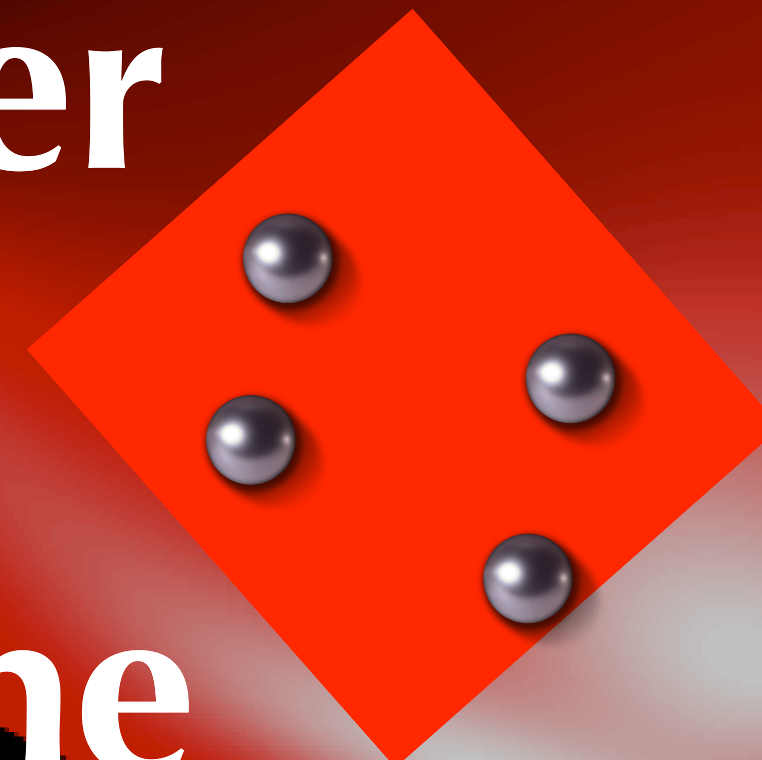
A multivariable Chinese remainder theorem and Diophantine approximation



Oliver Knill,

April 11, 2005

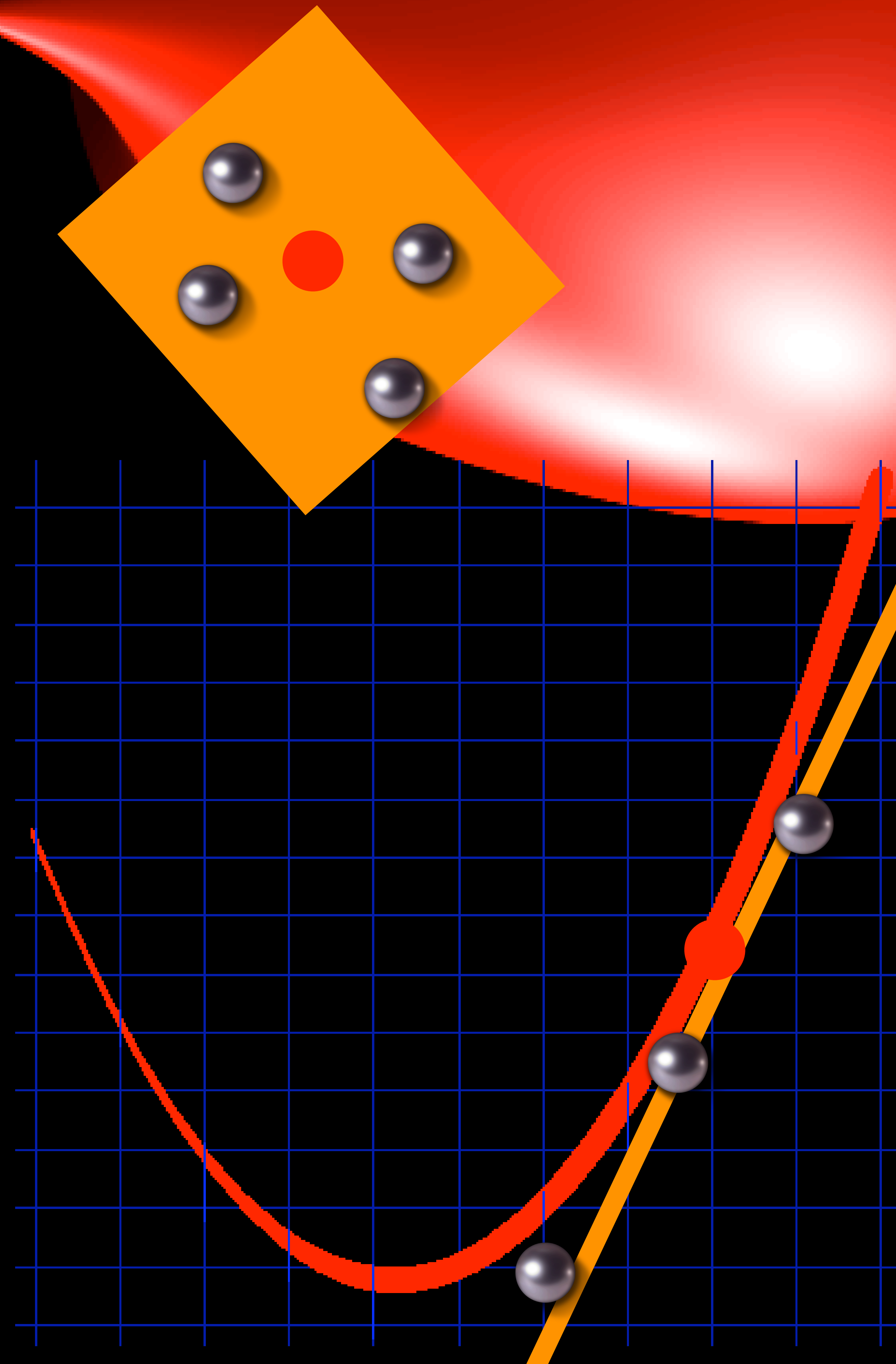
Abstract

The problem of counting and constructing lattice points near curves or surfaces has relations with dynamical systems theory as well as number theory.

We explain the relations using a lattice point result which can be proven with elementary methods and using the language of dynamical systems. In the multidimensional part, the quest leads to a multivariable Chinese remainder problems.

In a second part of the talk, we give an informal panorama of some relations between number theory and dynamical systems.

Talk overview



Counting lattice points

- ergodic theory
- dynamical systems

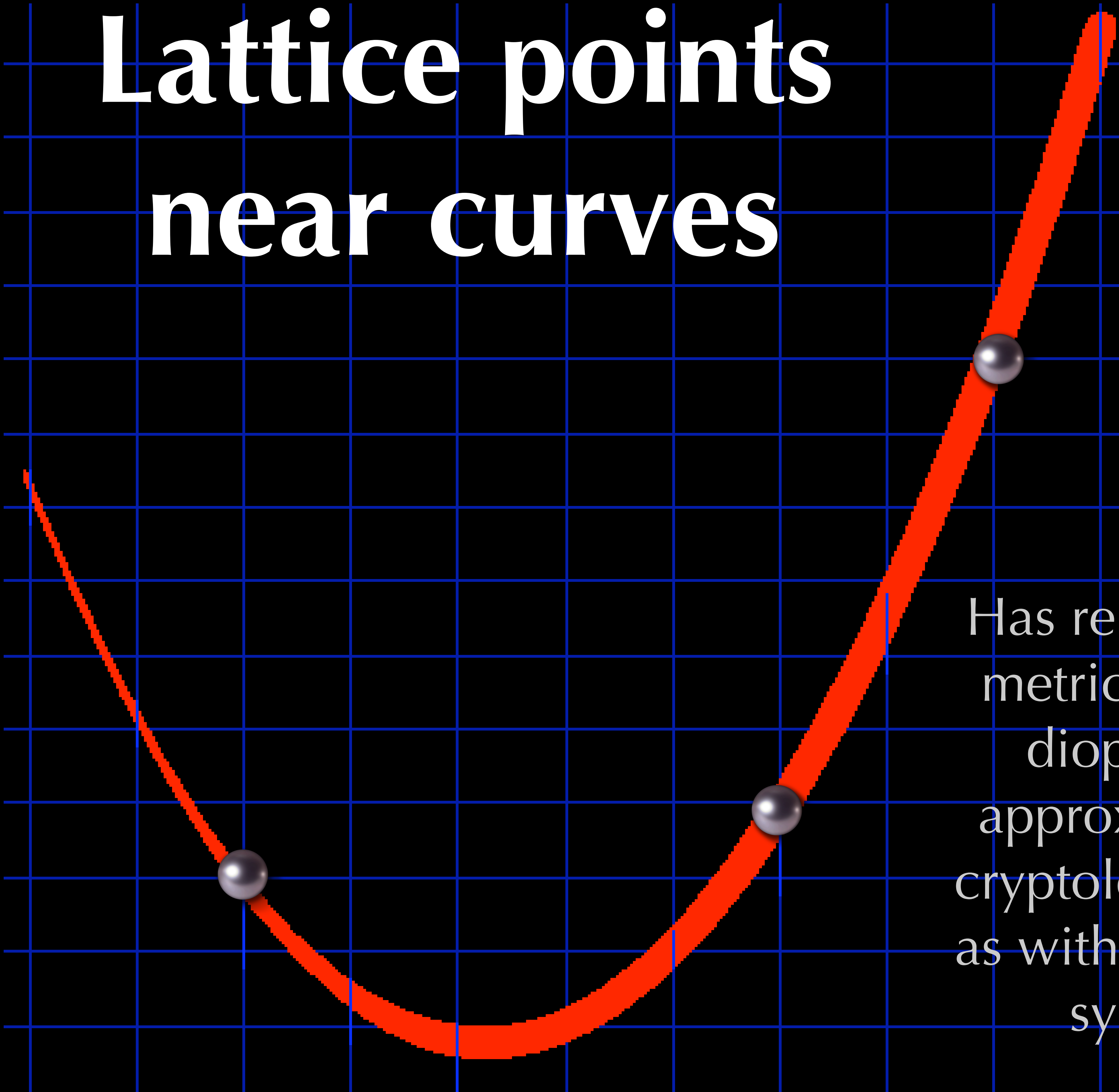
Constructing lattice points

- continued fraction
- Chinese remainder

Four type of problems

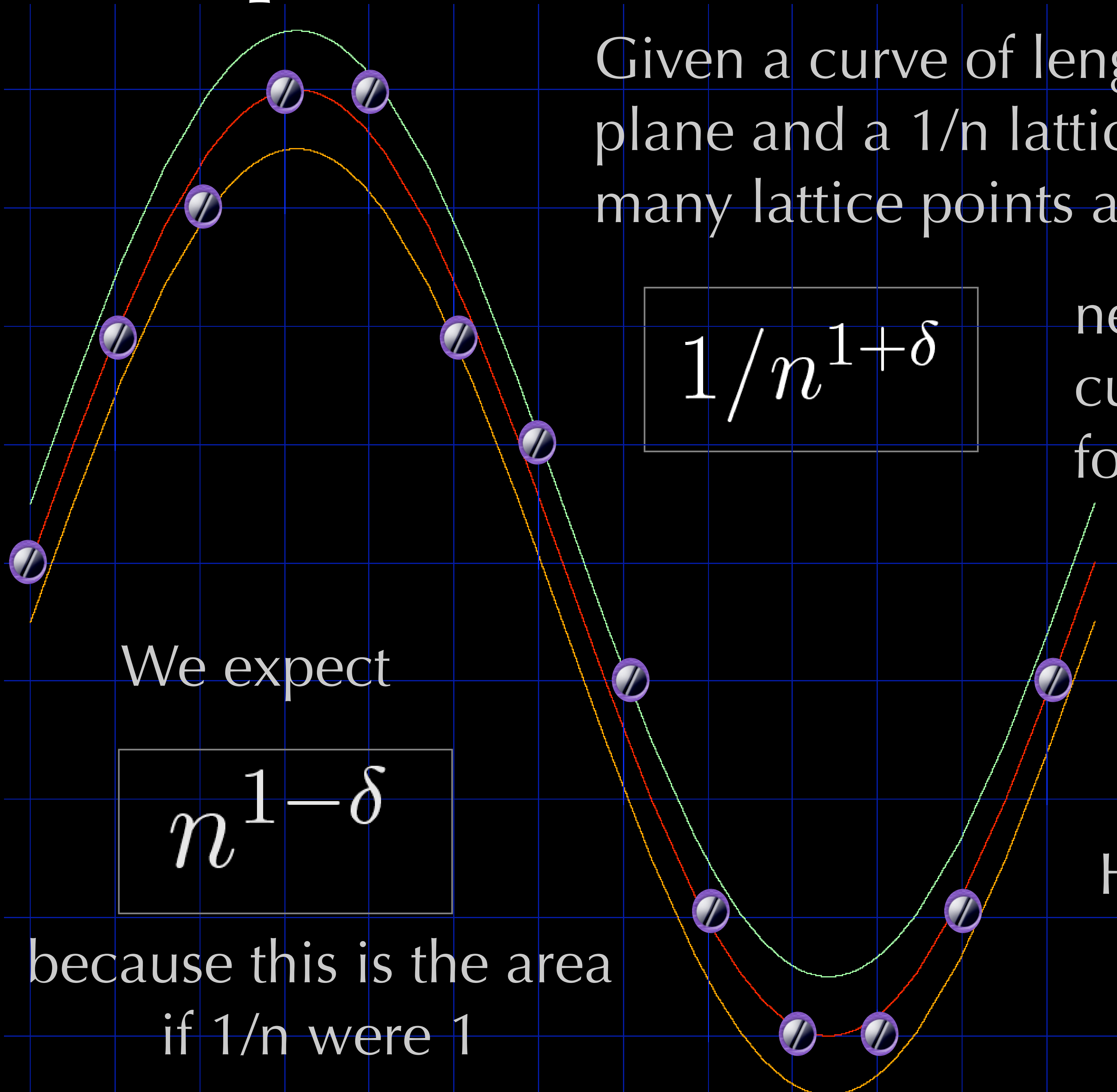
- What is the asymptotic number of 1/n lattice points in neighborhood of curve or surface
- Construct lattice points in a close neighborhood of the curve or surface.
- Construct lattice points on the curve or surface
- Establish criteria for extremality of the curve or surface

Lattice points near curves



Has relation with metric theory of diophantine approximations, cryptology as well as with dynamical systems.

A problem about curves



Given a curve of length 1 in the plane and a 1/n lattice. How many lattice points are there in a

$$1/n^{1+\delta}$$

neighborhood of the curve asymptotically for n to infinity?

We expect

$$n^{1-\delta}$$

because this is the area if 1/n were 1

How do we construct the points?

Theorem

For every smooth curve with finite length, there is a constant C such that for every $0 < \delta < 1/3$, the number $M(n,\delta)$ of $\frac{1}{n}$-lattice points in a $\frac{1}{n^{1+\delta}}$-neighborhood satisfies

$$\frac{M(n,\delta)}{n^{1-\delta}} \to C$$

- C depends on the orientation of the curve, but C is invariant under most translations
- for curves different from lines, C>0.
- C=0 possible for lines with Liouville slope.

Compare: (Schmidt 1964)

upper bound estimates work until 1/2 and imply:

Smooth curves for which the curvature is nonzero except for a finite set of points are extremal: almost all points on the curve are Diophantine vectors.

- prototype result in the metric theory of Diophantine approximation.
- there are generalizations to surfaces.
- In asymptotic result, have no conditions

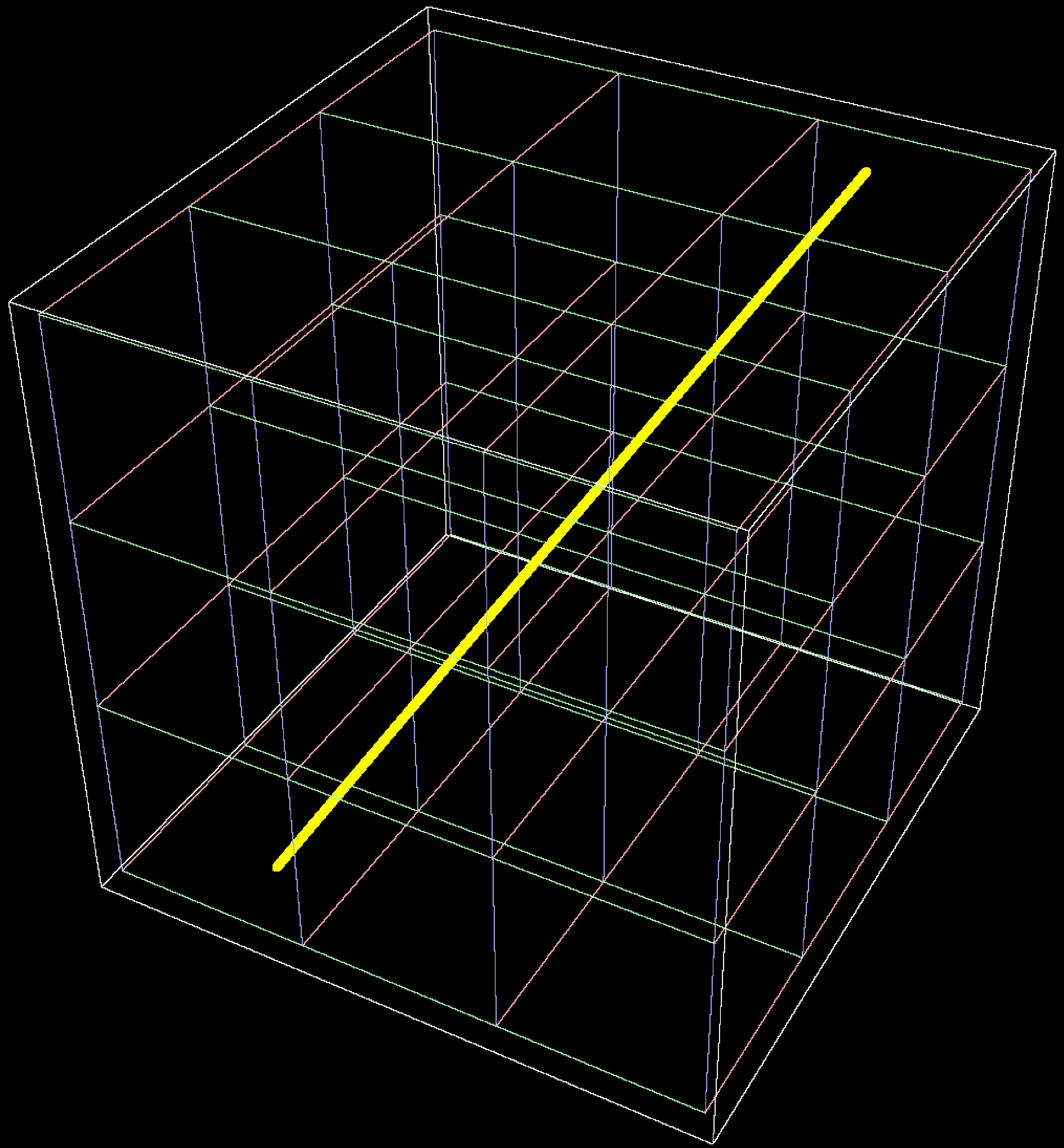
Generalization to higher dimensions

For every smooth d-dimensional manifold of finite d-volume in s-dimensional Euclidean space, there is a constant C such that for every $0 < \delta < d/(2s-d)$, the number $M(n,\delta)$ of $\frac{1}{n}$-lattice points in a $\frac{1}{n^{1+\delta}}$-neighborhood of the manifold satisfies

$$\frac{M(n,\delta)}{n^{d+\delta(s-d)}} \to C$$

The bound on delta is chosen so that the same method of linear approximation works.

