CONSTRUCTION OF PRME NUMBERS USING PRODUCTS OF IRRATIONALS

We showed several years ago (see https://www2.mae.ufl.edu/~uhk/LARGE-PRIMES.pdf) that products of irrational numbers can be expanded into infinite sequences of integers from 0 to 9. Such sequence can then be used to quickly generate prime numbers of any chosen length. We wish in this note to expand our thoughts on this topic.

Let us begin with the simple irrational product –

N=exp(1)*sqrt(7)/π^2=0.72869158876264230074125187084210521726280367117046675065843

with N expanded out to 60 digits. Next take out the first five digits after the decimal point , drop the decimal point, and them retain only the next fifty terms. This produces the 50 digit quasi random number-

is not quite random with the number of 0 through 9 appearing respectively_7,7,2
M=15887626423007412518708421052172628036711704667506

This number,4,4,7,7,5,0 times. This does not mean however that M can't be used to generate a large prime in the fifty digit range. The way to accomplish this is to carry out the computer manipulation-

for n from -20 to 20 do({ n, isprime(M+n)})od;

It produces a prime at n=5. That is, we have a new fifty digit long prime-

P=15887626423007412518708421052172628036711704667511

A big advantage of generating a prime by the present approach is that it can be stored very compactly and easy to transmit between sender and friendly receiver in public key cryptography. It will be understood only by someone realizing that –

5-N-50-5 means a fifty digit long prime P generated from N=exp(1)sqrt(7)/π^2

Next we generate a second prime based upon the irrational product N=11sqrt(π)/sqrt(1378). Out to fifty digits it reads-

N=0.52522212529845168662126048197312031277452918470714

Dropping the first three digits after the decimal, eliminating the decimal point, and then taking the next 40 digits and adding an n we get-

Q=2221252984516866212604819731203127745291+n

A search finds that n=98 . This produces the following 40 digit long prime-

Q := 2984516866212604819731203127745389

The designation for Q is-

3-N-40-98 with N=11exp(1)sqrt(πsqrt(1378)

We can construct a public key from the product of the primes P and Q. It reads-

15887626423007412518708421052172628036711704667511 x

2221252984516866212604819731203127745389

This produces the 90 digit long public key-

PK=35290437608994238607840136987152123616864914353825393535726090453003

625550039337308356779.

A mod(6) operation on this Public Key yields 5 meaning it lies along the radial line 6n+5 in a hexagonal integer spiral. P mod(6)=1 meaning it lies along the radial line 6n+1. Finally Q mod(6)=5 meaning it lies along the radial line 6n+5. Knowledge of these mod values considerably reduces the number of trails needed to break the semi-prime PK into its prime components.

U.H.Kurzweg
October 24, 2021
Gainesville, Florida