ACTA ARITHMETICA
162.3 (2014)

An extension of a theorem of Duffin and Schaeffer in Diophantine approximation

by

FAUSTIN ADICEAM (Maynooth)

For convenience, the following notation will be used throughout:

- $\lfloor x \rfloor$ $(x \in \mathbb{R})$: the integer part of x.
- $[\![x, y]\!]$ $(x, y \in \mathbb{R},\ x \leq y)$: interval of integers, i.e. $[\![x, y]\!] = \{n \in \mathbb{Z} : x \leq n \leq y\}$.
- $\mathrm{Card}(X)$ or $|X|$: the cardinality of a finite set X.
- $A^{\times}$: the set of invertible elements of a ring A.
- $\mathcal{P}$: the set of prime numbers.
- π: any prime number.
- $\varphi(n)$: Euler's totient function.
- $\tau(n)$: the number of divisors of a positive integer n.
- $\omega(n)$: the number of distinct prime factors dividing an integer $n \geq 2$ $(\omega(1) = 0)$.

1. Introduction and statement of the result. The well-known theorem of Duffin and Schaeffer [5] in metric number theory extends the classical theorem of Khintchine in the following way:

THEOREM 1.1 (Duffin & Schaeffer, 1941). *Let $(q_k)_{k\geq 1}$ be a strictly increasing sequence of positive integers and let $(\alpha_k)_{k\geq 1}$ be a sequence of nonnegative real numbers which satisfies the conditions:*

(a) $\sum_{k=1}^{\infty} \alpha_k = \infty$,
(b) $\sum_{k=1}^{n} \alpha_k \varphi(q_k)/q_k > c \sum_{k=1}^{n} \alpha_k$ *for infinitely many integers $n \geq 1$ and a real number $c > 0$.*

2010 *Mathematics Subject Classification*: 11J83, 11K60.
Key words and phrases: Diophantine approximation, theorem of Duffin and Schaeffer, metric number theory.

DOI: 10.4064/aa162-3-3

Then for almost all $x \in \mathbb{R}$ there exist infinitely many relatively prime integers p_k and q_k such that

$$\left| x - \frac{p_k}{q_k} \right| < \frac{\alpha_k}{q_k}.$$

Here as elsewhere, *almost all* must be understood in the sense that the set of exceptions has Lebesgue measure zero.

Several generalizations of Theorem 1.1 have been considered: on the one hand, the conjecture of Duffin and Schaeffer asks whether assumption (b) may be weakened to the divergence of the series $\sum_{k=1}^{n} \alpha_k\, \varphi(q_k) q_k^{-1}$. Even if the analogue of this issue has been proved in higher dimensions [15] or with some extra assumptions on the sequence $(\alpha_k)_{k\geq 1}$ [12], the full conjecture is still open. On the other hand, one may try to see to what extent Theorem 1.1 remains true when the numerators p_k and the denominators q_k of the fractional approximations are related by some stronger relationship (in a sense to be made precise) than coprimality.

Indeed, metric Diophantine approximation results in one dimension when the denominators of the rational approximants are confined to a prescribed set are numerous (see for instance [3, Theorem 5.9]). However, restrictions on numerators introduce new difficulties which do not always seem to be easy to overcome (see [3, p. 114], for an account on this fact). In a series of articles, [8]–[11], G. Harman tackled the problem and gave several results in the case where denominators and numerators were confined to vary within independent sets of integers.

The main theorems proved in this paper give another approach to this problem, studying the case where numerators and denominators are confined to dependent sets of integers in the sense that they are related, not only by the relation of Diophantine approximation of a given real number, but also by some congruential constraints.

