Fifteen Fundamental Theorems of Naturals

These fifteen theorems split into three groups. The first five relate to primes, the next five are about power remainders and the final five are about square sums. So:

I. Five Basic Theorems of Primes:

0 . Primes

1 . Infinity of Primes

2. Primes Divide Separately, The Vision Of Common multiples

3. Unique Prime Factorization, Without Vision Induction

4. Back To Vision, Multiple Differences

5. Practicalities, Unique Simplification of Fractions, Euclidian Algorithm

II. Five Basic Theorems of Power Remainders:

0. Blind Spots

1. First New Look: Multiple Cycles, Euler's Theorem

2. Second New Look: Multiple Lengths, Super Length Theorem

3. Third New Look: Roots, Full Super Length For Prime Dividers

4. Lucas Primality Test

5. Carmichael's Theorem

III. Five Basic Theorems of Square Sums

0. Ancient And New Combined

1. Perfect Pairs Under A Prime, Wilson's Theorems, Square Sums

2. Product Pairs, Square Root Complementarity, Euler Criterion, Square Complementarity

3. Inductive Square Sumness for Prime Factors of Simple Square Sums

4. Instant Square Sumness for Prime Factors of Simple Square Sums

5. Reversal for Prime Products, The special Role of 2

Primes

The most obvious sign of how the abstract reality of the natural numbers are magically inherent in the human mind, is the fact that children after they learn to count, can at once count from any number and in any fix steps, like 20, 23, 26, 29, . . .
This is what we later call as an arithmetical sequence. If the starter number is the same as the step, then we simply get the multiples of the start like: 7, 14, 21, 28, 35, . . .
A number is composite if it is a multiple, that is it appears in a multiple sequence not as a starter.
In other word, it is a product $m\,n$ with m not being 1 or as we say, it's a non trivial product.
So, a trivial product is $n = 1 \bullet n$, which is true for any n number and thus defines nothing.
An other third way of saying this is that the number has non trivial divider. But here we can regard the number itself as trivial too, just like the 1 which is trivial in every number.
So, a crucial distinction between this universal triviality of the 1 and the numbers themselves as dividers, is the concept of "factor". We exclude 1 but we don't exclude the number itself.
So a numbers is the trivial factor of itself but 1 is not factor ever.
Thus, 1 is the only number that has no factor, while all others have some, because themselves are such. If they have other, non trivial factors too, then they are composites, while if themselves are the only factors, then we call them primes.
This seemingly stupid allowing the number itself to be a factor, makes perfect sense as we go further. But I will show three examples right here at the start:
The first is a new concept not quite fortunately called being "relative primes". A modernized and straight out stupid name is being "co-primes". So, I will stick with relative primes.
This "simply" means that the two numbers have no common factor. So now it is important that primes have themselves as factor. And so 7 which is a prime is not relative prime with 14 because they have the 7 as common factor.
And indeed, 7 and 14 as a pair is really just the 7 multiple of 1 and 2 as pair.
In contrast, a 1 divider which is always common, taken out would not simplify the pair because they remain the same. So that's why we don't even regard 1 as potential "taking out", or factor.
So, relative primes should be called simple pairs that can not be simplified any more.
This vision explains not only the "strangeness" that primes are not relative primes to everything, but the even stranger fact that the number 1 is relative prime to everything. Indeed, 1 has no factor at all so it can not be simplified ever. This concept of relative primes or simple pairs, will be very useful, but I promised three examples so here comes the second which is the most crucial for using the word factor. In fact, the most important theorem of the natural numbers which is also called the Fundamental Theorem Arithmetic has a more proper name as Unique Prime Factorization Theorem = U.P.F.T. Here the word factorization refers to factors and since primes have only themselves as factors they are themselves their factorization too.
The c composite numbers can be written as non trivial $a\,b$ products, that is with both a and b not 1 and thus being factors. But more importantly then both must be smaller than c too.
So such factorization is a "decomposition" into smaller factors and in fact that's where the word composite comes from.
The smaller a , b numbers may be again composites and then we can decompose them again.
This process only stops if we reach primes that can not be decomposed any more.
For example:

$$60 = \begin{cases} 2 \cdot 30 = \begin{cases} 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 \\ 2 \cdot 5 \cdot 6 = 2 \cdot 5 \cdot 2 \cdot 3 \end{cases} \\ 3 \cdot 20 = \begin{cases} 3 \cdot 2 \cdot 10 = 3 \cdot 2 \cdot 2 \cdot 5 \\ 3 \cdot 4 \cdot 5 = 3 \cdot 2 \cdot 2 \cdot 5 \end{cases} \end{cases}$$

As we see, we went different ways but we always ended up with the same prime factors.
So the total prime factorization of a number is always the same except in order.

This explains the name Unique Prime Factorization.
To prove it is not trivial at all. At present, no public education system of any country includes this in its curriculum. For fifty years I myself wasn't sure if this should be taught in elementary or high school. Only recently became sure of the "yes" answer.
The beautiful and simple proof in the third section for the major step explains my view.

The third application of the usefulness of the word factor, allowing a number itself as divider and thus including primes, is exactly related to our first theorem, the infinity of primes:

Infinity of Primes

There is a perfect introduction to this theorem that actually shows that the opposite of our claim, that is having only finite many primes is not that absurd at all. The crucial function for this is the so called "factorial". Talking about stupid names, this takes the cake and of course has nothing to do with factors. The abbreviation of it is the exclamation sign and it simply means multiplying all numbers up to an n. So: n factorial = $n!$ = $2 \bullet 3 \bullet 4 \bullet \ldots \bullet n$. For example:
$100! = 2 \bullet 3 \bullet 4 \bullet \ldots \bullet 99 \bullet 100$. This is obviously a number so huge, that nobody can give it exactly, and yet everybody should explore it.
The weird thing about $100!$ is that it is multiple of all the 2, 3, 4, . . . , 99, 100 numbers.
Then of course, $100! + 2$ is a multiple of 2 too, in other words it is even.
Also, $100! + 3$ is a 3 multiple, that is triple. And so on.
So, $100! + 2$, $100! + 3$, $100! + 4$, . . . , $100! + 99$, $100! + 100$ are all composite numbers.
Of course, 100 can be any other n , so $n! + 2$, $n! + 3$, . . . , $n! + (n - 1)$, $n! + n$ are always a sequence of consecutive numbers that are all composite.
Arbitrary big n gives arbitrary big such block without a prime.
This in itself is a great result, but lets observe that instead of adding the 2, 3, . . . , n numbers, we could subtract them, that is count back, so:
$n! - 2$, $n! - 3$, . . . , $n! - (n - 1)$, $n! - n$ are always composites too.
So actually, we have two twin blocks without prime, and in between them are three numbers:
$n! - 1$, $n!$, $n! + 1$:

$$\underbrace{n! - n \ , \ldots , n! - 3 \ , \ n! - 2}_{\text{Composites}} \ , \ n! - 1 \ , \ n! \ , \ n! + 1 \ , \ \underbrace{n! + 2 \ , \ n! + 3 \ , \ldots , n! + n}_{\text{Composites}}$$

? ?

The $n! - 1$ and $n! + 1$ numbers could be called the factorial twins. They are definitely not multiples of any of the 2, 3, . . . , n numbers because $n!$ is and 1 isn't. The question marks under them show that we don't know whether they are composites or primes. Indeed, just because they are not dividable by 2, 3, . . . , n they could still have factors all bigger than n.
If that's the case, then the two blocks combine into a single, so from $n! - n$ up to $n! + n$, all numbers are composite, that is, there are no primes.
Is it possible that the primes would die out completely? Now we see that this is not so absurd.
What's really strange, is that exactly the above vision helps to refute this. Namely, either of the two factorial twins can produce a prime bigger than n. All we need is a second function beside the used factorial. I will abbreviate it as minfact (n) and here the "fact" really stands for factor while the "min" for minimal. This the promised third usefulness of factors. So now it's important that every number except 1 has factor and so this minfact function is defined too for all non 1 numbers. If n is prime then of course itself is the only factor so minfact (n) = n.
But most amazingly, yet quite simply, minfact (n) is always a prime.
Indeed, to be a prime means not having smaller factor. Now, if there were a smaller factor of minfact (n) then that would be a factor of n too, so minfact (n) couldn't be the minimal.

As we explained above, the factorial twins are not dividable by 2, 3, 4, . . . , n because the factorial is but 1 is not. So then the minfact (n ! – 1) and minfact (n ! + 1) primes can not be among 2, 3, 4, . . . , n either, so they are bigger than n.
To repeat the whole argument in crystal clear form: These two facts:
1.) minfact (n) is a prime for all n.
2.) minfact (n ! – 1) > n for all n.
mean at once that for every n we have a bigger than n prime, namely minfact (n ! – 1).
In spite of making it so clear and simple, there is an even shorter proof that was discovered by Kummer in the 19th century. He realized that if we just aim to prove that there are infinite many primes then we do not need to show how the minfact (n ! – 1) or minfact (n ! + 1) primes produce bigger primes than n. It's enough to know that every number has a prime factor.
We know this from minfact (n) of course but a prime factorization in any order shows it too.
The point is that this fact alone that every number has a prime factor implies the infinity of primes at once. And the argument is similar to the above but simpler in this part too. We don't need to multiply all numbers, that is form the factorial. We only have to multiply all those finite many primes that we assumed to exist only. If their product were a P then P + 1 had 1 remainder to all the primes and thus could not be dividable by any prime. So this impossible P + 1 number would contradict the truth that every number has prime factor.

Primes Divide Separately, The Vision Of Common Multiples

The fact that primes have no smaller factors, so are not factorizable, can be regarded as an "atomness". Of course, we mean it in the ancient Greek "atomism" sense because we know that actual physical atoms are not undividable, they contain smaller particles.
The more important continuation of this analogy is that if we don't cut atoms themselves that is avoid nuclear interactions but separate larger matters, then the individual atoms must go to one of the separated parts. So beside the internal atomness, there is this external one too. Of course, for the primes as atoms, the products represent the combinings. And then the fact that primes are atoms internally, that is not factorizable, should imply the external atomness, that if a p divides an a b product then p must "belong" to one of the factors, so p must divide either a or b.
Surprisingly this is not true due to a deeper reason, aside from this whole questionable analogy!
This deeper reason is that individuality doesn't exist in math! A prime like 7 can be in many numbers as factor and when we say 7, it means all of them. So "the 7 prime factor" is not really a "thing" rather a "kind of thing" only. Most amazingly, this same individuality loss appears in new physics too. Now, what all this deep "blubbering" boils down to is that instead of the "either or" conclusion we can only guarantee an "or".
So, if 7 divides an a b product then 7 must divide at least one of a or b but may divide both because "an other 7" can be there too.
The most surprising fact is that this seemingly so fundamental external atomness of primes that also gives the U.P.F.T. in such easy two steps, is itself not a trivial plausibility at all.
Those who calculate a lot with products will get a sense of this fact and sometimes fall into the trap of accepting it as plausibility. Once one realizes that this is a delusion and so 7 dividing some product does not imply at all that 7 should divide a member, one gets into real math.
A chase begins to make this external atomness of primes exact. This leads to a jungle.
Can we stick to plausibilities or should we abandon plausibility for exactness?

As I said, from this fact that primes divide separately, the two steps to proving unique prime factorization is standard and actually already Euclid used it. So this external atomness or separate dividability by primes is also called as Euclid's Lemma. The real point is to prove this.
There are many possible ways to prove it and for decades I wasn't sure if there is a truly simplest way. No matter what way we go, if we want to be didactical that is visual, then we have to widen our scope and go out of merely regarding the primes. But how far we should widen our scope?

The rule is simple! If we have alternate ways but with same “sweat” that is difficulty of steps then the best is the one that shows the widest reality.
The crucial minimal widening from primes is the relative primes and there is a very simple new Lemma that implies Euclid’s at once. It could be called the Relative Prime Product Dividability Lemma and it is a strange reversal of the goal of Euclid’s Lemma too.
In Euclid’s Lemma the divider is a p prime and we divide an a b product.
Now we regard any arbitrary and single c that we divide and rather the divider will be a b.
The crucial assumption is that both a and b divide c and so this c actually stands not for being composite rather being a common multiple of a and b.
The extra assumption is that a and b are relative primes, that is have no common factor.
Their only common divider is the trivial 1.
Then we claim that not only separately divide a and b but their product divides c too.

First we should show why this Lemma implies Euclid’s Lemma at once.
That claims that if p divides a and p divides b then p divides a or p divides b.
So we can assume that p doesn’t divide a but then we must show that p divides b.
Now the crucial point is that if p doesn’t divide a then since p has no other factor than itself there can be no common factor of p and a so they are relative primes.
So they can be used as a and b of the new Relative Prime Product Dividability Lemma.
The c common multiple must be chosen as a b of the Euclid’s Lemma.
The a being in the a b product of course at once shows that indeed this a b is a multiple of a.
But the assumed fact that p divides a b also means that this a b is a multiple of p too.
So indeed, a b is a common multiple of p and a. As we showed they are relative primes so by our new Lemma their product p a must divide a b too. In other words k p a = a b.
This then at once shows that k p = b so indeed, p divides b.

The hidden assumption in our new Lemma that c is a common multiple of a and b , reveals that the world of common multiples is the one that we need beside the named special assumption that a and b are relative primes. So first we should see some basic facts about c common multiples of any two a , b numbers.
These c are merely common values in the two set of multiples:

a , 2a , 3a , . . . and b , 2b , 3b , . . .

The real visual trick is to regard these as distances underneath each other on two half lines that start exactly above each other.
On the first half line we see the repeating a distances and underneath the b-s.
The c common multiples are distances where an m multiple of a will be the same as an n multiple of b so m a = n b are coinciding interval endings.
Amazingly, such existence of a coincidence is not obvious at all!
We can visualize that the repeated a lengths and the repeated b lengths would never end exactly under each other. And indeed, this is not only possible, but with arbitrarily chosen a and b intervals it is usually the case.
Our original problem of course is regarding not arbitrary intervals because a and b were whole numbers that is multiple lengths of a common u unit interval.
This common unit existence is amazingly identical with the coinciding!
Indeed, if for example the seventh of a is the same u as the fifteenth of b, then 15a and 7b must coincide because they are both (15 • 7) u. And in reverse too, if the 15a and 7b are coinciding then the (15 • 7) –th of this coinciding length must be a common u unit, because it is seventh of a and fifteenth of b. So, using the a and b intervals themselves as multipliers, plus the a b = b a exchangeability of the multiplication order for natural numbers is the cause of the coincidence existence for naturals that is for distances with common unit.
The Greeks were obsessed with the common unit problem and yet didn’t realize this simple road to coincidings.

The trivial $a\ b$ coincidence will be crucial for an other reason for our approach very soon too.
It will give the proof of our new Lemma.
The heuristic visual reason why we should regard coincidings is the following:
If there is a coinciding then from there everything starts again. Which also means that:

All coincidings are exactly just multiples of the first coinciding. $c = k\ f$

This k multiplier of the coincidings is actually already a common multiplier inside the $m = \frac{c}{a}$, $n = \frac{c}{b}$ multipliers because $m = \frac{c}{a} = \frac{k\ f}{a} = k\ \frac{f}{a}$ and $n = \frac{c}{b} = \frac{k\ f}{b} = k\ \frac{f}{b}$.
So these multipliers can not be relative primes when $c = k\ f$ with $k > 1$.

Quite amazingly though for the first f coinciding, the multipliers must be relative primes.

Indeed, if a $d > 1$ number divides both m , n multipliers of a $m\ a = n\ b = c$ coinciding, then the $\frac{m}{d}$ and $\frac{n}{d}$ multipliers give a coinciding as $\frac{m}{d}\ a = \frac{n}{d}\ b = \frac{c}{d}$.
So this is actually an earlier coinciding if $d > 1$.
But then for the first f coinciding the $m = \frac{f}{a}$, $n = \frac{f}{b}$ multipliers can not have such $d > 1$ common divider, that is can not have common factor, that is they must be relative primes.

The simple way to say these last two claims together is this:
The f first and only the first coinciding has relative prime multipliers.

Now we can regard the special $a\ b$ coinciding when a , b are assumed to be relative primes.
The multipliers are b and a and of course these are relative primes too being the same except in opposite order. But "there can only be one!", I mean relative prime multipliers, at the minimal.
So actually $a\ b = f$ the first coincidence.
Then by $c = k\ f$ we have actually now $c = k\ f = k\ a\ b$.
So indeed $a\ b$ divides c.
We proved the Relative Prime Product Dividability Lemma and earlier we showed how it implies Euclid's lemma that primes divide separately.

An interesting side question is whether Euclid's Lemma would imply back our new Lemma.
I look at this now, before the proof of U.P.F.T from Euclid's Lemma because it is educational in seeing how deep is the U.P.F.T. and how easy it is to take it for granted.

We regard a as $p_1\ p_2 \ldots p_m$ and c as $n\ b$.
Since a and b are relative primes, these p can not divide b.
Then by Euclid's Lemma they all must divide n. So their product divides n too and so:
$c = n\ b = k\ a\ b$.
We might feel that our error was to use a prime factorization of a but we are wrong.
To assume such is not an error because we didn't assume uniqueness that is the U.P.F.T.
The real error was to jump to the conclusion that just because some primes divide something then their product divides it too. This only comes about from the U.P.F.T.
Indeed, obviously there are prime factorizations of the $c = n\ b$ that has any of the p primes.
Simply because these divide and so we can start a prime factorization with each.
But then these prime factorizations go on their own ways. There is no reason that they would encounter all the other p-s too. But of course by a unique prime factorization this must happen.

Unique Prime Factorization, Without Vision Induction

As I mentioned, the two steps from Euclid's Lemma to the U.P.F.T. is straight forward.
The first step keeps the assumption of a p prime dividing a product but we generalize the $a\,b$ product to more members but at the same time we restrict all members to primes.
In short, we assume that p divides the $q_1\ q_2 \ldots q_n$ prime product.
The simple claim is then that p has to be one of the q-s, $p = q_j$.
We regard $q_1\ q_2 \ldots q_n$ as $q_1\, Q_1$ and then by Euclid's Lemma p divides q_1 or Q_1.
The first of course means $p = q_1$ because a different q_1 would only have itself as factor.
So if this p dividing q_1 alternative of the Euclid's Lemma is the case then we are finished.
If not, that is p only divides Q_1 then we again regard Q_1 as $q_2\, Q_2$.
The same logic shows that then p must be q_2 or must divide Q_2.
Continuing this way we encounter all q-s and at the last we get that p is $Q_n = q_n$.

Our next final step is to show that two equal $p_1\ p_2 \ldots p_m = q_1\ q_2 \ldots q_n$ prime products are actually the same except in order and so every p is identical with a q on the other side.
This identical means that we mean more than just equal because there can be repeating values.
So each must be corresponding to a particular one and if we distinguish these then their number is the same too. This of course implies that actually $m = n$ too.
The proof again goes in the members one by one but now on the left side.
Indeed, p_1 divides the right side and so has to be a q_j by our previous result.
Then we can divide both sides with p_1 and apply again our previous result to p_2.
Gradually, all p-s will find their pair among the q-s.

This was indeed short and we might be happy for such a perfect derivation of the U.P.F.T.

The visual road to the Relative Prime Product Dividability Lemma and then the derivation of Euclid's Lemma from that and the standard two steps from that to the U.P.F.T.

This is an optimal and simplest derivation in some sense that made me claim that the unique prime factorization should be high school subject.
But then again, I claim that math shouldn't be a subject at all!!!!!!!

