GLASNIK MATEMATIČKI
Vol. 45(65)(2010), 357 – 372

ON VAN DER CORPUT PROPERTY OF SQUARES

Siniša Slijepčević
University of Zagreb, Croatia

Abstract. We prove that the upper bound for the van der Corput property of the set of perfect squares is $O((\log n)^{-1/3})$, giving an answer to a problem considered by Ruzsa and Montgomery. We do it by constructing non-negative valued, normed trigonometric polynomials with spectrum in the set of perfect squares not exceeding n, and a small free coefficient $a_0 = O((\log n)^{-1/3})$.

1. Introduction

We say that a set D of integers is a *Poincaré* (*recurrent,* or *intersective*) set, if for any set A of integers with non-negative upper density

$$\rho(A) = \limsup_{n\to\infty} |A \cap [1,n]|/n > 0,$$

its difference set $A - A$ contains an element of D. There is also an equivalent ergodic theoretical characterization of the Poincaré property ([3]). Furstenberg and Sárközy proved independently that the sets of squares, sets of integer values of polynomials with integer coefficients such that $P(0) = 0$ and sets of shifted primes $p - 1$ and $p + 1$ are Poincaré sets ([3, 16, 17]).

Given any set of integers D, one can define the function $\alpha : \boldsymbol{N} \to [0, 1]$ as $\alpha(n) = \sup \rho(A)$, where A goes over all sets of integers whose difference set does not contain an element of $D \cap [1, n]$ (equivalent definitions of α can be found in [13]). One can then show that D is Poincaré if and only if

$$\lim_{n\to\infty} \alpha(n) = 0.$$

Upper bounds on the function α for the Poincaré sets mentioned above have been obtained by various authors ([4, 6, 7, 9, 15–18]), but even in the simplest

2010 *Mathematics Subject Classification.* 11P99, 37A45.
Key words and phrases. Sárközy theorem, recurrence, difference sets, positive definiteness, van der Corput property, Fourier analysis.

example of the set of squares, there is a huge gap between the best upper and lower bounds for α.

Kamae and Mendès France introduced in [5] a closely related notion of *van der Corput* (or *correlative*) sets, namely sets of integers D such that, given a real sequence $(x_n)_{n\in N}$, if all the sequences $(x_{n+d}-x_n)_{n\in N}$, $d\in D$, are uniformly distributed mod 1, then the sequence $(x_n)_{n\in N}$ is itself uniformly distributed mod 1 (characterizations of the van der Corput property are recalled in Section 2). Kamae and Mendès France also showed that van der Corput sets are Poincaré sets, and that all the examples mentioned above are van der Corput sets.

Ruzsa introduced a function $\gamma : \boldsymbol{N}\to[0,1]$ which quantifies the van der Corput property of a given set and gave several characterizations of γ ([8,13]). Analogously as above, a set D is a van der Corput set if and only if

$$\lim_{n\to\infty}\gamma(n)=0.$$

Ruzsa also showed that $\alpha\le\gamma$. Ruzsa and Montgomery set a problem of finding any upper bound for the function γ for any non-trivial van der Corput set, and in particular to find an upper bound for the function γ associated to the set of perfect squares ([8, unsolved problem 3], [13]). They also demonstrated that knowledge of upper bounds on the function γ would be useful, as γ has various characterizations related to uniform distribution and other properties of a set of integers.

In this paper we prove that for the set of squares, $\gamma(n)=O((\log n)^{-1/3})$, and develop a technique which can likely be applied to other van der Corput sets satisfying Kamae and Mendès France condition ([5, §3]). We note that I. Ruzsa in [12] announced the result that for the set of squares, $\gamma(n)=O((\log n)^{-1/2})$, but the proof was never published.

It is important to emphasize that the gap between functions α and γ can be arbitrarily large in relative terms. This was shown by Bourgain, who constructed a set D such that $\lim_{n\to\infty}\alpha(n)=0$, while $\gamma(n)$ is bounded away from zero ([2]). We argue in Section 2 that it is very difficult to obtain van der Corput bounds for perfect squares better than $O((\log n)^{-1})$. We also state the main result precisely in Section 2. In Section 3 we prove the main result, postponing two key technical steps to Sections 4, 5. In Section 6 we discuss an application of the main result to positive definite functions vanishing on squares.

2. Definitions and the main result

We first introduce the notation, mostly following [8]. If D is a set of integers, then $D_n=D\cap\{1,...,n\}$. We denote by $\mathcal{T}(D)$ the set of all cosine

polynomials

$$T(x) = a_0 + \sum_{d \in D_n} a_d \cos(2\pi d x), \tag{2.1}$$

$T(0) = 1$, $T(x) \geq 0$ for all x, where n is any integer and a_0, a_d are real numbers (i.e., T is a normed non-negative valued cosine polynomial with the spectrum in $D \cup \{0\}$).

Let μ be a Borel probability measure on the 1-torus $\boldsymbol{T}$ (parametrized with $[0,1)$). For $k \in \boldsymbol{Z}$ we define the Fourier coefficients of μ to be the numbers

$$\widehat{\mu}(k) = \int \exp(-2\pi i \cdot kx) d\mu(x).$$

Let $\mathcal{M}(D)$ be the set of all probability measures on $\boldsymbol{T}$ such that $\widehat{\mu}(k) \neq 0$ only when $|k| \notin D$.

