SAOUTER'S PRIMALITY CRITERION IN LEAN, A LADDER CONSTANT, AND A 25 RUNG ROUTE TO ODD GOLDBACH UP TO 10^{20}

STEVE HUBBARD

Abstract. This note gives Lean proofs, with no hypothesis, of the primality criterion of Saouter's paper, Lemma 1 for every even F, Theorems 1 and 2, and it records the reading of the constant on page 865 under which the formula agrees with the rest of the paper; separately, given the published even Goldbach computation to $4 \cdot 10^{18}$ as an explicit hypothesis, a ladder of 25 Proth primes reaches 10^{20} in the Lean kernel. The binary Goldbach conjecture remains open and this note makes no progress on it. The ternary Goldbach theorem for all odd numbers is Helfgott's (`arXiv:1312.7748`), and it is not formalized here and not used.

hexagon:2611.00159v1

1. Introduction and Main Statements

We formalize in Lean 4, with no hypothesis, Saouter's Lemma 1 for every even F and Theorems 1 and 2, record the reading of the constant on page 865 matching his ladder formula, and deduce ternary Goldbach up to 10^{20} from the published $4 \cdot 10^{18}$ even Goldbach bound via a ladder of 25 Proth primes.

Theorem M (Main statements)**.** (a) *Lemma 1 of Saouter holds for every even F, and Saouter's Theorems 1 and 2 hold, in Lean with no hypothesis;* (b) *assuming every even integer from 4 to $4 \cdot 10^{18}$ is a sum of two primes, every odd integer from 7 to 10^{20} is a sum of three primes, in Lean. See Theorems B, C and E for detail.*

The binary Goldbach conjecture remains open, and this note makes no progress on it. The ternary Goldbach theorem for all odd numbers is Helfgott's [2], `arXiv:1312.7748`, and it is not formalized here and not used.

To place the present formalization in the context of prior work, the primary references are Saouter's own verification to 10^{20} [6] using the even Goldbach input $4 \cdot 10^{11}$ from Sinisalo [7] and a prime ladder of about $250 \cdot 10^6$ rungs, together with the subsequent work of Helfgott and Platt [3], who verified the ternary Goldbach conjecture up to $8.875 \cdot 10^{30}$, far past this range, by the same ladder idea with Proth primes. The range 10^{20} is therefore not a new result. What the entry supplies is a short kernel-checked derivation.

We state the exact scope and limits of this verification at the outset:

- Saouter's ladder of about $250 \cdot 10^6$ rungs is not reverified; only the 100 values of Table 1 of [6] and the starting and ending primes (138412033 and 100000000209366024193) are checked in the Lean kernel.
- The 25-rung route is a different ladder built on a larger even Goldbach input ($4 \cdot 10^{18}$, from Oliveira e Silva, Herzog, and Pardi [4]) and does not check Saouter's computation.
- In Saouter [6], the formula on page 865 reads $N = 5 \cdot 2^{23} \cdot k + 1258213$ as printed, and is read as $N(k) = 5 \cdot 2^{23} \cdot k + 12582913$ with one digit 9 restored. The paper's method, table, starting and ending primes, and result all stand.

This note is for readers of Saouter's paper and of later ladder computations, and for those who want the primality criterion in a form that a proof assistant accepts.

2. Saouter's Method and Primality Criteria

In [6] (pages 863 to 866), Saouter verifies the odd Goldbach conjecture up to 10^{20}. The method on page 863 reduces the ternary problem on bounded intervals to the binary problem via a chain of primes: if N is odd, p is prime, and $N - p$ is a sum of two primes, then $N = p + (N - p)$ is a sum of three primes. Given the even Goldbach verification up to $4 \cdot 10^{11}$ by Sinisalo [7], one exhibits a strictly increasing sequence of primes

$$p_0 < p_1 < \cdots < p_P$$

such that $p_0 < 4 \cdot 10^{11}$, each consecutive step satisfies $p_{i+1} - p_i < 4 \cdot 10^{11}$, and $p_P > 10^{20}$. With step size bounded by $4 \cdot 10^{11}$, at least $250 \cdot 10^6$ primes are needed to reach 10^{20}.