The undeniable difficulty in math is a split between logic of visions and logic of proofs.
Without the first we are lying Formalists, without the second, we are naïve amateurs.
To encompass both, is a difficult job. Only few mathematicians have both the scope of seeing enough details to tell the full story and the honesty to try to tell it.
The lure of Formalism is very strong. It is the dark side of Mankind, the root of all evil.
A very appropriate big cycle of this general Formalism in mathematics can be pinpointed by the names of Euclid and Hilbert. Hilbert is regarded as the initiator of formalism but this is not the meaning I use with capital F. In fact, if there was ever an anti Formalist, it was Hilbert.
He said that if someone understands something in math then he can explain that to the first person in the street. His most obvious connection with Euclid could be that he reaxiomatized Geometry.
As we saw from the first section, Euclid himself was not merely a geometer but this is what he was most famous for, trying to axiomatize Geometry the first time. That's where the conflict of vision and proof appeared the first time with Formalism coming out as an ugly winner.
The hardest part to axiomatize was parallelity. This is the well known fact. The never mentioned part is a mystery, lying already in his whole axiomatization.
The non parallelity part of Euclid's axiomatization seemingly combines logic of meanings and logic of derivations without any conflict. But this is not true either. He draws attention to the intuitive facts like lines, crossings, points, distances, angles.

The simplest features of lines is that two always cross in one point and that two points determine a single line. So even a formal symmetry seems behind these two rules.
The first surprise is that these two rules or intuitive assumptions are not really independent. They seem to imply each other. Indeed, assume the first that is two lines crossing in one point and then if two points would determine two lines then these two would cross in two points contradicting our assumption. In reverse, assume that two points determine one line and then two lines crossing in two points would exactly give two points that determine two lines.
So we are playing with impossibilities. We envision them and thus derive contradictions. This is indirect thinking and it was and still is our specific human tool.
The bigger framework of this indirect thinking is the "isomorphism principle".
This is the crucial point of departure from animals. They only "think" in physical reality, not in the relations of the parts. A rat learns a maze much sooner than a human would.
But what a rat will never be able to do is to condense the rules of a maze as the sequence of turns: right, right, left, **. . .** This is the uncrossable limitation of all animals. Humans do miracles.
When a child learns the rules of chess, he will instantly, without any learning apply it to any physical reality. So, out in the park, will be able to play with the giant pieces just as naturally.
Of course, thinking in impossibilities is a further step on this journey.
But returning to our plausibilities about lines crossing and being determined by points, we have to realize that we made terrible mistakes. We only realize these mistakes if we step outside our plausibility world and look formally at what we say. First of all, not crossing in one point doesn't mean automatically crossing in two or more because it could mean nothing that is not crossing at all. Similarly, determining not one line doesn't mean two or more but might be nothing.
Once we open up these logical faults, we realize that the mentioned symmetry was faulty too.
Indeed, in crossings this "nothingness" is a reality, namely parallel lines don't cross at all, but among determinations the "nothingness" is impossible, two points always determine at least one line, even if the two points are the same and we have infinite many going through.
So already these seemingly plausible axioms must be reformulated. We have to state the determination in two steps. First that there is always such line and then for two different points claiming uniqueness. Then the crossings in maximum one point becomes a consequence, but the non crossing remains a hidden possibility. The logic of derivations screws up the logic of plausibilities from the very start.
We can not restrict our explanations to plausibilities because we become faulty.
We can restrict our explanations to derivations. This is Formalism, which today is merely a moral problem, lying. In the future it will be a logical problem too because it will turn out that there is a didactical logic. Certain truths will need the perfection of both logic.
So poor Euclid already had to depart from plausibilities from the start to reveal the truth. But at the crucial parallelity, this departure became a deeper problem, full blown Formalism.
He didn't realize that his departure has this danger, he didn't analyze how the plausibilities relate to his digging for truths. Namely, he didn't realize the crucial rule of plausibilities that they remain, reoccur on higher levels. So, to start talking about prallelity can not be didactically correct without telling the three obvious appearances. These are:
Having fix distance between the two lines.
Having the same angle to any third line crossing them.
Not crossing.
This puts the search for truth in a framework. Namely, how do these three imply each other?
This is external logic, not present in the logic of derivations at our present level of logic.
So the Formalist morons can ignore it as superficial blubbering.
Two thousand years later, when Hilbert reaxiomatized Geometry, he still wasn't aware of this didactical angle because now he was chasing something different. This new thing was relating to what I called the external mystery of parallelity. And that is the Set Theoretical meaning of Geometry. For Hilbert it meant merely to be even more precise. He already accepted very correctly that sets are the universal language of math. He stood up for Cantor who was still an "outlaw" and later died in an asylum. This was a tragedy but where is the mystery?
The mystery is why Euclid didn't regard the lines, circles all as sets of points.

The crossings as common elements are a crystal clear vision that we can not even avoid today.
Are we brainwashed by the silver platter of Set Theory?
The concept of a point as singularity, an element without elements is the plausibility, but actually Set Theory disowned this lovechild. So the plot thickened from the start.
After all these geometrical blubberings we must return to numbers and see what the crucial split between plausibilities and derivabilities means here.
The amazing news is that here there is a single method that provides all formal derivations if we strip away the meanings, the visions.
The most basic fact of logic is that there are only two elemental forms of claims, existence or universality. So we either claim that some kind of object exists or that all objects obey some conditions. What complicates this simplicity is that they can be combined. So we might claim that there is a number n that for every number m we have a certain $R(n, m)$ relation.
The main claim is still the existence of n but universality is involved as part of it. This is very rare about numbers because if we claim such n then we usually try to tell exactly what it is.
The reverse, main universality is the typical.
So we claim that for all n there is some m that the $R(n, m)$ is true.
A perfect example is the infinity of primes: For every n there is p so that: $n < p$ and p is prime.
Now, the heuristic method to prove such claims is called “induction”.
It simply means proving the claim for 1 and then proving that if it is true up to n then it is true for n too. A very primitive version is starting with 1 and then implies from n to $n + 1$.
The more general, implying from under n to n, is not merely more flexible but crucial to use the method for multiple universality. Here we claim that:

For all $n_1, n_2, ..$ there are $m_1, m_2, ..$ so that $R(n_1, n_2, ..., m_1, m_2, ..)$

Or in formal notation: $\forall n_1 \forall n_2 .. \exists m_1 \exists m_2 .. R(n_1, n_2, ..., m_1, m_2, ..)$

We can’t step through all value combinations simultaneously as increases by 1, but we might easily prove from all value combinations having values all under an N that it also follows with some values being N. And then this single N induction takes care of all n values.
Indeed, every n combination must have some maximal values and these as N was obtained.
An alternative vision of induction is obtained by looking at the negative of R:
If there are examples for this not R, that is counterexamples for R then there has to be one with minimal N. That is, with minimal maximal values of n-s. But then the undervalues are all non counterexamples and they imply that our claimed minimal counter example was false too.
The $1, 1, ..$ initial condition was still important here. Indeed, this has no under valued cases and so its truth is needed to derive the impossibilities of the $N = 2$ counter examples.
The assumption of existing n values themselves under N, is usually hidden somewhere in our arguments about these R implications. But if we don’t even have to assume the existence of these under values, then actually we prove the initial 1 case already within the induction step.
This gives a new twist in the negative view, if we continue the negative meanings inside the induction step. First of all, implications have their negative form. A implying B means not B implying not A. The A in our case is the universality of the under N R cases and B is the universality of the up to N R cases. And then the negatives can be changed from universalities to existence. Indeed: Not being true that something is always true about n-s means existing some counter example. So what we get is that the existence of an up to N case implies the existence of an under N one. And indeed, if there were a counterexample then we would have earlier and earlier ones infinitely, which is impossible. So infinite descent is created.
But as I tried to show, the original induction, or minimality or infinite descent are all the same principles looked merely differently by simple logical translations.
The final refinement of these methods is to allow something else than the maximals of n-s as N.
We can calculate something more flexible. A typical example is their product. Every value set has a product. So if we can prove from the value sets under a product that they imply the value sets with up to that product, then again we reach all value sets. The universality is guaranteed.

In the concrete situations these inductive reasonings always speak for themselves. It's not the achieved universality that is problematic, rather the surprising simplicity without a vision.
And yet, the relation to the visual logic is undeniable. A best example is the relative primeness and the separate dividing or external atomness of primes. The inductive proofs still rely on these, but totally differently as our long and visual explanations. There we painted worlds with details leading to new facts like the super common divider. Now we reprove things sticking to claims.

Claim:
If n , d are relative primes and $m\,n = k\,d$ then d divides m and n divides k.

Proof: Infinite descent on the $m\,n = k\,d$ value.

If d divides m then dividing both side with d we get $\frac{m}{d}\,n = k$ so n divides k too.

If n divides k then dividing both side with n we get $m = \frac{k}{n}\,d$ so d divides m too.

So, a counter example must be with both d doesn't divide m and n doesn't divide k.

If $n = d$ then they can only be relative primes if they are both 1 so our claim is true.

If $n > d$ then d divides $m\,n - m\,d = m\,(n - d)$, that is $m\,(n - d) = k'd < m\,n$.
Also, d is relative prime with $n - d$ too. So:
If $m\,n = k\,d$ is a counter example, d doesn't divide m, so we got a smaller counter example.

If $n < d$ then n divides $k\,d - k\,n = k\,(d - n)$, that is $m'n = k\,(d - n) < k\,d$.
Also, $d - n$ is relative prime with n too. So:
If $m\,n = k\,d$ is a counter example, n doesn't divide k, so we got a smaller counter example.

This was some sneaky argument. You have to go through a few times to see that it was real.

As we explained, the separate dividing by primes follows from this but is much weaker.
Now we give a proof for this too :

Claim:
If a p prime divides $m\,n$ then p divides m or p divides n.

Proof: (Infinite descent on $m\,n$ and $p = \text{minfact}\,(m\,n)$)

We'll show that there can be no such p , m , n values that are not obeying our claim.
If there were, then there were a minimal $m\,n$ product valued among these counterexamples.
In fact, among these there were ones with minimal p prime value too.
So our p, m, n are now such set. No smaller $m\,n$ product and p can exist as counter example.
We show that this leads to contradiction. Namely, we show that both p being less than m or n or being bigger than them leads to smaller counter examples. Of course p being one of them can not be a counterexample, so these are the only scenarios. An other way of saying this is that we create an infinite descent because in either case we show smaller counter example.
$p < m$ or n is the trivial case. Say $p < m$. Then p divides $m\,n - p\,n = (m - p)\,n < m\,n$.
If p didn't divide m nor n then it stands again. p doesn't divide $m - p$ nor n.
Now, if $p > m$, n then $p\,p > m\,n$. But p dividing $m\,n$ means $k\,p = m\,n$ and so here $k < p$.
This k must have some q prime factor for example $\text{minfact}\,(k)$ is one. Of course, $q < k < p$.
But then either q, m, n is again a smaller counterexample, or if q divides one of m or n say m, then dividing with that we get $\frac{k}{q}\,p = \frac{m}{q}\,n < m\,n$ and here p can not divide again separately if it didn't for m and n. So we got a smaller counter example again.

The U.P.F.T. seems like a fundamental theorem and as I said it is also called this way too but up until now we didn't really give applications of it.

To enhance the importance of the U.P.F.T. we can introduce the exponents for the repetitions among the prime factors:

$100 = 2 \bullet 2 \bullet 5 \bullet 5 = 2^2 \bullet 5^2$

But an unexpected extra advantage comes if we generalize the exponents to 0 too.
What should it mean? Well, first check out the rule of subtraction:

$\frac{5^7}{5^4} = \frac{\cancel{5 \bullet 5 \bullet 5 \bullet 5} \bullet 5 \bullet 5 \bullet 5}{\cancel{5 \bullet 5 \bullet 5 \bullet 5}} = 5^3 = 5^{7-4}$ In the special case, $\frac{5^4}{5^4} = 5^{4-4} = 5^0 = 1$

This 0 exponent being 1, becomes very convenient to "use" the actually non appearing prime factors:
$100 = 2^2 \bullet 3^0 \bullet 5^2$
Then if another number is produced the same way, like
$15 = 2^0 \bullet 3^1 \bullet 5^1$ we can easily calculate their product with the sum of exponents:
$100 \bullet 15 = 2^2 \bullet 3^1 \bullet 5^3$
So the prime factorization of products can be obtained by addition instantly.

A much more important theoretical consequence of the U.P.F.T. is that every number means a unique sequence of exponents. So, allowing 0 among the naturals, every finite ordered sequence or so called $(t_1, t_2, \ldots, t_n)$ tuple can be coded by a single c natural number.

Namely, as $c = 2^{t_1} \bullet 3^{t_2} \bullet 5^{t_3} \bullet \ldots \bullet p_n{}^{t_n}$. Here p_n is the n-th prime number.

This is surprising because there are much more tuples than individual numbers.
But as infinites they are the same.
To code just the duos is fairly easy. We can simply go by increasing totals:

$(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), (1,2), \ldots$

Or we can go by increasing maximal members:

$(0,0), (0,1), (1,0), (1,1), (0,2), (1,2), (2,0), (0,3), \ldots$

The code itself can be the position number. So for example (1, 1) has code 5 in the first system while 4 in the second.
Doing similarly for strict naturals that is avoiding 0, we can actually list all possible fractions:
$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \frac{3}{2}, \frac{3}{1}, \frac{1}{4}, \ldots$
Then looking at how these would lie on the number line, we get a shock because they densely "fill-up" the whole half line from 0 to infinity.

The coding of not just duos or trios but all tuples at once by single naturals was crucial when Gödel proved his famous Incompleteness Theorem. The basic idea was that using merely addition and multiplication we can express all effective derivation systems.
A best example is exponentiation.
The conventional way to define this from multiplication is: $\underbrace{x \; x \; x \; \ldots \; x}_{y \text{ many}} = x^y$

Of course this is not explicit due to the used "dots".

Peano replaced this loose definition by an effective generating system with two rules:

1.) $x^1 = x$

2.) If $x^v = w$ and $v + 1 = y$ and $w\,x = z$ then $x^y = z$

The fact that all effective systems are explicit from addition and multiplication then means that this system can also be replaced by a single formula containing only addition and multiplication plus logical symbols, including the mentioned two quantors that is existence and universality.

This is pretty unbelievable, though it doesn't alter the way we introduce exponentiation neither in elementary schools with "dots" nor in high schools with Peano rules.

But to see why the tuple coding is the crucial in proving this explicitness is also merely high school level math.

Strangely, we need not this c code, ordered to the $(t_1, t_2, . . , t_n)$ n-tuple of naturals because these themselves contain the "dots". Rather we need a reverse "decoder". A two variable $T(c, i)$ formula that for every c and i value gives t_i that is the i-th member of the c coded tuple.

The fact that we don't know when the tuple ends is not really a problem. The only point is that every tuple should be the beginning of these decoding values. How they continue is irrelevant.

Indeed, to claim that for example $x^y = z$ means merely to have a tuple that contains the numbers $(x, x^2, x^3, ... , x^y = z)$. To say this, is easy:

$$\exists\, c \;[\; T(c,1) = x \;\text{ and }\; \forall\, i < y\,(\, T(c, i+1) = x\, T(c, i)) \;\text{ and }\; T(c,y) = z \;].$$

This explicit formula is then equivalent to $x^y = z$, that is, it will be derivable for same values.

It's easy to see now that other derivation systems similarly become explicit with $T(c, i)$.

The obvious problem is that that the prime factorization exponents as coding is already containing exponentiation. So, Gödel had to use a simpler one, relying on merely multiplication. In fact, there are two equally beautiful solutions, both using basic facts of relative primes and the factorial.

Back To Visions, Multiple Differences

We are looking again at the two multiple sequences parallel and geometrically above each other.
But now we not merely look at the equalities rather all possible differences of the multiples.
The equalities are simply special 0 differences, so we clearly include the previous problem.
As usual, looking at a wider problem can actually simplify things but with the risk of becoming abstract and loosing sight of the special problem.
Amazingly, these m n – k d and k d – m n values behave similarly as the equalizations did.
So they are all merely multiples of the minimal. But the big difference is that this is not happening in an order of the sequences that is from left to right. That's why we said minimal and not first.
Also, a formal exactification is necessary. By minimal we have to say minimal non zero because otherwise this 0 difference is the obvious minimal and the others can't be multiples of this.
More to the point, where this minimal non zero difference appears is quite unpredictable.
The good news is that the repetition of the initial segments up to the first equality also means that these possible differences will repeat too. Of course bigger new differences appear later.
So we have to allow the infinite sequence to tell all possible differences but amazingly, this allowing actually helps to tell the possible small differences too, inside the first equality.
The logic of the crucial argument is the same here as was for the equalities:
So, first of all it is obvious that for any m n – k d or k d – m n differences the double triple or any j multiple again exists. Namely, (j m) n – (j k) d or (j k) d – (j m) n will be such.
The less trivial part is that if the difference was the minimal non zero, then every other has to be a multiple of it. At the equalities this was easy because they were simply one dimensional and so the first "next" equality was simply shifted version of the very first. Here, the possible differences are two dimensional in the sense that they are generated by the two m , k multipliers.
So we prove something else first, namely that difference of differences is difference.
Subtracting two m n – k d and m'n – k'd differences from each other we can combine the n-s and the d-s but instead of difference we might end up with a multiple sum.
Luckily, any m n + k d can be turned into difference as (m + k d) n – (k n – k) d.
So the difference of two differences is always a difference itself.
Knowing this now we can see why the minimal non zero difference must divide all others.
Indeed, we can subtract this minimal from any other and get a new difference. Repeating this, either the minimal divided the other and so we end up with 0 or we should get a remainder. But this would be a difference smaller than the minimal so this is impossible.
Amazingly, this same remainder refutation argument can be applied to not only the minimal difference and an other but the minimal and any of the two new unit numbers n and d.
Indeed, subtracting the minimal from these, we also get new differences. Or a more abstract way is to allow 0 multipliers and then n and d are automatically differences already.
At any rate, the end result is that the minimal difference must divide both n and d too. So it is a common divider of them. Now comes a trivial but crucial point about all multiple differences:
Any c common divider of n and d must divide any multiple difference made from n and d.
Indeed, multiples of n and d have all dividers of them and their differences contain the common ones too. But then the s minimal multiple difference is a common divider of n and d so that all other c common divider divides s. So the letter s stands not for being the smallest difference, rather being such "super common divider" of n and d.
This super common divider is obviously the earlier used g greatest common divider.
By its definition as g, it was not obvious at all that it is a super, that is contains all other dividers.
So, these multiple differences revealed that g is always s.
We can raise one objection to our arguments above. Namely, we assumed the existence of a minimal non zero difference though we saw that there are infinite many differences.
But infinite many numbers don't have to have a minimal. Luckily, it's easy to dodge this problem.
The new differences after the first equality are all big. Or to put it differently, the smaller ones are already all there before the first equality. These are finite many only.

There is a way to be more specific and regard only the remainders as special multiple differences.

In fact, we break the symmetry and use again d as the divider. So then we look at only one sequence of numbers: n , $2n$, $3n$, $4n$, . . . and from this, get its remainder sequence:

$$[n] \ , \ [2n] \ , \ [3n] \ , \ [4n] \ , \ . \ . \ .$$

Here [ ] denotes the remainder to d as it will always from now on.
This whole view is non geometric any more but it is useful because it emphasizes an other point. Namely, the easy concrete calculabilities of such remainder sequences.
This approach proves both the last section's result about the relative prime n , d and also the aboves about g being s. So we start from scratch explaining everything again.
As we'll see the multiple differences will still sneak into our approach but with a different emphasis, as merely alternative to remainders.

