Jumbled up thoughts

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: November 28, 2017)

Abstract

Prime numbers form like a set of bases for the integers, just like sinusoids form the bases for any function $f(x)$, the interesting thing is that this (primes as bases) is true for primes under the operation of additions, if we define some other operations then prime numbers won't be bases anymore.

Not sure if any of the techniques we have for spectral analysis can be derived from properties of primes or maybe the other around ¯\(°_o)/¯

-=-
=-

See if we can find $k, m > 1$ such that

$$(a \pm 1)^k = a^m \pm 1$$

where the min of $a \pm 1$ and a is an integer ≥ 2 (the answer is no and we'll see why). There are four cases total but two of them are equivalent

$$(a+1)^k = a^m + 1 \longleftrightarrow (a-1)^k = a^m - 1$$
$$(a+1)^k = a^m - 1 \longleftrightarrow (a-1)^k = a^m + 1$$

Let's denote $b = a + 1$ and tackle the case of $(a+1)^k = a^m + 1$ first which is equivalent to $(a-1)^k = a^m - 1$.

Let's start with b odd and therefore a even

$$b^k - 1 = a^m$$
$$(b-1)(b^{k-1} + b^{k-2} + b^{k-3} + \dots + b + 1) = a^m, \qquad b - 1 = a$$
$$b^{k-1} + b^{k-2} + b^{k-3} + \dots + b + 1 = a^{m-1}$$

Now if k is odd then on the LHS there will be an even number of terms containing b grouping them two by two

$$(b^{k-1} + b^{k-2}) + (b^{k-3} + b^{k-4}) + \dots (b^2 + b) + 1 = a^{m-1}$$

Each bracket is an even number therefore the total of the LHS is odd due to the +1 at the end but the RHS is even since a is even so the above is impossible.

If k is even

$$b^{k-2}(b+1)+b^{k-4}(b+1)+\cdots+(b+1)=a^{m-1}$$
$$(b+1)(b^{k-2}+b^{k-4}+\cdots+1)=a^{m-1}, \qquad b+1=a+2$$
$$\rightarrow (a+2) \mid a^{m-1}$$

we know that $\gcd(a+2,a)\leq 2$ so unless $a+2=4\rightarrow a=2$, there's a divisor of $a+2$ that doesn't divide a^{m-1} and so $(a+2)\nmid a^{m-1}$, the only thing left is to show that when $a=2$ we have no solution either.

In the case of $a=2$, $a+2=a^2$ and

$$(b^{k-2}+b^{k-4}+\cdots+1)=a^{m-3}$$

but the situation repeats if there are only odd number of terms in the LHS then just like above the sum of the LHS is odd while the RHS is even, if there are an even number of terms in the LHS then we have a similar situation again but this time

$$(b^2+1)(b^{k-4}+b^{k-8}+\cdots+1)=a^{m-3}$$

but this time since $b^2+1=10$, the LHS contains 5 as a prime factor while the RHS is a product of 2's only so there are no solutions $k,m>1$ if a is even.

The next case is a odd and b even, in this case just like before we have

$$b^{k-1}+b^{k-2}+b^{k-3}+\cdots+b+1=a^{m-1}$$

Again we split it into two cases, if there are an odd number of terms in the LHS, *i.e.* k is odd, then we can do the following

$$b^{k-1}+b^{k-2}+b^{k-3}+\cdots+b^2+b=a^{m-1}-1$$
$$b(b^{k-2}+b^{k-3}+\cdots+b+1)=a^{m-1}-1$$

Since initially we have an odd number of terms in the LHS after moving the constant 1 to the RHS we now have an even number of terms in the LHS and we can group them two by two like above

$$b(b^{k-3}(b+1)+b^{k-5}(b+1)+\cdots+(b+1))=a^{m-1}-1$$
$$b(b+1)(b^{k-3}+b^{k-5}+\cdots+1)=(a-1)(a^{m-2}+a^{m-3}+\cdots+1)$$

while we also expand the RHS like usual.

We now need more info to move on. Since $k > 1$ and b is even, if we do modulo 4 the LHS is $0 \equiv \pmod 4$, so to have a chance of a solution $a \equiv -1 \pmod 4$ and not only that but m has to be odd as well, this means $m-1$ is even and after extracting $(a-1)$ the second bracket in the RHS has an even number of terms as well.

This means we can group the terms two by two as well

$$b(b+1)(b^{k-3}+b^{k-5}+\cdots+1) = (a-1)(a^{m-3}(a+1)+a^{m-5}(a+1)+\cdots+(a+1))$$

$$b(b+1)(b^{k-3}+b^{k-5}+\cdots+1) = (a-1)\cancel{(a+1)}(a^{m-3}+a^{m-5}+\cdots+1), \qquad a+1=b$$

Now, $(b+1)$ is odd since b is even, also $(b+1)(b^{k-3}+b^{k-5}+\cdots+1)$ is odd since again b is even so the LHS is odd times odd which is odd while in the RHS $(a-1)$ is even since a is odd so the RHS is even, but we can't have an odd LHS equal to an even RHS so there's no solution for k odd.

