This is the author's version of the paper.
The final publication has appeared in J. Number Theory 128 (2008), 1195–1210.

The binary Goldbach problem with one prime of the form $p = k^2 + l^2 + 1$

Kaisa Matomäki*

(Department of Mathematics, Royal Holloway, University of London, Egham, Surrey, TW20 0EX, United Kingdom)

Abstract

We prove that almost all integers $n \equiv 0$ or $4 \pmod 6$ can be written in the form $n = p_1 + p_2$, where $p_1 = k^2 + l^2 + 1$ with $(k, l) = 1$. The proof is an application of the half-dimensional and linear sieves with arithmetic information coming from the circle method and the Bombieri-Vinogradov prime number theorem.

1 Introduction

After Vinogradov's [10, 11] ground-breaking proof of the ternary Goldbach problem, several authors [2, 6, 8] proved in the late 1930's that almost all even numbers can be expressed as a sum of two primes. On the other hand Linnik [5] has proved that there exists infinitely many prime numbers of the form $p = k^2 + l^2 + 1$. We couple these two theorems by proving

Theorem 1. *Let*

$$\mathcal{N} = \{n \leq N \mid n \equiv 0 \ \textit{or} \ 4 \pmod 6\}.$$

If $E(N)$ is the number of numbers $n \in \mathcal{N}$ that cannot be expressed in the form $n = p_1 + p_2$ with $p_1 = k^2 + l^2 + 1$, $(k, l) = 1$, then

$$E(N) \ll N(\log N)^{-A}$$

for any $A > 0$ with the implied constant depending only on A.

We use sieve methods to pick out primes of the form $k^2 + l^2 + 1$ and the circle method to pick out primes satisfying $n - p \in \mathbb{P}$. The sieve method we use goes back to Iwaniec's [3] work on quadratic forms representing prime numbers.

Consider $n \leq N$, $n \equiv 0$ or $4 \pmod 6$. We can clearly assume that $n \geq N(\log N)^{-A}$. The set $\{k^2 + l^2 \mid (k, l) = 1\}$ consists of numbers with no prime

*Email address: k.s.matomaki@rhul.ac.uk
MSC (2000): 11N05, 11P32, 11P55

factors belonging to $\mathcal{P}_3 = \{p \in \mathbb{P} \mid p \equiv 3 \pmod 4\}$. Thus it is natural to attack our current problem by applying the half-dimensional sieve to the set

$$\mathcal{A} = \{p - 1 < N \mid p \equiv 3 \pmod 8, n - p \in \mathbb{P}\}.$$

As usual we write for a finite set $\mathcal{F} \subseteq \mathbb{N}$ and a set of primes $\mathcal{P}$

$$P(z) = \prod_{p \in \mathcal{P}, p < z} p \quad \text{and} \quad S(\mathcal{F}, \mathcal{P}, z) = |\{a \in \mathcal{F} \mid (a, P(z)) = 1\}|.$$

Then by writing $\mathcal{P}_{3,n} = \{p \in \mathbb{P} \mid p \equiv 3 \pmod 4, p \nmid n-1\}$ there are $S(\mathcal{A}, \mathcal{P}_{3,n}, N) + O(\log N)$ primes p such that $p = k^2 + l^2 + 1$, $(k, l) = 1$ and $n - p \in \mathbb{P}$. We will conclude in Section 7 that for $n \geq \frac{N}{(\log N)^A}$, $n \in \mathcal{N}$ we have

$$S(\mathcal{A}, \mathcal{P}_{3,n}, N) \gg \frac{n}{(\log n)^{5/2}} - |E(n)|,$$

where

$$\sum_{n \in \mathcal{N}} |E(n)|^2 \ll N^3/(\log N)^A,$$

which clearly implies the theorem.

As in earlier works [3, 12] on problems involving $p = k^2 + l^2 + 1$, we write for $z = N^{1/\alpha}, \alpha \in [2, 4)$

$$S(\mathcal{A}, \mathcal{P}_{3,n}, N) = S(\mathcal{A}, \mathcal{P}_{3,n}, z) - T, \tag{1}$$

and obtain a lower bound for $S(\mathcal{A}, \mathcal{P}_{3,n}, z)$ by the half dimensional sieve and an upper bound for T by the linear sieve. In both cases we take advantage of a linear form of the error term.

Since each element $a \in \mathcal{A}$ has an even number of prime factors belonging to $\mathcal{P}_{3,n}$ and $2 \| a$, we have for $\alpha < 4$

$$\begin{aligned} T = |\{p \leq N \mid p = 1 + 2up_1p_2,\ p_1, p_2 \in \mathcal{P}_{3,n}, p_1 \geq p_2 \geq N^{1/\alpha}, \\ p_0 \mid u \implies p_0 \equiv 1 \pmod 4, n - p \in \mathbb{P}\}| + O(\log N). \end{aligned}$$

Define

$$\begin{aligned} \mathcal{L} = \{l = 2up_2 \mid u \leq N^{1-2/\alpha}, p \mid u \implies p \equiv 1 \pmod 4, \\ N^{1/\alpha} \leq p_2 < (N/u)^{1/2}, p_2 \in \mathcal{P}_{3,n}\}, \end{aligned}$$

$$\mathcal{L}_n = \{l \in \mathcal{L} \mid (l, n-1) = 1\}$$

and for each $l \in \mathcal{L}$

$$\mathcal{M}_n(l) = \{m = lp_1 + 1 \mid p_1 l < N, p_1 \equiv 3 \pmod 4, n - m \in \mathbb{P}\}.$$

Then T is at most the number of primes in $\cup_{l \in \mathcal{L}_n} \mathcal{M}_n(l)$ together with an error term of the order $\log N$. Thus

$$T \leq \sum_{l \in \mathcal{L}_n} \Big(S(\mathcal{M}_n(l), \mathcal{P}_n(l), (N/l)^{1/4}) + O((N/l)^{1/4}) \Big),$$

where $\mathcal{P}_n(l) = \{p \in \mathbb{P} \mid (p, nl) = 1\}$.

