

Difference Sets and Positive Exponential Sums. II: Cubic Residues in Cyclic Groups

Máté Matolcsi^{a,b} and Imre Z. Ruzsa^b

Received August 1, 2020; revised November 29, 2020; accepted June 17, 2021

Dedicated to the memory of I. M. Vinogradov

Abstract—By constructing suitable nonnegative exponential sums, we give upper bounds on the cardinality of any set B_q in cyclic groups \mathbb{Z}_q such that the difference set $B_q - B_q$ avoids cubic residues modulo q .

DOI: 10.1134/S0081543821040088

1. INTRODUCTION

This paper is a follow-up to [3], where we described the general properties connecting positive exponential sums and difference sets. In this second part, we apply the techniques of [3] to investigate the intersective properties of cubic residues in cyclic groups \mathbb{Z}_q . That is, by constructing suitable nonnegative exponential sums, we obtain upper bounds on the cardinality of any set $B_q \subset \mathbb{Z}_q$ such that the difference set $B_q - B_q$ avoids cubic residues modulo q . We will turn to the case of quadratic residues in a later publication, but let us mention here that Gabdullin [2] has recently achieved a non-trivial upper bound by a different method.

The ultimate aim of this research is to extend these results to the case of integers, i.e., give a strong upper bound on the cardinality of a set $B \subset \{0, 1, \dots, N\}$ such that $B - B$ does not contain any cubes or, more generally, k th powers for some fixed k .

In order to see the relation of the modular case to the integer case, we introduce the following notions.

We use the standard notation $e(x) = e^{2\pi ix}$ throughout the paper.

Definition 1.1. A nonnegative function

$$f^{(n)}(x) = a_0 + \sum_{j=1}^{n-1} a_j (e(j^k x) + e(-j^k x)) \geq 0, \quad x \in [0, 1], \quad f^{(n)}(0) = 1, \quad (1.1)$$

is called a k th power witness function of order n . Similarly, a nonnegative function

$$g^{(q)}(y) = b_0 + \sum_{j=1}^{q-1} b_j \left(e\left(\frac{j^k y}{q}\right) + e\left(-\frac{j^k y}{q}\right) \right) \geq 0, \quad y = 0, 1, \dots, q-1, \quad g^{(q)}(0) = 1, \quad (1.2)$$

is called a k th power modular witness function, modulo q . (The dependence of a_j on n and b_j on q will usually be suppressed in the notation.)

The normalization $f^{(n)}(0) = g^{(q)}(0) = 1$ is only for convenience, and will be used throughout this note. We remark that the coefficients a_j are automatically real as they are the Fourier (cosine)

^a Budapest University of Technology and Economics (BME), Egrý J. u. 1, H-1111 Budapest, Hungary.

^b Alfréd Rényi Institute of Mathematics, P.O. Box 127, H-1364 Budapest, Hungary.

E-mail addresses: matomate@renyi.hu (M. Matolcsi), ruzsa@renyi.hu (I. Z. Ruzsa).

coefficients of the real-valued function $f^{(n)}$. Also, we can assume without loss of generality (after averaging over j if necessary) that $b_j = b_{j'}$ whenever $j^k \equiv \pm j'^k \pmod q$. This makes the coefficients b_j real (because $g^{(q)}$ is a real-valued even function, and b_j are basically its Fourier coefficients, so they must be conjugate symmetric $b_j = \bar{b}_{-j}$, and they are also symmetric $b_j = b_{-j}$ by the assumption above, so they are in fact real).

