Divisor sums over $N - k^2$ modulo 4 for $N \equiv 6 \pmod 8$: a proof of a conjecture of Jirattikansakul, Kittipassorn, Kongsiri, Moonwichit and Sriamorn

Qianghao Wu

November 27, 2026

Abstract

Let $S(N) = \sum_{1 \le k < \sqrt{N}} \sigma_0(N - k^2)$, where $\sigma_0(m)$ is the number of positive divisors of m. Jirattikansakul, Kittipassorn, Kongsiri, Moonwichit and Sriamorn proved that $S(N) \equiv 0 \pmod 4$ for $N = An + B$ with $(A, B) \in \{(16, 14), (36, 30), (72, 42), (196, 70), (252, 114)\}$, and they conjectured that $S(N) \equiv 0 \pmod 4$ for all $N = 16n + 6$ (their Conjecture 7). We prove this conjecture. More generally, we prove that $S(N) \equiv 0 \pmod 4$ for every $N \equiv 6 \pmod 8$, as their computations suggest. The class $N \equiv 14 \pmod{16}$ is their case $(16, 14)$, so for that class our proof is a new proof of a known result. Their proof uses a congruence of Keith for partitions into exactly two part sizes, which was proved with modular forms. Our proof is elementary. It counts the solutions of $k^2 + ab = N$ with involutions, one of which is Zagier's involution from his one-sentence proof of Fermat's two-squares theorem. Lean 4 with Mathlib checks the theorem and Conjecture 7 from the definitions, with only the standard axioms. With Theorem 4 of the source, the result gives $\nu_2(N) \equiv -\sigma_1(N)/2 \pmod 4$ for all $N \equiv 6 \pmod 8$, where $\nu_2(N)$ is the number of partitions of N with exactly two part sizes. This consequence is not checked in Lean. This work has not yet been reviewed by experts. The computations, the proofs and the text were produced by AI models (from Anthropic and OpenAI), working under the author's direction.

1 Introduction

For a positive integer m, let $\sigma_0(m)$ be the number of positive divisors of m and $\sigma_1(m)$ their sum. For a positive integer N, put

$$S(N) = \sum_{1 \le k < \sqrt{N}} \sigma_0(N - k^2),$$

where k runs over the integers. The number $S(N)$ counts the triples (k, a, b) of positive integers with $k^2 + ab = N$. Hooley [5] studied the representations of N as the sum of a square and a product, and the asymptotic behaviour of this sum; we take this remark from [1, Section 1].

History. Let $\nu_2(N)$ be the number of partitions of N with exactly two part sizes. Keith [2] proved $\nu_2(An + B) \equiv 0 \pmod 4$ for $(A, B) \in \{(36, 30), (72, 42), (196, 70), (252, 114)\}$ with modular forms. DeWitt and Keith [3, 4] write that Keith also proved $\nu_2(16n + 14) \equiv 0 \pmod 4$, that this proof needed modular forms, and they give a combinatorial proof of it. Jirattikansakul, Kittipassorn, Kongsiri, Moonwichit and Sriamorn [1] connect ν_2 with S. Their Theorem 4 says: if $N = 2m$ with m odd and N is not a sum of two squares, then

$$\nu_2(N) + S(N) + \tfrac{1}{2}\sigma_1(N) \equiv 0 \pmod 4. \tag{1}$$

With Keith's congruences they prove (their Theorem 1) that $S(N) \equiv 0 \pmod 4$ for $N = An + B$ with $(A, B) \in \{(16, 14), (36, 30), (72, 42), (196, 70), (252, 114)\}$.

The conjecture. In their Section 5 the authors report computations for $N < 100{,}000$ which suggest that $S(N) \equiv 0 \pmod 4$ for all $N = 8n + 6$. They note that for $N = 8n + 6$ there are N with $\frac{1}{2}\sigma_1(N) \equiv 2 \pmod 4$ and $\nu_2(N) \equiv 2 \pmod 4$, so their method does not apply. The case n odd is $N = 16m + 14$, which their Theorem 1 covers. They state the remaining case as follows [1, Conjecture 7] (word for word from arXiv:2604.25394v1, the only version):

> Conjecture 7. Let $N = 16n+6$ for some nonnegative integer n. Then $\sum_{1\le k<\sqrt{N}} \sigma_0(N - k^2) \equiv 0 \pmod 4$.

Result. We prove Conjecture 7, and more generally $S(N) \equiv 0 \pmod 4$ for all $N \equiv 6 \pmod 8$ (Theorem 1). The new part is the class $N \equiv 6 \pmod{16}$. For the class $N \equiv 14 \pmod{16}$ the result is Theorem 1 of [1] for $(A, B) = (16, 14)$, and our proof is a new proof. The proof is elementary: it uses only finite sets, bijections and involutions. One of the involutions is the involution of Zagier's one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares [6]. We apply it to numbers that are not prime. Lean 4 [7] with Mathlib [8] checks the theorem and Conjecture 7 (Section 5).

