Dynamics of a Map of a Triangle and Some Open Problems in Theory of Numbers

Peter Maličký
Matej Bel University

Herl'any
April 16th, 2010

Európska únia
Európsky fond regionálneho rozvoja

Operačný program VÝSKUM a VÝVOJ

Agentúra Ministerstva školstva SR pre štrukturálne fondy EÚ

Podporujeme výskumné aktivity na Slovensku/
Projekt je spolufinancovaný zo zdrojov EÚ

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Table of contents

Problem to be solved

Given the plane triangle

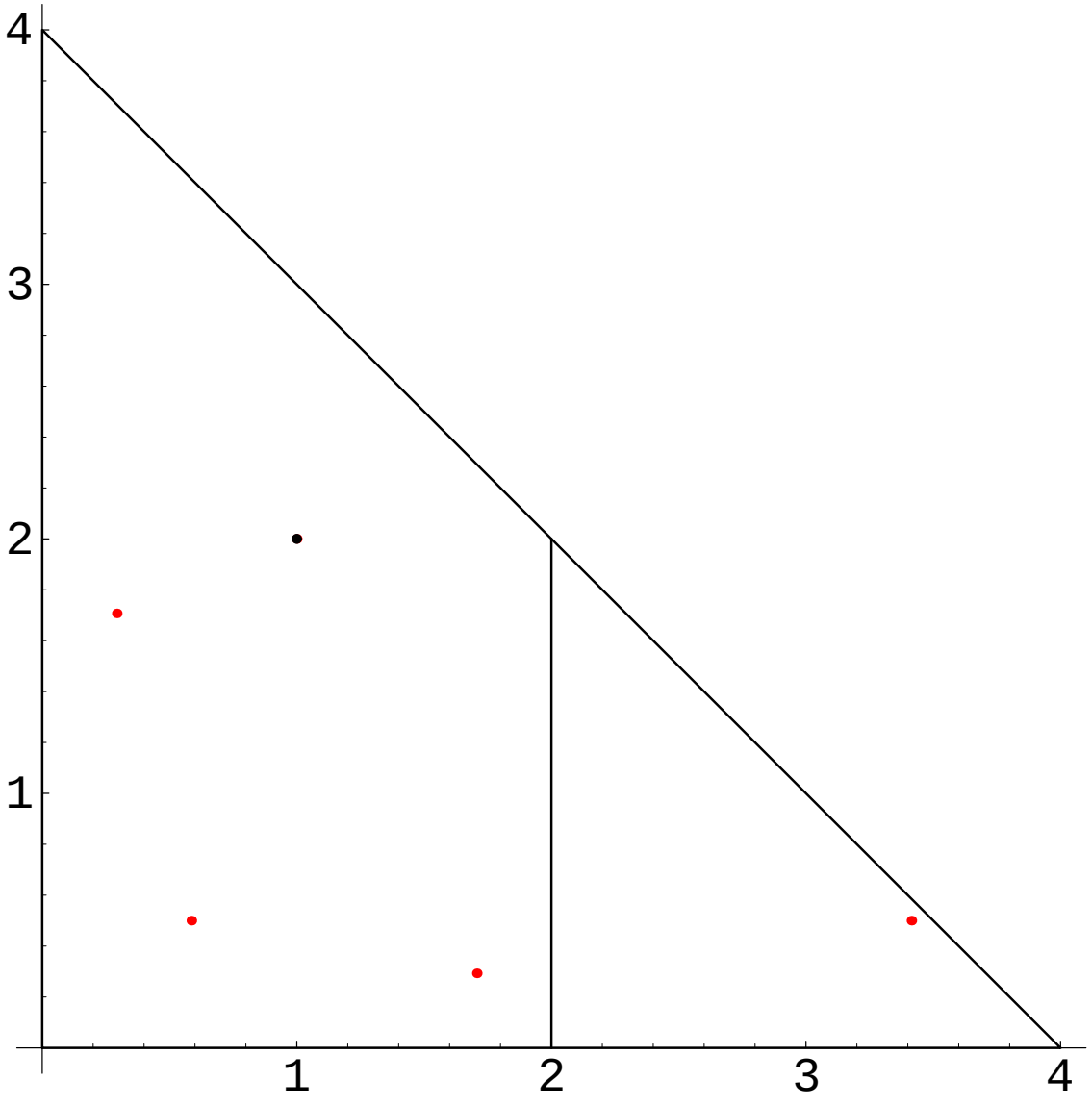
$$D = \{\, [x, y] : 0 \leq x,\ 0 \leq y,\ x + y \leq 4 \,\}$$

we consider the map

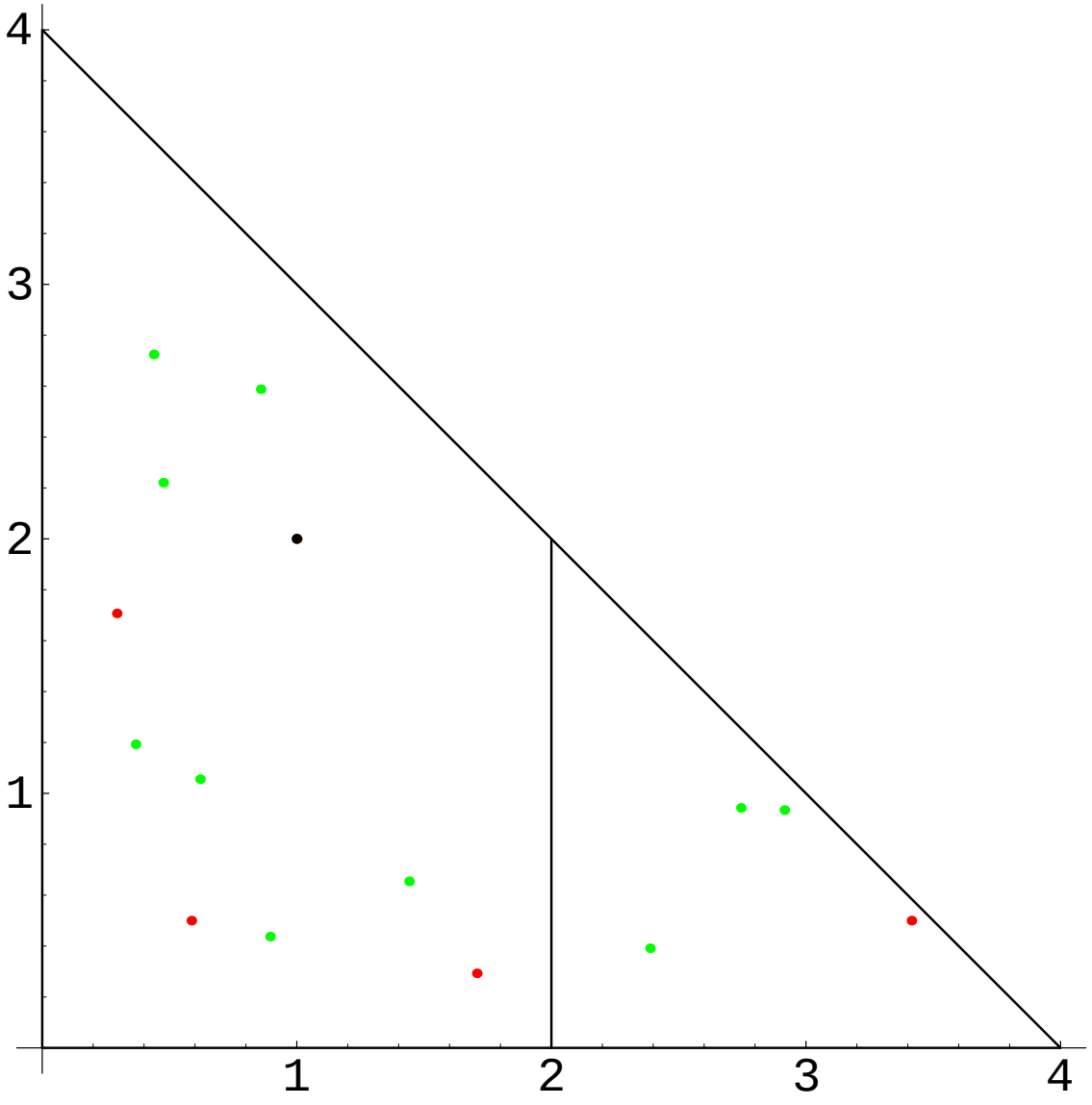
$$F : D \to D,\ [x, y] \mapsto [x(4 - x - y),\ xy]$$

and its periodic points.