Diophantine Slopes

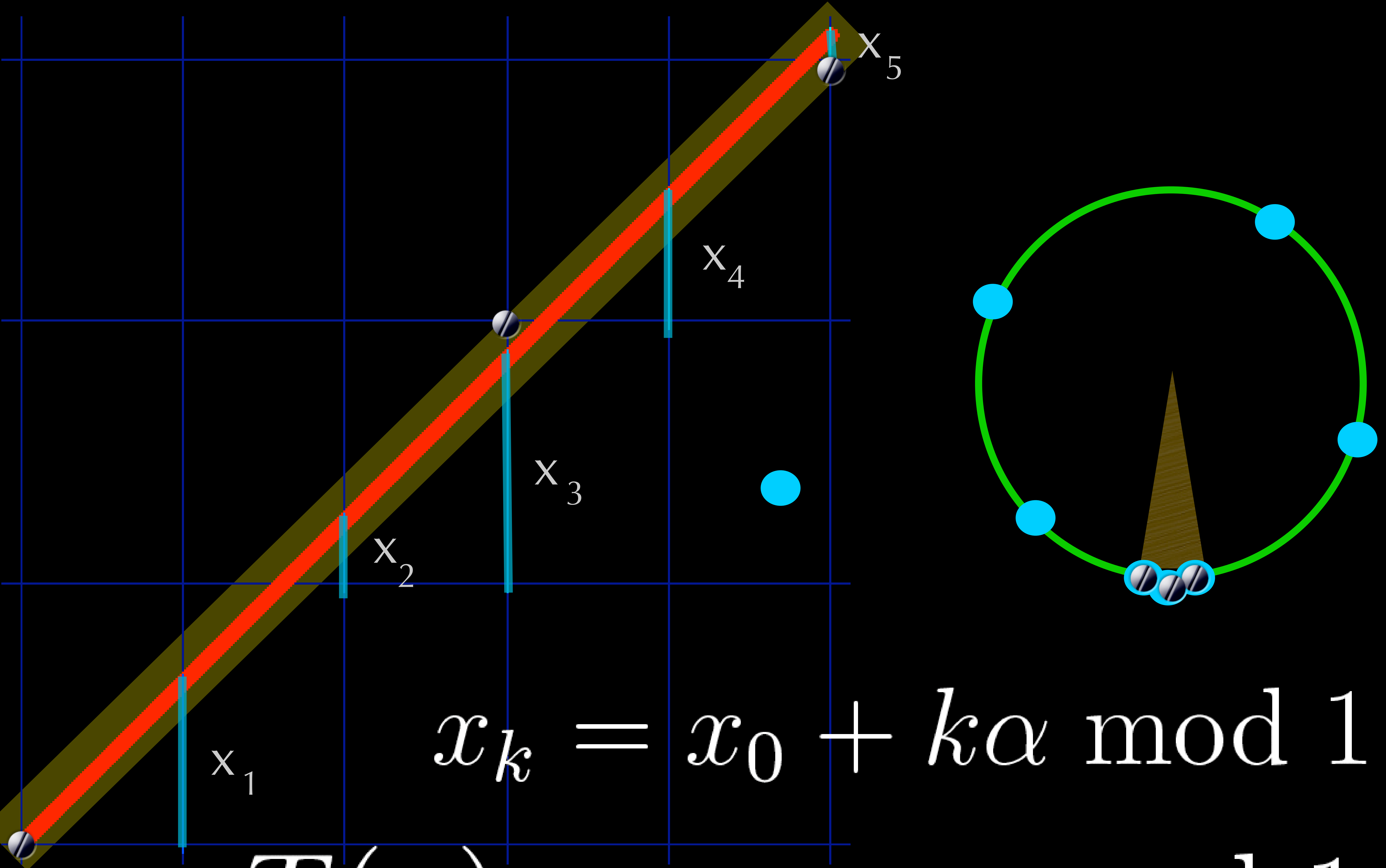


produce extremal lines in the plane or in space.

For Liouville slope, we have C=0.

Lattice points and dynamical systems

The case of the line

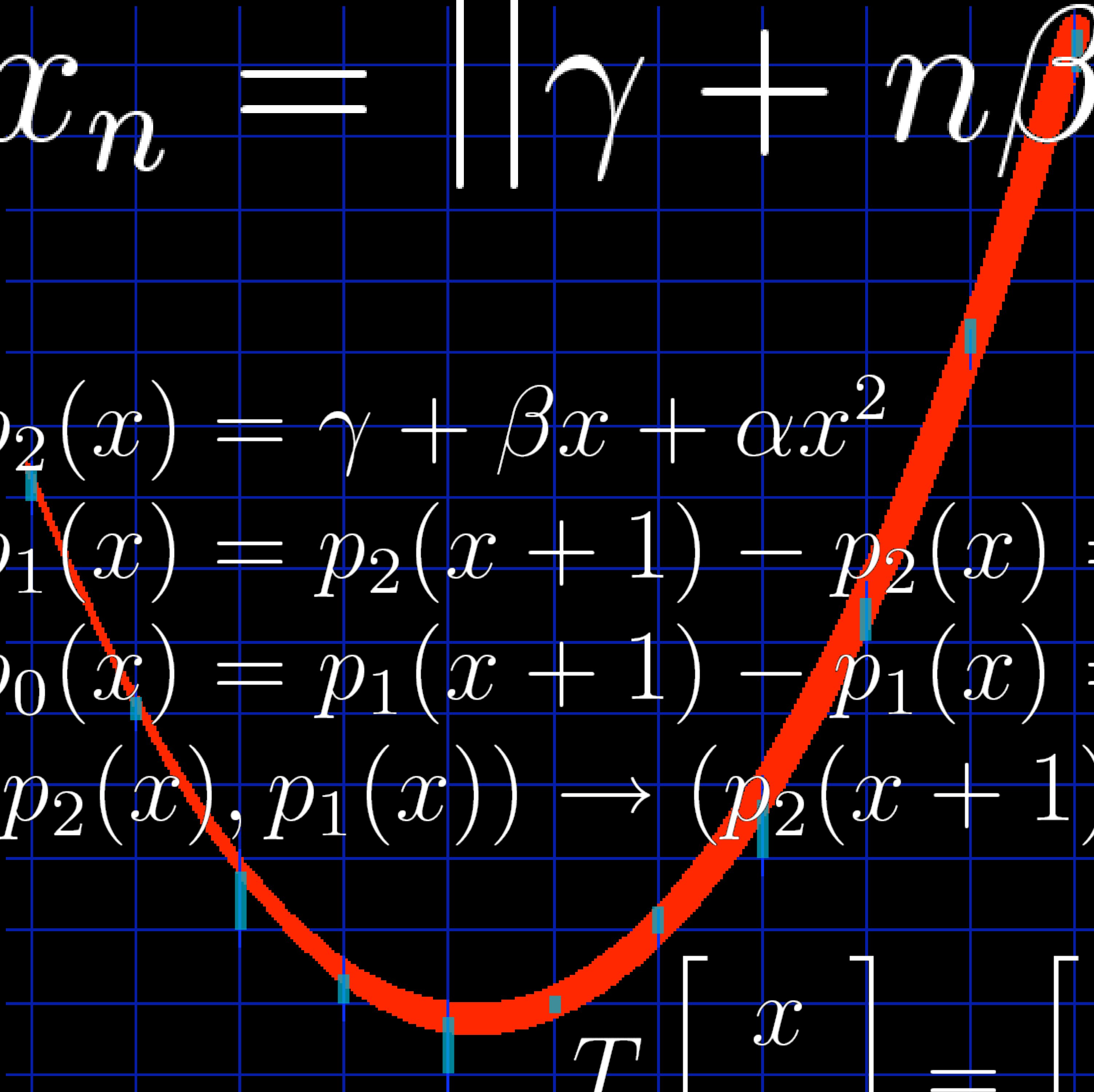


$$x_k = x_0 + k\alpha \bmod 1$$

$$T(x) = x + \alpha \bmod 1$$

The Parabola

$$x_n = ||\gamma + n\beta + n^2\alpha||$$



$$p_2(x) = \gamma + \beta x + \alpha x^2$$

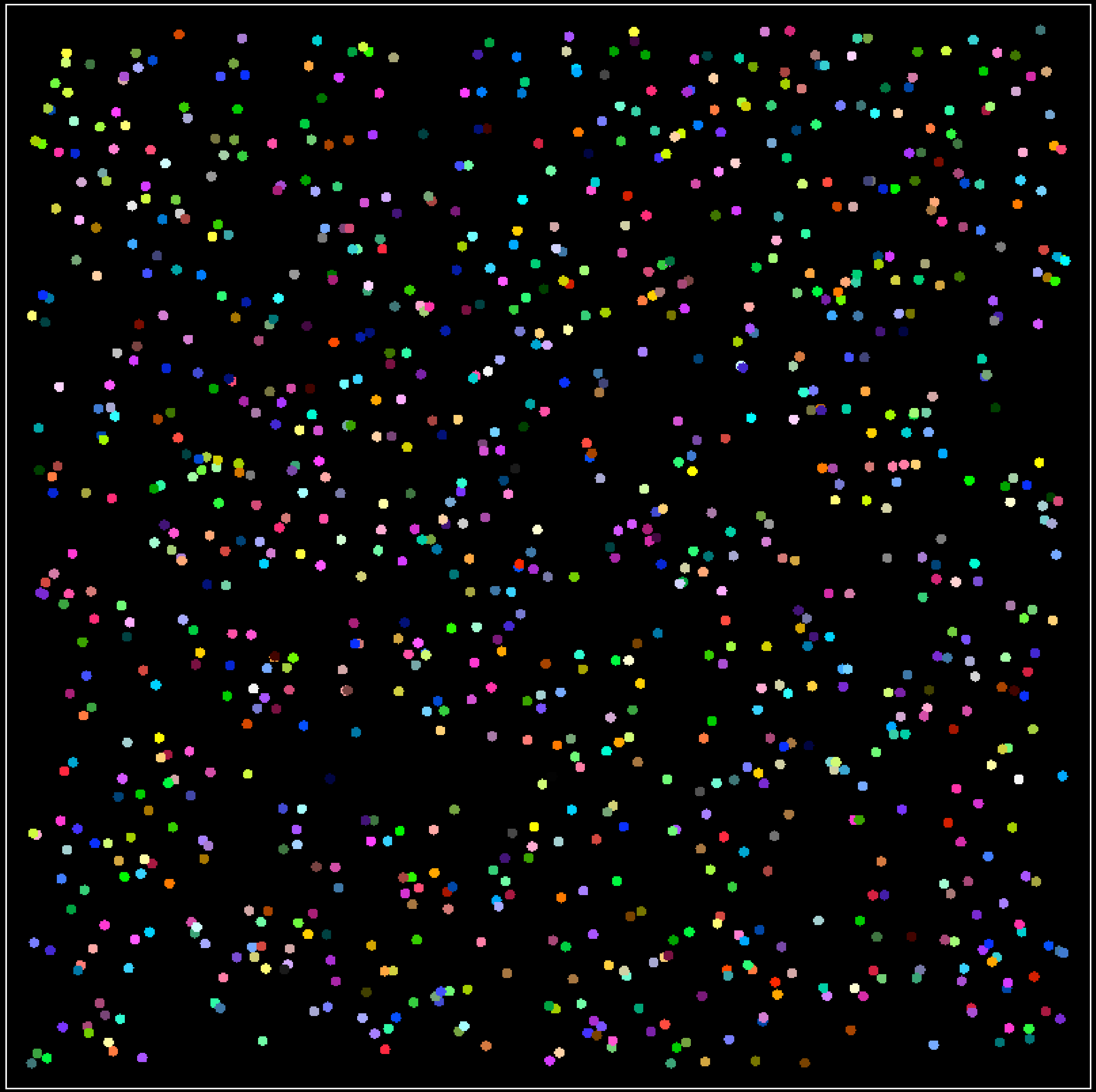
$$p_1(x) = p_2(x+1) - p_2(x) = \alpha + \beta + 2\alpha x$$

$$p_0(x) = p_1(x+1) - p_1(x) = 2\alpha$$

$(p_2(x), p_1(x)) \to (p_2(x+1), p_1(x+1))$ gives

$$T\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2\alpha \\ x + y \end{bmatrix}$$

Parabolic Sequences



The affine system is ergodic, but shows only a weak type of chaos.

Properties of this system

- strictly ergodic: uniquely ergodic and minimal.
- not integrable but integrable factors.
- no mixing but mixing factors.
- not even weak mixing.
- zero entropy (Pesin formula)

Zoo of dynamical systems

Integrable	Mixed	Mixed	Random
discrete spectrum	uniquely ergodic	integrable and hyperbolic behavior	hyperbolic Anosov