A simple example of a multiple remainder sequence with $n = 10$ and $d = 7$ is:

$$\begin{array}{cccccc} [10] & , & [20] & , & [30] & , & [40] & , & . & . & . \\ || & & || & & || & & || & & & & \\ 3 & & 6 & & 2 & & 5 & & & & \end{array}$$

Indeed:

$$3 = 10 - 7 \quad , \quad 6 = 20 - 2 \bullet 7 = 20 - 14 \quad , \quad 2 = 30 - 4 \bullet 7 = 30 - 28 \quad , \quad 5 = 40 - 5 \bullet 7 = 40 - 35$$

Even though our sequence is infinite, the appearing values can only be finite, maximum d many. So, a trivial fact is that there has to be a member that returns to an earlier value.
If the value is the same as the first $[n]$ then we call the "return" a "restart".
Playing with a few examples, the first crucial thing we realize is that to calculate the remainders we don't really have to use the bigger and bigger numbers in the brackets, rather we can use the last calculated members, add the fix n to that and calculate the remainder of this.
For example above the second member 6 is also $[3 + 10] = [13]$ which is not much simpler but then the third 2 is actually $[6 + 10] = [16]$ then $5 = [2 + 10] = [12]$.
The validification of this method is quite simple:

$$[(m + 1)\, n] \ = \ [m\, n \ + \ n \ ] \ = \ [\ k\, d + [m\, n] \ + \ n \ ] \ = \ [\ [m\, n] + n \ ]$$

Indeed, first of all the $[m\, n]$ remainder means that it is obtained from $m\, n$ by subtracting a d multiple, that is $[m\, n] = m\, n - k\, d$ and so $m\, n = k\, d + [m\, n]$.
Then, leaving off a d multiple doesn't change the remainder, that's why $k\, d$ can be omitted.
The official name for this heuristic method of calculating the members is "iteration".
Most of the time the iteration is the actual definition and the real problem is how the sequence behaves and obeys some non iterative rules. But here it is quite opposite. The iteration is the blessing against the original definition. Beside this blessing being the practical method of calculation, it has an instant theoretical consequence too. Namely it means that once we have a return then the following members repeat too. We simply must have a repeating cycle.
The logical question is what this cycle can be. Does it have to be a restart? Does it have to happen after some particular members? Which we'll usually call being simple.
The universal rule of return in any remainder sequence from a [B] member to an earlier [A] is quite simple:

$$[\ A \ ] \ = \ [\ B \ ] \quad \leftrightarrow \quad B - A \ = \ K\, d$$

Thus, in our case, from $B = m\, n$ a return to an $A = (m - k)\, n$, that is k place earlier, means: $m\, n \ - \ (m - k)\, n \ = \ k\, n \ = \ K\, d$ and so $[\ k\, n \ ] = 0$.

So a 0 definitely must appear before a first return. On the other hand, after a 0, we definitely will have [0 + n] = [n] that is a restart. So our whole sequence is a repetition of the initial segment up to the first 0 occurrence. In general terms: Our sequences have only restarts as returns. And: Every such must happen after a previous 0 that signals the restart, so the restarts are simple too.
We also know that the m = k d places are 0-s because [k d n] = 0.
So the only question is whether there can be other 0-s beside these trivial ones.
And amazingly this is exactly our original problem. If only the m = k d multiples of d allow 0 remainder in m n then this means that for d to divide m n , it must divide m.
So this is what we expect for d , n relative prime values.
In view of the repeating cycle, we only have to show that before the m = d first trivial 0, there can be no 0 at all. In general terms: With relative prime d , n there is no early simple restart.
Which is the same as not having early return either.
Indeed, we showed that all returns can only be simple restarts.
The idea to show that no 0 can appear before d, is the so called “pigeon hole” principle:
We’ll show that all the non 0 that is 1 , 2 , 3 , . . . , d – 1 potential values appear.
But we only have d – 1 many places or “holes” before d, namely 1 , 2 , 3 , . . . , d – 1.
Thus there is no room for 0 to appear. Only 1 , 2 , 3 , . . . , d – 1 appear, reordered.
This fullness of the possible remainders is our generalized claim for relative prime d , n.
This implies the no 0 occurrence before d and thus the general fact that d divides m.
But first we go with arbitrary d and n.
Here, the 0 can appear before the trivial m = d even more times and other values can repeat too.
So we have ugly situations but one beautiful fact remains.
Namely, that the possible values are simply multiples of the minimal non 0.
The heuristic trick to show this is to widen the scope of the remainders.
What is really an [m n] remainder ?
It is some repeated subtraction of d from m n , that is: m n – k d.
This fact that n is also multiplied with an m and d is also with a k, suggests a symmetry that we ignored by emphasizing only d as the divider. So what if we allow the switch in positions, that is subtracting not from an n multiple a d multiple rather from a d multiple an n .
Could such k d – m n values when are positive and fall under d bring in some new numbers or are they merely a new way of producing the same m n – k d remainders?
We show that they are merely new ways to get the same old remainders.
An example will show even a rule for this. So let d = 5 , n = 7 , m = 3.
The normal remainder is m n – k d = 3•7 – 4•5 = 1. Can we obtain it in reverse?
After a few trials we’ll figure it out as 3•5 – 2•7 = 1. So what’s the rule?
The 3 being the same is accidental. The point is that the opposite multipliers added give the two numbers n = 7 and d = 5. Indeed: 3 + 2 = 5 and 4 + 3 = 7. In general:
m n – k d = (n – k) d – (d – m) n = n d – k d – d n + m n.
This works for small multipliers under our numbers n and d.
We claim that for M n – K d “big” multiple differences, we can replace these, by simply using M’s m remainder to d and K’s k remainder to n.
Indeed, if M = a d + m and K = b n + k then writing these in their places:

(a d + m) n – (b n + k) d = a d n – b d n + m n – k d = (a – b) d n + m n – k d =

[(a – b) n – k] d + m n = [(a – b) d + m] n – k d. This was a remainder to d but

a < b makes this last form negative and a > b makes the previous form bigger than d.
So a = b and thus indeed this remainder is actually m n – k d.

Knowing that these multiple differences are always the good old remainders, gives us the tool to prove three fundamental claims:

1.) If r and t are two remainders that r + t < d then this r + t is a remainder too.
If r < t are two remainders then t – r is a remainder too. Indeed:
Adding or subtracting multiple differences we only create new multiple differences or sums.
Only multiple differences can have values under d and these are all remainders too.

2.) Applying additions repeatedly we see that remainder multiples under d are remainders.
And with subtraction, we see that remainders of remainders are also remainders.

3.) Subtracting remainders from d or n we again create multiple differences or sums .
So with using 1.) and 2.) : Remainders of remainders in d or n give remainders too.

Now lets regard the s smallest non 0 remainder.
First of all, the multiples of this, that is k s are all remainders up to d.
But actually there can be no others either. That is, every r remainder must be a multiple of s.
Indeed if it weren't then we had a remainder of s in r that is smaller remainder than s.
So indeed we obtained the remainder values as a multiple sequence, but we are not finished.
We still haven't used 3.) which gives the big surprise:
This s smallest remainder must divide both d and n too.
Indeed, otherwise again we could produce smaller remainder by the remainder of s in d or n.
This proves our claim for relative prime d and n.
Indeed, then s is 1 and so the remainders are all multiples of this, that is all values.
Thus 0 can not appear and so only d and its k d multiples as m can make [m n] = 0.
This means exactly that if d divides m n then d divides m.
An even bigger surprise is still there for the general situation:
Not only s divides both d and n but all common dividers of these two must divide s too.
So s is a "super common divider" of d and n.
Indeed, s itself is a multiple difference from d and n.
But any common dividers of them divide their multiples and differences of these, so divide s too.
Of course, this s super common divider is automatically the greatest common divider.
Such greatest common divider obviously exists for any two d and n numbers, and we just proved that it is always a super too.

Unique Simplification of Fractions, Euclidian Algorithm

You might wonder why I left something about fractions to the end of this section.
Indeed, fractions are elementary school stuff, practically the simplest thing after counting.
I am still not even sure whether they should be introduced before the negative numbers or after.
One thing is sure, they have to be introduced before the decimal point.
This is sometimes violated due to the use of pocket calculators.
This is not to say that calculators should be avoided. They are very useful to make the decimals plausible, even the infinite decimals.
What we definitely should avoid are those rare calculators that can use fractions.
In a sense this whole problem is over magnified because probably the primes themselves should merely be a "garden" not a "road".
This means that they can be introduced in elementary school but they don't belong to the unavoidable "must", that everybody has to go through. Fractions do!
And yet these two interrelate as we see soon. But we can not loose sight of the bigger picture.
The big picture is that kids hate math! The biggest lie is to deny this.
The next biggest lie is the "creative bullshit". This claims that we can make math joyful by directly regarding it as problem solving.
Just as reading and writing is a road to enjoy books and writing letters or even poems later, the same way math has a language of abstractions too. But just as learning reading and writing can be fun, the learning of math's basic language doesn't have to be torture either. It becomes a torture because it is not properly taught, namely too little is taught not too much.
The "creative bullshit" actually skips the fundamentals and suppresses real creativity that can only be awakened by first bringing out the innate a priory abstractions.
The crucial, absolutely irrefutable proof of my claims is when real motivation appears.
Not from manipulated external successes, rather by the awakened abstractions themselves.
When children solve the real problems with the drills we equip them, then instant real inner motivation and respect for the reality of the whole field awakens.
Subjectivity and objectivity unites, as it always must in learning.
But is there a minimal absolute road toward this? Yes there is. Hallelujah, praise the Lord.
And the Lord's name is Larichev. He created in the fifties this bible of mathematical minimum.
It was a systematic and didactical purification of our modern usage of variables, combined with the simplest practical self verification, the so called "word problems".
If you can not solve word problems you know nothing and if you can solve word problems then you can learn everything else yourself. It's that simple as that. The rest is politics.
Why we pretend to preach the importance of math but avoid to teach the tools.
Larichev solved the problem, we simply must stop lying.
So, I also stop talking about this whole thing now, and return to our garden, the primes.
As I mentioned, the logic of derivations is different from the logic of visions.
The $m\,n = k\,d$ equalities with given n and d values was much easier to see than the shorter inductive proofs. But now comes the big surprise. There is an even better visibility.

This $m\,n = k\,d$ can also be written as $\frac{n}{d} = \frac{k}{m}$.

So a given $\frac{n}{d}$ fraction's alternative forms are our earlier equalizing multipliers.

Now a much better notation is of course $\frac{n}{d} = \frac{N}{D}$.

This notation expresses our feeling of a common monotony of the numerator and denominator.
Indeed, to stay equal, the numerator and denominator both must decrease or increase together.

The first thing we learn about fractions is that they can be expanded : $\frac{2}{3} = \frac{4}{6} = \frac{6}{9}$

In fact, we use expansions to add fractions by first changing them to have common denominators.

To solve simple equations and thus word problems concretely, we have to use these fraction operations and yet we never really face a “simple” problem.

The reversal of expansion is simplification. In our results, we look at the numerator and denominator and if we see something common we simplify. We repeat this if possible. If they have no common factor any more, that is they are relative primes then the result is simple, can not be simplified any more. What we never contemplate is whether these simplifications are unique.
Or negatively: Could a fraction be simplified two ways with different simple result?
The “different” here of course means different numerator and denominator but same value.

So, could $\frac{n}{d} = \frac{N}{D}$ be true for both sides being simple fractions and not identical?

Our earlier result was that all equalizing multipliers are merely multiples of the minimal.
And these were the only relative prime equalizing multipliers.
So, this answers our question negatively at once.
But why does this feel so much more obvious here among fractions?
We clearly have here an example of the already mentioned higher plausibilities like the parallelity was in geometry. This analogy will become an amazing actual correspondence.
But first, lets try to inject our old minimal argument into the new fraction meaning directly.
The minimal version of a fraction is not a natural idea. It can be imagined though by trying out all smaller possible numerators and denominators and check equality by multiplying over.
Equal fractions must have same minimal version. Indeed, equality is “transitive” and so the smaller of two minimals were the real minimal.
The transitivity itself is plausible but actually only follows by multiplying over:

$\frac{n}{d} = \frac{N}{D} \rightarrow n D = d N$ and $\frac{N}{D} = \frac{\eta}{\delta} \rightarrow N \delta = D \eta$

So indeed: $n D N \delta = d N D \eta \rightarrow n \delta = d \eta \rightarrow \frac{n}{d} = \frac{\eta}{\delta}$

The crucial point is to prove why all equal fractions are expansions of their minimal.

$\frac{n}{d} = \frac{N}{D}$ implies not only $n D = d N$ but also $n D - n d = d N - n d$, that is:

$n (D - d) = d (N - n)$ which means also $\frac{n}{d} = \frac{N - n}{D - d}$.

So, the differences of the numerators and denominators from two versions of a fraction give also a third version. This can not be smaller than the minimal, so indeed between the expansions of the minimal there are no variants.
For years I thought this is the simplest possible way to show that equal fractions have common simplification. I knew that this difference fraction argument was pretty ad hoc but I accepted it.
Then one day after I simplified the Gaussian integers to the connector system to explain the square sums, I realized that there is a totally elementary geometrical proof for the minimal fractions.
The start is to have a better condition for equality than the sheer algebraic multiplying over and seeing $n D = d N$. Something that stays with fractions. This is the following:

Equal $\frac{n}{d} = \frac{N}{D}$ fractions can be expanded to be identical.

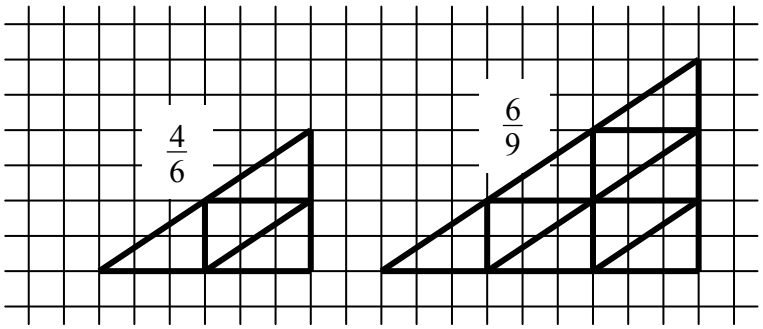
The first must be expanded by the trivial 1 valued fraction $\frac{N D}{N D}$ that is as: $\frac{n}{d} = \frac{n N D}{d N D}$.

The second by the known $n D = d N$ equality used as the 1 valued fraction $\frac{n D}{d N}$ that is as:

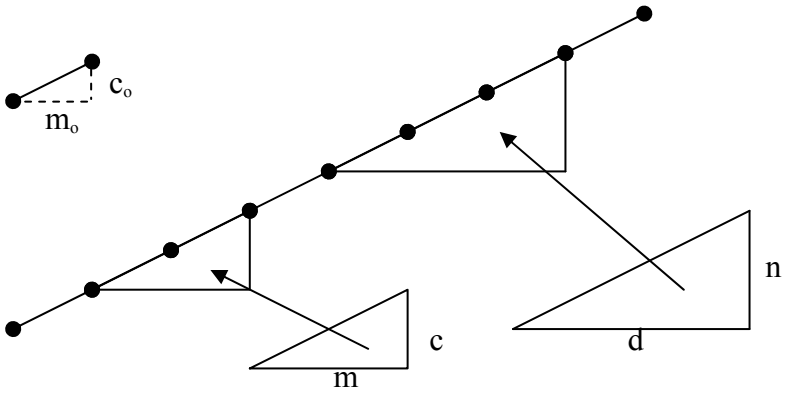
$\frac{N}{D} = \frac{N n D}{D d N}$. As we see, we obtained identical fractions: $n N D = N n D$, $d N D = D d N$.

The connector system is an infinite tiling with square tiles. No coordinates, just infinite squares.
The corners can be connected. The horizontal and vertical steps can correspond to a fraction.
By convention, the vertical being the numerator and the horizontal the denominator.

The expansions of $\frac{2}{3}$ like $\frac{4}{6}$, $\frac{6}{9}$ are combining of shifted copies and trivially mean parallel connectors:



Thus, the above fact that two equal fractions imply identical expansions, now also means that two equal fractions are parallel connectors. So these can be aligned, that is shifted to a common line:



Thus the common minimal simplification becomes self evident. Namely, as the minimal connector of that line, that repeats on it. So the whole ad hoc or indirect multiplicity proof is avoided.
Thus, we can prove the external atomness of primes, Unique Prime Factorization, all these things through simple geometry!
We should present the tiling or grid system at very early age. Even investigate the perpendicularities there. As we'll see, these lead to the geometry of square sums and the Gaussian integers. But to use the connectors as standard derivations is didactically incorrect.
To walk in the gardens is never forbidden, but we shouldn't declare such excursions into the wild, as roads that everybody must learn.
The idea of "roads" that everybody must learn sounds like some fascist totalitarian thought control. Yet it is in fact the most democratic step that a society can and must do.
Honest observations into real learnings and desire to teach, are that determine these roads.
Moron academic educational gurus will never promote such roads, rather introduce their new curriculums in their sneaky ways. That's real fascism. The new fascism of the modern age.
I mentioned the most solid road, Larichev's method of word problems. It is actually a proof. A proof of the fact that everybody can learn to solve word problems. There are no good ones and bad ones on a road. There are no marks. Everybody can walk talk read write and the early differences in how fast we learnt these things fade away and give rise to true differences in creativities using these "musts" as language.
But our privilege conserving, lying social structure promotes the differences from, the beginning.
Kids should be forced to help each other not pretentiously put up politically correct fronts behind which they already strive for one thing only, to be above the others.
So, "roads" are public utilities, allowing to travel, to discover and also to discover to help others.
Calculating with fractions is such road. And there is also a simple method that guarantees simplifications without guessings and proves uniqueness too. So obviously this is a road too.

The start of this method is if our result is a fraction with a bigger numerator like $\frac{54}{15}$.

The natural idea is to cut of the whole parts and keep only the remainder of 15 in 54 as new numerator: $\frac{54}{15} = 3\frac{9}{15}$. We call this a "mixed number" because it mixes whole and fraction.

Now comes an "insane" idea to turn this fractional part upside down and do the same again.
$\frac{15}{9} = 1\frac{6}{9}$. We do the same again: $\frac{9}{6} = 1\frac{3}{6}$. And finally : $\frac{6}{3} = 2$.
So the fraction parts must disappear because the last denominator divides perfectly.
Amazingly, it is perfect in an other sense too. Namely, it is the total simplifier in our original fraction. So, $\frac{54}{15}$ can be totally simplified by 3, giving $\frac{18}{5}$. The justification is quite simple.

Lets take an initial $\frac{N}{D}$ fraction with $N > D$ and reach the last $\frac{n}{d} = w$ whole fraction:

1.)
Cutting of whole parts keeps all common dividers for the next fractions. So all common dividers of the original numerator N and denominator D, divide this last d denominator too.
2.)
The new numerators are always remainders of the previous fraction. In other words, the previous ones are multiple sums from the new fractions: $54 = 3 \bullet 15 + 9$, $15 = 1 \bullet 9 + 6$, $9 = 1 \bullet 6 + 3$.
We can write this last into the previous, that one into the previous again, and so on.
Thus, the original numerator and denominator are also multiple sums from the last fraction.
But $n = w\,d$ so writing this into n, actually: $N = M\,d$ and $D = m\,d$.
So d divides both N and D.

1.) and 2.) means that d is the super common divider of N and D.

But that's not all. There are two theoretical points too:

1.)
The consecutive multiple sum multipliers are the whole parts.
So, the final M and m multipliers are also determined by the whole parts.
2.)
These whole parts are the same for equal initial fractions.
So by 1.) and 2.) M and m are the same too. So, equal fractions simplify to the same $\frac{M}{m}$.

This method was the Euclidian Algorithm. A "must" road that leads to many gardens.

Blind Spots

A power sequence is : n , n^2 , n^3 , . . .

Its remainders to a d divider are the power remainders : $[n]$, $[n^2]$, $[n^3]$, . . .

