THE THIRD AND FOURTH LEV–SONN PRIMES

KOREA SUPERINTELLIGENCE LABS

Abstract. Kalmynin calls a prime p a *Lev–Sonn prime* if $p = 2\alpha(\alpha-1)+1$ and $\binom{\alpha^2-1}{n-1+\alpha} \equiv (-1)^{n-1}\binom{\alpha^2-1}{\alpha} \pmod p$ for some n with $1 < n \le \alpha$, and asks whether there are infinitely many. His search over $\alpha \le 3000$ found two, $p = 13$ and $p = 41$. We exhibit the next two,

$$p = 25\,293\,378\,613 \quad (\alpha = 112\,458), \qquad p = 74\,857\,799\,381 \quad (\alpha = 193\,466),$$

and prove that they are the third and the fourth: for every α with $2 \le \alpha \le 300\,000$ the number $2\alpha(\alpha-1)+1$ is a Lev–Sonn prime if and only if $\alpha \in \{3, 5, 112\,458, 193\,466\}$. The congruence witnessing the first of the two new primes relates binomial coefficients with 616 862 and 991 481 decimal digits, and the one witnessing the second relates larger ones; the tool that makes them decidable is an exact telescoping identity whose correction factors are units modulo p, and which replaces the pair of binomial coefficients by two products of $n-1$ linear factors. A substitution in it removes α from one side entirely and turns the condition into $(2j+1)!! \equiv 2^j(\alpha+j)!/\alpha! \pmod p$ with $j = n-1$. We also correct the witness printed for $p = 41$: the pair $(\alpha, n) = (5, 5)$ recorded in the source is not a witness, $(5, 4)$ is, and it is the only one. Every theorem, proposition and lemma below is machine-checked in Lean 4.

1. Introduction

In [1], Kalmynin proves the Lev–Sonn conjecture on difference sets of quadratic residues [2] and Sárközy's conjecture on additive decompositions of the quadratic residues [4], by a version of Stepanov's method built on the polynomials of Hanson and Petridis [3]. The method compares the coefficients of a Hanson–Petridis polynomial with those of an explicit product, and each comparison produces a congruence between binomial coefficients modulo p; a contradiction is reached when no such congruence can hold. The closing section of [1] isolates the primes at which this mechanism does not immediately close, and poses the following problem, which we quote verbatim.

Problem 1.1 ([1, Problem 3 of v2])**.** Let us call p a Lev–Sonn prime, if $p = 2\alpha(\alpha-1)+1$ and for some $1 < n \le \alpha$ the congruence

$$\binom{\alpha^2-1}{n-1+\alpha} \equiv (-1)^{n-1}\binom{\alpha^2-1}{\alpha} \pmod p$$

holds. Are there infinitely many Lev–Sonn primes?

One line below it, [1] reports the numerical evidence, again verbatim:

> A quick search among the first 586 primes of the form $2\alpha(\alpha-1)+1$ (i.e. $\alpha \le 3000$) produced only two such primes $p = 13$ and $p = 41$, corresponding to $(\alpha, n) = (3, 3)$ and $(5, 5)$.

Both quotations are from the second version of [1] (28 May 2025), to which we pin the numbering: the first version (14 April 2025) carries the problem as its Question 3 and prints the congruence as $\binom{\alpha-1+d}{d-n} \equiv (-1)^{n-1}\binom{\alpha-1+d}{d-1}$, with $d = \alpha(\alpha-1)$ as in [1, §3]. Since $\alpha - 1 + d = \alpha^2 - 1$, the symmetry $\binom{N}{k} = \binom{N}{N-k}$ turns that into the congruence displayed above; the one substantive difference is the range, the first version asking only for $n \le \alpha$, at which $n = 1$ satisfies it identically. The sentence reporting the search is word for word the same in the two versions.

The name is coined in [1]; V. F. Lev and J. Sonn appear in it through the conjecture of [2], which is a different object from Problem 1.1. As far as we can determine, no subsequent work has taken the

search further: of the papers citing [1] that we could locate, only [6] mentions the name Lev–Sonn at all, and it does so for the conjecture, not for the primes.

The shape $p = 2\alpha(\alpha-1)+1 = (\alpha-1)^2+\alpha^2$ is the centred square, so the ambient sequence is the sequence of primes of the form $j^2+(j+1)^2$ [7, A027862]; the Lev–Sonn subsequence is not recorded there.

Results. Problem 1.1 asks a question about infinitude that we do not touch. What we do is carry the search of [1] two orders of magnitude further, and make the resulting list exact.

