FACTORING OF LARGE NUMBERS

It is well known that any number \( N \) can be represented as the product of a finite number of primes taken to the specified integer powers. Thus-

\[
13867 = (7)^2 (283) \quad \text{with} \quad \sqrt{13867} = 117.756..
\]

\[
23974723 = (151) (179) (887) \quad \text{with} \quad \sqrt{23974723} = 4896.398..
\]

\[
43567217 = (5021) (8677) \quad \text{with} \quad \sqrt{43567217} = 6600.546..
\]

\[
67537 = 67537
\]

The first three examples represent composite numbers while the last is a prime. Now we know from some of our earlier notes that all primes above \( p=3 \) have the form-

\[
p = 6n \pm 1, \quad \text{where} \quad n=1,2,3,4,\ldots
\]

This is a necessary but not sufficient condition for primes since there can be many composite numbers which also have this same form. We want to show here how to distinguish between a composite and prime number satisfying the \( 6n \pm 1 \) condition and from this deduce the product form of any number \( N \).

Since we don’t know beforehand into how many prime terms a number \( N \) will factor, we begin with the safe bet that if \( N \) is a semi-prime \( N=pq \), then \( p<\sqrt{N} \), provided that \( p<q \). If it is composed of three terms \( N=pqr \), even when some of the factors appear multiple times, then it is safe to assume that at least one of the primes is less than \( N^{1/3} \) and so on. So we definitely can state, regardless of the number of prime products present in \( N \), at least one of them will always be less than the square-root of \( N \) unless the number itself is already a prime. This fact is confirmed by looking at the divisors of the tree composite numbers shown above. Let \( p \) be this lowest prime factor. It will be given by 2 or 3 or \( p=6n \pm 1 \), with the \( n \) coming from the list \( n=1,2,3,4,\ldots, \approx \sqrt{N}/6 \), assuming \( N>>1 \). So if we divide \( N \) by all numbers \( 6n \pm 1 \) for \( n \) less than \( \sqrt{N}/6 \) one will typically find an integer value \( M \) at \( n=k \). Thus one of the prime factors \( 6k \pm 1 \) has been found. Next we look at the quotient \( M/(6m \pm 1) \) for \( m=1,2,3,\ldots, \approx \sqrt{M}/6 \). Since \( M \) is smaller than \( N \) the number of divisions required in this second case will be less. If we evaluate this new quotient, one typically finds a new prime \( 6m \pm 1 \) value for the new quotient which has the integer value \( K \). Should \( K \) turn out to be a prime, the calculations can stop. If not we proceed on to the next step repeating the procedure. Let us demonstrate the method for \( N=1353 \). There we have as follows-

\[
N=1357 \quad \text{so} \quad \sqrt{N}=36.837
\]

So try \( p=6n \pm 1 \) with \( k \approx 6 \), since 2 and 3 are not divisors

We find \( |N/(6(4)-1)|=59=M \) which is a prime

Hence 1357 factors into 23 x 59
This procedure can become rather lengthy when N gets large, but it is really the only way to separate composite numbers into its prime components. Should the number already be a prime, then the first quotient \( N/(6n\pm 1) \) will never equal an integer for the range of ns allowed. Take a look at the prime number \( N=67537 \) given earlier. In this case, on evaluating the quotient \( N/(6n\pm 1) \) for \( 1<n\leq 43.31 \), there are no integer solutions and hence \( N \) is prime.

Take next the larger composite number \( N=23974723 \) as given earlier. It does not divide by 2 or 3 and so we take the following additional steps–

\[
N=23974723 \text{ so that } \sqrt{N}=4896.398.
\]

So look at the quotient \( M= N/(6n\pm 1) \) for \( 1<k<\sqrt{N}/6 \approx 816 \). Using a computer to evaluate the quotient, we find at \( n=30 \) that \( M=133937 \). The root of \( M \) is 365.974. Since we are not sure that integer \( M \) is a prime, we look at the new quotient \( K=M/ (6m\pm 1) \) for \( 1<m<61 \). This produces the integer \( K=887 \) at \( m=25 \). Since 887 is a prime we can write down the factored number \( N=[6(30)-1][6(25)+1][887]=179 \times 151 \times 887 \).

The above procedure can be automated by applying the following steps:

1. Given \( N \) find \( \sqrt{N} \),
2. Evaluate \( N/(6n\pm 1) \) for \( n=1,2,\ldots,\approx \sqrt{N}/6 \) until an \( n \) is found for which the quotient equals integer \( M \). One will usually start the search using the lower allowed values of \( 6n\pm 1 \).
3. Assuming \( M \) to not a prime, continue on with the quotient \( M/(6m\pm 1) \) for \( m=1,2,\ldots,\approx \sqrt{M}/6 \) until \( m \) is found where the quotient equals an integer \( K \).
4. If \( K \) is a prime stop. Otherwise continue the procedure until a quotient is found which is a prime \( P \).
5. The factored number \( N \) will then be \( N=[6n\pm 1][6m\pm 1]\ldots [P] \)

You will note that the search becomes easier and easier as the numbers \( n, m, \) etc are found. Sometimes some of the values of \( n, m, \) etc can be equal to each other indicating a prime taken to a power. Should the number be a prime to begin with, then step (2) will produce no integer value for the allowed \( n \) range.

