

UPPER BOUNDS ON THE SOLUTIONS TO $n = p + m^2$

A. NAYEBI

Communicated by Michel Waldschmidt

ABSTRACT. Hardy and Littlewood conjectured that every large integer n that is not a square is the sum of a prime and a square. They believed that the number $\mathcal{R}(n)$ of such representations for $n = p + m^2$ is asymptotically given by

$$\mathcal{R}(n) \sim \frac{\sqrt{n}}{\log n} \prod_{p=3}^{\infty} \left(1 - \frac{1}{p-1} \left(\frac{n}{p}\right)\right),$$

where p is a prime, m is an integer, and $\left(\frac{n}{p}\right)$ denotes the Legendre symbol. Unfortunately, as we will later point out, this conjecture is difficult to prove and not *all* integers that are nonsquares can be represented as the sum of a prime and a square. Instead in this paper we prove two upper bounds for $\mathcal{R}(n)$ for $n \leq N$. The first upper bound applies to *all* $n \leq N$. The second upper bound depends on the possible existence of the Siegel zero, and assumes its existence, and applies to all $N/2 < n \leq N$ but at most $\ll N^{1-\delta_1}$ of these integers, where N is a sufficiently large positive integer and $0 < \delta_1 \leq 0.000025$.

1. Introduction

1.1. Background Information. In this paper, we consider the following conjecture of Hardy and Littlewood [4]:

MSC(2000): Primary: 11P32; Secondary: 11P55.

Keywords: Additive, Conjecture H, circle method.

Received: 16 January 2010, Accepted: 1 June 2010.

© 2011 Iranian Mathematical Society.

Conjecture 1.1 (Hardy-Littlewood; Conjecture H). *Every large integer n that is not a square is the sum of a prime and a square. The number $\mathcal{R}(n)$ of representations for $n = p + m^2$ is given asymptotically by*

$$(1.1) \quad \mathcal{R}(n) \sim \mathcal{P}(n) \frac{\sqrt{n}}{\log n}$$

$$(1.2) \quad \mathcal{P}(n) = \prod_{p=3}^{\infty} \left(1 - \frac{1}{p-1} \left(\frac{n}{p} \right) \right),$$

where p is a prime, m is an integer, and $\left(\frac{n}{p} \right)$ denotes the Legendre symbol.

In 1937, Davenport and Heilbronn [5] proved that Conjecture 1.1 holds for *almost* all natural numbers. In fact, they showed that if we define the exceptional set as

$$(1.3) \quad E(N) := \{n \leq N : n \text{ is neither a square nor the sum of a prime and a square}\},$$

then

$$(1.4) \quad |E(N)| \ll N \log^c N$$

for some $c < 0$. In 1968, Mieh [12] proved that (1.4) holds for arbitrary $c < 0$. Using the approach of Hardy and Littlewood [4] via theta-functions, Vinogradov [2] proved that there exist *effectively computable* constants $c < 1$ and $\gamma > 0$ such that $|E(N)| \leq \gamma N^c$. Br  nner, Perelli, and Pintz [9] used the methods of Montgomery and Vaughan [7] to prove the same result. Polyakov [11] independently demonstrated that the results of Vinogradov [2] hold without using Siegel's theorem, thereby enabling him to attain effective results. Basing his methods on those of [9], Wang [13] made the computation of c more rigorous and proved,

$$(1.5) \quad |E(N)| \ll N^{0.99}.$$

The exponent was subsequently improved by Li [8] to 0.9819.

Some work has been done in an attempt to verify the asymptotic formula for $\mathcal{R}(n)$ in Conjecture 1.1. Mieh [12] proved that

$$(1.6) \quad \mathcal{R}(n) = \mathcal{P}(n) \frac{\sqrt{n}}{\log n} \left(1 + O \left(\frac{\log \log n}{\log n} \right) \right)$$

holds for all but $O(N(\log N)^A)$ positive integers $n \leq N$ with any fixed $A < 0$. Polyakov also attempted to make progress on Conjecture 1.1

[10] [11]. For all but $\ll N \cdot \exp\{-c\sqrt{\log N}\}$ integers $n \leq N$, he obtained the following

$$(1.7) \quad \mathcal{R}(n) = \mathcal{P}(n) \frac{\sqrt{n}}{\log n} \left(1 + O \left(\exp \left\{ - \frac{\sqrt{\log n}}{\log^3 \log n} \right\} \right) \right).$$

Unfortunately, a mistake occurs in one of Polyakov's estimates [10], and "due to the possible existence of the Siegel zero, such a result is unlikely to be provable in the present state of knowledge" [9, pp. 347-8].

