Radical bound for Zaremba's conjecture

Nikita Shulga
La Trobe University

One World Numeration Seminar
26 March 2024

Setting

Let $q \geq 2$ be an integer and let a be an integer with $1 \leq a < q$, such that $\gcd(a, q) = 1$. Then a rational number a/q can be expanded into a finite simple continued fraction as

$$\frac{a}{q} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_r}}}} = [a_1, \ldots, a_r], \quad a_i \in \mathbb{Z}_+.$$

Note that each rational $a/q \in (0, 1)$ has two different representations

$$a/q = [a_1, a_2, \ldots, a_{r-1}, a_r] \quad \text{and} \quad a/q = [a_1, a_2, \ldots, a_{r-1}, a_r - 1, 1].$$

Zaremba's conjecture

Denote

$$K\left(\frac{a}{q}\right) = \max(a_1, \ldots, a_r).$$

Conjecture (Zaremba, 1971)

There exists an absolute constant M with the following property: for any positive integer q there exists a coprime to q, such that $K(a/q) \leq M$.

In fact, Zaremba's conjectured that for $M = 5$.

For large prime numbers q Hensley conjectured that even $M = 2$ should be enough.

Korobov's bound

Theorem (Korobov, 1963)

For prime number q there exists $1 \leq a < q$ such that

$$K(a/q) \ll \log q.$$

In fact, this result is also true for composite q.
Korobov's studied continued fractions with small partial quotients for the purposes of numerical integration.

Zaremba's conjecture for a.e. q

Theorem (Bourgain-Kontorovich, Ann. Math., 2011,2014)

The number of $q \in \{1, \ldots, N\}$ such that Zaremba's conjecture holds with $K(a/q) \leq M$ for this q is

$$N - O(N^{1-c(M)/\log\log N}), \quad c(M) > 0.$$

Further, if $M = 50$, then there is a positive proportion of such q.

Decreasing M: Frolenkov-Kan, Kan, Huang, Magge-Oh-Winter.

Theorem (Kan, 2016)

If $M = 4$, then for all but $o(N)$ numbers $q \in \{1, \ldots, N\}$ Zaremba's conjecture takes place.

Problems with the above results

- Korobov's result provide a rather weak bound of $\log q$.
- Bourgain-Kontorovich type results not just dont have any information about the set of possible exceptions, but it also doesn't provide information about the set, where the bound holds.

Neiderreiter's results

Those problems are somewhat solved by the following results.

Theorem (Neiderreiter, 1986)

For integer numbers of the form $q = 2^n$ or $q = 3^n$, $n \in \mathbb{N}$, there exists an integer a, coprime to q with

$$K(a/q) \leq 3.$$

Theorem (Neiderreiter, 1986)

For integer numbers of the form $q = 5^n$, $n \in \mathbb{N}$, there exists an integer a, coprime to q with

$$K(a/q) \leq 4.$$

Weak results of Niederreiter's type

After that, couple of more results were provided.

Theorem (Yodphotong-Laohakosol,2002)

For integer numbers of the form $q = 6^n$ *for any* $n \in \mathbb{N}$ *there exists an integer* a*, coprime to* q *with*

$$K(a/q) \leq 5.$$

Theorem (Komatsu, 2005)

For integer numbers of the form $q = 7^{c2^n}, (n \geq 0, c = 1, 3, 5, 7, 9, 11)$ *there exists an integer* a*, coprime to* q *with*

$$K(a/m) \leq 3.$$

How do Niederreiter's type results work?

Proofs rely on a famous folklore statement, knows as Folding lemma.

Lemma (Folding Lemma)

If $t_r/q_r = [a_1, \ldots, a_r]$ and b is a non-negative integer, then

$$\frac{t_r}{q_r} + \frac{(-1)^r}{bq_r^2} = [a_1, \ldots, a_r, b-1, 1, a_r - 1, a_{r-1}, \ldots, a_1]. \tag{1}$$

Niederreiter's strategy

To present first few explicit fractions with small partial quotients, and then apply Folding Lemma inductively to generate all other powers of 2. He started with $1/2, 3/4, 3/8, 7/16, 9/32$ and

$$\begin{aligned}\frac{25}{64} &= [2,1,1,3,1,2],\\ \frac{49}{128} &= [2,1,1,1,1,2,1,2],\\ &\vdots\\ \frac{791}{2048} &= [2,1,1,2,3,3,1,1,2,2].\end{aligned}$$

Main result

I present a generalisation of Niederreiter's type results.