Let us clarify here the connection of these definitions to the results of [3]. Consider the cyclic group $G = \mathbb{Z}_q$ of order q , and let $R_0^{(k)}$ denote the set of k th power residues mod q (including 0). Let $R_s^{(k)}$ denote the symmetrized set $R_s^{(k)} = R_0^{(k)} \cup -R_0^{(k)}$. We can think of the coefficients b_j as a function $h: G \rightarrow \mathbb{R}$, supported on $R_s^{(k)}$, defined in the following way: for any $r \in R_s^{(k)}$ let $h(r) = \sum_{j^3 \equiv \pm r} b_j$. The Fourier transform of h is then $\hat{h} = g^{(q)} \geq 0$. Therefore, the function h fits into the class of functions used in the definition of $\lambda(R_s^{(k)})$ in [3].

We will restrict our attention to the case $k = 3$ in this paper, the treatment of other odd values of k being similar. We will use the following notation in accordance with the one introduced in [3].

Definition 1.2. Let $C^{(q)}$ denote the set of non-zero cubic residues modulo q , and let $C_0^{(q)} = C^{(q)} \cup \{0\}$. Recall from [3] that $\delta(C_0^{(q)})$ denotes the maximal density (i.e., $|B_q|/q$) of a set $B_q \subset \mathbb{Z}_q$ such that $(B_q - B_q) \cap C^{(q)} = \emptyset$. Also, $\lambda(C_0^{(q)})$ denotes the minimal possible value of the constant term b_0 in expression (1.2) for $k = 3$.

In this note we will be interested in upper bounds on $\delta(C_0^{(q)})$, but let us also mention here what is known about lower bounds. For a prime $q = 3k + 1$, it is clear by the Ramsey number estimate $R(s, s) \leq 4^s$ that one can find a set $B_q \subset \mathbb{Z}_q$ of size at least $\lfloor \log_4 q \rfloor$ such that $(B_q - B_q) \cap C^{(q)} = \emptyset$. (After applying the Ramsey estimate, one can find either a suitable set B or a set $B' \subset \mathbb{Z}_q$, $|B'| \geq \lfloor \log_4 q \rfloor$, such that $B' - B' \subset C_0^{(q)}$. In the latter case, it suffices to consider $B = tB'$ for any non-cubic residue $t \in \mathbb{Z}_q$.) Also, a construction of a set B' such that $B' - B' \subset C_0^{(q)}$, $\log_6 q \lesssim |B'|$, not using the Ramsey theory, appears in [1, Theorem 3]. For a prime $q = 3k + 2$ the problem is trivial as $|B| \leq 1$. For a square-free integer $q = s_1 s_2 \dots s_m$, where $s_i = 3k_i + 1$, a straightforward direct product construction (see [3, Sect. 8]) gives a suitable set B with $|B| \geq \prod_{i=1}^m \lfloor \log_4 s_i \rfloor$. We are not aware of any stronger results, and numerical experiments seem to indicate that the logarithmic size is not far from the truth for primes $q = 3k + 1$.

We will obtain upper bounds on $\lambda(C_0^{(q)})$, and these will automatically imply upper bounds on $\delta(C_0^{(q)})$. In particular, according to [3, Theorem 1.4], any modular witness function $g^{(q)}$ in equation (1.2) testifies to an upper bound $|B_q| \leq b_0 q$ for the cardinality of a set $B_q \subset \mathbb{Z}_q$ such that $B_q - B_q$ avoids the k th power residues modulo q . Similarly, a k th power witness function $f^{(n)}$ will lead to an estimate $|B_0| \lesssim a_0 n^k$ for the cardinality of a set $B_0 \subset [1, \dots, n^k]$ such that $B_0 - B_0$ avoids the k th powers. Our aim, therefore, is to minimize the values of a_0 and b_0 in equations (1.1) and (1.2). We will only be concerned with the modular case in this note.

Notice that $f^{(n)}(x)$ automatically induces a modular witness function modulo $q = n$ by defining $g^{(n)}(y) = f^{(n)}(y/n)$, and if n is square-free then $f^{(n)}$ and $g^{(n)}$ have the same constant terms $a_0 = b_0$. Therefore, constructing modular k th power witness functions $g^{(q)}$ is *formally easier* than constructing k th power witness functions $f^{(n)}$. Conversely, in later publications of this series of papers we hope to construct a family of witness functions $f^{(n)}$ assuming that we already have a family of *self-compatible* modular witness functions $g^{(q)}$ at our disposal. Self-compatibility is a natural property defined here.

