# Bounded Partial Quotients in Continued Fractions and Zaremba's Conjecture

Akashdeep Das

**Abstract.** Zaremba's Conjecture, proposed in 1971, by mathematician, S.K. Zaremba, is a very interesting conjecture roaming the world of analytic number theory for the last 55 years. The conjecture claims that an absolute constant $A$ exists such that for every integer $q \geq 1$, there always exists an integer $a$ which is co-prime to $q$ for which all partial quotients in the continued fraction expansion of $a/q$ are bounded by $A$. The conjecture mainly focuses on Diophantine approximation and analytic number theory. We aim to link the arithmetic properties of rational numbers to the visual geometry of continued fractions. This paper will start off by exploring the backbone of the conjecture which includes the theory of bounded partial quotients. Then, it will also cover the analysis of different properties of finite continued fractions, continuants, and rational and Diophantine approximations. After that, it will explore modern approaches based on semi-group methods, matrix and semi-group formulation, density-one results, and more. Later, we focus on the breakthrough results which demonstrate that the conjecture holds for a density-one subset of the positive integers, and quantitative estimates for exceptional sets too. Finally, we explore the constraints that continue to obstruct a complete proof of the conjecture.

## 1. Introduction

Continued fractions have played a very important role in the field of number theory due to the work of great mathematicians such as Euclid, Euler, and Lagrange, because it provides some strangely, but more intuitively rational approximations to real numbers. One of the main questions in the modern theory of continued fractions concerns the behavior of partial quotients and the arithmetic information which is encoded within them. In 1971, Stanislaw K. Zaremba (S.K. Zaremba) proposed what is now known as the beautiful, the magnificent, the unsolved, Zaremba's Conjecture, which predicts that the existence of an absolute constant $A$ such that every positive integer $q$ occurs as the denominator of a rational number $a/q$, where $(a, q) = 1$, whose continued fraction expansion contains only partial quotients bounded by $A$. And, if mathematics has a habit of turning simple questions into lifelong research projects, then I would say that this conjecture is a perfect example of that! So, despite its simple statement, the conjecture remains unresolved for more than 55 years, and it has motivated strong developments across different topics like analytic number theory, Diophantine approximation, homogeneous dynamics, and arithmetic combinatorics. The study of bounded partial quotients extends far beyond the conjecture itself. *These never-ending ladder of fractions exhibit remarkable and clean approximation properties and arise naturally in problems which concern lattice point*

*distributions, pseudorandom number generation, and the group actions on arithmetic structures. Over the past several decades, a lot of progress has been made toward resolving Zaremba's Conjecture. For instance, groundbreaking work by Bourgain and Kontorovich demonstrate that the conjecture holds for a subset of the positive integers of natural density* 1*. These advances have revealed deep connections between continued fractions, thin semi-groups, expansion phenomena, and local-global principles as well!*

Before diving into equations, it's worth seeing how this conjecture quietly grew into something mathematicians have been arguing about for years! In the decades that followed the proposition of the conjecture, the problem attracted a lot of attention from analytic number theorists, with early partial progress in the late 20th century which focused on special cases and density results. *As outlined before, a major breakthrough came in 2012, when Jean Bourgain and Alex Kontorovich proved that a positive proportion of integers satisfy the conjecture's constraints, using tools from harmonic analysis and ergodic theory. And later work in the 2010s and 2020s refined these results by improving the bounds and extending the range of known cases by a minimum, but the full conjecture remains unresolved.*

In this paper, we develop the theory of bounded partial quotients and the mathematical framework underlying Zaremba's Conjecture. *Section I (Introduction)* provides the historical motivation and outlines the central question of how continued fractions encode rational numbers. *Section II (Preliminaries)* establishes the necessary background on continued fractions, convergents, and continuants. *Section III (Zaremba's Conjecture)* formally states the conjecture and explains its significance in number theory. *Section IV (Diophantine Approximation and Bounded Continued Fractions)* explores how approximation theory relates to bounded partial quotients. *Section V (Matrix and Semigroup Formulation)* introduces the algebraic reformulation using matrix products and semigroup dynamics. *Section VI (Bourgain-Kontorovich and Density-One Results)* discusses modern breakthroughs, including density-one theorems and partial solutions. *Section VII (Applications)* highlights the deep connections to areas such as dynamic computer systems, computational number theory, and dimensions, fractal structures. *Section VIII (Open Problems and Future Directions)* outlines unresolved questions and ongoing research directions. Finally, *Section IX (Conclusion)* discusses the broader significance of bounded continued fractions within contemporary number theory and outlines several open questions that continue to drive research in this magnificent field. We first start with a discussion of subsets.

## 2. Preliminaries

In this section we introduce the basic language of finite continued fractions, partial quotients, convergents, continuants, and bounded denominator sets. These objects form the arithmetic foundation for Zaremba's Conjecture. The main idea is that a rational number $a/q$ can be encoded by a finite sequence of

positive integers, while its denominator $q$ is produced from that sequence by a recurrence relation.

**Definition 1** (Finite Continued Fraction)**.** *Let $a_0 \in \mathbb{Z}$ and $a_1, \ldots, a_n \in \mathbb{N}$. A* finite continued fraction *is an expression of the form*

$$[a_0; a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

*The integers $a_0, a_1, \ldots, a_n$ are called the* partial quotients*. The integer $a_0$ is the integral part, while $a_1, \ldots, a_n$ determine the successive reciprocal structure of the expansion. Since the expansion terminates, every finite continued fraction represents a rational number.*

Finite continued fractions arise naturally from the Euclidean algorithm. Unlike decimal expansions, which depend on a chosen base, continued fractions encode the quotient structure obtained while computing greatest common divisors.[HW08] [Lut16] Their recursive form is

$$[a_0; a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_n]},$$

which is the basic mechanism behind the recurrence relations below.

**Definition 2** (Euclidean Algorithm)**.** *Let $p, q \in \mathbb{N}$ with $p > q$. The Euclidean algorithm is the finite division process*

$$\begin{aligned}
p &= a_0 q + r_1, && 0 \le r_1 < q, \\
q &= a_1 r_1 + r_2, && 0 \le r_2 < r_1, \\
r_1 &= a_2 r_2 + r_3, && 0 \le r_3 < r_2, \\
&\vdots && \vdots \\
r_{m-2} &= a_{m-1} r_{m-1} + r_m, && 0 \le r_m < r_{m-1}, \\
r_{m-1} &= a_m r_m. &&
\end{aligned}$$

*The final nonzero remainder is*

$$r_m = \gcd(p, q).$$

*The integers $a_0, a_1, \ldots, a_m$ are called the* Euclidean quotients*.*

Since the remainders strictly decrease,

$$q > r_1 > r_2 > \cdots > r_m > 0,$$

the algorithm terminates after finitely many steps. If

$$\frac{p}{q} = [a_0; a_1, \ldots, a_m],$$

then the partial quotients of the continued fraction are precisely the quotients appearing in the Euclidean algorithm. Thus a finite continued fraction is a compact encoding of the division process used to compute $\gcd(p, q)$.

**Definition 3** (Convergents)**.** *Let*

$$x = [a_0; a_1, \ldots, a_n]$$

*be a finite continued fraction. For $0 \le k \le n$, the $k$-th convergent of $x$ is*

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k].$$

*The integers $p_k$ and $q_k$ are called the numerator and denominator of the $k$-th convergent.*

The convergents are not independent rational numbers. They are linked by a pair of linear recurrence relations. These recurrences are the first place where the arithmetic structure of continued fractions becomes visible.

**Lemma 1** (Recurrence Relations for Convergents)**.** *Set*

$$p_{-2} = 0, \qquad p_{-1} = 1, \qquad q_{-2} = 1, \qquad q_{-1} = 0.$$

*Then, for every $k \ge 0$,*

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2}.$$

*Moreover,*

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k].$$

*Proof.* For each $a \in \mathbb{N}$, define

$$M(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}.$$

We claim that, for every $k \ge 0$,

$$M(a_0)M(a_1)\cdots M(a_k) = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}.$$

For $k = 0$, we have

$$M(a_0) = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix},$$

since $p_0 = a_0$, $p_{-1} = 1$, $q_0 = 1$, and $q_{-1} = 0$. Thus the claim is true in the base case.

Assume now that the claim holds for $k - 1$. Then

$$\begin{aligned} M(a_0)\cdots M(a_{k-1})M(a_k) &= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} a_k p_{k-1} + p_{k-2} & p_{k-1} \\ a_k q_{k-1} + q_{k-2} & q_{k-1} \end{pmatrix}. \end{aligned}$$

Hence

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2}.$$

The matrix product therefore gives the same fractional linear transformation as the continued fraction $[a_0; a_1, \ldots, a_k]$. Consequently,

$$[a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k}.$$

This proves the result. □

The next identity is the fundamental determinant relation for consecutive convergents. It shows that the numerators and denominators of adjacent convergents are arithmetically linked in the strongest possible way.

**Lemma 2** (Determinant Identity)**.** *For every $k \geq 0$,*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}.$$

*Proof.* From the matrix identity above,

$$M(a_0)M(a_1)\cdots M(a_k) = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}.$$

Taking determinants on both sides gives

$$\det(M(a_0)M(a_1)\cdots M(a_k)) = \det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}.$$

Since

$$\det M(a_i) = \det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = -1,$$

we obtain

$$\det(M(a_0)M(a_1)\cdots M(a_k)) = \prod_{i=0}^{k} \det M(a_i) = (-1)^{k+1}.$$

On the other hand,

$$\det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = p_k q_{k-1} - p_{k-1} q_k.$$

Therefore

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}.$$

□

This determinant identity immediately implies that every convergent is already in lowest terms. The proof is a standard divisibility argument.

**Corollary 1.** *For every $k \geq 0$,*

$$\gcd(p_k, q_k) = 1.$$

*Hence every convergent is written in lowest terms.*

*Proof.* Let

$$d = \gcd(p_k, q_k).$$

Then

$$d \mid p_k \qquad \text{and} \qquad d \mid q_k.$$

Hence $d$ divides every integer linear combination of $p_k$ and $q_k$. In particular,

$$d \mid \big(p_k q_{k-1} - p_{k-1} q_k\big).$$

By the determinant identity,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1} \in \{-1, 1\}.$$

Thus

$$d \mid 1.$$

Therefore $d = 1$, and so

$$\gcd(p_k, q_k) = 1.$$

□

We now isolate the denominator recurrence as its own object. This leads to the notion of a continuant, which will be used to describe denominator sets in a compact way.

**Definition 4** (Continuant)**.** *For positive integers $a_1, \dots, a_n$, the* continuant

$$\mathcal{K}_n(a_1, \dots, a_n)$$

*is defined recursively by*

$$\mathcal{K}_0 = 1, \qquad \mathcal{K}_1(a_1) = a_1,$$

*and, for $n \geq 2$,*

$$\mathcal{K}_n(a_1, \dots, a_n) = a_n \mathcal{K}_{n-1}(a_1, \dots, a_{n-1}) + \mathcal{K}_{n-2}(a_1, \dots, a_{n-2}).$$

The continuant records exactly the denominator produced by a finite string of partial quotients. This observation is one of the main bridges between continued fractions and the arithmetic sets appearing in Zaremba's Conjecture.

