# Sums of powers, a probabilistic approach

Jean-Marc Deshouillers

*Institut Mathématique de Bordeaux*

Journée arithmétique FraZa 2017
IMB, Bordeaux, November 8th, 2017

*En memoria de Javier Cilleruelo*

1. Sums of $k$ numbers which are $s$-th powers of integers ($2 \leq s \leq k$)

2. Squares and cubes

3. The Erdős-Rényi probabilistic model
   - Random sequences
   - Pseudo $s$-th powers
   - Poisson model for sums of $s$ pseudo $s$-th powers
   - Sums of $(s+1)$ pseudo $s$-powers

4. Javier Cilleruelo's contribution
   - Gaps between consecutive sums of $s$ pseudo $s$-powers
   - Additive complements to sums of $s$ pseudo $s$-powers
   - Sums of $(s+\epsilon)$ pseudo $s$-powers
   - Two words about the proofs

5. Arithmetical model and numerical tests

## Sums of $k$ numbers which are $s$-th powers of integers $(2 \le s \le k)$

We are interested in representing a non-negative integer $n$ as the sum of $k$ numbers which are $s$-th powers of non-negative integers $x_i$,

$$n = x_1^s + x_2^s + \cdots + x_k^s; \tag{1}$$

we let

$R_{s,k}(n)$ be the total number of those representations,

$r_{s,k}(n)$ be the number of representations with $x_1^s \le x_2^s \le \cdots \le x_k^s$ and

$r'_{s,k}(n)$ the number of representations with $x_1^s < x_2^s < \cdots < x_k^s$.

$\mathcal{A}_{s,k} = \{n \colon r_{s,k}(n) > 0\} = \{n \colon R_{s,k}(n) > 0\}$

We further count the number of integers $n$ up to the real number $x$ which are sums of $k$ $s$-th powers by the *counting functions*

$A_{s,k}(x) = \operatorname{Card} \mathcal{A}_{s,k} \cap [1, x] = \operatorname{Card} \{n \le x \colon r_{s,k}(n) > 0\}$

and their densities

$\liminf_{x\to\infty} A_{s,k}(x)/x$ and $\limsup_{x\to\infty} A_{s,k}(x)/x$.

What we can prove

For $k \geq s$

- $A_{s,s}(x) \leq (1 + o(1))x/s!$.
- $R_{s,k}(n)$ has order $n^{(k-s)/s}$ on average, i.e. $\sum_{n \leq x} R_{s,k}(n) \sim C_{s,k} x^{k/s}$.

For $k$ large with respect to $s$

- $A_{s,k}(x) = x + O(1)$ (Hilbert, answering Waring).
- $R_{s,k}(n) \sim \mathfrak{S}_{s,k}(n) n^{(k-s)/s}$ (Hardy-Littlewood).

What would we like to know

- Is $\liminf A_{s,s}(x)/x > 0$? or even ¿does $\lim A_{s,s}(x)/x$ exist and is positive?
- Is $R_{s,s+1}(n) > 0$ as soon as $\mathfrak{S}_{s,s+1}(n) > 0$ and $n$ large enough?

# Squares

What we know

4 squares. Every integer is a sum of 4 squares, i.e. $A_{2,4}(x) = \lfloor x \rfloor$. Lagrange (1770).

3 squares. Every integer which is not of the shape $4^a(8b+7)$ is a sum of 3 squares. Gauß, Legendre (ca 1800).

2 squares. $A_{2,2}(x) \sim Cx/\sqrt{\log x}$, as $x \to \infty$. Landau (1909).
The representation function of an integer as a sum of two squares $(R_{2,2})$ is multiplicative and thus rather erratic, taking very large values.

Let us write $\mathcal{A}_{2,2} = \{b_1 < b_2 < \cdots < b_n < \cdots\}$. We have $b_{n+1} - b_n < b_n^{1/4}$. Folklore (¡greedy algorithm!).