Consider first a subsequence $(q_k^d)_{k\geq 1}$ of the dth powers of the natural numbers ($d \geq 1$ is an integer). For any $q \in \mathbb{N}$ denote furthermore by $r_d(q)$ the cardinality of the set of dth powers in a reduced system of residues modulo q and set for simplicity

$$s_d(q) := r_d(q)/q. \tag{1}$$

THEOREM 1.2. *Let $(q_k)_{k\geq 1}$ be a strictly increasing sequence of positive integers and let $(\alpha_k)_{k\geq 1}$ be a sequence of positive real numbers. Fix an integer $a \geq 1$ and assume furthermore that:*

(a) $\sum_{k=1}^{\infty} \alpha_k = \infty$,
(b) $\sum_{k=1}^{n} \alpha_k s_d(q_k^d) > c \sum_{k=1}^{n} \alpha_k$ *for infinitely many positive integers n and a real number $c > 0$,*
(c) $\gcd(q_k, a) = 1$ *for all $k \geq 1$.*

Then for almost all $x \in \mathbb{R}$ there exist infinitely many relatively prime integers p_k and q_k such that

$$\left| x - \frac{p_k}{q_k^d} \right| < \frac{\alpha_k}{q_k^d} \quad \textit{and} \quad p_k \equiv a b_k^d \pmod{q_k}$$

for some $b_k \in \mathbb{Z}$ relatively prime to q_k.

Theorem 1.2 answers a question which appeared in a problem of simultaneous Diophantine approximation of dependent quantities: given an integer polynomial $P(X)$ and a real number x, what is the Hausdorff dimension of the set of real numbers t such that t and $P(t) + x$ are simultaneously τ-well approximable, where $\tau > 0$? The author proved [1] that such a simultaneous approximation implied an approximation of x by a rational number p/q^d, where d is the degree of $P(X)$ and where the integer p satisfies the congruential constraint mentioned in the conclusion of Theorem 1.2, with a the leading coefficient of $P(X)$. The emptiness of the set under consideration is obtained for almost all x as a consequence of the convergence part of the Borel–Cantelli Lemma when $\tau > d+1$ and Theorem 1.2 enables one to prove the optimality of this lower bound.

Theorem 1.2 can in fact be generalized in the following way:

THEOREM 1.3 (Extension of the theorem of Duffin and Schaeffer). *Let $(q_k)_{k\geq 1}$ be a strictly increasing sequence of positive integers and let $(\alpha_k)_{k\geq 1}$ be a sequence of positive real numbers. Let $(a_k)_{k\geq 1}$ be a sequence such that $a_k \in (\mathbb{Z}/q_k\mathbb{Z})^\times$ for all $k \geq 1$. For $k \geq 1$, denote by G_k a subgroup of $(\mathbb{Z}/q_k\mathbb{Z})^\times$ and by $a_k G_k$ the coset of a_k in the quotient of $(\mathbb{Z}/q_k\mathbb{Z})^\times$ by G_k. Assume furthermore that:*

(a) $\sum_{k=1}^{\infty} \alpha_k = \infty$,
(b) $\sum_{k=1}^{n} \alpha_k |G_k|/q_k > c \sum_{k=1}^{n} \alpha_k$ *for infinitely many positive integers n and a real number $c > 0$,*
(c) $\varphi(q_k)/(q_k^{1/2-\epsilon}|G_k|) \to 0$ *as k tends to infinity, for some $\epsilon > 0$.*

Then for almost all $x \in \mathbb{R}$ there exist infinitely many relatively prime integers p_k and q_k such that

$$\left| x - \frac{p_k}{q_k} \right| < \frac{\alpha_k}{q_k} \quad \textit{and} \quad p_k \in a_k G_k. \tag{2}$$

REMARK 1.4. In Theorem 1.3, if c is a real number such that

$$|G_k|/q_k > c > 0 \tag{3}$$

for all $k \geq 1$, then (b) holds. However, if, instead of (3), one can prove the weaker assertion

$$\sum_{k=1}^{n} |G_k|/q_k > cn \tag{4}$$

for some $c > 0$ and all integers $n \geq 1$, then, assuming that the sequence $(\alpha_k)_{k\geq 1}$ is non-increasing, condition (b) still holds true. This may be seen by making an Abel transformation on the left-hand side of (b).

It is likely that formula (4) can be proved for many sequences $(q_k)_{k\geq 1}$ that do not satisfy (3).

In fact, Theorem 1.2 happens to be a special case of Theorem 1.3 when G_k ($k \geq 1$) is taken as the group of dth powers in a reduced system of residues modulo q_k. Nevertheless, the proof of Theorem 1.2 turns out to be somehow more instructive as it makes it easier to highlight some technical difficulties without introducing additional cumbersome notation. The paper is therefore organized as follows: first some lemmas of an arithmetical nature are recalled (Section 2). They will be needed to prove Theorem 1.2 in Section 3, where the modifications to make in the proof to prove Theorem 1.3 will also be indicated.

