hexagon:2611.00370v1

EULER'S 1747 CONJECTURE ON SUMS OF INTEGERS WITH RESTRICTED PRIME FACTORS

WILL HOWE, GRANT HUFFMAN, JENSEN KOHLMEYER, AND LIAM KRUER

Abstract. We prove that every positive integer congruent to 2 modulo 4 is a sum of two positive integers whose prime factors are all congruent to 1 modulo 4, with 1 admitted as a summand. Euler proposed this statement in a letter to Goldbach dated May 6, 1747. The proof counts representations by four squares and bounds those containing a common prime divisor congruent to 3 modulo 4 in either coordinate pair. An average over a nonsplit torus normalizer converts the quaternionic Hecke bound into an error independent of the sieving prime. Elementary estimates then give the explicit threshold 64^4. An exact finite arithmetic certificate covers the remaining 4,194,304 integers in the required residue class.

1. Introduction

Let

$$\mathcal{P}_3 = \{p \text{ prime} : p \equiv 3 \pmod 4\}, \qquad \mathcal{A} = \{a \in \mathbb{Z}_{>0} : p \mid a \Longrightarrow p \equiv 1 \pmod 4\}.$$

The integer 1 belongs to $\mathcal{A}$. In his letter to Goldbach of May 6, 1747, Euler proposed that every integer of the form $4m+2$ can be split into two integers of the form $4x+1$, each having no divisor of the form $4p-1$. This is the assertion proved here. The statement appears in Letter 115 of the collected correspondence, together with a discussion in editorial note 10 [4, pp. 935–936].

Dietmann and Elsholtz proved that every sufficiently large positive integer congruent to 2 modulo 4 has the required decomposition [2]. Their argument uses a result of Greaves on four squares with two prime variables. We obtain an explicit threshold by counting all four-square representations and estimating the unwanted common divisors of the two coordinate pairs.

Theorem 1.1. *Every positive integer $n \equiv 2 \pmod 4$ admits a decomposition*

$$n = a + b, \qquad a, b \in \mathcal{A}.$$

The quantitative part of the proof establishes the result for $n \geq 64^4 = 16{,}777{,}216$ after removing factors from $\mathcal{A}$. Section 7 gives an exact arithmetic certificate for the finite range below this threshold. The spectral ingredient is the weight-two Ramanujan–Petersson bound, applied through the Jacquet–Langlands correspondence. All auxiliary constants are explicit.

2. Four-square representations and prime obstructions

Write $\sigma(u) = \sum_{d \mid u} d$ and $\tau(u) = \sum_{d \mid u} 1$. We first remove a multiplicative factor that already belongs to $\mathcal{A}$.

Lemma 2.1. *To prove Theorem 1.1, it suffices to consider $n = 2m$, where m is odd and every prime divisor of m belongs to $\mathcal{P}_3$.*

Proof. For any odd m, write $m = gm_0$, where $g \in \mathcal{A}$ and every prime divisor of m_0 belongs to $\mathcal{P}_3$. If $2m_0 = a + b$ with $a, b \in \mathcal{A}$, then $2m = ga + gb$ has the same property. □

Date: November 12, 2026.

2020 *Mathematics Subject Classification.* Primary 11P32; Secondary 11E25, 11F11, 11R52.

Key words and phrases. Euler's conjecture, sums of squares, restricted prime factors, Hurwitz quaternions, Hecke operators.

For the remainder of the analytic argument, $n = 2m$ satisfies Lemma 2.1. Put

$$\mathcal{R}(n) = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 = n\}.$$

These are signed, ordered representations. Jacobi's four-square formula gives

$$R(n) := |\mathcal{R}(n)| = 24\sigma(m). \tag{2.1}$$

Exactly two coordinates are odd, since a square is 0 or 1 modulo 4. Let $\mathcal{R}_{\mathrm{mix}}(n)$ consist of the representations in which each of (x_1, x_2) and (x_3, x_4) has opposite parity. Permuting coordinates shows that the six possible placements of the odd coordinates occur equally often. Four of them have the required parity, so

$$|\mathcal{R}_{\mathrm{mix}}(n)| = 16\sigma(m) = \frac{2}{3}R(n). \tag{2.2}$$

For $p \in \mathcal{P}_3$, let $b_p(n)$ count the elements of $\mathcal{R}_{\mathrm{mix}}(n)$ for which

$$(p \mid x_1 \text{ and } p \mid x_2) \quad \text{or} \quad (p \mid x_3 \text{ and } p \mid x_4).$$

