Values of Arithmetical Functions Equal to a Sum of Two Squares

William D. Banks*
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

Filip Saidak
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
filip@math.missouri.edu

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

*Corresponding Author

Abstract

Let $\varphi(n)$ denote the Euler function. In this paper, we determine the order of growth for the number of positive integers $n \le x$ for which $\varphi(n)$ is the sum of two square numbers. We also obtain similar results for the Dedekind function $\psi(n)$ and the sum of divisors function $\sigma(n)$.

1 Introduction

In 1970, Motohashi [6] showed that the number $N(x)$ of primes $p \le x$ of the form $p = a^2+b^2+1$ with $a, b \in \mathbb{Z}$ satisfies the lower bound $N(x) \gg x/(\ln x)^2$. Based on earlier work of Hooley [2], he conjectured that $N(x) \sim Cx/(\ln x)^{3/2}$ as $x \to \infty$, where

$$C = \frac{3}{2} \prod_{p\equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2} \left(1 - \frac{1}{p(p-1)}\right).$$

In a subsequent paper [7], he proved the upper bound $N(x) \ll x/(\ln x)^{3/2}$, but he was unable to obtain a lower bound of the same order of magnitude.

The problem of showing $N(x) \asymp x/(\ln x)^{3/2}$ was settled by Iwaniec [4] (see also [5]), who established tight upper and lower bounds for the number $N_{f,m,c}(x)$ of primes $p \le x$ of the form $mf(a,b) + c$ with $a, b \in \mathbb{Z}$, where f is a quadratic form with integral coefficients, $m, c \in \mathbb{Z}$, and f, m, c are subject to certain natural hypotheses. He also showed that the constant C originally conjectured by Motohashi cannot be correct, and he suggested that the factor $3/2$ should instead be replaced by $1/\sqrt{2}$. We remark that Motohashi's conjecture remains open at present.

Let $\varphi(n)$ denote the *Euler function*; that is,

$$\varphi(n) = \#\{1 \le a \le n : \gcd(a,n) = 1\} = n \prod_{p\,|\,n} \left(1 - \frac{1}{p}\right), \qquad n \ge 1.$$

Since $\varphi(p) = p-1$ for every prime p, $N(x)$ can be interpreted as the number of primes in the set

$$\{p \le x : \varphi(p) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}.$$

Passing from primes to all positive integers, let us consider the function $M(x)$ which counts the number of positive integers in the set

$$\{n \le x : \varphi(n) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}.$$

As a lower bound, one can use $M(x) \ge N(x) \gg x/(\ln x)^{3/2}$, but it is not immediately clear how to bound $M(x)$ from above. Our main result is the following:

Theorem 1. *For all $x \ge 2$, the following bound holds:*

$$M(x) = \#\{n \le x : \varphi(n) = a^2 + b^2 \textit{ for some } a, b \in \mathbb{Z}\} \ll \frac{x}{(\ln x)^{3/2}}.$$

In other words,

$$M(x) \asymp N(x) \asymp x/(\ln x)^{3/2}. \tag{1}$$

Theorem 1 is the special case $m = 1$ of Theorem 3, which is proved in Section 3 below; that section also contains several Mertens-type estimates for the classes of primes under consideration, which may be of independent interest.

Let $\psi(n)$ and $\sigma(n)$ denote the *Dedekind function* and the *sum of divisors function*, respectively; that is,

$$\psi(n) = n \prod_{p \mid n} \left(1 + \frac{1}{p}\right) \quad \text{and} \quad \sigma(n) = \sum_{d \mid n} d = \prod_{p^a \parallel n} \frac{p^{a+1} - 1}{p - 1}, \qquad n \ge 1.$$

In Section 4, we show that results analogous to Theorem 1 and thus to (1) hold also for the functions $\psi(n)$ or $\sigma(n)$. More precisely,

Theorem 2. *The following bounds hold:*

$$\#\{n \le x : \psi(n) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\} \asymp \frac{x}{(\ln x)^{3/2}}$$

and

$$\#\{n \le x : \sigma(n) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\} \asymp \frac{x}{(\ln x)^{3/2}}.$$

We expect that the methods of this paper can be adapted to obtain similar results for other quadratic forms besides $a^2 + b^2$.

Acknowledgements. The authors wish to thank Henryk Iwaniec for some useful conversations and the referee for some valuable comments which led to improvements in the manuscript. Part of this work was done during visits by F. L. and I. S. to the University of Missouri-Columbia, and during a visit by W. B. to the Universidad Nacional Autónoma de México; the support and hospitality of these institutions are gratefully acknowledged. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459.

2 Notation

Let $\mathbb{Z}$ denote the set of integers, and let $\mathbb{N}$ denote the set of natural numbers. Throughout, the letter p is always used to denote a *prime number*, while q always denotes a *prime power*.

In what follows, all implied constants in the symbols "O," "$\gg$" and "$\ll$" are *absolute*; in particular, they are uniform with respect to the parameters k and m which often occur in our arguments. For positive functions A and B, the notations $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent to the assertion that $A \le cB$ for some absolute constant $c > 0$.

For a real number $x > 0$, we define $\log x = \max\{\ln x,\, 2\}$, where $\ln x$ is the natural logarithm, and we put $\log_2 x = \log(\log x)$. Although our notation is highly nonstandard (it is much more common to put $\log x = \max\{\ln x,\, 1\}$ in order to handle various technical difficulties that can occur if x is very small), the function $\log x = \max\{\ln x,\, 2\}$ enjoys a rather convenient property; namely, $\log x$ is *submultiplicative*. Thus, the inequalities

$$\log(xy) \le \log x\, \log y \qquad \text{and} \qquad \log_2(xy) \le \log_2 x\, \log_2 y \tag{2}$$

hold for *all* $x, y > 0$. The properties (2) enable us to simplify our arguments substantially at several key places, and it is for the benefit of the overall exposition that we have chosen to employ a nonstandard notation; we hope that this will not lead to any confusion for the reader.