**Lemma 3.** *If*

$$\frac{a}{q} = [0; a_1, \dots, a_n],$$

*then*

$$q = \mathcal{K}_n(a_1, \dots, a_n).$$

*Proof.* Let $q_j$ be the denominator of the $j$-th convergent of $[0; a_1, \dots, a_n]$. Since $a_0 = 0$, the relevant denominator sequence begins with

$$q_0 = 1, \qquad q_1 = a_1.$$

For every $j \geq 2$, the recurrence relations for convergents give

$$q_j = a_j q_{j-1} + q_{j-2}.$$

On the other hand, the continuants satisfy

$$\mathcal{K}_0 = 1, \qquad \mathcal{K}_1(a_1) = a_1,$$

and, for every $j \geq 2$,

$$\mathcal{K}_j(a_1, \ldots, a_j) = a_j \mathcal{K}_{j-1}(a_1, \ldots, a_{j-1}) + \mathcal{K}_{j-2}(a_1, \ldots, a_{j-2}).$$

Thus the two sequences

$$\{q_j\}_{j=0}^{n} \qquad \text{and} \qquad \{\mathcal{K}_j(a_1, \ldots, a_j)\}_{j=0}^{n}$$

satisfy the same recurrence relation and the same initial conditions. Hence, by induction,

$$q_j = \mathcal{K}_j(a_1, \ldots, a_j) \qquad (0 \leq j \leq n).$$

Taking $j = n$, we obtain

$$q = q_n = \mathcal{K}_n(a_1, \ldots, a_n).$$

□

This observation is central to Zaremba's Conjecture: denominators of rational continued fractions are exactly continuants.

**Definition 5** (Bounded Partial Quotients)**.** *Let $A \geq 1$. A finite continued fraction*

$$[0; a_1, \ldots, a_n]$$

*has* partial quotients bounded by $A$ *if*

$$1 \leq a_i \leq A \qquad (1 \leq i \leq n).$$

*Equivalently, all partial quotients lie in the finite alphabet*

$$\mathcal{A}_A = \{1, 2, \ldots, A\}.$$

Thus bounded partial quotients mean that the continued fraction is built only from finitely many allowed digits. In this language, the condition that all partial quotients are bounded by $A$ can be written compactly as

$$(a_1, \ldots, a_n) \in \mathcal{A}_A^n.$$

**Example 1.** *The continued fraction*

$$[0; 1, 3, 2, 3, 1]$$

*has all partial quotients bounded by* 3*. In contrast,*

$$[0; 1, 3, 7, 2]$$

*does not have partial quotients bounded by* 3*, since one partial quotient is* 7*.*

We now define the denominator set associated with the finite alphabet $\mathcal{A}_A$. This set records all possible denominators that can be generated using only the digits $1, 2, \ldots, A$.

**Definition 6** (Zaremba Denominator Set)**.** *For $A \geq 1$, define*

$$\mathcal{D}_A = \left\{ q \in \mathbb{N} : \exists n \geq 1,\ \exists (a_1, \ldots, a_n) \in \mathcal{A}_A^n \text{ such that } q = \mathcal{K}_n(a_1, \ldots, a_n) \right\}.$$

*Equivalently,*

$$\mathcal{D}_A = \bigcup_{n \geq 1} \left\{ \mathcal{K}_n(a_1, \ldots, a_n) : (a_1, \ldots, a_n) \in \mathcal{A}_A^n \right\}.$$

*We call $\mathcal{D}_A$ the set of denominators generated by partial quotients bounded by $A$.*

The set $\mathcal{D}_A$ records exactly which integers occur as denominators of rational numbers whose continued fraction expansions are constructed from the finite alphabet $\mathcal{A}_A$. Consequently, the study of bounded partial quotients becomes the study of the arithmetic structure and distribution of the sets $\mathcal{D}_A$.

## 3. Zaremba's Conjecture

Having established the necessary theory of continued fractions, convergents, continuants, and bounded partial quotients, we now arrive at the central problem studied in this paper. The conjecture proposed by Stanisław Zaremba in 1971 concerns the extent to which bounded continued fractions can generate all positive integers as denominators. [Zar72]

Recall that, for a fixed integer $A \geq 1$, the denominator set is

$$\mathcal{D}_A = \left\{ q \in \mathbb{N} : \exists n \geq 1,\ \exists (a_1, \ldots, a_n) \in \mathcal{A}_A^n \text{ such that } q = \mathcal{K}_n(a_1, \ldots, a_n) \right\},$$

where

$$\mathcal{A}_A = \{1, 2, \ldots, A\}.$$

Thus $\mathcal{D}_A$ records precisely those denominators arising from finite continued fractions whose partial quotients belong to the alphabet $\mathcal{A}_A$. The central question is whether every positive integer belongs to such a set for some fixed finite value of $A$.

### 3.1. **Formal Statement.**

**Conjecture 1** (Zaremba's Conjecture)**.** *There exists an absolute constant $A \geq 1$ such that, for every integer $q \geq 1$, there exists an integer $a$ satisfying*

$$\gcd(a, q) = 1$$

*for which*

$$\frac{a}{q} = [0; a_1, a_2, \ldots, a_n], \qquad 1 \leq a_i \leq A \quad (1 \leq i \leq n).$$

*Equivalently,*

$$\boxed{\mathcal{D}_A = \mathbb{N}.}$$

In fully quantified form, the conjecture asserts that

$$\exists A \in \mathbb{N} \quad \forall q \in \mathbb{N} \quad \exists a \in \mathbb{Z} \quad \exists n \geq 1 \quad \exists (a_1, \ldots, a_n) \in \mathcal{A}_A^n$$

such that

$$\gcd(a, q) = 1 \qquad \text{and} \qquad \frac{a}{q} = [0; a_1, \ldots, a_n].$$

The word *absolute* is much more important than it sounds. It means that the same constant $A$ must work simultaneously for every denominator $q$. The value of $A$ may not depend on $q$, the numerator $a$, or the length $n$ of the continued fraction expansion.

3.2. **Equivalent Formulations.** The conjecture has several equivalent formulations, each emphasizing a different part of the arithmetic structure.

**Proposition 1.** *The following statements are equivalent:*

(1) *There exists $A \geq 1$ such that*
$$\mathcal{D}_A = \mathbb{N}.$$
(2) *There exists $A \geq 1$ such that every integer $q \geq 1$ admits a coprime numerator $a$ satisfying*
$$\frac{a}{q} = [0; a_1, \ldots, a_n], \qquad a_i \leq A.$$
(3) *There exists $A \geq 1$ such that every positive integer may be written in the form*
$$q = \mathcal{K}_n(a_1, \ldots, a_n)$$
*for some finite sequence*
$$(a_1, \ldots, a_n) \in \mathcal{A}_A^n.$$

*Proof.* We prove the equivalence by identifying denominators with continuants. For a continued fraction of the form
$$[0; a_1, \ldots, a_n],$$
let $q_n$ denote the denominator of the $n$-th convergent. From the recurrence relations for convergents,
$$q_n = a_n q_{n-1} + q_{n-2}.$$
The continuant satisfies the same recurrence,
$$\mathcal{K}_n(a_1, \ldots, a_n) = a_n \mathcal{K}_{n-1}(a_1, \ldots, a_{n-1}) + \mathcal{K}_{n-2}(a_1, \ldots, a_{n-2}),$$
with the same initial conditions. Hence
$$q_n = \mathcal{K}_n(a_1, \ldots, a_n).$$
Therefore,
$$\frac{a}{q} = [0; a_1, \ldots, a_n] \quad \Longleftrightarrow \quad q = \mathcal{K}_n(a_1, \ldots, a_n).$$
Thus a denominator $q$ occurs in a bounded continued fraction with digits in $\mathcal{A}_A$ if and only if
$$q \in \left\{ \mathcal{K}_n(a_1, \ldots, a_n) : n \geq 1,\ (a_1, \ldots, a_n) \in \mathcal{A}_A^n \right\}.$$
This set is exactly $\mathcal{D}_A$. Hence statements 1, 2, and 3 are equivalent. □

The third formulation is particularly useful because it removes the numerator from the problem entirely and recasts the conjecture as a question about the range of the continuant function when its arguments are restricted to a finite alphabet.

3.3. **Why the Conjecture is Difficult.** At first glance, Zaremba's Conjecture appears deceptively simple. Every rational number has a finite continued fraction expansion, and these expansions can be computed directly from the Euclidean algorithm. However, the difficulty of this conjecture does not lie in finding just

a continued fraction expansion. Rather, it lies in controlling the size of every partial quotient appearing in the expansion.

For a general rational number

$$\frac{a}{q} = [0; a_1, a_2, \ldots, a_n],$$

there is no reason to expect the partial quotients

$$a_1, a_2, \ldots, a_n$$

to remain small. Since these partial quotients are exactly the quotients appearing in the Euclidean algorithm applied to $q$ and $a$, a large partial quotient corresponds to a step in which one remainder is much larger than the next. These large quotients occur naturally, and they are not rare in ordinary continued fraction expansions.

Zaremba's Conjecture asks for something much stronger. It does not merely ask whether a particular rational number has bounded partial quotients. Instead, it asks whether, for every denominator $q$, there is at least one numerator $a$, coprime to $q$, such that the entire Euclidean algorithm for the pair $(q, a)$ uses only quotients from one fixed finite set,

$$\mathcal{A}_A = \{1, 2, \ldots, A\}.$$

Equivalently, the conjecture asks whether

$$\forall q \in \mathbb{N}, \qquad q \in \mathcal{D}_A$$

for a single absolute constant $A$. The same $A$ must work for every possible denominator, no matter how large or arithmetically complicated $q$ is.

Also, the conjecture predicts that every positive integer can be generated by the continuant recurrence

$$\mathcal{K}_n(a_1, \ldots, a_n) = a_n \mathcal{K}_{n-1}(a_1, \ldots, a_{n-1}) + \mathcal{K}_{n-2}(a_1, \ldots, a_{n-2}),$$

using only bounded digits

$$(a_1, \ldots, a_n) \in \mathcal{A}_A^n.$$

This is a severe restriction. The continuant recurrence builds denominators from a finite alphabet, yet the conjecture predicts that this restricted construction is still rich enough to produce every positive integer.

The central difficulty is therefore a tension between finiteness and universality. On one hand, the set of allowed digits is finite:

$$|\mathcal{A}_A| = A < \infty.$$

On the other hand, the set of target denominators is infinite:

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Zaremba's Conjecture states that a fixed finite alphabet of continued-fraction digits should generate all positive integers through the nonlinear continuant recurrence.

Another difficulty is that the conjecture is not simply a statement about individual fractions. For a fixed denominator $q$, there are many possible numerators $a$ with

$$(a, q) = 1.$$

Each choice of $a$ gives a different continued fraction expansion. The conjecture requires that among all these possible numerators, at least one produces only bounded partial quotients. Thus the problem is not to analyze one continued fraction, but to understand the entire family

$$\mathcal{R}_q = \left\{ \frac{a}{q} : 1 \le a < q,\ (a, q) = 1 \right\}.$$

In this sense, the conjecture can be viewed as a distribution problem. It asks whether the bounded continued fractions are sufficiently well distributed among rational numbers to hit every possible denominator. Even if bounded continued fractions are numerous, it is not obvious that their denominators cover all of $\mathbb{N}$. They could, in principle, miss infinitely many integers.

*This is why Zaremba's Conjecture is much deeper than its elementary statement suggests. It combines the Euclidean algorithm, rational approximation, recursive denominator growth, and arithmetic distribution into a single problem.* The conjecture states that a highly restricted class of continued fractions is arithmetically universal.

### 3.4. **Zaremba's Original Formulation.**

**Remark 1.** *In his original 1971 paper, Zaremba conjectured that one may take*

$$A = 5.$$

*That is, he predicted that every positive integer $q$ should occur as the denominator of a rational number whose continued fraction expansion uses only the digits*

$$1, 2, 3, 4, 5.$$

*Equivalently, his original prediction may be written as*

$$\mathcal{D}_5 = \mathbb{N}.$$

Although the modern form of the conjecture only requires the existence of some finite absolute constant $A$, the possibility that $A = 5$ suffices remains one of the most intriguing and interesting aspects of the problem.