Prior work on this question. On November 26 and 27, 2026 we searched the citations of [1] in Semantic Scholar (none were listed), the arXiv listing of [1] (one version, with no note of a proof), two public collections of AI-produced results, GitHub issues and archives where such results are posted, Zenodo, and the web. We found no proof of Conjecture 7. The papers [2] and [3] do not treat the class $16n + 6$.

2 The result

Theorem 1. *Let N be a positive integer with $N \equiv 6 \pmod 8$. Then $S(N) \equiv 0 \pmod 4$.*

Corollary 2 (Conjecture 7 of [1])**.** *For every integer $n \ge 0$, $\sum_{1\le k<\sqrt{16n+6}} \sigma_0(16n + 6 - k^2) \equiv 0 \pmod 4$.*

Table 1 gives the first values.

N	6	14	22	30	38	46	54	62
$S(N)$	4	8	16	16	16	32	28	20
N	70	78	86	94	102	110	118	
$S(N)$	40	32	36	52	40	32	52	

Table 1: $S(N)$ for the first values $N \equiv 6 \pmod 8$.

For a control, the class $N \equiv 2 \pmod 8$ gives $S(N) \bmod 4 = 1, 0, 3, 2$ at $N = 2, 10, 18, 26$, so the congruence is not a property of all $N \equiv 2 \pmod 4$. For $1 \le N \le 3000$, the classes $N \equiv 6$ and $N \equiv 14 \pmod{16}$ are the only classes modulo 16 on which $S(N) \bmod 4$ is always 0 (Section 5).

3 Proof

Fix $N \equiv 6 \pmod 8$. All variables are positive integers. Squares are $\equiv 0$, 1 or 4 (mod 8), and odd squares are $\equiv 1 \pmod 8$.

Lemma 3. *Let f be an involution of a finite set T, and let* Fix f *be its set of fixed points. Then $|T| \equiv |\operatorname{Fix} f| \pmod 2$. If P is a property such that $P(t)$ holds exactly when $P(f(t))$ fails, then $|T| = 2\,|\{t \in T : P(t)\}|$.*

Proof. The points that f does not fix form pairs $\{t, f(t)\}$. In the second case f has no fixed point, and each pair has exactly one point with property P. □

Let $X = \{(k, a, b) : k^2 + ab = N\}$. For a fixed k with $k^2 < N$, the pairs (a, b) are the factorizations of $N - k^2$, so $|X| = S(N)$. Let X_1 and X_0 be the parts of X with k odd and k even.

Odd k. Let k be odd. Then $n := N - k^2 \equiv 5 \pmod 8$.

1. If $ab = n$, then a and b are odd and $ab \equiv 1 \pmod 4$, so $a \equiv b \pmod 4$. Also $a \neq b$, because n is not a square. By Lemma 3 with the swap $(k, a, b) \mapsto (k, b, a)$ and the property $a < b$, $|X_1| = 2|X_1^<|$, where $X_1^<$ is the part of X_1 with $a < b$.

2. Let $Z = \{(k, x, y, z) : k \text{ odd},\ k^2 + x^2 + 4yz = N\}$. The map $(k, a, b) \mapsto (k, a, a, (b - a)/4)$ is a bijection from $X_1^<$ onto the part of Z with $x = y$. Its inverse is $(k, x, x, z) \mapsto (k, x, x + 4z)$. So $|X_1^<| = |\{t \in Z : x = y\}|$.

3. For a point of Z, $x^2 + 4yz = n$ with $n = N - k^2 \equiv 5 \pmod 8$. So x is odd, and $x \neq 2y$. Also $x + z \neq y$: otherwise $n = x^2 + 4(x + z)z = (x + 2z)^2$ is a square. So exactly one of the three conditions below holds, and Zagier's map [6], which keeps k, is defined on all of Z:

$$(x, y, z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x + z < y, \\ (2y - x,\ y,\ x + z - y) & \text{if } y < x + z \text{ and } x < 2y, \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y. \end{cases}$$

   The map keeps $x^2 + 4yz$ and positivity, and it is an involution of Z. Its fixed points are the points with $x = y$: the first and the third case have no fixed point, and in the second case $(2y - x, y, x + z - y) = (x, y, z)$ exactly when $x = y$. By Lemma 3 and step 2, $|Z| \equiv |X_1^<| \pmod 2$.

4. The swap $(k, x, y, z) \mapsto (k, x, z, y)$ is an involution of Z with fixed points $y = z$. So $|Z| \equiv |Z^=| \pmod 2$, where $Z^=$ is the part of Z with $y = z$.