2. Some auxiliary results. In this section are collected various results which will be needed later.

2.1. Some lemmas in arithmetic. For any integer $n \geq 2$, let $\tau(n)$ be the number of divisors of n and let $\omega(n)$ be the number of *distinct* prime factors dividing n. If

$$n = \prod_{i=1}^{r} \pi_i^{\alpha_i}$$

is the prime factor decomposition of the integer n, recall that

$$\omega(n) = r \quad \text{and} \quad \tau(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

The following lemma, which deals with some comparative growth properties of these two arithmetical functions, is well-known.

Lemma 2.1.

- *For any* $\epsilon > 0$, $\tau(n) = o(n^\epsilon)$.
- *For any* $\epsilon > 0$ *and any positive integer* m, $\omega(n) = o(\log n)$ *and* $m^{\omega(n)} = o(n^\epsilon)$.

Proof. See for instance [7, §22.11 and §22.13]. ∎

If $n \geq 2$ and $d \geq 1$ are integers, recall that $r_d(n)$ denotes the number of distinct dth powers in the reduced system of residues modulo n, and let $u_d(n)$ denote the number of dth roots of unity modulo n, that is,

$$r_d(n) = \mathrm{Card}\{m^d \pmod{n} : m \in (\mathbb{Z}/n\mathbb{Z})^\times\},$$
$$u_d(n) = \mathrm{Card}\{m \in \mathbb{Z}/n\mathbb{Z} : m^d \equiv 1 \pmod{n}\}.$$

Set furthermore $r_d(1) = u_d(1) = 1$.

REMARK 2.2. Let $u(f,n)$ be the number of solutions in x of the congruence

$$f(x) := \sum_{k=0}^{d} a_k x^k \equiv 0 \pmod{n}$$

for a given polynomial $f \in \mathbb{Z}[X]$ of degree d. It is well-known that, as a consequence of the Chinese Remainder Theorem, $u(f,n)$ is a multiplicative function of n. It follows that $u_d(n)$ is multiplicative with respect to n for any fixed d.

The following proposition gives explicit formulae for $r_d(n)$ and $u_d(n)$.

PROPOSITION 2.3. *The arithmetical functions $r_d(n)$ and $u_d(n)$ are multiplicative when d is fixed. Furthermore, if $n = \pi^k$, where $\pi \in \mathcal{P}$ and $k \geq 1$ is an integer, then*

$$r_d(n) = \frac{\varphi(\pi^k)}{u_d(\pi^k)}, \qquad u_d(n) = \begin{cases} \gcd(2d, \varphi(n)) & \text{if } 2 \mid d,\ \pi = 2 \text{ and } k \geq 3, \\ \gcd(d, \varphi(n)) & \text{otherwise,} \end{cases}$$

where φ is Euler's totient function.

Proof. See for instance [17]. ∎

2.2. Dirichlet characters and the Pólya–Vinogradov inequality. Let G be a finite abelian group, written multiplicatively and with identity e. A *character* χ over G is a multiplicative homomorphism from G into the multiplicative group of complex numbers. The image of χ is contained in the group of $|G|$th roots of unity.

It is readily seen that the set of characters over G form a group, called the dual group of G and written $\hat{G}$. Its unit χ_0 is the *principal* (or *trivial*) *character*, which maps everything in G to unity.

The following is well-known (see [6, Chapter 7]):

THEOREM 2.4.

(i) *There are exactly $|G|$ characters over G.*

(ii) *For any $g \neq e$,*

$$\sum_{\chi \in \hat{G}} \chi(g) = 0.$$

(iii) *For any non-principal character χ,*

$$\sum_{g \in G} \chi(g) = 0.$$

If $n > 1$ is an integer, consider the group $G = (\mathbb{Z}/n\mathbb{Z})^\times$. A character χ over G may be extended to all integers by setting $\chi(m) = \chi(m \pmod{n})$ if $\gcd(n,m) = 1$ and $\chi(m) = 0$ if $\gcd(n,m) > 1$. Such a function is called a *Dirichlet character to the modulus n* and will still be denoted by χ.