3 Sums of Squares and the Euler Function

Let $\mathcal{S}$ be the set of natural numbers that can be expressed as a sum of two square numbers:

$$\mathcal{S} = \{s \in \mathbb{N} : s = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}.$$

We set

$$\mathcal{M} = \{\text{squarefree } m \in \mathbb{N} : p \,|\, m \implies p \equiv 3 \pmod 4\},$$

and for any $m \in \mathcal{M}$ we put $m\mathcal{S} = \{ms : s \in \mathcal{S}\}$. From the standard characterization of those integers lying in $\mathcal{S}$, it is clear that $\mathbb{N}$ is the disjoint union of the sets $\{m\mathcal{S} : m \in \mathcal{M}\}$.

As a special case of Theorem 1 of [4], one finds the estimate:

$$\#\{p \le x : p-1 \in m\mathcal{S}\} \ll \frac{x}{\varphi(m)(\log x)^{3/2}}, \qquad \forall\, m \ll (\log x)^{3/2}.$$

Our principal tool in this paper is the following extension of this bound for larger values of m.

Lemma 1. *For all $m \in \mathcal{M}$ and $x > 0$, the following estimate holds:*

$$\#\{p \le x : p-1 \in m\mathcal{S}\} \ll \frac{x}{\varphi(m)(\log(x/m))^{3/2}}.$$

Proof. We may assume that $x > m$ since the result is trivial otherwise. Throughout the proof, let

$$\begin{aligned} \mathcal{N} &= \{n \in \mathbb{N} : p \,|\, n \implies p \equiv 3 \pmod 4\}, \\ \mathcal{R} &= \{n \in \mathbb{N} : p \,|\, n \implies p \not\equiv 3 \pmod 4\}. \end{aligned}$$

It is easy to see that $\mathcal{R} \subset \mathcal{S}$ and that $m\mathcal{S}$ is the disjoint union of the sets $\{md^2\mathcal{R} : d \in \mathcal{N}\}$; it therefore suffices to estimate $\#\{p \le x : p-1 \in md^2\mathcal{R}\}$ for each $d \in \mathcal{N}$ and then sum the results.

We apply the arithmetic form of the *large sieve inequality* (see, for example, Corollary 6.1 in §I.4.5 of [8]), which states that for any finite sequence of complex numbers $\{a_n : M < n \le M+N\}$, the bound

$$\left|\sum_{M<n\le M+N} a_n\right|^2 \le \frac{N-1+Q^2}{L} \sum_{M<n\le M+N} |a_n|^2 \tag{3}$$

holds, where

$$Q \ge 1, \qquad L = \sum_{k \le Q} \left(\mu^2(k) \prod_{p\,|\,k} \frac{w(p)}{p-w(p)}\right),$$

and for every prime p,

$$w(p) = \#\{h : 0 \le h < p,\ n \equiv h \pmod p \implies a_n = 0\}.$$

We begin with an estimate for the cardinality of the set

$$\mathcal{P}_b(x) = \{p \le x : p - 1 \in b\mathcal{R}\},$$

where $b \in \mathcal{N}$ and $b \le x$. Put $Q = \lceil (x/b)^{1/2} \rceil$, and let $\{a_n : Q < n \le Q^2\}$ be the finite sequence defined by

$$a_n = \begin{cases} 1 & \text{if } n \in \mathcal{R} \text{ and } bn+1 \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

If $p = bn+1$ lies in $\mathcal{P}_b(x)$, then $n \in \mathcal{R}$ and $n < x/b \le Q^2$; thus, either $a_n = 1$ or $n \le Q$. Taking $M = Q$ and $N = Q^2 - Q$ in (3), we see that

$$\#\mathcal{P}_b(x) \le Q + \sum_{Q<n\le Q^2} a_n \le Q + \frac{(Q^2-Q) - 1 + Q^2}{L} \ll Q + \frac{Q^2}{L}. \tag{4}$$

Now, for the sequence $\{a_n\}$ we are considering, one has for each prime $p \le Q$:

$$w(p) = \begin{cases} 2 & \text{if } p \equiv 3 \pmod 4 \text{ and } p \nmid b, \\ 1 & \text{otherwise.} \end{cases}$$

Therefore, according to Lemma 4.1 in Chapter 4 of [1], the following lower bound for L holds:

$$L \gg \prod_{p\le Q} \left(1 - \frac{w(p)}{p}\right)^{-1}.$$

The expression on the right is bounded below (see [9]) by

$$\prod_{\substack{p\le Q\\ p\,|\,b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p\le Q\\ p\equiv 3 \pmod 4}} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p\le Q} \left(1 - \frac{1}{p}\right)^{-1} \gg \frac{\varphi(b)}{b} (\log Q)^{3/2}.$$

Substituting this bound into (4) and using the fact that $Q \ll (x/b)^{1/2}$, we derive that

$$\#\mathcal{P}_b(x) \ll \frac{x}{\varphi(b)(\log(x/b))^{3/2}},$$

uniformly for all $b \in \mathcal{N}$ with $b \le x$.

By the remarks at the beginning of the proof,

$$\begin{aligned}\#\{p \le x : p-1 \in m\mathcal{S}\} &= \sum_{\substack{d\in\mathcal{N}\\ d\le (x/m)^{1/2}}} \#\mathcal{P}_{md^2}(x) \\ &\ll \sum_{\substack{d\in\mathcal{N}\\ d\le (x/m)^{1/2}}} \frac{x}{\varphi(md^2)(\log(x/md^2))^{3/2}}.\end{aligned}$$

The contribution for values of $d \le (x/m)^{1/4}$ is at most

$$\begin{aligned}\sum_{\substack{d\in\mathcal{N}\\ d\le (x/m)^{1/4}}} \frac{x}{\varphi(md^2)(\log(x/md^2))^{3/2}} &\ll \frac{x}{\varphi(m)(\log(x/m))^{3/2}} \sum_{d\in\mathcal{N}} \frac{1}{\varphi(d^2)} \\ &\ll \frac{x}{\varphi(m)(\log(x/m))^{3/2}}.\end{aligned}$$

For larger values of d, we also have

$$\begin{aligned}\sum_{\substack{d\in\mathcal{N}\\ (x/m)^{1/4}<d\le (x/m)^{1/2}}} \frac{x}{\varphi(md^2)(\log(x/md^2))^{3/2}} &\ll \frac{x}{\varphi(m)} \sum_{(x/m)^{1/4}<d\le (x/m)^{1/2}} \frac{1}{\varphi(d^2)} \\ &\ll \frac{x}{\varphi(m)(x/m)^{1/4}} \ll \frac{x}{\varphi(m)(\log(x/m))^{3/2}},\end{aligned}$$

where we use the well-known fact that the estimate

$$\sum_{d\ge y} \frac{1}{\varphi(d^2)} \ll \frac{1}{y}$$

holds for all positive real numbers y. The result now follows. □

We need the following analogue of Lemma 1 for prime powers q.

