Primes

1. Primes and Relative Primes

D

1.) A d natural number <u>divides</u> n or d is <u>divider</u> of n if $n = md$ with m natural too.

2.) Since $n = 1 \cdot n$ for every number, thus the 1 and n dividers of n are trivial.
The non 1 dividers of n are also called <u>factors</u> of it.
So the trivial divider n itself is allowed as trivial factor and only the universally trivial 1 is excluded. Thus the number 1 has no factors but all other numbers have.

3.) The numbers that have only the trivial factor themselves are called <u>primes</u>.
These are : 2 , 3 , 5 , 7 , 11 , 13 , 17 , . . .
The others that do have smaller factors too, are called <u>composites</u>.
Every a smaller factor of the c composite means a corresponding b so that $c = a\,b$.
So c can be written as non trivial product or as we say it, it is factorizable.
Primes of course are not factorizable because their only factor themselves has no pair.

4.) A <u>prime factorization</u> of a composite c is done by factorizing it as $c = a\,b$, then factorizing these a , b factors again and again if possible.
Since these factors are getting smaller and smaller, we must end up with unfactorizable primes. For example:

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

R

As we see, we went different ways but we always ended up with the same prime factors.
If n is a prime, then itself can be regarded as its trivial prime factorization.
Thus, in general: Every number except 1 can be uniquely factorized from primes.
This is called the Unique Prime Factorization Theorem, in short U.P.F.T.
This can be also expressed as follows:
If $p_1\,p_2 \ldots p_m = q_1\,q_2 \ldots q_n$ with all primes,
then, $m = n$ and the same primes appear on both sides.
The U.P.F.T. feels like a “natural” fact. But we learn to multiply at an early age, so the unique breakdown only seems obvious due to our familiarity with multiplying small values.
Regarding huge numbers nothing suggests that we couldn’t end up with different primes.

T

1.) Fundamental Theorem of Primes: Primes divide products separately.
That is: If p divides m n then p divides m or p divides n (maybe both)

2.) If a p prime divides a $q_1\,q_2 \ldots q_n$ product of primes then p is one of the q-s.

3.) U.P.F.T.: If $p_1\,p_2 \ldots p_m = q_1\,q_2 \ldots q_n$ with p , q all primes,
then $m = n$ and both sides contain the same primes.

P

1.) We use $<$ induction on the p primes. For $p = 2$, the claim means that if $m\,n$ is even, then m or n (or both) must be even. Indeed, the product of two odds is:
$m\,n = (2\,j + 1)\,(2\,k + 1) = 4\,j\,k + 2\,j + 2\,k + 1 = \text{even} + \text{even} + \text{even} + 1 = \text{odd}$.
Suppose our claim of separate dividability is true for all primes up to a p prime.
We must show that p divides separately again. For this it's enough to derive a contradiction from assuming that p doesn't divides separately, that is p divides an $m\,n$ product, but neither of m, n. We'll show that then p had to be composite.
p not dividing m, n these have r, s remainders to p, that is: $m = j\,p + r$, $n = k\,p + s$.
Then $m\,n = (j\,p + r)\,(k\,p + s) = j\,k\,p^2 + j\,p\,s + k\,p\,r + r\,s = K\,p + r\,s$
So p divides $r\,s$, say $p\,q = r\,s$. Also: $r, s < p \;\rightarrow\; p\,q = r\,s < p^2 \;\rightarrow\; q < p$
If $q = 1$, then at once $p = r\,s$ so since $r, s < p$ it is composite.
If $q \neq 1$, then let a prime factorization of q be: $p_1\ p_2\ \ldots\ p_k$
By our assumption the claim is true up to p, so $p_1, p_2, \ldots, p_k$ divide separately.
So in, $p\,q = p\ p_1\ p_2 \ldots p_k = r\,s$ too, p_1 divides r or s, say r.
So $p\ p_2 \ldots p_k = \frac{r}{p_1}\,s$. Then again p_2 divides $\frac{r}{p_1}$ or s, say s.
So $p\ p_3 \ldots p_k = \frac{r}{p_1}\frac{s}{p_2}$. And so on, all p_i can be removed and finally
$p = \frac{r}{p_1 \ldots}\ \frac{s}{p_2 \ldots}$. None of these two on the right can be p, because $r, s < p$ already.
So indeed, p turned out to be a composite as we claimed.

2.) By 1.), p must divide q_1 or $q_2 \ldots q_n$.
In the first case, $p = q_1$, in the second again p must divide q_2 or $q_3 \ldots q_n$.
In the first case, $p = q_2$, in the second again p must divide q_3 or $q_4 \ldots q_n$.
And so on, finally p must be one of them.

3.) By 2.) $p_1 = q_i$. Lets divide both sides with this, then $p_2 \ldots p_m = q_1\ q_{i-1}\ q_{i+1} \ldots q_n$
Again, $p_2 = q_j$ and so on, finally $p_m = q_k$.

R

The negative form of the Fundamental Theorem of Primes is that if p doesn't divide m and n then it can't divide $m\,n$. A special case of this is that: If $m, n < p$ then p can't divide $m\,n$. This special negative case implies the general negative form because if m, n have r, s remainders to p then $m\,n = (j\,p + r)\,(k\,p + s) = K\,p + r\,s$
Another way of saying the negative form is that: If n is not dividable by p, then $n, 2\,n, 3\,n, \ldots, m\,n, \ldots$ are only dividable by p for the $m = k\,p$ multiples.
Amazingly, if we try the $n, 2\,n, 3\,n, \ldots, (p-1)\,n$ to divide with p, we'll see that not only they are not dividable by p, but actually we'll get all the possible $1, 2, \ldots, p-1$ non zero remainders, merely in some other order. For example, with $n = 4$ and $p = 7$ the $4, 8, 12, 16, 20, 24$ numbers give the remainders $4, 1, 5, 2, 6, 3$.
If p is not a prime, merely a d number that has no common factor with n, then again $n, 2\,n, 3\,n, \ldots, (d-1)\,n$ give all non zero remainders to d.
For example, with $n = 4$ and $d = 9$ the
$4, 8, 12, 16, 20, 24, 28, 32$ numbers' remainders are: $4, 8, 3, 7, 2, 6, 1, 5$.
If d and n are totally unrestricted, then the remainder sequence is a bit more complicated. It is not merely a reordering but also some repetitions of an arithmetical sequence:
$0, s, 2\,s, 3\,s, \ldots, k\,s$, where s is the smallest remainder.
The most important difference being that, zero can appear among these too.
These ideas lead to a generalization of the concept of primes and three generalizations of the Fundamental Theorem of Primes:

D

d and n are relative primes if they have no common factor. Their only common divider is 1.
Thus, 1 is relative prime to any number because 1 has no factor at all.
Relative primes don't have to be primes, for example 4 and 9.
A prime of course is relative prime to all smaller numbers, but not to itself or its multiples.

T

1.) Fundamental Theorem of Relative Primes:
If d is relative prime to n , but it divides m n then it must divide m.
Observe that this implies the Fundamental Theorem of Primes. Indeed using a d prime, it will be relative prime to n exactly if it doesn't divide n and thus must divide m.
Also in reverse, the Fundamental Theorem of Primes implies this, but only through the Unique Prime Factorization. Indeed, d's prime factorization can only contain primes that don't divide n and since d divides m n, these prime factors all divide m n too and so m, by merely the Fundamental Theorem of Primes. But this doesn't mean that their product d also divides m. This follows only because these prime factors of d are all there in m's prime factorization.

2.) Remainder Theorem: Let [ ] denote the remainders to d. Then:
If s is the smallest non zero among [n] , [2 n] , . . . , [(d – 1) n] then:
1. s , 2 s , . . . , (d – 1) s, must appear among them too.
2. s is common divider of d and n.

If d is relative prime to n , then of course the only common divider is 1 so s must be 1.
Then we have all possible non zero remainders among [n] , [2 n] , . . . , [(d – 1) n].
But they are only d – 1 many, so they are actually exactly the non zero remainders.
So, 0 is missing and thus the first multiple of n that divides d is d n.
The remainders of m n will repeat for m multipliers after d and so we get the same group without zero, repeated and separated by the only zeros at m = k d.
So 2.) implies 1.) trivially but says much more detail about the remainders.

3.) Super Common Divider Theorem:
The greatest common divider of any d and n numbers is such that all common dividers of d and n divide it. So it is a "super" common divider too.

P

1.) We already showed above how U.P.F.T. proves it, but we give two proofs without this.
In this first one we use " < " induction again, but now on the m n product values.
For m n = 1 the claim is trivial, because m , n , d are all 1.
Suppose our claim is true for all values up to m n.
If d = n then they being relative primes means d = n = 1, so d divides m trivially.
If d < n and d divides m n then it also divides m n – m d = m (n – d).
But, d is relative prime to n – d too because all common dividers of d and n – d would divide d + n – d = n too. Thus, by the induction hypothesis, d divides m.
If n < d then d dividing m n can be looked as m n = c d that is n dividing c d.
So then the previous case d < n implies with exchanged roles, that n divides c.
But if c = q n then m n = c d = q n d → m = q d so indeed d divides m too.
Now we give a second amazing proof without U.P.F.T.
Observe that m n = c d is same as $\frac{n}{d} = \frac{c}{m}$. So the claim is merely the fact that a simple $\frac{n}{d}$ fraction can only be equal to $\frac{c}{m}$ if this is an expansion of $\frac{n}{d}$. Indeed, simple fractions are the ones where the n nominator and d denominator are relative primes.
In elementary school, the simplification was done by guessings or prime factorizations of the numerator and denominator. The assumptions that the prime factorizations are unique and thus, reveal all common factors and that we obtain a unique simple fraction were hidden.
Now we see that the claim of unique simplifications, itself implies the Fundamental Theorem of Relative Primes and thus the Fundamental Theorem of Primes too and the U.P.F.T.

The trick to see that the variants that is equal fractions are all expansions, is to regard something else than expansions and simplifications among them. Namely, minimality!

Indeed, if $\frac{n}{d} = \frac{n'}{d'}$ and $n < n'$, then also $d < d'$.

Thus, we can talk about "smaller" or "bigger" variants. So, there has to be a smallest minimal.
Now it's quite easy to show that all variants are multiples of this minimal!
There is a trick for this too, namely, looking at the difference of variants.

Easily, but surprisingly: $\frac{n}{d} = \frac{n'}{d'} \rightarrow \frac{n}{d} = \frac{n'-n}{d'-d}$ too.

Indeed: $n\,d' = d\,n'$ is the assumption and subtracting $n\,d = d\,n$ from it:
$n\,(d'-d) = d\,(n'-n)$ which is exactly the claim.
But this means with repeated subtractions, that the remainder variants are equal too.
So then if the minimal variant were not dividing an other, this would lead to a smaller remainder variant, contradicting the assumed minimality.

2.)

The repetition of the group, explaining the implication of 1.) also suggests that only the initial group should be examined. The trick to a proof is the exact opposite!
We will regard the seemingly obvious infinite sequence of remainders.
In the $r_m = [\,m\ n\,]$ infinite sequence we have three simple claims for new r_M remainders by an earlier r_m:

1. If $k\ r_m < d$ then there is $r_M = k\,r_m$. Namely, $M = k\,m$ will do, because:
   $r_{k\,m} = [k\ m\ n] = [k\ [m\ n]\,] = [k\ r_m\,] = k\ r_m$.

2. If $r_m > 0$ doesn't divide d, then there is $r_M > 0$, that $r_M < r_m$.
   Namely, let k be the first number that $k\ r_m > d$ and then, $M = k\,m$ will do.
   Indeed, $r_{k\,m} = [k\ m\ n] = [k\ r_m\,] = k\ r_m - d > 0$ by $k\ r_m > d$.
   And since $(k-1)\ r_m < d$ thus, $k\ r_m - d = r_{k\,m} < r_m$.

3. If $r_m > 0$ doesn't divide n, then there is $r_M > 0$, that $r_M < r_m$.
   Namely, let k be the first number that $k\ r_m > n$ and then, $M = k\,m - 1$ will do.
   Indeed, $r_{k\,m-1} = [(k\,m-1)\ n] = [k\ m\ n - n] = [k\ r_m - n] = k\ r_m - n > 0$ by $k\ r_m > n$
   And since $(k-1)\ r_m < n$ thus, $k\ r_m - n = r_{k\,m-1} < r_m$.

The 2 , 3 rules can be combined by saying:
If $r_m > 0$ doesn't divide both d and n then there is $r_M > 0$, that $r_M < r_m$.
Thus, the s smallest non zero remainder indeed must be a common divider of d and n.
Then by rule 1 , all multiples of s must appear as remainder too.

3.)

$r_m = [\,m\ n\,] = m\,n - c\,d$ so any common divider of d and n is dividing r_m too.
Thus the minimal s has this "super" property too, but it is a common divider too.
As we see 3.) became a trivial consequence of 2.)
But 3.) follows already from the U.P.F.T.
Indeed, by that, any factor of a number must contain the same prime factors as the number.
In fact, a factor means merely picking some prime factors with repetitions not exceeding the occurrences in the number's prime factorization either.
Common factors mean simply picking common prime factors with repetitions under the occurrences in either of the numbers.
The greatest common divider is simply all the common prime factors with highest occurrences from the two numbers. With the added case of being 1 if there are no common prime factors.
Thus the greatest common divider obviously "contains" all common ones.
We'll see soon that in reverse too, 3.) implies 1.)

R The crucial $\frac{n'-n}{d'-d}$ way to get a smaller fraction variant, could be regarded as an algorithm to find a common simplification of $\frac{n}{d}$ and $\frac{n'}{d'}$. Indeed:

After $\frac{n'-n}{d'-d} = \frac{n'-2n}{d'-2d} = \ldots = \frac{r}{s}$, we can do: $\frac{n-r}{d-s} = \frac{n-2r}{d-2s} = \ldots$ And so on!

Only regarding these new remainder fractions, we have decreasing variants and they can stop only if one "divides", that is simplification of the previous.
Then that will be simplification of all earliers and so of the original two fraction too.

For example, if we know $\frac{210}{252} = \frac{185}{222}$ then the remainder fractions are: $\frac{35}{30} = \frac{10}{12} = \frac{5}{6}$.

So $\frac{5}{6}$ is a common simplification of our original two equal fractions.

Here, this is the minimal too because it is already simple.
But this method doesn't guarantee the minimal.

From $\frac{210}{252} = \frac{180}{216}$ for example, the remainder fractions are the only $\frac{30}{36}$.

This is a common simplification but obviously not the minimal that is the simplest.

The biggest problem of course is that we needed two variants $\frac{n}{d} = \frac{n'}{d'}$ to start this process.

If only $\frac{n}{d}$ is given, then we are clueless to find a variant that is not expansion and thus will lead to $\frac{r}{s}$. It might even be that there is no such at all because $\frac{n}{d}$ is already the simple.

There is an algorithm that not only starts from $\frac{n}{d}$ but it will always tell the minimal variant

D **Euclidian Algorithm:**

The fundamental idea is that we again create "smaller" and "smaller" fractions in sense of numerators and denominators but now they won't even be variants that is equal. Instead they will all have the same possible simplifiers, that is common factors for the numerators and denominators. To keep the common factors and decrease the bigger of two numbers is easy! We simply have to subtract the smaller from the bigger. The difference must contain all common dividers.
So we regard the bigger of n, d say n and then simply subtract the other from it. So instead of $\frac{n}{d}$ we take $\frac{n-d}{d}$. Repeating this, will give the $\frac{n-2d}{d}$, . . , $\frac{n-kd}{d} = \frac{r}{d}$ sequence.

Then we switch roles, that is start to subtract r from d. This ends with an $\frac{r}{s}$.

Then again we switch roles and so on. Here again we can regard only the remainder fractions.
We stop when the numerator divides the denominator or vice versa.
Indeed, then the next remainder fraction would have to contain a zero.
The last remainder fraction will contain the perfect simplifier of the original fraction.
Namely as the smaller of its numerator or denominator.
If it is 1 then there is no simplification, the original was already simple.

For example, at $\frac{210}{252}$ the remainder fractions are the single $\frac{210}{42}$ because 42 divides 210.

Both fractions contain the same common dividers of the numerators and denominators, and so this 42 contains them too. But also, it divides the 210 too and thus divides all earlier numerators and denominators. So in fact 42 is the super common divider of 210 and 252.
So as a side result, this process proves again that all greatest common dividers are super.

But back to the simplification: $\frac{210}{42} = 5$ and $\frac{252}{42} = 6$ so, $\frac{210}{252} = \frac{5}{6}$.

Now lets try $\frac{65}{38}$. The remainder fractions are : $\frac{27}{38}$, $\frac{27}{11}$, $\frac{5}{11}$, $\frac{5}{1}$

So, $\frac{65}{38}$ can not be simplified.

An even more practical version of this Euclidian algorithm is done by using "mixed numbers" to calculate the remainders. Then of course we have to turn the fractional parts upside down:

$$\frac{210}{252} \rightarrow \frac{252}{210} = 1\frac{42}{210} \rightarrow \frac{210}{42} = 5$$

42 is the last denominator and thus the super common factor.

$$\frac{65}{38} = 1\frac{27}{38} \rightarrow \frac{38}{27} = 1\frac{11}{27} \rightarrow \frac{27}{11} = 2\frac{5}{11} \rightarrow \frac{11}{5} = 2\frac{1}{5} \rightarrow \frac{5}{1} = 5$$

1 is the last denominator and thus there is no common factor.

T The Euclidian Algorithm implies that all equal fractions have common simplification.
Thus it also implies the fundamental theorems of relative primes, primes and U.P.F.T.

P As we saw, the Euclidian Algorithm implies that the greatest simplifier of a fraction is super.
So, the smallest simplification is a simplification of all others. Thus enough to show that any two equal fractions have a common expansion because then the minimal simplification of that is a common simplification of them. For $\frac{n}{d} = \frac{n'}{d'}$ a common expansion is $\frac{n\,n'\,d'}{d\,n'\,d'}$.

Indeed, it's trivially an expansion of $\frac{n}{d}$, but also of $\frac{n'}{d'}$ because $n\,d' = d\,n'$.

There is an even more direct way to see that the Euclidian Algorithm implies common simplification for equal fractions, namely from this most practical last mixed number version:
The last denominator not only is the s super simplifier of the original fraction, but this s and the sequence of the whole parts determine the original fraction backwards.

For example above the last fraction $\frac{5}{1}$ is determined directly by s = 1 and the last whole 5.

Then the previous fraction $\frac{11}{5}$ is determined by obviously having the same denominator as the last numerator 5 and having 2 times this plus the last denominator 1 that is 11.

What's more, this determination from s and the whole parts, stays a product of s and some number determined by the whole parts. Thus the original numerator and denominator are also merely a product of s and some numbers determined by the whole parts.

But two equal fractions determine Euclidian Algorithms with same whole parts. So the two fractions have the same multipliers in their numerators and denominators.

Simplifying both with their own s , we must get the same simplified fractions.

2. Infinity of primes Prime functions

R The Unique Prime Factorization, is the reason why primes are so important.
Yet it doesn't reveal anything about the primes themselves. Indeed, not only it doesn't tell how the primes are among the composite numbers, but it doesn't even tell whether there are infinite many primes at all. Most amazingly, already Euclid was aware of this question and gave a rigorous proof for the infinity. Up to chapter 12, we collected the exact rules about primes, while those that only tell how they behave statistically, will be dealt in chapter 11-16. This at once reveals that the primes are a kind of mystery, a sequence of numbers with very simple definition and yet without any apparent pattern. We can always tell, what the next prime will be, namely the first number that is not dividable by any smaller except 1. The problem is that this simple rule doesn't tell anything about how soon if ever such number will pop up. And indeed they pop up quite irregularly. But the full depth of this mystery can be best understood if primes are compared with the relative primes. For these we had the "Junior Algorithm". Even though this algorithm is less than an explicit formula, it is still much more than what we have for primes which is basically nothing. In other words the only way to decide if a number is prime is by trying out all possible numbers as factors. Of course, here the word "possible" is the crucial fine print. The most obvious restriction is that a factor must be smaller than the number, in fact it must be smaller than its half. But for large numbers these obvious restrictions still leave too many numbers to be tried. Still, eliminating all multiples of smaller numbers is a very visual way to "find" the primes and appropriately it is called "sieving".

D k is n-sieved if it's a number up to n or a multiple of such. That is: $k = m\,j$ with $j \le n$
k is n-unsieved if it is not n-sieved. For example:
4-sieved numbers: $1, 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 24, 26, \ldots$
4-unsieved numbers: $5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, \ldots$

T 1.) Multiple of an n-sieved is also n-sieved.
2.) All primes bigger than n are n-unsieved.

D Let n_* denote the last prime up to n meaning n if it is prime.
Then $n\# := 2\cdot3\cdot5\cdot7\cdot11\cdot\ldots\cdot n_* =$ prime factorial of n.
The name refers to the $n! = 2\cdot3\cdot4\cdot\ldots\cdot n =$ factorial

T $n! + 1$, $n\# + 1$, $n! - 1$, $n\# - 1$
1.) are not dividable by any number from 2 to n
2.) are n-unsieved
3.) have only prime factors bigger than n.

P 1.)
$n! + 1$ has 1 remainder to $2, 3, 4, \ldots, n$ all.
$n\# + 1$ has 1 remainder to $2, 3, 5, \ldots, n_*$ all. But any number up to n is dividable by at least one of these, so $n\# + 1$ is not dividable by any number up to n either.
$n! - 1$ has 1 remainder to 2 since $(n! - 1) - 1 = n! - 2$ dividable by 2
2 remainder to 3 since $(n! - 1) - 2 = n! - 3$ dividable by 3
.
$(n - 1)$ remainder to n since $(n! - 1) - (n - 1) = n! - n$ dividable by $n - 1$

D By 2.) of previous theorem, for every n number there is n-unsieved , so it's meaningful that:
n^* := smallest n-unsieved number.

T

1.) n^* is prime.

2.) n^* is the first prime after n

P

1.) If $n^* = m\,a$ were with $m, a > 1$ then
if one of m, a were n-sieved then so would be n^* contradicting that it's n-unsieved,
if one of m, a were not n-sieved then it would contradict that n^* is the smallest.

2.) If a p prime were between n and n^* then p were a smaller than n^* n-unsieved number contradicting that n^* is the smallest.

R

Thus n* could also be defined as the first prime after n.
Unfortunately this theorem didn't give any information, how soon n^* comes after n.
The following theorems target this question:

T

If $p_1 = 2, p_2 = 3, \ldots p_n$ are the first n primes then there is a new prime before or at:

1.) Euclid: $p_1\ p_2 \ldots p_n - 1$

2.) Thue: $2^{n^2} - 1$ if $n \geq 2$

3.) Erdös: $4^n + 1$

P

1.) $p_1\ p_2 \ldots p_n - 1$ is not dividable by any of $p_1, p_2, \ldots p_n$.

2.)

For $n = 2, 3, 4$ we can see by checking it. For example $2^{2^2} - 1 = 2^4 - 1 = 15$ and between 3 and 15 there are many primes.
If $n \geq 5$ then $2^n > n^2$ because $2^5 = 32 > 5^2 = 25$ and if it's true for n then:
$2^{n+1} = 2^n \cdot 2 > n^2 \cdot 2 = n^2 + n\,n > n^2 + 3n > n^2 + 2n + 1 = (n+1)^2$
Thus of course $\left(2^n\right)^n = 2^{n^2} > \left(n^2\right)^n = n^{2n}$ too.
Now suppose that up to $2^{n^2} - 1$ there were no new primes!
Then all the $1, 2, 3, \ldots, 2^{n^2} - 1$ numbers could be written as $2^{e_1} \cdot 3^{e_2} \ldots p_n{}^{e_n}$.
Where e_1 can vary from 0 to $n^2 - 1$, e_2 can vary from 0 to less, e_3 up to even less, and so on. So if we assign to all of these exponents the same $0, 1, 2, \ldots, n^2 - 1$ possibilities, we get much more forms than we need to cover all numbers.
Since every exponent is assigned n^2 many values and there are n exponents, this gives $\left(n^2\right)^n = n^{2n}$ many forms.
Thus $n^{2n} > 2^{n^2} - 1$ so $n^{2n} \geq 2^{n^2}$ contradicting what we proved for $n > 5$.

3.)

First lets see that every N number can be written as $a^2\ 2^{b_1} \ldots p_k{}^{b_k}$ with $p_1, \ldots p_k$ being the primes up to N and $b_1, \ldots b_k$ all being 0, 1. Indeed all we have to do is regard a prime factorization of N as $2^{e_1} \ldots p_k{}^{e_k}$ and then a^2 is the product of prime powers with the largest even parts of the e exponents. The remaining 0, 1 exponents will be the b-s.
Now suppose that $p_1, p_2 \ldots p_n$ were all the primes up to $4^n + 1$.
Then all these numbers could be written as $a^2\ 2^{b_1} \ldots p_k{}^{b_k}$ with:
$a \leq \left[\ \sqrt{4^n + 1}\ \right] = 2^n$ and $b_1, \ldots b_n = 0, 1$.
This means $2^n\ 2^n = 4^n$ possibilities and thus couldn't cover $4^n + 1$ many values.

T Let $m\big|^n$ denote a "1-altered power" or in short "1-power" as $(m-1)^n + 1$. Then:

1.) If $m \geq 3$, $n \geq 2$ then $m\big|^n > m$

2.) If m is odd then $m\big|^n$ is also

3.) If $m \geq 3$ is odd and $n \geq 2$ is even, then in the $m\big|^n$, $\left(m\big|^n\right)\big|^n$, $\left(\left(m\big|^n\right)\big|^n\right)\big|^n$ . . . sequence none of the numbers has a non 1 divider that divides any of the previous members.

P 1.) $(m-1)^n + 1 > (m-1)^2 > m^2 - 2m = m^2 - 3m + m = m(m-3) + m \geq m\,0 + m = m$

2.) $(m-1)$ is even so $(m-1)^n$ is too, thus $(m-1)^n + 1$ is odd.

