Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 1182–1194
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Approximating reals by sums of two rationals

Tsz Ho Chan

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA

Received 7 December 2006; revised 8 April 2007
Available online 10 October 2007
Communicated by R.C. Vaughan

Abstract

We generalize Dirichlet's diophantine approximation theorem to approximating any real number α by a sum of two rational numbers $\frac{a_1}{q_1} + \frac{a_2}{q_2}$ with denominators $1 \leqslant q_1, q_2 \leqslant N$. This turns out to be related to the congruence equation problem $xy \equiv c \pmod{q}$ with $1 \leqslant x, y \leqslant q^{1/2+\epsilon}$.

Keywords: Diophantine approximation; Character sum; Exponential sum; Erdős–Turán inequality

1. Introduction

Dirichlet's theorem on rational approximation says

Theorem 1. *For any real number α and real number $N \geqslant 1$, there exist integers $1 \leqslant q \leqslant N$ and a such that*

$$\left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qN}. \tag{1}$$

While studying almost squares (see [4]), the author accidentally consider the question of approximating α by a sum of two rational numbers:

E-mail address: tchan@memphis.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.06.011

Question 1. Find a good upper bound for

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \tag{2}$$

with integers a_1, a_2 and $1 \leqslant q_1, q_2 \leqslant N$.

(This turns out to be unfruitful towards the study of almost squares.) One can continue further with approximating α by a sum of $n > 2$ rational numbers. We shall study this in another paper. These seem to be some new questions in diophantine approximation.

However, if one combines the two fractions in (2), it becomes

$$\left|\alpha - \frac{b}{q_1 q_2}\right|$$

with integers b and $1 \leqslant q_1, q_2 \leqslant N$. This looks like the left-hand side of (1) except that we require the denominator q to be of a special form, namely $q = q_1 q_2$ with $1 \leqslant q_1, q_2 \leqslant N$. In this light, our Question 1 is not so new after all. People have studied diophantine approximation where the denominator q is of some special form. For example,

(1) When q is a perfect square, see Zaharescu [11] with some history of the problem.
(2) When q is squarefree, see Harman [6], Balog and Perelli [3], Heath-Brown [7].
(3) When q is prime, see Heath-Brown and Jia [8] with some history of the problem.
(4) When q is B-free, see Alkan, Harman and Zaharescu [1].

Techniques from exponential sum, character sum, sieve method, and geometry of numbers were used in the above list of works. In this paper, we shall use exponential sum and character sum methods to study Question 1. It would be interesting to see if other methods can be applied. One distinct feature of our results (see next section) is that the upper bounds of (2) depend on single rational approximations $\frac{a}{q}$ of the real number α given by Dirichlet's theorem. Alternatively, we try to see how approximation by a sum of two rationals compares with single rational approximation.

The starting point of the argument is

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \leqslant \left|\alpha - \frac{a}{q}\right| + \left|\frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \tag{3}$$

by triangle inequality. The first term on the right-hand side of (3) is small by Dirichlet's theorem. Thus, it remains to obtain a good upper bound for the second term on the right-hand side of (3) (i.e. we can restrict Question 1 to rational α). By combining denominators and letting $b = a_1 q_2 + a_2 q_1$,

$$\left|\frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| = \frac{|a q_1 q_2 - b q|}{q q_1 q_2}.$$

Our goal is trying to make the numerator as small as possible, say $a q_1 q_2 - b q = r$ where $r > 0$ is small. Transforming this into a congruence equation (mod q), we have

$$q_1 q_2 \equiv r \bar{a} \pmod{q} \tag{4}$$

with $1 \leqslant q_1, q_2 \leqslant N$ where $a\bar{a} \equiv 1 \pmod{q}$. This gives some indication why Question 1 is related to the congruence equation problem stated in the abstract. Ideally, we want to solve (4) with $r = 1$. This seems too hard. So, we take advantage of allowing r to run over a short interval which gives Theorems 9–11 in the next section. We will also prove an almost all result, namely Theorem 8, towards Conjecture 4.

Throughout the paper, ϵ denotes a small positive number. Both $f(x) = O(g(x))$ and $f(x) \ll g(x)$ mean that $|f(x)| \leqslant Cg(x)$ for some constant $C > 0$. Moreover $f(x) = O_\lambda(g(x))$ and $f(x) \ll_\lambda g(x)$ mean that the implicit constant $C = C_\lambda$ may depend on the parameter λ. Also $\phi(n)$ is Euler's phi function and $d(n)$ is the number of divisors of n. Finally $|\mathcal{S}|$ stands for the cardinality of the set $\mathcal{S}$.

