LIST OF THE FIRST ONE-HUNDRED Q PRIMES

We have recently found a way to represent all positive integers in terms of their NUMBER FRACTION. The number fraction(denoted by f_N) is determined by evaluating the sum of all factors of a number excluding 1 and the number N itself and then dividing the result by the number. That is-

$$f_N = \frac{[\sum all\ \ factors\ of\ \ N] - (N+1)}{N}$$

In computer language one can write-

$$f_N = \frac{(\mathrm{add(i, i = divisors(N)) - (N+1))}}{\mathrm{N}} = \frac{\{\sigma(N) - (N+1)]}{N}$$

Here σ(N) is the sigma function of number theory. This formula shows at once that a number fraction corresponding to f_N=0 represents a prime number while larger f_Ns in excess of about 1 represents super-composites having many divisors. Take the number N=12345. Here we have –

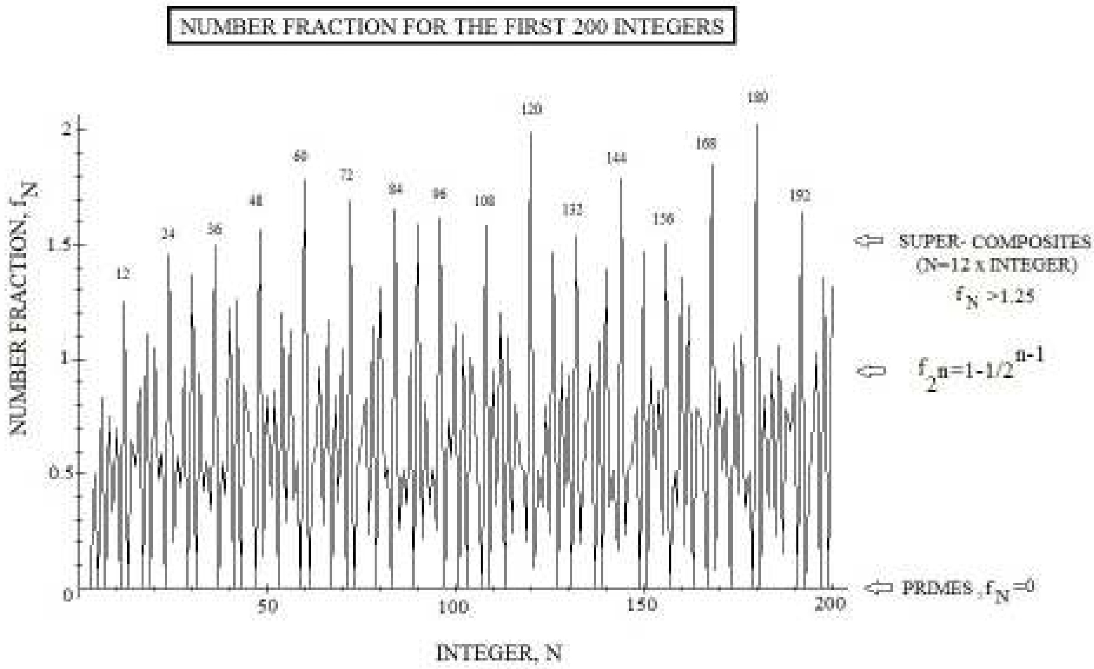
divisors(12345)= {1, 3, 5, 15, 823, 2469, 4115, 12345}

and-

f_N= evalf((add(i,i=divisors(12345))-(12345+1))/12345)=0.6018631025

This number is thus a composite number of intermediate composite value.

The number N=34583 has as its divisors {1, 34583} and hence f_N=0 so that the number is prime. To get some idea of the range in value of f_N we next look at the following graph of the Number Fraction versus N in the range 3<N<200-



What is seen is that the average value of f_N is near 0.6 and the maximum number fractions does not go much above about f_N=2. We notice in particular that the largest values occur for numbers which are a multiple of six and twelve and that in many cases such super-composite values are often either preceded or followed directly by a prime number. This suggests that primes above N=3 can be generated by-

Q=6(random number)±1

Not all of these Qs will be prime but they will, as we will show shortly, predict all primes above N=3. The following represents a list of the first 100 of these Q primes-

Q=6n+1={7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109, 127, 139, 151, 157, 163, 181, 193, 199, 211, 223, 229, 241, 271, 277, 283, 307, 313, 331, 337, 349, 367, 373, 379, 397, 409, 421, 433, 439, 457, 463, 487, 499, 523, 541, 547}

Q=6n-1={5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 191, 197, 227, 233, 239, 251, 257, 263, 269, 281, 293, 311, 317, 347, 353, 359, 383, 389, 401, 419, 431, 443, 449, 461, 467, 479, 491, 503, 509, 521, 557}

If we compare these values with our computer program for the ith prime we find the ithprime(102)=557. Thus the above list of the first 100 Q primes represents <u>all primes</u> except the first two of N=2 and N=3.

