Can. J. Math. Vol. **48** (3), 1996 pp. 512–526.

THE ADDITION OF PRIMES AND POWER

JÖRG BRÜDERN AND ALBERTO PERELLI

ABSTRACT. Let $k \geq 2$ be an integer. Let $E_k(N)$ be the number of natural numbers not exceeding N which are not the sum of a prime and a k-th power of a natural number. Assuming the Riemann Hypothesis for all Dirichlet L-functions it is shown that $E_k(N) \ll N^{1-\frac{1}{25k}}$.

1. **Introduction.** Let $k \geq 2$ be a fixed integer and p denote a prime number. One expects that a sufficiently large integer n can be written as

$$n = p + m^k \tag{1}$$

with a positive integer m whenever the polynomial $x^k - n$ is irreducible over $\mathbb{Q}$. If ω denotes the smallest prime dividing k it can be shown that there are about $N^{1/\omega}$ positive integers $n \leq N$ for which $x^k - n$ is reducible, see *e.g.* the Appendix in Zaccagnini's survey paper [12]. Writing $E_k(N)$ for the number of $n \leq N$ with (1) insoluble we then expect $E_k(N)$ to be quite small compared to N. An estimate of the shape

$$E_k(N) \ll_k N^{1-\delta(k)} \tag{2}$$

with some $\delta(k) > 0$ has been obtained independently by Brünner, Perelli and Pintz [2] and A. I. Vinogradov [10] when $k = 2$, and by Zaccagnini [11] in the general case. Assuming the Generalized Riemann Hypothesis (GRH), the Hardy-Littlewood method coupled with Weyl's inequality gives

$$E_k(N) \ll_{k,\epsilon} N^{1-\frac{2}{kK}+\epsilon} \tag{3}$$

with $K = 2^{k-1}$, see Mikawa [5] when $k = 2$ and Perelli and Zaccagnini [6] in the general case. When k is larger, Weyl's inequality can be replaced by I. M. Vinogradov's estimates. Still under GRH, this yields

$$E_k(N) \ll_k N^{1-\frac{c}{k^3 \log k}} \tag{4}$$

with some suitable $c > 0$. This was observed by Perelli and Zaccagnini [6].

The aim of this paper is to improve on (4).

THEOREM 1. *Let* $k \geq 2$. *Assume* GRH. *Then*

$$E_k(N) \ll_k N^{1-\frac{1}{25k}}.$$

This paper was written while A. Perelli was enjoying a visit to Sonderforschungsbereich 170 Geometrie und Analysis in Göttingen. Their support is gratefully acknowledged.

Received by the editors December 29, 1994.

AMS subject classification: 11P55.

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

It should be noted that the constant $\frac{1}{25}$ occurring in the exponent can be reduced for large k. Indeed, by optimizing certain parameters in our method one obtains $E_k(N) \ll_k N^{1-\frac{1}{c(k)k}}$ with $c(k) \longrightarrow 21.15\cdots$ as $k \longrightarrow \infty$. We have preferred a readily derived bound valid for all k.

To assess the strength of this bound it may be worth pointing out that an estimate of the form $E_k(N) \ll N^{1-\frac{1}{k}}$ appears to be the limit of current circle method technology, even if one assumes that all relevant exponential sums can be estimated or approximated with error not exceeding the square root of their length (we do not know how to do this, even under GRH).

Our proof of Theorem 1 is based on two principal sources. A "pruning method" based on Ramanujan sums allows for an enormously larger set of major arcs than would be expected in the presence of a k-th power. The other idea is the use of a mean value theorem which we describe in more detail in the next section.

Some but not all of our techniques carry over to the related problem of representing integers in the form $p_1 + p_2^k$ with primes p_i.

THEOREM 2. *Let $\mathcal{H}_k$ denote the set of all natural numbers n such that $n \equiv a+b^k \bmod q$ has solutions in reduced residues $a, b \bmod q$, for any positive integer q. Let $D_k(N)$ be the number of all $n \leq N$, $n \in \mathcal{H}_k$ which cannot be written as $n = p_1 + p_2^k$. Then, assuming* GRH,

$$D_k(N) \ll_k N^{1-\frac{c}{k^2 \log k}}$$

for some absolute constant $c > 0$.

Routine arguments show that $\mathcal{H}_k$ has positive density, so that indeed the bound in Theorem 2 is non-trivial.

Our notation is standard and can be understood from the context. We sometimes use $x \sim X$ as a shorthand for $X < x \leq 2X$. Statements involving ϵ are true for any $\epsilon > 0$, occasionally implicit constants may depend on ϵ. Note that this allows us to rewrite an estimate $A \ll X^\epsilon \log X$ as $A \ll X^\epsilon$, for example.

2. A mean value estimate.

The results of this section are independent of GRH. Let $k \geq 3$ be fixed. Let $\mathcal{A}_0(P) = \{p : p \sim P\}$. Then define sequences $\mathcal{A}_t(P)$ by

$$\mathcal{A}_{t+1}(P) = \{pr : p \sim P^{1/k}, p \equiv -1 \pmod{k}, r \in \mathcal{A}_t(P/p)\}.$$

There is also an explicit description of $\mathcal{A}_t(P)$ when $t \geq 1$. Indeed this is the sequence of all products $p_0 p_1 \cdots p_t$ with

$$\begin{gathered} p_0 \sim P^{1/k},\ p_1 \sim (P/p_0)^{1/k}, \ldots, p_0 p_1 \cdots p_t \sim P, \\ p_j \equiv -1 \pmod{k} \quad (0 \leq j \leq t-1). \end{gathered} \tag{5}$$

In particular there are certain constants c, c' depending only on t and k such that for any $p_0 \cdots p_t \in \mathcal{A}_t(P)$ one has

$$cP^{\theta^l/k} < p_l < c'P^{\theta^l/k} \quad (0 \leq l \leq t-1), \quad cP^{\theta^t} < p_t < P^{\theta^t} \tag{6}$$

where $\theta = 1 - \frac{1}{k}$. The numbers θ^l/k and θ^t are all distinct so that for P sufficiently large (in terms of t and k) the ranges for the p_j are distinct.

