

Failure of the local-global conjecture in thin (semi)groups

James Rickards

Saint Mary's University

james.rickards@smu.ca

21 April 2025

What is a thin group?

- “An infinite index subgroup of $\mathrm{SL}(n, \mathbb{Z})$ with full Zariski closure”

What is a thin group?

- “An infinite index subgroup of $SL(n, \mathbb{Z})$ with full Zariski closure”
- Generalize to semigroups in $GL(n, \mathbb{Z})$

Examples

- $\Gamma = \Gamma_0(2025)$ is NOT thin.

Examples

- $\Gamma = \Gamma_0(2025)$ is NOT thin.
- $\Gamma = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$ is NOT thin.

Examples

- $\Gamma = \Gamma_0(2025)$ is NOT thin.
- $\Gamma = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$ is NOT thin.
- $\left\langle \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 4 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$ IS thin.

Examples

- How about $\Gamma = \left\langle \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & -3 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 0 & -1 \\ -5 & 1 & -1 \\ 3 & 0 & 1 \end{pmatrix} \right\rangle$?

Examples

- How about $\Gamma = \left\langle \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & -3 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 0 & -1 \\ -5 & 1 & -1 \\ 3 & 0 & 1 \end{pmatrix} \right\rangle$?
- $\text{Zcl}(\Gamma) = \text{SL}(3)$;

Examples

- How about $\Gamma = \left\langle \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & -3 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 0 & -1 \\ -5 & 1 & -1 \\ 3 & 0 & 1 \end{pmatrix} \right\rangle$?
- $\text{Zcl}(\Gamma) = \text{SL}(3)$;
- Unknown if Γ is thin or not.

Examples

- How about $\Gamma = \left\langle \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & -3 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 0 & -1 \\ -5 & 1 & -1 \\ 3 & 0 & 1 \end{pmatrix} \right\rangle$?
- $\text{Zcl}(\Gamma) = \text{SL}(3)$;
- Unknown if Γ is thin or not.
- In general, it is a difficult question to determine if a group is thin or not.

Thin orbits

- Let $\Gamma \subseteq \mathrm{GL}(n, \mathbb{Z})$ be thin.

Thin orbits

- Let $\Gamma \subseteq \mathrm{GL}(n, \mathbb{Z})$ be thin.
- Let $v \in \mathbb{Z}^n$ be a primitive vector.

Thin orbits

- Let $\Gamma \subseteq \mathrm{GL}(n, \mathbb{Z})$ be thin.
- Let $v \in \mathbb{Z}^n$ be a primitive vector.
- Let $L : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be a linear functional.

Thin orbits

- Let $\Gamma \subseteq \mathrm{GL}(n, \mathbb{Z})$ be thin.
- Let $v \in \mathbb{Z}^n$ be a primitive vector.
- Let $L : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be a linear functional.
- What can we say about $L(\Gamma \cdot v) \subseteq \mathbb{Z}$?

Example: Zaremba

Definition

The continued fraction expansion of a real number $\alpha \in \mathbb{R}$ is $[a_0; a_1, a_2, a_3, \dots]$, where

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}.$$

Example: Zaremba

Definition

The continued fraction expansion of a real number $\alpha \in \mathbb{R}$ is $[a_0; a_1, a_2, a_3, \dots]$, where

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}.$$

Call the sequence a_1, a_2, \dots the *partial quotients* of α .

Example: Zaremba

Definition

The continued fraction expansion of a real number $\alpha \in \mathbb{R}$ is $[a_0; a_1, a_2, a_3, \dots]$, where

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}.$$

Call the sequence a_1, a_2, \dots the *partial quotients* of α .

If $\alpha \in \mathbb{Q}$, it has a finite expansion.

Zaremba: motivation

- Zaremba (60s and 70s): generate pseudo-random numbers via

$$x \rightarrow bx \pmod{c}, \quad \text{fixed coprime } b, c \in \mathbb{Z}$$

Zaremba: motivation

- Zaremba (60s and 70s): generate pseudo-random numbers via

$$x \rightarrow bx \pmod{c}, \quad \text{fixed coprime } b, c \in \mathbb{Z}$$

- If partial quotients of b/c contain large terms, the output is not random looking.

Zaremba: motivation

- Zaremba (60s and 70s): generate pseudo-random numbers via

$$x \rightarrow bx \pmod{c}, \quad \text{fixed coprime } b, c \in \mathbb{Z}$$

- If partial quotients of b/c contain large terms, the output is not random looking.
- If partial quotients of b/c are all small, the map seems good.

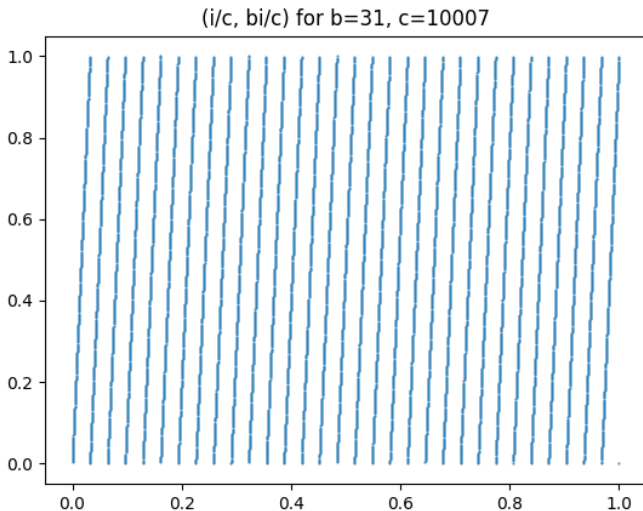
Zaremba: motivation

- Zaremba (60s and 70s): generate pseudo-random numbers via

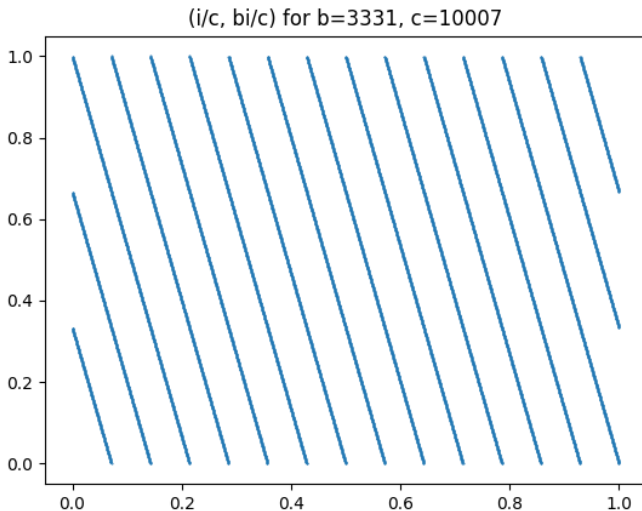
$$x \rightarrow bx \pmod{c}, \quad \text{fixed coprime } b, c \in \mathbb{Z}$$

- If partial quotients of b/c contain large terms, the output is not random looking.
- If partial quotients of b/c are all small, the map seems good.
- Conjecture: given c , there exists coprime b so that b/c has only small partial quotients.

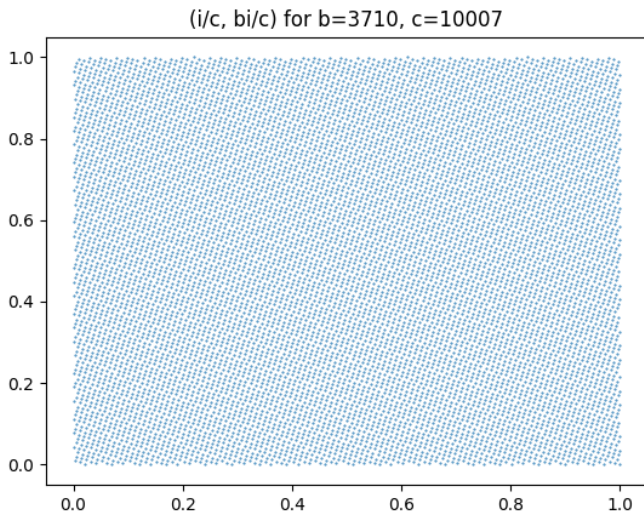
$$\frac{31}{10007} = [0; 322, 1, 4, 6]$$



$$\frac{3331}{10007} = [0; 3, 237, 1, 13]$$



$$\frac{3710}{10007} = [0; 2, 1, 2, 3, 3, 2, 2, 3, 1, 1, 2]$$



Zaremba's conjecture

Conjecture (Zaremba)

For every positive integer n , there exists a coprime integer m such that all the partial quotients of $\frac{m}{n}$ are bounded by A , where A is an absolute constant.

