A NEW FUNCTION FOR GENERATING PRIMES

If one looks at the sequence-

$$S = n^3 = \{1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, \ldots \}$$

and then takes the difference between the n+1 and n term, one finds the new sequence-

$$T = (n+1)^3 - n^3 = 1 + 3n + 3n^2 = \{7, 19, 37, 91, 127, 169, \ldots \}$$

Looking at the elements in this last sequence, we see that many of them are prime numbers while some are composites such as 91 and 169. When we first observed this behaviour we tried to generalize things by looking at a generating function of the form-

$$F(n, k) = (n + 1)^k - n^k = \sum_{m=0}^{k-1} \frac{k!}{m!(k-m)!} n^m$$

In looking at such sequences it became clear that, when k was a composite number, no terms in the sequence were prime. However when we replaced k by a prime p, then sequences containing multiple primes arise. This suggests we have a new prime number generator given by-

$$F(n, p) = \sum_{m=0}^{p-1} \frac{p!}{m!(p-m)!} n^m$$

Here p is any prime number and F is a p-1 order polynomial in n. For the first few primes this expression leads to the formulas-

$$F(n, 2) = 1 + 2n$$
$$F(n, 3) = 1 + 3n + 3n^2$$
$$F(n, 5) = 1 + 5n + 10n^2 + 10n^3 + 5n^4$$
$$F(n, 7) = 1 + 7n + 21n^2 + 35n^3 + 35n^4 + 21n^5 + 7n^6$$
$$F(n, 11) = 1 + 11n + 55n^2 + 165n^3 + 330n^4 + 462n^5 + 462n^6 + 330n^7 + 165n^8 + 55n^9 + 11n^{10}$$

From these formulas we find, for instance, the prime numbers-

$$F(2, 5) = 211 \quad \text{and} \quad F(9, 11) = 68618940391$$

Note that both 5 and 11 are primes as required.

One can automate the prime search by using the following two line MAPLE program-
\[ F := (n+1)^p - np; \]

for \( n \) from 1 to 20 do \{ \( n \), \( F \), isprime(\( F \)) \} od;

All solutions at fixed \( p \) for which the answer yields true will be primes. These primes can have a large number of digits. As an example, we find the 146 digit prime-

\[
F(25,97) = 174836719561207264287762220290379675156178701331776945090696781463427851076901470634592241122809368577077677652689940045545545284949240551
\]

Again, if \( p \) is not a prime then \( F(n,p) \) can’t be either. One can support this point by looking at the composite \( p = 9 \) and searching from \( n = 1 \) through 200. None of the resultant integers \( F(n,9) \) are found to be primes. This allows one to conjecture that –

Some of the numbers \( F(n,k) = (n+1)^k - nk \) will be prime numbers provided \( k \) is a prime, but \( F(n,k) \) will be a composite when \( k \) is not a prime.

A rigid proof of this observation remains to be found. We point out that all the numbers \( F(n,k) \), be they prime or composite, satisfy the condition that \( F(n,k) \mod(6) = 1 \). This means they are of the form \( 6n+1 \). Such numbers will produce about half of what we have termed the Q Primes and include the primes 7, 13, 19, 31, 37, etc. The other half of the Q Primes have the form \( 6n-1 \), and hence should be obtainable from-

\[ G(n,k) = F(n,k)-2 \]

They will include the Q Primes 5, 11, 17, 23, 29, 41, etc. and have the property that \( G(n,k) \mod(6) = 5 \). We have, for example, the primes-

\[
G(2,3) = F(2,3)-2 = 27-8-2 = 17 \quad \text{and} \quad G(3,4) = F(3,4)-2 = 173
\]

Note here that the condition that the \( k \) in \( G(n,k) \) be a prime is no longer necessary. However, the \( 6n \pm 1 \) condition continuous to hold for all prime numbers above 3.

What is of interest in the above results is that \( F(n,k) \) and \( G(n,k) \) each contain a large number of integers when \( n \) and \( k \) get large. This means one should be able to quickly construct a public key in the form of the large semi-prime-

\[
N = F(n_a, p_a) \cdot G(n_b, k_b) \quad \text{or} \quad N = F(n_a, p_a) \cdot (F(n_b, p_b)
\]

That is, for example,-

\[
F(2,17) \times G(5,9) = 673044169010639
\]

Here the information contained in the semi-prime \( N \) are the prime factors-
Once $N$ gets into the range above one-hundred, the factoring of $N$ becomes extremely time-consuming. This is why public keys used in cryptography are essentially unbreakable by adversaries using even the fastest supercomputers. The number of primes predicted by both the functions $F(n,p)$ and $G(n,k)$ are both expected to be infinite and have a much higher density of appearance than say Mersenne primes of which less than 50 are known today. All $F(n,p)$ primes lie along the diagonal $6n+1$ and all $G(n,k)$ primes lie along the diagonal line $6n-1$ in the type of integer spiral pattern which we came up with several years ago. Here is a graph of this spiral showing the diagonals along which all primes greater than 3 are found-

U.H.Kurzweg
July 1, 2015