If k is even then

$$b^{k-1}+b^{k-2}+b^{k-3}+\cdots+b+1 = a^{m-1}$$

$$(b+1)(b^{k-2}+b^{k-3}+\cdots+1) = a^{m-1}, \qquad b+1=a+2$$

$$\rightarrow (a+2) \mid a^{m-1}$$

But this is the same case as before with a even, $\gcd(a+2,a) \leq 2$ but this time since a is odd we don't even have the situation where $a+2=4$ and so there is a divisor of $(a+2)$ that doesn't divide a^{m-1} and so $(a+2) \nmid a^{m-1}$.

Now we tackle the case of $(a+1)^k = a^m - 1$ first which is equivalent to $(a-1)^k = a^m + 1$

$$b^k = (a-1)(a^{m-1}+a^{m-2}+\cdots+a+1), \qquad a-1=b-2$$

$$\rightarrow (b-2) \mid b^k$$

so again, this case can't work because $\gcd(b-2,b) \leq 2$ except for $b-2=2, a=3$ and $b=4$, in this case m is even thanks to modulo 4 so then

$$4^k = (3-1)(3^{m-2}(3+1)+3^{m-4}(3+1)+\cdots+(3+1))$$

$$2\cdot 4^{k-1} = 4(3^{m-2}+3^{m-4}+\cdots+1)$$

$$2\cdot 4^{k-2} = 3^{m-2}+3^{m-4}+\cdots+1$$

Now if there is an odd number of terms in the RHS then we are done because the sum of the RHS is then odd but the LHS is even, but if there are an even number of terms in the RHS we can group them two by two

$$\begin{aligned} 2 \cdot 4^{k-2} &= 3^{m-4}(3^2+1) + 3^{m-8}(3^2+1) + \cdots + (3^2+1) \\ &= 10(3^{m-4} + 3^{m-8} + \cdots + 1) \end{aligned}$$

so the RHS contains 5 as a divisor while the LHS doesn't so it won't work.

In conclusion, there is no such $k, m > 1$ such that $(a \pm 1)^k = a^m \pm 1$, for all integers $a > 1$.

Just a side note, we can make this a little more complicated by noticing that

$$2^m = (1+1)^m = \sum_{l=0}^{m} \binom{m}{l}$$

Also

$$(2+1)^k = \sum_{j=0}^{k} \binom{k}{j} 2^j = \sum_{j=0}^{k} \binom{k}{j} \sum_{n=0}^{j} \binom{j}{n}$$

And also

$$\begin{aligned} (3+1)^k &= \sum_{j=0}^{k} \binom{k}{j} 3^j = \sum_{j=0}^{k} \binom{k}{j} (2+1)^j \\ &= \sum_{j=0}^{k} \binom{k}{j} \sum_{n=0}^{j} \binom{j}{n} \sum_{i=0}^{n} \binom{n}{i} \end{aligned}$$

So for the purpose of wasting space any number n^k can be expressed as a nested binomial expansion

$$n^k = ((n-1)+1)^k = \sum_{j_1=0}^{k} \binom{k}{j_1} \sum_{j_2=0}^{j_1} \binom{j_1}{j_2} \cdots \sum_{j_{n-1}=0}^{j_{n-2}} \binom{j_{n-2}}{j_{n-1}}$$

So the question of whether there are $k, m > 1$ such that $(a+1)^k = a^m + 1$ can be restated as a statement about nested binomial expansions

$$\sum_{j_1=0}^{k} \binom{k}{j_1} \sum_{j_2=0}^{j_1} \binom{j_1}{j_2} \cdots \sum_{j_{n-1}=0}^{j_{n-2}} \binom{j_{n-2}}{j_{n-1}} = \sum_{i_1=0}^{m} \binom{k}{i_1} \sum_{i_2=0}^{i_1} \binom{i_1}{i_2} \cdots \sum_{i_{n-2}=0}^{i_{n-3}} \binom{i_{n-3}}{i_{n-2}} \pm 1$$

Another side note, any number is a product of power of primes, in that case any number can be expressed as a product of nested binomial sums and in this case we can use binomial sums as some sort of bases ¯\(°_o)/¯

But one other thing, does this mean that $0^0 = 1$? because according to the binomial expansion

$$\begin{aligned}(2+0)^3 &= \binom{3}{0}2^3 \cdot 0^0 + \binom{3}{1}2^2 \cdot 0^1 + \binom{3}{2}2^1 \cdot 0^2 + \binom{3}{3}2^0 \cdot 0^3 \\ 2^3 &= 2^3 \cdot 0^0 \\ 2^3/2^3 &= 0^0\end{aligned}$$

and so according to binomial expansion $0^0 = 1$:)

-=-

Given that we can factorize the following

$$\begin{aligned}x^k - 1 &= (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1) \\ x^k + 1 &= (x+1)(x^{k-1} - x^{k-2} + \cdots - x + 1), \qquad k = 2m+1\end{aligned}$$