In the opposite direction we remark that one can also find constants $0 < c_l < c_l'$ such that for any primes $p_0, \ldots, p_t$ with $p_l \equiv -1 \pmod{k}$ $(0 \le l \le t-1)$ and

$$c_l P^{\theta^l/k} < p_l \le c_l' P^{\theta^l/k} \quad (0 \le l \le t-1), \quad P < p_0 \cdots p_t \le 2P \tag{7}$$

one has $p_0 \cdots p_t \in \mathcal{A}_t(P)$.

LEMMA 1. *Let $k \ge 3$, $t \ge 0$, $s \ge 1$ and $\theta = 1 - \frac{1}{k}$. Let $I_k(P,s,t)$ denote the number of solutions of*

$$\sum_{i=1}^{s} (x_i^k - y_i^k) = 0$$

with $x_i \in \mathcal{A}_t(P), y_i \in \mathcal{A}_t(P)$. Then

$$I_k(P,s,t) \ll_{k,s,t} P^{2s-k+k(\theta^s+\theta^t)}.$$

PROOF. The lemma is trivial when $t = 0$ or $s = 1$. We now use induction on $s+t$. In doing so we may suppose that $t \ge 1$, $s \ge 2$. Any $x \in \mathcal{A}_t(P)$ can be written uniquely as $x = pr$ with $p \sim P^{1/k}$, $p \equiv -1 \pmod{k}$, $r \in \mathcal{A}_{t-1}(P/p)$ so that $I_k(P,s,t)$ equals the number of solutions to

$$(p_1r_1)^k + \cdots + (p_sr_s)^k = (p_{s+1}r_{s+1})^k + \cdots + (p_{2s}r_{2s})^k \tag{8}$$

with

$$p_i \sim P^{1/k}, \quad p_i \equiv -1 \pmod{k}, \quad r_i \in \mathcal{A}_{t-1}(P/p_i). \tag{9}$$

For a given value of p_1 and u satisfying $1 \le u \le 2s$ let $J(p_1,u)$ be the number of solutions of (8), (9) with the value of p_1 prescribed, and with exactly u of the $j \in \{1,2,\ldots,2s\}$ satisfying $p_j = p_1$. Then

$$I_k(P,s,t) \le \sum_{u=1}^{2s} \sum_{p_1} J(p_1,u) \tag{10}$$

where here and later p_1 is restricted as in (9). For some u we must have

$$I_k(P,s,t) \le 2s \sum_{p_1} J(p_1,u).$$

Note that $p_1 \nmid r_j$ for any j, by the remarks preceding Lemma 1. Considering (8) modulo p_1^k it follows that $J(p_1, 2s-1) = 0$ which excludes the possibility $u = 2s-1$. If $u = 2s$ we use $J(p_1,2s) = I_k(P/p_1, s, t-1)$ so that in this case

$$I_k(P,s,t) \ll \sum_{p_1} I_k(P/p_1, s, t-1).$$

However, $P/p_1 \ll P^\theta$ for p_1 in the range of summation. The induction hypothesis now yields $I_k(P,s,t) \ll P^\nu$ with $\nu = \frac{1}{k} + \theta(2s - k + k\theta^s + k\theta^{t-1})$. A short calculation confirms that $\nu \le 2s - k + k(\theta^s + \theta^t)$. This settles the induction in the case $u = 2s$.

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

Now suppose that $1 \leq u \leq s-2$. For a given p_1 let

$$g(\alpha) = \sum_{r \in \mathcal{A}_{t-1}(P/p_1)} e(\alpha r^k), \quad h(\alpha) = \sum_{\substack{p \sim P^{1/k}, p \neq p_1 \\ p \equiv -1 \pmod{k}}} \sum_{r \in \mathcal{A}_{t-1}(P/p)} e(\alpha p^k r^k).$$

Position the $u-1$ indices in $\{2, 3, \ldots, 2s\}$ with $p_j = p_1$, and write the number of solutions of (8),(9) with one such choice of positioning as an integral to see that

$$J(p_1, u) \leq \binom{2s-1}{u-1} \int_0^1 |g(\alpha p_1^k)|^u |h(\alpha)|^{2s-u} \, d\alpha.$$

By Hölder's inequality,

$$J(p_1, u) \ll K(p_1)^{\frac{u}{2s-2}} \left(\int_0^1 |h(\alpha)|^{2s} \, d\alpha \right)^{\frac{2s-2-u}{2s-2}}$$

where

$$K(p_1) = \int_0^1 |g(\alpha p_1^k)|^{2s-2} |h(\alpha)|^2 \, d\alpha.$$

By considering the underlying diophantine equations,

$$\int_0^1 |h(\alpha)|^{2s} \, d\alpha \leq I_k(P, s, t),$$

and $K(p_1)$ does not exceed the number of solutions of

(11) $$x_1^k - x_2^k = p_1^k (r_1^k + \cdots + r_{s-1}^k - r_s^k - \cdots - r_{2s-2}^k)$$

with

$$x_i \sim P, \quad r_i \in \mathcal{A}_{t-1}(P/p_1), \quad p_1 \nmid x_1 x_2.$$

By (11) we have $x_1^k \equiv x_2^k \pmod{p_1^k}$. Since $p_1 \equiv -1 \pmod{k}$ this gives $x_1 \equiv x_2 \pmod{p_1^k}$. However, $|x_1 - x_2| \leq P$, and $p_1^k > P$, so that $x_1 = x_2$. This shows

$$K(p_1) \leq P I_k(P/p_1, s-1, t-1).$$

Collecting together we deduce that

$$I_k(P, s, t) \ll \sum_{p_1} \bigl(P I_k(P/p_1, s-1, t-1) \bigr)^{\frac{u}{2s-2}} I_k(P, s, t)^{\frac{2s-2-u}{2s-2}}$$

whence

$$I_k(P, s, t) \ll P \Bigl(\sum_{p_1} I_k(P/p_1, s-1, t-1)^{\frac{u}{2s-2}} \Bigr)^{\frac{2s-2}{u}}.$$

