Bounded Partial Quotients and Zaremba's Conjecture

Akashdeep Das

Euler Circle

Mountain View, CA

July 3, 2026

Roadmap

What I Will Discuss

1. Finite continued fractions and bounded partial quotients.
2. How denominators arise from continuants and recurrences.
3. Zaremba's conjecture and the denominator set $\mathcal{D}_A$.
4. Matrix products and the semigroup orbit viewpoint.
5. Bourgain–Kontorovich's density-one progress.
6. Applications to good lattices, the Euclidean algorithm, and modular arithmetic.

$$\text{fractions} \Longrightarrow \text{recurrences} \Longrightarrow \text{matrix orbits} \Longrightarrow \text{arithmetic coverage}.$$

Main Question

The Central Problem

For every positive integer q, can we find a reduced fraction

$$\frac{p}{q}, \qquad 1 \leq p < q, \qquad (p,q) = 1,$$

whose continued fraction expansion has only small entries?

$$\frac{p}{q} = [0; a_1, a_2, \ldots, a_k], \qquad a_i \leq A.$$

Zaremba's Prediction

There should exist one universal constant A that works for every denominator q.

Finite Continued Fractions

For a rational number $0 < p < q$,

$$\frac{p}{q} = [0; a_1, a_2, \ldots, a_k] = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}.$$

$$a_1, a_2, \ldots, a_k \in \mathbb{Z}_{>0}.$$

Bounded Partial Quotients

The partial quotients are bounded by A if

$$\max\{a_1, a_2, \ldots, a_k\} \leq A.$$

The alphabet is finite: $\qquad a_i \in \{1, 2, \ldots, A\}.$

Examples of Denominators

$$[0;2,2] = \frac{1}{2+\frac{1}{2}} = \frac{2}{5}, \qquad q = 5,\ A = 2.$$

$$[0;2,3] = \frac{1}{2+\frac{1}{3}} = \frac{3}{7}, \qquad q = 7,\ A = 3.$$

$$[0;1,1,2] = \frac{3}{5}, \qquad q = 5,\ A = 2.$$

Key Point: The conjecture asks whether one fixed bound A can generate every denominator q.

Convergents

$$[0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k}$$

The numerators and denominators satisfy

$$p_{-1} = 1, \quad p_0 = 0, \qquad q_{-1} = 0, \quad q_0 = 1.$$

For $k \geq 1$,

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

Important: The denominator q_k is generated recursively from the partial quotients $a_1, \ldots, a_k$.

Continuants

The denominator q_k can be written as a continuant:

$$q_k = K(a_1, a_2, \ldots, a_k).$$

The continuant satisfies

$$K(a_1, \ldots, a_k) = a_k K(a_1, \ldots, a_{k-1}) + K(a_1, \ldots, a_{k-2}).$$

$$K(\emptyset) = 1, \qquad K(a_1) = a_1.$$

Zaremba in Continuant Form

For some fixed A, every $q \in \mathbb{Z}_{>0}$ should be expressible as

$$q = K(a_1, \ldots, a_k), \qquad 1 \leq a_i \leq A.$$

Formal Statement of Zaremba's Conjecture

Zaremba's Conjecture says that there is a universal constant A such that for every denominator $q \geq 1$, we can choose a reduced fraction

$$\frac{p}{q}, \qquad 1 \leq p < q, \qquad (p, q) = 1,$$

whose continued fraction expansion

$$\frac{p}{q} = [0; a_1, a_2, \ldots, a_k]$$

has uniformly bounded partial quotients:

$$a_i \leq A \qquad \text{for every } i.$$

Zaremba suggested that $A = 5$ may be sufficient.

The Denominator Set

For a fixed bound A, define

$$\mathcal{D}_A = \left\{ q \in \mathbb{Z}_{>0} : q \text{ is the denominator of } [0; a_1, \dots, a_k],\ 1 \le a_i \le A \right\}.$$

Then Zaremba's conjecture becomes

$$\mathcal{D}_A = \mathbb{Z}_{>0}$$

for some fixed A.

Meaning

Even though the allowed digits come from only

$$\{1, 2, \dots, A\},$$

the conjecture says the resulting denominators should cover all positive integers.

Matrix Encoding

Each partial quotient is encoded by

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

$$M(a_1) \cdots M(a_k) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} p_k \\ q_k \end{pmatrix}.$$

For example,

$$M(2)^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}.$$

Translation

The denominator q_k is the second coordinate of a matrix orbit point.

The Semigroup Viewpoint

Fix A. Define

$$\Gamma_A = \langle M(1), M(2), \ldots, M(A) \rangle \,.$$

This is the semigroup generated by the allowed matrices.

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

We study the orbit

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

Orbit Reformulation

Zaremba's conjecture asks whether every $q \in \mathbb{Z}_{>0}$ appears as the lower coordinate of some vector in $\Gamma_A e_2$.

Orbit Diagram

The continued fraction digits $a_1, \ldots, a_k$ are no longer viewed only as numbers. Each digit becomes a matrix choice, and multiplying these matrices moves the vector $e_2 = \binom{0}{1}$ through an integer orbit.

$$\boxed{\tbinom{0}{1}} \to \boxed{M(a_1)} \to \boxed{M(a_2)} \to \boxed{\cdots} \to \boxed{M(a_k)} \to \boxed{\tbinom{p}{q}}$$

bounded choices $a_i \leq A$

denominator q

Orbit Interpretation

continued fractions $\Rightarrow$ matrix products $\Rightarrow$ integer orbit problem.

Why This Is Hard

The recurrence

$$q_k = a_k q_{k-1} + q_{k-2}$$

looks simple, but the set of possible values is highly structured.