Two new Lev–Sonn primes (Section 7). The primes $p = 25\,293\,378\,613$ at $\alpha = 112\,458$, witnessed by $n = 76\,000$, and $p = 74\,857\,799\,381$ at $\alpha = 193\,466$, witnessed by $n = 62\,967$.

They are the third and the fourth (Section 8). For every α with $2 \le \alpha \le 300\,000$ — among which $34\,603$ give a prime $p = 2\alpha(\alpha-1)+1$, against the 586 of [1] — the number $2\alpha(\alpha-1)+1$ is a Lev–Sonn prime exactly when $\alpha \in \{3, 5, 112\,458, 193\,466\}$. So the four Lev–Sonn primes known are the first four, and there is no fifth below $1.8 \cdot 10^{11}$.

A correction (Section 6). The witness printed in [1] for $p = 41$ is $(\alpha, n) = (5, 5)$. It is not a witness: $\binom{24}{9} \equiv 14$ while $(-1)^4\binom{24}{5} \equiv 28 \pmod{41}$. The witness is $(\alpha, n) = (5, 4)$, and it is the unique one in the admissible range. The misprint is present in both versions of [1] and affects no assertion of that paper — 41 is a Lev–Sonn prime either way — but it is the only witness printed there for $p = 41$, so a reader who re-derives the example from the text meets a congruence that does not hold.

The method (Sections 3 and 4). At $\alpha = 112\,458$ the two binomial coefficients of Problem 1.1 have $616\,862$ and $991\,481$ decimal digits, so nothing can be decided by forming them. A Pascal telescope (Lemma 3.1) gives an exact identity in $\mathbb{Z}$ between $\binom{m}{\alpha+j}$ and $\binom{m}{\alpha}$ whose two correction factors are units modulo p; dividing by them (Theorem 3.3) turns Problem 1.1 at $n = j+1$ into the equality of two running products of j residues, one modular multiplication per factor. A further substitution, using $2(\alpha^2-\alpha) = p-1$, removes α from the left-hand product altogether and rewrites the condition as $(2j+1)!! \equiv 2^j(\alpha+j)!/\alpha!$ (Proposition 4.1). This is elementary, and we record it because it is the only route we know towards a test costing less than $\Theta(\alpha)$ per α; Section 9 explains why such a route, and not more computation, is what the problem now needs.

Every theorem, proposition and lemma below has been verified in Lean 4 against *Mathlib*; Section 10 says exactly which parts rest on compiled evaluation of a finite search and which are checked by the proof kernel alone. Numerical statements that lie outside the formal development — timings, population counts, the heuristic of Section 9 — are flagged as such where they occur.

Remark 1.2 (where the congruence comes from). Problem 1.1 is not arbitrary: it is the exact obstruction met by the coefficient comparison of [1, §3]. There $A \subset \mathbb{F}_p$ has $|A| = \alpha$ and the relevant multiplicative subgroup has order $d = \alpha(\alpha-1)$, so $\alpha+d-1 = \alpha^2-1$ and $p = 2\alpha(\alpha-1)+1$ is exactly the case $d = (p-1)/2$ of the quadratic residues. Comparing the coefficients of x^{d-2} and of x^{d-3}, [1] obtains, in these words and identically in either version,

$$\binom{\alpha+d-1}{d-2} \equiv -(\alpha-1)\binom{\alpha+d-1}{d}, \qquad \binom{\alpha+d-1}{d-3} \equiv (\alpha-1)\binom{\alpha+d-1}{d} \pmod{p},$$

each valid when the corresponding power sum of A is nonzero. Since $\alpha+d-1 = \alpha^2-1$ one has $\binom{\alpha^2-1}{d-k} = \binom{\alpha^2-1}{\alpha-1+k}$ and $\binom{\alpha+d-1}{d} = \binom{\alpha^2-1}{\alpha-1}$, while $(\alpha-1)\binom{\alpha^2-1}{\alpha-1} = \binom{\alpha^2-1}{\alpha}$ already in $\mathbb{Z}$. With these three substitutions the two relations read $\binom{\alpha^2-1}{\alpha+1} \equiv -\binom{\alpha^2-1}{\alpha}$ and $\binom{\alpha^2-1}{\alpha+2} \equiv \binom{\alpha^2-1}{\alpha}$: precisely the congruence of Problem 1.1 at $n = 2$ and at $n = 3$. A Lev–Sonn prime is therefore a prime of the shape at which some level of the comparison fails to yield a contradiction, and [1] introduces the problem with exactly that pointer: "Direct comparison of coefficients of Hanson–Petridis polynomials with corresponding products (see Section 3) also motivates the following problem."