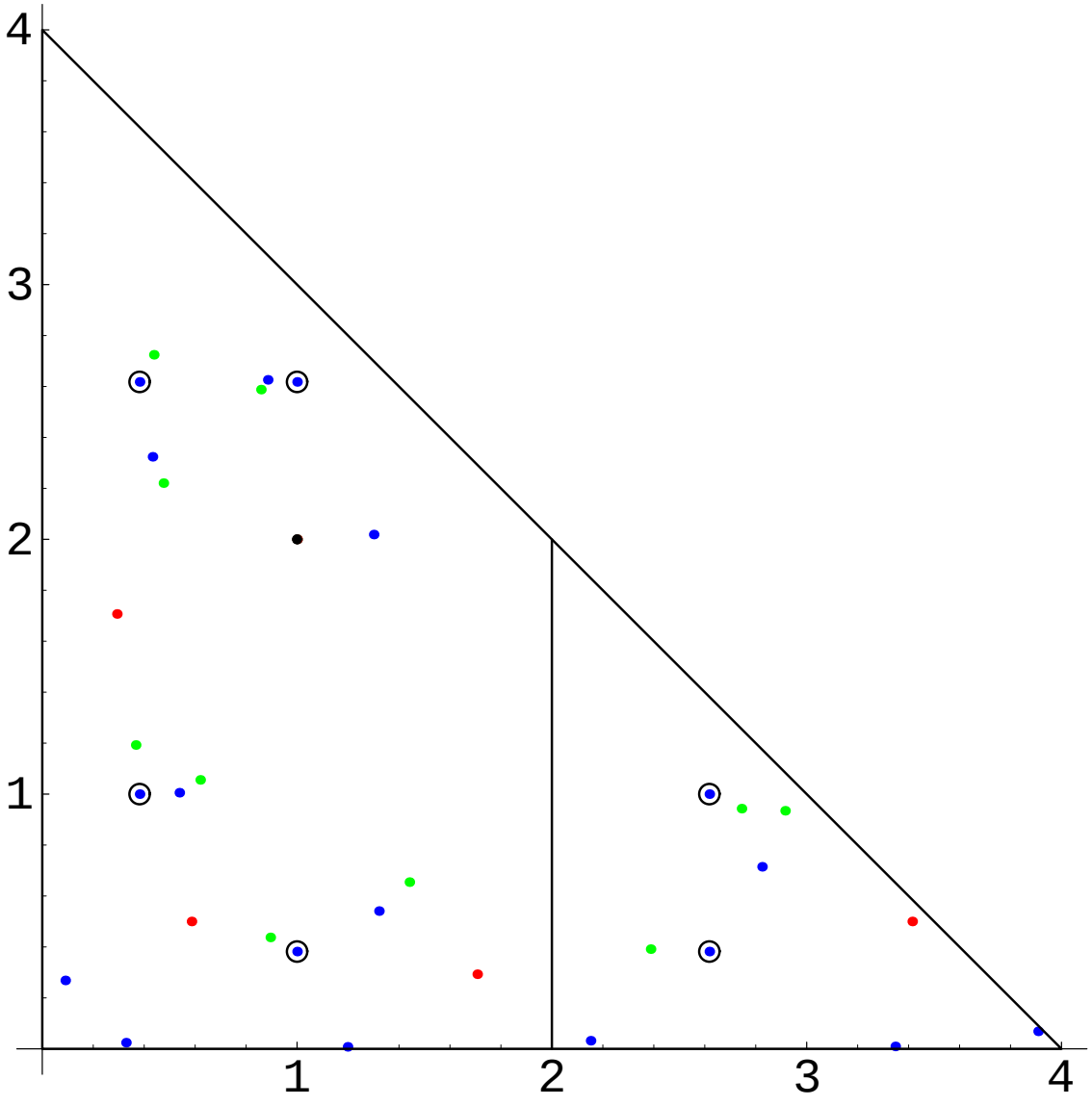
Interior points with period $n \leq 4$



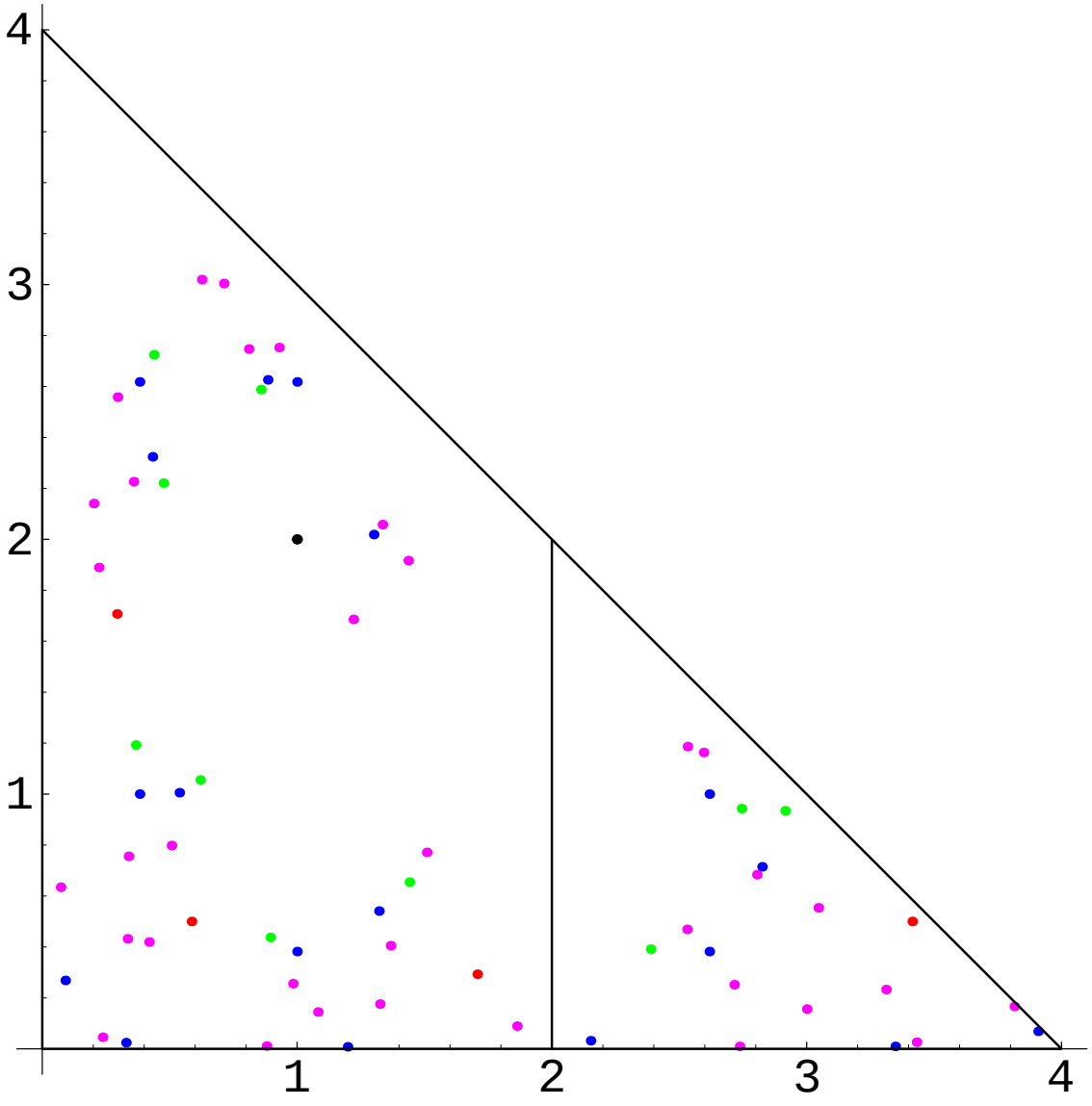
Interior points with period $n \leq 5$



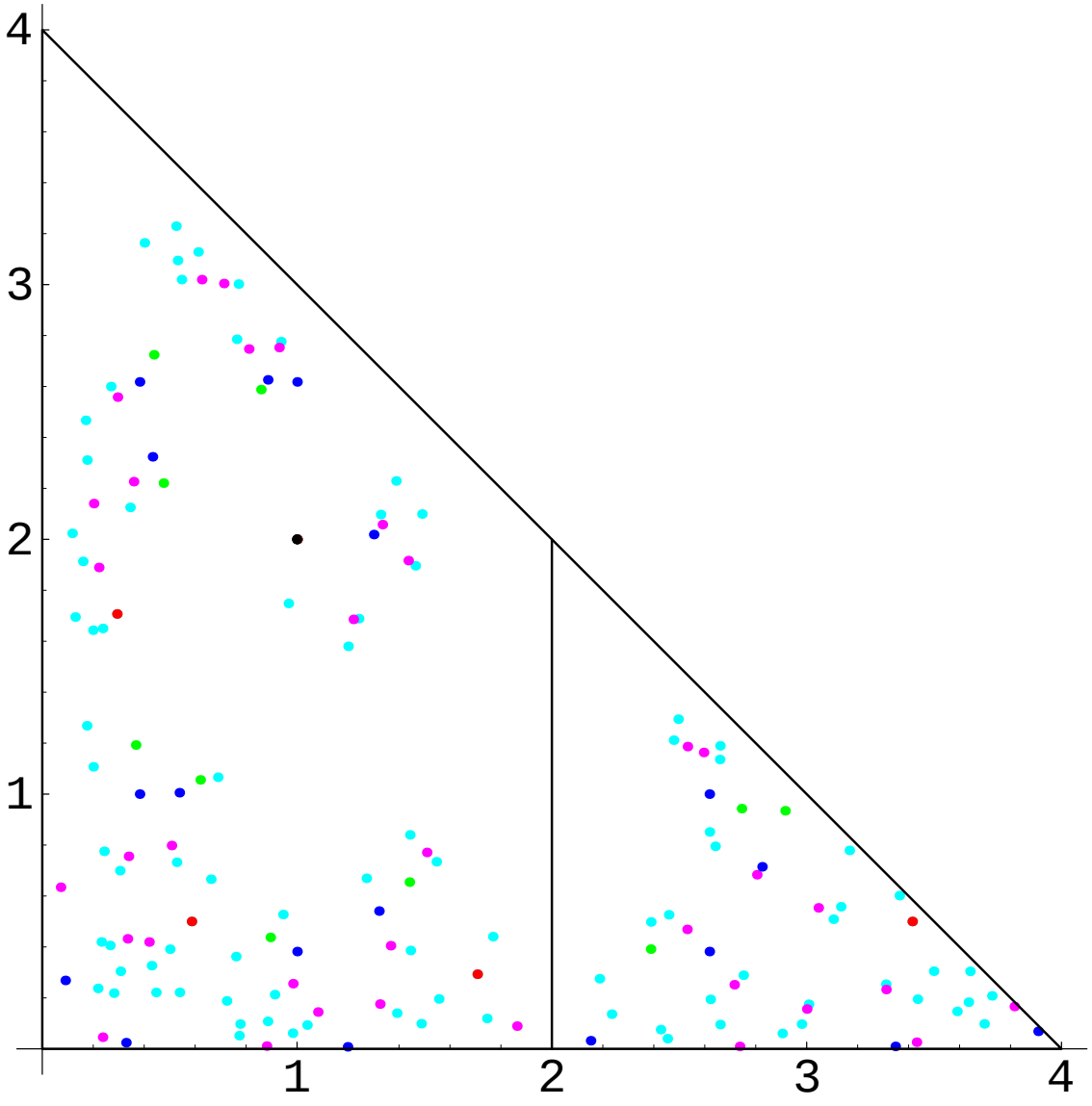
Interior points with period $n \leq 6$



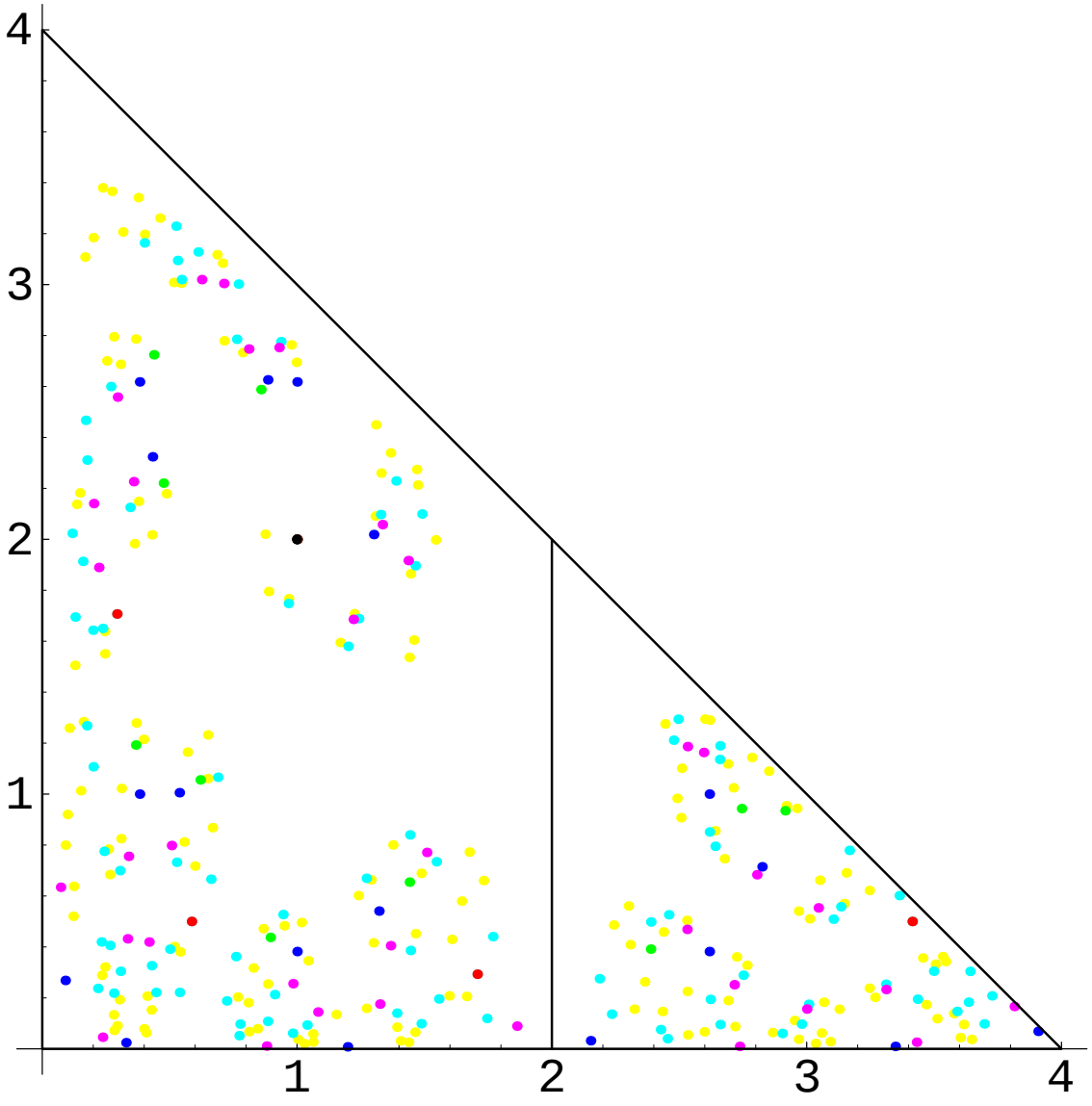
Interior points with period $n \leq 7$



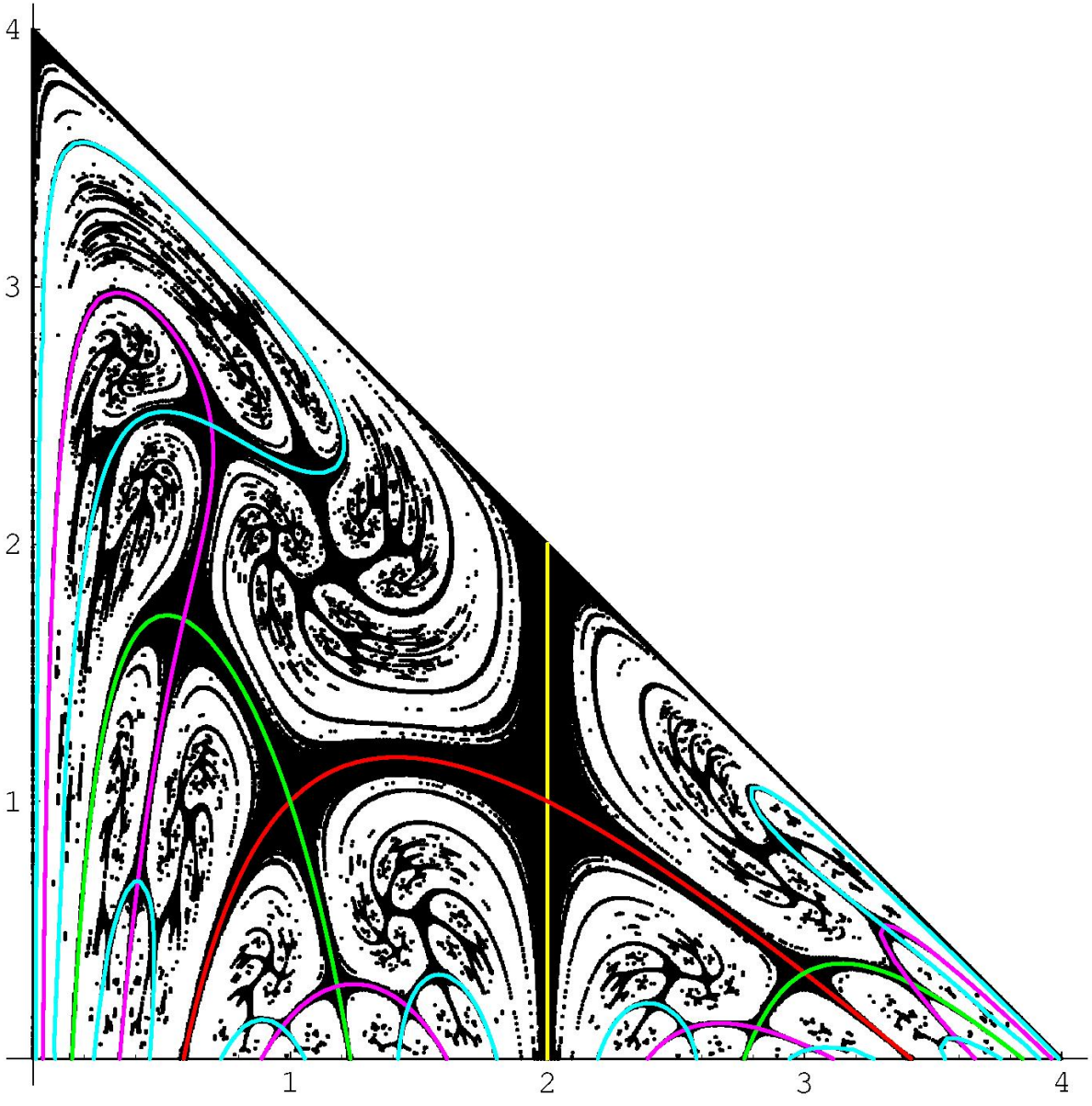
Interior points with period $n \leq 8$



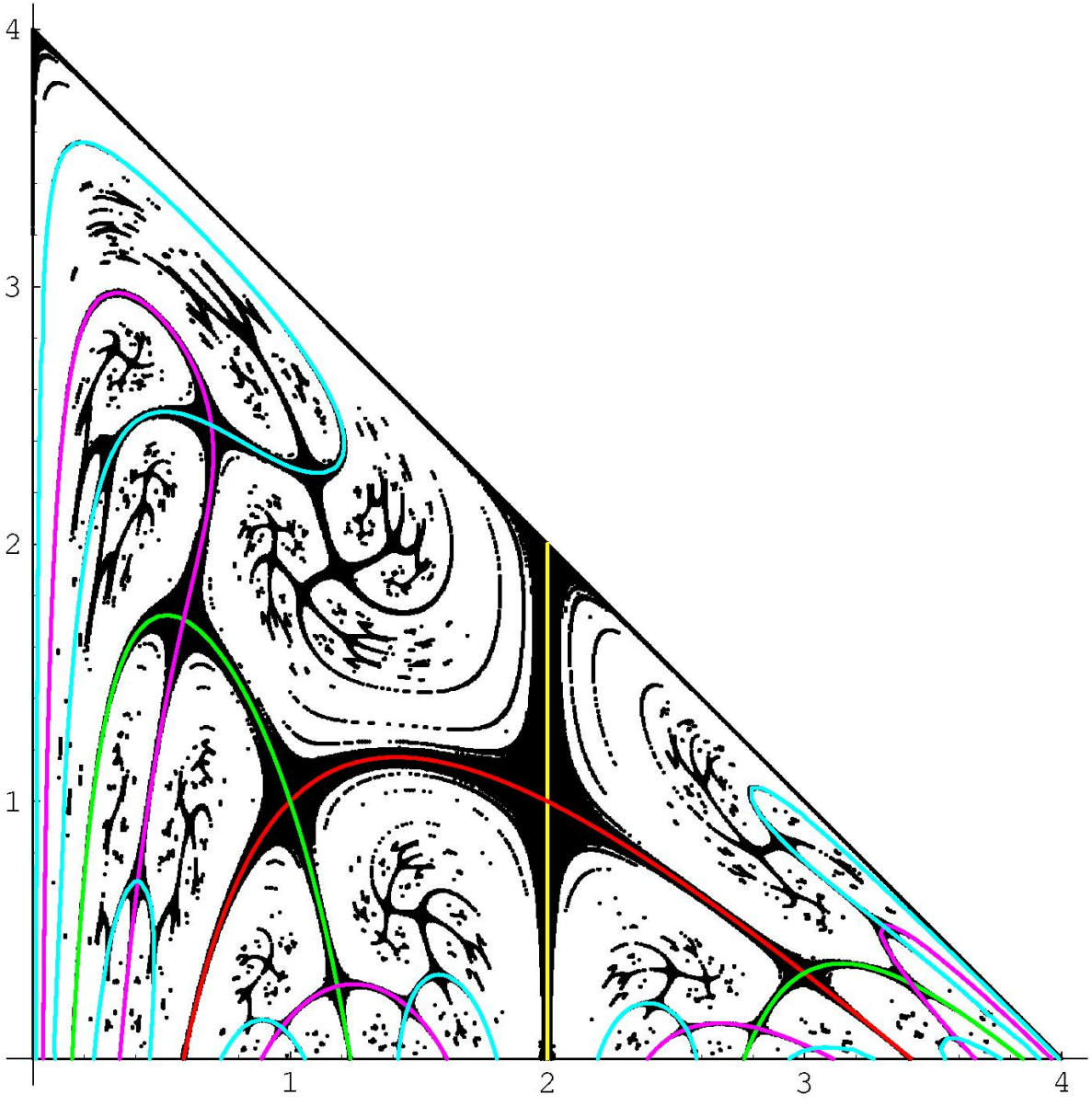
