FORMULA FOR THE GENERATION OF LARGE PRIME NUMBERS

The use for large prime numbers in the 50 to 1000 digit range has become very important in recent years because of the extensive use of asymmetric (or RSA) cryptographic techniques involving public keys. The idea behind a public key N =PQ is that it is constructed by taking the product of two large primes and the knowledge that it is extremely difficult to factor such a key even when using the fastest available super-computers. At the present time the largest N which has been factored after months of effort is one of 800 bit length or about 250 digits long. This means that to keep the public key N secure one must employ primes longer than about 125 digits each. At the same time the digit length of the primes should not be more than a couple of thousand because of number crunching complications which will rise in message encoding and decoding procedures. Thus one is very interested in quickly finding prime numbers lying in the range-

$$10^{200} < P < 10^{2000}$$

How can this be accompliched? One of the oldest techniques is to generate the numbers from the Mersenne formula P=2^x-1 for certain prime integers x. These numbers P are referred to as Mersenne Primes and occur only for a limited number of xs in a specified integer range for P. There are just six Mersenne primes which fall into the above stated range of interest. These are-

Exponent x	Digits in P=2^x-1
1279	386
2203	664
2281	687
3217	969
4253	1281
4423	1332

This data and other interesting facts about Mersenne Primes can be found at-

http://en.wikipedia.org/wiki/Mersenne_prime

One of the latest found primes of the Mersenne type is 2^43,112,609-1. The search for still larger Mersenne Primes continues but these efforts will add little to possible applications in cryptograpy. Since the six Mersenne Primes given in the above table are well known throughout the world, they provide little security for their full or partial use in public key generation.

As a result, one presently uses large prime numbers generated by random number generators and then tested for primality by techniques based on Fermat's Little Theorem. This works fine but can often require lengthy tests before a prime number is found. It also prevents storage and transmission of the resultant primes in the compact form of a simple formula.

We want here to discuss another approach to generating large primes based on an extention of the simple Mersenne Formula given above. The idea is to use an expansion of the form-

$$P = A + \sum_{n=1}^{k} c_n (b_n)^{x_n}$$

Here one chooses the values of the coefficients c_n, the base b_n, and the exponent x_n beforehand to make P fall into the desired digit length range. Once this has been accomplished one next varies the value of A until P is found to be prime. This procedure will produce a large group of primes in any desired digit range. It also allows one to store and transmit large primes P as the simple expression-

$$P = P[A,(c_1,c_2,c_3,..),(b_1,b_2,b_3,..),(x_1,x_2,x_3,..)]$$

For example, one can write by this method the primes P=13110 and P=531457 as P[29,(1),(2),(17)] and P[16,(1),(3),(12)], respectively. Here is a generated 90 digit prime-

P[80,(3,-4),(5,9),(127,67)=80+3(5^127)-4(9^67)=

176324152623343126195310446203158622987091305360947864347408326824097585841856401800996179

and a 336 digit prime-

P[-101,(1,-15),(3,13),(703,219)=

260760657795977467182935934851119067809022551929747636956330
214942399328095782521490826575506391588704756116917033902990 6
381836729433385412639791828112748246323177830363761618814049 9
683495409944582356259268313536541876264536242887249404593648 1
371145779347040467840688157603553979097683999979485219886961 3
255777310173278398698620385797 3

It took me just just 10 minutes to generate this last prime by carrying out the computer operation-

V:=3^703-15*13^219;
for n from –150 to +150 do {n,isprime(V+n)}od;

It picked up a true response for n=-101.