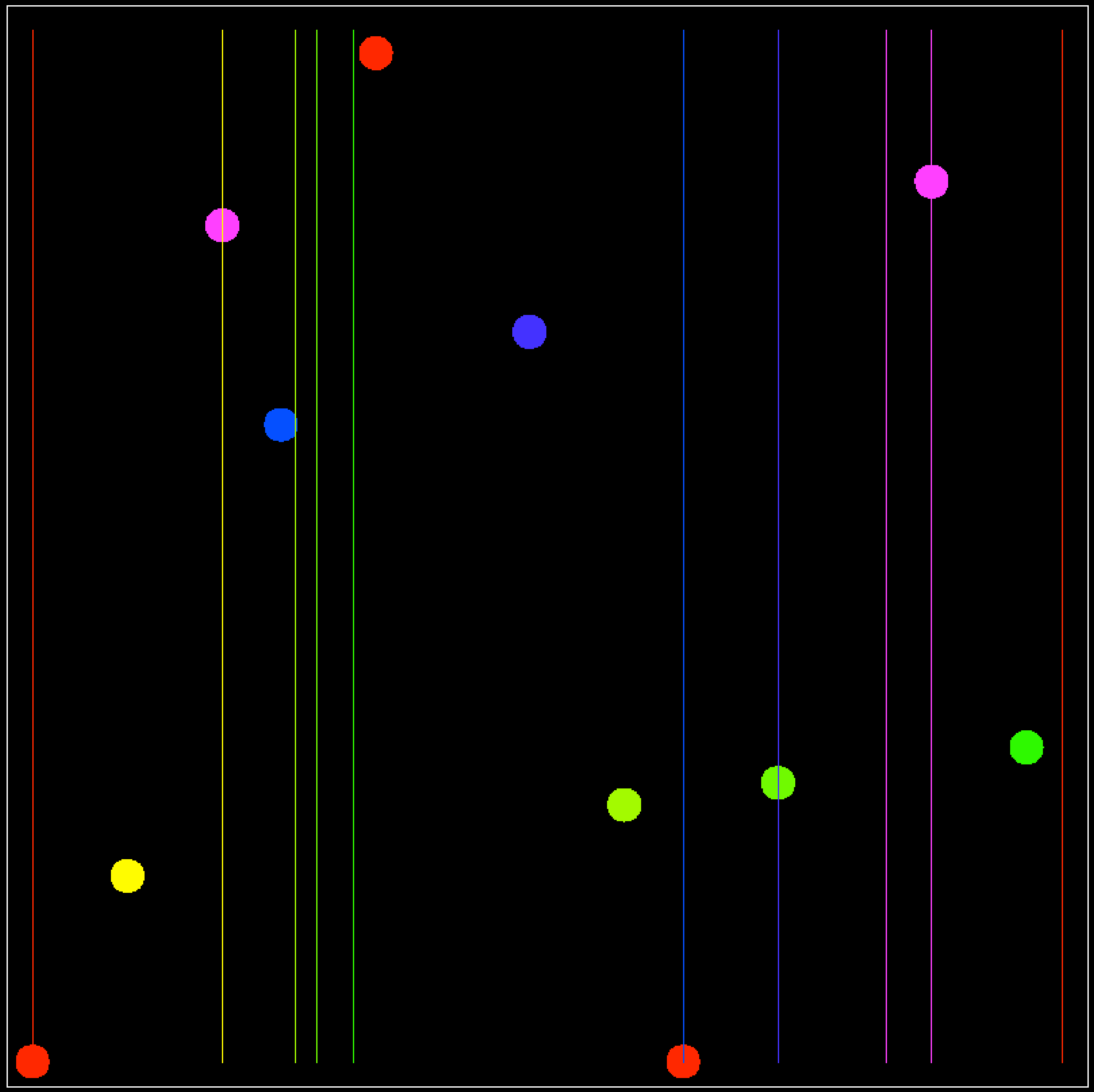
$T(x,y)=(x+a,x+y)$

$T(x,y)=(2x+y,x+y)$

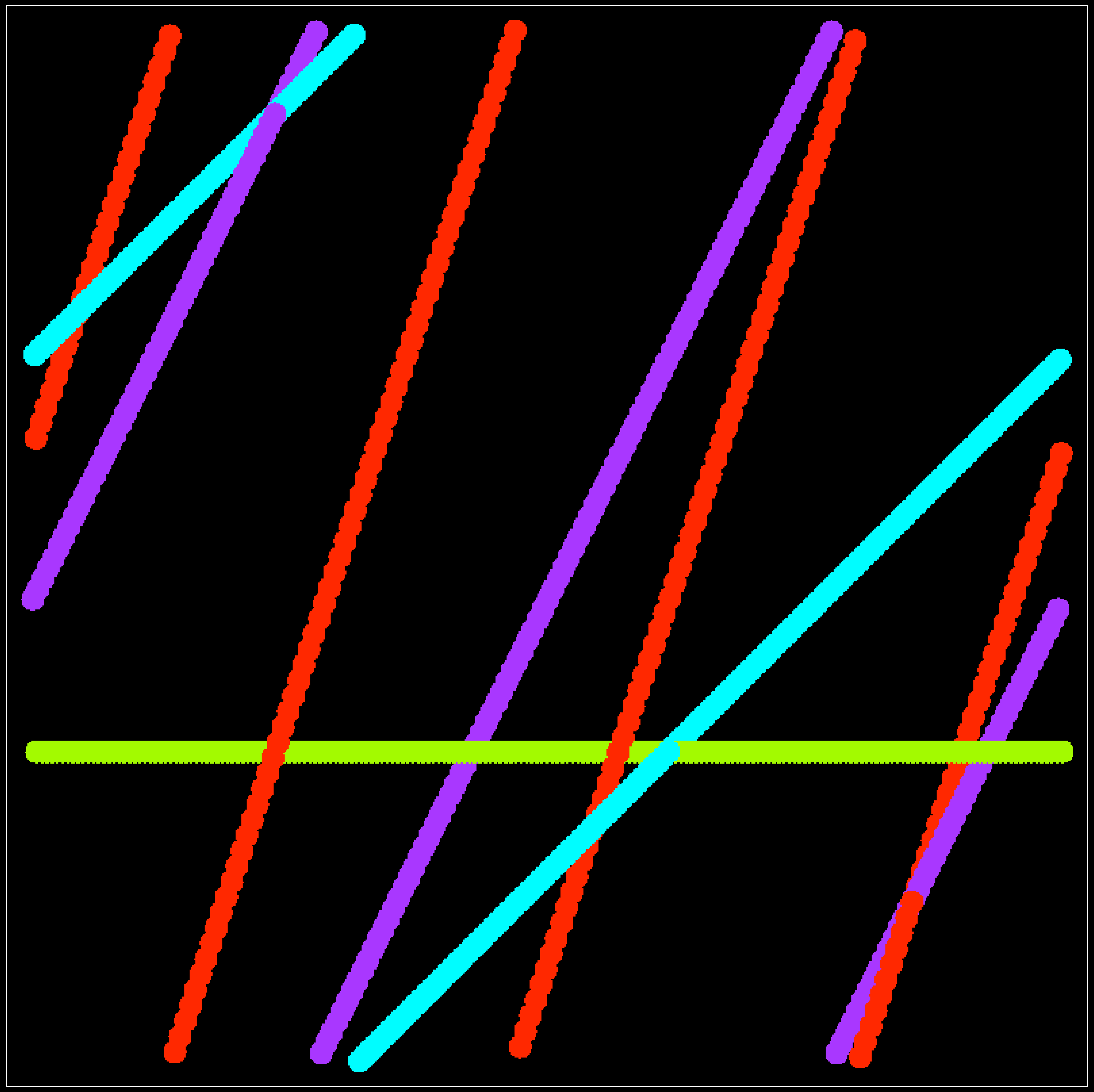
$T(x,y)=(x+a,y)$

$T(x,y)=(2x+y+4\sin(x),x)$

Integrable and mixing



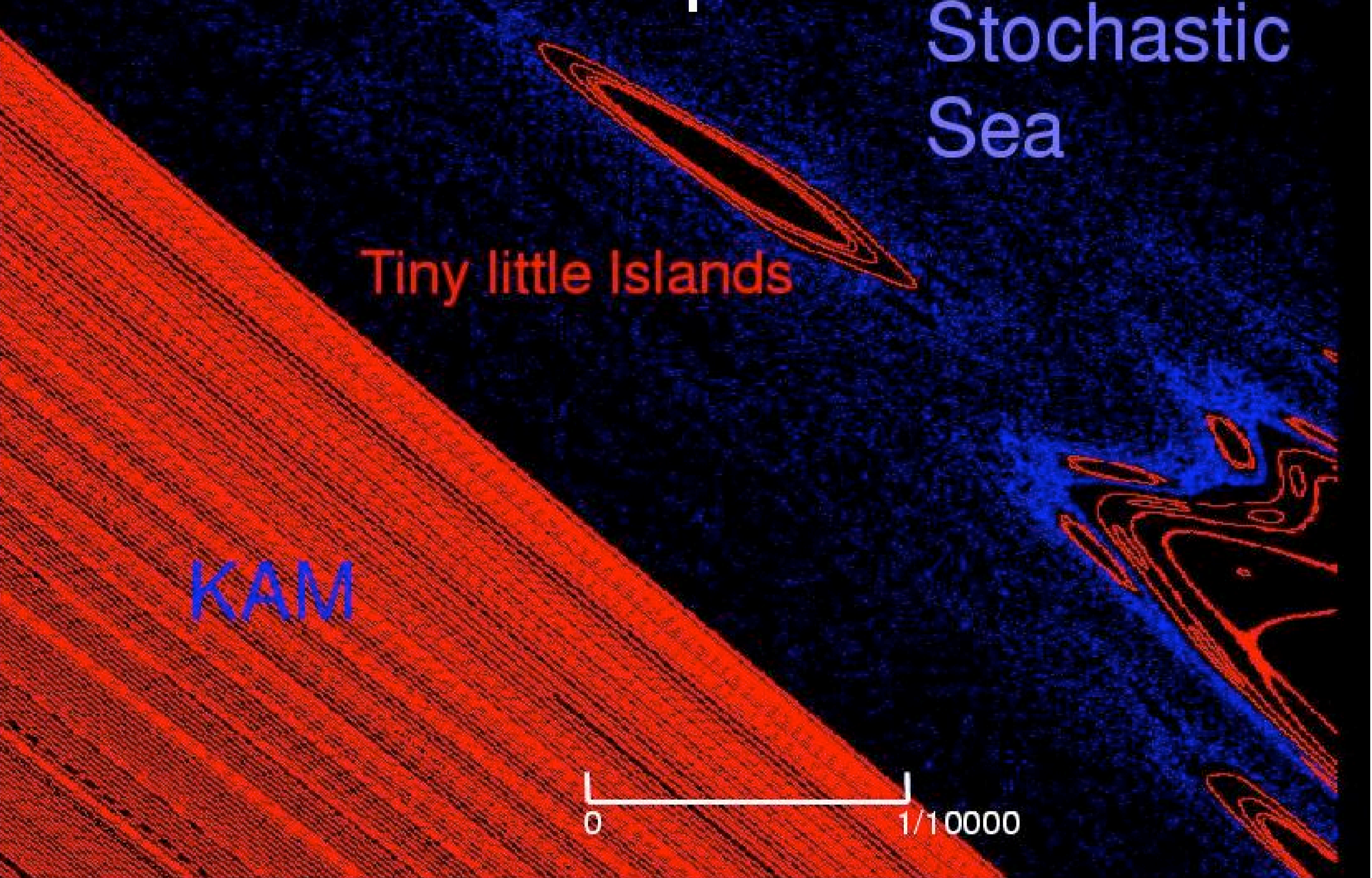
Vertical lines are translated in a regular way.



Conditioned to the y-coordinates, we see mixing (Lebesgue spectrum)

We have mixed stable and unstable behavior on the spectral level in one ergodic component. Compare with a different type of mixed behavior:

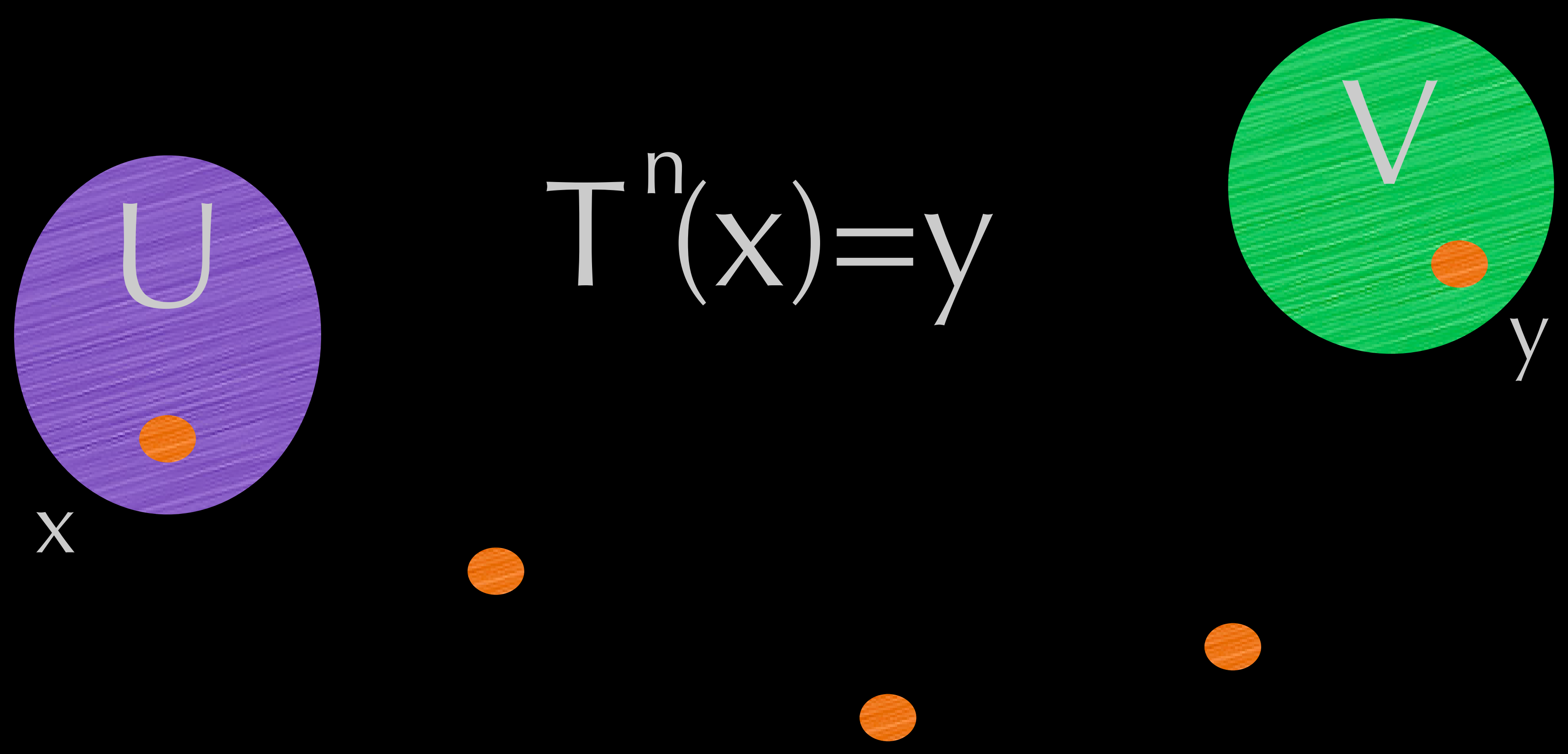
The Phase space



The discrete log problem for dynamical system

Discrete Log Problem

for dynamical systems



T(x)=ax usual logarithm on R

T(x)=ax mod p discrete logarithm on R

Prediction is in general not possible

- T(x) time evolution of atmosphere: predict storms
- T(x) evolution of an asteriod orbit: predict impact

Integrable systems

- For integrable system systems, the dynamical log problem can be solved.
- Is there a nonintegrable system, for which the discrete log problem can be solved efficiently?

- Integrable: every invariant measure leads to system with discrete spectrum

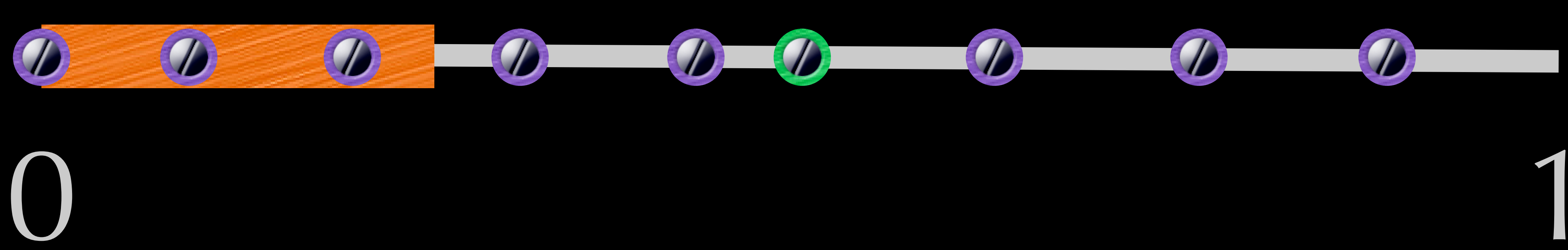
The lattice point problem is related with an ergodic lemma for Diophantine systems

An ergodic lemma

Given $\delta \in (0,1)$, define $A_n = [0, 1/n^\delta]$. For all $x \in [0,1]$,

$$\lim_{n\to\infty} \frac{1}{n^{1-\delta}} \sum_{k=1}^{n} 1_{A_n}(T^k(x)) \to 1\,.$$

A_n $\quad T(x) = x + \alpha$ **Diophantine**



for which more is known about the convergence:

For all $\epsilon > 0$ and all $0 \leq \theta < 1$, one has for almost all θ

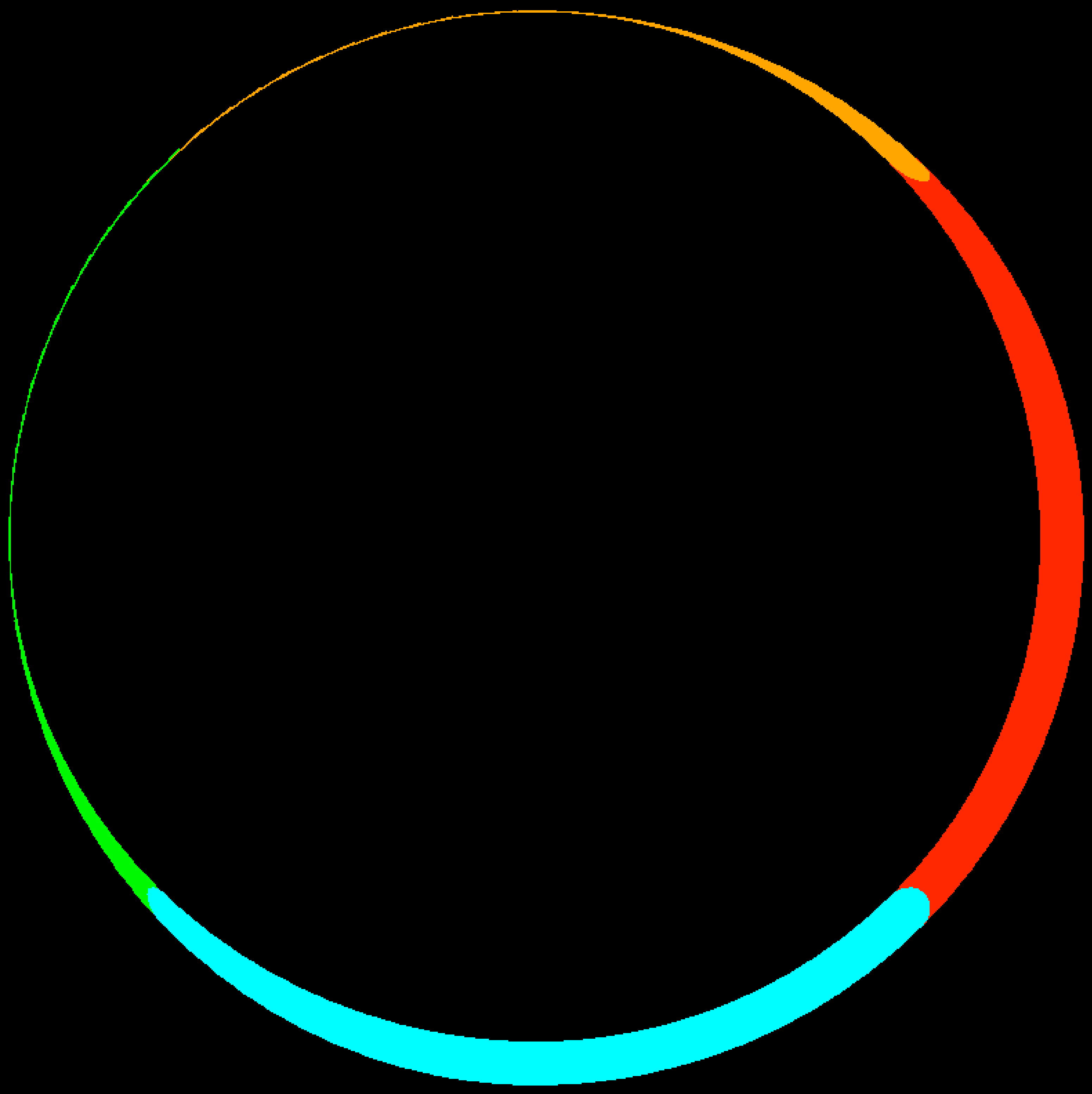
$$\frac{1}{n^{1-\theta}} \sum_{k=1}^{n} 1_{A_n}(x + k\alpha) = 1 + O(\frac{\log(n)^{2+\epsilon}}{n^{(1-\theta)/2}}) \; .$$

Paul Erdoes, Wolfgang Schmidt 1959/1960

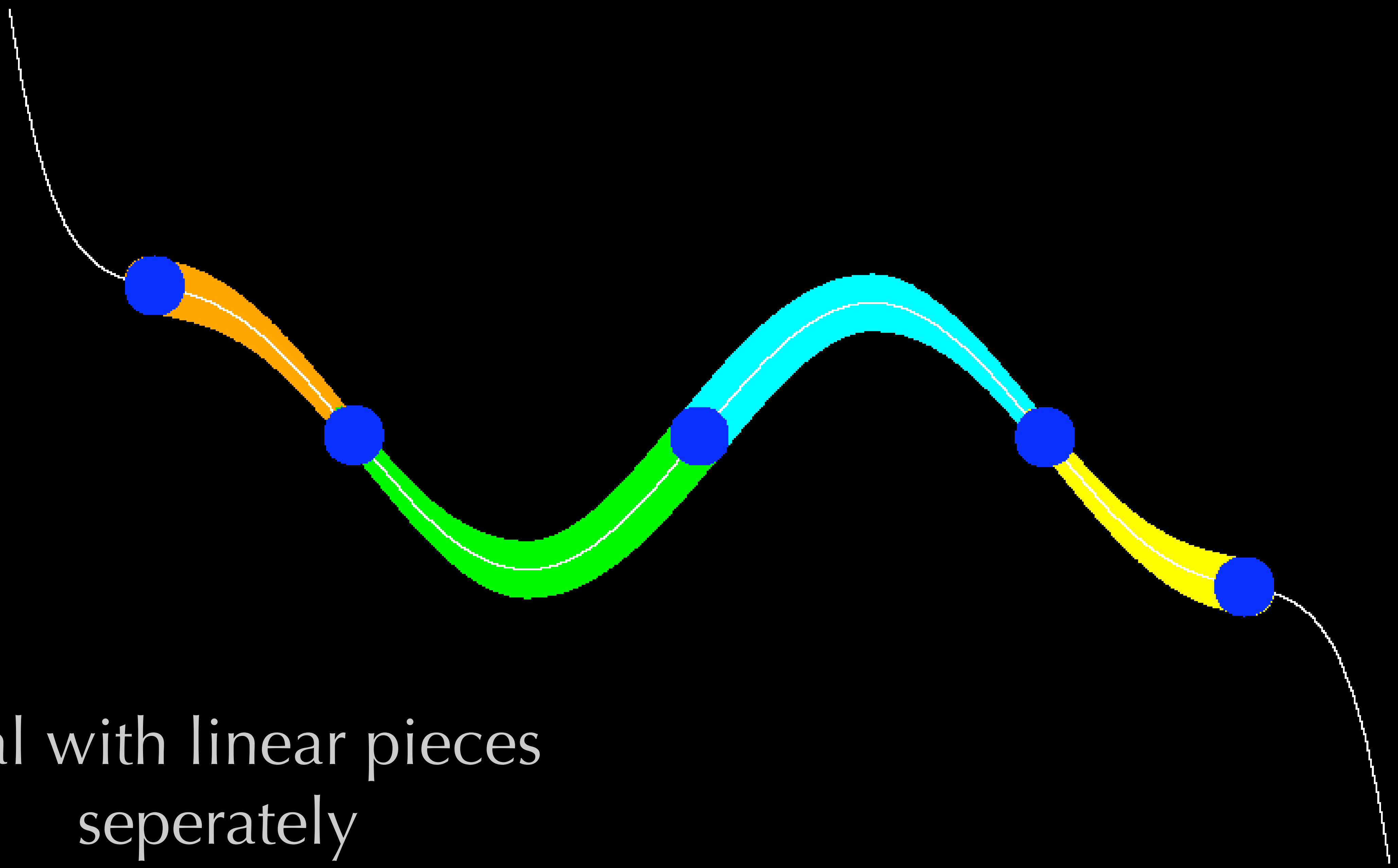
To the proof of the curve approximation result

- split curve up into piecewise concave or convex pieces which are graphs and prove the result for each piece seperately.
- Approximate the curve by splines for which each line has strongly Diophantine slope.