3.) $\left(\ldots\left(\left(m\big|^n\right)\big|^n\ldots\right)\big|^n = (m-1)^{n^k} + 1$ (on the left k many 1-powers are) Then:

$$\frac{\left[(m-1)^{n^K}+1\right]-2}{(m-1)^{n^k}+1} = \frac{(m-1)^{n^K}-1}{(m-1)^{n^k}+1} = \frac{\left[(m-1)^{n^k}\right]^{n^{K-k}}-1}{(m-1)^{n^k}+1} = \frac{a^N-1}{a+1} = a^{N-1} - a^{N-2} + \ldots - 1$$

Which is a whole number so every divider of the k-step 1-power divides the K-step – 2.
Then of course the only common dividers of the k-step and the K-step 1-powers can be 1 and 2. But because m is odd, 2 can't be a divider by 2.)

T There are infinite many primes.

P All the three theorems before the last one imply it directly.
Polya used an argument by the last theorem:
Indeed the infinite sequence of 1-powers must have newer and newer prime dividers.
The simplest such sequence is of course with $m = 3$, $n = 2$.

$(3-1)^2 + 1 = 2^2 + 1 = 5$

$(5-1)^2 + 1 = 2^4 + 1 = 17$

$(17-1)^2 + 1 = 2^8 + 1 = 257$

.
.

These will be later called as Mersenne twins or Fermat numbers.

D $p_n :=$ n-th prime $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, . . .

$d_n := p_{n+1} - p_n =$ n-th prime difference $d_1 = 1$, $d_2 = 2$, $d_3 = 2$, $d_4 = 4$, . . .

For $n > 1$

$\pi(n) :=$ prime counter = number of primes up to n including n if it is prime.

$\delta(n) := n^* - n_* =$ around-n prime difference $\delta(2) = 2^* - 2_* = 3 - 2 = 1$

$\delta(3) = 3^* - 3_* = 5 - 3 = 2$

$\delta(4) = 4^* - 4_* = 5 - 3 = 2$

For p_n and d_n we used index variables because $p(n)$ and $d(n)$ are used for the partitioning and divider number functions.

T

Trivial relations

1.) $\pi(p_n) = n \qquad \delta(p_n) = d_n \qquad p_{\pi(n)} = n_* \qquad d_{\pi(n)} = \delta(n)$

2.) d_n and $\delta(n)$ have the same values only at different n-s namely: $\delta(n) < d_n$
All d_n and $\delta(n)$ values are even except $d_1 = \delta(2) = 1$

3.) $\pi(n) \underset{3}{<} n_* \leq n < n^* \underset{4}{<} p_n \;,\; d_n < p_n \;,\; \delta(n) < n^*$
The question where d_n and $\delta(n)$ fit into the first line of inequalities apart from the obvious second and third, is the most important problems of primes.

R

Neither of $n! + 1$, $n\# + 1$, $n! - 1$, $n\# - 1$ has to be prime but they are many times.
Whether there are infinite many such primes or non primes or simultaneously, are hard questions. This raises the more general question:
Are there infinite many primes at all with 2 difference?
In other words, are there infinite many n that: $n_* = n - 1$, $n^* = n + 1$

Such primes are called twin primes. The Twin Prime Conjecture is that there are infinite many of them.
Though it is only believed to be true, it has already been proven that the reciprocal sum of twin primes is finite. So they are very rare among all primes. In the next section we'll see that they are still not as rare as we would imagine.

3. Twin composite blocks Infinity of gaps, gap conjectures

T

d_n and $\delta(n)$ take up arbitrary big values.

P

Blocks of consecutive composite numbers are between two consecutive primes, so it's enough to show that there are arbitrary long such blocks. Actually we show that there are two arbitrary long such blocks almost right after each other, namely with only three numbers separating them.
Lets regard the n numbers before and after n **!**:

$$\underbrace{(n!-n),(n!-n+1),\ldots(n!-2),(n!-1)}_{\text{all composites, } (n-1) \text{ long block}},\ \underbrace{n!}_{\text{composite}},\ \underbrace{(n!+1),(n!+2),\ldots(n!+n-1),(n!+n)}_{\text{all composites, } (n-1) \text{ long block}}$$

may be primes

Indeed: $n! \pm 2$ are dividable by 2.
$n! \pm 3$ are dividable by 3.
.
.
$n! \pm n$ are dividable by n.
Similarly we can see that using n # instead of n **!** we also get the same composite blocks.

R

As we said $n! \pm 1$ and $n\# \pm 1$ can be prime or composite. If $\pm$ are both composite then the above two composite blocks melt into one big 2n + 1 long block. This might seem very long but compared to n **!** or even to the smaller n # , it is not that long. In fact we always find blocks of composites with such 2n + 1 length much before n # . For example for n = 10, the first 21 long block is between $p_{189} = 1129$ and $p_{190} = 1151$. The $d_{189} = 1151 - 1129 = 22$ prime difference is of course 1 more than the gap or block. These primes are much smaller than $10! = 3628800$. The $10\# = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ only, but 209 and 211 are primes so we only have 10 long blocks and such length already appears earlier. But lets forget now for a second how <u>fast</u> the prime difference increases and instead look at how <u>jumpy</u> the increase is:
By the Twin Prime Conjecture its obvious that d_n always falls back to smaller values.
It seems that infinite many times the new highest values of d_n are not the next even numbers but bigger ones. Therefore since it also seems that all even values are taken up sooner or later, d_n has to fall back to values that haven't been taken before.
The following table shows two outbursts of d_n right after each other.

n where d_n gets new height	$d_n = p_{n+1} - p_n$	$\pi(n)$
2	$2 = 5 - 3$	1
4	$4 = 11 - 7$	2
9	$6 = 29 - 23$	4
24	$8 = 97 - 89$	9
30	$14 = 127 - 113$	10
99	$18 = 541 - 523$	25

By the way after $n = 30$, d_n goes back to $4, 6, 2, 10, 2, 6, 6$ but $\pi(n)$ slowly but surely by $n = 37$ reaches 12 and then at $n = 41, 43$ grows to 14. Then d_n goes up to 14 only twice more at $n = 72$ and 76 . Amazingly the value 16 first will be taken at $d_{282} = p_{283} - p_{282} = 1847 - 1831 = 16$. As we see after n = 31 , d_n never jumps above $\pi(n)$, that is: $d_n \underset{31}{<} \pi(n)$

The mentioned assumption that all even values are eventually taken up by d_n is called the Generalized Twin Primes or Polignac Conjecture. Just how far we are from proving this, is shown by that neither of the following two statements concerning differences between any two, not necessarily consecutive primes, are proved yet:

1.) For all k there are p , q primes so that $p - q = 2k$.

2.) There is a k so that are infinite many p , q pairs of primes with $p - q = 2k$.

A much weaker theorem about consecutive differences can be proved by a limit assumption that we explain in the followings:

We already proved that the $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots .$ sum of prime reciprocals is infinite.

On the other hand the $\frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots .$ sum of square reciprocals is finite, in fact its less than 1, namely as we mentioned already it is $\frac{\pi^2}{6} - 1$. It has been proved by Brun that the sum of reciprocals of the twin primes is again finite. The finite or infiniteness of reciprocal sums clearly indicate how frequent certain numbers are in the long run. So for example there are much more primes than squares. We might even think that if two reciprocal sums are both finite then the actual sum value is an indication of which sequence of numbers is more frequent among the naturals. But this is wrong because if a sequence is more frequent at low values then it still might give a much bigger sum even if it becomes very rare later. In fact we showed this to happen between the square and factorial reciprocal sums. In spite of this cautious remark it seems that in case of the squares versus the twin primes, the reciprocal sums are unreliable quite the opposite way. Indeed, though the twin primes give only a little bit more as reciprocal sum, they are much more frequent as sequence. In details:

$$\frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots . = \frac{\pi^2}{6} - 1 = .645$$

$$\left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \ldots . = 1.901$$

In this famous Brun sum every pair of twin primes is appearing with both members, so if we halve 1.901 we get hardly more than .645. Yet, just look at the following table that for the powers of 10 compares their square root, that is the number of squares up to them, with π_2, the number of twin primes up to them:

n	$\sqrt{n}$	$\pi_2(n)$	ratio
10^2	10	8	.8
10^4	100	205	2
10^6	1000	8,169	8
10^8	10,000	440,312	44
10^{10}	100,000	27,412,679	274

The tendency is clear: $\frac{\pi_2(n)}{\sqrt{n}} \to \infty$. Then of course the much bigger $\pi(n)$ should even more obey $\frac{\pi(n)}{\sqrt{n}} \to \infty$. Putting p_n into n : $\frac{n}{\sqrt{p_n}} \to \infty$ and squaring: $\frac{n^2}{p_n} \to \infty$ should be even more and for the reciprocal: $\frac{p_n}{n^2} \to 0$.

This last limit seems to be so obvious that it is quite unbelievable how difficult it is to prove it. Even more amazingly we'll prove quite easily, that $\frac{p_n}{n} \to \infty$ which shows that $\frac{p_n}{n^2} \to 0$ can't be that obvious after all. Anyway, we use this now to show:

T

Among the $d_1, d_2, \ldots$ prime differences, arbitrary high repetition of a value must occur.

P

Since $d_1 = 1$ only appears once, enough to look at the rest.

Let the maximal repetition of a value among $d_2, d_3, \ldots d_{n+1}$ be m.

Then $p_{n+2} - 3 = \underbrace{(5-3)}_{d_2=2} + \underbrace{(7-5)}_{d_3=2} + \underbrace{(11-7)}_{d_4=4} + \ldots + \underbrace{(p_{n+2} - p_{n+1})}_{d_{n+1}=?}$

We have n many d_k values and every one appears at most m times, so we have at least $\left[\frac{n}{m}\right] = n/m$ many different values. Here square bracket is the conventional and slash fraction line is our present abbreviation for the whole value or integer part of a fraction. Taking only the different d_k values, we clearly decrease their sum and regarding these as the smallest possible, that is as the first n/m even numbers, we decrease again, so:

$$p_{n+2} - 3 > 2 + 4 + \ldots + n/m \cdot 2 = 2\left(1 + 2 + \ldots + n/m\right) = 2 \cdot \frac{n/m\,(n/m + 1)}{2} = (n/m)^2 + n/m =$$

$$(n/m - r)^2 + (n/m - r) = \frac{n^2}{m^2} + \frac{n}{m}(1 - 2r) + r^2 - r > \frac{n^2}{m^2} - \frac{n}{m} - 1$$

So:
$$\underset{\downarrow\ 0}{\frac{p_{n+2}}{(n+2)^2}} > \underset{\downarrow\ 1}{\frac{n^2}{m^2(n+2)^2}} - \underset{\downarrow\ 0}{\frac{n}{m(n+2)^2}} + \underset{\downarrow\ 0}{\frac{2}{(n+2)^2}}$$

if there is an M > m

This is a contradiction so an M bound for m is impossible.

4. Factorials

T

If $n > 1$ and $[\ ]$ denotes the whole part, then:

1.) If n is prime then $(n-1)!$ is not dividable by n.

2.) If n is composite and > 9 then $\left[\frac{n}{2}\right]!$ is dividable by n.

3.) n is composite if and only if $\left[\frac{n}{2}\right]!$ is dividable by n or $n = 4$ or 9.

4.) n is prime if and only if $\left[\frac{n}{2}\right]!$ is not dividable by n and $n \neq 4, 9$

P

1.) A prime can only divide a product if it divides a member of it but $2 \cdot 3 \cdot 4 \ldots (n-1)$ has only members smaller than n.

2.) Let $n = a\,b$ with $2 \le a \le b$. Then $b = \frac{n}{a} \le \frac{n}{2}$ so $[b] = b \le \left[\frac{n}{2}\right]$.

If $a < b$ then both a , b appear in $\left[\frac{n}{2}\right]!$ as members. If $a = b$ then:

$n = a^2 > 9 \quad \rightarrow$

$n \ge 16 \quad \rightarrow \quad \sqrt{n} \ge 4 \quad \rightarrow \quad n \ge 4\sqrt{n} \quad \rightarrow \quad \frac{n}{2} \ge 2\sqrt{n} = 2a$

so $[2a] = 2a \le \left[\frac{n}{2}\right]$ too and thus a and $2a$ both appear as members in $\left[\frac{n}{2}\right]!$

3.) $n \ge 2 \quad \rightarrow \quad \frac{n}{2} \ge 1 \quad \rightarrow \quad n \ge \frac{n}{2} + 1 \quad \rightarrow \quad n - 1 \ge \frac{n}{2} \ge \left[\frac{n}{2}\right]$

So $(n-1)!$ includes $\left[\frac{n}{2}\right]!$ and thus by 1.) if n is prime then $\left[\frac{n}{2}\right]!$ is not dividable by n. So we only have to check the composites up to 9. These are 4, 6 , 8 , 9.
6 and 8 satisfy the condition, but 4 and 9 not so only these had to be mentioned.

4.) Same as 3.) in opposite form.

T

Wilson

1.) If $p > 2$ is prime then $(p-2)! - 1$ is dividable by p.

2.) If $p = 4k \pm 1$ is prime then $\left(\frac{p-1}{2}!\right)^2 \pm 1$ is dividable by p.

3.) $(p-1)! + 1$ is dividable by p for all p primes.

4.) There are infinite many n where $n! - 1$ is composite.
There are infinite many n where $n! + 1$ is composite.

P

1.)

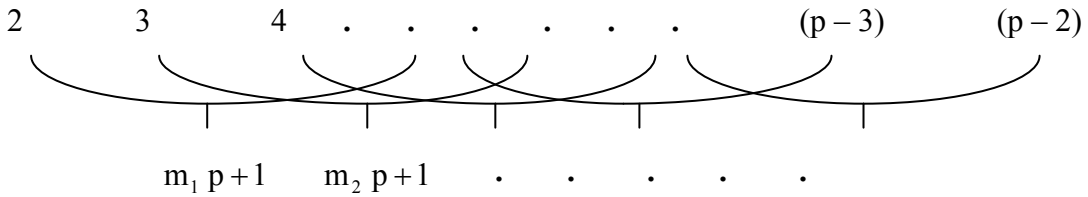
The products $2 \cdot 1$, $2 \cdot 2$, $2 \cdot 3$, . . . $2(p-1)$ all give different nonzero remainders to p. Indeed p can't divide any of them because it can't divide neither of the two factors. If two members gave the same remainders then their difference which is in the list, would be dividable by p. Since we listed $p - 1$ products, thus every possible 1 , 2 , . . . $p - 1$ remainder must be obtainable. In this proof we only look for the 1 remainder, so lets find in our list the 2 k member that gives 1 remainder and then to remember this lets connect 2 with k in the list of possible remainders:

1 , 2 , 3 , 4 , 5 , . . . k , . . . $(p-2)$, $(p-1)$

By the way, k must be $\frac{p+1}{2}$ because $2 \cdot \frac{p+1}{2} = p + 1$ indeed has 1 remainder to p and as we said there is only one.
Lets do the same list for 3 that is: $3 \cdot 1$, $3 \cdot 2$, $3 \cdot 3$, . . . $3 (p - 1)$.

We might even jump to say that in the list of remainders 3 should be connected to $\frac{p+1}{3}$.

Indeed $3 \cdot \frac{p+1}{3} = p + 1$ would give 1 remainder, but $p + 1$ is not necessarily dividable by 3. Of course there will be one that pairs up with 3 but we don't know exactly which one for any p. The same way we go through all numbers multiplied into a list and finding the pairs and connect them. We don't have to make list for numbers that were already connected because they would just give again the same pair. It's also clear that 1 and $(p - 1)$ will remain unconnected because $1 \cdot 1 = 1$ and $(p - 1)(p - 1) = p^2 - 2p + 1$ so these only give 1 remainder when multiplied with themselves. This raises the question whether any other k could give 1 remainder multiplied by itself and thus we couldn't connect it to another number. But this can't happen because k^2 having 1 remainder to p means: $k^2 - 1 = (k - 1)(k + 1) = mp$ so p must divide $k - 1$ or $k + 1$ which is only possible as $k-1 = 0$ or $k+1 = p$, giving the already mentioned 1 and $p - 1$ cases.
So the 2 , 3 , . . . $p - 2$ numbers will be nicely paired giving products $mp + 1$:



Thus $(p - 2)! = (m_1 p + 1)(m_2 p + 1) \ldots = M p + 1$ because if we carry out the multiplications then every term has p factor except when all the 1-s are multiplied.

2.)

$$(p-2)! = 2 \cdot 3 \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \ldots (p-2) = 2 \cdot 3 \ldots \frac{p-1}{2} \cdot (p-2) \ldots \left(p - \frac{p-1}{2}\right) =$$

$$2 \cdot 3 \ldots \frac{p-1}{2}\left[mp + (-1)^{\left(\frac{p-1}{2}-1\right)} \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right] = Np + (-1)^{\left(\frac{p-1}{2}-1\right)} \left(\frac{p-1}{2}!\right)^2 = Mp + 1$$

If $p = 4k + 1$ then $\frac{p-1}{2} - 1 = 2k - 1 =$ odd so:

$$-\left(\frac{p-1}{2}!\right)^2 = Mp + 1 - Np \quad \text{from which} \quad \left(\frac{p-1}{2}!\right)^2 + 1 = (N - M)p$$

If $p = 4k - 1$ then $\frac{p-1}{2} - 1 = 2k - 2 =$ even so:

$$\left(\frac{p-1}{2}!\right)^2 = Mp + 1 - Np \quad \text{from which} \quad \left(\frac{p-1}{2}!\right)^2 - 1 = (M - N)p$$

3.)
If $p > 2$ then by 1.) $(p - 2)! - 1$ so also $(p - 1)[(p - 2)! - 1] = (p - 1)! - p + 1$ so also $(p - 1)! + 1$ is dividable by p. For $p = 2$ we can check that $1 + 1 = 2$ is dividable by 2.

4.)
For $n = p - 2$ and $n = p - 1$ with p primes we get such numbers from 1.) and 3.)

T Prime criterias by Wilson

1.) $n > 2$ is prime if and only if $(n-2)! - 1$ is dividable by n.

2.) An odd $n > 2$ is prime if and only if one of $\left(\frac{n-1}{2}!\right)^2 \pm 1$ is dividable by n.

P 1.) If n is composite then $n \geq 4 \rightarrow 2n - 4 \geq n \rightarrow n - 2 \geq \frac{n}{2} \geq \left[\frac{n}{2}\right]$.

So by 3.) of our first theorem if n is composite but not 4 or 9 then automatically $(n-2)!$ is dividable by n and thus $(n-2)! - 1$ can't be.
For $n = 4$ or 9 :

$(4-2)! - 1 = 1$ and $(9-2)! - 1 = 5039$ is not dividable by 9.

2.) If n is odd then $\frac{n-1}{2} = \left[\frac{n}{2}\right]$ so again by 3.) of our first theorem if n is composite but not 9 then $\frac{n-1}{2}!$ is dividable by n and thus neither of $\left(\frac{n-1}{2}!\right)^2 \pm 1$ can be.

For $n = 9$:

$\left(\frac{9-1}{2}!\right)^2 \pm 1 =$ 577 and it is not dividable by 9 / 575 and it is not dividable by 9

R The above prime criterias are not practical. It's true that we don't have to do divisions but instead we have to use a huge number of multiplications. Even if we don't use the full numbers only the remainders, it is still too complicated.

5. Simple Square Sums, Splitting of Primes

T

1.) If n has 3 as remainder to 4 then it is not a square or square sum.

2.) If n has two forms as square or square sum, then it is composite.

P

1.) If a is even then a^2 has 0 remainder to 4 since $(2k)^2 = 4k^2$.
If a is odd then a^2 has 1 remainder to 4 since $(2k+1)^2 = 4k^2 + 4k + 1$
So, a square can't have 3 remainder to 4.
If a , b are both even then $a^2 + b^2$ has 0 remainder to 4.
If one of a , b is even and the other odd then $a^2 + b^2$ has 1 remainder to 4.
If a , b are both odd then $a^2 + b^2$ has 2 remainder to 4.
Thus $a^2 + b^2$ has never 3 remainder to 4 either.

2.) n clearly can't be 2 because its only form is 1 + 1. All evens are composite, so it's enough to show our claim for odd n. Then clearly the squares in the sum must be different. Thus:

$n = A^2 + a^2 = B^2 + b^2$ with $A > a \geq 0$ and $B > b \geq 0$ Then: $n\,[A^2 - a^2 + B^2 - b^2] =$

$n\,(A^2 - a^2) + n\,(B^2 - b^2) = (B^2 + b^2)(A^2 - a^2) + (A^2 + a^2)(B^2 - b^2) =$

$2(A^2 B^2 - a^2 b^2) = 2(A B - a b)(A B + a b)$ and lets observe that:

$$A B - a b < A B + a b = \frac{A^2 + B^2 - (A - B)^2}{2} + \frac{a^2 + b^2 - (a - b)^2}{2} < \frac{A^2 + a^2 + B^2 + b^2}{2} = n$$

So n [ ] = 2 ( ) ( ) with both ( ) factors < n.
A prime can't divide a product of smaller numbers, so n is composite.

R

Such composites do exist. For example:
$25 = 5^2 = 3^2 + 4^2$, $65 = 1^2 + 8^2 = 4^2 + 7^2$, $85 = 2^2 + 9^2 = 6^2 + 7^2$

D

If an $a^2 + b^2$ square sum is multiplied by a c^2, then it is again a square sum, because
$(a^2 + b^2)\,c^2 = a^2 c^2 + b^2 c^2 = (a c)^2 + (b c)^2 = A^2 + B^2$.
In reverse, if $A^2 + B^2$ can be written as $(a^2 + b^2)\,c^2$, then we say that it is simplified by bringing out c^2. If A , B have no common divider, except 1, that is A , B are relative primes, then $A^2 + B^2$ can not be simplified, so it is a simple square sum form.
An n number is simple square sum if it has a simple square sum form.
A non simple square sum form might give a value that is simple square sum.
For example: $5^2 + 5^2 = 50 = 1^2 + 7^2$

T

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 $A^2 + B^2 = p_1\ p_2 \cdot \cdot \cdot p_k$
then all these p_i prime factors are square sums.
Indeed, this already implies that they are simple because they are primes.

P

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 both 1, they can not be equal and thus we may assume that $A < B$. So: $p_{k-1}^2 \le p_{k-1}\, p_k \le p_1\, p_2 \ldots p_k = A^2 + B^2 < 2\, B^2$.
The two ends imply that $p^2 < 2\, B^2$ 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 $p_1, \ldots, p_{k-1}$ 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 $p = a^2 + b^2$.

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

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

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.

T Simple Square Sum Condition:
A number is a simple square sum, if and only if:
Every prime factor of it is square sum and has no more than one 2 factor. Consequence:
Generalized Simple Square Sum Theorem:
All factors of a simple square sum are also simple square sums.

P By previous theorem, we only have to show that:

1.) Multiplying a simple square sum with an odd square sum prime, gives a simple square sum
2.) An a^2+b^2 simple square sum is not dividable by 4.

1.) Let the simple square sum be $A^2 + B^2$ and the odd square sum prime $a^2 + b^2$.
Here $A^2 = B^2$ is possible for the only $1^2 + 1^2 = 2$ simple square sum,
but $a^2 = b^2$ is impossible, because $a^2 + b^2$ is assumed to be odd.

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

can be verified by squaring the sums.
We claim that at least one of these forms "works" that is, give non zero and relative prime members. Firstly, if both minus sums were zero then $B\,a = A\,b$ and $A\,a = B\,b$ would imply $a\,(B - A) = b\,(A - B)$, thus, $a = -b$ and thus, $a^2 = b^2$, contradicting that $a^2 + b^2$ is odd. Secondly, if both forms gave non relative primes then a common factor of the first two, were factor of any of their linear combinations, for example:
$a\left(A\,a + B\,b\right) + b\left(A\,b - B\,a\right) = A\left(a^2 + b^2\right)$ and $b\left(A\,a + B\,b\right) - a\left(A\,b - B\,a\right) = B\left(a^2 + b^2\right)$.
Similarly, a common factor of the second two were factor of:
$a\left(A\,a - B\,b\right) + b\left(A\,b + B\,a\right) = A\left(a^2 + b^2\right)$ and $a\left(A\,b + B\,a\right) - b\left(A\,a - B\,b\right) = B\left(a^2 + b^2\right)$.
Then of course, this common factor in both case can only be $a^2 + b^2$. Since it's a prime and A , B are relative primes. But then $a^2 + b^2$ would divide any linear combinations of the four sums: $\left(A\,a + B\,b\right)$, $\left(A\,b - B\,a\right)$, $\left(A\,a - B\,b\right)$, $\left(A\,b + B\,a\right)$. The first plus third gives 2 A a, the fourth minus the second gives 2 B a. So these contradict A , B to be relative primes.

2.) First of all, a , b can't be both even by simplicity.
If one is odd and the other even, then a^2+b^2 is odd.
Finally, if they are both odd, then:
$a^2 + b^2 = \left(2m+1\right)^2 + \left(2n+1\right)^2 = 4m^2 + 4m + 1 + 4n^2 + 4n + 1 = 4k + 2$

T Every $4\,k + 1$ prime is divider of an $n^2 + 1$.

P By Wilson 2.) $n = (2\,k)\,!$ works. Examples:
$k = 1 \rightarrow 4\,k + 1 = 5$ is prime, $(2\,k)\,! = 2$ and indeed, $2^2 + 1 = 5$ dividable by 5.
$k = 3 \rightarrow 4\,k + 1 = 13$ is prime, $(2\,k)\,! = 720$ and, $720^2 + 1 = 518401$ dividable by 13.
$k = 4 \rightarrow 4\,k + 1 = 17$ is prime, $(2\,k)\,! = 40320$ and, $40320^2 + 1 = 1625702401$ div. by 17.
Of course, much earlier $n^2 + 1$ can work. Above for 13, the first is 26 and for 17, itself.

T 1.) $4\,k + 1$ primes are unique square sums.
2.) $4\,k + 3$ primes are never square sums.

P

1.) The square sumness follows from Simple Square Sum Theorem and the previous one, because $n^2 + 1$ is simple square sum.
The uniqueness follows from first theorem 2.).