2 Sieving lemmata

First we introduce some more sieve notation. For a squarefree d with all its prime factors in $\mathcal{P}$, we let $\mathcal{F}_d = \{n \mid dn \in \mathcal{F}\}$. Let

$$|\mathcal{F}_d| = \frac{\omega(d)}{d} X + r(\mathcal{F}, d),$$

where $X > 1$ is independent of d and $\omega(d)$ is a multiplicative function that satisfies the condition $0 < \omega(p) < p$ for each $p \in \mathcal{P}$. Define further

$$\Omega(z) = \prod_{p<z, p\in\mathcal{P}} \left(1 - \frac{\omega(p)}{p}\right).$$

We say that a sieve is of dimension κ if there exists a constant $K \geq 2$ such that for all $z > w \geq 2$ we have

$$\prod_{\substack{w\leq p<z \\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log z}{\log w}\right)^{\kappa} \left(1 + \frac{K}{\log w}\right).$$

Now we are ready to state the main theorem of the Rosser-Iwaniec sieve. It follows as Theorem 1 of [4] by an obvious modification to the argument in Section 3 of [4].

Lemma 2. *Let $s = \log Q / \log z$. Then we have for certain functions $F(s)$ and $f(s)$ depending on κ*

$$S(\mathcal{F}, \mathcal{P}, z) \leq X\Omega(z)(F(s) + o_K(1)) + \sum_{d<Q, d|P(z)} c_d r(\mathcal{F}, d)$$

and

$$S(\mathcal{F}, \mathcal{P}, z) \geq X\Omega(z)(f(s) + o_K(1)) + \sum_{d<Q, d|P(z)} c'_d r(\mathcal{F}, d),$$

where $c_d, c'_d \ll 1$ depend only on Q and κ but not on $|\mathcal{F}|$, $\mathcal{P}$ or ω.

We will need the lower bound in the half-dimensional ($\kappa = 1/2$) case and the upper bound for the linear ($\kappa = 1$) case. In the half-dimensional case we have for $1 \leq s \leq 3$

$$f(s) = \sqrt{\frac{e^\gamma}{\pi s}} \int_1^s \frac{dt}{\sqrt{t(t-1)}},$$

where γ is Euler's constant. In the linear case we have $F(s) = \frac{2e^\gamma}{s}$ for $1 \leq s \leq 3$.

The following Bombieri-Vinogradov type result gives the arithmetical information needed for the applications of the sieve.

Lemma 3. *Let $L < N^{\beta}$ with $\beta < 1$ and $|d_{k,l}| \le 1$. Let $a_{k,l}$ be any sequence satisfying $(a_{k,l}, k) = 1$ for every k and l. Then for any $A > 0$ there exists a constant $A' > 0$ such that if for every $l \le L$ we have $Q_l \le (N/l)^{1/2}/(\log(N/l))^{A'}$, then*

$$\sum_{n=1}^{N} \left| \sum_{l \le L} \sum_{k \le Q_l} d_{k,l} \left(\sum_{\substack{p_1 \equiv a_{k,l} \, (\mathrm{mod}\, k) \\ p_1 l + p_2 = n}} 1 - \frac{\mathfrak{S}_n(l,k,a_{k,l})}{l\phi(k)} M_n(l) \right) \right|^2 \ll \frac{N^3}{(\log N)^A},$$

where the implied constant depends only on A and β,

$$M_n(l) = \sum_{m=2l}^{n-2} \frac{1}{\log \frac{m}{l} \log(n-m)}$$

and

$$\mathfrak{S}_n(l,k,a_{k,l}) = \prod_{p \nmid kln} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid kln} \left(1 + \frac{1}{p-1}\right) \delta((n - la_{k,l}, k)(n,l))$$

with $\delta(n)$ the Kronecker delta symbol.

Proof. We can add summation conditions $(n,l) = (n - la_{k,l}, k) = 1$ since if this does not hold, then $\mathfrak{S}_n(l,k,a_{k,l}) = 0$ and for any $n \in \mathcal{N}$ at most one pair (p_1, p_2) of primes satisfies the conditions $p_1 \equiv a_{k,l} \, (\mathrm{mod}\, k)$ and $p_1 l + p_2 = n$.

By writing

$$f_{k,l}(\alpha) = \sum_{\substack{pl \le N \\ p \equiv a_{k,l} \, (\mathrm{mod}\, k)}} e(\alpha p l) \quad \text{and} \quad f(\alpha) = f_{1,1}(\alpha)$$

we have

$$\sum_{\substack{p_1 \equiv a_{k,l} \, (\mathrm{mod}\, k) \\ p_1 l + p_2 = n}} 1 = \int_0^1 f_{k,l}(\alpha) f(\alpha) e(-n\alpha) d\alpha = I.$$

Next we divide the integral into major arcs and minor arcs. For that we write $Q = (\log N)^{A+14}$, $\eta = \frac{N}{Q}$,

$$\mathfrak{M} = \bigcup_{q \le Q} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q-1} \left(\frac{a}{q} - \frac{1}{\eta q}, \frac{a}{q} + \frac{1}{\eta q} \right) \quad \text{and} \quad \mathfrak{m} = \left(-\frac{1}{\eta}, 1 - \frac{1}{\eta} \right) \setminus \mathfrak{M}.$$

Then $I = I_{\mathfrak{M}} + I_{\mathfrak{m}}$ where $I_{\mathfrak{M}}$ corresponds to the integral on $\mathfrak{M}$ and $I_{\mathfrak{m}}$ to the integral on $\mathfrak{m}$. The claim follows by proving that

$$\sum_{n=1}^{N} \left| \sum_{l \le L} \sum_{k \le Q_l} d_{k,l} \left(I_{\mathfrak{M}} - \frac{\mathfrak{S}_n(l,k,a_{k,l})}{l\phi(k)} M_n(l) \right) \right|^2 \ll \frac{N^3}{(\log N)^A} \qquad (2)$$

and

$$\sum_{n=1}^{N}\left|\sum_{l\le L}\sum_{k\le Q_l} d_{k,l} I_{\mathfrak{m}}\right|^2 \ll \frac{N^3}{(\log N)^A}. \tag{3}$$

The proof of these occupy the following two sections.