In what follows, an upper bound on the sum of such characters over large intervals will be needed. A fundamental improvement on the trivial estimate given by the triangle inequality is the Pólya–Vinogradov inequality (see [6, Chapter 9]):

THEOREM 2.5 (Pólya & Vinogradov, 1918). *For any non-principal Dirichlet character* χ *over* $(\mathbb{Z}/n\mathbb{Z})^\times$ $(n>1)$ *and any integer* h,

$$\Big|\sum_{k=1}^{h}\chi(k)\Big| \le 2\sqrt{n}\log n.$$

REMARK 2.6. When χ is a so-called primitive character (which is the case if n is prime), the multiplicative constant 2 in the above may be replaced by 1. This refinement will not be needed.

3. The proof of the main results. The first part of this section is devoted to the proof of Theorem 1.2: all the tools introduced in the previous section will be used there. In the second subsection, all the modifications needed to prove Theorem 1.3 are given.

3.1. The proof of Theorem 1.2. The proof of Theorem 1.2 is a generalization of the proof of the theorem of Duffin and Schaeffer [5]. All the new notation to be used is summarized in Figure 1.

Notation	Parameters	Definition
$\varphi_\mu(n)$	$n\ge 2$, $\mu>0$	$\mathrm{Card}\{l\in [\![1,\mu n]\!] : \gcd(l,n)=1\}$
G_n	$n\ge 2$ integer	Any subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$
$G_n^{(d)}$	$d\ge 1$	Group of dth powers in a reduced system of residues modulo a fixed integer $n\ge 2$
aG_n	$a\in(\mathbb{Z}/n\mathbb{Z})^\times$, $n\ge 2$	Coset of a in the quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ by G_n, i.e. $aG_n=\{al : l\in G_n\}$
$\Psi_X(aG_n)$	$X>0$	$\mathrm{Card}\{l\in [\![1,X]\!] : l\in aG_n\}$
$d_n(G_n)$	$n\ge 2$	Index of G_n in $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e. $d_n(G_n)=\varphi(n)/\Psi_n(G_n)$

Fig. 1. Some additional notation

The key step to the proof of the theorem of Duffin and Schaeffer (Theorem 1.1) is the study of the regularity of the distribution of the numbers less than a given positive integer and relatively prime to this integer. The following is well-known and strengthens their result in [5, Lemma III].

Lemma 3.1. *Let μ be a positive real number and let $n \geq 2$ be an integer. Let $\varphi_\mu(n)$ denote the number of positive integers which are equal to or less than μn and relatively prime to n. Then for any $\epsilon > 0$,*

$$\varphi_\mu(n) = \varphi(n)(\mu + O(1/n^{1-\epsilon})).$$

Proof. See for instance [13, Theorem 3.1]. ∎

Duffin and Schaeffer provide an error term of the form $O(n^{-1/2})$ in Lemma 3.1, where the implied constant is absolute. In fact, even such an estimate is too accurate in the sense that their method only requires the error term to tend to zero uniformly in μ. This fact will be used to prove Theorem 1.2. The following theorem deals with the regularity of the distribution of the elements of a given subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ (where $n \geq 2$ is an integer) and is the key step to the generalization of the result of Duffin and Schaeffer.

Theorem 3.2. *Let μ be a positive real number, $n \geq 2$ be an integer and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Let G_n be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Denote by $\Psi_n(G_n)$ the cardinality of G_n (which is also the cardinality of aG_n) and by $d_n(G_n)$ the index of G_n in $(\mathbb{Z}/n\mathbb{Z})^\times$, that is,*

$$d_n(G_n) = \frac{|(\mathbb{Z}/n\mathbb{Z})^\times|}{|G_n|} = \frac{\varphi(n)}{\Psi_n(G_n)}.$$

Finally, for a real number $\mu > 0$ and an integer $n \geq 1$, let $\Psi_{\mu n}(aG_n)$ denote the number of positive integers k less than or equal to μn such that $k \in aG_n$. Then for any $\epsilon > 0$,

$$\Psi_{\mu n}(aG_n) = \Psi_n(G_n)\left(\mu + O\left(\frac{d_n(G_n)}{n^{1/2-\epsilon}}\right)\right).$$

Proof. The proof uses the Dirichlet characters introduced in Subsection 2.2 and some ideas which probably date back to the work of Erdős and Davenport [4] on character sums.