From the induction hypothesis and $P^\theta \ll P/p_1 \ll P^\theta$ we find that $I_k(P, s, t) \ll P^\mu$ where

$$\mu = 1 + \frac{2s-2}{u} \Bigl(\frac{1}{k} + \frac{u\theta}{2s-2} (2s - 2 - k + k\theta^{s-1} + k\theta^{t-1}) \Bigr).$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

The largest value occurs when $u = 1$ in which case $\mu = 2s - k + k\theta^s + k\theta^t$. This completes the proof of Lemma 1.

The knowledgeable reader will have noticed that Lemma 1 as well as its proof have a strong affinity to work of Heath-Brown [3] which in turn derives from Karatsuba [4]. However, there is one significant difference to the earlier versions. The range for p_t is rather long provided t is small. Heath-Brown does not have such large primes available, but it is this long range which makes it easy to use the Riemann Hypothesis in an efficient way as will be more apparent in the next section.

3. **The circle method: proof of Theorem 1.** As a precursor to the circle method work we examine the exponential sums

$$f_k(\alpha) = \sum_{p\sim P} (\log p) e(\alpha p^k). \tag{12}$$

The results we need are fairly standard so we will be brief but we shall also fix notation for later use.

Let χ be a Dirichlet character (mod$q$), and put

$$S_\chi(q,a) = \sum_{b=1}^{q} \chi(b) e\Big(\frac{ab^k}{q}\Big); \tag{13}$$

if $\chi = \chi_0$ is the principal character we write

$$S_{\chi_0}(q,a) = S_k^*(q,a). \tag{14}$$

If $q = q_1q_2$ with coprime q_1, q_2, we have $\chi(n) = \chi_1(n)\chi_2(n)$ with suitable characters χ_j modulo q_j. In (13) we write $b = b_1q_2 + b_2q_1$ with b_j mod q_j and then deduce the multiplication formula

$$S_\chi(q,a) = \chi_1(q_2)\chi_2(q_1) S_{\chi_1}(q_1, aq_2^{k-1}) S_{\chi_2}(q_2, aq_1^{k-1}). \tag{15}$$

We also write

$$v_k(\alpha) = \int_P^{2P} e(\alpha\gamma^k)\, d\gamma. \tag{16}$$

We base our work on the readily verified formula

$$f_k\Big(\frac{a}{q} + \beta\Big) = \frac{1}{\phi(q)} \sum_{\chi \pmod q} S_\chi(q,a) \sum_{p\sim P} (\log p)\bar{\chi}(p) e(\beta p^k) + O\big((\log P)^2\big) \tag{17}$$

valid when $(a,q) = 1$. Take $k = 1$ and $\beta = 0$, and note that $S_1^*(q,a) = \mu(q)$. Separate the principal character in (17), and evaluate the sum over p based on the Riemann Hypothesis for the Riemann zeta function. If χ is non-principal then $S_\chi(q,a)$ is a Gauss sum whence $|S_\chi(q,a)| \le \sqrt{q}$. The sums over p can be bounded based on GRH. We then have

$$f_1\Big(\frac{a}{q}\Big) = \frac{\mu(q)}{\phi(q)} P + O\big(\sqrt{qP}(\log P)^2\big).$$

By a standard partial summation we obtain

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

LEMMA 2. *Assume* GRH. *Let* $(a,q)=1$. *Then*

$$f_1\Big(\frac{a}{q}+\beta\Big)=\frac{\mu(q)}{\phi(q)}v_1(\beta)+O\Big(\sqrt{qP}(\log P)^2(1+P|\beta|)\Big).$$

Now suppose that $k\geq 2$. When q is prime with $q\not| \, k$ and $(a,q)=1$ we have $|S_\chi(q,a)|\leq k\sqrt{q}$. This follows from Weil's estimates when χ is non-principal (see Schmidt [7], Theorem 2G), and from Lemma 4.3 of Vaughan [8] when χ is principal. Equation (15) now shows that $|S_\chi(q,a)|\ll q^{1/2+\epsilon}$ when q is squarefree. As in the proof of Lemma 2 we infer

LEMMA 3. *Assume* GRH. *Let* $k\geq 2$, $(a,q)=1$ *and suppose that* q *is squarefree. Then*

$$f_k\Big(\frac{a}{q}+\beta\Big)=\frac{S_k^*(q,a)}{\phi(q)}v_k(\beta)+O(q^{\frac{1}{2}+\epsilon}P^{\frac{1}{2}}\big(1+P^k|\beta|\big)).$$

We are now in a position to begin our circle method approach to Theorem 1. Note that Theorem 1 is weaker than (3) for $k\leq 6$. Therefore we may assume that $k\geq 7$.

There is an unconventional bifurcation in the argument right at the beginning. Let

$$\mathcal{B}_d(k)=\Big\{n\in\mathbb{N}:\Big(n-1,\prod_{\phi(p)|k}p\Big)=d\Big\}. \tag{18}$$

As k is fixed, $\mathcal{B}_d(k)$ is non-empty only for finitely many d. Let N be large, and write

$$P=N^{1/k},\quad L=\log N. \tag{19}$$

Then put

$$f(\alpha)=\sum_{p\sim N}(\log p)e(\alpha p),\quad F_k(\alpha)=\sum_{x=p_0\cdots p_t\in\mathcal{A}_t(P)}(\log p_t)e(\alpha x^k); \tag{20}$$

here $t\in\mathbb{N}$ will be chosen later, and the ranges for the primes in the sum defining $F_k(\alpha)$ are determined by (5). For a d with $\mathcal{B}_d(k)$ non-empty we consider

$$r_d(n)=\int_0^1 f(\alpha)F_k(d^k\alpha)e(-\alpha n)\,d\alpha. \tag{21}$$

Note that $r_d(n)$ counts solutions of $p+(dx)^k=n$ with a certain weight, and with $p\sim N$, $x\in\mathcal{A}_t(P)$. In particular, $r_d(n)>0$ implies that (1) has a solution. We shall show that

$$\#\{n\in\mathcal{B}_d(k)\cap[(d+2)N,(d+3)N]:r_d(n)=0\}\ll N^{1-\frac{1}{25k}}L^{-1}. \tag{22}$$

This suffices to establish Theorem 1.