Since -1 is a quadratic nonresidue modulo p, the implication $p \mid x^2 + y^2 \implies p \mid x, y$ holds. Consequently, any representation outside all these exceptional sets supplies two positive odd summands in $\mathcal{A}$. It is therefore enough to prove

$$\sum_{p \in \mathcal{P}_3} b_p(n) < \frac{2}{3}R(n). \tag{2.3}$$

3. A uniform quaternionic estimate

Proposition 3.1. *For every $p \in \mathcal{P}_3$,*

$$\frac{b_p(n)}{R(n)} \le \frac{2}{p(p-1)} + \mathbf{1}_{p>3}\frac{\tau(m)\sqrt{m}}{3\sigma(m)}. \tag{3.1}$$

The estimate follows from a Hecke action on a finite quotient associated with the Hurwitz order.

3.1. **The Hurwitz order and its finite quotient.** Let $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ be the Hamilton quaternion algebra, where $i^2 = j^2 = -1$ and $k = ij = -ji$. Its reduced norm is

$$\mathrm{nrd}(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2.$$

The Hurwitz order is

$$\mathcal{H} = \mathbb{Z}^4 \ \cup \ (\mathbb{Z} + \tfrac{1}{2})^4,$$

with coordinates interpreted in the basis $1, i, j, k$. Its 24 units are the eight coordinate units and the sixteen elements $(\pm 1 \pm i \pm j \pm k)/2$.

The order $\mathcal{H}$ is norm-Euclidean. Indeed, rounding four real coordinates to integers gives a remainder of norm at most 1. Equality requires all four coordinates to be half-integers, in which case a Hurwitz half-integer gives remainder zero. Euclidean division implies that every right ideal is principal. In particular, the right ideal class number of $\mathcal{H}$ is one.

Let $Q_m = \{\alpha \in \mathcal{H} : \mathrm{nrd}(\alpha) = m\}$. Right multiplication by $1 + i$ is a bijection

$$Q_m \longrightarrow \mathcal{R}(2m). \tag{3.2}$$

For the inverse, divide an integral quaternion of norm $2m$ by $1+i$. The new coordinates are halves of the sums and differences in two coordinate pairs. The two odd coordinates of the original quaternion ensure that all four new coordinates are integers or all four are strict half-integers. Thus the inverse belongs to $\mathcal{H}$.

Fix $p \in \mathcal{P}_3$ with $p \nmid m$. The algebra B splits at every odd prime, and reduction identifies $\mathcal{H}/p\mathcal{H}$ with $M_2(\mathbb{F}_p)$, with reduced norm corresponding to determinant. Write

$$G_p = \mathrm{PGL}_2(\mathbb{F}_p), \qquad \rho_p : \{\alpha \in \mathcal{H} : p \nmid \mathrm{nrd}(\alpha)\} \longrightarrow G_p.$$

Let $\Gamma_p = \rho_p(\mathcal{H}^\times)$ and $Y_p = \Gamma_p \backslash G_p$. The only units with scalar reduction are ± 1, so

$$|\Gamma_p| = 12, \qquad |Y_p| = \frac{p(p^2-1)}{12}. \tag{3.3}$$

We equip $\mathbb{C}[Y_p]$ with the counting inner product.

3.2. **The Hecke operator and its spectral bound.** For m odd and $p \nmid m$, define

$$(T_m f)(\Gamma_p g) = \frac{1}{24} \sum_{\alpha \in Q_m} f(\Gamma_p \rho_p(\alpha) g). \tag{3.4}$$

Right multiplication by a unit permutes the left-unit classes in Q_m, so this is well-defined. It commutes with right translation by G_p. Quaternion conjugation permutes Q_m and gives projective inversion, which proves self-adjointness. Equations (2.1) and (3.2) give $T_m \mathbf{1} = \sigma(m)\mathbf{1}$.

