ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

ON EXCEPTIONAL SETS FOR NUMBERS REPRESENTABLE BY BINARY SUMS

SHUNG-FU CHIU AND MING-CHIT LIU

Dedicated to Prof. Wolfgang Schmidt on the occasion of his 60th birthday

1. Introduction and main results. We shall consider some problems concerning parts of Conjectures (**H**), (**I**) and (**L**) posed by Hardy and Littlewood [**6**], namely,

(**H**) Every large number is either a square or the sum of a prime and a square.

(**I**) Every large odd number is the sum of a prime and the double of a square.

(**L**) Every large number is either a cube or the sum of a prime and a (positive) cube.

Concerning (**H**) and (**L**), bounds for exceptional sets were obtained by Davenport and Heilbronn [**4**], and Miech [**13**]. The best known results were obtained by Brünner, Perelli and Pintz [**2**], and Zaccagnini [**24**] (Vinogradov [**23**] also gave a sketch of a different proof for the result in Theorem BPP-Z). They proved:

Theorem BPP-Z. *Let $k \geq 2$ be a fixed integer. Then there are positive effectively computable constants $\theta < 1$ and C depending on k only such that*

$$\text{Card}\,\{n \in \mathbf{N} : n \leq X,\ n \text{ is not a sum of a prime and a } k\text{th power}\} \leq CX^{\theta}.$$

On the other hand, Schwarz [**20**] and Plaksin [**17**] considered similar problems concerning (**H**) and (**L**), and could replace the kth power (of an integer) in Theorem BPP-Z by a kth power of a prime. In particular, it was proved:

Received by the editors on January 23, 1995, and in revised form on May 18, 1995.

Theorem P [**17**]. *Let $k \geq 2$ be a fixed integer. Then the number of positive integers $b \leq X$ satisfying $\gcd(b-1, \prod_{(p-1)|k} p) = 1$ such that b is not representable by the form $b = p_1 + p_2^k$, with p_1 and p_2 prime, is $\ll X^\theta$ where $0 < \theta < 1$ depends on k only.*

Here and throughout $\ll$ and $\gg$ are the Vinogradov symbols.

In this paper, we shall present some generalizations of these results to integers representable by binary sums with integer coefficients. Our results contain Theorem BPP-Z and Theorem P as special cases. Our investigation was motivated by the following work on equations with integer coefficients.

(i) Pitman [**16**] and Schmidt [**18, 19**] considered the diagonal equation, $a_1x_1^k + \cdots + a_sx_s^k = 0$ and obtained bounds in terms of the integer coefficients, $a_1, \ldots, a_s$ for nontrivial small integer solutions, $x_1, \ldots, x_s$;

(ii) Baker [**1**] considered the ternary equation, $a_1p_1 + a_2p_2 + a_3p_3 = b$ and obtained a bound in terms of the integer coefficients, a_1, a_2, a_3 for small prime solutions, p_1, p_2, p_3. Recent developments on Baker's problem show some interesting effects of these coefficients (see Section 2 in [**12**] for the relations with Linnik's theorem and the Linnik constant).

Following their direction, we shall consider the representations in Theorems BPP-Z and P with integer coefficients a_1 and a_2 and obtain the best forms of lower bounds in terms of a_1, a_2 for X.

Assume $k \geq 2$ is a fixed integer and a_1, a_2 are any integers satisfying

(1.1)
$$a_1a_2 \neq 0, \qquad \operatorname{Max}\{a_1, a_2\} \geq 1 \quad \text{and} \quad \gcd(a_1, a_2) := (a_1, a_2) = 1.$$

For $q \in \mathbf{N}$ define

(1.2)
$$\begin{cases} \mathcal{N}_1(q) & := \operatorname{Card}\{\langle n_1, n_2\rangle \in \mathbf{N}^2 : n_1, n_2 \leq q, (n_1, q) = 1 \quad \text{and} \\ & \qquad a_1n_1 + a_2n_2^k \equiv b \pmod q\}, \\ \mathcal{N}_2(q) & := \operatorname{Card}\{\langle n_1, n_2\rangle \in \mathbf{N}^2 : n_i \leq q, (n_i, q) = 1, i = 1, 2 \quad \text{and} \\ & \qquad a_1n_1 + a_2n_2^k \equiv b \pmod q\}, \\ \mathcal{N}_3(q) & := \operatorname{Card}\{\langle n_1, n_2\rangle \in \mathbf{N}^2 : n_1, n_2 \leq q, (n_1, q) = 1 \quad \text{and} \\ & \qquad a_1n_1 + a_2P(n_2) \equiv b \pmod q\}, \end{cases}$$

where $P(x) = x^2 + d_1x + d_2$ with d_1 and d_2 being any integers. The

method applied in most work in this field is the Hardy-Littlewood method (or the circle method) and hence, by the nature of this method, we shall restrict our attention to those $b \in \mathbf{N}$ satisfying the condition of congruent solvability,

$$\mathcal{N}_j(q) \geq 1 \quad \text{for each } q \in \mathbf{N}. \tag{1.3}$$

For $X > 1$, and $j = 1, 2, 3$ define

$$W_j(X) := \{b \in \mathbf{N} : b \leq X \text{ and (1.3) holds}\} \tag{1.4}$$

and

(1.5)

$$\begin{cases} E_1(X) & := \{b \in W_1(X) : b = a_1 p + a_2 n^k \text{ is insolvable for } p \text{ prime} \\ & \qquad \text{and } n \in N\}, \\ E_2(X) & := \{b \in W_2(X) : b = a_1 p_1 + a_2 p_2^k \text{ is insolvable for } p_1 \\ & \qquad \text{and } p_2 \text{ prime}\}, \\ E_3(X) & := \{b \in W_3(X) : b = a_1 p + a_2 P(n) \text{ is insolvable for } p \text{ prime}, \\ & \qquad \text{and } n \in N\}. \end{cases}$$

We shall obtain the following bounds on the cardinality of the exceptional sets $E_j(X)$.

Theorem 1. *There exist positive effectively computable constants A and $\theta < 1$ depending on k only such that*

$$\operatorname{Card} E_1(X) \leq X^\theta, \qquad \operatorname{Card} E_2(X) \leq X^\theta$$

whenever $X \geq \operatorname{Max}\{3, |a_1|, |a_2|\}^A$. When $k = 2$ and $X \geq \operatorname{Max}\{3, |a_1|, |a_2|, |d_1|, |d_2|\}^A$, we have

$$\operatorname{Card} E_3(X) \leq X^\theta.$$

The following (Theorem 2) guarantees that there are many elements in $W_j(X)$ so that the bounds in Theorem 1 are nontrivial. Let $\omega(a)$ be the number of prime divisors of the integer a.

Theorem 2. *We have*

$$\begin{aligned}\operatorname{Card} W_1(X) &\geq \operatorname{Card} W_2(X)\\ &\gg X\exp(-\omega(a_1)\log k)(\log\log(3|a_1a_2|))^{-1}\end{aligned}$$

where the implied constant in the $\gg$ *is effectively computable and depends on* k *only. The above inequality also holds for* $\operatorname{Card} W_3(X)$ *when* $k=2$.

Remark 1. The results on $\operatorname{Card} E_1$ and $\operatorname{Card} E_2$ in Theorem 1 contain Theorem BPP-Z and Theorem P, and the results on $\operatorname{Card} E_1$ (when $k=2$) and $\operatorname{Card} E_3$ in Theorem 1 relate to Conjecture (**I**).

Proof. For any prime power p^α and any pair $\langle n_1,n_2\rangle\in\mathbf{N}^2$ with $n_1,n_2\leq p^\alpha$, we have that $p\nmid n_1$ and $n_1+a_2n_2^k\equiv b\pmod{p^\alpha}$ if and only if $a_2n_2^k\not\equiv b\pmod p$ and $n_1\equiv b-a_2n_2^k\pmod{p^\alpha}$. So if $a_1=1$, then

$$\begin{aligned}\mathcal{N}_1(p^\alpha)&=\operatorname{Card}\{\langle n_1,n_2\rangle\in\mathbf{N}^2: n_1,n_2\leq p^\alpha, p\nmid n_1 \text{ and }\\ &\qquad\qquad n_1+a_2n_2^k\equiv b\pmod{p^\alpha}\}\\ &=\operatorname{Card}\{n_2\in\mathbf{N}: n_2\leq p^\alpha \text{ and } a_2n_2^k\not\equiv b\pmod p\}\\ &\begin{cases}=0 & \text{if } p|(a_2,b),\\ =p^\alpha-p^{\alpha-1}(k,p-1) & \text{if } p\nmid a_2b \text{ and } a_2^{-1}b \text{ is a } k\text{-th}\\ & \quad\text{power residue modulo } p,\\ \geq\phi(p^\alpha) & \text{otherwise}\end{cases}\qquad(1.6)\\ &\geq 1\quad\text{whenever } p\nmid(a_2,b).\end{aligned}$$

Here ϕ denotes the Euler totient function and a^{-1} denotes the inverse of the integer a modulo p. Hence, by the multiplicativity of $\mathcal{N}_1(q)$ (which has a proof similar to that of Lemma 3.2 in [**11**], cf. Lemma 4.2 below), we have

(1.7) $\mathcal{N}_1(q)\geq 1$ holds for all $q\in N$ whenever $(a_2,b)=1$ and $a_1=1$.