Definition 1.3. A family of k th power modular witness functions $g^{(q)}$ ($q = 1, 2, \dots$) of the form (1.2) is called *self-compatible* if $g^{(q_1)}(y_1) = g^{(q_2)}(y_2)$ whenever $y_1/q_1 = y_2/q_2$.

This paper will be devoted entirely to constructing a self-compatible family of modular witness functions for $k = 3$, which is a very interesting problem in itself.

2. CUBIC RESIDUES

Somewhat surprisingly, the case of cubic residues is considerably easier to handle than that of quadratic residues. This is due to the fact that $k = 3$ is an odd number and therefore -1 is automatically a cubic residue modulo q for any q . This implies that the set of cubic residues modulo $q = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ is always *symmetric* to 0. Also, it is equal to the direct product of the sets of cubic residues modulo $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$. Therefore, the results on direct products in [3, Sect. 8] can be invoked, and the problem reduces to forming nonnegative exponential sums with cubic residue frequencies in cyclic groups \mathbb{Z}_{p^α} of prime-power order. The self-compatibility property will be an automatic consequence of the construction.

We first consider the case of square-free moduli q , which is of independent interest in itself.

Theorem 2.1. *Let $q = p_1 p_2 \dots p_r s_1 s_2 \dots s_m$ be a square-free integer, where p_i denote primes of the form $3k + 2$, s_l denote primes of the form $3k + 1$, and if $3 \mid q$ then we list the prime 3 among the p_i . There exists a cubic witness function modulo q , $g^{(q)}(y) = b_0 + \sum_{j=1}^{q-1} b_j (e(j^3 y/q) + e(-j^3 y/q)) \geq 0$, $y = 0, 1, \dots, q - 1$, $g^{(q)}(0) = 1$, such that*

$$b_0 \leq \left(\prod_{i=1}^r \frac{1}{p_i} \right) \left(\prod_{l=1}^m \frac{2}{\sqrt{s_l}} \right) \leq \frac{2^m}{\sqrt{q}}. \tag{2.1}$$

That is, with the notation of Definition 1.2, we have

$$\lambda(C_0^{(q)}) \leq \frac{2^m}{\sqrt{q}} = O_\varepsilon(q^{-1/2+\varepsilon}) \tag{2.2}$$

for every $\varepsilon > 0$.

Proof. For a prime $p = 3k + 2$, all elements of \mathbb{Z}_p are cubic residues. Therefore, we can take the trivial witness function modulo p ,

$$g^{(p)}(y) = \frac{1}{p} \sum_{j=0}^{p-1} e\left(\frac{j^3 y}{p}\right), \tag{2.3}$$

with the constant term being $1/p$. That is, $\lambda(C_0^{(p)}) \leq 1/p$ (in fact, the equality holds). The same is true for $p = 3$, which is listed among the p_i if $3 \mid q$.

For a prime $s = 3k + 1$ the set $C^{(s)} \subset \mathbb{Z}_s$ of non-zero cubic residues modulo s is symmetric to zero, and consists of $(s - 1)/3$ elements. Denoting the cubic multiplicative characters on \mathbb{Z}_s by χ_0, χ_1 , and χ_2 (with χ_0 being the principal character), we have

$$\sum_{j=1}^{s-1} e\left(\frac{j^3 y}{s}\right) = \sum_{l=1}^{s-1} e\left(\frac{ly}{s}\right) \chi_0(l) + \sum_{l=1}^{s-1} e\left(\frac{ly}{s}\right) \chi_1(l) + \sum_{l=1}^{s-1} e\left(\frac{ly}{s}\right) \chi_2(l) \geq -1 - 2\sqrt{s}, \tag{2.4}$$

