SEMI-PRIMES AND THE NUMBER FRACTION

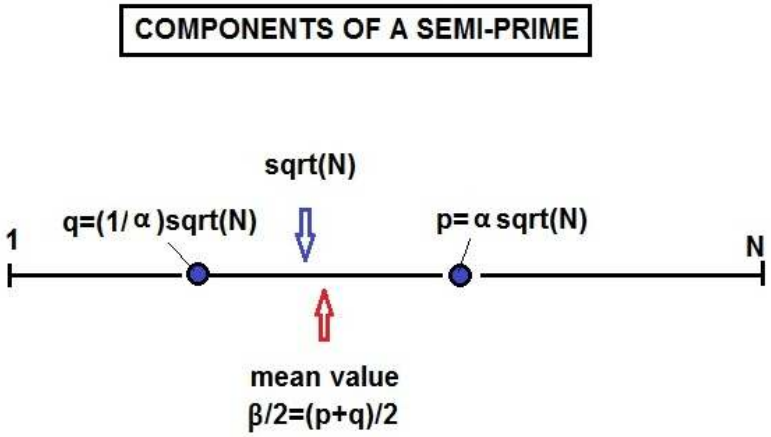
In an earlier note we have shown that any positive integer can be characterized by a number fraction defined as-

$$f = \frac{\sum divisors - (N+1)}{N}$$

This number is typically of the order of one, but ranges from f=0 for prime numbers to above two for certain super-composites. Our interest here is to examine the value of f when N=pq is a semi-prime consisting of the product of two primes p and q. Such semi-primes are of interest in cryptography because they cannot be rapidly factored when their length exceeds several hundred digits. The number fraction for any semi-prime will be-

f=[(p+q)]/N=(1/p)+(1/q)=[α+(1/α]/sqrt(N)=β/N

Here α and β are constants defined by p=αsqrt(N), q=(1/α)sqrt(N), and β=fN=p+q. Note that β will be an even integer while α typically is a non-integer. We can display these various quantities associated with a semi-prime as follows-



From these definitions we also have the identities-

β=(α+1/α)sqrt(N)

and

$$p=\{\beta+\sqrt{[(\beta)^2-4N]}\}/2=N/q$$

We can say that once β=fN has been found the semi-prime N=pq has essentially been factored.

Consider the trivial case of N=247 for which f=(13+19)/247 and β=32. Thus p={32+sqrt[1024-988]}/2=19 and q=247/19=13. Here α=19/sqrt(247)=1.208941.. . The easiest way to determine β with our home PC is to use the MAPLE command-

```
with(numtheory): N:=known semi-prime β:=evalf((add(i,i=divisors(N))-(N+1)));
```

The number fraction follows from β=fN. We can use this command to quickly calculate the value of β=p+q. When this result is combined with N=pq it produces explicit values for the factors of the semi-prime. This approach can be used to determine f and β for any semi-prime as long as N does not exceed the computer's factoring capabilities. Typically the value of f for semi-primes will be a number near zero but not zero which is reserved for primes only. Its finite value is-

$$f=[\alpha+(1/\alpha)]/\sqrt{N}>2/\sqrt{N}$$

since we are assuming p>sqrt(N) and q<sqrt(N). We can identify a semi-prime by noting that f lies somewhere above 2/sqrt(N). An alternative way of finding p and q for smaller N is to simply use the MAPLE command-

```
with(numtheory): divisors(N);
```

This will produce the four element output [1, q, p, N] from which the semi-prime factors can be read off directly.

Let us look in more detail at some specific semi-primes. For this purpose we choose the three semi-primes-

(1) - Arecibo Number N1=1679=23 x 73 which represents the number of digits contained in a message sent to outer space by the Arecibo radio telescope in 1974. Since the number of decimal digits in the factors are equal it can also be classified as a brilliant number with β=23+73=96. Briliant Numbers are a special sub-class of semi-primes which are easier to

factor than ones where p and q differ in the number of integer digits. The factors for N1 follow most directly from the divisors operation which yields divisors(N1)=[1, 23, 73, 1679].

(2) - Fermat Number N2=2^{32}+1=4294967297= 641 x 6700417. This number was first factored by Leonard Euler using some clever, pre-computer , mathematics. Here one has β=6701058 and the divisor operation yields divisors(N2)=[1, 641, 6700417, N2] . The number fraction is f=β/N2.