Set $a_1=1=a_2$. Then $W_1(X)=\{b\in\mathbf{N}: b\leq X\}$ and hence the set $E_1(X)$ in (1.5) becomes the set in Theorem BPP-Z. So our result for $E_1(X)$ in Theorem 1 contains Theorem BPP-Z.

Proof. For $a_1 = 1$ and for given a_2 and b with $(a_2, b) = 1$, we can obtain expressions for $\mathcal{N}_2(p^\alpha)$ similar to those in (1.6); one needs only to replace the only p^α in (1.6) by $\phi(p^\alpha)$. In particular, $\mathcal{N}_2(p^\alpha) = \phi(p^\alpha) - p^{\alpha-1}(k, p-1)$ if $p \nmid a_2 b$ and $a_2^{-1}b$ is a kth power residue modulo p. Then $\mathcal{N}_2(p^\alpha) = 0$ implies $(k, p-1) = p-1$, $p \nmid a_2 b$ and $a_2^{-1}b \equiv x^k \pmod p$ for some x, and hence $\phi(p)|k$, $p \nmid a_2 b$ and $p|a_2^{-1}b - 1$. So, if $a_1 = a_2 = 1$, and b satisfies $(b-1, \prod_{(p-1)|k} p) = 1$ then (1.3) holds for $j = 2$. Therefore, when $a_1 = 1 = a_2$, the set $E_2(X)$ in (1.5) contains the set of b in Theorem P. So our result for $E_2(X)$ in Theorem 1 contains Theorem P.

If we set $a_1 = 1$ and $a_2 = 2$, then the b in the set $E_1(X)$ are odd, since $(a_2, b) = 1$ in (1.7). Then our result for $E_1(X)$ in Theorem 1 pertains not only to (**H**) and (**L**), but also (**I**). Furthermore, when $k = 2$ and $d_1 = d_2 = 0$ (in $P(x)$), we have $E_3(X) = E_1(X)$. So our result for $E_3(X)$ in Theorem 1 concerns (**H**) and (**I**), too. □

Remark 2. The constant A in Theorem 1 must be larger than 1, and so the forms of the lower bounds in the conditions $X \geq \operatorname{Max}\{3, |a_1|, |a_2|\}^A$ and $X \geq \operatorname{Max}\{|a_1|, |a_2|, |d_1|, |d_2|\}^A$ in Theorem 1 are the best possible if we are not concerned with the exact value of each constant A.

Proof. We first consider $E_1(X)$. Suppose the constant $A \leq 1$. Let $a_1 = 1$, $a_2 \geq 3$ and put $X = a_2$ $(\geq \operatorname{Max}\{3, a_1, a_2\}^A)$. Then, for each b with $1 \leq b \leq X$, the equation $b = p + a_2 n^k$ is obviously insolvable for prime p and $n \in \mathbf{N}$ and so $E_1(X) = W_1(X)$. On the other hand, by (1.7) we have $\operatorname{Card} W_1(X) \geq \phi(a_2) = \phi(X)$. It follows that $\operatorname{Card} E_1(X) \gg X/\log\log X > X^\theta$ for any given θ with $0 < \theta < 1$, if a_2 is large. So we must have $A > 1$. The same argument works for $E_3(X)$, since we may consider $d_1 = d_2 = 0$. And a similar argument works for $E_2(X)$ as well. □

The method applied in the proof of Theorem 1 is the Hardy-Littlewood method with an application of Gallagher's theorem [**5**, Theorem 6] (see also [**21**, (3.7)]) on the density estimate of zeros of L-functions. In the proof, we shall consider the existence of the Siegel zeros (cf. (i) in [**2**, p. 348] and Lemma 3.1 in [**24**]). However, we need not consider the P_2-excluded zeros which played an important role in

[**2**] and [**24**] (see (iii) and (iv) in [**2**, p. 348] and [**24**, p. 403]). Therefore, in principle, our proof is simpler than, and different from, [**2**] and [**24**]. On the other hand, our proof is along the same lines as [**10, 11**] and [**9**] (which are developed from [**15**] and [**22**, Section 8.6]) but with a number of technical differences.

In our proof, the "second main term" caused by the possible existence of the Siegel zeros appears in M_3 (see (6.1) below). As in the previous works [**9, 10, 11**], we obtain an asymptotic form for M_3 in our Lemma 6.2(a) and absorb efficiently the effect due to M_3 by the "major main term," M_1, in the proof of our Lemma 6.3. In Lemma 6.4, the M_2 in (6.1) is estimated with the essential help of Gallagher's theorem in the form of our Lemma 3.1 below. We can compensate for the effect due to M_2 by $M_1 + M_3$ in (6.5), and hence prove our main results in Theorem 1 without considering the P_2-excluded zeros.

In order to demonstrate in detail how we can prove Theorem 1 without considering the P_2-excluded zeros and also, in the interest of clarity, we shall present all the essential lemmas which we have to apply. On the other hand, we shall omit the proofs for many of these lemmas when they can be proved by arguments similar to those employed in our previous works [**10, 11**] and [**9**] (although there are, in fact, some technical differences).

The proof for the upper bound of $\operatorname{Card} E_2(X)$ in Theorem 1 is similar to (but more complicated than) the proofs for $\operatorname{Card} E_j(X)$, $j = 1, 3$. Therefore, in Sections 2–6 we shall only consider $E_2(X)$. In Section 7, we shall give a proof for the lower bound of $\operatorname{Card} W_2(X)$ in Theorem 2. Some remarks on our proofs of Theorems 1 and 2 for the cases $j = 1$ and 3 will be given in Section 8.

2. The unit interval's dissection and the minor arcs. Let $X > 1$ be a large number such that

$$X \geq B^{\exp(\delta^{-2})}, \quad \text{where} \quad B := \operatorname{Max}\{3, |a_1|, |a_2|\} \tag{2.1}$$

and $\delta(< 1)$ is a small computable positive constant depending on k only, and define

$$N := 2X, \tag{2.2}$$

$$Q := N^{\delta}, \qquad T := N^{\sqrt{\delta}}, \qquad L := NQ^{-\xi/16}, \quad \text{where} \quad \xi := 4^{-k}, \tag{2.3}$$

and

$$\tau := N^{-1}T^{1/4}. \tag{2.4}$$

Then $Q < T < L < N$ and, by (2.1),

$$Q^{\delta} \geq B \tag{2.5}$$

for δ small enough. Let $k_1 = 1$ and $k_2 = k \geq 2$. For $j = 1, 2$, we write

$$L_j := L^{1/k_j} \quad \text{and} \quad N_j := N^{1/k_j}.$$

In the following, unless specified otherwise, the constants $c_1, c_2, \ldots$ and the implied constants in the symbols $\ll$, $\gg$ and O are effectively computable, positive and depend at most on δ and k.

We shall use $\chi \pmod q$ and $\chi_o \pmod q$ to denote a Dirichlet character and the principal character modulo q, respectively. For any real y and any positive integer q, we write $e(y)$ for $e^{2\pi iy}$ and $e_q(y)$ for $e(y/q)$. For $j = 1, 2$, and any character $\chi \pmod q$, define

$$\begin{cases} S_j(y) := \sum_{L_j < p \leq N_j} (\log p) e(p^{k_j} y) \quad \text{and} \\ S_j(\chi, y) := \sum_{L_j < p \leq N_j} \chi(p) (\log p) e(p^{k_j} y). \end{cases} \tag{2.6}$$

For any integers h, q such that $(h, q) = 1$, $1 \leq h \leq q \leq Q$, let $\mathbf{m}(h, q) := [(h - \tau)/q, (h + \tau)/q]$. These intervals are mutually disjoint and all lie in $[\tau, 1 + \tau]$. We call the intervals $\mathbf{m}(h, q)$ the *major arcs*. The union of the major arcs is denoted by $\mathcal{M}$ and its complement with respect to $[\tau, 1 + \tau]$ is called the *minor arcs*, which is denoted by $\mathcal{M}' := [\tau, 1 + \tau] \setminus \mathcal{M}$. Let

$$\mathcal{I}(b) := \int_{\tau}^{1+\tau} e(-bx) S_1(a_1 x) S_2(a_2 x)\, dx. \tag{2.7}$$

Then we can write

$$\begin{aligned} \mathcal{I}(b) &= \left(\int_{\mathcal{M}} + \int_{\mathcal{M}'} \right) e(-bx) S_1(a_1 x) S_2(a_2 x)\, dx \\ &:= \mathcal{I}_1(b) + \mathcal{I}_2(b). \end{aligned} \tag{2.8}$$

Lemma 2.1. *We have*

$$|\mathcal{I}_2(b)| < N^{1/k}Q^{-3\xi/2}$$

except for at most $XQ^{-\xi/4}$ *values of* b *where* $\xi = 4^{-k}$.