In the sequel we shall concentrate on the case $d=1$ and indicate the simple changes required for other values of d at a later stage.

Let $1\leq U\leq\sqrt{N}$, and define

$$\mathfrak{K}_U(q,a)=\{\alpha:|q\alpha-a|\leq UN^{-1}\}.$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

We write $\mathfrak{K}(U)$ for the union of all $\mathfrak{K}_U(q,a)$ with $1 \le a \le q \le U$, $(q,a) = 1$. Now let R, Q be parameters to be chosen later, with

$$1 \le R \le P \le Q \le N^{1/3}. \tag{23}$$

For simplicity we write $\mathfrak{M} = \mathfrak{K}(Q)$ and $\mathfrak{m} = [Q/N, 1 + Q/N] \setminus \mathfrak{M}$. Denote by $\mathfrak{N}$ the union of all $\mathfrak{K}_X(q,a)$ with $1 \le a \le q \le R$, $(q,a) = 1$; here $X = RL^{2t+2k}$.

For $\mathfrak{B} = \mathfrak{m}$ or $\mathfrak{M}$ let

$$r(n, \mathfrak{B}) = \int_{\mathfrak{B}} f(\alpha) F_k(\alpha) e(-\alpha n)\, d\alpha.$$

Our first goal is a mean square estimate for $r(n, \mathfrak{m})$. By Lemma 2 and partial integration,

$$f(\alpha) \ll N\phi(q)^{-1}(1 + N|\beta|)^{-1} + L^2\sqrt{qN}(1 + N|\beta|).$$

By Dirichlet's theorem, there are coprime a, q with $1 \le q \le N/Q$ and $|q\alpha - a| \le Q/N$. For $\alpha \in \mathfrak{m}$ we must have $q > Q$ whence

$$\sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \ll N^{1+\epsilon} Q^{-1/2}.$$

By Parseval's identity,

$$\int_0^1 |f(\alpha)|^2\, d\alpha \ll NL$$

and by Lemma 1, on considering the underlying diophantine equation,

$$\int_0^1 |F_k(\alpha)|^{2s}\, d\alpha \ll P^{2s-k+k\theta^s+k\theta^t+\epsilon} \ll P^{2s} N^{\theta^s+\theta^t-1+\epsilon}$$

for any $s \in \mathbb{N}$. By Bessel's inequality and Hölder's inequality we deduce that

$$\begin{aligned}\sum_n |r(n,\mathfrak{m})|^2 &\le \int_{\mathfrak{m}} |f(\alpha)F_k(\alpha)|^2\, d\alpha \\ &\le \left(\int_0^1 |F_k(\alpha)|^{2s}\, d\alpha\right)^{\frac{1}{s}} \left(\int_0^1 |f(\alpha)|^2\, d\alpha\right)^{1-\frac{1}{s}} \sup_{\mathfrak{m}} |f(\alpha)|^{\frac{2}{s}}.\end{aligned}$$

Collecting together we find that

$$\sum_n |r(n,\mathfrak{m})|^2 \ll P^2 N^{1+\epsilon+\frac{1}{s}(\theta^s+\theta^t)} Q^{-\frac{1}{s}}. \tag{24}$$

Let $f^*(\alpha)$ be defined on $\mathfrak{M}$ by $f^*(\frac{a}{q} + \beta) = \mu(q)\phi(q)^{-1}v(\beta)$ where

$$v(\beta) = \int_N^{2N} e(\beta\gamma)\, d\gamma.$$

We shall compare $r(n, \mathfrak{M})$ with $r^*(n, \mathfrak{M})$, where more generally we write

$$r^*(n, \mathfrak{B}) = \int_{\mathfrak{B}} f^*(\alpha) F_k(\alpha) e(-\alpha n)\, d\alpha$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

when $\mathfrak{B} \subset \mathfrak{M}$ is measurable. By Lemma 2,

$$\int_{\mathfrak{M}} |f(\alpha) - f^*(\alpha)|^2 \, d\alpha \ll N^{1+\epsilon} \sum_{q \le Q} q\phi(q) \int_{-Q/(qN)}^{Q/(qN)} (1 + N^2|\beta|^2)\, d\beta \ll Q^3 N^{\epsilon}.$$

By Bessel's inequality and trivial estimates we deduce that

$$\sum_n |r(n,\mathfrak{M}) - r^*(n,\mathfrak{M})|^2 \le \int_{\mathfrak{M}} \left| \bigl(f(\alpha) - f^*(\alpha)\bigr) F_k(\alpha) \right|^2 d\alpha \ll P^{2+\epsilon} Q^3. \tag{25}$$

Next we prune the major arcs $\mathfrak{M}$ to the decently thinner $\mathfrak{N}$. By standard estimates,

$$f^*\Bigl(\frac{a}{q} + \beta\Bigr) \ll N^{1+\epsilon} q^{-1} (1 + N|\beta|)^{-1}. \tag{26}$$