Zaremba's conjecture

Conjecture (Zaremba)

For every positive integer n , there exists a coprime integer m such that all the partial quotients of $\frac{m}{n}$ are bounded by A , where A is an absolute constant.

- $n = 54$ requires $A \geq 5$.

Zaremba's conjecture

Conjecture (Zaremba)

For every positive integer n , there exists a coprime integer m such that all the partial quotients of $\frac{m}{n}$ are bounded by A , where A is an absolute constant.

- $n = 54$ requires $A \geq 5$.
- Conjectured that $A = 5$ suffices.

Zaremba's conjecture

Conjecture (Zaremba)

For every positive integer n , there exists a coprime integer m such that all the partial quotients of $\frac{m}{n}$ are bounded by A , where A is an absolute constant.

- $n = 54$ requires $A \geq 5$.
- Conjectured that $A = 5$ suffices.
- Replace “all” with “all but finite”, conjectured that $A = 4$, then $A = 3$, and finally $A = 2$ suffices (Hensley's conjecture).

Zaremba's conjecture

Conjecture (Zaremba)

For every positive integer n , there exists a coprime integer m such that all the partial quotients of $\frac{m}{n}$ are bounded by A , where A is an absolute constant.

- $n = 54$ requires $A \geq 5$.
- Conjectured that $A = 5$ suffices.
- Replace “all” with “all but finite”, conjectured that $A = 4$, then $A = 3$, and finally $A = 2$ suffices (Hensley's conjecture).
- Best known result: if $A = 5$, a density 1 set of denominators appear (Bourgain—Kontorovich, Huang).

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.
- Let $F_{\mathcal{A}}$ be the set of rational numbers in $(0, 1)$ with all partial quotients from \mathcal{A} .

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.
- Let $F_{\mathcal{A}}$ be the set of rational numbers in $(0, 1)$ with all partial quotients from \mathcal{A} .
- Let $D_{\mathcal{A}} := \{d : d \text{ is a denominator in } F_{\mathcal{A}}\}$.

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.
- Let $F_{\mathcal{A}}$ be the set of rational numbers in $(0, 1)$ with all partial quotients from \mathcal{A} .
- Let $D_{\mathcal{A}} := \{d : d \text{ is a denominator in } F_{\mathcal{A}}\}$.
- Let $M_{\mathcal{A}} := \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} : a \in \mathcal{A} \right\}$, and take Γ to be the semigroup they generate.

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.
- Let $F_{\mathcal{A}}$ be the set of rational numbers in $(0, 1)$ with all partial quotients from \mathcal{A} .
- Let $D_{\mathcal{A}} := \{d : d \text{ is a denominator in } F_{\mathcal{A}}\}$.
- Let $M_{\mathcal{A}} := \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} : a \in \mathcal{A} \right\}$, and take Γ to be the semigroup they generate.
- $n \in D_{\mathcal{A}} \iff \exists \gamma \in \Gamma$ for which $\gamma \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} m \\ n \end{pmatrix}$ for some integer m :

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.
- Let $F_{\mathcal{A}}$ be the set of rational numbers in $(0, 1)$ with all partial quotients from \mathcal{A} .
- Let $D_{\mathcal{A}} := \{d : d \text{ is a denominator in } F_{\mathcal{A}}\}$.
- Let $M_{\mathcal{A}} := \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} : a \in \mathcal{A} \right\}$, and take Γ to be the semigroup they generate.
- $n \in D_{\mathcal{A}} \iff \exists \gamma \in \Gamma$ for which $\gamma \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} m \\ n \end{pmatrix}$ for some integer m :

$$\frac{3}{11} = [0; 3, 1, 2] \quad \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 11 \end{pmatrix}.$$

Zaremba and thin semigroups

- Let $\mathcal{A} \subseteq \mathbb{Z}^+$ be a non-empty alphabet.
- Let $F_{\mathcal{A}}$ be the set of rational numbers in $(0, 1)$ with all partial quotients from \mathcal{A} .
- Let $D_{\mathcal{A}} := \{d : d \text{ is a denominator in } F_{\mathcal{A}}\}$.
- Let $M_{\mathcal{A}} := \left\{ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} : a \in \mathcal{A} \right\}$, and take Γ to be the semigroup they generate.
- $n \in D_{\mathcal{A}} \iff \exists \gamma \in \Gamma$ for which $\gamma \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} m \\ n \end{pmatrix}$ for some integer m :

$$\frac{3}{11} = [0; 3, 1, 2] \quad \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 11 \end{pmatrix}.$$

- $D_{\mathcal{A}} = L(\Gamma \cdot v)$ where $L \begin{pmatrix} x \\ y \end{pmatrix} = y$ and $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Generalizing Zaremba

- Limiting set $F_{\mathcal{A}}$ has Hausdorff dimension $\delta_{\mathcal{A}} \in [0, 1]$.

Generalizing Zaremba

- Limiting set $F_{\mathcal{A}}$ has Hausdorff dimension $\delta_{\mathcal{A}} \in [0, 1]$.
- Count of denominators of size $\leq N$ (with multiplicity) is asymptotic to $C_{\mathcal{A}} N^{2\delta_{\mathcal{A}}}$.

Generalizing Zaremba

- Limiting set $F_{\mathcal{A}}$ has Hausdorff dimension $\delta_{\mathcal{A}} \in [0, 1]$.
- Count of denominators of size $\leq N$ (with multiplicity) is asymptotic to $C_{\mathcal{A}} N^{2\delta_{\mathcal{A}}}$.
- If $\delta_{\mathcal{A}} > 1/2$, the average multiplicity of a denominator goes to ∞ .

Generalizing Zaremba

- Limiting set $F_{\mathcal{A}}$ has Hausdorff dimension $\delta_{\mathcal{A}} \in [0, 1]$.
- Count of denominators of size $\leq N$ (with multiplicity) is asymptotic to $C_{\mathcal{A}} N^{2\delta_{\mathcal{A}}}$.
- If $\delta_{\mathcal{A}} > 1/2$, the average multiplicity of a denominator goes to ∞ .

Conjecture (Hensley)

If $\delta_{\mathcal{A}} > 1/2$, then $D_{\mathcal{A}}$ contains all but finitely many positive integers.

Hausdorff dimensions

- $\mathcal{A} = \{1, 2, 3, 4, 5\}$: $\delta_{\mathcal{A}} \approx 0.8368$;
- $\mathcal{A} = \{1, 2, 3, 4\}$: $\delta_{\mathcal{A}} \approx 0.7889$;
- $\mathcal{A} = \{1, 2, 3\}$: $\delta_{\mathcal{A}} \approx 0.7057$;
- $\mathcal{A} = \{1, 2\}$: $\delta_{\mathcal{A}} \approx 0.5313$;

Hausdorff dimensions

- $\mathcal{A} = \{1, 2, 3, 4, 5\}$: $\delta_{\mathcal{A}} \approx 0.8368$;
- $\mathcal{A} = \{1, 2, 3, 4\}$: $\delta_{\mathcal{A}} \approx 0.7889$;
- $\mathcal{A} = \{1, 2, 3\}$: $\delta_{\mathcal{A}} \approx 0.7057$;
- $\mathcal{A} = \{1, 2\}$: $\delta_{\mathcal{A}} \approx 0.5313$;
- $\mathcal{A} = \{2, 4, 6, 8, 10\}$: $\delta_{\mathcal{A}} \approx 0.5174$;

Hausdorff dimensions

- $\mathcal{A} = \{1, 2, 3, 4, 5\}$: $\delta_{\mathcal{A}} \approx 0.8368$;
- $\mathcal{A} = \{1, 2, 3, 4\}$: $\delta_{\mathcal{A}} \approx 0.7889$;
- $\mathcal{A} = \{1, 2, 3\}$: $\delta_{\mathcal{A}} \approx 0.7057$;
- $\mathcal{A} = \{1, 2\}$: $\delta_{\mathcal{A}} \approx 0.5313$;
- $\mathcal{A} = \{2, 4, 6, 8, 10\}$: $\delta_{\mathcal{A}} \approx 0.5174$;
- Bourgain-Kontorovich: this last alphabet misses $3 \pmod{4}$, disproving Hensley's conjecture.

