AN IMPROVED VERSION OF THE SIEVE OF ERATOSTHENES

One of the oldest and best known algorithms for picking out primes from a sequence of positive odd integers is the Sieve of Eratosthenes. Eratosthenes of Cyrene(276-195BC) was a polymath working at the famous Greek school in Alexandria, Egypt. He was a contemporary of Archimedes and is best known for obtaining the first accurate measurement of the circumference of the Earth. His sieve algorithm starts in essence with a list of the first n odd integers listed in ascending order as shown-

S={3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49,51,…}

One next takes the first odd number 3, which is a prime, and divides it into each subsequent term. Those terms which divide exactly produce the composite number sequence-

C_3={9, 15, 21, 27, 33, 39, 45, 51,…}

Next we repeat the procedure but divide by the second term in the sequence S, namely 5, which is also a prime. This manipulation produces a new sequence of composite numbers-

C_5={15, 25, 35, 45,.. }

Repeating the procedure one more time with 7, the third odd prime in S, produces the composite sequence-

C_7={21, 35, 49,…}

If we now remove those elements in S which are also present in C_3, C_5, and C_7, we are left with the prime number list-

P={3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,.. }

Note that some of the composite numbers in the C_p sequences overlap with each other such as 45 in C_3 and C_5. The maximum p required in C_p is typically equal to sqrt(largest term in S). For the above we have sqrt(51)=7.1414.. . Thus we can stop with C_7 to find all primes in the range 3<p<51. We note that the Eratosthenes algorithm can become rather cumbersome as the elements in S get large.

It is our purpose here to introduce a modified approach to the Sieve of Eratosthenes. The new approach is based on our recent observation that all primes have the form N=6n±1 provided that N>3. In addition to be prime, any number of the form N=6n+1 must also have the additional property that $p_n(p_n+6m)$ cannot equal N. Here p_n=5, 7, 11, 13,…≈sqrt(N) and m=1,2,3,… . Thus N=817=6(136)+1 is

a composite number since $p_n(p_n+6m)\equiv N$ for m=4 and $p_n=-3m+\sqrt{(9m^2+N)}=19$. When 19 is divided into 817 it produces 43. For a number N=6n-1 to be prime it is also necessary that $p_{n(}p_{n+1}+6m)$ be not equal to N. Thus N=135=6(23)-1 is not a prime number since 5(7+5m)=135 at m=4 and $p_n=5$.

To carry out a Eratosthenes Sieve operation on N=6n+1 and 6n-1 we start with the two odd number sequences-

$S_+=\{7,13,19,25,31,37,43,49,55,61,67,73,79,85,91,97,103,..\}$

and-

$S_-=\{5,11,17,23,29,35,41,47,53,59,65,71,77,83,89,95,101,..\}$

Next we generate the composite number sequences-

$C_{+,5,m}=25+30m=\{25,55,85,..\}$, $C_{+,7,m}=49+42m=\{49,91,..\}$

$C_{-,5,m}=35+30m=\{35,65,95,..\}$ $C_{-,7,m}=77+42m=\{77,..\}$

Removing these numbers from the respective S sequences, leaves us with-

$P_+=\{7,13,19,31,37,43,61,67,73,79,97,103,..\}$

and

$P_-=\{5,11,17,23,29,41,47,53,59,71,83,89,101,..\}$

We call the P_+ and P_- sequences the Q primes. They constitute essentially all the primes above N=3. One can construct tables of p_n versus m listing the composite numbers which must be eliminated from the original S_+ and S_- sequences to generate these P_+ and P_-prime lists . Here are two easily generated tables listing these composites over the range $5\leq p_n\leq 41$, $0\leq m\leq 7$ –

VALUE OF $N=p_n(p_n+6m)$ FOR 6n+1 COMPOSITES

p_n\m	0	1	2	3	4	5	6	7
5	25	55	85	115	145	175	205	235
7	49	91	133	175	217	259	301	343
11	121	187	253	319	385	451	517	583
13	169	247	325	403	481	559	637	715
17	289	391	493	595	697	799	901	1003
19	361	475	589	703	817	931	1045	1159
23	529	667	805	943	1081	1219	1357	1495
29	841	1015	1189	1363	1537	1711	1885	2059
31	961	1147	1333	1519	1705	1891	2077	2263
37	1369	1591	1813	2035	2257	2479	2701	2923
41	1681	1927	2173	2419	2665	2911	3157	3403