The identification is exact at the two levels the source prints, and only at those: [1, §3] computes the coefficients of x^{d-2} and of x^{d-3} and stops, two power sums being all its proof needs. That the comparison at a general level returns the congruence of Problem 1.1 at that level is the evident pattern, and presumably the reason the problem is posed for all $1 < n \le \alpha$; but the source does not assert

it and we have not carried out the general coefficient computation. Nothing below depends on it: Problem 1.1 is treated from here on as the self-contained statement it is.

2. Notation and setup

Throughout, $\alpha \geq 2$ is an integer and

$$p = p(\alpha) := 2\alpha(\alpha-1)+1 = (\alpha-1)^2+\alpha^2, \qquad m = m(\alpha) := \alpha^2-1.$$

The map $\alpha \mapsto p(\alpha)$ is injective on $\alpha \geq 2$ and p determines $\alpha = (1+\sqrt{2p-1})/2$, so indexing by α rather than by p loses nothing; we do so throughout.

Definition 2.1. Let $\alpha \geq 2$. An integer n is a *witness at* α if $1 < n \leq \alpha$ and

$$\binom{m}{n-1+\alpha} \equiv (-1)^{n-1}\binom{m}{\alpha} \pmod{p}. \tag{1}$$

We say α *carries a Lev–Sonn prime* — equivalently, $p(\alpha)$ is a *Lev–Sonn prime* — if p is prime and some witness at α exists.

Two elementary facts about the shape are used constantly. First,

$$p - m = (\alpha-1)^2 + 1 > 0, \tag{2}$$

so $m < p$: every binomial coefficient occurring in (1) has upper argument smaller than the modulus. Second,

$$2(\alpha^2-\alpha) = p-1, \tag{3}$$

which is the whole content of Section 4.

It is convenient to index witnesses by $j := n-1$, so that $1 \leq j < \alpha$ and (1) reads $\binom{m}{\alpha+j} \equiv (-1)^j\binom{m}{\alpha}$.

3. The telescoped unit-factor identity

The obstacle is size. At $\alpha = 112\,458$ one has $m = 12\,646\,801\,763$, and $\binom{m}{\alpha}$ has 616 862 decimal digits while $\binom{m}{n-1+\alpha}$ has 991 481; the corresponding coefficients at $\alpha = 193\,466$ are larger still. Forming either number to reduce it modulo an eleven-digit prime is possible but pointless, and inside a proof assistant, where $\binom{m}{k}$ is defined by Pascal's recursion, it is not possible at all. The following identity removes the need.

Lemma 3.1 (Pascal telescope)**.** *For all integers $m, \alpha \geq 0$ and $j \geq 0$,*

$$\binom{m}{\alpha+j}\prod_{i=1}^{j}(\alpha+i) \;=\; \binom{m}{\alpha}\prod_{i=1}^{j}(m-\alpha-i+1).$$

In particular, for $m = \alpha^2-1$ the right-hand product is $\prod_{i=1}^{j}(\alpha^2-\alpha-i)$.

Proof. Induction on j, the step being the Pascal relation $\binom{m}{k+1}(k+1) = \binom{m}{k}(m-k)$ at $k = \alpha+j$. No side condition is needed. In the degenerate range both sides vanish: if $\alpha > m$ then $\binom{m}{\alpha} = 0$ and $\binom{m}{\alpha+j} = 0$, while if $\alpha \leq m < \alpha+j$ then $\binom{m}{\alpha+j} = 0$ and the right-hand product contains the factor $m-\alpha-i+1$ at $i = m-\alpha+1 \leq j$, which is zero. □

Lemma 3.2. *Let $\alpha \geq 2$ with $p = p(\alpha)$ prime, and let $0 \leq j \leq \alpha$. Then $p \nmid \binom{m}{\alpha}$ and $p \nmid \prod_{i=1}^{j}(\alpha+i)$.*

Proof. If $p \mid \binom{m}{\alpha}$ then $p \mid m!$ by $\binom{m}{\alpha}\,\alpha!\,(m-\alpha)! = m!$, whence $p \leq m$, contradicting (2). Each factor satisfies $2 \leq \alpha+i \leq 2\alpha < p$, so no factor is divisible by p. □

Theorem 3.3 (the bridge)**.** *Let $\alpha \geq 2$ with $p = p(\alpha)$ prime and let $1 \leq j < \alpha$. Then*

$$\binom{m}{\alpha+j} \equiv (-1)^j\binom{m}{\alpha} \pmod{p} \qquad\Longleftrightarrow\qquad \prod_{i=1}^{j}(\alpha^2-\alpha-i) \;\equiv\; \prod_{i=1}^{j}\bigl(p-(\alpha+i)\bigr) \pmod{p}.$$