Interior points with period $n \leq 9$



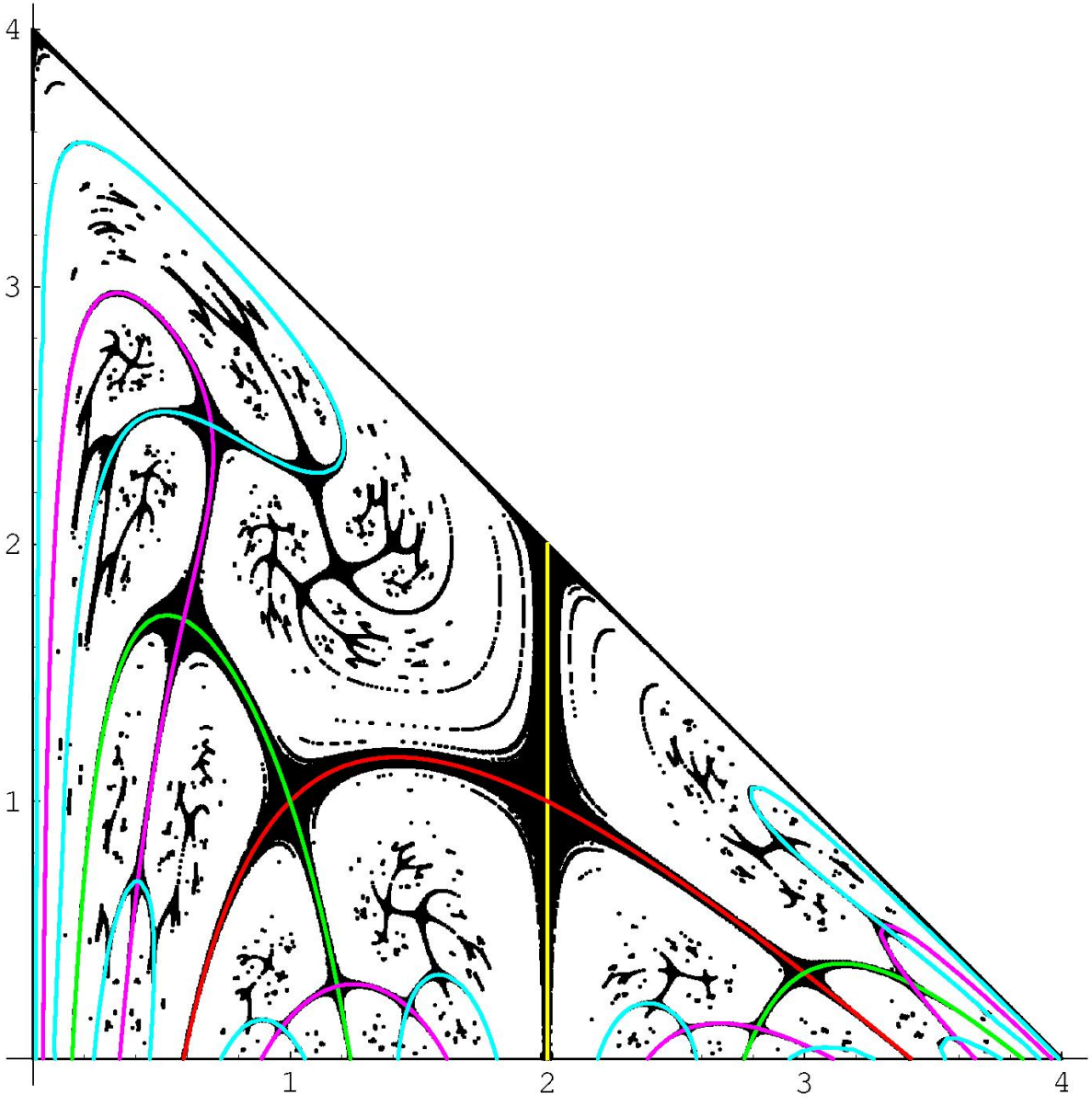
Interior points with period $n \leq 25$



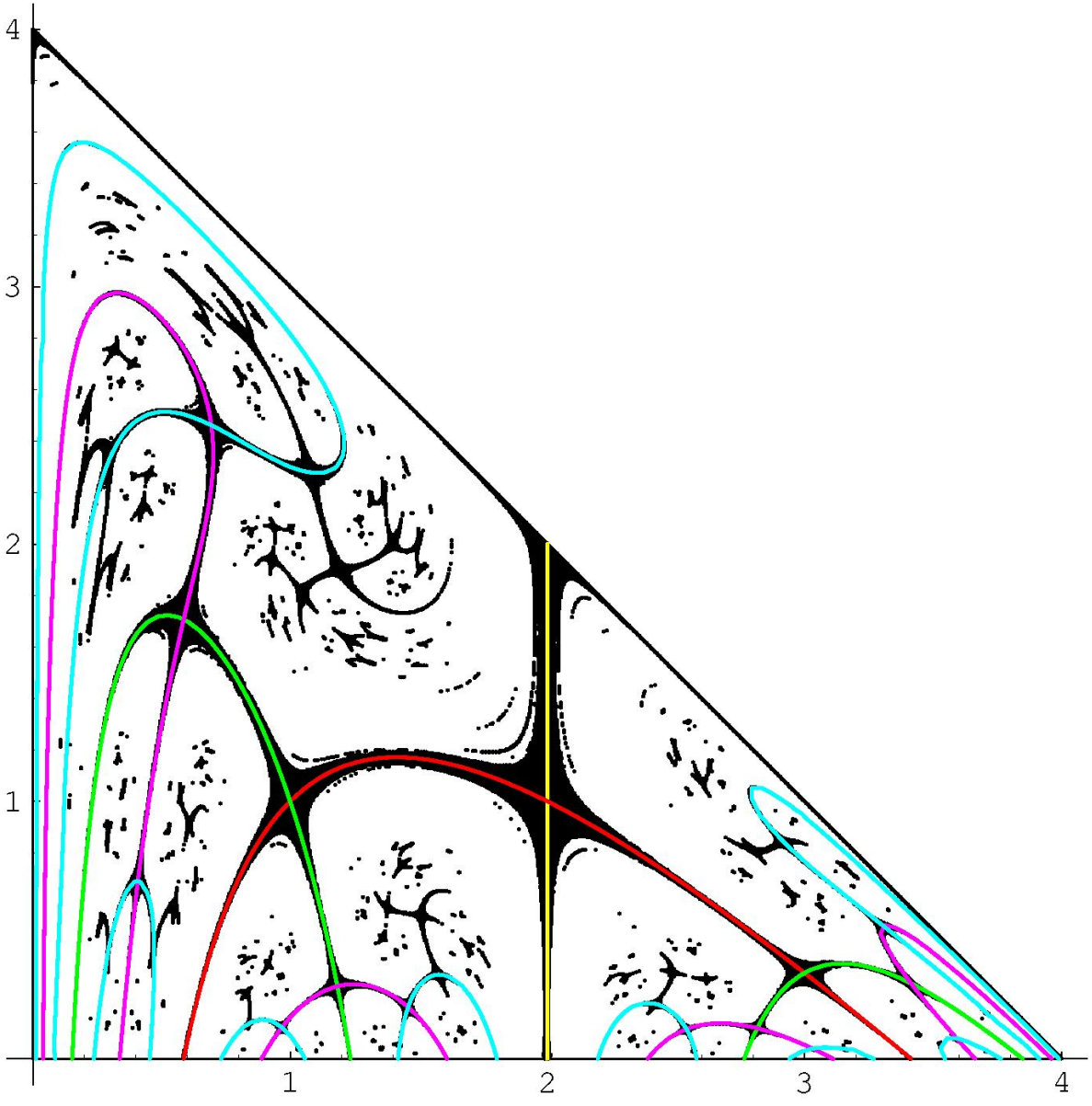
Interior points with period $n \leq 30$



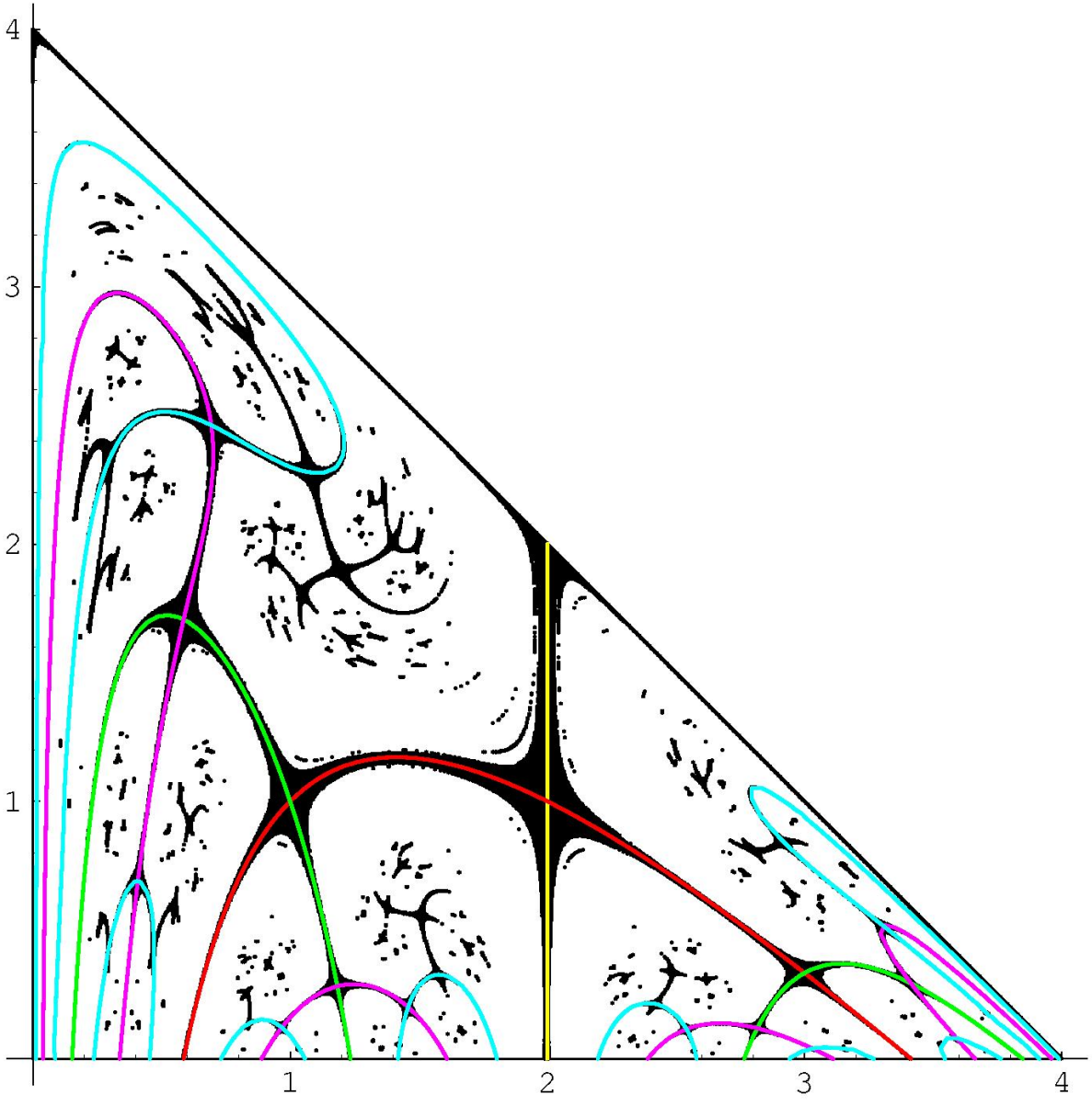
Interior points with period $n \leq 32$



Interior points with period $n \leq 35$



Interior points with period $n \leq 36$

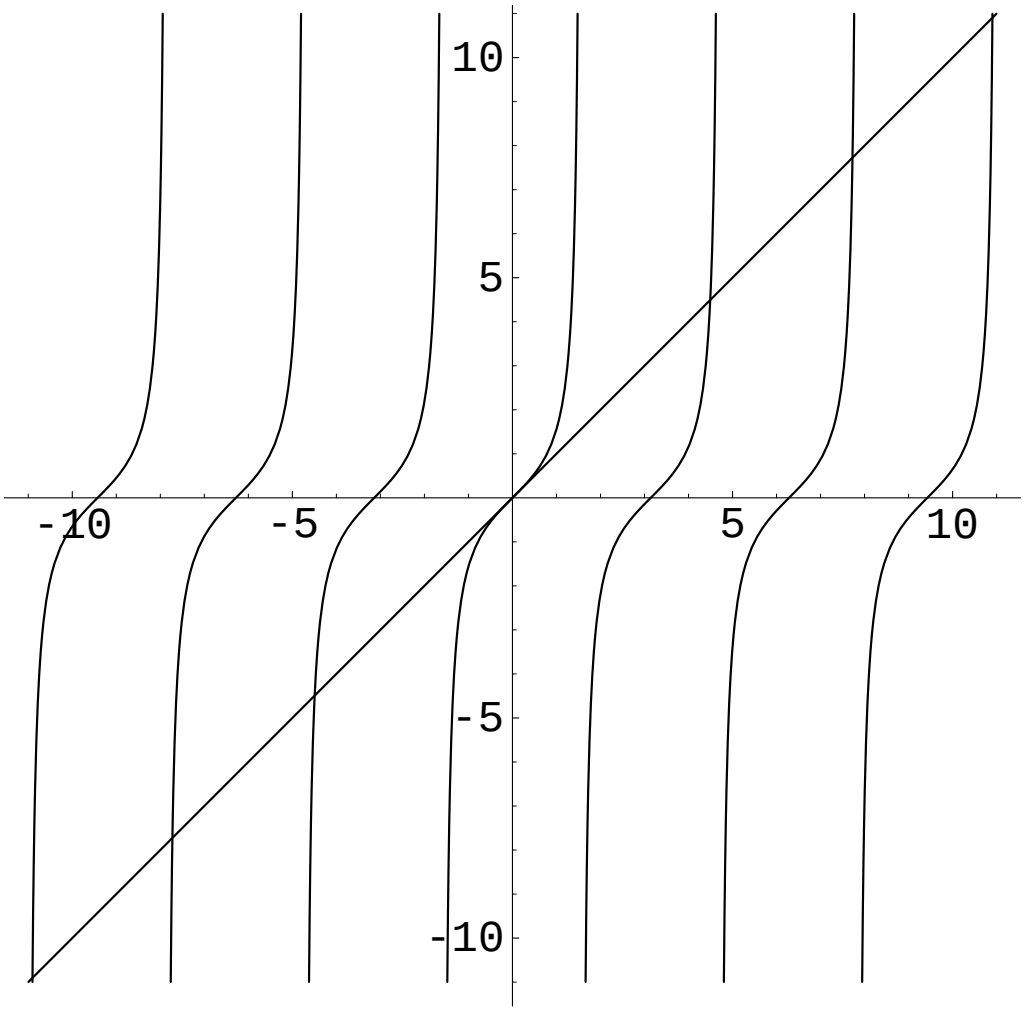


Attracting versus repulsive fixed points

