be the first application of what I call the Grid System. Which is nothing more than an infinite square-tiled plane. So it is not the usual grid points of a Descartes Plane because we do not need any coordination, origin whatsoever. By the way, complex numbers and even High School Coordinate Geometry should start without coordination too! On the other hand, later when coordination is introduced then Coordinate Geometry should be at once approached with vectors. Neither this nor the amazing simplicity of complex or Gaussian integers will be now explained. This is the first introduction of the Grid System for the crucial concept of what the title mentions, the Connectors. These are nothing more than distances connecting any two grid points. Later in upper Elementary School they can become directed, that is vectors but now they are just plain distances. The most amazing is what these mean now. The fractions!
So we always use these in the same direction, going upward and to confirm with the later use, we place the denominator horizontally and then the numerator upwards. The only point to see is that a connector may or may not have grid points on it. More crucially, if it has then those like beads follow in equal lengths, thus dividing the connector into equal sub connectors.
This vision at once shows that all sub connectors on a connector are multiples of the minimal.
The concept of expansion is also very visual as repeated shifts of the connector.
The first surprise is that a simplification of a fraction does not trivially fall on the connector.
It is a division of the horizontal forward and the vertical upward component with a common whole number and we can place it at the O left end for simplicity but nothing explains directly why it should fall onto the original connector. Of course, we can argue indirectly that an expansion of this simplified fraction becomes the original and so if the simplified fraction's connector wouldn't be on the original connector then expanding it we would get two different connectors for same components. But as we know two points determine a unique line.
I'll make now a little detour and show a bit more directly why a simplification aligns.

Amazingly, this alignment goes beyond our grid system because by $\frac{Y}{X} = \frac{y}{x}$ we have $xY = Xy$ and this multiplication equality is meaningful for real numbers that is distances as equal rectangle areas. This suggests a generalization of already the fractions as proportionalities but I will not continue this direction.
The xY and Xy rectangles are parts of the big XY rectangle and a smallest xy rectangle is part of both xY and Xy.



The $\frac{y}{x}$ point falling onto the $\frac{Y}{X}$ line can be proven by the following areal arguments:

$O\frac{y}{x}$ is the diagonal of xy and thus halves it into two triangles.
Taking these off from the equal grey rectangles we get two disjoint and equal areas.

Together these cover XY except the missing white rectangle having $\frac{y}{x}\frac{Y}{X}$ as diagonal.

This again halves and so adding these halves to the previous two equal areas we get that the $O\frac{y}{x} + \frac{y}{x}\frac{Y}{X}$ connection graph halves XY. But the $O\frac{Y}{X}$ diagonal also halves this.

So $\frac{y}{x}$ must fall onto $O\frac{Y}{X}$ because otherwise we had the $O\frac{y}{x}\frac{Y}{X}$ triangle area taken off from one half and added to the other so they couldn't remain equal.

From this detour we return to something very algebraic that can be explained easier after this geometric visualization. Namely, why the simplifications are not simplifications of each other yet they all being expansions of the smallest. Which is now evident as all connectors on a line being repetitions of the smallest. We can translate this geometrical triviality into algebra.

Let's introduce an "idiot subtraction" of two fraction as: $\frac{A}{B} \Theta \frac{A'}{B'} = \frac{A - A'}{B - B'}$.

This is the algebraization of the connector. Plus we can introduce a new third special form of the variants beside the trivial expansions and simplifications. Namely, using first an expansion and then a simplification of that expansion. We can call this as an "alteration".
Then it becomes true that the idiot subtraction of two alterations is again an alteration:

$$\frac{A}{B} \Theta \frac{A'}{B'} = \frac{A - A'}{B - B'} = \frac{\frac{ae}{s} - \frac{ae'}{s'}}{\frac{be}{s} - \frac{be'}{s'}} = \frac{a(\frac{e}{s} - \frac{e'}{s'})}{b(\frac{e}{s} - \frac{e'}{s'})} = \frac{a\frac{E}{S}}{b\frac{E}{S}} = \frac{\frac{aE}{S}}{\frac{bE}{S}}.$$

This of course implies that all alterations are merely expansions of the minimal alteration!
But this includes the simplifications too, so they are expansions of the minimal alteration.
But our original fraction determining its alterations is also just an expansion of the minimal alteration, so that minimal alteration is actually a simplification of our fraction.
Above we used the idiot subtraction of aligned, that is equal fractions. I just have to mention a similar but not directly relating concept. An idiot addition or dumb-sum of non equal totally simplified fractions plays a fundamental role in the Farey Fractions!

A heuristic direct proof of Euclid's Lemma

Again the "direct" merely means that we'll use no earlier results.
Let's recap our claim:
a , b are relative primes and $a \mid bc \quad \rightarrow \quad a \mid c$.

