# NUMBER FRACTION, PRIMES, AND SEMI-PRIMES

**In several earlier notes we have discussed the concepts of number fraction, property of Q primes , and the factoring of large semi-primes. It is our purpose here to bring all these concepts together. Our starting point will be to look at the definition of number fraction. We first came up with this concept about a year ago and define it by the formula-**

$$f(N)=\frac{\{\sigma(N)-N-1\}}{N}$$

**, where the sigma represents the sum of all the divisors of a number N. The sigma function σ(N) is known from number theory . Any positive integer N can always be expressed in terms of the product of its prime number components as-**

$$N=p_1^{a_1}\cdot p_2^{a_2}.p_3^{a_3}\cdot....$$

**where $p_n$ are prime numbers taken to the $a_n$th exponent. Thus, $658=2\cdot7\cdot47$ and $3425=5^2\cdot137$. It is known from number theory that the sigma function-**

$$\sigma(N)=\sum_{n=1}^{b}(nth\ \ factor\ of\ \ N)=\prod_{n=1}^{c}\frac{(p_n^{\,a_n+1}-1)}{(p_n-1)}$$

**Therefore a number such as $24=2^3\cdot3$ has a sigma function-**

$$\sigma(24)=1+2+3+4+6+8+12+24=60=(\frac{2^{3+1}-1}{2-1})(\frac{3^{1+1}-1}{3-1})=15\cdot4$$

**The number fraction for this same number will be-**

$$f(24)=\frac{60-24-1}{24}=\frac{35}{24}=1.4583...$$

**This fraction is about twice as large as the average value of f(N)=0.6 in the range $5<N<200$ indicating that 24 is a super-composite having many factors as shown. As already observed in earlier notes, this suggests that the numbers N+1 and/or N-1 have a good chance of being prime numbers for which f(N)=0. This is indeed the case for N=23 but not for N=25.**

**One can use an electronic computer to rapidly find the three quantities- the ifactor(N) , the sigma function σ(N), and the number fraction f(N)) for any positive integer. Here are a few examples-**

**$N=1404=2^2 3^3 13$ with $\sigma(N)=(7/1)(80/2)(168/12)=3920$ and $f(N)=2515/1404=1.7913$.**

**N=6241= $79^2$ so σ(N)=($79^3$-1)/78=6321 and f(N)=1/79=0.012658..**

**N=76893219=$3^5$·13·101·241 so σ(N)=(728/2)(168/12)(10201/100)(58080/240) =125789664 and f(N)=48896444/76893219=0.63590..**

**Notice that the number fractions f(N) are all small non-integers ranging from zero to not more than about three for any positive integer. An interesting result follows when N is a prime. Under that condition N=p and the sigma function becomes σ(p)=($p^2$-1)/(p-1)=p+1 . From this it follows that f(p)=0 as already mentioned earlier. Another result involves pure semi-primes which can be defined as N=p·q. For such semi-primes the number fraction tends to be very small but not zero. Explicitly one finds that-**

$$f_{semi-prime}(N) = \frac{(p+1)(q+1) - pq - 1)}{pq}$$

**From this it follows that p satisfies the quadratic equation-**

$$p^2 - pNf + N = 0$$

**The problem with this result is that one really has already found both p and q in obtaining f(N). Nevertheless it is a convenient check for semi-primes. Consider the trivial case of the semi-prime N=35. Here the factors are 1, 5, 7, and 35. Thus f(35)=(5+7)/35=12/35. Plugging into the quadratic for p we get-**

$$p^2 - p(35)(12/35) + 35 = 0$$

**This is equivalent to (p-5)(p-7)=0 and hence p=7 and q=5 or visa versa.**

**In examining the values of f(N) for the first 200 integers we find that all primes greater than three occur only under conditions were N=6n±1. <u>That is, for a number above N=3 to be prime it must have either the form 6n+1 or 6n-1.</u> This is , however, not a sufficient condition since there are many numbers with this form which are composite. We call all primes numbers which have the form 6n±1 Q Primes. Let us look at a few examples. We start with some cases where 6n±1 yields a prime-**