Even partial quotients

$$\frac{x}{y} \rightarrow \frac{y}{x + 2ky}$$

- $x \equiv 0 \pmod{2}, y \equiv 1 \pmod{4} \rightarrow x_{\text{new}} \equiv 1 \pmod{4}, y_{\text{new}} \equiv 0 \pmod{2}$

Even partial quotients

$$\frac{x}{y} \rightarrow \frac{y}{x + 2ky}$$

- $x \equiv 0 \pmod{2}, y \equiv 1 \pmod{4} \rightarrow x_{\text{new}} \equiv 1 \pmod{4}, y_{\text{new}} \equiv 0 \pmod{2}$
- $x \equiv 1 \pmod{4}, y \equiv 0 \pmod{2} \rightarrow x_{\text{new}} \equiv 0 \pmod{2}, y_{\text{new}} \equiv 1 \pmod{4}$

Refined conjecture

- There may exist congruence obstructions, i.e. $m \pmod{n}$ that cannot occur.

Refined conjecture

- There may exist congruence obstructions, i.e. $m \pmod{n}$ that cannot occur.
- If a number is not ruled out by a congruence, call it admissible.

Refined conjecture

- There may exist congruence obstructions, i.e. $m \pmod{n}$ that cannot occur.
- If a number is not ruled out by a congruence, call it admissible.

Conjecture

If $\delta_{\mathcal{A}} > 1/2$, then $D_{\mathcal{A}}$ contains all but finitely many admissible positive integers.

Refined conjecture

- There may exist congruence obstructions, i.e. $m \pmod{n}$ that cannot occur.
- If a number is not ruled out by a congruence, call it admissible.

Conjecture

If $\delta_{\mathcal{A}} > 1/2$, then $D_{\mathcal{A}}$ contains all but finitely many admissible positive integers.

- Kontorovich: more precise conjecture, incorporating a linear functional $L(x/y) = ax + by$ and an asymptotic count of the multiplicity.

Main Theorem

Theorem (R.-Stange)

Consider all rational numbers q which have a continued fraction of the form

$$q = [0; a_1, a_2, \dots, a_k, b, 1, 2]$$

where $a_k \in \{4, 8, 12, 16, \dots\} = 4\mathbb{Z}^+$ and $b \in \mathbb{Z}^+$. Then no denominator of q is a perfect square.

Main Theorem

Theorem (R.-Stange)

Consider all rational numbers q which have a continued fraction of the form

$$q = [0; a_1, a_2, \dots, a_k, b, 1, 2]$$

where $a_k \in \{4, 8, 12, 16, \dots\} = 4\mathbb{Z}^+$ and $b \in \mathbb{Z}^+$. Then no denominator of q is a perfect square.

Corresponding Hausdorff dimension is ≈ 0.6 .

All integers are admissible.

Main Theorem

Theorem (R.-Stange)

Consider all rational numbers q which have a continued fraction of the form

$$q = [0; a_1, a_2, \dots, a_k, b, 1, 2]$$

where $a_k \in \{4, 8, 12, 16, \dots\} = 4\mathbb{Z}^+$ and $b \in \mathbb{Z}^+$. Then no denominator of q is a perfect square.

Corresponding Hausdorff dimension is ≈ 0.6 .

All integers are admissible.

Computed up to 2×10^{13} , last missing non-square is $7968219670470 \approx 7.9 \cdot 10^{12}$.

Consequences

- The denominator of

$$q = [0; a_1, a_2, \dots, a_k, 1, 1, 2]$$

is $L(x, y) = 3x + 5y$, where

$$\frac{x}{y} = [0; a_1, a_2, \dots, a_k]$$

Consequences

- The denominator of

$$q = [0; a_1, a_2, \dots, a_k, 1, 1, 2]$$

is $L(x, y) = 3x + 5y$, where

$$\frac{x}{y} = [0; a_1, a_2, \dots, a_k]$$

- Taking $a_i \in \mathcal{A} = \{4, 8, 12, \dots, 128\}$ guarantees $\delta_{\mathcal{A}} > 1/2$.

Consequences

- The denominator of

$$q = [0; a_1, a_2, \dots, a_k, 1, 1, 2]$$

is $L(x, y) = 3x + 5y$, where

$$\frac{x}{y} = [0; a_1, a_2, \dots, a_k]$$

- Taking $a_i \in \mathcal{A} = \{4, 8, 12, \dots, 128\}$ guarantees $\delta_{\mathcal{A}} > 1/2$.
- Disproves the conjecture of Kontorovich

Proof outline

- Assume that one of $x, y \equiv 1 \pmod{4}$, and that $\left(\frac{x}{y}\right) = -1$.

Proof outline

- Assume that one of $x, y \equiv 1 \pmod{4}$, and that $\left(\frac{x}{y}\right) = -1$.
- Replace $\frac{x}{y}$ by $\frac{y}{x+4ky}$.

Proof outline

- Assume that one of $x, y \equiv 1 \pmod{4}$, and that $\left(\frac{x}{y}\right) = -1$.
- Replace $\frac{x}{y}$ by $\frac{y}{x+4ky}$.
- Congruence clearly preserved.
- Quadratic reciprocity: Kronecker symbol preserved.

Proof outline

- Assume that one of $x, y \equiv 1 \pmod{4}$, and that $\left(\frac{x}{y}\right) = -1$.
- Replace $\frac{x}{y}$ by $\frac{y}{x+4ky}$.
- Congruence clearly preserved.
- Quadratic reciprocity: Kronecker symbol preserved.
- Thus, denominator never a square!

Proof outline

- Assume that one of $x, y \equiv 1 \pmod{4}$, and that $\left(\frac{x}{y}\right) = -1$.
- Replace $\frac{x}{y}$ by $\frac{y}{x+4ky}$.
- Congruence clearly preserved.
- Quadratic reciprocity: Kronecker symbol preserved.
- Thus, denominator never a square!
- The “tail” of $[1, 1, 2]$: start the orbit at $\frac{3}{5}$ to have -1 Kronecker symbol.

Zaremba consequences

- Very strong numerical evidence towards being true.

Zaremba consequences

- Very strong numerical evidence towards being true.
- Considering pure denominators: must start orbit at $\frac{0}{1}$, which has $\left(\frac{0}{1}\right) = 1$.

Zaremba consequences

- Very strong numerical evidence towards being true.
- Considering pure denominators: must start orbit at $\frac{0}{1}$, which has $\left(\frac{0}{1}\right) = 1$.
- Unclear whether an obstruction will exist for a general linear functional.

Origin of the idea

- Wanted to make a subgroup of $SL(2, \mathbb{Z})$ that preserved Kronecker symbol.

Origin of the idea

- Wanted to make a subgroup of $\mathrm{SL}(2, \mathbb{Z})$ that preserved Kronecker symbol.

Definition

$$\Psi := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(4) : a, b, c, d \geq 0, \left(\frac{a}{b} \right) = 1 \right\}.$$

Origin of the idea

- Wanted to make a subgroup of $\mathrm{SL}(2, \mathbb{Z})$ that preserved Kronecker symbol.

Definition

$$\Psi := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(4) : a, b, c, d \geq 0, \begin{pmatrix} a \\ b \end{pmatrix} = 1 \right\}.$$

Proposition

Ψ is a semigroup.

Origin of the idea

- Wanted to make a subgroup of $SL(2, \mathbb{Z})$ that preserved Kronecker symbol.

Definition

$$\Psi := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(4) : a, b, c, d \geq 0, \left(\frac{a}{b} \right) = 1 \right\}.$$

Proposition

Ψ is a semigroup.

