EVALUATING THE $\sigma(N)$ and $S(N)=\sigma(N)-N-1$ POINT FUNCTIONS

We have shown in earlier articles on this web page that the semi-prime $N=pq$ factors into its components as-

$$[p,q]=S\pm\sqrt{S^2-N}$$

where $S(N)=[\sigma(N)-N-1]/2$ with $\sigma(N)$ being the sigma function (also known as the divisor function) of number theory. To find the prime components $p$ and $q$ for any semi-prime $N=pq$ one needs to only know the value of $S(N)$ or the related sigma function $\sigma(N)$. Now one’s home PC using a math package such as MAPLE or MATHEMATICA can easily generate the values of the divisor function for $N$s up to about 30 digit length in split seconds. Hence semi-primes of this size or smaller are readily factored using the above equality. For example one of the Fermat numbers $N=2^{32}+1=4294967297$ has $\sigma(N)=4301668356$ and $S(N)=3350529$. Plugging this value of $S$ into the above equation yields at once-

$$[p,q]= [641,6700117]$$

The famous Swiss mathematician Leonard Euler (1707-1783) was the first person to accomplish the factoring of this semi-prime. That he was able to do this in those pre-computer days, and without knowledge of $S(N)$, is truly amazing.

It is the purpose of this note to see if one can find some general formulas and other properties of $\sigma(N)$ and $S(N)$ for any $N$ not just those representing semi-primes. We start with a table giving some of these values for $N$ from 2 through 48

<table>
<thead>
<tr>
<th>N</th>
<th>$\sigma(N)$</th>
<th>2S(N)</th>
<th>N</th>
<th>$\sigma(N)$</th>
<th>2S(N)</th>
<th>N</th>
<th>$\sigma(N)$</th>
<th>2S(N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>0</td>
<td>17</td>
<td>18</td>
<td>0</td>
<td>32</td>
<td>63</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>0</td>
<td>18</td>
<td>39</td>
<td>20</td>
<td>33</td>
<td>48</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>2</td>
<td>19</td>
<td>20</td>
<td>0</td>
<td>34</td>
<td>54</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>0</td>
<td>20</td>
<td>42</td>
<td>21</td>
<td>35</td>
<td>75</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
<td>5</td>
<td>21</td>
<td>32</td>
<td>10</td>
<td>36</td>
<td>91</td>
<td>54</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>0</td>
<td>22</td>
<td>36</td>
<td>13</td>
<td>37</td>
<td>28</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td>6</td>
<td>23</td>
<td>24</td>
<td>0</td>
<td>38</td>
<td>60</td>
<td>21</td>
</tr>
<tr>
<td>9</td>
<td>13</td>
<td>3</td>
<td>24</td>
<td>60</td>
<td>35</td>
<td>39</td>
<td>56</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>18</td>
<td>7</td>
<td>25</td>
<td>31</td>
<td>5</td>
<td>40</td>
<td>90</td>
<td>49</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>0</td>
<td>26</td>
<td>42</td>
<td>15</td>
<td>41</td>
<td>42</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>28</td>
<td>13</td>
<td>27</td>
<td>40</td>
<td>12</td>
<td>42</td>
<td>96</td>
<td>53</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>0</td>
<td>28</td>
<td>56</td>
<td>27</td>
<td>43</td>
<td>44</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>24</td>
<td>8</td>
<td>29</td>
<td>30</td>
<td>0</td>
<td>44</td>
<td>84</td>
<td>39</td>
</tr>
<tr>
<td>15</td>
<td>24</td>
<td>8</td>
<td>30</td>
<td>72</td>
<td>41</td>
<td>45</td>
<td>78</td>
<td>32</td>
</tr>
<tr>
<td>16</td>
<td>31</td>
<td>14</td>
<td>31</td>
<td>32</td>
<td>0</td>
<td>46</td>
<td>72</td>
<td>25</td>
</tr>
</tbody>
</table>
When looking at this table certain regularities become apparent at once. First of all, if \( N \) is a prime then \( \sigma(N) = N+1 \) and \( S[N] = 0 \). Next we observe that:

\[
\sigma(2) = 3, \sigma(4) = 7, \sigma(8) = 15, \sigma(16) = 31, \sigma(32) = 63,
\]

This generalizes to the odd number:

\[
\sigma(2^n) = 2^{n+1} - 1 \quad \text{marked in red in the table.}
\]

So \( \sigma(2^6) = 127 \), \( \sigma(2^{23}) = 16777215 \), and \( \sigma(2^{97}) = 316912650057057350374175801343 \).

