Dynamical Systems and Number Theory

Oliver Knill,

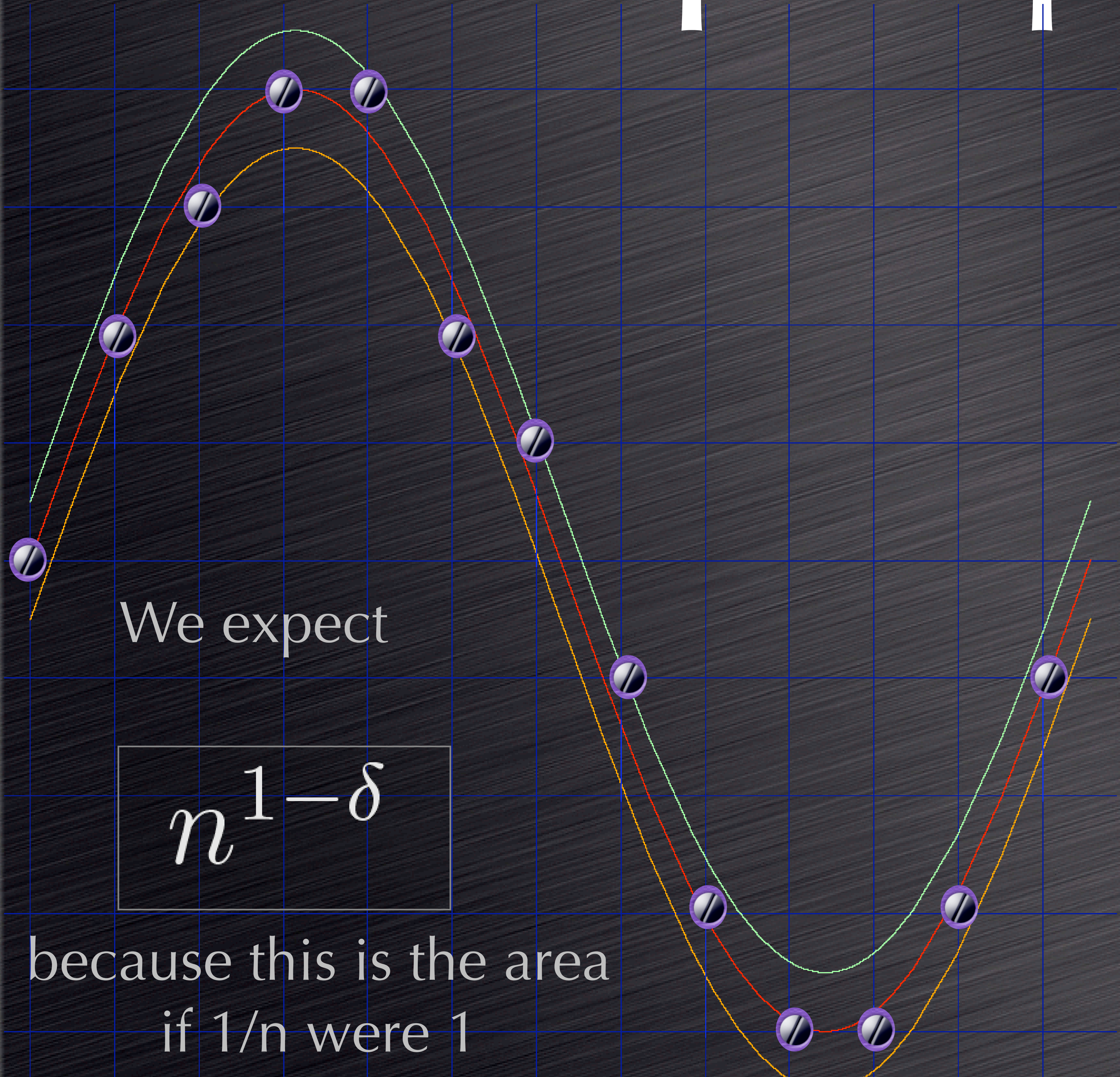
November 5, 2004

Abstract

- We discuss first a theorem in the metric theory of Diophantine approximation and its relation with an ergodic theorem which applies for certain dynamical systems.
- In the second part, we look at dynamical systems associated to real numbers as well as the relevance of number theory in perturbation theory or combinatorics.