Proposition

If $x, y \in \mathbb{Z}^+$, y is odd, and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Psi$, then

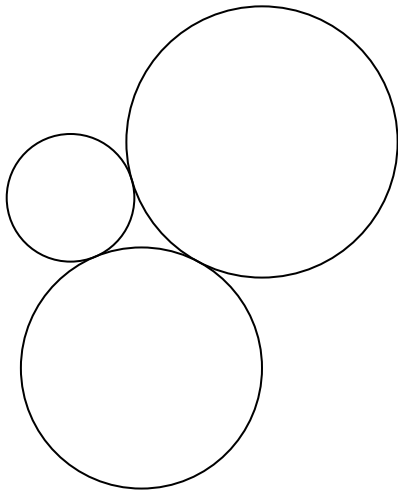
$$\begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

Apollonian circle packings

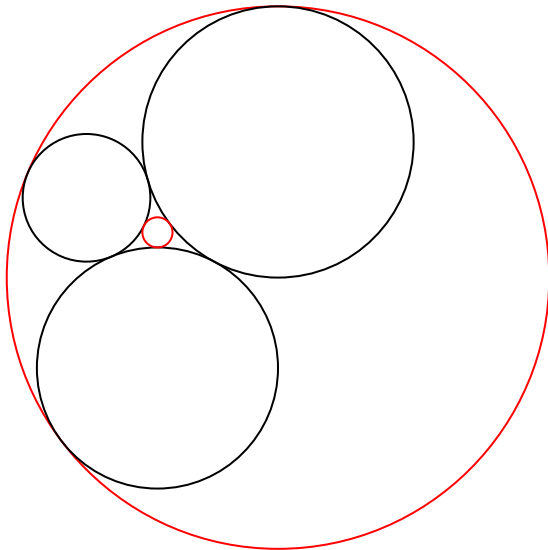
Theorem (Apollonius)

Let three mutually tangent circles be drawn in the plane. Then there are exactly two more circles that can be drawn that are mutually tangent to the original three circles.

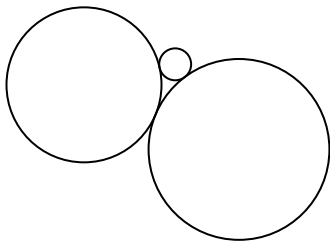
Example 1



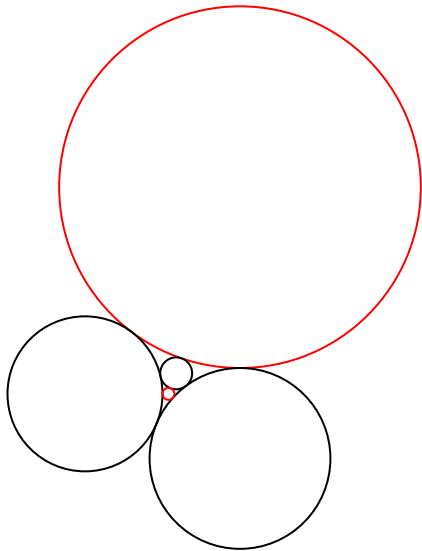
Example 1



Example 2



Example 2



Apollonian circle packing: repeat!

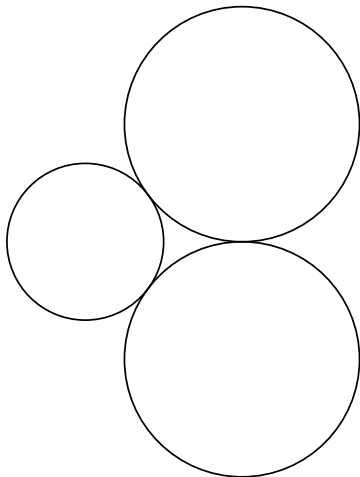


Figure 1: Generation 0

Apollonian circle packing: repeat!

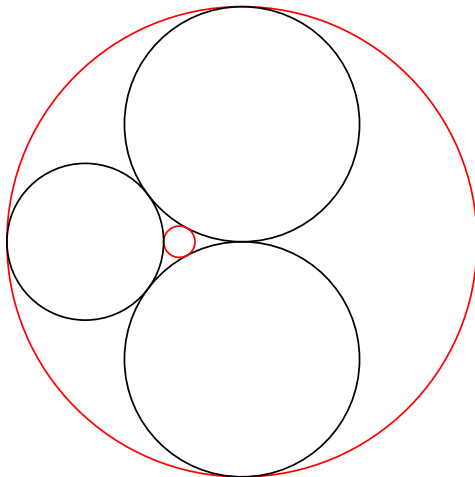


Figure 1: Generation 1

Apollonian circle packing: repeat!

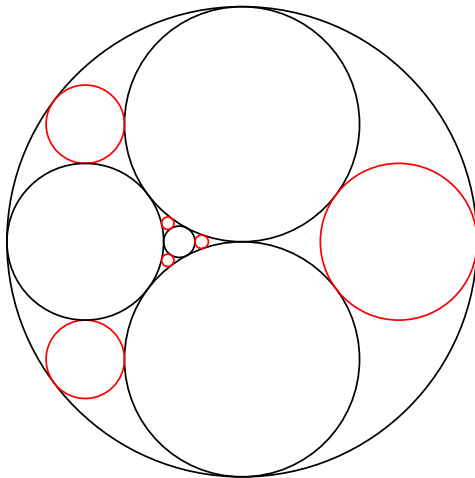


Figure 1: Generation 2

Apollonian circle packing: repeat!

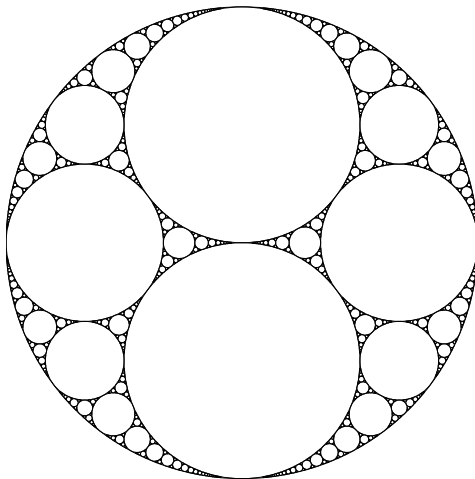


Figure 1: Radius $\geq \frac{1}{500}$.

Descartes equation

Definition

The curvature of a circle of radius r is $\frac{1}{r}$.

Descartes equation

Definition

The curvature of a circle of radius r is $\frac{1}{r}$.

Theorem (Descartes, Princess Elisabeth, 1643)

Let four mutually tangent circles have curvatures a, b, c, d . Then

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2.$$

Descartes equation

Definition

The curvature of a circle of radius r is $\frac{1}{r}$.

Theorem (Descartes, Princess Elisabeth, 1643)

Let four mutually tangent circles have curvatures a, b, c, d . Then

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2.$$

Definition

We call (a, b, c, d) a Descartes quadruple.

Circle swaps

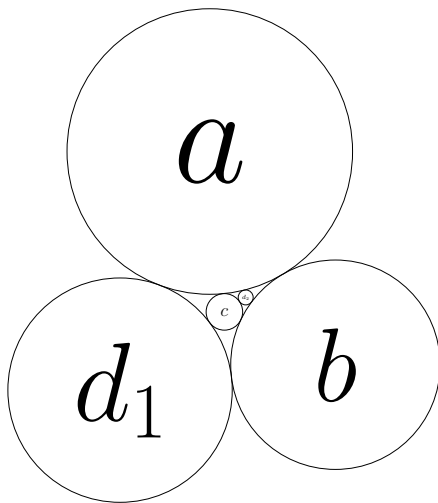


Figure 2: Swapping d_1 with d_2

Circle swaps - algebra

- $d = d_1$ and $d = d_2$ satisfy:

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2$$

Circle swaps - algebra

- $d = d_1$ and $d = d_2$ satisfy:

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2$$

- Rearrange:

$$d^2 - 2(a + b + c)d + 2(a^2 + b^2 + c^2) - (a + b + c)^2 = 0$$

Circle swaps - algebra

- $d = d_1$ and $d = d_2$ satisfy:

$$2(a^2 + b^2 + c^2 + d^2) = (a + b + c + d)^2$$

- Rearrange:

$$d^2 - 2(a + b + c)d + 2(a^2 + b^2 + c^2) - (a + b + c)^2 = 0$$

- Vieta jumping:

$$d_1 + d_2 = 2a + 2b + 2c$$

Example

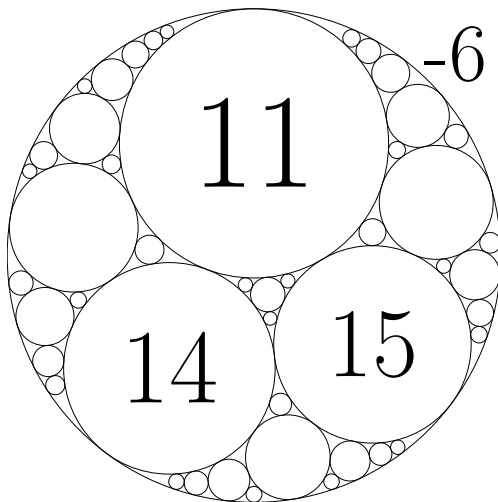


Figure 3: Quadruple $(-6, 11, 14, 15)$

Example

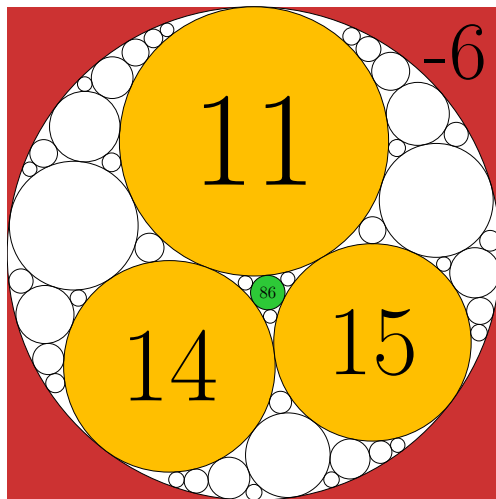


Figure 4: $2(11 + 14 + 15) - (-6) = 86$

Example

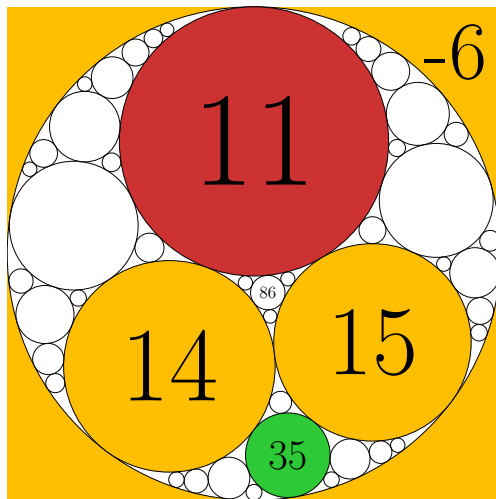


Figure 5: $2(-6 + 14 + 15) - 11 = 35$

Example

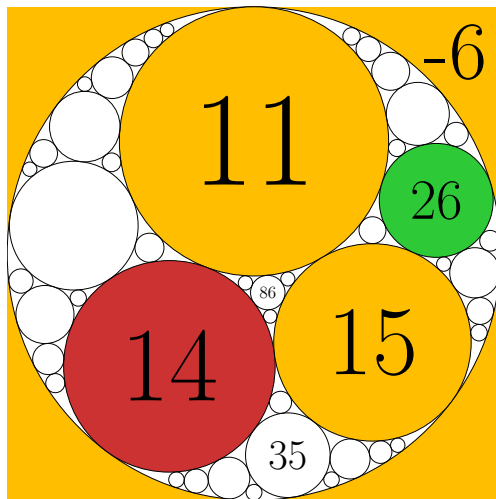


Figure 6: $2(-6 + 11 + 15) - 14 = 26$

Example

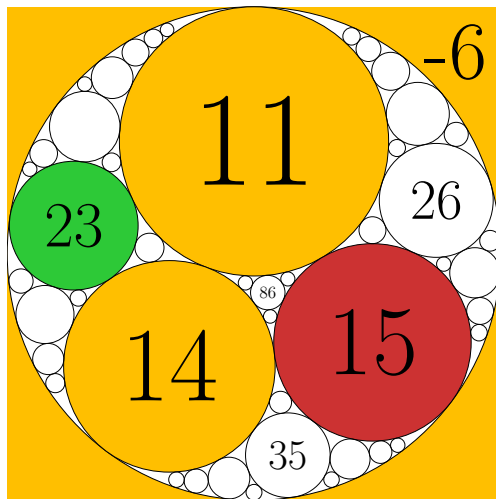


Figure 7: $2(-6 + 11 + 14) - 15 = 23$

Example

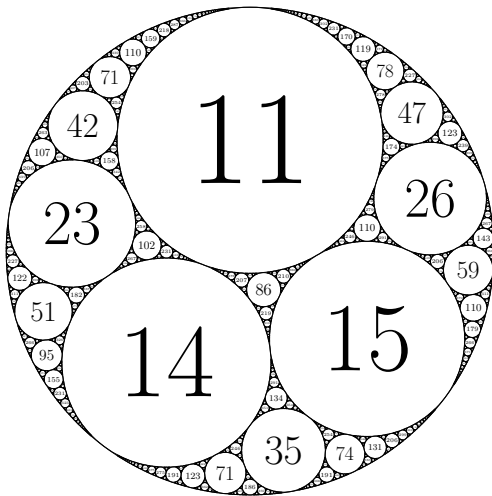


Figure 8: Repeat!

Integral theory

- If $a, b, c, d \in \mathbb{Z}$, then all curvatures are integers.

Integral theory

- If $a, b, c, d \in \mathbb{Z}$, then all curvatures are integers.
- Restrict to $\gcd(a, b, c, d) = 1$ (primitive).

Integral theory

- If $a, b, c, d \in \mathbb{Z}$, then all curvatures are integers.
- Restrict to $\gcd(a, b, c, d) = 1$ (primitive).

Question

What curvatures appear in a fixed primitive Apollonian circle packing?

Circle packings as thin groups

- The Apollonian group is

$$\Gamma = \left\langle \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix} \right\rangle.$$

Circle packings as thin groups

- The Apollonian group is

$$\Gamma = \left\langle \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix} \right\rangle.$$

- Let $v \in \mathbb{Z}^4$ be a primitive solution to the Descartes equation.

Circle packings as thin groups

- The Apollonian group is

$$\Gamma = \left\langle \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix} \right\rangle.$$

- Let $v \in \mathbb{Z}^4$ be a primitive solution to the Descartes equation.
- The curvatures of circles appearing in the corresponding circle packing are the entries of $\Gamma \cdot v$.

Circle packings as thin groups

- The Apollonian group is

$$\Gamma = \left\langle \begin{pmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{pmatrix} \right\rangle.$$

- Let $v \in \mathbb{Z}^4$ be a primitive solution to the Descartes equation.
- The curvatures of circles appearing in the corresponding circle packing are the entries of $\Gamma \cdot v$.
- This is a union of four thin group orbits.

Curvatures

Question

What curvatures appear in a fixed primitive Apollonian circle packing?

Curvatures

Question

What curvatures appear in a fixed primitive Apollonian circle packing?

- At most one negative curvature can appear.

Curvatures

Question

What curvatures appear in a fixed primitive Apollonian circle packing?

- At most one negative curvature can appear.
- Hausdorff dimension $\delta \approx 1.3057$, circles of curvature at most N grows like cN^δ .

Curvatures

Question

What curvatures appear in a fixed primitive Apollonian circle packing?

- At most one negative curvature can appear.
- Hausdorff dimension $\delta \approx 1.3057$, circles of curvature at most N grows like cN^δ .
- Congruence obstructions modulo 24.