In this paper, the first upper bound we prove for $\mathcal{R}(n)$ holds for *all* $n \leq N$ (N sufficiently large) with no exceptions. The second upper bound is achieved by way of Polyakov's [11] methods, although he uses his methods for the entirely different purpose of determining the cardinality of the exceptional set $E(N)$. This second upper bound assumes the possible existence of the Siegel zero, and consequently has an exceptional set. However, before we present the main results of this paper, we first define some nomenclature.

1.2. Notation. We will use some of the same notation used by Polyakov [11] for simplicity:

Suppose m and u are natural numbers; p is a prime; N is a sufficiently large positive integer; μ is the Möbius function; φ is Euler's totient function; $\mathcal{P}(n) := \prod_{p=3}^{\infty} \left(1 - \frac{1}{p-1} \left(\frac{n}{p} \right) \right)$ where (n/p) is the Legendre symbol; $0 < \delta \leq 0.0025$; $0 < \delta_1 \leq 0.000025$; $\epsilon > 0$; $Q = N^{\epsilon\delta}$; $\tau = N^{1-46\delta}$; $s = \sigma + it$ is a complex variable; c, c_1, c_2, \dots are absolute positive constants; χ is a Dirichlet character mod q ; χ_0 is the principal character mod q ; χ^* is the primitive character corresponding to χ ; \sum_{χ} is the summation over all characters mod q ; $\sum_{a \leq q}^*$ is the summation over a reduced system of residues mod q ; $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ is the L -function defined for $\sigma > 1$; β , also known as a Siegel zero, is an exceptional real zero (if it exists) in the region $\Re(s) \geq c \log^{-1} Q$ for the L -function $L(s, \tilde{\chi})$ with the real primitive character $\tilde{\chi}$ mod \tilde{r} where $\tilde{r} \leq Q = \exp\{\log^{1/2} N\}$; $\epsilon(\beta) = \epsilon(\beta, Q)$ is a function equal to 1 if β exists and is equal to 0 if otherwise; α and x are real variables; $e(x) = \exp\{2\pi i x\}$; B is a bounded quantity whose absolute value is bounded above by some constant that is independent of n and N .

1.3. Main Theorem. Now we are ready to state the central results of this paper.

Theorem 1.2. For all $n \leq N$,

$$(1.8) \quad \mathcal{R}(n) \leq 2 \cdot \mathcal{P}(n) \frac{N}{\log N} \left(1 + O \left(\frac{\log \log 3N}{\log N} \right) \right).$$

For all $N/2 < n \leq N$ except for at most $\ll N^{1-\delta_1}$ of these integers, if the Siegel zero β does indeed exist,

$$(1.9) \quad \mathcal{R}(n) \ll_N \mathcal{P}(n) N^{1/2} \exp \left\{ \frac{-c}{\delta} \right\} (1 - \beta) \log N.$$

If the Siegel zero does not exist, then the $(1 - \beta) \log N$ term in (1.9) is removed and the resultant bound holds for all $N/2 < n \leq N$ except for at most $\ll N^{1-\delta}$ of these integers. Note that δ and δ_1 are fixed, where $0 < \delta \leq 0.0025$ and $0 < \delta_1 \leq 0.000025$, as defined in §1.2.

Although we have not proven Conjecture 1.1 (which is unlikely to be proven in the current state of knowledge anyway), our results are of interest. The upper bounds in Theorem 1.2 involve $\mathcal{P}(n)$ (just like Conjecture 1.1 does), the treatment of the conjectural Siegel zero is explicit, the cardinality of the exceptional set in (1.9) is rather small since it is contained within the cardinality of the exceptional set given by Brünner, Perelli, and Pintz [9] (see our §1.1). Moreover, under the likely assumption that the Siegel zero β does not exist, the upper bound in (1.8) has no exceptions.