Lemma 2. *For all $m \in \mathcal{M}$ and $x > 0$, the following estimate holds:*

$$\#\{q \le x : \varphi(q) \in m\mathcal{S}\} \ll \frac{x}{\varphi(m)(\log(x/m))^{3/2}}.$$

Proof. As before, we may assume $x > m$ since the result is trivial otherwise. To simplify the notation slightly, we put

$$\mathcal{E}(m,x) = \frac{x}{\varphi(m)(\log(x/m))^{3/2}}.$$

We have

$$\#\{q \le x : \varphi(q) \in m\mathcal{S}\} = \#\{p \le x : p-1 \in m\mathcal{S}\} + \sum_{\alpha \ge 2} \sum_{\substack{q = p^\alpha \le x \\ \varphi(q) \in m\mathcal{S}}} 1.$$

By Lemma 1, it suffices to show that the double sum on the right is bounded by $O(\mathcal{E}(m,x))$.

Since $\varphi(2^\alpha) \in \mathcal{S}$ for all $\alpha \ge 1$, the contribution to the double sum coming from the prime $p = 2$ is at most $O(\log x)$ if $m = 1$, and it is 0 if $m \ne 1$; this is $O(\mathcal{E}(m,x))$ in either case.

For primes $p \equiv 1 \pmod 4$, we observe that $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ lies in $m\mathcal{S}$ if and only if $p - 1 \in m\mathcal{S}$. Thus, by Lemma 1, the contribution to the double sum coming from prime powers of this form is at most

$$\sum_{\alpha=2}^{\lfloor \frac{\ln x}{\ln 2} \rfloor} \sum_{\substack{p \le x^{1/\alpha} \\ p-1 \in m\mathcal{S} \\ p \equiv 1 \pmod 4}} 1 \ll \sum_{\alpha=2}^{\lfloor 2\log x \rfloor} \frac{x^{1/2}}{\varphi(m)} \ll \frac{x^{1/2}\log x}{\varphi(m)} \ll \mathcal{E}(m,x).$$

Similarly, if $p \equiv 3 \pmod 4$ and $2 \nmid \alpha$, then $p^{\alpha-1}(p-1)$ lies in $m\mathcal{S}$ if and only if $p - 1 \in m\mathcal{S}$ (since m is squarefree). By Lemma 1, the contribution to the double sum coming from prime powers of this form is at most

$$\sum_{\substack{\alpha=3\\ 2\nmid\alpha}}^{\lfloor\frac{\ln x}{\ln 2}\rfloor} \sum_{\substack{p\le x^{1/\alpha}\\ p-1\in m\mathcal{S}\\ p\equiv 3 \pmod 4}} 1 \ll \sum_{\alpha=3}^{\lfloor 2\log x\rfloor} \frac{x^{1/3}}{\varphi(m)} \ll \frac{x^{1/3}\log x}{\varphi(m)} \ll \mathcal{E}(m,x).$$

Finally, if $p\equiv 3 \pmod 4$, $2\,|\,\alpha$, and $\alpha\ge 2$, then $p^{\alpha-1}(p-1)$ lies in $m\mathcal{S}$ if and only if $p\,|\,m$ and $p-1\in(m/p)\mathcal{S}$. Since the last condition implies that $p>m^{1/2}$, there is at most one prime p of this form. Assuming that such a prime exists and using the inequality $\ln p\gg\log m$, we see that the contribution to the double sum coming from the powers of p is at most

$$\sum_{\substack{\alpha=2\\ 2\,|\,\alpha}}^{\lfloor\frac{\ln x}{\ln p}\rfloor} \sum_{\substack{p\le x^{1/\alpha}\\ p\,|\,m,\ p-1\in(m/p)\mathcal{S}\\ p\equiv 3 \pmod 4}} 1 \ll \frac{\log x}{\log m} \le \log(x/m),$$

where the last estimate follows from (2). Since $(\log(x/m))^{5/2}\ll x/m$ for $x>m$, we see that

$$\log(x/m) \ll \frac{x}{m\log(x/m)^{3/2}} \ll \mathcal{E}(m,x),$$

and this completes the proof. $\square$

Lemma 3. *For all $m\in\mathcal{M}$ and $x>0$, the following estimate holds:*

$$\sum_{\substack{q>x\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q} \ll \frac{1}{\varphi(m)(\log(x/m))^{1/2}}.$$

Proof. Since the condition $\varphi(q)\in m\mathcal{S}$ implies $q>m$, we may assume that $x\ge m$ in what follows. Let X_m denote the characteristic function of the set of prime powers $\{q : \varphi(q) \in m\mathcal{S}\}$, and let z an arbitrary real number such that $z > \max\{x, e^2 m\}$. By partial summation and Lemma 2, we have

$$\begin{aligned}
\sum_{\substack{x<q\le z\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q} = \sum_{x<n\le z} \frac{X_m(n)}{n} &= \frac{1}{z}\sum_{x<n\le z} X_m(n) + \int_x^z \frac{1}{t^2}\left(\sum_{x<n\le t} X_m(n)\right) dt \\
&= \frac{1}{z}\sum_{\substack{x<q\le z\\ \varphi(q)\in m\mathcal{S}}} 1 + \int_x^z \frac{1}{t^2}\left(\sum_{\substack{x<q\le t\\ \varphi(q)\in m\mathcal{S}}} 1\right) dt \\
&\ll \frac{1}{\varphi(m)}\left(\frac{1}{(\log(z/m))^{3/2}} + \int_x^z \frac{dt}{t(\log(t/m))^{3/2}}\right).
\end{aligned}$$