Charts made of Graphs



Concave or Convex pieces

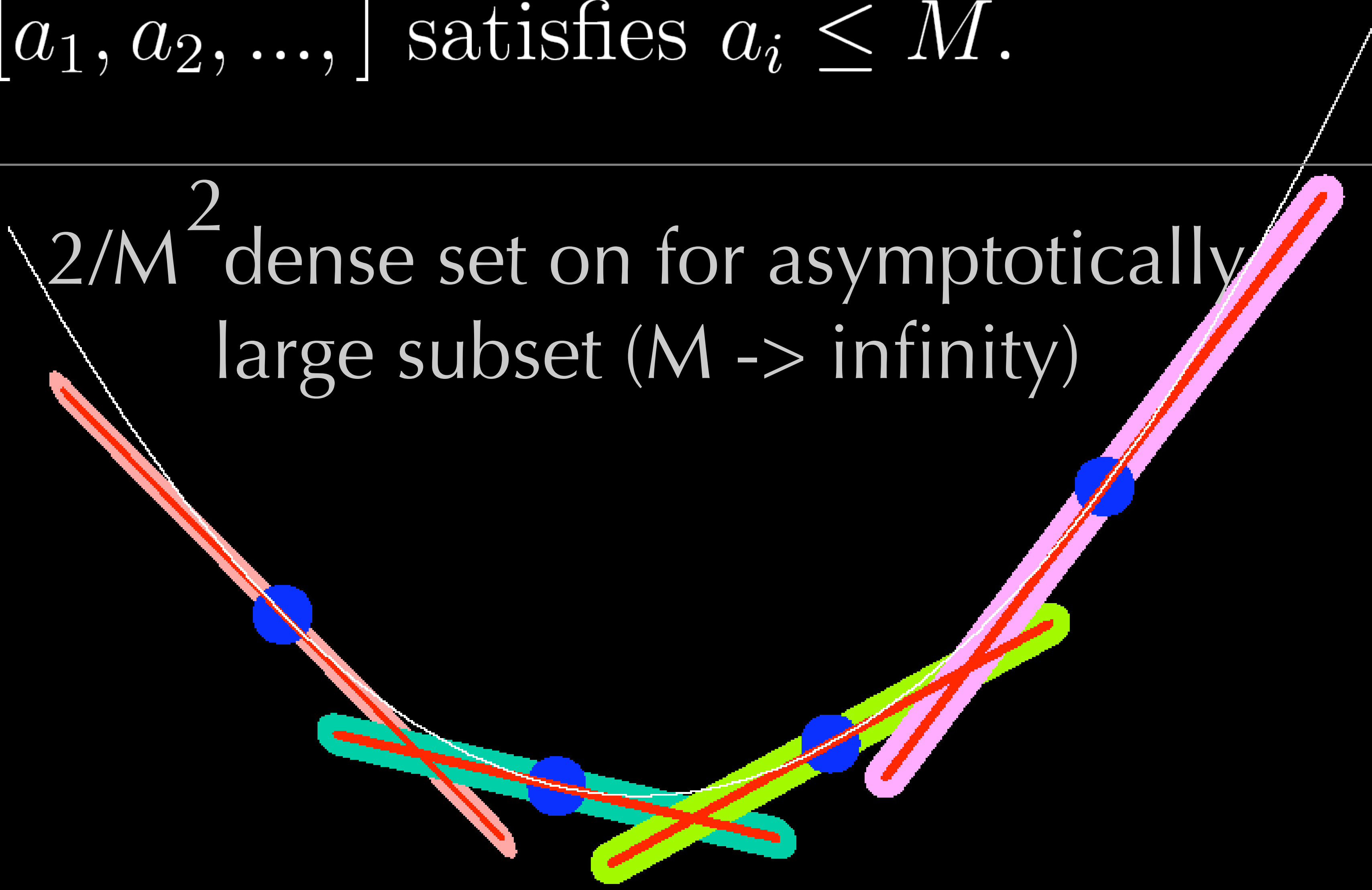


Deal with linear pieces
seperately

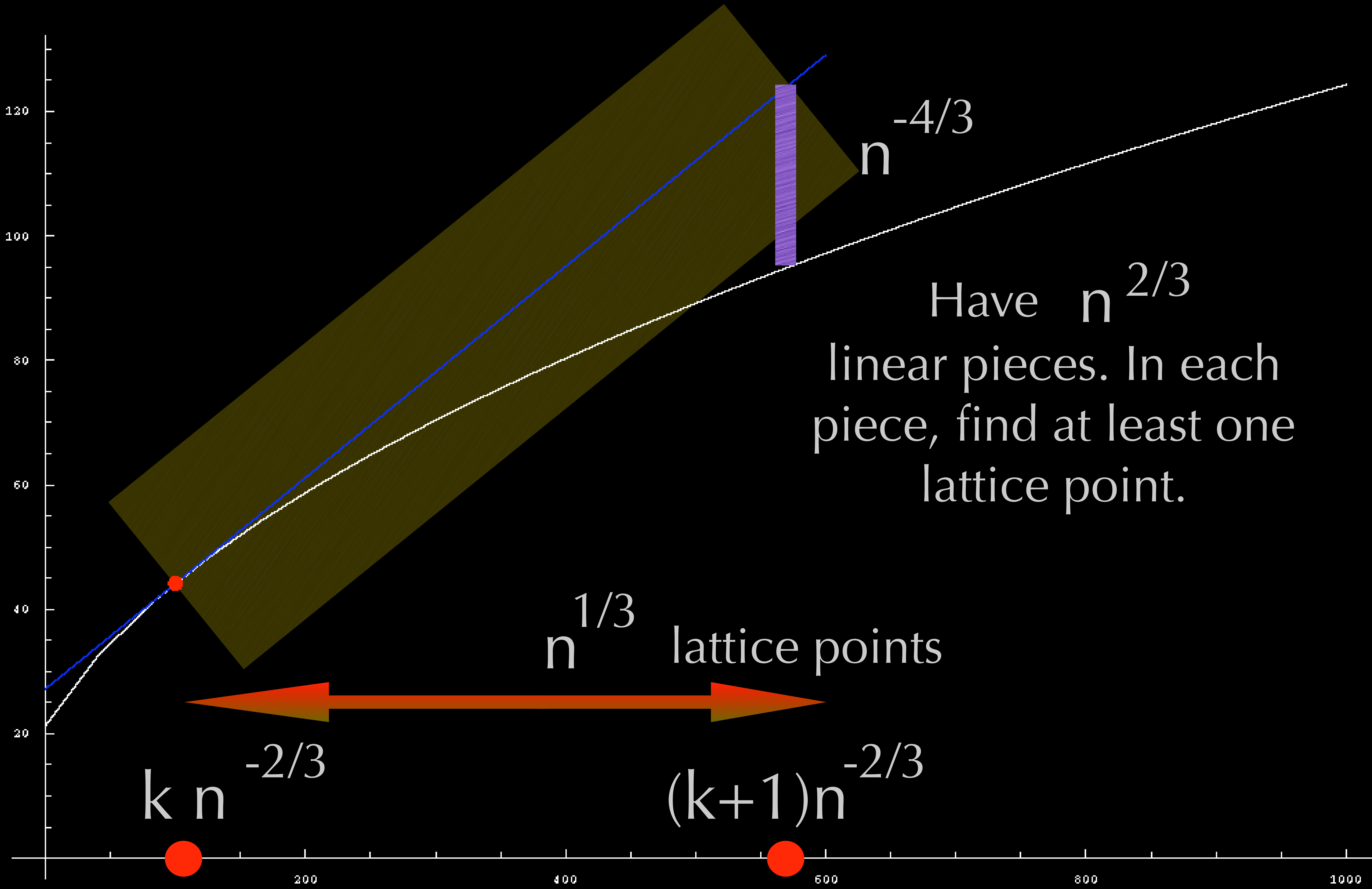
Diophantine Spline approximation

There exists a $2/M$ dense set E_M of numbers x in $[0,1]$ for which the continued fraction expansion $\alpha = [a_1, a_2, ...,]$ satisfies $a_i \leq M$.

$2/M^2$ dense set on for asymptotically large subset (M -> infinity)



Key estimate

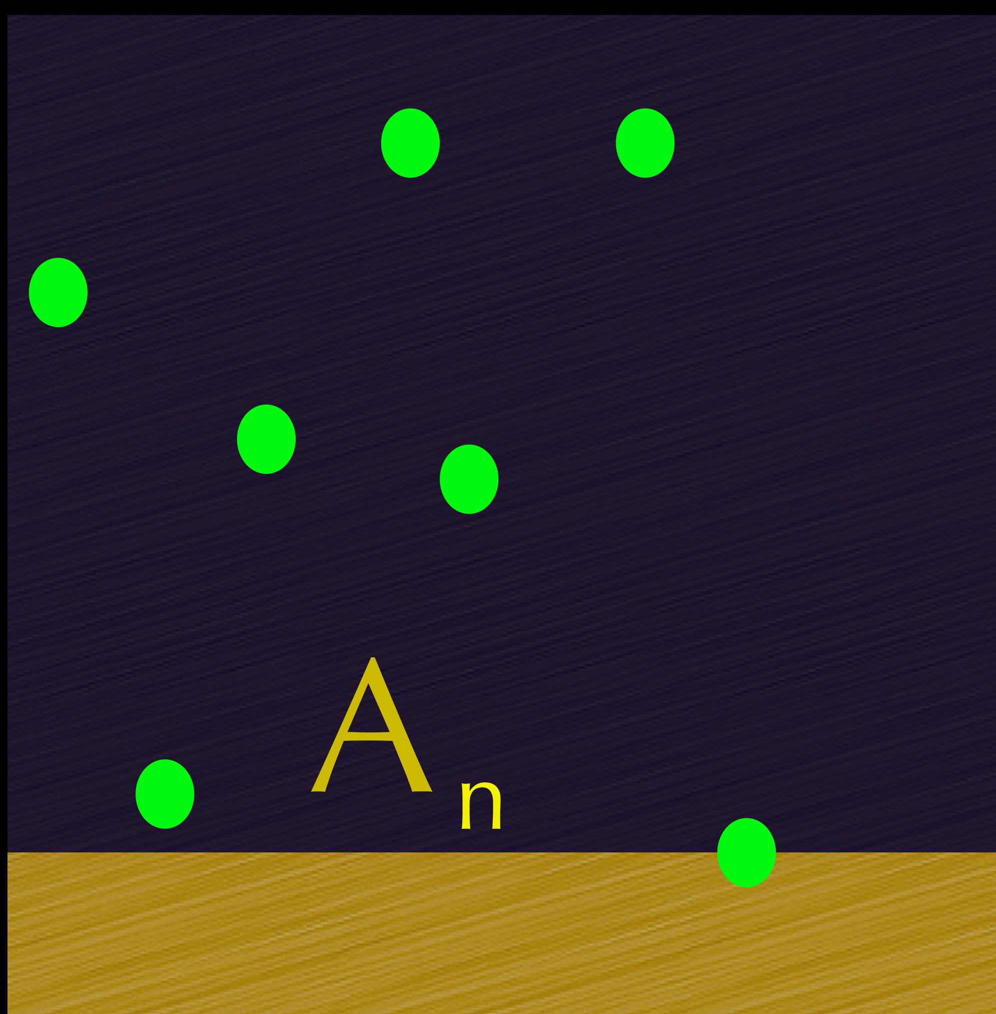


Have $n^{2/3}$ linear pieces. In each piece, find at least one lattice point.

Open: For larger delta?

Given $\delta \in (0,1)$, define $A_n = [0,1] \times [0, 1/n^\delta]$. For all $x \in \mathbf{T}^2$

$$\lim_{n\to\infty} \frac{1}{n^{1-\delta}} \sum_{k=1}^{n} 1_{A_n}(T^k(x)) \to 1\,.$$???



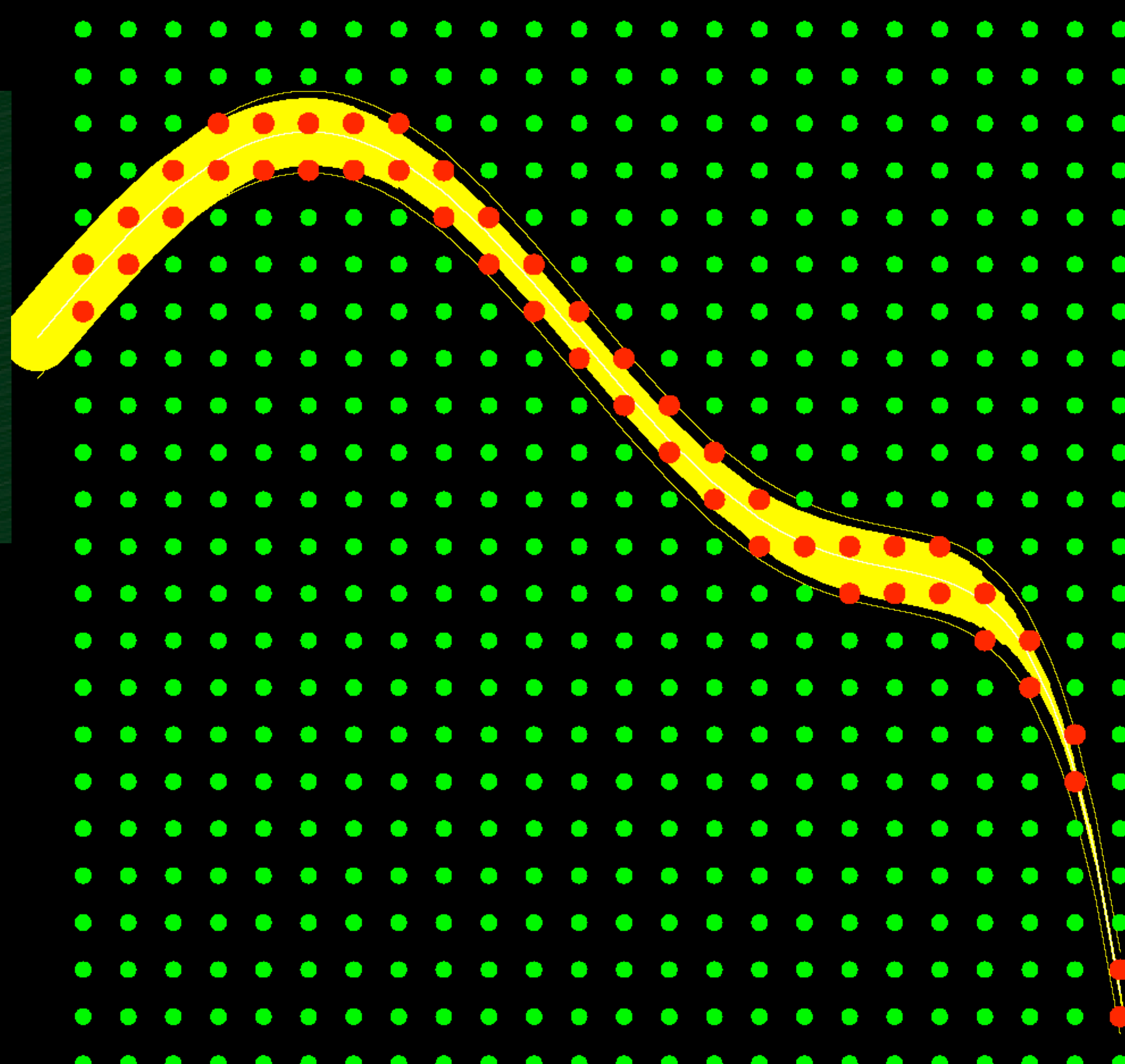
$$T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + a \\ x + y \end{bmatrix}$$

Numerical experiments indicate limit exists.

This is a Constructive Proof

Lattice points close to the curve are obtained by drawing tangents and computing lattice points close to that tangent using a continued fraction expansion. In higher dimensions, we have to solve linear equations modulo different moduli.

Number Theory



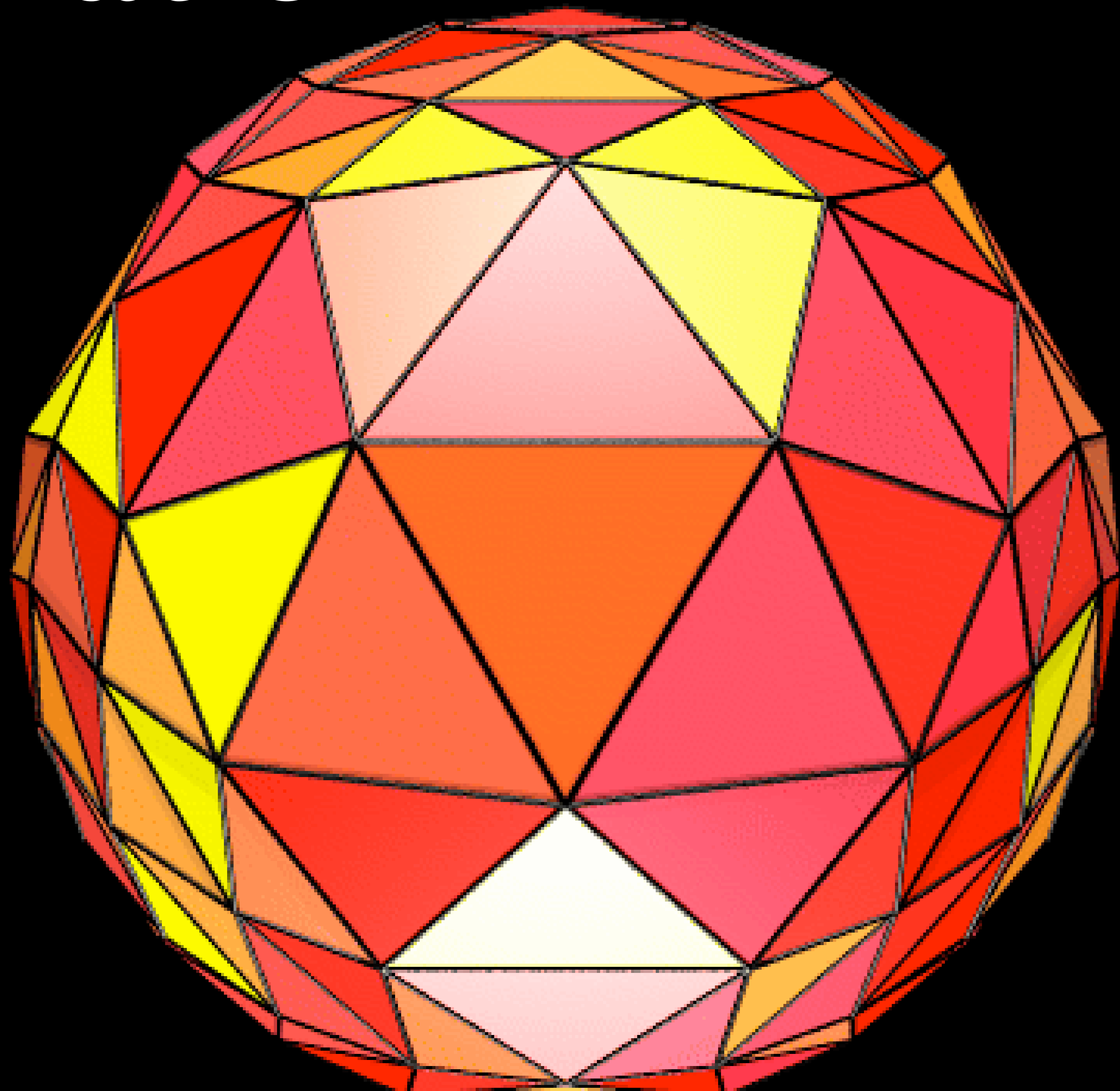
Computational number theory

Existence and construction

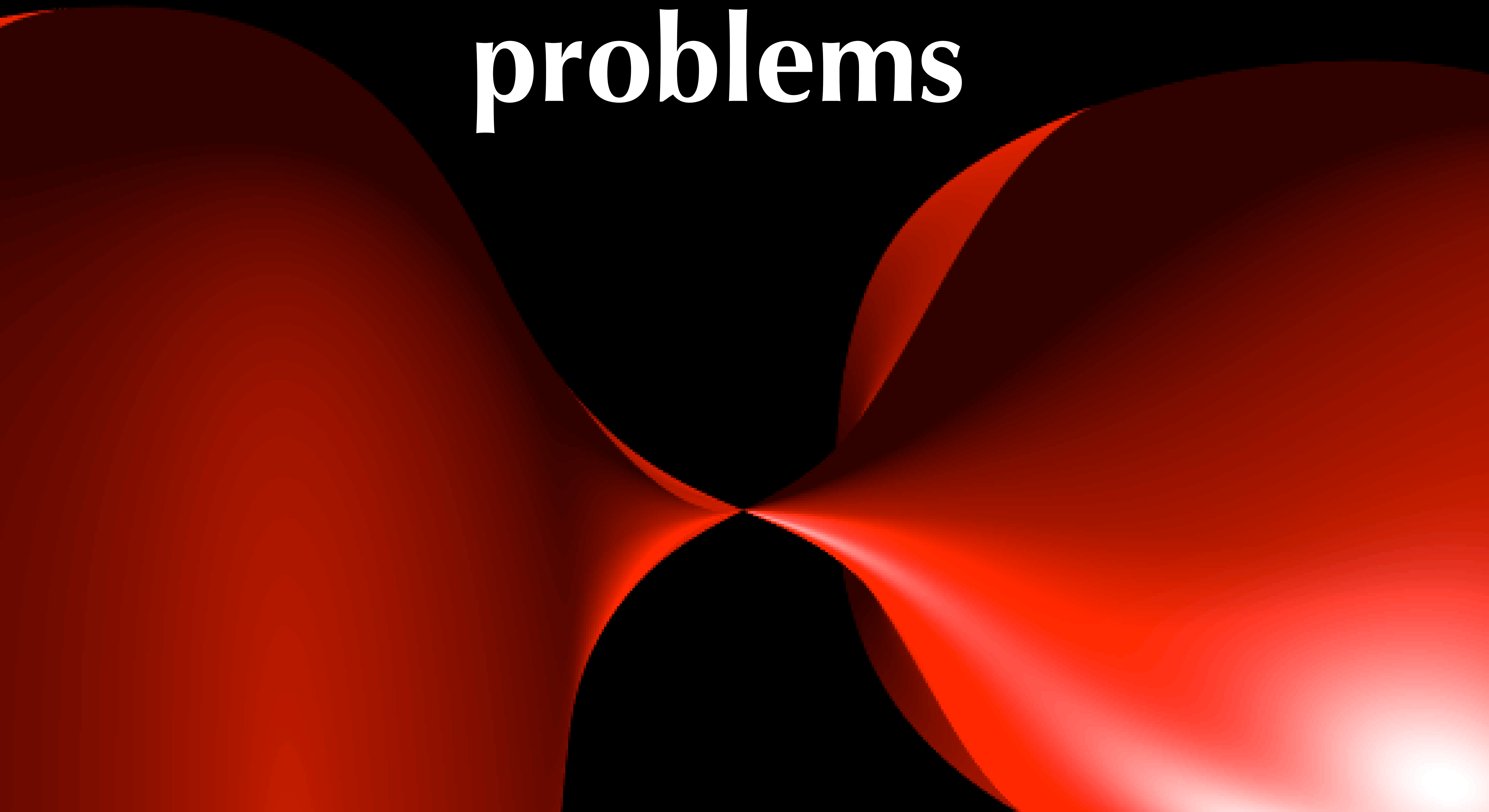
Complexity and efficient computation

Diophantine Polytope approximation

Approximate the surface by polyhedra or polytopes with Diophantine gradient vector



More about higher dimensional problems



Lattice points near surfaces

- Continued fraction alone does not solve the problem.
- Problem to characterize extremal surfaces.
- We deal with dynamical systems with higher dimensional time
- Constructive problem leads to multivariable Chinese remainder theorem.