To test primes rapidly at this scale without factoring $N-1$ in full, Saouter uses a special case of the primality criteria of Brillhart, Lehmer, and Selfridge [1]. We record the statements from page 864 of [6].

Lemma 1 (Saouter [6], page 864; from Theorem 5 of Brillhart, Lehmer, and Selfridge [1]). *Let $N = RF + 1$ be odd with F even, the factorization of F known, and $\gcd(R, F) = 1$. Suppose an integer a satisfies*

$$a^{N-1} \equiv 1 \pmod{N} \quad \text{and} \quad \gcd\bigl(a^{(N-1)/p} - 1,\, N\bigr) = 1$$

for every prime p dividing F. Write $R = 2Fs + r$ with $0 \le r < 2F$. If $N < 2F^3$, then N is prime if and only if $s = 0$ or $r^2 - 8s$ is not a perfect square.

Specializing F to a power of 2 eliminates all odd prime factors of F and reduces the Lucas-type hypotheses to a single modular exponentiation:

Theorem 1 (Saouter [6], page 864). *Let $N = 2^{22}R + 1$ with $N < 10^{20}$ and R odd, and suppose there is some integer a with*

$$a^{(N-1)/2} \equiv -1 \pmod{N}.$$

Write $R = 2 \cdot 2^{22}s + r$ with $0 \le r < 2 \cdot 2^{22}$. Then N is prime if and only if $s = 0$ or $r^2 - 8s$ is not a perfect square. The size condition of Lemma 1 holds since $2 \cdot (2^{22})^3 > 10^{20}$.

To avoid searching for a base a at each candidate, Saouter fixes $a = 5$ by restricting the residue class of N modulo 10:

Lemma 2 (Saouter [6], page 864). *A prime N of the form $10k + 3$ satisfies*

$$5^{(N-1)/2} \equiv -1 \pmod{N},$$

by Euler's criterion and quadratic reciprocity.

Theorem 2 (Saouter [6], page 864). *Let $N = 2^{22}R + 1$ with $N < 10^{20}$, $N \equiv 3 \pmod{10}$ and R odd, and suppose $5^{(N-1)/2} \equiv -1 \pmod{N}$. Write $R = 2 \cdot 2^{22}s + r$ with $0 \le r < 2 \cdot 2^{22}$. Then N is prime if and only if $s = 0$ or $r^2 - 8s$ is not a perfect square.*

The ladder generation algorithm on page 864 of [6] proceeds as follows:

1. Start at $p_0 = 138412033 = 33 \cdot 2^{22} + 1$, which is the least prime satisfying both $N = 2^{22}R + 1$ (R odd) and $N \equiv 3 \pmod{10}$.
2. From the current prime rung, step up by $95360 \cdot 2^{22}$, which is the largest multiple of $10 \cdot 2^{22}$ below $4 \cdot 10^{11}$.
3. Test the candidate for primality using Theorem 2; on a composite candidate, step down by $10 \cdot 2^{22}$ repeatedly until a prime is reached.

In Section 4, page 865 of [6], the ending prime of the ladder is reported as

$$100000000209366024193,$$

and Table 1 gives the initial 100 values of the parameter k for the ladder primes, where the formula on page 865 reads $N = 5 \cdot 2^{23} \cdot k + 1258213$.

3. Proposition A: The Formula Constant on Page 865

We begin by recording the arithmetic relationship between the formula as printed on page 865 and the candidate family defined on page 864.

Proposition A. *Let*

$$N(k) = 5 \cdot 2^{23} \cdot k + 12582913 \quad \text{and} \quad N'(k) = 5 \cdot 2^{23} \cdot k + 1258213,$$

where $N'(k)$ is the formula as printed on page 865 of [6]. *Then:*

(1) *Since $12582913 = 3 \cdot 2^{22} + 1$ and $5 \cdot 2^{23} = 10 \cdot 2^{22}$, we have*

$$N(k) = 2^{22}(10k + 3) + 1,$$

so $N(k) \equiv 3 \pmod{10}$ and the cofactor $R = 10k + 3$ is odd for every natural number k.