2. Preliminaries

In order to prove Theorem 1.2, we introduce some auxiliary functions and lemmas about these functions. We should inform the reader that any lemma that is presented without proof in this paper means that it has already been stated and proven by Polyakov [11]. Put

$$(2.1) \quad \begin{aligned} P(\alpha) &:= \sum_{Q < p \leq N} \log p e(p\alpha) \\ F(\alpha) &:= \sum_{\sqrt{N}/2 < n \leq \sqrt{N}} e(m^2 \alpha) \\ R(n) &:= \sum_{\substack{Q < p \leq N \\ n = p + m^2}} \sum_{\sqrt{N}/2 < m \leq \sqrt{N}} \log p. \end{aligned}$$

Note that $R(n)$ and $\mathcal{R}(n)$ are easily related by partial summation. An upper bound of \ll -type on $R(n)$ is applicable to $\mathcal{R}(n)$. Thus, for $N/2 <$

$$n \leq N,$$

$$(2.2) \quad R(n) = \int_0^1 P(\alpha)F(\alpha)e(-n\alpha)d\alpha = \int_{-1/\tau}^{1-1/\tau} P(\alpha)F(\alpha)e(-n\alpha)d\alpha.$$

Dirichlet's approximation theorem leads us to the notion that each $\alpha \in [-1/\tau, 1 - 1/\tau]$ can be represented in the form $\alpha = \frac{a}{q} + z$ for $1 \leq q \leq z$, $\gcd(a, q) = 1$, and $|z| \leq \frac{1}{q\tau}$. Let

$$(2.3) \quad \begin{aligned} M_1 &:= \{\alpha \in [-1/\tau, 1 - 1/\tau] : \text{for which } q \leq Q \\ &\quad \text{is in the indicated representation}\} \\ M_2 &:= \{\alpha \in [-1/\tau, 1 - 1/\tau] : \text{for which } q \leq Q \\ &\quad \text{is not in the indicated representation}\}. \end{aligned}$$

Now, put $R(n) = R_1(n) + R_2(n)$, where

$$(2.4) \quad \begin{aligned} R_1(n) &= \int_{M_1} P(\alpha)F(\alpha)e(-n\alpha)d\alpha \\ R_2(n) &= \int_{M_2} P(\alpha)F(\alpha)e(-n\alpha)d\alpha. \end{aligned}$$

Lemma 2.1. *For all $N/2 < n \leq N$ except for $\ll N^{1-\delta}$ integers n ,*

$$(2.5) \quad R_2(n) \ll n^{1/2-2\delta}.$$

Proof. By using Parseval's identity to show that

$$(2.6) \quad \sum_{n \leq N} R_2^2(n) \leq \max_{M_1} |F(\alpha)|^2 \int_0^1 |P(\alpha)|^2 d\alpha$$

where

$$(2.7) \quad \int_0^1 |P(\alpha)|^2 d\alpha = \sum_{Q < p \leq N} \log^2 N \ll N \log N,$$

Polyakov [11] proves that

$$(2.8) \quad \sum_{n \leq N} R_2^2(n) \leq N^{2-5\delta},$$

which implies our lemma. \square

As Polyakov [11] mentions, the following lemma is due to Karatsuba [1, Ch. IX, Sec. 2].

Lemma 2.2. *There exists a constant $c > 0$ such that $L(s, \chi^*) \neq 0$ for $\sigma \geq 1 - c \log^{-1} Q$ and for all primitive characters $\chi^* \pmod{r}$, where $r \leq Q$ and $Q \geq 2$, with the possible exception of at most one primitive character $\tilde{\chi} \pmod{\tilde{r}}$. If this character exists, then it is a quadratic character and the unique Siegel zero β for the L -function $L(s, \tilde{\chi})$ satisfies*

$$(2.9) \quad c_1 \tilde{r}^{-1/2} \log^{-2} \tilde{r} \leq 1 - \beta \leq c \log^{-1} Q.$$

Also, if there are any $L(s, \chi)$, where χ is a real character \pmod{q} , such that $L(\beta, \chi) = 0$ in (2.9), then $q \equiv 0 \pmod{\tilde{r}}$.