Proof. Reduce Lemma 3.1 modulo p and cancel, which Lemma 3.2 permits on both sides: $\binom{m}{\alpha}$ is a unit, and so is $\prod_{i=1}^{j}(\alpha+i)$. The sign is absorbed by $p-(\alpha+i)\equiv-(\alpha+i)$, which turns $(-1)^j\prod(\alpha+i)$ into $\prod\big(p-(\alpha+i)\big)$. □

Theorem 3.3 is what makes the problem computable. Both sides are running products: to decide (1) for every admissible n at a given α, keep two residues N_j and D_j modulo p, initialised at 1, update them by

$$N_j = N_{j-1}\cdot(\alpha^2-\alpha-j) \bmod p, \qquad D_j = D_{j-1}\cdot\big(p-(\alpha+j)\big) \bmod p,$$

and compare after each step. The cost is $2(\alpha-1)$ modular multiplications for the whole range of n, with no divisions, no inverses and no integers exceeding p^2. Each individual comparison $N_j = D_j$ is an equality of residues, but by Theorem 3.3 it is exactly equivalent to the congruence (1) between the two enormous binomial coefficients: nothing is approximated and nothing is replaced by a proxy.

One implementation remark. At the scale of Section 8 the modulus reaches $p \approx 1.8\cdot10^{11}$, and the products $N_{j-1}\cdot(\alpha^2-\alpha-j)$ then exceed 2^{63}. On the arithmetic used here that threshold separates single-word from arbitrary-precision multiplication, so it pays to split the multiplication into pieces that individually stay below it. The rewriting used is unconditionally valid.

Lemma 3.4. *For all natural numbers p, a, b and $s = 2^{19}$,*

$$\Big(\big(\lfloor a/s\rfloor\, b \bmod p\big)\, s \;+\; (a \bmod s)\, b\Big) \bmod p \;=\; ab \bmod p.$$

Proof. $\lfloor a/s\rfloor\, b\, s + (a \bmod s)\, b = ab$ exactly in $\mathbb{N}$, and replacing $\lfloor a/s\rfloor\, b$ by its residue changes the left-hand side by a multiple of p. □

Remark 3.5. Lemma 3.4 is a statement about speed, not about correctness: it holds for all a, b, p, and no bound is needed for its proof. For $p < 2^{40}$ — that is, for $\alpha < 7.4\cdot10^5$ — every intermediate value on the left stays below 2^{63}. On the machine used for this work, substituting it for the plain product made the sweep over the window $45\,000 < \alpha \le 100\,000$ run 9.4 times faster, and it is the reason the computation of Section 8 takes minutes rather than hours. This is a measurement on one implementation and one machine, not a mathematical claim.

4. The condition with α eliminated from one side

The right-hand product of Theorem 3.3 depends on α only through the shift $\alpha + i$; the left-hand product looks as if it depends on α quadratically. It does not, and (3) is the reason: $2(\alpha^2-\alpha-i)+(2i+1) = p$ exactly, so modulo p every numerator factor is $-(2i+1)/2$ and α disappears.

Proposition 4.1. *Let $\alpha \ge 2$ with $p = p(\alpha)$ prime and let $1 \le j < \alpha$. Then*

$$\binom{m}{\alpha+j} \equiv (-1)^j\binom{m}{\alpha} \pmod p \qquad\Longleftrightarrow\qquad \prod_{i=1}^{j}(2i+1) \;\equiv\; \prod_{i=1}^{j}(2\alpha+2i) \pmod p,$$

that is, if and only if

$$(2j+1)!! \;\equiv\; 2^j\,\frac{(\alpha+j)!}{\alpha!} \pmod p.$$

Proof. Since $p = 2\alpha(\alpha-1)+1$ is odd, 2 is a unit modulo p; multiply both sides of the right-hand congruence of Theorem 3.3 by 2^j. On the left, $2(\alpha^2-\alpha-i) \equiv -(2i+1)$ for each i by (3), so $2^j\prod_{i=1}^{j}(\alpha^2-\alpha-i) \equiv (-1)^j\prod_{i=1}^{j}(2i+1)$. On the right, $2^j\prod_{i=1}^{j}\big(p-(\alpha+i)\big) \equiv (-1)^j\prod_{i=1}^{j}(2\alpha+2i)$. Cancelling the common unit $(-1)^j$ gives the stated equivalence; the second form is the first, since $\prod_{i=1}^{j}(2i+1) = 3\cdot5\cdots(2j+1) = (2j+1)!!$ and $\prod_{i=1}^{j}(2\alpha+2i) = 2^j(\alpha+1)\cdots(\alpha+j)$. □

Proposition 4.1 is a substitution into the congruence of Problem 1.1 and we claim no more for it than that. Its interest is structural: the left-hand side is a double factorial that does not mention α, so as α varies over the primes of the shape one is asking how the fixed sequence $(2j+1)!!$ meets the moving sequence $2^j(\alpha+j)!/\alpha!$; and the right-hand side is a ratio of factorials in a range where

Wilson's theorem and the Gauss factorials apply. We were not able to find the reformulation written down, which is unsurprising — [1] states the congruence in binomial form and does not manipulate it — and we have checked it against the original form at all 79 401 pairs (α, j) with $\alpha < 400$ and $1 \le j < \alpha$, and at both new primes of Section 7, with no disagreement.