Let $d = \gcd(x \mp 1, x^{k-1} \pm x^{k-2} \pm \cdots \pm x + 1)$ then $d|k$

Proof. Let's first tackle the case of $x^k - 1$. Note that the following is a sum of some constant multiplied by some power of $(x-1)$

$$\frac{((x-1)+1)^k - k(x-1) - 1}{x-1} = (x-1)^{k-1} + \binom{k}{1}(x-1)^{k-2} + \cdots + \binom{k}{k-2}(x-1)$$

we need $-k(x-1)-1$ so that each term in the expansion multiplies some power of $(x-1)$ and so the following produces

$$\begin{aligned}x^{k-1} + x^{k-2} + \cdots + 1 - \frac{((x-1)+1)^k - k(x-1) - 1}{x-1} &= \frac{x^k - 1}{x-1} - \frac{((x-1)+1)^k - k(x-1) - 1}{x-1} \\ &= \frac{x^k - 1 - x^k + k(x-1) + 1}{x-1} \\ &= k\end{aligned}$$

and so $d|k$ since d divides the LHS.

By the same token, for $x^k + 1$, note that k is odd for it to be factorisable

$$\frac{((x+1)-1)^k - k(x-1) + 1}{x+1} = (x+1)^{k-1} - \binom{k}{1}(x+1)^{k-2} + \cdots - \binom{k}{k-2}(x+1)$$

and

$$\begin{aligned} x^{k-1} - x^{k-2} + \cdots - x + 1 - \frac{((x+1)-1)^k - k(x-1)+1}{x+1} \\ = \frac{(-x)^k - 1}{-x-1} - \frac{((x+1)+1)^k - k(x-1)+1}{x+1}, \qquad k \text{ is odd} \\ = \frac{x^k + 1 - x^k + k(x+1) - 1}{x+1} \\ = k \end{aligned}$$

and so in this case $d|k$ like before

-=-

Now back to some physics, last night I was thinking of what it means by combining relativity into quantum theory. We know that one of the main postulates of relativity is that nothing exceeds c, the speed of light in vacuum, we'll come back to this in a minute, but what does this mean for quantum mechanics?

The usual explanation is that only observables are physical and therefore their eigenvalues are physical. But does this mean that if we define a velocity operator, then it should not have eigenvalues exceeding c? This is usually not the case, as they say amplitudes (or eigenfunctions) are not physical, only the modulo square is.

But somehow it doesn't feel right. If the velocity operator does have eigenvalues exceeding c then if I choose eigenfunctions corresponding to those eigenvalues, I will have non-zero probability of exceeding the speed of light.

But of course, the first question one should ask is, does it make sense to define a velocity operator?

Going back to QFT, we don't have a velocity operator but we do have a momentum operator and as far as I recall there's no limit to maximum eigenvalue this momentum operator can have and I don't see anybody did this in any textbook.

Now, the question is, are wave function amplitudes really of no physical consequence? For Aharanov-Bohm it is, if it is of physical consequence then we must not be so cavalier about saying that as long as the modulo square is zero we are ok. Two, we might need to define a new operator that will cut off at c. Or three, we might need to rework the framework of quantum mechanics so that this will be included from the beginning.

Back to the aforementioned ground states, why do we need ground states even in quantum theory, if particles can go through energy barriers why can't they go below ground states? because as long as the modulo square is zero it should be ok right? *i.e.* there's no physical observable of going below the ground state. This might be the reason why quantum gravity is so hard, because a particle can have an amplitude inside singularity, *i.e.* we can have a superposition out of singular and non-singular states.

As I look deeper into this, it reminds me of how different relativity is from Newtonian mechanics. The framework is completely different while the equations are just the consequences of the change in framework. We didn't cut off maximum speed or something like that to get relativity but the concept of space time was completely changed.

In arriving at QFT we didn't do that, the framework of quantum mechanics was not radically altered, we only salted and peppered it to allow Lorentz invariants and transformations, I believe there are things we should modify to get relativistic quantum mechanics, seems like the concept of amplitudes, probabilities, superposition, they all have to change somehow instead of just fiddling around with a new hamiltonian like Dirac did or imposing Lorentz compliant commutator algebra, maybe the algebra itself has got to change

-=-

First fact, if $a \equiv b \pmod{c}$ then $(b, c) = (a, c)$, this follows directly from the property of gcd

$$(b, c) = (b + cn)$$

What we have is $d|k$, $(n, d) = 1$, what we want is $m \equiv n \pmod{d}$ and $(m, k) = 1$. For simplicity assume that $n \leq k$.

The goal here is to find an x such that $m = n + dx$ is co-prime to k, since $d|k$, we have k/d distinct values for x, *i.e.* $0 \leq x < k/d$, before we get $m = n + k$. If $(n, k) = 1$ then $(m = n + k, k) = 1$ as well and of course $m \equiv n \pmod{d}$ so we have found our m. If $(n, k) > 1$ we have to do more work.

By adding d to n we are actually cycling through different members of the residue class of k and not only that but we are actually cycling through different members, so we are cycling through k/d different members because say two of them are equivalent modulo k

then

$$n + dx_1 \equiv n + dx_2 \pmod{k}$$
$$\rightarrow k \mid d(x_1 - x_2)$$

but since $0 \leq x_{1,2} < k/d$, $d(x_1 - x_2) < k$ so the above is a contradiction.

