s(n) An Arithmetic Function of Some Interest, and Related Arithmetic

Gideon Samid, PhD
samidg@tx.technion.ac.il

Abstract: Every integer n > 0 ϵ ℕ defines an increasing monotonic series of integers: n_1, n_2, ...n_k, such that n_k = nk +k(k-1)/2. We define as s(m) the number of such series that an integer m belongs to. We prove that there are infinite number of integers with s=1, all of the form 2^t (they belong only to the series that they generate, not to any series generated by a smaller integer). We designate them as *s-prime* integers. All integers with a factor other than 2 are not s-prime (s>1), but are *s-composite*. However, the arithmetic *s* function shows great variability, lack of apparent pattern, and it is conjectured that s(n) is unbound. Two integers, n and m, are defined as *s-congruent* if they have a common s-series. Every arithmetic equation can be seen as an expression without explicit unknowns -- provided every integer variable can be replaced by any s-congruent number. To validate the equation one must find a proper match of such members. This defines a special arithmetic, which appears well disposed towards certain cryptographic applications.

s-series: 1. S-SERIES

An integer n > 0 ϵ ℕ will define a series n_1, n_2, n_3, ...n_k such that: n_k = nk + k(k-1)/2 denoted as the *s-series of n*

Thus:

```
1, 3, 6, 10, 15, 21, 28,....
2, 5, 9, 14, 20, 27, 35,....
10, 21, 33, 46, 60, 75, 91,....
100, 201, 303, 406, 510, 615,....
```

For a large integer n >> 0 there is a greater and greater chance that it would be a member of some s-series generated by a smaller integer m < n. Reminiscent of a similar reasoning regarding prime numbers (a larger integer is more likely to be composite), one would ask: is there a number that would be designated as the largest s-prime, where an s-prime is defined as an integer which is not a member of any s-series, other than the one generated by itself?

We can readily prove that:

Theorem 1: All integers of the form 2^t are *s-prime*, and hence there are infinite *s-primes*. (t an integer).

Proof: We can write

[1]……..$n = 2^t = kn + k(k-1)/2$

or: $2^{t+1} = 2kn + k(k-1) = k(2n + k - 1)$. If k is even: k=2r, we can write:

[2]……..$2^{t+1} = 2r(2n + 2r - 1)$

The expression (2n+2r-1) is odd and thus equation [1] cannot be fulfilled. If, k is odd: k=2r+1, then [1] becomes:

[3]…….$2^{t+1} = (2r+1)(2n + 2r+ 1 - 1)$

And the component (2r+1) is odd and again equation [1] can not be fulfilled.

If r=0 equation [3] is reduced to $2^{t+1} = 2n$, or $n=2^t$, indicating that a number of the form 2^t can be the first member of an s-series.

In summary, an integer of the form 2^t cannot be a member of an s-series other than the one generated by itself:

2^t, $2^{t+1} + 1$, $(3)2^t+3$, $2^{t+2}+6$,...

which proves theorem 1.

Theorem 2: There are no other *s-primes*, except the ones of the form 2^t

Proof: Every odd n belongs to the series generated by (n-1)/2. Thus for odd n $1 \leq s(n)$. For even n we write $n=2^tR$, where R > 1 is odd. We equate:

[4]……..$n=2^tR = nk + k(k-1)/2$

re-writing: $2^{t+1}R = 2nk + k(k-1) = k(2n + k -1)$

By setting $k=2^{t+1}$ we end up with: $R = 2n + 2^{t+1} -1$

If $R > 2^{t+1}$ then we can compute n to be: $n = (R - 2^{t+1} + 1)/2$

And thereby find values of (n,k) to satisfy [4]. Thus all n of the form 2^tR where R>1 is odd, and where $R > 2^{t+1}$ are <u>not</u> s-primes.

For all other odd R, namely where $R < 2^{t+1}$, we set k=R and:

$2^{t+1} = 2n + k - 1$

Substituting: $2^{t+1} = 2n + R - 1$. Leading to: $n = (2^{t+1} - R + 1)/2$

Since R is odd, $(2^{t+1} - R + 1)$ is even, and n computes to a positive integer. Since R is odd, we don't have to worry about the possibility of $R=2^t$.

