

APPROXIMATION BY SEVERAL RATIONALS

IGOR E. SHPARLINSKI

(Received 15 August 2007)

Abstract

Following T. H. Chan, we consider the problem of approximation of a given rational fraction a/q by sums of several rational fractions $a_1/q_1, \dots, a_n/q_n$ with smaller denominators. We show that in the special cases of $n = 3$ and $n = 4$ and certain admissible ranges for the denominators q_1, \dots, q_n , one can improve a result of T. H. Chan by using a different approach.

2000 *Mathematics subject classification*: 11J04, 11N25.

Keywords and phrases: rational approximations, multivariate congruences.

1. Introduction

Chan [1] has recently considered the question of approximating real numbers by sums of several rational fractions $a_1/q_1, \dots, a_n/q_n$ with bounded denominators.

In the special case of $n = 3$ the result of Chan [1] can be reformulated as follows. Given two integers a and $q \geq 1$, for any $Q \geq q$ there are integers a_i and q_i with $1 \leq q_i \leq Q^{1/2+o(1)}$, $i = 1, 2, 3$, and such that

$$\left| \frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2} - \frac{a_3}{q_3} \right| \leq \frac{1}{qQ^{1+o(1)}}.$$

We remark that the numerators a_1, a_2, a_3 can be negative.

In this paper we use a different approach to show that when Q is large enough, that is, when $Q \geq q^{2+\varepsilon}$, the same result holds with $1/3$ instead of $1/2$. We also obtain more explicit constants.

Similarly, for $n = 4$, we see from [1] that for any $Q \geq q$ there are integers a_i and q_i with $1 \leq q_i \leq Q^{2/5+o(1)}$, $i = 1, 2, 3, 4$, and such that

$$\left| \frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2} - \frac{a_3}{q_3} - \frac{a_4}{q_4} \right| \leq \frac{1}{qQ^{1+o(1)}}.$$

In this case, under the same condition $Q \geq q^{2+\varepsilon}$ we replace $2/5$ with $1/4$.

This work was supported in part by ARC grant DP0556431.

© 2008 Australian Mathematical Society 0004-9727/08 \$A2.00 + 0.00

Our approach is based on a result of [3] about the uniformity of distribution in residue classes of rather general products. More precisely, it is shown in [3] that for any set $\mathcal{X} \in [1, X]$ of integers x with $\gcd(x, q) = 1$ and for any interval $[Z + 1, Z + Y]$, for the number $M_{u,q}(\mathcal{X}; Y, Z)$ of solutions to the congruence

$$u \equiv xy \pmod{q}, \quad x \in \mathcal{X}, y \in [Z + 1, Z + Y],$$

we have

$$\sum_{u=1}^q \left| M_{u,q}(\mathcal{X}; Y, Z) - \#\mathcal{X} \frac{Y}{q} \right|^2 \leq \#\mathcal{X}(X + Y)q^{o(1)}. \tag{1}$$

2. Approximation by three rationals

THEOREM 1. *Let a and $q \geq 1$ be integers with $\gcd(a, q) = 1$. For any fixed $\varepsilon > 0$ and sufficiently large q , for any integer $Q \geq q^{2+\varepsilon}$ there are integers a_i and q_i with $1 \leq q_i \leq 2Q^{1/3}$, $i = 1, 2, 3$, and such that*

$$\left| \frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2} - \frac{a_3}{q_3} \right| \leq \frac{1}{qQ}$$

holds.

PROOF. We note that it is enough to show that there are positive integers $q_1, q_2, q_3 \leq 2Q^{1/3}$ with

$$q_1q_2q_3 \geq Q, \tag{2}$$

such that

$$\gcd(q_1, q_2) = \gcd(q_1, q_3) = \gcd(q_2, q_3) = 1, \tag{3}$$

and

$$aq_1q_2q_3 \equiv 1 \pmod{q}. \tag{4}$$

Indeed, from (4) we conclude that $aq_1q_2q_3 = 1 + bq$ for some integer b . Since (3) implies that

$$\gcd(q_1q_2, q_1q_3, q_2q_3) = 1,$$

then

$$b = a_1q_2q_3 + a_2q_1q_3 + a_3q_1q_2,$$

for some integers a_1, a_2, a_3 . Thus

$$\left| \frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2} - \frac{a_3}{q_3} \right| = \frac{1}{qq_1q_2q_3} \leq \frac{1}{qQ}.$$

Let us put $R = \lfloor 2Q^{1/3} \rfloor$. We may assume that $R < q$ since otherwise we simply choose $a_1 = 1, a_2 = a_3 = 0, q_1 = q, q_2 = q_3 = 1$.