If $m \le x < e^2 m$, then

$$\begin{aligned}
\int_x^z \frac{dt}{t(\log(t/m))^{3/2}} &\le 2^{-3/2}\int_m^{e^2 m} \frac{dt}{t} + \int_{e^2 m}^z \frac{dt}{t(\ln(t/m))^{3/2}} \\
&= 2^{-1/2} + 2^{1/2} - \frac{2}{(\log(z/m))^{1/2}},
\end{aligned}$$

while for $x \ge e^2 m$, since $\log(t/m) = \ln(t/m)$ for all $t \ge x$, we have

$$\int_x^z \frac{dt}{t(\log(t/m))^{3/2}} = \frac{2}{(\log(x/m))^{1/2}} - \frac{2}{(\log(z/m))^{1/2}}.$$

Taking $z \to \infty$, we obtain the stated result. □

Lemma 4. *For all $m \in \mathcal{M}$, $n \in \mathbb{N}$, and $x > 0$, the following estimate holds:*

$$\sum_{\substack{q\le x\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q\,(\log(x/qn))^{1/2}} \ll \frac{1}{\varphi(m)(\log(x/mn))^{1/2}}.$$

Proof. Since $\varphi(q) \in m\mathcal{S}$ implies $q > m$, we may assume that $x \ge m$. Let $y = (mx/n)^{1/2}$, and note that $x/yn = y/m = (x/mn)^{1/2}$. By Lemma 3, we have for the sum over $q > y$:

$$\sum_{\substack{y<q\le x\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q\,(\log(x/qn))^{1/2}} \ll \sum_{\substack{q>y\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q} \ll \frac{1}{\varphi(m)(\log(y/m))^{1/2}}$$

$$\ll \frac{1}{\varphi(m)(\log(x/mn))^{1/2}}.$$

Again by Lemma 3, we have for the sum over $q \le y$:

$$\sum_{\substack{q\le y\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q\,(\log(x/qn))^{1/2}} \ll \frac{1}{(\log(x/yn))^{1/2}} \sum_{\substack{q>1\\ \varphi(q)\in m\mathcal{S}}} \frac{1}{q} \ll \frac{1}{\varphi(m)(\log(x/mn))^{1/2}}.$$

Combining the preceding estimates, we finish the proof. □

Let $\mathcal{Q}$ denote the set of prime powers.

Lemma 5. *For some absolute constant $C > 0$, the estimate*

$$\sum_{\substack{(q_1,\ldots,q_k)\in\mathcal{Q}^k\\ q_1\cdots q_k\le x\\ \varphi(q_j)\in m_j\mathcal{S}\ \forall j}} \log(q_1\cdots q_k) \le kC^k \left(\prod_{j=1}^{k} \frac{1}{\varphi(m_j)}\right) \frac{x\log\mu}{(\log(x/m))^{1/2}}$$

holds for all $k \ge 1$, $m_1, \ldots, m_k \in \mathcal{M}$, and $x > 0$, where $m = m_1\cdots m_k$ and $\mu = \max\{m_1, \ldots, m_k\}$.

Proof. We proceed by induction on k.

The case $k = 1$ is straightforward. Indeed, if $m \in \mathcal{M}$, using Lemma 2 together with (2), we see that the estimate

$$\sum_{\substack{q\le x\\ \varphi(q)\in m\mathcal{S}}} \log q \le C\,\frac{x\log x}{\varphi(m)(\log(x/m))^{3/2}} \le C\,\frac{x\log m}{\varphi(m)(\log(x/m))^{1/2}}$$

holds for some absolute constant $C > 0$, since $\log q \le \log x$ for each term in the sum. This establishes the result for $k = 1$.

Taking C larger if necessary, let us assume that C is at least as large as the implied constant of Lemma 4.

Let us now suppose that the result has been established for some integer $k \geq 1$. Starting with the bound

$$k \log(q_1 \cdots q_{k+1}) \leq \sum_{j=1}^{k+1} \log(q_1 \cdots \widehat{q}_j \cdots q_{k+1}),$$

where $\widehat{q}_j$ indicates that the factor q_j has been omitted (in fact, the inequality would be an identity were it not for our slightly modified definition of the function log; see Section 2), we derive that

$$\begin{aligned}
&\sum_{\substack{(q_1,\dots,q_{k+1})\in\mathcal{Q}^{k+1} \\ q_1\cdots q_{k+1}\leq x \\ \varphi(q_j)\in m_j\mathcal{S}\ \forall j}} k\log(q_1\cdots q_{k+1}) \\
&\qquad \leq \sum_{\substack{(q_1,\dots,q_{k+1})\in\mathcal{Q}^{k+1} \\ q_1\cdots q_{k+1}\leq x \\ \varphi(q_j)\in m_j\mathcal{S}\ \forall j}} \sum_{j=1}^{k+1} \log(q_1\cdots \widehat{q}_j \cdots q_{k+1}) \\
&\qquad = \sum_{j=1}^{k+1} \sum_{\substack{q_j\leq x \\ \varphi(q_j)\in m_j\mathcal{S}}} \sum_{\substack{(q_1,\dots,\widehat{q}_j,\dots,q_{k+1})\in\mathcal{Q}^{k} \\ q_1\cdots\widehat{q}_j\cdots q_{k+1}\leq x/q_j \\ \varphi(q_i)\in m_i\mathcal{S}\ \forall i\neq j}} \log(q_1\cdots \widehat{q}_j \cdots q_{k+1}) \\
&\qquad \leq \sum_{j=1}^{k+1} kC^k \left(\prod_{\substack{1\leq i\leq k+1 \\ i\neq j}} \frac{1}{\varphi(m_i)}\right) \sum_{\substack{q_j\leq x \\ \varphi(q_j)\in m_j\mathcal{S}}} \frac{x\log\mu}{q_j\left(\log\left(\frac{x}{q_j\, m_1\cdots\widehat{m}_j\cdots m_k}\right)\right)^{1/2}}.
\end{aligned}$$

Dividing both sides by k and using Lemma 4 to estimate the last sum, it follows that

$$\sum_{\substack{(q_1,\dots,q_{k+1})\in\mathcal{Q}^{k+1}\\ q_1\cdots q_{k+1}\le x\\ q_j-1\in m_j\mathcal{S}\ \forall j}} \log(q_1\cdots q_{k+1}) \le C^k\sum_{j=1}^{k+1}\left(\prod_{\substack{1\le i\le k+1\\ i\ne j}}\frac{1}{\varphi(m_i)}\right)\frac{Cx\log\mu}{\varphi(m_j)(\log(x/m))^{1/2}}$$

$$= (k+1)C^{k+1}\left(\prod_{i=1}^{k+1}\frac{1}{\varphi(m_i)}\right)\frac{x\log\mu}{(\log(x/m))^{1/2}}.$$

This completes the induction and finishes the proof. □

Theorem 3. *For all $m\in\mathcal{M}$ and $x>0$, the following estimate holds:*

$$\#\{n\le x:\varphi(n)=m(a^2+b^2)\ \textit{for some}\ a,b\in\mathbb{Z}\}\ll\frac{c(m)x}{(\log(x/m))^{3/2}}$$

for some positive function $c(m)$ that depends only on m. Moreover, $c(m)\to 0$ as $m\to\infty$.

