On Finding All Solutions to the Goldbach Problem for *2N*

Matilda Walter

Abstract

We present a simple sieve algorithm for finding all existing solutions to the binary Goldbach problem for a given even number $2N > 4$.

As is well known, binary Goldbach Conjecture is a statement to the effect that all even numbers greater than *2*, can be written as a sum of two primes and those greater than *4*, as a sum of two odd primes. What we refer to as the 'Goldbach problem', is a question that pertains to finding any, or all, existing solutions for any given even number. What follows, is a complete solution to this problem.

Given $2N > 4$, all existing solutions to the above problem, are found by sieving through the set of all primes[1] $\leq N$, with the residue classes of a system of congruences satisfied by $2N$, i.e., the system $2N \bmod 2$, $2N \bmod 3, ...2N \bmod p_k$, where the moduli are all primes p_i such that $p_i \leq p_k < (2N)^{1/2} < p_{k+1}$. For each prime p that 'survives' the sieve, the number $(2N - p)$ will also be prime and the method finds all existing solutions.

The effectiveness of the procedure, depends on an observation that given a congruence such as

$$A + B \equiv C \bmod p,$$

we have that A will be incongruent to $C \bmod p$, unless B is congruent to $0 \bmod p$.

We now prove the claim that the proposed sieve picks out exactly, all of the existing solutions, from the set of all primes $\leq N$. .

Proof : Given $2N$, let p be any prime $\leq N$ and consider the following identity

$$p + (2N - p) = 2N$$

The identity leads to a valid congruence, taken, in turn, modulo each of the primes $p_i < (2N)^{1/2}$

$$p + (2N - p) \equiv 2N \bmod p_i$$

From the congruence, we deduce that p will be incongruent to $2N \bmod p_i$, unless

$$2N - p \equiv 0 \bmod p_i$$

for some $p_i < (2N)^{1/2}$. Therefore, if $(2N - p)$ is prime[2], it is a prime greater than any of the moduli and none of its residues, at these moduli, will equal zero. Consequently, p will be incongruent to $2N$, modulo each of the primes $< (2N)^{1/2}$ and it will pass the sieve.

[1] If $p < q$ are both prime, $p + q = 2N$ and p is one of the moduli, then $q \equiv 2N \bmod p$. In general, only the primes $\leq N$ can, but may not, survive the sieve. .

[2] We don't need to know whether $2N - p$ is, or isn't prime (!). What is shown, is that p will, or will not survive the sieve, depending on which is the case with $2N - p$, i.e., behavior of p with respect to the sieve faithfully reflects the primality, or lack thereof, on the part of $2N - p$.

If, on the other hand, $(2N - p)$ is composite, it has a prime divisor among the moduli. The residue of $(2N - p)$ modulo the divisor will be zero, hence, modulo the same divisor, p will be congruent to $2N$ and will be sieved out.

Since at least one prime from each prime pair that has $2N$ as its sum, is $\leq N$ and the sieve applies to all primes $\leq N$, it follows that the primes p, which survive, each paired with the respective $(2N - p)$, make up all of the solutions to the problem for $2N$. *QED*

As an example[3], consider $2N = 200$. Square root of *200* is just over *14*, hence, the moduli are primes less than *14*, namely, *2, 3, 5, 7, 11* and *13*. Primes $\leq N = 100$ that the sieve will be applied to, are *2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89* and *97*. The number $2N$ satisfies the following congruences with respect to the given moduli:

$$\begin{aligned} 200 &\equiv 0 \bmod 2 \\ 200 &\equiv 2 \bmod 3 \\ 200 &\equiv 0 \bmod 5 \\ 200 &\equiv 4 \bmod 7 \\ 200 &\equiv 2 \bmod 11 \\ 200 &\equiv 5 \bmod 13 \end{aligned}$$

The first congruence sieves out *2*. The second sieves out *5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83* and *89* (*2* has been sieved out already). The third sieves out none since *5* has already been sieved out. The fourth sieves out *67* (*11* and *53*, also congruent to *4 mod 7* have already been sieved out). Fifth sieves out *13* and *79* and the sixth congruence sieves out *31* (*83*, also congruent to *5 mod 13* has already been sieved out).

This leaves *3, 7, 19, 37, 43, 61, 73* and *97* as the survivors. To each of the survivors, corresponds a prime $(2N - p)$ and they are, respectively, *197, 193, 181, 163, 157, 139, 127* and *103*. For each of the primes that has been sieved out, $(2N - p)$ is composite, as it is divisible by the modulus, at which the residue of $2N$, has sieved out p.

Modern sieves, are primarily concerned with enumeration of solutions to some problem at hand. Here, the aim is that of the original, Eratosthenian sieve, the purpose of which is set partition.

The foregoing is not a solution to the Goldbach Conjecture, as it does not prove, or otherwise imply, existence of solutions for any even number > *2*. The proposed sieve, finds all *existing* solutions for a given even number and it has nothing to say about what its *own* output might be, i.e., whether, or not, any of the primes to which it applies, survive.

References

[1] H. Halberstam and H.-E. Richert - Sieve Methods, Academic Press, 1974

[2] C. Hooley - Applications of Sieve Methods to the Theory of Numbers, Cambridge Tracts in Mathematics N° 70, Cambridge University Press, 1976

[3] H. Iwaniec and J. Friedlander - Opera de Cribro, AMS Colloquium Publications Vol. 57, 2010

[3] The example is rather small, but a larger one would just be more of the same.