VALUES OF $N=p_n(p_{n+1}+6m)$ for 6n-1 COMPOSITES

Pn\m	0	1	2	3	4	5	6	7
5	35	65	95	125	155	185	215	245
7	77	119	161	203	245	287	329	371
11	143	209	275	341	407	473	539	605
13	221	299	377	455	533	611	689	767
17	323	425	527	629	731	833	935	1037
19	437	551	665	779	893	1007	1121	1235
23	667	805	943	1081	1219	1357	1495	1633
29	899	1073	1247	1421	1595	1769	1943	2117
31	1147	1333	1519	1705	1891	2077	2263	2449
37	1517	1739	1961	2183	2405	2627	2849	3071
41	1763	2009	2255	2501	2747	2993	3239	3485

From these tables one can read off that N=667=6(111)+1 is a composite but that N=401=6(67)-1 is a prime.

In the actual evaluation process of distinguishing a composite from a prime number, one generally does not use the Eratosthenes algorithm or any modification thereof, but rather looks at just the particular number N in question.

We can use the information employed in the above modified sieve approach, to quickly factor any smaller digit N by the following procedure-

(A)-Look at N mod(6) to determine which form of 6n±1 one is dealing with. Only numbers with mod(6) operations yielding 1 or 5 are of interest when looking for primes. We automatically have that any odd number having N mod(6)=3 must be a composite.

(B)-If N=6n+1 we require that $p_n(p_n+6m)=N$ for N to be a composite number. Thus-

$$p_n = -3m + \sqrt{9m^2 + N} \quad or \quad the \quad equivalent \quad m = \frac{N - p_n^{\,2}}{6p_n}$$

Here both p_n and m must be an integer when N is a composite. Also p_n maximum must be smaller than sqrt(N). Generally, this is a pretty easy search since the radical contains only m as a variable. Thus the one liner-

for m from 0 to m_{max} do {m,sqrt(9m^2+N)}od;

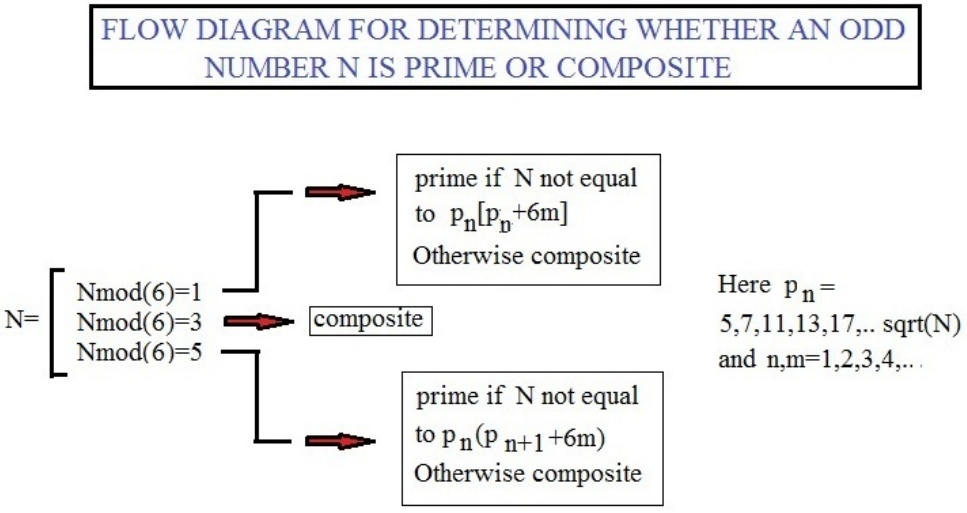
will very rapidly produce an answer. If the radical does not produce an integer value then N must be a prime. Sometimes it will be faster to use the second formula and look for integer solutions for m.

(C)-If N=6n-1 then we require that $p_n(p_{n+1}+6m)=N$ for N to be a composite. If this is not possible then N will be prime. This time we have no simple quadratic in p_n but we have –

$m=(N-p_np_{n+1})/6p_n$ equals an integer for composite Ns.

Should this not be so for p_n=5,7,11,..sqrt(N) , then N is prime.

One can summarize steps (A), (B), and (C) with the following flow diagram-



Let us proceed to demonstrate the procedure. Start with the very simple case-

N=179=6(30)-1 where sqrt(N)=13.3790.. and N mod(6)=5

We apply the test $m=(N-p_n p_{n+1})/6p_n$ which produces no integer solution for p_n=5,7,11,or 13. Hence 179 is a prime.