The following characterization of van der Corput sets is due to Kamae, Mendès France and Ruzsa ([5], [8], [13]):

THEOREM 2.1. *A subset D of $\boldsymbol{N}$ is a van der Corput set if and only if any of the following equivalent conditions hold:*
(i) $\sup_{\mu \in \mathcal{M}(D)} \mu(\{0\}) = 0$,
(ii) $\inf_{T \in \mathcal{T}(D)} a_0 = 0$.

We can associate to a set D two functions which describe how rapidly D is becoming a van der Corput set:

$$\delta(n) = \sup_{\mu \in \mathcal{M}(D_n)} \mu(\{0\}), \tag{2.2}$$

$$\gamma(n) = \inf_{T \in \mathcal{T}(D_n)} a_0. \tag{2.3}$$

Theorem 2.1 now implies that a set is van der Corput if and only if $\delta(n) \to 0$ as $n \to \infty$, or equivalently $\gamma(n) \to 0$ as $n \to \infty$. Ruzsa and Montgomery ([8, 14]) proved the following result:

$$\gamma(n) = \delta(n).$$

As was already noted in the introduction, the function γ also quantifies uniform distribution properties of a set D (see [8] for an exposition of the results). The function γ is an upper bound for the function α related to the Poincaré property (see introduction), and also likely related to ergodic theoretical and other properties related to the van der Corput property ([1] contains the most recent results).

We focus in this paper on finding an upper bound for the function γ associated to the set of perfect squares Q. Our approach is constructive: given $\delta > 0$, we explicitly construct a non-negative normed cosine polynomial (2.1) with coefficients in $Q_n \cup \{0\}$ and $a_0 = \delta$.

Constructing non-negative trigonometric polynomials with a sparse set of non-zero coefficients is not an easy task. We denote as usual $e(x) = \exp(2\pi i x)$, and note that the real part of

$$S(x, M) = \frac{1}{M} \sum_{k=1}^{M} e(k^2 x) \tag{2.4}$$

is a normed cosine polynomial. Recall that classical Weyl estimates show that, if $M \gg q$ and $|x - p/q| \leq 1/q^2$ for some rational p/q, $(p, q) = 1$, then

$$\left| \frac{1}{M} \sum_{k=1}^{M} e(k^2 x) \right| = O\left(q^{-1/2}\right) \tag{2.5}$$

(we prove a sharper version of (2.5) in Section 4). This means that for large M, the sum (2.4) is sufficiently small for all x which can be approximated by a rational with a large denominator; we only need to fix "small denominators". A natural approach would be to define

$$T_{L,M}(x) = \frac{1}{M} \sum_{k=1}^{M} \cos(2\pi L^2 k^2 x). \tag{2.6}$$

Then $T_{L,M}(x)$ is a cosine polynomial with non-zero coefficients only at perfect squares, such that it is close to 1 for x which can be approximated well by p/q, $q|L^2$. One can then hope that one can find appropriate normalized weights w_k such that for all x, the polynomial

$$T(x) = \sum_{L=1}^{L_{\max}} w_k T_{L,M}(x) \geq -\delta. \tag{2.7}$$

We show that we can choose weights w_k so that the values of $T_{L,M}(x)$ for rational x with small denominator cancel out. This is more difficult than it may seem, and is discussed in detail in Section 5. We also overcome the second difficulty of oscillatory behavior of $T(x)$ near rationals with a small denominator (see Proposition 3.3), and prove the following main result:

THEOREM 2.2. *If γ is the function (2.3) associated to the set of perfect squares Q, then $\gamma(n) = O((\log n)^{-1/3})$.*

The key step in the proof is using a constant L which is the smallest common multiplier of all the numbers between 1 and $O(1/\delta^2)$, and $n \geq L$. Lemma 5.4 implies that $\log n \geq \log L = O(1/\delta^2)$, so by inserting $\gamma(n) = \delta$ one sees that the best bound which can be obtained by pursuing that approach is $\gamma(n) = O((\log n)^{-1/2})$. It is very difficult to do better than that, as the Kamae and Mendès France criterion ([5, §3]), which is in our knowledge essentially the only known method of proving the van der Corput property of squares, also depends on showing that the sums (2.6) for $L = q!$ are small (more specifically, converge to 0 as $M \to \infty$ and x irrational).

We devote the rest of this section to comparing our result to other upper and lower bounds. Incidentally, our bound is essentially the same as the bound $\alpha(n) = O((\log n)^{-1/3+\varepsilon})$ obtained by Sárközy ([16]). In [9] the authors showed that $\alpha(n) = O((\log n)^{-c})$ for arbitrarily large c. We argue that the van der Corput property of squares is quantitatively fundamentally different than the Poincaré property, and that c can not be arbitrarily large.

We can denote by $\mathcal{T}^+(D)$ the set of all trigonometric polynomials (2.1) with nonnegative coefficients, and define $\gamma^+(n)$ as in (2.3), where the infimum goes over $\mathcal{T}^+(D_n)$. Then clearly $\gamma(n) \le \gamma^+(n)$. The methods developed in this paper actually enable constructing only polynomials with non-negative coefficients, and result with bounds on $\gamma^+(n)$. I. Ruzsa proved that for the set of squares, $\gamma^+(n) \gg (\log n)^{-1}$, which suggests that achieving $\gamma(n) = O((\log n)^{-c})$ for arbitrarily large c would be technically very difficult.

3. Construction of the trigonometric polynomial

Recall the definition of $S(x, M)$ defined in (2.4). We also introduce the function

$$S(x, L, M) = S(L^2 x, M) = \frac{1}{M} \sum_{k=1}^{M} e(k^2 L^2 x), \tag{3.1}$$

and $S(x, L, M)$ is also normed, $S(1, L, M) = 1$. The following estimate is essential in our construction.

