



HAL
open science

A lower bound concerning subset sums which do not cover all the residues modulo p .

Jean-Marc Deshouillers

► **To cite this version:**

Jean-Marc Deshouillers. A lower bound concerning subset sums which do not cover all the residues modulo p . Hardy-Ramanujan Journal, 2005, Volume 28 - 2005, pp.30-34. 10.46298/hrj.2005.85 . hal-01110947

HAL Id: hal-01110947

<https://hal.science/hal-01110947v1>

Submitted on 29 Jan 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A lower bound concerning subset sums which do not
cover all the residues modulo p

Jean-Marc DESHOUILLEERS¹

À la mémoire de S. Srinivasan

ABSTRACT

Let $c > \sqrt{2}$ and let p be a prime number. J.-M. Deshouillers and G. A. Freiman proved that a subset \mathcal{A} of $\mathbb{Z}/p\mathbb{Z}$, with cardinality larger than $c\sqrt{p}$ and such that its subset sums do not cover $\mathbb{Z}/p\mathbb{Z}$ has an isomorphic image which is rather concentrated; more precisely, there exists s prime to p such that

$$\sum_{a \in \mathcal{A}} \left\| \frac{as}{p} \right\| < 1 + O(p^{-1/4} \ln p),$$

where the constant implied in the “O” symbol depends on c at most. We show here that there exist a constant K depending on c at most, and such sets \mathcal{A} , such that for all s prime to p one has

$$\sum_{a \in \mathcal{A}} \left\| \frac{as}{p} \right\| > 1 + Kp^{-1/2}.$$

1 Let p be a prime number and \mathcal{A} be a set of distinct non-zero residue classes modulo p . We denote by \mathcal{A}^* the set of the subset sums of \mathcal{A} , that is to say

$$\mathcal{A}^* = \left\{ \sum_{b \in \mathcal{B}} b, \mathcal{B} \subset \mathcal{A} \right\}.$$

G. A. Freiman and the author proved (cf. [1]) the following result.

¹Supported by Université Victor Segalen Bordeaux 2 (EA 2961), Université Bordeaux1 and CNRS (UMR 5465)

Theorem 1. *Let $c > \sqrt{2}$. Let p be a prime number and \mathcal{A} be a subset of $\mathbb{Z}/p\mathbb{Z}$ with cardinality larger than $c\sqrt{p}$, such that its subset sums do not cover $\mathbb{Z}/p\mathbb{Z}$. There exists s prime to p such that*

$$\sum_{a \in \mathcal{A}} \left\| \frac{as}{p} \right\| < 1 + O(p^{-1/4} \ln p). \quad (1)$$

In this paper we prove that the error term cannot be arbitrary small. More precisely, we prove the following

Theorem 2. *Let $\sqrt{2} < c < 2$. There exists a positive real number K such that for all prime number p which is sufficiently large, there exists a subset \mathcal{A} of $\mathbb{Z}/p\mathbb{Z}$ with cardinality larger than $c\sqrt{p}$, such that its subset sums do not cover $\mathbb{Z}/p\mathbb{Z}$, and such that for every s prime to p , one has*

$$\sum_{a \in \mathcal{A}} \left\| \frac{as}{p} \right\| > 1 + Kp^{-1/2}. \quad (2)$$

2 Notation When a and b are two real numbers, we denote by $\langle a, b \rangle$ the set of the integers x from the interval $[a, b]$. For a real number u , we use the traditional notation $e(u) = \exp(2\pi iu)$ and $\|u\| = \min_{z \in \mathbb{Z}} |u - z|$; when $b \in \mathbb{Z}/p\mathbb{Z}$, the expression $e(b/p)$ (*resp.* $\|b/p\|$) denotes the common value of all the $e(\tilde{b}/p)$'s (*resp.* $\|\tilde{b}/p\|$), where \tilde{b} is any integer representing the class b ; we further let $|b|$ denote the minimum of $|\tilde{b}|$ over all the representative \tilde{b} of b , or equivalently $|b| = p\|b/p\|$.