If $x_0 = f(x_0)$ and $|f'(x_0)| < 1$ then

$$x_0 = \lim_{k \to \infty} x_k$$

where $x_k = f(x_{k-1})$ and x_1 is arbitrary but sufficiently closed to x_0.

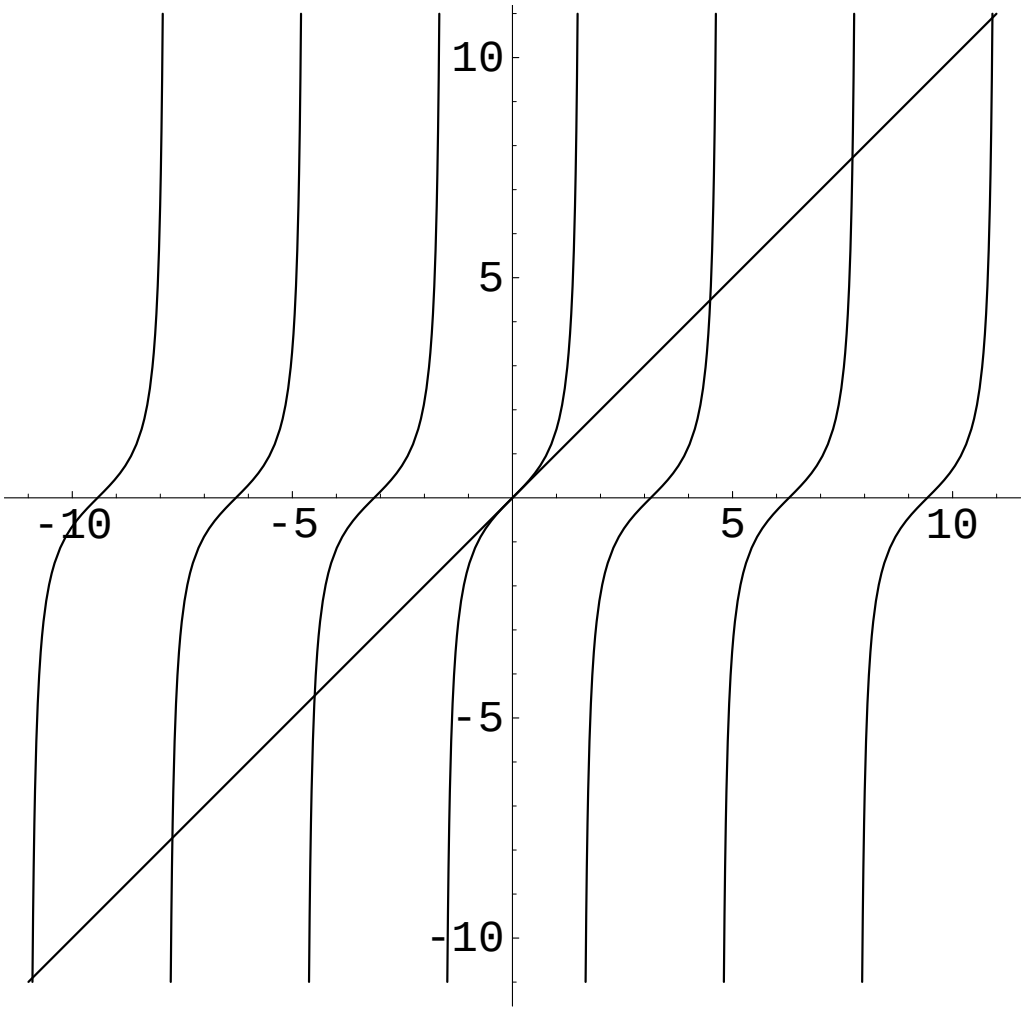


Attracting versus repulsive fixed points

If $x_0 = f(x_0)$ and $|f'(x_0)| < 1$ then

$$x_0 = \lim_{k \to \infty} x_k$$

where $x_k = f(x_{k-1})$ and x_1 is arbitrary but sufficiently closed to x_0.



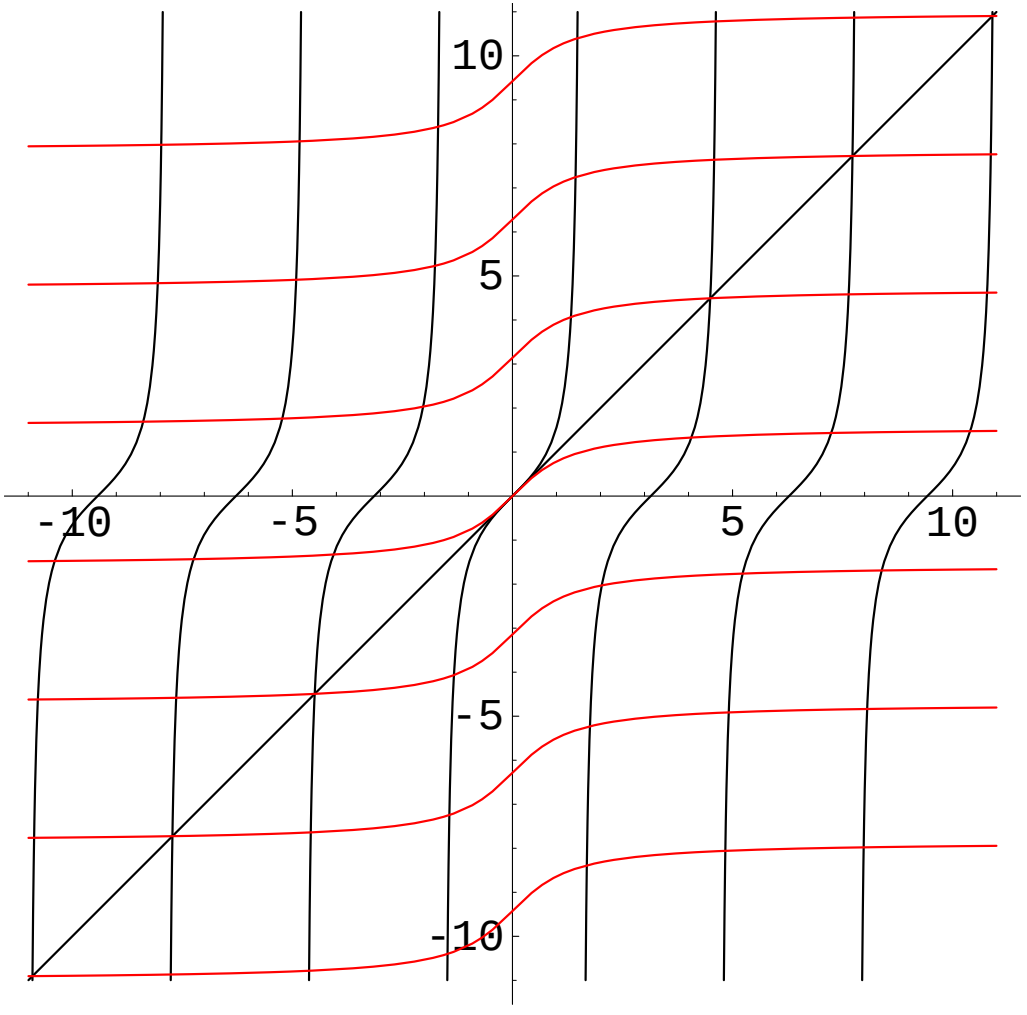
Attracting versus repulsive fixed points