Proof. Let

$$\mathcal{T}(m;x)=\{n\le x:\varphi(n)\in m\mathcal{S}\}.$$

We begin by estimating

$$\sum_{\substack{n\in\mathcal{T}(m;x)\\ \omega(n)=k}}\log n=\sum_{\substack{(p_1^{\alpha_1},\dots,p_k^{\alpha_k})\in\mathcal{Q}^k\\ p_1^{\alpha_1}\cdots p_k^{\alpha_k}\in\mathcal{T}(m;x)\\ p_1<\dots<p_k}}\log(p_1^{\alpha_1}\cdots p_k^{\alpha_k})=\frac{1}{k!}\sum_{\substack{(q_1,\dots,q_k)\in\mathcal{Q}^k\\ q_1\cdots q_k\in\mathcal{T}(m;x)\\ \gcd(q_i,q_j)=1\ \forall i\ne j}}\log(q_1\cdots q_k).$$

If $q_1\cdots q_k\in\mathcal{T}(m;x)$ and $\gcd(q_i,q_j)=1$ for all $i\ne j$, it is easy to see that the integers $m_1,\dots,m_k\in\mathcal{M}$ defined by $\varphi(q_j)\in m_j\mathcal{S}$, $j=1,\dots,k$, satisfy the relation $m_1\cdots m_k=mt^2$ for some *odd* integer $t\le(x/m)^{1/2}$. Moreover, since each m_j is *squarefree*, it follows that $m_j\le mt$. Using Lemma 5, we derive that

$$\sum_{\substack{(q_1,\ldots,q_k)\in\mathcal{Q}^k\\ q_1\cdots q_k\in\mathcal{T}(m;x)\\ \gcd(q_i,q_j)=1\ \forall i\neq j}} \log(q_1\cdots q_k) \le \sum_{\substack{t\le(x/m)^{1/2}\\ t\text{ odd}}} \sum_{\substack{(m_1,\ldots,m_k)\in\mathcal{M}^k\\ m_1\cdots m_k=mt^2}} \sum_{\substack{(q_1,\ldots,q_k)\in\mathcal{Q}^k\\ q_1\cdots q_k\le x\\ \varphi(q_j)\in m_j\mathcal{S}\ \forall j}} \log(q_1\cdots q_k)$$

$$\le \sum_{\substack{t\le(x/m)^{1/2}\\ t\text{ odd}}} \sum_{\substack{(m_1,\ldots,m_k)\in\mathcal{M}^k\\ m_1\cdots m_k=mt^2}} kC^k\left(\prod_{j=1}^k \frac{1}{\varphi(m_j)}\right)\frac{x\log(mt)}{(\log(x/mt^2))^{1/2}}.$$

For each term in the double summation, we use the bound

$$\begin{aligned}\prod_{j=1}^k \varphi(m_j) &= \prod_{j=1}^k\left(m_j\prod_{p\,|\,m_j}\left(1-\frac{1}{p}\right)\right) = mt^2\prod_{j=1}^k\prod_{p\,|\,m_j}\left(1-\frac{1}{p}\right)\\ &= mt^2\prod_{p\,|\,mt}\left(1-\frac{1}{p}\right)^{\#\{1\le j\le k:p\,|\,m_j\}}\\ &\ge mt^2\left(\frac{\varphi(m)}{m}\right)^k\prod_{p^\alpha\,\|\,t}\left(1-\frac{1}{p}\right)^{2\alpha} = m\left(\frac{\varphi(m)}{m}\right)^k\prod_{p^\alpha\,\|\,t}(p-1)^{2\alpha}.\end{aligned}$$

By (2), we also have

$$\frac{\log(mt)}{(\log(x/mt^2))^{1/2}} \le \frac{\log m}{(\log(x/m))^{1/2}}\,(\log t)^2.$$

Putting everything together, we obtain that

$$\sum_{\substack{n\in\mathcal{T}(m;x)\\ \omega(n)=k}} \log n \le \frac{kC^k m^{k-1}\log m}{\varphi(m)^k\cdot k!}\,\frac{x}{(\log(x/m))^{1/2}} \sum_{\substack{t\le(x/m)^{1/2}\\ t\text{ odd}}} \frac{\tau_k^*(mt^2)(\log t)^2}{\prod_{p^\alpha\,\|\,t}(p-1)^{2\alpha}},$$

where $\tau_k^*(n)$ denotes the number of k-tuples $(n_1,\ldots,n_k)$ of squarefree natural numbers such that $n_1\cdots n_k=n$. From the identity

$$\tau_k^*(n) = \prod_{p^\alpha\,\|\,n}\binom{k}{\alpha}, \tag{5}$$

it follows that (since $\Omega(m) = \omega(m)$)

$$\tau_k^*(mt^2) \le \tau_k^*(m)\tau_k^*(t^2) \le \tau_k(m)\tau_k^*(t^2) \le k^{\omega(m)}\tau_k^*(t^2)$$

for each term in the preceding sum, where $\tau_k(n)$ is the number of k-tuples $(n_1, \ldots, n_k)$ in $\mathbb{N}^k$ such that $n_1 \cdots n_k = n$. Consequently, we derive that

$$\sum_{\substack{n \in \mathcal{T}(m;x) \\ \omega(n)=k}} \log n \le T_k \frac{k^{\omega(m)+1} C^k m^{k-1} \log m}{\varphi(m)^k \cdot k!} \frac{x}{(\log(x/m))^{1/2}}, \tag{6}$$

where

$$T_k = \sum_{\substack{t \ge 1 \\ t \text{ odd}}} \tau_k^*(t^2)(\log t)^2 \prod_{p^\alpha \,\|\, t} (p-1)^{-2\alpha}.$$