The letter p denotes a prime number which is sufficiently large to satisfy all the implicit or explicit inequalities.

3 A lemma Before embarking on the construction of \mathcal{A} , we state and prove a preliminary technical lemma.

Lemma 1. *Let u and k be natural integers with $2 \leq u \leq 2k - 3$. Then any integer v in the interval $[k + 2, 2k^2 - 3k]$ can be expressed as a sum of at most v/k pairwise distinct elements from the interval $[k + 2, 5k]$.*

Proof of Lemma 1 The lemma is trivial when $k + 2 \leq v \leq 5k$ and we may now assume that $v > 5k$. Let us write $v = 2qk + r$ with $1 \leq q \leq 2k - 4$ and $3k < r \leq 5k$, and let us consider two cases

- if q is even, say $q = 2\ell$, we have $\ell \leq k - 2$ and we can write $2qk = \sum_{|h| \leq \ell, h \neq 0} (2k + h)$,

- if q is odd, say $q = 2\ell + 1$, we have $\ell \leq k - 2$ and we can write $2qk = \sum_{|h| \leq \ell} (2k + h)$.

In each case, we can represent v as a sum of $q + 1$ pairwise distinct integers from the interval $[k + 2, 5k]$, whence the result.

4 Construction of \mathcal{A}

4.1 We first construct an auxiliary suitable set of integers, \mathcal{E} . We recall that $\sqrt{2} < c < 2$ and let

$$L = \max\{12, \lfloor \frac{4 + c^2}{4 - c^2} + 1 \rfloor\} \text{ and } k = \lfloor \sqrt{\frac{p}{L^2 - 1}} + 1 \rfloor;$$

we thus have

$$(L^2 - 1)(k^2 - 4k + 4) \leq p \leq (L^2 - 1)(k^2 - 2k + 1).$$

We consider the set $\mathcal{B} = \langle k + 1, Lk \rangle$; we have

$$2 \sum_{b \in \mathcal{B}} b = (L^2 - 1)k^2 + (L - 1)k,$$

from which one deduces

$$(0.5L - 1)k - 0.5 \leq \sum_{b \in \mathcal{B}} b - (k + 1) - (p - 1)/2 \leq (L^2 + 0.5L)k.$$

By Lemma 1, when p is sufficiently large, we can find distinct elements in $\langle k + 2, 5k \rangle$ the sum of which is $\sum_{b \in \mathcal{B}} b - (k + 1) - (p - 1)/2$; let us denote by \mathcal{C} the set of those elements and let $\mathcal{D} = \mathcal{B} \setminus \mathcal{C}$. The set \mathcal{D} is included in $\langle k + 1, Lk \rangle$, contains $\{k + 1\} \cup \langle 5k + 1, Lk \rangle$ and satisfies

$$S := \sum_{d \in \mathcal{D}} d = (p - 1)/2 + (k + 1).$$

We finally define \mathcal{E} by

$$\mathcal{E} = \mathcal{D} \cup \{-d/d \in \mathcal{D} \text{ and } d > k + 1\}.$$

4.2 Let us now turn our attention to the set \mathcal{E}^* in \mathbb{Z} . Its largest positive element is S (defined as $\sum_{d \in \mathcal{D}} d = (p - 1)/2 + (k + 1)$), the sum of the positive elements of \mathcal{E} . We have *a priori* two ways to get the largest element in \mathcal{E}^* besides the one we just mentioned: either we subtract the smallest

positive element of \mathcal{E} (which is $k + 1$), or we add its negative element with the minimal absolute value (which is at most $-(k + 2)$); there are thus no element of \mathcal{E}^* between $S - (k + 1)$, which is $(p - 1)/2$ and S , which is strictly larger than $(p + 3)/2$. On the other hand, by a similar computation, the smallest element in \mathcal{E}^* is the sum of the negative elements of \mathcal{E} , which is $-(S - (k + 1)) = -(p - 1)/2$, and the smallest besides it, is larger than or equal to $-(S - (k + 1) - (k + 2)) = -(p - 1)/2 + (k + 2)$.