2.) Special case of first theorem 1.).

R

All odd primes are $4k + 1$ or $4k + 3$, so the previous theorem is indeed, the splitting of the primes, by the amazingly coinciding conditions of remainders to 4 and being square sums or not. The only prime left out is 2, which is a square sum, but not $4k + 1$.
This theorem is a gem of number theory, in the sense that it's meaning is very simple, yet its proof is very difficult. Anybody can understand what primes are in a few minutes, and then see how they fall into the obvious $4k + 1$ or $4k + 3$ cases, seemingly quite randomly. Then, showing that one is always a square sum, what's more uniquely, while the other is never, is quite a surprise. Our natural feeling is that something inherent in the primeness and remainders to 4, that makes this situation true, yet those inner conditions can not give a proof. We have to go outside, and investigate wider circumstances. The crucial question is how far we should go out to wider conditions. A formalist would say, as little as possible, namely just enough to get a proof.
Above, I went a bit further, because I proved the Simple Square Sum Theorem, even though the $4k + 1$ primes are factors of the special $n^2 + 1$ simple square sums. So, it would have been enough to prove that all prime factors of $n^2 + 1$ are square sums. And indeed, we could have gained a tiny bit shorter proofs for that. A few years ago, before I launched my attack against formalism within Mathematical Logic, I had finished my book on primes and had a few such proofs. I will present them in the remaining of this chapter, even though I find them appalling today. In fact, I changed this book, not only to prove the Simple Square Sum Theorem, but right after, I showed the full conditions of being simple square sum, having as trivial consequence the Generalized Simple Square Sum Theorem. This shows that there must be a wider picture behind the simple square sums, which I present in chapter 7.
Much more obvious is the need to see behind, that all $4k + 1$ primes are factors of an $n^2 + 1$. Indeed, we saw above how big $n^2 + 1$ was needed to imbed, even the small $4k + 1$ primes. The most fundamental detail in why all this complication occurs is that, though $n^2 + 1$ is merely a simple second order expression, when we're dealing with remainders, then the squares are automatically involving all the higher powers. Instead of dragging in Wilson 2.), to give a concrete $n^2 + 1$, in the next chapter, we'll continue the basic idea of Wilson's proof, namely the pairing of remainders. In fact, I will give two new proofs for that $4k + 1$ primes are dividers of an $n^2 + 1$. The first is a shorter version, but still containing the depth of the problems, while the second will be a more complete description of how the squares and higher powers relate.
Going deeper, in the two directions, namely into the simple square sums and into the imbedding of the $4k + 1$ primes, still leaves the puzzling question, why isn't a direct proof for the square sumness of the $4k + 1$ primes. Obviously, thousands of mathematicians tried this in vain. I think the full picture behind this separation, is still not clear.
So now we return to the promised "ugly" shorter proofs for the prime factors of $n^2 + 1$.

T

All p prime factors of $n^2 + 1$ are square sums.

P

p can't divide n so, let the remainder of p in n be A.

Then $n^2 + 1 = (k\,p + A)^2 + 1 = (k\,p)^2 + 2\,k\,p\,A + A^2 + 1$

Thus, $A^2 + 1 = M\,p$, with $M < p$, because $A < p$.

If $M = 1$ we are finished. If not, we will reduce it to smaller and smaller m, till it becomes 1.

As we decrease m, we'll decrease the left side too. The change starts from $A^2 + 1$, but must be given from the general $A^2 + B^2$ to $a^2 + b^2$ as follows:

$$M\,p = \frac{M^2}{M}\,p > \frac{\left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2}{M}\,p > \frac{(A-\alpha M)^2 + (B-\beta M)^2}{M}\,p =$$

$$\frac{A^2 + B^2 - 2A\,\alpha\,M - 2B\,\beta\,M + \alpha^2 M^2 + \beta^2 M^2}{M}\,p = \left(p - 2A\alpha - 2B\beta + \alpha^2 M + \beta^2 M\right)p = m\,p =$$

$$p^2 - 2pA\alpha - 2pB\beta + \left(A^2 + B^2\right)\left(\alpha^2 + \beta^2\right) = \left|\, p - A\alpha - B\beta \,\right|^2 + \left|\, B\alpha - A\beta \,\right|^2 = a^2 + b^2 .$$

The only problem is that these forms contain minus signs so we have to show that we still get positive numbers. Due to the absolute values we can't get negatives so we only have to show that we can't get zeros.
Firstly, m could only be zero if both $A - \alpha M$ and $B - \beta M$ were zero, which could only be if M divided both A and B and then $A^2 + B^2 = M\,p$ were dividable by M^2 implying $M = 1$.
Also none of a or b can be zero either because $m < M < p$ and so $m\,p$ can't be a square.

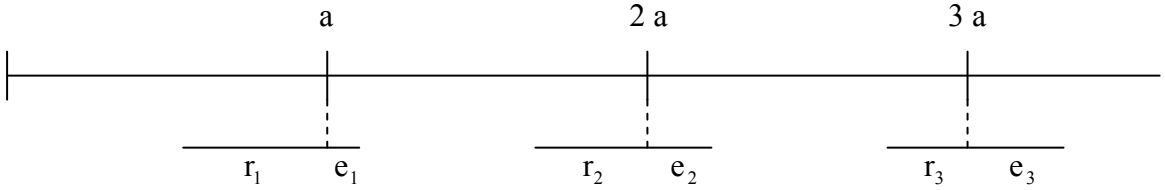
T All dividers of an $a^2 + 1$, are squares or square sums. Thus, the prime factors are square sums.

P A d divider of $a^2 + 1$ is little if $d < a$, and a D divider is large if $D > a$.
They come in pairs as $a^2 + 1 = d\,D$. For the extreme, $d = 1$ and $D = a^2 + 1$ dividers, the claim is trivial, since $1 = 1^2$ and $a^2 + 1 = a^2 + 1^2$. For $a = 1$, we only have these trivial dividers, so our claim is true. Suppose, that up to a A, our claim is true for all $a < A$.
We'll show how it inherits to A. Let $A^2 + 1 = d\,D$, again with $d < A < D$. Then:
$A = m\,d + a$ with $a < A$ and $A^2 + 1 = m^2 d^2 + 2\,m\,d\,a + a^2 + 1 = d\,D$, so $a^2 + 1 = d\,c$.
Since, for $a^2 + 1$ we know that our claim is true, thus d is square or square sum.
Now that we know, the claim is true for all little dividers of $A^2 + 1$, lets regard all prime dividers of the little dividers. These p_1 , . . . , p_m are little too, so they must be square sums, since they can't be squares. Also, for every D large divider, we have $A^2 + 1 = p_i \,.\,.\,. \,p_j\,D$.
Thus, enough to show the following lemma:
An $A^2 + B^2$ square ($B = 0$) or square sum divided by an $a^2 + b^2$ square sum prime factor, is again square or square sum.
This is exactly the lemma used in the Simple Square Sum Theorem earlier.

T Thue

If a , b are relative primes, and $b \neq 1$, then there are m , $c < \sqrt{b}$, so that
$m\,a - c$ or $m\,a + c = n\,b$. Thus, $(m\,a - c)\,(m\,a + c) = m^2\,a^2 - c^2 = N\,b$ for sure.

P The meaning of this theorem is quite visual, if we recall the generalized remainders of two a , b intervals. But now instead of just the remainders or gaps to the $m\,a$ multiples, the other halves of the b intervals, that is n b-s "excesses" over the $m\,a$, must be regarded too.



Our claim that $m\,a - c$ or $m\,a + c = n\,b$ can be restated as: $m\,a - n\,b$ or $n\,b - m\,a = c < \sqrt{b}$
This is a pretty strong claim because $\sqrt{b}$ is much smaller than b if b is a large number.
Yet at a smaller than $\sqrt{b}$ multiple of a, there is a remainder or excess, that is smaller than $\sqrt{b}$ too.
Now to the proof:

Lets list, the $0, 1, 2, \ldots, [\sqrt{b}]$ numbers and their "a" multiples: $0, a, 2a, \ldots, [\sqrt{b}]\,a$
The possible differences between the elements of these two lists, can be $([\sqrt{b}]+1)^2$ many.
Of course, $[\sqrt{b}]+1 > \sqrt{b} \rightarrow ([\sqrt{b}]+1)^2 > b$, so we have more than b many possible differences. The remainders of these differences to b can only be $0, 1, \ldots, b-1$, so b kind, and thus, at least two differences, say $|m_1 a - c_1|$ and $|m_2 a - c_2|$ have the same remainders to b. Having two differences means that $m_1 = m_2$ and $c_1 = c_2$ together are excluded, but we claim that in fact, none of them can be. Indeed, if $m_1 = m_2$, then since $b \neq 1$ thus, the same remainders to b, would mean $c_1 = c_2$ too. Also, if $c_1 = c_2$, then since a and b are relative primes, the same remainder would imply $m_1 = m_2$.
Then the differences of the differences, that is: $\big||m_1 a - c_1| - |m_2 a - c_2|\big|$ is dividable by b.
This difference can be changed to $\big||m_1 - m_2|a \mp |c_1 - c_2|\big|$.
Since $m_1 \neq m_2$ and $c_1 \neq c_2$, thus, $|m_1 - m_2| = m$ and $|c_1 - c_2| = c$ are from $1, 2, \ldots, [\sqrt{b}]$. So indeed, $m\,a \mp c = n\,b$, with natural $m, c < \sqrt{b}$.

T

All non 1 dividers of an $a^2 + 1$, are square sums. Thus, the prime factors too.

P

This is a sharpening of our previous theorem and it means that the square factors of $a^2 + 1$ are all square sums too. Indeed, for example: $7^2 + 1 = 50 = 2 \cdot 25$ and $25 = 5^2 = 4^2 + 3^2$.
Let $a^2 + 1 = k\,b$.
Thue's conditions stand for a and b, and so there are $m, c < \sqrt{b}$ that $m^2\,a^2 - c^2 = N\,b$.
Then multiplying our condition with m^2, we get: $m^2\,a^2 + c^2 = m\,q\,b = M\,b$.
Subtracting from this Thue, we get: $m^2 + c^2 = (M - N)\,b$
$m, c < \sqrt{b} \rightarrow m^2, c^2 < b \rightarrow m^2 + c^2 < 2\,b \rightarrow M - N = 1$.

6. Behind The $4k + 1$ Primes Being Factors of $n^2 + 1$

D

In the followings let q, r, s and bar denote remainders to a fix p prime.

T

1.) a.) $r, \overline{2r}, \overline{3r}, \ldots, \overline{(p-1)r}$ are all different.
b.) And these have all values from 1 to $p - 1$.

2.) a.) For every $r \in \{2, 3, \ldots, p-2\}$, there is a single $s \in \{2, 3, \ldots, p-2\}$ so that, $\overline{rs} = 1$. And for every r, this s is different and $\neq r$.
b.) $\overline{2 \cdot 3 \cdot \ldots \cdot (p-2)} = 1$, $\overline{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)} = p - 1$.

3.) If there is no r, such that $\overline{r^2} = q$, then:
a.) For every r, there is a single s, so that $\overline{rs} = q$.
And for every r, this s is different and $\neq r$.
b.) $\overline{q^{\frac{p-1}{2}}} = \overline{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)} = p - 1$.

4.) If $p = 4k + 1$, that is $\frac{p-1}{2} = 2k$ even, then:
a.) $\overline{(p-1)^{\frac{p-1}{2}}} = \overline{(p-1)^{2k}} = 1$.
b.) There is an r, so that $\overline{r^2} = p - 1$. So, $r^2 = kp + p - 1 = (k+1)p - 1 = mp - 1$.

P

1.) a.) If for $m < n$, $\overline{mr} = \overline{nr}$ were then $(n - m)r$ would be dividable by p.
b.) They are $p - 1$ many of them, all different, $< p$ and none of them 0.

2.) a.) By 1.) there is a unique s. We only have to show that $s \neq 1$ or $p - 1$ or r.
Indeed, $\overline{r \cdot 1} = r \neq 1$ or $\overline{r \cdot (p-1)} = \overline{rp - r} = p - r \neq 1$ and if $s = r$, then $\overline{rs} = \overline{r^2} = 1 \rightarrow r^2 - 1 = (r-1)(r+1) = mp$ were, but $r - 1 > 0$, $r + 1 < p$.
b.) The $2, 3, \ldots p-2$ numbers can be all paired according to $\overline{rs} = 1$ and so $\overline{2 \cdot 3 \cdot \ldots \cdot (p-2)}$ is the same as the product of these 1 value pairs, totaling 1.
Then of course, $\overline{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)} = p - 1$ at once.

3.) a.) Follows from 1.) and the condition that $\overline{r^2} \neq q$.
b.) They can be paired again by $\overline{rs} = q$. And now we have $\frac{p-1}{2}$ many pairs.

4.) a.) $\overline{(p-1)^{2k}} = \overline{\left((p-1)^2\right)^k} = \overline{(p^2 - 2p + 1)^k} = \overline{(p^2 - 2p + 1)}^k = 1^k = 1$
b.) If there weren't, then we could use 3.) b.) for $q = p - 1$ and thus,
$\overline{(p-1)^{\frac{p-1}{2}}} = p - 1$ were, contradicting a.).

D

Let q be a chosen non zero remainders from the possible $1, 2, \ldots, p-1$.

Those r remainders for which, $\overline{r^n} = q$, could be called the n-th roots of q, and denoted together as $\overline{\sqrt[n]{q}}$. Of course, there might not be such r and then, $\overline{\sqrt[n]{q}} = \varnothing$ = empty.

For $n = 2$, we simply use $\overline{\sqrt{q}}$. When $\overline{\sqrt[n]{q}}$ is not empty, we call q an n-th rootable.

T

1.) First complementarity

a.) If q is square rootable, then $\overline{\sqrt{q}} = \{ r , p - r \}$.

b.) Half of the $1, 2, \ldots, p-1$ remainders, are square rootable, half of them are not.

2.) First square rootability condition (Euler criterion)

a.) If q is square rootable, then $\overline{q^{\frac{p-1}{2}}} = 1$.

If q is non square rootable, then $\overline{q^{\frac{p-1}{2}}} = p - 1$.

b.) $\overline{\sqrt[\frac{p-1}{2}]{1}} = \{$ all square rootables $\}$

$\overline{\sqrt[\frac{p-1}{2}]{p-1}} = \{$all non square rootables$\}$

3.) Second complementarity

a.) For $p = 4k + 1$, that is if $\frac{p-1}{2} =$ even: If q is square rootable, then so is $p - q$ too.

b.) If $p = 4k + 1$, then for some q we have $q^2 + 1 = m\,p$.

4.) Second square rootability condition (Primitive roots)

If r is such that, $r , \overline{r^2} , \overline{r^3} , \ldots , \overline{r^{p-1}}$ are all different, that is they are $1, 2 , \ldots , p-1$, except in other order, then:

a.) $\overline{r^2} , \overline{r^4} , \ldots , \overline{r^{p-1}}$ are the square rootables.

b.) $r , \overline{r^3} , \ldots , \overline{r^{p-2}}$ are the non square rootables.

5.) Fermat's theorem

a.) $\overline{r^{p-1}} = 1$ for $r = 1 , 2 , \ldots , p-1$. In other words, $\overline{\sqrt[p-1]{1}} = \{1 , 2 , \ldots , p-1 \}$

b.) Unconditional form, $n^p - n = m\,p$ for all $n = 0 , 1 , 2 , 3 , \ldots$

The a.) form explains the name "primitive root" for the special r-s used in 4.).

Indeed, $r , \overline{r^2} , \overline{r^3} , \ldots , \overline{r^{p-1}}$ being different means the same that 1 only appears at the end as $\overline{r^{p-1}}$. Because, if it were earlier, then after it, r would reappear again.

So these special r-s are those that only appear in $\overline{\sqrt[p-1]{1}}$ (in which every non zero appears), but don't appear in any smaller root of 1. So, in the name "primitive root", "root" refers to "root of 1" and "primitive" to "highest only", that is $p - 1$.

By the way, to find such r primitive roots is not easy, in fact even to prove the existence of one, is quite difficult, as we'll see in Chapter 12. Early Restarts.

P

1.)

a.) If $q = \overline{r^2} = \overline{s^2}$ for two $r \neq s$, say $r > s$ remainders, then
$\overline{r^2} - \overline{s^2} = \overline{r^2 - s^2} = 0$ so $r^2 - s^2 = (r - s)(r + s) = m\,p$.
$r - s$ can't, so $r + s$ must be dividable by p.
But $r + s < 2\,p$, so $r + s = p$, so $s = p - r$.

b.) r and $p - r$ can't be same, since p is prime.
Thus, we have two different roots for all rootable q. Also, every $\{r , p - r\}$ pair can be such, so we have indeed halved the $\{1 , 2 , \ldots , p - 1\}$.

2.)

a.) For non square rootable q, $\overline{r\,s} = q$ sorts $\{1 , 2 , \ldots , p - 1\}$ into unique pairs.
Thus, $\overline{1 \cdot 2 \cdot \ldots \cdot (p-1)} = \overline{q^{\frac{p-1}{2}}}$.
For square rootable q, the two $r , p - r$ square roots of q, can be taken out of $\{1 , 2 , \ldots , p - 1\}$. The rest can be paired again. Also, $\overline{r\,(p-r)} = \overline{r\,p - r^2} = p - q$.
So now, $\overline{1 \cdot 2 \cdot \ldots \cdot (p-1)} = \overline{q^{\frac{p-1}{2}-1}\,(p-q)} = p - \overline{q^{\frac{p-1}{2}}}$.
For the $q = 1$ special case, we know that it is square rootable, so
$\overline{1 \cdot 2 \cdot \ldots \cdot (p-1)} = p - \overline{1^{\frac{p-1}{2}}} = p - 1$. Using this then:
For non square rootable q: $\quad p - 1 = \overline{q^{\frac{p-1}{2}}}$
For square rootable q: $\quad p - 1 = p - \overline{q^{\frac{p-1}{2}}} \;\rightarrow\; \overline{q^{\frac{p-1}{2}}} = 1$.

b.) By a.), $\overline{\sqrt[\frac{p-1}{2}]{1}} \supseteq \{$ all square rootables $\}$ and

$\overline{\sqrt[\frac{p-1}{2}]{p-1}} \supseteq \{$ all non square rootables $\}$.

$\overline{\sqrt[\frac{p-1}{2}]{1}}$ and $\overline{\sqrt[\frac{p-1}{2}]{p-1}}$ are disjoint, and the two sets on the right cover the full, $\{1 , 2 , \ldots , p - 1\}$, thus the two $\supseteq$ are actually $=$.

3.)
a.)

By first equality of 2.) b.) enough to show that if $q \in \overline{\sqrt[\frac{p-1}{2}]{1}}$, then $p - q \in$ too.
In other words, that if $\overline{q^{\frac{p-1}{2}}} = 1$ then, $\overline{(p-q)^{\frac{p-1}{2}}} = 1$ too. $\overline{(p-q)^{\frac{p-1}{2}}} = \overline{(p-q)^{2k}} = \overline{\left((p-q)^2\right)^k} = \overline{(p^2 - 2\,p\,q + q^2)^k} = \overline{(\,\overline{p^2 - 2\,p\,q + q^2}\,)^k} = \overline{\overline{q^2}^{\,k}} = \overline{(q^2)^k} = \overline{q^{2k}} = \overline{q^{\frac{p-1}{2}}}$

b.)

1 is square rootable, so by a.) $p - 1$ is too. Thus, $\overline{r^2} = p - 1$ for some r.
This means, $r^2 - (p - 1) = k\,p \;\rightarrow\; r^2 + 1 = (k + 1)\,p = m\,p$.

4.)

a.) $\overline{r^2}$, $\overline{r^4}$, . . . , $\overline{r^{p-1}}$ are all square rootable and since they are $\frac{p-1}{2}$ many different, they must be all the square rootables.

b.) They are all non square rootable by a.), and since they are $\frac{p-1}{2}$ many different, they must be all the non square rootables.

5.)

a.) By 2.) a.) $\overline{q^{\frac{p-1}{2}}} = 1$ for all q square rootables and

$\overline{q^{\frac{p-1}{2}}} = q - 1$ for all non square rootables.

The squared and then remaindered of the two equalities are the same.

$$\overline{q^{\frac{p-1}{2}}}^2 = \overline{\left(q^{\frac{p-1}{2}}\right)^2} = \overline{q^{p-1}} = \overline{1^2} = 1 \quad \text{and}$$

Same . . . $= \overline{(q-1)^2} = \overline{q^2 - 2q + 1} = 1$.

Thus, $\overline{r^{p-1}} = 1$ for all $r = 1, 2, \ldots, p-1$.

b.) Multiplying both sides with r, and taking the remainders:

$\overline{\overline{r^{p-1}} \cdot r} = \overline{r^p} = r$

This now stands for $r = 0$ too, and thus for all $0, 1, 2, \ldots, p-1$ remainders.

But then instead of r, it stands for all $\overline{n}$ remainders:

$\overline{n^p} = \overline{n}$ so $\overline{n^p - n} = 0$ so $n^p - n = m\,p$ for all $n = 0, 1, 2, 3, \ldots$

Now we give an elementary meaning and proof for this:

Lets call a (p , n) dial , a circular disc with p many windows on its perimeter.

This looks like a clock, but instead of the twelve numbers, we have p many windows.

Behind each window, instead of fix numbers, we can set n many symbols,

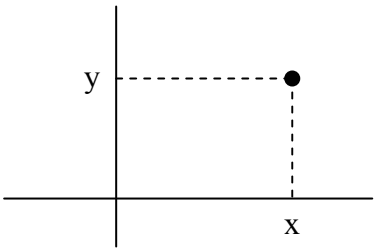
say $1, 2, \ldots, n$. Setting the symbols in each window, the obtained situation as a whole is called a display. Obviously, we have n^p many possible displays.

If all symbols are the same, then we say that the display is trivial. We have n many of such, so we have $n^p - n$ many non trivial displays. A display is "turnable" if there is a less than 360^o turn that puts it over itself. The trivial displays are of course turnable by any multiples of the $\frac{360}{p}$ smallest angle. But a non trivial display, even if it is turnable, can only be turned by a bigger than $\frac{360}{p}$ angle. The basic trick is to realize that if $m \cdot \frac{360}{p}$ is the minimal angle that can turn a display, then m must divide p.

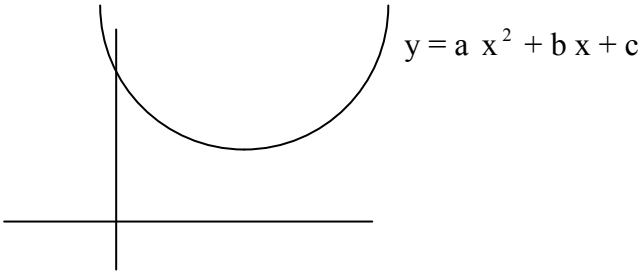
Indeed, all multiples of m give a correct turn again. What's more if m had an r remainder in p, then $-r \cdot \frac{360}{p}$ would turn the display into itself and so $r \cdot \frac{360}{p}$ were a correct turn too and smaller than $m \cdot \frac{360}{p}$. Then if p is a prime, there can not be any turnable non trivial displays. So, picking a display and regarding the possible $p - 1$ turns of it, we must get all new ones. Then we can again pick a new one in p variants, and so on. Thus, the $n^p - n$ total number of non trivial displays must be dividable by p.

7. Behind The Simple Square Sums

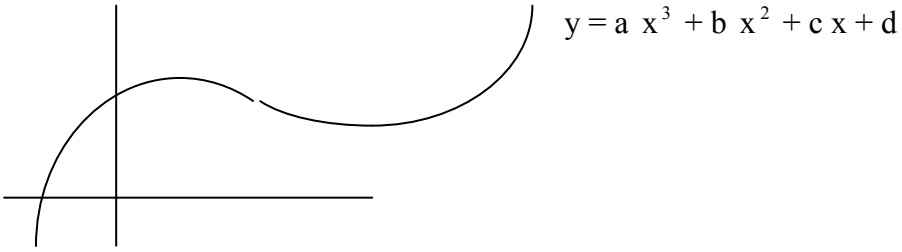
D The Descartes plane orders to every point a pair of real numbers, the two coordinates:



This is very useful to connect geometry with algebra. Namely, if two curves C and D are the set of points that satisfy two E (x , y) = 0 and F (x , y) = 0 equations, then the crossing points of C and D are exactly the common solutions of E (x , y) = 0 and F (x , y) = 0 .
Later, Descartes idea brought out a completely new possibility, namely to regard the (x , y) points as single numbers. The need for new numbers was realized earlier. The simple rule of "minus times minus equal plus" meant that negative numbers can't be squares. This is the basic reason for second order equations sometimes having no solutions. The Descartes system of course beautifully showed that in these cases, the parabola, that is the curve for the second order equations, is simply too high and thus, doesn't cross y = 0, that is the x axis.



But for third order equations, the curve is a double parabola, going from down to up, so there is always a root.



In general, odd order equations must have roots, but even order ones can have no root.
This "weirdness" disappears, if we are willing to accept the missing square roots of negative numbers. In a sense, this is similar to what we examined in the previous chapter, namely that the second order remainders already contain the complications of the higher ones. Here too, if we accept the simple square rooting of negative numbers, then all equations will have roots.
To be more specific:
If we accept a single new imaginary unit i, so that $i^2 = -1$, that is $i = \sqrt{-1}$, then the $x + y\,i$ combinations of real and imaginary numbers, are sufficient to guarantee roots for any order equations. But, the result was even more beautiful, because it showed that these $x + y\,i$ combinations are all we missed before. Indeed, any $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, n-th order polynom can be changed into:

$a_n \left(x - (x_1 + y_1 i) \right) \left(x - (x_2 + y_2 i) \right) \ . \ . \ . \ \left(x - (x_n + y_n i) \right)$

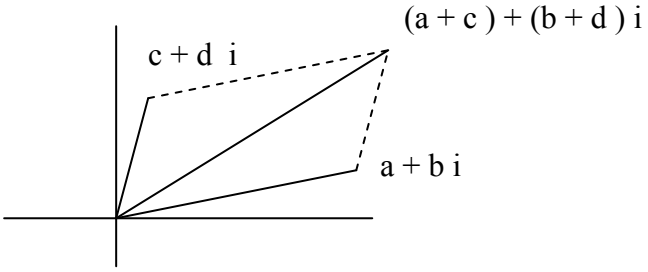
Then of course, the possible roots are the $x_1 + y_1 i$, $x_2 + y_2 i$, . . . , $x_n + y_n i$ new combination numbers, and they can only be n many or less, if same ones repeat.