Hence, choosing $\Psi(\alpha) = |F_k(\alpha)|^2$ in Lemma 2 of Brüdern [1], we have

$$\int_{\mathfrak{K}(2U)\setminus\mathfrak{K}(U)} |f^*(\alpha) F_k(\alpha)|^2 \, d\alpha \ll N^{1+\epsilon} U^{-1} \int_{\mathfrak{K}(2U)} |f^*(\alpha)|\, |F_k(\alpha)|^2 \, d\alpha \ll N^{1+\epsilon} P(1 + PU^{-1}).$$

We can cover $\mathfrak{M} \setminus \mathfrak{N}$ by $O(\log N)$ sets $\mathfrak{K}(2U) \setminus \mathfrak{K}(U)$ with $R < U \le Q$. By Bessel's inequality and the previous estimate,

$$\sum_n |r^*(n,\mathfrak{M}) - r^*(n,\mathfrak{N})|^2 \le \int_{\mathfrak{M}\setminus\mathfrak{N}} |f^*(\alpha) F_k(\alpha)|^2 \, d\alpha \ll N^{1+\epsilon} P^2 R^{-1}. \tag{27}$$

It is now necessary to approximate $F_k(\alpha)$ on $\mathfrak{N}$. We write $M = P^{\theta'}$ in the interest of clarity. In the notation introduced in (5) we write any $x = p_0 \cdots p_t \in \mathcal{A}_t(P)$ as $x = p_t r$; then

$$F_k(\alpha) = \sum_r \sum_{p_t \sim P/r} e(\alpha p_t^k r^k) \log p_t$$

with the sum over $r = p_0 \cdots p_{t-1}$ restricted to the ranges determined by (5). Apply Lemma 3 to the inner sum and observe $M \ll P/r \ll M$ to deduce that

$$\sum_{p_t \sim P/r} (\log p_t) e\Bigl(\Bigl(\frac{a}{q} + \beta\Bigr)(p_t r)^k \Bigr) = \frac{S^*(q, ar^k)}{r\phi(q)} v_k(\beta) + O\bigl((qM)^{\frac{1}{2}+\epsilon} (1 + M^k r^k |\beta|) \bigr)$$

provided q is squarefree. For $q \le P$ summing over r produces

$$F_k\Bigl(\frac{a}{q} + \beta\Bigr) = F_k^*\Bigl(\frac{a}{q} + \beta\Bigr) + O\bigl(P^{1+\epsilon} M^{-\frac{1}{2}} q^{\frac{1}{2}} (1 + N|\beta|) \bigr) \tag{28}$$

where

$$F_k^*\Bigl(\frac{a}{q} + \beta\Bigr) = \sum_r \frac{S^*(q, ar^k)}{r\phi(q)} v_k(\beta).$$

We now define

$$R^*(n) = \int_{\mathfrak{N}} f^*(\alpha) F_k^*(\alpha) e(-\alpha n)\, d\alpha$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

and then have, by Bessel's inequality, (26), (28) and the observation that $f^*(\alpha) = 0$ unless q is squarefree,

$$\sum_n |r^*(n, \mathfrak{R}) - R^*(n)|^2 \leq \int_{\mathfrak{R}} \left| f^*(\alpha)\big(F_k(\alpha) - F_k^*(\alpha)\big)\right|^2 d\alpha$$

$$\ll N^{2+\epsilon}P^2M^{-1} \sum_{q \leq R} \int_{-R/(qN)}^{R/(qN)} d\alpha \ll N^{1+\epsilon}P^2RM^{-1}. \tag{29}$$

It remains to evaluate $R^*(n)$. All the relevant information is contained in the next lemma the proof of which is postponed to the next sections.

LEMMA 4. *Suppose that $t \leq ck$ for some constant c. Then, for all but $O_c(N^{1+\epsilon}R^{-\frac{1}{2}})$ values of $n \in \mathcal{B}_1(k) \cap [3N, 4N]$ we have $R^*(n) > P^{1-\epsilon}$.*

We can now complete the proof of Theorem 1. By (24), (25), (27) and (29),

$$\sum_n |r_1(n) - R^*(n)|^2 \ll P^2N^{1+\epsilon}\Xi$$

where

$$\Xi = N^{\frac{1}{s}(\theta^s+\theta^t)}Q^{-\frac{1}{s}} + Q^3N^{-1} + R^{-1} + RM^{-1}.$$

Hence, the number of $n \in [3N, 4N)$ with $|r_1(n) - R^*(n)| > P^{1-2\epsilon}$ is $O(N^{1+2\epsilon}\Xi)$. For any $n \in \mathcal{B}_1(k) \cap [3N, 4N]$ which is not exceptional in Lemma 4 and satisfies $|r_1(n) - R^*(n)| < P^{1-2\epsilon}$ we have $r_1(n) \gg P^{1-\epsilon}$. Hence $r_1(n) = 0$ can hold for at most

$$O(N^{1+2\epsilon}\Xi + N^{1+\epsilon}R^{-1/2}) \tag{30}$$

values of $n \in \mathcal{B}_1(k) \cap [3N, 4N]$. We now choose $R = M^{2/3}$. Since $M < P$ this is in line with (23). We also choose $Q = N^\lambda$ with $0 < \lambda < \frac{1}{3}$. Then (30) reduces to $O(N^{1+\epsilon-\kappa})$ where

$$\kappa = \min\left(\frac{1}{s}(\lambda - \theta^s - \theta^t), 1 - 3\lambda, \frac{\theta^t}{3k}\right).$$

A simple but close to optimal choice is $s = 3k, t = 2k, \lambda = \frac{1}{3} - \frac{1}{60k}$. Using $\theta^k < \frac{1}{e}$ it is readily confirmed that $\kappa = \frac{\theta^t}{3k} > \frac{1}{25k}$ for $k \geq 10$. When $k = 9$ choose $s = 27, t = 17$. When $k = 8$ choose $s = 22, t = 15$, and when $k = 7$ choose $s = 19, t = 13$ to confirm $\kappa > \frac{1}{25k}$. This confirms (22) when $d = 1$, as required.