Recall the definition of a radical of an integer number n.

$$\mathrm{rad}(n) = \prod_{\substack{p \mid n \\ p \text{ prime}}} p.$$

Theorem (Sh., 2023)

For any integer $q \geq 2$, such that $q \neq 2^n, 3^n$, there exists a positive integer a with $1 \leq a < q$ and $\gcd(a, q) = 1$, such that $K(a/q) \leq \mathrm{rad}(q) - 1$.

Corollary

For any integer q of the form $q = 2^n 3^m$ for any $n, m \in \mathbb{N}_0$ there exists a positive integer a with $1 \leq a < q$ and $\gcd(a, q) = 1$, such that $K(a/q) \leq 5$.

This theorem also suits as an improvement of some results by Moshchevitin-Murphy-Shkredov.

Recent improvement to Korobov's bound

One of the most recent results is due to Moshchevitin, Murphy and Shkredov, they proved the following theorem.

Theorem (Moshchevitin-Murphy-Shkredov, 2022)

Let q be a positive sufficiently large integer with sufficiently large prime factors. Then there is a positive integer a with $\gcd(a, q) = 1$ and

$$K(a/q) \leq O(\log q / \log\log q). \tag{2}$$

Also, if q is a sufficiently large square-free number, then (2) takes place. Finally, if $q = p^n$, p is an arbitrary prime, then (2) holds for sufficiently large n.

Improvement of MMSh result

Remark

Using Theorem 9 we can improve Theorem 11 in the case $q = p^n$ for a prime number p. By Theorem 11 for n sufficiently large one has

$$K(a/q) \leq O(n \log p / \log(n \log p))$$

for some $1 \leq a < q$, coprime to p. For large enough n, say for $n \asymp p^2$, our Theorem 9 gives a better bound of $K(a/q) \leq p - 1$, as compared to

$$K(a/q) \leq O(p^2 \log p / \log(p^2 \log p)) = O(p^2)$$

from Theorem 11. When $n \gg p^2$, the bound obtained by Theorem 9 remains the same, but the bound obtained by Theorem 11 will become worse the larger the value of n is.

The main construction

The canonical representation of the number q is

$$q = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}, \tag{3}$$

where $p_1 < p_2 < \ldots < p_k$ are primes and n_i are positive integers. Hence $\mathrm{rad}(q) = p_1 \cdots p_k$.

Now consider a following iterative procedure: set $q_{(0)} := q$ and for $i \geq 1$ define $q_{(i)}$ from the equality

$$q_{(i-1)} = p_{(i)} \cdot q_{(i)}^2, \tag{4}$$

where

$$p_{(i)} = p_1^{v_1^{(i)}} p_2^{v_2^{(i)}} \cdots p_k^{v_k^{(i)}} \text{ with } v_j^{(i)} \in \{0, 1\} \text{ for all } i, j.$$

Note that for all i we have $p_{(i)} | \mathrm{rad}(q)$, so, in particular, $p_{(i)} \leq \mathrm{rad}(q)$.

The main construction 2

By the definition of the procedure (4), there exists $N \in \mathbb{N} \cup \{0\}$, such that

$$q_{(N)} > 1 \text{ and } q_{(N+1)} = 1.$$

After this step, the process terminates and we have $q_{(N+j)} = p_{(N+j)} = 1$, $j \geq 2$. Easy to see that $N = 0$ if and only if in (3) one has $n_1 = \ldots = n_k = 1$ and $N \geq 1$ otherwise.

We have $2 \leq q_{(N)} \leq \mathrm{rad}(q)$. We also note that $q_{(N)}$ is a square-free number.

Proof

We have two cases.

1) If $N = 0$, then $\mathrm{rad}(q) = q$. Consider a fraction $(q-1)/q$. We have $(q-1)/q = [1, q-2, 1]$. Hence for $a = q-1$ we get $K(a/q) \leq \mathrm{rad}(q) - 2$.

2) If $N \geq 1$, we further distinguish several cases.

2.1) $q_{(N)} \neq 2, 3, 6$.
As $q_{(N)}$ is a square-free number, this means that $q_{(N)} \geq 5$, and, in particular, $\mathrm{rad}(q) \geq q_{(N)} \geq 5$. For a square-free number $q_{(N)} \geq 5$ we have $\varphi(q_{(N)}) \geq 4$, where $\varphi(n)$ is an Euler's totient function.