## 4. Diophantine Approximation and Bounded Continued Fractions

Diophantine approximation studies how well real numbers can be approximated by rational numbers. In its classical one-dimensional form, the central quantity is

$$\left| x - \frac{p}{q} \right|, \qquad x \in \mathbb{R}, \quad \frac{p}{q} \in \mathbb{Q}, \quad q > 0.$$

Since rational numbers with large denominators are usually more complex, the quality of an approximation is measured by comparing the error with the size of $q$. Thus one asks how small

$$\left| x - \frac{p}{q} \right|$$

can be as $q \to \infty$. This perspective is directly related to Zaremba's Conjecture. Continued fractions do not merely represent rational numbers; they organize the best rational approximations to real numbers. The condition that partial quotients are bounded is therefore not only a combinatorial restriction on continued fraction digits, but also a strong Diophantine condition controlling the quality and regularity of rational approximation.

4.1. **Rational Approximation and Convergents.** We begin with the basic approximation property of convergents. Let

$$x = [a_0; a_1, a_2, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$$

and let

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n]$$

be its $n$-th convergent. The denominator sequence $\{q_n\}$ measures the arithmetic complexity of the approximants, while the error $|x - p_n/q_n|$ measures their accuracy.

**Lemma 4** (Approximation by Convergents)**.** *For every $n \geq 0$,*

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

*Proof.* Write the tail after the $n$-th partial quotient as

$$\alpha_{n+1} = [a_{n+1}; a_{n+2}, \ldots] > 0.$$

Then

$$x = [a_0; a_1, \ldots, a_n, \alpha_{n+1}] = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}.$$

Therefore

$$\begin{aligned} \left| x - \frac{p_n}{q_n} \right| &= \left| \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n} \right| \\ &= \left| \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n (\alpha_{n+1} q_n + q_{n-1})} \right|. \end{aligned}$$

By the determinant identity,

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1},$$

so

$$\left| q_n p_{n-1} - p_n q_{n-1} \right| = 1.$$

Hence

$$\left| x - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}.$$

Since

$$q_{n+1} = a_{n+1}q_n + q_{n-1} \qquad \text{and} \qquad \alpha_{n+1} > a_{n+1},$$

we have

$$\alpha_{n+1}q_n + q_{n-1} > q_{n+1}.$$

Thus

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

□

This lemma shows that convergents provide unusually strong rational approximations. In fact, they are essentially the best possible rational approximations with bounded denominator.

**Lemma 5** (Best Approximation Property)**.** *Let $x \in \mathbb{R} \setminus \mathbb{Q}$, and let $p_n/q_n$ be a convergent of $x$. If $a/b \in \mathbb{Q}$ satisfies*

$$0 < b < q_{n+1}, \qquad \frac{a}{b} \neq \frac{p_n}{q_n},$$

*then*

$$\left| q_n x - p_n \right| < \left| bx - a \right|.$$

*Proof.* The statement says that $p_n/q_n$ minimizes the linear form

$$|qx - p|$$

among all integer pairs $(p, q) \in \mathbb{Z}^2$ with $0 < q < q_{n+1}$, except for the pair $(p_n, q_n)$ itself. Equivalently, if

$$0 < b < q_{n+1} \qquad \text{and} \qquad (a, b) \neq (p_n, q_n),$$

then the primitive lattice vector $(p_n, q_n)$ gives a strictly closer approach to the line $p = qx$ than $(a, b)$. Thus no distinct rational number $a/b$ with $0 < b < q_{n+1}$ can satisfy

$$|bx - a| \leq |q_n x - p_n|.$$

Hence

$$|q_n x - p_n| < |bx - a|.$$

□

The preceding result explains why continued fractions are fundamental in Diophantine approximation: their convergents are not arbitrary rational approximations, but optimal ones. This is the reason that any arithmetic condition imposed on continued fraction digits has immediate consequences for rational approximation.

4.2. **Dirichlet's Approximation Theorem.** A central result in Diophantine approximation is Dirichlet's theorem, which guarantees that every irrational number has infinitely many good rational approximations.

**Theorem 1** (Dirichlet Approximation Theorem)**.** *For every irrational number $x \in \mathbb{R} \setminus \mathbb{Q}$, there exist infinitely many coprime integers $p, q$, with $q > 0$, such that*

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}.$$

*Proof.* Since $x \notin \mathbb{Q}$, its continued fraction expansion is infinite. Hence it has infinitely many convergents

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n].$$

By the approximation estimate for convergents,

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

Moreover, by the coprimality of convergents,

$$\gcd(p_n, q_n) = 1.$$

Therefore the pairs $(p_n, q_n)$ give infinitely many coprime rational approximations satisfying

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

This proves the theorem. □

Dirichlet's theorem says that the exponent 2 is universally attainable. However, the central issue is not merely the existence of good approximations. For Zaremba's Conjecture, the important question is whether one can obtain denominators while forcing the continued fraction digits to remain bounded.

4.3. **Approximation Constants.** It is useful to measure the quality of rational approximation through an exponent. For $x \in \mathbb{R}$, define the irrationality exponent

$$\mu(x) = \sup \left\{ \mu > 0 : \left| x - \frac{p}{q} \right| < \frac{1}{q^\mu} \text{ has infinitely many rational solutions } \frac{p}{q} \right\}.$$

Dirichlet's theorem implies that

$$\mu(x) \geq 2 \qquad (x \in \mathbb{R} \setminus \mathbb{Q}).$$

Some numbers admit much better approximations, while others are resistant to approximation beyond the Dirichlet exponent.

In geometric Diophantine approximation, one often replaces the denominator $q$ by a height function $H$, which measures arithmetic complexity. In the classical

case of rational numbers,

$$H\left(\frac{p}{q}\right) \asymp q$$

when $p/q$ is in lowest terms. Thus inequalities of the form

$$\left|x - \frac{p}{q}\right| \ll \frac{1}{q^{\mu}}$$

may be viewed as comparisons between distance and height. For the present paper, this interpretation is useful because Zaremba's Conjecture is also a height problem in disguise: it asks whether every height level $q$ can be realized by a rational number whose continued fraction digits come from a fixed finite alphabet.

4.4. **Bounded Partial Quotients.** We now explain the Diophantine meaning of bounded partial quotients. Let

$$x = [a_0; a_1, a_2, \ldots]$$

be irrational. We say that $x$ has bounded partial quotients if there exists $A \geq 1$ such that

$$a_n \leq A \qquad (n \geq 1).$$

Equivalently,

$$(a_1, a_2, \ldots) \in \mathcal{A}_A^{\mathbb{N}}, \qquad \mathcal{A}_A = \{1, 2, \ldots, A\}.$$

This condition strongly controls the growth of the denominators $q_n$. Indeed, since

$$q_{n+1} = a_{n+1}q_n + q_{n-1},$$

the bound $a_{n+1} \leq A$ implies

$$q_{n+1} \leq (A+1)q_n.$$

Thus consecutive denominators cannot grow too irregularly.

**Lemma 6.** *If $x = [a_0; a_1, a_2, \ldots]$ has partial quotients bounded by $A$, then for every convergent $p_n/q_n$,*

$$\left|x - \frac{p_n}{q_n}\right| > \frac{1}{(A+2)q_n^2}.$$

*Proof.* From the exact error formula for a convergent,

$$\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}, \qquad \alpha_{n+1} = [a_{n+1}; a_{n+2}, \ldots].$$

Since all partial quotients are at most $A$,

$$a_j \leq A \quad (j \geq 1),$$

we have

$$\alpha_{n+1} < A + 1.$$

Also $q_{n-1} < q_n$. Hence

$$\alpha_{n+1}q_n + q_{n-1} < (A+1)q_n + q_n = (A+2)q_n.$$

Therefore

$$\left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n(A+2)q_n} = \frac{1}{(A+2)q_n^2}.$$

□

This lemma shows that bounded partial quotients prevent the convergents from being too good. In other words, numbers with bounded partial quotients are badly approximable.

**Definition 7** (Badly Approximable Number)**.** *A real number $x$ is called* badly approximable *if there exists a constant $c(x) > 0$ such that*

$$\left| x - \frac{p}{q} \right| > \frac{c(x)}{q^2}$$

*for every rational number $p/q$.*

**Theorem 2** (Bounded Partial Quotients and Bad Approximation)**.** *An irrational number $x$ is badly approximable if and only if its continued fraction expansion has bounded partial quotients.*

*Proof.* Suppose first that the partial quotients of $x$ are bounded by $A$. The previous lemma gives

$$\left| x - \frac{p_n}{q_n} \right| > \frac{1}{(A+2)q_n^2}$$

for every convergent $p_n/q_n$. Since convergents are best approximations, any rational $p/q$ lies between two neighboring convergent scales and cannot approximate $x$ essentially better than the corresponding convergent. Hence there exists a constant $c(x) > 0$ such that

$$\left| x - \frac{p}{q} \right| > \frac{c(x)}{q^2} \qquad \left( \frac{p}{q} \in \mathbb{Q} \right).$$

Thus $x$ is badly approximable.

Conversely, suppose the partial quotients are unbounded. Then there exists a subsequence $a_{n_j+1} \to \infty$. For the corresponding convergents,

$$q_{n_j+1} = a_{n_j+1}q_{n_j} + q_{n_j-1},$$

so

$$\frac{q_{n_j+1}}{q_{n_j}} \to \infty.$$

Using the approximation estimate,

$$\left| x - \frac{p_{n_j}}{q_{n_j}} \right| < \frac{1}{q_{n_j}q_{n_j+1}},$$

we obtain

$$q_{n_j}^2 \left| x - \frac{p_{n_j}}{q_{n_j}} \right| < \frac{q_{n_j}}{q_{n_j+1}} \to 0.$$

Therefore no positive constant $c(x)$ can satisfy

$$\left| x - \frac{p}{q} \right| > \frac{c(x)}{q^2}$$

for all rational $p/q$. Hence $x$ is not badly approximable. This proves the equivalence. □

This theorem is one of the most important bridges between continued fractions and Diophantine approximation. It shows that bounded partial quotients are equivalent to a precise approximation-theoretic property.

4.5. **A Measure-Theoretic Heuristic.** Bounded partial quotients define a very special subset of the real line. For a fixed $A$, consider

$$\mathcal{B}_A = \{x \in [0,1] : x = [0; a_1, a_2, \ldots],\ a_i \in \mathcal{A}_A \text{ for all } i\}.$$

This is a Cantor-like set: at each stage of the continued fraction expansion, only finitely many digits are allowed. Although the set is infinite and highly structured, it is small from the viewpoint of Lebesgue measure.

To see why such sets are thin, recall that the Gauss map

$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor$$

generates the continued fraction expansion. The condition $a_1 = m$ corresponds to the interval

$$\frac{1}{m+1} < x < \frac{1}{m}.$$

Thus allowing only $1 \le a_1 \le A$ restricts $x$ to

$$\bigcup_{m=1}^{A} \left( \frac{1}{m+1}, \frac{1}{m} \right).$$

The total length of this first-stage set is

$$\sum_{m=1}^{A} \left( \frac{1}{m} - \frac{1}{m+1} \right) = 1 - \frac{1}{A+1}.$$

At each later stage, a similar restriction is imposed again. Heuristically, successive digit restrictions remove a positive proportion of the remaining intervals. This explains why the set of infinite continued fractions with all digits bounded by a fixed $A$ is extremely sparse, even though it has rich fractal structure.

This sparseness is precisely what makes Zaremba's Conjecture surprising. The conjecture does not claim that bounded continued fractions are common

among all real numbers. Instead, it predicts that their rational truncations are arithmetically rich enough to realize every denominator.