Let's recap, what we have is a choice of k/d numbers n_x in the form $n_x = n + dx$ with $0 \leq x < k/d$, all of which are unique modulo k. We want to see if one of them is co-prime to k, note also that $(n, k) > 1$.

Now assume that none of the $n + dx$ is co-prime to k so it means that each must have a common divisor with k. Let's write k in its primal constituents

$$k = p_1^{e_1} p_2^{e_2} \dots p_z^{e_z}$$

denote the set of distinct prime divisors of k and d as $\mathbb{K} = \{p_1, p_2, \dots, p_z\}$ and $\mathbb{D} = \{p_{d_1}, p_{d_2}, \dots, p_{d_s}\}$ respectively with $\mathbb{D} \subset \mathbb{K}$ then the set of distinct prime divisors of the numbers n_x must be in the set $\mathbb{N}_x = \mathbb{K} - \mathbb{D}$ since $(n, d) = (n_x = n + dx, d) = 1$.

Say $\#\mathbb{N}_x = t$ this means that $k/d \geq p_{j_1}^{e_{j_1}} p_{j_2}^{e_{j_2}} \dots p_{j_t}^{e_{j_t}} > 2^t > t$, *i.e.* some of the n_x will have the same common divisor.

Our task now is to distribute these t primes in $\mathbb{N}_x$ into k/d numbers $n_x = n + dx$. Each n_x can have more than one prime as a divisor of course.

Some important observation, if some $n + dx_i$ is divisible by some $p_{j_u} \in \mathbb{N}_x$ then any $n + dx_i + dp_{j_u} y$ is also divisible by p_{j_u}, the converse is also true, if two n_x's are divisible by p_{j_u} then their difference has to be $dp_{j_u} y$.

So we can think of the numbers n_x as a bitmap with k/d number of bits where the each n_x is represented by one bit. Once we choose a bit, say bit u to contain a prime p_{j_u} all other bits with a distance of multiples of p_{j_u} from this bit will also contain p_{j_u}.

In this way the bits containing p_{j_u} is $(u + sp_{j_u})$, *i.e.* bit position $u \pmod{p_{j_u}}$ will all contain p_{j_u}. Once we assign each bit a prime from $\mathbb{N}_x$ we have the following assignments

(we number our bits starting from bit 1 instead of 0)

$$\begin{array}{rcl} \textit{bit position} & & \textit{prime assignment} \\ b_1 \pm s_1 p_{j_1} \equiv c_1 \pmod{p_{j_1}} & \rightarrow & p_{j_1} \\ b_2 \pm s_2 p_{j_2} \equiv c_2 \pmod{p_{j_2}} & \rightarrow & p_{j_2} \\ & \vdots & \\ b_t \pm s_t p_{j_t} \equiv c_t \pmod{p_{j_t}} & \rightarrow & p_{j_t} \end{array}$$

note that bit 1 is just n and since $(n, k) > 1$, n must contain one of the primes and s_i is any integer (of course the total, $b_i \pm s_i p_{j_i}$, can't be less than zero of bigger than the total number of bits, k/d). The remaining question is whether there is a bit that wasn't represented by the above assignment and there is, thanks to Chinese Remainder Theorem there must be at least one. We can construct one quite easily, setup the Chinese remainders as follows

$$\begin{aligned} c &\equiv (c_1 + 1) \pmod{p_{j_1}} \\ c &\equiv (c_2 + 1) \pmod{p_{j_2}} \\ &\vdots \\ c &\equiv (c_t + 1) \pmod{p_{j_t}} \end{aligned}$$

Chinese remainder theorem guarantees that we have such c and that such a c is congruent modulo $p_{j_1} p_{j_2} \ldots p_{j_t}$ so this means that $c \leq p_{j_1} p_{j_2} \ldots p_{j_t}$ which is less than the total number of bits $k/d \geq p_{j_1}^{e_{j_1}} p_{j_2}^{e_{j_2}} \ldots p_{j_t}^{e_{j_t}}$. We can also construct other bits by changing the $+1$ into some other constant. Note that if the number of bits is less than t, the number of distinct primes the argument falls.

Thus we have shown that one of the n_x's must be co-prime to k and we can choose this one to be m.

-=-=-=-=- CHINESE REMAINDER POWER -=-=-=-=-

First Case

Believe it or not, the above proof about bit position and whatnot also serves as a proof that there are infinitely many primes. Suppose we only have finitely many primes $p_1, p_2, \ldots, p_n$. I can show that among the first $p_1 p_2 \cdots p_n$ natural numbers there are numbers that are not divisible by those primes as such there must be another prime

besides those n primes. On top of that I can tell you how many of those numbers there are.

How to see this? Easy, the Chinese to the rescue, set up the following system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{p_1} \\ x &\equiv a_2 \pmod{p_2} \\ &\vdots \\ x &\equiv a_n \pmod{p_n} \end{aligned}$$

as long as each $a_i \not\equiv 0 \pmod{p_i}$, x is guaranteed to be not divisible by any of those n primes, the solution of the above is guaranteed by our Chinese friend to exist, but not only that, it is also guaranteed to be less than $p_1 p_2 \cdots p_n$.