3 Major arcs

Consider first the contribution from the major arcs. Our argument is a modification of Tolev's [7] argument. We have

$$I_{\mathfrak{M}} = \sum_{q\le Q}\sum_{a=0}^{q-1}{}^{*} I(a,q),$$

where here and later * restricts the summation to a coprime to q and

$$I(a,q)=\int_{-1/(\eta q)}^{1/(\eta q)} f_{k,l}\left(\frac{a}{q}+\alpha\right) f\left(\frac{a}{q}+\alpha\right) e\left(-n\left(\frac{a}{q}+\alpha\right)\right) d\alpha.$$

Let

$$\Delta(x,q)=\max_{(a,q)=1}\max_{y\le x}\left|\pi(y,q,a)-\frac{1}{\phi(q)}\int_2^y \frac{dt}{\log t}\right|$$

and for $(m,q)=1$, $m\equiv a_{k,l} \pmod{(k,q)}$ let $b_{k,l}$ be the unique $\pmod{[k,q]}$ solution to the system of congruences

$$\begin{cases} x\equiv a_{k,l} & \pmod{k},\\ x\equiv m & \pmod{q}.\end{cases}$$

Then for $q\le Q$, $(a,q)=1$ we have

$$f_{k,l,x}\left(\frac{a}{q}\right) = \sum_{\substack{p\le x\\ p\equiv a_{k,l}\ \ (k)}} e\left(\frac{apl}{q}\right) = \sum_{\substack{1\le m\le q\\ m\equiv a_{k,l}\ \ ((k,q))}}^{*} e\left(\frac{alm}{q}\right) \sum_{\substack{p\le x\\ p\equiv b_{k,l}\ \ ([k,q])}} 1 + O(q)$$

$$= \sum_{\substack{1\le m\le q\\ m\equiv a_{k,l}\ \ ((k,q))}}^{*} e\left(\frac{alm}{q}\right)\left(\frac{1}{\phi([k,q])}\int_2^x \frac{dt}{\log t} + O(\Delta(x,[k,q]))\right) + O(q).$$

Thus by partial summation we have for $|\alpha|\le \frac{1}{q\eta}$

$$f_{k,l}\left(\frac{a}{q}+\alpha\right) = f_{k,l}\left(\frac{a}{q}\right)e(\alpha N) - \int_2^{N/l} f_{k,l,y}\left(\frac{a}{q}\right)\frac{d}{dy}e(\alpha l y)dy$$

$$= \frac{c_{k,l}(a,q)}{\phi([k,q])}\int_2^{N/l}\frac{e(\alpha l y)}{\log y}dy + O\left(Q\Delta\left(\frac{N}{l},[k,q]\right)\right),$$

where

$$c_{k,l}(a,q)=\sideset{}{^*}\sum_{\substack{1\le m\le q\\ m\equiv a_{k,l} \pmod{(k,q)}}} e\left(\frac{alm}{q}\right).$$

Here

$$\int_2^{N/l}\frac{e(\alpha ly)}{\log y}dy=\frac{1}{l}\int_{2l}^{N}\frac{e(\alpha y)}{\log(y/l)}dy=\frac{1}{l}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}+\frac{1}{l}\int_{2l}^{N}\frac{e(\alpha y)}{\log(y/l)}d\{y\}$$

$$=\frac{1}{l}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}+O\left(\frac{1+|\alpha|N}{l}\right)=\frac{1}{l}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}+O\left(\frac{Q}{ql}\right).$$

Thus

$$f_{k,l}\left(\frac{a}{q}+\alpha\right)=\frac{c_{k,l}(a,q)}{l\phi([k,q])}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log m/l}+O\left(Q\Delta\left(\frac{N}{l},[k,q]\right)\right)$$

and in particular evaluation of the Ramanujan sum $c_{1,1}(a,q)=\mu(q)$ for $(a,q)=1$ and an application of the prime number theorem give

$$f\left(\frac{a}{q}+\alpha\right)=\frac{\mu(q)}{\phi(q)}\sum_{m=2}^{N}\frac{e(\alpha m)}{\log m}+O(N\exp(-c(\log N)^{1/2})).$$

By substituting these into the definition of $I(a,q)$ we get

$$I(a,q)=\frac{\mu(q)c_{k,l}(a,q)}{l\phi([k,q])\phi(q)}e\left(-\frac{an}{q}\right)\int_{-1/(\eta q)}^{1/(\eta q)}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}\sum_{m=2}^{N}\frac{e(\alpha m)}{\log m}e(-n\alpha)d\alpha$$
$$+O\left(\frac{N}{kl}\exp(-c(\log N)^{1/2})+\frac{Q^2}{q\phi(q)}\Delta\left(\frac{N}{l},[k,q]\right)\right).$$

For $0<|\alpha|<1/2$ we have by partial summation

$$\left|\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}\right|\ll\max_{x\le N}\left|\sum_{m=1}^{x}e(\alpha m)\right|\ll\frac{1}{|\alpha|}.$$

Thus using this for l and $l=1$ we get

$$\int_{-1/(\eta q)}^{1/(\eta q)}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}\sum_{m=2}^{N}\frac{e(\alpha m)}{\log m}e(-n\alpha)d\alpha$$
$$=\int_{-1/2}^{1/2}\sum_{m=2l}^{N}\frac{e(\alpha m)}{\log(m/l)}\sum_{m=2}^{N}\frac{e(\alpha m)}{\log m}e(-n\alpha)d\alpha+O(\eta q)=M_n(l)+O(\eta q).$$

