THE GOLDBACH CONJECTURE

In 1742 in a letter to Leonard Euler the part-time mathematician Christian Goldbach stated that –

ANY EVEN NUMBER CAN BE EXPRESSED AS THE SUM OF TWO PRIMES

This is the famous Goldbach Conjecture which to this day remains one of the most important unproven theorems in Number Theory. It has been verified numerically to about 10^{14} but no proof for all even integers exists. A proof will be found when it is shown that for all positive integers N the equality-

$$P_n + P_m = 2N \ .$$

holds. Here P_n and P_m are two prime numbers. That this is obvious for the smaller prime numbers can be seen by looking at the following table-

P_n\ P_m	2	3	5	7	11	13	17	19	23
2	N=2								
3		3	4	5	7	8	10	11	13
5		4	5	6	8	9	11	12	14
7		5	6	7	9	10	12	13	15
11		7	8	9	11	12	14	15	17
13		8	9	10	12	13	15	16	18
17		10	11	12	14	15	17	18	20
19		11	12	13	15	16	18	19	21
23		13	14	15	17	18	20	21	23

We see there that generally there are several combinations of two primes and most prime combinations fall near the diagonal where $P_n=P_m$. For example we have –

$$2(12) = 5 + 19 = 7 + 17 = 11 + 13$$

In searching for two possible primes it will probably be of advantage to start with a value P_n=N-k where k is a positive integer. Thus for the above example one takes 12-k and notes that k=1 yields the first prime P_n=11. We next require that 2N-P_n also be a prime. In this case this is so since 24-11=13=P_m. If k=1 would not have produced two primes, one would go on and try k=2 and so on until both Pn and Pm are prime. This procedure can be automated and applied to any number. Consider N=234. The smallest value of k for which N-k=P_n is prime will be k=1. But N+k will not be prime. Hence the search continues finding on the fifth trial that N-5=229 is prime. Then looking at N+5 yields 239 which is also prime. Hence-

$$2(234) = 229 + 239$$

And so the Goldberg Conjecture holds for the even number 468. What is clear is that such a search procedure will become more cumbersome and produce values for P_n and P_m far renmoved from N. However since there are an infinite number of primes available it should always be possible to find two primes P_n=N-k and P_m+k . Let us try the search for two primes which sum to the large even number –

$$2N = 131072 = 2^{17} \ \ or \ \ N = 65536$$

Here is the search procedure-

(1)-Check N-k to see if it is prime. We find k=15 yields a prime P_n=65521
(2)-Next check N+k to see if it is prime. We find that it is also. Thus P_m=65551
(3)-This produces the solution-

$$131072 = 65521 + 65551$$

The above factoring procedure can be automated in our MAPLE program as-

```
for k from 0 to 100 do {isprime(N-k),isprime(N+k)}od
```

for a given N. Choosing N=2^{24}+6, we find the lowest value of k for which both N-k and N=k are prime is k=69. Thus we have that-

$$33554444 = 2(16777222) = 166777153 + 16777291$$

Extending the calculations to k=500 we find two other possibilities corresponding to k=285 and k=459. All that is required to satisfy the Goldbach Conjecture is one such pair of primes. Sometimes this type of search might require very large values for k.

Let us use the computer to find a prime number pair whose sum equals the seventeen digit number-

$$2N = 2(12345678987654321) = P_n + P_m$$

This time the PC spits out the answer k=80 so that one pair of primes is-

$$P_n = 12345678987654241 \ \ and \ \ P_m = 12345678987654401$$

Another set of primes is found by a random search at k=20002178, and yields-

$$P_n = 12345678967652143 \quad and \quad P_m = 12345679007656499$$

An interesting sidelight of possible use in breaking a public key R=$P_n \cdot P_m$ is that if 2N=P_n+P_m then one can eliminate P_m to get the quadratic equation-