A result on lattice points near curves

A lattice point problem



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

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.

More is known (Schmidt 1964)

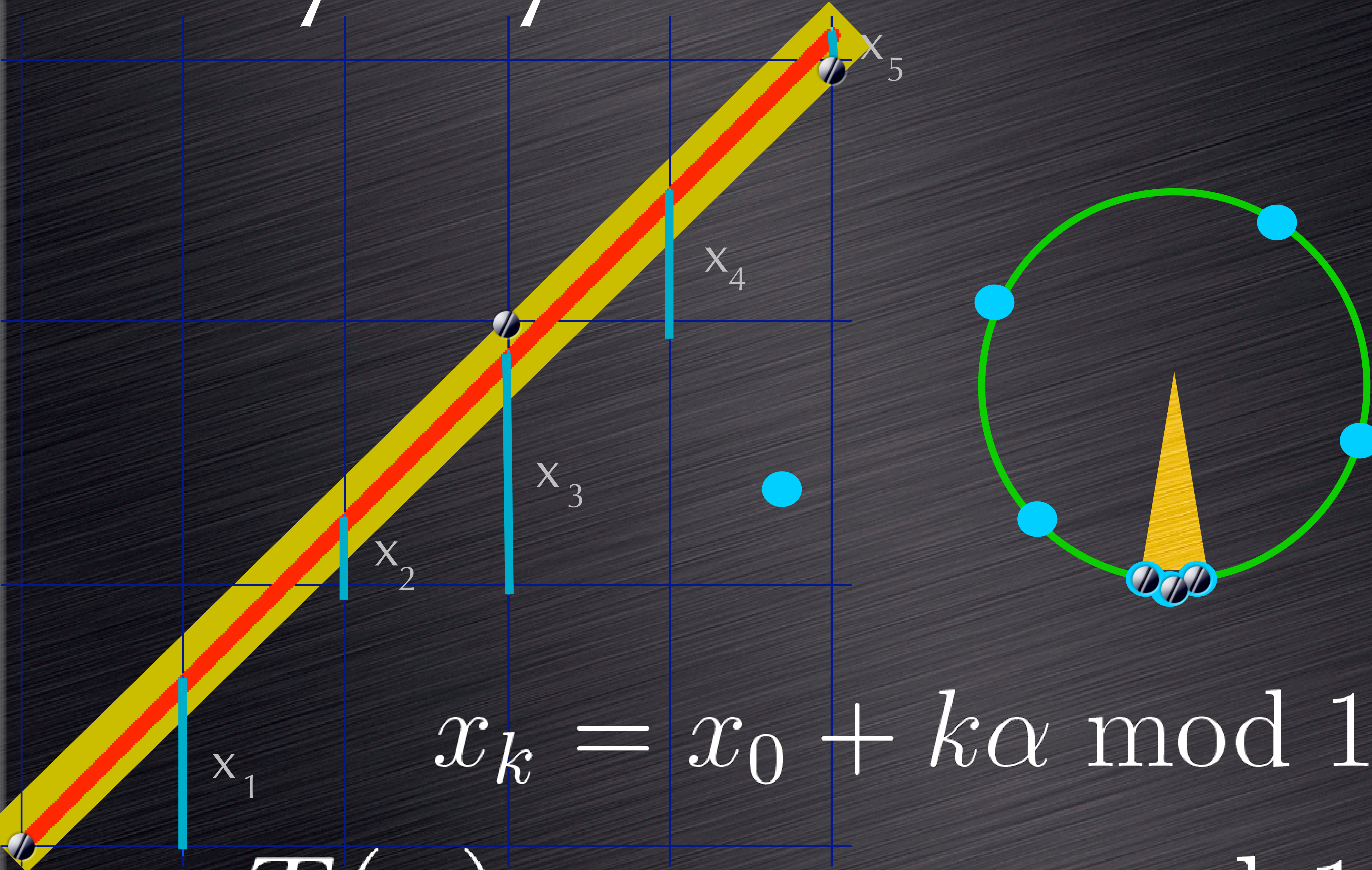
upper bound estimates work until 1/2 and imply:

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.