2. Some conjectures and results

By imitating Dirichlet's theorem, one might conjecture that there exist integers a_1, a_2, $1 \leqslant q_1, q_2 \leqslant N$ such that

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll \frac{1}{q_1 q_2 N^2}$$

as the two fractions combine to give a single fraction with denominator $q_1 q_2 \leqslant N^2$. However, this is very wrong as illustrated by the following example:

Let $\alpha = \frac{a}{p}$ for some prime number p with $N < p \leqslant 2N$ (guaranteed to exist by Bertrand's postulate) and integer a with $(a, p) = 1$. Then

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| = \left|\frac{a}{p} - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \geqslant \frac{1}{p q_1 q_2} \gg \frac{1}{q_1 q_2 N}. \tag{5}$$

So, the best upper bound one can hope for is

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll \frac{1}{q_1 q_2 N} \tag{6}$$

for some integers a_1, a_2, $1 \leqslant q_1, q_2 \leqslant N$. This follows directly from Theorem 1 by simply choosing $\frac{a_2}{q_2} = \frac{0}{1}$. On the other hand, one can easily get the bound

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll \frac{1}{N^2}. \tag{7}$$

For example, fix q_1 and q_2 to be two distinct primes in the interval $[N/4, N]$ (without loss of generality, we may assume $N \geqslant 12$), and consider the fractions $\frac{k}{q_1 q_2}$ with $(k, q_1 q_2) = 1$. Since one of k, $k+1$ or $k+2$ is not divisible by neither q_1 nor q_2, the distance between successive fractions is $\leqslant \frac{3}{q_1 q_2} \ll \frac{1}{N^2}$. Interpolating between (6) and (7), we make the following

Conjecture 2. *Let* $0 \leqslant \beta \leqslant 1$. *For any real number* α *and real number* $N \geqslant 1$, *there exist integers* $1 \leqslant q_1, q_2 \leqslant N$ *and* a_1, a_2 *such that*

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \leqslant \frac{1}{(q_1 q_2)^\beta N^{2-\beta}}.$$

From the above discussion, Conjecture 2 is true when $\beta = 0$ or 1. We leave the cases $0 < \beta < 1$ to the readers as a challenging open problem. In another direction, as shown by the example in (5), the approximation of a real number by a sum of two rationals depends on the rational approximation of α by a single rational number. Thus, we come up with

Conjecture 3. *For any small $\epsilon > 0$ and any $N \geqslant 1$, suppose α has a rational approximation $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^2}$ for some integers a, $1 \leqslant q \leqslant N^2$ and $(a, q) = 1$. Then*

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll_\epsilon \frac{1}{qN^{2-\epsilon}}$$

for some integers a_1, a_2, $1 \leqslant q_1, q_2 \leqslant N$. Note: We may restrict our attention to $q > N$ in the above rational approximation of α, for otherwise we can just pick $\frac{a_1}{q_1} = \frac{a}{q}$ and $\frac{a_2}{q_2} = \frac{0}{1}$.

Roughly speaking, this means that if one can approximate a real number well by a rational number, then one should be able to approximate it by a sum of two rational numbers nearly as well. Note that the example in (5) shows that this conjecture is best possible (apart from ϵ). As indicated in the Introduction, Conjecture 3 is related to a conjecture on congruence equation:

Conjecture 4. *Let ϵ be any small positive real number. For any positive integer q and integer c with $(c, q) = 1$, the equation*

$$xy \equiv c \pmod q$$

has solutions in $1 \leqslant x, y \ll_\epsilon q^{1/2+\epsilon}$.

We consider the following variation.

Conjecture 5. *Let $1/2 < \theta \leqslant 1$. There is a constant C_θ such that, for any positive integer q and integer c with $(c, q) = 1$, the equation*

$$xy \equiv c \pmod q$$

has solutions in $C_\theta N \leqslant x, y \leqslant 2C_\theta N$ with $(x, y) = 1$ for every $N \geqslant q^\theta$.

Assume Conjecture 5 for some $1/2 < \theta \leqslant 1$. Let $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^{1/\theta}}$ with $(a, q) = 1$ and $N < q \leqslant N^{1/\theta}$. Then, by Conjecture 5, there are C_θ, q_1, q_2 such that $C_\theta N \leqslant q_1, q_2 \leqslant 2C_\theta N$ and $q_1 q_2 \equiv \bar{a} \pmod q$ (because $q^\theta \leqslant N$). Here $\bar{a}$ denotes the multiplicative inverse of a modulo q. In particular, we have $aq_1q_2 \equiv 1 \pmod q$. So, $aq_1q_2 = kq + 1$ for some integer k. This gives $aq_1q_2 - kq = 1$ and

$$\left|\frac{a}{q} - \frac{k}{q_1 q_2}\right| = \frac{1}{qq_1q_2} \ll_\theta \frac{1}{qN^2}.$$

Since $(q_1, q_2) = 1$, the fraction $\frac{k}{q_1 q_2} = \frac{a_1}{q_1} + \frac{a_2}{q_2}$ for some integers a_1, a_2. Hence

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \leqslant \left|\alpha - \frac{a}{q}\right| + \left|\frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll_\theta \frac{1}{qN^{1/\theta}}.$$

Thus, if Conjecture 5 is true with $\theta = \frac{1}{2} + \epsilon$ for any small $\epsilon > 0$, then we have Conjecture 3. From Igor Shparlinski (see [9]), the author learns that Conjecture 5 is true for $\theta > \frac{3}{4}$.

Recently, M.Z. Garaev and A.A. Karatsuba [5] proved that

Theorem 6. *Let $\Delta = \Delta(m) \to \infty$ as $m \to \infty$. Then the set*

$$\left\{xy \pmod m\colon\ 1 \leqslant x \leqslant m^{1/2},\ S+1 \leqslant y \leqslant S + \Delta m^{1/2}\sqrt{\frac{m}{\phi(m)}}\log m\right\}$$

contains $(1 + O(\Delta^{-1}))m$ residue classes modulo m.