Let H_n be the quotient group of $(\mathbb{Z}/n\mathbb{Z})^\times$ by G_n. Any character χ over H_n may be extended to G_n by composing with the canonical homomorphism from G_n to H_n. Such a character will still be denoted by χ. Let $\hat{G}_{H_n}$ be the set of all characters over G_n arising from a character over H_n; it is readily seen that $\hat{G}_{H_n}$ is a subgroup of $\hat{G_n}$ of cardinality $|\hat{H}_n|$ (here the notation of Subsection 2.2 is kept).

Let $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ be the multiplicative inverse of $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. By Theorem 2.4, $|\hat{H}_n| = d_n(G_n)$ and the same theorem implies that

$$\Psi_{\mu n}(aG_n) = \frac{1}{d_n(G_n)} \sum_{k \in [\![1, \mu n]\!]} \sum_{\chi \in \hat{G}_{H_n}} \chi(\alpha k).$$

On inverting the order of summation, two contributions from the sum may be distinguished:

- One comes from the principal character and equals $\mathrm{Card}([\![1,\mu n]\!] \cap (\mathbb{Z}/n\mathbb{Z})^\times)$. Now, from Lemma 3.1,
$$\mathrm{Card}([\![1,\mu n]\!] \cap (\mathbb{Z}/n\mathbb{Z})^\times) = \varphi_\mu(n) = \varphi(n)\biggl(\mu + O\biggl(\frac{1}{n^{1-\epsilon}}\biggr)\biggr)$$
for any $\epsilon > 0$.
- The other comes from the $d_n(G_n)-1$ non-trivial characters and, by the Pólya–Vinogradov inequality (Theorem 2.5), each of them is bounded above in absolute value by $2\sqrt{n}\log n$.

Therefore, for any $\epsilon > 0$,
$$\Psi_{\mu n}(aG_n) = \frac{\varphi(n)}{d_n(G_n)}\biggl(\mu + O\biggl(\frac{1}{n^{1-\epsilon}}\biggr)\biggr) + \frac{d_n(G_n)-1}{d_n(G_n)} R_n(\mu),$$
where the remainder $R_n(\mu)$ satisfies $|R_n(\mu)| \le 2\sqrt{n}\log n$. Bearing in mind that $d_n(G_n) = \varphi(n)/\Psi_n(G_n)$ and that $\varphi(n) \ge n/2^{\omega(n)}$, Lemma 2.1 leads to the inequality
$$\biggl|\frac{R_n(\mu)}{\varphi(n)}\biggr| \le \frac{2\sqrt{n}\,2^{\omega(n)}\log n}{n} = O\biggl(\frac{1}{n^{1/2-\epsilon}}\biggr)$$
for any $\epsilon > 0$. This concludes the proof. ∎

The next result makes the link between Theorem 3.2 and Theorem 1.2 giving the repartition of the dth powers in a reduced system of residues modulo an integer. The notation of Theorem 3.2 is kept.

Corollary 3.3. *Let $n \ge 2$ and $a \ge 1$ be two coprime integers. Denote by $G_n^{(d)}$ the group of dth power residues in a reduced system of residues modulo n. Then for all $\epsilon > 0$,*
$$\Psi_{\mu n}(aG_n^{(d)}) = \Psi_n(G_n^{(d)})\biggl(\mu + O\biggl(\frac{1}{n^{1/2-\epsilon}}\biggr)\biggr),$$
where $\Psi_n(G_n^{(d)}) = r_d(n) = \varphi(n)/u_d(n)$ as defined in Proposition 2.3.

Proof. Keeping the notation of Theorem 3.2, first notice that $d_n(G_n^{(d)}) = u_d(n)$. Now, since the arithmetical function $u_d(n)$ is multiplicative (see Remark 2.2), Proposition 2.3 and Lemma 2.1 imply that
$$d_n(G_n^{(d)}) = u_d(n) \le (2d)^{\omega(n)} = O(n^\epsilon)$$
for any $\epsilon > 0$. The result then follows from Theorem 3.2. ∎

To prove Theorem 1.2, the following notation is convenient.