Looking at the sigma values for powers of three, we find the generalization:

\[
\sigma(3^n) = \frac{3^{n+1} - 1}{2} \quad \text{marked in blue in the table}
\]

Furthermore we find:

\[
\sigma(5^n) = \frac{5^{n+1} - 1}{4} \quad \text{marked in green in the table}
\]

Looking at the last three equations allows us to state the even more general value of \( \sigma(N) \) valid for all positive powers of primes:

\[
\sigma(p^n) = \frac{p^{n+1} - 1}{(p - 1)}
\]

In terms of \( S \) we get:

\[
S(p^n) = \frac{p(p^{n-1} - 1)}{2(p - 1)}
\]

This means, for example, that:

\[
S(11^{15}) = S(4177248169415651) = 208862408470782
\]

Although the equation for \( S(p^n) \) covers an infinite number of cases, it does not in general cover the cases \( S(pq) \) which are associated with the semi-primes \( N = pq \). To get the values for \( S(N) \) here we construct the following twenty row table starting with prime number 3. Not all combinations are included.-
One notices at once that $S(N)$, here equal to $(p+q)/2$, is just slightly larger than $\sqrt{N}$. So one has the inequality –

$$S(N) > \sqrt{N}$$

This observation is brought out more clearly by the following point graph:
Note that all points lie just slightly above $S(N) = \sqrt{N}$. The departure increases as the ratio $q/p$ increases.

To now find the exact value of $S(N)$ for any semi-prime $N = pq$ we try-

$$S(N) = M + \varepsilon$$

Here $M$ is the nearest integer above $\sqrt{N}$ and $\varepsilon$ is a parameter small compared to $M$. To find $\varepsilon$ we search the radical-

$$R = \sqrt{(M + \varepsilon)^2 - N} = \sqrt{\varepsilon^2 + 2\varepsilon M + (M^2 - N)}$$

by varying $\varepsilon$ until $R$ becomes an integer. A generic form of $S$ versus $R$ follows-
The purple dot is the location where both $S$ and $R$ take on integer values simultaneously. There $S = M + \varepsilon$.

Let us demonstrate things for $N = 3977$, where $\sqrt{N} = 63.0634$ and $M = 64$. We find $R = 28$ at $\varepsilon = 5$. Hence-

\[ S(3977) = 64 + 5 = 69 \]

For larger semi-primes the search for $\varepsilon$ which makes $R$ an integer can become rather lengthy but in principle the procedure will work for any size $N = pq$. Once $S(N)$ has been found the rest of the problem of factoring $N = pq$ into its prime components becomes trivial.

Pushing the limit of my home PC, I looked at the 34 digit long semi-prime-

\[ N = 3148002191173834598641513924426301 \]

It took about one minute on my home PC, using MAPLE, to find-

\[ \sigma(N) = 3148002191173834712713864334992704 \]

so that-

\[ S(N) = 57036175205283201 \]

From it follows the factorization-

\[ p = S(N) - \sqrt{S(N)^2 - N} = 46783219978914191 \]

and-
\[ q = S(N) + \sqrt{S(N)^2 - N} = 67289130431652211 \]

Notice here that we never had to use the much longer route involving \( \varepsilon \). The fact that I am able to find \( S(N)s \) for \( Ns \) up to 34 digit length with ease on my home computer makes me quite optimistic about supercomputers being able to factor large public keys of 100 digit length or so used in cryptography. The key to success in this field clearly lies in quickly being able to find values to the divisor function \( \sigma(N) \) and hence \( S(N) \) for large \( N = pq \).

U.H.Kurzweg
May 1, 2019
Gainesville, Florida