4.6. **Connection to Zaremba's Conjecture.** The results above clarify the meaning of bounded partial quotients. On the analytic side, bounded partial quotients correspond to badly approximable numbers. On the arithmetic side, Zaremba's Conjecture concerns rational numbers

$$\frac{a}{q} = [0; a_1, \dots, a_n]$$

whose finite continued fraction digits satisfy

$$(a_1, \dots, a_n) \in \mathcal{A}_A^n.$$

Thus the conjecture may be viewed as a finite rational analogue of the theory of badly approximable numbers. Instead of asking which real numbers have bounded partial quotients forever, Zaremba asks whether every denominator $q$ occurs at the end of some finite bounded continued fraction.

Equivalently, the conjecture asks whether the finite alphabet

$$\mathcal{A}_A = \{1, 2, \dots, A\}$$

is sufficient to generate all positive integers through continuants:

$$q = \mathcal{K}_n(a_1, \dots, a_n).$$

From the Diophantine approximation viewpoint, this means that every denominator should admit at least one rational representative whose Euclidean algorithm is uniformly controlled. This is why the conjecture lies naturally at the intersection of continued fractions, rational approximation, and arithmetic distribution.

The Diophantine approximation perspective also explains why the conjecture is difficult. Bounded partial quotients form a restricted symbolic system, while Zaremba's Conjecture asserts that this restricted system nevertheless produces all possible denominators. The next section develops the matrix and semigroup formulation that makes this arithmetic distribution problem more explicit.

## 5. Matrix and Semigroup Formulation

One of the most useful modern viewpoints on Zaremba's Conjecture is obtained by translating continued fractions into products of integer matrices. This changes the problem from one about rational numbers into one about matrix semigroups and their orbits.

### 5.1. **Continued-Fraction Matrices.**

**Definition 8.** *For $a \in \mathbb{N}$, define*

$$M(a) = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}.$$

*We call $M(a)$ the continued-fraction matrix associated with the digit $a$.*

Since

$$\det M(a) = -1,$$

each $M(a)$ is unimodular and hence belongs to $\mathrm{GL}(2,\mathbb{Z})$. The key point is that multiplication by $M(a)$ reproduces the same recurrence structure that appears in convergents and continuants.

**Lemma 7.** *For every $a \in \mathbb{N}$ and every column vector*

$$\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2,$$

*one has*

$$M(a)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x + ay \end{pmatrix}.$$

*Proof.* This follows directly from matrix multiplication:

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \cdot x + 1 \cdot y \\ 1 \cdot x + a \cdot y \end{pmatrix} = \begin{pmatrix} y \\ x + ay \end{pmatrix}.$$

□

Thus the matrix $M(a)$ sends the pair $(x, y)$ to $(y, x + ay)$, exactly mirroring the recurrence relation

$$u_k = a_k u_{k-1} + u_{k-2}.$$

5.2. **Matrix Representation of Convergents.** The following lemma gives the main connection between continued fractions and matrix products.

**Lemma 8.** *Let*

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n].$$

*Then*

$$M(a_0)M(a_1)\cdots M(a_n) = \begin{pmatrix} q_{n-1} & q_n \\ p_{n-1} & p_n \end{pmatrix},$$

*with the usual initial conventions for convergents.*

*Proof.* We prove the claim by induction on $n$. For $n = 0$, the statement agrees with the initial data for convergents. Suppose the formula holds for $n - 1$. Then

$$\begin{aligned} M(a_0)\cdots M(a_n) &= \begin{pmatrix} q_{n-2} & q_{n-1} \\ p_{n-2} & p_{n-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} \\ &= \begin{pmatrix} q_{n-1} & a_n q_{n-1} + q_{n-2} \\ p_{n-1} & a_n p_{n-1} + p_{n-2} \end{pmatrix}. \end{aligned}$$

Using

$$q_n = a_n q_{n-1} + q_{n-2}, \qquad p_n = a_n p_{n-1} + p_{n-2},$$

we obtain

$$M(a_0)\cdots M(a_n) = \begin{pmatrix} q_{n-1} & q_n \\ p_{n-1} & p_n \end{pmatrix}.$$

Thus the result follows by induction. □

This lemma shows that the arithmetic of convergents is encoded inside a single matrix product. In particular, numerators and denominators of continued fractions appear as entries of matrices in $\mathrm{GL}(2,\mathbb{Z})$.

5.3. **Continuants as Matrix Entries.** For Zaremba's Conjecture, the most important case is

$$[0; a_1, \ldots, a_n].$$

In this case, the denominator is the continuant

$$\mathcal{K}_n(a_1, \ldots, a_n).$$

**Lemma 9.** *For $a_1, \ldots, a_n \in \mathbb{N}$, the lower-right entry of*

$$M(a_1)M(a_2)\cdots M(a_n)$$

*is*

$$\mathcal{K}_n(a_1, \ldots, a_n).$$

*Proof.* Let $Q_n$ denote the lower-right entry of $M(a_1)\cdots M(a_n)$. From the previous matrix recurrence,

$$Q_n = a_n Q_{n-1} + Q_{n-2}.$$

The initial values are

$$Q_0 = 1, \qquad Q_1 = a_1.$$

These are exactly the initial conditions and recurrence defining the continuant:

$$\mathcal{K}_0 = 1, \qquad \mathcal{K}_1(a_1) = a_1, \qquad \mathcal{K}_n = a_n\mathcal{K}_{n-1} + \mathcal{K}_{n-2}.$$

Therefore

$$Q_n = \mathcal{K}_n(a_1, \ldots, a_n).$$

□

Thus every denominator generated by a finite continued fraction may be regarded as a distinguished entry of a matrix product.

5.4. **The Continued-Fraction Semigroup.** We now impose the bounded digit condition. Let

$$\mathcal{A}_A = \{1, 2, \ldots, A\}.$$

**Definition 9.** *For $A \geq 1$, define the continued-fraction semigroup*

$$\Gamma_A = \langle M(a) : a \in \mathcal{A}_A \rangle.$$

*Equivalently,*

$$\Gamma_A = \left\{ M(a_1)\cdots M(a_n) : n \geq 1,\ (a_1, \ldots, a_n) \in \mathcal{A}_A^n \right\}.$$

The word *semigroup* is important: $\Gamma_A$ is closed under multiplication, but we do not require it to contain inverses. Thus $\Gamma_A$ consists only of finite products of the allowed generators $M(1), M(2), \ldots, M(A)$.

The bounded continued fractions appearing in Zaremba's Conjecture are exactly the finite words in this semigroup. A sequence

$$(a_1, \ldots, a_n) \in \mathcal{A}_A^n$$

corresponds to the matrix

$$M(a_1) \cdots M(a_n) \in \Gamma_A.$$

5.5. **Semigroup Reformulation of Zaremba's Conjecture.** We now connect $\Gamma_A$ with the denominator set $\mathcal{D}_A$.

**Theorem 3** (Semigroup Reformulation)**.** *For $A \geq 1$ and $q \in \mathbb{N}$,*

$$q \in \mathcal{D}_A$$

*if and only if there exists a matrix*

$$\gamma = \begin{pmatrix} * & * \\ * & q \end{pmatrix} \in \Gamma_A.$$

*Proof.* Suppose first that $q \in \mathcal{D}_A$. By definition, there exist $n \geq 1$ and digits

$$(a_1, \ldots, a_n) \in \mathcal{A}_A^n$$

such that

$$q = \mathcal{K}_n(a_1, \ldots, a_n).$$

Since each $a_i \in \mathcal{A}_A$, the product

$$\gamma = M(a_1) \cdots M(a_n)$$

belongs to $\Gamma_A$. By the previous lemma, the lower-right entry of $\gamma$ is precisely

$$\mathcal{K}_n(a_1, \ldots, a_n) = q.$$

Hence

$$\gamma = \begin{pmatrix} * & * \\ * & q \end{pmatrix} \in \Gamma_A.$$

Conversely, suppose that

$$\gamma = M(a_1) \cdots M(a_n) = \begin{pmatrix} * & * \\ * & q \end{pmatrix} \in \Gamma_A.$$

By definition of $\Gamma_A$, each digit satisfies

$$a_i \in \mathcal{A}_A.$$

Since the lower-right entry of this product is

$$q = \mathcal{K}_n(a_1, \ldots, a_n),$$

we conclude that

$$q \in \mathcal{D}_A.$$

Therefore the two conditions are equivalent. □

Therefore Zaremba's Conjecture may be rewritten as the assertion that, for some finite $A$, every positive integer appears as the lower-right entry of a matrix in $\Gamma_A$:

$$\boxed{\exists A \geq 1 \quad \text{such that} \quad \{\gamma_{22} : \gamma \in \Gamma_A\} = \mathbb{N}.}$$

This is the matrix-semigroup form of the conjecture. It replaces the original continued-fraction question with a reachability problem for entries of matrices generated by a finite set of transformations.

5.6. **Orbit Interpretation.** The semigroup $\Gamma_A$ also acts on lattice vectors in $\mathbb{Z}^2$. Starting from the vector

$$e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

a product $\gamma = M(a_1) \cdots M(a_n)$ produces

$$\gamma e_2 = \begin{pmatrix} * \\ \mathcal{K}_n(a_1, \ldots, a_n) \end{pmatrix}.$$

Thus the denominator generated by the word $(a_1, \ldots, a_n)$ is the second coordinate of the orbit point $\gamma e_2$.

In this language, Zaremba's Conjecture asks whether the orbit

$$\Gamma_A e_2 = \{\gamma e_2 : \gamma \in \Gamma_A\}$$

contains a vector whose second coordinate is $q$, for every $q \in \mathbb{N}$. Equivalently,

$$\forall q \in \mathbb{N}, \quad \exists \gamma \in \Gamma_A \quad \text{such that} \quad (\gamma e_2)_2 = q.$$

This viewpoint is central to modern work on the conjecture. It allows the use of tools from dynamics, arithmetic combinatorics, expansion theory, and analytic number theory. In particular, the Bourgain-Kontorovich approach studies the distribution of entries of matrices in such thin semigroups and proves that, for suitable $A$, almost every integer occurs.

## 6. Bourgain-Kontorovich and Density-One Results

The modern breakthrough on Zaremba's Conjecture is due to Bourgain and Kontorovich, who proved that the conjecture is true for almost every positive integer. Their result does not show that every denominator occurs, but it shows that the set of possible exceptions has asymptotic density zero. Thus, in a precise counting sense, bounded continued fractions generate nearly all denominators. [BK14]

The key idea is to translate Zaremba's Conjecture into a problem about thin orbits of matrix semigroups. For a finite alphabet

$$\mathcal{A}_A = \{1, 2, \ldots, A\},$$

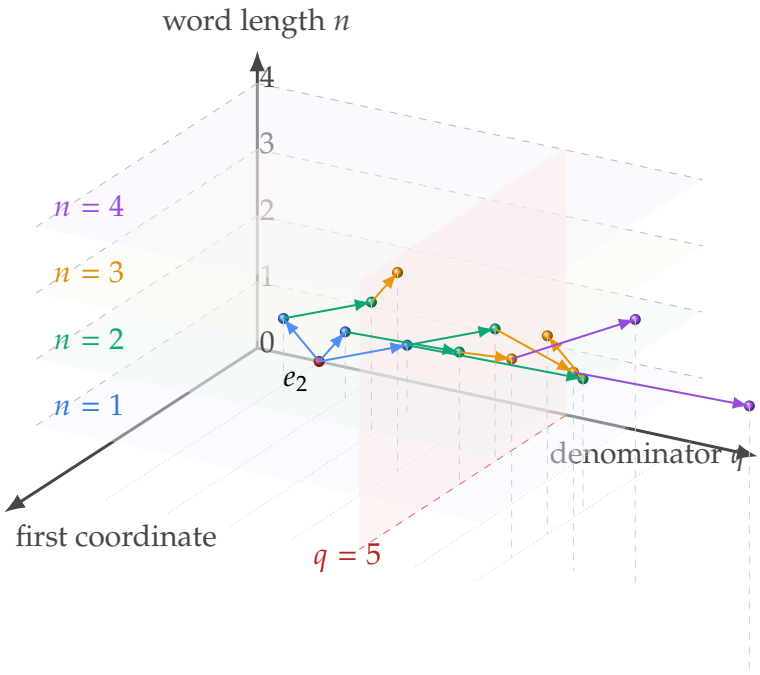


FIGURE 1. A three-dimensional geometric representation of the orbit $\Gamma_A e_2$. Each point corresponds to a lattice vector generated by a finite word in $\mathcal{A}_A$. The second coordinate is the denominator $q$, so Zaremba's Conjecture asks whether every positive denominator level is attained by some orbit point.

let

$$\mathcal{D}_A = \left\{ q \in \mathbb{N} : q = \mathcal{K}_n(a_1, \dots, a_n) \text{ for some } (a_1, \dots, a_n) \in \mathcal{A}_A^n \right\}.$$

Zaremba's Conjecture predicts that, for some absolute $A$,

$$\mathcal{D}_A = \mathbb{N}.$$

Bourgain and Kontorovich proved the weaker but very deep statement

$$\lim_{N \to \infty} \frac{\#(\mathcal{D}_A \cap [1, N])}{N} = 1$$

for some effectively computable finite alphabet. This means that the complement

$$[1, N] \setminus \mathcal{D}_A$$

has size $o(N)$. In other words, the bounded-denominator set misses at most a density-zero subset of the positive integers.