Lemma

For an integer number q with $\varphi(q) \geq 4$, there exists an integer $1 \leq a \leq q-1$, coprime to q, such that

$$\frac{a}{q} = [a_1, \ldots, a_n]$$

with the following properties:

- $n \geq 2$;
- $a_1 \geq 2$ *and* $a_n \geq 2$;
- $K(a/q) \leq \frac{q-1}{2}$.

Proof

Apply previous Lemma with $q = q_{(N)}$ to get a reduced fraction $a/q_{(N)}$, so there exists $a/q = [a_1, \ldots, a_n]$ with $n \geq 2,\ a_1, a_n \geq 2$ and $K(a/q_{(N)}) \leq (q_{(N)} - 1)/2$.

Application of Folding Lemma with

$$\frac{t_r}{q_r} = \frac{a}{q_{(N)}} \quad \text{and} \quad b = p_{(N)}$$

leads to

$$\frac{t_r}{q_r} + \frac{(-1)^r}{bq_r^2} = [a_1, \ldots, a_n, p_{(N)} - 1, 1, a_n - 1, \ldots, a_1] = \frac{a_{(N-1)}}{p_{(N)} \cdot q_{(N)}^2} = \frac{a_{(N-1)}}{q_{(N-1)}}.$$

We have two possible situations. If $p_{(N)} = 1$, then we get

$$K\left(\frac{a_{(N-1)}}{q_{(N-1)}}\right) \leq (q_{(N)} - 1)/2 + 1 = (q_{(N)} + 1)/2 \leq \mathrm{rad}(q) - 1.$$

To get the last inequality we used $q_{(N)} \leq \mathrm{rad}(q)$ and $\mathrm{rad}(q) \geq 5$.

If $p_{(N)} \geq 2$, then

$$K\left(\frac{a_{(N-1)}}{q_{(N-1)}}\right) \leq \max\left(p_{(N)} - 1, \frac{q_{(N)} - 1}{2}\right) \leq \mathrm{rad}(q) - 1.$$

End of the case $q_{(N)} \neq 2, 3, 6$

Now we iteratively apply Folding Lemma for $i = 1, 2, \ldots, N-1$ with

$$\frac{t_r}{q_r} = \frac{a_{(N-i)}}{q_{(N-i)}} \quad \text{and} \quad b = p_{(N-i)}$$

to get

$$\frac{t_r}{q_r} + \frac{(-1)^r}{bq_r^2} = [a_1, \ldots, a_1, p_{(N-i)} - 1, 1, a_1 - 1, \ldots, a_1] = \frac{a_{(N-i-1)}}{p_{(N-i)} \cdot q_{(N-i)}^2} = \frac{a_{(N-i-1)}}{q_{(N-i-1)}}.$$

After $N-1$ steps, the application of Folding Lemma provides us a fraction with denominator $q_{(0)} = q$ with all partial quotients bounded by $\mathtt{rad}(q) - 1$ and the process terminates.

Case $q_{(N)} = 2, 3, 6$

If $q_{(N)} = 3$ or 6, the application of Lemma 8 for $t_r/q_r = 1/q_{(N)}$ and $b = p_{(N)}$ gives us

$$\frac{t_r}{q_r} + \frac{(-1)^r}{bq_r^2} = [q_{(N)}, p_{(N)} - 1, 1, q_{(N)} - 1] = \frac{a_{(N-1)}}{p_{(N)} \cdot q_{(N)}^2} = \frac{a_{(N-1)}}{q_{(N-1)}}.$$

The resulting continued fraction $[q_{(N)}, p_{(N)} - 1, 1, q_{(N)} - 1]$ satisfy the first two properties from Lemma and $K(a_{(N-1)}/q_{(N-1)}) \leq \mathrm{rad}(q) - 1$, so we can continue the procedure as in the previous case.

If $q_{(N)} = 2$, then the first application of the Folding Lemma, depending on $p_{(N)}$, will generate either fraction $[2, p_{(N)} - 1, 2]$ or $1/4 = [4]$. In the first subcase we proceed as previously, in the latter we apply Folding Lemma manually one more time to get $[4, p_{(N-1)} - 1, 1, 3]$, so that we can start the iterative process using Lemma.