Let's fix an a and b and let $C(a,b) = C = \{ c ;\ a \mid bc \}$. The trivial members of C are the a , $2a$, $3a$, . . multiples of a. So our claim simply says that if a , b are relative primes then only these trivial members are the members of C.

The logical way would be to show that no number under a nor between two a multiples can be in C. This second is easy by the first but the first is a harder road that we'll pursue later.
Now as a "Gordian" slash, we prove the following lemma without the assumption of a , b being relative primes at all: If c_1 is the smallest C member then $C = \{ c_1, 2c_1, 3c_1, \ . \ . \ \}$.

Observe that $a \in C$ but if a , b are relative primes than a can not be $k\,c_1$ with $k > 1$.
Indeed, $a = k\,c_1 \mid b\,c_1$ implies $k \mid b$ and so with $k > 1$ then a , b were not relative primes.
So a must be c_1 and thus a , $2a$, $3a$, . . are indeed all the C members.

Now we prove our lemma, that $C = \{ c_1, 2\,c_1, 3\,c_1, \ . \ . \ \}$. Of course, all $k\,c_1$ are C members trivially, so we only must show that no C members can be between a $k\,c_1$ and $(k+1)\,c_1$.
Observe that a $c - c'$ difference of two $c > c'$ C members is a C member, that is $b(c - c')$ is an a multiple because $b(c - c') = bc - bc' = Ma - ma = (M - m)a$.
So with this a $c \in C$ between $k\,c_1$ and $(k+1)\,c_1$ would mean $c - k\,c_1 \in C$.
But observe that $c - k\,c_1 < (k+1)\,c_1 - k\,c_1 = c_1$.
So we had a C member under c_1 which is impossible because c_1 was the smallest.

The negative jungle

Euclid's Prime Lemma could be put in a "negative" form as:
If a p prime doesn't divide either of b , c then p will not divide bc either.

For the first prime 2, not being dividable by it is what we call as being odd and thus our negative version follows immediately by: $bc = (2m+1)(2n+1) = 4mn + 2m + 2n + 1 = 2M + 1$.
For the next prime 3, the non dividability means non "triple" numbers which means the possible members as $3m+1$, $3m+2$ and $3n+1$, $3n+2$. Trying out the four possible combinations we again get it easily that the result is always non triple.
Continuing this for more concrete primes, we get more and more possible combinations but strangely we can always verify our claim experimentally.

The general situation is that $bc = (pm + r)(pn + s) = p^2 mn + pm + pn + rs = pM + rs$, where r and s are any possible numbers under b and c. So we merely have to show that:

A p prime can not divide a product of two smaller numbers.

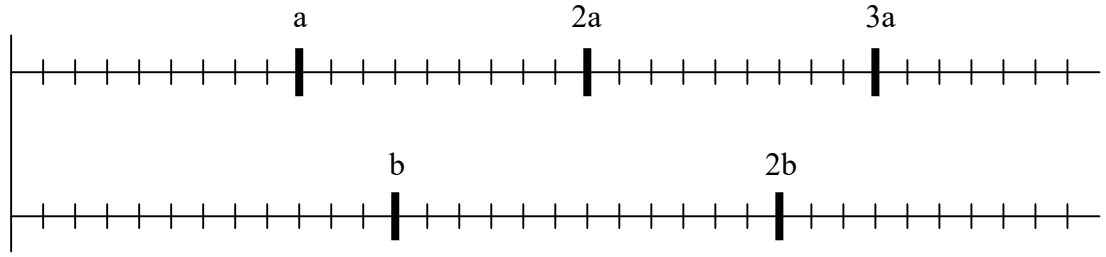
This seems hard to prove in one "slash" by the "jungle" of the individual cases.
Yet we found exactly such Gordian slash by regarding the c_1 minimal possible value at the previous proof of Euclid's Lemma. And of course in the Common Multiples or Variants Formulas the same minimality was used but with more meaningful minimal values.

We'll go through the "jungle" in the next section and so give a new proof again!
But now observe that to venture into the impossible can be a big trap!

This is important because there is a very famous, or rather infamous theorem that is about the impossible from the start. Fermat's last or "lost" theorem says that $a^n + b^n = c^n$ is impossible for $n > 2$ values. Could it be that in a wider world of possibles, there is a very short "Gordian" proof here too? Aside from this, it is indeed almost impossible that Fermat could have found a short proof even if such wider world does exist.

The jungle as the world of remainders

We'll go into the remainders to prove from inside why a prime can not divide a product of two smaller numbers. And yet we'll start with going outside, to common multiples geometrically:



These are now the coincidings, where a jb multiple is exactly under the ia multiple.
First of all, observe that for arbitrary a , b distances coinciding is not necessary at all.
We won't go into the interesting problems of this.
For a , b distances being whole numbers, that is mu , nu multiples of a common u unit as above in our picture, coinciding is certain.
Indeed, using as i , j multipliers the other's unit number we'll have: n(mu) = m(nu) = (mn) u.