**N=6(123)+1=739**

**N=6(6738)+1=40429**

**N=6(54176724)-1=325060343**

**Some composites of the form 6n±1 are-**

**N=6(541)-1=3245**

**N=6(2368)+1=14209**

**N=6(7623159)-1=45738953**

**To distinguish between prime and composite numbers among the 6n±1 numbers can become rather lengthy when N approaches lengths of fifty or so digits. What is clear from our examination of all odd numbers from 5 through 1001 is that all primes found in that range are Q Primes. This means that odd numbers of the form 6n±3 can never be a prime. In modular arithmetic language one has that if N mod(6) is equal to 0, 2, 3, or 4 it must be a composite number. While a N mod (6)value of 1 or 5 indicates a necessary but not sufficient condition for n to be a prime. Let us demonstrate with three more examples-**

**N=123456789 has N mod(6)=3 so it is a composite number**

**N=76293011 has N mod(6)=5 so it might be prime. A test shows it is indeed a prime**

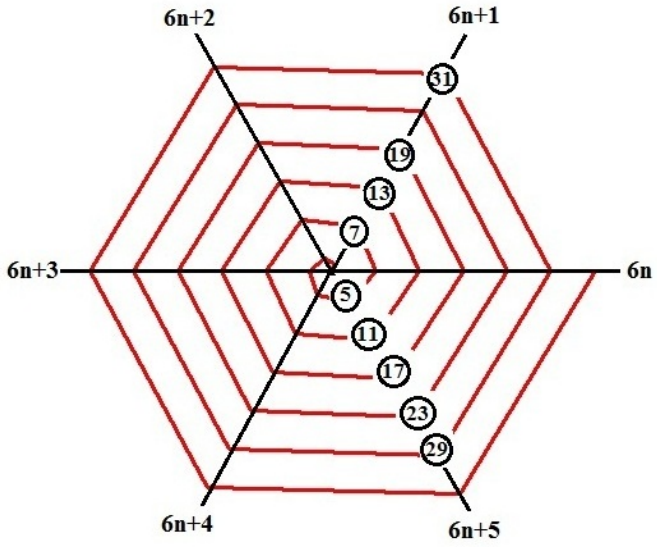
**N=3458923093428652 has N mod(6)=4 so it is an even number and must necessarily be a composite**

**Since a mod(6) operation just involves a division of N by 6 and a look at the remainder, it is a very simple operation no matter how large N becomes. We know at once that the 95 digit long number-**

**N=31415926535897932384626433832795028841971693993751058209749445923078164062862089986280348253421**

**cannot be a prime number since N mod(6)=3.**

**One can conveniently plot all integers including the primes in a diagram consisting of a spiral structure plus six radial lines as shown-**




**On the graph we indicate all primes from 5 through 31. They all fall nicely along the radial lines 6n+1 or 6n+5. In this Integer Spiral diagram all positive integers are represented in polar coordinates as [r,θ]=[N, πN/3] . We have only shown the primes. A number such as N=33 has N mod(6)=3 and so lies at polar coordinate point [33,11π] along the line 6n+3. All straight red lines drawn between N and N+1 form the spiral. Note that along a given diagonal the spacing between neighboring primes is always a multiple of six. Thus the prime N=13 lying along the diagonal in the first quadrant at the $2^{nd}$ turn of the spiral differs in magnitude by 6(3)=18 from N=31 found at the $5^{th}$ turn of the spiral. Note that subsequent numbers along a given diagonal have their last integer follow the sequence 5-1-7-3-9 and repeat. From this observation we have that all 6n±1 numbers ending in 5 (and greater than N=5) will be composite.**

**The secret for distinguishing primes from composites along the diagonals 6n±1 in the first and $4^{th}$ quadrant of the above integer spiral is to be able to quickly recognize those numbers along these lines which are divisible by a smaller prime less than about sqrt(N). The gaps at N=25 and N=35 in the above figure clearly stem from the fact that both are divisible by the lower prime 5. We can generalize this result to state that-**