We turn now to the estimation of T_k. By the multiplicativity of $\tau_k^*(n)$, the sub-multiplicativity of $\log n$, and the identity (5), we see that

$$T_k \le 3 + \prod_{p \ne 2} \left(1 + \sum_{\alpha=1}^{\lfloor k/2 \rfloor} \binom{k}{2\alpha} \frac{(\log p^\alpha)^2}{(p-1)^{2\alpha}} \right).$$

Let us suppose that $k \ge 32$. For an odd prime $p \le k^2$ and an integer $\alpha \ge 1$, we have $\log p^\alpha \le 2\alpha \log k$, hence

$$\begin{aligned} 1 + \sum_{\alpha=1}^{\lfloor k/2 \rfloor} \binom{k}{2\alpha} \frac{(\log p^\alpha)^2}{(p-1)^{2\alpha}} &\le 1 + 4(\log k)^2 \sum_{\alpha=1}^{\lfloor k/2 \rfloor} \binom{k}{2\alpha} \frac{\alpha^2}{(p-1)^{2\alpha}} \\ &\le 1 + (\log k)^2 \sum_{\beta=0}^{k} \binom{k}{\beta} \frac{\beta^2}{(p-1)^\beta} \\ &\le 1 + k^2 (\log k)^2 \left(1 + \frac{1}{p-1}\right)^k \\ &\le 2k^2 (\log k)^2 \exp\left(\frac{k}{p-1}\right). \end{aligned}$$

For the product over odd primes $p < 32k$, we therefore have by the Prime Number Theorem and Mertens' Theorem:

$$\begin{aligned}\prod_{\substack{p<32k\\ p\neq 2}}\left(1+\sum_{\alpha=1}^{\lfloor k/2\rfloor}\binom{k}{2\alpha}\frac{(\log p^{\alpha})^2}{(p-1)^{2\alpha}}\right) &\leq \prod_{\substack{p<32k\\ p\neq 2}}\exp\left(\frac{k}{p-1}+O(\log k)\right)\\ &\leq \exp\left(\sum_{p<32k}\frac{k}{p-1}+O(k)\right)=\exp(O(k\log_2 k)).\end{aligned} \tag{7}$$

Now suppose that $p > 32k$. Defining

$$f(p,\alpha)=\binom{k}{2\alpha}\frac{(\log p^{\alpha})^2}{(p-1)^{2\alpha}}, \qquad 1\leq \alpha\leq \lfloor k/2\rfloor,$$

we have

$$\frac{f(p,\alpha+1)}{f(p,\alpha)}=\frac{(\alpha+1)^2(k-2\alpha)(k-2\alpha-1)}{\alpha^2(2\alpha+2)(2\alpha+1)(p-1)^2}<\frac{(\alpha+1)^2}{\alpha^2(2\alpha+1)^2}\frac{(k-2\alpha)^2}{(32k)^2}<\frac{1}{2},$$

and therefore

$$\begin{aligned}1+\sum_{\alpha=1}^{\lfloor k/2\rfloor}\binom{k}{2\alpha}\frac{(\log p^{\alpha})^2}{(p-1)^{2\alpha}} &= 1+\sum_{\alpha=1}^{\lfloor k/2\rfloor}f(p,\alpha)\leq 1+f(p,1)\left(1+\tfrac{1}{2}+\tfrac{1}{4}+\dots\right)\\ &= 1+2f(p,1)\leq 1+k^2\frac{(\log p)^2}{(p-1)^2}\leq \exp\left(k^2\frac{(\log p)^2}{(p-1)^2}\right).\end{aligned}$$

Now for the product over odd primes $p > 32k$, we have:

$$\begin{aligned}\prod_{p>32k}\left(1+\sum_{\alpha=1}^{\lfloor k/2\rfloor}\binom{k}{2\alpha}\frac{(\log p^{\alpha})^2}{(p-1)^{2\alpha}}\right) &\leq \prod_{p>32k}\exp\left(k^2\frac{(\log p)^2}{(p-1)^2}\right)\\ &\leq \exp\left(2k^2\sum_{p>32k}\frac{(\ln p)^2}{p^2}\right)\end{aligned} \tag{8}$$

if k is larger than some absolute constant. To estimate the sum, let us suppose that k is also sufficiently large so that the inequality $\pi(x) \leq 2x/\ln x$

holds for all $x \ge k$. Then

$$\sum_{p>32k} \frac{(\ln p)^2}{p^2} = \sum_{j=6}^{\infty} \sum_{k2^{j-1}<p\le k2^j} \frac{(\ln p)^2}{p^2} \le 4 \sum_{j=6}^{\infty} \frac{(\ln(k2^j))^2}{k^2 4^j} \pi(k2^j)$$
$$\le 8 \sum_{j=6}^{\infty} \frac{(\ln(k2^j))^2}{k^2 4^j} \frac{k2^j}{\ln(k2^j)} = \frac{8}{k} \sum_{j=6}^{\infty} \frac{\ln k + j \ln 2}{2^j} = \frac{\ln k}{4k} + \frac{7 \ln 2}{k}.$$

Substituting this estimate into (8) and taking into account (7), we deduce that

$$T_k \le \exp(0.5k \log k + O(k \log_2 k)). \tag{9}$$

Using this estimate in (6) together with Stirling's formula for $k!$, and then summing over all values of $k \ge 1$, it is now clear that for some constant $c(m)$ (which we estimate below),

$$\sum_{n\in\mathcal{T}(m;x)} \ln n \le \sum_{n\in\mathcal{T}(m;x)} \log n \le \frac{c(m)\, x}{(\log(x/m))^{1/2}}. \tag{10}$$

If $x \ge e^2 m$, which we may assume otherwise the statement of the theorem is trivial, we have by partial summation:

$$\sum_{n\in\mathcal{T}(m;x)} \ln n = \#\mathcal{T}(m,x) \ln x - \int_m^x \frac{1}{t} \left(\sum_{n\in\mathcal{T}(m;t)} \ln n \right) dt,$$

thus, by (10), it follows that

$$\#\mathcal{T}(m,x) \ln x \le \frac{c(m)\, x}{(\ln(x/m))^{1/2}} + \int_m^x \frac{c(m)}{(\log(t/m))^{1/2}}\, dt.$$