6.1. **Density-One Form of Zaremba's Conjecture.** We first record the main result in the language used throughout this paper.

**Theorem 4** (Bourgain–Kontorovich Density-One Theorem)**.** *There exists an effectively computable integer $A \geq 1$ such that*

$$\lim_{N \to \infty} \frac{1}{N} \#\{q \leq N : q \in \mathcal{D}_A\} = 1.$$

*Equivalently,*

$$\#\{q \le N : q \notin \mathcal{D}_A\} = o(N).$$

This theorem should be compared with the full Zaremba conjecture,

$$\exists A \ge 1 \quad \text{such that} \quad \mathcal{D}_A = \mathbb{N}.$$

The Bourgain–Kontorovich theorem proves instead that

$$\exists A \ge 1 \quad \text{such that} \quad \mathcal{D}_A \text{ has natural density 1.}$$

Thus the theorem proves that bounded continued fractions generate almost every integer, but it does not rule out the possibility of infinitely many exceptional denominators.

**Definition 10** (Density One)**.** *A set $\mathcal{S} \subseteq \mathbb{N}$ has* density one *if*

$$\lim_{N\to\infty} \frac{\#(\mathcal{S} \cap [1, N])}{N} = 1.$$

*Equivalently, its complement has density zero:*

$$\#\big([1, N] \setminus \mathcal{S}\big) = o(N).$$

In this terminology, Bourgain and Kontorovich proved that, for a suitable finite alphabet $\mathcal{A}_A$, the denominator set $\mathcal{D}_A$ has density one.

6.2. **Hausdorff Dimension and Local Obstructions.** A major role in the Bourgain–Kontorovich work is played by the Cantor-like set of infinite continued fractions with bounded digits:

$$C_A = \{x \in (0, 1) : x = [0; a_1, a_2, \ldots],\ a_i \in \mathcal{A}_A \text{ for all } i\}.$$

This set is fractal. Its Hausdorff dimension is denoted by

$$\delta_A = \dim_H(C_A).$$

The larger the alphabet, the closer $\delta_A$ is to 1. A large value of $\delta_A$ means that the bounded continued-fraction system is still thin, but not too thin.

Bourgain and Kontorovich prove a refined local-global statement. For a general alphabet $\mathcal{A}$, not every residue class modulo $m$ need be represented by denominators in $\mathcal{D}_\mathcal{A}$. Therefore they introduce the notion of admissibility.

**Definition 11** (Admissible Denominator)**.** *Let $\mathcal{A} \subset \mathbb{N}$ be a finite alphabet. An integer $q$ is called* admissible *for $\mathcal{A}$ if it satisfies all finite congruence obstructions:*

$$q \in \mathcal{D}_\mathcal{A} \pmod{m} \qquad \text{for every } m \ge 2.$$

*The set of admissible integers is denoted by*

$$\mathfrak{A}_\mathcal{A} = \{q \in \mathbb{Z} : q \text{ is admissible for } \mathcal{A}\}.$$

For alphabets of the form

$$\mathcal{A}_A = \{1, 2, \ldots, A\},$$

the local obstruction problem behaves particularly well: for suitable $A$, there are no congruence obstructions. In that case, admissibility becomes automatic, and the density-one theorem may be stated directly in terms of $\mathcal{D}_A$.

The refined Bourgain–Kontorovich theorem may be summarized as follows.

**Theorem 5** (Almost Every Admissible Integer)**.** *There exists an effectively computable constant $\delta_0 < 1$ such that if*

$$\delta_A > \delta_0,$$

*then almost every admissible integer is represented as a denominator. More precisely, for some constant $c = c(A) > 0$,*

$$\frac{\#(\mathcal{D}_A \cap [N/2, N])}{\#(\mathfrak{A}_A \cap [N/2, N])} = 1 + O\Big(N^{-c/\log\log N}\Big)$$

*as $N \to \infty$.*

This is the true strength of the result. It says not merely that many denominators are produced, but that among the integers that pass all local congruence tests, almost all are actually produced by bounded continued fractions.

6.3. **Representation Numbers.** The proof studies not just whether a denominator appears, but how many times it appears. For $q \in \mathbb{N}$, define the representation number

$$R_N(q) = \#\left\{\gamma \in \Omega_N : \langle \gamma e_2, e_2 \rangle = q\right\},$$

where $\Omega_N \subset \Gamma_A$ is a carefully constructed finite ensemble of matrices of size approximately $N$, and

$$e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Since

$$\gamma e_2 = \begin{pmatrix} * \\ q \end{pmatrix},$$

the inner product

$$\langle \gamma e_2, e_2 \rangle$$

extracts the second coordinate, which is exactly the denominator. Therefore

$$R_N(q) > 0 \quad \Longrightarrow \quad q \in \mathcal{D}_A.$$

The expected total number of representations is controlled by the size of $\Omega_N$. Since the orbit has fractal dimension $\delta_A$, one expects

$$\#\Omega_N \asymp N^{2\delta_A}.$$

If these representations are spread roughly evenly among denominators of size $N$, then a typical denominator should have multiplicity about

$$\frac{\#\Omega_N}{N} \asymp N^{2\delta_A - 1}.$$

This heuristic already explains why the condition

$$\delta_A > \frac{1}{2}$$

is natural: if $\delta_A < 1/2$, then the expected multiplicity $N^{2\delta_A - 1}$ tends to 0, so the set is too sparse to cover almost all denominators.

6.4. **The Exponential Sum.** The central analytic object is an exponential sum over the matrix ensemble:

$$S_N(\theta) = \sum_{\gamma \in \Omega_N} e(\theta \langle \gamma e_2, e_2 \rangle), \qquad e(x) = e^{2\pi i x}.$$

The representation number is recovered as the Fourier coefficient

$$R_N(q) = \int_0^1 S_N(\theta) e(-q\theta)\, d\theta.$$

This identity is simply Fourier inversion. Indeed,

$$\int_0^1 e\big((m-q)\theta\big)\, d\theta = \begin{cases} 1, & m = q, \\ 0, & m \neq q. \end{cases}$$

Therefore

$$\begin{aligned} \int_0^1 S_N(\theta) e(-q\theta)\, d\theta &= \int_0^1 \sum_{\gamma \in \Omega_N} e(\theta \langle \gamma e_2, e_2 \rangle)\, e(-q\theta)\, d\theta \\ &= \sum_{\gamma \in \Omega_N} \int_0^1 e\big((\langle \gamma e_2, e_2 \rangle - q)\theta\big)\, d\theta \\ &= \#\{\gamma \in \Omega_N : \langle \gamma e_2, e_2 \rangle = q\} \\ &= R_N(q). \end{aligned}$$

This is where calculus enters the proof: the counting problem is converted into the study of an integral over the unit interval.

6.5. **Major and Minor Arcs.** The integral for $R_N(q)$ is analyzed using the Hardy–Littlewood circle method. One decomposes

$$[0,1] = \mathfrak{M} \cup \mathfrak{m},$$

where $\mathfrak{M}$ is the set of *major arcs* and $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$ is the set of *minor arcs*. The major arcs are neighborhoods of rational points with small denominator:

$$\mathfrak{M} = \bigcup_{r < Q} \bigcup_{\substack{a \bmod r \\ (a,r)=1}} \left[ \frac{a}{r} - \frac{Q}{N}, \frac{a}{r} + \frac{Q}{N} \right].$$

The parameter $Q$ grows slowly with $N$, typically of the form

$$Q = N^{c/\log\log N}.$$

The representation number is then written as

$$R_N(q) = M_N(q) + E_N(q),$$

where

$$M_N(q) = \int_{\mathfrak{M}} S_N(\theta) e(-q\theta)\, d\theta$$

is the major-arc contribution, and

$$E_N(q) = \int_{\mathfrak{m}} S_N(\theta) e(-q\theta)\, d\theta$$

is the minor-arc error.

On the major arcs, $\theta$ is close to a rational number:

$$\theta = \frac{a}{r} + \beta.$$

The main phenomenon is that $S_N(\theta)$ approximately factors into a modular part and a real analytic part:

$$S_N\left(\frac{a}{r} + \beta\right) \approx \nu_r(a)\, \varpi_N(\beta).$$

Here $\nu_r(a)$ is a congruence term measuring the distribution of the orbit modulo $r$, while $\varpi_N(\beta)$ is an archimedean term measuring the continuous size distribution.

This gives a factorization of the main term:

$$M_N(q) \approx \mathfrak{S}(q)\, \Pi_N(q),$$

where $\mathfrak{S}(q)$ is the *singular series* and $\Pi_N(q)$ is the *singular integral*. The singular series detects local congruence obstructions, while the singular integral supplies the expected analytic size. For admissible $q$, Bourgain and Kontorovich obtain a lower bound of the form

$$M_N(q) \gg \frac{1}{\log\log N} \frac{\#\Omega_N}{N}.$$

6.6. **A Compact Major-Arc Argument.** The following simplified proposition captures the role of the major arcs.

**Proposition 2** (Major-Arc Lower Bound)**.** *For admissible $q \asymp N$, the major-arc contribution satisfies*

$$M_N(q) \gg \frac{1}{\log\log N} \frac{\#\Omega_N}{N}.$$

*Proof.* On the major arcs, write

$$\theta = \frac{a}{r} + \beta.$$

The Bourgain–Kontorovich construction gives the approximate splitting

$$S_N\left(\frac{a}{r} + \beta\right) = \nu_r(a)\varpi_N(\beta) + O(Q^{-4}\#\Omega_N).$$

Substituting this into the major-arc integral gives

$$M_N(q) = \sum_{r<Q} \sum_{\substack{a \bmod r \\ (a,r)=1}} \nu_r(a) e\left(-q\frac{a}{r}\right) \int \varpi_N(\beta) e(-q\beta)\, d\beta + \text{error}.$$

The first factor is the truncated singular series

$$\mathfrak{S}_Q(q) = \sum_{r<Q} \sum_{\substack{a \bmod r \\ (a,r)=1}} \nu_r(a) e\left(-q\frac{a}{r}\right),$$

and the second factor is the singular integral

$$\Pi_N(q) = \int \varpi_N(\beta) e(-q\beta)\, d\beta.$$

For admissible $q$, the singular series is bounded below by

$$\mathfrak{S}_Q(q) \gg \frac{1}{\log\log q},$$

while the singular integral has the expected size

$$\Pi_N(q) \gg \frac{\#\Omega_N}{N}.$$

Since $q \asymp N$, this gives

$$M_N(q) \gg \frac{1}{\log\log N} \frac{\#\Omega_N}{N}.$$

□

This proposition shows why admissible integers should be represented: the main term is positive and of the expected order. The remaining task is to prove that the minor-arc error does not usually cancel this main term.