One can think of this as an almost all result towards Conjecture 4. With slight modification, one can get

Theorem 7. *Let $\Delta = \Delta(m) \to \infty$ as $m \to \infty$. For any small $\epsilon > 0$ and $m^{1/(2-\epsilon)} \leqslant N \leqslant m$, the set*

$$\left\{xy \pmod m\colon\ \frac{N}{4} \leqslant x \leqslant N,\ S+1 \leqslant y \leqslant S + \Delta m^{1/2}\sqrt{\frac{m}{\phi(m)}}\log m,\ (x, y) = 1\right\}$$

contains $(1 + O_\epsilon(\Delta^{-1}) + O_\epsilon(\frac{\Delta}{\log m}\sqrt{\frac{m}{\phi(m)}}))m$ residue classes modulo m.

Using Theorem 7, we can prove an almost all result towards Conjecture 3.

Theorem 8. *Let N be a positive integer. For any small $\epsilon > 0$, Conjecture 3 is true for all $0 \leqslant \alpha < 1$ except a measure of $O_\epsilon(\frac{1}{\sqrt{\log N}})$.*

Instead of an almost all result, one may try to prove Conjecture 3 with a bigger uniform upper bound. Inspired by a recent paper of Alkan, Harman and Zaharescu [1], a variant of the Erdős–Turán inequality gives

Theorem 9. *For any $\epsilon > 0$ and any $N \geqslant 1$, suppose α has a rational approximation $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^{5/4}}$ for some integers a, $1 \leqslant q \leqslant N^{5/4}$ and $(a, q) = 1$. Then*

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll_\epsilon \frac{1}{qN^{5/4-\epsilon}} \tag{8}$$

for some integers a_1, a_2, and prime numbers $1 \leqslant q_1 < q_2 \leqslant N$.

By a slight modification of the proof of Theorem 9, we have

Theorem 10. *For any $\epsilon > 0$ and any $N \geqslant 1$, suppose α has a rational approximation $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^{3/2}}$ for some integers a, $1 \leqslant q \leqslant N^{3/2}$ and $(a, q) = 1$. Then*

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll_\epsilon \frac{1}{qN^{3/2-\epsilon}} \tag{9}$$

for some integers a_1, a_2, $1 \leqslant q_1, q_2 \leqslant N$.

Conditionally, we have

Theorem 11. *Assume the Generalized Lindelöf Hypothesis. For any* $\epsilon > 0$ *and any* $N \geqslant 1$, *suppose* α *has a rational approximation* $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^{4/3}}$ *for some integers* a, $1 \leqslant q \leqslant N^{4/3}$ *and* $(a,q) = 1$. *Then*

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll_\epsilon \frac{1}{qN^{4/3-\epsilon}} \tag{10}$$

for some integers a_1, a_2, *and prime numbers* $1 \leqslant q_1 < q_2 \leqslant N$.

This is proved by a character sum method. Of course, the goal is trying to push the exponent of N in (8)–(10) to $2 - \epsilon$. Moreover, one may guess that Conjecture 3 is true even restricting q_1 and q_2 to prime numbers.

The paper is organized as follow. We first prove the almost all results, Theorems 7 and 8, in Section 3. Then we prove Theorems 9 and 10 in Sections 4 and 5, respectively. Finally, we prove Theorem 11 in the last section.

3. Almost all results: Theorems 7 and 8

First, we use Theorem 7 to prove Theorem 8.

Proof of Theorem 8. Consider $1 \leqslant q \leqslant N^{2-\epsilon}$, $0 \leqslant a \leqslant q$ with $(a,q) = 1$, and the intervals $I_{a,q} = \{\alpha\colon |\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^{2-\epsilon}}\}$. By Theorem 1, $I_{a,q}$'s cover the interval [0, 1]. From the note in Conjecture 3, we may restrict our attention to $q > N$.

We call $I_{a,q}$ good if there exist $\frac{N}{4} \leqslant q_1, q_2 \leqslant N$ with $(q_1, q_2) = 1$ such that $q_1 q_2 \equiv \bar{a} \pmod{q}$. Otherwise, we call $I_{a,q}$ bad. By Theorem 7, for a fixed q, there are at most

$$\left(O_\epsilon\left(\Delta^{-1}\right) + O_\epsilon\left(\frac{\Delta}{\log q}\sqrt{\frac{q}{\phi(q)}}\right)\right)q = O\left(\frac{q}{\sqrt{\log q}}\left(\frac{q}{\phi(q)}\right)^{1/4}\right) \tag{11}$$

bad $I_{a,q}$'s by choosing $\Delta = \sqrt{\log q}\,(\frac{\phi(q)}{q})^{1/4}$. For good $I_{a,q}$'s, we have $aq_1q_2 - bq = 1$ for some integer b, which gives

$$\left|\frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| = \left|\frac{a}{q} - \frac{b}{q_1q_2}\right| = \frac{1}{qq_1q_2} \ll \frac{1}{qN^2}$$

for some integers a_1, a_2 as $(q_1, q_2) = 1$. Therefore, for α in good $I_{a,q}$, there exist $\frac{N}{4} \leqslant q_1, q_2 \leqslant N$ and integers a_1, a_2 such that

$$\left|\alpha - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \leqslant \left|\alpha - \frac{a}{q}\right| + \left|\frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2}\right| \ll_\epsilon \frac{1}{qN^{2-\epsilon}}. \tag{12}$$