The equation

$$x = \tan x$$

is equivalent to

$$x = k\pi + \arctan x\,, \text{ where } k \in \mathbb{Z}.$$



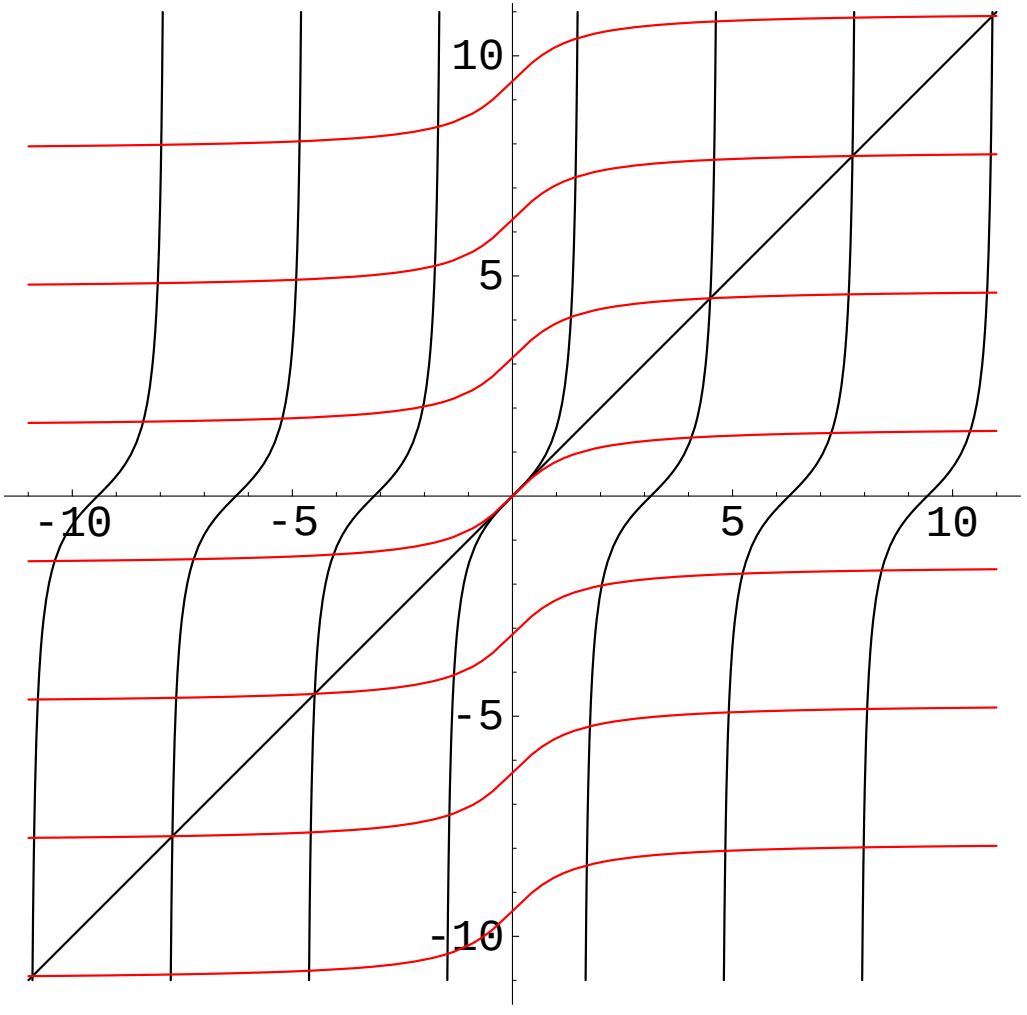
Attracting versus repulsive fixed points

The equation

$$x = \tan x$$

is equivalent to

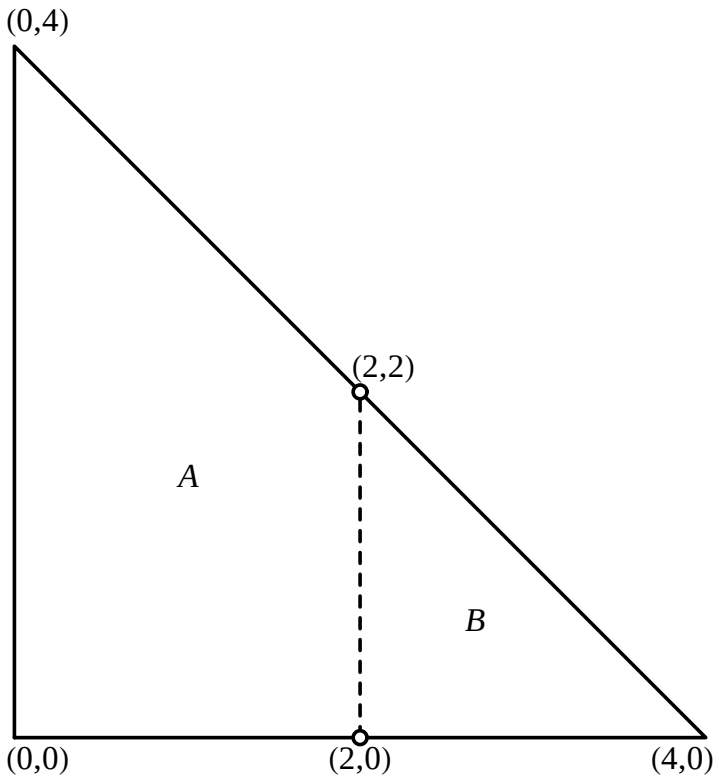
$$x = k\pi + \arctan x\,, \text{ where } k \in \mathbb{Z}.$$



Relationship between lower and interior periodic points

Theorem (Main result)

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.



Itinerary

For a fixed point P of the map F^n it is sufficient to consider its itinerary W as a sequence $(w_i)_{i=0}^{n-1}$ defined by

$$w_i = \begin{cases} a & \text{if } F^i(P) \in A\,, \\ b & \text{if } F^i(P) \in B\,. \end{cases}$$

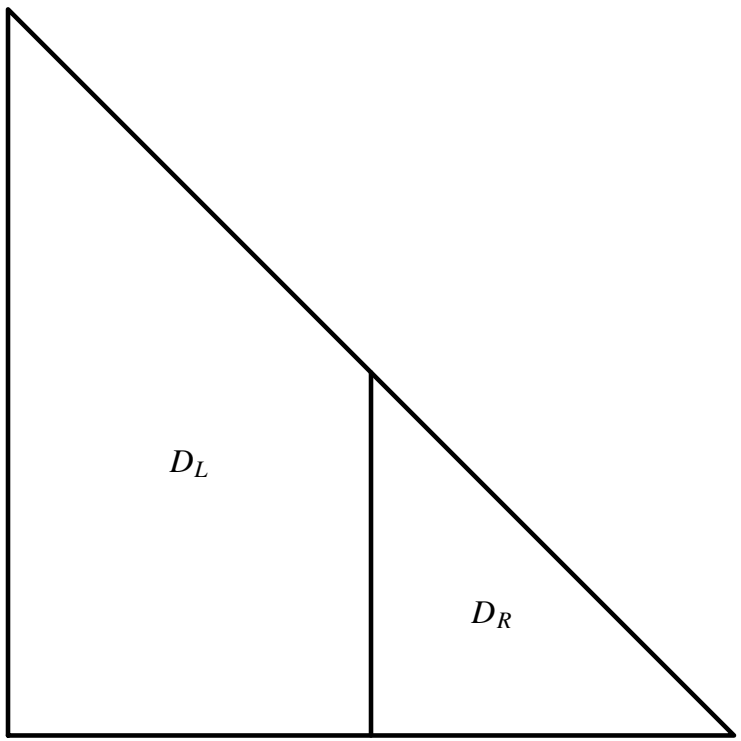
Such a sequence we will write in a shorten form

$$W = a^{j_1} b^{k_1} \dots a^{j_m} b^{k_m}\,.$$

Notation

It is natural to express the triangle D as the union

$$D = D_L \cup D_R \ ,$$



Notation

It is natural to express the triangle D as the union

$$D = D_L \cup D_R \ ,$$

where

$$D_L = \{\, [x, y] \in D : x \leq 2\} \ \text{ and}$$
$$D_R = \{\, [x, y] \in D : x \geq 2\} \ ,$$

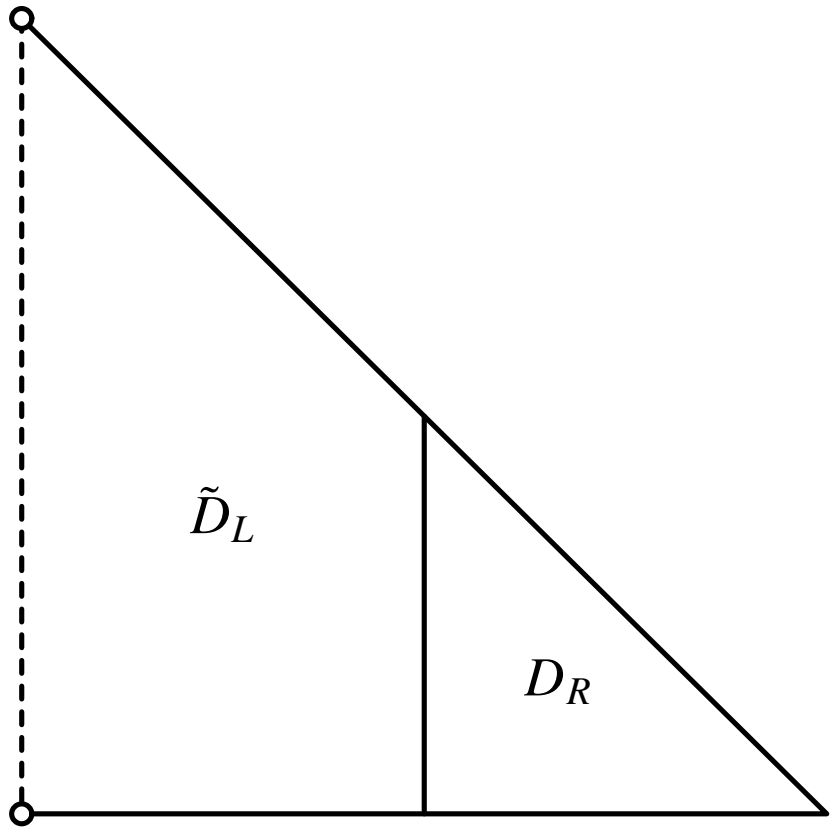
because

$$F(D_L) = D = F(D_R) \ .$$

Notation

Put also

$$\begin{aligned} \widetilde{D}_L &= \{\,[x,\,y] \in D : 0 < x \leq 2\} \text{ and} \\ \widetilde{D} &= D \setminus \{[0,0]\}. \end{aligned}$$



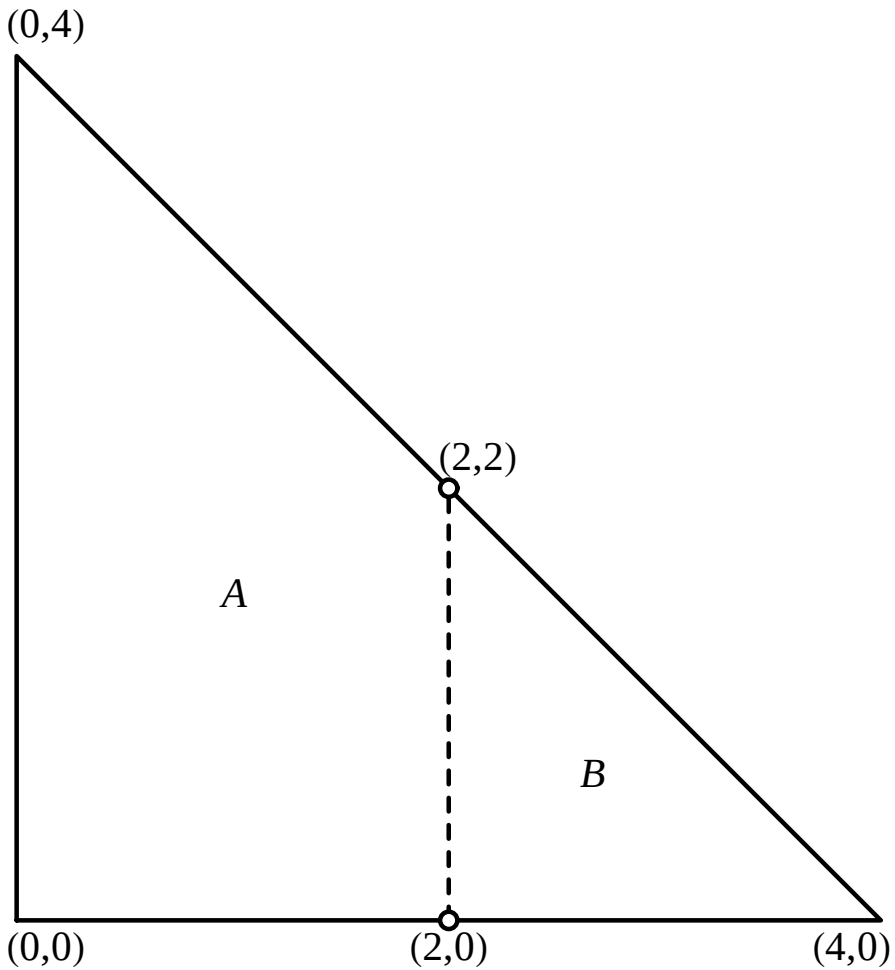
Inverse maps

The map F is not invertible, but F restricted to $\widetilde{D}_L$ and D_R is. The inverse maps of these restrictions are given by

$$L : \widetilde{D} \to \widetilde{D}_L\,, \quad [x,\, y] \mapsto \left[2 - \sqrt{4 - x - y},\ \frac{y}{2-\sqrt{4-x-y}}\right]$$

$$R : D \to D_R, \quad [x,\, y] \mapsto \left[2 + \sqrt{4 - x - y},\ \frac{y}{2+\sqrt{4-x-y}}\right]$$