Since

$$\int_m^x \frac{1}{(\log(t/m))^{1/2}}\, dt = 2^{-1/2}(e^2 m - m) + \int_{e^2 m}^x \frac{1}{(\ln(t/m))^{1/2}}\, dt$$
$$\le 2^{-1/2}(e^2 m - m) + \int_{e^2 m}^x \left(\frac{2}{(\ln(t/m))^{1/2}} - \frac{1}{(\ln(t/m))^{3/2}} \right) dt$$
$$= 2^{-1/2}(e^2 m - m) - 2^{1/2} e^2 m + \frac{2x}{(\ln(x/m))^{1/2}} < \frac{2x}{(\ln(x/m))^{1/2}},$$

we have therefore shown that

$$\#\mathcal{T}(m,x) \ll \frac{c(m)x}{\log(x/m)^{3/2}}.$$

To complete the proof, it remains only to show that $c(m) = o(1)$. In what follows, let us suppose that m is large enough to guarantee that the stated estimates hold. By (9), Stirling's formula for $k!$, and the estimate $\varphi(m) \gg m/\log_2 m$, we find that

$$\begin{aligned} c(m) &= \sum_{k=1}^{\infty} T_k \, \frac{k^{\omega(m)+1} C^k m^{k-1} \log m}{\varphi(m)^k \cdot k!} \\ &\ll \frac{\log m}{m} \sum_{k=1}^{\infty} \exp\left(-\tfrac{1}{2} k \log k + \omega(m) \log k + k \log_3 m + O(k \log_2 k)\right) \\ &\ll \frac{\log m}{m} \sum_{k=1}^{\infty} a_k(m), \end{aligned}$$

where

$$a_k(m) = \exp\left(-\tfrac{1}{3} k \log k + \omega(m) \log k + k \log_3 m\right).$$

Now let S_1 be the set of integers $k \ge 1$ that satisfy both inequalities $k \ge 4\omega(m)$ and $k \ge (\log_2 m)^{24}$. If k lies in S_1, then $\omega(m) \le k/4$ and $\log_3 m \le (\log k)/24$; therefore,

$$-\tfrac{1}{3} k \log k + \omega(m) \log k + k \log_3 m \le -\tfrac{1}{3} k \log k + \tfrac{1}{4} k \log k + \tfrac{1}{24} k \log k = -\tfrac{1}{24} k \log k.$$

Hence, it follows that

$$\sum_{k \in S_1} a_k(m) \ll \sum_{k \ge 1} \exp(-\tfrac{1}{24} k \log k) \ll 1. \qquad (11)$$

Let S_2 be the set of integers $k \ge 1$ for which $k \le (\log_2 m)^{24}$. In this case, we have

$$\begin{aligned} a_k(m) &\leq \exp\left(\omega(m)\log k + k\log_3 m\right) \\ &\leq \exp\left(O\left(\frac{\log m \log_3 m}{\log_2 m}\right)\right) \ll m^{o(1)}, \end{aligned}$$

where we used the fact that $\omega(m) \ll \log m/\log_2 m$. Since the cardinality of S_2 is at most $(\log_2 m)^{24} = m^{o(1)}$, we find that

$$\sum_{k\in S_2} a_k(m) \leq m^{o(1)}. \tag{12}$$

Finally, let S_3 denote the set of integers $k \geq 1$ such that the inequalities $(\log_2 m)^{24} < k \leq 4\omega(m)$ hold. For any $k \in S_3$, we have $k\log_3 m \leq \frac{1}{6}k\log k$ (otherwise, $k < (\log_2 m)^6$); hence, it follows that

$$a_k(m) \ll \exp\left(-\tfrac{1}{6}k\log k + \omega(m)\log k\right).$$

Defining

$$f_m(z) = -\tfrac{1}{6}z\log z + \omega(m)\log z,$$

we have

$$\frac{df_m(z)}{dz} = -\frac{1}{6} + \frac{\omega(m)}{z} - \frac{\log z}{6}, \qquad \frac{d^2 f_m(z)}{dz^2} = -\frac{1}{6z} - \frac{\omega(m)}{z^2},$$

which shows that $f_m(z)$ has a (unique) maximum for a value of z_0 satisfying $z_0 \log z_0 = (6 + o(1))\omega(m)$. From this we deduce that

$$f_m(z_0) = \omega(m)(\log\omega(m) - \log_2\omega(m)) + O(\omega(m)).$$

From the trivial inequality $\omega(m)! \leq m$ and Stirling's formula, we obtain

$$\omega(m)\left(\log\omega(m) + O(1)\right) \leq \log m.$$

Therefore,

$$f_m(z_0) \ll \log m - \omega(m) \log_2 \omega(m) + O(\omega(m)).$$

If S_3 is not empty, then $\omega(m) > \frac{1}{4}(\log_2 m)^{24}$; hence,

$$a_k(m) \ll \exp(f_m(z_0)) \ll \exp\left(\log m - \tfrac{1}{8}(\log_2 m)^{25}\right)$$

for all $k \in S_3$. Since S_3 has at most $4\omega(m) \ll \log m$ elements, it follows that

$$\sum_{k \in S_3} a_k(m) = o\left(\frac{m}{\log m}\right). \tag{13}$$

From our original bound,

$$c(m) \le \frac{\log m}{m} \sum_{k \ge 1} a_k(m),$$

we now deduce that $c(m) = o(1)$ from the estimates (11), (12) and (13), and this completes the proof of the theorem. □

From the proof of Theorem 3, it is clear that the function $c(m)$ can be chosen to satisfy the bound

$$c(m) \ll \exp\left(-c(\log_2 m)^{25}\right)$$

for any fixed constant $0 < c < \frac{1}{8}$; in particular, $c(m) \ll (\log m)^{-A}$ for any fixed constant $A > 0$. Though we have not attempted to do so, it would be interesting to understand the extent to which this upper bound can be strengthened.

4 Proof of Theorem 2

The upper bound for the first part of Theorem 2 is the special case $m = 1$ of the following theorem, whose proof is virtually identical to that of Theorem 3 (one simply replaces $p - 1$ by $p + 1$ in the various statements of Section 3).

