CONSTRUCTING TRUNCATED IRRATIONAL NUMBERS AND DETERMINING THEIR NEIGHBORING PRIMES

It is well known that there exist an infinite set of irrational numbers including π, sqrt(2), and e. Such quantities are of infinite length and have the property that they can never be represented as the ratio of two real numbers. Segments of irrational numbers of fifty digit length or so are of interest in connection with public key cryptography (RSA) where the product of two segments of different irrationals adjusted to be prime can lead to nearly unfactorable semi-primes N=pq. It is our purpose here to extend several of our earlier studies on semi-primes to generate some large segments of irrational numbers plus some related semi-primes using finite segments of the products of some of the better known irrationals.

Our starting point is to present a few the better known irrational numbers in terms of their basic definitions. We have –

$$\exp(1)=e=\sum_{nn=0}^{\infty}\frac{1}{n!}=2.718281828459045...$$

$$\pi=4\sum_{n=0}^{\infty}\frac{(-1)^n}{(1+2n)}=3.1415926535897932...$$

$$\ln(2)=\sum_{n=0}^{\infty}\frac{(-1)^n}{(1+n)}=0.69314718055994531...$$

$$\sqrt{2}=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+...}}}=1.4142135623730950...$$

$$\varphi=\frac{1+\sqrt{5}}{2}=1.6180339887498948...$$

$$\mathrm{J}_0(1)=\sum_{n=0}^{\infty}\frac{1}{(n!)^2}=2.2795853023360672...$$

$$\gamma=-\int_{t=0}^{\infty}\ln(t)\exp(-t)dt=0.57721566490153286...$$

These constitute the best known and often used irrational numbers occurring in the mathematical literature. They are part of an infinite set including such additional irrationals as-

$$\sqrt[p]{n}=\sqrt[p]{n_0}+\cfrac{(n-n_0)}{2\sqrt[p]{n_0}+\cfrac{(n-n_0)}{2\sqrt[p]{n_0}+...}}$$

Here p is a root of n and n_0 lies near n. Thus the square root of five, which appears in the definition of the golden ratio φ above, is given by the continued fraction-

$$\sqrt{5}=2+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+...}}}=2.2360679774997896964...$$

It is important to recognize that segments of such irrationals need not necessarily have their digits enter in a random manner. If they did then all digits between 0 and 9 would appear equally. Let us demonstrate this non-randomness by looking at the first
50 terms of exp(1) and π. Here we have-

e≈2.7182818284590452353602874713526624977572470937000

and-

π≈=3.1415926535897932384626433832795028841971693993751

so that the digit count looks as follows-

digit	0	1	2	3	4	5	6	7	8	9
e	6	3	8	4	5	5	3	8	5	3
π	1	5	5	8	5	5	4	4	5	8

The count shows that the fifty digit long segments of these two irrationals are not completely random because the appearances of the ten possible digits are not five each. The randomness will increase as the segment lengths and advance toward infinity. The fact that finite length segments of irrationals are not completely random should not interfere with quickly coming up with some truncated products of irrational numbers and the prime numb ers located in their neighborhoods. This will make possible the use of some semi-primes for public keys produced with a minimum of effort. In addition any of these primes will be identifiable by short and unique codes.

We choose to define a finite segment of an irrational number by the code-

$$L=n\left\{\sum_{k=1}^{K}\ a_k(p_k)\right\}m$$

Here a_k represents one of K common irrationals taken to the p_kth power. The segment starts with the n+1 term and is m digits long. Thissegment will be designated by M.