Then by writing

$$b_{k,l}(q)=\sideset{}{^*}\sum_{a=0}^{q-1}c_{k,l}(a,q)e\left(-\frac{na}{q}\right)$$

we have for $q \le Q$

$$\sum_{a=0}^{q-1}{}^{*} I(a,q) = \frac{\mu(q)b_{k,l}(q)}{l\phi(q)\phi([k,q])}(M_n(l) + O(\eta q))$$
$$+ O\left(\frac{N}{kl}\exp(-c(\log N)^{1/2}) + \frac{Q^2}{q}\Delta\left(\frac{N}{l}, [k,q]\right)\right)$$

We consider first the main term. There the function $b_{k,l}(q)$ is multiplicative with respect to q and by the assumption $(n,l) = (n - la_{k,l}, k) = 1$ we have

$$b_{k,l}(p) = \begin{cases} 1, & \text{if } p \nmid kln, \\ 1-p, & \text{if } p \nmid k,\ p \mid ln, \\ -1, & \text{if } p \mid k. \end{cases}$$

Let further

$$\lambda_{k,l}(q) = \frac{\mu(q)b_{k,l}(q)\phi(k)}{\phi(q)\phi([k,q])} = \frac{\mu(q)b_{k,l}(q)\phi((k,q))}{\phi(q)^2},$$

which is a multiplicative function of q. We also notice that for a square-free number q we have $|b_{k,l}(q)\phi((k,q))| = \phi((kln,q))$.

Then we have an Euler product

$$\sum_{q \le Q} \lambda_{k,l}(q) = \sum_{q \in \mathbb{N}} \lambda_{k,l}(q) + O\left(\sum_{q>Q} |\lambda_{k,l}(q)|\right)$$
$$= \mathfrak{S}_n(l,k,a_{k,l}) + O\left(\sum_{q>Q} \frac{\phi((kln,q))}{\phi(q)^2}\right).$$

Thus

$$I_{\mathfrak{M}} = \frac{\mathfrak{S}_n(l,k,a_{k,l})}{l\phi(k)} M_n(l) + O\Bigg(\sum_{q>Q} \frac{\phi((kln,q))}{l\phi(k)\phi(q)^2} M_n(l) + \sum_{q \le Q} \frac{\eta q \phi((kln,q))}{l\phi(k)\phi(q)^2}$$
$$+ \sum_{q \le Q} \frac{N}{kl}\exp(-c(\log N)^{1/2}) + \sum_{q \le Q} \frac{Q^2}{q}\Delta\left(\frac{N}{l}, [k,q]\right)\Bigg)$$
$$= \frac{\mathfrak{S}_n(l,k,a_{k,l})}{l\phi(k)} M_n(l) + O(E_1 + E_2 + E_3 + E_4),$$

say. Write

$$\sum\nolimits_i = \frac{1}{\log N} \sum_{n \le N} \left(\sum_{l \le L} \sum_{k \le Q_l} E_i\right)^2.$$

Here the logarithmic factor allows us to change each $\phi(r)$ to r. Then the estimate (2) follows by showing that $\sum_i \ll \frac{N^3}{(\log N)^{A+1}}$ for $i = 1,2,3,4$.

Consider first $\sum_1$. Since

$$\sum_{q\in\mathbb{N}} \frac{(r,q)}{q^2} = \sum_{s|r}\sum_{q\in\mathbb{N}} \frac{s}{(qs)^2} \ll \log r,$$

we have

$$\sum\nolimits_1 \ll N^2 \sum_{n\le N}\left(\sum_{l\le L}\sum_{k\le Q_l}\sum_{q>Q}\frac{(kln,q)}{klq^2}\right)\left(\sum_{l\le L}\sum_{k\le Q_l}\frac{1}{kl}\sum_{q>Q}\frac{(kln,q)}{q^2}\right)$$
$$\ll N^3(\log N)^3\sum_{n\le N}\sum_{l\le L}\sum_{k\le N}\sum_{q>Q}\frac{(kln,q)}{klnq^2} \ll N^3(\log N)^3\sum_{r\le N^3}\frac{\tau_3(r)}{r}\sum_{q>Q}\frac{(r,q)}{q^2}.$$

Next we divide the summation according to $s=(r,q)\le Q$ or $s>Q$ getting

$$\sum\nolimits_1 \ll N^3(\log N)^3\Bigg(\sum_{s\le Q}\sum_{r\le N^3/s}\frac{\tau_3(rs)}{rs}\sum_{q>Q/s}\frac{s}{(qs)^2}$$
$$+\sum_{Q<s\le N^3}\sum_{r\le N^3/s}\frac{\tau_3(rs)}{rs}\sum_{q\in\mathbb{N}}\frac{s}{(qs)^2}\Bigg) \ll \frac{N^3(\log N)^9}{Q} \ll \frac{N^3}{(\log N)^{A+1}}.$$

Next we consider $\sum_2$. Since

$$\sum_{q\le Q}\frac{(r,q)}{q} = \sum_{s|r}\sum_{q\le Q/s}\frac{s}{qs} \ll \tau(r)\log N,$$

we have

$$\sum\nolimits_2 \ll \sum_{n\le N}\left(\sum_{l\le L}\sum_{k\le Q_l}\frac{\eta\tau(kln)}{kl}\log N\right)^2 \ll \frac{N^3(\log N)^{13}}{Q} \ll \frac{N^3}{(\log N)^{A+1}}.$$

We have trivially $\sum_3 \ll \frac{N^3}{(\log N)^{A+1}}$. Finally by the Bombieri-Vinogradov prime number theorem [1] we have for sufficiently large A'

$$\sum\nolimits_4 \ll NQ^6\left(\sum_{l\le L}\sum_{k\le Q_lQ}\Delta\left(\frac{N}{l},k\right)\right)^2 \ll \frac{N^3}{(\log N)^{A+1}}.$$

Thus (2) holds.

