ACTA ARITHMETICA
LXXXV.1 (1998)

Sums of powers: an arithmetic refinement to the probabilistic model of Erdős and Rényi

by

Jean-Marc Deshouillers (Bordeaux),
François Hennecart (Talence) and Bernard Landreau (Talence)

Erdős and Rényi proposed in 1960 a probabilistic model for sums of s integral sth powers. Their model leads almost surely to a positive density for sums of s pseudo sth powers, which does not reflect the case of sums of two squares. We refine their model by adding arithmetical considerations and show that our model is in accordance with a zero density for sums of two pseudo-squares and a positive density for sums of s pseudo sth powers when $s \geq 3$. Moreover, our approach supports a conjecture of Hooley on the average of the square of the number of representations.

1. Introduction. The asymptotic behaviour of sums of two squares has been rather well known since Landau [9] proved in 1908 that their number up to x is asymptotically equal to $Cx/\sqrt{\log x}$, for some positive (explicitly determined) constant C. The similar question concerning sums of 3 cubes, 4 biquadrates, ..., s integral sth powers is not yet solved. Some numerical experiments performed by Barrucand [2] in 1968 led him to expect a zero asymptotic density for sums of 3 cubes and 4 biquadrates, whereas Hooley [8] presented in 1986 some arguments in favour of a positive density hypothesis. The first heuristic approach to this problem is that of Erdős and Rényi [4] who suggested in 1960 a probabilistic model for sums of s integral sth powers. The elements of a sequence having the asymptotic distribution of the sth powers are called *pseudo-squares* ($s = 2$), *pseudo-cubes* ($s = 3$) or *pseudo sth powers*. Erdős and Rényi announced a Poisson behaviour for the number of representations of an integer as a sum of s pseudo sth powers. The case $s = 2$ was completely proved in 1966 by Halberstam and Roth [6]. We are thankful to Prof. Wirsing who drew our attention to the paper by

1991 *Mathematics Subject Classification*: Primary 11P05; Secondary 60F99.
Ce travail a été réalisé au sein du laboratoire A2X, UMR CNRS-Bordeaux I n° 9936, avec le soutien de l'Université Victor Segalen Bordeaux 2.

Goguel [5] who proved the Poisson behaviour of the density of the sequences of the integers having a given number of representations as a sum of s pseudo sth powers. The claim of Erdős and Rényi was completed in the general case by Landreau [10]. This model has however the drawback to lead to a positive density for sums of 2 pseudo-squares. In the above-mentioned work, Hooley takes into consideration the mean-square of the number $r_s(n)$ of representations of an integer n as a sum of s integral sth powers; he gives many a non-trivial lower bound for it, and conjectures the validity, for $s \geq 3$, of the asymptotic relation

$$\frac{1}{x}\sum_{n\leq x} r_s^2(n) \underset{x\to\infty}{\longrightarrow} A_s^2\mathfrak{S} + s!A_s \tag{1}$$

where $A_s = \Gamma(1+1/s)^s$ and $\mathfrak{S} = \mathfrak{S}(s)$ is the singular series that naturally arises in the problem. He notes that this relation implies that the sequence of sums of sth powers has a positive asymptotic lower density when $s \geq 3$.

It is interesting to notice that the Erdős–Rényi model leads to $A_s^2 + s!A_s$ on the right hand side of (1). The additional arithmetic term $A_s^2(\mathfrak{S}-1)$ is introduced by Hooley to take into account the arithmetic irregularity of sth powers, as measured by the contribution of the non-trivial major arcs in the natural integral representation of the left hand side of (1).

We suggest here a family of probabilistic models which mimic not only the asymptotic behaviour of sth powers, but also their distribution in given arithmetic progressions. From now on, by pseudo sth powers, we mean integers from sequences generated by these models. For each of these models, we observe, among other features, that the mean-square of the number of representations of an integer n as a sum of s pseudo sth powers tends to a finite bound, but also that these sums have a positive asymptotic density. Moreover, when the modulus of the arithmetic progression considered tends multiplicatively to infinity (by taking all the prime powers into account) then the mean-square of the number of representations tends to the right hand side of (1) when $s \geq 3$. Under the same condition on the modulus, the asymptotic density for the sums of s pseudo sth powers tends to 0 when $s = 2$ and to a positive real number when $s \geq 3$.

2. General study of the model for a given modulus K. In order to take into account the irregularities of congruence type in the distribution of powers, we shall adapt to arithmetic progressions the general probabilistic model given in [10]. In the sequel, s denotes an integer greater than 1. Furthermore, the integers K and k will respectively represent the modulus and the first term of the arithmetic progression we consider.

For $n \geq 1$, we let

$$\alpha_n = \frac{1}{s(nK)^{1-1/s}},$$

and consider for $0 \leq k < K$ a family of sequences of independent Bernoulli random variables $(\xi_n^{(k)})_{n\geq 1}$ satisfying

$$P(\xi_n^{(k)} = 1) = \alpha_n \quad \text{and} \quad P(\xi_n^{(k)} = 0) = 1 - \alpha_n.$$

We define the increasing sequences of integral valued random variables $(\nu_l^{(k)})_{l\geq 1}$ as the sequences of the integers n such that $\xi_n^{(k)} = 1$. We then have

$$1 \leq \nu_1^{(k)} < \nu_2^{(k)} < \ldots < \nu_l^{(k)} < \ldots,$$

and

$$\xi_1^{(k)} + \xi_2^{(k)} + \ldots + \xi_{\nu_l}^{(k)} = l \quad \text{for all } l \geq 1. \tag{2}$$

We finally associate with the random variables $(\nu_l^{(k)})_{l\geq 1}$ the sequences $(\mu_l^{(k)})_{l\geq 1}$ defined by

$$\mu_l^{(k)} = \nu_l^{(k)} K + m(k^s),$$

where $m(k^s)$ is the residue of k^s modulo K.

The sequences $(\mu_l^{(k)})$ give a probabilistic model for the sequence of sth powers in congruence classes modulo K: indeed, as can be easily proved by following the arguments in [10]:

(i) almost surely, the sequence $(\mu_l^{(k)})_{l\geq 1}$ is infinite,

(ii) almost surely, $\mu_l^{(k)} \sim (Kl + k)^s$ as l tends to infinity.

Let now k_0 be a given residue modulo K. We denote by $\mathbf{k} = (k_1, \ldots, k_s)$ a solution of the congruence

$$k_1^s + \ldots + k_s^s \equiv k_0 \pmod{K}, \tag{3}$$

by $\mathcal{C}(k_0)$ the set of solutions of (3) and by $\varrho(k_0, K)$ the cardinality of $\mathcal{C}(k_0)$. For $\mathbf{k} = (k_1, \ldots, k_s) \in \mathcal{C}(k_0)$ and n congruent to k_0 modulo K, we denote by $R_{\mathbf{k}}(n)$ the number of representations of n as

$$n = \mu_{l_1}^{(k_1)} + \ldots + \mu_{l_s}^{(k_s)}, \tag{4}$$

with

$$\mu_{l_1}^{(k_1)} < \ldots < \mu_{l_s}^{(k_s)}. \tag{5}$$

Let us explain why we define $R_{\mathbf{k}}(n)$ in that way. Our main concern is to get information by probabilistic means about the density of the set of integers which can be represented as a sum of s sth powers. It is easy to see that the number of integers up to x which are sums of s sth powers, two of which at least being equal, is $O(x^{1-1/s})$, which will not affect density results. Thus we can restrict ourselves in (4) to representations with s different terms. Furthermore, in order to count each essentially different representation only once, we are naturally led to impose the condition (5).