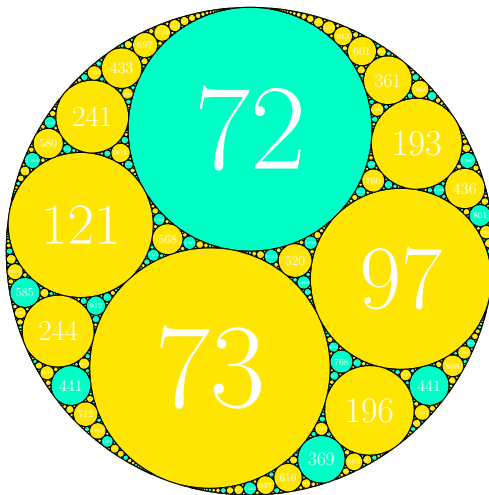


Figure 9: $(-36, 72, 73, 97)$, circles of curvature ≤ 20000

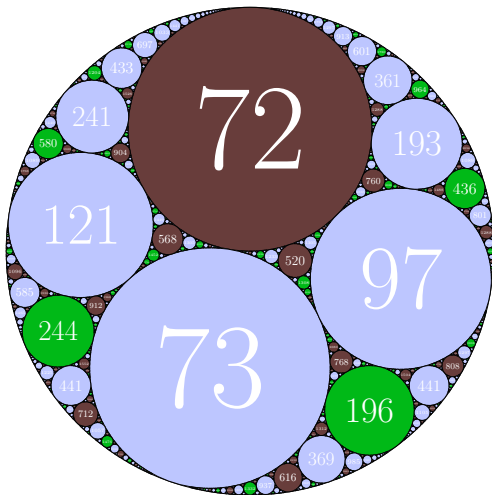


Figure 10: $(-36, 72, 73, 97)$, circles of curvature ≤ 20000

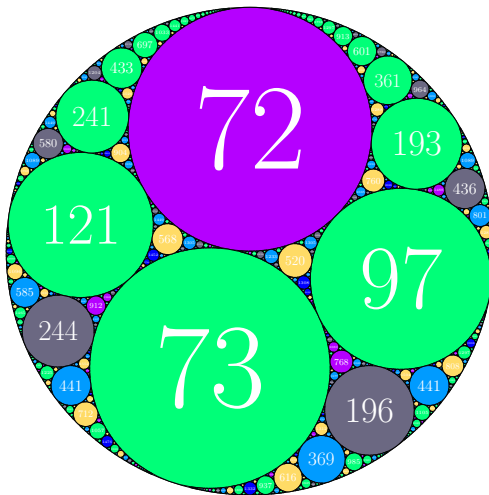


Figure 11: $(-36, 72, 73, 97)$, circles of curvature ≤ 20000

Missing curvatures

Definition

Let \mathcal{A} be a primitive Apollonian circle packing. Call a positive curvature c *missing* in \mathcal{A} if curvatures equivalent to $c \pmod{24}$ appear in \mathcal{A} but c does not.

Missing curvatures

Definition

Let \mathcal{A} be a primitive Apollonian circle packing. Call a positive curvature c *missing* in \mathcal{A} if curvatures equivalent to $c \pmod{24}$ appear in \mathcal{A} but c does not.

Conjecture (Local-global conjecture: Graham-Lagarias-Mallows-Wilks-Yan and Fuchs-Sanden)

The number of missing curvatures is finite.

Local-global is false!

Theorem (Haag-Kertzer-R.-Stange)

There exist infinitely many primitive Apollonian circle packings for which the number of missing curvatures up to N is $\Omega(\sqrt{N})$. In particular, the local-global conjecture is false for these packings.

Local-global is false!

- More generally, we find families of the form

$$cx^2 : c \in \{1, 2, 3, 6\}$$

$$dx^4 : d \in \{1, 4, 9, 36\}$$

which are entirely missing.

Local-global is false!

- More generally, we find families of the form

$$cx^2 : c \in \{1, 2, 3, 6\}$$

$$dx^4 : d \in \{1, 4, 9, 36\}$$

which are entirely missing.

- Such families are deemed *reciprocity obstructions*.

Local-global is false!

- More generally, we find families of the form

$$cx^2 : c \in \{1, 2, 3, 6\}$$

$$dx^4 : d \in \{1, 4, 9, 36\}$$

which are entirely missing.

- Such families are deemed *reciprocity obstructions*.
- Given a packing, we classify which (if any) reciprocity obstructions are present.

Local-global is false!

- More generally, we find families of the form

$$cx^2 : c \in \{1, 2, 3, 6\}$$

$$dx^4 : d \in \{1, 4, 9, 36\}$$

which are entirely missing.

- Such families are deemed *reciprocity obstructions*.
- Given a packing, we classify which (if any) reciprocity obstructions are present.
- Extensive computation suggests this list is complete.

Quadratic and quartic obstructions

Type	Quadratic	Quartic	L-G false	L-G open
$(6, 1, 1, 1)$				0, 1, 4, 9, 12, 16
$(6, 1, 1, -1)$		$n^4, 4n^4, 9n^4, 36n^4$	0, 1, 4, 9, 12, 16	
$(6, 1, -1)$	$n^2, 2n^2, 3n^2, 6n^2$		0, 1, 4, 9, 12, 16	
$(6, 5, 1)$	$2n^2, 3n^2$		0, 8, 12	5, 20, 21
$(6, 5, -1)$	$n^2, 6n^2$		0, 12	5, 8, 20, 21
$(6, 13, 1)$	$2n^2, 6n^2$		0	4, 12, 13, 16, 21
$(6, 13, -1)$	$n^2, 3n^2$		0, 4, 12, 16	13, 21
$(6, 17, 1, 1)$	$3n^2, 6n^2$	$9n^4, 36n^4$	0, 9, 12	8, 17, 20
$(6, 17, 1, -1)$	$3n^2, 6n^2$	$n^4, 4n^4$	0, 9, 12	8, 17, 20
$(6, 17, -1)$	$n^2, 2n^2$		0, 8, 9, 12	17, 20
$(8, 7, 1)$	$3n^2, 6n^2$		3, 6	7, 10, 15, 18, 19, 22
$(8, 7, -1)$	$2n^2$		18	3, 6, 7, 10, 15, 19, 22
$(8, 11, 1)$				2, 3, 6, 11, 14, 15, 18, 23
$(8, 11, -1)$	$2n^2, 3n^2, 6n^2$		2, 3, 6, 18	11, 14, 15, 23

Example

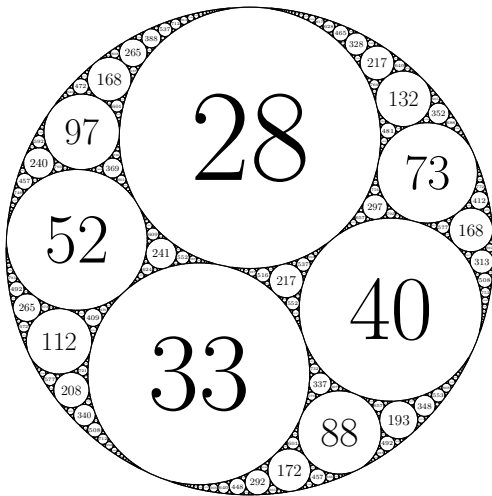


Figure 12: Missing $x^2, 2x^2, 3x^2, 6x^2$

Example

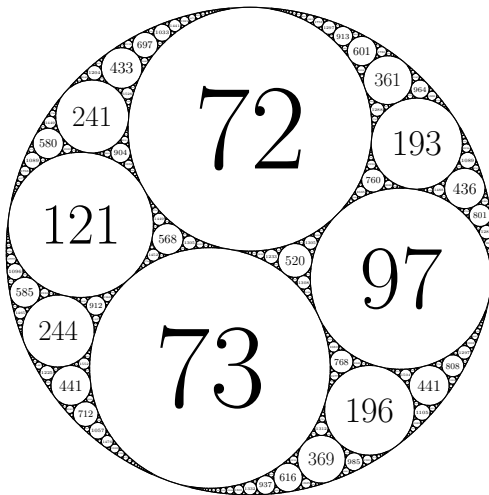


Figure 13: Missing $x^4, 4x^4, 9x^4, 36x^4$

Example

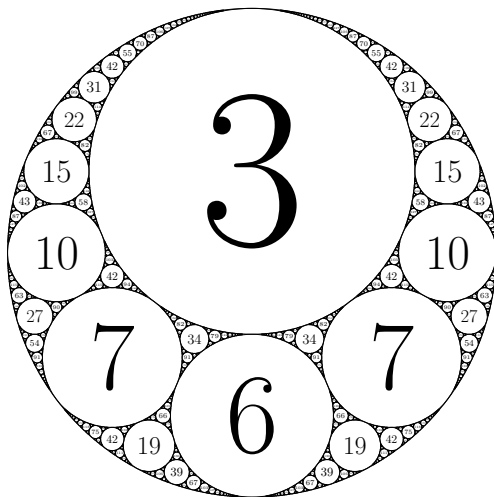


Figure 14: Missing $2x^2$

Example

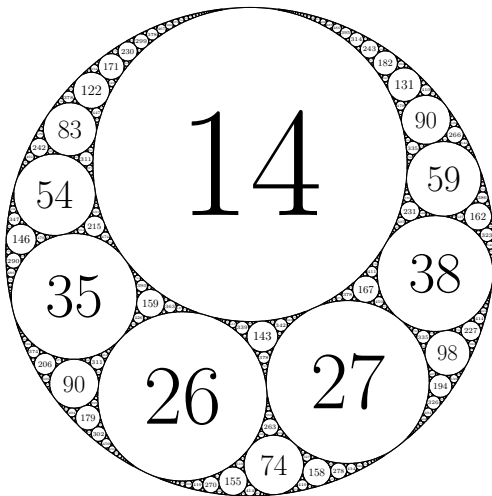


Figure 15: No reciprocity obstructions. Local-global may still be true!