The function

$$\chi_p(\Gamma_p g) = \left(\frac{\det(g)}{p}\right)$$

is well-defined because a scalar changes the determinant by a square and every element of Γ_p has square determinant. It satisfies $T_m \chi_p = (\frac{m}{p})\sigma(m)\chi_p$.

Lemma 3.2. *On $\{\mathbf{1}, \chi_p\}^\perp$, the operator norm of T_m is at most $\tau(m)\sqrt{m}$.*

Proof. Let $\mathrm{PB}^\times$ denote the algebraic group of projective units of B. At a finite prime $\ell \neq p$, take the projective image of $\mathcal{H}_\ell^\times$ as the local level. At p, take the kernel of reduction from $\mathrm{PGL}_2(\mathbb{Z}_p)$ to G_p. Denote the product of these compact open subgroups by $U(p)$. The class-number-one property gives

$$\mathrm{PB}^\times(\mathbb{Q}) \backslash \mathrm{PB}^\times(\mathbb{A}_f) / U(p) \simeq Y_p. \tag{3.5}$$

To see the stabilizer, choose an integral representative at every finite place. A rational quaternion carrying one such representative to another can, after rational rescaling, be taken to be a Hurwitz unit. Its remaining action at p is precisely Γ_p.

The usual unramified Hecke correspondence of index m on (3.5) is (3.4). In fact, its local right cosets at $\ell^e \parallel m$ specify integral right ideals of reduced norm ℓ^e. Combining these local ideals gives the integral right ideals of reduced norm m. Each is $\alpha\mathcal{H}$ for an $\alpha \in Q_m$, unique up to right multiplication by a unit. Returning to integral representatives gives $\rho_p(\alpha^{-1})$ at p. Conjugation sends these right-unit classes to the left-unit classes in (3.4), since projectively $\alpha^{-1} = \overline{\alpha}$.

One-dimensional automorphic representations factor through the reduced norm. Their restrictions to Y_p depend only on the determinant in $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$, so lie in the span of $\mathbf{1}$ and χ_p. The Jacquet–Langlands correspondence transfers the remaining representations to weight-two cuspidal representations, unramified at every prime dividing m [5, §16]. This use of the correspondence and the weight-two spectral bound is also described in [3, §8.4].

By Ramanujan–Petersson, at an unramified prime ℓ the normalized Satake parameters u_ℓ, v_ℓ have absolute value 1 [1]. In the normalization of (3.4), the index-ℓ^e eigenvalue is

$$\ell^{e/2} \sum_{r=0}^{e} u_\ell^r v_\ell^{e-r}.$$

The triangular cosets with diagonal (ℓ^r, ℓ^{e-r}) have multiplicity ℓ^r and spherical factor $\ell^{(e-2r)/2}$. Their product is $\ell^{e/2}$, giving the displayed normalization. The eigenvalue is at most $(e+1)\ell^{e/2}$ in absolute value. Multiplication over $\ell^e \parallel m$ proves the lemma. □

3.3. **Averaging over a torus normalizer.** Since $p \equiv 3 \pmod 4$, the subalgebra $\mathbb{F}_p[i]$ is the field $\mathbb{F}_{p^2}$. Let

$$C_p = \mathbb{F}_p[i]^\times / \mathbb{F}_p^\times \subset G_p, \qquad K_p = C_p \cup C_p \rho_p(j).$$

Conjugation by j induces the nontrivial field automorphism, so K_p is a subgroup of order $2(p+1)$. An invertible quaternion has its first or its second coordinate pair zero modulo p exactly when its projective reduction belongs to K_p. Since $\rho_p(1+i) \in C_p$, multiplication by $1+i$ preserves this condition.