Consequently by (11), (12) holds for all but a measure

$$\ll_\epsilon \sum_{N<q\leqslant N^{2-\epsilon}} \frac{q}{\sqrt{\log q}}\left(\frac{q}{\phi(q)}\right)^{1/4} \times \frac{1}{qN^{2-\epsilon}} \ll \frac{1}{\sqrt{\log N}}$$

of α in bad $I_{a,q}$'s. Here we use $\sum_{n\leqslant x}(\frac{n}{\phi(n)})^{1/4} \leqslant \sum_{n\leqslant x}\frac{n}{\phi(n)} \ll x$. □

The proof of Theorem 7 is almost the same as Theorem 6 of [5]. So we will give the main points only. The main modification is the set $\mathcal{V}$ to which we want it to resemble the set of primes $\leqslant m^{1/2}$ (the choice in [5]) but each element has size $\approx N$.

Sketch of proof of Theorem 7. Suppose $N \leqslant m \leqslant N^{2-\epsilon}$. Let $I = [N/4, N]$ and $I_k := (\frac{m^{1/2}}{2^k}, \frac{m^{1/2}}{2^{k-1}}]$ for $k = 1, 2, 3, \ldots$. Then $aI_k \subset I$ for $\frac{N2^k}{4m^{1/2}} < a \leqslant \frac{N2^k}{2m^{1/2}}$. Note that $\frac{N}{m^{1/2}} \geqslant N^{\epsilon/2}$. By Bertrand's postulate, there is a prime p_k with $\frac{N2^k}{4m^{1/2}} < p_k \leqslant \frac{N2^k}{2m^{1/2}}$ and $p_k I_k \subset I$. Now, one of $p_1, p_2, \ldots, p_{[4/\epsilon]+1}$ must be relatively prime to m. For otherwise $p_1 p_2 \ldots p_{[4/\epsilon]+1}$ divides m which implies $(\frac{N^{\epsilon/2}}{2})^{[4/\epsilon]+1} \leqslant m \leqslant N^{2-\epsilon}$. This is impossible for sufficiently large N.

Therefore, say for some $1 \leqslant K \leqslant [4/\epsilon] + 1$, p_K is relatively prime to m. We define $\mathcal{V} := \{p_K p\colon\ p \text{ is a prime in } (\frac{m^{1/2}}{2^K}, \frac{m^{1/2}}{2^{K-1}}],\ (p, m) = 1\}$. Clearly $\mathcal{V} \subset [N/4, N]$ and $|\mathcal{V}| \gg_\epsilon \frac{m^{1/2}}{\log m}$ as m is divisible by at most two different primes in the interval $(\frac{m^{1/2}}{2^K}, \frac{m^{1/2}}{2^{K-1}}]$. Using this $\mathcal{V}$ in the proof of Theorem 6 of [5], one can get that the set

$$S = \left\{xy \pmod m\colon\ x \in \mathcal{V},\ S+1 \leqslant y \leqslant S + \Delta m^{1/2}\sqrt{\frac{m}{\phi(m)}}\log m\right\}$$

contains $(1 + O_\epsilon(\Delta^{-1}))m$ residue classes modulo m. Now, we want to add the requirement $(x, y) = 1$ by dropping some residue classes. We are going to exclude those y's that are divisible by p_K or $p \in (\frac{m^{1/2}}{2^K}, \frac{m^{1/2}}{2^{K-1}}]$. For p_K, we exclude $O(\Delta m^{1/2-\epsilon}\sqrt{\frac{m}{\phi(m)}}\log m)$ y's as $p_K \gg N^{\epsilon/2}$. For each p, we exclude $O_\epsilon(\Delta\sqrt{\frac{m}{\phi(m)}}\log m)$ y's. So, in total, we exclude $O_\epsilon(\Delta m^{1/2}\sqrt{\frac{m}{\phi(m)}})$ y's. Therefore, we need to exclude at most $O_\epsilon(\Delta\frac{m}{\log m}\sqrt{\frac{m}{\phi(m)}})$ residue classes from S to ensure $(x, y) = 1$ and we have Theorem 7. □

4. Erdős–Turán inequality: Theorem 9

First, we recall a variant of Erdős–Turán inequality on uniform distribution (see, for example, R.C. Baker [2, Theorem 2.2]).

Lemma 12. *Let L and J be positive integers. Suppose that $\|x_j\| \geqslant \frac{1}{L}$ for $j = 1, 2, \ldots, J$. Then*

$$\sum_{l=1}^{L}\left|\sum_{j=1}^{J} e(lx_j)\right| > \frac{J}{6}.$$

Here $\|x\| = \min_{n\in\mathbb{Z}}|x - n|$, the distance from x to the nearest integer, and $e(x) = e^{2\pi i x}$.