What we expect

For the consecutive sums of two squares, we expect
$\forall \varepsilon > 0\colon\ b_{n+1} - b_n < b_n^{\varepsilon}$.

# Cubes

What we know.

7 cubes. Every large integer is a sum of 7 cubes, i.e. $A_{3,7} = x + O(1)$. Linnik (1942).

$R_{3,7}(n) \gg n^{4/3}$. Vaughan (1989).

Every integer larger than 454 is a sum of 7 cubes. Siksek (2016).

What we expect.

4 cubes. Is every large integer a sum of 4 cubes?

Is $7,373,170,279,850$ the largest integer $n$ for which $R_{3,4}(n) = 0$? D.-Hennecart-Landreau (2000).

3 cubes. Is $\liminf A_{3,3}(x)/x > 0$ ?

## The indicator (or characteristic) function of a subsequence of $\mathbb{N}_0$

Let $\mathcal{A}$ be a sequence of $\mathbb{N}_0$, say $\mathcal{A} = \{a_0 < a_1 < \cdots < a_n < \cdots\}$.
We can also represent it by a function $\chi_{\mathcal{A}}$ from $\mathbb{N}_0$ to $\{0, 1\}$ which associates to each integer $n$ the value 1 if and only if $n \in \mathcal{A}$. This gives a bijection between the subsequences of the integers and the sequences with values in $\{0, 1\}$.

## Random sequences

Let $\Omega$ be a probability space and $(\xi_n)_{n \geq 0}$ be a sequence of independent random variables with values in $\{0, 1\}$. To each $\omega \in \Omega$, we can associate the sequence $(\xi_n(\omega))_{n \geq 0}$. It is a sequence of 0 and 1 and we can associate to it a sequence of integers $\mathcal{A}_\omega$ such that $n \in \mathcal{A}_\omega$ if and only if $\xi_n(\omega) = 1$, or in other words

$$\chi_{\mathcal{A}_\omega}(n) = \xi_n(\omega).$$

We say that $\mathcal{A}$ is the random sequence associated to the sequence $(\xi_n)_{n \geq 0}$.

# Pseudo $s$-th powers

If one considers two consecutive $s$-th powers around $x$, their difference (thanks to Taylor) is something like
$(x^{1/s}+1)^s-(x^{1/s})^s \sim sx^{1-1/s}$.
We can thus say that, among $sx^{1-1/s}$ consecutive integers around $x$ there is generally one $s$-th power, or in other words, the heuristic probability that an integer $n$ is an $s$-th power is
$n/(sn^{1-1/s})$ which is equal to $1/sn^{1/s}$.

Using this remark, Erdős and Rényi, defined random sequence of pseudo $s$-th powers by asking the randon variables $\xi_n$ to satisfy the condition

$$\mathrm{Prob}(\xi_n) = \frac{1}{sn^{1/s}} \quad \text{for} \quad n \geq 1. \tag{2}$$

We shall denote with a tilda the quantities related to pseudo $s$-th powers, for example $\widetilde{r_{s,k}}(n), \widetilde{\mathcal{A}_{s,k}}, \widetilde{A_{s,k}}(x), \ldots$ and remember that those expressions are random variables. As such, everything is possible, e.g. $\widetilde{\mathcal{A}_{s,1}}_\omega = \emptyset$ for some $\omega \in \Omega$ or $\widetilde{\mathcal{A}_{s,1}}_\omega = \mathbb{N}$ for some (other) $\omega$, but we have

$$\text{Almost surely} : \widetilde{A_{s,1}}(x) \sim x^{1/s}, \text{ as } x \to \infty. \tag{3}$$

## Poisson model for sums of $s$ pseudo $s$-th powers

As in the real case, the number of representations can be easily handled **on average**:

$$\text{a.s.} \qquad \sum_{n \le x} \widetilde{r_{s,s}}(n) \sim \lambda_s x \quad \text{where} \quad \lambda_s = \Gamma(1/s)/\left(s^s s!\right). \tag{4}$$

Since $\widetilde{r_{s,s}}(n)$ is constant on average, it is natural to expect a Poisson distribution for its values. It is the aim of Erdős and Rényi to show

$$\text{a.s.} \qquad \forall d \ge 0 : \ \frac{1}{x} \operatorname{Card}\{n \le x : \widetilde{r_{s,s}}(n) = d\} \to e^{-\lambda_s} \frac{\lambda_s^d}{d!}. \tag{5}$$

The proof has been completed by Goguel (1975), using the method of moments.