Note that, on the one hand, the condition (5) is implied by the condition

$$\nu_{l_1}^{(k_1)} < \ldots < \nu_{l_s}^{(k_s)}, \tag{6}$$

and, on the other hand, it implies the condition

$$\nu_{l_1}^{(k_1)} \le \ldots \le \nu_{l_s}^{(k_s)}. \tag{7}$$

Let us denote by $R'_{\mathbf{k}}(n)$ the number of representations of n as (4) with the condition (6) and by $R''_{\mathbf{k}}(n)$ the number of representations of n as (4) with the condition (7). We then have

$$R'_{\mathbf{k}}(n) \le R_{\mathbf{k}}(n) \le R''_{\mathbf{k}}(n). \tag{8}$$

We finally denote by R_n (respectively R'_n, R''_n) the total number of representations when summing over all solutions $\mathbf{k} \in \mathcal{C}(k_0)$:

$$R_n = \sum_{\mathbf{k} \in \mathcal{C}(k_0)} R_{\mathbf{k}}(n) \quad (\text{resp. } R'_{\mathbf{k}}(n), R''_{\mathbf{k}}(n)). \tag{9}$$

2.1. *Local convergence in distribution.* Our first result deals with the behaviour of the sequence of random variables (R_n) when we consider a fixed congruence class k_0 modulo K.

THEOREM 1. *When $n \equiv k_0 \pmod K$ tends to infinity, the sequence of random variables (R_n) converges in distribution towards the Poisson law with parameter*

$$\lambda(k_0, K, s) = \gamma \frac{\varrho(k_0, K)}{K^{s-1}}, \quad \textit{where} \quad \gamma = \gamma(s) = \frac{\Gamma(1/s)^s}{s! s^s}.$$

Before embarking upon the proof, let us make a heuristic comment. The random variable R_n is a finite sum of random variables. By [10], each of them converges to a Poisson law with parameter γ/K^{s-1}. If we see them as being more or less independent, we expect their sum to converge towards a Poisson law with a parameter which is the sum of the parameters of each of them. Since there are $\varrho(k_0, K)$ of them, we may expect Theorem 1 to hold true.

Proof (of Theorem 1). We shall in fact establish Theorem 1 for the random variables R'_n. The method (developed in [10]) gives also clearly the same result for R''_n. Then using inequalities (8) and the distribution functions of R_n, R'_n, R''_n, it is clear that Theorem 1 also holds for R_n.

The class k_0 being fixed, for n large enough, $R'_{\mathbf{k}}(n)$ denotes the number of representations of $N_{\mathbf{k}} := (n - m(k_1^s) - \ldots - m(k_s^s))/K$ as

$$N_{\mathbf{k}} = \nu_{l_1}^{(k_1)} + \ldots + \nu_{l_s}^{(k_s)},$$

with $\nu_{l_1}^{(k_1)} < \nu_{l_2}^{(k_2)} < \ldots < \nu_{l_s}^{(k_s)}$.

This implies that

$$R'_{\mathbf{k}}(n) = \sum_{\mathbf{h}\in\mathcal{H}(N_{\mathbf{k}})} \xi_{h_1}^{(k_1)} \dots \xi_{h_s}^{(k_s)},$$

where $\mathcal{H}(N) = \{\mathbf{h} = (h_1, \dots, h_s) : 1 \le h_1 < \dots < h_s \le N, h_1 + \dots + h_s = N\}$ (we retain the notation of [10]).

We then have

$$R'_n = \sum_{\mathbf{k}\in\mathcal{C}(k_0)} \sum_{\mathbf{h}\in\mathcal{H}(N_{\mathbf{k}})} \xi_{h_1}^{(k_1)} \dots \xi_{h_s}^{(k_s)} = \sum_{\mathbf{k}\in\mathcal{C}(k_0),\, \mathbf{h}\in\mathcal{H}(N_{\mathbf{k}})} \theta_{\mathbf{k},\mathbf{h}},$$

where $\theta_{\mathbf{k},\mathbf{h}} = \xi_{h_1}^{(k_1)} \dots \xi_{h_s}^{(k_s)}$.

As in [10], we introduce the events $A_{\mathbf{k},\mathbf{h}} = \{\theta_{\mathbf{k},\mathbf{h}} = 1\}$ and the set $\mathcal{A} = \{A_{\mathbf{k},\mathbf{h}} : \mathbf{k} \in \mathcal{C}(k_0),\ \mathbf{h} \in \mathcal{H}(N_{\mathbf{k}})\}$. We also write $P_{[r]} = P(R'_n = r)$ and denote by $Q_{[r]}$ the quantity

$$Q_{[r]} := \sum_{A_1, A_2, \dots, A_r} P(A_1)P(A_2)\dots P(A_r) \prod_{A \ne A_1, \dots, A_r} P(\bar{A}),$$

the summation being performed over all r-subsets of $\mathcal{A}$. If the events A_i were independent, we would have $P_{[r]} = Q_{[r]}$.

As usual $\mathbf{E}$ and $\mathbf{D}$ will respectively denote the mathematical expectation and the dispersion of random variables. An upper bound for the error term $|P_{[r]} - Q_{[r]}|$ is then given, as in [10], in terms of

$$\Delta_r(n) = \sum_{A_1, \dots, A_r \in \mathcal{A}} P(A_1 \cap \dots \cap A_r) - P(A_1) \dots P(A_r), \qquad r \ge 2,$$

and

$$\mu(n) = \mathbf{E}(R'_n) = \sum_{A\in\mathcal{A}} P(A) = \sum_{\mathbf{k},\mathbf{h}} \mathbf{E}(\theta_{\mathbf{k},\mathbf{h}});$$

namely, we have

$$|P_{[r]} - Q_{[r]}| \le (r+1)\Delta_{r+1}(n) + \Delta_r(n) + \Delta_2(n)\frac{\mu(n)^r}{r!}. \tag{10}$$

The following lemma provides us with the main tools for ending the proof.

Lemma 1. *We have the following properties*:

(i) $\mu(n) \to \lambda(k_0, K, s)$ *as* $n \to \infty$,
(ii) $\Delta_r(n) = O_{r,s}(1/n^{1/s})$ *for* $r \ge 2$.

P r o o f. We have

$$\mu(n) = \sum_{\mathbf{k}\in\mathcal{C}(k_0)} \sum_{\mathbf{h}\in\mathcal{H}(N_{\mathbf{k}})} \alpha_{h_1}\alpha_{h_2}\dots\alpha_{h_s}$$
$$= \frac{1}{K^{s-1}} \sum_{\mathbf{k}\in\mathcal{C}(k_0)} \sum_{\substack{1\le h_1<\dots<h_s\le N_{\mathbf{k}}\\ h_1+\dots+h_s=N_{\mathbf{k}}}} \frac{1}{s^s(h_1\dots h_s)^{1-1/s}}.$$

But, when n tends to infinity (always staying in the class k_0 modulo K), all the integers $N_{\mathbf{k}}$ tend to infinity. It easily follows from Lemma 3 of [10] that $\mu(n)$ tends to $\gamma\varrho(k_0,K)/K^{s-1}$, which proves (i).