5. The primes of the source, verified

Proposition 5.1. *$p = 13$ is a Lev–Sonn prime at $\alpha = 3$, and $n = 3$ is the only witness at $\alpha = 3$. $p = 41$ is a Lev–Sonn prime at $\alpha = 5$.*

Proof. $p(3) = 13$ and $p(5) = 41$ are prime and $m(3) = 8$, $m(5) = 24$. At $\alpha = 3$ the two products of Theorem 3.3 agree at $j = 2$ and disagree at $j = 1$, so $n = 3$ is a witness and $n = 2$ is not; equivalently $\binom{8}{5} \equiv \binom{8}{3} \equiv 4 \pmod{13}$. At $\alpha = 5$ the products agree at $j = 3$; see Section 6 for the full witness list there. Every comparison involved is a product of at most four residues. □

Proposition 5.2. *There are exactly 586 values of α with $2 \le \alpha \le 3000$ for which $p = 2\alpha(\alpha - 1) + 1$ is prime; and among $2 \le \alpha \le 3000$ the only α carrying a Lev–Sonn prime are $\alpha = 3$ and $\alpha = 5$.*

Proof. The count is an exhaustive primality test of the 2999 integers $p(\alpha)$, $2 \le \alpha \le 3000$. The second assertion is Theorem 8.1 below, restricted to $\alpha \le 3000$; the proof of that theorem does not use this proposition, so there is no circularity. □

Proposition 5.2 is not a new result; it is a reproduction of the two numbers printed in [1], and we state it because it calibrates everything that follows. A search that disagreed with [1] below $\alpha = 3000$ would be evidence against the search, not against the source. It agrees, in the count and in the list of primes. The one place where it does not agree is the witness printed for $p = 41$, and that is the subject of the next section.

6. A correction to the printed witness for $p = 41$

The sentence quoted in Section 1 ends, verbatim,

> … produced only two such primes $p = 13$ and $p = 41$, corresponding to $(\alpha, n) = (3, 3)$ and $(5, 5)$.

We compared the two e-prints of [1] character by character at this sentence: it stands identically in the version of 14 April 2025 and in the version of 28 May 2025, down to the punctuation and the spacing, and it is the only place in either version where a pair (α, n) for $p = 41$ is printed. The first pair is correct (Proposition 5.1). The second is not.

Theorem 6.1. *Let $\alpha = 5$, so $p = 41$ and $m = 24$. Then $n = 5$ is* not *a witness at $\alpha = 5$, $n = 4$ is a witness, and $n = 4$ is the only witness in the admissible range $1 < n \le 5$.*

Proof. Both failing and succeeding cases are small enough to display. For $n = 5$,

$$\binom{24}{9} = 1\,307\,504 \equiv 14, \qquad (-1)^4 \binom{24}{5} = 42\,504 \equiv 28 \pmod{41},$$

and $14 \neq 28$, so (1) fails. For $n = 4$,

$$\binom{24}{8} = 735\,471 \equiv 13, \qquad (-1)^3 \binom{24}{5} \equiv -28 \equiv 13 \pmod{41},$$

so (1) holds. Uniqueness is the four comparisons $j = 1, 2, 3, 4$ of Theorem 3.3 at $\alpha = 5$, of which only $j = 3$ is an equality. In the formal development every one of these assertions is obtained through Theorem 3.3, so the binomial coefficients are never formed; the displayed values were computed separately, by direct evaluation, and agree. □

Remark 6.2. The misprint affects no assertion of [1]: 41 is a Lev–Sonn prime whichever n witnesses it, and no argument in that paper uses the witness. Its cost is to the reader, because $(5,5)$ is the only witness printed for $p=41$ and it fails. Nor does the failure depend on which version's notation the reader works in. In the notation of the first version, $\binom{\alpha-1+d}{d-n} \equiv (-1)^{n-1}\binom{\alpha-1+d}{d-1}$ with $\alpha=5$, $d=20$ and $n=5$ reads $\binom{24}{15} \equiv 14$ against $\binom{24}{19} \equiv 28 \pmod{41}$: the same two residues as above, since $\binom{24}{15}=\binom{24}{9}$ and $\binom{24}{19}=\binom{24}{5}$.