(2) *At* $k = 3$ *and* $k = 2384185796007$*, the formula* $N(k)$ *gives*

$$N(3) = 138412033 = 33 \cdot 2^{22} + 1,$$
$$N(2384185796007) = 10000000209366024193 = 2^{22} \cdot 23841857960073 + 1,$$

which are the starting and ending primes of [6]*, with* 23841857960073 *odd.*

(3) *For the printed form* $N'(k)$*, evaluation at* $k = 3$ *gives the composite number*

$$N'(3) = 127087333 = 19 \cdot 6688807,$$

$N'(k) \bmod 2^{22}$ *is never* 1 *for any natural number* k*, and* $N(k) = N'(k) + 11324700$*.*

(4) *Every one of the 100 printed values of* k *in Table 1 of* [6] *gives a prime* $N(k)$*, with largest consecutive step* $399968829440 = 95360 \cdot 2^{22}$ *by script.*

Proof. Since $2^{22} = 4194304$, direct multiplication yields

$$3 \cdot 2^{22} + 1 = 3 \cdot 4194304 + 1 = 12582912 + 1 = 12582913.$$

Consequently, for any natural number k,

$$N(k) = 5 \cdot 2^{23} \cdot k + 12582913 = 2^{22}(10k) + 2^{22} \cdot 3 + 1 = 2^{22}(10k + 3) + 1.$$

Because $2^{22} = (2^4)^5 \cdot 2^2 \equiv 6 \cdot 4 = 24 \equiv 4 \pmod{10}$, we have

$$N(k) \equiv 4(10k + 3) + 1 \equiv 12 + 1 \equiv 3 \pmod{10},$$

and $10k + 3 = 2(5k + 1) + 1$ is odd.

Substituting $k = 3$ into $N(k)$ gives $10(3) + 3 = 33$ and

$$N(3) = 33 \cdot 2^{22} + 1 = 138412033.$$

Substituting $k = 2384185796007$ gives $10k + 3 = 23841857960073$, which is odd, and

$$N(2384185796007) = 2^{22} \cdot 23841857960073 + 1 = 10000000209366024193.$$

In contrast, for $N'(k) = 5 \cdot 2^{23} \cdot k + 1258213$, the difference is constant:

$$N(k) - N'(k) = 12582913 - 1258213 = 11324700.$$

Since $5 \cdot 2^{23} \cdot k = 10k \cdot 2^{22}$ is a multiple of 2^{22}, we have $N'(k) \equiv 1258213 \pmod{2^{22}}$, which is never congruent to 1 $\pmod{2^{22}}$ for any k. At $k = 3$, $N'(3) = 138412033 - 11324700 = 127087333 = 19 \cdot 6688807$. Finally, each of the 100 values $N(k)$ for k in Table 1 is checked prime in the Lean kernel via Theorem 2 (`Table1Thm2.table1_prime_thm2`), each consecutive step is below $4 \cdot 10^{11}$ (`Table1.table1_gaps`), and by script the largest consecutive step is $399968829440 = 95360 \cdot 2^{22}$. □

Thus the formula on page 865 is read with constant $12582913 = 3 \cdot 2^{22} + 1$, with one digit 9 restored; note that $12582913 = 7 \cdot 1797559$ is itself composite, as it is only the constant term $N(0)$ corresponding to $k = 0$ rather than a rung of the ladder (which starts at $k = 3$). By script, 9 of the 100 values $N'(k)$ are prime, and a rerun of the paper's algorithm starting from 138412033 reproduces Table 1 of [6] exactly. No other change to [6] is needed.

4. Formalization of the Primality Criteria in Lean

We now turn to the Lean formalization of Lemma 1, Theorems 1 and 2, Lemma 2, and the Table 1 checks. Note also that Lemma 8 of Ramaré and Saouter [5] restates Lemma 1 with the factor argument.

