# Re: Towards a Formula for Primes

***Source:*** http://sci.tech−archive.net/Archive/sci.math/2007−05/msg01618.html

---

- *From*: "charleswehner@xxxxxxxxxxx" <charleswehner@xxxxxxxxxxx>
- *Date*: 9 May 2007 11:42:02 −0700

---

On 9 Mai, 16:34, Douglas Eagleson <eaglesondoug...@xxxxxxxxx> wrote:
.. On May 9, 10:30 am, Pubkeybreaker <pubkeybrea...@xxxxxxx> wrote:

.. > Wubba wubba wubba ........ More word salad; grab words at random
and
.. > paste
.. > them together.... The result has no meaning whatsoever.
..
.. Well, the test was to be a normal open thinker. And if you complain
.. of giberish the reality is gone from your area of interest. A
.. collection of words is to be examined using all thinking not jackass
.. predicate. So go home and complain on a different newsgroup.
..
.. Who gives a crap about your kind thinking correctly.− Zitierten Text
ausblenden −
..
I warned you that there are "flame warriors" who fight their flame
wars in the hope of winning what they think is a prize fight.

I catch the drift of what you were saying. You homed in on the notion
that a general formula for primes might only be found in geometry.

I will restate the problem.

There is no general formula for primes. The Japanese made a fuss when
they thought one had been discovered. Accordingly, if there is a
general formula for primes, those who claim there is should reveal it,
go to Japan and later go BACK to Japan to explain the hoax.

I do not believe all the Japanese top mathematicians, and their chief
economist were wrong.

If anybody has got a general formula for primes, I will personally
recommend them for the "Nobel Prize for Mathematics", which ALSO does
not exist.

There are recipes for "filters". For example, you accept 2 and 3 as
primes. Now, you go to 5 − a prime. Now you add 6. You get 11 − a
prime. Add 6 again. 17 is prime. Add 6. 23 is prime. Add 6. 29 is

prime. Add 6. You have 35. WHOOPS!

Try starting with 7. Add 6. 13 is prime. Add 6. 19 is prime. Add 6.
You have 25. WHOOPS!

This is the 6n plus−or−minus 1 algorithm.

You have to test each one by division by all previous primes, to overcome the "WHOOPS" numbers − the false primes.

A proper formula for primes needs so such test.

You refine the algorithm. Given a number suspected of being prime, you only need to divide by all primes up to the square−root of that number. Higher primes, if divided into a number, will give a quotient below the square−root which has already been tested. So higher numbers are superfluous.

The number of "WHOOPS" effects increases as the numbers grow larger. Huge numbers have a huge number of smaller primes "beneath them", up to the square root, which are possible factors. Accordingly, primes get rarer and rarer as the numbers grow. There are at the start, due to 6n plus−or−minus 1, one in three primes. In the range 2 to 65535 there are however only about 1 in TEN.

Refinements have been built upon refinements until the science of testing of primes has become very, very advanced. However, there is no general formula for primes.

The CIA know that. When the Diffie−Hellman algorithm for data encryption arrived, they got themselves a giant computer. The US government banned such methods of encoding as the random−book code, which cannot be broken. Instead, they put forward Diffie−Hellman as the Public Key Encryption algorithm. There are two primes. One is the public key, which anybody can use for coding. The other is the private key that only the recipient has got. And only the private key will decrypt the data.

By the time you have a hundred−figure number, primes are millions of millions apart. One would have to factorize millions of huge numbers to find the key. A personal computer cannot do this, but the CIA supercomputer with the very latest filter algorithms can. So the man in the street is allowed, under US law, to have secrets from some other man in the street, but not from the government.

What is holding up the GENERAL formula? That is to say, the one which encapsulates ALL the parameters of primes.

I had considered Gödel incompleteness. There are many things arithmetic cannot do, because of that incompleteness.

I had considered bringing in some property of Pythagorean GEOMETRY, so that the axioms of geometry might augment those of four−function arithmetic.