Proof. Following the same arguments as in the proof of Lemma 7.1 [**10**, cf. (7.5)], with the help of Theorem 1 in [**7**] we can obtain, for $k \geq 2$, $S_2(a_2x) \ll N^{1/k}Q^{-7\xi/4}$. Then by Parseval's identity,

$$\begin{aligned}\sum_{b=-\infty}^{\infty} |\mathcal{I}_2(b)|^2 &\leq \sup_{x\in\mathcal{M}'} |S_2(a_2x)|^2 \int_{\mathcal{M}'} |S_1(a_1x)|^2\,dx \\ &\ll N^{1+(2/k)}Q^{-7\xi/2}\log N. \qquad \square\end{aligned}$$

3. Lemmas for the major arcs and a simplification of $\mathcal{I}_1(b)$. In this section, we convert the integral on major arcs, $\mathcal{I}_1(b)$, to a simpler form so that we can obtain a useful lower bound for it in Section 6. To do this, we need the following well-known results on the exceptional zeros and zero-free regions of the Dirichlet L-functions $L(s,\chi)$.

It is known [**3**, p. 96] that there exists a small absolute constant c_1 $(< 1/2)$ such that for any $T > 1$, $L(\sigma + it, \chi) \neq 0$ whenever

$$\sigma > 1 - \frac{c_1}{\log T}, \qquad |t| \leq T$$

for all primitive characters $\chi \pmod q$, $q \leq T$, with the possible exception of at most one real primitive character $\tilde{\chi} \pmod{\tilde{r}}$. If it exists, $L(s,\tilde{\chi})$ has exactly one zero $\tilde{\beta}$, called the *exceptional zero* (the *Siegel zero*), which is real, simple and satisfies

$$\frac{c_2}{\tilde{r}^{1/2}\log^2\tilde{r}} \leq 1 - \tilde{\beta} \leq \frac{c_1}{\log T}, \tag{3.1}$$

for some absolute constant $c_2 > 0$. Moreover, if $\tilde{\beta}$ exists, the zero-free region can be widened [**5**, p. 336].

For $j = 1, 2$, any real y and any $\chi \pmod q$ with $q \leq T$, we define

$$I_j(y) := \int_{L_j}^{N_j} e(x^{k_j}y)\,dx, \qquad \tilde{I}_j(y) := \int_{L_j}^{N_j} x^{\tilde{\beta}-1}e(x^{k_j}y)\,dx$$

and

$$I_j(\chi, y) := \sum_{|\gamma|\le T}{}' \int_{L_j}^{N_j} x^{\rho-1} e(x^{k_j} y)\, dx,$$

where $\sum'_{|\gamma|\le T}$ denotes the summation over all the zeros $\rho = \beta + i\gamma$ of $L(s,\chi)$ in the region $1/2 \le \beta < 1$, excluding $\tilde{\beta}$.

Lemma 3.1. *There is a constant $c_3 > 0$ such that for any real $y \ge N^{1/2k}$ and any $\delta > 0$, we have*

$$\sum_{q\le T} \sideset{}{^*}\sum_{\chi(\mathrm{mod}\, q)} \sum_{|\gamma|\le T}{}' y^{\beta-1} \ll \Omega^2 \exp(-c_3/\sqrt{\delta}),$$

where $\sum^*_{\chi(\mathrm{mod}\, q)}$ is the summation over all primitive characters $\chi \pmod q$, and

$$\Omega := \begin{cases} (1-\tilde{\beta})\log T \quad (\le c_1) & \text{if } \tilde{\beta} \text{ exists,} \\ 1 & \text{otherwise.} \end{cases} \tag{3.2}$$

Here c_3 depends on k only while the implied constant in $\ll$ is absolute.

Proof. This can be proved by the same argument as in the proof of Lemma 2.1 in [**10**]. The proof depends essentially on Gallagher's theorem [**5**, Theorem 6]. □

Lemma 3.1 is applied mainly to the proof of Lemma 6.4 below.

For any character $\chi \pmod q$ and any integer m, let

$$C(\chi, q, m, k) := \sum_{l=1}^{q} \chi(l) e_q(l^k m), \tag{3.3}$$

$$\begin{cases} H_j(h,q,\eta) & := C(\chi_o, q, a_j h, k_j) I_j(a_j \eta) \\ & \quad -\delta_q C(\tilde{\chi}\chi_o, q, a_j h, k_j) \tilde{I}_j(a_j\eta) - G_j(h,q,\eta), \\ & \text{where} \\ G_j(h,q,\eta) & := \sum_{\chi(\mathrm{mod}\, q)} C(\bar{\chi}, q, a_j h, k_j) I_j(\chi, a_j \eta) \end{cases} \tag{3.4}$$

and

$$\delta_q := \begin{cases} 1 & \text{if } \tilde{\chi} \pmod{\tilde{r}} \text{ exists and } \tilde{r} \mid q, \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

By the same arguments as used in [**10**, Section 3], we can generalize all the results in Lemma 3.1 through Corollary 3.4 of [**10**] to any $k_2 \geq 2$. As in the proof of Lemma 3.3 in [**10**] we need our above Lemma 3.1 for the generalization. In particular, by a method similar to the proof of Lemma 3.3 in [**10**], we can prove that

$$I_2(a_2\eta), \qquad \tilde{I}_2(a_2\eta), \qquad I_2(x, a_2\eta) \ll N^{1/k}(L|a_2\eta|)^{-1/2}$$

if $|\eta| > \tau/q$, and that

$$\int_{-\infty}^{\infty} |E_\ell|^2 d\eta \ll \phi(q)^2 N^2 L^{-1} \log N$$

where E_ℓ $(\ell = 1, 2)$ is either

$$C(\chi_o, q, a_j h, k_j) I_j(a_j\eta) \quad \text{or} \quad -\delta_q C(\tilde{\chi}\chi, q, a_j h, k_j)\tilde{I}_j(a_j\eta)$$

or

$$-C(\bar{\chi}, q, a_j h, k_j) I_j(\chi, a_j\eta).$$

Following the same arguments as employed in deriving (3.15) in [**10**], we can prove

$$\mathcal{I}_1(b) = \sum_{q \leq Q} \phi(q)^{-2} \sum_{(h,q)=1} e_q(-bh) \times \int_{-\tau/q}^{\tau/q} e(-b\eta) H_1(h, q, \eta) H_2(h, q, \eta)\, d\eta + O\big(N^{1/k} Q^{-1}\big). \tag{3.6}$$

The next step is to extend the range of the integration in (3.6) to $(-\infty, \infty)$. Note that the product $H_1(h, q, \eta) H_2(h, q, \eta)$ is a sum of at most $(\phi(q) + 2)^2$ terms, each of the form $E_1 E_2$. Then,

$$\begin{aligned} \int_{\mathbf{R}\setminus[-\tau/q, \tau/q]} \big|E_1 E_2\big|^2 d\eta &\ll \big(\phi(q) N^{1/k} (L|a_2\tau/q|)^{-1/2}\big)^2 \int_{-\infty}^{\infty} |E_1|^2 d\eta \\ &\ll N^{1+(2/k)} Q^{-12}. \end{aligned}$$

For the last $\ll$, we also need (2.3) and (2.4). Thus by Parseval's identity,

$$\left|\int_{\mathbf{R}\setminus[-\tau/q,\tau/q]} e(-b\eta)E_1E_2\,d\eta\right| < N^{1/k}Q^{-3}$$

except for at most $\ll NQ^{-6}$ values of b. Therefore when the integration in (3.6) is extended to $(-\infty,\infty)$, the total error induced is

$$\ll \sum_{q\le Q}\phi(q)^{-2}\phi(q)(\phi(q)+2)^2N^{1/k}Q^{-3} \ll N^{1/k}Q^{-1}$$

except for at most $\sum_{q\le Q}\phi(q)(\phi(q)+2)^2NQ^{-6} \le 9NQ^{-2} < XQ^{-1}$ values of b (by (2.2)). Hence, in view of (3.6), we have

$$\begin{aligned}\mathcal{I}_1(b) = {}& \sum_{q\le Q}\phi(q)^{-2}\sum_{(h,q)=1} e_q(-bh)\\ & \times\int_{-\infty}^{\infty} e(-b\eta)H_1(h,q,\eta)H_2(h,q,\eta)\,d\eta\\ & + O\big(N^{1/k}Q^{-1}\big)\quad \text{except for at most } XQ^{-1} \text{ values of } b.\end{aligned}\tag{3.7}$$

We shall use (3.7) to obtain a lower bound for $\mathcal{I}_1(b)$ in Section 6. By this bound, (2.8) and the upper bound for $\mathcal{I}_2(b)$ in Lemma 2.1, we shall prove $\operatorname{Card} E_2(X) \le X^\theta$ in Section 6.