Regarding not just the coincidings but the in-between jb – ia or ia – jb values, they seem to be quite random. Best is to regard only the jb – ia differences under a, that is the remainders of a in the b multiples. This is how far the last ia ending is before a jb multiple.
The "overflow" of a would be how far the next a ending is after a b multiple.
But these are all remainders, by regarding the distances backwards from a coinciding.

Most surprisingly, all remainders are merely multiples of the smallest remainder g.
Even the existence of a smallest remainder is not obvious but observe that after the first [a , b] coinciding everything just repeats. So we only have finite many possible remainders.

Then observe that sums of remainders under a and positive differences of remainders are again remainders. Simply add or subtract the multipliers: (Jb – Ia) ± (jb – ia) = (J ± j) b – (I ± i) a.
The addition implies that if a k multiple of an r remainder is still under a then kr is also a remainder. Then the subtraction implies that the remainders of remainders in each other must be remainders too. And then these two imply what we claimed, that all remainders are merely multiples of the smallest g.

Now comes a big surprise about this g smallest remainder, though suggested by its notation.
It is actually the $< a , b >$ greatest common divider of a and b.
Firstly, g must divide both a and b. This is because any remainder of a remainder in a or b must be also a remainder. This follows from the multiplicity of the remainders and that for any r remainder a – r is a remainder too and if r is under b then b – r is remainder too.
Indeed, a – r is the mentioned overflow and b – r is the overflow at the last b multiple.
Secondly, any common divider of a and b must divide any jb – ia remainder, so g too.
So g must be $< a , b >$ and we obtained again that all common dividers divide this.

The Greatest Common Divider Formula $< a , b > = \frac{ab}{[a , b]}$ has also a new meaning and proof.

Let $r_1 , r_2 , . . . , r_j = 0$ be the remainders of a in b , 2b , . . , jb = [a , b].
These can not have repeating value because it would mean an earlier coinciding than [a , b].

Also, these remainders in increasing order must be $< a , b >$, $2 < a , b >$, . . , $i < a , b > = b$, the multiples of the $< a , b >$ smallest one, except here $r_j = 0$ corresponds to $i < a , b > = b$.

So these two sequences must have same many elements: $j = \frac{[a , b]}{a} = i = \frac{b}{< a , b >}$.

If a , b are relative primes, that is $< a , b > = 1$ then the possible positive remainders are all $1 , 2 , . . . , a – 1$ values. These all must occur as remainders of a in jb and for different j they are different before a coinciding. So the first coinciding can only happen at ab.
For the even more special case when $a = p$ is a prime and $b < p$, the remainders of p in $b , 2b , . . . , (p – 1) b$ must pick up all possible positive values up to $p – 1$.
So a zero remainder, that is dividability by p can not occur, simply because there is no room for it among all the different positive values that must occur.

Prime remainders arithmetic

The previous "world of remainders" was actually a special world inside the earlier used linear combinations, the most abstract approach. And now we mention an even narrower world that nevertheless is very beautiful and in some sense gives a more abstract picture.
We only regard a p prime divider and the possible $0 , 1 , 2 , . . . , p – 1$ possible remainders.
In this finite set we can create a world where the subtraction and division can also be perfectly introduced. So in a sense it will be better than the infinity of the naturals.
The trick is to regard everything as the possible remainder on a p division.
Let for example p be 7. Then $4 + 5 = 9$ goes over 7 and so it will be the remainder, that is 2.
Written as $4 + 5 \equiv 2$ and usually said as the two sides being congruent modulo 7.
Similarly $4 \cdot 5 = 20 \equiv 6$. Also very logically $4 – 5 = – 1 \equiv 6$. A 6 remainder is 1 excess.
The first deeper step is the road toward the division. $\frac{4}{5} \equiv r$ should mean that $r \cdot 5 \equiv 4$.
But this only makes sense if there is a unique such r. And this is true because if $r \cdot 5 \equiv 4$ and $s \cdot 5 \equiv 4$ were both true then $(r - s) \cdot 5 \equiv 0$ were true too which is impossible since a product of two numbers under 7 can not be dividable by 7.
Especially important is the division of 1 by an r , that is the $\frac{1}{r}$ reciprocal of r.
Then: $\frac{1}{1} \equiv 1$, $\frac{1}{2} \equiv 4$ or $\frac{1}{4} \equiv 2$, $\frac{1}{3} \equiv 5$ or $\frac{1}{5} \equiv 3$, $\frac{1}{6} \equiv 6$.
This is quite general, that is 1 and $p – 1$ are their own reciprocals but every other number has a pair. For 1 this is trivial and for $p – 1$ observe that $(p – 1)(p – 1) = p^2 – 2p + 1 \equiv 1$.
Thus $2 \cdot 3 \cdot . . . \cdot (p - 2) \equiv 1$ since it is a product of the pairs each giving 1 as value.
This at once shows again why a product can never become 0. By the way:
The previous equality is called Wilson's Theorem but usually written as: $(p – 2)! \equiv 1 \mod p$.
Also, all the above are also called as modular arithmetic.
Sounds abstract and indeed, I hate this whole modular notation.
It all can be directly replaced by using $| . . . |_p$ as the remainder to p.
So then Wilson's Theorem is simply: $| (p – 2)! |_p = 1$.

