MORE ON FACTORING LARGE SEMI-PRIMES

Recently we have introduced a new quantity valid for all positive integers defined by:

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

where $\sigma(x)$ is the sigma function representing the sum of all divisors of integer $x$ including 1 and $x$. We call this quotient $f(x)$ the **Number Fraction**. It has the interesting property that $f(x)=0$ for all prime numbers while composite numbers have $f(x)>0$. Large semi-primes $x=pq$, such as encountered in public key cryptography, will have values of $f(x)$ very close to zero and thus will typically be found in the immediate neighborhood of where $x$ is a super-composite with $f(x)>1$. Once such a semi-prime $x$ has been found, one can factor it as follows:

1) Calculate $f(x)=(p+q)/x$
2) Use the definition of the semiprime $x=p\times q$ to eliminate $q$
3) Evaluate $p=a+\sqrt{a^2-x}$, where $a=x\times f/2$
4) $q$ follows from $x/p$.

We next look at several specific cases starting with the Mersenne Number $x=2^{11}-1=2047$. This has $f=0.05471421593$ meaning it is not a prime number but probably is a semi-prime because of the smallness of $f$. Running through the four steps above produces:

```
\begin{align*}
a &:= 56.00000000 \\
p &:= 89.00000000 \\
q &:= 23.00000000
\end{align*}
```

Thus we find $2047=89 \cdot 23$ with very little effort.

Consider next a larger semi-prime, namely, that of Fermat which reads $x=2^{32}+1=4294967297$. It has a number fraction equal to $f(x)=0.001560211647$ so that:

```
\begin{align*}
a=xf/2 &:= 3350529 \\
p &= 6700417 \quad \text{and} \\
q &= 641
\end{align*}
```
This produces $4294967297 = 641 \cdot 6700417$. Fermat thought this number was a prime but Euler was the first to show, after considerable effort, that the number factors into the two primes shown. Looking in the immediate neighborhood of $x$ we have $f(x+1)= 1.000000003$ and $f(x-1)= 0.999999995$ which are super-composites.

As a third example let us first generate a large semi-prime and then factor it. We begin our search using an earlier observation that numbers with large $f(x)$ are often given by $x=1549 \cdot 6^k$. We consider here the case of $k=49$ to obtain the large $f(x)$ super-composite

$$x=208671283132153254989370540184529119739904$$

where $f(x)=2.00193673337636$. Subtracting one from $x$ yields the neighboring number

$$x=208671283132153254989370540184529119739903$$

which has the much lower value $f(x)=0.000002872069412$ suggesting that it is a semi-prime. Using this $x$ and running through steps (1) through (4) above yields

$$a := 0.2996592047 \cdot 10^{36}$$
$$p := 0.5993184094 \cdot 10^{36}$$
$$q := 348181.0000$$

The explicit value of $p$ follows via the division $x/348181$. That is-

$$p=599318409482864530199438051428794563.$$ 

Thus we have factored a 42 digit long semi-prime into its two components on our home PC with again relatively little effort.

Limitations of the present approach is that it requires precise value of the Number Fraction $f(x)$ which for a semi-prime is just $f(x)=(p+q)/x$. Our computer has no difficulty finding these factors for semi-primes of less than about 50 digit length but gets hung up when trying to factor hundred digit long semi-primes such as those encountered in public-key cryptography. With the aide of faster computers it should become possible in the near future to factor semi-primes of one hundred digit length or so.

U.H.Kurzweg
April 4, 2013