Theorem B (`BLS.lemma1`)**.** *Lemma 1 of Section 2 holds for every even* F*.*

Proof. Let $N = RF + 1$ satisfy the hypotheses of Lemma 1. By Pocklington's order argument applied to each prime power $p^e \parallel F$, the conditions $a^{N-1} \equiv 1 \pmod{N}$ and $\gcd(a^{(N-1)/p} - 1, N) = 1$ imply that the multiplicative order of a modulo any prime factor q of N is divisible by F. By Fermat's little theorem, $F \mid (q - 1)$, which puts every prime factor q of N in the residue class 1 $\pmod{F}$. Since products of integers congruent to 1 $\pmod{F}$ remain congruent to 1 $\pmod{F}$, every positive divisor of N is congruent to 1 $\pmod{F}$. Moreover, since F is even and $\gcd(R, F) = 1$, R must be odd; because $R = 2Fs + r$ and $2Fs$ is even, the remainder r is also odd.

Suppose first that N is composite. Then N factors as a product of two integers above 1,

$$N = (uF + 1)(vF + 1)$$

with integers $u, v \geq 1$. Expanding the product gives

$$RF + 1 = uvF^2 + (u + v)F + 1,$$

and dividing by F yields

$$R = uvF + u + v.$$

From the strict inequality $uvF^2 < (uF + 1)(vF + 1) = N < 2F^3$, dividing by F^2 gives $uv < 2F$. Since $u, v \geq 1$, we have $(u - 1)(v - 1) \geq 0$, so

$$u + v \leq uv + 1 \leq 2F.$$

Because R is odd and F is even, the term uvF is even, whence $u + v = R - uvF$ is odd. Since $2F$ is even and $u + v$ is odd, the weak inequality $u + v \leq 2F$ forces the strict inequality

$$u + v < 2F.$$

Furthermore, since $u + v$ is odd, one of u, v is even and the other is odd, so their product uv is even. We may therefore write

$$R = 2F\left(\frac{uv}{2}\right) + (u + v) \quad \text{with} \quad 0 < u + v < 2F.$$

By uniqueness of the quotient s and remainder r in Euclidean division of R by $2F$, we obtain

$$s = \frac{uv}{2} \geq 1 \quad \text{and} \quad r = u + v.$$

Consequently,

$$r^2 - 8s = (u + v)^2 - 4uv = (u - v)^2,$$

which is a perfect square.

Conversely, suppose that $s \geq 1$ and $r^2 - 8s = t^2$ for an integer $t \geq 0$. Since r is odd, r^2 is odd, so $t^2 = r^2 - 8s$ is odd, which implies that t is odd. Therefore $r + t$ and $r - t$ are both even, and

$$u = \frac{r + t}{2}, \qquad v = \frac{r - t}{2}$$

are integers satisfying

$$u + v = r \qquad \text{and} \qquad uv = \frac{r^2 - t^2}{4} = \frac{8s}{4} = 2s > 0.$$

Since $uv = 2s > 0$ and $u + v = r > 0$, both u and v are strictly positive integers ($u, v \geq 1$). Multiplying the factors $uF + 1 > 1$ and $vF + 1 > 1$ gives

$$(uF + 1)(vF + 1) = uvF^2 + (u + v)F + 1 = 2sF^2 + rF + 1 = (2Fs + r)F + 1 = RF + 1 = N,$$

which shows that N is composite. Thus N is prime if and only if $s = 0$ or $r^2 - 8s$ is not a perfect square. □

Theorem C. *Saouter's Theorem 1 (for both a natural base and an integer base), Lemma 2, and Theorem 2 (in both directions) hold in Lean with no hypothesis; Lemma 2 shows that the hypothesis on* 5 *holds for every prime* $N \equiv 3 \pmod{10}$*, so the test rejects no prime of this class, and the form* `Thm2.theorem2_if` *keeps the hypothesis on* 5 *and replaces* $N < 10^{20}$ *by* $N < 2 \cdot (2^{22})^3$*, for the direction from the square test to primality. The Lean names are* `Thm1.theorem1`*,* `Thm1.theorem1_int`*,* `Paper.lemma2`*,* `Thm2.theorem2`*, and* `Thm2.theorem2_if`*.*

Proof. Let $F = 2^{22}$ and $N = 2^{22}R + 1$ with R odd. Then $\gcd(R, 2^{22}) = 1$, and the only prime dividing F is $p = 2$. From the congruence $a^{(N-1)/2} \equiv -1 \pmod{N}$, squaring both sides yields the Fermat condition $a^{N-1} \equiv 1 \pmod{N}$. Moreover, for the unique prime divisor $p = 2$ of F, we have $a^{(N-1)/2} - 1 \equiv -2 \pmod{N}$, so

$$\gcd\big(a^{(N-1)/2} - 1,\, N\big) = \gcd(-2, N) = 1$$

because $N = 2^{22}R + 1$ is odd. The size threshold of Lemma 1 is

$$2F^3 = 2 \cdot (2^{22})^3 = 2^{67} = 147573952589676412928 > 10^{20},$$

so Lemma 1 applies directly to establish Theorem 1.