Proposition 3.1. *If L, M are integers, $x \in [0, 1]$ and $|x - p/q| \le \varepsilon$, $(p, q) = 1$, then*

$$|S(x, L, M)| = \vartheta_L(q) + O\left(\frac{\sqrt{\log q}}{\sqrt{M}} + \frac{\sqrt{q \log q}}{M} + L^2 M^2 \varepsilon\right), \tag{3.2}$$

$$\vartheta_L(q) = \begin{cases} 1, & q | L^2, \\ 0, & q/(q, L^2) \equiv 2 (\mathrm{mod}\, 4), \\ r^{-1/2} & \textit{otherwise,} \end{cases} \tag{3.3}$$

where $r = q/(q, 2L^2)$. Furthermore, if $q | L^2$, then

$$S(x, L, M) = 1 + O(L^2 M^2 \varepsilon). \tag{3.4}$$

We dedicate the next section to the proof of Proposition 3.1, modifying well-known bounds on S based on the Weyl exponential sum methods. The key difference to what is common in the literature is the attention we put in evaluating precisely the leading term, e.g. in the case $L = 1$ typically only bounded in the form $O(q^{-1/2})$. This is essential to achieve the optimal bound at the end. We also discuss in Section 4 why we use the unweighted exponential sum S rather than a weighted version.

To simplify working with (3.2) and (3.4), we set

$$\tau_L(q) = \begin{cases} 1, & q|L^2, \\ 0, & q/(q,L^2) \equiv 2 (\mathrm{mod}\, 4), \\ -r^{-1/2} & \text{otherwise}, \end{cases} \tag{3.5}$$

$$E_{L,M}(q,\varepsilon) = \min\left\{ c_1 \left(\frac{\sqrt{\log q}}{\sqrt{M}} + \frac{\sqrt{q \log q}}{M} + L^2 M^2 \varepsilon \right), 2 \right\},$$

where $r = q/(q, 2L^2)$ and the constant in $E_{L,M}(q,\varepsilon)$ is the larger of the constants in the error terms in (3.2) and (3.4). We can then rewrite (3.2), (3.4) as

$$\operatorname{Re} S(x,L,M) \geq \tau_L(q) - E_{L,M}(q,\varepsilon), \tag{3.6}$$

where $|x - p/q| \leq \varepsilon$, $(p,q) = 1$. We will say in the following that functions τ or E have a certain property for each $x \in [0,1]$, if for a given x they have that property for some $(p,q) = 1$, $\varepsilon \geq 0$, where $|x - p/q| \leq \varepsilon$.

Ideally, for a given $\delta > 0$, we would like to choose constants L, M large enough so that $\tau - E$ is for each x bounded from below by $-\delta$. As this is not possible for either of the terms, we will need to average over many 'L' (the term τ) and over many 'M' (the term E) to achieve that. We start with the term τ.

PROPOSITION 3.2. *Say $\delta > 0$. There exist constants $\lambda > 0$ and $1 = L_0 \leq L_1 \leq ... \leq L_l = L_{\max}$, $\Lambda = \sum_{k=0}^{l} \lambda^k$ such that for any integer $q > 0$,*

$$\frac{1}{\Lambda} \sum_{k=0}^{l} \lambda^k \tau_{L_k}(q) \geq -\delta/2, \tag{3.7}$$

and $L_{\max} = O(\exp c_2 (1/\delta)^2)$.

We dedicate the entire Section 5 to the proof of Proposition 3.3, as it consists of several steps somewhat combinatorial in character.

We now focus on the error term E.

PROPOSITION 3.3. *Say $\delta > 0$ is small enough and $L \geq \exp(1/\delta)$. Given any $x \in [0,1]$, there exist constants $1 \leq M_1 \leq ... \leq M_m = M_{\max}$ depending only on L, δ and constants p_k, q_k, ε_k, $k = 1, ..., m$, where $(p_k, q_k) = 1$ and $\varepsilon_k = |x - p_k/q_k|$, such that*

$$\frac{1}{m} \sum_{k=1}^{m} E_{L,M_k}(q_k, \varepsilon_k) \leq \delta/2, \tag{3.8}$$

and $M_{\max} = O(L^{c_3 \cdot 1/\delta})$.

PROOF. Choose m so that $8/\delta \leq m \leq 9/\delta$. We set $M_k = L^{2(m+k)}, R_k = L^{4(m+k)}$, $k = 1, ..., m$. For a given $x \in [0,1]$, Let p'_k/q'_k, $(p'_k, q'_k) = 1$, be

the sequence of Dirichlet's approximations of x, i.e., the rationals such that $1 \le q'_k \le R_k$ and

$$|x - p'_k/q'_k| \le 1/(q'_k R_k).$$

We can also assume without loss of generality that q'_k is an increasing sequence. Now, let n be the largest index such that $q'_n \le L^{4m}$ (n can also be 0). We define $p_k/q_k = p'_n/q'_n$ for $k \le n$, $p_k/q_k = p'_{n+1}/q'_{n+1}$ for $k \ge n+1$, and $\varepsilon_k = |x - p_k/q_k|$. We note that for δ small enough (independent of L), $\log q_k \le \log R_m \le L^{1/2}$.