Next, put

$$(2.10) \quad \begin{aligned} V(a, q) &:= \sum_{1 \leq m \leq q} e\left(m^2 \frac{a}{q}\right) \\ K(z) &:= \sum_{N/4 < m \leq N} \frac{e(mz)}{2\sqrt{m}}. \end{aligned}$$

Thus, $R_1(n) = R_1^{(1)}(n) + R_1^{(2)}(n) + R_1^{(3)}(n)$ if

$$\begin{aligned} R_1^{(1)}(n) &= \left(\sum_{q \leq Q} \frac{\mu(q)}{q\varphi(q)} \sum_{a \leq q}^* V(a, q) e\left(-n \frac{a}{q}\right) \right) \\ &\quad \times \left(\int_{-1/(q\tau)}^{1/(q\tau)} T(z, 1) K(z) e(-nz) dz \right. \\ &\quad \left. - \epsilon(\beta) \sum_{\substack{q \leq Q \\ q \equiv 0 \pmod{\tilde{r}}}} \frac{\tau(\tilde{\chi}\chi_0)}{q\varphi(q)} \sum_{a \leq q}^* V(a, q) \tilde{\chi}(a) \right) \\ &\quad \times \left(e\left(-n \frac{a}{q}\right) \int_{-1/(q\tau)}^{1/q(\tau)} T(z, \beta) K(z) e(-nz) dz \right) \\ R_1^{(2)}(n) &= \sum_{q \leq Q} \sum_{a \leq q}^* \int_{-1/(q\tau)}^{1/(q\tau)} P\left(\frac{a}{q} + z\right) \left(F\left(\frac{a}{q} + z\right) - \frac{V(a, q)}{q} K(z) \right) \\ &\quad e\left(-n \left(\frac{a}{q} + z\right)\right) dz \end{aligned}$$

$$R_1^{(3)}(n) = \sum_{q \leq Q} \frac{1}{q\varphi(q)} \sum_{a \leq q} {}^*V(a, q) e\left(-n \frac{a}{q}\right) \sum_{\chi} \chi(a) \tau(\tilde{\chi}) \\ \times \int_{-1/(q\tau)}^{1/(q\tau)} K(z) W(\chi, z) e(-nz) dz,$$

where, as defined by Montgomery and Vaughan [7],

$$T(z, \gamma) = \sum_{Q < u \leq N} u^{\gamma-1} e(uz)$$

and

$$W(\chi, z) = \sum_{Q < p \leq N} \chi(p) \log p e(pz)$$

in which $\chi \neq \chi_0$ and $\chi \neq \tilde{\chi}\chi_0$, and $\tau(\chi)$ is the Gauss sum.

In order to develop an upper bound for $R_1(n)$ we need three more lemmas.

Lemma 2.3. For $N/2 < n \leq N$,

$$R_1^{(1)}(n) \\ = \Sigma(n, Q) \sum_{n=u+m} \frac{1}{2\sqrt{m}} - \epsilon(\beta) \Sigma(n, Q, \beta) \sum_{n=u+m} \frac{u^{\beta-1}}{2\sqrt{m}} + BN^{1/2-34\delta} \quad (2.11)$$

where

$$\Sigma(n, Q) = \sum_{q \leq Q} \frac{\mu(q)}{q\varphi(q)} \sum_{a \leq q} {}^*V(a, q) e\left(-n \frac{a}{q}\right) \quad (2.12)$$

$$\Sigma(n, Q, \beta) = \sum_{\substack{q \leq Q \\ q \equiv 0 \pmod{\tilde{r}}} \frac{\tau(\tilde{\chi}\chi_0)}{q\varphi(q)} \sum_{a \leq q} {}^*V(a, q) \tilde{\chi}(a) e\left(-n \frac{a}{q}\right). \quad (2.13)$$

Lemma 2.4. It follows from the relation given in (2.7) that for all $N/2 < n \leq N$,

$$R_1^{(2)}(n) \ll N \sum_{q \leq Q} \sum_{a \leq q} {}^* \int_{-1/(q\tau)}^{1/(q\tau)} \left(q + \frac{N}{q\tau}\right) dz. \quad (2.14)$$