**A number N will be prime if it equals 6n±1 provided that (6n±1)/p remains a non-integer for all primes p<sqrt(N)**

**Let us test the number N=6(36)+1=217. Here 217/p for p=3, 5, 7, 11, 13 yields an integer value of 31 at p=7 . Thus N=217=7 x 31 is a composite number as found by just 3 divisions. Consider next much larger Fermat number $N=2^{32}+1=4294967297$. Here N mod (6)=5 so it could possibly be a prime. However running the computer program-**

**for n from 1 to 120 do{ithprime, (2^32+1)/ithprime(n)} od;**

**yields an integer value for $(2^{32}+1)/641$ of 6700417 . Thus, 4294967297=641 x 670041 and we have a composite number as first noted by Leonard Euler. The fact that it took a total of 116 divisions to get this result gives an indication of how time consuming this prime number test can become. The effort increases dramatically with increasing N with the number of required divisions possibly as high as the number of primes lying between 5 and sqrt(N). One can of course be lucky and need only a much smaller number of divisions as Euler found with $N=2^{32}+1$.**

**To separate the Q Primes from composites, we start with the sequences-**

**U=6n+1={7,13,19,25,31,37,43,49,55,61,67,73,79,85,91,97,103,109,115,121,127,133,139,145,151,157,163,169,175,181,187,193,199,205,211,217,223,229,235,241,247,253,259,265,271,277,283,289,295,301}**

**and-**

**V=6n-1={5,11,17,23,29,35,41,47,53,59,65,71,77,83,89,95,101,107,113,119,125,131,137,143,149,155,161,167,173,179,185,191,197,203,209,215,221,227,233,239,245,251,257,263,269,275,281,287,293,305}**

**Both are easy to write down since the spacing between neighbors is always six.**

**We next filter out composite terms by carrying out the divisions-**

$$\frac{(6n+1)}{p_n} \quad and \quad \frac{(6n-1)}{p_n} \quad for \quad p_n = 5,7,11,13,17,19,23,\ldots < \sqrt{N}$$

**and throwing out those Ns for which these quotients produce integers. In studying the sequences U and V, we have found a way to speed up this division considerably by a filtering process based on noting that those numbers of the form N=6n+1 which satisfy the formula-**

**$N=p_m(p_m+6m)$ for $p_n$=5,7,11,13,17,19, <sqrt(N) and m=0,1,2,3,4,…**

**are composite numbers. This producers the 6n+1 sequence of composite numbers-**

**$U_{composite}$={25,49,55,85,91,115,121,133,145,169,175,187,205,211,217,235,247,253,259,265}.**

**When we eliminate $U_{composite}$ from U we obtain the following list of 6n+1 Q Primes-**

**$U_{prime}$={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} .**

**A very interesting consequence of this approach is that it also gives us the ability to quickly determine the components of large composite numbers of the form 6n+1 which could also be semi-primes. Take, for example, the very well known case of N=455839=6(75973)+1 which is often used to demonstrate the Lenstra Elliptic Curve Factorization Method. Solving the above equation N=p(p+6m), we get-**

$$p = -3m + \sqrt{9m^2 + N}$$

**Recognizing that p must be an integer, one only needs to find the value of m for which the radical is an integer. We find this occurs at m=27 yielding the radical value of 680. Hence p=599 and q=N/p=761. It took just 27 divisions to get this result compared the 109 divisions it takes to evaluate p by looking at the quotient $N/p_n$=integer. Other cases exist where the quotient approach is superior to the radical evaluation approach. This occurs when p<<q as it does for $N=2^{32}+1$.**