4 Minor arcs

In this section we show that (3) holds. In order to do that we first change the order of summation and integration giving

$$\sum_{n=1}^{N}\left|\sum_{l\le L}\sum_{k\le Q_l} d_{k,l}I_{\mathfrak{m}}\right|^2 = \sum_{n=1}^{N}\left|\int_{\mathfrak{m}}\left(f(\alpha)\sum_{l\le L}\sum_{k\le Q_l}d_{k,l}f_{k,l}(\alpha)\right)e(-n\alpha)d\alpha\right|^2.$$

By Bessel's inequality the right hand side is at most

$$\int_{\mathfrak{m}}\left|f(\alpha)\sum_{l\le L}\sum_{k\le Q_l} d_{k,l}f_{k,l}(\alpha)\right|^2 d\alpha \le \left(\max_{\alpha\in\mathfrak{m}}|f(\alpha)|\right)^2$$

$$\cdot \sum_{\substack{l_1\le L\\ l_2\le L}}\sum_{\substack{k_1\le Q_{l_1}\\ k_2\le Q_{l_2}}} |d_{k_1,l_1}d_{k_2,l_2}| \sum_{\substack{p_1l_1\le N\\ p_1\equiv a_{k_1,l_1}\quad (k_1)}}\sum_{\substack{p_2l_2\le N\\ p_2\equiv a_{k_2,l_2}\quad (k_2)}} \int_0^1 e(\alpha(l_1p_1-l_2p_2))d\alpha.$$

The integral on the right hand side disappears unless $p_1l_1 = p_2l_2$ and is 1 otherwise.

Consider first the contribution from summands with $p_1 = p_2$. Then $l_1 = l_2$ and thus by writing $k = [k_1, k_2]$ the contribution of these terms is

$$\ll \left(\max_{\alpha\in\mathfrak{m}}|f(\alpha)|\right)^2 \sum_{l\le L}\sum_{k\le Q_l^2}\tau_3(k)\sum_{\substack{pl\le N\\ p\equiv a_{k_1,k_2,l_1,l_2}\quad (k)}} 1$$

$$\ll \left(\max_{\alpha\in\mathfrak{m}}|f(\alpha)|\right)^2 \sum_{l\le L}\sum_{k\le N/l}\tau_3(k)\left(\frac{N}{kl}+1\right) \ll \left(\max_{\alpha\in\mathfrak{m}}|f(\alpha)|\right)^2 N(\log N)^4 \quad (4)$$

Consider then the contribution from the terms with $p_1 \ne p_2$. By writing $r = l_1p_1 = l_2p_2 = sp_1p_2$ we see that contribution from these terms is

$$\ll (\max_{\alpha\in\mathfrak{m}}|f(\alpha)|)^2|\mathcal{S}|, \quad (5)$$

where

$$\mathcal{S} = \big\{(s,p_1,p_2,k_1,k_2) \mid p_1 \equiv a_{k_1,sp_2} \quad (k_1), p_2 \equiv a_{k_2,sp_1} \quad (k_2),$$
$$k_1 \le \left(\tfrac{N}{sp_2}\right)^{1/2}, k_2 \le \left(\tfrac{N}{sp_1}\right)^{1/2}, sp_1p_2 \le N\big\}$$

We define further $\mathcal{S}(S,P_1,P_2,k_1,k_2) = \{(s,p_1,p_2,k_1,k_2) \in \mathcal{S} \mid s \sim S, p_1 \sim P_1, p_2 \sim P_2\}$, where $m \sim M \iff M \le m < 2M$. Then

$$|\mathcal{S}| \ll (\log N)^3 \sum_{k_1\le N^{1/2}}\sum_{k_2\le N^{1/2}} \max_{S,P_1,P_2}{}^{\dagger} |\mathcal{S}(S,P_1,P_2,k_1,k_2)|, \quad (6)$$

where † indicates the conditions

$$SP_1P_2 \le N, \quad SP_2 \le N/k_1^2 \quad \text{and} \quad SP_1 \le N/k_2^2.$$

Under these conditions

$$|\mathcal{S}(S,P_1,P_2,k_1,k_2)| \le S\left(\frac{P_1}{k_1}+1\right)\left(\frac{P_2}{k_2}+1\right) = \frac{SP_1P_2}{k_1k_2}+\frac{SP_1}{k_1}+\frac{SP_2}{k_2}+S$$

$$\le \frac{N}{k_1k_2}+\frac{N}{k_1k_2^2}+\frac{N}{k_1^2k_2}+\left(\frac{N}{P_2k_1^2}\right)^{1/2}\left(\frac{N}{P_1k_2^2}\right)^{1/2} \le \frac{4N}{k_1k_2}.$$

This together with (4), (5) and (6) implies

$$\sum_{n=1}^{N} \left| \sum_{l \le L} \sum_{k \le Q_l} d_{k,l} I_{\mathfrak{m}} \right|^2 \ll N(\log N)^5 \left(\max_{\alpha \in \mathfrak{m}} |f(\alpha)| \right)^2 .$$