NOTATION. For any real number $x \in [0, 1/2)$ and any integer $k \geq 1$, let E_k^x denote the collection of intervals of the form

$$\left(\frac{p}{q_k^d} - \frac{x}{q_k^d}, \frac{p}{q_k^d} + \frac{x}{q_k^d}\right)$$

where $0 < p < q_k^d$ is an integer relatively prime to q_k and satisfying $p \equiv ab^d \pmod{q_k}$ for an integer b prime to q_k (with the notation of Corollary 3.3, this amounts to claiming that $p \in [\![0, q_k^d]\!]$ and $p \in aG_{q_k}^{(d)}$). Here and in what follows, the integer a is fixed and assumed to be relatively prime to q_k for all $k \geq 1$.

For simplicity, set furthermore $E_k := E_k^{\alpha_k}$ for all integers $k \geq 1$.

As mentioned in [16, p. 27], it is enough to consider the case where the sequence $(\alpha_k)_{k\geq 1}$ in Theorem 1.2 takes its values in the interval $[0, 1/2)$. This assumption can be dropped, but this leads to some additional complications which are not of interest.

With the notation of Corollary 3.3, E_k is the set in $(0, 1)$ consisting of

$$\Psi_{q_k^d}(aG_{q_k}^{(d)}) = \Psi_{q_k^d}(G_{q_k}^{(d)}) = \Psi_{q_k}(G_{q_k}^{(d)})q_k^{d-1} \tag{5}$$

open intervals each of length $2\alpha_k/q_k^d$ with centers at p/q_k^d, where p and q_k are integers satisfying the aforementioned constraints ($\Psi_{q_k^d}(aG_{q_k}^{(d)})$ is the number of integers $p \in [\![0, q_k^d]\!]$ such that $p \in aG_{q_k}^{(d)}$. From the fact that the integer a is coprime with q_k, it should be obvious that $\Psi_{q_k^d}(aG_{q_k}^{(d)}) = \Psi_{q_k^d}(G_{q_k}^{(d)})$).

If (s, t) is some interval in $(0, 1)$, an estimate of the measure of the set common to E_k and the interval (s, t) is needed. To that end, notice that, for any integer $n \geq 1$ and any real number $\mu > 0$, $\Psi_{\mu n^d}(aG_{q_k}^{(d)})$ counts the number of positive integers p less than or equal to μn^d such that $p \in aG_{q_k}^{(d)}$.

Let $k \geq 1$ be an integer. The number of intervals in E_k whose centers lie in (s, t) is exactly $\Psi_{tq_k^d}(aG_{q_k}^{(d)}) - \Psi_{sq_k^d}(aG_{q_k}^{(d)})$. From this it follows that at least $\Psi_{tq_k^d}(aG_{q_k}^{(d)}) - \Psi_{sq_k^d}(aG_{q_k}^{(d)}) - 2$ such intervals are entirely contained in (s, t) and at most $\Psi_{tq_k^d}(aG_{q_k}^{(d)}) - \Psi_{sq_k^d}(aG_{q_k}^{(d)}) + 2$ of them touch (s, t). Thus the measure of the set common to E_k and (s, t) is

$$\frac{2\alpha_k}{q_k^d}\big(\Psi_{tq_k^d}(aG_{q_k}^{(d)}) - \Psi_{sq_k^d}(aG_{q_k}^{(d)}) + \theta\big), \tag{6}$$

where $|\theta| \leq 2$.

However, since for any $\mu > 0$, $\lfloor \mu q_k^{d-1} \rfloor$ is the greatest integer m satisfying $mq_k \leq \mu q_k^d$, we get

$$\Psi_{\mu q_k^d}(aG_{q_k}^{(d)}) = \lfloor \mu q_k^{d-1} \rfloor \Psi_{q_k}(G_{q_k}^{(d)}) + \mathrm{Card}\{p \in [\![\lfloor \mu q_k^{d-1} \rfloor q_k, \mu q_k^d]\!] : p \in aG_{q_k}^{(d)}\}.$$