4. Lemmas for the singular series and the singular integral. We are going to present some preliminary lemmas for the singular series $\sum A(q)$ (see (4.3)) and the singular integral (see Lemma 4.6).

We use $\operatorname{ord}_p(n)$ to denote the largest integer ω such that $p^\omega \mid n$. For any prime p, we denote

$$\tau_p := \operatorname{ord}_p(k)+1 \quad\text{and}\quad \theta_p := 1+[2/p]\tag{4.1}$$

where $[x]$ is the largest integer not exceeding x. For any characters $\chi_1,\chi_2 \pmod q$, define

$$\text{(4.2)}\qquad \begin{cases} Z(q) & := Z(q;\chi_1,\chi_2) := \sum_{(h,q)=1} F(h) \\ & \text{and} \\ Y(q) & := Y(q;\chi_1,\chi_2) := \sum_{h=1}^{q} F(h), \end{cases}$$

where $F(h) = e_q(-bh)\prod_{j=1}^{2} C(\chi_j, q, a_j h, k_j)$. Put

$$\text{(4.3)}\qquad A(q) := \phi(q)^{-2} Z(q;\chi_o,\chi_o).$$

Following the same arguments as those employed in proving Lemma 3.1 through Corollary 3.5, and Lemma 3.9 in [**11**], we can prove the following Lemmas 4.1 through 4.6, except for Lemma 4.1(b) and Lemma 4.3(b). So here we shall only provide a brief proof for these two parts of the lemmas.

Lemma 4.1. *Let* $\chi \pmod{p^\alpha}$ *be any character with* $\alpha \geq 0$. *We have*

(a) $C(\chi, p^\alpha, m, k) = 0$ *if* χ *is primitive,* $\alpha \geq 1$ *and* $p \mid m$;

(b) $C(\chi\chi_o, p^t, m, k) = 0$ *if* χ_o *is modulo* p^t, $p \nmid m$ *with* $t \geq \tau_p + \operatorname{Max}\{\theta_p, \alpha\}$;

(c) $|C(\chi, p^\alpha, m, k)| \leq \big(k, \phi(p^\alpha)\big)(2,p)(m, p^\alpha)^{1/2} p^{\alpha/2}$.

Lemma 4.1 is applied in the proofs of Lemma 4.3(a) and (b), and Lemma 4.4(a) and (b).

Lemma 4.2. *$Z(q)$, $Y(q)$, $\mathcal{N}_2(q)$ and $A(q)$ are multiplicative functions of q.*

Lemma 4.3. *For any* $\chi_1, \chi_2 \pmod{q}$ *with* $q \leq X$, *we have*

(a) $Z(q;\chi_1,\chi_2) \ll \phi(q) qB$;

(b) $\sum_{b \leq X} |Z(q;\chi_1,\chi_2)| \ll X\phi(q)^{1/2} qB$.

Lemma 4.4. *For* $j = 1, 2$, *let* $\chi_j \pmod{p^{\alpha_j}}$ *be primitive characters and* $\alpha = \operatorname{Max}\{\alpha_1, \alpha_2\}$. *For any* $t \geq \alpha$, *let* $Z(p^t) = Z(p^t; \chi_1\chi_o, \chi_2\chi_o)$ *and* $Y(p^t) = Y(p^t; \chi_1\chi_o, \chi_2\chi_o)$ *where* χ_o *is of modulus* p^t. *We have*

(a) $Z(p^\alpha) = Y(p^\alpha)$;

(b) $Z(p^t) = 0$ *if* $t \geq \tau_p + \operatorname{Max}\{\theta_p, \alpha\}$;

(c) $\sum_{\nu=\alpha}^{\eta} \phi(p^\nu)^{-2} Z(p^\nu) = \phi(p^\eta)^{-2} Y(p^\eta)$ *for any* $\eta \geq \alpha \geq 0$.

Corollary 4.5. (a) $A(p^t) = 0$ *for* $t \geq \tau_p + \theta_p$;

(b) $p^t \phi(p^t)^{-2} \mathcal{N}_2(p^t) = p^{\tau_p+\theta_p-1} \phi(p^{\tau_p+\theta_p-1})^{-2} \mathcal{N}_2(p^{\tau_p+\theta_p-1})$ *for* $t \geq \tau_p + \theta_p - 1$.

Lemma 4.6. (a) *For any complex numbers* ρ_j *with* $0 < \operatorname{Re}\rho_j \leq 1$, $j = 1, 2$, *we have*

$$\int_{-\infty}^{\infty} e(-b\eta) \prod_{j=1}^{2} \left(\int_{L_j}^{N_j} x^{\rho_j - 1} e(a_j \eta x^{k_j})\, dx \right) d\eta \tag{4.4}$$
$$= N^{1/k} (k|a_2|)^{-1} \int_{\mathcal{D}} x_2^{\,-1+(1/k)} \prod_{j=1}^{2} (Nx_j)^{(\rho_j-1)/k_j}\, dx_1,$$

where $x_2 = (bN^{-1} - a_1 x_1) a_2^{\,-1}$ *and* $\mathcal{D} = \{x_1 :\ L/N \leq x_1, x_2 \leq 1\}$.

(b) *We have* $\int_{\mathcal{D}} x_2^{\,-1+(1/k)}\, dx_1 \gg Q^{-\xi/16}$ *for all* b *such that* $3BL \leq b \leq X$, *where* $\xi = 4^{-k}$.

We now give a proof for Lemma 4.1(b) and Lemma 4.3(b).

Proof of Lemma 4.1(b). For $1 \leq l \leq p^t$, let $l = u + vp^{t-\tau_p}$. Write $q = p^{\tau_p - 1}$. Then by $t \geq \tau_p + \theta_p$ and repeated application of Lemma 8.2 in [**8**] we have $l^q \equiv u^q + qu^{q-1} v p^{t-\tau_p} \pmod{p^t}$. By raising both sides of the congruence to the power of k/q, we get $l^k \equiv u^k + k u^{k-1} v p^{t-\tau_p} \pmod{p^t}$. Using this and $t \geq \tau_p + \alpha$,

$$C(\chi\chi_o, p^t, m, k) = \sum_{(u, p^{t-\tau_p})=1} \chi(u) e(u^k m/p^t)$$
$$\times \sum_{v=0}^{p^{\tau_p}-1} e(k u^{k-1} v m/p^{\tau_p}) = 0$$

since the last inner sum vanishes. □

Proof of Lemma 4.3(b). By (4.2) and Lemma 4.1(c),

$$\sum_{b=1}^{q} |Z(q;\chi_1,\chi_2)|^2 = \sum_{(h,q)=1} q \prod_{j=1}^{2} |C(\chi_j, q, a_j h, k_j)|^2 \ll \phi(q) q^3 B^2.$$

The lemma follows by applying the Cauchy-Schwarz inequality. □

For any p, we define

$$s(p) := p^{\tau_p+\theta_p-1} \phi(p^{\tau_p+\theta_p-1})^{-2} \mathcal{N}_2(p^{\tau_p+\theta_p-1}). \tag{4.5}$$

By (1.2) and (4.2) we have $q^{-1}Y(q;\chi_o,\chi_o) = \mathcal{N}_2(q)$. Then, in view of Lemma 4.4(c) with $\alpha = 0$ and (4.3), we have

$$s(p) = 1 + A(p) + \cdots + A(p^{\tau_p+\theta_p-1}). \tag{4.6}$$

5. Lemmas for the transition from singular series to singular products. The principal difficulty in treating the singular series arises from the fact that $\sum_{q=1}^{\infty} |A(q)|$ is not convergent in general. We shall apply the techniques in [**22**, Section 8.6] to overcome the difficulty by approximating the singular series by a finite product in Lemma 5.5(b) below.