# The model versus the reality

From the previous relation (5), we get

$$\text{a.s.} \qquad \frac{1}{x}\,\text{Card}\{n \le x\colon \widetilde{r_{s,s}}(n) \neq 0\} \to 1 - e^{-\lambda_s} \tag{6}$$

or

$$a.s. \quad \widetilde{A_{s,s}}(x) \sim (1 - e^{-\lambda_s})x, \qquad \text{as} \qquad x \to \infty,$$

which tells us that the sums of $s$ pseudo $s$-th powers have a density.
In the real life, the only case we know is that of squares, where we know that sums of two squares have a zero density...
However, we shall see in the last part that some arithmetic may be plugged into the Erdős-Rényi model, leading to a probabilistic model

- with zero density for sums of two pseudo-squares,
- with positive density for $s \ge 3$,
- that density being consistant with numerical evidence for $s = 3$ and $s = 4$.

# Sums of $(s+1)$ pseudo $s$-powers

Iosifescu and D. proved in 2000 that the pseudo $s$-th powers are *a.s.*. The main result is that there exist two positive constants $u = u(s)$ and $v = v(s)$ such that

$$a.s. \quad \exp(-vn^{1/s}) \le \mathrm{Prob}(\widetilde{R_{s,s+1}}(n) = 0) \le \exp(-un^{1/s}).$$

**Question 1**. Do we have $\mathrm{Prob}(\widetilde{R_{s,s+1}}(n) = 0) \le \exp(-wn^{1/s})$?

The fact that the pseudo $s$-th powers are a basis of order $s+1$ simply follows by Borel-Cantelli.

The largest integer which is not a sum of at most $s+1$ pseudo-$s$ powers is thus a random variable which is *a.s.* finite.

**Question 2** What is the law of the largest integer which is not a sum of at most $s+1$ pseudo-$s$ powers?

Answer to this question would confirm our belief that 7,373,170,279,850 is the largest integer which is not a sum of 4 cubes (already mentioned).

## Gaps between consecutive sums of $s$ pseudo $s$-powers

Let us write

$$\widetilde{\mathcal{A}_{s,s}} = \{b_1 < b_2 < \cdots < b_n < \cdots\}$$

**Theorem (Cilleruelo and D., 2016)**

*We have almost surely*

$$\limsup_{n\to\infty} \frac{b_{n+1} - b_n}{\log b_n} = \frac{1}{\lambda_s} = \frac{s^s s!}{\Gamma^s(1/s)}.$$

This is consistant with the fact that the density of $\widetilde{\mathcal{A}_{s,s}}$ is $1 - e^{-\lambda_s}$.

# Additive complements to sums of $s$ pseudo $s$-powers

**Theorem (Cilleruelo, Lambert, Plagne and D., 2016)**

*Let $\mathcal{C}$ be a fixed sequence of integers satisfying*

$$\liminf_{x\to\infty} \frac{C(x)}{\log x} > \lambda_s^{-1}.$$

*Then, a.s. every sufficiently large integer is a sum of $s$ pseudo $s$-th powers and an element of $\mathcal{C}$.*

*Let $\mathcal{D}$ be a fixed sequence of integers satisfying*

$$\liminf_{x\to\infty} \frac{D(x)}{\log x} < \lambda_s^{-1}.$$

*Then, a.s., there exist infinitely integers which cannot be represented as the sum of $s$ pseudo $s$-th powers and an element of $\mathcal{D}$.*