Case $q = 2^n 3^m$

We know that the potential values of $q_{(N)}$ are $q_{(N)} = 2, 3$ or 6. Fractions $1/2 = [2], 1/3 = [2, 1], 1/6 = [5, 1]$ satisfy $K(1/q_{(N)}) \leq 5$. By definition, $q_{(N-1)} = p_{(N)} q_{(N)}^2$, where $p_{(N)} \in \{1, 2, 3, 6\}$ and $q_{(N)} \in \{2, 3, 6\}$. Consider the fractions

$$\begin{array}{llll}
\frac{1}{2^2} = [4], & \frac{3}{2 \cdot 2^2} = [2,1,2], & \frac{5}{3 \cdot 2^2} = [2,2,2], & \frac{7}{6 \cdot 2^2} = [3,2,3], \\
\frac{2}{3^2} = [4,2], & \frac{5}{2 \cdot 3^2} = [3,1,1,2], & \frac{8}{3 \cdot 3^2} = [3,2,1,2], & \frac{17}{6 \cdot 3^2} = [3,5,1,2], \\
\frac{11}{6^2} = [3,3,1,2], & \frac{17}{2 \cdot 6^2} = [4,4,4], & \frac{23}{3 \cdot 6^2} = [4,1,2,3,2], & \frac{49}{6 \cdot 6^2} = [4,2,2,4,2].
\end{array}$$

These fraction cover all possible values of $q_{(N-1)}$ and for all fractions $a/q_{(N-1)}$, one has $K(a/q_{(N-1)}) \leq 5$. For every fraction except $1/2^2 = [4]$, the length of continued fraction expansion is $n \geq 2$ and $2 \leq a_1, a_n \leq 4$. For them we do the same procedure as before.

Final case of $q_{(N)} = 2, q_{(N-1)} = 4$

Consider all possible values of $q_{(N-2)}$, generated by $1/4 = [4]$:

$$\frac{7}{2^4} = [2,3,2], \quad \frac{9}{2 \cdot 2^4} = [3,1,1,4], \quad \frac{13}{3 \cdot 2^4} = [3,1,2,4], \quad \frac{29}{6 \cdot 2^4} = [3,3,4,2].$$

As before, for each continued fraction here, its length n satisfies $n \geq 2$ and $2 \leq a_1, a_n \leq 4$.

So we can continue the same iterative procedure as before. This concludes the proof.

Remark on the result of MMSh

By Theorem of MMSh, when d is a sufficiently large square-free integer, there exists a, coprime to d, such that

$$K(a/d) \leq O(\log d / \log\log d).$$

By the iterative procedure from the proof of Theorem our main result, we reduce any number q to a square-free number $q_{(N)}$ in finite number of steps. Afterwards, we start building continued fractions with given properties starting from $q_{(N)}$ and going back to the number $q := q_{(0)}$.

MMSh Theorem guarantees that for the square-free number $d = q_{(N)} = p_1 \cdots p_k$ one can find an integer a, coprime to $q_{(N)}$ with

$$K(a/q_{(N)}) \leq O(\log q_{(N)} / \log\log q_{(N)}).$$

Starting from this fraction as a seed fraction of our iterative procedure, we can apply Folding Lemma with $b \in \mathcal{D}$, where $\mathcal{D}$ is the set of small divisors of $q_{(N)}$ defined as

$$\mathcal{D} = \left\{ m \in \mathbb{N} \,:\, m | q_{(N)} \text{ and } m \leq O(\log q_{(N)} / \log\log q_{(N)}) \right\}.$$

This set is always non-empty, because $1 \in \mathcal{D}$.

Remark on the result of MMSh 2

Then using the same iterative procedure as in the proof of the main result, one will generate all numbers q of the form

$$p_{i_1}^{n_1} \cdots p_{i_j}^{n_j} d^{2^n} \quad \text{for all} \quad p_{i_1} \cdots p_{i_j} \in \mathcal{D},\ n_1, \dots, n_j \in \mathbb{N} \cup \{0\}, n \in \mathbb{N}.$$

In particular, as $1 \in \mathcal{D}$, iterative application of Folding Lemma will generate all numbers of the form $d^{2^n}, n \in \mathbb{N}$ with the same bound

$$K(a/d^{2^n}) \leq O(\log d / \log \log d)$$

for sufficiently large square-free integer d and some number a coprime to d.

Thank you!