We now consider the case $r=2$. In $\Delta_2(n)$ we may restrict our attention to pairs $\{A_1,A_2\}$ where A_1,A_2 are dependent and neglect the terms $P(A_1)P(A_2)$. We have

$$\Delta_2(n) = \sum_{A_1,A_2\in\mathcal{A}} P(A_1\cap A_2) - P(A_1)P(A_2) \le \Delta_2'(n) := \sum_{A_1\sim A_2} P(A_1\cap A_2),$$

where $A_1\sim A_2$ means that A_1 and A_2 are dependent. The method of the proof of Lemma 5 in [10] leads to $\Delta_2'(n) \ll_{r,s} 1/n^{1/s}$. We further get, by the correlation inequality of [10] $\Delta_r(n) \ll_{r,s} \Delta_2'(n)$, which is (ii).

We go back to the proof of Theorem 1. We now have

$$P_{[r]} = Q_{[r]} + O_{r,s}\left(\frac{1}{n^{1/s}}\right). \tag{11}$$

Estimating $Q_{[r]}$ as in [10] leads to

$$Q_{[r]} = e^{-\lambda(k_0,K,s)}\frac{(\lambda(k_0,K,s))^r}{r!} + O_{r,s}\left(\frac{1}{n^{1-1/s}}\right).$$

We then have

$$\lim_{n\to\infty} P_{[r]} = e^{-\lambda(k_0,K,s)}\frac{(\lambda(k_0,K,s))^r}{r!},$$

which proves Theorem 1.

2.2. *Density of integers with r representations.* In this section, we are concerned with the density of the sets

$$S_r := \{n\in\mathbb{N} : R_n = r\}, \qquad r\ge 0.$$

As in [10], we prove the following result.

Theorem 2. *Almost surely, the set S_r has density*

$$\delta_r(K) := \frac{1}{K}\sum_{k \bmod K} \frac{(\lambda(k,K,s))^r}{r!}e^{-\lambda(k,K,s)}. \tag{12}$$

P r o o f. As in the proof of Theorem 1, we shall in fact establish the result for the random variables R_n' and simply notice that the method leads

to the same result for R''_n. This leads to Theorem 2 since the inequalities (8) imply that

$$\{n \in \mathbb{N} : R''_n \le r\} \subset \{n \in \mathbb{N} : R_n \le r\} \subset \{n \in \mathbb{N} : R'_n \le r\}.$$

Now assume that we have proved that almost surely the density of the two sets $\{n \in \mathbb{N} : R'_n \le r\}$ and $\{n \in \mathbb{N} : R''_n \le r\}$ is equal to $\sum_{j=0}^{r} \delta_j(K)$. It is clear that almost surely the set $\{n \in \mathbb{N} : R_n \le r\}$ has the same density and by subtracting, the result of Theorem 2 follows.

Let us return to the random variables R'_n. For each integer $r \ge 0$, we first introduce the Bernoulli random variables $\varepsilon_r(n)$ which take the value 1 if $R'_n = r$ and 0 otherwise, then the random variables

$$\zeta_r(N) := \frac{1}{N} \sum_{n=1}^{N} \varepsilon_r(n).$$

In what follows, we prove that the sequence $(\zeta_r(N))$ of random variables almost surely converges towards $\delta_r(K)$.

We have

$$\mathbf{E}(\zeta_r(N)) = \frac{1}{N} \sum_{n=1}^{N} \mathbf{E}(\varepsilon_r(n)).$$

Since we have, for each k modulo K,

$$\lim_{\substack{n\to\infty \\ n\equiv k \bmod K}} \mathbf{E}(\varepsilon_r(n)) = \frac{(\lambda(k,K,s))^r}{r!} e^{-\lambda(k,K,s)},$$

we easily get

$$\lim_{N\to\infty} \mathbf{E}(\zeta_r(N)) = \frac{1}{K} \sum_{k \bmod K} e^{-\lambda(k,K,s)} \frac{(\lambda(k,K,s))^r}{r!}. \tag{13}$$

Following the method in [10], we prove that $\mathbf{D}(\zeta_r(N)) = O(N^{-1/s})$ and by Lemma 2 of [10], we deduce the announced result for the almost sure density of the set $\{n \in \mathbb{N} : R'_n \le r\}$. This ends the proof of Theorem 2.

The special case $r = 0$ of Theorem 2 leads to

Corollary. *The set of integers which can be represented as a sum of s pseudo sth powers has almost surely a density, namely*

$$1 - \delta_0(K) = 1 - \frac{1}{K} \sum_{k \bmod K} e^{-\lambda(k,K,s)}.$$

3. Behaviour of the model when the modulus K tends to infinity. Up to now, we have been working with a fixed modulus K; in order to take into account all the congruences, we shall let K tend "multiplicatively"

to infinity. For that purpose we consider the sequence $(K_B)_{B\geq 0}$ defined by

$$K_B = \prod_{p^\alpha \leq B} p^\alpha,$$

and let B tend to infinity.

THEOREM 3. *When B tends to infinity, the quantity $\delta_0(K_B)$ tends increasingly towards a limit, denoted by δ_0, which for $s \geq 3$ satisfies*

$$0 < \delta_0 < 1. \tag{14}$$

Proof. Let us first prove that $\delta_0(K_B)$ is an increasing function of B. Let indeed K and $q \geq 1$ be given. By the Chinese Remainder Theorem, and the convexity of $x \mapsto e^{-\lambda x}$, we have

$$\begin{aligned}
\delta_0(Kq) &= \frac{1}{Kq} \sum_{k' \bmod Kq} \exp\left(-\gamma \frac{\varrho(k', Kq)}{(Kq)^{s-1}}\right) \\
&= \frac{1}{K} \sum_{k \bmod K} \sum_{l=0}^{q-1} \frac{1}{q} \exp\left(-\gamma \frac{\varrho(k+lK, Kq)}{(Kq)^{s-1}}\right) \\
&\geq \frac{1}{K} \sum_{k \bmod K} \exp\left(-\gamma \sum_{l=0}^{q-1} \frac{1}{q} \cdot \frac{\varrho(k+lK, Kq)}{(Kq)^{s-1}}\right) \\
&= \frac{1}{K} \sum_{k \bmod K} \exp\left(-\gamma \frac{1}{K^{s-1}q^s} \sum_{l=0}^{q-1} \varrho(k+lK, Kq)\right) \\
&= \frac{1}{K} \sum_{k \bmod K} \exp\left(-\gamma \frac{\varrho(k, K)}{K^{s-1}}\right) = \delta_0(K).
\end{aligned}$$

Furthermore, we always have $e^{-\gamma} = \delta_0(1) \leq \delta_0(K_B) \leq 1$, which proves the existence of the limit δ_0, $0 < \delta_0 \leq 1$.

We prove in the following that the limit δ_0 is strictly smaller than 1 for $s \geq 3$.