This amazing result of the n-th order polynoms being reducible to a product of x minus combination numbers, follows backwards if we can guarantee that there is at least one combination root. This became known as the Fundamental Theorem of Algebra. Gauss proved it first, in fact he gave eight different proofs for it. He was also the first to use the Descartes plane for the new $x + y i$ combination numbers. All we have to do is regard the unit of the y axis as $i = \sqrt{-1}$, then a point is not (x , y) pair anymore, rather the single $x + y i$ combination or so called complex number. Even more beautiful is, that now we can add, subtract, multiply or divide, points, simply by obeying the rules of algebra.

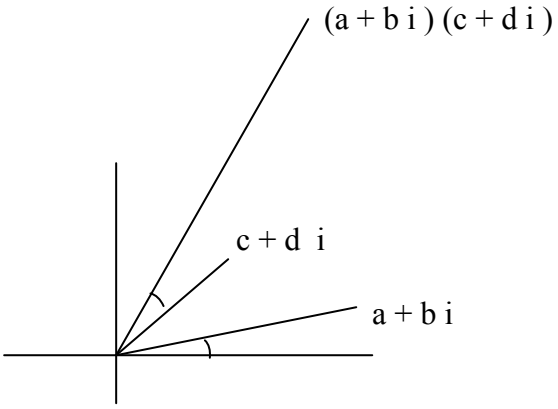
For example, $(a + b i) + (c + d i) = (a + c) + (b + d) i$

$(a + b i)(c + d i) = a c + a d i + b c i + b d i^2 = (a c - b d) + (a d + b c) i$ since $i^2 = -1$.

The addition as easy to see, corresponds to the old addition of vectors.



But the big surprise is that the multiplication means merely combining the angles from the x axis and multiplying the actual lengths.



So, while the addition was a shifting from one member with the other member, the multiplication is a turning from one member with the other. This heuristic meaning at once puts the original $i^2 = -1$ assumption in new light. Indeed, $i^2 = i \cdot i$, so we turn i itself with 90^o , thus getting to -1. In fact, -1 itself is a 180^o turn. Then, $(-1)(-1)$ is two 180^o turns, giving 360^o and thus, 1. So now the old "minus times minus equal plus" rule gained a new and final justification as well.

But there was another direction where Gauss ventured with his complex numbers, namely applying it to number theory. The idea is simply regard the $x + y i$ combinations, but only with x , y whole numbers. Of course, these are the grid points of the Descartes plane. The grids falling onto the x axis are the normal integers, while on the y axis are the imaginary integers. The real important ones for us, in the followings, will be the grids not on the x or y axis, and we'll call them duals. This name refers to the fact that these actually do have two components, but as we'll see there is a secondary meaning too, because the duals and their mirrored pairs to the x axis form a duo.

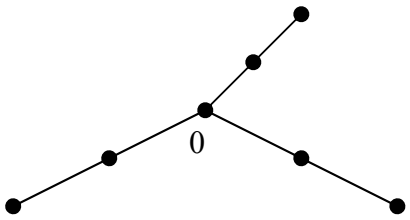
Just as in number theory, among the Gaussian or complex integers, the basic concern is dividability. The definition is obvious: An $A + B\,i$ is dividable by $a + b\,i$, if there is a $c + d\,i$, so that $A + B\,i = (a + b\,i)(c + d\,i)$.
Just as 1 was a trivial divider of any number, now we have four units: $1\ ,\ -1\ ,\ i\ ,\ -i$
and indeed, any number is dividable by these. For example, $\frac{2+3i}{i} = x + y\,i$, so

$2 + 3\,i = (x + y\,i)\,i = x\,i + y\,i^2 = -y + x\,i$ so $y = -2\ ,\ x = 3$ and $\frac{2+3i}{i} = 3 - 2\,i$

Just as among the natural numbers, there were the primes that were only dividable by 1 and themselves, here there are ones that can only be divided by the four units and themselves or unit variants of themselves. Above, for example, $3 - 2\,i$ was merely an i variant of $2 + 3\,i$.
These only trivially dividable numbers, will be called irreducible, so we can use the word prime, for the old natural primes. The old composites are therefore now generalized as reducibles. The most amazing fact is that not all the old primes remain irreducible in our new wider number system.
For example, $2 = (1 + i)(1 - i) = 1 - i^2 = 1 + 1$ or $5 = (2 + i)(2 - i) = 2^2 - i^2 = 4 + 1$.
So 2 and 5 are reducible. Remember, that $-1\ ,\ i\ ,\ -i$ multiples are regarded as mere variants. But since $1 = (-1)(-1) = i(-i)$, thus we can use these to get variant products for the same value. For example, $5 = (2 + i)(2 - i) = (2 + i)\,i\,(2 - i)(-i) = (2\,i - 1)(-2\,i - 1)$
So, this is not regarded as a new way of reducing 5.
Then as we can guess, the result is that all numbers can be "uniquely" obtained from irreducible factors. "Uniquely" if we ignore variants! This is the corresponding theorem of the U.P.F.T. (Unique Prime Factorization Theorem). Even the proof can be obtained the same way, that is first proving the Fundamental Theorem of Irreducibles, which claims that irreducibles divide products separately. Even the proof of this can be obtained similarly. This might sound impossible first, because among naturals we used remainders and an induction from smaller primes to bigger. How could this work here in two dimension where there is no obvious smaller larger relation between the numbers? Luckily, the distance from the origin can be used as size. Indeed, for variants, this remains the same, but multiplication with other numbers increases it.
As it turns out, not only there is remainder among the grid points, but usually more different, namely maximum 4 possible remainders can be obtained.

D

1.) Two duals are <u>same directional</u>, if they are on same half lines from the origin.



2.) A dual is <u>minimal</u> if it is the closest to the origin on its direction.
<u>The minimal of</u> a dual is the minimal on its direction.

3.) An $A + B\,i$ dual, is <u>multiple</u> of $a + b\,i$ if $A + B\,i = m\,a + m\,b\,i$ with $m = 2\ ,\ 3\ ,\ \ldots$
A dual is <u>simple</u> if it is not multiple of any.
A dual is <u>a simple of</u> an other, if it is simple and the other is multiple of it.

4.) Two duals are <u>mirror directional</u> if their directions are mirrored to the x axis.

5.) Two duals are <u>symmetrical</u> if they are symmetrical to the x axis.
Then one is called the <u>conjugate</u> of the other.

T

1.) a.) Every non minimal dual is multiple of its minimal.
b.) A dual is simple, if and only if it is minimal.
c.) The minimal of a dual is the only simple of it.
d.) Two simple, can't be same directional.

2.) a.) $a + b\,i$ is simple, if and only if a , b are relative primes.
b.) The simple of $A + B\,i$ is $\frac{A}{g} + \frac{B}{g}\,i$.
where g = greatest common divider of $|A|$ and $|B|$.

3.) The conjugate of $a + b\,i$ is $a - b\,i$.

4.) Two duals are mirror directional, if and only if their simples are symmetrical.

5.) a.) Every factor of a simple dual is a simple dual.
b.) Every simple dual breaks down to irreducible duals.

6.) a.) The product of two duals $(A + B\,i)(C + D\,i)$ is a natural n,
if and only if the duals are mirror directional.
b.) Then the product of their conjugates $(A - B\,i)(C - D\,i)$ is again n.
c.) Thus, if an $A + B\,i$ divides a natural, then the $A - B\,i$ conjugates divides it too.

7.) a.) A product becomes the conjugate, if its factors are conjugated:
$(a - b\,i)(c - d\,i)$ = conjugate of $(a + b\,i)(c + d\,i)$.
b.) If a dual is irreducible, then its conjugate is too.
c.) A simple dual can't be dividable by an irreducible and it's conjugate too.

8.) a.) The product of two irreducible conjugates is a reducible prime.
b.) Every reducible prime is such product $(a + b\,i)(a - b\,i) = a^2 + b^2$
c.) An $a + b\,i$ dual is irreducible, if and only if $(a + b\,i)(a - b\,i) = a^2 + b^2 =$ prime

D

An n natural is simple square sum if there are a , b relative primes, so that $n = a^2 + b^2$.

T

Generalized Simple Square Sum Theorem.
Every d factor of an n simple square sum, is also a simple square sum.

P

$n = a^2 + b^2 = (a + b\,i)(a - b\,i)$ with $a \pm b\,i$ simple duals.
Thus, by 5.) b.) n breaks down to irreducible duals.
By 6.) c.), d is a product of a symmetrical subset, from these duals.
By 7.) c.), every one of the conjugate pairs is dividing either $a + b\,i$ or $a - b\,i$.
Lets separate them by this! Then we get two conjugate duals, that are dividers of
$a + b\,i$ and $a - b\,i$ respectively and their product is d.
By 5.) a.) , these two are simple and so their product d is a simple square sum.

8. Non Simple Square Sums, Square Differences

T

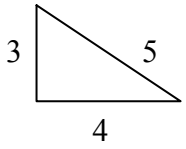
1.) A number is non simple square sum if and only if it is
a simple square sum multiplied by a square containing 2 or $4k+3$ prime factors .

2.) A number is a square sum if and only if:
it has no, or has even many of each $4k+3$ prime factors, and
if it has no or has even many 2 factors, then it has $4k+1$ prime factor too.

3.) A square number is a simple square sum if and only if it has only $4k+1$ prime factors.
A square number is a square sum if and only if it has some $4k+1$ prime factor.

R

The easy 3.) conditions for square numbers, shows in itself that there must be a special meaning. And indeed, $c^2 = a^2 + b^2$ is a case of the Pythagoras Theorem with whole numbers as sides.
Originally, the Pythagoreans believed that all distances can be measured by whole numbers, that is with common units. When they realized that $\sqrt{2}$, that is the hypotenuse of an equal sided right angle triangle is not commeasurable with the sides, they were quite confused. Later, all this became clear and then the special whole numbers that can be the sides became known as Pythagorean triplets. Simplest such is $3, 4, 5$.
Indeed, $3^2 + 4^2 = 5^2$.
Of course, any multiple of a Pythagorean triple is again such.
For example, $6, 8, 10$. Indeed, $6^2 + 8^2 = 10^2$.



The real question was how to find non multiple, new, that is simple Pythagorean triplets.
By our result of 8.), for a c, a triplet is possible if and only if c has some $4k+1$ prime factor and simple triplet is possible if and only if c has only $4k+1$ prime factors.
Without realizing the full picture, involving the splitting of prime factors, the greeks and maybe even the Babylonians already observed the followings:

T

1.) If $c = a^2 + b^2$ is odd and simple
then $c^2 = \left(b^2 - a^2\right)^2 + \left(2ab\right)^2$ and is again odd and simple.

2.) If $c^2 = A^2 + B^2$ is simple:
then A, B have different parity and thus c is odd too and if A was the odd
$c = \frac{c-A}{2} + \frac{c+A}{2}$ is a simple square sum again.

3.) $c^2 = A^2 + B^2$ is simple, if and only if for some a, b :
$c = a^2 + b^2$ and $b^2 - a^2 = A$ and $2ab = B$.

P

1.) $c^2 = \left(a^2 + b^2\right)^2 = a^4 + b^4 + 2a^2 b^2 = b^4 + a^4 - 2b^2 a^2 + 4a^2 b^2$
c^2 is obviously odd and $a+b$ and $b-a$ are odd too.
In fact, these two can't have any common prime factors with 2 or a or b. Thus:
$b^2 - a^2 = (a+b)(b-a)$ and $2ab$ can't have common prime factors at all.

2.) A and B can't be both even by the condition of simplicity. If they were both odds then: $A^2 + B^2 = (2m+1)^2 + (2n+1)^2 = 4M + 2$ couldn't be a square.
So let A be the odd and then: $c^2 - A^2 = (c - A)(c + A)$ is the B^2 even square, so $\frac{c^2 - A^2}{4} = \frac{c - A}{2}\ \frac{c + A}{2}$ is a square too. But $c - A$ and $c + a$ can't have common factors, otherwise c and a and thus a and b had too.
So $\frac{c - A}{2}$ and $\frac{c + A}{2}$ are both squares.

3.) The "if" direction is 1.) itself.
For the "only if", by 2.) $a = \sqrt{\frac{c - A}{2}}$ and $b = \sqrt{\frac{c + A}{2}}$ are wholes and they do because:
$b^2 - a^2 = \frac{c + A}{2} - \frac{c - A}{2} = A$ and $2ab = 2\sqrt{\frac{c - A}{2}}\ \sqrt{\frac{c + A}{2}} = \sqrt{c^2 - A^2} = B$.

R The classic formula of 1.) easily produces the newer and newer Pythagorean Triplets:

$5 = 1^2 + 2^2 \rightarrow 5^2 = (2^2 - 1^2)^2 + (2 \cdot 1 \cdot 2)^2 = 3^2 + 4^2$

$13 = 2^2 + 3^2 \rightarrow 13^2 = (3^2 - 2^2)^2 + (2 \cdot 2 \cdot 3)^2 = 5^2 + 12^2$

$17 = 1^2 + 4^2 \rightarrow 17^2 = (4^2 - 1^2)^2 + (2 \cdot 1 \cdot 4)^2 = 15^2 + 8^2$

$65 = 5 \cdot 13$ so this itself has two different simple square sum forms with the formula of the square sum multiplication, we used on page 20 :

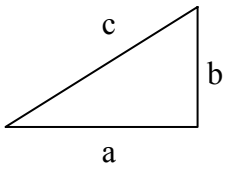
$65 = 5 \cdot 13 = (1^2 + 2^2)(2^2 + 3^2) = (1 \cdot 2 + 2 \cdot 3)^2 + (2 \cdot 2 - 3 \cdot 1)^2 = (1 \cdot 3 + 2 \cdot 2)^2 + (3 \cdot 2 - 1 \cdot 2)^2$

$65 = 1^2 + 8^2 \rightarrow 65^2 = (8^2 - 1^2)^2 + (2 \cdot 1 \cdot 8)^2 = 63^2 + 16^2$ and

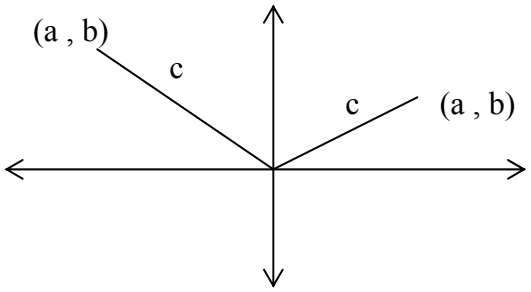
$65 = 4^2 + 7^2 \rightarrow 65^2 = (7^2 - 4^2)^2 + (2 \cdot 4 \cdot 7)^2 = 33^2 + 56^2$

If we return to the general square sums but with the Pythagorean meaning, then we get an amazing application:

So now a , b are wholes, but $c = \sqrt{a^2 + b^2}$ not necessarily:



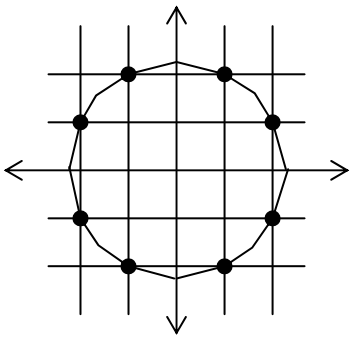
If further a , b can be any integers, then c is the distance of the (a , b) grid point of the Descartes coordinate system from the origin:



D

1.) Let $P(r)$ denote the number of grid points on the perimeter of the circle with r radius and centered in the origin.
For example: The figure shows $P(r) = 8$.

2.) Let $A(r)$ denote the number of grid points inside or on the circle.
For example: In the figure $A(r) = 17$



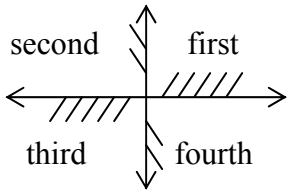
T

1.) For large r: $A(r) \approx r^2 \pi$

2.) $\pi = \lim_{r \to \infty} \frac{A(r)}{r^2}$

R

The grid points can only be on circles with $r = \sqrt{n}$ radiuses. So it would be enough to find a formula for this and then $A\left(\sqrt{n}\right) = P(0) + P(1) + P\left(\sqrt{2}\right) + P\left(\sqrt{3}\right) + \ldots + P\left(\sqrt{n}\right)$ might also be calculable.
$A\left(\sqrt{n}\right)$ is always $4k + 1$ because the origin $(0, 0)$ is a special grid, but all others repeat in the four quadrants. We might think that this has an importance to find formulas but it isn't so.
In fact, we ignore the origin and regard only one quadrant, that is calculate $\frac{P\left(\sqrt{n}\right)}{4}$ and $\frac{A\left(\sqrt{n}\right)-1}{4}$ to get nice formulas.
The girds on the x, y axes are regarded but only in one of the quadrants. Most logical if we take the ones on the $+x$ in the first, $+y$ in the second, $-x$ in the third and $-y$ in the fourth:



So, the beautiful formulas without proof and their consequence for π:

T

1.) The number of grid points on the $\sqrt{n}$ radius circle in one quadrant, is the same as how many more $4k + 1$ dividers n has than $4k + 3$:

$$\frac{P\left(\sqrt{n}\right)}{4} = D_{4k+1}(n) - D_{4k+3}(n) \qquad n > 0$$

For example: $\frac{P\left(\sqrt{5}\right)}{4} = D_{4k+1}(5) - D_{4k+3}(5) = 2 - 0 = 2$

2.) The number of grid points in the $\sqrt{n}$ radius circle in one quadrant, ignoring the origin:

$$\frac{A\left(\sqrt{n}\right)-1}{4} = \left[\frac{n}{1}\right]-\left[\frac{n}{3}\right]+\left[\frac{n}{5}\right]-\left[\frac{n}{7}\right]+ \ . \ . \ .$$

Where the square brackets denote the whole parts.

For example: $\frac{A\left(\sqrt{5}\right)-1}{4} = \left[\frac{5}{1}\right]-\left[\frac{5}{3}\right]+\left[\frac{5}{5}\right] = 5-1+1 = 5$

3.) $\frac{\pi}{4} = \frac{\lim A\left(\sqrt{n}\right)}{4n} = 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+ \ . \ . \ .$

R

Fermat looked into whether "Pythagorean" triplets exist for higher exponents: $a^n + b^n = c^n$
He couldn't find such whole numbers for any n > 2 exponents and claimed he found a proof for this non existence. He must have made some error or a wishful exaggeration because since then thousands of mathematicians tried to find a general proof in vain.
Even the special n = 3 , 4 , . . cases are hard to prove to be impossible. These and actual checks for higher exponents suggested that this so called Fermat's Last or more appropriately Fermat's Lost Theorem is true. After the Four Color Conjecture has been proved with the help of computers and the Continuum Hypothesis was proved to be undecidable, this remained the most important simple, unsolved problem. Finally, a very long and very difficult proof has been found.
There are just as simple unsolved number theoretical problems, but they all relate to the relative randomness of primes. Fermat's Last Theorem is quite different, it tells a definite sharp prediction that goes against randomness. Thus, it was a hint in the direction to go when it turned out that it had a connection to a completely different field of mathematics and indeed it was proved by settling an other conjecture in that field.
Finally, the other two such sharp predictions that are unsolved yet are the Rieman and Poincare conjectures.

T

Square differences

1.) $n = A^2 - a^2$ if and only if:
$n = B \cdot b$ with $B > b$ and B , b being either both even or both odd.

2.) a.) 3 , 5 , 7 , . . . odds are all square differences.
b.) 8 , 12 , 16 , . . . 4-multiples are all square differences.
c.) 2 , 6, 10 , . . . non 4-multiple evens are never square differences.
d.) 1 and 4 are not square differences.

3.) n is a unique square difference if and only if n is:
a.) odd prime or
b.) square of odd prime or
c.) four times a prime or
d.) four times the square of a prime

P

1.) For the "if" direction, with $B = A + a$, $b = A - a$ clearly:
$n = B \cdot b$, $B > b$ and B , b are either both even or both odd.
For the "only if" direction, with $A = \frac{B+b}{2}$, $a = \frac{B-b}{2}$:
A and a are whole and $n = A^2 - a^2$.

2.) a.) $2k+1 = (2k+1) \cdot 1$
b.) $4k = 2k \cdot 2$ with $k > 1$
c.) If B and b are either both even or odd then $B \cdot b$ is either odd or $4k$.
d.) $B \cdot b = 1$ is impossible with $B > b$.
$B \cdot b = 4$ with $B > b$ is only possible as $4 \cdot 1 = 4$ but 4 is even, 1 is odd.

3.) Among odds to have unique $B \cdot b$ means that $b = 1$ so:
B must be odd prime or square of it.
Among 4-multiples only $4p$ and $4p^2$ give unique B , b as:
$4 \cdot 2$, $4 \cdot 3$, $5 \cdot 4$, $7 \cdot 4$, $11 \cdot 4$, . . . and
$4 \cdot 2^2 = 8 \cdot 2$, $4 \cdot 3^2 = 18 \cdot 2$, $4 \cdot 5^2 = 50 \cdot 2$, $4 \cdot 7^2 = 98 \cdot 2$ . . .

9. Generation problem

R

The irregular sequence of primes makes it very plausible that a single formula can not calculate all the primes. This assumption of course can only be meaningful if we specify what we mean by a "formula". The simplest meaning could be an expression using only the four basic operations. Indeed, such basic formula can not calculate the primes. Even more surprisingly it can't even calculate a subset of the primes, that is it can't give only prime values. In spite of this, some quite simple basic formulas give "a lot of" primes. Most famous such $x^2 + x + 41$ was already known by Euler. This has only prime values for all x places between -40 and $+39$.
This is a consequence of the empirical fact that:

$41\ ,\ 41+2 = 43\ ,\ 43+4 = 47\ ,\ 47+6 = 53\ ,\ 53+8 = 61\ ,\ .\ .\ .\ .\ .\ .\ .\ .$
$41 + 2 + 4 + . . . + 2\cdot 38 = 41 + \frac{2+76}{2}\cdot 40 = 1601$ are all primes.

Indeed, $x^2 + x + 41$ at x = 0 gives 41, at x = 1 gives 43, at x = 2 gives 47 and so on, in general: at $x + 1$ gives $(x+1)^2 + (x+1) + 41 = x^2 + x + 41 + 2\cdot(x+1)$ so the next values of Euler's formula are always obtainable from the previous, by simply adding the double of the new place. At x = 38 in the sequence that is at x + 1 = 39 in the formula giving the last prime. Indeed, $40^2 + 40 + 41 = 40^2 + 80 + 1 = 41^2$ obviously not a prime.
The negative places simply follow from the positive ones because:
$(-x)^2 + (-x) + 41 = (x-1)^2 + (x-1) + 41.$
At $x = 41$ the value is: $41^2 + 2\cdot 41 = 41(41+2) = 41\cdot 43$ is composite again but then at x = 42 the value is: $41\cdot 43 + 2\cdot 42$ which is a prime. We don't have to calculate this to check it because there is a general feature of $x^2 + x + 41,$ namely that it can have only factors bigger than 40.
Indeed, let d be a factor of a value at the $x = md + r$ place!
If $(md+r)^2 + (md+r) + 41 = md(md + 2r + 1) + (r^2 + r + 41)$ is dividable by d, then $r^2 + r + 41$ is dividable too. But if $d \le 40$ then $r \le 39$ and for these values we know already that $r^2 + r + 41$ is a prime bigger than 40 so they can't have a factor $d \le 40$.
Also $x^2 + x + 1 < x^2 + 2x + 1 = (x+1)^2$ so $x^2 + x + 1$ must have a prime factor $< x + 1$.
So at the above $x = 42$ place the $41\cdot 43 + 2\cdot 42$ value could only have 41 as a prime factor but it can't because $2\cdot 42$ doesn't have it. Similarly we can analyze other values of this interesting second order formula. Yet we don't know if it takes up infinite many prime values! Of course we can be sure that it takes up infinite many composite values because at $x = m\cdot 41$ it is always dividable by 41.
A much wider range of formulas can be obtained if we allow logical symbols to define numbers from the basic operations. These could be called explicit formulas.
A different direction of generalization is to regard only "effective", that is case by case calculable operations.
For example the $<$ relation is explicitly definable by addition because:
$x < y$ if and only if some z added to x gives y. In short: $x < y \leftrightarrow \exists\ z\ ,\ x + z = y.$
On the other hand, the multiplication can not be explicitly expressed from addition, only effectively as: $x\cdot 1 = x$ and $x\cdot(y+1) = x\cdot y + x$

In mathematical logic, Gödel's famous incompleteness theorem used the argument that all effective calculations can be explicit from addition and multiplication. A usually unmentioned but very amazing side effect of this is that the exponentiation can also be expressed directly from multiplication with logical symbols. The usual method of defining exponentiation is of course the effective way, similarly to the above definition of multiplication: $x^1 = x$ and $x^{y+1} = x^y \cdot x$.
Of course we don't need Gödel's argument here because the explicitness of effectivity is quite obvious for the case of prime numbers. Indeed, they can be defined as numbers that are not dividable by smaller ones (this is the explicit way) or effectively as the sequence of n-unsieved numbers as we did in section one.
Surprising results were achieved by regarding calculations that only use equation systems with the basic operations. Amazingly there is such system that can yield the totality of primes.
An even older attempt to get primes than the above mentioned Euler's formula was to regard higher powers. As it turns out, the simplest rules follow from three basic identities involving the difference or sum of two powers:

T

1.) For all n: $B^n - b^n = (B - b)\,[\,B^{n-1} + B^{n-2}\,b + \ldots\ldots + B\,b^{n-2} + b^{n-1}\,]$
2.) For even n: $B^n - b^n = (B + b)\,[\,B^{n-1} - B^{n-2}\,b + \ldots\ldots + B\,b^{n-2} - b^{n-1}\,]$
3.) For odd n: $B^n + b^n = (B + b)\,[\,B^{n-1} - B^{n-2}\,b + \ldots\ldots - B\,b^{n-2} + b^{n-1}\,]$

P

All three can be checked by multiplying them.
A few examples:

$B^3 - b^3 = (B-b)\,[\,B^2 + B\,b + b^2\,]$
$B^4 - b^4 = (B-b)\,[\,B^3 + B^2\,b + B\,b^2 + b^3\,]$
$B^4 - b^4 = (B+b)\,[\,B^3 - B^2\,b + B\,b^2 - b^3\,]$
$B^3 + b^3 = (B+b)\,[\,B^2 - B\,b + b^2\,]$

R

The $b = 1$ special cases and even more the $B = 2$ cases of those, deserve special names:

D

$B^n - 1$ and $B^n + 1$ are called the power twins for the B^n power.
$2^n - 1$ is called the n-th Mersenne number and is denoted as M_n.
$2^n + 1$ is called the twin of M_n and of course it is $M_n + 2$.