6.7. **The Minor-Arc Estimate.** The difficult part of the Bourgain–Kontorovich argument is the minor-arc estimate. Instead of proving a strong pointwise bound for every $q$, they prove a strong average bound:

$$\sum_{q \asymp N} |E_N(q)|^2 \ll \frac{(\#\Omega_N)^2}{N} Q^{-c}$$

for some $c > 0$. This is an $L^2$-estimate. It means that large errors can occur only rarely.

The proof uses the bilinear structure of matrix products. If

$$\gamma = \gamma_1 \gamma_2,$$

then

$$\langle \gamma e_2, e_2 \rangle = \langle \gamma_1 \gamma_2 e_2, e_2 \rangle = \langle \gamma_2 e_2, {}^t\gamma_1 e_2 \rangle.$$

Thus the phase

$$e(\theta\langle \gamma e_2, e_2\rangle)$$

becomes bilinear in two lattice vectors. This is the arithmetic structure that allows Cauchy–Schwarz, Poisson summation, and Vinogradov-type bilinear estimates to be used.

The ensemble $\Omega_N$ is not simply all matrices of norm $< N$. It is carefully decomposed as

$$\Omega_N = \mathfrak{X}\,\Xi_1\Xi_2\cdots\Xi_J,$$

where the factors $\Xi_j$ have controlled eigenvalues, controlled expanding directions, and nearly multiplicative norms. This construction allows the authors to keep the matrix products large enough to represent denominators of size $N$, while still retaining enough factorization to estimate exponential sums.

6.8. **From Major and Minor Arcs to Density One.** We now prove, in simplified form, how the density-one conclusion follows once the major-arc lower bound and the minor-arc $L^2$-estimate are known.

**Proposition 3** (Density-One Consequence)**.** *Assume that for all admissible $q \asymp N$,*

$$M_N(q) \gg \frac{\#\Omega_N}{N\log\log N},$$

*and that*

$$\sum_{q\asymp N} |E_N(q)|^2 \ll \frac{(\#\Omega_N)^2}{N} Q^{-c}.$$

*Then the number of admissible $q \asymp N$ that are not represented is*

$$\ll NQ^{-c/2}(\log\log N)^2.$$

*In particular, this exceptional set has density zero.*

*Proof.* Let $\mathcal{E}_N$ be the set of admissible integers $q \asymp N$ for which $R_N(q) = 0$. For $q \in \mathcal{E}_N$,

$$0 = R_N(q) = M_N(q) + E_N(q),$$

so

$$|E_N(q)| = M_N(q).$$

By the major-arc lower bound,

$$|E_N(q)| \gg \frac{\#\Omega_N}{N\log\log N}.$$

Hence

$$1 \ll \frac{N^2(\log\log N)^2}{(\#\Omega_N)^2}|E_N(q)|^2.$$

Summing over $q \in \mathcal{E}_N$, we obtain

$$\#\mathcal{E}_N \ll \frac{N^2(\log\log N)^2}{(\#\Omega_N)^2} \sum_{q \asymp N} |E_N(q)|^2.$$

Using the minor-arc estimate gives

$$\#\mathcal{E}_N \ll \frac{N^2(\log\log N)^2}{(\#\Omega_N)^2} \cdot \frac{(\#\Omega_N)^2}{N} Q^{-c}.$$

Therefore

$$\#\mathcal{E}_N \ll NQ^{-c}(\log\log N)^2.$$

Since $Q = N^{c_0/\log\log N}$, the factor $Q^{-c}$ tends to zero as a negative power of $N^{1/\log\log N}$. Thus

$$\#\mathcal{E}_N = o(N).$$

This proves the density-one consequence. □

This argument is the heart of the method. The major arcs show that admissible denominators should appear with positive expected multiplicity, and the minor arcs show that the error is too small on average to destroy this positivity for more than a density-zero set of integers.

6.9. **Why the Result Matters.** The Bourgain–Kontorovich theorem is not the full Zaremba conjecture, but it is a major confirmation of its underlying philosophy. Zaremba predicted that a fixed finite alphabet should generate every denominator. Bourgain and Kontorovich proved that, for a suitable fixed finite alphabet, it generates almost every denominator:

$$\mathcal{D}_A = \mathbb{N} \quad \text{up to a density-zero exceptional set.}$$

The proof shows that the semigroup orbit

$$\Gamma_A e_2$$

is thin but still arithmetically well distributed. This is a striking local-global phenomenon: local congruence conditions and archimedean size constraints predict representation, and the theorem proves that these predictions are correct for almost every admissible integer.

The result also explains why matrix methods are essential. Continued fractions alone reveal the recurrence

$$q_n = a_n q_{n-1} + q_{n-2},$$

but the matrix formulation exposes additional structure:

$$\langle \gamma_1\gamma_2 e_2, e_2\rangle = \langle \gamma_2 e_2, {}^t\gamma_1 e_2\rangle.$$

This bilinear identity is what makes analytic number theory applicable. It turns a problem about continued-fraction denominators into a problem about exponential sums over thin matrix semigroups.

Thus the Bourgain-Kontorovich theorem marks the point where Zaremba's Conjecture moves from elementary continued fractions into modern analytic number theory, combining fractal geometry, semigroup dynamics, Fourier analysis, and the circle method. It remains open whether the exceptional set can be removed completely, but the density-one theorem shows that any possible exceptions are extremely sparse.

## 7. Applications

Although Zaremba's Conjecture is a problem in number theory, its ideas appear naturally in several applied areas. The reason is that continued fractions measure the arithmetic structure of rational numbers. If

$$\frac{a}{q} = [0; a_1, \dots, a_n],$$

then the partial quotients $a_1, \dots, a_n$ record the successive quotient steps in the Euclidean algorithm for the pair $(q, a)$. Thus the condition

$$1 \le a_i \le A \qquad (1 \le i \le n)$$

means that the Euclidean algorithm is uniformly controlled.

Zaremba's Conjecture predicts that this kind of control is available for every denominator. More precisely, it asserts that there exists an absolute constant $A \ge 1$ such that for every $q \in \mathbb{N}$, there exists $a \in \mathbb{Z}$ with

$$(a, q) = 1$$

and

$$\frac{a}{q} = [0; a_1, \dots, a_n], \qquad (a_1, \dots, a_n) \in \mathcal{A}_A^n, \qquad \mathcal{A}_A = \{1, 2, \dots, A\}.$$

Equivalently, every positive integer should be obtainable as a continuant:

$$q = \mathcal{K}_n(a_1, \dots, a_n), \qquad (a_1, \dots, a_n) \in \mathcal{A}_A^n.$$

This statement is useful because bounded continued fractions give regular arithmetic behavior. In applications, such regularity appears in uniform distribution, low-discrepancy point sets, pseudorandom number generation, and lattice geometry.

### 7.1. **Quasi-Monte Carlo Methods and Numerical Integration.**

One of the classical motivations for Zaremba's Conjecture comes from numerical integration. [HKS25] Suppose one wants to approximate an integral over the unit square:

$$I(f) = \int_0^1 \int_0^1 f(x, y)\, dx\, dy.$$

A numerical integration rule replaces this integral by a finite average:

$$I_N(f) = \frac{1}{N} \sum_{j=0}^{N-1} f(x_j, y_j),$$

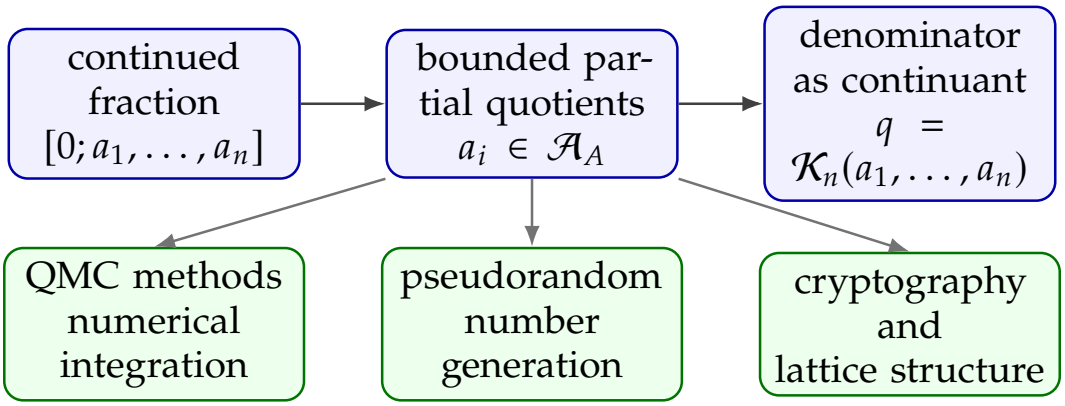


FIGURE 2. Application structure of bounded continued fractions. The same bounded-digit condition that appears in Zaremba's Conjecture also controls modular distribution, numerical integration, pseudorandom generation, and lattice behavior.

where

$$(x_j, y_j) \in [0,1)^2.$$

The integration error is

$$\mathcal{E}_N(f) = \left| I(f) - I_N(f) \right|.$$

Thus the problem is not only to choose many points, but to choose points that are distributed evenly throughout the square.

In ordinary Monte Carlo integration, the points are chosen randomly. In quasi-Monte Carlo methods, the points are deterministic and are designed to have low discrepancy. If

$$\mathcal{P}_N = \{z_0, z_1, \ldots, z_{N-1}\} \subset [0,1)^s,$$

then the star discrepancy of $\mathcal{P}_N$ is

$$D_N^*(\mathcal{P}_N) = \sup_{\mathbf{t} \in [0,1]^s} \left| \frac{1}{N} \#\{z_j \in [0, \mathbf{t}) : 0 \le j < N\} - \mathrm{vol}([0, \mathbf{t})) \right|.$$

Here

$$[0, \mathbf{t}) = [0, t_1) \times [0, t_2) \times \cdots \times [0, t_s).$$

This quantity measures the largest difference between the actual proportion of points in a box and the volume of that box.

The reason discrepancy matters is the Koksma–Hlawka inequality:

$$\left| \frac{1}{N} \sum_{j=0}^{N-1} f(z_j) - \int_{[0,1]^s} f(\mathbf{x})\, d\mathbf{x} \right| \le V_{\mathrm{HK}}(f)\, D_N^*(\mathcal{P}_N).$$

Here $V_{\mathrm{HK}}(f)$ is the Hardy–Krause variation of $f$. In two dimensions, if $f$ is sufficiently smooth, this variation is controlled by ordinary calculus quantities.

For example, one may bound it using first derivatives on the boundary and the mixed second derivative:

$$V_{\mathrm{HK}}(f) \le \int_0^1 \left|\frac{\partial f}{\partial x}(x,1)\right| dx + \int_0^1 \left|\frac{\partial f}{\partial y}(1,y)\right| dy + \int_0^1 \int_0^1 \left|\frac{\partial^2 f}{\partial x \partial y}(x,y)\right| dx\, dy.$$

Therefore the numerical integration error is controlled by two factors:

$$\boxed{\text{smoothness of } f \quad \text{and} \quad \text{uniformity of the point set.}}$$

The calculus of $f$ determines $V_{\mathrm{HK}}(f)$, while the arithmetic of the points determines $D_N^*(\mathcal{P}_N)$.

A particularly important deterministic construction is a rank-one lattice rule. For a denominator $q$ and a numerator $a$ satisfying $(a,q) = 1$, define

$$\mathcal{P}_q(a) = \left\{ \left( \frac{j}{q}, \left\{ \frac{aj}{q} \right\} \right) : 0 \le j < q \right\}.$$

This gives $q$ points in the unit square. The first coordinate moves evenly through the fractions $j/q$, while the second coordinate is produced by the modular slope $a/q$. Since multiplication by $a$ permutes the nonzero residue classes modulo $q$, the coprimality condition

$$(a,q) = 1$$

is essential.