because the last two sums have absolute value \sqrt{s} (see [4, Lemma 4.3]). Therefore, after normalization, we may take

$$g^{(s)}(y) = \frac{2\sqrt{s} + 1}{2\sqrt{s} + s} + \frac{1}{2\sqrt{s} + s} \sum_{j=1}^{s-1} e\left(\frac{j^3 y}{s}\right) \geq 0, \quad y = 0, \dots, s - 1, \quad g^{(s)}(0) = 1, \tag{2.5}$$

and the constant term satisfies $(2\sqrt{s} + 1)/(2\sqrt{s} + s) \leq 2/\sqrt{s}$. That is, $\lambda(C_0^{(s)}) \leq 2/\sqrt{s}$.

Finally, the group \mathbb{Z}_q is the direct product of the groups \mathbb{Z}_{p_i} and \mathbb{Z}_{s_l} , and the set of cubic residues $C_0^{(q)}$ modulo q is symmetric to zero and equals the direct product of the sets $C_0^{(p_i)}$ and $C_0^{(s_l)}$. Therefore, the direct product construction of [3, Theorem 8.1] can be applied, and equation (35)

in [3] implies $\lambda(C_0^{(q)}) = (\prod_{i=1}^r \lambda(C_0^{(p_i)}))(\prod_{l=1}^m \lambda(C_0^{(s_l)}))$, and the bound given in (2.1) follows. Finally, estimate (2.2) follows from the fact that $2^m = O(q^\varepsilon)$. \square

Remark 2.2. For primes of the form $s = 3k + 1$ the estimate $\lambda(C_0^{(s)}) \leq 2/\sqrt{s}$ is asymptotically optimal, and therefore the exponent in the bound $\lambda(C_0^{(q)}) = O(q^{-1/2+\varepsilon})$ cannot be improved.

Via Theorem 1.4 in [3] the bound (2.2) above immediately implies the same upper bound for the density of sets avoiding cubic residues.

Corollary 2.3. *For any $\varepsilon > 0$ and any square-free positive integer q , the density $\delta(B_q)$ of any set $B_q \subset \mathbb{Z}_q$ such that the difference set $B_q - B_q$ avoids cubic residues modulo q satisfies $\delta(B_q) = O_\varepsilon(q^{-1/2+\varepsilon})$.*

Now we turn to general (non-square-free) moduli q . The direct product construction can still be applied in this case, but the construction of witness functions modulo prime powers is slightly more technical.

Lemma 2.4. *Using the notation of Definition 1.2, we have*

$$\lambda(C_0^{(p^m)}) = \lambda(C_0^{(p)})^{[(m+2)/3]} \tag{2.6}$$

for any prime $p \neq 3$ and any integer $m \geq 1$ (the notation $[x]$ stands for the integer part of any number x). For $p = 3$ we have

$$\lambda(C_0^{(3^{3m})}) = \lambda(C_0^{(27)})^m. \tag{2.7}$$

Proof. Let $p \neq 3$. We prove the lemma by induction on m . For $m = 1$ the statement is trivial. Let $m \geq 2$, and let us identify the residue classes modulo p^m with the numbers $0, 1, \dots, p^m - 1$.

The structure of the cubic residues modulo p^m is the following: for $0 < t \leq p^{m-1} - 1$ and $0 \leq l \leq p - 1$ we have $t + lp^{m-1} \in C^{(p^m)}$ if and only if $t \in C^{(p^{m-1})}$. For $t = 0$, we have two different cases. If 3 does not divide $m - 1$ then $lp^{m-1} \in C^{(p^m)}$ if and only if $l = 0$. If $3 \mid m - 1$ then $lp^{m-1} \in C^{(p^m)}$ if and only if $l \in C_0^{(p)}$.