# Sums of $(s+\epsilon)$ pseudo $s$-powers

**Theorem (Cilleruelo, Lambert, Plagne and D.)**

*Let $c > (\lambda_s(1-2\lambda_s))^{-1}$. Almost surely, a sequence of pseudo $s$-th powers $\widetilde{\mathcal{A}}$ has the following property: any large enough integer $n$ can be written in the form*

$$n = a_1 + \cdots + a_{s+1}, \quad \textit{with} \quad a_i \in \widetilde{\mathcal{A}} \quad \textit{and } a_{n+1} < (c \log n)^s.$$

**Question 3**. Can one replace $c > (\lambda_s(1-2\lambda_s))^{-1}$ by $c > (\lambda_s)^{-1}$?

**Question 4**. Show that the statement of the theorem does not hold any longer if $c < \lambda_s^{-1}$.

# A word about the proofs

If $r \geq t+1$ and $r' \geq t+1$, we have

$$\sum_{\omega \sim \omega'}^{*} P(E_\omega \cap E_{\omega'}) \leq \sum_{\substack{1 \leq x_1, \dots, x_t \\ a_1x_1 + \dots + a_tx_t < z \\ b_1x_1 + \dots + b_tx_t < z'}} (x_1 \cdots x_t)^{-1+1/s} \times$$

$$\left( \sum_{\substack{1 \leq u_{t+1}, \dots, u_r, \\ a_{t+1}u_{t+1} + \dots + a_ru_r \\ = z - (a_1x_1 + \dots + a_tx_t)}} (u_{t+1} \cdots u_r)^{-1+1/s} \right) \times \left( \sum_{\substack{1 \leq v_{t+1}, \dots, v_{r'}, \\ b_{t+1}v_{t+1} + \dots + b_{r'}v_{r'} \\ = z' - (b_1x_1 + \dots + b_tx_t)}} (v_{t+1} \cdots v_{r'})^{-1+1/s} \right).$$

By Lemma 2.1 i) we have

$$\begin{aligned} \sum_{\omega \sim \omega'}^{*} P(E_\omega \cap E_{\omega'}) &\ll \sum_{\substack{x_1, \dots, x_t \\ a_1x_1 + \dots + a_tx_t < z \\ b_1x_1 + \dots + b_tx_t < z'}} (x_1 \cdots x_t)^{-1+1/s} \times \\ &\times \quad \Big(z - (a_1x_1 + \dots + a_tx_t)\Big)^{\frac{r-t}{s}-1} \Big(z' - (b_1x_1 + \dots + b_tx_t)\Big)^{\frac{r'-t}{s}-1}. \\ &\ll \sum_{\substack{x_1, \dots, x_t \\ a_1x_1 + \dots + a_tx_t < z \\ b_1x_1 + \dots + b_tx_t < z'}} (x_1 \cdots x_t)^{-1+1/s} \big(z - (a_1x_1 + \dots + a_tx_t)\big)^{-t/s} \big(z' - (b_1x_1 \end{aligned}$$