For Lemma 2 (`Paper.lemma2`), if $N = 10k + 3$ is prime, then N is odd and $N \equiv 3 \pmod 5$. Since $5 \equiv 1 \pmod 4$, quadratic reciprocity and Euler's criterion give

$$5^{(N-1)/2} \equiv \left(\frac{5}{N}\right) = \left(\frac{N}{5}\right) = \left(\frac{3}{5}\right) = -1 \pmod N.$$

Theorem 2 is Theorem 1 at $a = 5$. Lemma 2 shows that the hypothesis on 5 holds for every prime $N \equiv 3 \pmod{10}$, so the test rejects no prime of this class. The form `Thm2.theorem2_if` keeps the hypothesis on 5 and replaces $N < 10^{20}$ by $N < 2 \cdot (2^{22})^3$, for the direction from the square test to primality. □

Deviation and Range Remark on the Final Prime. We record one point regarding the range of Theorem 2 as stated on page 864 of [6]. The ending prime of Saouter's ladder is

$$N = 100000000209366024193 > 10^{20},$$

so it lies outside the range $N < 10^{20}$ stated in Theorem 2, as it must in order for the ladder to cross 10^{20}. However, it lies well below the Lemma 1 bound

$$2 \cdot (2^{22})^3 = 2^{67} = 147573952589676412928,$$

so the primality criterion still applies. In Lean, `Thm2.last_prime` uses the wider form `Thm2.theorem2_if` with hypothesis $N < 2 \cdot (2^{22})^3$. Specifically, for $N = 100000000209366024193$, the parameters are

$$R = 23841857960073,$$
$$s = 2842170,$$
$$r = 7960713,$$
$$r^2 - 8s = 63372928731009,$$

and $r^2 - 8s = 63372928731009$ is not a square since it lies strictly between 7960711^2 and 7960712^2.

Theorem D. *All 100 rungs $N(k)$ from Table 1 of* [6]*, together with the starting prime* 138412033 *and the ending prime* 100000000209366024193*, are checked prime in the Lean kernel by the criterion of Theorem 2 using one modular power each. Among the 100 rungs of Table 1, 11 have $s = 1$ and the rest have $s = 0$, by script. The 100 Table 1 rungs begin at* 138412033*, are strictly rising, and have every consecutive step strictly below $4 \cdot 10^{11}$, with largest step* $399968829440 = 95360 \cdot 2^{22}$ *by script. The Lean names are `Table1Thm2.table1_prime_thm2`, `Thm2.first_prime`, `Thm2.last_prime`, `Table1.table1_head`, and `Table1.table1_gaps`.*

Proof. Each rung is checked in the Lean kernel via `decide +kernel` applied to Theorem 2 (`Table1Thm2.table1_prime_thm2`, `Thm2.first_prime`, and `Thm2.last_prime`), and the ordering and step bounds on the 100 rungs are checked directly in `Table1.table1_head` and `Table1.table1_gaps`. □

5. The 25-Rung Proth Ladder to 10^{20}

Separately from the verification of Saouter's criteria and Table 1, we construct a 25-rung ladder of Proth primes that derives the ternary Goldbach range up to 10^{20} from the published even Goldbach range $4 \cdot 10^{18}$.