Partition



Lower fixed point of F^n

Note that $F : [x, 0] \mapsto [f(x), 0]$, where
$f : \langle 0, 4\rangle \to \langle 0, 4\rangle$, $f(x) = x(4 - x)$ is the logistic map, which is conjugated with the tent map
$T : \langle 0, 1\rangle \to \langle 0, 1\rangle$, $T(t) = 1 - |1 - 2t|$

Lower fixed point of F^n

Note that $F : [x, 0] \mapsto [f(x), 0]$, where
$f : \langle 0, 4\rangle \to \langle 0, 4\rangle,\ f(x) = x(4 - x)$ is the logistic map, which is conjugated with the tent map
$T : \langle 0, 1\rangle \to \langle 0, 1\rangle\ , T(t) = 1 - |1 - 2t|$ via the conjugation
$h : \langle 0, 1\rangle \to \langle 0, 4\rangle,\ h(t) = 4\sin^2(\pi t/2)$.

Lower fixed point of F^n

Note that $F : [x, 0] \mapsto [f(x), 0]$, where
$f : \langle 0, 4\rangle \to \langle 0, 4\rangle$, $f(x) = x(4 - x)$ is the logistic map, which is conjugated with the tent map
$T : \langle 0, 1\rangle \to \langle 0, 1\rangle$, $T(t) = 1 - |1 - 2t|$ via the conjugation
$h : \langle 0, 1\rangle \to \langle 0, 4\rangle$, $h(t) = 4\sin^2(\pi t/2)$. Since any fixed point of the map T^n is of the form $2k/(2^n \pm 1)$,

Lower fixed point of F^n

Note that $F : [x, 0] \mapsto [f(x), 0]$, where
$f : \langle 0, 4\rangle \to \langle 0, 4\rangle$, $f(x) = x(4 - x)$ is the logistic map, which is conjugated with the tent map
$T : \langle 0, 1\rangle \to \langle 0, 1\rangle$, $T(t) = 1 - |1 - 2t|$ via the conjugation
$h : \langle 0, 1\rangle \to \langle 0, 4\rangle$, $h(t) = 4\sin^2(\pi t/2)$. Since any fixed point of the map T^n is of the form $2k/(2^n \pm 1)$, any lower fixed point of the map F^n is of the form $\left[4\sin^2 \frac{k\pi}{2^n \pm 1}, 0\right]$,

Lower fixed point of F^n

Note that $F : [x, 0] \mapsto [f(x), 0]$, where
$f : \langle 0, 4\rangle \to \langle 0, 4\rangle,\ f(x) = x(4 - x)$ is the logistic map, which is conjugated with the tent map
$T : \langle 0, 1\rangle \to \langle 0, 1\rangle\ , T(t) = 1 - |1 - 2t|$ via the conjugation
$h : \langle 0, 1\rangle \to \langle 0, 4\rangle,\ h(t) = 4\sin^2(\pi t/2)$. Since any fixed point of the map T^n is of the form $2k/(2^n \pm 1)$, any lower fixed point of the map F^n is of the form $\left[4\sin^2 \frac{k\pi}{2^n \pm 1}, 0\right]$, where n and k are integers such that $0 < n$ and $0 \leq 2k < 2^n \pm 1$.

Lower fixed point of F^n

Note that $F : [x, 0] \mapsto [f(x), 0]$, where
$f : \langle 0, 4\rangle \to \langle 0, 4\rangle$, $f(x) = x(4 - x)$ is the logistic map, which is conjugated with the tent map
$T : \langle 0, 1\rangle \to \langle 0, 1\rangle$, $T(t) = 1 - |1 - 2t|$ via the conjugation
$h : \langle 0, 1\rangle \to \langle 0, 4\rangle$, $h(t) = 4\sin^2(\pi t/2)$. Since any fixed point of the map T^n is of the form $2k/(2^n \pm 1)$, any lower fixed point of the map F^n is of the form $\left[4\sin^2 \frac{k\pi}{2^n \pm 1}, 0\right]$, where n and k are integers such that $0 < n$ and $0 \leq 2k < 2^n \pm 1$.

Jacobi matrix

Let $P = [x_0, 0] \in D$ be a fixed point of the map F^n. In this case $P = \left[4 \sin^2 \frac{k\pi}{2^n \pm 1}, 0\right]$. Then the Jacobi matrix of the map F^n at the point P has a form

$$\begin{pmatrix} \lambda_1 & \mu \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \mp 2^n & \mu \\ 0 & \prod_{i=0}^{n-1} x_i \end{pmatrix},$$

where

$$[x_i, 0] = F^i(P) .$$

Jacobi matrix

Let $P = [x_0, 0] \in D$ be a fixed point of the map F^n. In this case $P = \left[4\sin^2 \frac{k\pi}{2^n \pm 1}, 0\right]$. Then the Jacobi matrix of the map F^n at the point P has a form

$$\begin{pmatrix} \lambda_1 & \mu \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \mp 2^n & \mu \\ 0 & \prod_{i=0}^{n-1} x_i \end{pmatrix},$$

where

$$[x_i, 0] = F^i(P) .$$

Formula for λ_2

Since

$$x_i = 4 \sin^2 \frac{2^i k\pi}{2^n \pm 1} ,$$

we have

$$\lambda_2 = \prod_{i=0}^{n-1} 4 \sin^2 \frac{2^i k\pi}{2^n \pm 1} .$$

Formula for λ_2

Since

$$x_i = 4 \sin^2 \frac{2^i k\pi}{2^n \pm 1} ,$$

we have

$$\lambda_2 = \prod_{i=0}^{n-1} 4 \sin^2 \frac{2^i k\pi}{2^n \pm 1} .$$

Question

Take $n = 60$, sign $-$ and $k = 5124095576030431$.

$$\lambda_2 = ?$$

Classification

For λ_2 we have the possibilities

Saddle point

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1,$

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{17}$

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{17}$

Nonhyperbolic point

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$,

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{15}$

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$, e.g. $x_0 = 4 \sin^2 \frac{\pi}{15}$

Repulsive point

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{15}$

Repulsive point

$1 < \lambda_2$,

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{15}$

Repulsive point

$1 < \lambda_2$, e.g. $x_0 = 4\sin^2 \frac{3\pi}{17}$

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{15}$

Repulsive point

$1 < \lambda_2$, e.g. $x_0 = 4\sin^2 \frac{3\pi}{17}$

Remark

All above points $[x_0, 0]$ have period 4.

Classification

For λ_2 we have the possibilities

Saddle point

$0 \leq \lambda_2 < 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{17}$

Nonhyperbolic point

$\lambda_2 = 1$, e.g. $x_0 = 4\sin^2 \frac{\pi}{15}$

Repulsive point

$1 < \lambda_2$, e.g. $x_0 = 4\sin^2 \frac{3\pi}{17}$

Remark

All above points $[x_0, 0]$ have period 4.

Classification

Saddle point

Lower periodic points with period n and $0 < \lambda_2 < 1$ appear for all $n \geq 4$.

Classification

Saddle point

Lower periodic points with period n and $0 < \lambda_2 < 1$ appear for all $n \geq 4$.

Nonhyperbolic point

Classification

Saddle point

Lower periodic points with period n and $0 < \lambda_2 < 1$ appear for all $n \geq 4$.

Nonhyperbolic point

Lower periodic points with period n and $\lambda_2 = 1$ appear for infinitely many n, e.g. $n = 4 \cdot 3^i \cdot 5^j$, where $i \geq 0$, $j \geq 0$.

Classification

Saddle point

Lower periodic points with period n and $0 < \lambda_2 < 1$ appear for all $n \geq 4$.

Nonhyperbolic point

Lower periodic points with period n and $\lambda_2 = 1$ appear for infinitely many n, e.g. $n = 4 \cdot 3^i \cdot 5^j$, where $i \geq 0$, $j \geq 0$.

Repulsive point

Classification

Saddle point

Lower periodic points with period n and $0 < \lambda_2 < 1$ appear for all $n \geq 4$.

Nonhyperbolic point

Lower periodic points with period n and $\lambda_2 = 1$ appear for infinitely many n, e.g. $n = 4 \cdot 3^i \cdot 5^j$, where $i \geq 0$, $j \geq 0$.

Repulsive point

Lower periodic points with period n and $1 < \lambda_2$ appear for all $n \geq 1$.

Classification

Saddle point

Lower periodic points with period n and $0 < \lambda_2 < 1$ appear for all $n \geq 4$.

Nonhyperbolic point

Lower periodic points with period n and $\lambda_2 = 1$ appear for infinitely many n, e.g. $n = 4 \cdot 3^i \cdot 5^j$, where $i \geq 0$, $j \geq 0$.

Repulsive point

Lower periodic points with period n and $1 < \lambda_2$ appear for all $n \geq 1$.

Main result

Theorem

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.

Explicit examples

Theorem

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.

Example

Explicit examples

Theorem

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.

Example

(i) If $P = [0, 0]$ then $Q = [1, 2]$ and $W = a$.

Explicit examples

Theorem

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.

Example

(i) If $P = [0, 0]$ then $Q = [1, 2]$ and $W = a$.

(ii) If $P = \left[4 \sin^2 \frac{\pi}{17}, 0\right]$ then $Q = \left[1 - \frac{\sqrt{2}}{2}, 1 + \frac{\sqrt{2}}{2}\right]$ and $W = a^3 b$.

Explicit examples

Theorem

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.

Example

(i) If $P = [0, 0]$ then $Q = [1, 2]$ and $W = a$.

(ii) If $P = \left[4\sin^2 \frac{\pi}{17}, 0\right]$ then $Q = \left[1 - \frac{\sqrt{2}}{2}, 1 + \frac{\sqrt{2}}{2}\right]$ and $W = a^3 b$.

(iii) If $P = \left[4\sin^2 \frac{\pi}{63}, 0\right]$ then $Q = \left[1, \frac{3+\sqrt{5}}{2}\right]$ and $W = a^4 b^2$.

Explicit examples

Theorem

Let P be a lower saddle fixed point of the map F^n. Then there is an interior fixed point Q of F^n with the same itinerary.

Example

(i) If $P = [0, 0]$ then $Q = [1, 2]$ and $W = a$.

(ii) If $P = \left[4\sin^2 \frac{\pi}{17}, 0\right]$ then $Q = \left[1 - \frac{\sqrt{2}}{2}, 1 + \frac{\sqrt{2}}{2}\right]$ and $W = a^3 b$.

(iii) If $P = \left[4\sin^2 \frac{\pi}{63}, 0\right]$ then $Q = \left[1, \frac{3+\sqrt{5}}{2}\right]$ and $W = a^4 b^2$.

Sufficient condition for saddle point

Theorem

Let $P = \left[4\sin^2 \frac{k\pi}{2^n \pm 1}, 0\right]$, *where* n *and* k *are integers such that* $0 < n$ *and*

$$0 \leq k \leq \frac{\sqrt{2}(2^n \pm 1)}{\pi \cdot 2\sqrt{2n+1/4}} .$$

Then P *is a saddle fixed point of* F^n.

Notation

Let $\mathrm{IntFix}(F^n)$ be the set of all interior fixed points of the map F^n and $\mathrm{IntPer}(F, n)$ be the set all interior n-periodic of the map F.

Notation

Let $\mathrm{IntFix}(F^n)$ be the set of all interior fixed points of the map F^n and $\mathrm{IntPer}(F, n)$ be the set all interior n-periodic of the map F.

Estimates

Corollary

For cardinalities of $\mathrm{IntFix}(F^n)$ *and* $\mathrm{IntPer}(F, n)$ *we have the estimates*

1. $\#\,\mathrm{IntFix}(F^n) \geq \frac{2\sqrt{2}}{\pi} \cdot 2^{n-\sqrt{2n+1/4}}$

Estimates

Corollary

For cardinalities of $\mathrm{IntFix}(F^n)$ *and* $\mathrm{IntPer}(F, n)$ *we have the estimates*

1. $\#\,\mathrm{IntFix}(F^n) \geq \frac{2\sqrt{2}}{\pi} \cdot 2^{n-\sqrt{2n+1/4}}$
2. $\#\,\mathrm{IntPer}(F, n) \geq \frac{2\sqrt{2}}{\pi} \left(2^{n-\sqrt{2n+1/4}} - 2^{1+\frac{n}{2}}\right)$

Estimates

Corollary

For cardinalities of $\mathrm{IntFix}(F^n)$ *and* $\mathrm{IntPer}(F, n)$ *we have the estimates*

1. $\#\,\mathrm{IntFix}(F^n) \geq \frac{2\sqrt{2}}{\pi} \cdot 2^{n-\sqrt{2n+1/4}}$
2. $\#\,\mathrm{IntPer}(F, n) \geq \frac{2\sqrt{2}}{\pi} \left(2^{n-\sqrt{2n+1/4}} - 2^{1+\frac{n}{2}}\right)$
3. $\#\,\mathrm{IntPer}(F, n) \geq (2-\varepsilon)^n$
   for $0 < \varepsilon < 1$ *and sufficiently large* n.