Lattice points near planes

To find lattice points close to to the plane

$$ax + by + d = z$$

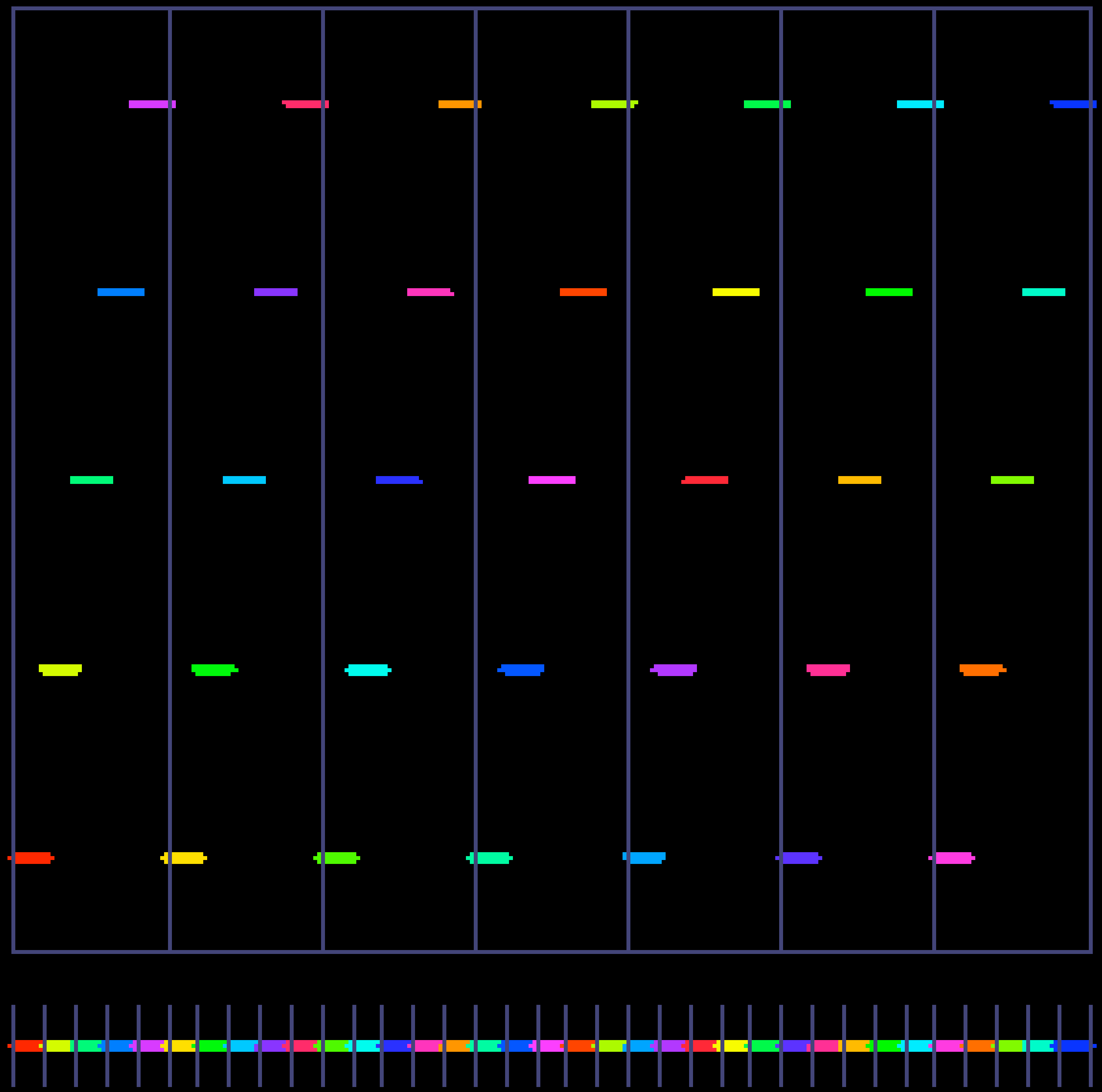
we have to find pairs (n,m) for which the fractional part

$$\{\alpha n + \beta m + t\}$$

is small. There are three cases:

α	rational	β	rational
α	rational	β	irrational
α	irrational	β	irrational

Double Rational Case



If α = p/q
and β = r/s
and gcd(q,s)=1, then
there are m<q,n<s
with

$$\{\alpha n + \beta m + t\}$$ <1/qs

Semi rational case

α = p/q

The map T(x) = x+ β modulo 1/q

corresponds to the map T(x) = x + q β

This one dimensional problem is solved by Tchebychev

if r/s is the periodic approximation of β

there are n<q, m<s such that

$$\{\alpha n + \beta m + t\} < 3/(qs)$$

Irrational case

- This is the most interesting case.
- For Diophantine vectors, there are small solutions.
- To construct solutions, we need to do solve amultivariable Chinese remainder problem.

Systems of linear modular equations

$$a\,x + b\,y = u \mod p$$
$$c\,x + d\,y = v \mod q$$

How do we find small solutions? What is the "kernel".

special case:

Chinese remainder Theorem

If gcd(p,q)=1,
gcd(a,p)=1,
gcd(c,q)=1,there exists a solution x.

$$a\,x = u \mod p$$
$$c\,x = v \mod q$$

A multivariable Chinese remainder theorem

$$\begin{aligned} a\,x + b\,y &= u \quad \text{mod} \quad p \\ c\,x + d\,y &= v \quad \text{mod} \quad q \end{aligned}$$

If gcd(p,q)=1 and in each row, there is one coeficient, which is relatively prime to the modulus, then there is a unique solution in a paralellepiped of area pq.

Sun Tsu's Suan Ching

孫子算經序

孫子曰夫算者天地之經緯羣生之元首五常之本末陰陽之父母星辰之建號三光之表裏五行之準平四時之終始萬物之祖宗六藝之綱紀稽羣倫之聚散考二氣之降升推寒暑之迭運步遠近之殊同觀天道精微之兆基察地理從橫之長短采神祇之所在綜成敗之損益窮道德之理究性命之情立規矩準方圓謹法度約尺丈立權衡平重輕剖毫釐析黍絫歷億

孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉勅注釋

度之所起起於忽欲知其忽蠶吐絲為忽十忽為一絲十絲為一毫十毫為一氂十氂為一分十分為一寸十寸為一尺十尺為一丈十丈為一引五十尺為一端四十尺為一疋六尺為一步二百四十步為一畝三百步為一里

稱之所起起於黍十黍為一絫十絫為一銖二十四銖為一兩十六兩為一斤三十斤為一鈞

History

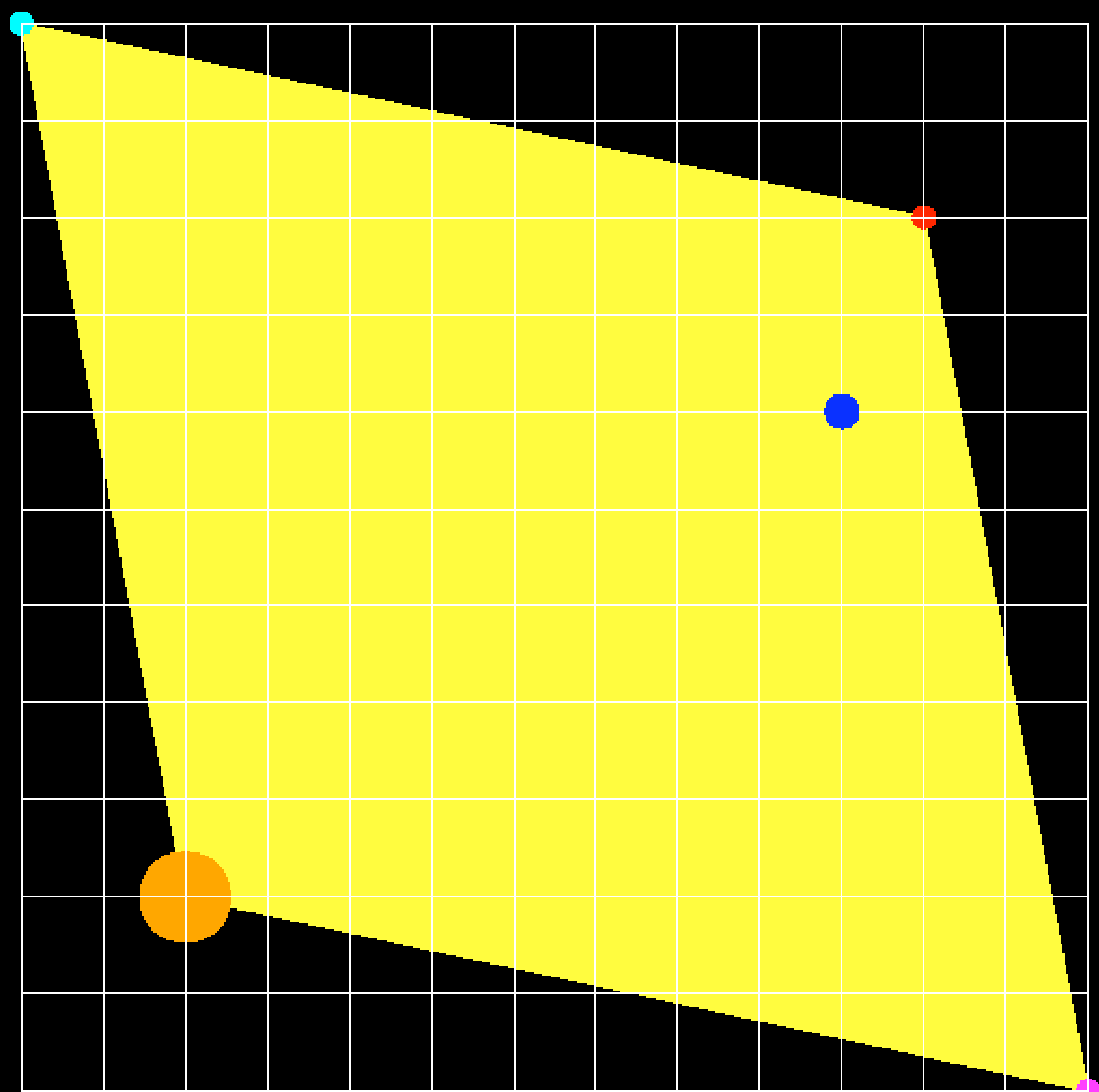
Sun Tsu Suan Ching	Master Suns Mathematical Manual	100
Nicomachus of Gerasa	Pythagorei introd. aritith. libri duo	100
Brahmagupta	Brahma Sphuta Siddhanta	600
Qin Jiushao	Shushu Jiuzhang full algorithm	1247
Gauss	Disquisitiones Arithmeticae	1801
Schoenemann	1 linear eq. several variables	1839
Alexander Wylie	Article in North China Herald	1852

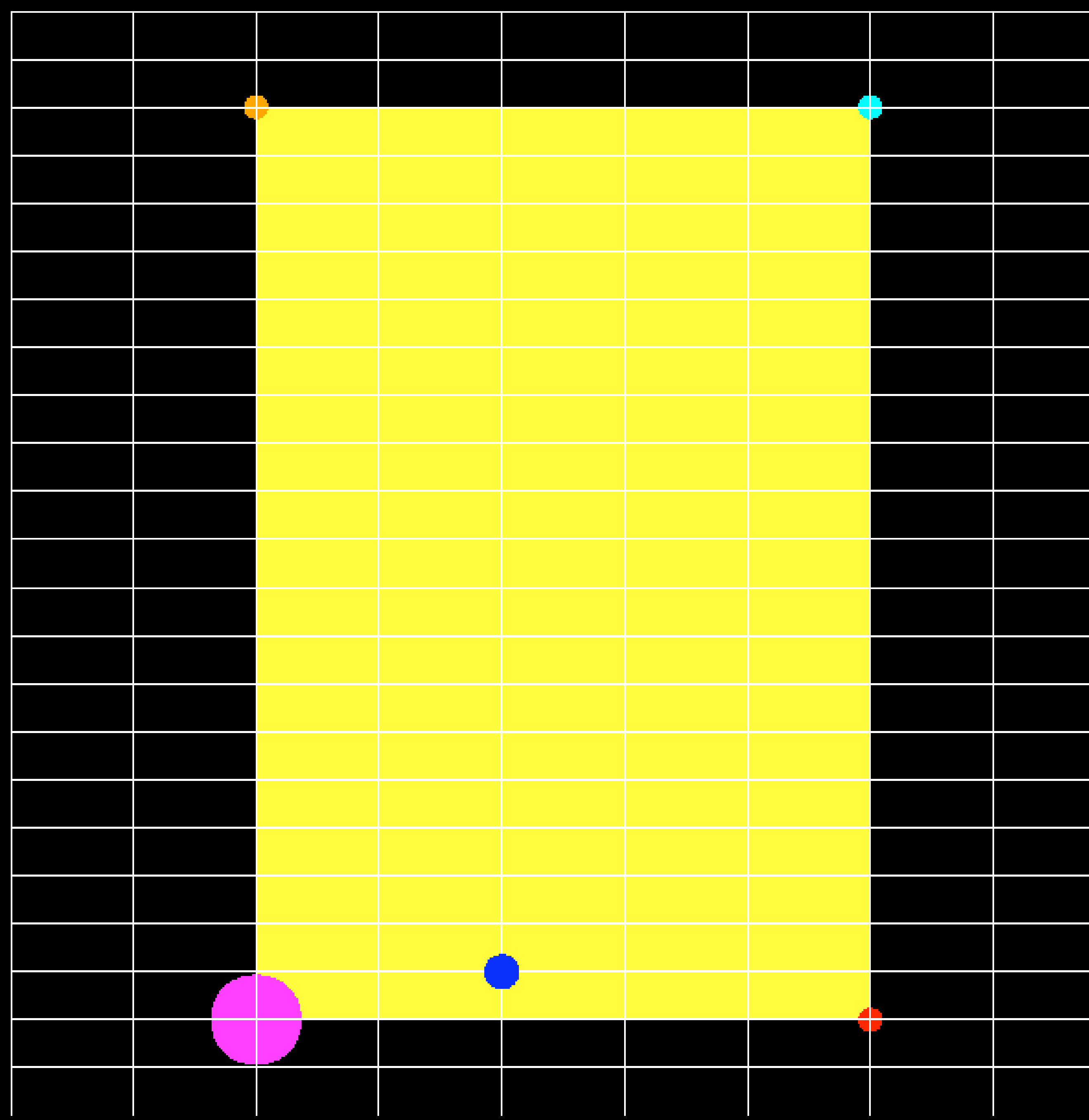
An example

4x+17y=2 mod 5
11x+13y=1 mod 19

has the solution x=8,y=5

(11,-2), (-2,9) span the kernel





How to solve $4x+17y=2 \mod 5$, $11x+13y=1 \mod 19$?

- Plug in $x(t)=(t,0)$. This gives the problem

$$4t = 2 \mod 5$$
$$11t = 1 \mod 19$$

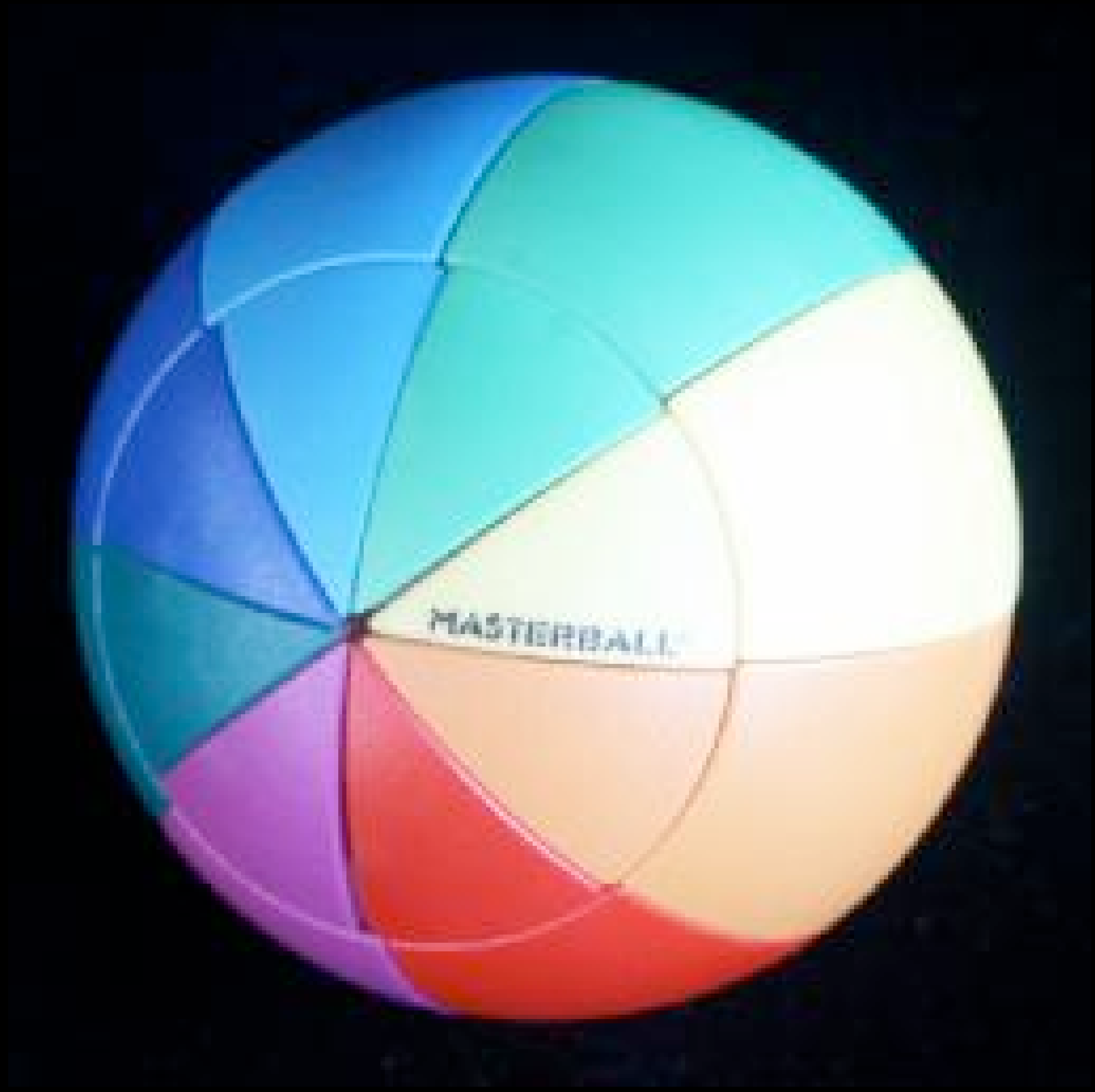
which is already a Chinese remainder theorem problem.