This gives (3) since by Dirichlet's approximation theorem (Lemma 2.1 of [9]) and Theorem 3.1 of [9] we have

$$\max_{\alpha \in \mathfrak{m}} |f(\alpha)| \ll \frac{N(\log N)^4}{Q^{1/2}}.$$

□

5 A lower bound for $S(\mathcal{A}, \mathcal{P}_{3,n}, z)$

Proposition 4. *Let $1 \le \alpha \le 6$ and let $M_n(l)$ be defined as above. Then*

$$S(\mathcal{A}, \mathcal{P}_{3,n}, z) \ge \frac{3C_1(n)}{4\sqrt{\log N}} \int_1^{\alpha/2} \frac{dt}{\sqrt{t(t-1)}} M_n(1)(1+o(1)) + E_1(n),$$

where

$$C_1(n) = \prod_{\substack{p|n \\ p \equiv 1 \quad (4)}} \left(1 - \frac{1}{p-1}\right)^{-1} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|(n-1)n \\ p>3 \\ p \equiv 3 \quad (4)}} \left(1 - \frac{1}{p-2}\right)^{-1}$$
$$\cdot \prod_{\substack{p>3 \\ p \equiv 3 \quad (4)}} \frac{1 - \frac{1}{p-2}}{1 - \frac{1}{p}} \prod_{p \equiv 3 \quad (4)} \left(1 - \frac{1}{p^2}\right)^{1/2}$$

and

$$\sum_{n \in \mathcal{N}} |E_1(n)|^2 \ll N^3/(\log N)^A.$$

Proof. As mentioned above, we use the half-dimensional sieve. Let $n \in \mathcal{N}$. Let d be a squarefree integer with all the prime factors belonging to $\mathcal{P}_{3,n}$. Let a_d be the unique residue class $\pmod{8d}$ such that $a_d \equiv 3 \pmod 8$ and $a_d \equiv 1 \pmod d$. Then

$$|\mathcal{A}_d| = |\{p \in \mathbb{P} | p \equiv a_d \quad (8d), n - p \in \mathbb{P}\}| = \frac{\mathfrak{S}_n(1, 8d, a_d)}{4\phi(d)} M_n(1) + R_n(d)$$
$$= \frac{M_n(1)}{4\phi(d)} \prod_{p \nmid 8dn} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p | 8dn} \left(1 + \frac{1}{p-1}\right) \delta((n-3, 8)(n-1, d)) + R_n(d)$$
$$= \frac{\omega_n(d)}{d} X_n + R_n(d),$$

where

$$\frac{\omega_n(d)}{d} = \frac{1}{\phi(d)} \prod_{p \mid \frac{d}{(n,d)}} \frac{1+\frac{1}{p-1}}{1-\frac{1}{(p-1)^2}} = \frac{1}{\phi(d)} \prod_{p \mid \frac{d}{(n,d)}} \left(1 - \frac{1}{p-1}\right)^{-1}$$

and

$$\begin{aligned} X_n = &\frac{1}{4} \prod_{p \mid 2n} \left(1 + \frac{1}{p-1}\right) \prod_{p \nmid 2n} \left(1 - \frac{1}{(p-1)^2}\right) M_n(1) \\ = &\frac{1}{2} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid n, p>2} \left(1 - \frac{1}{p-1}\right)^{-1} M_n(1). \end{aligned}$$

Hence for $p \in \mathcal{P}_{3,n}$

$$\omega_n(p) = \begin{cases} \frac{p}{p-1}, & \text{if } p \mid n, \\ \frac{p}{p-2}, & \text{if } p \nmid n. \end{cases}$$

and

$$\begin{aligned} \Omega_n(z) = &\prod_{\substack{p \in \mathcal{P}_{3,n} \\ p<z}} \left(1 - \frac{\omega_n(p)}{p}\right) = \prod_{\substack{p<z, p \mid n \\ p \equiv 3 \quad (4)}} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{p<z, p \nmid (n-1)n \\ p \equiv 3 \quad (4)}} \left(1 - \frac{1}{p-2}\right) \\ = &(1+o(1)) \prod_{\substack{p \mid n \\ p \equiv 3 \quad (4)}} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{p \mid (n-1)n \\ p>3 \\ p \equiv 3 \quad (4)}} \left(1 - \frac{1}{p-2}\right)^{-1} \prod_{\substack{3<p<z \\ p \equiv 3 \quad (4)}} \left(1 - \frac{1}{p-2}\right). \end{aligned}$$

By writing $L(\chi, 1; y) = \prod_{p<y}(1 - \chi(p)/p)^{-1}$ with χ the non-trivial character $(\bmod 4)$, we have

$$\begin{aligned} \prod_{\substack{p<z \\ p \equiv 3 \,(\bmod 4)}} \left(1 - \frac{1}{p}\right) = &\sqrt{2L(\chi, 1; z) \prod_{\substack{p<z \\ p \equiv 3 \,(\bmod 4)}} \left(1 - \frac{1}{p^2}\right) \prod_{p<z} \left(1 - \frac{1}{p}\right)} \\ = &(1+o(1)) \sqrt{\frac{\alpha\pi}{2e^\gamma \log N}} \prod_{p \equiv 3 \,(\bmod 4)} \left(1 - \frac{1}{p^2}\right)^{1/2} \end{aligned}$$

by Mertens' formula and the fact $L(\chi, 1) = \frac{\pi}{4}$. Thus by the half-dimensional sieve (Lemma 2 with $\kappa = 1/2$) we have by choosing $Q = N^{1/2}/(\log N)^{A'}$

$$S(\mathcal{A}, \mathcal{P}_{3,n}, z) \geq \frac{3C_1(n)}{4\sqrt{\log N}} \int_1^{\alpha/2} \frac{dt}{\sqrt{t(t-1)}} M_n(1)(1+o(1)) + \sum_{d<Q} c'_d R_n(d).$$