Consider the subgroup $H = \{0, p^{m-1}, \dots, (p - 1)p^{m-1}\} \subset \mathbb{Z}_{p^m}$. Then $H \cong \mathbb{Z}_p, \mathbb{Z}_{p^m}/H \cong \mathbb{Z}_{p^{m-1}}$, and we can apply the general result concerning subgroups and factor groups in [3, Theorem 7.2]. Namely, by formula (29) in [3] and the structure of the set $C_0^{(p^m)}$ described above, we obtain $\lambda(C_0^{(p^m)}) \geq \lambda(C_0^{(p^{m-1})})$ if 3 does not divide $m - 1$, and $\lambda(C_0^{(p^m)}) \geq \lambda(C_0^{(p^{m-1})})\lambda(C_0^{(p)})$ if $3 \mid m - 1$. This proves the lower bound in the inductive step.

To prove the upper bound, we apply a simple construction. Let

$$g^{(p)}(y) = b_0^{(p)} + \sum_{j \in C^{(p)}} b_j^{(p)} e\left(\frac{ jy }{ p }\right) \tag{2.8}$$

be a witness function modulo p such that $b_0^{(p)}$ is minimal, i.e., $b_0^{(p)} = \lambda(C_0^{(p)})$ (a simple compactness argument shows that the minimal value of $b_0^{(p)}$ can indeed be attained). Similarly, let

$$g^{(p^{m-1})}(y) = b_0^{(p^{m-1})} + \sum_{t \in C^{(p^{m-1})}} b_t^{(p^{m-1})} e\left(\frac{ ty }{ p^{m-1} }\right) \tag{2.9}$$

be a witness function modulo p^{m-1} such that $b_0^{(p^{m-1})} = \lambda(C_0^{(p^{m-1})})$. Define

$$g^{(p^m)}(z) = \sum_{t \in C^{(p^{m-1})}} \frac{ b_t^{(p^{m-1})} }{ p } \sum_{l=0}^{p-1} e\left(\frac{ (t + lp^{m-1})z }{ p^m }\right) + h_0(z), \tag{2.10}$$

where $h_0(z) = b_0^{(p^{m-1})}$ if 3 does not divide $m - 1$, and $h_0(z) = b_0^{(p^{m-1})}(b_0^{(p)} + \sum_{j \in C^{(p)}} b_j^{(p)} e(jz/p))$ if $3 \mid m - 1$. Clearly, $g^{(p^m)}(0) = 1$ and the constant term of $g^{(p^m)}(z)$ is equal to $b_0^{(p^{m-1})} = \lambda(C_0^{(p^{m-1})})$ if 3 does not divide $m - 1$, while it is $b_0^{(p^{m-1})}b_0^{(p)} = \lambda(C_0^{(p^{m-1})})\lambda(C_0^{(p)})$ if $3 \mid m - 1$. We claim that $g^{(p^m)}(z)$ is indeed a witness function modulo p^m , i.e., $g^{(p^m)}(z) \geq 0$ for $z = 0, 1, \dots, p^m - 1$. If $z = py$ then a substitution into the definitions shows that

$$g^{(p^m)}(z) = g^{(p^m)}(py) = g^{(p^{m-1})}(y) \geq 0. \tag{2.11}$$

If $z = py + j$ where $j \neq 0$, then for each $t \in C^{(p^{m-1})}$ we have

$$\sum_{l=0}^{p-1} e\left(\frac{(t + lp^{m-1})z}{p^m}\right) = e\left(\frac{t(py + j)}{p^m}\right) \sum_{l=0}^{p-1} e\left(\frac{lj}{p}\right) = 0;$$

therefore

$$g^{(p^m)}(z) = g^{(p^m)}(py + j) = h_0(py + j) = b_0^{(p^{m-1})}g^{(p)}(j) \geq 0. \tag{2.12}$$

This proves the upper bound in the inductive step and completes the proof of the lemma for $p \neq 3$.