Now, how many of those numbers are there? Each a_i runs from $1, \ldots, p_i - 1$, so there are

$$(p_1 - 1)(p_2 - 1) \cdots (p_n - 1) = \varphi(p_1 p_2 \cdots p_n)$$

which is consistent with what we already know about φ. The slight difference between this and Euclid's proof is that, this shows that even numbers less than $p_1 p_2 \cdots p_n$ already contain new primes, Euclid showed that numbers bigger than $p_1 p_2 \cdots p_n$ start requiring new primes but here we show that way before that we already need new primes.

Second Case

Talking about φ, our Chinese friend can also help us prove that if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$. Simply by setting up the following system of congruences

$$\begin{aligned} x &\equiv a_m \pmod{m} \\ x &\equiv a_n \pmod{n} \end{aligned}$$

as long as $a_{m,n}$ are co-prime to m and n then it will be co-prime to mn as well. The question now is if there is another number that is co-prime to mn but is not co-prime to m or n, well the answer is obviously no because if a number y is co-prime to mn when we break it down to the system of congruences $y \equiv c_m \pmod{m}$ and $y \equiv c_n \pmod{n}$, $c_{m,n}$ will be co-prime to m and n respectively.

Since there are $\varphi(m)$ and $\varphi(n)$ numbers co-prime to m and n, our Chinese friend guarantees there are only $\varphi(m)\varphi(n)$ unique solutions modulo mn.

-=-

Doing problem solving is in a essence doing a depth first search, starting from the root node (which is the problem node), we map out different approaches we can take to tackle the problem, we usually employ greedy algorithm to choose the most promising branch. We then traverse deeper into this particular branch to see if we can get to a solution.

The problem is sometimes we get too comfortable with a certain approach and gravitate towards that branch no matter what (note that greedy algorithm doesn't always pay off). Also, sometimes we need to go too deep into a branch to see if an approach works.

So if we can put some values into the edges of this tree maybe we can deploy Dijkstra or even dynamic programming approaches to choose the best approach in problem solving.

Of course the challenge is that most times we don't even know what branches (approaches) are available, we need to create new ones and that is where the real challenge lies.

-=-

How to proof that given two real numbers $a < b$, there is a rational number between them, in fact there are infinitely many rational numbers between them. My strategy is as follows, but first, let's see it with an example, take two numbers 0.1 and 0.2, we want to find a rational number, m/n, between them where m and n are integers,.

What do we do? what we do is "stretch" the interval by multiplying both numbers by some big number so that we can generate integers between them, for example, multiply both by 10 and we get $[0.1, 0.2] \to [1, 2]$ we haven't inserted an integer between them yet, so we need a bigger number, let's try 20 and we get $[0.1, 0.2] \to [2, 4]$, and we have an integer between them, *i.e.* 3, and if we divide it by 20 we get our rational number in between 0.1 and 0.2, and if we check, $\frac{3}{20} = 0.15$ is indeed between 0.1 and 0.2.

We can generate more integers between them by multiplying them by an even bigger number, say 2000, then the interval becomes $[0.1, 0.2] \to [200, 400]$ and this time we have 199 integers in between, if we divide each of those by 2000, we have 199 rational numbers between $[0.1, 0.2]$.

So here goes the proof. Take the difference between a and b

$$\Delta = b - a$$

the goal is to make this interval to contain integer, so if we pick $n = \lceil 1/\Delta \rceil$

$$n(b-a) \geq 1$$

but here we are still not guaranteed to have an integer in between them, but the solution is obvious, if we want N integers between them we just need to multiply n by $N+1$

$$(N+1)n(b-a) \geq N+1$$

so any integer in between $((N+1)na, (N+1)nb)$ divided by $(N+1)n$ will be the rational number between (a, b) and there are at least N of them and since we can set any N we want there are infinitely many rational numbers between any two real numbers a and b.

We can also use the above to show that there are infinitely many irrational numbers between two real numbers a and b. The trick is to add an irrational number to both a and b, *i.e.* first we pick a rational number between two real numbers $a+\pi$ and $b+\pi$

$$a + \pi < \frac{m}{n} < b + \pi$$

this means that

$$a < \frac{m}{n} - \pi < b$$

since m/n is rational adding $-\pi$ makes it irrational, so that means that there are infinitely many irrational numbers between any two real numbers. However, we can choose any irrational number we want besides π, something like $\sqrt{2}, \sqrt{3}, \ldots$.

The usual proof for the existence of a rational between two real numbers is as follows, select a rational number such that

$$\frac{1}{n} < b - a$$

choose m such that

$$m - 1 \leq na < m$$

so

$$\frac{m}{n} - \frac{1}{n} \leq a < \frac{m}{n}$$

therefore

$$b = (b - a) + a > \frac{1}{n} + \left(\frac{m}{n} - \frac{1}{n}\right)$$
$$b > \frac{m}{n} > a$$

-=-

=-=-

Proof that $p^{1/n}$ is irrational where $n > 1$ and p is prime, assume it's rational a/b with $(a, b) = 1$ then

$$\frac{a^n}{b^n} = p$$
$$\to p \mid a^n$$

which means that $p|a$ which also means $p^{n-1}|b^n$ which also means $p|b$, a contradiction since $(a, b) = 1$, the interesting question now is how to design a new irrational number, maybe using continued fraction?