Theorem E. *Assuming every even integer from 4 to $4 \cdot 10^{18}$ is a sum of two primes, every odd integer from 7 to 10^{20} is a sum of three primes. The Lean statement `ProthLadder.ternaryGoldbachUpTo_1e20_of_even` proves `EvenGoldbachUpTo (4 * 10 ^ 18)` → `TernaryGoldbachUpTo (10 ^ 20)`, where the hypothesis `EvenGoldbachUpTo (4 * 10 ^ 18)` is passed as an explicit argument, never declared as an axiom, and it is not proved here.*

Proof. We check the ladder primes by Proth's theorem (`Proth.proth`): if $0 < k < 2^{m+1}$, $N = k \cdot 2^{m+1} + 1$, and there is a natural number a such that

$$a^{k \cdot 2^m} \equiv -1 \pmod N,$$

then N is prime.

We take $m + 1 = 34$, so each of the 25 rungs has the form

$$N = k \cdot 2^{34} + 1$$

with $0 < k < 2^{34}$ and witness base a as listed in Table 1. The starting rung in Table 1 is

$$3999998442578378753 = 232830553 \cdot 2^{34} + 1,$$

and the ending rung is

$$9999983948045221889 = 5820765157 \cdot 2^{34} + 1.$$

TABLE 1. The 25 Proth prime rungs $N = k \cdot 2^{34} + 1$ and witness bases a for Theorem E.

k	a	k	a
232830553	3	3259628295	13
465661177	3	3492458899	3
698491779	5	3725289523	3
931322415	7	3958120159	3
1164153045	7	4190950765	3
1396983685	3	4423781383	3
1629814317	11	4656612025	3
1862644839	5	4889442663	5
2095475355	7	5122273297	3
2328305925	7	5355103933	3
2561136565	3	5587934515	3
2793967113	5	5820765157	3
3026797689	5		

Let $B = 4 \cdot 10^{18}$. In Lean, the chain relation (`Ladder.Step2`, checked for our sequence in `ProthLadder.rungs_chain`) checks that, starting from 3 followed by the 25 rungs, each step strictly rises and has difference at most $B - 2$, with largest step

$$3999999971586736128.$$

The reach lemma (`ProthLadder.rungs_reach`) checks that the ending rung plus $B = 4 \cdot 10^{18}$ satisfies

$$9999983948045221889 + 4 \cdot 10^{18} = 10399983948045221889 \geq 10^{20}.$$

The single-interval covering step (`Ladder.ternary_step`) establishes that if p is an odd prime, n is odd, and

$$p + 4 \leq n \leq p + B,$$

then $n - p$ is even and satisfies $4 \leq n - p \leq B$; by `EvenGoldbachUpTo B`, $n - p$ is a sum of two primes, so $n = p + (n - p)$ is a sum of three primes. Since each consecutive step in the chain is at most $B - 2$, and since B is even and p is odd, $p + B$ is odd, and $p' + 4 \leq p + B + 2$, so the odd integers covered from p' continue directly after those covered from p. Induction along the chain (`Ladder.ternary_of_ladder2`), starting at $p = 3$ (which covers odd n from $3 + 4 = 7$ to $3 + B$), therefore covers every odd integer n from 7 to 10^{20}. □

Sanity Instance and Rung Count Comparison. To confirm that the definitions and ladder induction have no hidden vacuity, the formalization includes a sanity instance with no hypothesis (`ProthLadder.ternaryGoldbachUpTo_293_vacuity`): applying the exact same ladder lemma with $B = 100$ and prime rungs 97 and 193, where `ProthLadder.evenGoldbachUpTo_100` is proved directly in the kernel, yields `TernaryGoldbachUpTo 293` with nothing assumed.

The rung count comparison (with the second quotient in `Paper.rung_count`) is:

$$\frac{10^{20}}{4 \cdot 10^{18}} = 25, \qquad \text{against} \qquad \frac{10^{20}}{4 \cdot 10^{11}} = 250 \cdot 10^6 \quad \text{in Saouter [6].}$$

This saving comes entirely from the larger even Goldbach input $4 \cdot 10^{18}$, which is the published computation of Oliveira e Silva, Herzog, and Pardi [4], and not from any new idea. The ladder structure is Saouter's [6] and the use of Proth primes is that of Helfgott and Platt [3], Section 3.

