FINDING THE SIGMA FUNCTION AND NUMBER FRACTION FOR LARGE INTEGERS

It is well known that any positive integer can be represented as the product of primes p taken to specified integer powers n. As an example consider-

$$N=26789=7 \times 43 \times 89$$

, where the powers of the three primes shown are restricted to n=1.

If we take the sigma function of p^n =26789^1 and use its properties, we get-

$$\sigma(26789) =\sigma(7)\sigma(43)\sigma(89)=8*44*90=31680$$

Also we know that the number fraction (first discovered by us about a decade ago and defined as f(N)=[σ(N)-N-1]/N) is given for this number by-

$$f(26789) =4890/26789=0.1825376\ldots$$

It is possible to generalize things and find the values of any σ (N) and f(N) for all positive values of N=p^n. Finding these two values (which play a major role in modern day cryptography) will be the topic of this article.

We begin with noting that-

$$\sigma(p\hat{}1)=1+p \ , \ \sigma(p\hat{}2)=(1+p+p\hat{}2) \ , \ \sigma(p\hat{}n)=\sum_{k=0}^{n} p\hat{}k$$

for any prime p. Also,by use of the geometric series, we can simplify the sum to get-

$$\boldsymbol{\sigma(p\hat{}n)=(p\hat{}(n+1)-1)/(p-1)}$$

This result reduces to the simple form σ(p)=p+1 whenever the power n equals one. Using the above definition of f(N) we can also obtain the closed form-

$$\mathbf{f(p^n)=[\sigma(p^n)-p^n-1]/p^n =(1-p^{1-n})/(p-1)}$$

Thus we can conclude, once p and n are known, that the values of $\sigma(p^n)$ and $f(p^n)$ follow directly from these last two equations. Note that for large p the number σ(p^n) lies just slightly above p^n and the number fraction f(p^n) lies close to 1/p.

Let us test out these last two equations for several different large primes with n greater than one. For the first of these we look at-

$$N= p\hat{}n= 38561\hat{}3= 57338306752481$$

. For this case our MAPLE program yields the following instantaneously-

$$\sigma(p^n)= 57339793741764 \quad \text{and} \quad f(p^n)= 0.00002593360994\ldots$$

A second example involves the eighty digit long prime-

$$p=1588762642300741251870842105217262803671170466751 1$$

taken to the n=12 power. It produces in a split second-

$\sigma(p^{12})=$
2586474688865252461133649390606988790975929271864451029030181681208882129640
8226865310129717568361751045082043040585662835698131663570407924764494024962
4288425658410651056741781389879993365906526965406619725102895201685103624113
5517204420732154178754949231561574234052173311129216214609849027816882788718
0688355961713547848542581814794990973258810305140660213153884325102739887318
3384630738172108202382531228993532748995473103238742350674359146826944080323
6349214250218548852873088798957442572152284948268952914949984622155650091077
77378889891792958374312506959034506190070257878172427129

and-

$$f(p^{12})= 0.629420640550728186499885412428188856822797527817 17\times10^{(-49)}$$

These last two examples of the sigma and f function for large $N=p^n$ have shown that there is no difficulty in quickly finding these values especially when n=1 which includes the case of semi-primes. Let us show how one can factor such a semi-prime. We start with any large semi-prime N=pq and take its sigma function getting--

$$\sigma(N)=\sigma(p)\sigma(q) =(p+1)(q+1)=pq+(p+q)+1$$

Replacing q by N/p, one finds-

$$p^2-p[\sigma(N)-N-1]+N=0 \quad \text{or the equivalence} \quad p^2-p[Nf(N)]+N=0$$

Solving the second of these for p produces the prime factors-

$$p=Nf(N)/2-\sqrt{[Nf(N)/2]^2-N} \quad \text{and} \quad q=N/p= Nf(N)/2+\sqrt{[Nf(N)/2]^2-N}$$

We have chosen the signs to make p<q. One sees from this last result that all that is required to factor any semi-prime is to know $f(N)=[\sigma(N)-N-1]/N$. Most advanced mathematics programs, such as Maple and Mathematica, give the values of sigma out to some twenty places, so semi-primes out to about 40 decimal places can be factored directly with a minimum of computer time. Let us demonstrate things for the forty digit long semi-prime-

$$N=1774319431086405772344947305713375666887$$

Using our Maple computer program on our home PC takes about two minutes to find –

$$\sigma(N)= 1774319431086405772436364835972631404176$$

Plugging this σ(N) into the equation $p^2-p[\sigma(N)-N-1]+N=0$ and using $q=N/p$ produces within an extra split second the factors-

$$p= 27961320846321979937 \quad \text{and} \quad q= 63456209412934657351$$

With the advent of ever faster supercomputers and the possibility of future quantum computers matching their hype, one hundred digit long semi-primes should be factorable shortly using the above approach. This will make present day public key cryptography obsolete.

U.H.Kurzweg
December 27, 2023
Gainesville, Florida