-=-

=-=-

Completeness of the real numbers $\mathbb{R}$ means that $\mathbb{R}$ has no gaps, it is not so with the rationals, for example the set $\{r \in \mathbb{Q}, r^2 < 2\}$ does not have a least upper bound in $\mathbb{Q}$.

Say there is a least upper bound a/b such that $a^2/b^2 > 2$ then

$$\frac{a^2}{b^2} - 2 > 0$$

we can show that there's another rational number such that it is smaller than a/b but its square is still bigger than 2 rendering it smaller than the least upper bound, a contradiction.

Pick another number $\frac{a}{b+\Delta}$ where Δ is a rational number, we want this number to still be greater than $\sqrt{2}$

$$\frac{a^2}{(b + \Delta)^2} > 2$$
$$a^2 - 2b^2 - \Delta(4b + 2\Delta) > 0$$

since we can set Δ to be as small as possible we can always set the above inequality to be true, for example first choose $\Delta = 0.1$ which is a rational number, if this is too big we move the decimal point $\Delta = 0.01$ and so on.

Or we can just invoke the fact that there are infinitely many rational between any two real numbers and we are done.

-=-

We can also extend congruence to rational numbers

$$\frac{a}{b} \equiv c \pmod{d}$$

as long as $(b, d) = 1$, we can think of it as $ab^{-1} \equiv c \pmod{d}$ and b has an inverse as long as $(b, d) = 1$.

Because if d divides

$$\frac{a}{b} - c = \frac{a - cb}{b}$$

then $d|(a - cb)$ or $a - cb \equiv 0 \pmod{d}$ however, if $(b, d) \neq 1$ then we know from our experience that for c to have a solution (b, d) must divide a, so if $(b, d) = 1$ we are guaranteed to have a solution.

What happens if we add two fractions?

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'} \equiv C \pmod{d}$$

suppose $C \not\equiv c + c' \pmod{d}$ that means $C \equiv c + c' + \Delta \pmod{d}$ and

$$\begin{aligned}
\frac{ab' + a'b - Cbb'}{bb'} &\equiv \frac{ab' + a'b - (c + c' + \Delta)bb'}{bb'} \pmod{d} \\
&\equiv \frac{(a - cb)b' + (a' - c'b')b - \Delta bb'}{bb'} \pmod{d} \\
&\equiv -\Delta \pmod{d}
\end{aligned}$$

meaning $\Delta \equiv 0 \pmod{d}$ and therefore $C \equiv c + c' \pmod{d}$.

With this in mind we can show that

$$\sum_{x=1}^{p-1} \frac{1}{x} \equiv 0 \pmod{p}$$

where p is an odd prime. This is because $1/x \equiv x^{-1} \pmod{p}$ so the sum becomes

$$\sum_{x=1}^{p-1} x^{-1} \pmod{p}$$

and we know that the inverse of every element of $(\mathbb{Z}/p\mathbb{Z})^*$ is unique therefore

$$\begin{aligned}\sum_{x=1}^{p-1} x^{-1} \pmod{p} &\equiv \sum_{x=1}^{p-1} x \pmod{p} \\ &\equiv \frac{(p-1)p}{2} \pmod{p} \\ &\equiv 0 \pmod{p}\end{aligned}$$

another show of force of the power of congruence :)

-=-

Another fun thing to do with congruence, given

$$2^4 + 5^4 = 2^7 \cdot 5 + 1 = 641$$

show that $2^{32} + 1 \equiv 0 \pmod{641}$. The above two equations mean that

$$\begin{aligned}2^7 \cdot 5 + 1 &\equiv 0 \pmod{641} \\ 5 &\equiv -(2^7)^{-1} \pmod{641}\end{aligned}$$

so

$$\begin{aligned}2^4 + 5^4 &\equiv 2^4 + (-(2^7)^{-1})^4 \pmod{641} \\ 0 &\equiv 2^4 + 2^{-28} \pmod{641} \\ \rightarrow 0 &\equiv 2^{32} + 1 \pmod{641}\end{aligned}$$

since $(2, 641) = 1$, 2 has an inverse.

-=-=-=-=-=- PRIME NUMBER THEOREM -=-=-=-=-=-

What do you need to analytically prove the prime number theorem? Here's a list of things

- Equivalence between $\pi(x) \sim x/\log x$ and $\psi(x) \sim x$.

- Integral of ψ, $\psi_1 = \int_1^\infty \psi(x)dx$ and how to express this integral in terms of a sum of $\Lambda(n)$, answer: Abel's identity.
- The correspondence between the asymptotic form of ψ_1 and ψ, *i.e.* the asymptotic form of ψ is just the derivative of the asymptotic form of ψ_1, since ψ_1 is the integral of ψ.
- Integral form of ψ_1/x^2. To do this we need the summation form of $\zeta'(s)/\zeta(s)$, this is gathered through the properties of Dirichlet series.
- Various properties of $\zeta(s)$ and $\zeta'(s)$ along the line $\sigma = 1$ so that we can integrate the above along $\sigma = 1$.
- A very important one, Riemann-Lebesgue lemma to show that the integral above is zero.
- And finally sum subtle technical things where we exchange sums and integrals.