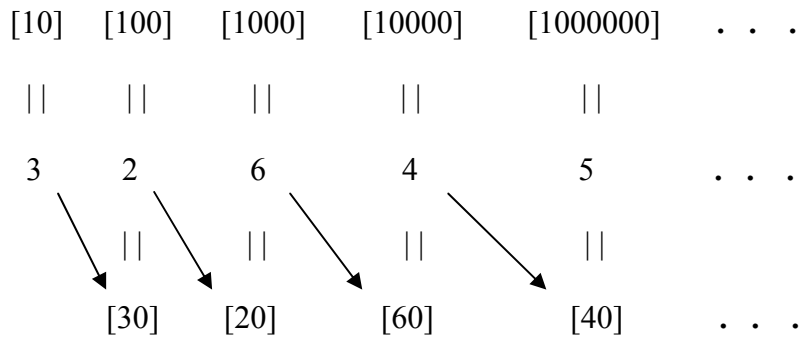
The iterativeness of the multiple remainders was caused by:

$[(m+1)\,n] = [\,m\,n\ +\ n\,] = [\,j\,d + [m\,n]\ +\ k\,d + [n]\,] = [\,K\,d + [m\,n] + [n]\,] = [[m\,n] + [n]]$

Here the argument of iterativeness is:

$[n^{m+1}] = [n^m\ n] = [\,(\,j\,d + [n^m]\,)\,(\,k\,d + [n]\,)\,] = [\,K\,d\ +\ [n^m]\,[n]\,] = [[n^m]\,[n]]$.

Here, this is an even bigger advantage because n^m grows to billions in few members already.
As an example with the iterative calculation for $n = 10$ base and $d = 7$ divider is:



As we can see, the remainders can be calculated from the much smaller bottom values, obtained from the previous remainder.
This calculability of the members from the previous members means again that once we have a return, the whole sequence becomes a repetition of a fix segment.
The return can happen to the very beginning, that is to the $[n]$ value and then we call it a restart.
Then the repeat is an initial segment.

The simple restart after a 0 at the multiple remainders was caused by: $[\,0\ +\ [n]\,] = [n]$.
The corresponding simple restart here is caused by a 1 remainder: $[\,1 \bullet\ [n]\,] = [n]$.
But this similarity then becomes very different:
At multiple remainders we always had only restarts as returns. Also, simplicity, that is previous 0 was always the case. In fact, the only real problem was what appears before the first 0.
We solved this problem. The remainders were multiples of the minimal.
At relative prime d , n these were all possible values 1 , 2 , . . . , $d-1$.
For non relative prime d , n this is impossible because any c common factor of d , n is factor of all the remainders by $r = m\,n - k\,d$.

This same logic applies here among power remainders, by $r = n^m - k\,d$.
So, for non relative prime d , n here too the c common factors of d , n are factors in all the remainders too. In particular, 1 can not appear in such non relative prime sequences.
But in reverse, the relative primeness is enough to guarantee 1 , that is simple restart.
Indeed, the theoretical condition of the return is the same again:

$[n^m] = [n^{m-k}]\ \leftrightarrow\ n^m - n^{m-k} = n^{m-k}(n^k - 1) = K\,d\ \leftrightarrow$ d divides $n^{m-k}(n^k - 1)$

So if d , n are relative primes then d , n^{m-k} are relative primes too and so d divides n^k-1, that is $[n^k] = 1$. Thus, we actually have a simple restart before this return at m.
This of course implies that before the first 1 occurrence at $m = \mu(d , n)$ we can not have return.
In this initial segment up to μ, we must have all different remainders and not including 0 or 1.
And the whole remainder sequence is a repetition of this initial segment.
The non occurrence of 0 is trivial because it can only occur if d divides n and then the whole sequence is all 0-s.
A full analysis of the returns in general would mean a full analysis of how it is possible that d divides n^{m-k} (n^k-1). This would tell when must a return be restart without being simple.
This obviously involves the examinations of composite d-s and their prime factors.
It is too difficult now and instead we go towards the simple or 1 occurrences.

The biggest difference from the multiple remainders is that while there we had the trivial 0-s at the $m = k\,d$ places because $[k\,d] = 0$, here we don't have such trivial 1 occurrences.
This is not quite true because we do have trivial 1 occurrences that can be gradually applied to less and less trivial situations. The most obvious case is $n = k\,d + 1$ as base and then $[n] = 1$, so we have a full 1 sequence. The next, one step less trivial situations is $n = k\,d - 1$ and then we have the alternating remainders $d-1$, 1 :

$$[k\,d-1] \quad [(k\,d-1)^2] \quad [(k\,d-1)^3] \quad [(k\,d-1)^4] \quad . \quad . \quad .$$

$$\begin{array}{cccc} || & || & || & || \\ d-1 & 1 & d-1 & 1 \end{array}$$

Defining other n bases through d, we can create 1-s at particular places.
This gradual de-trivialization of 1 occurrences was never systematically examined because a totally different 1 occurrence took the role of the trivial or standard 1 places.
The original discoverers were ancient Chinese mathematicians who observed for $n = 2$ base that we always have a 1 occurrence at the $d-1$ place if the d divider is an odd prime number.
In short : $[2^{p-1}] = 1$ or p divides $2^{p-1}-1$ for all primes above 2.

Indeed : 3 divides $2^2-1 = 3$, 5 divides $2^4-1 = 15$, 7 divides $2^6-1 = 63$, and so on.

Of course, the 1 at $p-1$ means we have 1-s at all $k(p-1)$ and restarts at $k(p-1)+1$.
So, these as trivial simple restart places mean one step shorter period than in multiple remainders.
They had the 0-s at $m = k\,d$ and the restarts at $m = k\,d + 1$.
These $k(p-1)$ as trivial or standard 1 places, at once define the new meaning of "early" too.
At multiple remainders an "earliness" meant a 0 before $m = d$ and it happened exactly if d , n were not relative primes.
Here earliness means a 1 remainder before $d-1$ for relative prime d , n.
This 1 of course implies a restart at d and so in general an early restart means any restart before d or even more generally an early return is any return before d.
Since for non relative prime d , n we have only remainders with common factors, we can not have all possible numbers under d as remainders and so earliness is an absolute must.
In fact as we'll see, even only relative prime n with d is actually guaranteeing earliness and only prime d can have non early return which is of course simple restart.
But can we have earliness with prime dividers too? Yes we can.
In fact, our example above with $n = 2$ and $p = 7$ is already a case:
The standard $m = p-1 = 6$ is not the first 1 place. Indeed, $m = 3$ gives 1 remainder too because $[2^3] = [8] = 1$.

So, the Chinese mathematicians must have known that, $p-1$ is not always the first exponent that gives 1 remainder but it's a sure place for that. But what's the importance of this fix 1 place?
It's very probable that they were aware of how hard it is to verify primalities for big primes.
We have to check smaller primes whether they divide or not.

In contrast, to establish $[2^{p-1}] = 1$ is easy because we don't have to calculate the huge 2^{p-1} value rather use iteration.

Of course, this prime testing is only reliable if for composite d we can never have $[2^{d-1}] = 1$.
Unfortunately, this is not true. The first such composite is $d = 341 = 11 \bullet 31$.
This can be obtained by continuing the above outlined de-trivialization of particular n bases.
We'll come to it in a second.
As I mentioned this was never done, even though it is easy, almost elementary school stuff.
The ancient Chinese mathematicians missing it is understandable because it requires newer algebraic notations. But Euler missing this 341 counter example is almost unbelievable.
This was a first sign of a general phenomenon of tunnel vision or blind spots, that continue with much more shocking examples by Gauss. In fact, the fourth theorem of this section is almost a trivial consequence of the previous by Gauss if we only regard derivabilities.
Of course derivabilities are not the essence of math.
The true reason of these blind spots for Gauss was exactly his obsession with proofs only.
It is not only not fashionable to tell these things, they are actual taboos.
The taboos and lies start much earlier.
Number theory starts with Fermat who rediscovered, generalized the ancient results and recognized all new basic laws, including one that became the most important unsolved problem of mathematics. The conflict of Fermat as a person was that he knew a lot but proved almost nothing.
That wouldn't have been a conflict if he hadn't vision himself as the very smart derivator.
This was the fashionable, the expected from mathematicians at his time already.
He was a Judge so it's even more shocking that he was a compulsive liar. Modern moron commentators contemplate whether he had indeed a proof for his infamous "Last" or more appropriately "Lost" Theorem. Of course he didn't and he knew it exactly well. He simply muddied the water so he could claim credit later. In his letters to his friends he also often claimed to have proofs that he could not give "due to lack of space for the lengthy derivation".

Fermat generalized the above Chinese rule for all n bases, that is claimed that $[n^{p-1}] = 1$ except for the trivial cases when p divides n and so we have all 0-s.
So, this so called Fermat's Little Theorem establishes the standard 1 places as $p-1$ for all bases.
He continued the mistake of assuming the false belief that this can only be with primes, which is now even bigger mistake than by the Chinese mathematicians because for arbitrary n bases there are trivial counter examples. The simplest is the mentioned $n = d+1$ giving all 1-s.
The next less trivial counter examples come from the mentioned $n = d-1$, giving the alternating remainders $d-1$ and 1. If d is odd then this means a definite 1 at the $d-1$ = even place.

The first three cases $d = 3, 5, 7$ are primes, so this 1 is guaranteed by $[n^{p-1}] = 1$ that is Fermat's Little Theorem too. But then at $d = 9$ we get our first non trivial counter example for this theorem being true only for primes. With base $n = d-1 = 8$ we have $[n^{d-1}] = [8^8] = 1$.
The next composite odd is $d = 15$ and $[14^{14}] = 1$. And so on.
We can create infinite many such counterexamples with odd composite d-s and $n = d-1$.
These composite d cases only work because the n base is chosen this particular way.

So the logical question is whether all n bases have a composite d that $[n^{d-1}] = 1$.
Yes they have but to find a d to n is much harder.
There is a simple strategy though. We can try to design $d-1$ as an $a\,b$ product.
Then: $n^{d-1} = n^{a\,b} = (n^a)^b$

Now if n^a can be made as $m\,d + 1$ then the b power of this will be automatically same.

Or even if n^a is $m\,d - 1$ but b is even, then similarly we get 1 remainder.
So, lets check out the bases from the trivially solved 8, back down to 2.

For $n = 7$ the simplest try is $d - 1 = 2\,b$. Then $7^{2\,b} = (7^2)^b = 49^b$ So:
$49 = 48 + 1 = m\,d + 1$ or $49 = 50 - 1 = m\,d - 1$. So 48 or 50 must contain factors that will be d.
This of course must be composite and also $2\,b + 1$, so odd.
48 has no odd composite factor. 50 has 25. So $d = 25 = 2\,b + 1$ giving $b = 12$:

$$[7^{24}] = [(7^2)^{12}] = [49^{12}] = [(2 \bullet 25 - 1)^{12}] = [m \bullet 25 + 1] = 1$$

For $n = 6$ again the simplest $2\,b$ as $d - 1$ means $6^2 = 36 = 35 + 1 = 37 - 1$.
37 is prime so useless. 35 is good as itself. So $d = 35 = 2\,b + 1$ giving $b = 17$:

$$[6^{34}] = [(6^2)^{17}] = [36^{17}] = [(35 + 1)^{17}] = [m \bullet 35 + 1] = 1$$

For $n = 5$ $a = 2$ doesn't work because $5^2 = 25 = 24 + 1 = 26 - 1$ but neither of 24 , 26 have odd composite factor. Trying the next simplest $a = 3$, we get $5^3 = 125 = 124 + 1 = 126 - 1$.
So 124 or 126 must be $m\,d$ with d being composite and $3\,b + 1$. The 124 is good itself .
So $d = 124 = 3\,b + 1$ giving $b = 41$:

$$[5^{123}] = [(5^3)^{41}] = [125^{41}] = [(124 + 1)^{41}] = [m \bullet 124 + 1] = 1$$

For $n = 4$ trying again $a = 2$ means $4^2 = 16 = 15 + 1 = 17 - 1$. The 15 is good itself because it is composite and odd. So $d = 15 = 2\,b + 1$ giving $b = 7$:

$$[4^{14}] = [(4^2)^7] = [16^7] = [(15 + 1)^7] = [m \bullet 15 + 1] = 1$$

For $n = 3$ $a = 2$ doesn't work because $3^2 = 9$ and neither 8 or 10 have composite odd factor.
Similarly $a = 3, 4, 5$ fail. With $a = 6$, $3^6 = 729$, so 728 or 730 must have a composite and $6\,b + 1$ factor as d. And indeed $728 = 8 \bullet 91$ and 91 is composite and $6 \bullet 15 + 1$. So:

$$[3^{90}] = [(3^6)^{15}] = [729^{15}] = [(8 \bullet 91 + 1)^{15}] = [m \bullet 91 + 1] = 1$$

Finally, the smallest $n = 2$ is the most difficult. The first working a is 10 and $2^{10} = 1024$.
1023 has a composite $10\,b + 1$ factor 341. So $d = 341 = 10\,b + 1$ giving $b = 34$:

$$[2^{340}] = [(2^{10})^{34}] = [1024^{34}] = [(3 \bullet 341 + 1)^{34}] = [m \bullet 341 + 1] = 1$$

The full list from $n = 7$ to 2 for the first composite d values with sketched proofs:

$n = 7$	first d is	$25 = 5 \bullet 5$	indeed	$[7^{25-1}] = [7^{24}] = [(7^2)^{12}] = 1$
$n = 6$		$35 = 5 \bullet 7$		$[6^{35-1}] = [6^{34}] = [(6^2)^{17}] = 1$
$n = 5$		$124 = 2 \bullet 2 \bullet 31$		$[5^{124-1}] = [5^{123}] = [(5^3)^{41}] = 1$
$n = 4$		$15 = 3 \bullet 5$		$[4^{15-1}] = [4^{14}] = [(4^2)^7] = 1$
$n = 3$		$91 = 7 \bullet 13$		$[3^{91-1}] = [3^{90}] = [(3^6)^{15}] = 1$
$n = 2$		$341 = 11 \bullet 31$		$[2^{341-1}] = [2^{340}] = [(2^{10})^{34}] = 1$

Fermat "of course" never proved his Little Theorem. Leibniz proved it first but he also believed it to be a test of primality and all these above simple arguments avoided his vision.
The big step came with Euler. He generalized the Little Theorem to a grand result that gives a 1 place determined by d for all power remainder sequences with d , n relative primes.
There is a vision behind this theorem that finally regards things as they should be, that is as remainder sequences.
The currently still floating proofs for Fermat's Little Theorems are all obsolete and stupid.
The only correct way is to go to relative prime d , n.
Apart from the proof being cleaner, the step to the relative prime bases with d has its heuristic reason that we missed up until now.
We regarded relative prime d , n merely to guarantee simple restarts.
This step was justified by the fact that any c common factor of d and n is factor all remainders due to their definitions as $r = m\, n - k\, d$ or $r = n^m - k\, d$.
We can put this in a more visual form if we introduce $\Phi(d)$ as the set of all numbers under d that are relative primes with d. For example $\Phi(10) = \{ 1 , 3 , 7 , 9 \}$.
So with this, we can simply say that if d , n are not relative primes then the remainders in either of our sequences can only come from numbers under d that are outside $\Phi(d)$.
And now comes an easy but surprising fact. There is one single respect in which the power remainders are simpler than the multiple remainders. Namely, for them this law is reversible.
For the multiple remainders this law is not reversible and we know this from the fact that for relative prime d , n the possible remainders were not $\Phi(d)$ rather all values up to d.
This was much better than just being in $\Phi(d)$, so we didn't even mention Φ back then.
But the reason the law of being outside Φ doesn't reverse to being inside, is also clear.
Namely, in $r = m\, n - k\, d$ the m multiplier can have all kinds of factors, so a c common factor of r and d doesn't have to divide n.
In contrast, in $r = n^m - k\, d$ the m is not bringing in new prime factors. n^m has only the prime factors of n. So, a common prime factor of r , d must be in n^m and so in n too.
Or in reverse, if d , n are relative primes that is have no common prime factor then r , d must be too. So: For relative prime d , n the power remainders are all in $\Phi(d)$.

Euler's grand discovery was that $\Phi(d)$ not only determines the possible remainders as set but it determines easily a fix 1 remainder position for all bases too.
We knew already that for relative prime d , n there have to be 1 places.
We can even argue further in different bases parallel and thus create multiple exponents that give 1 remainders for all bases. Then we can examine how these determine smaller common 1 giving exponents. We'll go into these complications in our Second New Look in section 2.).
But Euler's Theorem avoids all this and gives a 1 giving exponent easily for all bases.
Namely, as the number of elements in $\Phi(d)$ denoted as $\varphi(d)$. So:

$$[\, n^{\varphi(d)} \,] = 1 \quad \text{for} \quad \text{all} \quad n \in \Phi(d).$$

It's enough to make the claim this way, that is only for n bases in $\Phi(d)$ because then the other bigger than d relative primes are $n + K\, d$ and follow by : $[\, (n + K\, d)^k \,] = [\, n^k \,]$.

The Φ , φ notations are perfect to express how Fermat's Little Theorem is really just a special case of Euler's result. Indeed, for a prime d , $\Phi(d) = \{ 1 , 2 , 3 , \ldots , d-1 \}$ and $\varphi(d) = d - 1$.

We saw that already the most special $[\, 2^{p-1} \,] = 1$ old Chinese law gave only a fix 1 place but not necessarily the μ minimal one where $[\, 2^{\mu} \,] = 1$. Indeed at $p = 7$, $\mu = 3$ not 6.
The fact that 3 divides 6 is not accidental. As we already explained:

In all power remainder sequences where there is 1 occurrence, that is in the ones where d , n are relative primes, all 1 occurrences are at the multiples of the μ minimal one.

Indeed, the μ long initial segment ending with 1 is simply repeating.

This fact will give one way to prove Euler's theorem.

Namely, showing that $\mu(d , n)$ divides $\varphi(d)$ for all n bases.

As expectable, this means that for some n bases $\mu(d , n)$ is only a factor of $\varphi(d)$ so $\mu < \varphi$.

On the other hand, compared with Fermat's claim that only guaranteed a 1 at $p-1$,
for composite d , obviously $\varphi(d) < d-1$, thus $\varphi(d)$ is already giving an early or better place.

Thus, the prime dividers still offer a question.

We know that sometimes $p-1$ is not the first 1 occurrence either, but is it at least true that there is always a base n at which $p-1$ is the first?

Already Euler asked this question and observed that yes, there are such perfect bases for all primes where $p-1$ is the first 1 place. He called these n bases as primitive roots for the p prime divider. Gauss accepted his naming and found a proof for this fact.

To understand this seemingly stupid name, we must tell why we called these bases primitive roots "for" p and not "of" p. The reason is simple. They are the $p-1$ roots <u>of</u> 1 because the $p-1$ powers of them become 1. So, just as we regard powers as remainders, we can regard roots too.

More generally, any m-th root of any r remainder is n if $[n^m] = r$.

Just as the roots in algebra mean not only these reverse powers but solutions of sums of powers, that is polynoms, here too, these enter the scene. The big difference is that the most basic rule of having maximum as many roots as the order of the polynom, is not true among remainders any more. Even the simpler root concept as reverse power, shows this. In fact even the simplest, second order case, that is square roots can be more than two.

For example with $d = 8$ divider there are four square roots of 1.

Indeed, all four elements of $\Phi(8) = \{ 1 , 3 , 5 , 7 \}$ will give a 1 at the second power:

$[1^2] = [3^2] = [5^2] = [7^2] = 1$

The good news is that with prime dividers, the maximality of m many m-th roots is again true.

The bad news is that to see this we have to go to polynoms in general.

This then will prove the theorem of Gauss too to have primitive roots for prime dividers.

This will be the third theorem of our five.

But neither Euler nor Gauss realized that in the two facts:

1.) For non prime d : For all base n, there is always 1 before the $d-1$ place.
2.) For prime d : There is base n, so that there is no 1 before the $d-1$ place.

The two consequences are exact opposites and so they offer a perfect primality test.

Lucas realized this much later and this will be our fourth theorem.

But there was an other direction of much more surprising blind spots too.