In the case $k \le n-1$, using $\varepsilon_k \le 1/R_n$ and $q_k \le L^{4m}$, we get

$$E_{L,M_k}(q_k, \varepsilon_k) \le L^{1/2}/M_k^{1/2} + L^{2m}L^{1/2}/M_k + L^2 M_k^2/R_n \le 3L^{-1/2}.$$

In the case $k \ge n+2$, using $\varepsilon_k \le 1/(q_{n+1}R_{n+1}) \le 1/(L^{4m}R_{n+1})$ and $q_k \le R_{n+1}$ we get

$$E_{L,M_k}(q_k, \varepsilon_k) \le L^{1/2}/M_k^{1/2} + R_{n+1}^{1/2}L^{1/2}/M_k + L^2 M_k^2/(L^{4m}R_{n+1}) \le 3L^{-1/2}.$$

We conclude that for δ small enough (independent of L), for all k except $k = n, n+1$, $E_{L,M_k}(q_k, \varepsilon_k) \le \delta/4$ holds. As for all k, $E_{L,M_k}(q_k, \varepsilon_k) \le 2$ and $m \ge 8/\delta$, we easily obtain (3.8). Finally, $M_{\max} = L^{4m} = O(L^{c_3 \cdot 1/\delta})$ with $c_3 = 36$. □

We now complete the proof of Theorem 2.3. Say $\delta > 0$ is given. We construct the cosine polynomial

$$T(x) = \frac{1}{m\Lambda} \sum_{j=1}^{l} \sum_{k=1}^{m} \lambda^j \operatorname{Re} S(x, L_j, M_k), \tag{3.9}$$

where the constants $l, L_1, ..., L_l = L_{\max}$ are as constructed in Proposition 2.2 and the constants $m, M_1, ..., M_m = M_{\max}$ are as constructed in Proposition 3.3 by choosing $L = L_{\max}$. Using (3.6), (3.7), (3.8) and the fact that $E_{L,M}$ is non-decreasing in L, we obtain for each $x \in [0,1]$

$$T(x) \ge \frac{1}{m\Lambda} \sum_{j=1}^{l} \sum_{k=1}^{m} \lambda^j \left(\tau_{L_j}(q_k) - E_{L_{\max},M_k}(q_k, \varepsilon_k)\right) \ge -\delta/2 - \delta/2 = -\delta.$$

The polynomial (3.9) is normed, has non-zero coefficients only at perfect squares, and the largest non-zero coefficient is at $n = M_{\max}^2 L_{\max}^2 = O(\exp(2c_2c_3(1/\delta)^3)$, hence $\delta = O((\log n)^{-1/3})$.

4. Exponential sum estimates

To prove Proposition 3.1, we will here adapt classical upper bounds on $S(x, M)$ based on the Weyl's method, following mostly the approach and notation from [8, Section 3]. As was mentioned earlier, we do the adaptation

to evaluate precisely the leading term below. Recall the definition of $\vartheta_L(q)$ in (3.3), and then

$$\vartheta_1(q) = \begin{cases} 1, & q = 1, \\ 0, & q \equiv 2 (\mathrm{mod}\, 4), \\ r^{-1/2} & \text{otherwise}, \end{cases}$$

where $r = q/(q,2)$.

PROPOSITION 4.1. *If p/q is a rational, $(p,q) = 1$, then*

$$|S(p/q, M)| = \vartheta_1(q) + O\left(\sqrt{\log q}/\sqrt{M} + \sqrt{q \log q}/M\right).$$

PROOF. Say $T = M^2|S|^2$, and then by substituting $h = k - j$ we see that

$$T = \sum_{k,j=1}^{M} e((k^2 - j^2)p/q) = \sum_{h=1-M}^{M-1} \sum_{k=1}^{M-|h|} e(h^2 p/q) e(2khp/q) =$$

$$= \sum_{q|2h} (M - |h|) e(h^2 p/q) + \sum_{\rceil q|2h} e(h^2 p/q) \sum_{k=1}^{M-|h|} e(2khp/q), \tag{4.1}$$

where h in both sums in the second row goes from $1 - M$ to $M - 1$.

We first estimate the right-hand sum in (4.1). If $q|2h$ does not hold,

$$\left| \sum_{k=1}^{M-|h|} e(2khp/q) \right| \leq 1/(2\,\|2hp/q\|), \tag{4.2}$$

where $\|x\|$ denotes the distance from x to the nearest integer. Choose a segment of variables h which are not multipliers of r and of length $r - 1$, and then we deduce that

$$\sum_{h=kr+1}^{(k+1)r-1} \frac{1}{2\,\|2hp/q\|} = O(q \log q) \tag{4.3}$$

(see e.g. [8], p. 40 for details of evaluating (4.2) and (4.3)). As there are at most $2M/r + 2 \leq 4M/q + 2$ such segments, that, (4.2) and (4.3) imply that the absolute value of the right-hand sum in (4.1) is at most

$$O(M \log q + q \log q). \tag{4.4}$$

To evaluate the left-hand sum in (4.1), we discuss two cases depending on the remainder of q mod 4.

If $q \equiv 0, 1,$ or $3 (\mathrm{mod}\, 4)$, then $q|2h$ if and only if $q|h^2$, and then $e(h^2 p/q) = 1$. If we set $r = q/(q,2)$, then $q|2h$ if and only if $r|h$ and the left-hand sum in (4.1) becomes

$$\sum_{r|h} (M - |h|) = 2 \sum_{k=1}^{M/r+1} (M - rk) + O(M) = M^2/r + O(M) + O(q). \tag{4.5}$$

Summing (4.4) and (4.5) we deduce that $T = M^2/r + O(M\log q + q\log q)$, which completes the proof in these cases.