$$P_n^2 - 2NP_n + R = 0$$

with the two roots-

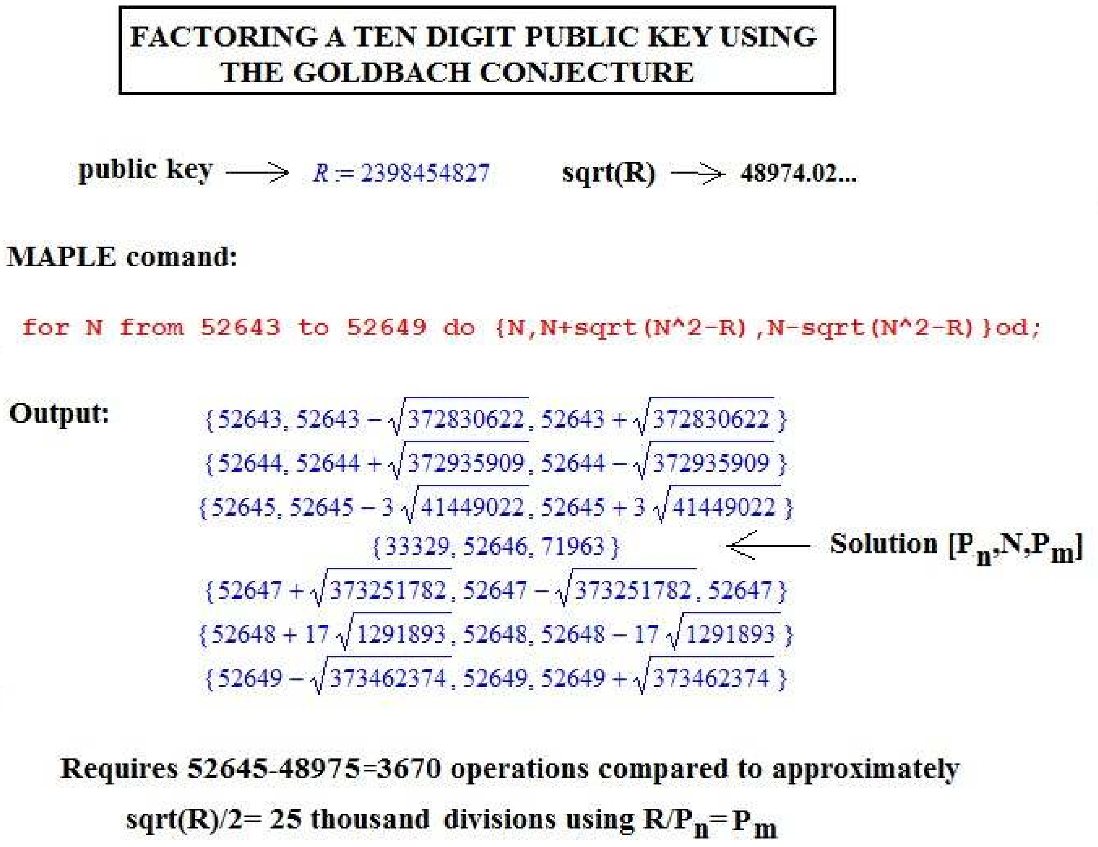
$$P_m = N + \sqrt{N^2 - R} \quad and \quad P_n = N - \sqrt{N^2 - R}$$

Thus to find the component primes of R one simply needs to find the value of N for which the radical equals an integer.

Suppose we are given the public key R=3007 and we work out the value of N for which the radical in the above solution equals an integer. Running our computer program, starting with the integer N nearest to sqrt(R)=54.836 this shows when N=64 that the radical will have the integer value of 33. Hence the public key is factored to yield-

$$R = 3007 = 31x97$$

Next , we show in the following figure how to factor a large ten digit public key-



FACTORING A TEN DIGIT PUBLIC KEY USING THE GOLDBACH CONJECTURE

public key ⟶ $R := 2398454827$ **sqrt(R)** ⟶ **48974.02...**

MAPLE comand:

```
for N from 52643 to 52649 do {N,N+sqrt(N^2-R),N-sqrt(N^2-R)}od;
```

Output:

$$\{52643, 52643-\sqrt{372830622}, 52643+\sqrt{372830622}\}$$
$$\{52644, 52644+\sqrt{372935909}, 52644-\sqrt{372935909}\}$$
$$\{52645, 52645-3\sqrt{41449022}, 52645+3\sqrt{41449022}\}$$
$$\{33329, 52646, 71963\} \longleftarrow \textbf{Solution } [P_n,N,P_m]$$
$$\{52647+\sqrt{373251782}, 52647-\sqrt{373251782}, 52647\}$$
$$\{52648+17\sqrt{1291893}, 52648, 52648-17\sqrt{1291893}\}$$
$$\{52649-\sqrt{373462374}, 52649, 52649+\sqrt{373462374}\}$$

Requires 52645-48975=3670 operations compared to approximately sqrt(R)/2= 25 thousand divisions using $R/P_n=P_m$

In this example it took some 3670 trials starting with N=48975 to find the correct solution. This seems rather large, but really is small compared to the twenty five thousand divisions required by brute force division of $R/P_n=P_m$ to accomplish the same result. Since breaking an even number into two primes is generally easier than breaking a public key into its two prime components, the present approach using the Goldbach Conjecture might prove useful in quickly factoring large public keys.

That the Goldbach Conjecture is valid for all N is highly likely since the number of primes is infinite and those lying between 1 and N is approximately N/ln(N) according to the Prime Number Theorem. A proof for all N still awaits but this should not hinder its application to other mathematical problems.

Goldbach(1690-1764) was an interesting character. He was born the son of a German protestant minister in Koenigsberg, Prussia, travelled widely throughout Europe befriending many of the leading mathematicians of his day including N.Bernoulli, Euler, and Leibnitz, was a member of the St.Petersburg Academy of Sciences, and later a tutor to czar Peter II, plus served in the Russian Ministry of Foreign Affairs. He spoke and communicated fluently in Latin, German, French, and Russian with some understanding of English and Italian.

January 2012