- this is a prototype result in the metric theory of Diophantine approximation.
- there are generalizations to surfaces.

Relation with dynamical system theory

Dyn.Sys. from Line

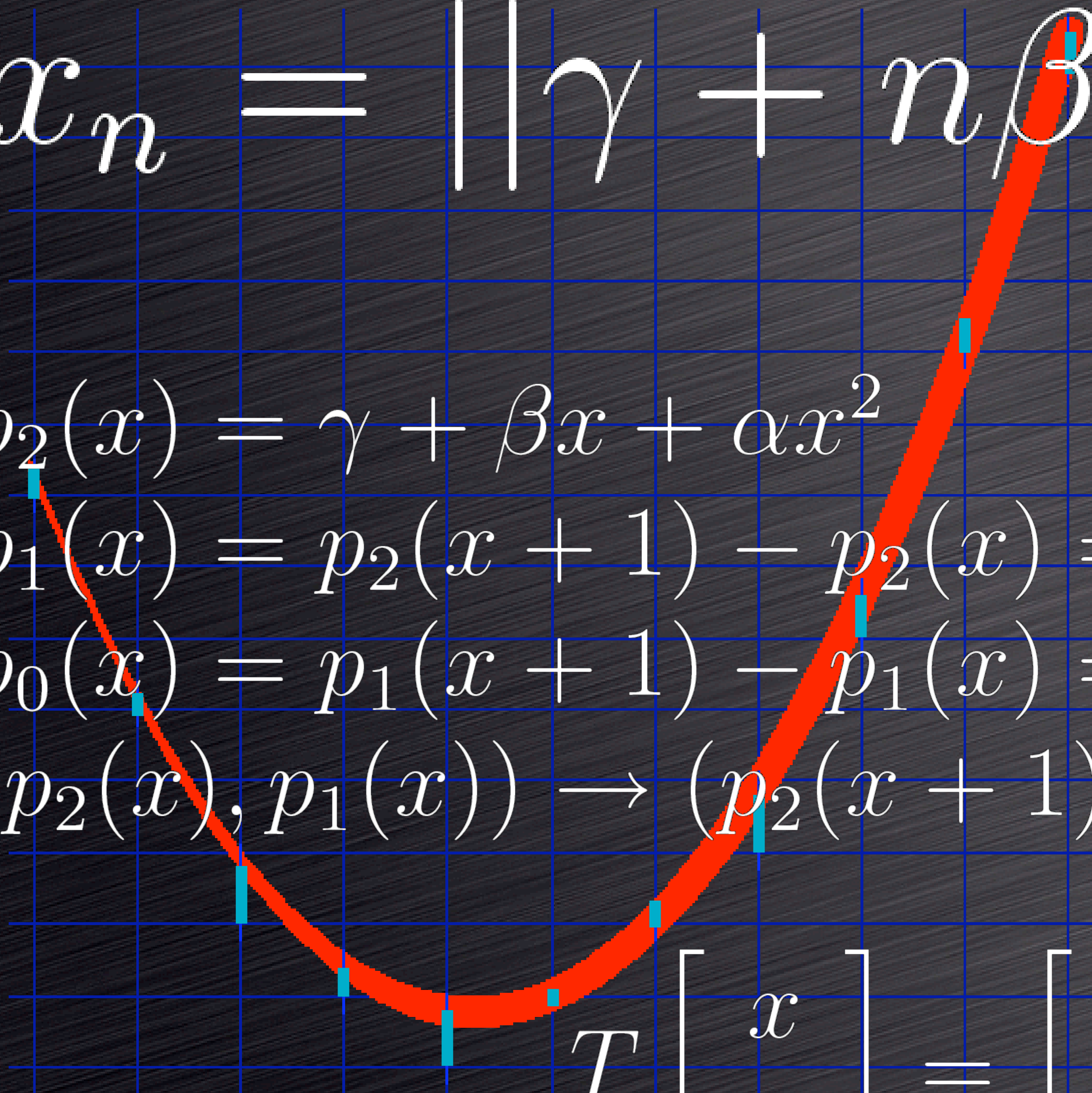


$$x_k = x_0 + k\alpha \bmod 1$$