Thus the claim follows from Lemma 3 with $L = 1$. □

6 An upper bound for T

Proposition 5. *Let $\alpha \geq 1$ and let T, $C_1(n)$ and $M_n(l)$ be defined as above. Then*

$$T \leq \frac{12C_1(n)W(\alpha)+o(1)}{(\log N)^{1/2}}M_n(1)+E_2(n),$$

where

$$W(\alpha) = \frac{\alpha}{8\sqrt{2}}\int_2^\alpha \frac{t-2+(t-1)\log(t-1)}{t^2(t-1)(1-t/\alpha)^{1/2}}dt$$

and

$$\sum_{n\in\mathcal{N}} |E_2(n)|^2 \ll N^3/(\log N)^A$$

Proof. We use the linear sieve to obtain an upper bound for T. Let $l \in \mathcal{L}$ and let d be a squarefree integer satisfying $(d,l)=1$. Let $a'_{d,l}$ be the unique residue class $\pmod{4d}$ such that $la'_{d,l} \equiv -1 \pmod d$ and $a'_{d,l} \equiv 3 \pmod 4$. Write

$$\begin{aligned}
&|\mathcal{M}_n(l)_d| = |\{p_1 \in \mathbb{P} \mid lp_1 \leq N, p_1 \equiv a'_{d,l} \pmod{4d}, n-1-lp_1 \in \mathbb{P}\}| \\
=&\frac{\mathfrak{S}_{n-1}(l,4d,a'_{d,l})}{2l\phi(d)}M_n(l)+R_n(l,d) = \frac{M_n(l)}{2l\phi(d)}\prod_{p\nmid 4dl(n-1)}\left(1-\frac{1}{(p-1)^2}\right) \\
&\cdot \prod_{p\mid 4dl(n-1)}\left(1+\frac{1}{p-1}\right)\delta((n-1-la'_{d,l},4d)(n-1,l))+R_n(l,d).
\end{aligned}$$

Then we have for $l \in \mathcal{L}_n$ and d such that all the prime factors of d belong to $\mathcal{P}_n(l)$

$$|\mathcal{M}_n(l)_d| = \frac{\omega_n(l,d)}{d}X_n(l)+R_n(l,d),$$

where

$$\frac{\omega_n(l,d)}{d} = \frac{1}{\phi(d)}\prod_{p\mid\frac{d}{(d,l(n-1))}}\frac{1+\frac{1}{p-1}}{1-\frac{1}{(p-1)^2}}$$

and

$$\begin{aligned}
X_n(l) =& \frac{M_n(l)}{2l}\prod_{p\nmid 4l(n-1)}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\mid 4l(n-1)}\left(1+\frac{1}{p-1}\right) \\
=&\frac{M_n(l)}{l}\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{p\mid l\\ p>2}}\left(1-\frac{1}{p-1}\right)^{-1}\prod_{p\mid n-1}\left(1-\frac{1}{p-1}\right)^{-1}.
\end{aligned}$$

Hence for $p \in \mathcal{P}_n(l)$

$$\omega_n(l,p) = \begin{cases} \frac{p}{p-1}, & \text{if } p \mid n-1, \\ \frac{p}{p-2}, & \text{if } p \nmid n-1. \end{cases}$$

and

$$\Omega_n(l,z) = \prod_{\substack{p\in\mathcal{P}_n(l)\\ p<z}}\left(1-\frac{\omega_n(l,p)}{p}\right) = \prod_{\substack{p|n-1\\ p\nmid l, p<z}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p\nmid l(n-1)n\\ p<z}}\left(1-\frac{1}{p-2}\right)$$

$$=3(1+o(1))\prod_{p|n-1}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p|l,p\nmid n\\ p>3}}\left(1-\frac{1}{p-2}\right)^{-1}\prod_{\substack{p|(n-1)n\\ p>3}}\left(1-\frac{1}{p-2}\right)^{-1}$$

$$\cdot\prod_{3<p<z}\frac{1-\frac{1}{p-2}}{1-\frac{1}{p}}\prod_{p<z}\left(1-\frac{1}{p}\right).$$

The linear sieve (Lemma 2 with $\kappa = 1$) gives for $Q_l = (N/l)^{1/2}/(\log N/l)^{A'}$

$$S(M_n(l),\mathcal{P}_n(l),(N/l)^{1/4}) \leq \Omega_n(l,(N/l)^{1/4})X_n(l)e^{\gamma}(1+o(1)) + \sum_{d<Q_l, d|\mathcal{P}_n(l)} c_{d,l}R_n(l,d).$$

Using Mertens' formula and summing over $l \in \mathcal{L}_n$ gives

$$T \leq (12+o(1))\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{p|(n-1)n\\ p>3}}\left(1-\frac{1}{p-2}\right)^{-1}\prod_{p>3}\frac{1-\frac{1}{p-2}}{1-\frac{1}{p}}$$

$$\cdot\sum_{l\in\mathcal{L}_n}\frac{f_n(l)M_n(l)}{l\log(N/l)} + \sum_{l\in\mathcal{L}_n}\sum_{d<Q_l,d|\mathcal{P}_n(l)} c_{d,l}R_n(l,d) + \sum_{l\in\mathcal{L}_n}O((N/l)^{1/4})), \quad (7)$$

where

$$f_n(m) = \begin{cases}\displaystyle\prod_{p|m,p>2}\left(1-\frac{1}{p-1}\right)^{-1}\prod_{\substack{p|m,p\nmid n\\ p>3}}\left(1-\frac{1}{p-2}\right)^{-1}, & \text{if } (m,n-1)=1,\\ 0, & \text{if } (m,n-1)>1.\end{cases}$$

To evaluate the sum over l in the main term we need two more lemmata that correspond to Lemmata 3 and 4 of [12]. The following result follows similarly to Lemma 3 of [12].