To bring out this direction, we first emphasize the base universality in Fermat's Little Theorem and Euler's theorem by introducing our fourth category "absolute".

The first three categories are return, restart and simple, which we used as places that is exponents in a fixed base power remainder sequence.

The ancient Chinese rule $[2^{p-1}] = 1$ or its consequence $[2^p] = 2$ was base specific.
So non "absolute".

Fermat's Little Theorem: $[n^{p-1}] = 1$ or $[n^p] = [n]$ is true for all n that are not p multiples. So we can call the p primes as "absolute" simple restarts by excluding these trivial bases.

Euler's theorem $[n^{\varphi(d)}] = 1$ or its consequence $[n^{\varphi(d)+1}] = [n]$ again can be stated by saying that $\varphi(d)+1$ is an absolute simple restart. Of course now this absolute means all bases relative prime with d.

Observe that in this nomenclature we also shifted return and restart itself from referring to the exponents where it happens with a given d, to the d divider as exponent itself.

In every power remainder sequence with relative prime n base with a fix d divider, the 1 places are simply the multiples of the $\mu(d, n)$ first one. So, any exponent that is dividable by all $\mu(d, n)$ initial segment lengths for $n \in \Phi(d)$, is an absolute 1 place.
The product of all these $\mu(d, n)$ is such and their lowest common multiple is the first such.
This locomult $\{ \mu(d, n) ; n \in \Phi(d) \}$ first absolute 1 place is abbreviated as $\lambda(d)$.
It is also called as "least universal exponent" or Carmichael's function.
Of course as expectable, in most bases $\mu(d, n)$ will be factor of $\lambda(d)$, so $\mu(d, n) < \lambda(d)$ too.
Euler's theorem gives also an absolute 1 place as $\varphi(d)$, so obviously $\lambda(d) \leq \varphi(d)$.
$\varphi(d)$ must be a multiple of all $\mu(d, n)$-s too but not necessarily the minimal, that is the lowest common multiple, so we expect that for most d we should have actually $\lambda(d) < \varphi(d)$.
And of course $\varphi(d)$ shouldn't be multiple of $\lambda(d)$ necessarily at all.
But it is! And the reason is simple: The $\lambda(d)$ minimal absolute 1 place is always an actual $\mu(d, n)$ initial segment length for some n base.
This will be the result of our Second New Look after the First that gives Euler's theorem.

Lets see some examples of these functions:
At $d = 7$ both φ and λ give 6 but as we saw, $\mu(7, 2) = 3$
Both 2 and odd prime factors of d can lead to λ becoming smaller than φ. For example:
$\varphi(8) = 4$ because $\Phi(8) = \{ 1, 3, 5, 7 \}$ but $\lambda(8) = 2$ and $\varphi(15) = 8$ but $\lambda(15) = 4$.

Right now, instead of our chase for earliness, we can try to chase absoluteness.
That is, to find exponents with 1 remainders for all bases as far as possible.
Obviously, then quite oppositely to the earliness chase, the latest exponent is the best.
So, the amateur Fermat is laughing at us as we forget about $\varphi(d)$ and $\lambda(d)$ and require 1 occurrence at $d-1$. That is $[n^{d-1}] = 1$ for all n relative prime with d. So:

d is absolute simple restart if $[n^{d-1}] = 1$ for all n relative prime with d.

But we can chase absoluteness further!
For bases non relative prime with d, we obviously can not have $[n^{d-1}] = 1$
because all remainders have the c common factors of d and n too.
But we can have its consequence $[n^d] = [n]$ that is we can have restart at d. So:

d is absolute restart if $[n^d] = [n]$, that is d divides $n^d - n$ for all n.

But this is still not all folks, because we can be even more general by merely requiring that at d we have a return for all bases. So:

d is absolute return if $[n^d] = [n^m]$, with some $m < d$ for all n.

Obviously, absolute restarts are absolute returns by definition. But also, absolute returns are absolute simple restarts too because the relative prime bases imply the simple restarts automatically.
So if all absolute simple restarts are absolute restarts, then all these three concepts are the same.
Lets start with absolute restarts!
Without even knowing if there are such d, there is an obvious fact following for such d-s.

Namely, that all f factors of d must divide $n^d - n$ for all n too.
This clearly makes it seem even more strange if such d existed.
But now we use this for two specific situations to get two specific consequences:

1.)

Using a p prime factor of d as base n : any f factor of d must divide $p^d - p$.
Again, this seems quite unbelievable to be true for all f factors with a fix p.
But we ignore this feeling and merely derive that f can not be p^2.

Indeed, p^2 divides p^d but can not divide p, thus p^2 can not divide $p^d - p$.
So, d can not have repeated prime factors, or as they say, it has to be "square free".

2.)

Using now a p prime factor of d as f : p divides $n^d - n$ for all n.

Or using $< >$ as remainder to p we have: $<n^d> = <n>$. So:
d is a restart in all of these new p , n sequences with any p prime factor of d and base n.
By Gauss' Theorem there is an n base that $p-1$ is the first exponent giving 1.
Obviously this is a sequence where n is not a multiple of p and the restarts are simple.
In fact, all other 1 places are the $k(p-1)$ multiples and all restarts are $k(p-1)+1$.
So, $d = k(p-1)+1$ that is $p-1$ must divide $d-1$.

The unbelievable fact is that these two final consequences in reverse imply an absolute restart:

If d has no repeated prime factors and for all p ones $p-1$ divides $d-1$, then
d is absolute restart, that is $[n^d] = [n]$, that is d divides $n^d - n$ for all n.
Even more unbelievably this is almost trivial again.
Indeed, enough to show that all p prime factors of d divide

$$n^d - n = n(n^{d-1} - 1) = n(n^{k(p-1)} - 1) = n((n^k)^{p-1} - 1).$$

And this follows from Fermat's Little Theorem used as $[(n^k)^{p-1}] = 1$.

Korselt recognized all this but he didn't know if there are absolute restarts.
Carmichael found the first examples.
The smallest is $561 = 3 \bullet 11 \bullet 17$ because: 2 , 10 , 16 all divide 560.

There are two easy clues that helped to find this smallest example quite easily by a few trials.

Firstly, such d numbers are odd. Otherwise $d-1$ were odd, but having a single 2 factor would also mean having at least one odd p and thus the even $p-1$ would divide the odd $d-1$.

Secondly, these d must have at least three prime factors. Indeed:
If $p < q$ were the only, that is $d = pq$ were then observe the following two facts:
$q-1$ divides $p(q-1) = pq - p$ and $q-1$ can not divide the smaller $p-1$.
So $q-1$ can not divide $d-1 = pq-1 = (pq-p)+(p-1)$ either.

By a quite recent result there are infinite many such Carmicheal numbers or absolute restarts.

This 561 number is similar to 341. That was missed by Euler, this was missed by Gauss.
Obviously, it's not these numbers but the whole directions behind them that were the blind spots.
The interesting question is how they would react if we traveled back in time and showed them.
Unfortunately, I know exactly well. They would try to diminish the importance of these facts.
Euler despised Fermat and never realized that he merely became a more refined liar.
Then Gauss criticized Euler for his not quite precise proofs and he never realized that he merely became an even better liar. And the modern liars find all this criticism as sacrilege.
But Formalism is nothing less than lying. To write down the proofs and not telling what we see behind them as wider reality is not motivated by revealing the truth to others, rather by vanity.
The systems of verifications as social process became more and more entangled.
Those who "deal" in life and don't even care about truth, are riding the verification by any audience. Scientists and mathematicians avoid a lowest level of lies that the totally blind masses have to choose from. But being in the inner sanctum merely makes their seemingly smaller lies actually bigger. Until the conflict of this doesn't even awaken, the mathematician is nothing.
So, not to know about how the blind spots and the personal weakness interrelates is the full darkness. Once the conflict is acknowledged then the painful travel begins.

I confronted two living geniuses with these ideas. The first was Paul Cohen the second Paul Erdös. My English was pretty poor back when I attacked Cohen but the next day he returned with some interesting reactions. Erdös replied a few times to my attacks but he had absolutely no concept of the depth of my arguments. He was truly an example of how such a smart person can be that stupid. But I caught him by his own lies, he had to retract things he said before.
Strangely, my militant anti Formalism is purely a political question. It is the politics of truth.
Just as Timothy Leary's grand realizations remained a Politics of Ecstasy.
My claim is that there is a Didactical Logic that is above the Logic of Derivations.
If I am right then the future will prove this and our present obsession with Formalism will fade away through some conflicts. Truth is simple and accessible to everybody.
But to short-circuit common sense is a tendency. Society has its own agenda. Civilization, history, is a self revealing lie. The more the past is accepted as lie, the less the present is viewed as such.
But these big things can not become conscious without being meticulous about small lies.
So, mathematicians are the perfect candidates to catch their own lies because they are dealing with details. And yet this doesn't happen usually.
Gauss said that Fermat's Last Theorem is "not that important" even though he knew exactly well that it was the most important. Simply because he didn't make a meticulous derivational claim. The same way he destroyed a human being Janos Bolyai without telling a lie in the derivational sense. But it was a lie in his own system of truths too. So it's not the question of lying rather the realm of acceptable lies that matters.
The two greatest geniuses of the twentieth century, Einstein and Gödel lived in most intricate lies.
The point again is that these seemingly personal lies are entangled with the blind spots.

But now lets return to the absolute returns.
As we said they are the same as absolute restarts if the absolute simple restarts are absolute restarts too.
Instead of proving this on its own, it's more interesting to show that d absolute simple restarts imply the same two Korselt conditions, that is:

all p prime factors being non repeating and $p-1$ dividing $d-1$.

The reason for this road being better, is that being absolute simple restart has a more concrete alternative definition. Namely that $\lambda(d)$ divides $d-1$.

$\lambda(d)$ can be calculated by three rules:

1.) For $d = 2^k$ with $k = 1, 2$, $\lambda(2) = 1$, $\lambda(4) = 2$, with $k > 2$, $\lambda(2^k) = 2^{k-2}$

2.) For $d = p^k$ with odd p prime $\lambda(p^k) = p^{k-1}(p-1)$.

3.) For $d = a\,b$ with relative prime a, b $\lambda(a\,b) = \text{locomult}(\lambda(a), \lambda(b))$.
Where locomult means the lowest common multiple.
Repeating this, gives λ directly for any $p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ through 1.) and 2.) :
$\lambda(p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}) = \text{locomult}(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \ldots, \lambda(p_m^{k_n}))$.

Then from these rules:
First of all $\lambda(d)$ is always even except for $d = 2$ which is not an absolute simple restart.
So, other even d-s can not be either because $\lambda(d)$ can not divide the odd $d-1$.
A p prime factor of d can not divide $d-1$.
But by 2.) and 3.), a repeating p odd prime factor of d must divide $\lambda(d)$.
For d absolute simple restart, $\lambda(d)$ divides $d-1$. So d can not have repeated odd prime factor.
Finally, for the non repeating odd p prime factors, again by 2.) and 3.) :
$p-1$ must divide $\lambda(d)$ and so for absolute simple restart, $d-1$ too.

So, these three rules of $\lambda(d)$ are the real reasons of the Korselt conditions.
The claim of these rules is Carmichael's theorem and it will be the last in our five theorems.

The fact that being absolute simple restart implies to be absolute restart, raises the question of non absolute, individual bases with restart at d but not being simple, that is not having 1 at $d-1$.
Could the simplest base 2 for example have a restart at d that is definitely not simple?
We know that relative primeness, that is here odd d implies simplicity and we can see this here directly too. Indeed, then the restart at d that is $2 = 2^d - k\,d$ means that k is even and so dividing with 2 we get $1 = 2^{d-1} - \frac{k}{2}\,d$.
In reverse, we also know that non relative prime divider that is here even d will definitely forbid simplicity because all remainders must be even.

So, we merely have to find an even d that $[2^d] = 2$
The first example was found only in 1950 by Lehmer as $d = 161038$.
Though it was hard to find, it's quite easy to verify:

$d = 2 \bullet 73 \bullet 1103$, $d-1 = 9 \bullet 29 \bullet 617$, $2^9 - 1 = 7 \bullet 73$, $2^{29} - 1 = 233 \bullet 1103 \bullet 2089$
Thus:
$2^9 - 1$ divides $2^{d-1} - 1$ so 73 divides it too. $2^{29} - 1$ divides $2^{d-1} - 1$ so 1103 divides it too.

Thus, $73 \bullet 1103$ divides $2^{d-1} - 1$ too and then of course $2 \bullet 73 \bullet 1103$ divides $2^d - 2$.

After this modern result about 2 powers, we should revisit the past.
The ancient Chinese mathematicians loved to double numbers and check their remainders.
That's how they discovered $[2^{p-1}] = 1$.

But these 2 powers are modern too because the computer memories are based on base 2.
Every kid knew few years ago what "Nintendo 64" was. Now with bigger memories they stopped using these numbers. Kids should know these binary numbers at least up to the ten power, that is:
2 , 4 , 8 , 16 , 32 , 64 , 128 , 256 , 512 , 1024.
This last tenth binary was crucial earlier in creating the 341 composite example for Fermat's Little theorem with base 2.

A much simpler idea even than checking remainders was to subtract and also add 1 to these binaries. These 2^m-1 and 2^m+1 could be called the binary twins.
When Fermat rediscovered the old Chinese results he generalized these too.
He regarded all bases. Here the corresponding twins are the n^m-1 and n^m+1 power twins.

The amazing world of the binary and power twins starts with three modern laws:

For all m powers:

$$a^m - b^m = (a-b)[a^{m-1} + a^{m-2}b + a^{m-3}b^2 + .. + ab^{m-2} + b^{m-1}]$$

For even m powers:

$$a^m - b^m = (a+b)[a^{m-1} - a^{m-2}b + a^{m-3}b^2 - .. + ab^{m-2} - b^{m-1}]$$

For odd m powers:

$$a^m + b^m = (a+b)[a^{m-1} - a^{m-2}b + a^{m-3}b^2 + .. - ab^{m-2} + b^{m-1}]$$

These can be checked by simply carrying out the multiplication and see the canceling members.
A few, concrete examples are:

$$a^3 - b^3 = (a-b)[a^2 + ab + b^2]$$
$$a^4 - b^4 = (a-b)[a^3 + a^2b + ab^2 + b^3]$$
$$a^4 - b^4 = (a+b)[a^3 - a^2b + ab^2 - b^3]$$
$$a^3 + b^3 = (a+b)[a^2 - ab + b^2]$$

Now some obvious facts:

If n is odd then the n^m-1 and n^m+1 power twins are even.
If n is even then the n^m-1 and n^m+1 power twins are odd.
If $n>2$ and $m>1$ then n^m-1 is composite. We use n as a and 1 as b in first above.

If m is composite j k then 2^m-1 is composite too.
We use 2^j as a , 1 as b and k as m in first above: $2^{jk}-1 = (2^j)^k - 1^k = (2^j-1)[\ ]$

If $n>1$ and $m=jk$ with k odd, then n^m+1 is composite.
We use n^j as a , 1 as b and k as m in the third above:
$n^m+1 = n^{jk} + 1^k = (n^j)^k + 1^k = (n^j+1)[\ ]$

Now some not so obvious things, yet following from the aboves:

If n^m-1 is prime then $n=2$ and m is prime. That is:
Small power twin can only be prime as small binary twin with prime exponent.

If n^m+1 is prime then n is even and $m=2^k$. That is:
Big power twin can only be prime with even base and binary power.

The two n^m-1 and n^m+1 power twins both can never be primes except for:
$2^2 - 1 = 3$ and $2^2 + 1 = 5$

Such prime exponent small binary twins, that is 2^p-1, are called Mersenne candidates.

The binary powered and 2 base big twins, that is $2^{2^k}+1$, are called Fermat numbers.

The reason that these ones are not called candidates merely numbers, is that they don't seem to give primes after already $k = 4$, while the first ones seem to give infinite many primes and infinite many failing composites too. But we have no proofs for these behaviors.

Originally both were believed to be perfect, always producing primes. Indeed:

$2^2-1 = 3$, $2^3-1 = 7$, $2^5-1 = 31$, $2^7-1 = 127$ But then:

$2^{11}-1 = 2047 = 23 \bullet 89$

Similarly:

$2^{2^0}+1 = 3$, $2^{2^1}+1 = 5$, $2^{2^2}+1 = 17$, $2^{2^3}+1 = 257$, $2^{2^4}+1 = 65537$ But then:

$2^{2^5}+1 = 2^{32}+1 = 4\,294\,967\,297 = 641 \bullet 6\,700\,417$ As Euler observed it first.

In spite of the mentioned uncertainty about the Mersenne candidates and Fermat numbers, there are two theorems perfectly telling the prime cases theoretically:

Lucas:

Let $L_2 = 4$ and $L_{m+1} = L_m{}^2 - 2$
So: $L_3 = 4^2 - 2 = 14$, $L_4 = 14^2 - 2 = 194$, $L_5 = 194^2 - 2 = 37634$, . . .
Then for $m > 2$, 2^m-1 is prime if and only if it is factor of L_m.

For example:

$2^3 - 1 = 7$ is factor of $L_3 = 14$, $2^4 - 1 = 15$ is not factor of $L_4 = 194$,

$2^5 - 1 = 31$ is factor of $L_5 = 37634$ and so on.

Pepin:

For $k > 0$, $F_k = 2^{2^k}+1$ is prime if and only if it is factor of $3^{\frac{F_k - 1}{2}} + 1$.

For example:

$2^{2^1}+1 = 5$ is factor of $3^{\frac{5-1}{2}} + 1 = 10$,

$2^{2^2}+1 = 17$ is factor of $3^{\frac{17-1}{2}} + 1 = 3^8 + 1 = 6561 + 1 = 6562 = 17 \bullet 386$.

First New Look: Multiple Cycles, Euler's Theorem

The end result of multiple remainders was that if d , n are relative primes then the remainders:

$[n]$, $[2n]$, $[3n]$, . . . , $[(d-1)\,n]$ are merely a reordered version of : 1 , 2 , 3 , . . , $(d-1)$.

There are two ways to see this.
Either from the fact that a relative prime d with n if divides $m\,n$ then it must divide m.
Indeed, then the above remainders are all different, since d can not divide
$j\,n - i\,n = (j-i)\,n = m\,n$ because $m < d$ and so $[i\,n] \neq [j\,n]$.
Thus, we must have all possible $d-1$ many values because we have that many places.
Or, we can use this same pigeon hole principle in reverse to show that only 1 , 2 , 3 , . . , $(d-1)$ can appear as remainders, that is 0 can not appear, if they all must appear. Indeed, there is no more "hole" for a 0. This non appearance of 0 actually implies the basic assumption above about the d divider dividing m. This was the way we went. Namely, by regarding all possible d , n situations and showing through the multiple differences that all remainders are multiples of the s minimal which is also a super common divider of d and n. Then for relative prime d , n obviously $s = 1$ and so we get all possible non zero remainders. So this was how we proved the above law of relative prime d divider which implied the separate dividing of primes and that implied Unique Prime Factorization. But then we showed alternative proofs with induction.
Now we only care about the fact which we repeat again:

If n is relative prime with d then multiplying the numbers 1 , 2 , 3 , . . , $(d-1)$ with n and taking the remainders to d we obtain all different remainders.
This implies that for any subset from these numbers under d, we also get all different remainders of the n multiples. In particular, using all the relative primes with d under d, that is the

$\Phi(d) = \{ r_1 , r_2 , . . . , r_{\varphi(d)} \}$ set, we can also form $n\Phi(d) = \{ n r_1 , n r_2 , . . , n r_{\varphi(d)} \}$ and

then $[n\Phi(d)] = \{ [n r_1] , [n r_2] , . . , [n r_{\varphi(d)}] \}$ which are all different.