The intersection $\Gamma_p \cap K_p$ consists of the four projective classes of $1, i, j, k$. Let

$$\mathcal{O}_p = \{\Gamma_p k : k \in K_p\}, \quad f_p = \mathbf{1}_{\mathcal{O}_p}, \quad \mu_p = \frac{|\mathcal{O}_p|}{|Y_p|} = \frac{6}{p(p-1)}.$$

There are $(p+1)/2$ points in $\mathcal{O}_p$. Each left-unit class whose reduction lies in $\mathcal{O}_p$ has exactly eight elements reducing into K_p. Counting all representations therefore gives

$$b_p(n) \le 8(T_m f_p)(\Gamma_p). \tag{3.6}$$

The function f_p is invariant under right translation by K_p. The same is true of $T_m f_p$, hence

$$(T_m f_p)(\Gamma_p) = \frac{\langle f_p, T_m f_p \rangle}{|\mathcal{O}_p|}. \tag{3.7}$$

The norm map $\mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$ is surjective. The orbit $\mathcal{O}_p$ therefore has equally many points in the two determinant classes. Thus $f_p - \mu_p \mathbf{1}$ is orthogonal to both $\mathbf{1}$ and χ_p, and

$$\|f_p - \mu_p \mathbf{1}\|_2^2 = |\mathcal{O}_p|(1-\mu_p).$$

Lemma 3.2 and (3.7) imply

$$(T_m f_p)(\Gamma_p) \le \sigma(m)\mu_p + \tau(m)\sqrt{m}(1-\mu_p). \tag{3.8}$$

For $p = 3$ one has $\mu_p = 1$, so the second term vanishes. Combining (3.6) and (3.8) with $R(n) = 24\sigma(m)$ proves Proposition 3.1 when $p \nmid m$.

Completion of the proof of Proposition 3.1. Suppose $p \mid m$. If a coordinate pair is divisible by p, the other pair has sum of squares zero modulo p, so all four coordinates are divisible by p. Hence $b_p(n) = 0$ when $p^2 \nmid m$ and $b_p(n) = 16\sigma(m/p^2)$ otherwise. Writing $m = p^e u$ gives

$$\frac{\sigma(m/p^2)}{\sigma(m)} = \frac{p^{e-1}-1}{p^{e+1}-1} < \frac{1}{p^2}.$$

It follows that $b_p(n)/R(n) \le 2/(3p^2) \le 2/[p(p-1)]$. □

4. Large primes and elementary lattice counting

For $t \ge 0$, let $N_{\mathrm{mix}}(t)$ be the number of signed, ordered pairs $(x, y) \in \mathbb{Z}^2$ with opposite parity and $x^2 + y^2 \le t$.

Lemma 4.1. *For every $t \ge 0$, one has $N_{\mathrm{mix}}(t) \le 2(t+1)$.*

Proof. Each orbit under quarter-turns has four elements and a unique representative with $x > 0$ and $y \ge 0$. Write

$$x + y = 2u + 1, \qquad x - y = 2v + 1, \qquad u \ge 0, \quad -u \le v \le u.$$

Assign to this pair the positive integer $L = u^2 + u + v + 1$. For fixed u, these labels run from $u^2 + 1$ to $(u+1)^2$. The labels are therefore distinct. Moreover,

$$\frac{x^2 + y^2 + 1}{2} = L + v^2 \ge L.$$

At most $\lfloor (t+1)/2 \rfloor$ labels can occur. Multiplication by four gives the claimed upper bound. □

Define

$$M(n) = \max_{1\le u\le n} \prod_{\substack{q^e \| u \\ q\equiv 1 \pmod 4}} (e+1).$$

The two-square formula implies $r_2(u) \le 4M(n)$ for $1 \le u \le n$, where r_2 counts signed, ordered representations.

Lemma 4.2. *For every $P \ge 3$,*

$$\frac{1}{R(n)} \sum_{\substack{p>P \\ p\in\mathcal{P}_3}} b_p(n) \le \frac{4}{3} M(n) \left(\sum_{\substack{p>P \\ p\in\mathcal{P}_3}} \frac{1}{p^2} + \frac{\#\{p \in \mathcal{P}_3 : P < p \le \sqrt{n}\}}{n} \right). \tag{4.1}$$

Proof. If p divides the first coordinate pair, divide that pair by p. Lemma 4.1 leaves at most $2(n/p^2+1)$ possibilities. The other pair has positive norm, because its coordinates have opposite parity, and has at most $4M(n)$ representations. Accounting for either pair gives

$$b_p(n) \le 16M(n)(n/p^2+1).$$

Such a prime is at most $\sqrt{n}$, since the pair it divides is nonzero. Sum this estimate and use $R(n) = 24\sigma(m) \ge 12n$. □