Our first step is to study the local behaviour of sums of s integral sth powers. It will be convenient to introduce a notation for the normalized value of $\varrho(k, K)$, namely $\mathfrak{s}(k, K) = \varrho(k, K)/K^{s-1}$. Our aim is to get convenient lower bounds for $\mathfrak{s}(k, K)$. In a second step, we prove Theorem 3 for $s \geq 5$. The cases of cubes and biquadrates require a different approach, and will be studied in a last step.

3.1. *Local behaviour of sums of s integral sth powers.* Let $s \geq 2$. The function $\mathfrak{s}(k, q)$ is multiplicative as a function of q. By the orthogonality relation $q^{-1} \sum_{r=1}^{q} e(hr/q) = 1$ or 0 depending on the divisibility of h by q,

we deduce the relation

$$\mathfrak{s}(k,q) = \sum_{d|q} S_k(d) = \prod_{p|q} \sum_{p^m|q} S_k(p^m), \tag{15}$$

where

$$S_k(q) = \sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-s} S(q,a)^s e(-ak/q), \tag{16}$$

and

$$S(q,a) = \sum_{x=1}^{q} e(ax^s/q). \tag{17}$$

We denote by $c_n(k)$ the Ramanujan sum, which satisfies (cf. [7])

$$\begin{aligned} c_n(k) &= \sum_{\substack{m=1\\(m,n)=1}}^{n} e(-mk/n) \\ &= \mu\Big(\frac{n}{(k,n)}\Big)\frac{\varphi(n)}{\varphi(n/(k,n))}, \end{aligned} \tag{18}$$

where μ and φ respectively denote the Möbius and the Euler function.

We recall two classical lemmas (see Lemmas 4.3 and 4.4 of [11]) concerning the Gauß sums defined in (17).

LEMMA 2. *Let A be the set of non-principal characters modulo p of order $d = (s, p-1)$. For $(a,p) = 1$, we have*

$$S(p,a) = \sum_{\chi\in A} \overline{\chi}(a)\tau(\chi), \tag{19}$$

where $\tau(\chi) = \sum_{x=1}^{p-1} \chi(x)e(x/p)$ has modulus $\sqrt{p}$.

For any integer $s \geq 2$ and any prime p, we denote by τ the exponent of p in s, and we define

$$t(s,p) = \begin{cases} \tau+1 & \text{if } p>2 \text{ or } p=2 \text{ and } (2,s)=1, \\ \tau+2 & \text{if } p=2 \text{ and } 2\,|\,s. \end{cases}$$

LEMMA 3. *Let $(a,p) = 1$. For any integer $l \geq t(s,p)+1$, we have*

$$S(p^l,a) = \begin{cases} p^{l-1} & \text{if } l \leq s, \\ p^{s-1}S(p^{l-s},a) & \text{if } l > s. \end{cases} \tag{20}$$

These results lead to the following lemma:

LEMMA 4. *Let p and s be coprime. Let $l = us + v$, with $1 \le v \le s$.*

(i) *For $v \ge 2$, we have*

$$S_k(p^l) = \begin{cases} 0 & \text{if } p^{l-1} \nmid k, \\ -\dfrac{1}{p^{s+1-v}} & \text{if } p^{l-1} \parallel k, \\ \dfrac{p-1}{p^{s+1-v}} & \text{if } p^l \mid k. \end{cases} \tag{21}$$

(ii) *For $v = 1$, we have*

$$|S_k(p^l)| \le \begin{cases} 0 & \text{if } p^{l-1} \nmid k, \\ \dfrac{(d-1)^s}{p^{(s-1)/2}} & \text{if } p^{l-1} \parallel k, \\ \dfrac{(d-1)^s}{p^{s/2-1}} & \text{if } p^l \mid k, \end{cases} \tag{22}$$

where $d = (p-1, s)$.

P r o o f. We adapt the proof of Lemma 4.7 of [11] to our needs. From (20), we get

$$S_k(p^l) = p^{-us} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^l} (p^{-v} S(p^v, a))^s e(-ak/p^l).$$

We then write each a as $a = bp^v + c$ with $1 \le b \le p^{l-v}$, $1 \le c \le p^v$ and $(p, c) = 1$. The sum over b is equal to p^{l-v} or 0 according as p^{l-v} divides k or not. In the first case, we write $k = hp^{l-v}$. For $v > 1$, we get $S(p^v, c) = p^{v-1}$ from (20), whence

$$S_{p^{l-v}h}(p^l) = p^{-s} \sum_{\substack{c=1 \\ (c,p)=1}}^{p^v} e(-ch/p^v),$$

which involves the Ramanujan sum $c_{p^v}(k)$. Relations (21) simply come from (18). For $v = 1$, we use Lemma 2 to write

$$S_{p^{l-1}h}(p^l) = p^{-s} \sum_{\chi_1 \in A} \cdots \sum_{\chi_s \in A} \tau(\chi_1) \dots \tau(\chi_s) \sum_{c=1}^{p-1} \overline{\chi_1 \dots \chi_s(c)} e(-ch/p).$$

When $p \mid h$ (i.e. when $p^l \mid k$), the sum over c is equal to $p-1$ or 0 according to whether $\chi_1 \dots \chi_s$ is principal or not. And when $(p, h) = 1$, its value is -1 if $\chi_1 \dots \chi_s$ is principal and $\chi_1 \dots \chi_s(h)\overline{\tau(\chi_1 \dots \chi_s)}$ otherwise. We now use the fact that $|\tau(\chi)| = \sqrt{p}$ to conclude the proof of Lemma 4.

When p is large, we use the above estimates to get lower bounds for the quantity $\mathfrak{s}(k, p^\alpha)$ of direct interest to us. It leads to

LEMMA 5. *For $s \geq 5$, we have*

$$\mathfrak{s}(k, p^\alpha) \geq 1 - s^s/p^{s/2-1}. \tag{23}$$

P r o o f. Since (23) is trivial for $p \leq s$, we restrict our attention to the case when $(p, s) = 1$.

Assume first that p and k are coprime. Then (21) and (22) show that $\mathfrak{s}(k, p^\alpha) = 1 + S_k(p)$ for any $\alpha \geq 1$. Using (22) again and the trivial inequality $(p-1, s) \leq s$, we deduce the results.

Now suppose that p divides k, and let us write $k = p^m h$ with $m \geq 1$ and $(p, h) = 1$, $\alpha = us + v$, $m = ws + z$ where $u, w \geq 0$ and $1 \leq v, z \leq s$. We can write

$$\mathfrak{s}(k, p^\alpha) = \begin{cases} 1 + \displaystyle\sum_{\beta=0}^{w-1} \sum_{l=1}^{s} S_k(p^{\beta s+l}) + \sum_{l=1}^{z} S_k(p^{ws+l}) + S_k(p^{m+1}) & \text{if } m < \alpha, \\ 1 + \displaystyle\sum_{\beta=0}^{u-1} \sum_{l=1}^{s} S_k(p^{\beta s+l}) + \sum_{l=1}^{v} S_k(p^{us+l}) & \text{if } m \geq \alpha. \end{cases}$$