**Likewise we observe that composite numbers of the form N=6n-1 can be represented by-**

**$N=p_n(p_{n+1}+6m)$ with $p_n$=5,7,11,13,…<sqrt(N) and m=0,1,2,3,..**

**This formula produces the sequence –**

**$V_{composite}$={35,65,77,95,119,125,143,155,161,185,203,209,215,221,245,275,287}**

**Eliminating $V_{composite}$ from V produces the 6n-1 Q Primes-**

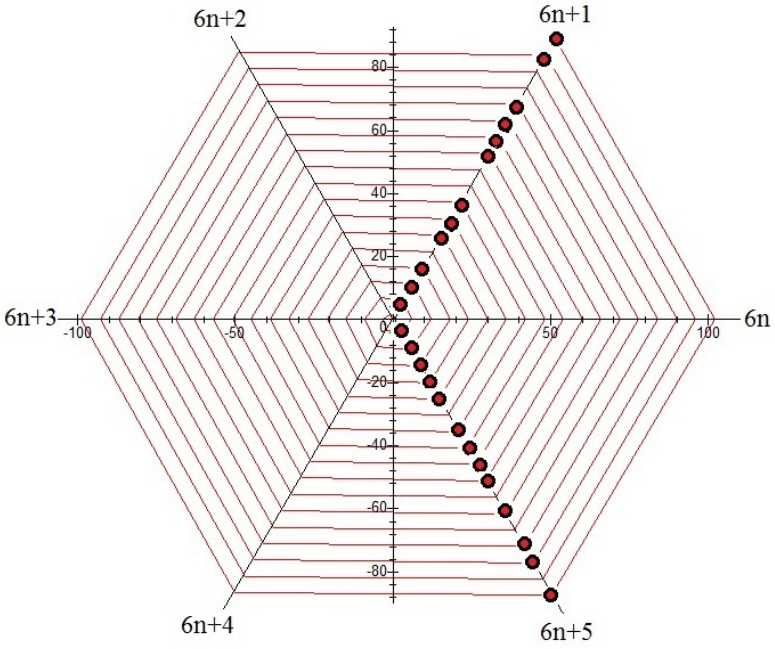
**$V_{prime}$={5,11,17,23,29,41,47,53,59,71,83,89,101,107,113,131,137,149,167,173,179,191,197,227,233,239,251,257,263,269,281,293}**

**These $U_{primes}$ and $V_{primes}$ fall along the lines 6n+1 and 6n+5 in the above diagram , respectively. It also locates the observed gaps which represent $U_{composite}$ and $V_{composite}$. Although the equation for composite number N when N mod(6)=5 does not allow us to solve for m without specifying a $p_{n+1}$, one can work things backwards to generate a large composite number of the type 6n-1. Using our computer we know that the 1000nds prime is 7919 and the 1001 prime equals 7927, so that we can write-**

**N=7919(7927+6*3497)=228930371**

**This number is a semi-prime equal to N=7919 x 28909 and it has N mod(6)=5. In improved Hexagonal Number Spiral showing the first 25 Q Primes as given found in the above $U_{prime}$ and $V_{prime}$ sequences is shown here-**

INTEGER SPIRAL SHOWING THE FIRST 25 Q PRIMES




**The well known Mersenne primes have the form $M=2^p-1$ where p equals certain primes. The operation M mod(6) always yields 1 and hence all Mersenne Primes lie along the 6n+1 diagonal in the first quadrant and form a sub-sequence of $U_{prime}$ which has the form-**

**$M_{prime}$={7, 31, 127, 8191, 131071, 524287, 2147483647,…}**

**The Fermat Primes have the form $F=2^{2\wedge n}+1$ for n=1,2,3,. . One has F mod(6)=5 and so all Fermat primes lie along the radial line 6n+5 in the fourth quadrant. They form a sub-sequence of $V_{prime}$ and read-**

**$F_{prime}$={5, 17, 257, 65537}**

**So far no one has been able to find a Fermat Prime for n=5 and higher, leaving one with just the four Fermat Primes shown. It is difficult to accept the consensus that there likely are an infinite number of Mersenne Primes but only four Fermat Primes considering that the spacing in the sequences in both $U_{prime}$ and $V_{prime}$ are relatively small multiples of six and so are bound to be hit by $M_{prime}$ and $F_{prime}$ multiple times. All we know at the moment is that so far no $F_{primes}= 2^{2\wedge n}+1$ have been found for 4<n<21 . Several more recent attempts have even been made for special cases where 2^n equals several million without success. Nevertheless, my bet is that**

**eventually someone will find a Fermat Prime for n>>21 by using a powerful enough supercomputer.**

**June 2013**