In summary: every integer of the form 2^tR, where R>1 is odd, is a member of at least one s-series other than the one generated by itself. Hence theorem 2 is proven.

Examples: for n=38, we write $n=2^119$. Since $19 > 2^2$ we set: $k=2^2=4$, and $n= (19 - 2^2 + 1)/2 = 8$.

Indeed, the number 8 generates the series: 8, 17, 27, **38**, 50, 63, 77, 92,....

Which happens to be the only series (other than itself) that the number 38 belongs to.

For n=24, we write $n=2^33$. Here $R = 3 < 2^4$ and thus we set: k = R = 3, and
$n = (2^4 - 3 + 1)/2 = 7$

Indeed, the integer 7 generates the s-series: 7, 15, **24**, 34, 45, 57, 70

If $m \in \mathbb{N}$ is the k-th element in a series generated by n, we shall denote this as: $m =*(n,k)$. If m belongs to series generated by $n_1, n_2, n_3, ...n_i$ we shall write: $m =*(n_1 ,k_1) =*(n_2 ,k_2) =*(n_3 ,k_3)=..... =*(n_i ,k_i)$

We denote the series generator, n, as the denominator, and the ordinal placement, k, as the nominator. Every integer can be defined by at least one pair of [denominator;nominator].

We shall now define an arithmetic function s(n) to express these results, and investigate the patterns of s.

s-series: 1.1. THE ARITHMETIC FUNCTION s(n)

s(n) will simply represent the number of s-series that integer $n \in \mathbb{N}$ belongs to. Since each integer, n, originates a series: $n_1, n_2, n_3, ...n_k$ we have $1 \leq s(n)$ for all $n \in \mathbb{N}$.

The opposite question is: *Is s(n) bound?* This is still an open question. One might conjecture that it is not. Theorems 1 and 2 together prove that positive integers with s(n)=1 become rarer and rarer, as n increases. Generally numbers $m < 2n$ have a "chance" for n to be a member of their series. Thus with increasing n, s(n) would increase too -- boundless. But that remains to be proven.

The table below shows the s_{max} values at increasing ranges:

Integer Range	Highest s-value (S_{max})	Integer with S_{max}
1 -- 10	3	9
1 -- 100	6	45
1 -- 1000	16	945
1 -- 10000	24	9009

The number 945, for instance, belongs to the self generated sequence:

945, 1891, 2838, 3786, 4735,....

As well as to 15 more series; the ones generated by:

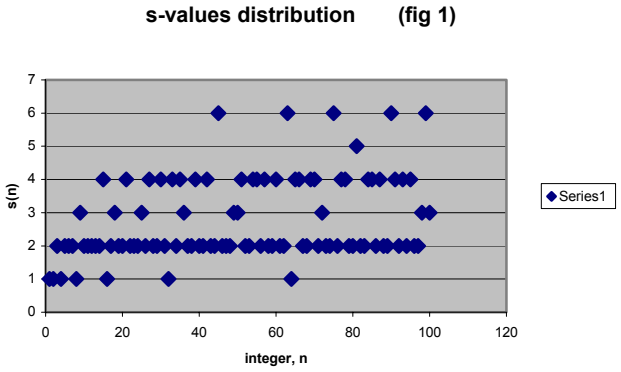
2,10, 17, 22, 35, 44, 56, 61, 90, 101, 132, 155, 187, 314, 472

For instance, the series generated by 101 computes to: 101, 203, 306, 410, 515, 621, 728, 836, **945**,.... And the series generated by 155 computes to: 155, 311, 468, 626, 785, **945**,....