Using (21) and (22), we obtain $|S_k(p^{\beta s+1})| \leq (s-1)^s/p^{s/2-1}$ when $\beta s + 1 \leq m$, and $|S_k(p^{\beta s+l})| = (p-1)/p^{s+1-l}$ for $2 \leq l \leq s$ and $\beta s + l \leq m$. Thus we deduce for $0 \leq \beta < \min(u, w)$ that

$$\sum_{l=1}^{s} S_k(p^{\beta s+l}) \geq D_{p,s},$$

where $D_{p,s} = 1 - (s-1)^s/p^{s/2-1} - 1/p^{s-1}$. Then

$$\mathfrak{s}(k, p^\alpha) \geq \begin{cases} 1 + wD_{p,s} + \left(-\dfrac{(s-1)^s}{p^{s/2-1}} - \dfrac{1}{p^{s-1}} \right) & \text{if } m < \alpha \text{ and } z \leq s-1, \\ 1 + (w+1)D_{p,s} - \dfrac{(s-1)^s}{p^{(s-1)/2}} & \text{if } m < \alpha \text{ and } z = s, \\ 1 + uD_{p,s} + \left(-\dfrac{(s-1)^s}{p^{s/2-1}} - \dfrac{1}{p^{s-1}} + \dfrac{1}{p^{s-v}} \right) & \text{if } m \geq \alpha. \end{cases}$$

This gives

$$\mathfrak{s}(k, p^\alpha) \geq 1 - \frac{(s-1)^s + 1}{p^{s/2-1}} \geq 1 - \frac{s^s}{p^{s/2-1}}, \tag{24}$$

whenever $D_{p,s} \geq 0$. This condition is fulfilled for any prime p such that

$$p^{s/2-1} \geq s^s. \tag{25}$$

When inequality (25) is not satisfied, relation (23) is trivial. That finishes the proof of the lemma.

When p is small, we prove a lower bound for $\mathfrak{s}(k,p^\alpha)$ for some classes of integers k. For this purpose, we directly study the congruences

$$x_1^s + x_2^s + \ldots + x_s^s \equiv k \pmod{p^\alpha}, \qquad 1 \le x_i \le p^\alpha. \tag{26}$$

We have the following result:

LEMMA 6. *Let $t = t(s,p)$ and assume that congruence* (26) *has a non-trivial solution for $\alpha = t$. Then, for any $\nu \ge 1$,*

$$\mathfrak{s}(k,p^\nu) \ge p^{-t(s-1)}. \tag{27}$$

Proof. When $\nu \le t$, this clearly gives $\varrho(k,p^\nu) \ge 1$ and (27) follows. In the case when $\nu > t$, we apply Lemma 2.13 of [11] and deduce that

$$\varrho(k,p^\nu) \ge p^{(\nu-t)(s-1)}.$$

This ends the proof of the lemma.

3.2. *Sums of s pseudo sth powers* ($s \ge 5$). Let $s \ge 5$, and $\gamma = \gamma_s$ the gamma factor introduced in Theorem 1. We give a non-trivial upper bound, uniform in K, for the quantity

$$\delta_0(K) = \frac{1}{K}\sum_{k=1}^{K} \exp(-\gamma \mathfrak{s}(k,K)), \tag{28}$$

introduced in Theorem 2.

The constants C_n that appear below are positive and do not depend on k nor K.

We define the following subset:

$$\mathbf{E}_K = \{k \bmod K : p \le s^4 \Rightarrow k \equiv 1 \pmod{p^{t(s,p)}}\}.$$

We then have $|\mathbf{E}_K| \ge C_1 K$, when K is large enough. Let indeed $P_1 = \prod_{p \le s^4} p^{t(s,p)}$; we have

$$|\mathbf{E}_K| = \sum_{\substack{k \bmod K \\ k \equiv 1 \,(\mathrm{mod}\, P_1)}} 1 = (1+o(1))K/P_1 \quad \text{as } K \to \infty.$$

On the other hand, from (23) we get

$$\mathfrak{s}(k,K) \ge \prod_{\substack{p \mid K \\ p > s^4}} \left(1 - \frac{s^s}{p^{s/2-1}}\right) \prod_{\substack{p^\alpha \| K \\ p \le s^4}} \mathfrak{s}(k,p^\alpha).$$

For k in $\mathbf{E}_K$, congruence (26) has a non-trivial solution when $\alpha = t(s,p)$ for any prime $p \le s^4$, namely $k \equiv 1^s + (s-1)\cdot 0^s \pmod{p^{t(s,p)}}$. Thus, by Lemma 6, the second product is larger than $\prod_{p \le s^4} p^{-(s-1)t(s,p)} > 0$, which depends only on s. A lower bound for the first product is obtained by suppressing the conditions on K. This gives a positive convergent Eulerian

product, the value of which is independent of K. We thus have $\mathfrak{s}(k,K) \geq C_2$, which leads for K large enough to

$$\delta_0(K) \leq \frac{|\mathbf{E}_K|}{K} e^{-\gamma C_2} + \frac{K - |\mathbf{E}_K|}{K} \leq 1 - C_3 < 1. \tag{29}$$

Using again the fact that $q \,|\, K$ implies $\delta_0(q) \leq \delta_0(K)$, we deduce that (29) remains true for any integer $K \geq 1$, which proves Theorem 3 when $s \geq 5$.

3.3. *Case of cubes and biquadrates.* In the case of cubes and biquadrates, we have to follow a different approach. Although the expression we have for δ_0 is not multiplicative, it is possible to expand the exponential function into a power series and then, for fixed K, to interchange the order of the summations. We thus get

$$\begin{aligned}\delta_0(K) &= \sum_{i\geq 0} \frac{(-\gamma)^i}{i!} \cdot \frac{1}{K} \sum_{k \bmod K} \mathfrak{s}(k,K)^i \\ &= \sum_{i\geq 0} \frac{(-\gamma)^i}{i!} \mathfrak{S}_i(K) = 1 - \gamma \mathfrak{S}_1(K) + \frac{\gamma^2}{2} \mathfrak{S}_2(K) - \dots\end{aligned}$$

where $\mathfrak{S}_i(K)$ (for $i \geq 1$), is defined by

$$\mathfrak{S}_i(K) := \frac{1}{K} \sum_{k \bmod K} \mathfrak{s}(k,K)^i = \frac{1}{K} \sum_{k \bmod K} (\varrho(k,K)/K^{s-1})^i.$$

Thanks to the multiplicativity of ϱ, the function $\mathfrak{S}_i$ is multiplicative, and we further notice the following properties:

(i) For any K, we have $(1/K)\sum_{k \bmod K} \mathfrak{s}(k,K) = 1$ and thus, $\mathfrak{S}_1(K) = 1$.

(ii) The function $\mathfrak{S}_i$ is multiplicatively increasing; this simply follows from the convexity of $x \mapsto x^i$.