What is special here is that these are not only different, but are all members of $\Phi(d)$.
The reason is simply that all $[n r_i]$ must be relative prime with d.
Indeed, any q common prime factor of d and $[n r_i] = n r_i - k\,d$ would have to divide $n r_i$ but both members are relative prime with d so q can not divide them.

So actually: $[n\Phi(d)] = \Phi(d)$.

Also, a product of remainders is the remainder of the product and so the total product of the two sides are: $[n r_1 \; n r_2 \; . . \; n r_{\varphi(d)}] = [r_1 r_2 \; . . \; r_{\varphi(d)}] = [B]$.

But the left side can be changed to: $[n^{\varphi(d)} r_1 r_2 \; . . \; r_{\varphi(d)}] = [A\,B]$

So: $[A\,B] = [B]$. We jump to the conclusion that $[B] = 0$ or $[A] = 1$.

But our B is a product of relative primes with d. So, B is relative prime with d too, not dividable by d and so $[B] \neq 0$. So, we obtained that $[A] = [n^{\varphi(d)}] = 1$ exactly Euler's theorem.

Unfortunately we made an error. The conclusion of $[B] = 0$ or $[A] = 1$ is not universally true.

A simple counter example is $A = 6$, $B = 4$, $d = 10$. Indeed, then $[6 \bullet 4] = [4]$.

Only already with the condition of B being relative prime with d can we get $[A] = 1$. Namely:

$[A\,B] = [B] \rightarrow d$ divides $A\,B - B = B\,(A - 1) \rightarrow d$ divides $A - 1 \rightarrow [A] = 1$.

Even with this correction, the result came out pretty much from nowhere. So a second, much more tedious proof shows the reasons better why $\varphi(d)$ must be a 1 remainder place:

We already cleared that these 1 places are exactly the multiples of the first μ exponent where $[n^{\mu}] = 1$. So, all we have to prove is that μ divides $\varphi(d)$.
The remainders up to this first 1, that is the initial segment n , $[n^2]$, . . . , 1 are all different elements from $\Phi(d)$. If they are all of them then of course $\mu = \varphi(d)$ so we are finished.
What we must show is that if not, that is there are left out elements of $\Phi(d)$, then those can be distributed into groups with same μ many members. To find these groups is easy.
All we have to do is multiply n , $[n^2]$, . . . , 1 with any outside one and take remainders.
First of all, these will be all different values and secondly, using different outside multipliers, two such sequence will be either having all different elements or having all same elements, that is merely be a reordered version of an other.

As a concrete example, let: $d = 13$, $n = 3$. So thee initial segment is 3 , 9 , 1.

$\Phi(13) = \{ 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 \}$ so the outside elements are:

2 , 4 , 5 , 6 , 7 , 8 , 10 , 11 , 12

Multiplying these with the initial segment and taking remainders, we get nine sequences:

2	times	3 , 9 , 1	=	6 , 18 , 2	and taking remainders:	6 , 5 , 2
4	times	3 , 9 , 1	=	12 , 36 , 4	and taking remainders:	12 , 10 , 4
5	times	3 , 9 , 1	=	15 , 45 , 5	and taking remainders:	2 , 6 , 5
6	times	3 , 9 , 1	=	18 , 54 , 6	and taking remainders:	5 , 2 , 6
7	times	3 , 9 , 1	=	21, 63 , 7	and taking remainders:	8 , 11 , 7
8	times	3 , 9 , 1	=	24 , 72 , 8	and taking remainders:	11 , 7 , 8
10	times	3 , 9 , 1	=	30 , 90 , 10	and taking remainders:	4 , 12 , 10
11	times	3 , 9 , 1	=	33 , 99 , 11	and taking remainders:	7 , 8 , 11
12	times	3 , 9 , 1	=	36 ,108 , 12	and taking remainders:	10 , 4 , 12

And indeed, these nine contains actually three sets: $\{ 2 , 5 , 6 \}$, $\{ 4 , 10 , 12 \}$, $\{ 7 , 8 , 11 \}$ which are disjoint. So, regarding the initial segment's set $\{ 1 , 3 , 9 \}$ as well, we actually distributed the full $\Phi(13)$ as $\{ 1 , 3 , 9 \} + \{ 2 , 5 , 6 \} + \{ 4 , 10 , 12 \} + \{ 7 , 8 , 11 \}$.
That's why 3 divides the full number of elements $\varphi(13) = 12$.

To see why this must happen always, we "simply" have to widen our view from power sequences to geometrical sequences.
I put the simple in quotation mark not because it will be complicated rather because the simplicity that is 1 occurrence stops this way.
The arithmetical sequences are also a generalization of multiples if we start from any fix value:

s , $s + n$, $s + 2n$, $s + 3n$, . . . The multiplicative or geometrical version is:

s , $s\,n$, $s\,n^2$, $s\,n^3$, . . .

Using remainders to a d divider, we again have obvious iterative sequences calculable from the last remainders. And of course again the values can only be under d, so we must have return.
In power sequences we saw that the relative primeness of n with d guaranteed simple restart.
Now we can tell why this allowing of s multiplier is such a tricky tool:
It still guarantees that the return is restart but it doesn't have to be simple!
Indeed, if both the n base and the s starter are relative prime with d, then firs of all the remainders are again from $\Phi(d)$. And now for a return from m to m –k we have again:

$$[s\,n^m] = [s\,n^{m-k}] \qquad \leftrightarrow \qquad s\,n^m - s\,n^{m-k} = s\,n^{m-k}(n^k - 1) = K\,d$$ So:

If both s and n are relative prime with d, then d must divide again $n^k - 1$, that is $[n^k] = 1$.
This now means $[s\,n^k] = s$, so we had an earlier return to the start that is restart.
So the first return must be a restart and all remainders up to it are different.
So we have initial segments repeating exactly as before but they don't have to end with 1.
A more important internally new way to regard these segments is as being determined by the initial member and the iterative rule of multiplying by the n base and taking remainder.
Then a better name for these initial segments is cycles because the iterativeness only depends on the base n and so starting with any element from them, we get the same elements in a shifted order but after the end continuing with the beginning. Exactly like a clock.
This way of course the initial element lost its role
The same was true for our old initial segments ending with 1.
But there the iterativeness was merely an extra feature and we regarded the powers as defining.
So starting a new power sequence with an $[n^k]$ member we would get only powers with multiple exponents of k and not a recycling of the same old segment.
Also, we would again only get 1 at the end of our new segment that could have new length too.
Most importantly, this new iterative or cycle vision would have meant no advantage at all.

Multiplying a fix old n , $[n^2]$, . . , 1 initial segment with an r remainder, we create a new segment that is obviously n iterative. It starts with $s = [r\,n]$ and ends with r.
By the cycle view, this is the same set as if we started with r, the last or any other member and use n multiplication and remainder iteration from it.
For example, using the base n itself as multiplier r, we simply shift the old segment into the new $[n^2]$, . . , 1 , [n]. This member before the last [n] being 1 was consequence of this shift but we can verify it also by knowing that the old 1 was $[n^\mu]$ and so the previous was $[n^{\mu-1}]$ and then : $[n\ [n^{\mu-1}]] = [n^\mu] = 1$. Similarly we can see exactly how multiplying with any other member, we get a bigger shift but the same set. It is interesting but still useless.
The crucial idea is to multiply our fix segment with all possible r remainders especially with the outside ones not in the segment. We have no idea how many are there in $\Phi(d)$. It is really depending on d and seemingly not at all on our fix segment. And yet, our segment's length μ must divide the number of elements in $\Phi(d)$ that is $\varphi(d)$. Most amazingly, this follows instantly from this iterative or cyclic picture of the multiplied segments. Indeed:

1.) The segments will all be same or totally disjoint sets with μ members.
2.) Every r element of $\Phi(d)$ is in one. Namely, definitely in the one that was multiplied by r.

This second proof still contained the ad hoc idea of multiplying the remainders with a fix one.
It's also quite insane that we regarded only a single initial segment.
For every n base taken from $\Phi(d)$, we have its own initial segment with $\mu(d, n)$ length.
We should examine these initial segments simultaneously! That's the real structure of $\Phi(d)$.
This we shall do in the next chapter and in a sense it will turn out to be the fundamental theorem of power remainders. Unfortunately, it doesn't prove Euler's theorem.

Even more strangely, there will be a third different view of power remainders that does prove Euler's theorem for primes, that is Fermat's Little theorem. And then the final theorem that is the calculation of $\lambda(d)$ does imply the whole Euler's theorem but uses it too.

In a sense, we have a grander version of the conflict I mentioned above when showed how the initial segment remains the same by self multiplication. The conflict is that we can see something abstractly and then concrete verifications still give new details.
The point of mathematics is to see how things are!
Since the discovery of Set Theory by Cantor, we realized that in New Math simple arguments can mean very deep truths. So here it is quite obvious that a derivation itself does not contain the full truth of the matter. For me a big step was going back to old classical math and to see that the same complicated situations were always there, except the older Formalism ignored it.
The stupid or parrot Formalists who use derivations as an "ego dance" are not worth criticizing.
They go from the details to the whole, have no vision themselves so can not spread one either.
These are like the bad teachers using their little notebooks for decades and still unable to explain thing from their heads. Indeed, their heads contain only forms, dead derivations.
More dangerous are the ones who do have visions but keep it to themselves.
Some of these even believe that the proofs tell the full story.
In extreme cases like the above Euler's theorem, the smart mathematicians can not deny that the three features, shortness, abstractness and "ad hoc"-ness hide a much deeper reality, but in their opinion to talk about this is useless.
In my view, that's the only way to spread vision through derivations.
Without playing with numbers, calculating examples, one can not even see the meanings of definitions and theorems. But the structure of derivations is above that level and one doesn't have to do more examples to enter this higher level. If we could do infinite many examples we wouldn't need derivations. So in a sense derivations are the essence of math.
My claim that there exists didactical logic means that everybody can enter the higher level.
Now you can defy this by saying that if someone is lazy to even see examples and thus comprehend the problems then how can he enter the world behind derivations. This has real conflict in it but still avoids the bigger conflict outside of it.
In short, I assume a student that can be awakened.
Pouring abstractions over people as the new method of education is an evolutionary detour to silence the ones who want to be awakened but are helpless to find even the questions before the answers.
Abstraction merely hides the basic didactical problems.
The same ad hoc multiplying idea we explained above is used in the actual proof of the Lagrange theorem that the order of sub groups must divide the main order. Now, one can say that exactly this abstractness justifies the use of ad hoc methods. It might be true.
So a bigger problem is when to go abstract.
Obviously not at the beginning.
The remainder sequences are a beautiful, totally concrete vision.
To understand the depth of it you have to calculate a few concrete remainder sequences.
Starting with groups and rings is insane because there is no defined reality.
This doesn't mean you can not go to higher abstractions gradually stepping through concrete realities. You can do that even in a short article.
The Wikipedia math articles are the total opposite.
Insane abstractions in vicious cycles if someone tries to follow the definitions.
Pure and intentional evil to turn people away from even trying to understand.

Second New Look: Multiple Lengths, Super Length Theorem

The fundamental theorem of the multiple remainders was the existence of an s remainder that is super common divider of d and n.
All common dividers of d and n divide this s. Plus: All other remainders are multiples of s.
Or in other words, the obviously existing greatest common divider turned out to be super and the remainders were all the multiples of it.
A corresponding fundamental theorem here among power remainders is more sophisticated.
Here, everything boils down to the three functions $\mu(d, n)$, $\varphi(d)$, $\lambda(d)$.
By their definitions the only obvious facts are that $\mu(d, n) \le \varphi(d)$ and $\mu(d, n) \le \lambda(d)$.
Indeed:
An initial segment can maximum contain all $\Phi(d)$ elements, so can be maximum $\varphi(d)$ long.
Also, $\lambda(d)$ being the lowest common multiple of all $\mu(d, n)$ lengths, must be also at least as big as they each.
Any common multiple of these lengths is an exponent that gives 1 for all bases, so this lowest common multiple $\lambda(d)$, is the first such absolute 1 place.
Euler's theorem revealed that all $\mu(d, n)$ divide $\varphi(d)$, so in other words $\varphi(d)$ is also an absolute 1 place. Thus of course $\lambda(d) \le \varphi(d)$. So: $\mu(d, n) \le \lambda(d) \le \varphi(d)$.
This second new look will reprove and refine $\lambda(d) \le \varphi(d)$ plus refine $\mu(d, n) \le \lambda(d)$ too.
Formally, the easiest to start with this refinement of $\mu(d, n) \le \lambda(d)$. Namely, the logical question is if for any d divider there are always n bases where equality stands.
Bingo! That's exactly one way to say our claim:
The minimal absolute 1 place is always actual at some s base: $\lambda(d) = \mu(d, s)$.
First of all, this indeed proves $\lambda(d) \le \varphi(d)$ again because $\lambda(d) = \mu(d, s) \le \varphi(d)$.
But as I said, it refines it too. Indeed, by Euler's theorem all $\mu(d, n)$ divide $\varphi(d)$.
So, these special $\mu(d, s)$ ones divide it too and so $\lambda(d)$ also divides $\varphi(d)$.
So when $\lambda(d)$ is smaller than $\varphi(d)$, it is much smaller, because it is factor of it.
But didactically it's better to start without λ and φ rather claim our new fundamental theorem as an analogue of the old, about the s super common divider but with big differences:
First of all, unlike at the multiple remainders where d and n were unrestricted, here we only look at relative prime ones that is in $\Phi(d)$.
Secondly, here we will have more special or super remainders.
Thirdly, the real reason for this plurality is that the "super"ness is about the length of the initial segments initiated by the remainders. Indeed, more s remainders have same $\mu(d, s)$ value.
The "super"ness itself is similar, meaning that all other $\mu(d, r)$ divide $\mu(d, s)$.
Plus, the old second part that the remainders are all multiples of s, here "corresponds" to a perfect reversal of the first part. So, all factors of $\mu(d, s)$ are equal to some $\mu(d, r)$.
A trivial consequence of this super length of course is that it has to be the maximal, so we can reformulate our claim as:
The maximal initial segment length is multiple of all other initial segment lengths. Plus:
All of its factors must be lengths of some initial segments.
This truly sounds fundamental and even Euler's theorem could have its true reason in it.
Indeed, since all $\mu(d, n)$ lengths divide the $\mu(d, s)$ maximal, it's enough if this divides $\varphi(d)$.
This would even suggest the idea that $\Phi(d)$ is somehow distributable into disjoint groups having this $\mu(d, s)$ maximal initial lengths and that's why it must divide $\varphi(d)$.
But to see that things are much more complicated is best to regard two examples.

$d = 20$	and	$d = 13$:
$\Phi(20) = \{ 1, 3, 7, 9, 11, 13, 17, 19 \}$		$\Phi(13) = \{ 1, 2, 3, \ldots, 12 \}$
$\varphi(20) = 8$		$\varphi(13) = 12$

Initial segments	μ	Initial segments	μ
1	1	1	1
3 , 9 , 7 , 1	4	2 , 4 , 8 , 3 , 6 , 12 , 11 , 9 , 5 , 10 , 7 , 1	12
7 , 9 , 3 , 1	4	3 , 9 , 1	3
9 , 1	2	4 , 3 ,12 , 9 , 10 , 1	6
11 , 1	2	5 , 12 , 8 , 1	4
13 , 9 , 17 , 1	4	6 , 10 , 8 , 9 , 2 , 12 , 7 , 3 , 5 , 4 , 11 , 1	12
17 , 9 , 13 , 1	4	7 , 10 , 5 , 9 , 11 , 12 , 6 , 3 , 8 , 4 , 2 , 1	12
19 , 1	2	8 , 12 , 5 , 1	4
		9 , 3 , 1	3
		10 , 9 , 12 , 3 , 4 , 1	6
		11 , 4 , 5 , 3 , 7 , 12 , 2 , 9 , 8 , 10 , 6 , 1	12
		12 , 1	2

There are three steps toward our fundamental law.
Initial segments will be called segments in short and denoted as $\{ r , \ldots , 1 \}$. Its length is $\mu(r)$.
1.) Factors:
Every $[r^k]$ remainder from an $\{ r , \ldots , 1 \}$ segment will initiate a segment that has length that divides $\mu(r)$ and in reverse every m that divides $\mu(r)$ is the length of an $\{ [r^k] , \ldots , 1 \}$.
Indeed, using μ for $\mu(r)$ we have $[r^{\mu}] = 1$ and so $[(r^k)^{\mu}] = [(r^{\mu})^k] = 1$ too.
Thus μ is definitely an exponent that makes 1 from $[r^k]$ and so $\mu([r^k])$ divides μ.
Also, $[(r^{m})^{m}] = 1$ so with $k =$ we got a member that becomes 1 at m. And of course it can not become at a factor of m because it would mean r becoming too at a factor of μ.
2.) Products:
The segments are each complete worlds in themselves containing all products and divisions.
In particular, the reciprocal of any $[r^k]$ is $[r^{\mu-k}]$ because $[[r^k][r^{\mu-k}]] = 1$.
If two segments' lengths $\mu(r)$ and $\mu(s)$ are relative primes then:
a.) Only 1 can be common member of $\{ r , \ldots , 1 \}$ and $\{ s , \ldots , 1 \}$.
Indeed, by 1.) any other common member would mean a common factor in the lengths.

b.) There is a $t \in \Phi(d)$ that $\mu(t) = \mu(r)\mu(s)$. Namely, $t = [r s]$ is such.
First observe that this t is indeed in $\Phi(d)$ because this is a complete world too, products are in.
Enough to prove that $\mu(t) = \mu(r s)$ and $\mu(r)\mu(s)$ divide each other.

$$[(r s)^{\mu(r)\mu(s)}] = [(r^{\mu(r)})^{\mu(s)}][(s^{\mu(s)})^{\mu(r)}] = 1$$

Thus $\mu(r)\mu(s)$ is a 1 giving exponent of $r s$ and so $\mu(r s)$ must divide this.
For the reverse, enough to show that $\mu(r)$ and $\mu(s)$ divide $\mu(r s)$ separately because being relative primes, this implies that their product divides too. To see this, observe that:

$[(r\,s)^{\mu(r\,s)}] = [r^{\mu(r\,s)}]\,[s^{\mu(r\,s)}] = 1$ means that $[r^{\mu(r\,s)}] = [[\frac{1}{s}]^{\mu(r\,s)}]$.

$[r^{\mu(r\,s)}] \in \{r, \ldots, 1\}$ and $[[\frac{1}{s}]^{\mu(r\,s)}] \in \{s, \ldots, 1\}$ but these two have only 1 as common element, so $[r^{\mu(r\,s)}] = 1$ and $[[\frac{1}{s}]^{\mu(r\,s)}] = 1$ which implies $[s^{\mu(r\,s)}] = 1$.

These two then indeed imply that $\mu(r)$ and $\mu(s)$ divide $\mu(r\,s)$.

In our first example we don't have such relative prime lengths but in the second we do the 3 lengths with 2 or 4 lengths. And indeed we have the 6 and 12 product lengths.

Also observe that these relative prime segments indeed have only 1 as common member.

3.) The super length.

We want to combine 1.) and 2.) and show that the maximal length is multiple of all others.

A first idea is to regard the prime factors of all lengths. These are lengths too and relative primes.

So we could multiply these but this wouldn't cover all factors of all lengths which are lengths.

The better version is to regard all prime factors with highest possible occurrence in some length.

The total product of these indeed must be a common multiple of all lengths and a length itself.

Thus it is the maximal. Since it is the lowest common multiple of all lengths, it is actually $\lambda(d)$.

Our steps revealed why all initial segment lengths divide the maximal, but they didn't reveal why the maximal lengths should always divide $\varphi(d)$. So, the earlier proofs of Euler's theorem remain the only "explanation". They of course did not regard the maximals rather any of them.

As we go further and ask more about the maximals we do get particular explanations why they divide $\varphi(d)$ for more concrete reasons than Euler's theorem.

This makes the whole thing even worse, because this fact does not depend on the particulars.