Consider next one of the Mersenne Numbers \( N=2^{23}-1=8388607 \). Here the first quotient to be tested is \( N/(6n\pm 1) \) over the range \( 1<n<\sqrt{N}/6 \approx 483 \), So we have a potential search involving 966 divisions. However we can always stop after one integer value for the quotient has been found. We carry out a computer search taking smaller chunks of \( n \) at any one time and starting with \( n=1 \). We do so with aid of the one line computer program–

\[
N:8388607; \text{ for } n \text{ from 1 to 50 do } \{n, N/(6\times n+1), N/(6\times n-1)\}\text{od;}
\]

Already at \( n=8 \) we find \( p=6(8)-1=47 \) and the quotient value becomes \( M=178481 \) for which \( \sqrt{M}=422.47 \). So we next look at the quotient \( M/(6m\pm 1) \) over the range \( 1<m<70 \). This time
the search over the entire allowed range for \( m \) produces no integer results, so that \( M \) must be a prime. We thus have the final result that \( 2^{23}-1=47 \times 178481 \).

A convenient way to keep track of the factoring process is by means of a factoring tree schematic as shown-

```
FACTORING TREE
```

```
N=46497129
   /
  /  
 5495043
   /
   /
2214149
   /
   /
 316307
   /
   /
 67
   /
4721
```

\[ N = 46497129 = 3 \times 7 \times 7 \times 67 \times 4721 = 3 \times [6(1)+1]^2 \times [6(11)+1] \times [6(787)+1] \]

One records there the generation of primes at each step of the factoring process and circles the final set of primes which in the diagram are 3-7-7-67-4721. Note that all the primes above \( p=3 \) have the form \( 6n \pm 1 \).

In connection with factoring trees, we have encountered a set of numbers which read-

\[ \begin{align*}
2 \\
6 \\
30 \\
210 \\
2310 \\
30030 \\
510510 \\
9699690
\end{align*} \]

Do you recognize the sequence? If you do, then it is clear that the next number is 223092870.

We can define these numbers as-

\[ N(n) = \prod_{k=1}^{n} p_k = (p_n)! \]
where \(p_k\) are the prime numbers 2, 3, 5, 7, 11, 13, 17, 19, … . The numbers \(N(n)\) have the interesting property that they equal the product of all primes from 2 through \(p_n\) without any repetitions. Note that this type of prime number factorial has been known for at least 100 years. It has, however, received considerably less attention than the better known factorial prime number \(n!\pm 1 = 5, 7, 23, 719, 5039, …\). Note that \(N(n)\) satisfies the identity:

\[
p_{n+1}! = p_{n+1}(p_n)!
\]

so that \((p_5)! = 11(210) = 2310\) and \((p_8) = 19(510510) = 9699690\). The fact that all \(N(n)\)'s for \(n > 3\) end in 0 follows from the fact that \(p_1 \times p_3 = 2 \times 5 = 10\). A short table for \([n, p_n, (p_n)!]\) follows:

<table>
<thead>
<tr>
<th>(n)</th>
<th>(p_n)</th>
<th>((p_n)!)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>210</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>2310</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>30030</td>
</tr>
<tr>
<td>7</td>
<td>17</td>
<td>510510</td>
</tr>
<tr>
<td>8</td>
<td>19</td>
<td>9699690</td>
</tr>
<tr>
<td>9</td>
<td>23</td>
<td>223092870</td>
</tr>
<tr>
<td>10</td>
<td>29</td>
<td>6469693230</td>
</tr>
<tr>
<td>11</td>
<td>31</td>
<td>200560490130</td>
</tr>
<tr>
<td>12</td>
<td>37</td>
<td>7420738134810</td>
</tr>
<tr>
<td>13</td>
<td>41</td>
<td>304250263527210</td>
</tr>
<tr>
<td>14</td>
<td>43</td>
<td>13082761331670030</td>
</tr>
<tr>
<td>15</td>
<td>47</td>
<td>614889782588491410</td>
</tr>
</tbody>
</table>

We note that some of the forms \((p_n)!\pm 1\) are prime numbers. Among these are:

\((p_6)!-1 = 30029\)

\((p_{11})!+1 = 200560490131\)

\((p_{13})!-1 = 304250263527209\)

\((p_{24})!-1 = 23768741896345550770650537601358309\)

Oct. 6, 2014