The pair $(5,5)$ therefore stands in the version of 14 April 2025 and again in that of 28 May 2025, whose posted comment records that misprints were corrected. As of 29 August 2026 these are the only two versions on the arXiv; the abstract page carries no journal reference and no erratum, and we have found no published version of the paper. We have not written to the author; doing so before submission remains an option, and the version list should in any case be re-checked then.

Remark 6.3. A second, purely bibliographic slip in the same paper, recorded here because it is the kind that propagates: the bibliography of [1] dates [4] to 2021. The correct year is 2012; the Crossref record of the DOI printed there, and the zbMATH entry, both give Acta Arith. **155** (2012), no. 1, 41–51.

7. Two new Lev–Sonn primes

Theorem 7.1. $p = 25\,293\,378\,613 = 2 \cdot 112\,458 \cdot 112\,457 + 1$ *is a Lev–Sonn prime. A witness at* $\alpha = 112\,458$ *is* $n = 76\,000$*: with* $m = \alpha^2 - 1 = 12\,646\,801\,763$*,*

$$\binom{m}{188\,457} \equiv (-1)^{75\,999}\binom{m}{112\,458} \equiv 8\,962\,693\,066 \pmod{p}.$$

Theorem 7.2. $p = 74\,857\,799\,381 = 2 \cdot 193\,466 \cdot 193\,465 + 1$ *is a Lev–Sonn prime. A witness at* $\alpha = 193\,466$ *is* $n = 62\,967$*: with* $m = \alpha^2 - 1 = 37\,429\,093\,155$*,*

$$\binom{m}{256\,432} \equiv (-1)^{62\,966}\binom{m}{193\,466} \equiv 5\,628\,973\,554 \pmod{p}.$$

Proof of Theorems 7.1 and 7.2. Each statement has two parts. Primality of the eleven-digit modulus is established by a certificate checked inside the proof kernel, with no appeal to compiled evaluation. The congruence is Theorem 3.3 at $j = n-1$, so what has to be exhibited is the equality of the two running products after 75 999 steps (respectively 62 966 steps); that computation — two modular multiplications and one comparison per step — is the exhaustive part, and it is delegated to compiled evaluation. The two residues displayed above are not needed for the proof; they are reported because they were produced by a third, independent route, namely by forming $\binom{m}{n-1+\alpha}$ and $\binom{m}{\alpha}$ as integers and reducing them, and they match. □

Remark 7.3. The integers whose congruence Theorem 7.1 asserts have 991 481 and 616 862 decimal digits. Producing them is feasible — it is how the check just described was made, at a cost of seconds per pair rather than minutes — but it is not a method: the classification of Section 8 needs about $5\cdot10^9$ individual comparisons, and those near the top of its range would each be a million-digit computation if done that way. Theorem 3.3 replaces every one of them by two machine-word multiplications.

8. The classification below $\alpha = 300\,000$

Theorem 8.1. *For every integer* α *with* $2 \le \alpha \le 300\,000$*,*

$$p(\alpha) = 2\alpha(\alpha-1)+1 \text{ is a Lev–Sonn prime} \iff \alpha \in \{3,\ 5,\ 112\,458,\ 193\,466\}.$$

Consequently 13*,* 41*,* 25 293 378 613 *and* 74 857 799 381 *are the first four Lev–Sonn primes: no Lev–Sonn prime other than these four satisfies* $p \le p(300\,000) = 179\,999\,400\,001$*.*

Proof. The implication from right to left is Proposition 5.1 together with Theorems 7.1 and 7.2. The implication from left to right is an exhaustive search, and we describe exactly what it checks. For each α in $[2, 300\,000]$ other than the four listed, one of two certificates is produced.

- A divisor d of $p = p(\alpha)$ with $1 < d < p$. The divisor is found by unverified trial division, but the three conditions $1 < d$, $d < p$ and $p \bmod d = 0$ are re-tested before use, so nothing is trusted about the search that produced d; a wrong answer simply fails the test. Then p is composite and α carries no Lev–Sonn prime whatever the congruence does.
- Otherwise the two running products of Theorem 3.3 are advanced through $j = 1, \dots, \alpha - 1$ and found to differ at every step. Should p be prime, Theorem 3.3 then refutes (1) for every admissible n; should it not be, α carries no Lev–Sonn prime by Definition 2.1. Either way it carries none, and no primality proof is required.