(3) -Our own 1419 digit long semi-prime
N3=8310156141770664028473082208699073780052685376325307469402107133959602689896691896035032731216930858107852071782870166608315150555573006919965664155263485238567282304692288601470739491126861039980682941401576686051928255243720678786776173793493537243350816597826091520075485189157725239497195502019597612528343684991195159279461569923531275472432424272577339417575675078653324284761009050791025075875696619237026080434792415363567234142289530068205038168482876049822727681397362718510332857439565774985202966049870597136648550023339335577105118559233933182035210484875314195043827096947477183071705276374015998582332795102369518676779368560742788282281141086648213622936210337548044170610023425884122475892426789957818671081533464105706010141038351496726382335217922060902623932009681124918342324196087440009639153583102902775592876722450382072446027789937605724601462460023675192656604466252301082955400844355392617177858214320630264195241799765207813667055991674926759503652892070327177352179507038110784414854014806582215780217561365982652956912846895264704749640599857730198771529908876950450674385500870996393441901619712720987946797045869368016865937079374378789285425097349981440741106812943124099593287239655420153608405936582361486045797707773329320890421098292794582019698463219948106686827849858303507143746061634339962096314401446307138604451116365425482085157804690779483463574273896049901091822010077604 67

which I posted on the internet several years ago as a challenge. So far no one has succeeded in factoring it nor do I think anyone will for another ten years or so .

Our computer shows that the value of f for the Arecibo semi-prime is f=β/N1=0.057176. When this value is substituted into the above general solution for p , one finds p=73 and q=N1/p=23 just as found by the divisor operation. In addition we have that α= p/sqrt(N1)=1.7815 and β=p+q=96. The latter result implies that p and q are located symmetrically about the mean value β/2= 48. The first part shows that p is positioned at a location about 1.8 times larger than the square root of N1.

Look next at the Fermat Number N2=2^{32}+1. Here our PC produces a number fraction f=0.0015602116469 in a split second. Substituting into the above formula for p we find p=6700417 and q=631 . That Euler was able to obtain this same result over 200 years ago without the benefit of computers is indeed amazing. He was lucky in the sense that q is here

a very small compared to sqrt(N2). Notice that in this case α=p/sqrt(N2)=102.2402.. is a large constant implying that p and q are both located a long distance from the mean value of β/2=3350524 . It becomes more difficult to factor large semi-primes when such large separations are present provided q does not become too small as in the Fermat Number case. The alternate way to generate p and q for N2 is to use the MAPLE command divisors. The values found by that approach are identical.

Finally we look at the third semi-prime N3 listed above. This 1419 digit number lies above the factoring capabilities of our PC and that of all other extant computers in the world of which we are aware. This despite the fact that I was able to construct the number in just a few minutes.

In testing out our PCs capability for generating f and β for larger semi-primes N, we find it is able to handle numbers up to about 50 digit length. This is the same size integer which one can evaluate by the MAPLE commands ifactor(N) or divisors(N). All of these approaches for finding p and q are essentially brute force methods in which N is divided by every prime lying between 1 and sqrt(N) until the prime corresponding to q is found.

One of the largest semi-primes our home PC can factor by the f-β approach is the 53 digit long number-

N4=13469199089641601294165099996964705019718136187846657

A three minute calculation using our MAPLE computer program produces-

f= 0.44116467626487923142327146037278660463551113175302260221705750206918599086356416 x 10^{-23} =β/N4

From this result we can infer that-

α= 512.00000000000000000001129372954773376738405293782438986436318008725589036674 08…

and-

p=α sqrt(N4)= 594211218856982531951579627 51

with-

q=(1/α) sqrt(N4)= 226673591177742970257407

Two other examples of large semi-primes which readily factor in a few seconds are

the Mersenne Number –

$$N5=2^{109}-1= 649037107316853453566312041152511$$

which factors into-

q=745988807 and p=870035986098720987332873

The semi-prime-

N6= 886062124309309435329002990455546 21

which factors into-

p=4700705565677722603 and q=18849555921538807

The success of the above factoring approach depends essentially on the time it takes to find the value of the number fraction f = β/N. This will be about the same as the time taken by the MAPLE operations divisors(N) or ifactor(N) . One is out of luck when attempting to use such brute force approaches for semi-primes of a hundred digit length or more. The calculation times for factoring very large Ns become extremely long even when employing more elegant factoring techniques such as the elliptic curve factorization method or the generalized grid technique. I don't expect any one will be able to factor the 1419 digit public key given by N3 above any time soon. The size of this 4700 bit number (recall that bit/digit=ln(10)/ln(2)=3.3219..) lies considerably above the largest semi-prime which has so far been factored by anyone. The public key in most common use in today's cryptography is RSA-2048 (617 decimal digits). It is close to being broken as suggested by the withdrawal of an earlier $100,000 reward for being able to factor it. It may be time to rethink use of public keys and rather revert to weakly encrypted information hidden in electromagnetic micro-pulses used in conjunction with normal public microwave transmissions and satellites. The basic rule among cryptographers is that a message is secure as long as your opponents can't detect or decode it.

January 31, 2013