We can write: 945 =
(2,42)=(10,35)=*(17,30)=*(22,27)=*(35,21)=*(44,18)=*(56,15)=*(61,14)=(90,10)=
(101,9)=(132,7)=*(155,6)=*(187,5)=*(314,3)=*(472,2)=*(945,1)

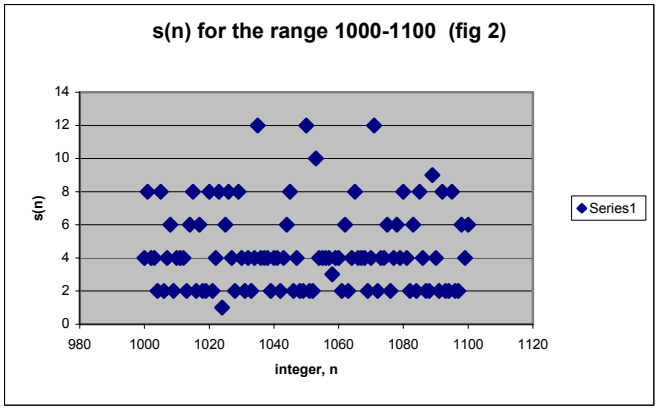
And state: s(945)=16

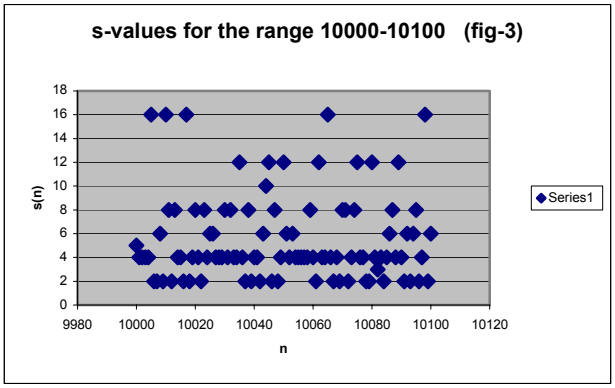
The second question regarding the s-function is its pattern, or lack thereof. Figure 1 depicts the distribution of s(n) for the range 1-100. s=2 is the most popular, but surprisingly there are more integers with s=4 than integers with s=3. And there is only a single case of s=5, while there are 5 integers with s=6.



Charting a similar depiction of s-function for the range 1000-1100 (fig 2) yields additional peculiarities: there are no s=5,7,11; there are three integers with s=12, a single case of s=1,3,9,10, and s=4 is the most common.

When one examines the range 10000-10100 more peculiarities arise. There are no s=1,7,9,11,13,14,15, but there are 5 integers with s=16. (fig-3)





It appears that the s function behaves "strangely".

s-series: 2. CONGRUENCE

Two integers n,m ϵ ℕ will be regarded as "s-congruent" if there is a third integer, p ϵℕ, such that both n, and m are members of the s-series generated by p. We denote congruence as n =~ m, or n ~= m. or: $\sim(n,m)_{cong.}$

Hence 492 =~ 117 since the number p=58 claims both as members:

58, **117**, 177, 238, 300, 363, 427, **492**...

However, the generating number p'=9 also claims these two numbers in its series:

9,19,30,42,55,69,84,100,**117**,135,154,174,195,217,240,264,289,315,342,370,399,429,460,**492**,...

We define the number of series that claim both numbers as members as the *Order Of The Congruence.* The question comes to mind: *is the order of a congruence a bound number?* And if so which are two integers that claim it? A simpler version would be construed by asking the same with respect to some range of integers (L,H): for that range which is the highest order of congruence, and what is a pair of integers that claims it.

Obviously a number is congruent with itself: *n* ~= *n*, and for all odd numbers we can write: 2n+1 ~= n. s-primes are not congruent with any number but themselves. The higher the s-value of two integers, the greater the likelihood that they are congruent.

s-congruence can be readily extended to several integers: $\sim(n_1, n_2, n_3, ...n_k)_{cong.}$

Which implies that there exists a number p that claims all the congruent numbers as members of its s-series.