If $q \equiv 2 (\mathrm{mod}\, 4)$, then for $q|2h$, $e(h^2p/q)$ alternates between ± 1. Again $q|2h$ if and only if $r|h$ and the left-hand sum in (4.1) becomes

$$\sum_{r|h}(M-|h|)e(h^2p/q) = 2\sum_{k=1}^{M/r+1}(M-rk)(-1)^k + O(M) = O(M)+O(q). \tag{4.6}$$

Summing (4.4) and (4.6) we obtain $T = O(M\log q + q\log q)$ which completes the proof if $q \equiv 2 (\mathrm{mod}\, 4)$. □

We now complete the proof of Proposition 3.1. Using Proposition 4.1, relation $S(p/q, L, M) = S(L^2p/q, M)$ and the fact that the error term is non-decreasing in q, we easily deduce that

$$|S(p/q, L, M)| = \vartheta_L(q) + O\left(\sqrt{\log q}/\sqrt{M} + \sqrt{q\log q}/M\right). \tag{4.7}$$

Now say $|x - p/q| \le \varepsilon$. As for any k between 1 and M,

$$\left|e(k^2L^2x) - e(k^2L^2p/q)\right| \le 2\pi k^2L^2|x - p/q| \le 2\pi M^2L^2\varepsilon.$$

We deduce that

$$|S(x, L, M) - S(p/q, L, M)| = O(M^2L^2\varepsilon). \tag{4.8}$$

Combining (4.7) and (4.8) we obtain the first part of Proposition 3.1. We note that for any integer n, $S(n, M) = 1$, hence if $q|L^2$, $S(p/q, L, M) = 1$. Combining that and (4.8) we obtain the second part of Proposition 3.1.

The error term $M^2L^2\varepsilon$ above is not too good. We would like to replace the exponential sum S with a weighted exponential sum such that an analogue of Proposition 3.1 holds with a better error term, that means an error term such that the exponent on M is less than twice the exponent on ε. In that case, averaging over "M" and Proposition 3.2 would not be required, and the bound in Theorem 2.2 would be improved to $O((\log n)^{-1/2})$. We dedicate the rest of this section to discussing why two possible approaches do not achieve that. One approach is choosing weights which simulate Dirichlet's kernel as in [9], and the other is simulating Fejér's kernel.

Dirichlet's kernel. The authors in [9] worked with weighted exponential sums, and simulated normed Dirichlet's kernel

$$D_M(x) = \frac{1}{2M+1}\sum_{k=-M}^{M} e(kx).$$

Instead of $S(x, M)$ they defined the weighted sum $T(x, M)$ approximating $D_M(x)$ as

$$T(x, M) = \frac{1}{M'}\sum_{k=1}^{M} 2ke(k^2x),$$

where M' is chosen so that $T(1,M)=1$. If $|x-p/q|=\varepsilon$, then

$$T(x,M)=S(p/q,q)T(\varepsilon,M)+O((q\log q)^{1/2}(1/M+M\varepsilon))$$

([9], relation (8)). As $T(\varepsilon,M)=1+O(M^2\varepsilon)$, the error term is essentially the same as in Proposition 3.1 (the authors in [9] also use the fact that $T(\varepsilon,M)$ is close to 0 when ε is small but not too small, which is opposite to our needs. We would wish to bound $T(\varepsilon,M)$ close to 1 for small ε).

Fejér's kernel. Following the idea of I. Ruzsa, one can choose weights to simulate the normed Fejér's kernel

$$\Delta_M(x)=\frac{1}{M}\sum_{k=-M}^{M}\left(1-\frac{|k|}{M}\right)e(kx)=\frac{1}{M^2}\left(\frac{\sin\pi Mx}{\sin\pi x}\right)^2,$$

with the purpose to dampen the oscillations of S at integers and rational numbers with small denominator. Instead of $S(x,M)$ we can define

$$V(x,M)=\frac{1}{M''}\sum_{k=1}^{M}k\left(1-\frac{k^2}{M^2}\right)e(k^2x)$$

where M'' is chosen so that $V(x,M)=1$. One can then show that, if $|x-p/q|=\varepsilon$,

$$V(x,M)=S(p/q,q)\Delta_{M^2}(\varepsilon)+O(Mq\varepsilon).$$

As for small ε, $\Delta_k(\varepsilon)=1+O(k^2\varepsilon^2)$, we get $\Delta_{M^2}(\varepsilon)=1+O(M^4\varepsilon^2)$. The error term $M^4\varepsilon^2$ which replaces $M^2\varepsilon$ in Proposition 3.1 in the case $L=1$ is better, but does not enable us to improve the bound in Theorem 2.2.

5. Proof of Proposition 3.3

Recall the definition of $\tau_L(q)$ in (3.5). We prove here that we can find a linear combination of various τ_L so that its value for any q is not smaller than $-\delta$ for a given small $\delta>0$. The difficulty lies in the following. As was explained in the introduction, choosing a very composite L seems to be enough: say n is greater than $1/\delta^2$, and L is the smallest common multiplier of all numbers between 1 and n. Then for most q, $\tau_L(q)\geq-\delta$. Specifically, for numbers q which divide L^2, $\tau_L(q)=0$, and for numbers q which have a prime factor larger than n, $\tau_L(q)\geq-\delta$. We, however, have no control over behavior of $\tau_L(q)$ for which $q/(q,2L^2)$ is small (for example, multipliers of $2L^2$ with a small number, but also many other cases). This problem arises for any L.