The first equation has the solution $t=3$. Now take the path $(3,0) + 5\,t\,(0,1)$ which still solves the first equation and leads to the problem

$$33 + 65\,t = 1 \mod 19$$

which is solved by $t=15$. We found the solution $(42,210)$

About a masterball puzzle adventure:



Relation of lattice point problems with cryptography

Factorization of n=pq

A basic idea of many algorithms is by Legendre:
find x,y such that $x^2=y^2 \mod n$

Also related is finding solutions to the quadratic equation $x^2=1 \mod n$, we could factor n.

$4^2 = 1 \mod 15$ 4-1 is factor

It is actually enough find x, such that $x^2 \mod n$ is small.
Sieving methods allow then to find x so that $x^2 \mod n$ is a square

Factorization algorithms like Fermat method, Morrison-Brillard, Quadratic sieve are based on this principle.

Quest for small squares

$$f(x) = \sqrt{2n^2 + xn + a^2}$$

For a lattice point (x, y) on the curve we have

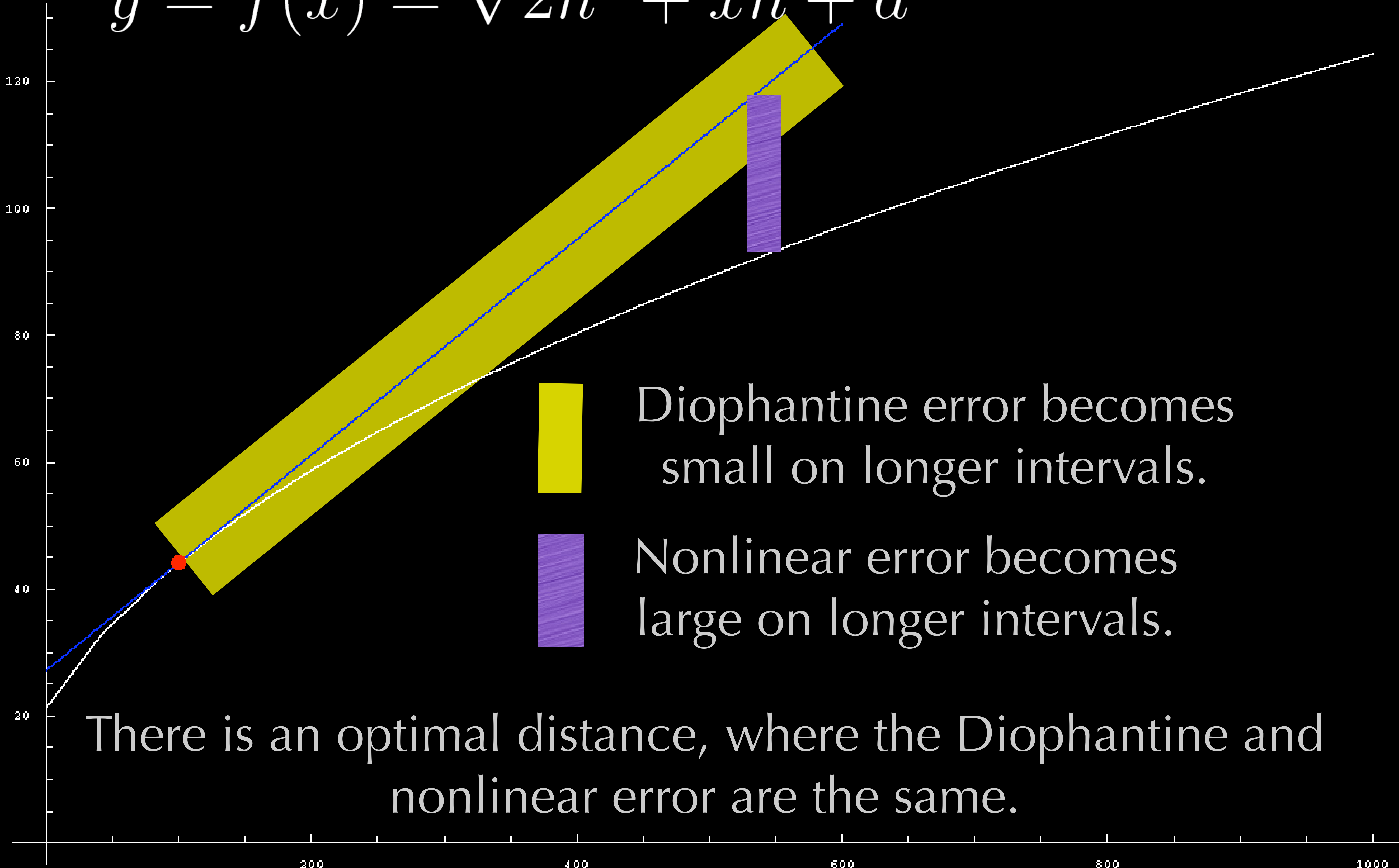
$$y^2 = 1 \bmod n$$

and $y - 1$ is a factor of n.

The goal is to find lattice points close to that curve.

Linear Approximation

$$y = f(x) = \sqrt{2n^2 + xn + a^2}$$



Diophantine error becomes small on longer intervals.

Nonlinear error becomes large on longer intervals.

There is an optimal distance, where the Diophantine and nonlinear error are the same.

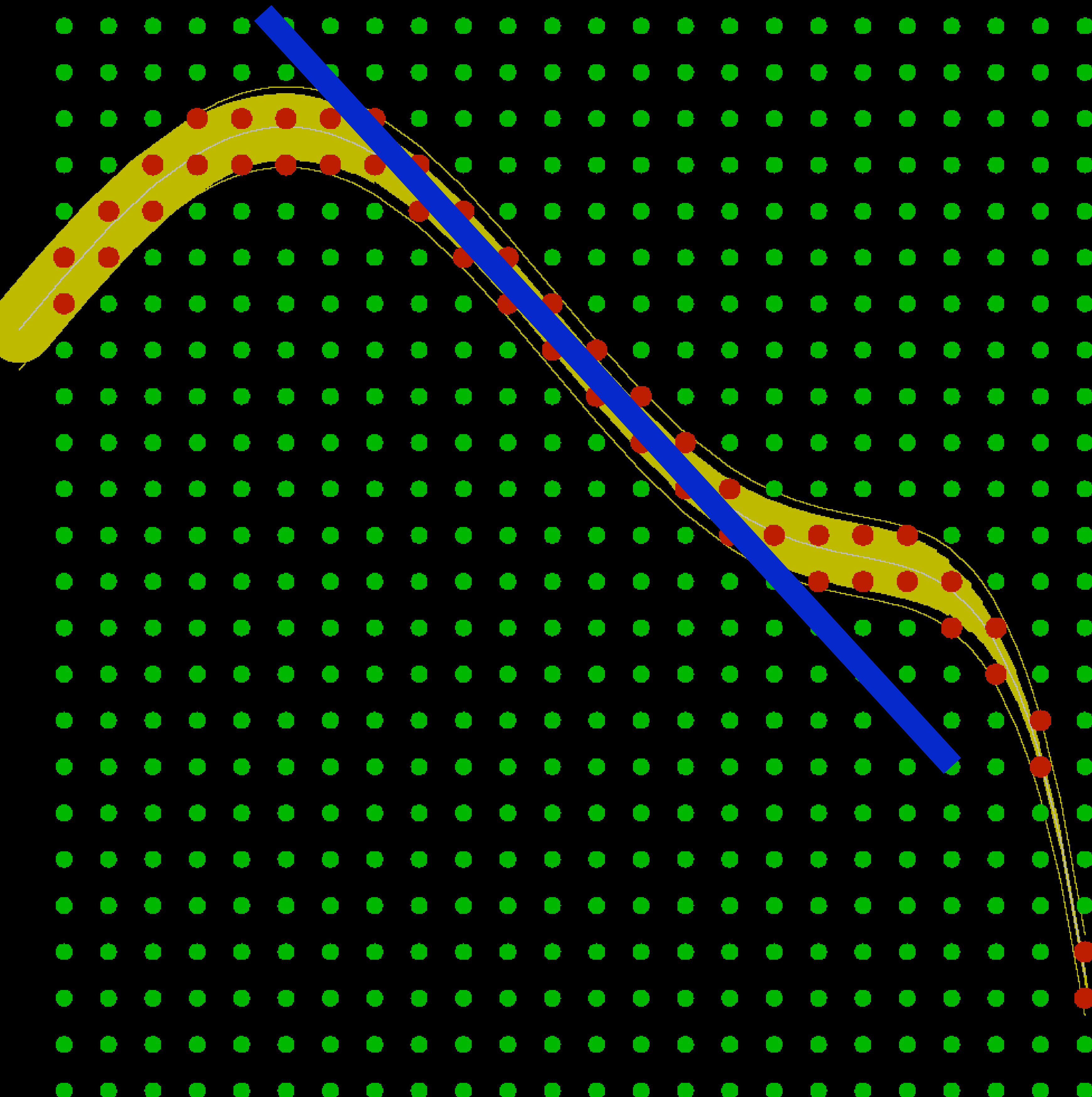
Estimate

$y = \sqrt{2n^2 + nx}$ has tangent at $(0, \sqrt{2n^2+1})$ with slope $1/\sqrt{8}$ which is stronly Diophantine.

- Diophantine error: $1/x$
- Nonlinearity error: $f''(0)x^2 = \frac{-1}{8\sqrt{2}} x^2/n$

Errors the same for $x = n^{1/3}$. There are lattice points in a $n^{-1/3}$ neighborhood. If $dy = O(n^{-1/3})$, then $dy^2 = O(nn^{-1/3}) = O(n^{2/3})$. The method generates squares of this order.

Are there better curves?

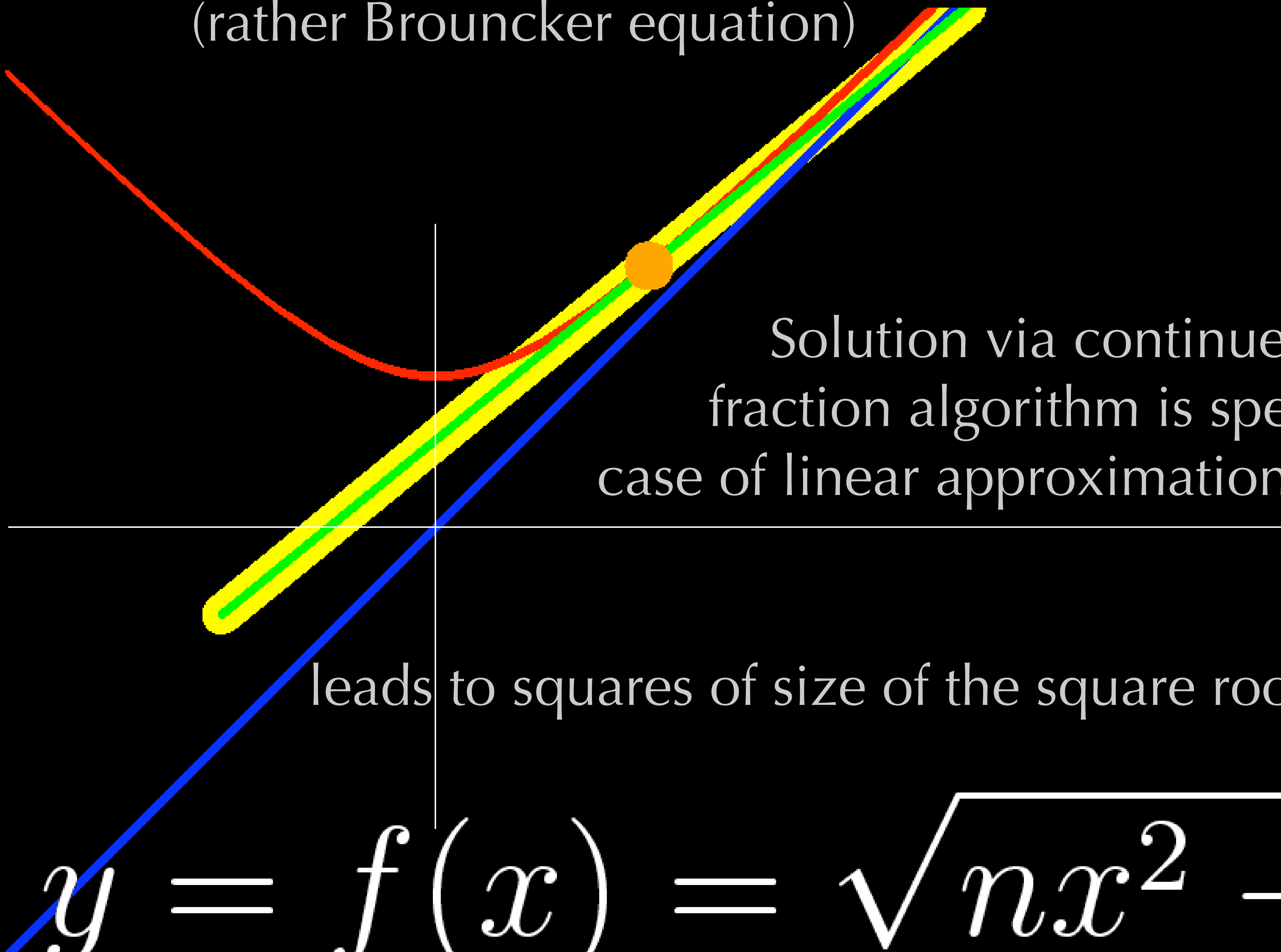


i.e near
inflection points

If factoring integers
is really
hard, we can not
expect to find good
curves.

Pell equation

(rather Brouncker equation)



Solution via continued fraction algorithm is special case of linear approximation method

leads to squares of size of the square root of n.

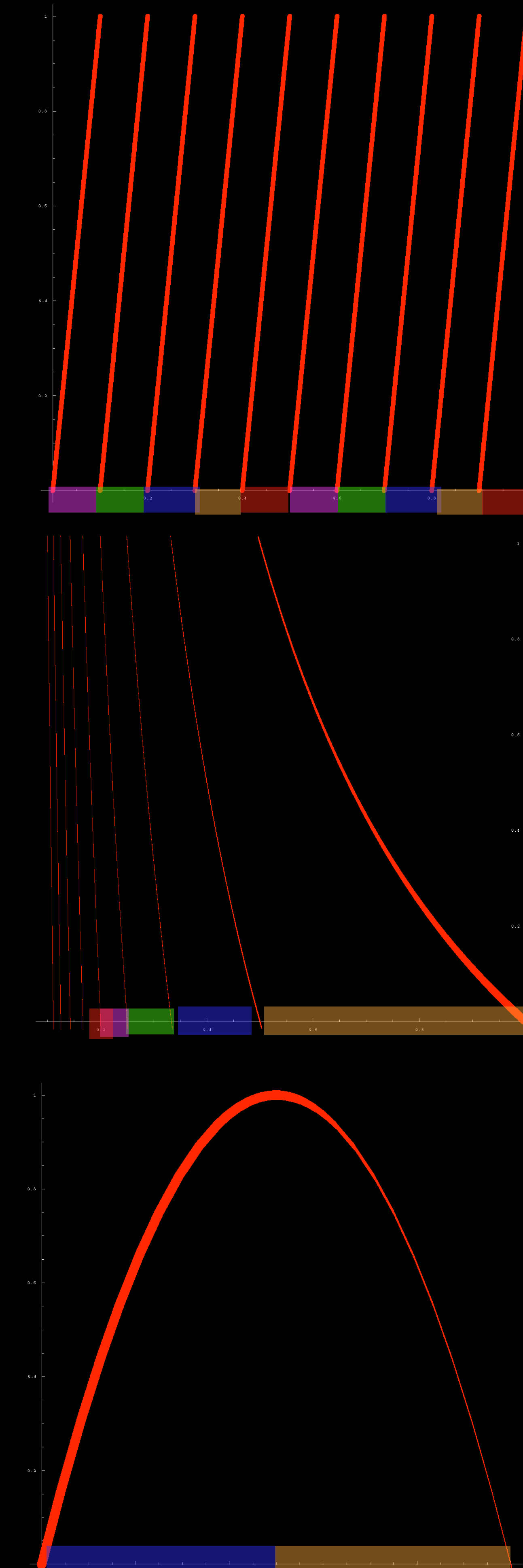
$$y = f(x) = \sqrt{nx^2 + 1}$$

Other relations between number theory and dynamical systems

Representation of numbers

Principle: T random map on [0,1]. A1,...,An partition. The itinerary or the orbit defines x.

- T(x) = 10 x mod 1,   decimal expansion
- T(x)= 1/x mod 1, continued fraction expansion
- T(x)=β x mod 1, β algorithm
- T(x)=4x(1-x) theory of 1D maps



Dynamical systems associated to a number

Take closure of all shifts of the itinery sequence to get a compact metric space of sequences. The shift defines a topological system. Can look at properties like

- minimality
- mixing
- entropy
- decay of correlations
- Koopman spectrum

$$\{x_n\}_{n=1}^{\infty} \in A^{\mathbf{N}}$$

$$T(x)_n = x_{n+1} \text{ shift}$$

$$X \text{ closure of } \{T^n(x)\}_{n=1}^{\infty}.$$

The quest for pi

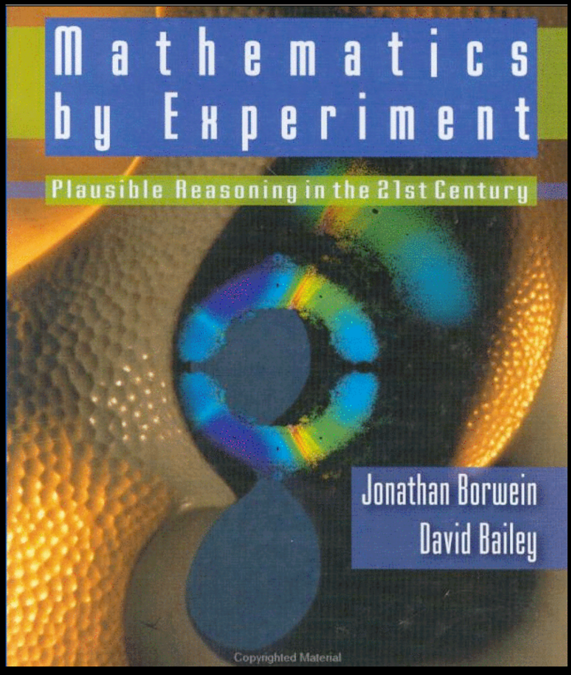
$$\begin{aligned}
x &= 31415926535897932384626433832795028\ldots \\
T(x) &= 14159265358979323846264338327950288\ldots \\
T^2(x) &= 41592653589793238462643383279502884\ldots \\
T^3(x) &= 15926535897932384626433832795028841\ldots \\
\ldots & \quad \ldots
\end{aligned}$$

Is the closure $X = \{0, ..., 9\}^{\mathbf{N}}$? Does the shift define a Bernoulli system on X?