For $p = 3$ the proof is similar. The structure of the cubic residues modulo 3^{3m} is the following: for $0 < t \leq 3^{3(m-1)} - 1$ and $0 \leq l \leq 26$ we have $t + l \cdot 3^{3(m-1)} \in C^{(3^{3m})}$ if and only if $t \in C^{(3^{3(m-1)})}$. For $t = 0$, we have $l \cdot 3^{3(m-1)} \in C^{(3^{3m})}$ if and only if $l \in C_0^{(27)}$.

Consider the subgroup $H = \{0, 3^{3(m-1)}, \dots, 26 \cdot 3^{3(m-1)}\} \subset \mathbb{Z}_{3^{3m}}$. Then we have $H \cong \mathbb{Z}_{27}$, $\mathbb{Z}_{3^{3m}}/H \cong \mathbb{Z}_{3^{3(m-1)}}$, and formula (29) in [3] implies $\lambda(C_0^{(3^{3m})}) \geq \lambda(C_0^{(3^{3(m-1)})})\lambda(C_0^{(27)})$. This proves the lower bound in the inductive step.

To prove the upper bound, we define

$$g^{(3^{3m})}(z) = \sum_{t \in C^{(3^{3(m-1)})}} \frac{b_t^{(3^{3(m-1)})}}{27} \sum_{l=0}^{26} e\left(\frac{(t + l \cdot 3^{3(m-1)})z}{3^{3m}}\right) + b_0^{(3^{3(m-1)})} \left(b_0^{(27)} + \sum_{j \in C^{(27)}} b_j^{(27)} e\left(\frac{jz}{27}\right) \right) \tag{2.13}$$

and note that $g^{(3^{3m})}(0) = 1$, the constant term is $\lambda(C_0^{(3^{3(m-1)})})\lambda(C_0^{(27)})$, for $z = 27y$ we have

$$g^{(3^{3m})}(z) = g^{(3^{3m})}(27y) = g^{(3^{3(m-1)})}(y) \geq 0, \tag{2.14}$$

and for $z = 27y + j$ where $j \neq 0$ we have

$$g^{(3^{3m})}(z) = g^{(3^{3m})}(27y + j) = b_0^{(3^{3(m-1)})}g^{(27)}(j) \geq 0. \quad \square \tag{2.15}$$

This lemma enables us to prove our main result concerning cubic residues in cyclic groups.

Theorem 2.5. *For*

$$\varepsilon = -\log\left(1 - \frac{2}{2 + \cos(\pi/13) + \sin(3\pi/26)}\right) \frac{1}{3 \log 13} \approx 0.1195 \tag{2.16}$$

there exists a self-compatible family $g^{(q)}(y)$ of cubic modular witness functions of the form (1.2) such that $b_0 \leq q^{-\varepsilon}$. In particular,

$$\lambda(C_0^{(q)}) \leq q^{-\varepsilon} \tag{2.17}$$

for every $q \geq 1$.

Proof. If $q \neq 3$ is a prime of the form $3k + 2$, we define the modular witness function $g^{(q)}(y)$ by equation (2.3) and note that $\lambda(C_0^{(q)}) = q^{-1}$. If q is a prime of the form $3k + 1$, we define $g^{(q)}(y) = b_0^{(q)} + b^{(q)} \sum_{j=1}^{q-1} e(j^3y/q)$ such that $b_0^{(q)} + (q - 1)b^{(q)} = 1$, $g^{(q)}(y) \geq 0$ for $0 \leq y \leq q - 1$, and $b_0^{(q)}$ is minimal possible, i.e., $b_0^{(q)} = \lambda(C_0^{(q)})$ (it is easy to see that all the coefficients of $e(j^3y/q)$ can be assumed to be equal by averaging; cf. [3, Proposition 5.2]). By equation (2.5) we note that $\lambda(C_0^{(q)}) \leq (2\sqrt{q} + 1)/(2\sqrt{q} + q) \leq q^{-0.36}$ for $q \geq 31$. For $q = 7, 13$, and 19 direct computation shows that $\lambda(C_0^{(q)}) \leq q^{-3\epsilon}$ with equality for $q = 13$.