To resolve this and cancel out values of small $q/(q,2L^2)$, we construct an approximate geometric sequence of very composite "L's". This idea is coded in the Lemma 5.1 below. For clarity, we write $\tau(L,q)$ instead of $\tau_L(q)$. Note that if L and q have only one common prime number p in their decompositions,

then for $p = 2$,

$$\tau(p^j, p^k) = \begin{cases} 1, & j - k/2 \geq 0, \\ 0, & j - k/2 = -1/2, \\ -p^{j+1/2-k/2} & \text{otherwise}, \end{cases}$$

and for $p \geq 3$,

$$\tau(p^j, p^k) = \begin{cases} 1, & j - k/2 \geq 0, \\ -p^{j-k/2} & \text{otherwise}. \end{cases}$$

LEMMA 5.1. *Say p is a prime and μ a real number such that $1 > \mu \geq p^{-1/2}$. Then for any non-negative integers n, k,*

$$\sum_{j=0}^{n} \mu^j \tau(p^j, p^k) \geq -\frac{1}{1-\mu}\mu^{n+1}. \tag{5.1}$$

PROOF. The case $k = 0$ is trivial, so say $k \geq 1$. Denote the left-hand side of (5.1) with $A_n(p, k)$. Say m is the largest index between 0 and n such that $m - k/2 < 0$, hence $m - k/2 \leq -1/2$. We evaluate $A_m(p, k)$ in three cases. If $p \geq 3$, then using first $m - k/2 \leq -1/2$ and then $-p^{-c} \geq -\mu^{2c}$ for $c \geq 0$, we get

$$\begin{aligned} A_m(p,k) &= -\sum_{j=0}^{m} \mu^j p^{j-k/2} \geq -\sum_{j=0}^{m} \mu^j p^{j-m-1/2} \geq -\sum_{j=0}^{m} \mu^{2m+1-j} = \\ &= -\sum_{j=m+1}^{2m+1} \mu^j \geq -\sum_{j=m+1}^{\infty} \mu^j. \end{aligned}$$

Now assume $p = 2$ and $m - k/2 = -1/2$. As $\tau(p^m, p^k) = 0$, similarly as above we deduce that

$$\begin{aligned} A_m(p,k) &= -\sum_{j=0}^{m-1} \mu^j p^{j+1/2-k/2} = -\sum_{j=0}^{m-1} \mu^j p^{j-m} \geq -\sum_{j=0}^{m-1} \mu^{2m-j} = \\ &= -\sum_{j=m+1}^{2m} \mu^j \geq -\sum_{j=m+1}^{\infty} \mu^j. \end{aligned}$$

Finally, if $p = 2$ and $m - k/2 \leq -1$, repeating at the end the last couple of steps as in the case $p \geq 3$ we obtain

$$A_m(p,k) = -\sum_{j=0}^{m} \mu^j p^{j+1/2-k/2} \geq -\sum_{j=0}^{m} \mu^j p^{j-m-1/2} \geq -\sum_{j=m+1}^{\infty} \mu^j.$$

Inserting that in $A_n(p, k)$, we see that most of the terms cancel out:

$$A_n(p,k) = A_m(p,k) + \sum_{j=m+1}^{n} \mu^j \geq -\sum_{j=n+1}^{\infty} \mu^j = -\frac{1}{1-\mu}\mu^{n+1}.$$

□

In the next step, we will fix the weights so that they do not depend on the prime p. For clarity of the argument and notation, we write $\lambda = 2^{-1/2}$.

LEMMA 5.2. *Say $l > 0$ is an integer. For each prime number p there exist integers $0 = d_0 \le d_1 \le ... \le d_l$ such that for any integer $k \ge 0$,*

$$\sum_{j=0}^{l} \lambda^j \tau(p^{d_j}, p^k) \ge -5\lambda^l, \tag{5.2}$$

and

$$p^{d_l} < 2^{2l}. \tag{5.3}$$

PROOF. Let e be an integer such that $2^{e+1} > p \ge 2^e$. Dividing l with e we get the quotient f and the remainder g, $l = f \cdot e + g$. We define coefficients d_j so that $d_0 = d_1 = ... = d_{e-1} = 0$, and every e coefficients we increase it by 1 until we reach $f \cdot e$, and then $d_{f\cdot e} = ... = d_{f\cdot e+g} = f$.

We denote the left-hand side of (5.2) with $B_l(p,k)$, and we set $\mu = 2^{-e/2} = \lambda^e$. We note that $\mu \ge p^{-1/2}$, apply Lemma 5.1 and deduce that

$$\begin{aligned} B_{f\cdot e-1}(p,k) &= \sum_{j=0}^{f-1}(1+\lambda+...+\lambda^{e-1})\mu^j\tau(p^j,p^k) \ge \\ &\ge -\frac{1+\lambda+...+\lambda^{e-1}}{1-\mu}\mu^f = -\sum_{j=ef}^{\infty}\lambda^j. \end{aligned} \tag{5.4}$$

We analyse two cases. Say first $\tau(p^f, p^k) = 1$, and then using (5.4) we get

$$B_l(p,k) = B_{f\cdot e-1}(p,k) + \sum_{j=ef}^{l}\lambda^j \ge -\sum_{j=l+1}^{\infty}\lambda^j = -\frac{\lambda}{1-\lambda}\lambda^l.$$