In particular, for any K, we have

$$\mathfrak{S}_i(K) \geq \mathfrak{S}_i(1) = 1.$$

For any $x \geq 0$, we have

$$1 - x \leq \exp(-x) \leq 1 - x + x^2/2,$$

which implies that for any K we have

$$1 - \gamma \leq \delta_0(K) \leq 1 - \gamma + \tfrac{1}{2}\gamma^2 \mathfrak{S}_2(K).$$

Our program now is to show that, when K multiplicatively tends to infinity, $\mathfrak{S}_2(K)$ tends to a value $\mathfrak{S} < 2/\gamma$. We first express $\mathfrak{S}_2(K)$ in terms of the Gauß sums $S(K,a)$ defined in (17). We have

$$(30)\qquad \sum_{a=1}^{K}|S(K,a)|^{2s} = \sum_{\substack{1\le h_1,\dots,h_s\le K\\ 1\le h'_1,\dots,h'_s\le K}}\sum_{a=1}^{K} e\Big(\frac{a(h_1^s+\dots+h_s^s-h_1'^s-\dots-h_s'^s)}{K}\Big) = K\sum_{k=1}^{K}\varrho(k,K)^2,$$

which implies that

$$\mathfrak{S}_2(K)=\sum_{a=1}^{K}\Big|\frac{S(K,a)}{K}\Big|^{2s}.$$

By writing $a=hp^{\alpha-\beta}$, where $1\le h<p^\beta$, $(h,p)=1$, in (30), and using

$$\frac{S(p^\alpha,hp^{\alpha-\beta})}{p^\alpha}=\frac{S(p^\beta,h)}{p^\beta},$$

we get

$$(31)\qquad \mathfrak{S}_2(p^\alpha)=\sum_{\beta=0}^{\alpha}\sum_{\substack{h=1\\(h,p)=1}}^{p^\beta-1}\Big|\frac{S(p^\beta,h)}{p^\beta}\Big|^{2s}=\sum_{\beta=0}^{\alpha}\Omega(p^\beta),$$

where

$$\Omega(p^\beta):=\sum_{\substack{h=1\\(h,p)=1}}^{p^\beta-1}\Big|\frac{S(p^\beta,h)}{p^\beta}\Big|^{2s};$$

we thus get, by the multiplicativity of $\mathfrak{S}_2$,

$$\mathfrak{S}_2(K)=\prod_{p^\alpha\|K}\sum_{0\le\beta\le\alpha}\Omega(p^\beta).$$

Lemma 3 and the estimate

$$S(p,a)=O(\sqrt{p})\quad\text{ for }(a,p)=1,$$

deduced from Lemma 2, lead for $s\ge 3$ to $\Omega(p)=O(1/p^2)$ and $\Omega(p^\beta)=O(1/p^\beta)$ for $\beta\ge 2$.

This implies that $\mathfrak{S}_2(K)$ has a limit, let us call it $\mathfrak{S}$, as K multiplicatively tends to infinity. We have

$$(32)\qquad \mathfrak{S}=\sum_{K=1}^{\infty}\sum_{\substack{k \bmod K\\(k,K)=1}}\Big|\frac{S(K,k)}{K}\Big|^{2s}=\sum_{K=1}^{\infty}\Omega(K) = \prod_{p}\Big(\sum_{\beta=0}^{\infty}\Omega(p^\beta)\Big)=\prod_{p}X(p).$$

We indeed recognize in $\mathfrak{S}$ the singular series considered by Hooley in [8]. Using the inequalities obtained by Hooley for the case of cubes and biquadrates (up to corrections of minor computational inaccuracies)

$$3.09 < \mathfrak{S} < 3.55 \text{ (for cubes)} \quad \text{and} \quad 10.5 < \mathfrak{S} < 12.7 \text{ (for biquadrates)},$$

and the value $1/\gamma(3) = 8.42\ldots$ for cubes and $1/\gamma(4) = 35.55\ldots$ for biquadrates, we get $\delta_0 < 0.91$ for cubes and $\delta_0 < 0.98$ for biquadrates, which ends the proof of Theorem 3.

REMARK. The relation $\sum_{r=0}^{\infty} \delta_r(K) = 1$ implies that the $\delta_r(K)$ cannot all be increasing. It is however possible to show that the sequence $\delta_r(K_B)$ has a limit as B tends to infinity.

Let us consider the function f defined over $\mathbb{R}_+$ by $f(x) := (x^r/r!)e^{-x}$ and let $K, q \geq 1$ be two integers; we have

$$\delta_r(Kq) - \delta_r(K) = \frac{1}{K} \sum_{k \bmod K} \frac{1}{q} \sum_{l \bmod q} f(\gamma\mathfrak{s}(k + lK, Kq)) - f(\gamma\mathfrak{s}(k, K)).$$

We use the Taylor identity

$$f(y) - f(x) = f'(x)(y - x) + \tfrac{1}{2} f''(\theta)(y - x)^2,$$

for some $\theta \in [x, y]$. We have

$$\begin{aligned}
&\delta_r(Kq) - \delta_r(K) \\
&\quad = \frac{1}{K} \sum_{k \bmod K} f'(\gamma\mathfrak{s}(k, K)) \frac{1}{q} \sum_{l \bmod q} \gamma(\mathfrak{s}(k + lK, Kq) - \mathfrak{s}(k, K)) \\
&\qquad + \frac{1}{2K} \sum_{k \bmod K} \frac{1}{q} \sum_{l \bmod q} \gamma^2 f''(\theta_{k,l})(\mathfrak{s}(k + lK, Kq) - \mathfrak{s}(k, K))^2.
\end{aligned}$$

The first sum is clearly zero and we note that the function f'' is bounded over $\mathbb{R}_+$, thus we have, for some convenient constant C depending only on r,

$$\begin{aligned}
&|\delta_r(Kq) - \delta_r(K)| \\
&\quad \leq C \frac{\gamma^2}{2} \cdot \frac{1}{K} \sum_{k \bmod K} \frac{1}{q} \sum_{l \bmod q} (\mathfrak{s}(k + lK, Kq) - \mathfrak{s}(k, K))^2 \\
&\quad \leq C \frac{\gamma^2}{2} \left(\mathfrak{S}_2(Kq) + \mathfrak{S}_2(K) - \frac{2}{K} \sum_{k \bmod K} \mathfrak{s}(k, K) \frac{1}{q} \sum_{l \bmod q} \mathfrak{s}(k + lK, Kq) \right) \\
&\quad = C \frac{\gamma^2}{2} (\mathfrak{S}_2(Kq) - \mathfrak{S}_2(K)).
\end{aligned}$$

We have proved below that the function $\mathfrak{S}_2(K_B)$ has a limit as B tends multiplicatively to infinity, thus the same result holds for the sequence $\delta_r(K_B)$.

4. Density of sums of two pseudo-squares

4.1. *Statement of the result.* We show that our model gives sums of two pseudo-squares a density that tends to zero as K multiplicativity tends to infinity in such a way that any integer divides K from some point onward. More precisely, we have the following

THEOREM 4. *When B tends to infinity, we have*

$$\frac{1}{\sqrt{\log B}} \ll 1 - \delta_0(K_B) \ll \frac{\sqrt{\log\log B}}{\sqrt{\log B}},$$

where $K_B = \prod_{p^\alpha \le B} p^\alpha$.

4.2. *Local behaviour of sums of two squares.* For $s = 2$ and $q = p^\alpha$, relation (15) becomes

$$\mathfrak{s}(k, p^\alpha) = \sum_{m=0}^{\alpha} \frac{1}{p^{2m}} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^m} S(p^m, a)^2 e(-ak/p^m).$$

Quadratic Gauß sums are well known (cf. [1]); we have

$$S(q,a) = \begin{cases} \sqrt{q} & \text{if } q \equiv 1 \pmod 4, \\ i\sqrt{q} & \text{if } q \equiv 3 \pmod 4, \\ 0 & \text{if } q \equiv 2 \pmod 4, \\ (1+i)\sqrt{q} & \text{if } q \equiv 0 \pmod 4, \end{cases} \tag{33}$$

and we summarize in the following lemma easy consequences of these relations.

