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 of 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 $2N \bmod 2$, $2N \bmod 3, \ldots 2N \bmod p_k$, 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 process, the number $(2N - p)$ will also be prime and all existing solutions are found in this manner. 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 $0 \bmod p$.

The claim that the proposed sieve correctly picks out all of the existing solutions among the primes $\leq N$ will now be demonstrated.

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

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

From the identity we get 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* modulo each of the 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, hence, none of its residues at these moduli will be zero. Consequently, p will be incongruent to *2N* modulo each of the primes $< (2N)^{1/2}$ and, as a result, it will survive 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 do not need to know whether $2N - p$ is, or is not 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, p modulo the same divisor, 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 that survive, each coupled to 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:

$$200 \equiv 0 \bmod 2$$
$$200 \equiv 2 \bmod 3$$
$$200 \equiv 0 \bmod 5$$
$$200 \equiv 4 \bmod 7$$
$$200 \equiv 2 \bmod 11$$
$$200 \equiv 5 \bmod 13$$

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 $4 \bmod 7$ have already been sieved out). Fifth sieves out 13 and 79 and the sixth congruence sieves out 31 (83, also congruent to $5 \bmod 13$ has already been sieved out).

This leaves $3, 7, 19, 37, 43, 61, 73$ and 97 as the survivors, to each of which corresponds a prime $2N - p$. These are, respectively, $197, 193, 181, 163, 157, 139, 127$ and 103. For each of the primes that have been sieved out, $2N - p$ is composite, as it is divisible by the modulus, at which the residue of $2N$ 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. Should a counter-example to the Conjecture exist, the sieve will show that there are no solutions by sieving out all of the primes $\leq N$.

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^{o} 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.