T

1.) If B is odd then the power twins are even. If B is even then the power twins are odd.
2.) If $B > 2$, $n > 1$ then $B^n - 1$ is composite.
3.) If $B = 2$ and n is composite, then $B^n - 1 = 2^n - 1$ is composite.
4.) If $B \geq 2$ and n has odd factor, then $B^n + 1$ is composite

P

1.) Odd number's power is odd, even's power is even.
2.) $B^n - 1 = (B-1)[\quad]$ by 1.) of previous theorem and here neither (B – 1) nor [ ] is 1.
3.) $2^n - 1 = 2^{m\cdot k} - 1 = \left(2^m\right)^k - 1^k = \left(2^m - 1\right)[\quad]$
4.) $B^n + 1 = B^{m\cdot k} + 1 = \left(B^m\right)^k + 1^k = \left(B^m + 1\right)\left\{\left(B^m\right)^{k-1} - \ldots.\right\}$
Here k is an odd factor of n so we used 3.) of previous theorem.

T For $n > 1$

1.) If $B^n - 1$ is prime, then $B = 2$ and n is prime.
In other words, only the M_p prime indexed Mersenne numbers can be primes among the smaller members of the power twins.

2.) If $B^n + 1$ is prime, then B = even and $n = 2^k$.
In particular, among the twins of Mersenne numbers, only M_{2^k} can be primes.

3.) Power twins can't be both primes, that is twin primes, except $2^2 - 1 = 3$ and $2^2 + 1 = 5$.

P

1.) By previous 2.) B must be 2 and then by previous 3.) n must be prime.

2.) By previous 1.) B must be even and then by previous 4.) n can't have odd factor.

3.) $n = p$ and $n = 2^k$ exclude each other except for $p = 2$ and $k = 1$.

D The prime indexed M_p Mersenne numbers are called Mersenne candidates.

The 2^k indexed $M_{2^k} + 2 = 2^{2^k} + 1$ Mersenne twins are called Mersenne twin candidates or F_k Fermat numbers.

R Both candidates: $M_p = 2^p - 1$ and $M_{2^k} + 2 = F_k = 2^{2^k} + 1$ seemed to be "working" for small values, that is they produce only primes. But then they fail:

1.) $M_2 = 2^2 - 1 = 3$ $M_3 = 2^3 - 1 = 7$ $M_5 = 2^5 - 1 = 31$ $M_7 = 2^7 - 1 = 127$
But then: $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$

2.) $F_0 = 2^{2^0} + 1 = 3$ $F_1 = 2^{2^1} + 1 = 5$ $F_2 = 2^{2^2} + 1 = 17$ $F_3 = 2^{2^3} + 1 = 257$
$F_4 = 2^{2^4} + 1 = 65537$
But then: $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4{,}294{,}967{,}297 = 641 \cdot 6700417$
as Euler observed it first.

The continuing candidates turned out to be totally different stories for the two cases.
The M_p Mersenne candidates seem to be popping up both successful primes and failing composites. Most amazingly, still Mersenne in the 17-th century, predicted which ones will be successful and which will fail. His predictions turned out to have only a few errors. To do this without computers is quite a mysterious result to me. Even today, we only have less than forty proven Mersenne primes and about the same many proven failed Mersenne candidates. In fact, up to about $n = 300$ all $M_n = 2^n - 1$ Mersenne numbers are factorized.
The other direction, that is the twin candidates or Fermat numbers $M_{2^k} + 2 = F_k$ is much harder of course, because it is growing much faster. Amazingly, after the failing F_5 that Euler discovered, all new ones also failed. So though we have only less than hundred proven cases, this empirical evidence suggests that there are no more primes among $F_k = 2^{2^k} + 1$ beyond the above listed $k = 0, 1, 2, 3, 4$ cases.

R The infinite tendencies are totally unproven. In other words:
We have no proofs that M_p and F_k will have infinite many primes or composites.
In spite of all this uncertainty, we do have perfect criterias for both candidates to be primes.
Of course these are not settling the above questions and are not even practical to decide primalities directly!

T Lucas

Let $L_2 = 4$ and $L_{n+1} = L_n{}^2 - 2$ the so called Lucas sequence.
Example: $L_3 = 4^2 - 2 = 14$, $L_4 = 14^2 - 2 = 194$, $L_5 = 194^2 - 2 = 37634$, . . .
Then for $n > 2$ M_n is prime if and only if it is factor of L_n.
Example: $M_3 = 2^3 - 1 = 7$ is factor of $L_3 = 14$ and indeed, 7 is prime.
$M_4 = 2^4 - 1 = 15$ is not factor of $L_4 = 194$ and indeed, 15 is not prime.
$M_5 = 2^5 - 1 = 31$ is factor of $L_5 = 37634$ and indeed, 31 is prime.

T Pepin

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

R Even more amazingly, both the Mersenne and the Fermat primes have connections to two seemingly totally different problems:

10. Perfect numbers, polygon numbers

D

Let $\{a\}$ denote the set of all dividers of a.
Let $a \cap b$ abbreviate $\{a\} \cap \{b\}$, that is the set of common dividers of a and b.
Then of course $a \cap b = 1$ means that a , b are relative primes.
Let $\sum \{a\}$ denote the sum of all the numbers in $\{a\}$, that is the sum of all dividers of a.
An a is a "perfect number" if $\sum \{a\} = 2\,a$.
Example: $\sum \{6\} = \sum \{1 , 2 , 3 , 6\} = 12 = 2 \cdot 6$, so 6 is a perfect number.

T

1.) If $a \cap b = 1$ then $\sum \{a\,b\} = \sum \{a\} \sum \{b\}$.

2.) If p is prime then $\sum \{p^e\} = 1 + p + \ldots + p^e = \dfrac{p^{e+1} - 1}{p - 1}$.

3.) $\sum \{p_1^{e_1} \ldots p_k^{e_k}\} = \dfrac{p_1^{e_1+1} - 1}{p_1 - 1} \ldots \dfrac{p_k^{e_k+1} - 1}{p_k - 1}$

4.) Euclid

If $2^n - 1$ is prime then $2^{n-1}\left(2^n - 1\right)$ is perfect. Or in today's notation:

If M is Mersenne prime, then $\dfrac{M+1}{2}\,M$ is perfect.

P

1.) Let the dividers of a be: $1, a_1, a_2, \ldots, a$ and b's: $1, b_1, b_2, \ldots, b$.
Then since a , b are relative primes, the dividers of a b are:
$1, a_1, \ldots, a, b_1, \ldots, b, a_1 b_1, \ldots, a\,b$ where all multiples appear.
The sum of these, is the same as: $(1 + a_1 + \ldots + a)\,(1 + b_1 + \ldots + b)$

2.) , 3.) are trivial. For 4.):

$$\sum \left\{2^{n-1}\left(2^n - 1\right)\right\} = \frac{2^n - 1}{2 - 1}\,\frac{\left(2^n - 1\right)^2 - 1}{\left(2^n - 1\right) - 1} = \left(2^n - 1\right)\frac{2^{2^n} - 2 \cdot 2^n}{2^n - 2} = \left(2^n - 1\right)2^n = 2\left[2^{n-1}\left(2^n - 1\right)\right]$$

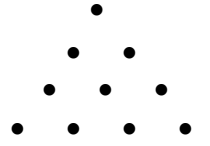
R

Euclid's condition can be given a visual meaning.

$2^{n-1}\left(2^n - 1\right) = \dfrac{M+1}{2}\,M = 1 + 2 + \ldots + M$

Such sums of numbers up to a number, are also called triangular numbers for the obvious reason that dots placed in such shape give this sum. For example for a 4 sided triangle:

$T_4 =$

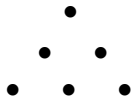


1
2
3
4 $\quad 1 + 2 + 3 + 4 = T_4 = 10$

In general:

$T_m = \dfrac{m+1}{2}\,m$, thus if M is a Mersenne prime then T_M is a perfect number.

For example:



$$T_{M_2} = T_{\left(2^2-1\right)} = T_3 = \frac{4}{2}3 = 6$$

$$T_{M_3} = T_{\left(2^3-1\right)} = T_7 = \frac{8}{2}7 = 28$$

$$T_{M_5} = T_{\left(2^5-1\right)} = T_{31} = \frac{32}{2}31 = 496$$

$$T_{M_7} = T_{\left(2^7-1\right)} = T_{127} = \frac{128}{2}127 = 8128$$

R The quest for finding all perfect numbers was initiated by the Pythagoreans.
Euclid's condition didn't solve the problem. First of all, $2^{n-1}\left(2^n-1\right)$ gives only even perfect numbers and even for them 2^n-1 must be a prime. Only a dozen such primes were known and even today we only have less than forty of them, as I mentioned. Euler improved the situation by proving that for even perfect numbers Euclid's condition is necessary:

T If an even number is perfect then it is $2^{n-1}\left(2^n-1\right)$, with 2^n-1 being a prime. In other words: Every even perfect number is a triangular number with a side, that is prime and 2^n-1 too.

P Let our even number be $2^{n-1}\,m$ with m not having factor 2. Then, it being perfect:

$\Sigma\left\{2^{n-1}\,m\right\} = \frac{2^n-1}{2-1}\Sigma\{m\} = \left(2^n-1\right)\Sigma\{m\} = 2\left[2^{n-1}\,m\right] = 2^n\,m$ So:

$$\Sigma\{m\} = \frac{2^n\,m}{2^n-1} = \frac{m+\left(2^n-1\right)m}{2^n-1} = \frac{m}{2^n-1} + m$$

$\frac{2^n\,m}{2^n-1}$ is whole but 2^n and 2^n-1 have no common factor, so m is dividable by 2^n-1 that is, $\frac{m}{2^n-1}$ is whole and is a divider of m.
Of course m is also a divider of m. Thus, $\Sigma\{m\}$ that is the sum of all dividers of m, being $\frac{m}{2^n-1} + m$ means that these two members of the sum are <u>all</u> the dividers of m.
But, 1 is a divider too, so $\frac{m}{2^n-1}$ must be 1. The only other divider is m itself, so it is a prime.
Together, these two mean that $m = 2^n-1$ and it is a prime.

R The application of Fermat primes is a much newer result than the perfect number connection to the Mersenne primes. In a sense it came out of the blue but now we can see that it was the tip of an iceberg.
Dissecting a d distance into n equal parts is a beautiful elementary construction. The trick is to use an arbitrary a distance that we measure n times after each other and then we project this $n\,a$ distance onto our d and thus projecting the dissection with it. The same trick doesn't work for angles and it was accepted since ancient times that even just to cut an α angle into three equal parts can not be done for arbitrary α with ruler and compass. This mentioning of "arbitrary" angle was important because unlike among distances, among angles we have a special one, namely the full 360^o. Indeed, for example to trisect 360^o is obvious because 120^o can be obtained as the double or complementing part of 60^o to a line, that is 180^o and 60^o itself is the angles of an equal sided triangle. Or even more directly the six section of 360^o can be obtained by using the radius of a circle on its perimeter. Similarly n-secting 360^o is the same as constructing the n equal sided polygon into a circle.
The constructions of pentagon, hexagon, octagon were well known.
For arbitrary angle we have the following beautiful result:

T Let the $a\,,\,b\,>\,1$ natural numbers have the g greatest common divider. Then:

1.) There are $n < a$ and $m < b$ naturals, so that $g\,=\,m\,a - n\,b$.

2.) The smallest common multiple of $a\,,\,b$ is $s\,=\,\frac{a\,b}{g}$.

3.) If a d distance is cut into a and b many equal parts with the $A_1\,,\,\ldots\,A_{a-1}$ and $B_1\,,\,\ldots\,B_{b-1}$ points then there will be A_n and B_m with $\frac{d}{s}$ distance between.

4.) If an α angle is cut into a and b many equal parts with the $A_1\,,\,\ldots\,A_{a-1}$ and $B_1\,,\,\ldots\,B_{b-1}$ lines then there will be A_n and B_m with $\frac{\alpha}{s}$ angle between.

5.) If for an α angle $\frac{\alpha}{a}$ and $\frac{\alpha}{b}$ are constructible then $\frac{\alpha}{s}$ is also.

P

1.) In section 1 at third proof of 1.), we already showed that if $a\,,\,b$ are relative primes then 1 is a remainder in the beginning sequence: $a\,,\,2\,a\,,\,\ldots\,,\,(b-1)\,a$ on division by b. That is, $1\,=\,m\,a - n\,b$ with $m < b\;,\;n < a$. If $a\,,\,b$ have the g greatest common divider then $\frac{a}{g}$ and $\frac{b}{g}$ are relative primes, so $1\,=\,m\,\frac{a}{g} - n\,\frac{b}{g}$.
Multiplying this with g gives our claim.

2.) By the U.P.F.T. the greatest common divider is the product of all common prime factors while the smallest common multiple is the product of all prime factors without repeating the common ones twice. And of course, $a\,b$ contains all with the common ones twice.

3.) By 1.) $g\,=\,m\,a - n\,b$. This multiplied with the $\frac{d}{a\,b}$ distance and using 2.) gives:

$$\frac{d}{\frac{a\,b}{g}}\;=\;\frac{d}{s}\;=\;m\,\frac{d}{b} - n\,\frac{d}{a}\;=\;B_m\,-\,A_n$$

4.) Same as 3.) with an arch used instead of d.

5.) Trivial by 4.).

R Thus, from the constructability of $\frac{360^o}{3} = 120^o$ and $\frac{360^o}{5} = 72^o$ follows $\frac{360^o}{15} = 24^o$.
Or this can be seen directly too because $24 = 2 \cdot 74 - 120$.
Of course we can easily half any angle, so the following sided polygons were constructible before Gauss: $3, 4, 5, 6, 8, 10, 12, 15, 16$. The missing $7, 9, 11, 13, 14$ smaller sides and the next 17 were pretty much accepted as unsolvable cases. Thus, when Gauss at age 17 succeeded in constructing the 17 polygon, it was a bombshell. But his personal fate changed too because this success made him decide to become a mathematician. Today, his statue in Goettingen stands on a 17 polygon base.
The solution of the pentagon, that is the construction of $\frac{360^o}{5} = 72^o$ is based on the fact that in the equal sided triangle with 72^o base angles, these are exactly double of the third top angle 36^o. A naïve idea would be to follow this line and choose other top angles so that the two base angles are other multiple of that. Tripling gives $\alpha + 2 \cdot 3\,\alpha = 7\,\alpha = 180$ and quadrupling gives $\alpha + 2 \cdot 4\,\alpha = 9\,\alpha = 180$. Since none of these work, nobody went further to check higher multiples and indeed, nobody would have guessed that if the base angle is 8 times the top, that is $\alpha + 2 \cdot 8\,\alpha = 17\,\alpha = 180$ then the triangle can be constructed. But even more amazing is the general pattern behind why it is solvable. After all 8 is a power of 2 but so was 4. Yes, but $\alpha + 2 \cdot 4\,\alpha = 9\,\alpha$ is not a prime multiple, while $\alpha + 2 \cdot 8\,\alpha = 17\,\alpha$ is. So we have to have duplicated base angles but also prime times of the top angle in total for the whole triangle. Now if $p\ \alpha$ is the total angle then $(p - 1)\ \alpha$ is the two base angles together and if each is obtainable as doublings of α then they together, that is $(p - 1)\ \alpha$ also and so must be $2^n\,\alpha$. Thus, $p - 1 = 2^n$ or $p = 2^n + 1$, that is $M_n + 2$ Mersenne twin. As we saw, the only candidates among these to be prime are the $n = 2^k$ cases, that is the $F_k = 2^{2^k} + 1$ Fermat numbers. Also we saw, that only five is known, namely the first five for $k = 0, 1, 2, 3, 4$.
We might think that this uncertainty about Fermat primes is the iceberg I mentioned above, but no. It is a much more important connection that was left in a mess after Gauss' discovery. Namely, a fundamental duality between the constructions of geometry and the equations of algebra. Just as the Euclidian Algorithm wasn't fully realized by Euclid also Gauss' special constructability condition for the circular polygons wasn't followed by a description of how the constructible distances and angles can relate to algebraic conditions in general. In fact, the whole negative problem of non constructability was left in dark. Even the reverse of the Fermat-prime condition for n polygons was not proved by Gauss only in 1836 by Wantzel. This will be mentioned in the book on Polynoms.
The general problem of constructible distances and angles will be dealt in a separate book.

11. Restarts Fermat's theorem, composite restarts

R A favorite pastime of ancient chinese mathematicians was doubling numbers and checking remainders. So they clearly knew the importance of prime numbers and realized the following "pattern" that breaks down already at 11:

1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	. .
2	4	8	16	32	64	128	256	512	1024	2048	. .
1	**3**	**7**	15	**31**	63	**127**	255	511	1023	**2047**	. .

Indeed, when the doubling numbers are primes: 2 , 3 , 5 , 7, the doubling results minus 1 are too: 3 , 7 , 31 , 127. But then 11 is prime and yet $2047 = 23 \cdot 89$. We saw this already as $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ being the first failing Mersenne candidate.
Strangely, the four primes 3 , 7 , 31 , 127 have all 1 remainder to the corresponding doublings 2 , 3 , 5 , 7 and even though 2047 is not a prime it again has 1 remainder to 11.
This keeps on continuing for all prime doublings and even more strangely, only for the primes.
In present notations this means that the prime indexed Mersenne numbers, that is the Mersenne candidates have all 1 remainder to their index and only these.
Then of course, regarding the doublings themselves, they give 2 remainders exactly at the primes:

1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	. .
2	4	8	16	32	64	128	256	512	1024	2048	. .
0	0	2	0	2	4	2	0	4	4	2	. .

This pattern is perfect in that half of the claim that it will always give 2 remainder at primes. Sadly it still breaks down in its exclusiveness because $341 = 11 \cdot 31$ doublings would give a number with also remainder 2 to 341. This number is so enormously big that the old chinese mathematicians couldn't handle it. Of course, today to prove our claim we don't have to calculate with big numbers because of our abstract ways of using letters, that is variables. An other trick is to go back from the 2 remainder to using 1 remainder but in a different way. Namely, 2^n having 2 remainder to n means the same as 2^{n-1} having 1 remainder to n. Indeed, doubling a number, the remainder doubles too, so 2 can only come from 1. This can be clearly seen in the above sequence and probably the chinese mathematicians regarded this already as the more important pattern by shifting the doublings with one place and checking the remainders there:

1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	. .
	2	4	8	16	32	64	128	256	512	1024	. .
	0	1	0	1	2	1	0	4	2	1	. .

But more importantly the 1 remainder is special because it remains the same for products. That is, if two numbers a , b both have 1 remainder to a d divider then ab has 1 too:
Indeed, if $a = md + 1$ and $b = nd + 1$, then $ab = (md + 1)(nd + 1) = mndd + md + nd + 1$.
This also implies that if a number has 1 remainder then its powers also have the same.
Using this with the exponent 340 will at once prove what we claimed above.
Indeed, lets observe that $2^{10} = 1024 = 3 \cdot 341 + 1$ so 2^{10} has 1 remainder to 341.
Then $2^{340} = \left(2^{10}\right)^{34}$ also has 1 remainder to 341 and 2^{341} has 2 remainder to 341.
And of course, as we mentioned $341 = 11 \cdot 31$ is not a prime.
This counter example for the exclusiveness of primes was pretty much coming "out of the blue" but there is a more "logical" way too. In fact, this method will give a whole possible sequence of counter examples. We use the same basic idea that a power of 1 remainder gives again 1 but now we use the claimed rule itself to defeat its exclusiveness to primes.
First I show it in general and then check the examples.

Observe that, 2^n has 1 remainder to 2^n-1 obviously, so $\left(2^m\right)^n = \left(2^n\right)^m$ has also 1 remainder to 2^n-1. If an n has the property that, 2^{n-1} has 1 remainder to n then this can also be expressed as $2^{n-1}-1$ being dividable by n, that is by saying that $\frac{2^{n-1}-1}{n}$ is a whole.

So we can use the previous power trick with $m = 2\cdot\frac{2^{n-1}-1}{n}$ which means that:

$\left(2^n\right)^{2\cdot\frac{2^{n-1}-1}{n}} = 2^{2(2^{n-1}-1)} = 2^{2^n-2} = 2^{(2^n-1)-1}$ has 1 remainder to 2^n-1.

But this exactly means that 2^n-1 is again a number having the property. So then to refute that the property is only true for primes we only need to find a 2^n-1 that is not prime in spite of n being a prime. As we saw, this was already the case for $n = 11$ because $2^{11}-1 = 2047 = 23\cdot 89$. Now the argument with concrete numbers:

$2^{3-1} = 4$ has 1 remainder to 3 but also 2^3 has 1 remainder to $2^3-1 = 7$.

Thus, $\left(2^3\right)^{2\cdot\frac{2^{3-1}-1}{3}} = 2^{\left(2^3-1\right)-1} = 2^{7-1} = 2^6$ has also 1 remainder to 7.

Similarly: $2^{5-1} = 16$ has 1 remainder to 5 but also 2^5 has 1 remainder to $2^5-1 = 31$.

Thus, $(2^5)^{2\cdot\frac{2^{5-1}-1}{5}} = 2^{(2^5-1)-1} = 2^{31-1} = 2^{30}$ has also 1 remainder to 31. Similarly:

From $2^{7-1} = 64$ having 1 remainder to 7, we get 2^{126} again having 1 remainder to 127.

Up to here our method always gave new prime cases, namely 7 , 31 , 127. But then: From $2^{11-1} = 1024$ having 1 remainder to 11 we get 2^{2046} having 1 remainder to $2047 = 23\cdot 89$.

Fermat was the one who rediscovered the old chinese rule with two generalizations:

Firstly, he realized that not only it is true, that the Mersenne candidates have 1 remainder to their index, but if a Mersenne candidate is a failing one like, $M_{11} = 2047 = 23\cdot 89$, then the factors have 1 remainder too: $23 = 2\cdot 11+1$, $89 = 8\cdot 11+1$.

Secondly, $M_p - 1 = 2^p - 2$ being dividable by p suggests a more general rule of $B^p - B$ being dividable by p.

Amazingly, just as the old chinese mathematicians, he also missed the 341 counter example and the self application with the 2047 counter example too. Even in the second generalization, that is $B^p - B$ having p as factor, he tacitly assumed that it can only stand for primes. Actually he never even proved his claim for primes. Later, when Leibniz gave the proof, he expressively stated that it is only true for primes. They both would have been very surprised to learn that not only 341 is a counter example for B = 2 but the hardly bigger 561 is a composite that makes $B^{561} - B$ dividable by 561 for any B. Most amazingly the proof for this is so simple that they could have grasped it at once. But then came Euler, Gauss and they missed it too!!! Fermat of course had a more basic misbelieve too, namely that all F_k are primes. As we mentioned Euler discovered that F_5 is composite but still missed the other very simple fact that all F_k are suitable exponents for base 2 and so F_5 is also a counter example to the old chinese and Fermat's and Leibniz's new mistake. I mention all this because this ignorance of the composite cases was a bit like a hypnotic spell that lingered on till the 20-th century, but I will handle it in this section before going to the last that deals with the much older discoveries of Euler and Gauss. Now about Fermat's second generalization:

Looking at the sequence of B , B^2 , B^3 , . . . powers, but regarding only their remainders to an d divider, this reminds us of our earlier remainder sequence for the n , $2n$, . . . , $(p-1)\,n$ multiples from section 1. There, the fact that all 1 , 2 , . . . , $p-1$ remainders appeared was an amazing side result to prove that 0 couldn't appear and so a prime can't divide a product of smaller numbers. Here with powers the situation is more complicated in the sense that not all remainders must appear. On the other hand the situation is simpler in the sense that at B^{p-1} always the 1 remainder appears unless p divides B and thus all remainders are 0.

Indeed, Fermat's generalization that $B^p - B$ is dividable by p means exactly that B^p has the same remainder to p as B, so by $B^p = B\ B^{p-1}$ if B has not 0 remainder to p then B^{p-1} must have 1. An occurrence of 1 of course in general, guaranties a restart of the sequence.
Clearly the remainders of $B, B^2, B^3, \ldots$ must return to an earlier value because they can only be finite many. But they don't have to restart.
I'll give an example for this and that will also show how to calculate easily the power remainders. Let $B = 22$, $d = 20$ and we'll have four sequences. The first is the B powers which automatically can be replaced by the b remainder's powers, but they still grow too fast, so we'll only multiply the last remainders in the third sequence. Finally, the fourth line just shows the resulting remainders. The bar denotes the remainders to $d = 20$.