Proof of Theorem 9. Let $\epsilon > 0$, $N \geqslant 1$ and $1+\epsilon \leqslant \phi \leqslant 2$. Suppose α has a rational approximation $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^\phi}$ for some integers a, $N^{2-\phi+\epsilon} \leqslant q \leqslant N^\phi$ and $(a,q)=1$ (Note: The situation when $q < N^{2-\phi+\epsilon}$ is trivial as one can simply pick any two distinct primes q_1, q_2 in the interval $[N/4, N]$ and successive fractions with denominator q_1q_2 has spacing $O(\frac{1}{N^2}) = O(\frac{1}{qN^{2-\epsilon}})$). We try to find integers k and distinct prime numbers $q_1, q_2 \in \mathcal{P}$ (the set of prime numbers in the interval $[N/2, N]$) such that

$$\left|\frac{a}{q} - \frac{k}{q_1q_2}\right| < \frac{1}{qN^{\phi-\epsilon}} \quad \text{or} \quad \left\|\frac{q_1q_2a}{q}\right\| < \frac{1}{qN^{\phi-2-\epsilon}}.$$

In view of the above lemma, to prove Theorem 9, it suffices to show

$$\sum_{l=1}^{L}\left|\sum_{\substack{q_1,q_2\in\mathcal{P}\\ q_1\neq q_2}} e\left(\frac{lq_1q_2a}{q}\right)\right| \leqslant \frac{1}{6}\big(|\mathcal{P}|^2 - |\mathcal{P}|\big)$$

with $L := [qN^{\phi-2-\epsilon}]+1$. By triangle inequality, it suffices to show

$$S_1 + S_2 := \sum_{l=1}^{L}\left|\sum_{q_1,q_2\in\mathcal{P}} e\left(\frac{lq_1q_2a}{q}\right)\right| + \sum_{l=1}^{L}\left|\sum_{q_1\in\mathcal{P}} e\left(\frac{lq_1^2a}{q}\right)\right| \leqslant \frac{1}{7}|\mathcal{P}|^2 \tag{13}$$

for N sufficiently large. Note that $1 \leqslant L \leqslant q$ as $1+\epsilon \leqslant \phi \leqslant 2$. By Cauchy–Schwarz inequality and orthogonality of $e(x)$,

$$\begin{aligned} S_2^2 &\leqslant \left(\sum_{l=1}^{L} 1\right)\left(\sum_{l=1}^{L}\left|\sum_{q_1\in\mathcal{P}} e\left(\frac{lq_1^2a}{q}\right)\right|^2\right) \leqslant L\left(\sum_{l=1}^{q}\left|\sum_{q_1\in\mathcal{P}} e\left(\frac{lq_1^2a}{q}\right)\right|^2\right) \\ &= Lq \sum_{q_1\in\mathcal{P}} \sum_{\substack{q_2\in\mathcal{P}\\ q_2^2\equiv q_1^2 \pmod q}} 1 \ll \begin{cases} Lqd(q)N & \text{if } q > N, \\ Ld(q)N^2 & \text{if } q \leqslant N \end{cases} \end{aligned}$$

because $(q_1,q) = 1 = (q_2,q)$, and $n^2 \equiv b \pmod q$ has $O(2^{\omega(q)}) = O(d(q))$ solutions for n when $(b,q)=1$. Here $\omega(q)$ denotes the number of distinct prime divisors of q. Therefore as $L = [qN^{\phi-2-\epsilon}]+1$ and $q \leqslant N^\phi$,

$$\begin{aligned} S_2 &\ll \begin{cases} qN^{\phi/2-1/2-\epsilon/2}d(q)^{1/2} & \text{if } q > N, \\ q^{1/2}N^{\phi/2-\epsilon/2}d(q)^{1/2} & \text{if } q \leqslant N \end{cases} \\ &\ll d(q)^{1/2}\max\big(N^{3\phi/2-1/2-\epsilon/2}, N^{\phi/2+1/2-\epsilon/2}\big). \end{aligned}$$

By Chebychev's estimate or the prime number theorem, and $d(q) \ll_\epsilon q^{\epsilon/4} \leqslant N^{\epsilon/2}$, one can check that $S_2 \leqslant \frac{1}{14}|\mathcal{P}|^2$ when $\phi \leqslant 5/3$ and N is sufficiently large depending on ϵ.

It remains to deal with S_1. Our approach is inspired by Vinogradov's work [10]. Write

$$d_r = \sum_{\substack{l \leqslant L,\, q_1 \in \mathcal{P} \\ lq_1 = r}} 1.$$

Since $l \leqslant L \leqslant qN^{\phi-2-\epsilon} + 1 \leqslant N^{2\phi-2-\epsilon} + 1 \leqslant N^{2-\epsilon} + 1 \ll N^2$, we need to consider $r \leqslant LN \ll N^3$. But then r is divisible by at most three $q_1 \in \mathcal{P}$. Thus $d_r \leqslant 3$. Then

$$S_1 \leqslant \sum_{r=1}^{LN} d_r \left| \sum_{q_2 \in \mathcal{P}} e\left(\frac{rq_2 a}{q}\right) \right|. \tag{14}$$