5. Explicit arithmetic estimates

Lemma 5.1. *Under the hypotheses of Lemma 2.1,*

$$\frac{\tau(m)m}{\sigma(m)} \le \frac{23}{10} m^{1/5}, \qquad M(n) \le \frac{11}{5} n^{1/5}. \tag{5.1}$$

Proof. For $p^e \| m$, $e \ge 1$, one has

$$\frac{(e+1)p^e}{\sigma(p^e)p^{e/5}} \le \frac{p}{p+1} \frac{e+1}{p^{e/5}}.$$

For the second bound, the corresponding local factor is $(e+1)/q^{e/5}$. At a prime at least 32, both factors are at most 1, since $e+1 \le 2^e \le p^{e/5}$.

For smaller primes, the ratio of successive values of $(e+1)/p^{e/5}$ is $(e+2)/((e+1)p^{1/5})$, which decreases with e. The maximizing positive exponent is therefore determined by $(e+2)^5 \le p(e+1)^5$. The required values are

$p \in \mathcal{P}_3$, $p < 32$	3	7	11	19	23	31
Maximizing positive e	4	2	1	1	1	1
$q \equiv 1 \pmod 4$, $q < 32$	5	13	17	29		
Maximizing positive e	2	1	1	1		

Taking the maximum with 1 allows each prime to be absent. The products of the fifth powers of the resulting local bounds are

$$C_1^5 = \frac{183143120027364343}{2849934139195392} < \left(\frac{23}{10}\right)^5,$$
$$C_2^5 = \frac{7962624}{160225} < \left(\frac{11}{5}\right)^5.$$

Multiplication over the prime factors proves both assertions. □

Lemma 5.2. *The following bounds hold for real $t \geq 0$ and $P \geq 3$.*

$$\#\{p \in \mathcal{P}_3 : 3 < p \leq t\} \leq \frac{2t}{15} + 1, \tag{5.2}$$

$$\sum_{\substack{p>P \\ p\in\mathcal{P}_3}} \frac{1}{p^2} \leq \frac{2}{15P} + \frac{2}{P^2}, \tag{5.3}$$

$$2\sum_{p\in\mathcal{P}_3} \frac{1}{p(p-1)} < \frac{21}{50}. \tag{5.4}$$

Proof. Every prime in $\mathcal{P}_3$ exceeding 3 belongs to one of the eight residue classes

$$\mathcal{S} = \{7, 11, 19, 23, 31, 43, 47, 59\} \pmod{60}.$$

Let $A(t)$ count the positive integers at most t in these classes. Checking the eight jumps in one period gives

$$-\frac{14}{15} \leq A(t) - \frac{2t}{15} \leq \frac{14}{15}.$$

Periodicity extends the bound to every $t \geq 0$, and proves (5.2). For $t \geq P$ it also gives

$$A(t) - A(P) \leq \frac{2}{15}(t - P) + 2.$$

Partial summation yields

$$\sum_{\substack{k>P \\ k \bmod 60\in\mathcal{S}}} \frac{1}{k^2} = 2\int_P^\infty \frac{A(t) - A(P)}{t^3}\, dt \leq \frac{2}{15P} + \frac{2}{P^2}.$$

For $P \geq 3$, this set contains all the primes in (5.3). Finally, direct summation through 60 gives

$$2\sum_{p\in\mathcal{P}_3} \frac{1}{p(p-1)} \leq \sum_{p\in\{3,7,11,19,23,31,43,47,59\}} \frac{2}{p(p-1)} + \frac{120}{59}\left(\frac{2}{15\cdot 60} + \frac{2}{60^2}\right) < \frac{21}{50}.$$

Here $p/(p-1) \leq 60/59$ for $p > 60$, so (5.3) bounds the remainder. □

6. The analytic range

Proposition 6.1. *Suppose $n = 2m \geq 64^4$, where m is odd and all its prime divisors belong to $\mathcal{P}_3$. Then $n \in \mathcal{A} + \mathcal{A}$.*