Let

$$R_p(m) := \sum_{l=1}^{p-1} e_p(lm), \qquad \tau(\chi) := \sum_{l=1}^{q} \chi(l) e_q(l)$$

and

$$\mathcal{A}_p := \{\chi (\mathrm{mod} p) : \ \chi^k = \chi_o, \ \chi \neq \chi_o\}.$$

For each $\chi \in \mathcal{A}_p$, let

$$g(\chi) := \phi(p)^{-2} R_p(a_1) \tau(\chi) \tau(\overline{\chi}) \chi(-1) \overline{\chi}(a_2)$$

and

$$g_p := \phi(p)^{-2} R_p(a_1) R_p(a_2).$$

Using techniques similar to those used in the proofs of Lemmas 6.2 through 6.6 in [**9**] we can prove the following Lemmas 5.1 through 5.4.

Lemma 5.1. *We have*

$$A(p) = \sum_{\chi \in \mathcal{A}_p} g(\chi)\chi(b) + g_p R_p(b).$$

This lemma is used in the proofs of Lemmas 5.2 and 5.4. In the proof of our Lemma 5.1, we need Lemma 4.3 in [**22**].

Lemma 5.2. (a)

$$|g(\chi)| \le \begin{cases} 2(p-1)^{-1} & \text{if } p \nmid a_1, \\ 2 & \text{if } p \mid a_1, \end{cases}$$

for any $\chi \in \mathcal{A}_p$;

$$|g_p| \ \le \begin{cases} (p-1)^{-2} & \text{if } p \nmid a_1 a_2, \\ (p-1)^{-1} & \text{if } p \mid a_1 a_2. \end{cases}$$

(b)

$$|A(p)| \le \begin{cases} 4kp^{-1} & \text{if } p \nmid a_1 a_2, \\ 2k & \text{if } p \mid a_1 a_2. \end{cases}$$

Lemma 5.2(a) is applied in the proof of Lemma 5.4.

Lemma 5.3.

(a) *For any* $U \ge 1$,

$$\sum_{q \le U} |A(q)| \ll U^{\xi/64} B^2 \quad \text{where} \quad \xi = 4^{-k}.$$

(b) *Assume* (1.3) *for* $j = 1, 2$. *Then*

$$\prod_{p \le Q} s(p) \gg (\log Q)^{-4k} B^{-2}.$$

Lemma 5.4. *For any given U with $1 \le U \le Q$ and any positive integer r, we have*

$$\sum_{b \le X} \Big| \prod_{\substack{p \le Q \\ p \nmid r}} s(p) - \sum_{\substack{q \le U \\ (q,r)=1}} A(q) \Big| \ll XU^{-1/3} Q^{\xi/64}.$$

This implies that

$$\sum_{\substack{q \le U \\ (q,r)=1}} A(q) = \prod_{\substack{p \le Q \\ p \nmid r}} s(p) + O\big(U^{-1/3} Q^{3\xi/64}\big),$$

except for at most $XQ^{-\xi/32}$ values of b with $1 \le b \le X$.

For $r \ge 1$, define

$$\sigma := \sigma(r) := \prod_{p \mid r} p^{\beta_p}, \tag{5.1}$$

where $\beta_p := \tau_p + \operatorname{Max}\{\theta_p, \operatorname{ord}_p(r)\} - \operatorname{ord}_p(r) - 1$, and τ_p and θ_p are defined as in (4.1). Note that for any $p \mid r$, if $p \nmid 2k$ then $\tau_p = 1 = \theta_p$ and $\beta_p = 0$. Hence, $p \mid \sigma$ implies $p \mid 2k$ and $\beta_p \le \tau_p + \theta_p - 1 \le 2\operatorname{ord}_p(2k)$. Thus

$$\sigma \quad \text{divides} \quad \prod_{p \mid 2k} p^{2\operatorname{ord}_p(2k)} = 4k^2. \tag{5.2}$$

Lemma 5.5. *Let $\chi_j \pmod{r_j}$, $j = 1, 2$, be primitive characters and $r = [r_1, r_2] \le Q$. Let $\xi = 4^{-k}$. Then*

(a)

$$\sum_{b \le X} \Big| \sum_{\substack{q \le Q \\ r \mid q}} \phi(q)^{-2} Z(q) \Big| \ll Xr^{-1/2} Q^{\xi/64} B^3;$$

(b)

$$\sum_{b\le X}\Big|\sum_{\substack{q\le Q\\ r\mid q}}\phi(q)^{-2}Z(q)-\phi(\sigma r)^{-2}Y(\sigma r)\prod_{\substack{p\le Q\\ p\nmid r}}s(p)\Big|\ll XQ^{-(1/5)+(\xi/32)}B.$$

The implied constants in the above $\ll$ depend on k only.

Proof. (a) For any q divisible by r, we write $q=q'q''$ such that $(q'',r)=1$ and every prime factor in q' divides r. Then by Lemma 4.2 and (4.3),

$$\sum_{\substack{q\le Q\\ r\mid q}}\phi(q)^{-2}Z(q)=\sum_{\substack{q'\le Q\\ r\mid q'}}\phi(q')^{-2}Z(q')\sum_{\substack{q''\le Q/q'\\ (q'',r)=1}}A(q''). \tag{5.3}$$

For $j=1,2$, write $\chi_j \pmod{r_j}=\prod_{p\mid r}\chi_{j_p}\pmod{p^{\mathrm{ord}_p(r_j)}}$. Then each χ_{j_p} is primitive. By Lemma 4.4 (a) and (b), we see that

$$Z(p^{\mathrm{ord}_p(r)};\chi_{1_p}\chi_o,\chi_{2_p}\chi_o)=Y(p^{\mathrm{ord}_p(r)};\chi_{1_p}\chi_o,\chi_{2_p}\chi_o)$$

and

$$Z(p^{\mathrm{ord}_p(q')})\neq 0\quad\text{implies}$$
$$\mathrm{ord}_p(q')\le\tau_p+\mathrm{Max}\{\theta_p,\mathrm{ord}_p(r)\}-1=\beta_p+\mathrm{ord}_p(r).$$

Thus by writing $r=r'r''$ such that $(r'',2k)=1$ and every prime factor in r' divides $2k$, and by Lemma 4.2, we have

$$Z(r'')=Y(r'')\ . \tag{5.4}$$

And by (5.1), we have $Z(q')\neq 0$ implies $q'\mid\sigma r$ (i.e., $\mathrm{ord}_p(q')\le\beta_p+\mathrm{ord}_p(r)$ for all $p\mid q'$). Since $r\mid q'$, we conclude from this that

$$Z(q')\neq 0\quad\text{implies}\quad q'=ur\quad\text{for some } u\mid\sigma. \tag{5.5}$$

Thus

$$\sum_{\substack{q'\le\sigma r\\ r\mid q'}}\phi(q')^{-2}|Z(q')|=\sum_{u\mid\sigma}\phi(ur)^{-2}|Z(ur)|. \tag{5.6}$$

Recalling the definition of r', and by Lemma 4.2 and $(u, r'') = 1$ (by (5.2)), we see that (5.5), (5.4) and (5.1) give

$$\sum_{\substack{q' \le \sigma r \\ r \mid q'}} \phi(q')^{-2} Z(q') = \sum_{u \mid \sigma} \phi(ur')^{-2} Z(ur') \phi(r'')^{-2} Y(r'')$$

$$= \prod_{p \mid r'} \Bigg(\sum_{\nu = \mathrm{ord}_p(r')}^{\beta_p + \mathrm{ord}_p(r')} \phi(p^\nu)^{-2} Z(p^\nu) \Bigg) \phi(r'')^{-2} Y(r'').$$

By Lemma 4.4(c), the last product over $p \mid r'$ is

$$\prod_{p \mid r'} \phi(p^{\beta_p + \mathrm{ord}_p(r')})^{-2} Y(p^{\beta_p + \mathrm{ord}_p(r')}) = \phi(\sigma r')^{-2} Y(\sigma r').$$

Hence, by Lemma 4.2, we have

$$\sum_{\substack{q' \le \sigma r \\ r \mid q'}} \phi(q')^{-2} Z(q') = \phi(\sigma r)^{-2} Y(\sigma r). \tag{5.7}$$

Note that $\sigma \le 4k^2$ (by (5.2)) and then, if $u \mid \sigma$, we have $ur \le 4k^2 Q \le X$ (by (2.2) and (2.3)). By (5.5), (5.6), Lemma 4.3(b) (with $ur \le X$) and $\sigma \ll k^2$, we have

$$\sum_{b \le X} \sum_{\substack{q' \le Q \\ r \mid q'}} \phi(q')^{-2} |Z(q')| \le \sum_{b \le X} \sum_{u \mid \sigma} \phi(ur)^{-2} |Z(ur)|$$

$$\ll X r^{-(1/2)+(\xi/64)} B. \tag{5.8}$$

Hence by (5.3), Lemma 5.3(a), (5.8) and $r \le q'$, we have

$$\sum_{b \le X} \Bigg| \sum_{\substack{q \le Q \\ r \mid q}} \phi(q)^{-2} Z(q) \Bigg| \ll X r^{-1/2} Q^{\xi/64} B^3.$$

This proves part (a).