The second term on the right-hand side of this equation is $\Psi_{\nu q_k}(aG_{q_k}^{(d)})$, where

$$\nu := \frac{\mu q_k^d - \lfloor \mu q_k^{d-1} \rfloor q_k}{q_k} \in [0,1).$$

Therefore, from Corollary 3.3,

$$\begin{aligned}\Psi_{\mu q_k^d}(aG_{q_k}^{(d)}) &= \lfloor \mu q_k^{d-1} \rfloor \Psi_{q_k}(G_{q_k}^{(d)}) + \Psi_{\nu q_k}(aG_{q_k}^{(d)}) \\ &= \Psi_{q_k}(G_{q_k}^{(d)})\left(\lfloor \mu q_k^{d-1} \rfloor + \mu q_k^{d-1} - \lfloor \mu q_k^{d-1} \rfloor + O\left(\frac{1}{q_k^{1/2-\epsilon}}\right)\right) \\ &= \Psi_{q_k^d}(G_{q_k}^{(d)})\left(\mu + O\left(\frac{1}{q_k^{d-1/2-\epsilon}}\right)\right) \quad \text{for any } \epsilon > 0.\end{aligned}$$

Putting this into (6) and denoting by λ the one-dimensional Lebesgue measure, the measure of the set common to E_k and (s,t) is seen to be

$$\frac{2\alpha_k}{q_k^d}\Psi_{q_k^d}(G_{q_k}^{(d)})(t-s+\delta) = \lambda(E_k)(t-s)(1+\delta),$$

where $\delta \ll (q_k^{d-1/2-\epsilon}(t-s))^{-1}$ for any $\epsilon > 0$ (here, when a and b are real numbers, $a \ll b$ is the Vinogradov notation meaning that there exists a constant $c > 0$ such that $a \leq cb$).

Thus the following lemma has almost been proven.

LEMMA 3.4. *Let A be a subset of the unit interval $(0,1)$ consisting of a finite number of intervals. Then there exists a constant $c_A > 0$ which depends only on the set A such that for any integer $k \geq 1$,*

$$\lambda(A \cap E_k) \leq \lambda(A)\lambda(E_k)(1 + c_A \rho(q_k)),$$

where

$$\rho(q_k) = O\left(\frac{1}{q_k^{d-1/2-\epsilon}}\right) \quad \textit{for any } \epsilon > 0.$$

Proof. The lemma has been proven in the case where A is a single interval. The general case follows easily. See Lemma IV in [5]. ∎

All the tools necessary for the proof of Theorem 1.2 are now available. In fact, the proof has been reduced to that of the theorem of Duffin and Schaeffer, which may be found in [5, pp. 248–250]. In the latter, the reference to Lemma IV should be replaced by the reference to Lemma 3.4 above and inequalities (13) there should be read as follows:

> *By assumption, there are arbitrarily large integers n and m such that*
>
> $$\sum_{j=n}^{m} \alpha_j > 1 \quad \textit{and} \quad \sum_{j=n}^{m} \alpha_j s_d(q_k^d) > \frac{1}{2}c\sum_{j=n}^{m}\alpha_j,$$
>
> *where*
>
> $$s_d(q_k^d) = \Psi_{q_k^d}(G_k^{(d)})/q_k^d.$$

For the latter, see the definitions of $s_d(q)$ in (1), of $\Psi_{q_k}(G_k^{(d)})$ in Corollary 3.3 and of $\Psi_{q_k^d}(G_k^{(d)})$ in (5).

This concludes the proof of Theorem 1.2.

3.2. The proof of Theorem 1.3. In the course of the proof of Theorem 1.2, the main step was the proof of Theorem 3.2 and the fact that the subgroup $G_n^{(d)}$ of $(\mathbb{Z}/n\mathbb{Z})^\times$ was sufficiently large in the sense that, for some $\epsilon > 0$,

$$d_n(G_n^{(d)})/n^{1/2-\epsilon} \to 0$$

as n tends to infinity, with the notation of Corollary 3.3. Otherwise, no use whatsoever of any specific property of the group of dth powers in a reduced system of residues modulo n was made. Consequently, apart from some minor modifications due to the fact that, in Theorem 1.2, the denominators of the rational approximants are prescribed to be dth powers, the same proof as that provided for Theorem 1.2 demonstrates Theorem 1.3.