When k is large this argument can be improved slightly by choosing $s = Ak$, $t = Bk$ and optimizing the values of A, B. With $A = 3.051\cdots$, $B = 1.95\cdots$ one finds $(k\kappa)^{-1} \longrightarrow 21.15\cdots$, as mentioned in the introduction.

4. The main term. This section will reduce the proof of Lemma 4 to a problem on the singular series, the latter being dealt with in the next section. Writing

$$H^*(q, r, n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S_k^*(q, ar^k)e\left(-\frac{an}{q}\right), \tag{31}$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

$$I(n,\xi) = \int_{-\xi}^{\xi} v(\beta)v_k(\beta)e(-\beta n)\,d\beta \tag{32}$$

we have

$$R^*(n) = \sum_{q\le R} \frac{\mu(q)}{\phi(q)^2} \sum_r \frac{H^*(q,r,n)}{r} I\big(n, X/(qN)\big) \tag{33}$$

where $X = RL^{2k+2t}$, recalling the definition of $\mathfrak{R}$ and the convention about summations over r from the previous section.

Further progress depends on bounds for $H^*(q,r,n)$ which we now derive. For fixed r and n the function $H^*(q,r,n)$ is multiplicative in q. Thanks to the factor $\mu(q)$ in (33) we may now restrict attention to prime values of q. If p is prime, $p \not| r$ we have $S_k^*(p, ar^k) = S_k^*(p,a)$ whence

$$H^*(p,,r,n) = H^*(p,n) \tag{34}$$

where $H^*(p,n) = H^*(p,1,n)$ in the interest of brevity. Let $\rho^*(n,p)$ denote the number of solutions of the congruence $m^k \equiv n \pmod p$ with $p \not| m$. From (31) we see that

$$H^*(p,n) = p\rho^*(n,p) - \phi(p). \tag{35}$$

If $p|r$ then $S^*(p, ar^k) = \phi(p)$, and (31) yields

$$H^*(p,r,n) = H^*(p,p,n) = \begin{cases} -\phi(p) & \text{if } p \not| n \\ \phi(p)^2 & \text{if } p|n. \end{cases} \tag{36}$$

Now $0 \le \rho^*(n,p) \le k$ so that (35) gives $|H^*(p,n)| \le kp$. Combining this with (34) and (36) we deduce that

$$|\mu(q)H^*(q,r,n)| \le k^{\omega(q)} q(q,r,n) \tag{37}$$

where $\omega(q)$ is the number of different prime factors of q, and (q,r,n) is the greatest common divisor of q, r and n.

We can now replace $I\big(n,X/(qN)\big)$ with $I(n,\infty)$ in (33). Indeed, by standard estimates,

$$I\big(n,X/(qN)\big) - I(n,\infty) \ll NP \int_{X/(qN)}^{\infty} (1+N\beta)^{-2}\,d\beta \ll PqX^{-1}.$$

By (37) and crude estimates, the total error of inserting $I(n,\infty)$ in place of $I\big(n,X/(qN)\big)$ in (33) does not exceed

$$\ll \frac{P}{X} \sum_{q\le R} \sum_r k^{\omega(q)} \frac{q^2(q,r)}{\phi(q)^2 r} \ll PRX^{-1}L^{k+2} \ll PL^{2-2t-k}.$$

This shows

$$R^*(n) = I(n,\infty) \sum_{q\le R} \frac{\mu(q)}{\phi(q)^2} \sum_r \frac{H^*(q,r,n)}{r} + O(PL^{2-2t-k}). \tag{38}$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

In the next step we replace $H^*(q,r,n)$ with $H^*(q,n)$, by brute force. By (34) and (37),

$$\sum_{q\le R}\frac{|\mu(q)|}{\phi(q)^2}\sum_r r^{-1}|H^*(q,r,n)-H^*(q,n)| \ll \sum_{q\le R}\sum_{r:(r,q)>1} k^{\omega(q)}\frac{|\mu(q)|q(q,n)}{\phi(q)^2 r}$$

$$(39) \qquad \ll L^{k+1}d_{k+1}(n)\max_{q\le R}\sum_{r:(r,q)>1}\frac{1}{r}.$$

Let q_0 be a value q where the maximum in (39) is attained. Any r occurring in the summation is of the form $p_0\cdots p_{t-1}$ where the p_i satisfy (5). Now $t\le ck$ so that $\theta^l\ge\theta^t\ge c_1$ for $l\le t$; here c_1 denotes a constant depending on c only (not on k). Since $q_0\le R\le P$ there can be at most kc_1^{-1} primes $p|q_0, p>P^{\theta^l/k}$. Let $\mathcal{P}$ denote the set of all primes $p|(q_0,r)$ for some $r=p_0\cdots p_{t-1}$; then $\#\mathcal{P}\le kc_1^{-1}$ by the previous remark. It follows that

$$\sum_{r:(r,q_0)>1}\frac{1}{r}\ll\sum_{p_i\in\mathcal{P}}\sum_{r'}\frac{1}{p_ir'}$$

where r' runs over all numbers $r'=p_0\cdots p_{i-1}p_{i+1}\cdots p_{t-1}$ and $r=p_ir'$. However, $p_i\ge P^{c_1/k}$ whence

$$(40) \qquad \sum_{r:(r,q_0)>1}\frac{1}{r}\ll P^{-\delta}$$

for some $\delta=\delta_k>0$. A familiar argument based on Fourier's inversion formula (see Vaughan [9], p. 165, for a model) confirms the lower bound in

$$(41) \qquad P\ll I(n,\infty)\ll P \quad (3N<n\le 4N)$$

the corresponding upper bound being a rather easier deduction directly from (32) and standard bounds for v and v_k. Combining (38), (39), (40) and (41) we now deduce

$$(42) \qquad R^*(n)=I(n,\infty)\mathfrak{S}^*(n,R)\sum_r\frac{1}{r}+O(PL^{2-2t-k})$$

where

$$(43) \qquad \mathfrak{S}^*(n,R)=\sum_{q\le R}\frac{\mu(q)}{\phi(q)^2}H^*(q,n).$$

Elementary prime number theory and (5) show that

$$\sum_r\frac{1}{r}\gg L^{-t}$$

so that Lemma 4 follows from (42) and the following lower bound for the singular series.