Fix a packing

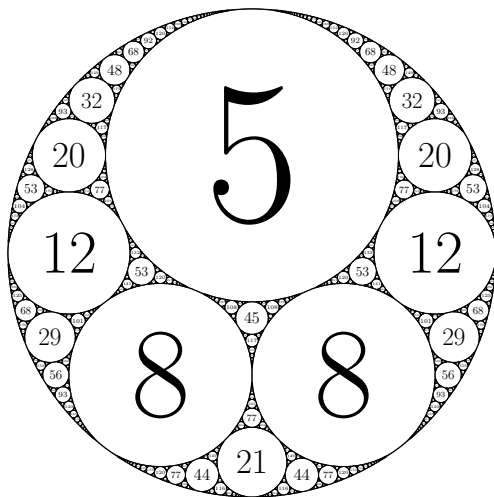


Figure 16: $(-3, 5, 8, 8)$

Fix a circle

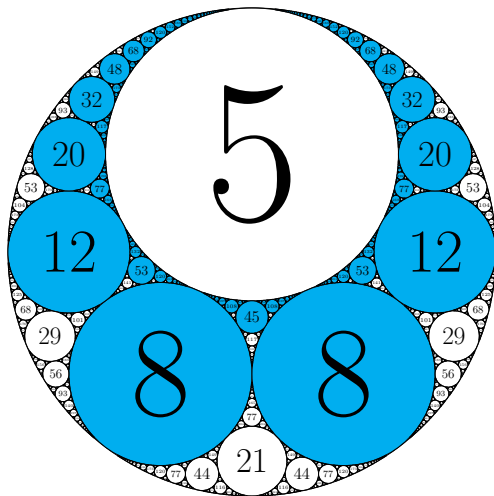
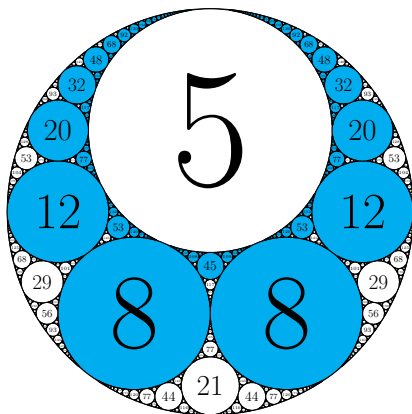


Figure 17: Circles tangent to curvature 5 circle

Curvatures of circles tangent to a fixed circle

Possible curvatures:

$-3, 8, 12, 20, 32, 45, 48, 53, 68, 77, \dots$



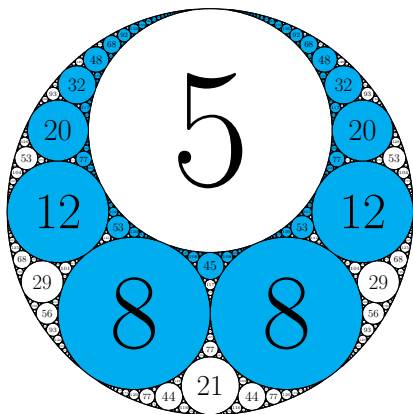
Curvatures of circles tangent to a fixed circle

Possible curvatures:

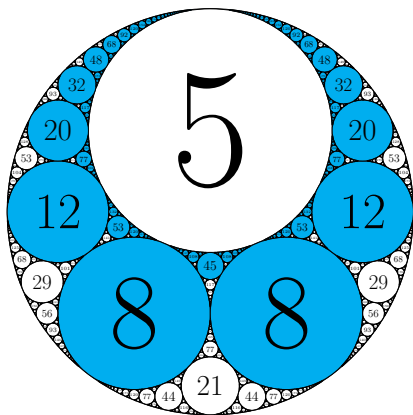
$-3, 8, 12, 20, 32, 45, 48, 53, 68, 77, \dots$

Consider the quadratic function

$$f(x, y) = 13x^2 + 24xy + 13y^2 - 5$$



Curvatures of circles tangent to a fixed circle



Possible curvatures:

$$-3, 8, 12, 20, 32, 45, 48, 53, 68, 77, \dots$$

Consider the quadratic function

$$f(x, y) = 13x^2 + 24xy + 13y^2 - 5$$

Note that

$$\begin{array}{ll} -3 = f(1, -1), & 8 = f(1, 0), \\ 12 = f(2, -1), & 20 = f(3, -2), \\ 32 = f(4, -3), & 45 = f(1, 1), \dots \end{array}$$

Tangent circles

Observation of Sarnak:

$$\{\text{values of } f(x, y) \text{ with } x, y \text{ coprime integers}\} = \{\text{curvatures of tangent circles}\}$$

Tangent circles

Observation of Sarnak:

$$\{\text{values of } f(x, y) \text{ with } x, y \text{ coprime integers}\} = \{\text{curvatures of tangent circles}\}$$

In general, from (a, b, c, d) , to the first circle we associate

$$(a + b)x^2 + (a + b + c - d)xy + (a + c)y^2 - a.$$

The unshifted quadratic form has discriminant $-4a^2$.

Tangent circles

In our case,

$$f(x, y) \equiv 13x^2 + 24xy + 13y^2 - 5 \equiv 3x^2 - 6xy + 3y^2 \equiv 3(x - y)^2 \pmod{5}$$

Tangent circles

In our case,

$$f(x, y) \equiv 13x^2 + 24xy + 13y^2 - 5 \equiv 3x^2 - 6xy + 3y^2 \equiv 3(x - y)^2 \pmod{5}$$

If a circle of curvature c is tangent to the curvature 5 circle and $\gcd(c, 5) = 1$, then

$$\left(\frac{c}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Tangent circles

In our case,

$$f(x, y) \equiv 13x^2 + 24xy + 13y^2 - 5 \equiv 3x^2 - 6xy + 3y^2 \equiv 3(x - y)^2 \pmod{5}$$

If a circle of curvature c is tangent to the curvature 5 circle and $\gcd(c, 5) = 1$, then

$$\left(\frac{c}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

In particular, it cannot be square!

General case

Definition

Let \mathcal{C} be a circle of curvature a , and let a tangent circle have curvature b with $\gcd(a, b) = 1$. Define

$$\chi_2(\mathcal{C}) = \left(\frac{b}{a}\right) \in \{-1, 1\}.$$

General case

Definition

Let \mathcal{C} be a circle of curvature a , and let a tangent circle have curvature b with $\gcd(a, b) = 1$. Define

$$\chi_2(\mathcal{C}) = \left(\frac{b}{a}\right) \in \{-1, 1\}.$$

A similar computation shows that this is well defined in the packing $(-3, 5, 8, 8)$.

Quadratic reciprocity

If \mathcal{C}_1 and \mathcal{C}_2 are tangent with coprime curvatures a, b , then

$$\chi_2(\mathcal{C}_1) = \left(\frac{b}{a}\right) = \left(\frac{a}{b}\right) = \chi_2(\mathcal{C}_2),$$

as one of them is $1 \pmod{4}$.