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

The Parabola

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



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

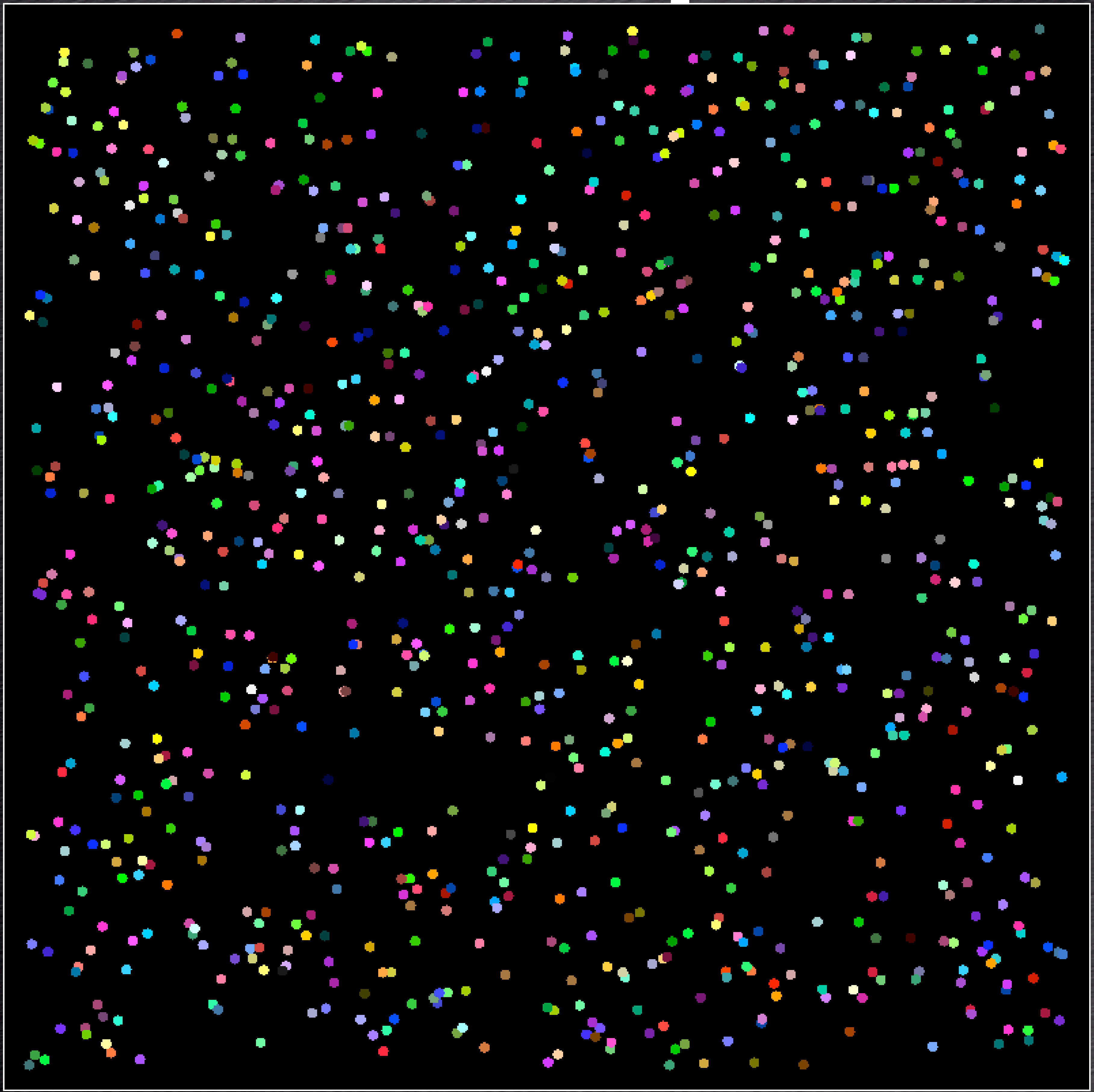
$$p_1(x) = p_2(x+1) - p_2(x) = \alpha + \beta + 2\alpha x$$