Bayley,Borwein,Plouffe: If

$$x_n = 16x_{n-1} + \frac{120n^2 - 89n + 16}{512n^4 - 1024n^3 + 712n^2 - 206n + 21}$$

is equidistributed in $[0, 1]$, then π is 16-normal.



Popularizing the Riemann hypothesis

$$\mu(n) = \begin{cases} 0 & p^2 | n \\ (-1)^k & n = p_1 \cdots p_k. \end{cases}$$

$M(x) = \sum_{n \le x} \mu(n)$ Mertens function

$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$

$\mu(n)$ random: law of iterated logarithm

$$\limsup_{n \to \infty} \sum_{k=1}^{n} \frac{\mu(k)}{\sqrt{2n \log \log(n)}} \le 1$$

Riemann hypothesis

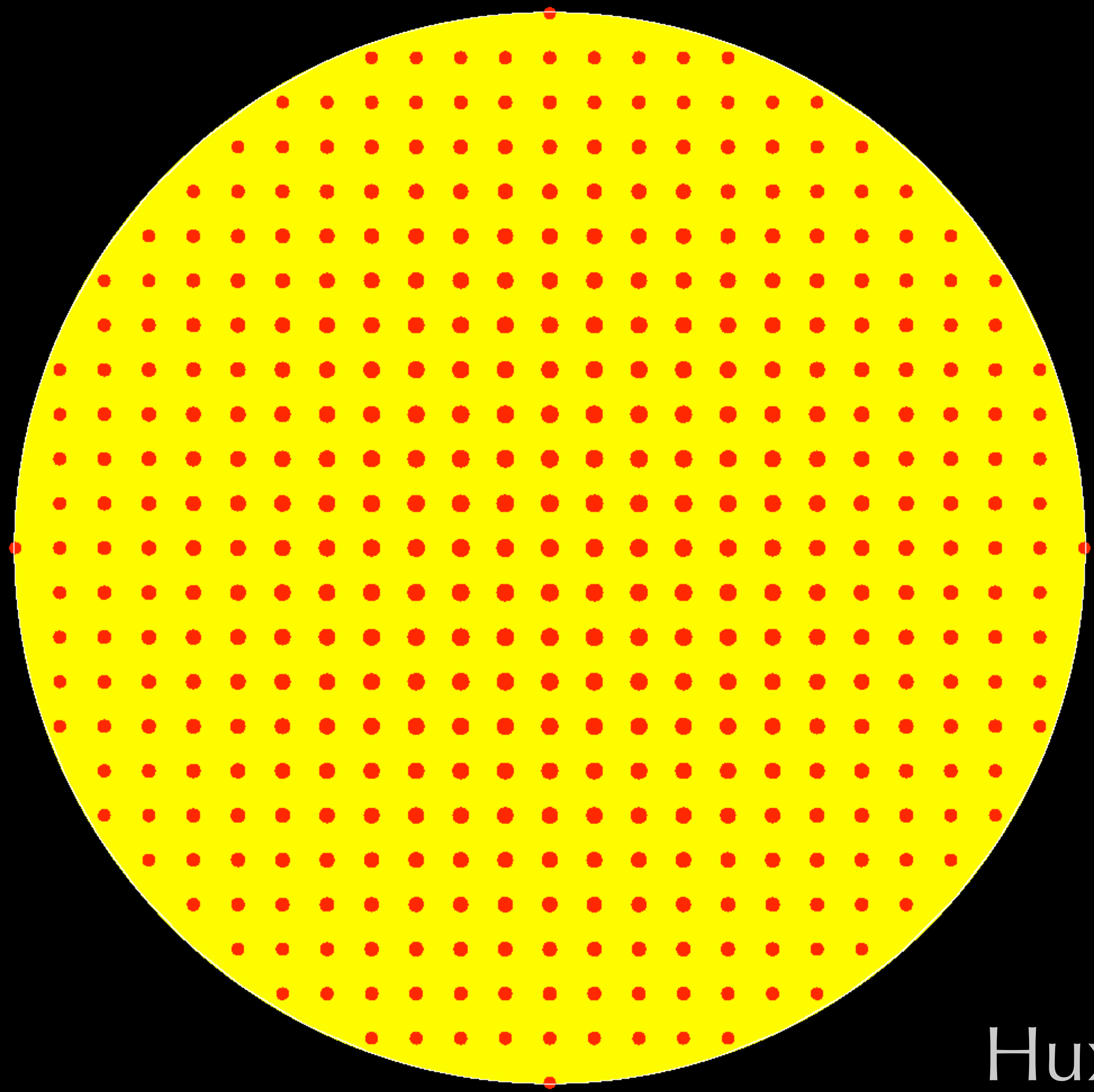
Show that the Moebius sequence is sufficiently random. Then the Riemann zeta function can not have zeros away from the line Re(z)=1/2.

Experiments indicate however that the Moebius sequence has correlations. The dynamical system is not Bernoulli. Nevertheless, the Riemann hypothesis can be seen as a problem on a specific dynamical system. The formulation:

Riemann hypothesis: $M(x) = O(x^{1/2+\epsilon})$ for every $\epsilon > 0$.

is often used when popularizing the problem. It allows to explain the problem without using complex numbers.

The
Gauss problem



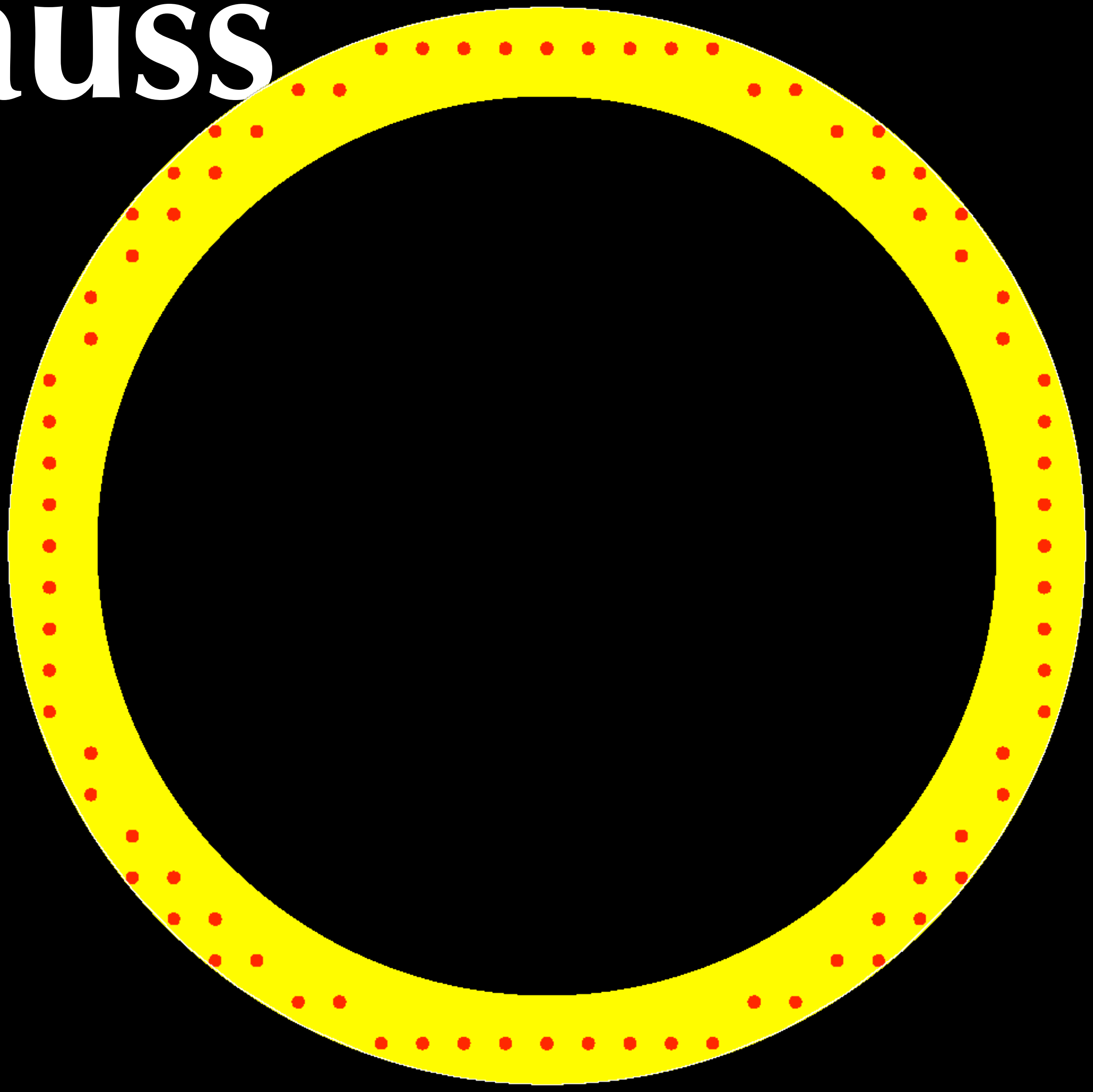
Gauss Circle Problem

Huxley: theta=46/74=0.64....

$$g(r) = \pi r^2 + E(r)$$

For $\theta > 1/2$, there is C such that $E(r) \leq C r^\theta$

What does Gauss problem tell about boundary?



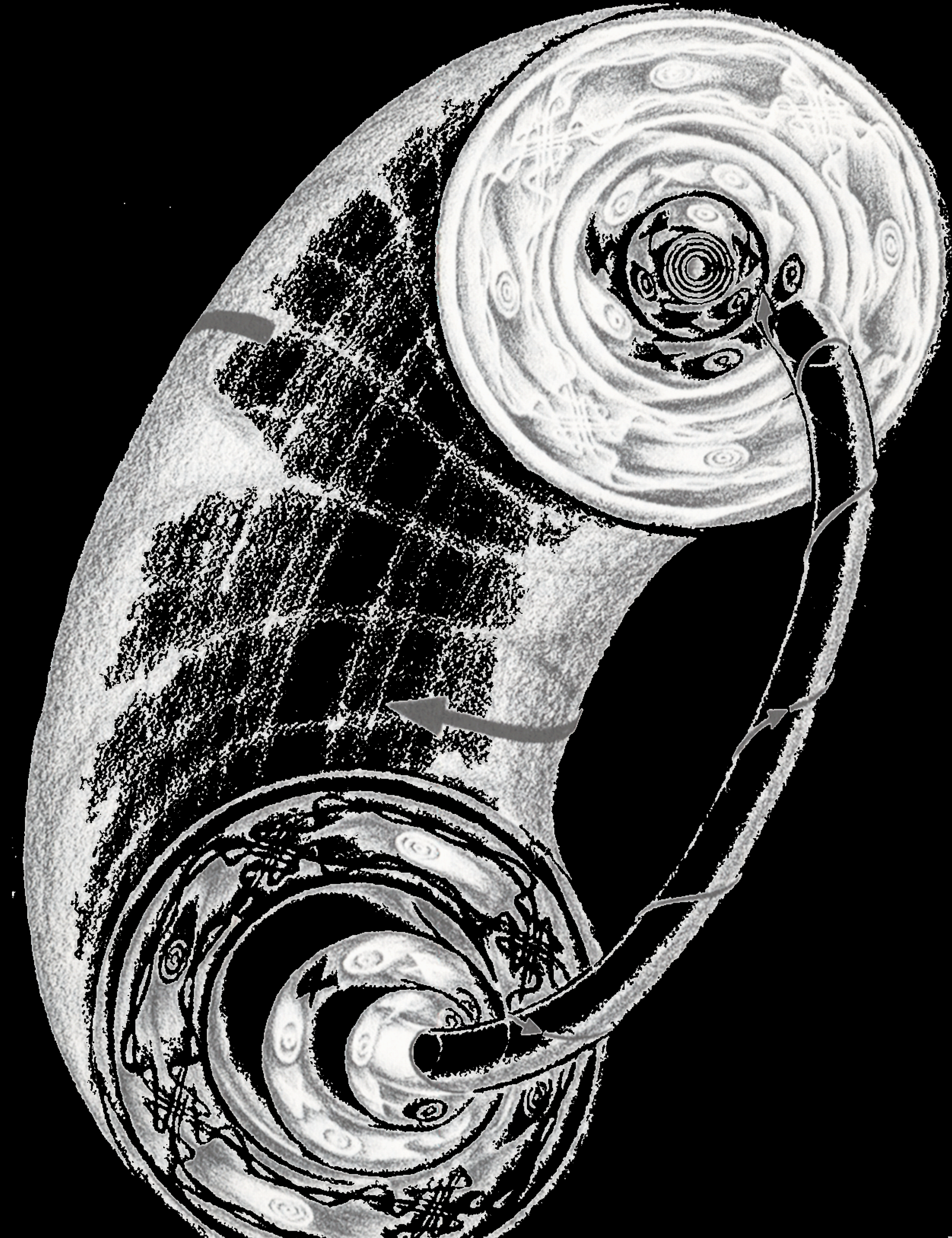
Heuristics:

Assume Gauss lattice problem:

$$g(n+\frac{1}{n^\theta})-g(n-\frac{1}{n^\theta}) = \pi(n+\frac{1}{n^\theta})^2-\pi(n-\frac{1}{n^\theta})^2+O(n^\epsilon) = 4\pi n^{1-\theta}+O(n^\epsilon) \ .$$

For $\theta < 1/2$, that there are $O(n^{1-\theta})$ lattice points in $n^{-\theta}$ neighborhood.

Perturbation theory



- persistence of invariant KAM tori.
- conjugation of dynamical systems to its linearization.
- strong implicit function theorem.

(Image source: R. Abraham and J. Marsden, 1978)

Figure 8.3-3. The VAK, according to Arnold [1963b].

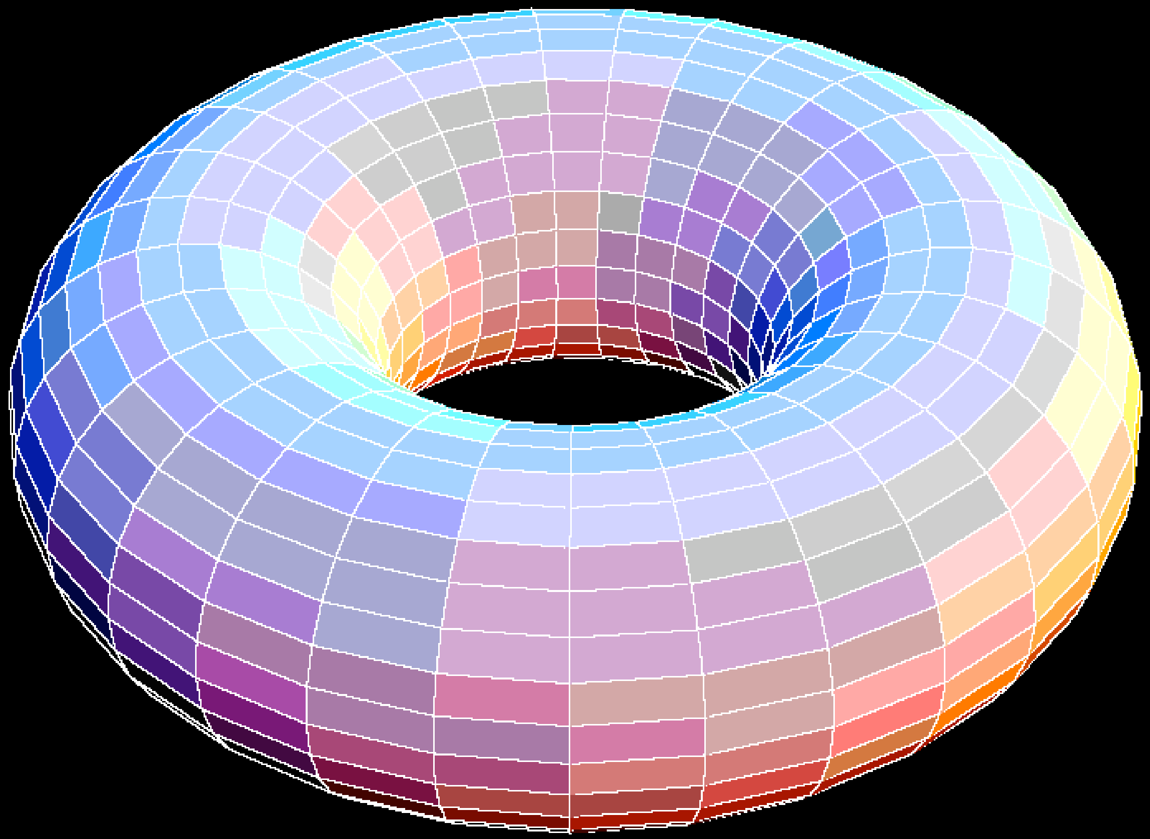
Spectral Theory of flows

$\int_X f(x)f(T^t x)\ dx = (f, U^t f) = \hat{\mu}_f(t)$ spectral measures.

Hof-Knill: If a flow T_t admits a cyclic approximation with speed $g(u) = o(u^{-r})$, then every spectral measure of the flow is supported on set of Hausdorff dimension $\leq 2/(r+1)$.

Katok: flow under function f with rotation number α. If $q_n^4|\alpha - \frac{p_n}{q_n}| = o(q_n^{-\tau})$, then flow admits cyclic approximation with speed $g(u) = o(u^{-2-\tau})$.

Differential equations

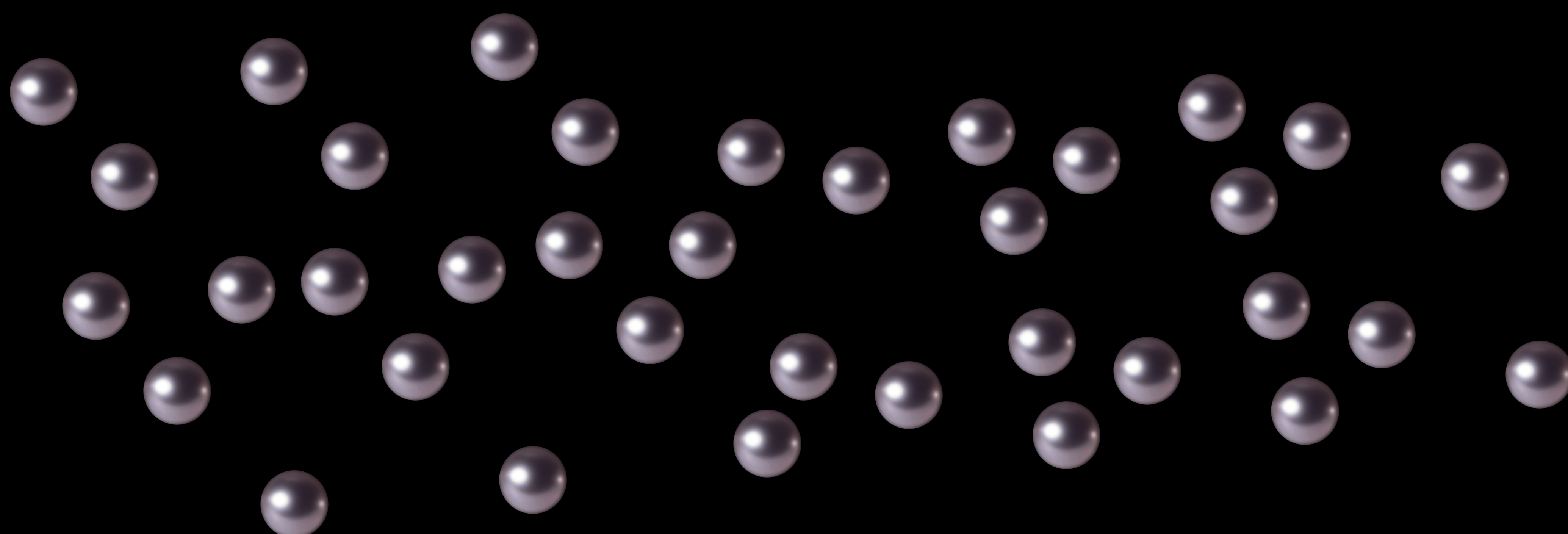


Flow on $\mathbf{T}^2 := \mathbf{R}^2/\mathbf{Z}^2$ given by differential equation

$$\frac{dx}{dt} = \frac{1}{F(x,y)}, \qquad \frac{dy}{dt} = \frac{1}{\lambda F(x,y)}.$$

generically has zero dimensional spectrum.

