Several years ago we came up with a new number theory constant which clearly distinguishes compound from prime numbers. We call it the number fraction. It is defined as:

\[
f(N) = \frac{\sigma(N) - (N + 1)}{N}
\]

, where \(\sigma(N)\) is the sigma constant from number theory which represents the sum of all the divisors of a number \(N\). The presence of \(N\) in the denominator of this function is to keep \(f(N)\) from growing too rapidly. The interesting thing about the number fraction is that it indicates that \(N\) is a prime if and only if \(f(N)=0\). For all other cases \(f(N)>0\), assuming that \(N\) is a positive integer. For \(N=217\) we get \(f=121/243\) and therefore 217 is a composite. When \(N=521\) we find \(f=0\) meaning 521 is a prime.

We noticed in several earlier noted, when plotting \(f(N)\) versus \(N\), that \(f(N)\) tends to take on its largest local values when \(N\) is a multiple of six. Thus for \(N=96\) the value of \(f(96)\) equals \(155/96\). In addition, when looking at the immediate neighbors at \(N=(6n+1)\) they often produce prime numbers such as \(f(96+1)=0\). We have chosen to call such primes Q-Primes. A short list of these Q-Primes follows:

<table>
<thead>
<tr>
<th>n</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>6n+1</td>
<td>7</td>
<td>13</td>
<td>9</td>
<td>-</td>
<td>31</td>
<td>37</td>
<td>43</td>
<td>-</td>
<td>-</td>
<td>61</td>
<td>67</td>
<td>73</td>
<td>79</td>
<td>-</td>
</tr>
<tr>
<td>6n-1</td>
<td>5</td>
<td>11</td>
<td>7</td>
<td>23</td>
<td>29</td>
<td>-</td>
<td>41</td>
<td>47</td>
<td>53</td>
<td>63</td>
<td>-</td>
<td>71</td>
<td>-</td>
<td>83</td>
</tr>
</tbody>
</table>

Notice that there are several examples of double primes such as 7-5, 13-11, 31-29, 43-41, and 73-71. Also there are certain gaps meaning that not all numbers of the form \(6n\pm1\) need to be prime. The most surprising thing about these results is that the number of \(f(N)=0\) over any chosen range \(5 \leq N < b\), where \(b\) is an arbitrary larger integer, match precisely the total number of primes predicted by our MAPLE computer program using its ithprime operator. So for the range \(5 \leq N \leq 40\) our MAPLE program predicts exactly ten primes( 5, 7, 11, 13, 17, 19, 23, 29, 31, 37). Comparing this with the following \(f(N)\) plot-
we see that all of these are Q-Primes. That this result is not a fluke, we also looked at the primes in the range 1985<N<2072. The numbers of expected primes according to our computer program is precisely thirteen which agrees with the following graph for Q-Primes in this range-

We have also extended our search for the number of primes in a given ranges well above N=2000 and still find that the number of primes are precisely equal to all the Q-Primes(N=6n±1) in the chosen range. These observations lead one to the important conclusions that-
(1) All primes above N=3 must be Q-Primes of the form 6n±1. In terms of modular arithmetic this means N mod(6)=1 or N mod(6)=5. Numbers greater than 3 for which N mod(6)=3 can never be primes.
(2) The N=6n±1 requirement is a necessary but not sufficient condition for N to be a Q-Prime. There are also an infinite number of composites of this form such as any number ending in 5 or one representing the square of any odd number.

The first condition excludes the primes 2 and 3 which are not covered by the 6n±1 rule. The second condition allows for the appearance of the blanks in the above table. Thus 9, 25, 35,... are composites yet also have the form 6n±1.