# Another word about the proof of "Gaps"

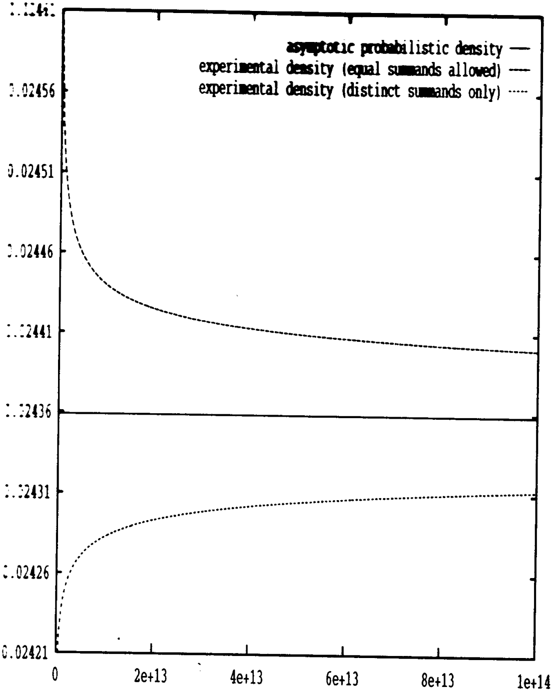
Let $\mu > 0$ be given. We define the events
$F_i^{(\mu)} = \{sA \cap [i, i + \mu \log i] = \emptyset\}$, and wish to prove
(*) $\quad \text{Prob}\left(F_i^{(\mu)}\right) = i^{-\mu\lambda_s + o(1)}$.
We think of Borel-Cantelli and understand why $1/\lambda_s$ is a threshold.
The expression $F_i^{(\mu)}$ itself is the intersection of all the events stating that $a_1 + \cdots + a_s$ is not in the interval $[i, i + \mu \log i]$. If those events were independent, some combinatorics would be enough to establish (*).
Fortunately, $F_i^{(\mu)}$ is the intersection of complementary events which are natural in our model, and a magic inequality due to Jansson permits us to consider them as almost independent... at the cost of some acrobatic manipulations. Again, this quasi-independence permits us to apply a modified version of Borel-Cantelli.

By the way, this correlation inequality can be used at no cost in different questions (gaps, complementary sequences...,) where we have a clear threshold, but is responsible for some approximations in other questions (sums of $s + 1$ or $s + \varepsilon$ pseudo $s$-th powers).

# Arithmetical model and numerical tests

The model for the pseudo $s$-th powers only takes care of the "infinite valuation". Around 2000, Hennecart, Landreau and D. have developed probabilistic models which also take care of the distribution of the pseudo $s$-th powers in arithmetic progressions. For fixed $K$, we forced the pseudo $s$-th powers to be distributed as the real $s$-th powers in all the arithmetic progressions modulo any integer less than K. For example, this leads *a.s.* to a density $\delta_s(K)$ for the sums of s pseudo $s$-th powers. Moreover, when $K$ tends to infinity, $\delta_s(K)$ tends to 0 when $s = 2$ and to a positive limit when $s \geq 3$. We also made some numerical experiments for $s = 3$ and $s = 4$.

**Question 5.** Find a probabilistic model for squares in which Landau asymptotics for sums of two squares is *a.s.* valid for sums of 2 pseudo-squares.


asymptotic probabilistic density
experimental density (equal summands allowed)
experimental density (distinct summands only)
.02456
0.02451
.02446
.02441
.02436
.02431
.02426
0.02421
0
2e+13
4e+13
6e+13
8e+13
1e+14

$j = j - 1$

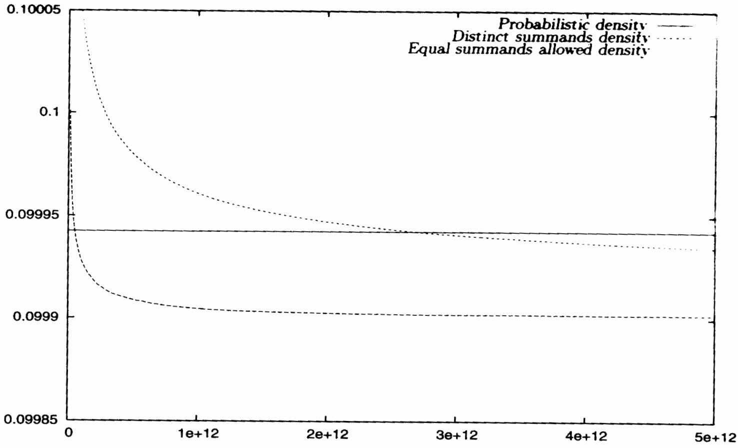



**Fig. 1.** The experimental and probabilistic densities

... in Figure 1 that for small values of ...

... observed i...