LEMMA 7. *If $p \equiv 1 \pmod 4$ then*

$$\begin{aligned} \mathfrak{s}(k, p^\alpha) &= \sum_{h=0}^{\alpha} \frac{c_{p^h}(k)}{p^h} \\ &= \begin{cases} (\beta+1)(1-1/p) & \text{if } p^\beta \parallel k \text{ and } \beta \le \alpha - 1, \\ 1 + \alpha(1-1/p) & \text{if } p^\alpha \mid k. \end{cases} \end{aligned} \tag{34}$$

If $p \equiv 3 \pmod 4$ then

$$\begin{aligned} \mathfrak{s}(k, p^\alpha) &= \sum_{h=0}^{\alpha} (-1)^h \frac{c_{p^h}(k)}{p^h} \\ &= \begin{cases} 1 + 1/p & \text{if } p^\beta \parallel k \text{ and } \beta \text{ even} \le \alpha - 1, \\ 0 & \text{if } p^\beta \parallel k \text{ and } \beta \text{ odd} \le \alpha - 1, \\ 1 & \text{if } p^\alpha \mid k \text{ and } \alpha \text{ even}, \\ 1/p & \text{if } p^\alpha \mid k \text{ and } \alpha \text{ odd}. \end{cases} \end{aligned} \tag{35}$$

For $p = 2$, we have

$$\mathfrak{s}(k, 2^\alpha) = \begin{cases} 1 & \text{if } \alpha \le 1 \text{ or } (\alpha \ge 2 \text{ and } 2^{\alpha-1} \mid k), \\ 1 + (-1)^{(d-1)/2} & \text{if } 0 \le \gamma \le \alpha - 2,\ k = d2^\gamma \text{ and } (d, 2) = 1. \end{cases} \tag{36}$$

4.3. *A lower bound for $\delta_0(K_B)$.* Our aim is to show that $\delta_0(K_B) = 1 + o(1)$; thanks to the trivial upper bound, it is enough to obtain a lower bound of this type.

Let $Q_B^{(1)}$ (resp. $Q_B^{(3)}$) denote the product of the prime numbers at most equal to B and congruent to 1 (resp. 3) modulo 4, and let

$$Q_B = \prod_{p \le B} p = 2Q_B^{(1)} Q_B^{(3)}.$$

We further denote by $n_1(k)$ (resp. $p_3(k)$) the number (resp. the product) of those prime factors of an integer k which are congruent to 1 (resp. 3) modulo 4, i.e.

$$n_1(k) = \sum_{\substack{p \equiv 1 \,(\mathrm{mod}\, 4) \\ p \mid k}} 1, \qquad p_3(k) = \prod_{\substack{p \equiv 3 \,(\mathrm{mod}\, 4) \\ p \mid k}} p.$$

Let $\tau = 1 + (e \log 2)/2$ and

$$\mathbf{E}_B = \{k \text{ modulo } Q_B : p_3(k) > (\log B)^\tau \text{ and } n_1(k) < (e \log_2 B)/2\}. \tag{37}$$

We first recall some classical results concerning primes in arithmetic progressions:

LEMMA 8. *For $i \in \{1, 3\}$ and B tending to infinity, we have*

$$\sum_{\substack{p \equiv i \,(\mathrm{mod}\, 4) \\ p \le B}} \frac{1}{p-1} = \frac{1}{2} \log\log B + O(1), \tag{38}$$

$$\prod_{\substack{p \equiv i \,(\mathrm{mod}\, 4) \\ p \le B}} \left(1 - \frac{1}{p}\right) = \frac{c(i)}{\sqrt{\log B}}(1 + o(1)) \quad \text{for some } c(i) > 0. \tag{39}$$

The first result is deduced from the Mertens formula on primes in arithmetic progressions, namely for a and q coprime,

$$\sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{1}{p} = \frac{1}{\phi(q)} \log\log x + O(1)$$

(see [3], p. 57). The second result directly follows from this by taking the logarithm.

Since Q_B is squarefree, we deduce from (34) that $\mathfrak{s}(k, Q_B^{(1)})$ is not larger than $2^{n_1(k)}$. By (35), we get $\mathfrak{s}(k, p_3(k)) = 1/p_3(k)$; if $(p, k) = 1$ and $p \equiv 3$

(mod 4) then $\mathfrak{s}(k,p) = 1 + 1/p$. Hence, if $k \in \mathbf{E}_B$ we have

$$\mathfrak{s}(k,Q_B) = \mathfrak{s}(k,Q_B^{(1)})\mathfrak{s}(k,Q_B^{(3)})\mathfrak{s}(k,2)$$
$$\leq \frac{2^{n_1(k)}}{p_3(k)} \prod_{\substack{p\equiv 3 \,(\mathrm{mod}\, 4)\\ p\leq B\\ (p,k)=1}} \left(1+\frac{1}{p}\right) \leq (\log B)^{-1} \prod_{\substack{p\equiv 3 \,(\mathrm{mod}\, 4)\\ p\leq B}} \left(1+\frac{1}{p}\right).$$

This, combined with (39), gives for every sufficiently large B and every k in $\mathbf{E}_B$,

$$\mathfrak{s}(k,Q_B) \leq \frac{C_7}{\sqrt{\log B}}. \tag{40}$$

We shall show that $\mathbf{E}_B$ contains almost all integers modulo Q_B. We define $\mathbf{F}_B$ as the complementary set of $\mathbf{E}_B$ in the set of classes modulo Q_B, and we write $\mathbf{F}_B$ as the union of the two subsets

$$\mathbf{F}'_B = \{k \bmod Q_B : p_3(k) \leq (\log B)^\tau\},$$
$$\mathbf{F}''_B = \{k \bmod Q_B : n_1(k) \geq (e \log\log B)/2\}.$$

We begin by giving an upper bound for the cardinality of the set $A_h(q,q')$, where $(q,q') = 1$ and q is squarefree, of integers k in $[1,qq']$ such that (q,k) is the product of exactly h distinct prime factors of q; if we write

$$F(q) = \sum_{p\mid q} \frac{1}{p-1}, \tag{41}$$

we have

$$|A_h(q,q')| \leq \varphi(q)q' \frac{F^h(q)}{h!}. \tag{42}$$

(This is readily seen by writing

$$|A_h(q,q')| = \sum_{1\leq j_1<\ldots<j_h\leq t} |\{1 \leq k \leq qq' : p \,|\, (k,q) \Leftrightarrow p \in \{p_{j_r}\}_{1\leq r\leq h}\}|$$
$$= \varphi(q)q' \sum_{1\leq j_1<\ldots<j_h\leq t} \Big(\prod_{r=1}^{h} \frac{1}{\varphi(p_{j_r})}\Big),$$

where $p_1 < \ldots < p_t$ denote the distinct prime factors of q.) Relation (42) and the inequality (cf. [6], p. 149)

$$\sum_{x\geq X} \frac{Y^x}{x!} \leq (eY/X)^X, \quad \text{valid for } 0 < Y \leq X,$$