For a large such k, the chance for a high order of congruence becomes very low.

s-series: 3. IMPLICIT EQUATIONS

Given two integers, a, and b, one could interpret each integer to be replaceable by any other congruent integer, and explore:

a =?= b

Meaning: is there a number p such that a ~= p, and b ~= p. If there exists such an integer p then one would write: a =~= b

Note that a =~= b does not imply a ~= b. Example: Let a=93, and b=405 The number 240 is congruent to both:

240 ~= 93, both belong to the series generated by 49. 240 ~=405, both belong to the series generated by 79. But 93 !~= 405 ("!~=" designates not congruent), since 93 has an s value of 4, and the respective generating numbers are: 13, 30, 46, and 93. None of these numbers claims 405 as member:

```
13, 27,42,58,75,93,112,132,153,175,198,222,247,273,300,328,357,387,418,450

30, 61,93,126,160,195,231,268,306,345,385,426,...

46,93,141,190,240,291,343,296,450,...

93,187,282,378, 475,...
```

This gives rise to a whole slew of equations like:

a =?= 2b; ab =?= c; a^t =?= b; etc....

or to equations with one or two unknowns:

f(a,b,x) =?= 0 *Is there a variable x that would make that equation whole?*

Note that if there is an x such that f(a,b,x)=0 then there exists an x such that f(a,b,x) =~= 0, since any number is congruent to itself. One could regard this newly defined s-algebra as an extension of the normal integral algebra, which may be regarded as a private case thereof.

For example: [5]…… 3 + x =?= 4

x=1 is a solution. Are there more? Let's try x=3:

6 =?= 4

4 generates the series: 4,9,15,22,**30**,39,49

6 generates the series: 6,13,21,**30**,40,...

The number 30 is shared by both series therefore: 6 =~= 4, while clearly 6 !~= 4,. So the value x=3 is a solution to the original equation, [5]. How many more solutions are there?

s-series: 4. ONE WAY FUNCTIONS

The apparent lack of pattern of the arithmetic s(n) function may suggest one-way algorithms or prospective usefulness. Example:

Procedure P1:

1. given integers n,k, compute n_k=*(n,k)=nk+k(k-1)/2.
2. compute n^*_k , as the next to the smallest number such that: $n^*_k = *(n_k, l)$, for some integer l
3. If $n^*_k \leq T$, where T is a preset limit, then n^*_k is the output of P1. Otherwise substitute n with n^*_k and repeat steps 2, and 3.

It is conjectured that after some cycles this procedure will halt. If it does, it appears to be a very strong one-way function, that might be used potentially as a hashing algorithm.

Note that if P1 were to be defined as choosing the smallest congruent number, then it would have run the risk of endless recycling.

P1 suffers from the issue of indeterminate computing time, since for low T values, P1 might cycle quite a few times.

An alternative is **Procedure P2**:

1. given integers n,k, compute n_k=*(n,k)=nk+k(k-1)/2.

2. compute n^*_k , as the next to the smallest number such that: $n^*_k = *(n_k, l)$, for some integer *l*.
3. Substitute n with n^*_k and repeat steps 2, r times. The result is the output of P2.

For example: n = 5, k =4 1. *(5,4)=26. 26 belongs only to two series, the one generated by 5, and the one generated by itself, hence: $n^*_1 = 26$. We compute: *(26,4)= 110. 110 belongs to four series, generated by 5,20,26,110. Hence $n^*_2 =20$. *(20,4)= 86, which belongs to a series generated by 20 and itself. So we compute *(86,4)= 350. 350 is generated by: 2,8,47,68,86,350, so $n^*_3 =8$, and if r=3 then 8 is the result of P2. For P1, if T=10, then 8 is the result there too, because the earlier outputs; 26, 20 where larger than T=10.

s-series: 5. SUMMARY

The definition of an s-series generated by every positive integer leads into a special s-arithmetic, and s-algebra with some loose similarities with known relationships. s-primes like regular primes are infinite in number, despite some intuitive sense that there might be a largest one. Both primes get diluted at large numbers, however, the regular primes exhibit defying irregularity, while the s-prime are very regular. In both types of primes one could find a stretch of any desired count that would be free from primes. When it comes to composite numbers the comparison is in reverse. Regular composites are "regular", every other number is even, for instance. s-composites appears to defy any set pattern or order, in terms of their arithmetic s-function. For such a simple arithmetic primitive the s-series claim a certain measure of mathematical beauty.