The most obvious case of the maximal length dividing $\varphi(d)$ is when it is $\varphi(d)$, that is we have base with full initial segment, or as Euler called such base, a primitive root.

Their possible existence or non existence or their number is not coming out from the fundamental picture either. But an other way of saying this, does come out as $\lambda(d) = \varphi(d)$.

We gave a calculating method for $\lambda(d)$ as Carmichael's theorem and now we can see why that should be the most difficult final theorem.

In fact if we had a similar calculation method for $\varphi(d)$, then this $\lambda(d) = \varphi(d)$ form of the existence of primitive roots at d, would at once give an effective method to tell these d exactly.

Luckily $\varphi(d)$ is much simpler than $\lambda(d)$ and so a similar method needs only two rules:

1.) For $d = p^k$ with any p prime $\varphi(p^k) = p^{k-1}(p-1)$.

2.) For $d = a\,b$ with relative prime a , b $\varphi(a\,b) = \varphi(a)\varphi(b)$.

Repeating this, gives φ directly for any $p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ through 1.) :

$\varphi(p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}) = \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}) \ldots \varphi(p_m^{k_n})$.

To prove these rules is easy by the meaning of $\Phi(d)$ and thus $\varphi(d)$ alone.

Obviously, rule 1.) here includes rule 2.) of $\lambda(d)$ for odd prime powers, so for these at once the two functions are the same.

Also, this rule 1.) coincides with the earlier 1.) for only 2 and 4.

And, finally the crucial combining rules can only coincide for a single 2 factor and an odd prime power because only for function values of these will "locomult" and multiplication be the same.

This follows from simple parity considerations.

So, we obtained that primitive roots, that is bases with full initial segments exist exactly for the following d dividers: 2 , 4 , odd prime powers , doubles of odd prime powers.

Gauss proved this result too without recognizing the rules for $\lambda(d)$, that is Carmichael's theorem.

Third New Look: Roots, Full Super Length For Prime Dividers

The amazing weakness of our previous new look and of the fundamental theorem obtained by it was that it didn't lead to Euler's theorem. It didn't show that the maximal segment length must divide the total number of remainders $\varphi(d)$. We couldn't find some magical groups in $\Phi(d)$.
Only the old multiple cycles can do the magic as we used them in the proof of Euler's theorem.
The only thing we obtained again without Euler's theorem is that $\lambda(d) \leq \varphi(d)$.
From this of course with $d = p$ prime divider $\lambda(p) \leq \varphi(p) = p-1$.

This section's new third angle will show that with prime divider if $[n^m] = 1$ is true for k many different $n_1, n_2, \ldots, n_k$ bases all under p then $k \leq m$ must be.

But $[n^{\lambda(d)}]$ is true for all n in $\Phi(d)$ so for $\varphi(d)$ many different bases under d.

So, with $d = p$ prime too, we have $p-1$ many solutions of $[n^{\lambda(p)}] = 1$. So $p-1 \leq \lambda(d)$.

Thus together with the previously obtained $\lambda(p) \leq p-1$, we will get $\lambda(p) = p-1$.
Then of course $[n^{\lambda(p)}] = [n^{p-1}] = 1$.

So we'll obtain Fermat's Little Theorem without Euler's.
That's interesting but wouldn't worth all the trouble.
And indeed, the real importance of $\lambda(p) = p-1$ is that by our previous fundamental theorem we also have $\mu(p, s) = \lambda(p)$ and so we also must have $\mu(p, s) = p-1$.
So we have full initial segment or primitive root for every p prime divider.

For $m = 1$ our claim simply means that there is maximum one n under p that $[n] = 1$.
That's trivial! This n is exactly 1.
For $m = 2$ our claim is not trivial but exact again. Indeed:
$[n^2] = 1$ is true for both 1 and $p-1$ because: $1^2 = 1$ and $[(p-1)^2] = [p^2 - 2p + 1] = 1$.
The non trivial part is that in between 1 and $p-1$ we don't have solution.

To see this, we simply have to go back to basics and see indirectly what it would mean $[n^2] = 1$.
Obviously that p divides $n^2 - 1 = (n-1)(n+1)$.
The first member is under p and if n is less than $p-1$ than the second is too.
Also they are both above 0 if n is above 1.
So, p can divide none of the two members if n is between 1 and $p-1$.
Of course primes divide separately, so these p can not divide their product either.
But, this is not the only complication because even our seemingly trivial exactness fails if 1 and $p-1$ are the same that is $p = 2$.
This shows that as m gets bigger and bigger our claim is becoming more and more difficult to see by some factorization plus the exactness can disappear too.
In fact, at $m = p$ quite generally we can't have m many solutions because there are only $p-1$ many remainders. But even for m under p we will have mostly less than m many solutions.
For example at $p = 5$ and $m = 3$ the possible remainders are 1, 2, 3, 4 and we have only one solution 1 and 2, 3, 4 are not: $[2^3] = 3$, $[3^3] = 2$, $[4^3] = 4$.

The factorization for $n^3 - 1$ is $(n-1)(n^2 + n + 1)$.

So again the first member is only dividable by p as the trivial $n = 1$ solution and so it would be enough to show that p can divide the second member for maximum two n values.
Then apart from these three values there can be no more, so we indeed have maximum three.
So, the outlines of a possible induction are already here.

The good news is that this factorization is universal:

$n^m - 1 = (n-1)(n^{m-1} + n^{m-2} + n^{m-3} + .. + n + 1)$

The bad news is that the second member is more complicated than the left side and the previous exponent $m-1$, guarantees maximality for only $n^{m-1} - 1$.

The solution is obvious. We have to widen our scope and prove maximality for forms that include both $n^m - 1$ and $n^m + n^{m-1} + n^{m-2} + .. + n + 1$.

A pretty wide such form is $n^m + a_1 n^{m-1} + a_2 n^{m-2} + .. + a_{m-1} n + a_m$.

The crucial truth about these forms is the following:

For every $n^m + a_1 n^{m-1} + a_2 n^{m-2} + .. + a_{m-1} n + a_m$ and n_o there are:

$b_1, b_2, . . , b_{m-1}$ and c so that: $n^m + a_1 n^{m-1} + a_2 n^{m-2} + .. + a_{m-1} n + a_m =$

$(n - n_o)(n^{m-1} + b_1 n^{m-2} + b_2 n^{m-3} .. + b_{m-2} n + b_{m-1}) + c.$

Indeed, the highest n^m power of n is already the same on both sides.
To make n^{m-1} the same too, we need that $a_1 = b_1 - n_o$ so we make $b_1 = a_1 + n_o$.
To make n^{m-2} the same we need that $a_2 = b_2 - n_o b_1$ so we make $b_2 = a_2 + n_o b_1$.
And so on, for the last n power: $a_{m-1} = b_{m-1} - n_o b_{m-2}$ so we make $b_{m-1} = a_{m-1} + n_o b_{m-2}$.
And for the final a_m we need that $a_m = c - n_o b_{m-1}$ so we make $c = a_m + n_o b_{m-1}$.
We can regard this whole process as division by $n - n_o$ and then c is the "remainder".

A trivial consequence of this identity is that if n_o was a number that written into n would make the left side be dividable by p then the obtained last c must also be.
Indeed, on the right side then the first member $(n - n_o)$ is dividable by p so the whole product is too and so the second member of the sum c must be too.

Now the more universal claim about remainders is this:

$n^m + a_1 n^{m-1} + a_2 n^{m-2} + .. + a_{m-1} n + a_m$ can be dividable by p for maximum m

many n values under p.

The $m = 1$ case now claims that $n + a_1$ is dividable by p for maximum one n value under p.
Indeed, $n + a_1 = K p$ implies $n = K p - a_1 = p - [a_1 - (K - 1) p]$.
So n is exactly $p - r$ with r being the remainder of p in a_1.

Now assuming it being true up to m we have two cases:
If there is no n value under p that makes the m case dividable by p then we are finished because nothing that is 0 is under m.
If there is at least one n_o under p that makes it dividable by p then using that:

$$n^m + a_1 n^{m-1} + a_2 n^{m-2} + .. + a_{m-1} n + a_m =$$

$$(n - n_o)(n^{m-1} + b_1 n^{m-2} + b_2 n^{m-3} .. + b_{m-2} n + b_{m-1}) + c.$$

with c being dividable by p.
Thus every n value that makes the left side be dividable by p must make the product be dividable too on the right. But this product is dividable by p only if one of its members is.
The first $(n - n_o)$ is only dividable for one value under p namely n_o.
The second by the induction assumption has maximum $m - 1$ many such n values.
So the left side can have maximum m many such n values.

Lucas Primality Test

To see is if a number is prime is not easy. We have to try smaller numbers to divide with.
We don't have to try all of them but still a lot.
In contrast, to verify $[n^{d-1}] = 1$ is easy because we can calculate remainders with our original step by step method from previous ones.
So Fermat's Little Theorem would be a perfect tool to tell primes easily if it were only true for these. This is not so and yet there is a prime test with it.
The idea is the two main theorems we used by names. Euler's and Gauss'.
From Euler's theorem it follows that for a non prime d we can not have $d-1$ long initial segment in any base we try. Indeed: $\mu(d, n) \le \lambda(d) \le \varphi(d) < d-1$. Quite oppositely:
Gauss' theorem tells that for $d = p$ prime we do have such n that $\mu(d, n) = d-1$.
So finally, Lucas put 1 and 1 together and realized that we can tell if d is prime from these two results with absolute certainty.
Of course not as easily as Fermat's Little Theorem directly would do it with a single iterative calculation but almost as easily:
We first of all check $[n^{d-1}] = 1$ for some randomly chosen $n < d$ base.
If it's not true then we trivially failed, d can not be prime by merely Fermat's Little Theorem.
If $[n^{d-1}] = 1$ then we are not sure yet because there are composite solutions. One thing is sure though, namely that at least n and d are relative primes because otherwise we cant have 1 remainders at all. So then by Euler's theorem if d is not prime then an earlier 1 at a place that divides $d-1$ must occur.
The prime factors of $d-1$ as places obviously have $[n]$ remainders by Fermat's Little theorem.
So we don't have to try these but we still have much more composite factors of $d-1$ to try.
Luckily, if an f factor as exponent gives 1 remainder then all multiples of f give too.
So it would be enough to test some particular F factors of $d-1$ so that all other f, are factors of such. Obviously the least many such F would be the best solution.
Amazingly the same many is enough as the number of prime factors.
Namely, these F should be all possible division results of $d-1$ with its prime factors.
Indeed, every f factor of $d-1$ must have a prime factor not in f, so must divide such division result. And of course, a 1 at f means the same at F.
So we divide $d-1$, with all of its prime factors and check these F results what $[n^{F-1}]$ is.
If all give non 1 then d is prime. Because they guarantee the same for all f.
If we find one that is not 1 then we still don't know because we might simply chose a wrong n base that doesn't guarantee a full initial segment. Of course Gauss' theorem guarantees such, so we have to choose a new n.
If d is prime then sooner or later we find an n where all F-s will give 1.

Carmichael's Theorem

Ancient And New Combined

This is a short prelude to our new section about the square sums. Unlike in the previous section where the prelude, the Blind Spots was a long journey, here we don't need that many details.
The ancient attention to square sums was related to the most famous old geometrical theorem, the Pythagoras Theorem that relates the sides of the right angle triangles as: $x^2 + y^2 = z^2$.
This newer x, y, z letter notation instead of the old fashioned a, b, c is due to the importance of the Descartes coordinate system. If x and y are the coordinates of a point, then z is its distance from the origin. More importantly, the same stands between two points, so if x and y are the coordinate differences, then z is the distance of the two points. This distance between two points is the most important invariant against the whole coordination idea. Indeed, the distances between points should not depend on what coordinate system we use to place the points in. To put it an other way: The distances are objective facts against the subjective descriptions of coordinate systems. Physics in general is using descriptions too but aims for the objective, invariant facts. So it's no wonder that the new mechanics of Relativity, turned out to be an amazing generalization of the Pythagoras Theorem. But now we jumped ahead, so let's return to the past.
The natural question was whether these sides in a right angled triangle can be whole numbers, that is multiples of a common unit.
And indeed the simplest example is $3^2 + 4^2 = 5^2$ because $9 + 16 = 25$.
An obvious fact is that multiplying the bases under same exponents with a common c number will make same multiple power values. So quite generally, if $x^n + y^n = z^n$ then we'll have also equality of the n powers with using the cx, cy, cz bases. In our simplest $3^2 + 4^2 = 5^2$ Pythagorean Triple using the simplest $c = 2$ common number we obtain that: $6^2 + 8^2 = 10^2$.
With $c = 3$ we get: $9^2 + 12^2 = 15^2$.
This trivial method of getting new triples raises the question that what are the genuine triples not obtainable this way. The condition of this is quite simple, namely the x, y, z numbers can not contain any common factor. Most importantly, this is enough for x and y because if equality stands then a c common factor of these is automatically must be in c too.
So we get the crucial refinement of $x^n + y^n$ power sums to "simple" power sums if x and y are relative primes. In particular, the ancient question became how we can get all the simple square sums that are squares. The surprisingly simple realization was that all such must be the square of a z value that itself is the square sum of u, v non equal numbers. This was merely an observation. Our simplest case is the simplest example: $3^2 + 4^2 = 5^2$ is a simple square sum and indeed 5 itself is $1^2 + 2^2$ so a square sum of two different values.
$1^2 + 1^2 = 2$ or $2^2 + 2^2 = 8$ are not suitable candidates for z because $u = v$ here.
And indeed, neither of these have squares that are square sums.
The smallest example bigger than 1 and 2 is obviously 2 and 3 so $z = 2^2 + 3^2 = 13$.
And voila $13^2 = 169$ is indeed a simple square sum as: $25 + 144 = 5^2 + 12^2$.
The Babylonians were even able to find the simple formulas that give x and y, from u and v.
$x = v^2 - u^2$ and $y = 2uv$ assuming that $u < v$. And indeed:
$(v^2 - u^2)^2 + (2uv)^2 = v^4 + u^4 - 2v^2u^2 + 4u^2v^2 = v^4 + u^4 + 2v^2u^2 = (v^2 + u^2)^2$.
So $x^2 + y^2 = z^2$ follows for these x and y values.
Of course, the crucial point was still missing, namely to prove that these give all possible simple square sums. Amazingly, two simple formulas prove that too:

$$u = \sqrt{\frac{z-x}{2}} \quad , \quad v = \sqrt{\frac{z+x}{2}}$$

First observe that at once, $u^2 + v^2 = \frac{z-x}{2} + \frac{z+x}{2} = z$.

This came out too easy and so we feel that something must be wrong but actually everything is fine. The unused y value is hidden in the condition that $x^2 + y^2 = z^2$ is a simple square sum. Then it's easy to see that this makes actually possible that our formulas work.
There are two obvious steps! First, why the fractions under the square roots are wholes.
And then, why they are square numbers too. So the square root gives wholes too.
For these fractions to be wholes, means that $z - x$ and $z + x$ are even.
To see this, first lets remember that the simplicity or relative primeness is enough for two values from the x, y, z triple.
In particular for 2 factors or evenness too, already two can not be such.
So maximum one of x, y, z can be even. But a different argument shows that one must be:
Indeed, all odd x, y, z numbers would mean all odd powers too and so $x^n + y^n$ were even while the other side z^n is odd. So quite generally, exactly one of x, y, z is even.
At the special $x^2 + y^2 = z^2$ Pythagorean case, the even can not be z.
Indeed, the square of an even number is $(2k)^2 = 4k^2$ and thus, is dividable by 4.
Now the other side would have the sum of the two odd squares. But:
The square of an odd number is $(2k+1)^2 = 4k^2 + 4k + 1$ and thus, has 1 remainder to 4.
So, the sum of two such numbers must have 2 remainder to 4 and thus, could not be equal to the other side, which as we showed, was dividable by 4.
So, z must be odd and one of x or y is odd too. Their role is symmetrical, so we can choose y to be the even. Then, z and x are the odds and so, indeed, $z - x$ and $z + x$ are evens, so the fractions in our formulas give whole numbers. But why are they squares? This is a bit trickier:
First observe, that $\frac{z-x}{2}$ and $\frac{z+x}{2}$ are relative primes too. Indeed, if they had a c common factor, then this c would divide their sums and differences, which happen to be z and x.
But of course, we assumed that these are relative primes. So the two fractions are relative primes.
Now comes the real trick, lets multiply these together:

$$\frac{z-x}{2} \bullet \frac{z+x}{2} = \frac{(z-x)(z+x)}{4} = \frac{z^2-x^2}{4} = \frac{y^2}{4} = \left(\frac{y}{2}\right)^2$$

We showed already that y was the even, so $\frac{y}{2}$ is a whole and thus, the product of the two fractions is a square for sure. But why are they squares themselves?
Simply, because they are relative primes. The $\frac{y}{2}$ number can be anything, having any kind of prime factors, like $2 \bullet 3 \bullet 3 \bullet 5 \bullet 13$. But, the square of this will definitely mean doubling all these prime factors. Now, since the two fractions multiplied is equal to this square, it must have double occurrences of all prime numbers. But also, them being relative primes means they don't share any prime factors. So indeed, both of them contain doubles of different prime factors. So, both of them are squares. Thus, we proved that our formulas for the "reverse" of Babylon are wholes.
I am not going into now why the Babylonians couldn't find these reverse formulas.
What is more important is that you can go on the net today, type in Pythagorean Triples and you'll find a flood of overcomplicated and stupid abstractions except the formulas I showed.
This is that should concern you and if it's not then you are in deep trouble yourself!

We have to see that even though the Babylonian solution was reversed, in some sense the reversal was not perfect. Namely, though we did produce all the simple square sums that are squares, we did produce non simple ones too! For example, $6^2 + 8^2 = 10^2$ is produced because 10 itself is a square sum from two different values. On the other hand $9^2 + 12^2 = 15^2$ is not produced.

The reasons for these imperfections is that the whole question of when the square sum is itself square is in some sense an artificial one. We have to say “in some sense” because in an other sense it is non artificial at all, rather leads to the deepest problem of Number Theory.
The person who explored both of these “senses” was Fermat the original great number theorist.
The first direction that avoids the restriction that a square sum should be square itself, leads to the grand view that it is much better to see what numbers can be simple square sums in general. And this has to do with their prime factors. Then we can ask when the primes themselves are square sums and can observe an amazing law that goes much deeper than the above Pythagorean goose chase.
The primes are all odds except the single 2 and so a natural new evenness or oddness among the odd primes could be whether they are $4k+1$ or $4k-1$ types.
$5, 13, 17, 29, \ldots$ are the $4k+1$ primes and the rest $3, 11, 19, \ldots$ are the $4k-1$.
These seem to appear and mix without any rule so it is amazing that:
The $4k+1$ primes are all square sums in a unique way and the $4k-1$ ones are never.
So the $4k$ splitting of the primes coincides with their square sumness!!!
This will be the main line of this section!
But Fermat became more famous for his other direction that is pursuing the square sum being square question. The surprising fact is that other bigger exponents never produce power sums that equal a same power. So $x^n + y^n = z^n$ is impossible for any n bigger than 2.
This is amazing because the two x and y values can vary already so to miss all whole z is a big thing with one fix chosen n too, but to miss all whole z for all n exponents should either be some triviality or some very difficult meta law. It turned out to be this second.
This became clear soon because even the simplest n after 2, the 3 exponent case became a nightmare. In fact, Fermat himself could only sketch the $n=4$ impossibility.
Of course he claimed the general rule and even pretended a proof on a margin.
He did similar lies with other proofs in his letters, blaming the lack of space or time.
He was a genius entering into the times when rigorous proofs started to be more important than smart recognizings. So he stretched the truth a bit. By the way he was a lawyer.
The two giants Euler and Gauss despised Fermat and failed to see the irony behind the whole pain that Fermat “made them” enter.
Euler’s proof for the impossibility of $n=3$ case was not perfect and I explain that fiasco in an other article. It is relating to the first road that regards square sums on their own.
Gauss was the one who saw behind that road but his new “complex” numbers were more than just number theoretical tools. In fact, his tragedy was that he felt the deep physical applications of the future but couldn’t see the new physics yet.
The reactions to frustrations can be very sad.
Fermat’s straight out lies are less concerning to me than Euler’s denial or Gauss’ white lies.
When they asked him about Fermat’s Last Theorem he pretended that it is not that vital.
We still live in denial about it even after it has been proven.