A measure of the total number of primes expected in the range $N_1<N<N_2$ follows from the Fundamental Theorem for Primes. For large N one has the total number of primes equal to-

$$\text{Number of Primes} \approx [(N_2/\ln(N_2)-N_1/\ln(N_1)]$$

If $N_1=6000$ and $N_2=6020$ we expect the total number of primes in this range to be [6020/ln(6020)-6000/ln(6000)=2.034 while the actual number is two primes, namely N=6(1001)+1=6007 and N=6(1002)-1=6011. So again we see that the Q definition covers all primes in this given range.

Let us next show how one can quickly generate very large Q primes. The easiest way to do this is to pick a large random number R and then evaluate isprime[6(R+n)+1] and isprime[6(R+n)-1] by varying n through a small range. The R is easiest to pick by just copying a set of digits from a combination of irrational numbers such as –

$R=[\pi \, \text{sqrt}(2)/\exp(1)]10^k=$
1634445292479835509920482389420615372333245322395692016471053262171616896764070

67640709

when k=80. If we now run n over the range 0 to 60, we find n=51 makes Q= 12(R+51)-1 a prime number. This number reads-

Q=1961334350975802611904578867304738446799894386874830419765263914605940
027611689119

There are very few other techniques of which I am aware which can generate such large primes as rapidly.

Next, let us demonstrate a way to break large semi-primes N=pq into their component form for the case where both p and q are Q primes. Let us start with the two Q primes p=6n-1 and q=6m-1, with n and m to be determined. Going to the above list of Q primes we choose the product N=30523 not yet revealing which n and m were used. One has-

$$N= 30523=(6n-1)(6m-1)=36nm-6(n+m)+1 \quad \text{where } N \bmod(6)=1$$

Letting U=nm and V=n+m, this is equivalent to the Diophantine Equation-

$$6U-V=(N-1)/6=5087$$

The solution can be written down at once after noting that 5087 mod (6)=5 so that [U,V]=[0,-5] . It reads-

$$U=0+k \quad \text{and} \quad V=-5+6k$$

The value of p will be given by-

$$p=6n-1=(3V-1)\pm \mathrm{sqrt}[(3V-1)^2-N)]$$

We can now vary the integer k over a chosen range until one finds the k which makes p an integer. Here we find k=11 produces-

$$p=6(39)-1=233 \quad \text{and} \quad q=6(22)-1=131$$

Some additional complications are introduced when one does not know before hand whether the plus or minus sign has been used in the generation of the Q primes p and q. This however should not be a major problem since the mod(6) value for N will offer guidance as to the choice. If N mod(6)=5 we know that the this semi-prime must be composed of the product N=(6n-1)(6m+1). If N mod(6)=1 then this semi-prime will be represented either by N=(6n+1)(6m+1) or N=(6n-1)(6m-1).

Take next the larger semi-prime-

$$N=1853965513=pq=(6n-1)(6m-1) \text{ where } N \bmod(6)=1$$

This is equivalent to the Diophantine Equation-

$$6U-V=308994252=K$$

Since here K mod(6)=0 , we have the integer solutions-

$$U=nm=k \quad \text{and} \quad V=n+m=6k \quad \text{with } k=1, 2, 3,\ldots$$

The quadratic equation for p again reads-

$$p=3V-1\pm \mathrm{sqrt}[3V-1)^2-N]$$

The term in the radical is not positive until k>2393. This suggests redefining-

$$U=2393+s \quad \text{and} \quad V=6(2393+s)=14358+6s$$

Solving the quadratic equations for q by taking the minus sign in front of the radical, one finds an integer solutions for q of 25307 at s=345. This produces -

$$p=6(12210)-1=73259 \quad \text{and} \quad q=6(4218)-1=25307$$

It took 345 trial calculations to obtain this result. The difficulty with the present approach is that one does not know beforehand how far the value of s will be removed from zero. Some help is offered by noting that generally U>>V for large N and the ratio U/V must be consistent with the ratio nm/(n+m)≈m , where n and m are integers with n>>m.

The most difficult part of the above procedure is finding the value of k which makes the radical involved in generating p become a perfect square. This search is easiest to accomplish using an electronic computer. The procedure will always work but can become quite time consuming when N approaches lengths of several hundred digits or so.

U.H.Kurzweg
Gainesville, Florida
October 11, 2012