We now consider:

- the set \mathcal{S} consisting of integers $s \in [R/3, R/2]$;
- the set \mathcal{P} consisting of primes $p \in [R/2, 3R/4]$ with $\gcd(p, q) = 1$;
- the set \mathcal{L} consisting of primes $\ell \in [3R/4, R]$ with $\gcd(\ell, q) = 1$.

Since q may have at most $O(\log q)$ prime divisors, by the prime number theorem we see that

$$\#\mathcal{S}, \#\mathcal{P}, \#\mathcal{L} \geq R^{1+o(1)}.$$

Clearly, if we take $q_1 = s \in \mathcal{S}$, $q_2 = p \in \mathcal{P}$ and $q_3 = \ell \in \mathcal{L}$ then (3) is satisfied and we also have (2). Thus it is enough to show that the congruence

$$spl \equiv 1 \pmod{q}, \quad s \in \mathcal{S}, p \in \mathcal{P}, \ell \in \mathcal{L},$$

has a solution. For an integer $u \in [1, q]$ we denote by $N(u)$ the number of solutions to the congruence

$$sp \equiv u \pmod{q}, \quad s \in \mathcal{S}, p \in \mathcal{P}. \tag{5}$$

Let \mathcal{U} be the set of integers $u \in [1, q]$ for which the above congruence has a solution, that is, $N(u) > 0$. It is enough to show that the congruence

$$u\ell \equiv 1 \pmod{q}, \quad u \in \mathcal{U}, \ell \in \mathcal{L}, \tag{6}$$

has a solution.

Also let \mathcal{V} be the set of remaining integers $u \in [1, q]$ with $N(u) = 0$. It follows from [3] that

$$\sum_{u=1}^q \left| N(u) - \frac{\#\mathcal{S}\#\mathcal{P}}{q} \right|^2 \leq R^2 q^{o(1)};$$

see (1). Hence

$$\#\mathcal{V} \left(\frac{\#\mathcal{S}\#\mathcal{P}}{q} \right)^2 \leq R^2 q^{o(1)},$$

which implies that $\#\mathcal{V} \leq R^{-2} q^{2+o(1)}$. Recalling that $R \geq 2Q^{1/3} - 1 \geq q^{2/3+\varepsilon/3}$, we see that

$$\#\mathcal{L} - \#\mathcal{V} = R^{1+o(1)} - R^{-2} q^{2+o(1)} > 0,$$

provided that q is large enough. Therefore the congruence (6) has a solution, which concludes the proof. □

3. Approximation by four rationals

We now use a similar approach for approximations by four rational fractions.

THEOREM 2. *Let a and $q \geq 1$ be integers with $\gcd(a, q) = 1$. For any fixed $\varepsilon > 0$ and sufficiently large q , for any integer $Q \geq q^{2+\varepsilon}$ there are integers a_i and q_i with $1 \leq q_i \leq 2Q^{1/4}$, $i = 1, 2, 3$, and such that*

$$\left| \frac{a}{q} - \frac{a_1}{q_1} - \frac{a_2}{q_2} - \frac{a_3}{q_3} - \frac{a_4}{q_4} \right| \leq \frac{1}{qQ}$$

holds.

PROOF. We proceed as in the proof of Theorem 1. In particular, we see that it is enough to show that there are positive integers $q_1, q_2, q_3, q_4 \leq 2Q^{1/4}$ with

$$q_1q_2q_3q_4 \geq Q, \tag{7}$$

such that

$$\gcd(q_i, q_j) = 1, \quad 1 \leq i < j \leq 4, \tag{8}$$

and

$$aq_1q_2q_3q_4 \equiv 1 \pmod{q}.$$

Let us put $R = \lfloor 2Q^{1/4} \rfloor$. As before, we remark that we may assume that $R < q$ since otherwise the result is trivial.