5. On $Z^=$, x is odd (step 3), so the swap $(k, x, y, y) \mapsto (x, k, y, y)$ is an involution of $Z^=$. Its fixed points are the points (k, k, y, y) with $2k^2 + 4y^2 = N$. Let F be their number.

So $|X_1^<| \equiv F \pmod 2$, and $|X_1| = 2|X_1^<| \equiv 2F \pmod 4$.

Even k. Let k be even. Then $N - k^2 \equiv 2 \pmod 4$.

6. If $ab = N - k^2$, then exactly one of a, b is even. By Lemma 3 with the swap $(k, a, b) \mapsto (k, b, a)$ and the property "b is even", $|X_0| = 2|X_b|$, where X_b is the part of X_0 with b even.

7. The map $(k, a, b) \mapsto (k, b/2, 2a)$ is an involution of X_b. Its fixed points are the points $(k, a, 2a)$, that is, k even and $k^2 + 2a^2 = N$.

8. The map $(k, k, y, y) \mapsto (2y, k, 2k)$ is a bijection from the fixed points of step 5 onto the fixed points of step 7: $(2y)^2 + 2k^2 = N$. Its inverse is $(k', a, 2a) \mapsto (a, a, k'/2, k'/2)$; here a is odd, because $2a^2 = N - k'^2 \equiv 2 \pmod 4$.

So $|X_b| \equiv F \pmod 2$, and $|X_0| = 2|X_b| \equiv 2F \pmod 4$.

Conclusion. $S(N) = |X_1| + |X_0| \equiv 2F + 2F \equiv 0 \pmod 4$. This proves Theorem 1. □

Example 4. Let $N = 22$. Then $|X| = S(22) = 16$. The set $X_1^<$ is $\{(1, 1, 21), (1, 3, 7), (3, 1, 13)\}$, so $|X_1| = 6$. The set Z has 7 points, among them $(1, 1, 1, 5)$, $(1, 3, 3, 1)$ and $(3, 1, 1, 3)$ with $x = y$. The only point of Z with $k = x$ and $y = z$ is $(3, 3, 1, 1)$, so $F = 1$. The set X_b is $\{(2, 1, 18), (2, 3, 6), (2, 9, 2), (4, 1, 6), (4, 3, 2)\}$, so $|X_0| = 10$. The only fixed point of step 7 is $(2, 3, 6)$, the image of $(3, 3, 1, 1)$ in step 8. Then $S(22) = 6 + 10 = 16$.

Remark 5. The first proof that we found used Jacobi's four-square formula and a count of representations as sums of five squares. That proof is not checked in Lean, and we do not give it here.

4 A consequence for partitions into two part sizes

Every $N \equiv 6 \pmod 8$ is $2m$ with m odd, and it is not a sum of two squares, because $a^2 + b^2 \not\equiv 6 \pmod 8$ [1, Section 5]. So (1) applies, and with Theorem 1 it gives

$$\nu_2(N) \equiv -\tfrac{1}{2}\sigma_1(N) \pmod 4 \qquad \text{for all } N \equiv 6 \pmod 8.$$

Let $N \equiv 14 \pmod{16}$, so $N = 2m$ with $m \equiv 7 \pmod 8$. Then $\sigma_1(N) = 3\sigma_1(m)$. The divisors of m form pairs $\{\delta, m/\delta\}$ with $\delta < m/\delta$, because m is not a square. In each pair, the residues modulo 8 are $\{1, 7\}$ or $\{3, 5\}$, so $\delta + m/\delta \equiv 0 \pmod 8$. Thus $\sigma_1(m) \equiv 0 \pmod 8$ and $\frac{1}{2}\sigma_1(N) \equiv 0 \pmod 4$. This gives again $\nu_2(16n+14) \equiv 0 \pmod 4$, the congruence of Keith that DeWitt and Keith reprove combinatorially [3].

This section depends on Theorem 4 of [1]. We did not check the proof of that theorem, and this section is not in Lean. A brute-force count confirms $\nu_2(N) \equiv -\frac{1}{2}\sigma_1(N) \pmod 4$ for all $N \equiv 6 \pmod 8$ with $N \le 700$.