Proof. Set $X = n^{1/4} \geq 64$ and $P = 2X$. Proposition 3.1, Lemma 5.1, and (5.2) give

$$\frac{1}{R(n)} \sum_{\substack{p\leq P \\ p\in\mathcal{P}_3}} b_p(n) \leq \frac{21}{50} + \frac{\tau(m)\sqrt{m}}{3\sigma(m)}\left(\frac{4X}{15} + 1\right)$$

$$\leq \frac{21}{50} + \frac{23}{30}\, 2^{3/10} X^{-1/5}\left(\frac{4}{15} + \frac{1}{X}\right). \tag{6.1}$$

For the large primes, Lemmas 4.2–5.2 give

$$\frac{1}{R(n)} \sum_{\substack{p>P \\ p\in\mathcal{P}_3}} b_p(n) \leq \frac{44}{15} X^{4/5}\left(\frac{1}{15X} + \frac{1}{2X^2} + \frac{2}{15X^2} + \frac{1}{X^4}\right)$$

$$= \frac{44}{15} X^{-1/5}\left(\frac{1}{15} + \frac{19}{30X} + \frac{1}{X^3}\right). \tag{6.2}$$

The prime-count term in (4.1) was bounded by $2/(15\sqrt{n}) + 1/n$.

For $X \geq 64$,

$$X^{-1/5} \leq \frac{4}{9}, \qquad 2^{3/10} < \frac{5}{4}, \qquad X^{-1} \leq \frac{1}{64}.$$

The first two inequalities follow by raising to the fifth and tenth powers. Adding (6.1) and (6.2) now gives

$$\begin{aligned}\frac{1}{R(n)} \sum_{p \in \mathcal{P}_3} b_p(n) &\leq \frac{21}{50} + \frac{23}{30} \cdot \frac{5}{4} \cdot \frac{4}{9} \left(\frac{4}{15} + \frac{1}{64} \right) \\ &\quad + \frac{44}{15} \cdot \frac{4}{9} \left(\frac{1}{15} + \frac{19}{30 \cdot 64} + \frac{1}{64^3} \right) \\ &= \frac{21235493}{33177600} < \frac{2}{3}.\end{aligned}$$

Equations (2.2) and (2.3) therefore supply the required representation. □

7. The finite range

We give the finite arithmetic certificate in terms of binary indicators and finite sets. Put $H = 2^{22} - 1 = 4{,}194{,}303$ and define

$$\varepsilon_j = \prod_{\substack{p \leq 4096 \\ p \in \mathcal{P}_3}} \left(1 - \left\lfloor \frac{4j+1}{p} \right\rfloor + \left\lfloor \frac{4j}{p} \right\rfloor \right) \quad (0 \leq j \leq H), \qquad \varepsilon_j = 0 \quad (j < 0). \tag{7.1}$$

Each factor is 0 if $p \mid 4j+1$ and is 1 otherwise. Thus $\varepsilon_j \in \{0, 1\}$.

Lemma 7.1. *For $0 \leq j \leq H$, one has $\varepsilon_j = 1$ exactly when $4j + 1 \in \mathcal{A}$.*

Proof. The integer $4j + 1 \leq 64^4 - 3$ is odd and congruent to 1 modulo 4. Its prime factors belonging to $\mathcal{P}_3$ occur an even number of times, counting multiplicity. If any occur, at least two occur. At least one of these factors is then no larger than $\sqrt{4j+1} < 4096$. Formula (7.1) detects precisely this possibility. □

Let $J = \{0 \leq i \leq 78 : \varepsilon_i = 1\}$. The corresponding possible summands are

$$\begin{aligned}\{4i + 1 : i \in J\} = \{&1, 5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 73, 85, 89, 97, \\ &101, 109, 113, 125, 137, 145, 149, 157, 169, 173, 181, 185, \\ &193, 197, 205, 221, 229, 233, 241, 257, 265, 269, 277, 281, \\ &289, 293, 305, 313\}.\end{aligned}$$

For $1 \leq a \leq 313$, $a \equiv 1 \pmod 4$, define the exact integer

$$U(a) = \sum_{k=0}^{H} \prod_{i=0}^{(a-1)/4} (1 - \varepsilon_i \varepsilon_{k-i}). \tag{7.2}$$

It counts the indices still unrepresented when the first summand is at most a. Table 1 records successive values of (7.2); all quantities are integers.