We now consider:

- the set \mathcal{S} consisting of integers $s \in [R/4, R/3)$;
- the set \mathcal{P} consisting of primes $p \in [R/3, 2R/3)$ with $\gcd(p, q) = 1$;
- the set \mathcal{L} consisting of primes $\ell \in [2R/3, 3R/4)$ with $\gcd(\ell, q) = 1$;
- the set \mathcal{R} consisting of primes $r \in [3R/4, R]$ with $\gcd(r, q) = 1$.

Again, by the prime number theorem,

$$\#\mathcal{S}, \#\mathcal{P}, \#\mathcal{L}, \#\mathcal{R} \geq R^{1+o(1)}.$$

Clearly, if we take $q_1 = s \in \mathcal{S}$, $q_2 = p \in \mathcal{P}$, $q_3 = \ell \in \mathcal{L}$ and $q_4 = r \in \mathcal{R}$ then (8) is satisfied and we also have (7). Thus it is enough to show that the congruence

$$splr \equiv 1 \pmod{q}, \quad s \in \mathcal{S}, p \in \mathcal{P}, \ell \in \mathcal{L}, r \in \mathcal{R},$$

has a solution.

As in the proof of Theorem 1 we note the set \mathcal{V} of integers $u \in [1, q]$ for which the congruence (5) does not have a solution is of cardinality $\#\mathcal{V} \leq R^{-2}q^{2+o(1)}$.

Let \mathcal{W} be the set of integers $w \in [1, q]$ which are of the form $w \equiv \ell r \pmod{q}$ with $\ell \in \mathcal{L}$ and $r \in \mathcal{R}$. We note that $\#\mathcal{L}\#\mathcal{R} = R^{2+o(1)}$ products ℓr are distinct integers in

the interval $[1, R^2]$. Since there are at most $R^2/q + 1$ integers $t \in [1, R^2]$ in the same residue class modulo q , we obtain

$$\#\mathcal{W} \geq R^{2+o(1)}(R^2/q + 1)^{-1}.$$

Since $R^2 \geq (2Q^{1/4} - 1)^2 \geq Q^{1/2} \geq q^{1+\varepsilon/2}$ (provided q is large enough) we see that $R^2/q + 1 \leq 2R^2/1$. Hence $\#\mathcal{W} = q^{1+o(1)}$. We now see that

$$\#\mathcal{W} - \#\mathcal{V} = q^{1+o(1)} - R^{-2}q^{2+o(1)} > 0,$$

provided that q is large enough. The desired result now follows. \square

We remark that in both Theorems 1 and 2 the coefficient 2 in the bound on the denominators can be replaced by any constant $c > 1$.

4. Comments

It is natural to try to use (1) to improve the corresponding bound from [1] for larger values of n too. Although some results can be obtained in this way, for $n \geq 5$ we have not been able to achieve this. In fact, it seems quite plausible that for $n \geq 5$, instead of using the bound (1) from [3], one can study the solvability of the congruence

$$q_1 \cdots q_n \equiv 1 \pmod{q},$$

with ‘small’ q_1, \dots, q_n by using bounds of multiplicative character sums in the same style as in [2, 4].

Acknowledgement

The author is grateful to Tsz Ho Chan for useful discussions.

References

- [1] T. H. Chan, ‘Approximating reals by sums of rationals’, Preprint, 2007 (available from <http://arxiv.org/abs/0704.2805>).
- [2] I. E. Shparlinski, ‘On the distribution of points on multidimensional modular hyperbolas’, *Proc. Japan Acad. Sci., Ser. A* **83** (2007), 5–9.
- [3] I. E. Shparlinski, ‘Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average’, *Michigan Math. J.* to appear.
- [4] I. E. Shparlinski, ‘On a generalisation of a Lehmer problem’, Preprint, 2006 (available from <http://arxiv.org/abs/math/0607414>).

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au