LEMMA 5. *For all but $O(N^{1+\epsilon}R^{-1/2})$ values of $n\in\mathcal{B}_1(k)\cap[3N,4N]$ one has $\mathfrak{S}^*(n,R)\gg L^{-k}$.*

5. **The singular series.** The treatment of the truncated singular series $\mathfrak{S}^*(n,R)$ follows the general pattern of Section 4 of Perelli and Zaccagnini [6]. We will only sketch the argument, indicating the changes to be made.

Let

$$\Pi^*(R,n)=\prod_{p\le R}\left(1-\frac{H^*(p,n)}{\phi(p)^2}\right),$$

$$\mathcal{D}=\{q:\mu(q)\neq 0, p|q\Rightarrow p\le R\}.$$

Then

$$\Pi^*(R,n)-\mathfrak{S}^*(R,n)=\sum_{\substack{R<q\le V\\ q\in\mathcal{D}}}A^*(q,n)+\sum_{\substack{q>V\\ q\in\mathcal{D}}}A^*(q,n)=S_1+S_2, \tag{44}$$

say, where

$$A^*(q,n)=\frac{\mu(q)}{\phi(q)^2}H^*(q,n),\qquad V=\exp\bigl(L(\log L)^{3/2}\bigr).$$

We estimate S_2 by Rankin's method. By (37) one has

$$S_2\le\sum_{q\in\mathcal{D}}\left(\frac{q}{V}\right)^{1/L}|A^*(q,n)|$$

$$=V^{-1/L}\prod_{p\le R}\left(1+\frac{p^{1/L}}{\phi(p)^2}|H^*(p,n)|\right)\ll\exp(-C(\log L)^{3/2}) \tag{45}$$

for some $C=C(k)>0$, uniformly in n.

To treat S_1 we introduce the number $\rho(n,p)$ of solutions of the congruence $m^k\equiv n \pmod p$ and note that

$$\rho^*(n,p)=\begin{cases}\rho(n,p) & \text{if } p\not| n,\\ 0 & \text{if } p|n.\end{cases} \tag{46}$$

Moreover let $\mathcal{C}(r)$ denote the set of all primitive (whence non-principal) Dirichlet characters modulo r with χ^k principal. For later use we record here the familiar inequality

$$\#\mathcal{C}(r)\le(k-1)^{\omega(r)} \tag{47}$$

and the well-known identity

$$\rho(n,p)-1=\sum_{\chi\in\mathcal{C}(p)}\chi(n).$$

From the latter we have

$$\prod_{p|r}\bigl(\rho(n,p)-1\bigr)=\sum_{\chi\in\mathcal{C}(r)}\chi(n)=\Sigma(r,n), \tag{48}$$

say.

From now on we write $d=(q,n)$. Then, by (31), (46) and (48),

$$A^*(q,n)=\frac{\mu(q)q}{\phi(q)^2}(-1)^{\omega(d)}\frac{\phi(d)}{d}\sum_{rm=q/d}\frac{1}{m}\Sigma(r,n).$$

Hence, a little rearrangement yields

$$S_1 = \sum_{\substack{d|n\\ d\in\mathcal{D}}} \frac{\mu(d)(-1)^{\omega(d)}}{\phi(d)} \sum_{\substack{r\le V/d\\ r\in\mathcal{D}\\ (r,n)=1}} \frac{\mu(r)r}{\phi(r)^2}\Sigma(r,n) \sum_{\substack{R<drm\le V\\ m\in\mathcal{D}\\ (m,n)=1}} \frac{\mu(m)}{\phi(m)^2}. \tag{49}$$

If $(r,n)>1$ then $\Sigma(r,n)=0$. Therefore we may drop the condition $(r,n)=1$ in (49).

Let $\delta>0$ be small. By (47) and (48) we have

$$\sum_{\substack{d|n\\ d\in\mathcal{D}}} \frac{\mu(d)(-1)^{\omega(d)}}{\phi(d)} \sum_{\substack{r\le RN^{-\delta}\\ r\in\mathcal{D}}} \frac{\mu(r)r}{\phi(r)^2}\Sigma(r,n) \sum_{\substack{R<drm\le V\\ m\in\mathcal{D}\\ (m,n)=1}} \frac{\mu(m)}{\phi(m)^2}$$

$$\ll L\sum_{d|n}\frac{1}{d}\sum_{r\le RN^{-\delta}}\frac{(k-1)^{\omega(r)}}{r}\sum_{m>R/(dr)}\frac{1}{m^2} \ll N^{-\delta/2}. \tag{50}$$

Moreover, for $n\le 4N$,

$$\sum_{\substack{d|n\\ d\in\mathcal{D}}} \frac{\mu(d)(-1)^{\omega(d)}}{\phi(d)} \sum_{\substack{RN^{-\delta}<r\le V/d\\ r\in\mathcal{D}}} \frac{\mu(r)r}{\phi(r)^2}\Sigma(r,n) \sum_{\substack{R<mdr\le V\\ m\in\mathcal{D}\\ (m,n)=1}} \frac{\mu(m)}{\phi(m)^2}$$

$$= \sum_{\substack{d|n\\ d\in\mathcal{D}}} \frac{\mu(d)(-1)^{\omega(d)}}{\phi(d)} \sum_{\substack{m\le VN^{\delta}/(dR)\\ m\in\mathcal{D}\\ (m,n)=1}} \frac{\mu(m)}{\phi(m)^2} \sum_{\substack{\max(RN^{-\delta},R/(md))\le r\le V/(dm)\\ r\in\mathcal{D}}} \frac{\mu(r)r}{\phi(r)^2}\Sigma(r,n)$$

$$\ll L \max_{(d,m):dm\le V}\Bigg|\sum_{\substack{\max(RN^{-\delta},R/(md)\le r\le V/(dm)\\ r\in\mathcal{D}}} \frac{\mu(r)r}{\phi(r)^2}\Sigma(r,n)\Bigg|$$

$$= L\Bigg|\sum_{\substack{V_1\le r\le V_0\\ r\in\mathcal{D}}} \frac{\mu(r)r}{\phi(r)^2}\Sigma(r,n)\Bigg| = L|\tilde{S}_1| \tag{51}$$

say; here $RN^{-\delta}\le V_1<V_0\le V$ correspond to a pair (d,m) where the maximum occurs.