Lemma 6. *Let $u(m)$ be the characteristic function of integers whose prime factors are of the form $4k+1$. Then*

$$\sum_{m\leq x} u(m)f_n(m) = \frac{x}{2\sqrt{2\log x}}C_n + O\left(\frac{x}{(\log x)^{3/2}}\right),$$

where

$$C_n = \prod_{p\equiv 3\,(\mathrm{mod}\,4)} \left(1-\frac{1}{p^2}\right)^{1/2} \prod_{\substack{p\equiv 1\,(\mathrm{mod}\,4)\\ p|n-1}} \left(1-\frac{1}{p-2}\right)$$
$$\cdot \prod_{\substack{p\equiv 1\,(\mathrm{mod}\,4)\\ p|n}} \frac{1-\frac{1}{p-2}}{1-\frac{1}{p-1}} \prod_{p\equiv 1\,(\mathrm{mod}\,4)} \frac{1-\frac{1}{p}}{1-\frac{1}{p-2}}.$$

The proof of the following lemma is analogous to Lemma 4 of [12]. The only change is the use of the previous Lemma in the place of Wu's Lemma 3.

Lemma 7. *Let $\mathcal{L}_n$, $f_n(m)$, $W(\alpha)$ and C_n be defined as above and let $m \geq N(\log N)^{-A}$. Then*

$$\sum_{l\in\mathcal{L}_n} \frac{f_n(l)}{l(\log m/l)^2} = \frac{W(\alpha)C_n + o(1)}{(\log m)^{3/2}}.$$

By using $\log(N/l) \geq \log(m/l)$ for $m \leq N$ and using the previous lemma for $m > N(\log N)^{-A}$ arising from $M_n(l)$, the first sum over l in (7) is

$$\leq (1+o(1)) \sum_{\frac{N}{(\log N)^A} \leq m \leq n-2} \frac{C_n W(\alpha)}{(\log m)^{3/2}\log(n-m)} = \frac{C_n W(\alpha) + o(1)}{(\log N)^{1/2}} M_n(1).$$

This implies

$$T \leq \frac{12C_1(n)W(\alpha)+o(1)}{(\log N)^{1/2}} M_n(1) + \sum_{l\in\mathcal{L}_n} \sum_{d<Q_l, d|\mathcal{P}_n(l)} c_{d,l} R_n(l,d) + \sum_{l\in\mathcal{L}} O((N/l)^{1/4}).$$

Since $|R_n(l,d)| \leq 1$ if $l \in \mathcal{L}\setminus\mathcal{L}_n$ or $(d,n) > 1$, we can change the summation over l to go over the set $\mathcal{L}$ and the summation over d to go over $d < Q_l, (d,l) = 1$ with error $\ll N(\log N)^{-A}$. Thus the claim follows from Lemma 3 by choosing there

$$d_{d,l} = \begin{cases} c_{d,l}, & \text{if } l\in\mathcal{L},\ (d,l)=1 \text{ and } |\mu(d)|=1,\\ 0, & \text{else.}\end{cases}$$

□

7 Proof of the theorem

By (1) and Propositions 4 and 5 we have, for $n \geq \frac{N}{(\log N)^A}$ and $1 \leq \alpha \leq 6$,

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}_{3,n}, N) \geq & (1+o(1)) \frac{3C_1(n)M_n(1)}{2\sqrt{2\log N}} \Bigg(\frac{1}{\sqrt{2}} \int_1^{\alpha/2} \frac{dt}{\sqrt{t(t-1)}} \\ & - \alpha \int_2^{\alpha} \frac{t-2+(t-1)\log(t-1)}{t^2(t-1)(1-t/\alpha)^{1/2}} dt \Bigg) + E_1(n) - E_2(n), \end{aligned}$$

where $\sum_{n\in\mathcal{N}}(|E_1(n)|+|E_2(n)|)^2 \ll N^3/(\log N)^A$. By evaluating the integrals with $\alpha = 9/4$ and noticing that $C_1(n) \gg 1$ for $n \in \mathbb{N}$, we obtain

$$S(\mathcal{A}, \mathcal{P}_3(n), N) \gg \frac{M_n(1)}{(\log N)^{1/2}} - |E_1(n)| - |E_2(n)|,$$

which implies the claim as stated in the introduction.

Acknowledgments

The author thanks Glyn Harman for his helpful comments and suggestions. The author was supported by EPSRC grant GR/T20236/01.

References

[1] E. Bombieri. On the large sieve. *Mathematika*, 12:201–225, 1965.

[2] T. Estermann. On Goldbach's problem: Proof that almost all even positive integers are sums of two primes. *Proc. London Math. Soc.* (2), 44:307–314, 1938.

[3] H. Iwaniec. Primes of the type $\phi(x, y) + a$ where ϕ is a quadratic form. *Acta Arith.*, 21:203–234, 1972.

[4] H. Iwaniec. Rosser's sieve. *Acta Arith.*, 36:171–202, 1980.

[5] Ju. V. Linnik. An asymptotic formula in an additive problem of Hardy and Littlewood (Russian). *Izv. Akad. Nauk SSSR, ser. math.*, 24:629–706, 1960.

[6] N. G. Tchudakoff. On the density of the set of even numbers which are not representable as a sum of two odd primes. *Izv. Akad. Nauk SSSR Ser. Nat.*, 2:25–40, 1938.

[7] D. I. Tolev. On the number of representations of an odd integer as a sum of three primes, one of which belongs to an arithmetic progression. *Proceedings of the Steklov Institute of Mathematics*, 218:414–432, 1997.

[8] J. G. van der Corput. Sur l'hypothèse de Goldbach pour presque tous les nombres pairs. *Acta Arith.*, 2:266–290, 1937.

[9] R. C. Vaughan. *The Hardy-Littlewood method*. Cambridge University Press, second edition, 1997.

[10] I. M. Vinogradov. Representation of an odd number as a sum of three primes. *C. R. Acad. Sci. URSS*, 15:6–7, 1937.

[11] I. M. Vinogradov. Some theorems concerning the theory of primes. *Rec. Math. Moscou*, 2:179–195, 1937.

[12] J. Wu. Primes of the form $p = 1 + m^2 + n^2$ in short intervals. *Proc. Amer. Math. Soc.*, 126(1):1–8, 1998.