Perfect Pairs Under A Prime, Wilson's Theorems, Square Sums

We are again looking at remainders of a p prime. Also, we'll use a fundamental fact of remainders in general, namely that if two a , b numbers have 1 remainders to a d divider, then their product will also have 1 remainder to d. Indeed: If $a = m\ p + 1$ and $b = n\ p + 1$ then,

$a\ b = (m\ p + 1)\ (n\ p + 1) = m\ p^2 + m\ p + n\ p + 1 = M\ p + 1$

This then inherits to products with arbitrary many members, in particular any powers of numbers with 1 remainder, will also have 1 remainder.

The remainders to a p prime are the numbers under it, that is 1 , 2 , 3 , . . . , $(p - 1)$.

These are their own remainder to p, but multiplying already two of them can easily be much bigger than p. Multiplying all of them will give the huge number abbreviated as $(p - 1)$ **!** and called as the factorial of $(p - 1)$. Strangely, the more important first theorem of Wilson will give not this factorial's remainder, rather the one step earlier, that is $(p - 2)$ **!** . The remainders to p will again be abbreviated with $[\ ]$ and so, the claim will be: $[(p - 2)\ !] = 1$. This of course, at once gives $[(p - 1)\ !]$ too as $p - 1$. So why is the total product upto $p - 2$ simpler?

To see this, we have to define the "perfect pairs" under p and regard the products combined from those pairs, rather than going in increasing order. So what is this perfect pairing? The answer is fitting into our fundamental principle regarding the 1 remainders and so, two r , s remainders of a p are perfect pairs if their product $r\ s$ has 1 remainder: $[r\ s] = 1$

The first surprising fact is that the perfect pairs are quite unpredictable! If one uses a concrete p prime, say 13, and then picks a remainder, say 5, then it takes a lot of trial and error to find the perfect pair of 5, which is 8 because $5 \bullet 8 = 40 = 3 \bullet 13 + 1$.

The second more important surprise is that in spite of this, all numbers under p will have its unique pair, except the 1 and $p - 1$ numbers. These two are actually their own perfect pairs.

Indeed, $1 \bullet 1 = 1$ so 1 is actually a self perfect pair for any p and

$(p - 1)\ (p - 1) = p^2 - 2\ p + 1 = p\ (p - 2) + 1$.

To see this amazing pairing of the 2 , 3 , . . . , $p - 2$ numbers, one simply has to pick a fix r remainder and then try all possible values as the s second member. Or to put it another way, one simply has to regard the r , $2\ r$, $3\ r$, . . . , $(p - 2)\ r$, $(p - 1)\ r$ products or rather their remainders. Then, it is easy to see that these remainders must be all different. Indeed, if $s\ r$ and $t\ r$ would have the same remainder, that is $[s\ r] = [t\ r]$ were, then this would mean that $t\ r - s\ r$ is a multiple of p. But, $t\ r - s\ r = [t - s]\ r$ and both $t - s$ and r are under p and thus, not dividable by p, which implies that their product is not dividable either. Indeed, a prime must divide products separately. This was the heuristic external atomness of primes.

Thus, the $[r]$, $[2\ r]$, $[3\ r]$, . . . , $[\ (p - 2)\ r\ ]$, $[\ (p - 1)\ r\ ]$ list contains all different values.

But, they are $p - 1$ many and there are only $p - 1$ many possible values under p.

So, by the so called "pigeon hole" principle, we actually must have all possible values appearing.

Thus, our particular 1 desired remainder must also appear. As we mentioned above, if r is chosen as 1 or $p - 1$, then we know that the 1 remainder is the first or the last in the list.

For any other r, a unique s pair will make $[s\ r] = 1$ because we only have one 1 appearing.

But also, for all $r \neq 1$ or $p - 1$ chosen values, the s pair of r cannot be itself r.

To see this, we again use the pigeon hole principle in an even more limited version, namely we can show that an $s = r$ scenario, that is $[r^2] = 1$ condition can only stand for two r values.

Then, since we know that $r = 1$ and $r = p - 1$ are true cases, thus, these are the only ones.

Now to show that only two solutions are for $[r^2] = 1$, we can simply regard a second $[s^2] = 1$.

Then, these two imply that $[s^2 - r^2] = 0$ and so, $s^2 - r^2 = (s - r)\ (s + r) = m\ p$.

So, p must divide one of the members. It obviously can't divide $s - r$, so it has to divide $s + r$.

This itself is less than $2\ p$, so it actually must be p. And thus, $s = p - r$, so for every 1 remainder giving r^2, there is only one other, its $p - r$ complement. By the way, we see this being true for our actual 1 square remainders because 1 and $p - 1$ are indeed complementing ones.

Now that we know that among the $2, 3, \ldots, p-2$ remainders, there is a unique and different pair for every one, we can pair these next to each other and calculate their product in this way:

$$(p-2)! = 2 \bullet 3 \bullet \ldots \bullet p-2 = (2 \bullet \frac{p+1}{2}) \bullet (3 \bullet ?) \bullet (4 \bullet ?) \bullet \ldots \bullet (? \bullet ?)$$

I placed the pairs in parenthesis merely for better visualization.

The perfect pair of 2 at the start is definitely $\frac{p+1}{2}$ but already in the second parenthesis I merely placed a question mark for the perfect pair of 3. Indeed, we might think that it has to be $\frac{p+1}{3}$ but it is not certain whether $p+1$ is dividable by 3 at all. So, the perfect pair of 3 is not always this. In the last pair, I had to place question marks for both members. This is so because the $2, 3, 4, \ldots$ as first members is not really an increasing sequence.

Indeed, once we find a second member, then that mustn't be tried anymore as first. For example, the perfect pair of 3 could be 4, and then $(4 \bullet ?)$ won't even appear. In spite of this complication, we will have definitely $\frac{p-3}{2}$ many perfect pairs, because we have $p-3$ many numbers to start with. Even more importantly, if we look at the remainder of our product, then it can be calculated pair by pair, each giving a definite 1 value, thus proving our claim:

$$[(p-2)!] = [2 \bullet \frac{p+1}{2}] \bullet [3 \bullet ?] \bullet [4 \bullet ?] \bullet \ldots \bullet [? \bullet ?] = 1$$

Another way to say this without remainders is that $(p-2)! = M\,p + 1$.

Wilson's second theorem will use this first, but also rearrange the $2 \bullet 3 \bullet \ldots \bullet p-2$ product in a different third order as $2 \bullet 3 \bullet 4 \bullet \ldots \bullet \frac{p-1}{2} \bullet (p-2) \bullet (p-3) \bullet \ldots \bullet (p - \frac{p-1}{2})$.

So up to the middle, that is upto $\frac{p-1}{2}$, we went in increasing order, but then the rest of the bigger numbers, we put them in decreasing order, starting from the last $p-2$. It's easy to check, that then indeed the last member must be $\frac{p+1}{2}$, but this itself written in the $p - \frac{p-1}{2}$ form.

The reason for these strange "forced" $p-r$ forms for the second half, is used by realizing that multiplying those in an algebraic manner, must give an $m\,p \pm 2 \bullet 3 \bullet \ldots \bullet \frac{p-1}{2}$ value.

The $\pm$ depends on how many members we have in this second half, namely if $\frac{p-1}{2}$ is odd, then we have even many members, that is a $+$ value from these even many negative members.

If $\frac{p-1}{2}$ is even, then the $-$ sign will stand. In short:

$$(p-2)! = 2 \bullet 3 \bullet 4 \bullet \ldots \bullet \frac{p-1}{2} \bullet (p-2) \bullet (p-3) \bullet \ldots \bullet (p - \frac{p-1}{2}) =$$

$$\frac{p-1}{2}! \,(m\,p \pm \frac{p-1}{2}!) = N\,p \pm \left(\frac{p-1}{2}!\right)^2 = M\,p + 1. \text{ Thus:}$$

$$\left(\frac{p-1}{2}!\right)^2 = (M-N)\,p + 1 \quad \text{if } \frac{p-1}{2} \text{ is odd. And:}$$

$$\left(\frac{p-1}{2}!\right)^2 = (N-M)\,p - 1 \quad \text{if } \frac{p-1}{2} \text{ is even.}$$

So, $\left(\frac{p-1}{2}!\right)^2$ has 1 remainder to p if $\frac{p-1}{2}$ is odd, but has -1 or rather $p-1$ remainder if $\frac{p-1}{2}$ is even. Strangely, this less simple case is the more important. It can also be said as:

If $\frac{p-1}{2}$ is even, then $\left(\frac{p-1}{2}!\right)^2 + 1$ is dividable by p.

First of all, $\frac{p-1}{2}$ being even, that is $2k$ also means that $p = 4k + 1$. These primes are:

$5 = 4 \bullet 1 + 1$, $13 = 4 \bullet 3 + 1$, $17 = 4 \bullet 4 + 1$, $29 = 4 \bullet 7 + 1$, . . . , $p = 4k + 1$

And these are all dividing the $((2k)!)^2 + 1$ numbers. And indeed:

5 divides $((2 \bullet 1)!)^2 + 1 = 2^2 + 1 = 5$
13 divides $((2 \bullet 3)!)^2 + 1 = (6!)^2 + 1 = 720^2 + 1 = 518401$
17 divides $((2 \bullet 4)!)^2 + 1 = (8!)^2 + 1 = 40320^2 + 1 = 1625702401$

The relationship of this second Wilson theorem to our main subject is clear, once we realize that $\left(\frac{p-1}{2}!\right)^2 + 1$ is actually a square sum, because $1 = 1^2$.
In fact, such square plus one numbers, are always simple square sums, because 1 is relative prime to any number.
As I mentioned in the prelude, Fermat realized that the $4k + 1$ versus $4k - 1$ splitting of the primes coincides with their square sumness, namely the $4k + 1$ ones are exactly the square sums only and what's more uniquely. But the really hard part is the mere fact that all $4k + 1$ primes are square sums. Indeed the impossibility for $4k - 1$ primes and the uniqueness for $4k + 1$ ones are easy exercises.
Wilson's second theorem concretely gives a square sum, but it only claims that the $4k + 1$ primes divide this square sum. Amazingly, from this we can prove through our investigations, that the prime itself is a square sum.
The reason for this seemingly over complicated road to show that all $4k + 1$ primes are square sums, is easy. Namely, just as our initial idea, the perfect pairs under a prime, are unpredictable, yet always true, similarly, this square sumness of the $4k + 1$ primes is unpredictable too.
Indeed, just looking at the examples:
$5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, . . .
The square members show no obvious pattern or method to be obtained from the total value.
But unlike above at the perfect pairings, where the existence was a fairly easy exercise, here even the existence is a very hard road. The point is to start from the much easier fact, that these primes divide a simple square sum. Then, the amazing fact, that the prime factors of a simple square sum, themselves must be such, will provide the proof. Wilson's second theorem, gave an explicit simple square sum in the form of $\left(\frac{p-1}{2}!\right)^2 + 1$, of which p is definitely a factor of.
In the next paragraph, we will make a detour and merely generalize the ideas used above.
This will give a second proof of the fact that a $4k + 1$ prime is factor of an $r^2 + 1$ but now with some r remainder of p.
So, it gives a much smaller simple square sum than Wilson's second theorem.
The drawback is that this r will not be given explicitly. Merely, its existence will be proven.

Product Pairs, Square Root Complementarity, Euler Criterion, Square Complementarity

Amazingly, the whole starting idea of the previous paragraph, that is the chasing of the 1 remainders was not that important in the proof of Wilson's first theorem. In other words, perfect pairs do exist if we strive for not $[r\ s] = 1$ rather any $[r\ s] = q$ value under p, that is regard product pairs with any q remainder value.
The proof for example that we can have only two complementing self pairs that is $[r^2] = q$ and $[s^2] = q$, now will go identically because these also mean $s^2 - r^2 = (s - s)(s + r) = mp$.
But now these r and $s = p - r$ values can be regarded as the "square roots" of q. So our result indeed means the second claim in our title, that is complementing square roots.
The third claim, the so called Euler Criterion comes about by calculating again the remainder of total product or factorial. The square roots of q again must be left out from the numbers under p but now these are not 1 and $p - 1$ rather can be any other complementing two members.
So again instead of having $\frac{p-1}{2}$ many pairs, we only have $\frac{p-1}{2} - 1$ many and these all have q remainders so their product would have $[q^{\frac{p-1}{2}-1}]$. This of course is a false value for the total factorial's remainder because the two square roots must be included. Luckily they are complementing, so:

$$[(p-1)!] = [1 \bullet 2 \bullet 3 \bullet \ldots \bullet (p-1)] = [r\ (p-r)\ q^{\frac{p-1}{2}-1}] = [[rp - r^2]\ q^{\frac{p-1}{2}-1}] =$$

$$[(p - [r^2])\ q^{\frac{p-1}{2}-1}] = [(p-q)\ q^{\frac{p-1}{2}-1}] = [p\ q^{\frac{p-1}{2}-1} - q^{\frac{p-1}{2}}] = p - [q^{\frac{p-1}{2}}]$$

We again used remainders in products, but also twice the fact that: $[m\ p - x] = p - [x]$

Of course we know this $[(p-1)!]$ value from Wilson's first theorem also to be as $p - 1$.

Thus then $[q^{\frac{p-1}{2}}] = 1$.

Unfortunately we made a little mistake because we assumed that q must have square roots.
If it doesn't then luckily the situation even simpler because all members will be in perfect pairs and exactly $\frac{p-1}{2}$ many such pairs give: $[(p-1)!] = [q^{\frac{p-1}{2}}] = p - 1$.

Now we see why this theorem is called Euler Criterion. Indeed, the value of $[q^{\frac{p-1}{2}}]$ is either 1 or $p - 1$ according to whether $q = [r^2]$ or $q \neq [r^2]$. So we have a criteria for this.

This theorem can also be regarded as a refinement of Fermat's earlier, so called Little Theorem that $[q^{p-1}] = 1$. Indeed, squaring the two cases of the Euler Criterion, both gives this equality.

A more important use of Euler's Criterion is when we simply check out this criteria of q being a square or not, for the complementing $p - q$ too:

$$[(p-q)^{\frac{p-1}{2}}] = [mp + (-q)^{\frac{p-1}{2}}] = \begin{cases} [q^{\frac{p-1}{2}}] \text{ if } \frac{p-1}{2} = 2k \text{ so } p = 4k+1 \\ p - [q^{\frac{p-1}{2}}] \text{ if } \frac{p-1}{2} = 2k-1 \text{ so } p = 4k-1 \end{cases}$$

Indeed, $(-q)$ to an even power is plus, while to an odd is minus.

These are exactly the values of the $[(p-1)!]$ split, but that was according to whether q is not square or square. But, $[q^{\frac{p-1}{2}}] = p-1$ or 1 and these two can't be equal, so this identical split can only happen if the complements themselves obey two laws:
For $p = 4k+1$, the square q-s are complements among themselves and thus of course, the non squares too. For $p = 4k-1$, the complements of square q-s are exactly the non square q-s.
$q = 1$ is always a square, so $p-1$ is always a square at $p = 4k+1$ but never at $p = 4k-1$. So:
$p = 4k+1 \rightarrow p-1 = [r^2] \rightarrow r^2 = mp + p - 1 = (m+1)p - 1 \rightarrow r^2 + 1 = (m+1)p$
In short: Every $4k+1$ prime divides an $r^2 + 1$.

Inductive Square Sumness for Prime Factors of Simple Square Sums

As I mentioned, the fundamental big claim from which the square sumness of the $4k+1$ primes follows, is that all prime factors of a simple square sum are simple square sums too.
The point of course is that they have to be square sums, because a prime can only be simple square sum anyway:

Simple Square Sum Theorem:
All prime factors of a simple square sum are also simple square sums.
In other words:
If A, B are relative primes and $A^2 + B^2 = p_1 p_2 \ldots p_k$
then all these p_i prime factors are square sums.
Indeed, this already implies that they are simple because they are primes.

Proof:
The smallest simple square sum is $1^2 + 1^2 = 2$, and the claim is obvious here because it is a prime. Suppose our claim is true for all simple square sums up to the $N = A^2 + B^2$.
We'll show how the claim inherits to N. If N is a prime then again it is trivially true.
So, we can assume N has at least two prime factors and that these are named increasingly:
$p_1 \le p_2 \le \ldots \le p_k$.
Since A and B are relative primes and not 1, they can not be equal and thus we may assume that $A < B$. So: $p_{k-1}^2 \le p_{k-1} p_k \le p_1 p_2 \ldots p_k = A^2 + B^2 < 2B^2$
The two ends imply that $p^2 < 2B^2$ for all p prime factors except maybe the biggest p_k.
Since p divides $A^2 + B^2$, if it would divide A or B it would have to divide both, contradicting that they are relative primes. So p cant divide neither of them.
Thus, we can form a, b remainders or excesses by:

$A = m\,p \pm a$, $B = n\,p \pm b$ with $a, b < \frac{p}{2}$. Then :

$A^2 + B^2 = m^2\,p^2 + a^2 \pm 2\,m\,p\,a + n^2\,p^2 + b^2 \pm 2\,n\,p\,b$. So, p divides $a^2 + b^2$ too.

Let the greatest common divider of a and b be g. This of course is maximum $a, b < \frac{p}{2}$.

Thus, p can not divide g but divides $a^2 + b^2 = g^2\left[\left(\frac{a}{g}\right)^2 + \left(\frac{b}{g}\right)^2\right]$.

So, p divides $\left[\left(\frac{a}{g}\right)^2 + \left(\frac{b}{g}\right)^2\right] \le a^2 + b^2 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 = \frac{p^2}{2} < B^2 < A^2 + B^2 = N$

By the induction assumption the [ ] simple square sum has only square sum prime factors and thus all these p are such. If incidentally p_k was the same $p^2 < 2\,B^2$ kind, then we are finished. If it is not, so it was too big to be covered by the above argument then we use a trick.
We'll divide N gradually with the small p_1 , . . . , p_{k-1} and show, that the results are again square sums, finally obtaining it for p_k too. Thus, the following lemma is enough:

If an n square or square sum has a p square sum prime factor, then $\frac{n}{p}$ is again a square or square sum.
This lemma allows squares but in our case, knowing that p_k is a single biggest prime factor, we can not get squares, thus only square sums. Now to prove the lemma:

Let $n = A^2 + B^2$ and $p = a^2 + b^2$.

$$\frac{A^2+B^2}{a^2+b^2} = \begin{cases} \left(\frac{A\,a+B\,b}{a^2+b^2}\right)^2 + \left(\frac{A\,b-B\,a}{a^2+b^2}\right)^2 \\ \left(\frac{A\,a-B\,b}{a^2+b^2}\right)^2 + \left(\frac{A\,b+B\,a}{a^2+b^2}\right)^2 \end{cases}$$

can be verified by squaring the sums in the numerators.
At least one of the forms will contain wholes, thus giving the square or square sum.
Indeed, $a^2 + b^2$ divides $a^2\left(A^2 + B^2\right) - B^2\left(a^2 + b^2\right) = \left(A\,a + B\,b\right)\left(A\,a - B\,b\right)$
So $a^2 + b^2$ being prime, divides at least one of these two factors, which makes at least one of the two first fractions above a whole. Then of course, the other member must be a whole too.

Instant Square Sumness for Prime Factors of Simple Square Sums

Reversal for Prime Products, The special Role of 2