(b) We first consider $r \le Q^{2/5}$. Then by $\sigma \le 4k^2$ we have $\sigma r \le Q$ since Q is large. Hence by (5.5) the condition $q' \le \sigma r$ in the sum in (5.7)

can be replaced by $q' \le Q$, and (5.7) holds for $\sum_{q' \le Q, r|q'} \phi(q')^{-2} Z(q')$, too. In this case, by (5.3), (5.7), (5.5), Lemmas 4.3(a) and 5.4, we have

$$\begin{aligned}
&\sum_{b \le X} \Big| \sum_{\substack{q \le Q \\ r|q}} \phi(q)^{-2} Z(q) - \phi(\sigma r)^{-2} Y(\sigma r) \prod_{\substack{q \le Q \\ p \nmid r}} s(p) \Big| \\
&\qquad = \sum_{b \le X} \Big| \sum_{\substack{q' \le Q \\ r|q'}} \phi(q')^{-2} Z(q') \Big(\sum_{\substack{q'' \le Q/q' \\ (q'', r) = 1}} A(q'') - \prod_{\substack{q \le Q \\ p \nmid r}} s(p) \Big) \Big| \\
&\qquad \ll \sum_{u|\sigma} (ur)^{\xi/32} B \sum_{b \le X} \Big| \sum_{\substack{q'' \le Q/(ur) \\ (q'', r) = 1}} A(q'') - \prod_{\substack{q \le Q \\ p \nmid r}} s(p) \Big| \\
&\qquad \ll \sum_{u|\sigma} (ur)^{\xi/32} B X \big(Q/(ur) \big)^{-1/3} Q^{\xi/64} \\
&\qquad \ll X Q^{-(1/3)+(\xi/64)} r^{(1/3)+(\xi/32)} B,
\end{aligned}$$

which is $\le X Q^{-(1/5)+(\xi/32)} B$ if $r \le Q^{2/5}$.

If $r > Q^{2/5}$, by part (a), we have

$$\sum_{b \le X} \Big| \sum_{\substack{q \le Q \\ r|q}} \phi(q)^{-2} Z(q) \Big| \ll X Q^{-(1/5)+(\xi/32)} B$$

since $B \le Q^{\delta}$ (in (2.5)). Next, by (4.5) and $\mathcal{N}_2(p^t) \le \phi(p^t)^2$ (by (1.2)), we have $s(p) \le p^{\tau_p + \theta_p - 1}$. Furthermore, if $p \nmid 2k$ then $\tau_p = 1 = \theta_p$ and hence we have $s(p) = 1 + A(p)$ by (4.6). Therefore, by Lemma 5.2(b), $|A(p)| \le \phi(p)$ (by (4.3)) and $\tau_p + \theta_p - 1 \le 2\mathrm{ord}_p(2k)$, so

$$\begin{aligned}
\prod_{\substack{p \le Q \\ p \nmid r}} s(p) &= \prod_{\substack{p \le Q \\ p \nmid 2kr \\ p \nmid a_1 a_2}} s(p) \prod_{\substack{p \le Q \\ p \nmid 2kr \\ p | a_1 a_2}} s(p) \prod_{\substack{p \le Q \\ p | 2k \\ p \nmid r}} s(p) \\
&\le \prod_{p \le Q} (1 + 4kp^{-1}) \prod_{p | a_1 a_2} (1 + \phi(p)) \prod_{p | 2k} p^{\tau_p + \theta_p - 1} \\
&\ll (\log Q)^{4k} B^2.
\end{aligned}$$

Hence, by (5.7), (5.6), Lemma 4.3(b), $\sigma \le 4k^2$ and $B \le Q^{\delta}$, for $r > Q^{2/5}$, we obtain

$$\begin{aligned}\sum_{b\le X}\Big|\phi(\sigma r)^{-2}Y(\sigma r)\prod_{\substack{p\le Q\\ p\nmid r}} s(p)\Big| &\le \sum_{b\le X}\sum_{u\mid\sigma}\phi(ur)^{-2}|Z(ur)|\Big|\prod_{\substack{p\le Q\\ p\nmid r}} s(p)\Big| \\ &\ll \sum_{u\le 4k^2}(ur)^{-(1/2)+(\xi/64)}XB(\log Q)^{4k}B^2 \\ &\ll XQ^{-(1/5)+(\xi/32)}B.\end{aligned}$$

Then part (b) remains valid in the case $r > Q^{2/5}$. □

6. The major arcs and the completion of the proof that Card $E_2(X) \le X^{\theta}$ in Theorem 1. In this section, we shall use the results in Sections 4 and 5 to obtain a lower bound (in Lemma 6.5) for $\mathcal{I}_1(b)$.

From (3.4), we see that $H_1(h,q,\eta)H_2(h,q,\eta)$ is a sum of at most 9 terms which belong to 3 categories:

(T_1) the term $\prod_{j=1}^{2} C(\chi_o, q, a_j h, k_j) I_j(a_j\eta)$;

(T_2) the 5 terms each of which has at least one $G_j(h,q,\eta)$ as a factor;

(T_3) the remaining 3 terms.

For $i = 1,2,3$, let

$$M_i := \sum_{q\le Q}\phi(q)^{-2}\sum_{(h,q)=1} e_q(-bh)\int_{-\infty}^{\infty} e(-b\eta) \times \{\text{the sum of terms in } (T_i)\}\, d\eta.$$

Note that each M_i is real and $M_3 = 0$ if $\tilde{\beta}$ does not exist or $\tilde{r} > Q$ (since $\delta_q = 0$ in (3.5)). By (3.7), we have

$$\mathcal{I}_1(b) = M_1 + M_2 + M_3 + O\big(N^{1/k}Q^{-1}\big) \tag{6.1}$$

except for at most XQ^{-1} values of b.

Let $\sigma = \sigma(\tilde{r})$ be defined as in (5.1) and χ_o be of modulo $\sigma\tilde{r}$. Set

$$\begin{aligned}\mathcal{G}(1) &:= (\sigma\tilde{r})^{-1}Y(\sigma\tilde{r}; \tilde{\chi}\chi_o, \chi_o),\\ \mathcal{G}(2) &:= (\sigma\tilde{r})^{-1}Y(\sigma\tilde{r}; \chi_o, \tilde{\chi}\chi_o)\end{aligned}$$

and

$$\mathcal{G}(1,2) := (\sigma\tilde{r})^{-1} Y(\sigma\tilde{r}; \tilde{\chi}\chi_o, \tilde{\chi}\chi_o).$$

Also let $E := N^{1/k}(k|a_2|)^{-1}$, $F := x_2^{-1+(1/k)}$, $G := (Nx_1)^{\bar{\beta}-1}$, $H := (Nx_2)^{(\bar{\beta}-1)/k}$ and

$$\begin{cases} \mathcal{P}_o := E\int_D F dx_1, & \mathcal{P}(1) := E\int_D FG dx_1, \\ \mathcal{P}(2) := E\int_D FH dx_1, & \mathcal{P}(1,2) := E\int_D FGH dx_1, \end{cases} \tag{6.2}$$

where x_2 and $\mathcal{D}$ are defined as in (4.4).

Lemma 6.1. *We have*

$$M_1 = \mathcal{P}_0 \prod_{p\le Q} s(p) + O\big(N^{1/k} Q^{-(1/3)+(7\xi/64)}\big)$$

except for at most $XQ^{-\xi/32}$ *values of* b *with* $1 \le b \le X$.

Proof. The lemma can be proved by techniques similar to those used in the proof of Lemma 7.1 in [**9**], by our Lemma 5.4. □

Lemma 6.2. *Let* $\sigma = \sigma(\tilde{r})$ *be defined as in* (5.1). *If the exceptional zero* $\tilde{\beta}$ *exists and* $\tilde{r} \le Q$, *then*

(a)

$$M_3 = \phi(\sigma\tilde{r})^{-2}\sigma\tilde{r}\left(\prod_{\substack{p\le Q\\ p\nmid\tilde{r}}} s(p)\right)\left(-\sum_{j=1}^{2}\mathcal{G}(j)\mathcal{P}(j) + \mathcal{G}(1,2)\mathcal{P}(1,2)\right) + O\big(N^{1/k}Q^{-(1/5)+(\xi/8)}B\big)$$

except for at most $3XQ^{-\xi/32}$ *values of* b *with* $1 \le b \le X$;

(b)

$$M_3 \ll N^{1/k}\tilde{r}^{-1/2}Q^{7\xi/64}B^3$$

except for at most $3XQ^{-\xi/32}$ *values of* b *with* $1 \le b \le X$.

