DETERMINING PRIMES

A prime number P is any positive integer which can be divided only by 1 and itself. It differs from composite numbers which have additional divisors. As we have shown in earlier notes above, any prime greater than p=3 is equivalent to a Q prime defined as-

$$Q=6n\pm1$$

, where n is a positive integer. One can construct a table of the first twenty-five primes as follows-

P prime via computer program	Q prime defined by 6n±1
2	-
3	-
5	6(1)-1=5
7	6(1)+1=7
11	6(2)-1=11
13	6(2)+1=13
17	6(3)-1=17
19	6(3)+1=19
23	6(4)-1=23
29	6(5)-1=29
31	6(5)+1=31
37	6(6)+1=37
41	6(7)-1=41
43	6(7)+1=43
47	6(8)-1=47
53	6(9)-1=53
59	6(10)-1=59
61	6(10)+1=61
67	6(11)+1=67
71	6(12)-1=71
73	6(12)+1=73
79	6(13)+1=79
83	6(14)-1=83
89	6(15)-1=89
97	6(16)+1=97

What is clear from this table is that any prime above P=3 is equivalent to a Q prime. At the same time it is recognized that not all 6n±1 are prime numbers. Certainly Qs which are divisible by a lower prime fail to be prime. Thus Q=6(4)+1=25,

Q=6(8)+1=49, Q=6(6)-1=35 are composite numbers. It is, however, very interesting that all primes above P=3 have the property that-

$$P \bmod(6)=1 \text{ or } 5$$

This means that a prime such as P= 1467920133451 yields P mod(6)=1 and P= 123456791 has P mod(6)=5. Any odd number subject to a mod(6) operation yielding 3 can never be a prime. Thus we know that the 39 digit long number –

$$N=456723108745338992349075615353107312371$$

must be a composite number since a mod(6) operation yields 3. I know this is not a prime although my home PC is incapable of actually factoring this number into its components in any reasonable amount of time.

Note again that a mod (6) operation on a number yielding 1 or 5 is a necessary but not sufficient condition for a number to be prime. A good example of this is the Fermat number $N=2^{32}+1$, where a mod(6) operation produces 5, yet, as first shown by Euler, the number is actually a composite and can be written as-

$$N=4294967297=641 \times 67004517$$

Let us look in more detail at some other odd numbers N and test them for primeness. Begin with N=2759 which yields N mod(6)=5 suggesting it might be a prime. However a follow up test R=N/(6n+1) , run with our MAPLE program-

```
for n from 0 to 8 do {n, 2759/(6*n+1)}od;
```

produces the [n,R] pair [5, 89]. This means 2789 is composite with one of its factors being the prime 89. The second prime follows from q=N/89=31. The mod (6) value of 5 for 2789 dictates that p and q are of the form 6n+1 and 6n-1 respectively, and visa versa. In any evaluation of R it will be sufficient to just look in the range $1<n<\text{sqrt}(N)/6$ so that the upper limit on n to be considered for N=2789 will be 8.

Let us next look at the ten digit odd number N=1189405577 whose mod(6) operation also yields 5. This again suggests we might be dealing with a prime number. However, it calls for an R=N/(6n±1) test before this can be confirmed. The form of N says that the term in the denominator of R have opposite signs for 6n±1. corresponding to p and q. Also we know that either n or m must lie somewhere between 1 and sqrt(N)/6≈5748. It suggests we search near the halfway point of n=2873 so that the ratio test reads R=N/[6(2873+k)+1], with k running from –B to +B. We find, with aid of our MAPLE program, that R has an integer value at k=673 showing that N is not prime but rather a composite number N=p·q with p=6(2873+673)+1=21277. The other factor equals q=B/p=55901. Note that q=6(9317)-1.

Many other odd numbers will break up into not just the product of two primes but rather into the product of multiple primes. Under that condition the value of n required for factoring the number N can become quite small. Take the case of-

N=39689=13x43x71

Here N mod(6)=5 so we try N/(6n+1) for an R test. Already at n=2 it yields 3053, showing that one of the factors of N is 6(2)+1=13. The number 3053 is not yet a prime. We thus do the additional search R=3053/(6n+1) and find the pair [n,R]=[7,71] meaning that 3053=43x71. Combining these results produces the three prime number product which is equivalent to 39689.

What is clear from the above examples is that , although it is easy to classify any odd numbers N having a mod(6) value of 3 as composite, the proof that odd numbers having mod(6) values of either 1 or 5 are prime can be a lengthy process especially as N gets larger. The number of divisions required that Ns with a mod(6) values of 1 or 5 are prime typically will require some sqrt(N)/6 divisions when N is a semi-prime N=pq. For a hundred digit long semi-prime, whose mod(6) value is not 3, will require some 10^{49} divisions which is beyond the capability of even the fastest supercomputers to accomplish within a few hours.

March 2013