Now say $\tau(p^f, p^k) \le 0$, and then for all $j \le f-1$, $\tau(p^j, p^k) = p^{-1/2}\tau(p^j, p^{k-1})$. The function $\tau(p^f, p^k)$ is always greater or equal than $-p^{-1/2}$. Using that, (5.4) and $-p^{-1/2} \ge -\mu = -\lambda^e$, and finally $ef + e \ge l + 1$, we deduce that

$$\begin{aligned} B_l(p,k) &= p^{-1/2}B_{f\cdot e-1}(p,k-1) - \sum_{j=ef}^{l}\lambda^j p^{-1/2} \ge \\ &\ge -\sum_{j=ef+e}^{\infty}\lambda^j - \sum_{j=ef+e}^{l+e}\lambda^j \ge -\frac{2\lambda}{1-\lambda}\lambda^l. \end{aligned}$$

As $2\lambda/(1-\lambda) < 5$, (5.2) holds. The relation (5.3) follows from $p^{d_l} = p^f < 2^{ef+f} \le 2^{2ef} \le 2^{2l}$. □

We now show why it is enough to study only primes.

LEMMA 5.3. *Say $L_1, ..., L_l$ is a sequence of integers such that $L_j | L_{j+1}$ for all $j = 1, ..., l$. Then for each integer q, there exists a prime p such that for all j,*

$$\tau(L_j, q) \geq \tau(p^{d_j}, p^k), \tag{5.5}$$

where p^{d_j}, p^k are factors in the prime decompositions of L_j, q respectively.

PROOF. Let $m+1$ be the smallest index such that $q | L_{m+1}^2$ (if there is no such m, we set $m = l$). If $m = 0$, $q | L_k$ for all k, and we choose any prime p in the prime decomposition of q. Now say $1 \leq m \leq l$, and let $r = q/(q, L_m^2)$. If $r \equiv 2 (\mathrm{mod}\, 4)$, we set $p = 2$, otherwise we choose any prime p in the prime decomposition of r. For $k \geq m+1$, both sides of (5.5) are equal to 1. For $k \leq m$, it is straightforward to check (5.5). □

We now finally construct all variables in Proposition 3.3. Choose l so that $\delta/20 \leq 2^{-l/2} \leq \delta/10$, and let $\lambda = 2^{-1/2}$, $\Lambda = \sum_{j=0}^{l} 2^{-j/2}$. We set $n = 2^l$. Let $2 = p_1 < p_2 < ... < p_s < n$ be all the prime numbers between 1 and n, and let d_j^i be the exponents constructed in Lemma 5.2, associated to the prime p_i, $i = 1, ..., s$, $j = 0, ..., l$. We set

$$L_j = \prod_{i=1}^{s} p_i^{d_j^i}.$$

Now applying Lemma 5.3 and then Lemma 5.2 we deduce that for any $q \in \boldsymbol{N}$,

$$\frac{1}{\Lambda} \sum_{j=0}^{l} \lambda^j \tau(L_j, q) \geq \frac{1}{\Lambda} \sum_{j=0}^{l} \lambda^j \tau(p^{d_j}, p^k) \geq -5 \cdot 2^{-l/2} \geq -\delta/2.$$

To complete the proof of Proposition 3.3, we only need to estimate $L_{\max} = L_l$.

LEMMA 5.4. *If K is the smallest common multiplier of all numbers between 1 and n, then $K \leq \exp(c_5 \cdot n)$, $c_5 = 1.04$.*

PROOF. This is [10, Theorem 12]. □

We now see that (5.3) implies that $L_{\max} \leq K^2$, and by Lemma 5.4, $K \leq \exp^{c_6 (1/\delta)^2}$, $c_6 = 1.04 \cdot 400$.

6. Positive definite functions vanishing of squares

Now we discuss an application of Theorem 2.2 to positive definite functions on $\boldsymbol{Z}/n\boldsymbol{Z}$ vanishing of squares.

We say that a number $\alpha \in \boldsymbol{Z}/n\boldsymbol{Z}$ is a perfect square, if $\alpha \equiv \pm k^2 (\mathrm{mod}\, n)$ for some integer k, $k^2 < n/2$. The fact that the set of squares is a Poincaré set with estimates obtained in [9] can be interpreted as follows:

THEOREM 6.1 (Sárközy, Furstenberg, Pintz, Steiger, Szeméredi). *If $A \subset \boldsymbol{Z}/n\boldsymbol{Z}$ such that $|A|/n \geq d_4(\log n)^{-d(n)}$, $d(n) = d_5 \log\log\log\log n$, then $A-A$ contains a perfect square.*

We now note that $A-A$ is not containing a perfect square if and only if the function $1_A * 1_{-A} = 1_A * 1_A^*$ vanishes on perfect squares $\boldsymbol{Z}/n\boldsymbol{Z}$. The function $f = 1_A * 1_{-A}$ is positive definite on $\boldsymbol{Z}/n\boldsymbol{Z}$ (i.e., all its Fourier coefficients are real and non-negative, see [11]).

We can generalize the notion of density of a set to all non-zero complex valued positive definite functions $f \in \boldsymbol{C}(\boldsymbol{Z}/n\boldsymbol{Z})$, and define it as

$$\rho(f) = \widehat{f}(0)/(nf(0)).$$

One can easily check that $\rho(1_A * 1_{-A}) = |A|/n$, so this is indeed a natural generalization of the concept of density of a set.