The distribution of $\mathcal{P}_q(a)$ depends on the arithmetic structure of the rational slope $a/q$. If

$$\frac{a}{q} = [0; a_1, \ldots, a_n]$$

has very large partial quotients, then the point set can have visible arithmetic imbalance. In contrast, if the partial quotients are bounded,

$$a_i \le A,$$

then no step in the Euclidean algorithm is allowed to dominate the structure of the rational slope. This is why bounded continued fractions are useful in the construction of good lattice rules.

**Proposition 4** (Zaremba and QMC Point Sets)**.** *Assume Zaremba's Conjecture holds for an absolute constant $A$. Then for every sample size $q$, there exists a numerator $a$ such that the rank-one lattice rule*

$$\mathcal{P}_q(a) = \left\{ \left( \frac{j}{q}, \left\{ \frac{aj}{q} \right\} \right) : 0 \le j < q \right\}$$

*is generated by a rational number $a/q$ whose partial quotients are bounded by $A$.*

*Proof.* By Zaremba's Conjecture, for every $q \in \mathbb{N}$, there exists an integer $a$ with

$$(a,q) = 1$$

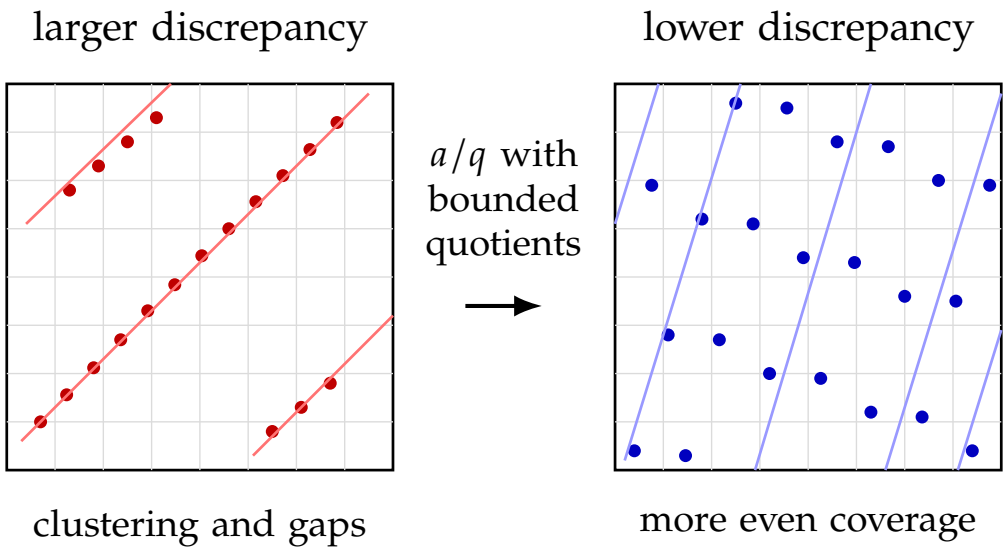


FIGURE 3. Schematic comparison of point distributions in the unit square. In a rank-one lattice rule, the arithmetic of the slope $a/q$ affects how evenly the points cover the domain. Bounded partial quotients help avoid extreme arithmetic imbalance.

such that

$$\frac{a}{q} = [0; a_1, \ldots, a_n], \qquad 1 \le a_i \le A.$$

Using this numerator, define the point set $\mathcal{P}_q(a)$. Since $(a, q) = 1$, multiplication by $a$ is a permutation modulo $q$. Therefore the points are generated from a valid modular lattice rule. Moreover, the slope $a/q$ has bounded partial quotients, so the arithmetic structure of the rule is controlled uniformly in $q$. □

This gives the application meaning of Zaremba's Conjecture. It says that for every possible number of points $q$, one can choose a modular slope $a/q$ whose continued-fraction expansion is uniformly bounded. Thus the conjecture provides a number-theoretic foundation for constructing good deterministic point sets for numerical integration.

7.2. **Cryptography, Encryption, and Continued-Fraction Cryptanalysis.** Continued fractions also appear in cryptography, especially in the analysis of encryption systems based on modular arithmetic. Modern encryption schemes often depend on arithmetic structures that are easy to compute in one direction but difficult to reverse without secret information. For example, RSA encryption is based on the difficulty of factoring a large composite number

$$N = pq,$$

where $p$ and $q$ are large primes. The public key contains $N$ and an exponent $e$, while the private key contains an exponent $d$ satisfying

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Equivalently, there exists an integer $k$ such that

$$ed - k\varphi(N) = 1.$$

This equation is central because it links the public exponent $e$, the hidden private exponent $d$, and the unknown value $\varphi(N)$.

Continued fractions become important when the private exponent $d$ is too small. Dividing the equation

$$ed - k\varphi(N) = 1$$

by $d\varphi(N)$, we obtain

$$\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{d\varphi(N)}.$$

Since $\varphi(N)$ is close to $N$ for RSA moduli, the fraction $k/d$ can become a very strong rational approximation to $e/N$. Continued fractions are designed precisely to detect such unusually good rational approximations.

The following theorem explains why this matters.

**Theorem 6** (Continued-Fraction Approximation Criterion)**.** *Let $x \in \mathbb{R}$. If a rational number $p/q$ satisfies*

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2},$$

*then $p/q$ is a convergent of the continued fraction expansion of $x$.*

This result gives a direct cryptographic consequence. If the RSA private exponent $d$ is too small, then $k/d$ becomes such a strong approximation to $e/N$ that it appears among the convergents of the continued fraction expansion of $e/N$. An attacker can then compute the continued fraction of $e/N$, test its convergents, and potentially recover the private exponent.

**Proposition 5** (Small-Exponent RSA Weakness)**.** *Suppose the RSA private exponent $d$ is small enough that*

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

*for some integer $k$. Then $k/d$ occurs as a convergent of the continued fraction expansion of $e/N$. Hence continued fractions can be used to test whether the private exponent is vulnerable.*

*Proof.* Apply the continued-fraction approximation criterion with

$$x = \frac{e}{N} \qquad \text{and} \qquad \frac{p}{q} = \frac{k}{d}.$$

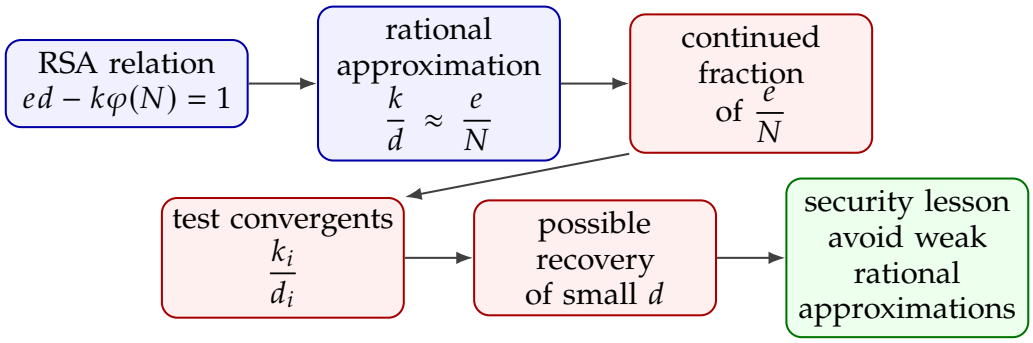


FIGURE 4. Continued fractions in RSA cryptanalysis. A small private exponent can make $k/d$ an unusually good rational approximation to $e/N$. Continued fractions detect such approximations through convergents, which can expose weak encryption parameters.

The hypothesis gives

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

Therefore $p/q = k/d$ must be a convergent of the continued fraction expansion of $x = e/N$. Thus, if $d$ is small enough, searching through the convergents of $e/N$ can reveal the private exponent. □

This application shows that continued fractions are not merely theoretical objects. They can reveal hidden structure inside encryption parameters. In RSA, a dangerous situation occurs when the public ratio $e/N$ has a convergent whose denominator is the private exponent $d$. The continued fraction expansion therefore acts as a detector for weak rational approximations.

The relationship with Zaremba's Conjecture is conceptual but important. Zaremba's Conjecture studies rational numbers

$$\frac{a}{q}$$

whose continued-fraction digits are uniformly bounded:

$$\frac{a}{q} = [0; a_1, \ldots, a_n], \qquad a_i \le A.$$

Such fractions have controlled rational-approximation behavior. In contrast, cryptanalytic attacks often exploit rational numbers that are too well approximated by small denominators. Thus, both Zaremba's Conjecture and continued-fraction cryptanalysis study the same underlying phenomenon:

| continued fractions measure how rational numbers approximate one another. |
|---|

This does not mean that Zaremba's Conjecture is itself an encryption method. Rather, it shows that the same number-theoretic tools used to understand bounded continued fractions also help explain why certain encryption parameters

are secure or insecure. Continued fractions provide a bridge between pure Diophantine approximation and practical questions about encryption strength.

Finally, continued fractions also connect to lattice-based cryptography. The Euclidean algorithm is the two-dimensional prototype of lattice reduction. For a rational number $a/q$, one can associate the modular lattice

$$\mathcal{L}_{a,q} = \{(x, y) \in \mathbb{Z}^2 : y \equiv ax \pmod{q}\}.$$

The geometry of this lattice is influenced by the continued fraction expansion of $a/q$. Large partial quotients correspond to unbalanced reduction steps, whereas bounded partial quotients correspond to more regular two-dimensional lattice geometry. Modern lattice-based cryptographic systems work in much higher dimensions, but the underlying idea of controlling short vectors and reduction behavior has its simplest model in continued fractions.

Therefore, continued fractions appear in cryptography in two complementary ways: they can expose weak encryption parameters through rational approximation, and they provide the two-dimensional foundation for understanding lattice reduction, a central idea behind lattice-based cryptographic systems.

## 8. Future Directions and Open Problems

Zaremba's Conjecture remains a central open problem in the theory of continued fractions. The conjecture predicts that there exists an absolute constant $A \geq 1$ such that every positive integer $q$ appears as the denominator of a reduced fraction

$$\frac{a}{q} = [0; a_1, \ldots, a_n], \qquad 1 \leq a_i \leq A.$$

Equivalently,

$$\mathcal{D}_A = \mathbb{N}$$

for some fixed finite alphabet

$$\mathcal{A}_A = \{1, 2, \ldots, A\}.$$

The Bourgain–Kontorovich density-one theorem shows that this equality is true for almost every denominator, but the full conjecture asks for every denominator. The remaining difficulty is therefore concentrated in the possible exceptional set:

$$\mathcal{E}_A(N) = [1, N] \setminus \mathcal{D}_A.$$

The density-one theorem implies that, for a suitable $A$,

$$\#\mathcal{E}_A(N) = o(N).$$

The full conjecture would require the much stronger conclusion

$$\#\mathcal{E}_A(N) = 0$$

for all $N$, after fixing one absolute alphabet.