$\overline{22}$	$\overline{22^2}$	$\overline{22^3}$	$\overline{22^4}$	$\overline{22^5}$	$\overline{22^6}$	$\overline{22^7}$	$\overline{22^8}$	$\overline{22^9}$	. . . .
2	$\overline{2^2}$	$\overline{2^3}$	$\overline{2^4}$	$\overline{2^5}$	$\overline{2^6}$	$\overline{2^7}$	$\overline{2^8}$	$\overline{2^9}$	. . . .
2	4	$\overline{4 \cdot 2}$	$\overline{8 \cdot 2}$	$\overline{16 \cdot 2}$	$\overline{12 \cdot 2}$	$\overline{4 \cdot 2}$	$\overline{8 \cdot 2}$	$\overline{16 \cdot 2}$	. . . .
2	4	8	16	12	4	8	16	12	. . . .

As we see in this example, not only the original 2 remainder never restarts but the 4 that returns will not be the remainder at 22^{20} as with prime dividers always, but much earlier at 6. The earliness itself can happen at primes too. So the big p cycle can contain smaller ones in it too. In the next section we'll get into Euler's generalization which for a general d finds a guaranteed earlier restart than d, but that won't guarantee the earliest even for primes. Such earliest restart for primes was cleared up by Gauss and we'll finish the whole subject with that.

D Choosing a B and d, the remainders of $B, B^2, B^3, \ldots$ at some k exponent must have a return to an earlier remainder. If it goes back to the beginning, then k is called a restart.
If B^{k-1} has 1 remainder then, k is called simple restart. It is obviously a restart too.
The d divider itself can be a return or restart but obviously for only B-s that are not d multiples. If it is like this for all such bases then we call it total.

T

1.) Simple restarts:
   a.) If B, d have a c common factor then c divides all remainders.
   Thus with non rel. prime B, d there can be no simple restart.
   b.) If B, d are rel. prime then all returns are simple restarts. Multiples of a first.

2.) Fermat's theorem:
   a.) Conditional form: If a p prime doesn't divide B then p is simple restart.
   b.) Unconditional form: Every p prime is total restart.

3.) Dividers of $B^p - 1$:
   The $B^p - 1$ number can have only two kinds of prime dividers:
   Firstly, all the prime dividers of $B - 1$ and some $mp + 1$.

4.) $B = 2$
   If q is the M_p Mersenne candidate or a factor of it, then:
   a.) What Fermat discovered: q is $mp + 1$.
   b.) What Fermat missed: q is simple restart.
   For M_d Mersenne non candidates:
   c.) If d is composite restart then M_d is a composite simple restart divider.
   d.) There are infinite many M_d simple restart divider non candidates.
   For Fermat numbers:
   e.) All F_k are simple restart dividers.

5.) Composite total restarts:
  a.) Korselt:
    If d has no repeated prime factors but for any p prime divider of d, $p-1$ divides $d-1$, then d is total restart.
  b.) Chernick:
    If $6k+1$, $12k+1$, $18k+1$ are all primes then their $P(k)$ product is a total restart.
  c.) 561 , 1105 , 1729 , 2465 are the first four total restarts.
  d.) For $k = 1$, 6 , 35 , 45 , 51 , 55 , 56 $P(k)$ are total restarts.

6.) Composite total simple restart:
  a.) Carmichael:
    If d is total simple restart then $d = p_1 p_2 \ldots p_k$ with $k \geq 3$ all p_i different and all $p_i - 1$ divides $d-1$.
  b.) d is total restart if and only if it is simple restart for all B relative prime to d.

P

1.) b.)

If we have a return from m to $m-k$ then d divides $B^m - B^{m-k} = B^{m-k}(B^k - 1)$, so B , d being relative primes, d divides $B^k - 1$ so k is a simple restart. If k is the minimal such then we cant have returns before k and so indeed all returns are these.

2.) We already gave two proofs one for a.) and one for b.) , at end of Ch. 6. New ones:

a.)

If p doesn't divide B then the $\overline{B}$, $\overline{2B}$, . . . , $\overline{(p-1)B}$ remainders to p are exactly the $1, 2, \ldots, p-1$ non zero remainders but in some other order. A special consequence of this is what was also our main goal there, namely that if $0 < q, r < p$ then $\overline{qr} \neq 0$.

We'll use both the remainder sequence and this consequence but combined with the obvious fact that a product's remainder can be taken by replacing the members with their remainders:

$$\overline{AB} = \overline{(mp+a)(mp+b)} = \overline{Mp+ab} = \overline{ab} = \overline{\overline{A}\,\overline{B}}$$

Using this repeatedly for more members, we at once get that if $0 < q_1, \ldots, q_k < p$ then $\overline{q_1 \ldots q_k} \neq 0$. Or as a special case $\overline{1 \cdot 2 \cdot \ldots \cdot (p-1)} = \overline{(p-1)!} \neq 0$. Of course from Wilson we know that this is $p-1$ but we don't want to use this, only the fact that it is not 0.

Now the trick is to calculate the product remainder for the full sequence in two different ways:

$$\overline{B \cdot 2B \cdot \ldots \cdot (p-1)B} = \begin{cases} \overline{B^{p-1}(p-1)!} = \overline{\overline{B^{p-1}}\;\overline{(p-1)!}} = \overline{\overline{B^{p-1}}\,r} \\ \overline{\overline{B} \cdot \overline{2B} \cdot \ldots \cdot \overline{(p-1)B}} = \overline{(p-1)!} = r \neq 0 \end{cases}$$

Thus, at once $\overline{B^{p-1}} \neq 0$, that is $\overline{B^{p-1}} \geq 1$. Then from $\overline{\overline{B^{p-1}}\,r} = r$ we get $\overline{\overline{B^{p-1}}\,r - r} = \overline{(\overline{B^{p-1}} - 1)\,r} = 0$ but $\overline{qr} \neq 0$ for $q > 0$ so $\overline{B^{p-1}} - 1 = 0$.

b.)

For $B = 1$ it's trivial. Suppose it's true up to a B and then the difference to the $B+1$ case is

$$\left((B+1)^p - (B+1)\right) - \left(B^p - B\right) = (B+1)^p - B^p - 1 = \binom{p}{1} B^{p-1} + \binom{p}{2} B^{p-2} + \ldots + \binom{p}{p-1} B$$

Every $\binom{p}{k} = \dfrac{p(p-1)\ldots(p-k+1)}{2 \cdot 3 \cdot \ldots \cdot k}$ is a whole and must have the p factor since p is a prime and so can't be divided by the factors of the denominator.

Thus, $(B+1)^p - (B+1)$ is again dividable by p.

3.)
The first kind are trivial from the inheritance of the 1 remainders from B to B^p.
The q prime dividers of $B^p - 1$, don't divide B, so we can use 2.) b.).
So they divide $B^{q-1} - 1$. For those q that don't divide $B - 1$, we can use 1.) a.) :
p must be the minimal and $q - 1$ is a multiple. Thus $q - 1 = m\,p$ and $q = m\,p + 1$.
4.) a.)
In 3.) at $B = 2$ no factor can divide $B - 1 = 1$, so all prime factors are $mp + 1$. Thus, any product of these is also $mp + 1$.
4.) b.) Trivial from 2.) b.) and a.).
4.) c.)
We already showed that only candidates can be prime, so the non candidates are all composite.
For the simple restart:

$$2^{M_d - 1} - 1 = 2^{2^d - 2} - 1 = 2^{m\,d} - 1 = (2^d)^m - 1^m = (2^d - 1)[\ ] = M_d\ [\ ]$$

4.) d.)
By c.) if d is composite restart then M_d , $M_{(M_d)}$, $M_{(M_{(M_d)})}$, . . is such sequence.

The smallest such d is $341 = 11 \cdot 31$ namely:
$2^{341-1} = 2^{340} = (2^{10})^{34} = (3 \cdot 341 + 1)^{34}$ has 1 remainder to 341.
We could also use as d, $M_{11} = 23 \cdot 89$ by b.) above or F_5 by the following e.) or the numbers in 5.) c.).
4.) e.)

$$2^{F_k - 1} - 1 = 2^{(2^{2^k} + 1) - 1} - 1 = 2^{2^{2^k}} - 1 = 2^{\left(2^{k+1}\,\frac{2^{2^k}}{2^{k+1}}\right)} - 1 =$$

$$2^{\left(2^{k+1}\,2^{[2^k - (k+1)]}\right)} - 1 = \left(2^{2^{k+1}}\right)^{2^{[2^k - (k+1)]}} - 1 \text{ so it is dividable by}$$

$2^{2^{k+1}} - 1$, which itself is $\left(2^{2^k}\right)^2 - 1$ and so is dividable by $2^{2^k} + 1 = F_k$.

5.) a.)
Lets choose a B. If a p prime divider of d divides B then it obviously divides $B^d - B$ too.
If p doesn't divide B then it doesn't divide $B^{\frac{d-1}{p-1}}$ either and so by 2.) a.) p divides
$(B^{\frac{d-1}{p-1}})^{p-1} - 1 = B^{d-1} - 1$ and so $B^d - B$ too.

Thus, all p prime dividers of d divide $B^d - B$ and so by the condition of no repeated prime factors, d itself divides $B^d - B$.

5.) b.)
$P(k) = (6k + 1)(12k + 1)(18k + 1) = 36^2 \cdot k^3 + 11 \cdot 36 \cdot k^2 + 36 \cdot k + 1$
So $P(k) - 1$ is dividable by $36k$ and so by $6k$, $12k$, $18k$ too. Thus, follows from a.).

5.) c.)
$561 = 3 \cdot 11 \cdot 17$ $\quad$ $1105 = 5 \cdot 13 \cdot 17$ $\quad$ $1729 = 7 \cdot 13 \cdot 19$ $\quad$ $2465 = 5 \cdot 17 \cdot 29$
They all satisfy Korselt's condition. Only the third is Chernick's type.

5.) d.)
$P(1) = (6+1)(12+1)(18+1) = 1729 \quad P(6) = 37 \cdot 73 \cdot 109 = 294409$
The rest of them can be verified similarly one by one.

6.) The proof of this requires more involved details depending on the next section.

R Carmichael's result that at total restarts simplicity follows for all relative prime B, d, raises the problem to give examples for particular B bases where it doesn't follow. Strangely the first example came only in 1950 by Lehmer with $B = 2$ base. Obviously in this case a restart is simple if and only if it is odd and all our examples were such.
The smallest even restart is $d = 161038$. Though it was hard to find, it's quite easy to verify:

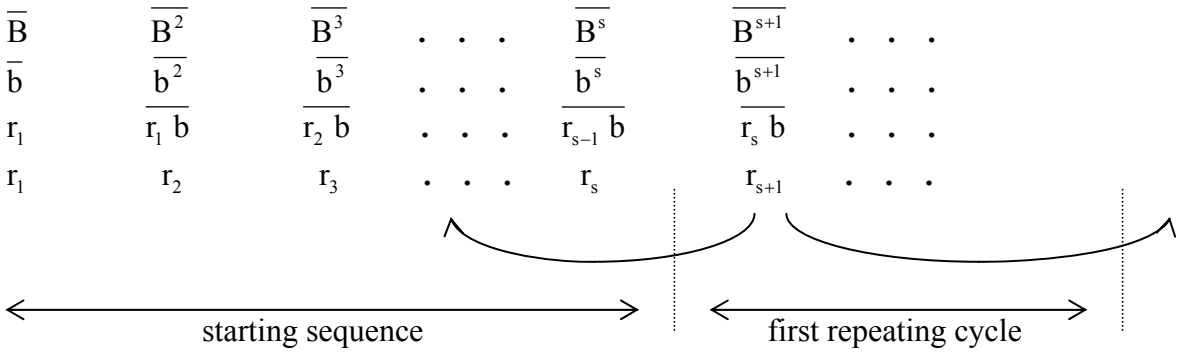
$d = 161038 = 2 \cdot 73 \cdot 1103$ while $d - 1 = 9 \cdot 29 \cdot 617$ also:
$2^9 - 1 = 7 \cdot 73$ while $2^{29} - 1 = 233 \cdot 1103 \cdot 2089$ and thus
$2^9 - 1$ divides $2^{d-1} - 1$ so 73 divides it too.
$2^{29} - 1$ divides $2^{d-1} - 1$ so 1103 divides it too.
Thus, $73 \cdot 1103$ divides $2^{d-1} - 1$ too and then of course $2 \cdot 73 \cdot 1103$ divides $2^d - 2$.

R What we called restart is usually called B-probable prime or with $B = 2$, as probable prime.
Total restarts are referred to as absolute probable primes.
When these are not primes then they are called pseudo primes.
Total simple restarts are called Carmichael numbers.
The simple restarts are also called in some books as fermatians.

12. Early restarts Euler's theorem, primitive roots, second splitting of primes

R

Our concept of restart was any k exponent at which the remainder to a d, in the sequence $B, B^2, \ldots$ is the same as of the initial B. In other words, $B^k - B$ is dividable by d.
Simplicity meant B^{k-1} having 1 remainder and thus causing k to be a restart.
The guaranteed restarts of the last section imply that restarts in general should be interesting when they are smaller than the divider, in other words when they are early.
The ultimate goal would be to find a formula for the s smallest exponent where B^s has 1 remainder to d. Unfortunately, such formula doesn't exist even for $d = p$ primes.
Our example for $d = 22$, $B = 20$ showed that restarts are not always happening.
In the general situation $r_s = \overline{B^s}$ is just the last remainder after which $r_{s+1} = \overline{B^{s+1}}$ becomes a previous value. The s could stand for "starting" because $r_1, r_2, \ldots, r_s$ is indeed the starting sequence after which a return will come.



Easy to see that such return that is not a restart can only happen if b and d are not relative primes. In fact if they are relative primes then we have simple restart. To be precise:

D

$\Phi(d)$:= set of smaller than d natural numbers that are relative primes to d.
$\varphi(d)$:= number of numbers in $\Phi(d)$.

T

If $b \in \Phi(d)$ then:

1.) $\overline{r\, b} = \overline{s\, b} \rightarrow r = s$ where r, s are two remainders.

2.) $b, \overline{b^2}, \overline{b^3}, \ldots$ must re-occur with b, so $\overline{b^{s+1}} = b$, that is we have restart.

3.) The last element of the starting sequence $\overline{b^s}$ is 1. That is, the restart is simple too.

4.) If $m, M \in \Phi(d)$ then, $\overline{m\, b}, \overline{m\, b^2}, \ldots, \overline{m\, b^s}$ and $\overline{M\, b}, \overline{M\, b^2}, \ldots, \overline{M\, b^s}$:
   a.) both contain only elements from $\Phi(d)$.
   b.) both contain all different elements.
   c.) if have a common element then the previous and next in them are also common.
   d.) so they are either totally different or just recycling of each other.

5.) The different possible $\overline{m\, b}, \overline{m\, b^2}, \ldots, \overline{m\, b^s}$ subsets of $\Phi(d)$ are:
   a.) disjoint and all have s many elements.
   b.) together contain every r element of $\Phi(d)$ because $r = \overline{r\, b^s}$.
   c.) thus, s divides $\varphi(d)$, that is $\varphi(d) = m\, s$.
   d.) in particular, if $b > 1$ then s is $\varphi(d)$ or a factor of it.

6.) $\overline{b^{\varphi(d)}} = \overline{b^{ms}} = \overline{\overline{b^{s}}^{m}} = 1$

P All steps follow from the previous ones.

T Generalizations of Fermat's theorem

1.) Conditional form or Euler's theorem:

If B, d are relative primes then $\overline{B^{\varphi(d)}} = 1$, that is d divides $B^{\varphi(d)} - 1$.

2.) Unconditional form or Rédei's theorem:

$\overline{B^{d}} = \overline{B^{d-\varphi(d)}}$, that is d divides $B^{d} - B^{d-\varphi(d)} = B^{d-\varphi(d)}\,(B^{\varphi(d)} - 1)$.

P 1.) Let $\overline{B} = b$ then $\overline{B^{m}} = \overline{\overline{B}^{m}} = \overline{b^{m}}$. If further more B, d are relative primes then $b \in \Phi(d)$, so by 6.) of previous theorem $\overline{B^{\varphi(d)}} = \overline{b^{\varphi(d)}} = 1$.

2.) To get Euler from Rédei: B, d being relative primes means that B has no prime divider that divides d, thus $B^{d-\varphi(d)}$ has neither and so the full d must divide $B^{\varphi(d)} - 1$.
Now let $d = {p_1}^{e_1} \cdot \cdot \cdot {p_k}^{e_k}$. If p_i doesn't divide B, that is ${p_i}^{e_i}$ is a relative prime to B then by Euler ${p_i}^{e_i}$ divides $B^{\varphi(d)} - 1$. If p_i does divide B, lets observe that p_i, ${p_i}^{2}$, . . . , ${p_i}^{e_i}$ are all elements outside $\Phi(d)$ so $e_i \le d - \varphi(d)$ and so ${p_i}^{e_i}$ divides ${p_i}^{d-\varphi(d)}$ and thus also $B^{d-\varphi(d)}$.
So the relative prime ${p_1}^{e_1}$, . . , ${p_k}^{e_k}$ factors each divide $B^{d-\varphi(d)}$ or $B^{\varphi(d)} - 1$, so their product d divides the product of this two, as Rédei claims.

R Since for a p prime $\Phi(p) = \{1, 2, \ldots, p-1\}$ and $\varphi(p) = p - 1$, thus here Euler leads back to Fermat's conditional form while Rédei to the unconditional form.
There are two accepted names that express the starting sequence and the special full starting sequences:

D 1.) The s starting sequence length, that is the smallest exponent for which $\overline{b^{s}} = 1$ is called the <u>order of b to d.</u>

2.) If the starting sequence is full, that is b, $\overline{b^{2}}$, . . . , $\overline{b^{s}}$ is $\Phi(d)$ that is, the order of b is $s = \varphi(d)$ then b is called a <u>primitive root of d.</u>

R The two obvious line of question are:

1.) For what d do we have full starting sequence, that is primitive root?
What are these then? How many are there?

2.) If b is not a primitive root of d then what earlier simple restart can be given than $\varphi(d)$?
That is, can we find an $f(d) < \varphi(d)$ so that $\overline{b^{f(d)}} = 1$?
$s(d)$ would be the best but as we said it's too difficult.

We'll only answer most of these for $d = p$ prime so we might wonder why didn't we handle them in the previous section? Well, because we need the above theorem even for primes.
In fact, the only easy answers for non primes are to the second and third questions in 1.).
More exactly: If we have one primitive root of d, then telling all of them and how many are there, is easy:

T

1.) If b is a primitive root of d, then an r is also one if and only if:
$r = \overline{b^k}$ with k relative prime to $\varphi(d)$.
2.) If there is primitive root of d then there are exactly $\varphi(\varphi(d))$ many.

P

1.)
An r primitive root of d can only be a relative prime remainder to d and all these are some $\overline{b^k}$ because b is primitive root so b, $\overline{b^2}$, . . . , $\overline{b^{\varphi(d)}}$ is the full $\Phi(d)$.
If k and $\varphi(d)$ have a c common divider, that is $k = m\,c$, $\varphi(d) = M\,c$ then
$\overline{r^M} = \overline{\overline{b^k}^M} = \overline{(b^{m\,c})^M} = \overline{(b^{M\,c})^m} = \overline{\overline{b^{\varphi(d)}}^m} = 1$
If $c > 1$ and thus $M < \varphi(d)$ were, then M were an earlier simple restart than $\varphi(d)$, that is $\varphi(d)$ were not the order of b^k, so $\overline{b^k}$ were not primitive root of d.
Now we have to show that on the other hand all k without such common divider will do.
That is $(b^k)^s = 1$ with the smallest s happens at $s = \varphi(d)$.
$\overline{(b^k)^s} = \overline{b^{k\,s}} = 1$ implies that $k\,s$ is a multiple of b's starting exponent, that is $\varphi(d)$.
But if k is a relative prime to $\varphi(d)$ then this means that s is a multiple of $\varphi(d)$.
Then of course the only possibility is $s = \varphi(d)$ to make it minimal.
2.) Trivial by 1.).

R

Now we'll prove that there is primitive root for any p prime. The proof is a reenactment of the theorem on the number of primitive roots above, but with crucial differences.
We'll also need some new facts about the remainder roots, that involves polynoms:

T

1.) $\overline{\sqrt[n]{R}}$ has at most n elements.
2.) If n divides $p - 1$ then $\overline{\sqrt[n]{1}}$ has exactly n elements.

P

1.)
Unfortunately, to see this we have to look at the more general:
$x^n \pm R_{n-1}\,x^{n-1} \pm \ldots \pm R_1\,x \pm R_0$ polynoms. Such can be easily divided by an $(x - q)$ with a similar division process as for numbers and leaving a possible Q remainder. So:
$x^n \pm R_{n-1}\,x^{n-1} \pm \ldots \pm R_1\,x \pm R_0 = (x-q)(x^{n-1} \pm r_{n-2}\,x^{n-2} \pm \ldots \pm R_0) + Q$.
Now if q is root of the original polynom in remainder sense, that is:
$\overline{q^n \pm R_{n-1}\,q^{n-1} \pm \ldots \pm R_1\,q \pm R_0} = 0$ then this implies that on the right $Q = 0$ because writing q in x the first factor becomes 0. So if q is such root then:
$x^n \pm R_{n-1}\,x^{n-1} \pm \ldots \pm R_1\,x \pm R_0 = (x-q)(x^{n-1} \pm r_{n-2}\,x^{n-2} \pm \ldots \pm r_0)$.
This then implies that if the right side r-polynom had maximum $n - 1$ many roots then, the left R-polynom can have only n many roots, namely the previous $n - 1$ many and q.
Thus we get an induction because the $n = 1$ case is trivial since $x \pm R_0$ has only one root.
Then as a special case $x^n - R$ can also have maximum n many roots. Thus $\overline{x^n} = R$ too.
2.)
$x^{p-1} - 1 = (x^n - 1)(x^{p-1-n} + x^{p-1-2n} + \ldots + x^n + 1)$.
By Fermat $1, 2, \ldots, p - 1$ are all roots of the left side, thus $p - 1$ many in total.
By 2.) $x^n - 1$ has maximum n many and by its proof, the other factor, maximum $p-1-n$ many roots. But $p - 1 = n + (p-1-n)$ so these factors must have this maximal many roots.

T

1.)

If s divides $p-1$ and b, r both have order s then $r = \overline{b^k}$ with k relative prime to $\varphi(s)$

2.)

If $\psi(s)$ denotes the number of remainders that have order s for an s divider of $p-1$ then $\psi(s) \le \varphi(s)$.

3.)

The sum of all $\psi(s)$ for the s dividers of $p-1$ is $p-1$. In short: $\sum_{s|p-1} \psi(s) = p-1$

4.) $\sum_{d|n} \varphi(d) = n$ in general.

5.) $\psi(s) = \varphi(s)$ For all s dividers of $p-1$. In particular $\psi(p-1) = \varphi(p-1)$, that is: There are $\varphi(p-1)$ many primitive roots of p.

P

1.)

By 2.) of previous theorem $\overline{\sqrt[s]{1}}$ has s many elements.

$b, \overline{b^2}, \ldots, \overline{b^s}$ are all elements because $\overline{(b^k)^s} = \overline{(b^s)^k} = \overline{(\overline{b^s})^k} = 1$.

Since b has order s these are all different, so they are exactly the set $\overline{\sqrt[s]{1}}$.

But r is element of this too, and so $r = \overline{b^k}$.

If k and s had a $c \neq 1$ common divider then already $\frac{s}{c}$ were a simple restart:

$\overline{r^{\frac{s}{c}}} = \overline{(\overline{b^k})^{\frac{s}{c}}} = \overline{(b^k)^{\frac{s}{c}}} = \overline{(b^{mc})^{\frac{s}{c}}} = \overline{(b^m)^s} = \overline{(b^s)^m} = \overline{(\overline{b^s})^m} = 1$.

2.)

Each r that has order s, is a different $\overline{b^k}$ with k relative prime to s.
So these k-s are a subset of $\Phi(s)$ and thus their number is $\le \varphi(s)$.

3.)

Every number from $1, 2, \ldots, p-1$ has one unique order.

4.)

Let n_d denote the set of those numbers up to n, that have d as their greatest common divider with n and let $|n_d|$ be their number. Then $\sum_{d|n} |n_d| = n$ is trivial because every number up to n has one unique greatest common divider with n. But $|n_d| = \varphi(\frac{n}{d})$ because n_d contains those $m\,d$ multiples for which m is relative prime to $\frac{n}{d}$. So $\sum_{d|n} \varphi(\frac{n}{d}) = n$.

Finally, this sum is the same as we claimed because the list of dividers is the same as the $\frac{n}{d}$-s.

5.)

By 2.) it's enough to show that $\psi(s) < \varphi(s)$ is impossible if s divides $p-1$.
If it were for an $s \mid p-1$ then $\sum_{s|p-1} \psi(s) < \sum_{s|p-1} \varphi(s)$ would be too
but by 3.) the left is $p-1$ and by 4.) the right is $p-1$ too, contradicting $<$.

R

Gauss showed that the numbers that have primitive roots, are: 2, 4, p^k or $2p^k$ with $p > 2$.
As we saw, to get the full set of primitive roots from one, is fairly easy. To find a crucial one, we have to use prime tables that contain this data. For special cases there can be formulas that give a definite primitive root, as we see soon.
Euler's theorem was the obvious generalization of Fermat's theorem.
Euler criterion mentioned in Chapter 10 is more like a sharpening of Fermat's theorem.
A third direction of sharpening could be to find a reversible form of Fermat's theorem.

The last section's wide variety of composite restarts showed that direct reversibility is not true, but now with our result that primes have primitive roots, there is a quite obvious way to get around. Euler was probably well aware of this third way too but since he didn't prove the existence of primitive roots even for primes, he didn't explicitly stated it. In fact, this was only done by Lucas in 1887 because he realized that more importantly this reversible form is the basis of a prime testing criteria.
The logical idea is to claim that if d is a restart but there are no earlier restarts, then d must be a prime. This is a very imprecise statement yet, because we didn't specify the B base. And indeed, the primes are B-restarts for all B but we also know that prime dividers can have early restarts for some B. So the only thing we can hope is that some B will lead to no early restart. Indeed, this is what primitive roots of a prime guarantee. Of course, it's enough to test the $b < d$ bases and if d is a prime then a primitive root b with $d-1$ earlier simple restart will be encountered. So both the b bases and their exponents must be tested but luckily at least the exponents only have to be checked for factors of $d-1$ and these might be known from other considerations.