Lemma 2.5. Put $q = kr$ where $\gcd(k, r) = 1$ (because otherwise $R_1^{(3)}(n)$ would be 0), then for all $N/2 < n \leq N$,

$$(2.15) \quad \begin{aligned} R_1^{(3)}(n) = & \left(\sum_{r \leq Q} \frac{1}{r\varphi(r)} \sum_{\chi^* \pmod r} \tau(\overline{\chi^*}) \sum_{a_1 \leq r} {}^*V(a_1, r) \right) \\ & \cdot \left(\chi^*(a_1) e\left(-n \frac{a_1}{r}\right) \int_{-1/r\tau}^{1/r\tau} K(z) W(\chi^*, z) e(-nz) dz \right) \\ & \cdot \left(\sum_{\substack{k \leq Q/r \\ \gcd(k, r)=1}} \frac{\mu(k)}{k\varphi(k)} \sum_{a \leq k} {}^*V(a, k) e\left(-n \frac{a}{k}\right) + BN^{1/2-2\delta} \right). \end{aligned}$$

The last set of two lemmas deals with auxiliary functions that will later be useful in developing an upper bound for $R(n)$.

Lemma 2.6. Let $\mathcal{P}(n)$ be defined as in §1.2, then for all $n \leq N$, except for $\ll N^{0.7}$ of these integers,

$$(2.16) \quad \Sigma(n, Q) = \mathcal{P}(n) + Bn^{-2\delta_1}.$$

Lemma 2.7. If $r \leq Q$, then for all $n \leq N$, except for $\ll N^{1-\delta_1}$ of these integers, $\gcd(t, n) \leq N^{1-\delta_1}$.

Now we are ready to prove our main theorem.

3. Proof of Theorem 1.2

Since $R(n) = R_1(n) + R_2(n)$ and in Lemma 2.1 we prove an upper bound for $R_2(n)$, all we have to do is to prove an upper bound for $R_1(n)$. In order to do so, we examine $R_1^{(1)}(n)$, $R_1^{(2)}(n)$, and $R_1^{(3)}(n)$, individually.

In (2.11) of Lemma 2.3, a simplified expression is given for $R_1^{(1)}(n)$. $\Sigma(n, Q)$ is evaluated in Lemma 2.6. Similarly, $\epsilon(\beta)$ is defined to be either 1 or 0 depending on the existence of β . Hence, in order to prove an upper bound for $R_1^{(1)}(n)$, we must prove upper bounds for $\sum_{n=u+m} \frac{1}{2\sqrt{m}}$, $\Sigma(n, Q, \beta)$, and $u^{\beta-1}$.

It follows from Lemma 2.7 that for all $N/2 < n \leq N$, with $t = \tilde{r}$, except for $\ll N^{1-\delta_1}$ of these integers, when $\tilde{r} > N^{3.6\delta_1}$ [11],

$$(3.1) \quad \Sigma(n, Q, \beta) \ll n^{-2\delta_1}.$$

From Lemma 2.2, it follows that for $Q < u \leq N$,

$$(3.2) \quad 1 - u^{\beta-1} = \int_{\beta}^1 u^{s-1} \log u ds \geq c_3(1 - \beta) \log n,$$

which implies

$$(3.3) \quad u^{\beta-1} \leq 1 - c_3(1 - \beta) \log n.$$

It is easy to see that

$$(3.4) \quad \sum_{n=u+m} \frac{1}{2\sqrt{m}} \leq \frac{\zeta(2)}{2}.$$

As a result, if the Siegel zero β exists, then

$$(3.5) \quad R_1^{(1)}(n) \ll \left(\sum_{n=u+m} \frac{1}{2\sqrt{m}} \right) \times \left(\mathcal{P}(n) + Bn^{-2\delta_1} - n^{-2\delta_1}(1 - c_3(1 - \beta) \log n) \right) + BN^{1/2-34\delta}.$$

If the Siegel zero β does not exist, then

$$(3.6) \quad R_1^{(1)}(n) \ll \left(\sum_{n=u+m} \frac{1}{2\sqrt{m}} \right) \left(\mathcal{P}(n) + Bn^{-2\delta_1} \right) + BN^{1/2-34\delta}.$$