The whole search is one exhaustive finite computation, delegated to compiled evaluation; the passage from its Boolean output to the statement above is proved in the kernel. □

The size of the search is worth recording, since it is the reason the result is a result and not a remark. Of the 299 999 values $\alpha \le 300\,000$, exactly 34 603 give a prime $p(\alpha)$; for those — apart from the four exceptional values, about which the search asserts nothing — no composite certificate exists and the full scan runs. Among them $\alpha \le 3000$ contributes 586, which is the population examined in [1]. The scan length at α is $\alpha - 1$, so the total is

$$\sum_{\substack{2 \le \alpha \le 300\,000 \\ p(\alpha) \text{ prime}}} (\alpha - 1) \;\approx\; 4.95 \cdot 10^9$$

comparisons, each of two modular multiplications; this took 458 seconds of processor time. Relative to the search reported in [1] the range is 100 times longer and the population of tested primes 59 times larger. (The count 586 is itself part of the formal development, as Proposition 5.2; the count 34 603 is reported by the search and was reproduced by an independently written program, but it is not part of the formal statement of Theorem 8.1, which speaks only of which α carry a Lev–Sonn prime.)

Controls. An exhaustive negative result is worth exactly as much as the definition it ranges over, so we record three checks that a misstated version of Definition 2.1 would fail.

Proposition 8.2. (i) *$p(2) = 5$ is prime and is not a Lev–Sonn prime. In particular it is false that every prime of the form $2\alpha(\alpha - 1) + 1$ is a Lev–Sonn prime.*

(ii) *It is false that* 13 *and* 41 *are the only Lev–Sonn primes.*

(iii) *At $\alpha = 4$ the two running products of Theorem 3.3 agree at $j = 3$ — equivalently, by direct evaluation, $\binom{15}{7} \equiv (-1)^3 \binom{15}{4} \equiv 10 \pmod{25}$ — while $p(4) = 25$ is not prime. So the primality clause of Definition 2.1 is not vacuous.*

Proof. (i) is the scan at $\alpha = 2$, a single comparison. (ii) is Theorem 7.1. For (iii), the comparison at $\alpha = 4$, $j = 3$ together with $25 = 5^2$. Here Theorem 3.3 assumes p prime and so is unavailable, and the split matters: what is verified inside the formal development is the equality of the two running products at $\alpha = 4$, $j = 3$, and the non-primality of 25; the congruence between binomial coefficients modulo the composite modulus 25, displayed above, was checked by direct evaluation outside it. For (iii) the two happen to agree, but for composite p the running products carry no general information about (1), and we claim none. □

Part (iii) is the substantial one, because the congruence side alone is a weak condition. Running the comparison of Theorem 3.3 at every $\alpha \le 45\,000$ regardless of whether $p(\alpha)$ is prime, it fires for 13 371 of the 44 999 values, against the two that satisfy both requirements in that range. That ratio is a measurement made by the search program outside the formal development, and it is quoted as an indication of scale only: for composite $p(\alpha)$ what is being counted is the equality of the two running products, which is then no longer equivalent to (1).

9. How much further a search should go

Problem 1.1 remains open, and nothing here bears on it. What the computation does supply is a quantitative reason to stop computing.

Model the residue $\prod_{i\le j}(\alpha^2-\alpha-i)\cdot\big(\prod_{i\le j}(p-(\alpha+i))\big)^{-1}$ as uniform in $\mathbb{F}_p^*$ and independent across j. Then α carries a Lev–Sonn prime with probability about $(\alpha-1)/p \approx 1/(2\alpha)$, and the expected number of Lev–Sonn primes with $\alpha \le A$ is

$$E(A) \;=\; \sum_{\substack{\alpha\le A\\ p(\alpha)\ \text{prime}}} \frac{\alpha-1}{p(\alpha)}.$$

Computed exactly, E takes the values

$$E(3\,000)=1.40, \qquad E(3\cdot 10^5)=1.70, \qquad E(10^6)=1.76, \qquad E(10^7)=1.86.$$

Two readings, both worth having. First, $E(A)\to\infty$, so the heuristic answer to Problem 1.1 is *yes*; but the divergence is of order $\log\log A$, so no counting argument of this shape can produce a proof, and the four observed primes against $E(3\cdot 10^5)=1.70$ expected is a mild excess only — for a Poisson variable with $\lambda=1.6985$, $\Pr[X\ge 4]=0.093$. Second, and more usefully, the entire range $3\cdot 10^5<\alpha\le 10^7$ is expected to contain about 0.16 further Lev–Sonn primes. Since the scan costs $\Theta(\alpha)$ per α and no test of one α in $o(\alpha)$ is known, that range needs $4.30\cdot 10^{12}$ comparisons, which is 86 times the entire search to 10^6 described next — of the order of 80 processor-hours at the rate that search ran — for an expected yield of essentially nothing.