Let us look at a specific example. Take-

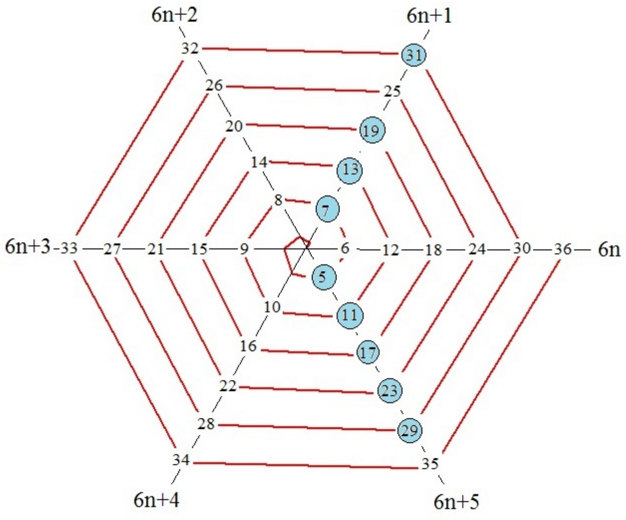
$$M = 6\{e(4)\pi(1/3)\sqrt{2}\}50$$

This code produces the fifty digit long segment-

M=20561719700183321091032163999752467815519924062956

Using a bit of modular arithmetic, we have M mod(6)=4 which implies that that M lies along the radial line 6n+4 in the following hexagonal integer spiral-

HEXAGONAL INTEGER SPIRAL AND THE LOCATION OF THE FIRST FEW Q PRIMES



We have shown in several earlier notes (look at both our MATFUNC and TECH-BLOG pages for the years 2012-15) that all primes greater than 3 must lie along the two radial lines 6n±1 . In the graph these primes are designated by blue circles. To find all primes in the immediate vicinity of M will require we look at-

isprime(M+3+6n) and isprime(M+1+6n)

This is an easy search using the one line program-

```
for n from -20 to 20 do {n, isprime(M+2±1+6n)}od;
```

In a split second one finds that the two closest primes are M+33 and M-53. These read-

P_1= 20561719700183321091032163999752467815519924062989

and-

P_2= 20561719700183321091032163999752467815519924062903

Here P_1 mod(6)=1 and P_2 mod(6)=5. Note that 5 is equivalent to -1 in the hexagonal diagram . So P_1 will be a blue circle along the radial line 6n+1 and P_2 one of the blue cirles along 6n-1.

As can be seen, it took very little effort to find the above primes since determining whether or not a number is prime is provided by a very simple computer evaluation. In addition we now have a way to store and transmit large prime numbers by a code which itself can be encrypted. For example we can completely describe the fifty digit long prime P_1 by-

$$P_1=M+33=6\{e(4),2(1/2),\pi(-3)\}50+33$$

Although the product of P_1 and P_2 will not make a good public key N because of their proximity to each other, one can easily construct a couple of primes separated from each other by orders of magnitude. Such a semi-prime N will be almost unbreakable whenever the number of digits in the Ps is large enough. Let us demonstrate this for-

$M_3=7\{7(1/3)\varphi(3)e(-2)\}50$ where M_3 mod(6)=3

and-

$M_4=10\{p(2)J01(1)\ln2(-1/2)\}45$ where M_4 mod(6)=2

In this case we find the nearest primes to be –

$P_3=M_3-4=$ 63552926881980889613675963543218124574814405573391

and-

$P_4=M_4+107=$ 877417163204700272439074887933536826672618567

One can easily verify by computer that these last two numbers of 50 and 45 digit length, respectively, are prime numbers. Their product yields the 95 digit long semi-prime-

N=5576242881814340943208982418465733854221871308350631963612648387748928
0769816293964697067750697

Without a knowledge of either P_3 or P_4 it is highly unlikely that anyone including our “big data” National Security Agency (NSA) would be successful in factoring this N in any reasonable amount of time using even their latest high speed computers.

Although the RSA approach to secret message transmission is at present still secure using fifty or so long prime numbers, this will not continue to hold with time. Longer and longer prime numbers will be required calling into question the efficacy of public keys N in RSA cryptography. It suggests that perhaps one should consider a new and simpler approach to encrypted electronic message transmission based on the present method of using encoded forms for certain large irrational numbers segments adjusted to be primes. One could envision a way the product of M and a message S would be sent as D=Sn on the public airwaves. If the sender simultaneously sends a second signal containing an encrypted form of M which only he and a friendly receiver would understand, the message will have been secretly transmitted. Consider the case were the message is S=12345 and M is defined as-

$$M=5\{7(1/2)p(-1/5)\}20= 55190400454190093113.$$

The encrypted message becomes-

$$D=(M)(S)= 681325493606976699479985$$

There is no way an adversary could decipher D. However the friendly receiver (knowing what M is) will be able to rapidly decode things as D/M=S=12345.

UHK
June 21, 2016