6. Cited Input, Verification Status, and Data Availability

6.1. **Differences from the source.** We list the differences between the Lean formalization and [6]:

(a) the constant on page 865, read as in Proposition A;
(b) the last prime, as in the remark on the final prime;
(c) Lean states the base as a natural number and as an integer, the paper as an integer;

(d) the 25 rung ladder starts at 3 and uses steps at most $B-2$, the paper starts at p_0 and asks steps below $4 \cdot 10^{11}$;
(e) Lemma 2 is stated in `ZMod p`.

The Section 3 sentence "No other change" means no other change to the formula. In addition, in Lean s and r are the natural number quotient and remainder of R by $2F$; $(N-1)/2$ is natural division of $2^{22}R$ by 2, exact since $2^{22}R$ is even; `IsSquare` is taken over the integers, so a negative $r^2 - 8s$ is not a square, matching "not a perfect square"; and the case $F = 0$ of `BLS.lemma1` is empty since $N < 2F^3$ does not hold.

6.2. **Input Table.** There is one cited input in Theorem E, and none elsewhere in this note. Table 2 records its bibliographic details, printed wording, normalization, and Lean representation. It is a computation, cited as such and never stated as proved.

TABLE 2. External cited input used in Theorem E (and nowhere else).

Field	Specification
Source	T. Oliveira e Silva, S. Herzog, and S. Pardi [4], *Empirical verification of the even Goldbach conjecture and computation of prime gaps up to* $4 \cdot 10^{18}$, Math. Comp. 83, no. 288, 2014, 2033 to 2060.
Printed statement	Abstract, page 2033: the conjecture is "confirmed to be true for all even numbers not larger than $4 \cdot 10^{18}$".
Normalization	Inclusive at $4 \cdot 10^{18}$, for all even integers n with $n \geq 4$.
Lean form	`EvenGoldbachUpTo N`, defined as: for all n, `Even n`, $4 \leq n$, $n \leq N$, `IsGoldbachSum n`, instantiated at $N =$ `4 * 10 ^ 18`.
Role in Lean	Explicit hypothesis in `ProthLadder.ternaryGoldbachUpTo_1e20_of_even`; never an axiom.

6.3. **Verification Status Table.** Every claim in this note is classified into one of four categories: **Kernel** (checked by the Lean 4 kernel), **Script** (checked by external script and not used in any Lean proof), **Hand** (a statement checked by hand in this note and not in Lean), or **Cited** (external published computation). Table 3 gives the mapping.

The proofs printed in this note are written for the reader; the Lean proofs are the check.

6.4. **Data Availability and Build Reproduction.** All Lean names in this note are under the namespace `GoldbachLean.Saouter1998`. The Lean 4 formalization is publicly available under the Apache-2.0 license:

- **Repository:** `https://github.com/sthubbar/goldbach-lean`
- **Folder:** `entries/saouter1998`
- **Full commit hash:** `39d1ce6db8b634233ed29c2aa3e3dcf1218400dc`
- **Palomar Registry listing:** `PALOMAR-2026-11-02-000012` version 1, available at `https://palomar-registry.org/entry.html?id=PALOMAR-2026-11-02-000012&version=1` (note that Palomar is a listing and not peer review).
- **Toolchain:** Lean and Mathlib `v4.35.0-rc3`.
- **Build instruction:** Running `lake build` inside `entries/saouter1998` completes in 57 s in a cloud build with cached Mathlib.
- **Audit file and foundations:** All main statements are collected and compared in `ChallengeSaouter1998.lean`, which exports 19 theorems. The proofs depend only on the Lean axioms `propext`, `Classical.choice`, and `Quot.sound`. Every finite primality and arithmetic check uses `decide +kernel` and never `native_decide`; each rung verification costs one modular power on numbers below 2^{67}.

Steve Hubbard designed the research program and directed this work. AI tools, Claude, Codex, Gemini and Antigravity, were used to write the Lean code and draft the text. AI agents also did the checks of the Lean against the source, and no human expert has reviewed the mathematics. The author takes full responsibility for the content.

TABLE 3. Verification status of all claims and components (categories: Kernel, Script, Hand, Cited).