That expectation is consistent with what a direct search finds. We ran the same search in a separate, unverified program to $\alpha\le 10^6$ — 104 893 primes of the shape, about 57 minutes of processor time — and it returns the same four values of α and no fifth. We stress that this computation is outside the formal development and is not offered as a theorem; its only role is to say that certifying the range $3\cdot 10^5<\alpha\le 10^6$ would add no new prime to the list of Theorem 8.1, merely a longer guarantee.

Everything in this section lies outside the formal development. The counts 104 893 and 34 603, the comparison totals, and the values of E and of the Poisson tail were each produced twice, from independently written programs, and agree; the timings are single measurements on one machine and should be read as such. The model itself is a model: four terms constrain nothing, and the argument is offered as a reason to spend effort elsewhere, not as evidence about Problem 1.1.

The productive direction is therefore structural, and Proposition 4.1 is where we would start: it asks when the fixed double factorial $(2j+1)!!$ meets $2^j(\alpha+j)!/\alpha!$ modulo p, and factorial ratios in an interval of this shape are the natural habitat of Wilson's theorem and of the Gauss factorials $(p-1)!_m$. A test deciding one α in $o(\alpha)$ operations, if one exists, would move the reachable range by orders of magnitude at once; more processor time will not.

We also record, for whoever continues the list, that the sequence

$$13, \qquad 41, \qquad 25\,293\,378\,613, \qquad 74\,857\,799\,381$$

does not appear in the on-line encyclopedia of integer sequences, although the ambient sequence of primes $j^2+(j+1)^2$ does [7, A027862].

10. Verification

Every theorem, proposition and lemma of this paper has been formally verified in Lean 4 (toolchain `v4.32.0`) against *Mathlib*, and the development contains no `sorry`; repository reference to be added at submission. The exceptions, flagged where they appear, are the numerical side remarks: the timings and the speed comparison of Remark 3.5, the population count 34 603 and the ratio 13 371/44 999 of Section 8, the decimal digit counts, and everything in Section 9. The reasoning layer is checked by the proof kernel alone, depending on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`: this covers Lemmas 3.1, 3.2 and 3.4, Theorem 3.3, Proposition 4.1, Proposition 5.1, Theorem 6.1, Proposition 8.2(i) and (iii), the primality of 25 293 378 613 and of 74 857 799 381, and the derivation of each mathematical statement from the Boolean output of the corresponding finite search. Part (ii) of Proposition 8.2 is the one control that is not kernel-only: it is Theorem 7.1 and inherits its compiled evaluation. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly three finite searches: the 75 999-step and 62 966-step scans witnessing Theorems 7.1 and 7.2; the primality

count of Proposition 5.2; and the sweep of Theorem 8.1 over $2 \le \alpha \le 300\,000$. Nothing else uses it, and in particular the small congruences of Sections 5 and 6 and the control of Proposition 8.2(iii) are decided by kernel reduction. The trial division inside the sweep is unverified by design, since its output is re-tested (Theorem 8.1). Every numerical value quoted was first produced by an implementation written independently of the formal development — a C program for the searches and counts, a Python program that forms the million-digit binomial coefficients directly for the individual congruences — and these agree with the formal development on all five congruences examined one by one, namely $(\alpha, n) = (3, 3)$, $(5, 4)$, $(5, 5)$, $(112\,458, 76\,000)$ and $(193\,466, 62\,967)$, on the counts 586 and 34 603, and on the residues displayed in Theorems 7.1 and 7.2.

References

[1] A. Kalmynin, *On additive irreducibility of multiplicative subgroups*, arXiv:2504.10202 (v1, 14 April 2025; v2, 28 May 2025).

[2] V. F. Lev and J. Sonn, *Quadratic residues and difference sets*, Quart. J. Math. **68** (2017), no. 1, 79–95, doi:10.1093/qmath/haw002.

[3] B. Hanson and G. Petridis, *Refined estimates concerning sumsets contained in the roots of unity*, Proc. London Math. Soc. (3) **122** (2021), 353–358, doi:10.1112/plms.12322.

[4] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p*, Acta Arith. **155** (2012), no. 1, 41–51, doi:10.4064/aa155-1-4.

[5] I. D. Shkredov, *Sumsets in quadratic residues*, Acta Arith. **164** (2014), no. 3, 221–243, doi:10.4064/aa164-3-2.

[6] S. Kim, C. H. Yip and S. Yoo, *Multiplicative irreducibility of shifted multiplicative subgroups*, J. London Math. Soc. **114** (2026), no. 3, Paper No. e70688, doi:10.1112/jlms.70688; arXiv:2602.20919.

[7] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`; entry A027862, primes of the form $j^2 + (j+1)^2$.