We now move on to formulate an upper bound for $R_1^{(2)}(n)$. This is a rather easy task to complete since Polyakov [11] already proves it. Using (2.7), it follows from Lemma 2.3,

$$(3.7) \quad R_1^{(2)}(n) \ll N^{100\delta}.$$

Lastly, we prove an upper bound for $R_1^{(3)}(n)$. If we consider the sum in (2.15) of Lemma 2.5 for $r \leq N^{5\delta}$ then we can denote this first partial sum as $R_1^{(3.1)}(n)$. If we consider the same sum for $N^{5\delta} < r \leq Q$, then we can denote this second partial sum as $R_1^{(3.2)}(n)$. Hence, $R_1^{(3)}(n) = R_1^{(3.1)}(n) + R_1^{(3.2)}(n)$. Polyakov [11] proves that for all $n \leq N$ except for $\ll N^{0.7}$ of these integers,

$$(3.8) \quad R_1^{(3.1)}(n) \ll (\mathcal{P}(n) + Bn^{-2\delta_1}) \sum_{r \leq N^{5\delta}} \sum_{\chi^* \pmod r} \left(\int_{-1/(r\tau)}^{1/(r\tau)} |W(\chi^*, z)|^2 dz \right)^{1/2}.$$

The double sum in (3.8) was considered by Montgomery and Vaughan [7] who showed that if the Siegel zero β exists for $n \leq N$,

$$(3.9) \quad \sum_{r \leq N^{5\delta}} \sum_{\chi^* \pmod r} \left(\int_{-1/(r\tau)}^{1/(r\tau)} |W(\chi^*, z)|^2 dz \right)^{1/2} \ll N^{1/2} \exp \left\{ \frac{-c}{\delta} \right\} (1 - \beta) \log N,$$

and in the absence of an exceptional zero β ,

$$(3.10) \quad \sum_{r \leq N^{5\delta}} \sum_{\chi^* \pmod r} \left(\int_{-1/(r\tau)}^{1/(r\tau)} |W(\chi^*, z)|^2 dz \right)^{1/2} \ll N^{1/2} \exp \left\{ \frac{-c}{\delta} \right\}.$$

With the assistance of Lemma 2.7, with $t = r$ and $\delta_1 = \delta$, Polyakov [11] proves that independent of the existence of the Siegel zero β , for all $N/2 < n \leq N$, except for $\ll N^{1-\delta}$ of these integers,

$$(3.11) \quad R_1^{(3.2)}(n) \ll N^{1/2-2\delta}.$$

Combining our results yields two upper bounds for $R(n)$ for $N/2 < n \leq N$. The first bound assumes the existence of β and holds for all but at most $\ll N^{1-\delta_1}$ of these integers,

$$(3.12) \quad R(n) \ll_N \mathcal{P}(n) N^{1/2} \exp \left\{ \frac{-c}{\delta} \right\} (1 - \beta) \log N.$$

Note that we only considered the case of $\tilde{r} > N^{3.6\delta_1}$ when obtaining the estimate in (3.12). For $\tilde{r} \leq N^{3.6\delta_1}$, we have then that for all $n \leq N$ except for $\ll N^{0.7}$ of these integers, $|\Sigma(n, Q, \beta)| \leq \mathcal{P}(n) + Bn^{-2\delta_1}$, from which one derives that the bound in (3.12) still holds.

The second bound assumes that β does not exist, and holds for all $N/2 < n \leq N$ except for at most $\ll N^{1-\delta}$ of these integers,

$$(3.13) \quad R(n) \ll_N \mathcal{P}(n) N^{1/2} \exp \left\{ -\frac{c}{\delta} \right\}.$$

We can also obtain an unconditional upper bound on $\mathcal{R}(n)$ of the correct order of magnitude with no exceptions by way of sieve methods. We will derive an upper bound on $\mathcal{R}_k(n)$, the number of representations for the equation $n = p + m^k$ where $k \geq 2$, and then take the case for $k = 2$.