Estimates

Corollary

For cardinalities of $\mathrm{IntFix}(F^n)$ *and* $\mathrm{IntPer}(F, n)$ *we have the estimates*

1. $\#\,\mathrm{IntFix}(F^n) \geq \frac{2\sqrt{2}}{\pi} \cdot 2^{n-\sqrt{2n+1/4}}$
2. $\#\,\mathrm{IntPer}(F, n) \geq \frac{2\sqrt{2}}{\pi} \left(2^{n-\sqrt{2n+1/4}} - 2^{1+\frac{n}{2}}\right)$
3. $\#\,\mathrm{IntPer}(F, n) \geq (2-\varepsilon)^n$
   for $0 < \varepsilon < 1$ *and sufficiently large* n.

Hypotheses

Hypothesis 1

If $P \in D$ is a lower repulsive (nonhyperbolic) fixed point of F^n, then there is no interior fixed point of F^n with the same itinerary.

Hypothesis 2

If $P \in D$ is a lower saddle fixed point of F^n, then there is a unique interior fixed point of F^n with the same itinerary.

Hypotheses

Hypothesis 1

If $P \in D$ is a lower repulsive (nonhyperbolic) fixed point of F^n, then there is no interior fixed point of F^n with the same itinerary.

Hypothesis 2

If $P \in D$ is a lower saddle fixed point of F^n, then there is a unique interior fixed point of F^n with the same itinerary.

Hypothesis 3

$$\liminf_{n->\infty} \frac{\#\,\mathrm{IntFix}(F^n)}{2^n} > 0\,.$$

Hypotheses

Hypothesis 1

If $P \in D$ is a lower repulsive (nonhyperbolic) fixed point of F^n, then there is no interior fixed point of F^n with the same itinerary.

Hypothesis 2

If $P \in D$ is a lower saddle fixed point of F^n, then there is a unique interior fixed point of F^n with the same itinerary.

Hypothesis 3

$$\liminf_{n->\infty} \frac{\#\,\mathrm{IntFix}(F^n)}{2^n} > 0\,.$$

Nonexistence

Theorem

Let $W = a^{j_1} b^{k_1} \cdots a^{j_m} b^{k_m}$ *be an itinerary such that* $j_i > 0$, $k_i > 0$ *and* $\sum_{i=1}^{m} (j_i + k_i) = n$. *If*

$$\sum_{i=1}^{m} k_i \geq \sum_{i=1}^{m} j_i^2 \,,$$

then there is no interior fixed point of the map F^n *with the itinerary* W.

Nonexistence

Theorem

Let $W = a^{j_1} b^{k_1} \cdots a^{j_m} b^{k_m}$ *be an itinerary such that* $j_i > 0$, $k_i > 0$ *and* $\sum_{i=1}^{m} (j_i + k_i) = n$. *If*

$$\sum_{i=1}^{m} k_i \geq \sum_{i=1}^{m} j_i^2 \,,$$

then there is no interior fixed point of the map F^n *with the itinerary* W.

Theorem

Let $W = a^{j_1} b^{k_1} \cdots a^{j_m} b^{k_m}$ *be an itinerary such that* $j_i > 0$, $k_i > 0$ *and* $\sum_{i=1}^{m} (j_i + k_i) = n$.

(i) *If*

$$\sum_{i=1}^{m} k_i \geq \frac{\ln 2}{\ln 3} \sum_{i=1}^{m} j_i^2 - \frac{\ln(4 - 2\sqrt{2})}{\ln 3} \sum_{i=1}^{m} j_i + m \,,$$

then there is no interior fixed point of the map F^n *with the itinerary* W.

Theorem

Let $W = a^{j_1} b^{k_1} \cdots a^{j_m} b^{k_m}$ *be an itinerary such that* $j_i > 0$, $k_i > 0$ *and* $\sum_{i=1}^{m} (j_i + k_i) = n$.

(i) *If*

$$\sum_{i=1}^{m} k_i \geq \frac{\ln 2}{\ln 3} \sum_{i=1}^{m} j_i^2 - \frac{\ln(4 - 2\sqrt{2})}{\ln 3} \sum_{i=1}^{m} j_i + m \,,$$

then there is no interior fixed point of the map F^n *with the itinerary* W.

(ii) *If*

$$\sum_{i=1}^{m} k_i \leq \frac{\ln 2}{\ln 3} \sum_{i=1}^{m} j_i^2 - \frac{\ln \frac{\pi^2}{2}}{\ln 3} \sum_{i=1}^{m} j_i - \frac{\ln \frac{32}{3\pi^2}}{\ln 3} m \,,$$

then there exists an interior fixed point of the map F^n *with the itinerary* W.

Theorem

Let $W = a^{j_1} b^{k_1} \cdots a^{j_m} b^{k_m}$ *be an itinerary such that* $j_i > 0$, $k_i > 0$ *and* $\sum_{i=1}^{m} (j_i + k_i) = n$.

(i) *If*

$$\sum_{i=1}^{m} k_i \geq \frac{\ln 2}{\ln 3} \sum_{i=1}^{m} j_i^2 - \frac{\ln(4 - 2\sqrt{2})}{\ln 3} \sum_{i=1}^{m} j_i + m \,,$$

then there is no interior fixed point of the map F^n *with the itinerary* W.

(ii) *If*

$$\sum_{i=1}^{m} k_i \leq \frac{\ln 2}{\ln 3} \sum_{i=1}^{m} j_i^2 - \frac{\ln \frac{\pi^2}{2}}{\ln 3} \sum_{i=1}^{m} j_i - \frac{\ln \frac{32}{3\pi^2}}{\ln 3} m \,,$$

then there exists an interior fixed point of the map F^n *with the itinerary* W.

Motivation

Take $x_0 = 4\sin^2 \frac{\pi}{55} = 4\sin^2 \frac{19605\pi}{2^{20}-1}$.

Motivation

Take $x_0 = 4\sin^2 \frac{\pi}{55} = 4\sin^2 \frac{19605\pi}{2^{20}-1}$.

The period of $[x_0, 0]$ is 20.

Motivation

Take $x_0 = 4\sin^2\frac{\pi}{55} = 4\sin^2\frac{19605\pi}{2^{20}-1}$.
The period of $[x_0, 0]$ is 20.
Fixe an odd integer m.

Motivation

Take $x_0 = 4\sin^2\frac{\pi}{55} = 4\sin^2\frac{19605\pi}{2^{20}-1}$.
The period of $[x_0, 0]$ is 20.
Fix an odd integer m.
Let A_m be the set of all points of the form $4\sin^2\frac{k\pi}{m}$, where $k \leq \frac{m-1}{2}$ is coprime to m.

Motivation

Take $x_0 = 4\sin^2\frac{\pi}{55} = 4\sin^2\frac{19605\pi}{2^{20}-1}$.
The period of $[x_0, 0]$ is 20.
Fix an odd integer m.
Let A_m be the set of all points of the form $4\sin^2\frac{k\pi}{m}$, where $k \leq \frac{m-1}{2}$ is coprime to m.
All these points are periodic with the same period.

Motivation

Take $x_0 = 4\sin^2\frac{\pi}{55} = 4\sin^2\frac{19605\pi}{2^{20}-1}$.
The period of $[x_0, 0]$ is 20.
Fix an odd integer m.
Let A_m be the set of all points of the form $4\sin^2\frac{k\pi}{m}$, where $k \leq \frac{m-1}{2}$ is coprime to m.
All these points are periodic with the same period.

Main formula

Since

$$\prod_{k=1}^{m-1} \sin \frac{k\pi}{m} = \frac{m}{2^{m-1}}$$

we obtain

$$\prod_{k=1}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m} = \prod_{k=1}^{m-1} 2 \sin \frac{k\pi}{m} = m\,.$$

Main formula

Since

$$\prod_{k=1}^{m-1} \sin \frac{k\pi}{m} = \frac{m}{2^{m-1}}$$

we obtain

$$\prod_{k=1}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m} = \prod_{k=1}^{m-1} 2 \sin \frac{k\pi}{m} = m\,.$$

We are interested in

$$\prod_{\substack{k=1 \\ \mathrm{GCD}(k,m)=1}}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m}$$

Main formula

Since

$$\prod_{k=1}^{m-1} \sin \frac{k\pi}{m} = \frac{m}{2^{m-1}}$$

we obtain

$$\prod_{k=1}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m} = \prod_{k=1}^{m-1} 2 \sin \frac{k\pi}{m} = m\,.$$

We are interested in

$$\prod_{\substack{k=1 \\ \mathrm{GCD}(k,m)=1}}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m} = \begin{cases} p \text{ if } m = p^i\,, \text{ where } p \text{ is prime} \\ 1 \text{ otherwise} \end{cases}$$

Main formula

Since

$$\prod_{k=1}^{m-1} \sin \frac{k\pi}{m} = \frac{m}{2^{m-1}}$$

we obtain

$$\prod_{k=1}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m} = \prod_{k=1}^{m-1} 2 \sin \frac{k\pi}{m} = m\,.$$

We are interested in

$$\prod_{\substack{k=1 \\ \mathrm{GCD}(k,m)=1}}^{\frac{m-1}{2}} 4 \sin^2 \frac{k\pi}{m} = \begin{cases} p \text{ if } m = p^i\,, \text{ where } p \text{ is prime} \\ 1 \text{ otherwise} \end{cases}$$

Case $m = p^i$, where p is prime

Let $m = p^i$, where p is a prime.

If A_m is an orbit then corresponding $\lambda_2 = p > 1$.

Case $m = p^i$, where p is prime

Let $m = p^i$, where p is a prime.
If A_m is an orbit then corresponding $\lambda_2 = p > 1$. So, this orbit is repelling.

Case $m = p^i$, where p is prime

Let $m = p^i$, where p is a prime.
If A_m is an orbit then corresponding $\lambda_2 = p > 1$. So, this orbit is repelling.
If A_m contains at least two orbits then $\lambda_2 < 1$ appears for some orbit.

Case $m = p^i$, where p is prime

Let $m = p^i$, where p is a prime.
If A_m is an orbit then corresponding $\lambda_2 = p > 1$. So, this orbit is repelling.
If A_m contains at least two orbits then $\lambda_2 < 1$ appears for some orbit.

Case $m \neq p^i$

If A_m is an orbit then corresponding $\lambda_2 = 1$.

If A_m contains at least two orbits then one of the following holds

- $\lambda_2 = 1$ for all orbits in A_m.

Case $m \neq p^i$

If A_m is an orbit then corresponding $\lambda_2 = 1$.
If A_m contains at least two orbits then one of the following holds

- $\lambda_2 = 1$ for all orbits in A_m.
- $\lambda_2 \neq 1$ for all orbits in A_m, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.

Case $m \neq p^i$

If A_m is an orbit then corresponding $\lambda_2 = 1$.
If A_m contains at least two orbits then one of the following holds

- $\lambda_2 = 1$ for all orbits in A_m.
- $\lambda_2 \neq 1$ for all orbits in A_m, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.
- $\lambda_2 = 1$, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.

Case $m \neq p^i$

If A_m is an orbit then corresponding $\lambda_2 = 1$.
If A_m contains at least two orbits then one of the following holds

- $\lambda_2 = 1$ for all orbits in A_m.
- $\lambda_2 \neq 1$ for all orbits in A_m, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.
- $\lambda_2 = 1$, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.

Case $m \neq p^i$

If A_m is an orbit then corresponding $\lambda_2 = 1$.
If A_m contains at least two orbits then one of the following holds

- $\lambda_2 = 1$ for all orbits in A_m.
- $\lambda_2 \neq 1$ for all orbits in A_m, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.
- $\lambda_2 = 1$, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.

The last possibility was not observed.

Case $m \neq p^i$

If A_m is an orbit then corresponding $\lambda_2 = 1$.
If A_m contains at least two orbits then one of the following holds

- $\lambda_2 = 1$ for all orbits in A_m.
- $\lambda_2 \neq 1$ for all orbits in A_m, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.
- $\lambda_2 = 1$, $\lambda_2 < 1$ and $\lambda_2 > 1$ appear for some orbits.

The last possibility was not observed.

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2, m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$.

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2, m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2, m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\operatorname{ord}(2, m) = \#G(2, m)$.

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that

$$\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$$

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that $\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$ for $m = p_1^{i_1} \cdot p_2^{i_2} \ldots \cdot p_s^{i_s}$.