PROPOSITION 6.2. *Say $f \in \boldsymbol{C}(\boldsymbol{Z}/n\boldsymbol{Z})$ is non-zero, positive definite. Then $\rho(f)$ is well defined, $0 \leq \rho(f) \leq 1$. Furthermore, $\rho(f) = 1$ if and only if f is constant.*

PROOF. As for all positive definite functions, $f = 0$ if and only if $f(0) = 0$, $\rho(f)$ is clearly well defined and non-negative. Calculating we get $\widehat{f}(0) = |\widehat{f}(0)| = |\sum_\alpha f(\alpha)| \leq \sum_\alpha |f(\alpha)| \leq n|f(0)| = nf(0)$, hence $\rho(f) \leq 1$. The equality holds in the inequalities above if the arguments and absolute values respectively of $f(\alpha)$ are constant. □

We can now formulate the following strengthening of Theorem 6.1 as a Corollary of Theorem 2.2.

COROLLARY 6.3. *Say $f \in \boldsymbol{C}(\boldsymbol{Z}/n\boldsymbol{Z})$ is non-zero, positive definite, such that $\rho(f) \geq d_6(\log n)^{-1/3}$ for some constant d_6. Then f can not vanish on all perfect squares in $\boldsymbol{Z}/n\boldsymbol{Z}$.*

PROOF. Let $T(x) = \delta + \sum a_d \cos(2\pi dx)$, where sum goes over all $d \in Q_{n/2}$, be the non-negative cosine polynomial constructed in Theorem 2.2, and say $f \in \boldsymbol{C}(\boldsymbol{Z}/n\boldsymbol{Z})$ is non-zero, positive definite, and $\rho(f) > \delta$. We define a function $g \in \boldsymbol{C}(\boldsymbol{Z}/n\boldsymbol{Z})$ as

$$g(\alpha) = \frac{1}{2}\begin{cases} a_d, & \alpha \equiv \pm d (\mathrm{mod}\, n), d \in Q_{n/2}, \\ 2\delta, & \alpha = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then by choice of $T(x)$, g is positive definite, $g(0) = \delta$, $\widehat{g}(0) = 1$. If f vanishes on squares, we get

$$\delta \cdot f(0) = f \cdot g = \sum_\alpha \frac{1}{n}\widehat{f}(\alpha)\widehat{g}(-\alpha) \geq \frac{1}{n}\widehat{f}(0)\widehat{g}(0) = \frac{1}{n}\widehat{f}(0),$$

hence $\rho(f) \leq \delta$ which is a contradiction (we used the notation $f \cdot g = \sum_\alpha f(\alpha)g(\alpha)$ where $\sum_\alpha$ stands for $\sum_{\alpha \in Z/nZ}$, a form of Parseval's identity on Z/nZ and positive definiteness of f, g). □

One can show that finding the functions α, γ is essentially the same as finding the sharpest formulations of Theorem 6.1 and Corollary 6.3.

Acknowledgements.

The author wishes to thank Professor Andrej Dujella for his help, and to Professor Imre Z. Ruzsa for useful advice and encouragement.

References

[1] V. Bergelson and E. Lesigne, *Van der Corput sets in Z^d*, Colloq. Math. **110** (2008), 1–49.
[2] J. Bourgain, *Ruzsa's problem on sets of recurrence*, Israel J. Math. **59** (1987), 151–166.
[3] H. Furstenberg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math., **31** (1977), 204–256.
[4] B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. J., **114**, (2002) (2) 215–238.
[5] T. Kamae, M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. **31** (1978), 335–342.
[6] J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. **123** (2006), 57–95.
[7] J. Lucier, *Difference sets and shifted primes*, Acta Math. Hungar. **120** (2008), 79–102.
[8] H. L. Montgomery, Ten lectures on the interface between analytic number theory and harmonic analysis, AMS, Providence, 1994.
[9] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural integers whose difference set contains no squares*, J. London Math. Soc. **37** (1988), 219–231.
[10] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
[11] W. Rudin, Fourier analysis on groups, Wiley, 1962.
[12] I. Z. Ruzsa, *Uniform distribution, positive trigonometric polynomials and difference sets*, in Semin. on Number Theory, 1981/1982, Univ. Bordeaux I, Talence, 1982, Exp. No. 18, 18pp.
[13] I. Z. Ruzsa, *Connections between the uniform distribution of a squence and its differences*, in Topics in Classical Number Theory, Vol. I, II (Budapest, 1981), Colloq. Math. Soc. Jànos Bolyai, **34**, North-Holland, Amsterdam, 1984, 1419–1443.
[14] I. Z. Ruzsa, *On measures of intersectivity*, Acta Math. Hungar. **43** (1984), 335–340.
[15] I. Z. Ruzsa and T. Sanders, *Difference sets and the primes*, Acta Arith. **131** (2008), 281–301.
[16] A. Sárközy, *On difference sets of integers I*, Acta Math. Acad. Sci. Hungar. **31** (1978), 125–149.
[17] A. Sárközy, *On difference sets of integers III*, Acta Math. Acad. Sci. Hungar. **31** (1978), 355–386.
[18] S. Slijepčević, *A polinomial Sárközy-Furstenberg theorem with upper bounds*, Acta Math. Hungar. **98** (2003), 111–128.

S. Slijepčević
Department of Mathematics
University of Zagreb
Bijenička 30
10000 Zagreb
Croatia
E-mail: slijepce@math.hr

Received: 13.3.2009.
Revised: 20.9.2009. & 17.1.2010. & 14.3.2010.