To establish the size of the prime number one first evaluates the sum P-A. Lets say I want a prime number which is 200 digits long. Then I first make a random try –

P-A=3*6^234+5*9^129

This evaluates to a 188 digit long number. Hence I raise the exponent 234 to 256 and one now has a 200 digit number. Next I use the MAPLE program-

W:=3*6^256+5*9^129
For n from -m to +m do {n,isprime(W+n)}od

This time it took a me about 15 minutes evaluating things in 200 unit chunks until the computer spit out n=2896 as true. Hence we find, among numerous other possible 200 digit long primes, the prime-

P[2896,(3,5),(6,9),(256,129)]=

48288237367186684536185291740731912194930740441008553259612381139792832987949909815299583440559623645889548948958730003394595164708254751837601636977269302922320269307492769462133629353407936103013 09

It should be pointed out from the basic Prime Number Theorem that the value of A can become quite large when P-A is large. One knows that the number of expected primes up to a number N is approximately N/ln(N) and that up to a number M it is M/ln(M). Hence a simple calculation suggests that the distance between neighboring primes will be about -

$$\Delta s = \frac{[M-N]}{\left[\frac{M}{\ln(M)} - \frac{N}{\ln(N)}\right]}$$

If we now take M=1.1N and N=10^m, then we find-

$$\Delta s \approx m\ln(10) \; for \quad m >> 1$$

One should expect the first value of A to be comparable in magnitude to Δs. Thus for the 175 digit long number-

$$P = A + 5^{237} + 11^{73} + 3\cdot 13^{156}$$

We find in the range -7000<A<7000 that P will be prime if A==-6312, -4890, -3806, -1302, 172, 2652, 2728, 4770, and 6634. Thus the spacing between neighboring As is about 13,000/9≈1440. The above Δs approximation gives a somewhat lower estimate of Δs=175 ln(10)=403. The Δs criterion can therefore be thought as only an estimate for the number of integers in the separation of A values lying between prime values of P.

The number of large primes which can be generated by the present method are very large (actually infinite) and should be able to play an important role in the quickl production of public keys for RSA cryptography. This is because an adversary would not be able to come up with the multiple combinations of A, c, b, and x which can be used to generate a given prime

P. It might even be safe to transmit a coded version of one of these larger P_S to a friendly receiver and he in turn could send a return coded version of his own generated P_R. This would place into the hands of both the sender and receiver the ability to generate a public key $N=P_RP_S$ which will not be breakable by a third party. Secure encoded messages could then be sent either way by the sender and receiver without anyone else being able to decipher things.

Here is a final example of a large prime number generated by the above method. First we pick at random the number-

P-A=(3*7^317)+(3*11^409)+(13^283)

Here we are dealing with a 427 digit number. A simple evaluation for different values of A near zero leads to the value A=-240 needed to make P prime. Other values found in the -3000<A<20,000 range are A=-2910, 1786, 4758,7632, 10558, 13782, 16626, and 19392. We were aided in finding these other values of A by noting that $\Delta s=427\ln(10)=983$. The actual distance between neighboring As is about 2800. Using A=-240, we have the prime-

P[-240,(3,3,1),(7,11,13),(317,409,283)]=

25511117581317856181195580850588293152398235571560367343655961546638739124033630305658119899856751546626372320279086027937084264301013764660323095746847477211362371405062923453396609340907156310358056665789784113834431966657933184931258531905177956447776135896231377773976004118570590211271016814150751329010996223716403956915224916328609542576526945608622071468724961949344904050487501319916999768807753331821909931945113090 51

Taking the product of this last prime with the smaller 176 digit prime-

P[-576,(1,1,3),(5,11,13),(239,73,157)] =

232395422242099756268052355753015190466675634516757401506702794167464003771320537709251685815022038632196789867858759475867062317770437394994494659321226274139894247820935192 79

leads to the Public Key-

PubKey =
592866694217821785192693378178254166505160156612214219004010044966818093723875774888246798817378218437987092393269006416497817974198482782480974479048374790013821022133919589702819575414773720994144460270372427951185412194650000160710706167323223510631109782964102037282356395215964690541864390582505591461931338593341826342198954307919878451233532347219662591438289795713829200306350266045245263425339752719489581324388431012294815079715304014190007663225407973314948484565597389563675328808651296756820762665436217372639654236137304426496402763676535845649315172704647460041937279411649062617956942 29

If a code breaker were not aware of either one of the two Ps used in this last product, there would be no way at present he could successfully factor this 602 digit Public Key.

July 2011