T

1.) If B^{d-1} has 1 remainder to the composite d, that is d is a composite simple B-restart, then for some f factor of $d-1$, B^f has 1 remainder already, that is there is early simple restart at a factor of $d-1$.

2.) For any p prime there is such $b < p$ that no b^m has 1 remainder to p for $m < p-1$.

3.) Lucas basic prime criteria: d = prime if and only if for some $b < d$:
b^{d-1} has 1 remainder to d, but b^F has never, with $F = \frac{d-1}{p}$, where p is a prime factor of $d-1$.

P

1.) B must be relative prime to d so by Euler's theorem there is a smallest s so that B^s has 1 remainder and all other such exponents are multiples of s including $d-1$. Thus s is such f.
2.) Such b means that it's a primitive root and we showed that there is such for p primes.
3.) For a prime, the criteria is obviously true by Fermat and 2.)
For a non prime, by 1.) we only have to show that no f factors of $d-1$ as exponents can give 1 remainders in general. If an f exponent gives 1 then its multiples do too. Going up to $d-1$ is useless because we already know this for $d-1$. But going one factor less means that $d-1$ divided by some prime factor must be a power giving 1 too. So if we know this is impossible for all prime factors then this refutes all f too.

R

By Euler's theorem the s order of $b > 1$ divides $\varphi(d)$ or in case of prime, $p-1$.

$p-1$ is even so 2 is a definite factor and thus so is $\frac{p-1}{2}$ too. So the minimal possibility is if $\frac{p-1}{2}$ is also a prime because then clearly there are no other factors of $p-1$.

T

For a p prime with $\frac{p-1}{2}$ also being a prime:

1.) If $b > 1$ and $\overline{b^2}$, $\overline{b^{\frac{p-1}{2}}}$ are not 1, then b is a primitive root of p.

2.) If $\overline{2^{\frac{p-1}{2}}} \neq 1$, that is $= p-1$ then 2 is a primitive root of p.

P

1.) Clearly $p-1$ itself is the only divider that leads to 1 remainder so it is the order of b, that is b is primitive root of p.

2.) 1.) implies it with $b=2$ because: $\overline{b^2} = \overline{2^2} = \overline{4} = 4 \neq 1$.

R

For $p=5$: $\frac{5-1}{2} = 2$ is prime and $\overline{2^2} = 4$ so 2 is primitive root of 5.

For $p=7$: $\frac{7-1}{2} = 3$ is prime but $\overline{2^3} = \overline{8} = 1$ so the criteria is not useable.

For $p=11$: $\frac{11-1}{2} = 5$ is prime and $\overline{2^5} = \overline{32} = 10$ so 2 is primitive root of 11.

For $p=13$: $\frac{13-1}{2} = 6$ is not prime so the criteria is not usable again.

$p=59$ is the first usable again, so 2 is primitive root of 59.

As we see, this is not a practical method. It would be nicer to know exactly when $\overline{2^{\frac{p-1}{2}}} = 1$.

T

Second splitting of primes

1.) $\overline{2^{\frac{p-1}{2}}} = 1$ if and only if $p = 8k \pm 1$ so $\overline{2^{\frac{p-1}{2}}} = p-1$ if and only if $p = 8k \pm 3$.

2.) 2 is square rootable if and only if $p = 8k \pm 1$.

3.) If $\frac{p-1}{2}$ is also prime then 2 is a primitive root of p if and only if $p = 8k \pm 3$.

P

We only show their relationship:

1.) $\Leftrightarrow$ 2.) by Euler criterion.

1.) $\Rightarrow$ 3.) by previous 2.).

R

Previous 2.) clearly relates to Mersenne and Fermat numbers.

As we already know, all factors of the $M_p = 2^p - 1$ Mersenne candidates are $mp + 1$.

Of course, here m must be even because M_p is odd so can't have even factor either.

Also, if $2p + 1$ is factor, then it is the smallest and so it is a prime.

For $p = 4k - 1$ primes, that is for half of the primes the reverse of this is true and thus we get a powerful way to show failing Mersenne candidates.

Now for the Fermat numbers, as we also told, F_5 was discovered to be composite by Euler. He didn't just guess that 641 is a factor, he had a very good clue because he knew what type of numbers can be factors at all. This is the second part of our next, last theorem:

T

1.) If $p = 4k - 1$ prime and $P = 2p + 1$ is also prime then it is a factor of $M_p = 2^p - 1$.

2.) Every divider of $F_k = 2^{2^k} + 1$ is $m \cdot 2^{k+2} + 1$.

P

1.) $P = 2p + 1 = 2(4k - 1) + 1 = 8k - 1$ so by previous 1.) $2^{\frac{P-1}{2}}$ has 1 remainder to P.

Thus, $M_p = 2^p - 1 = 2^{\frac{P-1}{2}} - 1$ is dividable by P.

P can't be 1 nor M_p if $p > 2$ so it is a factor of M_p.

2.) Let p be a prime divider of $2^{2^k} + 1$, then

$\left(2^{2^k}\right)^2 - 1 = \left(2^{2^k} + 1\right)\left(2^{2^k} - 1\right) = Mp$ so

$\left(2^{2^k}\right)^2 = 2^{2 \cdot 2^k}$ has 1 remainder to p.

In fact, $2 \cdot 2^k$ is the order of 2.

Indeed, if it weren't then a factor of it were but that were a divider of 2^k and so 2^{2^k} would also have 1 remainder to p, contradicting that p divides $2^{2^k} + 1$.

So $2 \cdot 2^k$ divides all other exponents that give 1 remainder, including $p - 1$.

For $k > 1$ this implies that $p = 8k + 1$, so by previous 1.), $2^{\frac{p-1}{2}}$ gives 1 remainder and so $2 \cdot 2^k$ divides $\frac{p-1}{2}$ too. Thus, $\frac{p-1}{2} = m \cdot 2 \cdot 2^k$ so $p = m \cdot 2^{k+2} + 1$

For other non prime dividers it follows by regarding the product of primes.

13. Factor sieving Calculating φ

R

In **2. Infinity of Primes**, we used sieving to define the n* next prime. There, by sieving we meant crossing out all numbers that are multiples of an n or smaller number. A smarter way is not to look at all the smaller numbers only the factors of n. In other words, we cross out all numbers that are multiples of n or have common factor with n. In negative form this means to keep all relative primes to n.
Later, we even introduced $\Phi(n)$ for the set of all smaller relative primes to n and $\varphi(n)$ for the number of these. This was needed for Euler's theorem but we didn't go into how $\varphi(n)$ is behaving. Now we re-define these in a more general way, not just looking the smaller than n numbers but up to an N.

D

1.)
k is n-factor sieved if it's a non 1 divider of n, or a multiple of such.
That is, $k = m\,j$ with $j \neq 1$ dividing n. Observe that if n is prime then the n-factor sieved numbers are not "sieved" by a factor of n since it has none. Still, these numbers all except n itself have factor that divides n, so the name is still fairly acceptable.

2.)
$\overline{\Phi}(n, N)$ **:=** set of n-factor sieved numbers up to N. Example: $\overline{\Phi}(4, 6) = \{2, 4, 6\}$.
$\overline{\Phi}(n) = \overline{\Phi}(n, n)$ Example: $\overline{\Phi}(6) = \{2, 3, 4, 6\}$

3.)
$\Phi(n, N)$ **:=** set of numbers up to N not in $\overline{\Phi}(n, N)$. Example: $\Phi(4, 6) = \{1, 3, 5\}$
$\Phi(n) = \Phi(n, n)$ Example: $\Phi(6) = \{1, 5\}$
Clearly $\Phi(n, N)$ is the relative primes to n up to N and $\Phi(n)$ is the relative primes to n.

4.)
$\varphi(n, N)$ **:=** number of elements in $\Phi(n, N)$. $\varphi(n)$ **:=** number of elements in $\Phi(n)$.

5.)
$\prod(n, N)$ **:=** set of primes from after n up to N. $\prod(N)$ **:=** $\prod(1, N)$
$\pi(n, N)$ **:=** number of elements in $\prod(n, N)$. $\pi(N)$ **:=** number or elements in $\prod(N)$

6.)
$\{x + \overline{\Phi}(n)\}$ **:=** set of numbers: $x + k_1, x + k_2, \ldots$ with $k_i \in \overline{\Phi}(n)$.
In other words, it is $\overline{\Phi}(n)$ shifted up with x.

T

1.) $\{m\,n + \overline{\Phi}(n)\}$ contains no primes.

2.) $\prod\big(m\,n, (m+1)\,n\big) \subseteq \{m\,n+1, m\,n+2, \ldots, m\,n+n\} - \{m\,n + \overline{\Phi}(n)\}$

3.) $\pi\big(m\,n, (m+1)\,n\big) \leq \varphi(n)$

4.) $\pi(N) \leq \left(\left[\frac{N}{n}\right] + 1\right)\varphi(n) \leq \frac{N}{n}\varphi(n) + \varphi(n)$

P

1.) Every element is $m\,n + d$, with $d \neq 1$ and d dividing n, so d divides the element too.

2.) Trivial by 1.).

3.) $\overline{\Phi}(n)$ has $n - \varphi(n)$ many elements, so $\{m\,n + \overline{\Phi}(n)\}$ has also.
$\{m\,n + 1\ ,\ .\ .\ .\ ,\ m\,n + n\}$ has n elements.
Thus, their difference has $n - (n - \varphi(n)) = \varphi(n)$ many elements and so by 2.), $\prod\left(m\,n\ ,\ (m+1)\,n\right)$ has no more than this.

4.) $$\pi(N) = \underset{\varphi(n)}{\pi(1,n)} + \underset{\varphi(n)}{\pi(n\ ,\ 2n)} + \underset{\varphi(n)}{\pi(2n\ ,\ 3n)} + \ .\ .\ .\ . + \underset{\pi\left(\left[\frac{N}{n}\right] n\ ,\ \left(\left[\frac{N}{n}\right]+1\right) n\right)}{\pi\left(\left[\frac{N}{n}\right] n\ ,\ N\right)}$$

D

1.) $\{x \bullet \Phi(n\ ,\ N)\}$:= set of numbers: $x\ k_1\ ,\ x\ k_2\ ,\ .\ .\ .$ with $k_i \in \Phi(n\ ,\ N)$.

T

1.) If the p prime is factor of n, then $\Phi(p\,n\ ,\ N) = \Phi(n\ ,\ N)$, $\varphi\ (p\,n\ ,\ N) = \varphi\ (n\ ,\ N)$.

2.) If the p prime is not factor of n, then:

$$\overline{\Phi}(p\,n\ ,\ N) = \overline{\Phi}(n\ ,\ N) \cup \left\{p \bullet \Phi\left(n\ ,\left[\frac{N}{p}\right]\right)\right\}$$

$$\Phi(p\,n\ ,\ N) = \Phi\ (n\ ,\ N) - \ \_\ ,\ ,\ \_$$

$$\varphi\ (p\,n\ ,\ N) = \varphi\ (n\ ,\ N) - \varphi\left(n\ ,\left[\frac{N}{p}\right]\right)$$

3.) If the $p_1\ ,\ p_2\ ,\ .\ .\ .\ ,\ p_k$ primes are all factors of N, then

$$\varphi\,(p_1\ .\ .\ .\ p_k\ ,\ N) = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ .\ .\ \left(1-\frac{1}{p_k}\right).$$

4.) Φ - φ reciprocity paradox:
Let $p_1\ ,\ .\ .\ .\ ,\ p_k$ be the prime factors of N and
$q_1\ ,\ .\ .\ .\ ,\ q_m$ the primes smaller than N that are not factors of N. Then,

a.) $\Phi(N)$ depends on $q_1\ ,\ .\ .\ .\ ,\ q_m$, namely:

$$\Phi(N) = \left\{m\ ;\ m = {q_1}^{\beta_1}\ .\ .\ .\ {q_m}^{\beta_m} \leq N\ ,\ \beta_1\ ,\ .\ .\ .\ ,\beta_m = 0,1,2,\ .\ .\ .\right\}.$$

b.) $\varphi(N)$ depends on $p_1\ ,\ .\ .\ .\ ,\ p_k$, namely:

$$\varphi(N) = N\left(1-\frac{1}{p_1}\right)\ .\ .\ \left(1-\frac{1}{p_k}\right).$$

P

1.) Trivial because n and $p\,n$ have the same factors.

2.)
If p is not factor of n, then the $\Phi\ (n\ ,\ N)$ elements multiplied by p are new factors of $p\,n$.
For example: $\overline{\Phi}\,(4\ ,\ 20)\ =\ \{2\ ,\ 4\ ,\ 6\ ,\ 8\ ,\ 10\ ,\ 12\ ,\ 14\ ,\ 16\ ,\ 18\ ,\ 20\}$.
Then $p = 3$ is not factor of 4 and indeed: $3\ \Phi\,(4\ ,\ 20)\ =\ 3\ \{1\ ,\ 3\ ,\ 5\ ,\ 7\ ,\ .\ .\ .\}\ =$
$\{3\ ,\ 9\ ,\ 15\ ,\ .\ .\ .\}$ are all new factors of $3\cdot 4$, or multiples of such.
Of course, only up to $\left[\frac{N}{p}\right] = \left[\frac{20}{3}\right] = 6$ should we go, that is $1\ ,\ 3\ ,\ 5\ ,$ yielding $\{3\ ,\ 9\ ,\ 15\}$.
So, $\overline{\Phi}\,(12\ ,\ 20)\ =\ \Phi\,(4\ ,\ 20)\ \cup\ 3\ \Phi\,(4\ ,\ 6)$. The other two equations follow from the first.

3.)
For $k = 1$, $\varphi\,(p\ ,\ N)\ =\ N - \frac{N}{p_1}\ =\ N\left(1 - \frac{1}{p_1}\right)$.
Suppose it's true up to $k - 1$ and then using φ from 2.) $\varphi\,(p_1\ .\ .\ .\ p_k\ ,\ N)\ =$
$\varphi\ (p_k\ (p_1\ .\ .\ .\ p_{k-1})\ ,\ N)\ =\ \varphi\,(p_1\ .\ .\ .\ p_{k-1}\ ,\ N)\ -\ \varphi\,(p_1\ .\ .\ .\ p_{k-1}\ ,\ \left[\frac{N}{p_k}\right])\ =$

$$N\left(1 - \frac{1}{p_1}\right)\ .\ .\ .\ \left(1 - \frac{1}{p_{k-1}}\right)\ -\ \frac{N}{p_k}\left(1 - \frac{1}{p_1}\right)\ .\ .\ .\ \left(1 - \frac{1}{p_{k-1}}\right)\ =\ N\left(1 - \frac{1}{p_1}\right)\ .\ .\ .\ \left(1 - \frac{1}{p_k}\right).$$

Observe that the Unique Prime Factorization Theorem was used tacitly by assuming that $p_1\ .\ .\ .\ p_{k-1}$ is not multiple of p_k, which was a condition for using 2.).

4.) a.) Trivial.
b.) By 1.) $\varphi\,(N)\ =\ \varphi\,(N\ ,\ N)\ =\ \varphi\,(p_1\ .\ .\ .\ p_k\ ,\ N)$ and then follows from 3.).

14. Limits The four levels

T

1.) $\varphi(N) \to \infty$, namely: If N is odd or dividable by 4, then $\varphi(N) > \sqrt{N}$.
If N has only one 2 factor, then $\varphi(N) > \sqrt{\frac{N}{2}}$.

2.) $\frac{\varphi(N)}{N}$ is between 0 and 1 for all N.

3.) $\frac{\varphi(N)}{N}$ gets arbitrary close to 1, namely: If p is a prime $> \frac{1}{\varepsilon}$, then $\frac{\varphi(p)}{p} > 1 - \varepsilon$

4.) $\frac{\varphi(N)}{N}$ gets arbitrary close to 0, namely: If p is a prime, so that:
$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{p} > \frac{1}{\varepsilon}$, then $\frac{\varphi(2\cdot3\cdot5\cdot7\cdot11\cdot\ldots p)}{2\cdot3\cdot5\cdot7\cdot11\cdot\ldots p} < \varepsilon$.

5.) $\frac{\pi(N)}{N} \to 0$.

6.) $\frac{p_n}{n} \to \infty$.

P

1.)

If N is odd, that is all prime factors $p_i > 2$, then for these: $p_i - 1 > \sqrt{p_i} = p_i^{\frac{1}{2}}$ and so:

$$\varphi(N) = N\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right) = p_1^{\alpha_1}\ldots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right) =$$

$$p_1^{\alpha_1}\frac{p_1-1}{p_1}\ldots p_k^{\alpha_k}\frac{p_k-1}{p_k} = p_1^{\alpha_1-1}(p_1-1)\ldots p_k^{\alpha_k-1}(p_k-1) >$$

$$p_1^{\alpha_1-\frac{1}{2}}\ldots p_k^{\alpha_k-\frac{1}{2}} \geq p_1^{\frac{\alpha_1}{2}}\ldots p_k^{\frac{\alpha_k}{2}} = \sqrt{N}.$$

If N is dividable by 4, that is $p_1 = 2$ and $\alpha_1 \geq 2$, then $\varphi(N) =$

$$2^{\alpha_1-1}(2-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1) \geq 2^{\frac{\alpha_1}{2}}\,p_2^{\frac{\alpha_2}{2}}\ldots p_k^{\frac{\alpha_k}{2}} = \sqrt{N}.$$

If $p_1 = 2$ and $\alpha_1 = 1$, then $\varphi(N) =$

$$2^0(2-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1) > p_2^{\frac{\alpha_2}{2}}\ldots p_k^{\frac{\alpha_k}{2}} = \sqrt{\frac{N}{2}}.$$

2.) Obvious by the meaning or the calculation of $\varphi(N)$.

3.) $\frac{\varphi(p)}{p} = 1 - \frac{1}{p} > 1 - \frac{1}{\frac{1}{\varepsilon}} = 1 - \varepsilon$.

4.)

First of all, there is such p, because $\sum \frac{1}{n} = \infty$ and there are infinite many primes.

$$\frac{\varphi(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot \ldots p)}{2\cdot 3\cdot 5\cdot 7\cdot 11\cdot \ldots p} = (1-\frac{1}{2})\ (1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7})(1-\frac{1}{11})\ \ldots\ (1-\frac{1}{p}) =$$

$$\frac{1}{1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots} + \frac{1}{1+\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+\ldots} + \ldots + \frac{1}{1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\ldots} =$$

$$\frac{1}{1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots+\frac{1}{p-1}+\frac{1}{p}+\ldots} < \frac{1}{\frac{1}{\varepsilon}} = \varepsilon .$$

Observe that up to $\frac{1}{p}$, all reciprocals appear in this denominator because every number up to p is prime product of smaller primes.

5.)

From the previous section, $\pi(N) \le \frac{N}{n}\varphi(n) + \varphi(n)$ and so $\frac{\pi(N)}{N} \le \frac{\varphi(n)}{n} + \frac{\varphi(n)}{N}$.

Choosing for n, the primes of 4.), N can increase, so that $\frac{\varphi(n)}{n}$ and $\frac{\varphi(n)}{N}$ both $\to 0$.

6.)

Choose N to be the p_n prime sequence function in 5.). Then: $\frac{\pi(p_n)}{p_n} = \frac{n}{p_n} \to 0$.

R The meaning of 5.) and 6.) seems quite obvious.

$\frac{\pi(N)}{N} \to 0$ means that the number of primes is increasing very slowly.

$\frac{p_n}{n} \to \infty$ means that the n-th prime is increasing very fast.

On page 13 we saw experimentally that the $\pi_2(N)$ number of twin primes is much more than the number of squares, that is: $\frac{\pi_2(N)}{\sqrt{N}} \to \infty$. So obviously, $\frac{\pi(N)}{\sqrt{N}} \to \infty$ too.

Then with $N = p_n$ again $\frac{n}{\sqrt{p_n}} \to \infty$ and so, $\frac{n^2}{p_n} \to \infty$ too, or $\frac{p_n}{n^2} \to 0$.

So in short: $\pi(n)$ grows much slower than n but much faster than $\sqrt{n}$.

p_n grows much faster than n but much slower than n^2. In even shorter forms:

$$\sqrt{n} << \pi(n) << n \qquad \text{and} \qquad n << p_n << n^2 .$$

The obvious question is whether there are two functions, one between $\sqrt{n}$ and n and one between n and n^2, that are growing exactly as $\pi(n)$ and p_n? This question is meaningless in this form, because obviously there are such, namely $\pi(n)$ and p_n themselves. Of course, what we meant was functions calculable from n. But then still the "growing exactly" remains to be specified.

There are four levels of approximating an empirical function, like $\pi(n)$ with an $f(n)$.
The perfect solution is if $\pi(n) - f(n) \to 0$. This is abbreviated as: $\pi(n) \approx f(n)$.
This of course, is impossible if the functions have whole values, as in our case.
The next best thing is if $\pi(n) - f(n)$ doesn't tend to 0, but still remains under a finite value.
Since, $\pi(n)$ itself goes to infinity, this would be still a very good approximation.
We had such "bounded" approximation for the $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$ sum, namely as $\log n$.

Indeed: $\frac{1}{2} + \frac{1}{3} + \ldots < \log n < 1 + \frac{1}{2} + \frac{1}{3} + \ldots$ so $\log n - (\frac{1}{2} + \frac{1}{3} + \ldots) < 1$.

$\pi(n)$ changes very erratically, as we know from the huge composite blocks and reoccurring twin primes, so to expect such approximation for $\pi(n)$ is still too much!
The next two approximation levels are relative forms of the previous two. This means that instead of the $\pi(n) - f(n)$ difference, we regard the relative size of this difference compared

with the $\pi(n)$ value. That is, we look at $\frac{\pi(n) - f(n)}{\pi(n)} = 1 - \frac{f(n)}{\pi(n)}$.

This then can again actually tend to 0 or just be bounded by a finite value.
If it tends to 0, it is the same as $\frac{f(n)}{\pi(n)} \to 1$, which is abbreviated as: $\pi(n) \sim f(n)$.

We feel that $\pi(n) \approx f(n)$, $\pi(n) - f(n) < B$, $\pi(n) \sim f(n)$ and $\frac{\pi(n) - f(n)}{\pi(n)} < B$ are four weakening levels of approximations. But that's not true in general! For example, if $\pi(n) \to 0$ then any $f(n) \to 0$ will provide a $\approx$ approximation, but not necessarily a $\sim$ one. On the other hand, if $\pi(n)$ is increasing, like in our case, then indeed, the four levels are weakening.
As we said, to find a $\approx$ approximation for $\pi(n)$ is impossible. If however, we create from $\pi(n)$ a "smoothened" function, then we can find a $\approx$ for that and from that a $\sim$ for $\pi(n)$.
Such smoothening is quite logical as $\frac{\pi(n)}{n}$ or its reciprocal $\frac{n}{\pi(n)}$. The first is the frequency of primes up to n and as n grows it's quite plausible that this frequency approaches an ideal probability function. The second is the average jump or gap between primes up to an n.
As it turned out: $\frac{n}{\pi(n)} \approx \log n - 1$

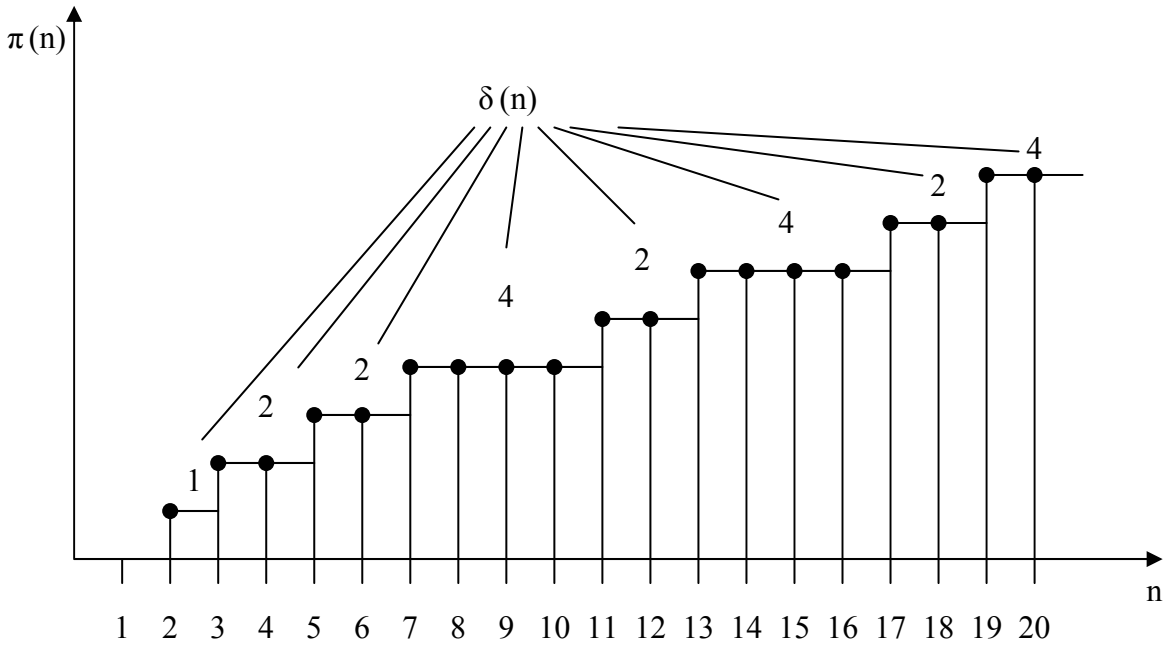
Thus of course, $\frac{n}{\pi(n)} \sim \log n - 1$ is also true, that is: $\frac{\frac{n}{\pi(n)}}{\log n - 1} \to 1$, which implies that:

$\frac{\frac{n}{\pi(n)}}{\log n} = \frac{\frac{n}{\log n}}{\pi(n)} \to 1$, that is $\pi(n) \sim \frac{n}{\log n}$. So indeed, we easily obtained a $\sim$ approximation for $\pi(n)$. Of course, if above we had instead of $\log n - 1$ any $\log n \pm c$, it would still imply the same $\sim$ approach for $\pi(n)$. This is especially interesting because the historical road to the $\approx \log n - 1$ ideal approach was in some sense reversed. This means that though mathematicians tried to guess $\frac{n}{\pi(n)}$, they also realized that to <u>prove</u> it, would require to prove the $\pi(n) \sim \frac{n}{\log n}$ consequence first. As it turned out this consequence was the real hard part and Hadamar and Poussin only succeeded at the end of the 19th century. Then, the already guessed $\approx \log n - 1$ became the consequence and so the hard part $\pi(n) \sim \frac{n}{\log n}$ became called the Prime Number Theorem.