By Cauchy–Schwarz inequality and orthogonality of $e(x)$,

$$\begin{aligned} S_1^2 &\leqslant \left(\sum_{r=1}^{LN} d_r^2\right)\left(\sum_{r=1}^{LN}\left|\sum_{q_2 \in \mathcal{P}} e\left(\frac{rq_2 a}{q}\right)\right|^2\right) \leqslant 9LN \sum_{r=1}^{q([LN/q]+1)} \left|\sum_{q_2 \in \mathcal{P}} e\left(\frac{rq_2 a}{q}\right)\right|^2 \\ &= 9LN\left(\left[\frac{LN}{q}\right]+1\right) q \sum_{q_1 \in \mathcal{P}} \sum_{\substack{q_2 \in \mathcal{P} \\ q_2 \equiv q_1 \pmod{q}}} 1 \\ &\leqslant 9LN\left(\left[\frac{LN}{q}\right]+1\right) q \sum_{N/2 \leqslant q_1 \leqslant N} \sum_{\substack{N/2 \leqslant q_2 \leqslant N \\ q_2 \equiv q_1 \pmod{q}}} 1 \ll \begin{cases} (LN)^2 N & \text{if } q > N, \\ (LN)^2 \frac{N^2}{q} & \text{if } q \leqslant N \end{cases} \end{aligned}$$

as $LN \geqslant qN^{\phi-1-\epsilon} \geqslant q$. Therefore as $L = [qN^{\phi-2-\epsilon}] + 1$ and $q \leqslant N^{\phi}$,

$$S_1 \ll \begin{cases} qN^{\phi-1/2-\epsilon} & \text{if } q > N \\ q^{1/2} N^{\phi-\epsilon} & \text{if } q \leqslant N \end{cases} \ll \max\bigl(N^{2\phi-1/2-\epsilon}, N^{\phi+1/2-\epsilon}\bigr).$$

By Chebychev's estimate or the prime number theorem, one can check that $S_1 \leqslant \frac{1}{14}|\mathcal{P}|^2$ when $\phi \leqslant 5/4$ and N is sufficiently large depending on ϵ. Consequently, we have (13) as long as $\phi \leqslant 5/4$ and N sufficiently large. We set $\phi = 5/4$.

By the contrapositive of Lemma 12, there exist distinct prime numbers $q_1, q_2 \in \mathcal{P}$ such that $\|\frac{q_1 q_2 a}{q}\| < \frac{1}{qN^{5/4-2-\epsilon}}$ for sufficiently large N. In other words $|\frac{a}{q} - \frac{k}{q_1 q_2}| \ll_\epsilon \frac{1}{qN^{5/4-\epsilon}}$ for some integer k. Hence

$$\left|\alpha - \frac{k}{q_1 q_2}\right| \leqslant \left|\alpha - \frac{a}{q}\right| + \left|\frac{a}{q} - \frac{k}{q_1 q_2}\right| \ll_\epsilon \frac{1}{qN^{5/4-\epsilon}}$$

which gives Theorem 9 as $(q_1, q_2) = 1$ and we can write $k = a_1 q_2 + a_2 q_1$ for some integers a_1, a_2. $\square$

5. Theorem 10

The proof of Theorem 10 is almost the same as Theorem 9. We shall be content to indicate the necessary modifications.

Proof of Theorem 10. Without loss of generality, we can assume $q > N$ as indicated in the note of Conjecture 3. The starting point is almost the same as that of Theorem 9. The difference is that we want $q_1 \in \mathcal{P}$ but any integer $q_2 \in [N/2, N]$ with $(q_1, q_2) = 1$. Equivalently we need $q_2 \neq q_1$ since q_1 is a prime in $[N/2, N]$. Instead of (13), it suffices to show

$$S_1 + S_2 := \sum_{l=1}^{L} \left| \sum_{q_1 \in \mathcal{P}} \sum_{N/2 \leqslant q_2 \leqslant N} e\left(\frac{l q_1 q_2 a}{q}\right) \right| + \sum_{l=1}^{L} \left| \sum_{q_1 \in \mathcal{P}} e\left(\frac{l q_1^2 a}{q}\right) \right| \leqslant \frac{1}{7} |\mathcal{P}|^2. \tag{15}$$

Now S_2 is treated the same way as in Theorem 9. So $S_2 \leqslant \frac{1}{14}|\mathcal{P}|^2$ when $\phi \leqslant 5/3$ and N is sufficiently large depending on ϵ.

As for S_1, instead of (14), we have

$$S_1 \leqslant \sum_{r=1}^{q([LN/q]+1)} d_r \left| \sum_{N/2 \leqslant q_2 \leqslant N} e\left(\frac{r q_2 a}{q}\right) \right| \ll \frac{LN}{q} \sum_{r=1}^{q} \left| \sum_{N/2 \leqslant q_2 \leqslant N} e\left(\frac{r q_2}{q}\right) \right|$$

as $(a, q) = 1$. Now summing according to the greatest common divisor $d = (r, q)$,

$$S_1 \ll \frac{LN}{q} \sum_{d|q} \sum_{\substack{r' \leqslant q/d \\ (r', q/d)=1}} \left| \sum_{N/2 \leqslant q_2 \leqslant N} e\left(\frac{r' q_2}{q/d}\right) \right| \leqslant \frac{LN}{q} \sum_{d|q} \sum_{r' \leqslant q/d} \min\left(N, \frac{1}{\| \frac{r'}{q/d} \|}\right)$$

$$\ll \frac{LN}{q} \sum_{\substack{d|q \\ d<N}} \left(\sum_{r' \leqslant q/N} N + \sum_{q/N < r' \leqslant q/d} \frac{q/d}{r'} \right) + \frac{LN}{q} \sum_{\substack{d|q \\ d \geqslant N}} \sum_{r' \leqslant q/d} N \ll LN d(q) \log q.$$

Recall $L = [q N^{\phi - 2 - \epsilon}] + 1$ and $q \leqslant N^{\phi}$, thus $S_1 \leqslant \frac{1}{14}|\mathcal{P}|^2$ as long as $\phi \leqslant 3/2 < 5/3$. This proves Theorem 10. □

6. Character sum method: Theorem 11

First let us prove a simple lemma which is needed at the end of the proof of Theorem 11.