An effective approach

We want to look again into the hard yard that we avoided with our Gordian solution.

As we mentioned, the no between c values easily follows from no vales under p.
A non dividability with p simply means having some $r > 0$ remainder at dividing with p.
But between kp and $(k+1)p$ the same remainders will repeat as under p.
Indeed, let again $| bc |_p$ denote the remainder and then $| b(c + p) |_p = | bc |_p$. So indeed:
We must only show that for all c values under p : $| bc |_p \neq 0$.
In fact, the same repeating of the remainders is true for b too: $| (b + p)c |_p = | bc |_p$.
So actually we only must show that for all $b , c < p$: $| bc |_p \neq 0$.

Let's see the actual $|\,bc\,|_p$ values for the first few primes:

$p = 2 \;\rightarrow\; (b,c) = (1,1) \;\rightarrow\; |\,bc\,|_p = 1 \neq 0.$

$p = 3 \;\rightarrow\; (b,c) = (1,1)\,,\,(1,2)\,,\,(2,1)\,,\,(2,2) \;\rightarrow\; |\,bc\,|_p = 1\,,\,2\,,\,2\,,\,1 \neq 0.$

$p = 5 \;\rightarrow\; (b,c) = (1,1)\,,\,(1,2)\,,\,(1,3)\,,\,(1,4)\,,\,(2,1)\,,\,(2,2)\,,\,(2,3)\,,\,(2,4)\,,\,(3,1)\,,\,(3,2)\,,\,(3,4)\,,$
$(4,1)\,,\,(4,2)\,,\,(4,3)\,,\,(4,4) \;\rightarrow\; |\,bc\,|_p = 1\,,\,2\,,\,3\,,\,4\,,\,2\,,\,4\,,\,1\,,\,3\,,\,3\,,\,1\,,\,2\,,$
$4\,,\,3\,,\,2\,,\,1.$

As we see, the remainders are totally irregular but "magically" never become 0.

A machine could calculate these remainders and never even "realize" this claim.
A proof seems even harder for us too and yet we did prove it earlier with our Gordian slash.
Or by the minimality used in the Variants Theorems and the Common Multiples Formula.

To find a bridge between the two sides, the easy earlier proofs and the amazing factual diversity of the remainders now starts with replacing the p prime with arbitrary a.

In fact, then the external assumption of this is avoided for the machine and so it can just use a as the two other variables $b\,,\,c$.
Then of course it will not be true anymore that a 0 remainder can not come about!

But if Euclid's Prime Lemma is true then for a prime a it can not happen. So in reverse:
If a non 0 remainder is encountered then a must be a composite number.

This is the Effective version of Euclid's Prime Lemma. The machine can not derive this either but we get a better vision of why the primality condition was needed.

So when is a composite? Simply if for some d : $d \mid a$ and $d \neq 1$ and $d \neq a$.
But where do we find such d? We don't have to! The machine will find it for us!
Indeed, the first c that it will encounter, exactly our earlier c_1 is such a d.

Effective Euclid's Lemma:

Let $\neg|$ abbreviate not dividing. Then Euclid's Lemma can be said as:

For some $b\,,\,c$: $a \mid bc$ but $a \neg| b$ and $a \neg| c \;\rightarrow$
For some d : $d \mid a$ and $d \neq 1$ and $d \neq a$. That is, a is a composite.

Let $C(a,b) = C = \{\, c\,;\, bc \in [a] = \{\, a\,,\,2a\,,\,3a\,,\,\ldots\,\}\,\}$ and the smallest $c \in C$ be c_1.
We can show again that $c = k\,c_1$ and also:
$ba \in [a] \;\rightarrow\; a \in C \;\rightarrow\; a = k\,c_1 \;\rightarrow\; c_1 \mid a.$
$a \neg| b \;\rightarrow\; b \notin [a] \;\rightarrow\; 1 \notin C \;\rightarrow\; c_1 \neq 1.$
For some $c \in C$: $a \neg| c \;\rightarrow$ For some $c \in C$: $c \notin [a] \;\rightarrow\; c_1 \neq a.$
Indeed if $c_1 = a$ then all $c \in C$ is ka and so $\in [a]$.

So c_1 is our claimed d and thus a is a composite.