It is the purpose of this note to distinguish those values of 6n±1 which are primes from those which are composite. We know that any number N can always be written as a multiple product of primes. That is-

\[ N = p_1^\alpha \cdot p_2^\beta \cdot p_3^\gamma \cdot \ldots = p_1 \cdot M \]

Here α,β,γ are integer powers of their respective primes p_n. The number M is the remaining term after factoring out p_1 to the first power. Assuming p_1 to be the smallest of the prime numbers in the product, it is clear that-

\[ p_1 = 6m \pm 1 < \sqrt{N} \quad \text{or} \quad m < \frac{\sqrt{N} \pm 1}{6} \approx \frac{\sqrt{N}}{6} \quad \text{for} \quad N \gg 1 \]

Now if N/(6m±1) yields an integer value in the given range of m, the number N is a composite. If this quotient yields no integer value, then N is a prime.

Let us demonstrate the procedure by looking at several specific larger integers
Consider first the number N=28361=6(4727)-1=28361. In terms of modular arithmetic, we have N mod(6)=5 (or the equivalent -1). It has the sqrt(N)/6 ≈ 28. So, applying the one line computer program-

```
for m from 1 to 28 do {m,evalf(28361/(6*m+1)),evalf(28361/(6*m-1))} od;
```

In the vicinity of m=13, it produces the result-

{11, 423.2985075, 436.3230769}
{12, 388.5068493, 399.4507042}
{13, 359, 368.3246753 ←solution (integer residue=359)}
{14, 341.6987952, 333.6588235}
{15, 318.6629213, 311.6593407}
From it we have that \( N = 28361 = 359 \times [6(13)+1] = 359 \times 79 \). It took just 13 divisions to factor this number when starting at \( m = 1 \). We could of course also have chosen to start the expansion at \( 28/2 = 14 \) and then hit the answer in just two quotient evaluations.

Take next the number \( N = 18401893 \) which has \( N \mod(6) = 1 \). This means we can write \( N = 6(3066982)+1 \). Also we have \( \sqrt{N}/6 \approx 715 \). Running a search starting with \( m = 1 \), we already find an integer solution at \( m = 7 \). The integer residue there is \( M = 427951 \). Also \( f(M) = 0 \). So one has-

\[
N = 18401893 = [6(7)+1][427951] = 43 \times 427951
\]

This is a composite consisting of two primes. Numbers of this type are often referred to as semi-primes. We were lucky in this case to have \( m \) small and the fact that the residue was also a prime. If this had not been the case one would have to breakup \( M \) by a similar procedure. If one had found no integer residue in the range \( 1 < m \leq \sqrt{N}/6 \), then the number \( N \) would be a prime.

Another number is the semi-prime \( N = 455839 \) which has \( N \mod(6) = 1 \) and \( \sqrt{N}/6 \approx 113 \). This number is often used to demonstrate the effectiveness of the Lenstra elliptic curve factorization method. Running our computer calculations, we find no integer residue until \( m = 100 \) is reached. There the residue is 761. This represents one of the primes in the product for \( N \). The second prime is 
\[
N/761 = 599
\]
When a number \( N \) is composed of just the product \( N = p_1 \times p_2 \) and these lie close to each other, as they do in this last case, the use of such a product for a public key in cryptography is very vulnerable to code breakers. To make the factoring of such semi-primes secure as public keys one wants to make \( p_1 \) and \( p_2 \) hundreds of digits long and also have \( 3 << p_1 << p_2 \).

Using the above results, we are now in a position to distinguish whether numbers of the form \( N = 6n \pm 1 \) are Q-Primes or composites. The rule to distinguish the two possibilities is-

**If for any \( m \) in \( 3 < m < \sqrt{N}/6 \) the quotient \( N/(6m \pm 1) \) yields an integer value then \( N \) is a composite. If there are no integer quotients in the same range then \( N \) is a prime.**

A few days ago we found a new graphical way to present the Q-Primes as points along the two diagonals of a triangular integer spiral as shown-
The primes, shown in blue, all lie along the two diagonal lines $6n+1$ and $6n-1$. and are separated from each other by integer factors of six. Gaps along these diagonals indicate composite numbers such as 25 and 35. The vertexes of this spiral are located, in polar coordinates, at-

$$[r, \theta] = [N, N\pi/3]$$

May 1, 2015