Let \mathcal{A} stand for a general integer sequence to be “sifted” and let \mathfrak{P} stand for a “sifting” set of primes. Moreover, $S(\mathcal{A}; \mathfrak{P}, z)$ is a sifting function where $z \geq 2$ is a real number. In the case of the present problem, we are sifting the set of numbers $n - m^2$ in order to estimate

how often it is prime. The appropriate method we will utilize is to obtain a Selberg upper bound for $S(\mathcal{A}; \mathfrak{P}, z)$. Typically, an upper bound produced by Selberg's method is of \ll -type; however, by incorporating several important theorems of Halberstam and Richert [6], more explicit estimates can be yielded. We should note that neither the problem of the sum of a prime and a square nor the problem of the sum of a prime and a k -th power is dealt with in [6].

The sequence that is to be sifted for $1 < Y \leq N$ is

$$\mathcal{A} = \{n - m^k : N - Y < n \leq N\}$$

From Theorem 5.3 of Halberstam and Richert [6], we let $F(n)$ to be a distinct irreducible polynomial with integral and positive leading coefficients, and let $\rho_k(p, n)$ denote the number of solutions to the congruence

$$m^k - n \equiv 0 \pmod{p},$$

with n constant for the purposes of the congruence. Also, N and Y are real numbers satisfying

$$1 < Y \leq N.$$

Hence from [6] and taking $g = 1$,

$$\begin{aligned} |\{n : N - Y < n \leq N, n - m^k = p\}| &\leq 2 \prod_p \left(1 - \frac{\rho_k(p, n) - 1}{p - 1}\right) \\ &\quad \cdot \frac{Y}{\log Y} \left(1 + O\left(\frac{\log \log 3Y}{\log Y}\right)\right). \end{aligned}$$

Now we take the case for $k = 2$. Thus for $Y = N$,

$$\begin{aligned} (3.14) \quad |\{n : 0 < n \leq N, n - m^2 = p\}| &\leq 2 \prod_p \left(1 - \frac{\left(\frac{n}{p}\right)}{p - 1}\right) \\ &\quad \cdot \frac{N}{\log N} \left(1 + O\left(\frac{\log \log 3N}{\log N}\right)\right). \end{aligned}$$

Theorem 1.2 follows. Note that the O constants may be subject to the dependency mentioned in Remark 1 of Halberstam and Richert [6, Ch. 5, Sec. 6].

4. A note on the combinatorial sieve

Of course, Selberg's method is not the only sieve method that can be used to obtain an upper bound on $\mathcal{R}(n)$ for $n \leq N$ with no exceptions. For instance, we can obtain an upper bound for $S(\mathcal{A}; \mathfrak{P}, z)$ via a combinatorial sieve, as Zaccagnini [3] mentions. Hence, as in the derivation of (3.14), our upper bound will be applicable to $\mathcal{R}_k(n)$ and then we will take the case for $k = 2$. We proceed as follows.

The sequence that is to be sifted for $u \geq 1$ and $N^{1/u} \geq 2$ is

$$\mathcal{A} = \{n - m^k : 0 \leq n \leq N\}$$

Lemma 4.1. *Let $F_1(n), \dots, F_g(n)$ be distinct irreducible polynomials with integral and positive leading coefficients where $F(n) = F_1(n) \cdots F_g(n)$. Let $\rho(p, n)$ denote the number of solutions to the congruence*

$$F(n) \equiv 0 \pmod{p}.$$

Assume that for all primes p

$$\rho(p, n) < p.$$

Let $q = q(N, u)$ denote a number having no prime divisors less than $N^{1/u}$ and satisfying $\frac{\log q}{\log N} \ll 1$.

Then

$$\begin{aligned} (4.1) \quad & |\{n : 0 \leq n \leq N, F_i(n) = q_i \text{ for } i = 1, \dots, g\}| \\ &= N \prod_{p < N^{1/u}} \left(1 - \frac{\rho(p, n)}{p}\right) \left\{1 + O_F(\exp\{-u(\log u - \log \log 3u - \log g - 2)\}) + O_F(\exp\{-\sqrt{\log N}\})\right\}. \end{aligned}$$

Proof. Lemma 4.1 is Theorem 2.6 of Halberstam and Richert [6]. \square

Remark 4.2. *The O constant in (4.1) at most depends upon the degrees and coefficients of F .*