Next consider-

N=817=6(136)+1 sqrt(N)=28.583.. and N mod(6)=1

Here we use the computer program-

```
seq([n,ithprime(n),(817-ithprime(n)^2)/(ithprime(n))],n=6..10);
```

This produces the output-

[6, 13, 648/13], [7, 17, 528/17], [8, 19, 24], [9, 23, 288/23], [10, 29, -24/29]

From this result we see that p_n=19 yields the integer value 6m=24. Hence we have that 817=19·(19+24)=19·43. This fact can also be read off directly from the above table for N=6n+1.

Next look at -

N=4043=6(674)-1 sqrt(N)=63.58.. and N mod(6)=5

Here we have $p_n(p_{n+1}+6m)\equiv N$ if the number is composite. The computer program for this 6n-1 number reads-

```
seq([n,ithprime(n),(4043-ithprime(n)*(ithprime(n+1)))/(ithprime(n))],n=3..7);
```

and we find the solution-

[3, 5, 4008/5], [4, 7, 3966/7], [5, 11, 3900/11], [6, 13, 294], [7, 17, 3720/17]

Thus we have a composite number since p_n=13 and $p_{n+1}+6m$=17+294=311.
This time the above table was too small to cover this case.

A number of historical interest is $N=2^{11}-1=2047=6(341)+1$. It was the first Mersenne number to be recognized as composite. To validate this point we look at sqrt($9m^2+2047$) and recognize that it takes on the integer value 56 at m=11. Thus p=-33+56=23 and 2047=23·89. We can achieve this result somewhat faster by looking for integer values for m using p_n=5,7,11,13,17,19,23.

Consider next the larger ten digit number-

$N=2^{32}+1=4294967295$ where sqrt(N)=65535.999. and N mod(6)=5.

This is the famous Fermat Number which was first shown to be composite by Leonard Euler. To test the number N we use the Maple program-

```
for n from 1 to 120 do
{n,ithprime(n),(N-ithprime(n)*ithprime(n+1))/(6*ithprime(n))}od;
```

It yields an integer value m= 1116629 occurring for p_n=641 which happens to be the 116^{th} prime. Thus we have that –

$$N=2^{32}+1=(641)\cdot(6700417)$$

Note that 641 mod(6)=5 and 6700417 mod(6)=1 this makes sense since their product is a 6n-1 number.

As another example consider the huge odd number-

N= 7562398132894677851092583557573 41

It is prime or composite? The answer is that it is composite since N mod(6)=3.The actual factoring of such a large number may not always be possible in a short period of time. It takes my home PC about 1 second to factor this number into its prime products-

N= (3)(61)(17812357)(152702004050171)(354727)(4283)

With ever faster super-computers of the type available to the NSA, large public keys involving semi-primes up to 100 digit length used in encryption are becoming vulnerable to decoding, making any type of secret electronic communication vulnerable.

Finally, we should point out that the formulas for finding composites used above work equally well for finding semi-primes which are characterized by having N be the product of just two primes. The way we can generate these is to first find two large primes which are neighbors and then pick a value for m which makes 6n±1 consist of just two prime products. Here are two examples. If we start with

$$p_n=3457187,\ p_{n+1}=3457193,\text{ and } p_{n+2}=3457193$$

we can generate the large semi-primes–

$N=p_n(p_n+6947179)=156058323505807=(3457187)(45140261)$ which has N mod(6)=1

and-

$N=p_{n+1}(p_{n+2}+375389)=19738913939603=(5709527)(3457189)$ which has N mod(6)=5.

The trick to generating large semi-primes is thus to have a list of large p_n values . Our MAPLE math program allows primes as large as ithprime(90,000)=1159523. We can get around this limit by simply writing down a large number M=6(n+k)±1 where n is a large number chosen at random and then integer k is adjusted till a prime is found. Let us demonstrate. Take the number-

M=6(271828182845904523536028747135266249775724709369995957496696762772407663035354759457138217852 52+k)+1

We find this number to be prime for k=5, so that-

p_n=
1630969097075427141216172482811597498654348256219975744980180576634445978212128556742829307115 41

is a large prime generated by exp(1) used as the random number source. Next we generate a large m using the first 94 digits of π. This produces the huge 191 digit long composite number-

$N=6n+1=p_n(p_n+6m)=$
2967490627631282496159641717110679494566169592686209175299031656794578796590124703890964793939119581794729194329200250590682850469718795176455970347559886901736798658562023211339633486262681 3

As expected N mod(6)=1. One can be certain that this number has never seen the light of day before. See if you can factor it to determine whether or not it is a semi-prime. This includes the folks at NSA.

July 8, 2013