Quadratic reciprocity

If \mathcal{C}_1 and \mathcal{C}_2 are tangent with coprime curvatures a, b , then

$$\chi_2(\mathcal{C}_1) = \left(\frac{b}{a}\right) = \left(\frac{a}{b}\right) = \chi_2(\mathcal{C}_2),$$

as one of them is $1 \pmod{4}$.

Consider the following graph:

- vertices = circles;
- edges between tangent circles of coprime curvature.

Quadratic reciprocity

If \mathcal{C}_1 and \mathcal{C}_2 are tangent with coprime curvatures a, b , then

$$\chi_2(\mathcal{C}_1) = \left(\frac{b}{a}\right) = \left(\frac{a}{b}\right) = \chi_2(\mathcal{C}_2),$$

as one of them is $1 \pmod{4}$.

Consider the following graph:

- vertices = circles;
- edges between tangent circles of coprime curvature.

This graph is connected! Thus χ_2 is constant across the packing.

Sample path

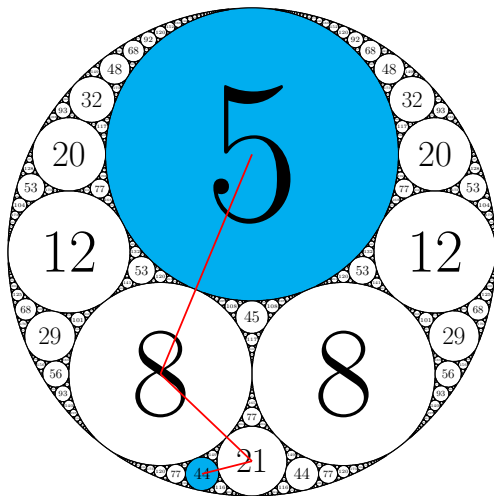


Figure 18: One coprime path

Consequences

We already observed that $\chi_2 = -1$ for the curvature 5 circle.

Consequences

We already observed that $\chi_2 = -1$ for the curvature 5 circle.

Thus $\chi_2 = -1$ for the entire packing!

Consequences

We already observed that $\chi_2 = -1$ for the curvature 5 circle.

Thus $\chi_2 = -1$ for the entire packing!

If a curvature was a perfect square, then

$$\chi_2(\mathcal{C}) = \left(\frac{b}{n^2} \right) = 1,$$

contradiction.

New conjecture

Definition

Call a curvature that is not ruled out by congruence conditions or one of our reciprocity obstructions *sporadic*.

New conjecture

Definition

Call a curvature that is not ruled out by congruence conditions or one of our reciprocity obstructions *sporadic*.

Conjecture

There are finitely many sporadic curvatures.

In other words, we have found the only exceptions to the local-global conjecture.

Back to thin orbits

- Let $\Gamma \subseteq \mathrm{GL}(n, \mathbb{Z})$ be thin.
- Let $v \in \mathbb{Z}^n$ be a primitive vector.
- Let $L : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be a linear functional.
- What can we say about $L(\Gamma \cdot v) \subseteq \mathbb{Z}$?

$L(\Gamma \cdot v)$ standard obstructions

- **Inherited:** obstructions may exist for an algebraic set containing Γ .

$L(\Gamma \cdot v)$ standard obstructions

- **Inherited:** obstructions may exist for an algebraic set containing Γ .
- **Definiteness:** $L(\Gamma \cdot v)$ may only represent numbers above/below a certain cutoff.

$L(\Gamma \cdot v)$ standard obstructions

- **Inherited:** obstructions may exist for an algebraic set containing Γ .
- **Definiteness:** $L(\Gamma \cdot v)$ may only represent numbers above/below a certain cutoff.
- Let $S(N) = \{n \in \mathbb{Z} : |n| \leq N, n \in L(\Gamma \cdot v)\}$ be counted *with multiplicity*.

$L(\Gamma \cdot v)$ standard obstructions

- **Inherited:** obstructions may exist for an algebraic set containing Γ .
- **Definiteness:** $L(\Gamma \cdot v)$ may only represent numbers above/below a certain cutoff.
- Let $S(N) = \{n \in \mathbb{Z} : |n| \leq N, n \in L(\Gamma \cdot v)\}$ be counted *with multiplicity*.
- **Counting:** often, $|S(N)| \sim CN^\delta$ for some δ , the critical exponent.

$L(\Gamma \cdot \nu)$ standard obstructions

- **Inherited:** obstructions may exist for an algebraic set containing Γ .
- **Definiteness:** $L(\Gamma \cdot \nu)$ may only represent numbers above/below a certain cutoff.
- Let $S(N) = \{n \in \mathbb{Z} : |n| \leq N, n \in L(\Gamma \cdot \nu)\}$ be counted *with multiplicity*.
- **Counting:** often, $|S(N)| \sim CN^\delta$ for some δ , the critical exponent.
- **Congruence:** an integer n is *admissible* if integers equivalent to $n \pmod{d}$ occur in $L(\Gamma \cdot \nu)$ for all $d \in \mathbb{Z}^+$.

$L(\Gamma \cdot \nu)$ standard obstructions

- **Inherited:** obstructions may exist for an algebraic set containing Γ .
- **Definiteness:** $L(\Gamma \cdot \nu)$ may only represent numbers above/below a certain cutoff.
- Let $S(N) = \{n \in \mathbb{Z} : |n| \leq N, n \in L(\Gamma \cdot \nu)\}$ be counted *with multiplicity*.
- **Counting:** often, $|S(N)| \sim CN^\delta$ for some δ , the critical exponent.
- **Congruence:** an integer n is *admissible* if integers equivalent to $n \pmod{d}$ occur in $L(\Gamma \cdot \nu)$ for all $d \in \mathbb{Z}^+$.
- Congruence obstructions boil down to a single modulus.

Local-global conjecture

- These obstructions *completely* describe $L(\Gamma \cdot v)$.

Local-global conjecture

- These obstructions *completely* describe $L(\Gamma \cdot v)$.
- Typical statement: “For all sufficiently large integers n such that $n \pmod{N} \notin X$, $n \in L(\Gamma \cdot v)$.”

Local-global conjecture

- These obstructions *completely* describe $L(\Gamma \cdot v)$.
- Typical statement: “For all sufficiently large integers n such that $n \pmod{N} \notin X$, $n \in L(\Gamma \cdot v)$.”
- Our two examples disprove this philosophy by adding in *reciprocity obstructions*.

What is a reciprocity obstruction?

- Congruence obstructions are a symptom of *strong approximation*, a property of the *group*.

What is a reciprocity obstruction?

- Congruence obstructions are a symptom of *strong approximation*, a property of the *group*.
- Individual orbits may or may not have a corresponding congruence obstruction.

What is a reciprocity obstruction?

- Congruence obstructions are a symptom of *strong approximation*, a property of the *group*.
- Individual orbits may or may not have a corresponding congruence obstruction.
- Should be an analogous definition for reciprocity obstructions.

What is a reciprocity obstruction?

- Congruence obstructions are a symptom of *strong approximation*, a property of the *group*.
- Individual orbits may or may not have a corresponding congruence obstruction.
- Should be an analogous definition for reciprocity obstructions.
- Required to *prove* that a group has no reciprocity obstructions.

What is a reciprocity obstruction?

- Congruence obstructions are a symptom of *strong approximation*, a property of the *group*.
- Individual orbits may or may not have a corresponding congruence obstruction.
- Should be an analogous definition for reciprocity obstructions.
- Required to *prove* that a group has no reciprocity obstructions.
- Need more examples!

Non-Apollonian circle packing

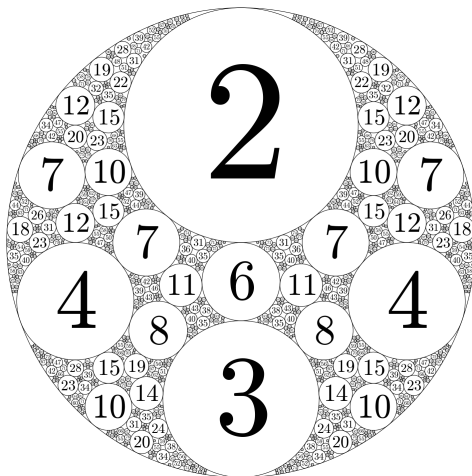


Figure 19: A non-Apollonian circle packing (Katherine E. Stange)