- The digits a_i are restricted to a finite alphabet.
- The denominator grows nonlinearly.
- Different words may produce the same denominator.
- We need coverage of every integer, not only many integers.

Core Difficulty

Counting many orbit points is not enough. One must show that no denominator level is missed.

Bourgain–Kontorovich Theorem

Density-One Progress

Bourgain and Kontorovich proved that for sufficiently large A, almost every positive integer satisfies Zaremba's conjecture.

In denominator-set notation,

$$\#(\mathcal{D}_A \cap [1, N]) = N(1 + o(1)) \qquad \text{as } N \to \infty.$$

Equivalently,

$$\frac{\#([1, N] \setminus \mathcal{D}_A)}{N} \to 0.$$

Meaning

The exceptional set has density zero, but Zaremba still asks if it is empty.

Density-One Meaning

A set $S \subseteq \mathbb{Z}_{>0}$ has natural density one if

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

So the Bourgain–Kontorovich theorem says

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

Important Distinction

almost every denominator works $\neq$ every denominator works.

A sparse infinite exceptional set could still remain.

Fractal Geometry Connection

Let

$$C_A = \{x \in [0,1] : x = [0; a_1, a_2, a_3, \ldots],\ 1 \le a_i \le A\}.$$

This is a Cantor-like set.

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

As the alphabet grows,

$$\delta_A \to 1 \qquad \text{as } A \to \infty.$$

Idea

When A is large, the bounded-digit set becomes large enough to support strong counting and distribution methods.

Original Motivation: Good Lattices

Zaremba's work was motivated by numerical integration:

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

A lattice rule approximates this integral by

$$I(f) \approx \frac{1}{q} \sum_{n=0}^{q-1} f\left(\frac{n}{q}, \left\{\frac{np}{q}\right\}\right).$$

The sample points are

$$\mathcal{P}_{p,q} = \left\{\left(\frac{n}{q}, \left\{\frac{np}{q}\right\}\right) : 0 \leq n < q\right\}.$$

Modular Arithmetic and Cryptography

Many cryptographic systems rely on modular arithmetic. A basic operation is finding a modular inverse:

$$ax \equiv 1 \pmod{m}.$$

This is solved using the extended Euclidean algorithm when

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

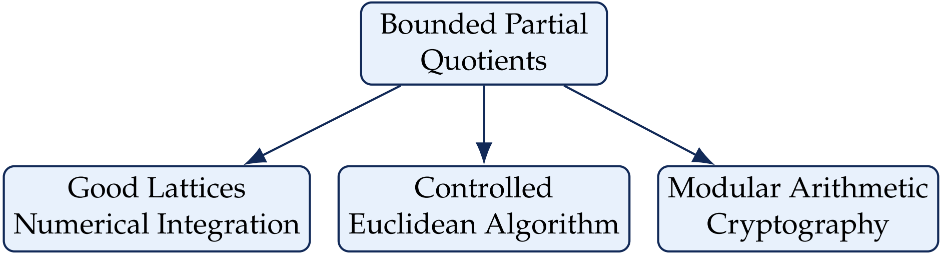
$$\text{Euclidean algorithm} \implies \text{modular inverses} \implies \text{cryptographic computations.}$$

Careful Connection

Zaremba's conjecture is not directly a cryptography theorem, but it is connected to the same number-theoretic tools: Euclidean algorithms, modular inverses, and rational approximation.

Applications

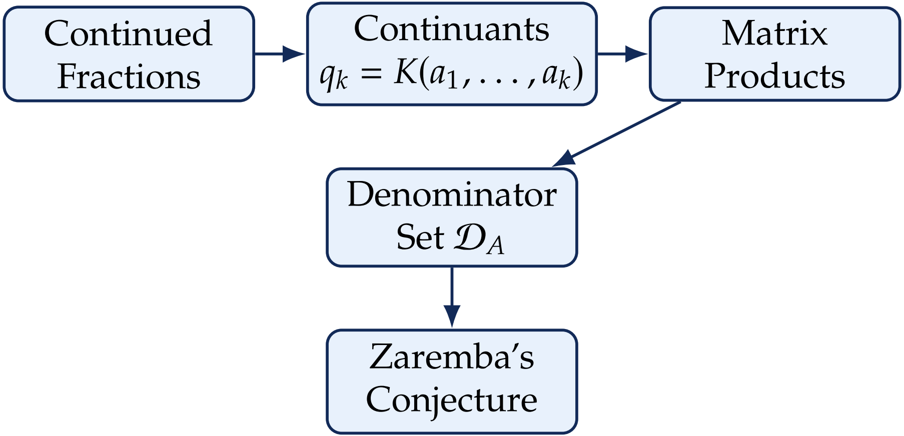
Bounded partial quotients appear beyond pure continued fractions. They help describe arithmetic control in lattice rules, algorithmic number theory, and modular computations.



bounded partial quotients $\implies$ controlled arithmetic structure.

Big Picture

The main surprise is that the denominator q is not just the bottom of a fraction. It can be studied as the output of a word made from a bounded alphabet $\{1, 2, \ldots, A\}$.



Conclusion

- Continued fractions encode rationals using partial quotients.
- Bounded partial quotients restrict the allowed arithmetic steps.
- Denominators arise from continuants, recurrences, and matrix products.
- Zaremba's conjecture predicts that every positive integer occurs.
- Bourgain–Kontorovich proved that almost every denominator occurs.
- The topic connects to good lattices, numerical integration, Euclidean algorithms, and modular arithmetic.

Final Takeaway

Zaremba's conjecture turns a simple-looking denominator question into a deep bridge between number theory, dynamics, geometry, and applications.