8.1. **From Density One to Every Denominator.** The most important open problem is to upgrade the Bourgain–Kontorovich theorem from density one to

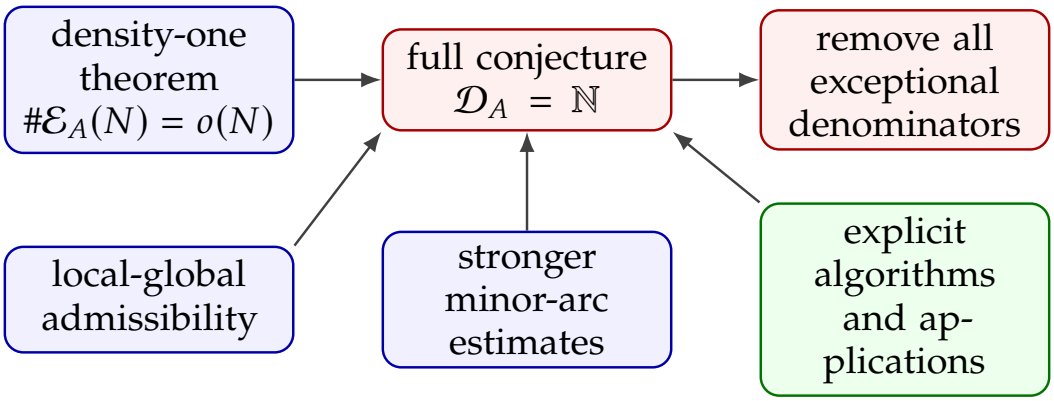


FIGURE 5. Future directions for Zaremba's Conjecture. The main challenge is to move from density-one representation to complete representation of every denominator. This requires sharper control of exceptional denominators, stronger minor-arc estimates, better understanding of local obstructions, and explicit construction methods.

a pointwise statement. In the density-one result, one proves that almost every integer is represented:

$$\lim_{N\to\infty} \frac{\#(\mathcal{D}_A \cap [1,N])}{N} = 1.$$

However, this still allows the possibility of infinitely many missing denominators. The full conjecture requires

$$\forall q \in \mathbb{N}, \qquad q \in \mathcal{D}_A.$$

In terms of representation numbers, the goal is to prove that for every $q$, there exists a matrix $\gamma \in \Gamma_A$ such that

$$\langle \gamma e_2, e_2 \rangle = q.$$

Equivalently, one wants

$$R_N(q) > 0$$

for every relevant denominator $q$, not merely for almost every $q$.

The Bourgain–Kontorovich method proves that the minor-arc errors are small on average. A natural future direction is to strengthen this average control into more pointwise control. In simplified form, their method separates

$$R_N(q) = M_N(q) + E_N(q),$$

where $M_N(q)$ is the major-arc main term and $E_N(q)$ is the minor-arc error. The known method shows that

$$\sum_{q \asymp N} |E_N(q)|^2$$

is small enough to control almost all $q$. To prove the full conjecture, one would need a method strong enough to prevent

$$E_N(q)$$

from canceling $M_N(q)$ for any denominator $q$.

Thus, one major open problem is:

| Can the average minor-arc estimate be replaced by a pointwise estimate? |
|---|

Such a result would be extremely powerful, but it is also very difficult because the matrix semigroup $\Gamma_A$ is thin. Unlike a full lattice group, it has fractal growth and does not contain enough elements for standard equidistribution methods to apply directly.

8.2. **Optimizing the Alphabet.** Another natural direction is to understand how small the alphabet can be. Zaremba originally suggested that one might be able to take a very small constant, commonly written in the form

$$A = 5.$$

This leads to the sharper question

$$\mathcal{D}_5 = \mathbb{N}?$$

Even if the full conjecture is difficult for arbitrary $A$, small alphabets are important because they represent the strongest possible boundedness condition. The smaller $A$ is, the more rigid the continued fractions become.

For a fixed alphabet

$$\mathcal{A}_A = \{1, 2, \ldots, A\},$$

there is a corresponding Cantor-like set

$$C_A = \{x = [0; a_1, a_2, \ldots] : a_i \in \mathcal{A}_A\},$$

with Hausdorff dimension

$$\delta_A = \dim_H(C_A).$$

As $A$ increases, $\delta_A$ increases toward 1. Larger alphabets give more flexibility and make analytic methods easier to apply. Smaller alphabets are more restrictive and therefore harder.

This gives another open problem:

| How small can $A$ be while still having $\mathcal{D}_A = \mathbb{N}$? |
|---|

A complete solution would not only prove Zaremba's Conjecture but would also identify the optimal strength of the bounded partial quotient condition.

8.3. **Local-Global Principles.** For a general finite alphabet $\mathcal{A}$, not every residue class modulo $m$ must be represented by denominators in $\mathcal{D}_{\mathcal{A}}$. Thus, one must distinguish between integers that are genuinely impossible because of congruence obstructions and integers that are merely not yet known to be represented.

This leads to the notion of admissibility. An integer $q$ is admissible for $\mathcal{A}$ if it passes all finite congruence tests:

$$q \in \mathcal{D}_{\mathcal{A}} \pmod{m} \qquad \text{for every } m \geq 2.$$

The local-global philosophy asks whether these congruence conditions are the only obstructions. In this language, a major open problem is:

$$\boxed{\text{If } q \text{ is admissible and sufficiently large, must } q \in \mathcal{D}_{\mathcal{A}}?}$$

This question is especially natural when the Hausdorff dimension

$$\delta_{\mathcal{A}}$$

is greater than $1/2$. The threshold $1/2$ appears because the number of bounded continued-fraction rationals up to height $N$ grows roughly like

$$N^{2\delta_{\mathcal{A}}}.$$

If

$$\delta_{\mathcal{A}} < \frac{1}{2},$$

then this count is too small to cover a positive proportion of integers. If

$$\delta_{\mathcal{A}} > \frac{1}{2},$$

then there are enough candidates in principle, but one still needs to prove that they are distributed correctly among the integers.

8.4. **Explicit Construction Algorithms.** A different direction is algorithmic. Zaremba's Conjecture is existential: it predicts that for every $q$, there exists some numerator $a$ such that

$$\frac{a}{q} = [0; a_1, \ldots, a_n], \qquad a_i \leq A.$$

However, an applied or computational version asks for an efficient way to find such an $a$.

This leads to the algorithmic problem:

$$\boxed{\text{Given } q, \text{ can one efficiently construct } a \text{ with bounded partial quotients?}}$$

Even partial algorithms are useful. For example, one may search over finite words

$$(a_1, \ldots, a_n) \in \mathcal{A}_A^n$$

and compute the continuant

$$\mathcal{K}_n(a_1, \ldots, a_n).$$

The difficulty is that the number of possible words grows exponentially with $n$, while many different words may produce denominators of comparable size. An effective algorithm would need to exploit the semigroup structure

$$\Gamma_A = \langle M(a) : a \in \mathcal{A}_A \rangle$$

rather than perform a brute-force search.

Such algorithms would also strengthen the practical applications of Zaremba's Conjecture. In quasi-Monte Carlo methods, pseudorandom number generation, and modular lattice constructions, one does not only want to know that a good numerator exists. One wants to compute it.

8.5. **Connections to Applications.** The applications discussed earlier suggest further questions. In numerical integration, one may ask whether bounded continued-fraction denominators produce uniformly good rank-one lattice rules for broad classes of functions. In pseudorandom number generation, one may ask how bounded partial quotients affect higher-dimensional serial correlations. In cryptography, continued fractions already play a role in detecting weak rational approximations, but the connection between bounded partial quotients and secure lattice structure deserves further study.

These directions can be summarized by the implication

$$\begin{aligned}\text{bounded partial quotients} &\Longrightarrow \text{controlled Euclidean algorithm}\\ &\Longrightarrow \text{regular modular and lattice behavior.}\end{aligned}$$

Future work may clarify exactly how strong this implication is in computational settings.

8.6. **Conclusion.** The known results show that the Zaremba's Conjecture is really close to being true in an asymptotic sense. Bourgain and Kontorovich proved that bounded continued fractions generate a density-one set of denominators. The remaining challenge is to remove the exceptional set completely.

The main future directions are therefore:

(i) prove representation for every denominator,

(ii) optimize the alphabet size $A$,

(iii) understand local-global principles for general alphabets,

(iv) improve minor-arc and thin-orbit estimates,

(v) develop explicit algorithms for constructing the numerator $a$.

Together, these problems show why the Conjecture remains important. It is a question about continued fractions, and also a bridge between Diophantine approximation, fractal geometry, matrix semigroups, analytic number theory, computational applications, and even more.

## 9. Conclusion

The conjecture lies at a beautiful intersection of continued fractions, Diophantine approximation, matrix semi-groups, and analytic number theory. At its core, the conjecture asks whether there exists a fixed constant $A$ such that every positive integer $q$ can be realized as the denominator of a reduced fraction

$$\frac{a}{q} = [0; a_1, \ldots, a_n], \qquad 1 \le a_i \le A.$$

Equivalently, it asks whether the denominator set

$$\mathcal{D}_A = \{q \in \mathbb{N} : q = \mathcal{K}_n(a_1, \ldots, a_n) \text{ for some } a_i \in \mathcal{A}_A\}$$

can equal all of $\mathbb{N}$ for a single finite alphabet

$$\mathcal{A}_A = \{1, 2, \ldots, A\}.$$

This formulation shows that the conjecture is not merely about continued fractions, but about whether a very restricted arithmetic system can still generate every possible denominator.

The matrix and semigroup formulation gives the conjecture a deeper geometric meaning, which adds on to arithmetic theory. By encoding continued fractions using products of matrices, the problem becomes a question about the orbit

$$\Gamma_A e_2$$

inside the integer lattice. The denominator is extracted as the second coordinate of an orbit point, so Zaremba's Conjecture asks whether this thin but structured orbit intersects every positive denominator level. This perspective explains why modern methods like the circle method, exponential sums, major and minor arc analysis, and thin-orbit theory enter the problem.

The theorem of Bourgain and Kontorovich represents the most important and instrumental modern breakthrough toward the conjecture. Their density-one result shows that, for a suitable fixed alphabet, almost every positive integer occurs as a denominator. In other words,

$$\#([1, N] \setminus \mathcal{D}_A) = o(N).$$

This does not yet prove the full conjecture, since there may still be infinitely many exceptional denominators. However, it confirms the central philosophy of the Conjecture: bounded continued fractions are far more abundant and arithmetically powerful than one might initially expect.

The applications further show why the conjecture is beyond just pure number theory. Bounded partial quotients give controlled Euclidean algorithms, and this control appears naturally in quasi-Monte Carlo methods, numerical integration, pseudorandom number generation, encryption analysis, and lattice geometry. In each setting, the same idea reappears:

$$\text{bounded partial quotients} \Longrightarrow \text{controlled arithmetic structure.}$$

Thus continued fractions provide a bridge between theoretical Diophantine approximation and practical problems involving uniform distribution, modular arithmetic, and cryptographic structure.

Although the full conjecture remains open, the existing results show that the problem is both deep and highly structured. Future progress will likely require a stronger control of the exceptional set, sharper minor-arc estimates, better understanding of local-global principles, and more explicit algorithms for constructing good numerators $a$ for each denominator $q$. Zaremba's Conjecture still remains compelling and intriguing to modern mathematicians to date,

because it asks a very simple question with profound consequences: ***can every integer be generated from a continued fraction whose digits are bounded once and for all?***

## Acknowledgements

The author would like to thank Dr. Simon Rubinstein-Salzedo for providing the environment to make this paper possible and Arianna Ridgeway for providing the resources and general support throughout the process.

## References

[BK14] Jean Bourgain and Alex Kontorovich. On zaremba's conjecture. *Annals of Mathematics*, 180(1):137–196, 2014.

[HKS25] Fred J. Hickernell, Nathan Kirk, and Aleksei G. Sorokin. Quasi-monte carlo methods: What, why, and how?, 2025.

[HW08] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 6 edition, 2008.

[Lut16] Andrew Lutz. Number theory notes, 2016. Summer 2016 lecture notes.

[Zar72] S. K. Zaremba. La méthode des "bons treillis" pour le calcul des intégrales multiples. In *Applications of Number Theory to Numerical Analysis*, pages 39–119. Academic Press, New York, 1972. Proceedings of the Symposium, Université de Montréal, 1971.

Akashdeep Das: Euler Circle, Mountain View, CA 94040
*E-mail address*: akashdeepdas.gma@gmail.com