15. Gap and density Local and total averages

R It is the jumps, the gaps between primes that make $\pi(n)$ and p_n grow irregularly. So why is the obsession to approximate $\pi(n)$ and p_n? Remember, that n^* is the first prime after n and n_* is the last prime up to n. Shouldn't we first approximate $\delta(n) = n^* - n_*$ and $d_n = p_{n+1} - p_n$? Indeed, these lie behind but they are much harder too. Lets just think of the twin primes! They show that δ and d go back to the minimal 2 value again and again and probably jump back to other, maybe even all smaller values infinitely. Yet in average, the gaps are increasing because the primes become less and less. Are the gaps increasing relative to the size of the numbers too? No, in fact, $\frac{\delta(n)}{n} \to 0$ follows from $\pi(n) \sim \frac{n}{\log n}$. This has nothing to do with the particular $\log n$ function, but simply is a consequence of that if a function $\pi(n)$ is approximated by a smooth function f, then its jumps $\delta(n)$ must relatively be diminishing. This of course also means that $\frac{d_n}{p_n} \to 0$. But it doesn't mean automatically that $\frac{d_n}{n} \to 0$ too. This is also true but to prove it, is even harder than the Prime Number Theorem. We conjectured in the third section in the book Primes, that $d_n \underset{31}{<} \pi(n)$. If we could prove that, then $\frac{\pi(n)}{n} \to 0$ would imply at once the same for d_n. So probably to prove $d_n \underset{31}{<} \pi(n)$ is even harder (I don't even know if it has been shown). All this would suggest that we better turn back and forget about the gaps. Yet we won't because they still are the only way to make sense of $\pi(n)$ and p_n.

To tame $\delta(n)$ and d_n, we have to take some average of these and there are two ways of this. A local average would mean that around a big N, we add up a smaller n many and divide the sum by n. This is pretty messy because it depends on the relation of N and n. A huge simplification is if we take the average from the beginning. Such total average is clearly smaller than the local, because the smaller beginning gaps bring it down. Lets see how $\pi(n)$ grows with its "plateaus" as $\delta(n)$.



Clearly up to an n, the total sum of the plateaus is $n-2$ and there are $\pi(n)$ many plateaus, so their average is $\frac{n-2}{\pi(n)}$. As n gets bigger this is about the same as $\frac{n}{\pi(n)}$, which is thus the total average of the gaps. With an other approach $\frac{d_1+d_2+\ldots+d_n}{n}$ is the average and $d_1+d_2+\ldots+d_n=(3-2)+(5-3)+\ldots+(p_{n+1}-p_n)=p_{n+1}-2$. So the average is about $\frac{p_{n+1}}{n}$. If $\frac{d_n}{n}=\frac{p_{n+1}-p_n}{n}\to 0$, as we said above, then of course, $\frac{p_{n+1}}{n}$ is about the same as $\frac{p_n}{n}$. By the Prime Number Theorem, $\pi(n)\sim\frac{n}{\log n}$ and $p_n\sim n\log n$ too. This confirms what we achieved, that both $\frac{n}{\pi(n)}$ and $\frac{p_n}{n}$ give the average gap from the beginning and even more, it suggests that this average is $\log n$. However, we have to be careful because the $\sim$ relation is just a ratio limit, so for example it is true instead of $\log n$ for $\log n+c$ too, with any c constant. Of course, we could say, why shouldn't be the simplest case be the natural law? Well, amazingly the law will be the simplest case but it isn't $\log n$. How could that be? Remember, that we took the total average, simply because the local was too difficult to calculate. Well, for nature it is not difficult. So, $\log n$ is actually the local average of gaps, while the total is smaller, namely $\log n-1$. We might wonder how can it only be 1 less, but we have to see that the majority of the gap values are towards the n. Strangely, there is another "-1" complication involved too, for a much simpler reason though. We use the expression "gap" for the values of δ and d, but actually these are jumps, not gaps. The gaps are 1 less than the jumps because $\delta(n)=n^*-n_*$ includes one of the primes, or to see it even simpler looking at a sequence of binary digits: $0\,0\,1\,0\,\underbrace{1\,0\,0\,0\,0\,1}\ldots$

the jump = 5, but the gap = 4. We might ask which is more natural, the jump or the gap? The answer is definitely the jump, for the following reasons: The jump tells how many on a longer interval are the 1-s or the primes in our case. For example, if we want to know how many primes are from $1\,000\,000$ to $1\,000\,100$, then the 100, which is the interval must be divided by the average jump, not the average gap! And indeed, $\log n$ is this jump, not the gap.
Since, $\log n=\log_{10} n\cdot\log 10$ and $\log_{10} n$ is about the number of digits and $\log 10\cong 2.3$, thus we can easily tell the number of primes from $1\,000\,000$ to $1\,000\,100$.
$\log_{10} 1\,000\,000=6$, so the jump is $6\cdot 2.3\cong 14$ and so $\frac{100}{14}\cong 7$ primes should be.
To say that around $1\,000\,000$ every 14-th number is prime is the same as saying that around $1\,000\,000$ a number $\frac{1}{14}$ chance of being a prime.

So $\frac{1}{\log n}$ is the probability of primeness around n.
Gauss not only realized this but used it in an ingenious way to derive a better approximation for $\pi(n)$ than $\frac{n}{\log n}$. The full story is that Legendre, a few years earlier, empirically guessed the $\frac{n}{\pi(n)}\approx\log n-1$ relation, but wasn't sure of the 1 really being exactly 1 and he calculated it by his tables to be 1.08. Of course, Legendre was looking for $\pi(n)$, so he gave it as $\frac{n}{\log n-1.08}$. But $\approx$ does not stand between $\pi(n)$ and even the perfect $\frac{n}{\log n-1}$. This is simply because $\frac{n}{\pi(n)}$ is tame, while $\pi(n)$ itself is wild, that is jumpy.

In Gauss' life, it wasn't proved yet, but later it turned out, that his approach was even better than $\frac{n}{\log n - 1}$. And later even better than his approach were found. Today, it seems that $\pi(n)$ doesn't have a simple "best" approximation, so it was indeed an obsession, to chase it at all. Still, Gauss' approach is something absolute, because it leads to the $\frac{n}{\pi(n)} \approx \log n - 1$ relation, if the later proved Prime Number Theorem is applied for it. But more importantly, the heuristic principle behind Gauss' approach is that brings it above Legendre's. So lets see it!

If $\frac{1}{\log n}$ is the probability of a number being prime around n, then the number of primes up to an n, that is $\pi(n)$ could be obtained by adding up the products of smaller intervals, multiplied with their chances. Of course, the smaller the intervals are, the better the approximation will be. The smallest interval seems to be a single number so we might think that the best approximation is $\frac{1}{\log 2} + \frac{1}{\log 3} + \ldots + \frac{1}{\log n}$. But we can widen our view and regard $\frac{1}{\log x}$ as a continuous probability density, that is a value that when multiplied with a Δx interval, gives the number of primes in Δx. Then, $\sum \Delta x \cdot \frac{1}{\log x}$ is the area under the $\frac{1}{\log x}$ function refined with Δx to be smaller and smaller. The usual name for such area is the integral, with an $\int$ replacing $\sum$.

So, $\int_2^x \frac{dx}{\log x}$ is Gauss' approximation for $\pi(x)$, which became abbreviated as Li (x).

As we saw in earlier book, we have tricks to calculate these integrals or areas. Unfortunately, $\frac{1}{\log x}$ is not a lucky function and it doesn't have a ready made area function. In other words, Li (x) can not be expressed explicitly as a simpler function from basic ones. But there are easier approximations for Li (x) than for $\pi(x)$ originally and this is how the $\frac{n}{\log x - 1}$ can also be obtained as one such very good approximation. Of course, beside all these theoretical points, Li (x) can be calculated with computers for arbitrary value and can be compared with the actual $\pi(x)$.

Finally, a very strange result of Littlewood, says that Li (x) goes infinitely many times under and above $\pi(x)$, so it indeed behaves like a very good approaching function, even though its difference from $\pi(x)$ is getting bigger and bigger up to infinity. This again suggests what I said earlier, that $\pi(x)$ is not "meant to be" approached with simpler functions.

16. Factorial Prime Factorization Stealing the holy grail

R As I said, the Prime Number Theorem was a very hard delivery after a hundred year pregnancy. In this century, Erdös and Selberg, following a controversial exchange of ideas, came to two so called elementary proofs, but these are still very complicated.
Yet, amazingly if we assume that the primes are appearing with a regularity, which of course is not true in reality, then the role of $\log n$ in the Prime Number Theorem can be derived.
Of course, it's not a proper proof and that's why I called it, the "stealing" of the holy grail.

D 1.) Let $(m)_p$ denote the exponent of the p prime, in the prime factorization of m. Ex:
$84 = 2^2 \cdot 3 \cdot 7$, so $(84)_2 = 2$, $(84)_3 = 1$, $(84)_5 = 0$, $(84)_7 = 1$, $(84)_{11} = 0$, . . .

2.) Let $\underset{m}{\overset{n}{\sim}}$ denote $\left[\frac{n}{m}\right]$, that is the whole part of $\frac{n}{m}$.

T Factorial's Prime Factorization Theorem:

$$n! = 2^{\left(\frac{n}{2}+\frac{n}{4}+\ldots\right)} \cdot 3^{\left(\frac{n}{3}+\frac{n}{9}+\ldots\right)} \ldots p^{\left(\frac{n}{p}+\frac{n}{p^2}+\ldots\right)} \approx 2^n \cdot 3^{\frac{n}{2}} \cdot \ldots p^{\frac{n}{p-1}}$$

P $(n!)_p = (2)_p + (3)_p + (4)_p + \ldots + (n-1)_p + (n)_p$
If we omit the zero members and rearrange the rest by combining the same values in increasing order, then:

$$(n!)_p = \underbrace{\left(\underset{p}{\overset{n}{\sim}} - \underset{p^2}{\overset{n}{\sim}}\right)\cdot 1}_{\text{number of 1s}} + \underbrace{\left(\underset{p^2}{\overset{n}{\sim}} - \underset{p^3}{\overset{n}{\sim}}\right)\cdot 2}_{\text{number of 2s}} + \underbrace{\left(\underset{p^3}{\overset{n}{\sim}} - \underset{p^4}{\overset{n}{\sim}}\right)\cdot 3}_{\text{number of 3s}} + \ldots$$

$$+\underset{p^2}{\overset{n}{\sim}} \qquad +\underset{p^3}{\overset{n}{\sim}} \qquad +\underset{p^4}{\overset{n}{\sim}} + \ldots$$

Indeed, the $(m)_p = 1$ satisfying m-s are those that are dividable by p, but not with p^2, so their number is $\underset{p}{\overset{n}{\sim}} - \underset{p^2}{\overset{n}{\sim}}$.

Similarly, there are $\underset{p^2}{\overset{n}{\sim}} - \underset{p^3}{\overset{n}{\sim}}$ many m-s satisfying $(m)_p = 2$, and so on. Then:

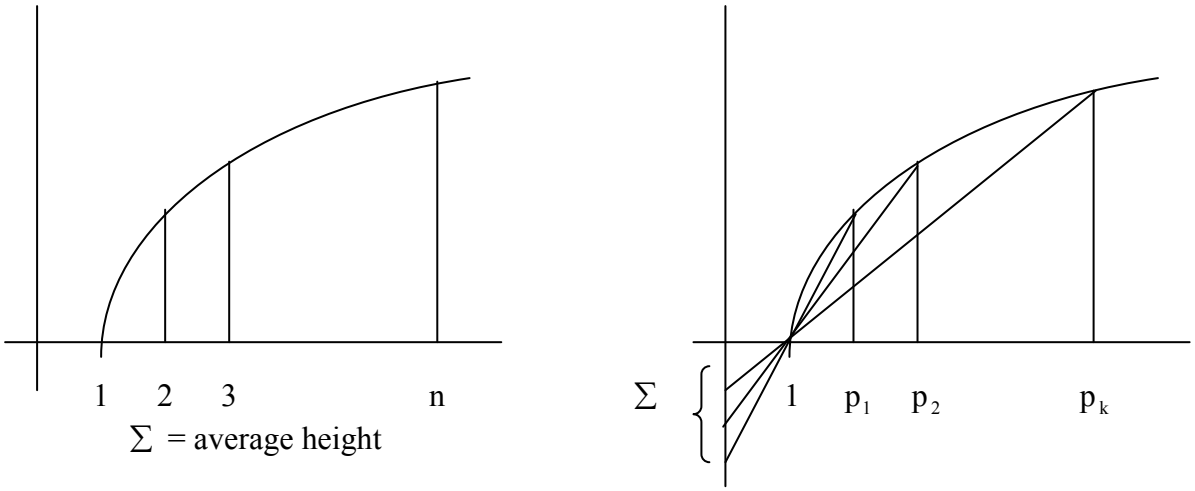
$(n!)_p = \underset{p}{\overset{n}{\sim}} + \underset{p^2}{\overset{n}{\sim}} + \underset{p^3}{\overset{n}{\sim}} + \ldots \approx \frac{n}{p-1}$ because with proper fraction instead of the $\sim$, the equality is true as can be checked by multiplying the equation with $p-1$.

R Now we can use this theorem and the assumption that the primes have a $P(x)$ probability density function, to get a caricature of the Prime Number Theorem.

$$n! \approx 2^n \cdot 3^{\frac{n}{2}} \cdot \ldots p^{\frac{n}{p-1}} = p_1^{\frac{n}{p_1-1}} \cdot p_2^{\frac{n}{p_2-1}} \cdot \ldots p_k^{\frac{n}{p_k-1}}$$

Taking $\log n$ of both sides and dividing by n:

$$\frac{1}{n} \sum_{i=1}^{n} \log(i) \quad \approx \quad \sum_{i=1}^{k} \frac{\log p_i}{p_i - 1}$$



Changing to continuous x variable and integrals instead of sums:

$$\underbrace{\frac{1}{n} \int_{1}^{n} \log x \, dx} \quad \approx \quad \int_{1}^{n} \frac{\log x}{x-1} P(x) \, dx$$

$$\frac{1}{n} \left[x \log x - x \right]_1^n = \log n - 1 + \frac{1}{n} \approx \log n \quad \approx \quad \int \frac{\log x}{x-1} P(x) \, dx$$

Differentiating, that is finding the function of which these are the areas of:

$\log n$ is of $\frac{1}{n}$ and $\int \frac{\log x}{x-1} P(x) \, dx$ is of $\frac{\log x}{x-1} P(x)$. So:

$\frac{1}{n} \approx \frac{\log n}{n-1} P(n)$, so $P(n) \approx \frac{1}{\log n}$.

From this then, $\pi(n) \approx n \, \overline{P}(n)$ where $\overline{P}$ is an average density.

This $\overline{P}$ is very close to P, in fact as we remember, it is actually $P - 1$, so:

$$\pi(n) \sim \frac{n}{\log n}$$

17. Window Conjectures

D

1.) $w = (0\ 0\ 1\ 0\ 1\ \ldots\ 1\ 0)$ binary tuple containing k 1-s is called a k-window.
w_i denotes the place of the i-th 1. For example above, $w_1 = 3$, $w_2 = 5$, and so on.

2.) $w(n)$ for $n = 0, 1, 2, \ldots$ denotes the natural k-tuples, obtained by placing the w window after n, and collecting the natural numbers at the 1 places.
For example, the above window placed after $n = 3$, looks like:
$0\ ,\ 1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\ ,\ 7\ ,\ 8\ ,\ \ldots$
$(0\quad 0\quad 1\quad 0\quad 1\ \ldots\ 1\quad 0)$
So, $w(3) = (6\ 8\ \ldots)$. Clearly in general:
$w(0) = (w_1, w_2, \ldots, w_k)$ and $w(n) = (n + w_1, n + w_2, \ldots, n + w_k)$

3.) $W(n)$ denotes the product of the elements of $w(n)$.

4.) w is factorless over an $\{n_1, n_2, \ldots\}$ set of numbers, if there is no common factor of the $W(n_1), W(n_2), \ldots$ numbers.

T

Conjectures

I.) If w is factorless over $0, 1, 2, \ldots$ then,
for infinite many n, $w(n)$ contains only primes.

II.) If w is factorless over $0, d, 2d, \ldots$ then,
for infinite many md, $w(md)$ contains only primes.

III.) If w is factorless over $0, 1, 2, \ldots$ then,
for infinite many n, $w(n)$ contains consecutive primes.

IV.) If for $w = (1\ \ldots\ 1\ \ldots\ 1\ \ldots\ \ldots\ 1)$ that is
$w_1 = 1$, $w_2 = 1 + d$, $\ldots$, $w_k = 1 + (k - 1)\,d$ and d is a multiple of all the primes up to $k - 1$, then there are infinite many n that $w(n)$ contains consecutive primes.

R

Obviously, II → I with $d = 1$. More amazingly:

T

1.) II → III

2.) III → IV

P

1.) By I there are infinite many all prime $w(n)$, so we can add enough 0-s in the front to change w into 1, where $w(0)$ is all prime and $w_1 > w_k - w_1$, that is $2\,w_1 > w_k$ and of course then $2\,w_i > w_k$ too.
By $2\,w_i > w_k$, the $w(0)$ elements are not factors of any other numbers up to w_k.
Let d be the multiple of all these other numbers, that is
$d = 2 \cdot 3 \cdot \ldots (w_1 - 1)(w_1 + 1) \ldots (w_2 - 1)(w_2 + 1) \ldots (w_k - 1)(w_k + 1)$
By the aboves, the $w(0)$ elements are not factors of d either, since they are primes.
Now we show, that w is factorless over $0, d, 2d, \ldots$
Suppose, that p is a factor of $W(0)$.
Then clearly, p is one of the elements of $w(0)$ and p can't be a factor of d either.
So, $md + w_1, md + w_2, \ldots, md + w_k$ each is dividable by p only for one unique m value from $0, 1, 2, \ldots, p - 1$. (For example, $m_i = 0$ for the mentioned $w_i = p$.)
This gives k possible values for which $W(0), W(d), \ldots, W((p - 1)\,d)$ is dividable by p. But, $k \le w_k - w_1 < w_1 \le p$ so $k < p$ and thus, from the listed p many w products, some will be not dividable by p.
So by II there are infinite many among $0, d, 2d, \ldots$ where $w(md)$ is all primes.
We claim that those all primes are consecutive as well.

Indeed, if B is a number between two w (md) elements, md + w_i and md + w_{i+1}, then B = md + b with b between w_i and w_{i+1}. But such b-s are factors of d, so they are factors of B = md + b too.

2.) All we have to show is that the condition on the d of the equally spaced k window, implies the factorlessness, because then III implies IV trivially.
If p is a factor of d, then W (0) = 1· (1 + d) (1 + 2d) . . . (1 + (k – 1) d) has 1 remainder to p, so p is not factor of it.
If p is not factor of d and p ≥ k, then in any W (n) = n (n + d) . . . (n + (k – 1) d), the members all have different remainders to p. Indeed, if two were the same then their difference qd were dividable by p with q ≤ k, which is impossible if d isn't.
Furthermore, the W (0) , W (1) , . . . , W (p – 1) products have each members with 1 more remainders to p than the previous one.

R IV obviously implies Polignac's General Twin Prime Conjecture because:
with w = (1 0 . . . 0 1) that is $w_1 = 1$, $w_2 = 2m$ and 2m is multiple of 2.
Or directly, II implies it again with the same w because:
W (0) = 1· (1 + 2m) , W (1) = 2· (2 + 2m) and they have no common factor.
Indeed, 2 is not factor of 2m + 1 and 2m + 1 and 2m + 2 are consecutive numbers.

R The special condition of conjecture IV is necessary, in fact it is necessary for not only equally distanced consecutive, but equally distanced ones in general:

T If n , n + d , n + 2d , . . . , n + (k – 1) d are all primes,
then d is multiple of all primes up to k – 1.

P First of all, n ≥ k, otherwise n + nd were among the sequence which is clearly composite.
Let p < k be a prime and r_1 , r_2 , . . , r_k the remainders of n , n + d , . . , n + (p – 1) d) to p. None of these remainders is 0, because p < k ≤ n < n + d < . . .
So the 1 , 2 , . . . , p – 1 values are taken at p places. And thus, at least two are the same and so their difference, which is md with m < p, is dividable by p. So p is factor of d.

R For special sequences we can even tell how they must start:

T If n , n + d , n + 2d , . . . , n + (k – 1) d are all primes,
and k is prime too and not a factor of d, then n = k.

P Enough to show that among p prime many, equally but not p multiple distanced
a_1 , a_2 , . . . , a_p numbers, at least one is dividable by p.
Then, with all primes, this p must be a_1. And indeed, if a_1 , a_2 , . . . , a_p had only
1 , 2 , . . . , p – 1 remainders to p, then two of them had the same remainder, and their difference, which is md, were dividable by p, contradicting that d weren't.
Examples:
For k = 3, the minimal d is 2. Then n = 3, so the sequence is: 3 , 5 , 7.
For k = 5, the minimal d is 2·3 = 6. Then n = 5, so the sequence is: 5 , 11 , 17 , 23 , 29.
For k = 7, the minimal d is 2·3·5 = 30. Then n = 7, so the sequence should be:
7 , 37 , 67 , 97 , 127 , 157 , 187. But, 187 = 11·17 , so it is not good.
The smallest d that works for k = 7, is 150.

R Another consecutive prime conjecture follows from II which is just as surprising as IV:

T Conjecture V: There are k consecutive pairs of twin primes for every k.

R For II $\rightarrow$ V, the window must be chosen with some trick to generate the twins and the factorlessness too.

R We might wonder why we didn't require that a window should start and end with 1, that is $w_1 = 1$, w_k = length of the window. The last one is indeed logical, because the end 0-s have no effect, but beginning 0-s can have three effects:

1.) They delay the starting of the application of the window.
2.) For a window that we are going to use over $0, d, 2d, \ldots$ the number of these beginning 0-s can interrelate with the value of d.
3.) The usage of longer and longer "dummy" beginning 0-s can lead to a seemingly amazing reformulation of our conjectures as follows:

T 1.) Let $w = (\_\_\_\_\_)$ and $w' = (\underbrace{0 \ldots 0}_{Md\ 0\text{-s}} \_\_\_\_\_)$. Then,

a.) $w'(0) = w(Md)$, $w'(1) = w(Md + d)$, $\ldots$

b.) If w is factorless over $0, d, 2d, \ldots$ then w' is also.

c.) A $w(md)$ all prime containing value of w is not value of w', if $m < M$.

d.) All the all prime containing values of w' are values of w too.

2.) Let II' be:
If w is factorless over $0, d, 2d, \ldots$ then, there is an md where $w(md)$ is all prime.
Then II' $\rightarrow$ II.

3.) Similar, weaker I', III', IV' forms imply I, III, IV.

P 1.) Trivial.

2.) Let w be all prime at $m_1 d$. Add $(m_1 + 1) d$ many 0-s in front of w to get w_1.
By 1.) b.) above, w_1 is factorless and so by II' again it will be all prime at say, $m_2 d$.
Then, again we add $(m_2 + 1) d$ many 0-s in front of w_1 to get w_2. And so on, by 1.) c.) we always get new all primes, but by 1.) d.), these will all be values of w.

3.) Trivial.

18. Gap Conjectures

R Since the average of the gaps is log, we expect that any function that would limit the gaps from a point, must be bigger than this. The strongest conjecture is by Cramer:

$n > 7 \rightarrow \delta(n) < (\log(n))^2$ which implies that: $p^* - p \underset{11}{<} (\log p)^2$

From this we can get an infinity of conjectures for any root of p that is for $\sqrt[k]{p}$.

Namely, we can check the first N value that $(\log n)^2 \underset{N}{<} \sqrt[k]{n}$ and then check the primes up to N and find out from what P will they satisfy $p^* - p < \sqrt[k]{p}$.

This then would imply: $p^* - p \underset{P}{<} \sqrt[k]{p}$.

The reason is simply that after N we definitely must have $(\log p)^2 < \sqrt[k]{p}$.

Indeed, $(\log p)^{2k} < p$ can be written as $x^{2k} < e^x$ with $x = \log p$.

The $y = x^{2k}$ parabola crosses the $y = e^x$ exponential function at a trivial point between 1 and 2 but then it crosses again much later from which point e^x will be bigger forever.

For the simplest $k = 2$ square root conjecture:

$p^* - p \underset{11}{<} (\log p)^2 \underset{6400}{<} \sqrt{p}$ Indeed, $\sqrt{6400} = 80$ and $(\log 6400)^2 = 76.8$

From $P = 127$ up to $N = 6400$ $p^* - p < \sqrt{p}$ can be checked for all primes to be true, so

$$p^* - p \underset{127}{<} \sqrt{p}$$

(The previous prime before 127 is 113, and $127 - 113 = 14 > \sqrt{113}$)

This idea should initiate a search for suitable roots and thus avoid Cramer's Conjecture.

In 1930 Hoheisel proved that for the $\theta = 1 - \frac{1}{3300}$ exponent there is P that:

$$p^* - p \underset{P}{<} p^{\theta}.$$

Amazingly, the better results still all stayed above the "magic" $\frac{1}{2}$ value that came out so easily above from Cramer's Conjecture.

Up today, $\theta = \frac{5}{8}, \frac{7}{12}, \frac{11}{20}, \frac{1}{2} + \frac{1}{21}, \frac{11}{20} - \frac{1}{384}$ values were proved.