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

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

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

Parabolic Sequences



Zoo of dynamical systems

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

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

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

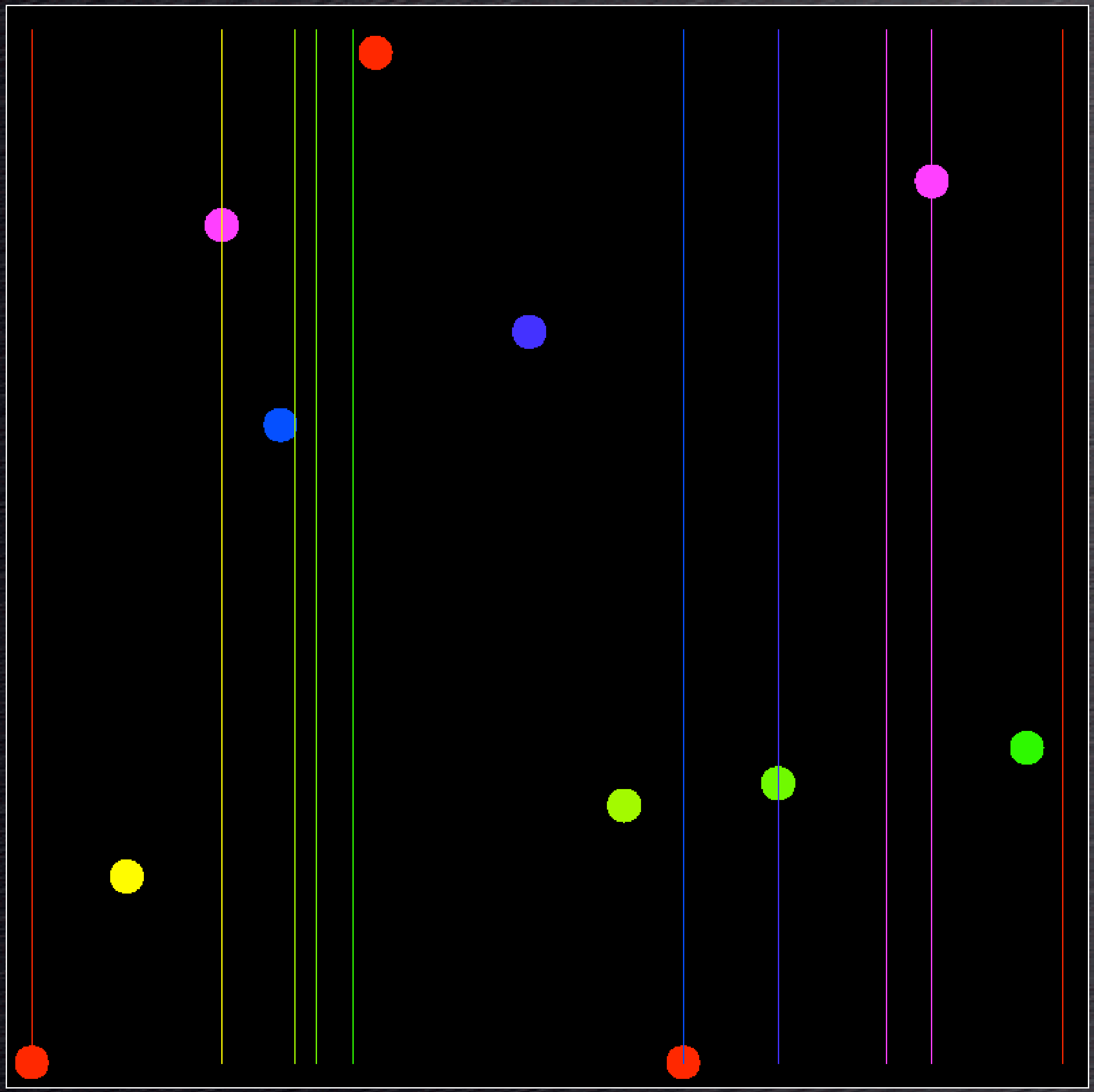
$T(x,y)=(2x+y+4\sin(x),x)$

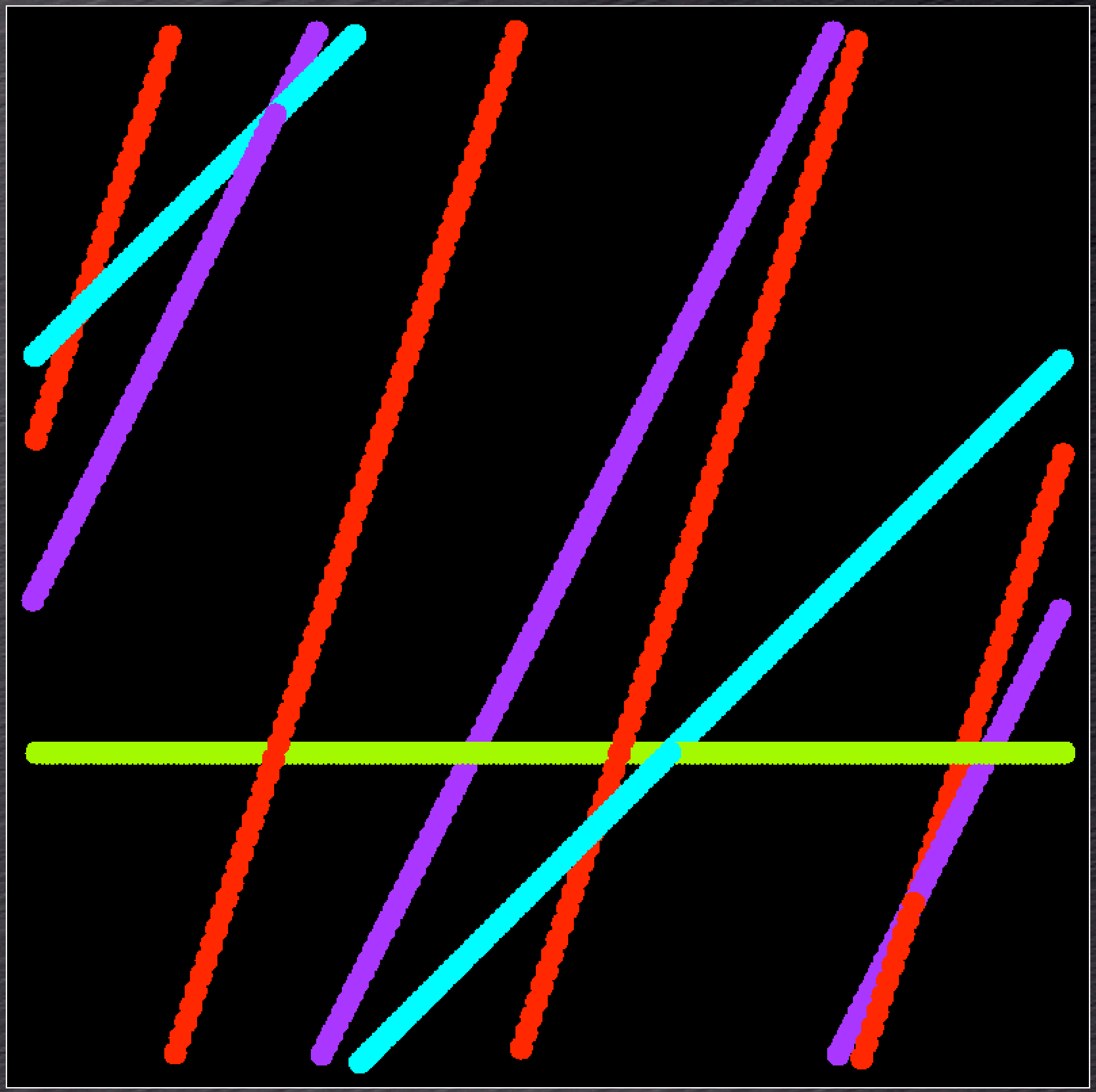
$T(x,y)=(2x+y,x+y)$

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)

