Jumbled up thoughts

Stefanus Koesno[1]

[1] Somewhere in California

San Jose, CA 95134 USA

(Dated: August 9, 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. 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

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

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

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

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

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

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

3

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 $0 \equiv$ (mod 4), so to have a chance of a solution $a \equiv -1$ (mod 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(2+0)^3 = \binom{3}{0}2^3 \cdot 0^0 + \binom{3}{1}2^2 \cdot 0^1 + \binom{3}{2}2^1 \cdot 0^2 + \binom{3}{3}2^0 \cdot 0^3$$

$$2^3 = 2^3 \cdot 0^0$$

$$2^3/2^3 = 0^0$$

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

-=-
=-=-

Given that we can factorize the following

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

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

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

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

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

$$= k$$

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

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

6

and

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

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

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

denote the set of distinct prime divisors of k and d as $\mathbb{K} = \{p_1, p_2, \ldots, p_z\}$ and $\mathbb{D} = \{p_{d_1}, p_{d_2}, \ldots, p_{d_s}\}$ 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 $k/d \geq p_{j_1}^{e_{j_1}} p_{j_2}^{e_{j_2}} \ldots p_{j_t}^{e_{j_t}} > 2^t > t$, *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

9

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

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

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

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

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.

-=-

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.

-=-