Theorem 4. *For all $m \in \mathcal{M}$ and $x > 0$, the following estimate holds:*

$$\#\{n \le x : \psi(n) \in m\mathcal{S}\} \ll \frac{c(m)x}{(\log(x/m))^{3/2}}$$

for some positive function $c(m)$ that depends only on m. Moreover, $c(m) \to 0$ as $m \to \infty$.

The analogue of Lemma 1 with $p-1$ replaced by $p+1$ clearly gives the desired lower bounds for both parts of Theorem 2. To complete the proof, it remains only to establish the upper bound:

$$\#\{n \le x : \sigma(n) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\} \ll \frac{x}{(\ln x)^{3/2}}. \tag{14}$$

Noting that $\sigma(n) = \psi(n)$ for squarefree integers n, we have the following corollary of Theorem 4.

Corollary 1. *For all $m \in \mathcal{M}$ and $x > 0$, the following estimate holds:*

$$\#\{n \le x : \sigma(n) \in m\mathcal{S} \text{ and } n \text{ is squarefree}\} \ll \frac{c(m)x}{(\log(x/m))^{3/2}}$$

for some positive function $c(m)$ that depends only on m. Moreover, $c(m) \to 0$ as $m \to \infty$.

Recall that an integer $k \ge 1$ is said to be *powerful* if $p^2 \,|\, k$ whenever $p \,|\, k$. Let $\mathcal{T}$ be the set of positive integers $n \le x$ such that $k \,|\, n$ for some powerful integer $k > (\ln x)^4$. Then

$$\#\mathcal{T} \le \sum_{\substack{k > (\ln x)^4 \\ k \text{ powerful}}} \sum_{\substack{n \le x \\ k \,|\, n}} 1 \le x \sum_{\substack{k > (\ln x)^4 \\ k \text{ powerful}}} \frac{1}{k} \ll \frac{x}{(\ln x)^2},$$

where for the above estimate we have used the known fact that

$$\#\{k \le y \mid k \text{ powerful}\} \ll \sqrt{y}$$

for all real numbers y (for a more precise statement, see Theorem 14.4 in [3]), together with partial summation. Thus, to establish the estimate (14), it suffices to prove the same upper bound for the number of integers $n \le x$ with $\sigma(n) \in \mathcal{S}$ and $n \notin \mathcal{T}$. Let n be one such integer. Write $n = k\ell$, where k is *powerful*, ℓ is squarefree, and $\gcd(k, \ell) = 1$; then k and ℓ are uniquely determined by n. Let us write

$$f(k) = \prod_{\substack{p^a \,\|\, \sigma(k) \\ p \equiv 3 \pmod 4 \\ a \equiv 1 \pmod 2}} p.$$

Clearly,

$$f(k) \le \sigma(k) \ll k \log_2 k \ll (\ln x)^5.$$

Since $\sigma(n) = \sigma(k)\sigma(\ell) \in \mathcal{S}$, it follows that $\sigma(\ell) \in f(k)\mathcal{S}$. By Corollary 1, we have that

$$\begin{aligned}
\#\{n \le x : \sigma(n) \in \mathcal{S} \text{ and } n \notin \mathcal{T}\} &\le \sum_{\substack{k \le (\ln x)^4 \\ k \text{ powerful}}} \sum_{\substack{\ell \le x/k \\ \ell \text{ sqfree} \\ \sigma(\ell) \in f(k)\mathcal{S}}} 1 \\
&\ll \sum_{\substack{k \le x \\ k \text{ powerful}}} \frac{x}{k(\log(x/kf(k)))^{3/2}} \\
&\ll \frac{x}{(\ln x)^{3/2}} \sum_{\substack{k \le x \\ k \text{ powerful}}} \frac{1}{k} \ll \frac{x}{(\ln x)^{3/2}},
\end{aligned}$$

where we have used the fact that $kf(k) \ll (\ln x)^9$ in the third step. This completes the proof of Theorem 3.

5 Remarks

A well-known asymptotic formula of Landau asserts that

$$\#\{n \le x : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\} \sim C_0 \frac{x}{(\ln x)^{1/2}},$$

where

$$C_0 = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2} = 0.7642\cdots.$$

In view of Theorem 1, it seems reasonable to expect the asymptotic formula

$$\#\{n \le x : \varphi(n) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\} \sim C_1 \frac{x}{(\ln x)^{3/2}} \tag{15}$$

to hold for some constant $C_1 > 0$. More generally, we can ask whether it is true that for any integer $k \ge 1$, there is a constant $C_k > 0$ for which the asymptotic formula

$$\#\{n \le x : \varphi^{(k)}(n) = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\} \sim C_k \frac{x}{(\ln x)^{k+1/2}} \tag{16}$$

holds, where $\varphi^{(k)}(n)$ denotes the k-th iterate of the Euler function. It is likely that any proof of (16) (or even (15)) will require an asymptotic formula for the number primes $p \le x$ with $p - 1 = a^2 + b^2$ (that is, a proof of Motohashi's conjecture). On the other hand, it might be possible to establish the precise rate of growth of the function on the left side of (16) when $k \ge 2$, perhaps by extending the ideas of this paper. It would also be interesting to have heuristic formulas for the constants $\{C_k : k \ge 1\}$.

Of course, similar questions can be posed for the Dedekind function and for the sum of divisors function as well.

References

[1] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Mathematical Society Monographs, No. 4, Academic Press, London-New York, 1974.

[2] C. Hooley, 'On the representation of a number as the sum of two squares and a prime', *Acta Math.*, **97** (1957), 189–210.

[3] A. Ivić, *The Riemann Zeta-Function. Theory and Applications*, Dover, Mineola, NY, 2003.

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

[5] H. Iwaniec, 'Primes represented by quadratic polynomials in two variables', *Acta Arith.*, **24** (1974), 435–459.

[6] Y. Motohashi, 'On the distribution of prime numbers which are of the form $x^2 + y^2 + 1$', *Acta Arith.*, **16** (1970), 351–363.

[7] Y. Motohashi, 'On the distribution of prime numbers which are of the form x^2+y^2+1, II', *Acta Math. Acad. Sci. Hung.*, **22** (1971), 207–210.

[8] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, University Press, Cambridge, UK, 1995.

[9] K. Williams, 'Mertens' theorem for arithmetical progressions', *J. Number Theory*, **6** (1974), 353–359.