5 How the result was checked

Lean. The file `lean/Solution.lean` (492 lines) imports only Mathlib. It proves the two theorems below, whose statements are copied in `lean/Challenge.lean` with `sorry` in place of the proofs:

```
theorem sum_card_divisors_mod_four (N : ℕ) (hN : N % 8 = 6) :
    (∑ k ∈ (range N).filter (fun k : ℕ => 1 ≤ k ∧ (k : ℝ) < Real.sqrt (N : ℝ)),
      (N - k ^ 2).divisors.card) ≡ 0 [MOD 4]

theorem conjecture_7 (n : ℕ) :
    (∑ k ∈ (range (16 * n + 6)).filter
        (fun k : ℕ => 1 ≤ k ∧ (k : ℝ) < Real.sqrt ((16 * n + 6 : ℕ) : ℝ)),
      (16 * n + 6 - k ^ 2).divisors.card) ≡ 0 [MOD 4]
```

The statements use only Mathlib definitions. Here n runs over $\mathbb{N}$, which contains 0. The index k satisfies $1 \le k$ and $k < \sqrt{N}$ with the real square root, as in the source. The finite range $\{0, \dots, N-1\}$ removes no index, because $1 \le k < \sqrt{N}$ gives $k \le k^2 < N$. For each index, $k^2 < N$, so the truncated subtraction of $\mathbb{N}$ gives the true value $N - k^2 \ge 1$, and `Nat.divisors` of a positive number is its set of positive divisors. So the summand is $\sigma_0(N - k^2)$. The proof follows Section 3 step by step: it defines X, Z, $X_1^<$, X_b and the maps as finite sets and functions on $\mathbb{N}^3$ and $\mathbb{N}^4$, proves Lemma 3 with `Finset.sum_involution`, and proves the equivalence of $k < \sqrt{N}$ and $k^2 < N$ with `Real.lt_sqrt`. The proof uses no `native_decide`, so the axiom list below has no `Lean.ofReduceBool`.

We ran three checks with Lean v4.36.0 and Mathlib v4.36.0. `#print axioms` prints `[propext, Classical.choice, Quot.sound]` for both theorems. An audit script compiles the file and finds no `sorry`, no new axiom and no `debug.skipKernelTC` in its 151 declarations. `lake comparator` checks that the proof file proves exactly the theorems of `Challenge.lean` with only these axioms; it prints `Your solution is okay!`.

Numerical checks. These checks are not needed for the Lean result. They are exact integer computations in Python.

- A direct computation from the definitions, with σ_0 by trial division, finds $S(N) \equiv 0 \pmod 4$ for all 375 values $N \equiv 6 \pmod 8$ with $N \le 3000$. It also gives the values and the control in Section 2 and the sets of the example.
- A brute-force count of each set of Section 3 confirms each step 1 to 8 and the conclusion for all 500 values $N \equiv 6 \pmod 8$ with $N \le 4000$.
- A divisor sieve finds $S(N) \equiv 0 \pmod 4$ for all $N \equiv 6 \pmod 8$ with $N \le 3 \cdot 10^6$ (187 500 values in each of the classes 6 and 14 (mod 16)). For $N \le 3 \cdot 10^5$ and moduli $A = 16, 32, 64$, the only classes B mod A on which $S(N) \equiv 0 \pmod 4$ always holds are the classes with $B \equiv 6 \pmod 8$.
- The brute-force count of ν_2 of Section 4, for $N \le 700$.

6 Limits

1. The formally checked result is exactly the two theorems of `lean/Challenge.lean`. We matched these statements to the source by hand (Section 5); this match is the part of the result that the machine does not check.
2. The new part of the result is the class $N \equiv 6 \pmod{16}$. The class $N \equiv 14 \pmod{16}$ was already proved in [1, Theorem 1].
3. Section 4 depends on Theorem 4 of [1], which we did not check and which is not in Lean.
4. Conjecture 8 of [1], about which progressions $An + B$ can have $S(N) \equiv 0 \pmod 4$ for all n, is not addressed. Our computations show only the classes listed in Section 5, for a finite range.
5. Our search for prior work cannot exclude a proof that is not indexed by the sources we searched.

References

[1] S. Jirattikansakul, T. Kittipassorn, K. Kongsiri, N. Moonwichit and K. Sriamorn, Congruences via partitions with exactly two part sizes, arXiv:2604.25394v1 (2026). https://arxiv.org/abs/2604.25394

[2] W. J. Keith, Partitions into a small number of part sizes, Int. J. Number Theory 13 (2017), 229–241. doi:10.1142/S1793042117500130; arXiv:1502.00366v4. https://arxiv.org/abs/1502.00366

[3] E. R. DeWitt and W. J. Keith, Combinatorial proof of a congruence for partitions into two sizes of part, arXiv:2507.13566v1 (2025). https://arxiv.org/abs/2507.13566

[4] E. R. DeWitt and W. J. Keith, Combinatorial proof of a congruence for partitions into two sizes of part, Int. J. Number Theory 22 (2026), 1075–1084. doi:10.1142/S1793042126500569

[5] C. Hooley, On the representation of a number as the sum of a square and a product, Math. Z. 69 (1958), 211–227. doi:10.1007/BF01187402

[6] D. Zagier, A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, Amer. Math. Monthly 97 (1990), 144. doi:10.2307/2323918

[7] The Lean 4 theorem prover. https://github.com/leanprover/lean4

[8] The Mathlib Community, Mathlib. https://github.com/leanprover-community/mathlib4