GENERATING LARGE PRIMES USING COMBINATIONS OF IRRATIONAL NUMBERS

Modern day cryptology relies heavily on the use of public keys K which are the products of two large primes p and q. The primes are typically about 100 digits in length so that the public key constructed from them becomes almost impossible to break in finite time with even the fastest modern day super-computers. In addition, part of the security measures being taken to prevent encryption compromise is to change these public keys often which calls for the generation of thousands of large prime numbers. Typically such numbers are constructed using random number generators. This can often make a search for primes rather laborious and the storage of many of such primes becomes a problem. We propose here an alternate method for generating large primes based on using combinations of irrational numbers. Not only will such an approach be shown to be quite fast, it also has the distinct advantage that such primes can be stored efficiently.

It is known that many constants encountered in mathematics are irrational numbers in the sense that they cannot be represented as the quotient of two rational numbers. The best known of such constants are π, exp(1), sqrt(2), ln(2), and the golden ratio [1+sqrt(5)]/2. The sequential appearance of the digits in each of these constants are essentially random as can be easily verified by noting that the ratio of even numbers(0,2,4,6,8) to odd numbers(1,3,5,7,.9) becomes essentially one as the digit count approaches infinity. For example, the first hundred digits of sqrt(2) contain 48 even and 52 odd digits.

We begin our prime number construction by first writing down some well known irrational mathematical constants to 100 digit accuracy. This leads to-

π=
3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706 8

exp(1)=
2.71828182845904523536028747135266249775724709369995957496696762772407663035354759457138217852516642 7

[1+sqrt(5)]/2=
1.61803398874989484820458683436563811772030917980576286213544862270526046281
890244970720720418939113 8

sqrt(2)=
1.41421356237309504880168872420969807856967187537694807317667973799073247846210703885038753432764157 3

ln(2)=
.69314718055994530941723212145817656807550013436025525412068000949339362196969471560586332699641868 75

Any combination of these constants will also produce an irrational number once the decimal point has been removed. We will designate such large digit numbers by N. The number N is next adjusted to fit the form 6n+1 or 6n-1, since we have shown in several earlier notes (see http://www2.mae.ufl.edu/~uhk/MATHFUNC.htm) that all primes above three have this form. The adjustment entails first determining N mod(6) and then adding a small number 'a' to N to bring N+a into compliance with 6n±1. Once this has been done all primes in the neighborhood can be determined by searching N+a+6k over a small range of the integer k until a prime is encountered. That is, N+a+6k becomes a prime.

Let us demonstrate the procedure by finding a prime p based on the 90 digit expansion-

$A:=\sqrt{2}\ln 2/\pi = .312025858078207203648521755410552436986027465111950912853$
$165341074749716615733412809020659$

Multiplying A by 10^{90} produces the 90 digit random number-

N=312025858078207203648521755410552436986027465111950912853165341074749
716615733412809020659

We find N mod(6)=1 so we can set a=0 and do a search for the prime in the form N+6k . The one line MAPLE program which allows us to do so is-

for k from -50 to 50 do {k, isprime(N+a+6*k)}od;

Running the program shows that k=18 produces the prime p=N+6(18). That is-

p=312025858078207203648521755410552436986027465111950912853165341074749
716615733412809020767

Next let us find a second prime q of 90 digit length. This time we generate the number N from A= exp(1)^2*(1+sqrt(5)]/2. The number $N=A*10^{90}$ reads-

N=119557439128494976242815312498993526059074537858375287516106625293811
638810057700278312010

for which N mod(6) =2. This suggests a=+3 or -1. Choosing a=-1, means we should search over k until N-1+6k is prime. Doing so in the range -50<k<50 produces primes for k=23, k=-1 and k=22. Taking the value k=-1 we get the prime number-

q=11955743912849497624281531249899352605907453785837528751610662529381163881005770027831200 3

Multiplying p and q together will produce an essentially unbreakable 179 digit long public key-

K := 3730501253 3701670200 4720142055 4044403683 1456101517 8103844234
6073370456 2786411924 1596830903 0103955615 5759485098 1476882924
5254728465 1276030655 2316821145 0627651939 5201160326 132366301

It took very little time and effort to produce this result. Considering there must be an infinite number of other combinations involving the above mathematical constants, it seems that thousands of prime numbers of 100 digit length or more can be rapidly produced by the present approach. What is especially noteworthy about this way of finding large ps and qs is that they can conveniently be stored in terms of very simple formulas. The above derived primes can be stored as-

$$p = \left\lfloor \sqrt{2}\ln(2)/\pi \right\rfloor_{90} 10^{90} + 6(18) \quad \text{and} \quad q = \left\lfloor [\exp(1)]^2 \frac{(1+\sqrt{5})}{2} \right\rfloor_{90} 10^{90} + 6(-1)$$

Here the subscript refers to the number of digits used in A, 10^{90} is needed to remove the decimal point, and the last number equals a+6k.

A few additional large prime numbers produced by the present technique follow-

$$p = \left\lfloor goldenratio)^4 \right\rfloor_{60} 10^{60} - 6(46)$$

$$p = [\pi^2/(\sqrt{2})^3]_{50} 10^{50} + 6(33)$$

$$p = \left\lfloor (\frac{(1-\sqrt{5}}{2})\text{^}3*\exp(-4)*\ln(8)/\sqrt{2} \right\rfloor_{90} 10^{90} + 3 + 6(37)$$

$$p = \left\lfloor (\frac{(1+\sqrt{5}}{2})\text{^}3*\exp(-4)*\ln(8)/\sqrt{2} \right\rfloor_{90} 10^{90} + 3 + 6(37)$$

From these we can generate several different public keys such as the 110 digit long key-

$$K = \{ \left\lfloor goldenratio)^4 \right\rfloor_{60} 10^{60} - 6(46) \} \{ [\pi^2/(\sqrt{2})^3]_{50} 10^{50} + 6(33) \}$$

Even NSA will have a hard time trying to factor this public key without some prior partial knowledge of one of the primes .

Finally we point out that in defining N from A it is not necessary that one starts from the first digit. We could also generate the prime p from-

$$N = [A]_{\beta-\alpha} 10^{\beta-\alpha}$$

where the digits are taken over the range $[\alpha, \beta]$. So, for example A=sqrt(π) taken from the 10^{th} to the 50^{th} digit produces a prime-

p=90551602729816748334114518279754945611 41

Using this type of N will make it even harder for an adversary to factor the resultant K.