Claim or Component	Lean Module / Identifier or Reference	Status
Proposition A: identities for $N(k)$ and $N'(k)$, $N(3) = 138412033$, $N(2384185796007) = 100000000209366024193$, that $N'(3)$ is composite, $N'(k) \bmod 2^{22} \neq 1$, $N(k) - N'(k) = 11324700$	`Paper`, `Table1.printed_three_composite`	Kernel
Proposition A: leastness of $p_0 = 138412033$ (text, not used in proofs); count that 9 of 100 values $N'(k)$ are prime; rerun of Saouter's algorithm from 138412033 reproducing Table 1; largest Table 1 step $399968829440 = 95360 \cdot 2^{22}$; count that 11 of the 100 Table 1 rungs have $s = 1$	External check scripts	Script
Theorem B: Saouter's Lemma 1 for every even F	`BLS.lemma1`	Kernel
Theorem C: Saouter's Theorem 1 (natural and integer base), Lemma 2, and Theorem 2 (both directions and $N < 2 \cdot (2^{22})^3$ form)	`Thm1.theorem1`, `Thm1.theorem1_int`, `Paper.lemma2`, `Thm2.theorem2`, `Thm2.theorem2_if`	Kernel
Theorem D: primality of all 100 Table 1 rungs, starting prime 138412033, and ending prime 100000000209366024193; ordering and step bound below $4 \cdot 10^{11}$	`Table1Thm2.table1_prime_thm2`, `Thm2.first_prime`, `Thm2.last_prime`, `Table1.table1_head`, `Table1.table1_gaps`	Kernel
Theorem E: implication from `EvenGoldbachUpTo (4 * 10 ^ 18)` to `TernaryGoldbachUpTo (10 ^ 20)`, Proth criterion, 25 rungs, chain, reach, ladder step, induction, sanity check to 293, and $10^{20}/(4 \cdot 10^{11}) = 250 \cdot 10^6$	`ProthLadder.ternaryGoldbachUpTo_1e20_of_even`, `Proth.proth`, `Ladder.Step2`, `ProthLadder.rungs_chain`, `ProthLadder.rungs_reach`, `Ladder.ternary_step`, `Ladder.ternary_of_ladder2`, `ProthLadder.ternaryGoldbachUpTo_293_vacuity`, `ProthLadder.evenGoldbachUpTo_100`, `Paper.rung_count`	Kernel
$12582913 = 7 \cdot 1797559$, by multiplication; $N'(3) = 19 \cdot 6688807$; $10^{20}/(4 \cdot 10^{18}) = 25$	Checked by hand in this note	Hand
Even Goldbach verification up to $4 \cdot 10^{18}$ (hypothesis of Theorem E)	Oliveira e Silva, Herzog, and Pardi [4]	Cited
Saouter's full ladder of about $250 \cdot 10^6$ rungs (with Sinisalo's $4 \cdot 10^{11}$ input [7]); Helfgott and Platt's verification to $8.875 \cdot 10^{30}$ [3]; Helfgott's ternary Goldbach theorem [2]	[6], [7], [3], [2] (not reverified)	Cited

REFERENCES

[1] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), no. 130, 620–647.

[2] H. A. Helfgott, *The ternary Goldbach conjecture is true*, `arXiv:1312.7748`, 2013.

[3] H. A. Helfgott and D. J. Platt, *Numerical verification of the ternary Goldbach conjecture up to* $8.875 \cdot 10^{30}$, Exp. Math. **22** (2013), 406–409.

[4] T. Oliveira e Silva, S. Herzog, and S. Pardi, *Empirical verification of the even Goldbach conjecture and computation of prime gaps up to* $4 \cdot 10^{18}$, Math. Comp. **83** (2014), no. 288, 2033–2060.

[5] O. Ramaré and Y. Saouter, *Short effective intervals containing primes*, J. Number Theory **98** (2003), 10–33.

[6] Y. Saouter, *Checking the odd Goldbach conjecture up to* 10^{20}, Math. Comp. **67** (1998), no. 222, 863–866, `doi:10.1090/S0025-5718-98-00928-4`.

[7] M. K. Sinisalo, *Checking the Goldbach conjecture up to* $4 \cdot 10^{11}$, Math. Comp. **61** (1993), no. 204, 931–934.

INDEPENDENT RESEARCHER