-=-

$$n! > \left(\frac{n}{e}\right)^n$$

Start with k an integer starting from 2

$$\begin{aligned} k \geq x, \qquad & x \geq 1 \\ \rightarrow \log k \geq \log x & \\ \int_{k-1}^{k} \log k \; dx = \log k \geq \int_{k-1}^{k} \log x \; dx & \end{aligned}$$

so

$$\begin{aligned} \sum_{k=2}^{n} \log k \geq \sum_{k=2}^{n} \int_{k-1}^{k} \log x \; dx & \\ \rightarrow \log n! \geq \int_1^n \log x \; dx & \\ \log n! \geq n \log n - n + 1 & \\ \log n! - (n \log n - n) \geq 1 & \end{aligned}$$

exponentiating, we get the inequality we want.

-=-

Show that $y^2 = x^3 + 16$ only has $(x, y) = (0, \pm 4)$ as solutions.

$$(y-4)(y+4) = x^3$$

For y odd $\gcd(y-4, y+4) = 1$ since the common divisors must divide $8 = 2 \cdot 2 \cdot 2$ but $y \pm 4$ is odd so it doesn't have 2 as a factor, thus their gcd is 1. In this case $y-4$ and $y+4$ are both cubes but there are not cubes separated by 8.

This means x and y are both even, but if that's the case

$$(2y_1)^2 = (2x_1)^3 + 16$$
$$y_1^2 = 2x_1^3 + 4$$

this means $2|y_1$ thus

$$(2y_2)^2 = 2x_1^3 + 4$$
$$2y_2^2 = x_1^3 + 2$$

this means $2|x_1$

$$2y_2^2 = (2x_2)^3 + 2$$
$$y_2^2 = 4x_2^3 + 1$$

and

$$(y_2 - 1)(y_2 + 1) = 4x_2^3$$

if y_2 is even we are done because the LHS is odd and the RHS is even, so $x_2 = 0$, if y_2 is odd then $(y_2 \pm 1)/2 = a_\pm$ and $a_+ - a_- = 1$

$$a_+ a_- = x_2^3$$
$$a_+(a_+ - 1) = x_2^3$$

and $\gcd(a_+, a_+ - 1) = 1$ so each of them must be a cube but there are no two cubes separated by 1. Except for ± 1 and 0 but that also means that $x_2 = 0$.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Just a problem I saw "somewhere" :) Find all solutions to

$$x^3 + y^3 + z^3 = (x + y + z)^3$$

well, I initally assumed they were all integers but it is not so, this is an "implicit" equation unlike Fermat's last theorem, we can't just randomly set two of them and the last will follow.

Expanding the RHS and canceling similar terms from LHS

$$\begin{aligned} 0 &= 3yz^2 + 3xz^2 + 3y^2z + 6xyz + 3x^2z + 3xy^2 + 3x^2y \\ &= 3(yz^2 + xz^2 + y^2z + 2xyz + x^2z + xy^2 + x^2y) \\ &= 3((y + x)z^2 + 2xyz + x^2(z + y) + (x + z)y^2) \end{aligned}$$

at this point we want to factorize the RHS, my initial idea was to do a quadratic formula for y, thus I massaged it into $ay^2 + by + c$, as to why I chose y I'm not sure :)

$$\begin{aligned} yz^2 + xz^2 + y^2z + 2xyz + x^2z + xy^2 + x^2y &= y^2(z + x) + y(z^2 + 2xz + x^2) + (xz^2 + x^2z) \\ &= y^2(z + x) + y(z + x)^2 + xz(z + x) \\ &= (z + x)(y^2 + y(z + x) + xz) \\ &= (z + x)(y + z)(y + x) \end{aligned}$$

but as you can see I didn't even need to use the quadratic formula LOL

Thus the solutions to

$$x^3 + y^3 + z^3 = (x + y + z)^3$$

is given by

$$0 = (z + x)(y + z)(y + x)$$

any of them brackets equal zero and we're good which means that at least one of them has to be negative.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

My reflection on the quadratic reciprocity formula (by Gauss of course who else). My first question is that how does one relate a number in mod p to another congruence mod q because it seems like this is what the reciprocity formula is all about.

But I was wrong, looking at different proofs what I found is this

1. We know that for a modulo prime p the following numbers (and only the following numbers) are quadratic residues modulo p

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

2. From Euler's formula we know that for a prime p

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$$

which can be shown fairly easily by expressing a in terms of a primitive root of p.

3. So either for Euler's formula or by listing all the quadratic residues modulo p, we need to do $\frac{p-1}{2}$ operations to determine whether a number is a quadratic residue or not, no other way around it.

4. This minimum of $\frac{p-1}{2}$ operations also applies even if we use Gauss's lemma that starts with multiplying a into a sequence of $\frac{p-1}{2}$ numbers

$$x \in \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$$

such that the Legendre symbol is given by

$$\left(\frac{a}{p}\right) = (-1)^n \pmod{p}$$

where n is the number of numbers ax that is congruent to $-x$ modulo p. We still need to do $\frac{p-1}{2}$ operations but this is a move in the right direction because calculating $(-1)^n$ is easy, we do not need to do $\frac{p-1}{2}$ operations we just need to know the parity of n.