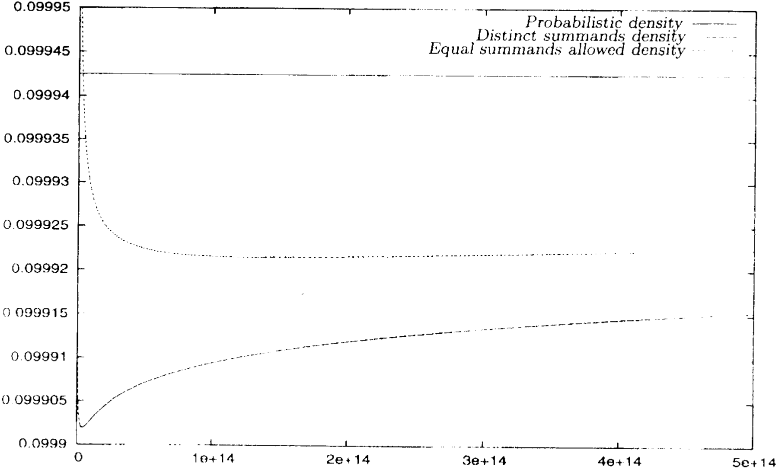



**Fig. 3.** The experimental and probabilistic densities

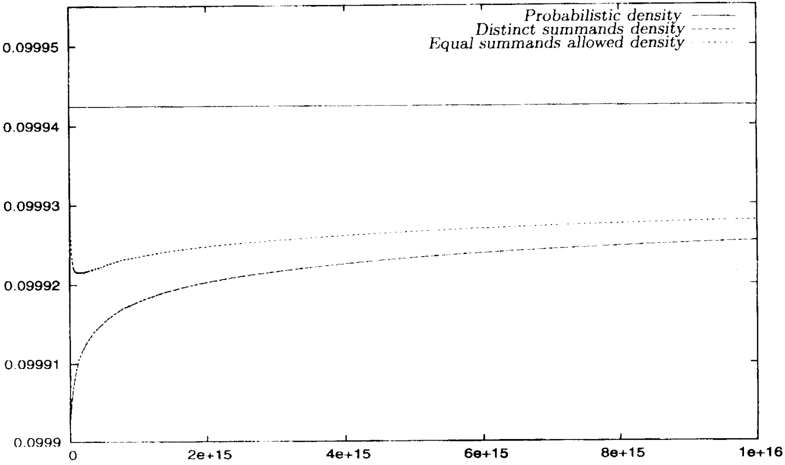



**Fig. 4.** The relative experimental and probabilistic densities in the class 1 mod 503

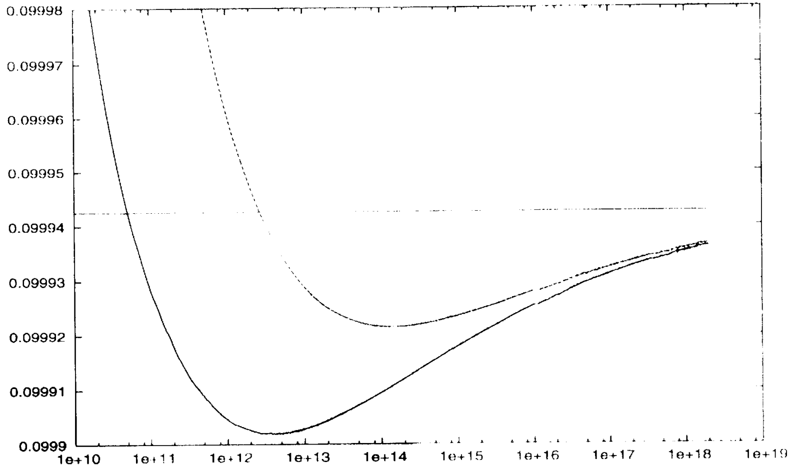



**Fig. 8.** The extrapolated experimental densities and the probabilistic density viewed in logarithmic scale