The evaluation in the table can equivalently be performed by the following finite-set recurrence, which specifies every removal. Start with $C_0 = \{0, 1, \ldots, H\}$. In increasing order, for each $i \in J$ replace the current set C by

$$C \setminus \{k : i \leq k \leq H,\ \varepsilon_{k-i} = 1\}. \tag{7.3}$$

The indicators themselves are obtained by starting with all indices retained and, for each of the 287 primes $p \leq 4096$ in $\mathcal{P}_3$, removing the progression

$$\frac{3p-1}{4}, \quad \frac{3p-1}{4} + p, \quad \frac{3p-1}{4} + 2p, \quad \ldots \quad \text{through } H.$$

TABLE 1. The finite arithmetic certificate. Each column pair gives an upper bound a for the first summand and the number $U(a)$ of indices remaining.

a	$U(a)$	a	$U(a)$	a	$U(a)$
1	2 849 643	101	6 561	229	8
13	1 261 334	149	756	277	2
29	364 708	193	57	289	1
61	71 867	205	23	313	0

There are 1,344,661 retained indices. The recurrence (7.3) ends with the empty set, as recorded by $U(313) = 0$.

Proposition 7.2. *For every $n \equiv 2 \pmod 4$ with $2 \le n < 64^4$, there are $a, b \in \mathcal{A}$ such that $n = a+b$. The smaller summand can be chosen at most 313.*

Proof. Write $n = 4k + 2$, where $0 \le k \le H$. Since $U(313) = 0$, one of the factors in the kth product in (7.2) vanishes. Thus $\varepsilon_i = \varepsilon_{k-i} = 1$ for some $0 \le i \le 78$ with $i \le k$. Lemma 7.1 gives

$$n = (4i + 1) + (4(k - i) + 1) \in \mathcal{A} + \mathcal{A}.$$

One of these summands is at most 313. □

Proof of Theorem 1.1. Use Lemma 2.1 to write $n = g(2m_0)$ with $g \in \mathcal{A}$ and every prime divisor of m_0 in $\mathcal{P}_3$. Proposition 6.1 applies if $2m_0 \ge 64^4$. Proposition 7.2 applies otherwise. In both cases, multiply the resulting two summands by g. □

ACKNOWLEDGMENT

OpenAI Codex generated the mathematical argument, performed the exact calculations, and drafted the manuscript under human direction.

REFERENCES

[1] P. Deligne, *La conjecture de Weil. I*, Publ. Math. Inst. Hautes Études Sci. **43** (1974), 273–307. doi:10.1007/BF02684373.

[2] R. Dietmann and C. Elsholtz, *Sums of two numbers having only prime factors congruent to one modulo four*, in *Number Theory Week 2017*, Banach Center Publications **118** (2019), 177–179. doi:10.4064/bc118-11.

[3] J. S. Ellenberg, P. Michel, and A. Venkatesh, *Linnik's ergodic method and the distribution of integer points on spheres*, in *Automorphic Representations and L-Functions*, Tata Institute of Fundamental Research Studies in Mathematics **22** (2013), 119–185. Author manuscript (§8.4).

[4] L. Euler, *Letter to Christian Goldbach, May 6, 1747*, Letter 115, in F. Lemmermeyer and M. Mattmüller (eds.), *Correspondence of Leonhard Euler with Christian Goldbach*, Opera Omnia, Series IVA, vol. 4, online edition, Bernoulli–Euler-Gesellschaft, Basel, 2016, 935–936. doi:10.12685/publbez.1.2016.

[5] H. Jacquet and R. P. Langlands, *Automorphic Forms on* GL(2), Lecture Notes in Mathematics **114**, Springer, Berlin, 1970, §16. doi:10.1007/BFb0058988.

Email address: howew@purdue.edu

Email address: huffma97@purdue.edu

Email address: jenwin@purdue.edu

Email address: kruerl@purdue.edu