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that $\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$ for $m = p_1^{i_1} \cdot p_2^{i_2} \ldots \cdot p_s^{i_s}$. The period of the point $4\sin^2 \frac{k\pi}{m}$ is

$$\frac{\mathrm{ord}(2,m)}{2} \text{ if } -1 \in G(2,m)$$

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that $\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$ for $m = p_1^{i_1} \cdot p_2^{i_2} \ldots \cdot p_s^{i_s}$. The period of the point $4\sin^2 \frac{k\pi}{m}$ is

$$\frac{\mathrm{ord}(2,m)}{2} \text{ if } -1 \in G(2,m)$$

and

$$\mathrm{ord}(2,m) \text{ otherwise } .$$

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that $\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$ for $m = p_1^{i_1} \cdot p_2^{i_2} \ldots \cdot p_s^{i_s}$. The period of the point $4\sin^2 \frac{k\pi}{m}$ is

$$\frac{\mathrm{ord}(2,m)}{2} \text{ if } -1 \in G(2,m)$$

and

$$\mathrm{ord}(2,m) \text{ otherwise } .$$

Moreover $-1 \in G(2,m)$

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that $\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$ for $m = p_1^{i_1} \cdot p_2^{i_2} \ldots \cdot p_s^{i_s}$. The period of the point $4\sin^2 \frac{k\pi}{m}$ is

$$\frac{\mathrm{ord}(2,m)}{2} \text{ if } -1 \in G(2,m)$$

and

$$\mathrm{ord}(2,m) \text{ otherwise } .$$

Moreover $-1 \in G(2,m)$ if and only if there is $\alpha > 0$ such that

$$\mathrm{ord}(2,p_j^{i_j}) = 2^\alpha(2u_j+1) \text{ for all } j = 1,\ldots,s\,.$$

The value of period

Let $\mathbb{Z}_m^*$ be the multiplicative group of the ring $\mathbb{Z}_m$ and $G(2,m)$ be the group generated by class of 2 in $\mathbb{Z}_m^*$. Denote by $\varphi(m) = \#\mathbb{Z}_m^*$ and $\mathrm{ord}(2,m) = \#G(2,m)$. Note that $\mathrm{ord}(2,m) = \mathrm{LCM}\left(\mathrm{ord}(2,p_1^{i_2}), \mathrm{ord}(2,p_2^{i_2}), \ldots, \mathrm{ord}(2,p_s^{i_s})\right)$ for $m = p_1^{i_1} \cdot p_2^{i_2} \ldots \cdot p_s^{i_s}$. The period of the point $4\sin^2 \frac{k\pi}{m}$ is

$$\frac{\mathrm{ord}(2,m)}{2} \text{ if } -1 \in G(2,m)$$

and

$$\mathrm{ord}(2,m) \text{ otherwise } .$$

Moreover $-1 \in G(2,m)$ if and only if there is $\alpha > 0$ such that

$$\mathrm{ord}(2,p_j^{i_j}) = 2^{\alpha}(2u_j+1) \text{ for all } j = 1,\ldots,s\,.$$

Number of orbits

The number of orbits in A_m is

$$\frac{\varphi(m)}{\operatorname{ord}(2,m)} \text{ if } -1 \in G(2,m)$$

and

$$\frac{\varphi(m)}{2\operatorname{ord}(2,m)} \text{ otherwise } .$$

Number of orbits

The number of orbits in A_m is

$$\frac{\varphi(m)}{\operatorname{ord}(2,m)} \text{ if } -1 \in G(2,m)$$

and

$$\frac{\varphi(m)}{2\operatorname{ord}(2,m)} \text{ otherwise } .$$

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$,

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$,

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square and 2 generates the group of squares in $\mathbb{Z}^*_{p^i}$.

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square and 2 generates the group of squares in $\mathbb{Z}^*_{p^i}$.
  (This is possible only for $p \equiv -1 \pmod 8$.)

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square and 2 generates the group of squares in $\mathbb{Z}^*_{p^i}$.
  (This is possible only for $p \equiv -1 \pmod 8$.)
  For example for $p = 7, 23, 47$ and any $i \geq 1$,

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square and 2 generates the group of squares in $\mathbb{Z}^*_{p^i}$.
  (This is possible only for $p \equiv -1 \pmod 8$.)
  For example for $p = 7, 23, 47$ and any $i \geq 1$, but not for $p = 31$ and $p = 127$ and any $i \geq 1$.

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square and 2 generates the group of squares in $\mathbb{Z}^*_{p^i}$.
  (This is possible only for $p \equiv -1 \pmod 8$.)
  For example for $p = 7, 23, 47$ and any $i \geq 1$, but not for $p = 31$ and $p = 127$ and any $i \geq 1$.

Particularly for $p \equiv 1 \pmod 8$ the set A_m contains at least two orbits.

Number of orbits for $m = p^i$

Let $m = p^i$, where p is a prime. The set A_m is an orbit if and only if one of the following holds.

- 2 generates the group $\mathbb{Z}^*_{p^i}$
  (This is possible only for $p \equiv \pm 3 \pmod 8$.)
  For example for $p = 3, 5, 11, 13, 19, 29$ and any $i \geq 1$, but not for $p = 43$ and $p = 109$ any $i \geq 1$.
- 2 is a square in $\mathbb{Z}^*_{p^i}$, -1 is not a square and 2 generates the group of squares in $\mathbb{Z}^*_{p^i}$.
  (This is possible only for $p \equiv -1 \pmod 8$.)
  For example for $p = 7, 23, 47$ and any $i \geq 1$, but not for $p = 31$ and $p = 127$ and any $i \geq 1$.

Particularly for $p \equiv 1 \pmod 8$ the set A_m contains at least two orbits.

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.

The set A_m is an orbit if and only if

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,
- either $i = 1$ or $q - 1$ is not divisible by p.

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,
- either $i = 1$ or $q - 1$ is not divisible by p.

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,
- either $i = 1$ or $q - 1$ is not divisible by p.

This is true for $m = 3^i \cdot 5^j, 3 \cdot 7^j, 5^i \cdot 7^j, 3^i \cdot 23^j$,

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,
- either $i = 1$ or $q - 1$ is not divisible by p.

This is true for $m = 3^i \cdot 5^j, 3 \cdot 7^j, 5^i \cdot 7^j, 3^i \cdot 23^j$, but not for $m = 3^i \cdot 7^j$ and $i \geq 2$.

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,
- either $i = 1$ or $q - 1$ is not divisible by p.

This is true for $m = 3^i \cdot 5^j, 3 \cdot 7^j, 5^i \cdot 7^j, 3^i \cdot 23^j$, but not for $m = 3^i \cdot 7^j$ and $i \geq 2$.

Number of orbits for $m \neq p^i$

Let m be divisible by at least two primes.
The set A_m is an orbit if and only if

- $m = p^i q^j$, where $p < q$ are primes and $i, j > 0$,
- the sets A_{p^i} and A_{q^j} are orbits,
- $p \not\equiv q \pmod 8$,
- $\mathrm{GCD}(p-1, q-1) = 2$,
- either $i = 1$ or $q - 1$ is not divisible by p.

This is true for $m = 3^i \cdot 5^j, 3 \cdot 7^j, 5^i \cdot 7^j, 3^i \cdot 23^j$, but not for $m = 3^i \cdot 7^j$ and $i \geq 2$.

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

Let p be a prime, $a \neq 0$ and $i \geq 1$ be integers.

- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

Let p be a prime, $a \neq 0$ and $i \geq 1$ be integers.

- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

Let p be a prime, $a \neq 0$ and $i \geq 1$ be integers.

- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,
- If $(a \mod p^2)$ generates the group $\mathbb{Z}_{p^2}^*$ then $(a \mod p^i)$ generates $\mathbb{Z}_{p^i}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

Let p be a prime, $a \neq 0$ and $i \geq 1$ be integers.

- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,
- If $(a \mod p^2)$ generates the group $\mathbb{Z}_{p^2}^*$ then $(a \mod p^i)$ generates $\mathbb{Z}_{p^i}^*$,
- If $(a \mod p^2)$ generates the group of squares in $\mathbb{Z}_{p^2}^*$ then $(a \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

Let p be a prime, $a \neq 0$ and $i \geq 1$ be integers.

- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(a \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(a \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,
- If $(a \mod p^2)$ generates the group $\mathbb{Z}_{p^2}^*$ then $(a \mod p^i)$ generates $\mathbb{Z}_{p^i}^*$,
- If $(a \mod p^2)$ generates the group of squares in $\mathbb{Z}_{p^2}^*$ then $(a \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,
- If $(2 \mod p^2)$ generates the group $\mathbb{Z}_{p^2}^*$ then $(2 \mod p^i)$ generates $\mathbb{Z}_{p^i}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,
- If $(2 \mod p^2)$ generates the group $\mathbb{Z}_{p^2}^*$ then $(2 \mod p^i)$ generates $\mathbb{Z}_{p^i}^*$,
- If $(2 \mod p^2)$ generates the group of squares in $\mathbb{Z}_{p^2}^*$ then $(2 \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$,

Relations between $\mathbb{Z}_p^*$, $\mathbb{Z}_{p^2}^*$ and $\mathbb{Z}_{p^i}^*$

- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates $\mathbb{Z}_{p^j}^*$,
- If $i > j \geq 1$ and $(2 \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$ then $(2 \mod p^j)$ generates the group of squares in $\mathbb{Z}_{p^j}^*$,
- If $(2 \mod p^2)$ generates the group $\mathbb{Z}_{p^2}^*$ then $(2 \mod p^i)$ generates $\mathbb{Z}_{p^i}^*$,
- If $(2 \mod p^2)$ generates the group of squares in $\mathbb{Z}_{p^2}^*$ then $(2 \mod p^i)$ generates the group of squares in $\mathbb{Z}_{p^i}^*$,

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then $2^{p-1} \equiv 1 \pmod{p^2}$.

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then
$2^{p-1} \equiv 1 \,(\text{mod } p^2)$.

A prime with this property is called a Wieferich prime.

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then
$2^{p-1} \equiv 1 \,(\text{mod}\ \ p^2)$.
A prime with this property is called a Wieferich prime.
There are known only two Wieferich primes $p = 1093$ and 3511.

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then
$2^{p-1} \equiv 1 \,(\mathrm{mod}\ \ p^2)$.
A prime with this property is called a Wieferich prime.
There are known only two Wieferich primes $p = 1093$ and 3511.
The other ones have to be greater than $6.7 \cdot 10^{15}$.

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then
$2^{p-1} \equiv 1 \,(\mathrm{mod}\ \ p^2)$.
A prime with this property is called a Wieferich prime.
There are known only two Wieferich primes $p = 1093$ and 3511.
The other ones have to be greater than $6.7 \cdot 10^{15}$.
However 2 does not generate $\mathbb{Z}_p^*$ for $p = 1093$ and 3511.

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then
$2^{p-1} \equiv 1 \,(\mathrm{mod}\ \ p^2)$.
A prime with this property is called a Wieferich prime.
There are known only two Wieferich primes $p = 1093$ and 3511.
The other ones have to be greater than $6.7 \cdot 10^{15}$.
However 2 does not generate $\mathbb{Z}_p^*$ for $p = 1093$ and 3511.
On the other hand 2 generate the group of squares in $\mathbb{Z}_{3511}^*$ but not in $\mathbb{Z}_{3511^2}^*$.

Wieferich primes

If 2 generates $\mathbb{Z}_p^*$, but not $\mathbb{Z}_{p^2}^*$, then
$2^{p-1} \equiv 1 \,(\mathrm{mod}\ \ p^2)$.
A prime with this property is called a Wieferich prime.
There are known only two Wieferich primes $p = 1093$ and 3511.
The other ones have to be greater than $6.7 \cdot 10^{15}$.
However 2 does not generate $\mathbb{Z}_p^*$ for $p = 1093$ and 3511.
On the other hand 2 generate the group of squares in $\mathbb{Z}_{3511}^*$ but not in $\mathbb{Z}_{3511^2}^*$.

Artin conjecture

The question whether 2 generates $\mathbb{Z}_p^*$ for infinitely primes is a part the Artin conjecture.

It is also interesting whether 2 generates the group of squares in $\mathbb{Z}_p^*$ for infinitely primes of the form $p = 8j - 1$.

Artin conjecture

The question whether 2 generates $\mathbb{Z}_p^*$ for infinitely primes is a part the Artin conjecture.
It is also interesting whether 2 generates the group of squares in $\mathbb{Z}_p^*$ for infinitely primes of the form $p = 8j - 1$.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and $q = 2p + 1$ be the corresponding safe prime.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and $q = 2p + 1$ be the corresponding safe prime. Then A_q is an orbit.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and $q = 2p + 1$ be the corresponding safe prime. Then A_q is an orbit.

Remark

The question whether there are infinitely many Sophie Germain primes is open.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and $q = 2p + 1$ be the corresponding safe prime. Then A_q is an orbit.

Remark

The question whether there are infinitely many Sophie Germain primes is open. Primes
2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233 are Sophie Germaine primes.

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and $q = 2p + 1$ be the corresponding safe prime. Then A_q is an orbit.

Remark

The question whether there are infinitely many Sophie Germain primes is open. Primes
2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233 are Sophie Germaine primes.
The corresponding safe primes are
$5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467.$

Sophie Germaine primes and safe primes

A prime p is said to be Sophie Germaine prime if $q = 2p + 1$ is also prime. In such a case q is called a safe prime.

Theorem

Let p be a Sophie Germain prime and $q = 2p + 1$ be the corresponding safe prime. Then A_q is an orbit.

Remark

The question whether there are infinitely many Sophie Germain primes is open. Primes
2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233
are Sophie Germaine primes.
The corresponding safe primes are
$5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467.$