PROPERTIES OF THE SIGMA FUNCTION FOR INTEGER POWERS OF PRIMES

The sigma function σ(N) for any integer is defined as the sum of all its divisors. Here are two examples--

σ(12)=1+2+3+4+6+12=28 and σ(16)=1+2+4+8+16=31

This point function takes on a local minimum whenever N is a prime P. For any prime we have-

σ(P)=1+P

so that σ(31)=32. It is our purpose here to examine the sigma function P taken to power n and to look at semi-primes.

Let us begin by writing down the values of σ(N) or the first few primes and their powers. Here is a table easily established by simple addition-

P	n	P^n	σ
2	1	2	3
2	2	4	7
2	3	8	15
2	4	16	31
3	1	3	4
3	2	9	13
3	3	27	40
3	4	81	121
5	1	5	6
5	2	25	31
5	3	125	156
5	4	625	781
7	1	7	8
7	2	49	57
7	3	343	400
7	4	2401	2801

Note how the sigma function for a given prime increases as n is increased. We see from the table that σ(5^5)=σ(3125)=5(625)+(781)=3906. One can also generalize the result as-

σ(P^n)=σ[P^(n-1)]+P^n

Expanding the left hand side of this last equation we find-

σ(P^n)= $\sum_{k=0}^{n} P^k$

On using the geometric series we have the finite sum equals [P^(n+1)-1]/(P-1) . Hence we have the general identity for the sigma function of any prime P taken to the nth power given by-

$$\sigma(P^n)=\sum_{k=0}^{k=n} P^k = \frac{P^{(n+1)}-1}{P-1}$$

So, for example, we find-

$$\sigma(7^5)=\sigma(16807)=19608$$

Note that it is always true that $P^n<\sigma(P^n)$. A test for P being prime is that any of the following identities equals one-

$$1=\sigma(P)-P$$

$$1=\sigma(P^2)-P(1+P)$$

$$1=\sigma(P^3)-P(1+P+P^2)$$

To test whether P=1379 is a prime, we get from the first of these equations that-

$$1 < 1584-1379=205$$

So 1379=7x197is a composite number and not a prime.

Consider next any semi-prime N=pq, where p and q are primes. Taking the sigma function of such a composite yields-

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

So the sum of the two primes equals-

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

This means that if we know $\sigma(N)$ then we have the two equations-

$$pq=N \quad \text{and} \quad p+q=\sigma(N)-(1+N)$$

Eliminating either p or q from these produces the closed form solution-

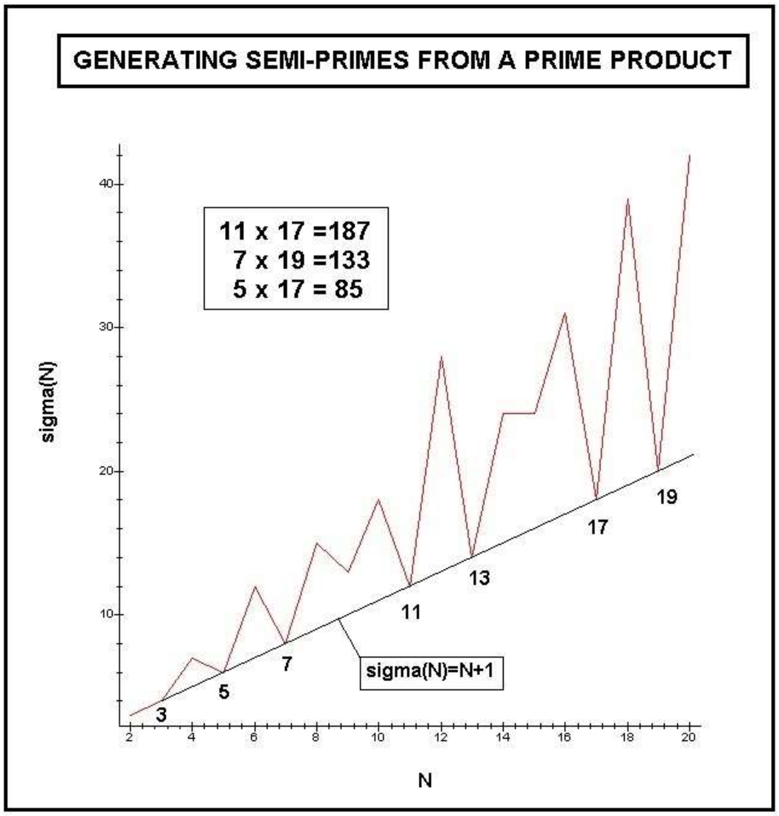
$$[p,q]=S\pm\sqrt{S^2-N)}$$

, with $S=[\sigma(N)-N-1]/2$. My laptop using MAPLE is able to give the value of $\sigma(N)$ for Ns up to about forty digits in times of two minutes or less. Pushing my think pad laptop to its limit, here is the factoring of the following 40 digit long semi-prime in a little less than two minutes-

1774319431086405772344947305713375666887=
27961320846321079937 x 63456209412934657351

This approach for factoring large semi-primes is indeed remarkable and suggests that the use of this approach using super-computers should allow one to use the present approach to factor Ns in the one hundred digit length making RSA cybersecurity obsolete.

A final point we wish to make concerning the use of the sigma function. If one plots $\sigma(N)$ versus N the following pattern emerges-



As already mentioned earlier, sigma(N) has local minima at N equal to a prime. Also we see that it is an easy matter to generate semi-primes by reversing the procedure and taking the product of any two of the primes shown. Thus the semi-prime N=187 is the product of the two primes 11 and 17. It is also possible to generate triple-primes by taking the product of three primes . Thus N=7 x 13 x 19=1729 is such a triple prime.

U.H.Kurzweg
July 4, 2023
Gainsville, Florida.
Happy 4th of July