If $q = p^m$ is a power of a prime $p \neq 3$, then we define $g^{(q)}(y)$ by induction on m as in Lemma 2.4. Equation (2.6) shows that $\lambda(C_0^{(q)}) \leq q^{-\epsilon}$. The self-compatibility property follows from equation (2.11).

For $q = 27$ we define $g^{(27)}(y) = b_0^{(27)} + b^{(27)} \sum_{j \in C^{(27)}} e(jy/27)$ such that $g^{(27)}(0) = 1$, $g^{(27)}(y) \geq 0$ for $y = 0, 1, \dots, 26$, and $b_0^{(27)} = \lambda(C_0^{(27)})$ (again, the non-leading coefficients can be assumed to be equal by averaging). For $q = 3^{3m}$ we define $g^{(q)}(y)$ by induction on m as in Lemma 2.4. For $q = 3^{3m-1}$ and $q = 3^{3m-2}$ we define $g^{(q)}(y) = g^{(3^m)}(3y)$ and $g^{(q)}(y) = g^{(3^m)}(9y)$, respectively. Self-compatibility follows from this definition and equation (2.14). Direct computation of $\lambda(C_0^{(27)})$ and equation (2.7) show that for any $q = 3^\alpha$ we have $\lambda(C_0^{(q)}) \leq q^{-\epsilon}$.

Finally, let $q = p_0^{\alpha_0} p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be the prime factorization of q , where $p_0 = 3$ if it appears in q . The set of cubic residues $C_0^{(q)}$ modulo q is symmetric to zero and equals the direct product of the sets $C_0^{(p_i^{\alpha_i})}$. Furthermore, as in the construction of [3, Theorem 8.1] we define the cubic witness function $g^{(q)}(y) = b_0^{(q)} + \sum_{j \in C^{(q)}} b_j^{(q)} e(jy/q)$ as the direct product of the cubic modular witness functions $g^{(p_i^{\alpha_i})}$. It is straightforward that the self-compatibility property is preserved under direct products, and

$$\lambda(C_0^{(q)}) \leq b_0^{(q)} = b_0^{(3^{\alpha_0})} \left(\prod_{i=1}^r \lambda(C_0^{(p_i^{\alpha_i})}) \right) \leq q^{-\epsilon}. \quad \square$$

Again, via [3, Theorem 1.4] the bound (2.17) above immediately implies the same upper bound for the density of sets avoiding cubic residues.

Corollary 2.6. *For ϵ given by (2.16) and any positive integer q , the density $\delta(B_q)$ of any set $B_q \subset \mathbb{Z}_q$ such that the difference set $B_q - B_q$ avoids cubic residues modulo q satisfies $\delta(B_q) \leq q^{-\epsilon}$.*

ACKNOWLEDGMENTS

The authors are grateful to the reviewer for his/her suggestions which have improved the presentation of the paper.

FUNDING

M. Matolcsi was supported by the NKFIH grant nos. K132097 and K129335. I. Z. Ruzsa was supported by the NKFIH grant no. K129335.

REFERENCES

1. S. D. Cohen, “Clique numbers of Paley graphs,” *Quaest. Math.* **11** (2), 225–231 (1988).
2. M. R. Gabdullin, “Sets in \mathbb{Z}_m whose difference sets avoid squares,” *Sb. Math.* **209** (11), 1603–1610 (2018) [transl. from *Mat. Sb.* **209** (11), 60–68 (2018)].
3. M. Matolcsi and I. Z. Ruzsa, “Difference sets and positive exponential sums. I: General properties,” *J. Fourier Anal. Appl.* **20** (1), 17–41 (2014).
4. R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed. (Cambridge Univ. Press, Cambridge, 1997), Cambridge Tracts Math. **125**.