It is well known that any positive integer may be represented as the product of powers of primes. In general one has –

\[ N = \prod_{n} (p_n)^{\alpha_n} \]

with examples including-

\[ 684 = 2^2 \cdot 3^2 \cdot 19 \quad \text{and} \quad 9935433 = 2^3 \cdot 3^2 \cdot 131 \]

A special subclass of such a product expansion occurs when the powers \( \alpha_n \) equal to unity. This produces the numbers-

\[ M = \prod_{n} p_n \]

which among others yields the numbers-

\[ 61 = 61 \quad , \quad 1555 = 5 \cdot 311 \quad , \quad 4085 = 5 \cdot 19 \cdot 43 \]

One notices that an \( M \mod(6) \) operations on these last three specific results yields 1, 5, and 5, respectively. No matter what other numbers of the type \( M \) we choose, a \( \mod(6) \) operation always produces either 1 or 5. This means that all \( M \) numbers have the property that-

\[ M = 6n+1 \quad \text{or} \quad M = 6n-1 \]

providing one excludes the primes \( p=2 \) and \( p=3 \) from these expansions.

**PRIMES:**

A prime is any positive integer which is divisible only by itself and one. It is represented by the number \( M \) when the latter contains only a single integer. The first few primes greater than 3 are-

\[ p = \{ 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots \} \]

These may be conveniently cast into two groups-

\[ (6n+1) = \{ 7, 13, 19, 31, 43, 67, 73, 79, 97, \ldots \} \]

and-

\[ (6n-1) = \{ 5, 11, 17, 23, 29, 41, 71, 83, 89, \ldots \} \]
There are no primes found which are of the form other than $6n\pm 1$ as long as $p \geq 5$. For example-

$$p = 48972345609213578953 = [6(8162057601535596492)+1]$$

A convenient way to see if a number is prime or composite is to make use of the number fraction $f(N)$ which was discovered by us about a decade ago. It is defined as:

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

where $\sigma(N)$ is the sigma function of number theory. What is interesting about this function is that $f(N)=0$ whenever $N$ is a prime and greater than 1 when $N$ has numerous divisors, and above 1.5 for super-composites. For the twenty digit long $p$ given above one finds $f(N)=0$. It was the plot of this function over a wide range of $N$ which first convinced us of the fact that all primes above $p=3$ have the form of either $6n+1$ or $6n-1$. Here is a graph of $f(N)$ over the range $5<N<200$-

In thinking about how to conveniently graph primes, we came up with the following hexagonal spiral integer plot-
Unlike a standard Ulam Spiral where primes are scattered all over the x-y plane, the present graph beautifully places primes along only the radial lines 6n+1 or 6n+5 (equivalent to 6n-1).

The distance between the primes along radial lines 6n+1 and 6n-1 is always in multiples of six. This means, for instance that the distance between 13 and 31 is 6x3 and the distance between 5 and 41 is 6 x 6. In general we have-

\[ p_b - p_a = [(6m \pm 1) - (6n \pm 1)] = 6(m - n) = \text{even number} \]

, when the two primes lie along the same diagonal. If they lie on different diagonals then the difference equals a multiple of six plus 2. Thus the difference between the prime numbers 131=6(22)-1 and 351=6(58)+1 is 6(39)+2=234

When two primes are neighbors such as 5-7 or 17-19 they are referred to as twin-primes. They are easy to spot in the above graph since they lie along the same spiral turn on opposite radial lines 6n±1. An example of a twin prime out at N=55440 looks as follows in a f(N) versus N graph-
The fact that such twin primes often occur in the immediate vicinity of a super-composite is not a fluke but rather a fairly common occurrence.

**SEMI-PRIMES:**

When $M$ contains just two primes, it is referred to as a semi-prime. As with primes, such numbers satisfy $N = pq = 6n \pm 1$ where the primes $p$ and $q$ can lie on the same or opposite radial lines containing primes. Such prime number combinations are of special interest in connection with public key cryptography where they can be used to transmit coded messages. There are four distinct types of twin primes which may be formed by primes $p = 6n \pm 1$ and $q = 6m \pm 1$. Such semi-primes fill in the gaps along the $6n \pm 1$ radial lines. In the above hexagonal spiral graph I have marked them in orange.

The factoring of semi-primes can become a difficult and time-consuming process when $N$ gets large. There are four possible arrangements of such semi-primes. These are-

$$ M(2) = N = (6n+1)(6m+1) = (6n-1)(6m-1) = (6n+1)(6m-1) = (6n-1)(6m+1) $$

The first two correspond to $M \mod(6)=1$ and the second two to $N \mod(6)=5$. We have developed formulas for factoring $N$ in these four cases. The solution is based upon the fact that $nm > (n \pm m)$ for larger semi-primes. For cases one and two we get the solution-
\[ n = 0.5\{\pm(H + 6k) \pm \sqrt{(H + 6k)^2 - (B - k)}\} \]

where \( A = \frac{(n-1)}{6}, H = A \mod(6) \) and \( B = (A - A \mod(6))/6 \). One must carry out a search by changing the constant \( k \) until the radical assumes a positive integer value. Having found \( n \), the rest of the problem for finding \( p \) and \( q \) becomes trivial.