Lemma 13. *Let q be a positive integer and $B \geqslant 1$ be any real number. Then the number of integers between 1 and B relatively prime to q is $B\frac{\phi(q)}{q} + O(d(q))$.*

Proof. Using properties of Möbius function $\mu(n)$, the number of integers between 1 and B relatively prime to q is

$$\sum_{\substack{1 \leqslant n \leqslant B \\ (n,q)=1}} 1 = \sum_{1 \leqslant n \leqslant B} \sum_{\substack{d|n \\ d|q}} \mu(d) = \sum_{\substack{1 \leqslant d \leqslant B \\ d|q}} \mu(d) \sum_{\substack{1 \leqslant n \leqslant B \\ d|n}} 1 = \sum_{\substack{1 \leqslant d \leqslant B \\ d|q}} \mu(d) \left(\frac{B}{d} + O(1) \right)$$

$$= B\sum_{d|q}\frac{\mu(d)}{d} + O\Bigg(B\sum_{\substack{d>B\\ d|q}}\frac{\mu(d)}{d}\Bigg) + O\big(d(q)\big) = B\frac{\phi(q)}{q} + O\big(d(q)\big). \qquad \square$$

Proof of Theorem 11. Let $\epsilon > 0$, $N \geqslant 1$ and $1+\epsilon \leqslant \phi \leqslant 2-2\epsilon$. Without loss of generality, we may assume N is sufficient large. Suppose α has a rational approximation $|\alpha - \frac{a}{q}| \leqslant \frac{1}{qN^\phi}$ for some integers a, $N^{2-\phi-\epsilon} < q \leqslant N^\phi$ and $(a,q)=1$ (the case $q \leqslant N^{2-\phi-\epsilon}$ is trivial as indicated in the proof of Theorem 9). We will try to find integer k and distinct prime numbers $N/2 \leqslant q_1, q_2 \leqslant N$ such that $|\frac{a}{q} - \frac{k}{q_1q_2}|$ is small. This is equivalent to $|aq_1q_2 - kq|$ being small which leads us to consider

$$aq_1q_2 \equiv b \pmod q \tag{16}$$

with distinct $q_1, q_2 \in \mathcal{P}$, the set of primes in the interval $[N/2, N]$ that are relatively prime to q, and $b \in \mathcal{B}$, the set of integers in the interval $[1, B]$ with $B \leqslant q$ to be chosen later.

Let χ denote a typical Dirichlet character modulo q. By orthogonality of characters, the number of solution to (16) is

$$\# = \frac{1}{\phi(q)}\sum_{\chi}\sum_{\substack{q_1,q_2\in\mathcal{P}\\ q_1\neq q_2}}\sum_{b\in\mathcal{B}}\chi(aq_1q_2)\overline{\chi}(b) \tag{17}$$

where the sum $\sum_\chi$ is over all Dirichlet character modulo q, and $\bar{z}$ denotes complex conjugate of z. We want $\# > 0$. We separate the contribution from the principal character in (17) and get

$$\# = \frac{1}{\phi(q)}|\mathcal{P}|\big(|\mathcal{P}|-1\big)|\mathcal{B}_q| + \frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\sum_{\substack{q_1,q_2\in\mathcal{P}\\ q_1\neq q_2}}\sum_{b\in\mathcal{B}}\chi(aq_1q_2)\overline{\chi}(b) := \#_1 + \#_2$$

where $\mathcal{B}_q$ denotes the set of numbers in $\mathcal{B}$ that are relatively prime to q. Now

$$\begin{aligned}
\#_2 &= \frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\sum_{q_1,q_2\in\mathcal{P}}\sum_{b\in\mathcal{B}}\chi(aq_1q_2)\overline{\chi}(b) - \frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\sum_{q_1\in\mathcal{P}}\sum_{b\in\mathcal{B}}\chi\big(aq_1^2\big)\overline{\chi}(b),\\
|\#_2| &\leqslant \frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\Big|\sum_{q_1\in\mathcal{P}}\chi(q_1)\Big|^2\Big|\sum_{b\in\mathcal{B}}\chi(b)\Big| + \frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\Big|\sum_{q_1\in\mathcal{P}}\chi^2(q_1)\Big|\Big|\sum_{b\in\mathcal{B}}\chi(b)\Big|\\
&:= S_1 + S_2.
\end{aligned}$$

Using trivial estimate on $\sum_{q_1}$ and Cauchy–Schwarz inequality, we have

$$S_2 \leqslant \frac{|\mathcal{P}|}{\phi(q)}\Big(\sum_{\chi}1\Big)^{1/2}\Big(\sum_{\chi}\Big|\sum_{b\in\mathcal{B}}\chi(b)\Big|^2\Big)^{1/2} \leqslant |\mathcal{P}||\mathcal{B}|^{1/2} \leqslant |\mathcal{B}|^{1/2}N$$

by orthogonality of characters (note that $B \leqslant q$).