Now we may proceed exactly as in Section 4 of Perelli and Zaccagnini [6] since $\tilde{S}_1$ has a very similar shape to that of the quantity S_1 in Perelli and Zaccagnini [6], the only difference being a factor $\phi(r)/r$ (and a slightly different range of summation) which clearly causes no problems. Hence we get

$$\sum_{3N<n\le 4N} |\tilde{S}_1| \ll N^{1+2\delta}R^{-1/2}, \tag{52}$$

and from (44), (45), (51), (52) we deduce that

$$\mathfrak{S}^*(R,n) = \Pi^*(R,n) + O(\exp(-C(\log L)^{3/2}) \tag{53}$$

for all but $O(N^{1+3\delta}R^{-1/2})$ values of $n\in[3N,4N]$. However, we have

$$\Pi^*(R,n) = \prod_{p\le R}\left(1-\frac{p}{\phi(p)^2}\rho^*(n,p)+\frac{1}{\phi(p)}\right).$$

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

Note that an individual factor vanishes if and only if $\rho^*(n,p) = \phi(p)$, and is positive if $\rho^*(p) < \phi(p)$. But $\rho^*(n,p) = \phi(p)$ implies $\phi(p)|k$ and $p|n-1$ which contradicts $n \in \mathcal{B}_1(k)$. Now use (46) and $\rho(n,p) \leq k$ for $p \not| n$ to see that

$$\Pi^*(R,n) \gg \prod_{\substack{p|n \\ p\leq R}} \left(1 + \frac{1}{\phi(p)}\right) \prod_{\substack{p\not| n \\ k<p\leq R}} \left(1 - \frac{k}{p}\right) \gg (\log R)^{-k}.$$

Since δ is arbitrary, Lemma 5 follows from (53).

It is the very last paragraph which has forced us to introduce the sets $\mathcal{B}_d(k)$. The partial singular product $\Pi^*(R,n)$ would not be positive for $n \in \mathcal{B}_d(k)$ with $d > 1$. The introduction of d into the underlying diophantine equation (compare (21)) repairs this defect, and the above argument applies to $\mathcal{B}_d(k)$ with no essential differences.

6. **Proof of Theorem 2.** A proof of Theorem 2 can be given along very similar lines. However, Lemma 1 is of course not available. With $f(\alpha)$ and $f_k(\alpha)$ given by (12) and (20), and recalling (19) we consider

$$\int_0^1 f(\alpha)f_k(\alpha)e(-\alpha n)\,d\alpha. \tag{54}$$

We redefine the parameters Q, R by

$$Q = N^{\frac{1}{3}-\frac{1}{k}}, \quad R = P^{1/6} \tag{55}$$

but then define $\mathfrak{m}, M, N$ as before. By Theorem 5.1 and (5.37) of Vaughan [8], on considering the underlying diophantine equations,

$$\int_0^1 |f_k(\alpha)|^{2kl}\,d\alpha \leq L^{2kl} \int_0^1 \Big|\sum_{x\leq 2P} e(\alpha x^k)\Big|^{2kl} d\alpha \ll P^{2kl-k+\frac{1}{2}k^2\theta^l+\epsilon}. \tag{56}$$

for any positive integer l. We take $l = k[\log k]$ and put $s = kl$. We can now use (56) in the argument leading to (24) to show that

$$\int_{\mathfrak{m}} |f(\alpha)f_k(\alpha)|^2\,d\alpha \ll NP^2N^{-c/s} \tag{57}$$

for some constant $c > 0$ not depending on k. This bound is appropriate for the minor arcs. The treatment of $\mathfrak{M}$, its pruning to $\mathfrak{N}$ and the evaluation of the main term can be performed as in the proof of Theorem 1, the details being even simpler.

References

1. J. Brüdern, *A problem in additive number theory*, Math. Proc. Cambridge Philos. Soc. **103**(1988), 27–33.
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. D. R. Heath-Brown, *The fractional part of αn^k*, Mathematika **35**(1988) 28–37.
4. A. A. Karatsuba, *On the function $G(n)$ in Waring's problem*, Izv. Akad. Nauk SSSR Ser. Mat. **49**(1985), 935–947.
5. H. Mikawa, *On the sum of a prime and a square*, Tsukuba J. Math. **17**(1993), 299–310.

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press

6. A. Perelli and A. Zaccagnini, *On the sum of a prime and a k-th power*, Izv. Ross. Akad. Nauk Ser. Mat. **59**(1995), 185–200.

7. W. M. Schmidt, *Equations over finite fields*, Berlin, 1976.

8. R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge, 1981.

9. ———, *On Waring's problem for cubes*, J. Reine Angew. Math. **365**(1986) 122–170.

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

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

12. ———, *Additive problems with prime numbers*, to appear.

Mathematisches Institut A
Pfaffenwaldring 57
D-70511 Stuttgart
Germany
e-mail: bruedern@fermat.mathematik.uni-stuttgart.de

Dipartimento di Matematica
Via Dodecaneso 35
I-16146 Genova
Italy
e-mail: perelli@dima.unige.it

https://doi.org/10.4153/CJM-1996-026-8 Published online by Cambridge University Press