

Did Euclid Know That 5 is Prime?
A Preliminary Report

Roger Waggoner
University of Louisiana at Lafayette
rwag@louisiana.edu

Let's begin by looking at Euclid's proof that the collection of primes is infinite. The modern version is usually presented something like this. If p_1, p_2, \dots, p_n are primes, then the number

$A = 1 + \prod_{i=1}^n p_i$ is not a multiple of any of the p_i 's. Thus the prime factors of A must be different

from p_1, p_2, \dots, p_n . That is, for any given finite set of primes, we can always find a prime which is not in that set. Thus the set of all primes is not finite.

Euclid's actual proof, [2], used three primes, rather than n . The numbers are represented as line segments, and instead of saying that a number B is a multiple of A , he says that B is measurable by A . If you had pieces of rope of integer lengths, you could determine if a piece was prime by seeing if it was measurable by any smaller piece, other than the unit piece.

Imagine this scene. We have a young Euclid. Lots of time and lots of rope. He notices that 2 and 3 are prime while 4 is not. He is interested in finding more primes. He could just start testing numbers, but he wants to be sure of success. He uses the idea in his proof. What primes does he discover? Here is the beginning of a sequence $\{A_0, A_1, A_2, \dots\}$ of numbers that he would test, along with their prime factors.

A_i	<u>New Primes</u>
2	2
$1 + 2 = 3$	3
$1 + 2 \cdot 3 = 7$	7
$1 + 2 \cdot 3 \cdot 7 = 43$	43
$1 + 2 \cdot 3 \cdot 7 \cdot 43 = 1807$	13, 139

In the fifth stage, the two new primes are listed in ascending order. At this stage we have to make a decision about the definition of A_5 . Let's define $A_{n+1} = 1 + (\text{product of previously used primes}) (\text{first unused prime})$. Thus $A_5 = 1 + 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13$ and $A_6 = 1 + 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 \cdot 139$.

Continuing, we get

$A_5 = 23479$	53, 443
$A_6 = 3263443$	3263443
$A_7 = 172962427$	11, 269, 58453
$A_8 = 76622354719$	47653, 1607923
$A_9 = 250052687147974075$	5, 129491, 77241719393

$$A_{10} = 2750579558627714815 \quad 550115911725542963$$

Notice that 5 finally shows up as a factor of A_9 . The original title of this talk was “5 is the fifteenth prime”. Also, 5^2 is actually a factor of A_9 . That’s the first time a prime factor of multiplicity greater than 1 appears. 5 is also a factor of A_{10} . This phenomenon is possible because 5 was not used to produce A_{10} . It is also of some interest to note that the TI-92 calculator failed to factor A_9 completely. Which primes are we producing here? Will 17 ever show up? Will we eventually get any prime we want?

In January, 2003, this author had a private conversation with Ezra Brown at the Joint Mathematics Meetings in Baltimore. According to Brown, if one alters the sequence of A_n ’s by using only the smallest new prime at each stage, and discard any other new primes, then it is an open question as to whether you will generate all primes. If you follow this procedure, your sequences look like this.

<u>A_i</u>	<u>New Primes</u>
2	2
3	3
7	7
43	43
1807	13
23479	53
1244335	5
6221671	6221671
38709183810571	38709183810571

Notice here that 5 is now the seventh prime. Also, after the first few steps this sequence of primes doesn’t look at all like the first one. What’s going on here? I don’t have a clue.

Here is yet one more way to generate new primes in a method similar to Euclid’s. In forming the sequence of A_i ’s, what if we didn’t discard anything? Let $A_{n+1} = 1 + \prod_{i=1}^n A_i$.

We get the following sequences.

<u>A_i</u>	<u>New Primes</u>
2	2
3	3
7	7
43	43
1807	13, 139
3263443	3263443
10650056950807	547, 607, 1033, 31051
113423713055421844361000443	29881, 67003, 9119521, 6212157481

We have fifteen primes, but not 5

Notice that $A_{n+1} = 1 + \prod_{i=1}^n A_i = 1 + A_n \left(\prod_{i=1}^{n-1} A_i \right) = 1 + A_n (A_n - 1) = A_n^2 - A_n + 1$.

We can generate the sequence of A_i 's by starting at 2 and iterating the function $f(x) = x^2 - x + 1$.

Where does 5 appear in our list of primes? Reduce the A_i 's, mod 5. You get 2, 3, 2, 3, This pattern continues forever. In iterating $f(x) = x^2 - x + 1$, find the residue, mod 5, of A_i before inputting it into the function. $f(2) = 3$ and $f(3) = 2$, so the residues of the A_i 's will alternate 2, 3, 2, 3, 5 will never appear in our list of primes.

You can test any prime p this way. Try 31. The residues of the A_i 's, mod 31 are

2, 3, 7, 12, 9, 11, 18, 28, 13, 2, ...

What happens after 2 appears for the second time? $f(2) = 3$, $f(3) = 7$, etc. The pattern repeats, just like with a repeating decimal. 31 will never appear in this list of primes.

Try 13. The residues, mod 13 are 2, 3, 7, 4, 0. 13 appears at the fourth iteration. (We already know that).

If we arrange our primes in the usual order we have 2, 3, 7, 13, 43, ...

Will any of the missing primes less than 43 ever appear? No.

What's the next prime in the sequence?

The residues of the A_i 's, mod 73, are 2, 3, 7, 43, 55, 51, 69, 21, 56, 15, 65, 0.

Thus 73 is the next term in the sequence, appearing as a factor of A_{11} . (Nothing between 43 and 73 works.) The next prime to appear in the sequence is 139.

There are a lot of questions one can ask about these sequences.

For instance:

What are the densities of the three sequences?

Changing the initial value of A_0 to a number other than 2 can produce very different sequences.

When does changing the initial value change the collection of primes produced? Can changing the initial value change the density of the resulting sequence of primes?

It is relatively easy to test any prime for the third sequence. Is there an easier way? That is, could one test 1212121 without going through a possible 1212121 steps?

What if we threw in some randomness? Generate a sequence like this. For each prime p , choose elements at random from $\{0, 1, 2, \dots, p-1\}$, with replacement. p is in our sequence if we choose 0 before another number is chosen twice. How does the expected value of the number of primes in this sequence compare to our third sequence?

Other questions could be forthcoming.

1. Brown, Ezra, private conversation in Baltimore, MD, Jan 2003.
2. Fauvel, John and Gray, Jeremy, "The History of Mathematics: A Reader", the Open University and the MAA, Washington, D.C. 1987.