4.3 Let \mathcal{A} be the canonical image of \mathcal{E} on $\mathbb{Z}/p\mathbb{Z}$. We show that \mathcal{A}^* does not cover $\mathbb{Z}/p\mathbb{Z}$: let us consider the point $(p + 3)/2$ (or more correctly, its canonical image in $\mathbb{Z}/p\mathbb{Z}$). The only integers in \mathcal{E}^* that can cover this point are $(p + 3)/2$, which is impossible, or $(p + 3)/2 - p = -(p - 3)/2 = -(p - 1)/2 + 1$, which is again impossible. Thus \mathcal{A} is different from $\mathbb{Z}/p\mathbb{Z}$.

5 No dilation of \mathcal{A} leads to a small sum It remains to show that relation (2) is satisfied.

5.1 We first consider the case when s is 1 or -1 . In this case, we have $\sum_{a \in \mathcal{A}} \|sa/p\| = 2(S/p) - (k + 1)/p = 1 + k/p > 1 + ((1/\sqrt{(L^2 - 1)}) \cdot p^{-1/2})$.

5.2 When $1 < |s| < p/(2Lk)$, we have $\|sa/p\| = |s| \cdot \|a/p\|$ and so $\sum_{a \in \mathcal{A}} \|sa/p\| > |s| \cdot (1 + k/p) > 2$.

5.3 Let us now consider the case when $p/(2Lk) \leq |s| \leq p/((L - 6)k)$. The interval $\langle 5k + 1, 6k \rangle$ is in \mathcal{D} and for any integer d in this interval we have $2/L < |s|d/p < p/2$; this implies $\sum_{a \in \mathcal{A}} \|sa/p\| > 2k/L$, which is larger than 2 when p is large enough.

5.4 We finally consider the case when $p/((L - 6)k) \leq |s| < p/2$. For any real number x we have $2\pi\|x\| \geq 2|\sin(\pi x)| \geq 2\sin^2(\pi x) = 1 - \cos(2\pi x) = 1 - \Re(e(x))$. Since the interval $\langle 5k + 1, Lk \rangle$ is included in \mathcal{D} , we have

$$\begin{aligned} \sum_{a \in \mathcal{A}} \|sa/p\| &\geq \sum_{h=5k+1}^{Lk} \|sh/p\| \geq \frac{1}{2\pi} \sum_{h=5k+1}^{Lk} (1 - \Re(e(sh/p))) \\ &= \frac{1}{2\pi} ((L - 5)k - \Re(\sum_{h=5k+1}^{Lk} e(sh/p))). \end{aligned}$$

We further have

$$|\Re(\sum_{h=5k+1}^{Lk} e(sh/p))| \leq |\sum_{h=5k+1}^{Lk} e(sh/p)| \leq \frac{2}{2|\sin(\pi s/p)|},$$

and since $|s|$ is less than $p/2$, we have

$$|\Re(\sum_{h=5k+1}^{Lk} e(sh/p))| \leq \frac{p}{2|s|} \leq (L-6)k.$$

We thus have

$$\sum_{a \in \mathcal{A}} \|sa/p\| \geq k/(2\pi) \geq 2,$$

as soon as p is sufficiently large.

This ends the proof of Theorem 2.

6 Concluding remarks In order to get a result of the type $\sum_{a \in \mathcal{A}} \|\frac{as}{p}\| < 1 + \Omega(p^{-1/2})$, we need, with our construction, to have an upper bound for $\text{Card}(\mathcal{A})$ of the type $c\sqrt{p}$ with $c < 2$, and we believe that when c tends to 2, such a result cannot be valid.

In the other direction, we conjecture that, in Theorem 1, the upper bound for the error term may be replaced by $O(p^{-1/2})$. However, our construction may be adapted to show that such an error term cannot be valid when $\text{Card}(\mathcal{A}) = o(p^{-1/2})$.

References

- [1] Deshouillers, J-M., Freiman, G. A., When subset sums do not cover all the residues modulo p