imply

$$|\mathbf{F}''_B|/Q_B = \frac{1}{Q_B^{(1)}} \sum_{h \ge (e\log\log B)/2} |A_h(Q_B^{(1)})|$$
$$\le \frac{\varphi(Q_B^{(1)})}{Q_B^{(1)}} \Big(\frac{eF(Q_B^{(1)})}{(e\log\log B)/2} \Big)^{(e\log\log B)/2},$$

then by (38) and (39),

$$|\mathbf{F}''_B|/Q_B \le \frac{C_8}{\sqrt{\log B}}. \tag{43}$$

On the other hand, $|\mathbf{F}'_B|$ does not exceed the number of integers k mod Q_B coprime to $P_B = \prod_{(\log B)^\tau < p \le B,\, p \equiv 3 \,(\mathrm{mod}\, 4)} p$. This leads to

$$|\mathbf{F}'_B| \le \sum_{\substack{k=1 \\ (k,P_B)=1}}^{Q_B} 1 = Q_B \sum_{d \mid P_B} \frac{\mu(d)}{d} = Q_B \prod_{p \mid P_B} \Big(1 - \frac{1}{p}\Big),$$

and relation (39) implies

$$|\mathbf{F}'_B|/Q_B \le C_9 \frac{\sqrt{\log\log B}}{\sqrt{\log B}}. \tag{44}$$

From relations (40), (43) and (44) we get

$$\delta_0(Q_B) \ge Q_B^{-1} \sum_{k \in \mathbf{E}_B} \exp(-\gamma \mathfrak{s}(k, Q_B))$$
$$\ge (1 - C_{10}\sqrt{\log\log B/\log B}) \exp(-\gamma C_7/\sqrt{\log B})$$
$$\ge 1 - C_{11}\sqrt{\log\log B/\log B}.$$

Since Q_B divides K_B, we have $\delta_0(Q_B) \le \delta_0(K_B)$, whence

$$1 - \delta_0(K_B) \le C_{11}\sqrt{\log\log B/\log B}. \tag{45}$$

This is the upper bound in Theorem 4.

4.4. *An upper bound for* $\delta_0(K_B)$. Let us write $K_B = K_B^{(1)} K_B^{(2)} K_B^{(3)}$ where the prime factors of $K_B^{(1)}$ (resp. $K_B^{(3)}$) are congruent to 1 (resp. 3) modulo 4 and $K_B^{(2)} = 2^{[\log B/\log 2]}$, and let us denote by $\mathbf{H}_B$ the set of the classes modulo K_B which are coprimes with $K_B^{(3)}$ and congruent to 1 modulo 4. For $B \ge 4$ we have

$$|\mathbf{H}_B| = \frac{K_B}{4} \cdot \frac{\varphi(K_B^{(3)})}{K_B^{(3)}} \ge C_{12} \frac{K_B}{\sqrt{\log B}}. \tag{46}$$

Let k be in $\mathbf{H}_B$; by Lemma 7, we have

$$\begin{aligned}\mathfrak{s}(k,K_B) &= \mathfrak{s}(k,K_B^{(2)})\mathfrak{s}(k,K_B^{(1)})\mathfrak{s}(k,K_B^{(3)})\\ &\geq \prod_{\substack{p\equiv 1 \pmod 4\\ p\leq B}}\left(1-\frac{1}{p}\right)\prod_{\substack{p\equiv 3 \pmod 4\\ p\leq B}}\left(1+\frac{1}{p}\right),\end{aligned}$$

and by (39), we deduce $\mathfrak{s}(k,K_B)\geq C_{13}$. Then

$$\delta_0(K_B)\leq \frac{|\mathbf{H}_B|}{K_B}\exp(-\gamma C_{13})+\frac{K_B-|\mathbf{H}_B|}{K_B}\leq 1-\frac{C_{14}}{\sqrt{\log B}}.$$

This gives the lower bound in Theorem 4.

5. Around Hooley's conjecture. In [8], C. Hooley studies the expression

$$M(x):=\sum_{n\leq x} r^2(n),$$

for $s\geq 3$, where $r(n)$ denotes the number of representations of the integer n as a sum of s integral sth powers, and gives the following conjecture.

Conjecture (Hooley). *As x tends to infinity, we have*

$$M(x)\sim (A_s^2\mathfrak{S}+s!A_s)x,$$

where $A_s=\Gamma(1+1/s)^s$ and $\mathfrak{S}$ denotes the singular series that occurs in (32).

This conjecture can be reformulated in terms of the number $r'(n)$ of representations of n as

$$n=n_1^s+\ldots+n_s^s \quad \text{with } n_1<\ldots<n_s,$$

which corresponds to our random variable R_n defined in (9). With $\gamma=A_s/s!$, Hooley's conjecture becomes

$$\sum_{n\leq x}(r'(n))^2\sim(\gamma^2\mathfrak{S}+\gamma)x \quad \text{as } x \text{ tends to infinity.}$$

It is interesting to check the behaviour of our model. We define the random variables $\Phi_N(K)$ by

$$\Phi_N(K)=\frac{1}{N}\sum_{n=1}^{N}R_n^2(K),$$

where $R_n(K)$ denotes the number of representations of n as a sum of s pseudo sth powers with the model corresponding to modulus K. The method of the third named author (cf. [10]) that we already used in the proof of Theorem 2 leads to the following

Proposition. *The sequence $(\Phi_N(K))$ of random variables almost surely converges to $\gamma^2\mathfrak{S}_2(K)+\gamma$.*

It is satisfactory to notice that as K multiplicatively tends to infinity, $\mathfrak{S}_2(K)$ tends to $\mathfrak{S}$.

References

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Amer. Math. Soc., Providence, 1963.

[2] P. Barrucand, *Sur la distribution empirique des sommes de trois cubes ou de quatre bicarrés*, C. R. Acad. Sci. Paris A 267 (1968), 409–411.

[3] H. Davenport, *Multiplicative Number Theory*, Markham, 1967.

[4] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), 83–110.

[5] J. H. Goguel, *Über Summen von zufälligen Folgen natürlichen Zahlen*, J. Reine Angew. Math. 278/279 (1975), 63–77.

[6] H. Halberstam and R. F. Roth, *Sequences*, Clarendon Press, Oxford, 1966.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, 1985.

[8] C. Hooley, *On some topics connected with Waring's problem*, J. Reine Angew. Math. 369 (1986), 110–153.

[9] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. (3) 13 (1908), 305–312.

[10] B. Landreau, *Modèle probabiliste pour les sommes de s puissances s-ièmes*, Compositio Math. 99 (1995), 1–31.

[11] R. C. Vaughan, *The Hardy–Littlewood Method*, Cambridge Univ. Press, 1981.

Mathématiques Stochastiques
Université Victor Segalen Bordeaux 2
F-33076 Bordeaux Cedex, France
E-mail: J-M.Deshouillers@u-bordeaux2.fr

Laboratoire d'Algorithmique
Arithmétique Expérimentale
Unité Mixte de Recherche CNRS 9936
Université Bordeaux I
F-33405 Talence Cedex, France
E-mail: hennec@math.u-bordeaux.fr
landreau@math.u-bordeaux.fr

Received on 15.11.1996
and in revised form on 10.10.1997 (3074)