Now, recall a well-known consequence of the Generalized Lindelöf Hypothesis:

$$\sum_{n\leqslant N}\chi(n)\ll_\epsilon N^{1/2}q^\epsilon \tag{18}$$

for non-principal character $\chi\pmod q$. Using this and the orthogonality of characters, we have

$$\begin{aligned}S_1 &\ll_\epsilon |\mathcal{B}|^{1/2}q^\epsilon\frac{1}{\phi(q)}\sum_\chi\Bigg|\sum_{q_1\in\mathcal{P}}\chi(q_1)\Bigg|^2\leqslant|\mathcal{B}|^{1/2}q^\epsilon\sum_{\substack{q_1,q_1'\in\mathcal{P}\\ q_1\equiv q_1'\ (\mathrm{mod}\ q)}}1\\ &\leqslant |\mathcal{B}|^{1/2}q^\epsilon\sum_{\substack{N/2\leqslant q_1,q_1'\leqslant N\\ q_1\equiv q_1'\ (\mathrm{mod}\ q)}}1\leqslant|\mathcal{B}|^{1/2}q^\epsilon N\left(\frac{N}{q}+1\right).\end{aligned}$$

Thus

$$|\#_2|\ll_\epsilon|\mathcal{B}|^{1/2}q^\epsilon N\left(\frac{N}{q}+1\right)\ll\begin{cases}|\mathcal{B}|^{1/2}q^\epsilon N & \text{if } q>N,\\ |\mathcal{B}|^{1/2}q^\epsilon\frac{N^2}{q} & \text{if } q\leqslant N;\end{cases}$$

while

$$\#_1\geqslant\frac{|\mathcal{P}|^2|\mathcal{B}_q|}{2\phi(q)}$$

for N sufficiently large. Therefore, replacing ϵ with $\epsilon/4$, we have $\#>0$ if

$$\frac{|\mathcal{P}|^2|\mathcal{B}_q|}{\phi(q)}\gg_\epsilon|\mathcal{B}|^{1/2}q^{\epsilon/4}N\quad\text{and}\quad\frac{|\mathcal{P}|^2|\mathcal{B}_q|}{\phi(q)}\gg_\epsilon|\mathcal{B}|^{1/2}\frac{N^2}{q^{1-\epsilon/4}}.$$

By Chebychev's estimate or the prime number theorem, $|\mathcal{P}|\geqslant\frac{N}{2\log N}-2>\frac{N}{3\log N}$ as $q\leqslant N^2$ can be divisible by at most two $q_1\in\mathcal{P}$. Consequently by Lemma 13, (16) has some solutions $q_1,q_2\in\mathcal{P}$ with $q_1\neq q_2$, and $1\leqslant b\leqslant B=\max(\frac{q^{2+0.6\epsilon}}{N^2},q^{0.6\epsilon})$. In other words, we can find distinct primes $q_1,q_2\in\mathcal{P}$ and integer k such that

$$\left|\frac{a}{q}-\frac{k}{q_1q_2}\right|\ll_\epsilon\max\left(\frac{q^{1+0.6\epsilon}}{N^4},\frac{1}{q^{1-0.6\epsilon}N^2}\right). \tag{19}$$

The right-hand side of (19) is $\ll_\epsilon\frac{1}{qN^{\phi-\epsilon}}$ if $q^{2+0.6\epsilon}\leqslant N^{4-\phi+\epsilon}$. This is true when $\phi\leqslant 4/3$ as $q\leqslant N^\phi$ (Note: $0.6\times 4/3<1$). This proves Theorem 11. □

Note. One can get a weaker unconditional result with $\phi\leqslant 6/5$ using Pólya–Vinogradov inequality instead of (18).

Acknowledgments

The author would like to thank Angel Kumchev for some helpful comments on the almost all results, Sidney Graham for some stimulating discussions, and George Grossman for suggestions on exposition. The author also thanks the referee for some helpful corrections.

References

[1] E. Alkan, G. Harman, A. Zaharescu, Diophantine approximation with mild divisibility constraints, J. Number Theory 118 (2006) 1–14.
[2] R.C. Baker, Diophantine Inequalities, London Math. Soc. Monogr. (N.S.), vol. 1, Oxford Univ. Press, New York, 1986.
[3] A. Balog, A. Perelli, Diophantine approximation by square-free numbers, Ann. Sc. Norm. Super. Pisa Cl. Sci. (4) 11 (3) (1984) 353–359.
[4] T.H. Chan, Finding almost squares II, Integers 5 (1) (2005), A23, 4 pp. (electronic).
[5] M.Z. Garaev, A.A. Karatsuba, On a symmetric congruence and its applications, arXiv: math.NT/0503164, preprint.
[6] G. Harman, Diophantine approximation with square-free integers, Math. Proc. Cambridge Philos. Soc. 95 (3) (1984) 381–388.
[7] D.R. Heath-Brown, Diophantine approximation with square-free numbers, Math. Z. 187 (3) (1984) 335–344.
[8] D.R. Heath-Brown, C. Jia, The distribution of αp modulo one, Proc. London Math. Soc. (3) 84 (1) (2002) 79–104.
[9] I.E. Shparlinski, Primitive points on a modular hyperbola, Bull. Pol. Acad. Sci. Math. 54 (3–4) (2006) 193–200.
[10] I.M. Vinogradov, The Method of Trigonometrical Sums in the Theory of Numbers, Dover Publications Inc., Mineola, New York, 2004.
[11] A. Zaharescu, Small values of $n^2\alpha \pmod 1$, Invent. Math. 121 (2) (1995) 379–388.