For cases three and four we find:

\[ n = \pm(0.5)\{\left( H + 6k \right) \pm \sqrt{(H + 6k)^2 + 4(B - k)}\} \]

where this time \( A = \frac{(N+1)}{6} \) and the other variables \( H \) and \( B \) remain as before. One notes the sign change before the 4 in the radical from the earlier cases.

Let us demonstrate the factoring technique for the semi-prime \( N=23381 \) where \( N \mod(6)=5 \). Here \( B=649 \) and \( H=3 \) and we need to solve the radical-

\[ S = \sqrt{(3 + 6k)^2 + 4(649 - k)} \]

Doing so, we find \( S=55 \) for \( k=3 \). Hence \( n=17 \) and \( m=38 \) to yield \( p=6(17+1)=103 \) and \( q=6(38)-1=227 \). The main difficulty in this factoring process remains finding the right \( k \) as \( N \) gets large. This is especially so when \( N \) approaches 100 digit long form as used in cryptography.

**TRIPLE-PRIMES:**

This represents a third special form of \( M \) in which we have a number \( K \) produced by the product of any three primes, again for all the primes being 5 or greater. That is-

\[ K = p_a \cdot p_b \cdot p_c \]

Again this product must be of the form \( 6n\pm1 \) and lie along either the \( 6n+1 \) or \( 6n-1 \) radial line. It will fill in part of those gaps left after the primes and semi-primes have been placed. One such small triple prime is found at \( 125=5 \times 5 \times 5 \) it lies along the radial line \( 6n-1 \). Another triple prime is \( 2233=7 \times 11 \times 29 \) which lies along \( 6n+1 \) at the 372\textsuperscript{nd} turn of the spiral. At the present there has been essentially no use of triple-primes made in cryptography but this may change. Factoring of large triple primes will be harder than factoring large semi-prime since it involves the extra requirement that one first find a prime number divisor before factoring the remaining semi-prime. Quadruple primes involving the product of two semi-primes will be even more difficult to factor. Take, for example, the simple quadruple composite \( M=59983 \). Here one would first try division by
5, then 7. The second try works to yield 8569. Continuing on with a division by 11 yields 779. Continuing the divisions by 13, 17, 19 yields 41 at 19. But 41 is a prime so we have:

\[ M = 59983 = 7 \times 11 \times 19 \times 41 \]

Factoring larger Ms can become rather nasty. Use of quadratic primes and higher M for public keys could also throw off an adversary since he may not be aware that a different n-tuple system is being employed. As a little challenge, I leave it for the reader to factor the four prime product \( N = 177155142977180550724173864429983 \). Even the fastest NSA super-computers will have trouble factoring this number.

**N-TUPLE PRIMES:**

These are defined as:

\[ M(n) = \prod_{k=3}^{n} p_k \]

Here we are neglecting the terms \( p_1 = 2 \) and \( p_2 = 3 \) as they would spoil the condition that \( M(n) \) lies along the 6n+1 or 6n+5 radial lines. Also it represents a specials inclusive case of an n-tuple prime since all the primes between 5 and n are being used. The number increases quite rapidly with n. Here is a short table:

<table>
<thead>
<tr>
<th>n</th>
<th>ithprime(n)</th>
<th>M(n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>35</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>385</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>5005</td>
</tr>
<tr>
<td>7</td>
<td>17</td>
<td>85085</td>
</tr>
<tr>
<td>8</td>
<td>19</td>
<td>1616615</td>
</tr>
<tr>
<td>9</td>
<td>23</td>
<td>37182145</td>
</tr>
<tr>
<td>10</td>
<td>29</td>
<td>1078282205</td>
</tr>
<tr>
<td>11</td>
<td>31</td>
<td>33426748355</td>
</tr>
<tr>
<td>12</td>
<td>37</td>
<td>1236789689135</td>
</tr>
<tr>
<td>13</td>
<td>41</td>
<td>50708377254535</td>
</tr>
<tr>
<td>14</td>
<td>43</td>
<td>2180460221945005</td>
</tr>
<tr>
<td>15</td>
<td>47</td>
<td>102481630431415235</td>
</tr>
</tbody>
</table>

The numbers all end in 5 as expected because of \( p_3 \). Also one has the identity:

\[ M(n+1) = \text{ithprime}(n+1)M(n) \]

Thus the term \( M(16) \) reads \( 53 \times 102481630431415235 = 5431526412865007455 \).