Remark 3.5. Condition (c) in Theorem 1.3 is derived from the fact that the Pólya–Vinogradov inequality (Theorem 2.5) gives $2\sqrt{n}\log n$ as an upper bound for the absolute value of the sum of values of a non-principal Dirichlet character to the modulus n and the fact that

$$\frac{2\sqrt{n}\,2^{\omega(n)}\log n}{n} = o\left(\frac{1}{n^{1/2-\epsilon}}\right)$$

for any $\epsilon > 0$ (see the proof of Theorem 3.2). Therefore, any improvement of the Pólya–Vinogradov inequality would lead to a condition weaker than (c). However, stated in this form, the exponent $1/2 - \epsilon$ for some $\epsilon > 0$ appearing in condition (c) cannot be improved if a general result is required: indeed, assuming the Riemann Hypothesis for L-functions (i.e. the Generalized Riemann Hypothesis), E. Bach [2] has shown that a sharper upper bound for the sum of values of a non-principal Dirichlet character to the modulus n was $2\sqrt{n}\log\log n$. Up to a constant, this is best possible since in 1932 Paley [14] proved that there exist infinitely many quadratic characters χ (i.e. characters of the form $\chi(n) = (\frac{n}{m})$ for some odd integer m, where $(\frac{n}{m})$ is the Jacobi symbol) with the property that there exists a constant $c > 0$ such that for some $N \in \mathbb{N}^*$,

$$\Big|\sum_{n=1}^{N} \chi(n)\Big| > c\sqrt{n}\log\log n.$$

Acknowledgements. The author would like to thank his PhD supervisor Detta Dickinson for suggesting the problem and for discussions which helped to develop ideas put forward. He is supported by the Science Foundation Ireland grant RFP11/MTH3084.

References

[1] F. Adiceam, *Vertical shift and simultaneous diophantine approximation on polynomial curves*, to appear.
[2] E. Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*, thesis, Univ. California, Berkeley, 1985.
[3] Y. Bugeaud, *Approximation by Algebraic Numbers*, Cambridge Tracts in Math. 160, Cambridge Univ. Press, 2004.
[4] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math., Debrecen 2 (1953), 252–265.
[5] R. J. Duffin and A. C. Schaeffer, *Khintchine's problem in metric Diophantine approximation*, Duke Math. J. 8 (1941), 243–255.
[6] W. J. Ellison and M. Mendès France, *Les nombres premiers*, Actualités Sci. Industr. 1366, Hermann, Paris, 1975.
[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, 1960.
[8] G. Harman, *Metric Diophantine approximation with two restricted variables I: Two square-free integers, or integers in arithmetic progressions*, Math. Proc. Cambridge Philos. Soc. 103 (1988), 197–206.
[9] G. Harman, *Metric Diophantine approximation with two restricted variables II: A prime and a square-free integer*, Mathematika 35 (1988), 59–68.
[10] G. Harman, *Metric Diophantine approximation with two restricted variables III: Two prime numbers*, J. Number Theory 29 (1988), 364–375.
[11] G. Harman, *Metric Diophantine approximation with two restricted variables IV: Miscellaneous results*, Acta Arith. 53 (1989), 207–216.
[12] A. Haynes, A. Pollington, and S. Velani, *The Duffin–Schaeffer conjecture with extra divergence*, Math. Ann. 353 (2012), 259–273.
[13] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I: Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge Univ. Press, 2007.
[14] R. E. A. C. Paley, *A theorem of characters*, J. London Math. Soc. 7 (1932), 28–32.
[15] A. D. Pollington and R. C. Vaughan, *The k-dimensional Duffin and Schaeffer conjecture*, Mathematika 37 (1990), 190–200.
[16] V. G. Sprindžuk, *Metric Theory of Diophantine Approximations*, Winston, 1979.
[17] I. M. Vinogradov, *Elements of Number Theory*, Dover Publ., New York, 1954.

Faustin Adiceam
Department of Mathematics
National University of Ireland at Maynooth
Maynooth, Co. Kildare, Ireland
E-mail: faustin.adiceam@maths.nuim.ie

Received on 10.8.2012
and in revised form on 16.12.2013 (7161)