Note that as stated by Halberstam and Richert [6], the expression to the right side of the equality in (4.1) is equivalent to

$$(4.2) \quad (u \cdot \exp\{-\gamma\})^g \prod_p \left(1 - \frac{\rho_k(p, n) - 1}{p - 1}\right) \left(1 - \frac{1}{p}\right)^{-g+1} \frac{N}{\log N} \\ \cdot \left(1 + O(\exp\{-u(\log u - \log \log 3u - \log g - 2)\}) + O\left(\frac{u}{\log N}\right)\right).$$

We take $g = 1$. Hence, we obtain from Lemma 4.1 and (4.2) an upper bound on $\mathcal{R}_k(n)$ of the correct order of magnitude

$$|\{n : 0 < n \leq N, n - m^k = p\}| \\ \leq (u \cdot \exp\{-\gamma\}) \prod_p \left(1 - \frac{\rho_k(p, n) - 1}{p - 1}\right) \frac{N}{\log N} \\ \times \left(1 + O(\exp\{-u(\log u - \log \log 3u - 2)\}) + O\left(\frac{u}{\log N}\right)\right).$$

For $k = 2$ and $n \leq N$ sufficiently large ($N^{1/u} \geq 2$ and $u \geq 1$), we have

$$(4.3) \quad \mathcal{R}(n) \leq (u \cdot \exp\{-\gamma\}) \mathcal{P}(n) \frac{N}{\log N} \\ \cdot \left(1 + O(\exp\{-u(\log u - \log \log 3u - 2)\}) + O\left(\frac{u}{\log N}\right)\right).$$

As in (3.14), the upper bound achieved in (4.3) has no exceptions for $n \leq N$. Note that the O constants may be subject to the dependency mentioned in Remark 4.2.

Acknowledgments

The author wishes to thank Alberto Perelli, Alessandro Languasco, Charles R. Greathouse IV, and the anonymous referee(s) for their assistance and helpful comments. The author is also grateful to David H. Low and Mohammad S. Moslehian for assisting with any typesetting issues.

REFERENCES

- [1] A. A. Karatsuba, *Principles of Analytic Number Theory*, (Russian), Second edition, "Nauka", Moscow, 1983.
- [2] A. I. Vinogradov, The binary Hardy-Littlewood problem, (Russian), *Acta Arith.* **46** (1985) 33–56.
- [3] A. Zaccagnini, Additive Problems with Prime Numbers, Number theory II, *Rend. Sem. Mat. Univ. Politec. Torino* **4** (1995) 471–486.
- [4] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio numerorum', III: On the expression of a number as a sum of primes, *Acta Math.* **44** (1923) 1–70.
- [5] H. Davenport and H. Heilbronn, Note on a result in the additive theory of numbers, *Proc. London Math. Soc.* **43** (1937) 142–151.
- [6] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Mathematical Society Monographs, Academic Press, London-New York, 1974.
- [7] H. L. Montgomery and R. C. Vaughan, The exceptional set in Goldbach's problem, *Acta Arith.* **27** (1975) 353–370.
- [8] H. Li, The exceptional set for the sum of a prime and a square, *Acta Math. Hungar.* **99** (2003) 123–141.
- [9] R. Br  nner, A. Perelli, and J. Pintz, The exceptional set for the sum of a prime and a square, *Acta Math. Hungar.* **53** (1989) 347–365.
- [10] I. V. Polyakov, On the exceptional set for the sum of a prime and a perfect square, Translated in: *Math. USSR, Izv.* **19** (1982) 611–641.
- [11] I. V. Polyakov, Sum of a prime and a square, (English, Russian original) *Math. Notes* **47**(4) 373–380 (1990), translation from: *Mat. Zametki* **47**(4) 90–99 (1990).
- [12] R. J. Miech, On the equation $n = p + x^2$, *Trans. Amer. Math. Soc.* **130** (1968) 494–512.
- [13] T. Wang, On the Exceptional Set for the Equation $n = p + k^2$, *Acta Math. Sin. (N. S.)* **11** (1995) 156–167.

Aran Nayebi

727 Moreno Avenue, Palo Alto, California, USA 94303-3618

Email: aran.nayebi@gmail.com