I found the neogenesis of primes in that geometry, and thought I was on the right lines. My Pythagorean Perimeters Theorem actually CREATES a prime, when a coprime duple turns into a coprime triple.

I was BRILLIANTLY shot down in flames by "Quasi", when he showed that simple addition will do this.

I examined the "anatomy" of a logical adding machine, and of a logical subtracting machine. I showed that they are "mirror−image twins". The functions they carry out − addition and subtraction − are also "mirror−image−twins". They share a similar set of properties.

So, as a corollary (which in mathematics means "a thing proven at the same time"), Quasi had proven that simple subtraction will also contain the neogenesis of primes, although he did not state this himself.

So I gave up the approach to look for the solution in geometry. I now know that geometry offers no more help than addition and subtraction do.

My mind has now turned to the PSEUDO−RANDOMNESS of the occurrence of "Whoops".

Many moons ago, I was given an AEG invention to develop. It was called the "pseudo−noise technique" for secure signalling. A shift−register had an exclusive−OR (XOR) gate attached to it, such as at the two most significant places. The output from that XOR went back into the least significant position.

If such a pseudo−noise generator has all zeroes in it, zeroes will be fed back. It will stay "latched up" in the all−zero state.

Apart from that, there are (2 to the power n) patterns possible in the register. So the pseudo−random pattern will repeat after every (2 to the power n) less 1 clock cycles.

It is DETERMINISTIC. That is to say, if one loads a 1 into each of two such generators in the same position, and starts them up, running on the same clock, the outputs will match. That was the basis of the invention − a local and a remote pseudo−random code are compared.

Related to pseudo−randomness is IRRATIONALITY. Strictly, according to the Pythagoreans, this means not being a ratio of whole numbers. However, one can enrich ones understanding of this.

There are infinite irrational numbers, including e and pi.

Consider e.

You take 1, and put it into the result. You also take 1 as the term.
Divide the term by 1 and add into the result.
Divide the term by 2 and add into the result.
Divide the term by 3 and add into the result.
Continue FOREVER.

There is NEWNESS in the denominator. First it is 1, then 2 then 3, and so on. This NEWNESS scrambles the digits that are generated, and makes them unpredictable.

The "term" is a factorial. So I call this style of irrationality FACTORIAL IRRATIONALITY. It shares its properties with the hyperbolic sine and hyperbolic cosine, in a tangled way.

consider pi.

You take 4 and put it into the result.
Divide 4 by 3 and subtract from the result.
Divide 4 by 5 and add to the result.
Divide 4 by 7 and subtract from the result.
Divide 4 by 9 and add to the result.
Continue FOREVER.

The denominator is rising steadily in twos. This is the source of the NEWNESS that creates unpredictable digits in pi. This style of irrationality is therefore a LINEAR IRRATIONALITY.

However, all forms of irrationality are DETERMINISTIC.

One wonders whether pseudo−randomness and irrationality are closely related.

It may be that the conventional arithmetic cannot handle pseudo−random events, like the pseudo−random appearance of "WHOOPS" that I first started with.

If that is so, it may prove necessary to introduce the XOR function into conventional four−function arithmetic just to cope with pseudo−randomness.

Such a mathematical system I would dub "transarithmetic". Perhaps it exists out there under a different name, but if not you read it here first.

The test really is to see whether the XOR function can mirror the primes. If for example, one XORs a growing number against another growing number, the algorithm will still be deterministic. However, the (2 to the power n) will be growing steadily, so that the sequence

− like the sequence of primes − will be infinite. It is looking good.
But will the psudo−randomness EXACTLY match the primes, in some configuration − or is there some reason for it to be impossible?

There is no point in adding the OR and the AND function into arithmetic, because then it would be a LOGIC.

So I am toying with the idea that arithmetic cannot find a general formula unless it has at least one XOR in it. That is a possibility. Quasi has steered me away from taking the neogenesis of primes in geometry too seriously.

Charles Douglas Wehner

.