Almost periodic Sphere packings



Packing defined by an interval I on the circle and two irrational rotations. Take a lattice point as as center of a sphere, if n a + m b is in I, otherwise, dont.

Recurrence

Van der Waerden theorem (1927): If Z is partitioned into finitely many sets $B_1, ..., B_q$, then one of those sets contains arbitrary large arithmetic sequences.

Multiple Birkhoff recurrence theorem by Furstenberg: For any topological system $(X, T_1, ..., T_l)$ with time Z^l, there exists a multiple recurrent $x \in X$. (Exists sequence $n_k \to \infty$ with $T_1^{n_k}(x) \to x, ..., T_l^{n_k}(x) \to x$.)

Proof of Van der Waerden: For every l, there exists a set B_l which contains arithmetic sequence of length l: take $X = \{1, ..., q\}^Z$ and $T_1(x)_n = x_{n+1}, T_2(x) = x_{n+2}, ..., T_l(x) = x_{n+l}$.

Diophantine properties

Diophantine condition

$\exists \epsilon > 0, C > 0$ such that

$$||n \cdot \alpha|| \geq C|n|^{-d-\epsilon}$$

for all $n = (n_1, ..., n_d)$.

Diophantine: Diophantine condition for all $\epsilon > 0$. (Full measure.)

Strongly Diophantine: Diophantine condition for $\epsilon = 0$. (Zero measure).

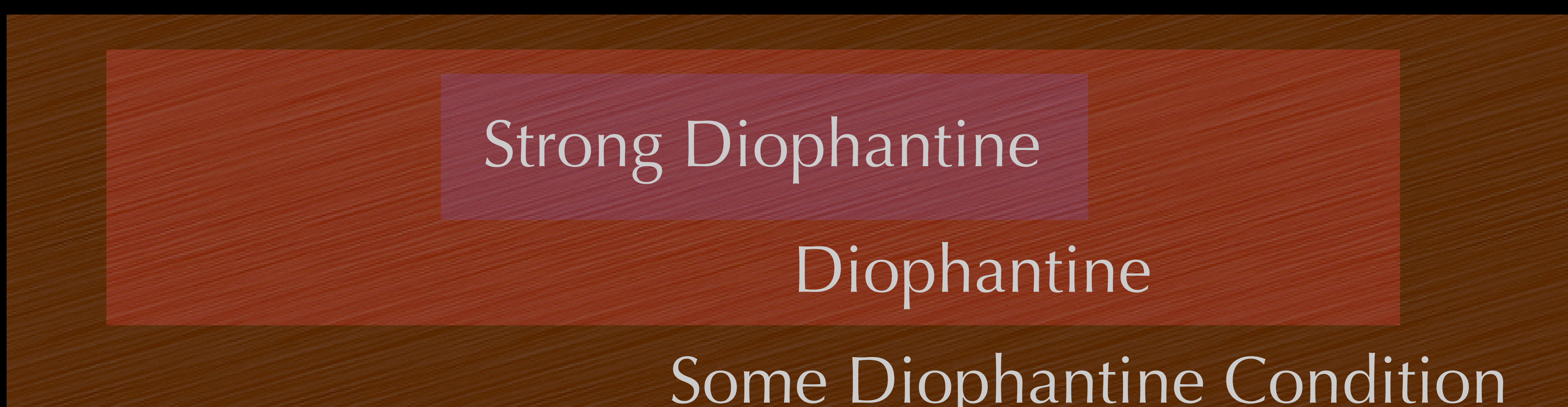
Diophantine vectors

The least upper bound of $\delta > 0$ such that

$$||a\alpha + b\beta|| \leq [\max(a,b)]^{-\delta}$$

has infinitely many solutions is $\delta = 2$.

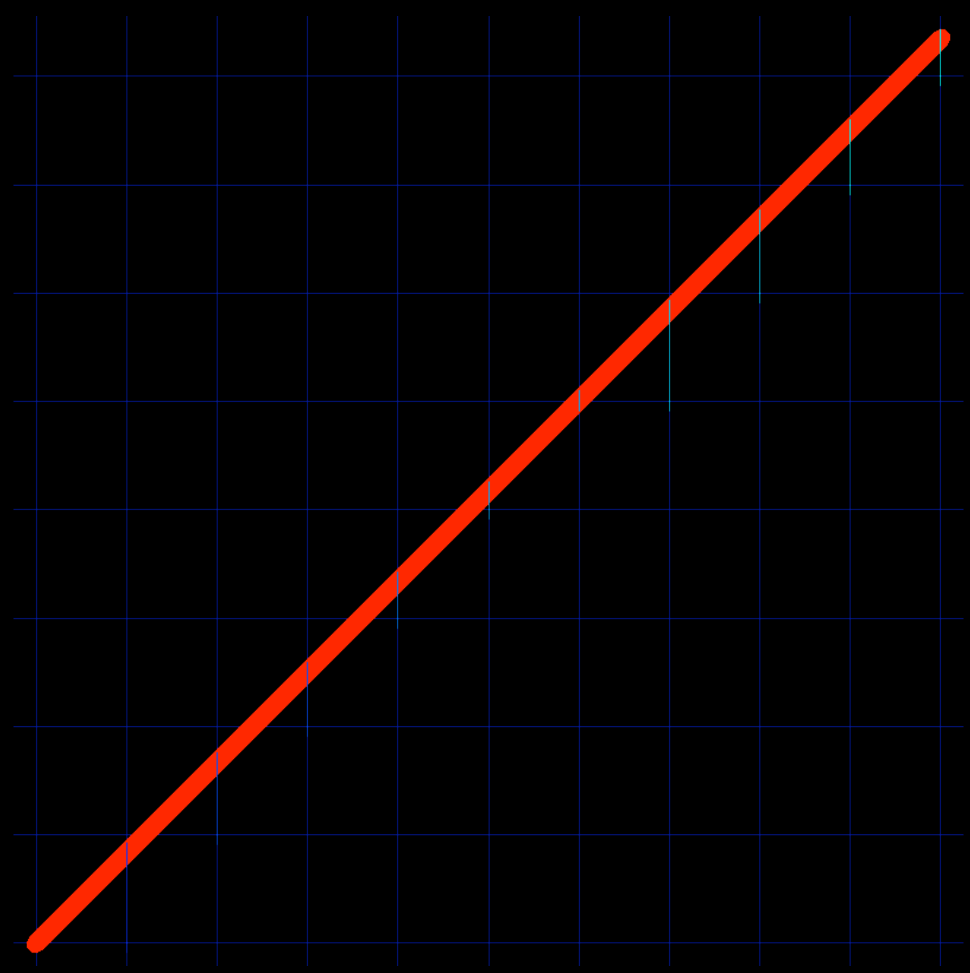
($||x||$ is distance to $\mathbf{Z}$)



Liouville slope

for all m there are irreducible fractions p_n/q_n

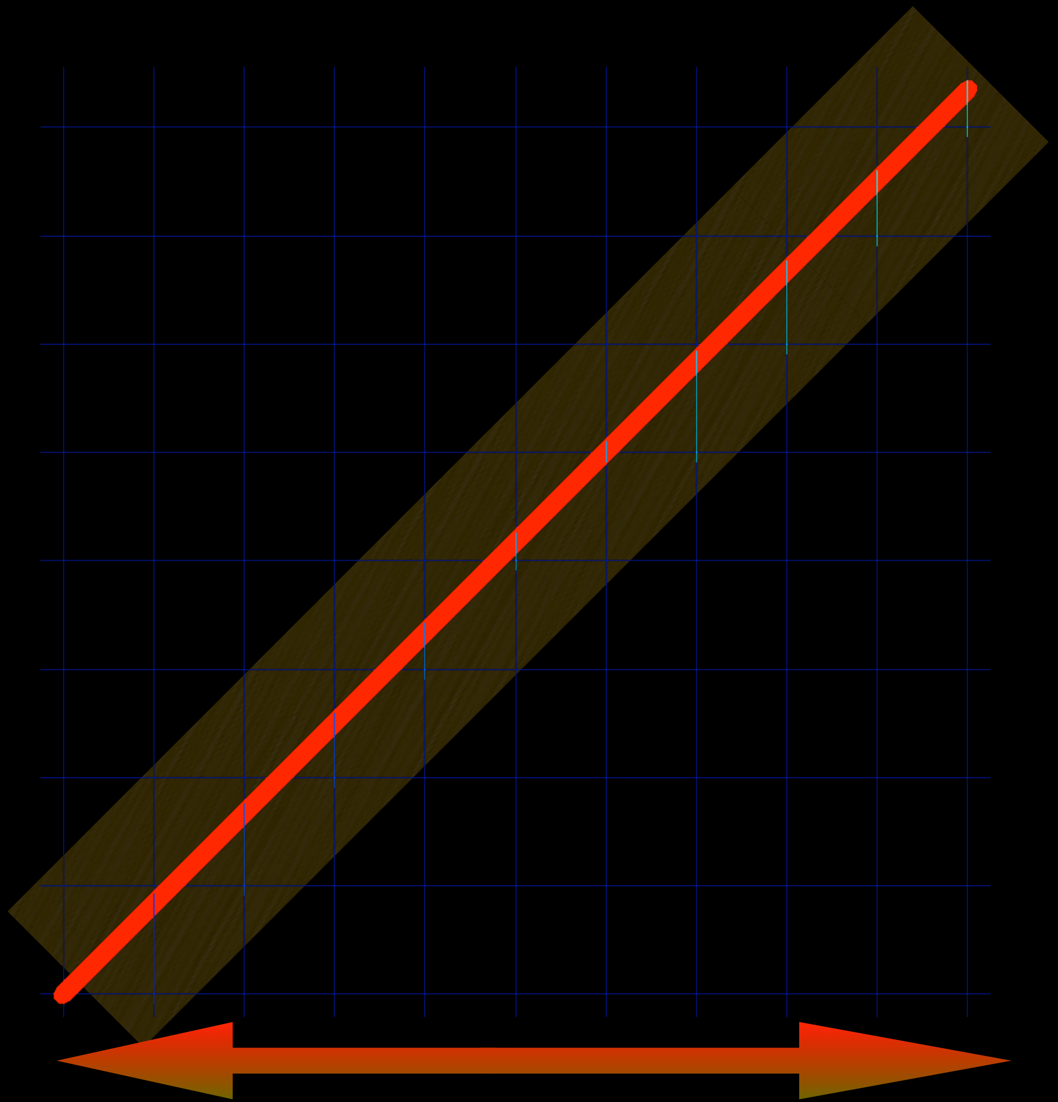
$$q_n^m \cdot |\alpha - \frac{p_n}{q_n}| \to 0$$



"close to rational slope"

Strong Diophantine slope

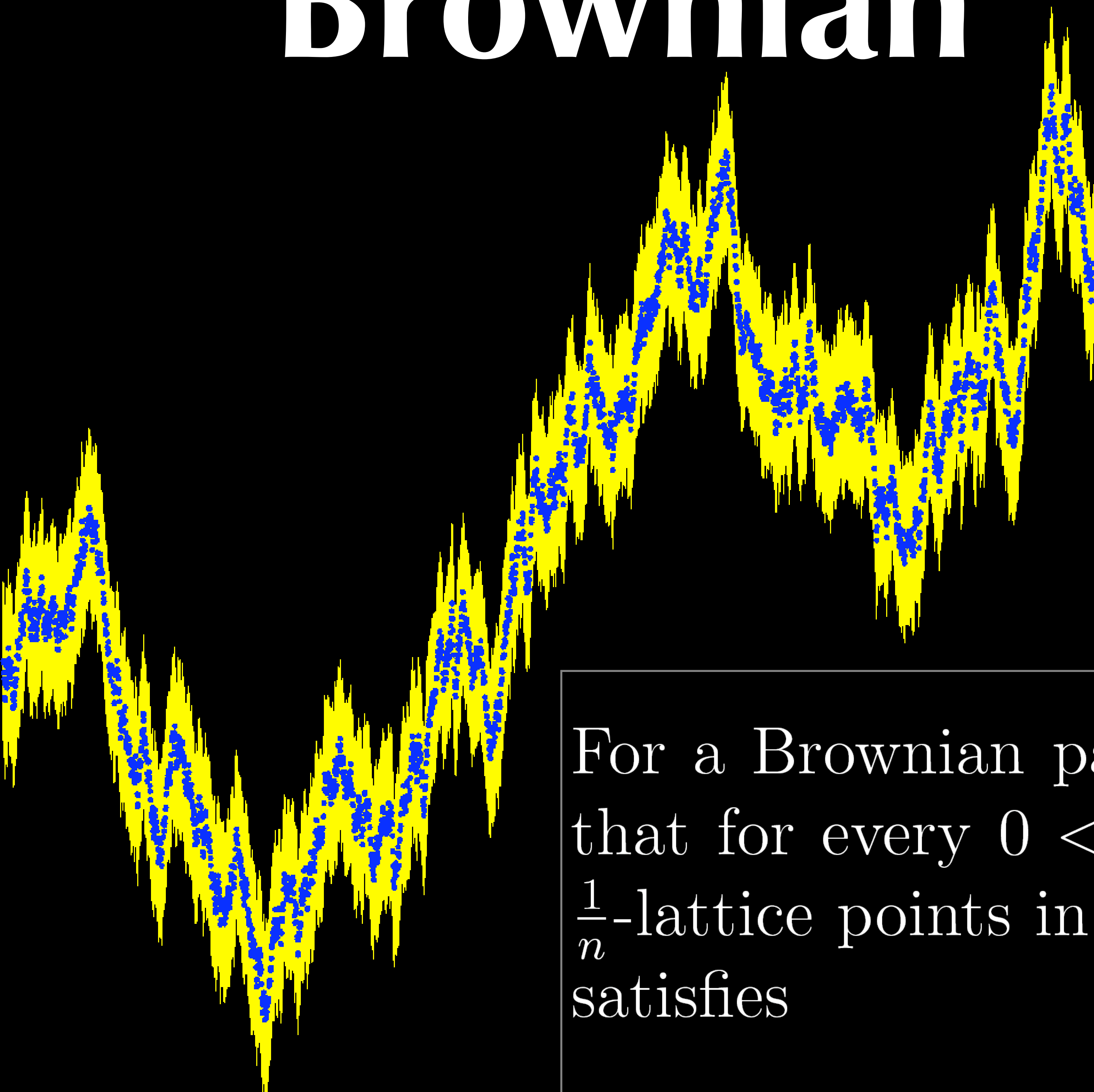
Strong Diophantine condition: have bounded continued fraction expansion.



Curve of length Cn has a lattice point in 1/n neighborhood

A random version of the curve approximation result.

Lattice points near Brownian paths



For a Brownian path, there is a constant C such that for every $0 < \delta < 1$, the number $M(n,\delta)$ of $\frac{1}{n}$-lattice points in a $\frac{1}{n^{1+\delta}}$-neighborhood (in $C(R)$) satisfies

$$\frac{M(n,\delta)}{n^{1-\delta}} \to C$$

Corollary in metric theory of Diophantine approximation.

Known in that theory (see Sprindzuk 1969):

Brownian paths are extremal: for almost all x, the vector (x,B(x)) is Diophantine.

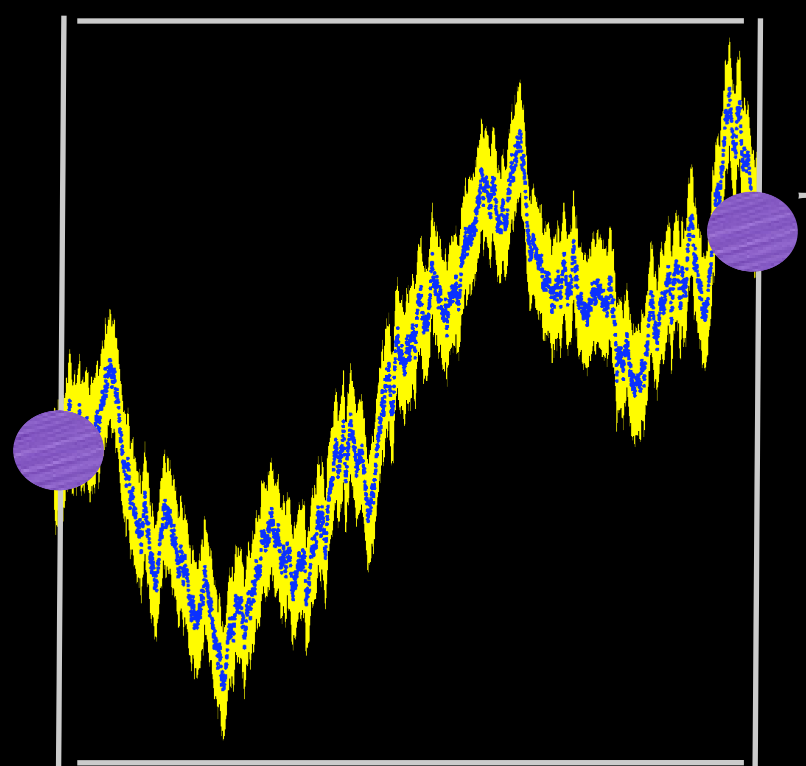
Analogue ergodic result:

$T : [0,1] \to [0,1]$ random such that $\int xT^n(x)\,dx - 1/4$ decays exponentially fast.

Given $\delta \in (0,1)$, define $A_n = [0, 1/n^\delta]$. For all $x \in [0,1]$,

$$\lim_{n\to\infty} \frac{1}{n^{1-\delta}} \sum_{k=1}^{n} 1_{A_n}(T^k(x)) \to 1\,.$$

A map associated to Brownian motion



T has strong decay of correlations.

Largers powers of the "Poincare return map" of Brownian motion with respect to a 1/n lattice will look like a Bernoulli system

A Brownian path defines a sequence x of consecutive distances to 1/n lattice. The closure of this sequence defines a compact set on which the shift map acts.

$X_k(x) = 1_{[0,\frac{1}{n^\delta}]}(T^k x)$ IID, mean: $p = \frac{1}{n^\delta}$ and variance: $p(1-p)$.
$S_n(x) = \sum_{k=1}^{n)} X_k(x)$ with mean $np = n^{1-\delta}$ and variance $np(1-p) = n^{1-\delta}(1-p)$. Given $\epsilon > 0$, the sets

$$B_n = \{|\frac{S_n(x)}{n^{1-\delta}} - 1| > \epsilon\}$$

have by the Tchebychev inequality

$$|B_n| \leq \frac{\mathrm{Var}[S_n/n^{1-\delta}]}{\epsilon^2} = \frac{\mathrm{Var}[S_n]}{n^{2-2\delta}\epsilon^2} = \frac{1-p}{\epsilon^2 n^{1-\delta}} \; .$$

For $\delta < 1$, this goes to 0. Borel-Cantelli implies for $\kappa > 1+\delta$ from $\sum_n |B_{n^\kappa}| < \infty$ that $|\limsup_n B_{n^\kappa}| = 0$. But this implies (...) that almost surely, no x is in infinitely many B_n.