Even calculating the parity of n actually takes $\frac{p-1}{2}$ operations

$$n \mod 2 = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{ax}{p} \right\rfloor$$

(note that this formula only works if a is odd).

5. Finally when we come to the quadratic reciprocity formula itself

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

it seems that we need to only do half the work, once we know $\left(\frac{p}{q}\right)$ we know the other Legrende symbol as well (to get $\left(\frac{p}{q}\right)$ we still need to do $\frac{p-1}{2}$ operations), but this is not true, calculating $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ still takes $\frac{p-1}{2} + \frac{q-1}{2}$ operations but the good thing is that since we are dealing with -1 we only need to know the parity of the exponent thus it saves us some time.

So the moral of the story for me is that quadratic reciprocity formula is the tale of how to transform the same information into a more useful more efficient form,*i.e.* just like the conservation of energy in physics, here the amount of work cannot be reduced, but efficiency can certainly be increased.

This is in direct contrast to the situation in $\mathbb{Z}$, to check if a number n is a perfect square we sort of need to do only roughly $\sqrt{n}$ operations, one way to see this is to realize that a perfect square is a sum of consecutive odd numbers

$$n^2 = 1 + 3 + 5 + \ldots$$

which is clearer if you draw them out in terms of boxes (the benefit of this approach is that we need not do any multiplication).

P.S. of course my favorite proof of the quadratic reciprocity formula is the one utilizing Chinese Remainder Theorem, but even in that case, the $\frac{p-1}{2}$ operations cannot be avoided.

-=-

On the formula for $\left(\frac{2}{p}\right)$, we start with Wilson's formula

$$(p-1)! \equiv -1 \pmod{p}$$

we then notice that, for example $p = 5$

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot 4 &\equiv 2(1 \cdot 2) \cdot (1 \cdot 3) \\ &\equiv 2\left(\frac{5-1}{2}\right)! \cdot (1 \cdot -2) \\ &\equiv 2^{\frac{5-1}{2}} \left(\frac{5-1}{2}\right)!(-1) \cdot \left(\frac{5-1}{2}\right)! \end{aligned}$$

and for $p = 11$

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 &\equiv 2(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5) \cdot (1 \cdot 3 \cdot 5 \cdot 7 \cdot 9) \\ &\equiv 2^{\frac{11-1}{2}} \left(\frac{11-1}{2}\right)! \cdot (1 \cdot -2 \cdot 3 \cdot -4 \cdot 5) \\ &\equiv 2^{\frac{11-1}{2}} \left(\frac{11-1}{2}\right)!(-1)^2 \cdot \left(\frac{11-1}{2}\right)! \\ &\equiv 2^{\frac{11-1}{2}} (-1)^{\lfloor (11-1)/4 \rfloor} \left(\left(\frac{11-1}{2}\right)!\right)^2 \end{aligned}$$

Therefore

$$\begin{aligned} (p-1)! &\equiv 2^{\frac{p-1}{2}} (-1)^{\lfloor (p-1)/4 \rfloor} \left(\left(\frac{p-1}{2}\right)!\right)^2 \\ (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2}\right)!\right)^2 &\equiv 2^{\frac{p-1}{2}} (-1)^{\lfloor (p-1)/4 \rfloor} \left(\left(\frac{p-1}{2}\right)!\right)^2 \\ (-1)^{(p-1)/2 + \lfloor (p-1)/4 \rfloor} &\equiv 2^{\frac{p-1}{2}} \end{aligned}$$

so we didn't need Wilson's formula after all but as you see we need something to generate $2^{\frac{p-1}{2}}$, and this is the recurring theme throughout quadratic reciprocity, be it Gauss's lemma or in calculating the parity of the exponent in Gauss's lemma. I intially thought of Wilson's formula not for the factorial but for the -1 since Legendre's symbols are either ± 1 ot 0.

-=-

Why the minus sign? the integrand is $\frac{(-x)^s}{e^x - 1}$, there's a minus sign in front of x. This is due to the choice of contour. Note that we are going from $+\infty$ to left all the way to 0 and then to the right all the way to $+\infty$.

If there's no minus sign and this is the cut we choose, then

$$\begin{aligned} x^s &= e^{s \log x + 0 \cdot \pi i}, && \text{going from } +\infty \text{ to } 0 \\ x^s &= e^{s \log x + 2 \cdot \pi i}, && \text{going from } 0 \text{ to } +\infty \end{aligned}$$

and when we add the two integrals we get zero

$$e^{s\log x+0\cdot\pi i}-e^{s\log x+2\cdot\pi i}=0$$

so if we don't want the minus sign we need to choose the other cut, coming from $-\infty$ to zero and back to $-\infty$ so that the phases will be πi and $-\pi i$.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Compact here means closed and bounded.

The whole integral is zero thanks to a corollary of Goursat theorem which says that

$$\oint_C f(z)dz=\sum_{k=1}^{n}\oint_{C_k} f(z)dz$$

where the contours C_k's are all inside of C.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-