Proof. The lemma can be proved in a way similar to the proof of Lemma 4.2 in [**11**], by our Lemma 4.6(a), and Lemma 5.5(b) and (a). □

Lemma 6.3. *Let Ω be defined as in* (3.2). *We have*

$$M_1 + M_3 \geq \Omega^2 \mathcal{P}_o \prod_{p \leq Q} s(p) + O\big(N^{1/k} Q^{-(1/5)+(\xi/8)} B\big)$$

except for at most $4XQ^{-\xi/32}$ values of b with $1 \leq b \leq X$.

Proof. The lemma can be proved in a way similar to the proof of Lemma 4.3 in [**11**], by our Corollary 4.5(b), Lemma 6.1, and Lemma 6.2(a). □

Lemma 6.4. *We have*

$$M_2 \ll \Omega^2 \exp(-c_3/\sqrt{\delta}) \mathcal{P}_o \prod_{p \leq Q} s(p) + O\big(N^{1/k} Q^{-(1/5)+(\xi/8)} B\big)$$

except for at most $5XQ^{-\xi/32}$ values of b with $1 \leq b \leq X$. Here c_3 and the implied constant in $\ll$ are independent of δ.

Proof. The lemma can be proved in a way similar to the proof of Lemma 7.4 in [**9**], by our Lemma 4.6(a), Lemma 5.5(b), and Lemma 3.1. □

Lemma 6.5. *Let $W_2(X)$ be defined as in* (1.4). *We have*

$$\mathcal{I}_1(b) \gg N^{1/k} Q^{-5\xi/8},$$

except for at most $10XQ^{-\xi/32}$ values of $b \in W_2(X)$, where $\xi = 4^{-k}$.

Proof. Case 1. $\tilde{\beta}$ does not exist or $\tilde{\beta}$ exists with $\tilde{r} > Q$.

We have $M_3 = 0$. Applying Lemmas 6.1 and 6.4 to (6.1) with a small $\delta > 0$, we have

$$\mathcal{I}_1(b) \geq \frac{1}{2} \mathcal{P}_o \prod_{p \leq Q} s(p) + O\big(N^{1/k} Q^{-(1/5)+(\xi/8)} B\big), \tag{6.3}$$

except for at most $6XQ^{-\xi/32}$ values of $1 \le b \le X$. Assuming (1.3), and by (6.2), Lemmas 4.6(b), 5.3(b) and $B \le Q^{\delta}$ (in (2.5)), we have

$$\mathcal{P}_o \prod_{p \le Q} s(p) \gg N^{1/k} B^{-1} Q^{-\xi/16} (\log Q)^{-4k} B^{-2} \gg N^{1/k} Q^{-3\xi/32}, \tag{6.4}$$

except for at most $6BXQ^{-\xi/16}$ ($= 3BL$ by (2.2) and (2.3)) values of $b \in W_2(X)$. The O-term in (6.3) can be neglected since $\xi = 4^{-k}$, and hence $\mathcal{I}_1(b) \gg N^{1/k} Q^{-3\xi/32}$, except for at most $7XQ^{-\xi/32}$ values of $b \in W_2(X)$.

Case 2. $\tilde{\beta}$ exists and $Q^{\xi/2} < \tilde{r} \le Q$.

Applying Lemmas 6.1, 6.4 and 6.2(b) to (6.1) with a small $\delta > 0$ and $\tilde{r} > Q^{\xi/2}$, we have

$$\mathcal{I}_1(b) \ge \frac{1}{2} \mathcal{P}_o \prod_{p \le Q} s(p) + O\big(N^{1/k} Q^{-9\xi/64} B^3\big),$$

except for at most $9XQ^{-\xi/32}$ values of $1 \le b \le X$. Then by (6.4) and $B \le Q^{\delta}$, we again have $\mathcal{I}_1(b) \gg N^{1/k} Q^{-3\xi/32}$, except for at most $10XQ^{-\xi/32}$ values of $b \in W_2(X)$.

Case 3. $\tilde{\beta}$ exists and $\tilde{r} \le Q^{\xi/2}$.

Applying Lemmas 6.3 and 6.4 to (6.1) with a small $\delta > 0$,

$$\mathcal{I}_1(b) \ge \frac{1}{2} \Omega^2 \mathcal{P}_o \prod_{p \le Q} s(p) + O\big(N^{1/k} Q^{-(1/5)+(\xi/8)} B\big), \tag{6.5}$$

except for at most $9XQ^{-\xi/32}$ values of $1 \le b \le X$. Now by (3.2), (3.1), $\tilde{r} \le Q^{\xi/2}$ and $Q \le T$ (in (2.3)),

$$\Omega = (1 - \tilde{\beta}) \log T \gg Q^{-\xi/4} (\log Q)^{-1}.$$

Then by (6.4),

$$\Omega^2 \mathcal{P}_o \prod_{p \le Q} s(p) \gg Q^{-\xi/2} (\log Q)^{-2} N^{1/k} Q^{-3\xi/32} \gg N^{1/k} Q^{-5\xi/8},$$

except for at most $6BXQ^{-\xi/16}$ values of $b \in W_2(X)$. Again, the O-term in (6.5) can be neglected since $\xi = 4^{-k}$ and hence $\mathcal{I}_1(b) \gg N^{1/k}Q^{-5\xi/8}$, except for at most $10XQ^{-\xi/32}$ values of $b \in W_2(X)$. □

Combining (2.8), Lemma 6.5 and Lemma 2.1, we have

$$\mathcal{I}(b) = \mathcal{I}_1(b) + \mathcal{I}_2(b) \gg N^{1/k}Q^{-5\xi/8},$$

except for at most $XQ^{-\xi/33}$ values of $b \in W_2(X)$.

In view of (2.6), the integral $\mathcal{I}(b)$ in (2.7) is equal to $\sum (\log p_1)(\log p_2)$, where the summation $\sum$ is over all p_1, p_2 satisfying $L < p_1 \le N$, $L^{1/k} < p_2 \le N^{1/k}$, and the equation $b = a_1p_1 + a_2p_2^k$. If $\sharp(b)$ denotes the number of such pairs $\langle p_1, p_2\rangle$, then $\mathcal{I}(b)$ is clearly $\le \sharp(b)\log^2 N$. That is,

$$\sharp(b) \ge \mathcal{I}(b)(\log N)^{-2} \gg N^{1/k}Q^{-5\xi/8}(\log N)^{-2} > 0,$$

except for at most $XQ^{-\xi/33}$ values of $b \in W_2(X)$. This completes the proof of $\operatorname{Card} E_2(X) \le X^\theta$ in Theorem 1.

7. The lower bound for $\operatorname{Card} W_2(X)$ in Theorem 2. By Corollary 4.5(b),

$$\mathcal{N}_2(p^{\tau_p+\theta_p-1}) \ge 1$$

implies

$$\mathcal{N}_2(p^t) \ge 1 \quad \text{for } t \ge \tau_p + \theta_p - 1,$$

and, on the other hand, by (1.2),

$$\mathcal{N}_2(p^{\tau_p+\theta_p-1}) \ge 1$$

implies

$$\mathcal{N}_2(p^t) \ge 1 \quad \text{for } 1 \le t \le \tau_p + \theta_p - 1.$$

Therefore by Lemma 4.2, (1.3) holds for $\mathcal{N}_2(q)$ if and only if

$$\mathcal{N}_2(p^{\tau_p+\theta_p-1}) \ge 1 \tag{7.1}$$

for all primes p.

In view of (4.5) and (4.6), for $p \nmid 2k$ (so $\tau_p = 1 = \theta_p$ by (4.1)), (7.1) holds if and only if $A(p) > -1$. By Lemma 5.2(b), we have $|A(p)| \le 4kp^{-1} < 1$ if $p \nmid a_1 a_2$ and $p \ge 4k+1$. Hence

(7.2) (7.1) holds for those $p \ge 4k+1$ satisfying $p \nmid a_1 a_2$.

Let $p_1, \dots, p_u$ and $q_1, \dots, q_v$ be all those primes $\ge 4k+1$ which divide a_1 and a_2 respectively. Note that $p_i \ne q_j$ for all i, j since $(a_1, a_2) = 1$ (in (1.1)). Let

$$m := \prod_{p \le 4k} p^{\tau_p + \theta_p - 1} \prod_{i=1}^{u} p_i \prod_{j=1}^{v} q_j.$$

Lemma 7.1. *There are at least*

$$\prod_{i=1}^{u} \frac{\phi(p_i)}{k} \prod_{j=1}^{v} \phi(q_j)$$

values of $b \pmod m$ *for which* (1.3) *holds for* $\mathcal{N}_2(q)$.

Proof. For each p_i, $1 \le i \le u$, the congruence in $\mathcal{N}_2(p_i)$ (see (1.2)) becomes

$$b \equiv a_2 n^k \pmod{p_i}. \tag{7.3}$$

Thus $\mathcal{N}_2(p_i) \ge 1$ if b satisfies (7.3) for some n with $1 \le n \le p_i - 1$. For each q_j, $1 \le j \le v$, the congruence in $\mathcal{N}_2(q_j)$ becomes

$$b \equiv a_1 l \pmod{q_j} \tag{7.4}$$

and so $\mathcal{N}_2(q_j) \ge 1$ if b satisfies (7.4) for some l with $1 \le l \le q_j - 1$. For each $p \le 4k$, (7.1) holds for those b satisfying

$$b \equiv a_1 + a_2 \pmod{p^{\tau_p + \theta_p - 1}}.$$

Note that $\tau_p + \theta_p - 1 = 1$ if $p \ge 4k+1$ (by (4.1)). Hence, in view of (7.2), for each n_i^k with $1 \le n_i \le p_i - 1$, $i = 1, \dots, u$, and for each l_j with $1 \le l_j \le q_j - 1$, $j = 1, \dots, v$, if b satisfies the system of congruences

$$\begin{cases} b \equiv a_2 {n_i}^k \pmod{p_i} & \text{for } i = 1, \dots, u, \\ b \equiv a_1 l_j \pmod{q_j} & \text{for } j = 1 \dots, v, \\ b \equiv a_1 + a_2 \pmod{p^{\tau_p + \theta_p - 1}} & \text{for } p \le 4k, \end{cases} \tag{7.5}$$

then (7.1) holds for all primes p and so (1.3) holds for $\mathcal{N}_2(q)$. Now by the Chinese remainder theorem, the system of congruences (7.5) has a unique solution $b \pmod m$. Note that for each $i = 1, \dots, u$, there are exactly $\phi(p_i)/\big(k, \phi(p_i)\big)$ $(\geq \phi(p_i)/k)$ incongruent ${n_i}^k \pmod{p_i}$; and for each $j = 1, \dots, v$, there are exactly $\phi(q_j)$ incongruent $l_j \pmod{q_j}$. Thus, in total, there are at least

$$\prod_{i=1}^{u} \frac{\phi(p_i)}{k} \prod_{j=1}^{v} \phi(q_j)$$

such systems of congruences for $1 \leq n_i \leq p_i - 1$, $i = 1, \dots, u$, and $1 \leq l_j \leq q_j - 1$, $j = 1, \dots, v$. Hence Lemma 7.1 follows immediately. □

By Lemma 7.1 and noting that $\prod_{p \leq 4k} p^{\tau_p + \theta_p - 1}$ depends only on k, we have, for large X

$$\begin{aligned} \operatorname{Card} W_2(X) &\geq \frac{X}{m} \prod_{i=1}^{u} \frac{\phi(p_i)}{k} \prod_{j=1}^{v} \phi(q_j) \\ &\geq X \Bigg(\prod_{p \leq 4k} p^{\tau_p + \theta_p - 1} \Bigg)^{-1} k^{-\omega(a_1)} \prod_{i=1}^{u} \frac{\phi(p_i)}{p_i} \prod_{j=1}^{v} \frac{\phi(q_j)}{q_j}. \end{aligned}$$

Finally, by (1.4) and (1.2), obviously we have $\operatorname{Card} W_1(X) \geq \operatorname{Card} W_2(X)$. This proves the results for $W_1(X)$ and $W_2(X)$ in Theorem 2.

8. Remarks on the proofs of bounds concerning $E_j(X)$, $j = 1, 3$ and $W_3(X)$. The proofs of $\operatorname{Card} E_j(X) \leq X^\theta$, $j = 1, 3$ in Theorem 1 are very similar to (and also simpler than) that for $\operatorname{Card} E_2(X) \leq X^\theta$. However, the following technical differences in their proofs should be pointed out.

(i) For $j = 1$, instead of using Theorem 1 [**7**] in the proof of our Lemma 2.1, we apply Weyl's inequality (see, for example, Lemma 2.4 in [**22**]).

(ii) For $j = 3$, instead of our Lemma 4.1(c), we use Hua's fundamental lemma [**8**, Theorem 1] to estimate $\sum_{l=1}^{q} e_q(a_2 P(l))$. In the proof

of the lemma corresponding to our Lemma 5.1, one writes $P(l)$ in the form of a completed square modulo odd q, then one applies Lemma 4.3 in [**22**].

Concerning the proof of the lower bound for $\operatorname{Card} W_3(X)$ in Theorem 2 we first apply Theorem 2.24 in [**14**] to prove that $\mathcal{N}_3(p^{\operatorname{ord}_p(a_1)+1}) \geq 1$ for any prime p if (α) $b \equiv a_1 + a_2 P(1) \pmod{p^{2\tau+1}}$, where $\tau = \operatorname{ord}_p(P'(1))$ or if (β) $p|a_1$ and the congruence $b \equiv a_2 P(n) \pmod{p}$ has a solution n satisfying $p \nmid P'(n)$. One then uses these results to obtain a lemma similar to our Lemma 7.1.

REFERENCES

1. A. Baker, *On some diophantine inequalities involving primes*, J. Reine Angew. Math. **228** (1967), 166–181.

2. R. Brünner, A. Perelli and J. Pintz, *The exceptional set for the sum of a prime and a square*, Acta Math. Hungar. **53** (1989), 347–365.

3. H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, 1980.

4. H. Davenport and H. Heilbronn, *Note on a result in the additive theory of numbers*, Proc. London Math. Soc., **43** (1937), 142–151.

5. P.X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. **11** (1970), 329–339.

6. 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.

7. G. Harman, *Trigonometric sums over primes* I, Mathematika **28** (1981), 249–254.

8. L.K. Hua, *Additive theory of prime numbers*, Transl. Math. Monographs (**13**), Amer. Math. Soc., 1965.

9. M.C. Leung and M.C. Liu, *On generalized quadratic equations in three prime variables*, Monatsh. Math. **115** (1993), 133–167.

10. M.C. Liu and K.M. Tsang, *Small prime solutions of linear equations*, *Théorie des nombres*, de Gruyter, 1989, 595–624.

11. ———, *Small prime solutions of some additive equations*, Monatsh. Math. **111** (1991), 147–169.

12. ———, *Recent progress on a problem of A. Baker*, Séminaire de Théorie des Nombres, Paris, 1991–1992, Progr. Math. **116**, Birkhäuser, 1993, 121-133.

13. R.J. Miech, *On the equation* $n = p + x^2$, Trans. Amer. Math. Soc. **130** (1968), 494–512.

14. H.L. Montgomery, I. Niven and H.S. Zuckerman, *An introduction to the theory of numbers*, 5th ed., John Wiley, New York, 1991.

15. H.L. Montgomery and R.C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.

16. J. Pitman, *Bounds for solutions of diagonal equations*, Acta Arith. **19** (1971), 223–247.

17. V.A. Plaksin, *On a question of Hua Loo-Keng*, Math. Notes **47** (1990), 278–286 (English transl.); Mat. Zametki **47**(1990), 78–90 (Russian).

18. W.M. Schmidt, *Small zeros of additive forms in many variables*, Trans. Amer. Math. Soc. **248** (1979), 121–133.

19. ———, *Small zeros of additive forms in many variables* II, Acta Math. **143** (1979), 219–232.

20. W. Schwarz, *Weitere, mit einer Methode von Erdös-Prachar erzielte Ergebnisse*, Math. Nachr. **23** (1961), 327–348.

21. A. Selberg, *Remarks on sieves*, *Proceedings of the 1972 Number Theory Conference*, University of Colorado, Boulder, 205–216.

22. R.C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, 1981.

23. A.I. Vinogradov, *On a binary problem of Hardy-Littlewood*, Acta Arith. **46** (1985), 33–56 (Russian).

24. A. Zaccagnini, *On the exceptional set for the sum of a prime and a k-th power*, Mathematika **39** (1992), 400–421.

Department of Mathematics, The University of Hong Kong, Pokfulam, Hong Kong