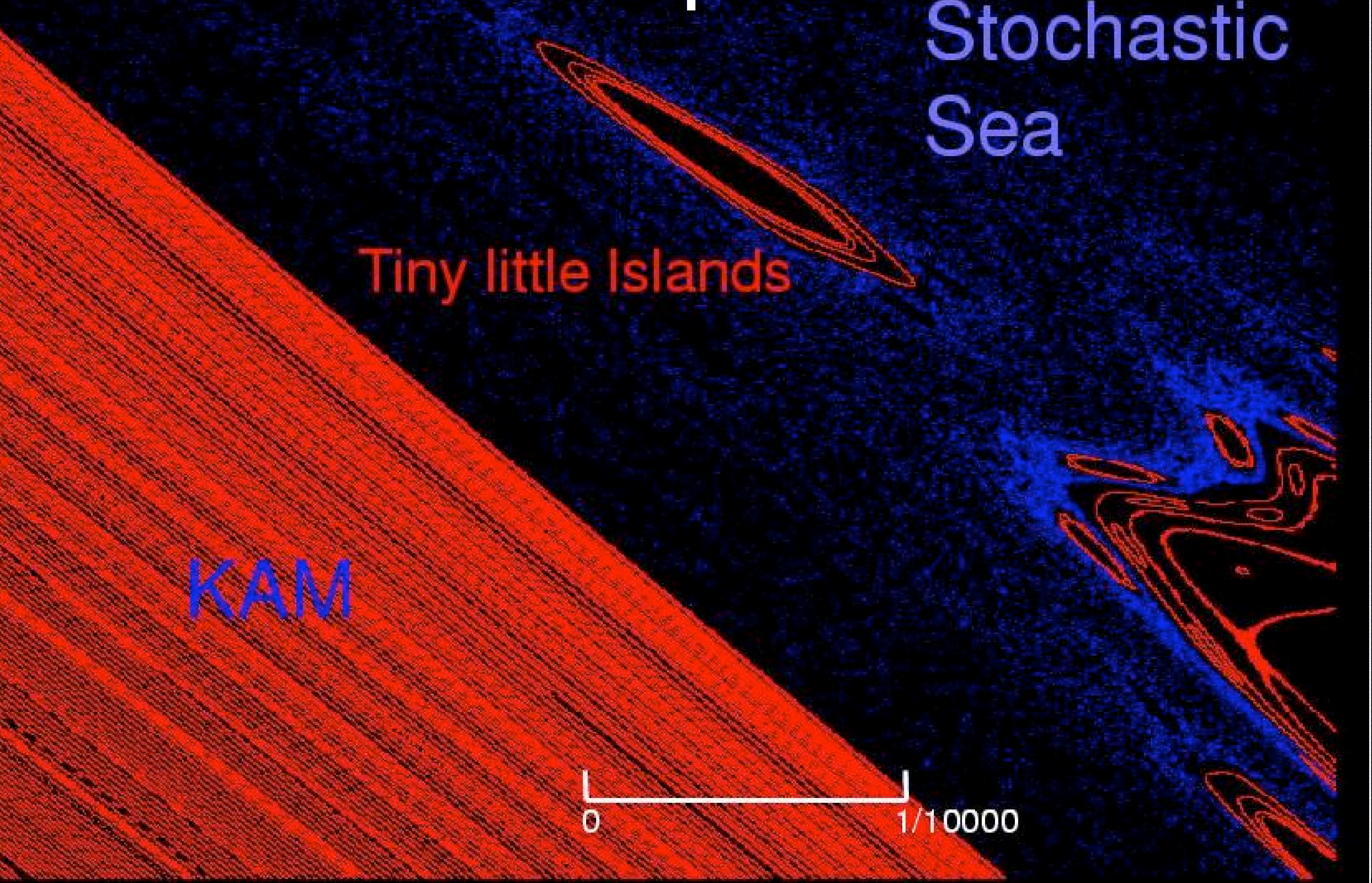
Integrable and mixing





A different type of stable/unstable behavior

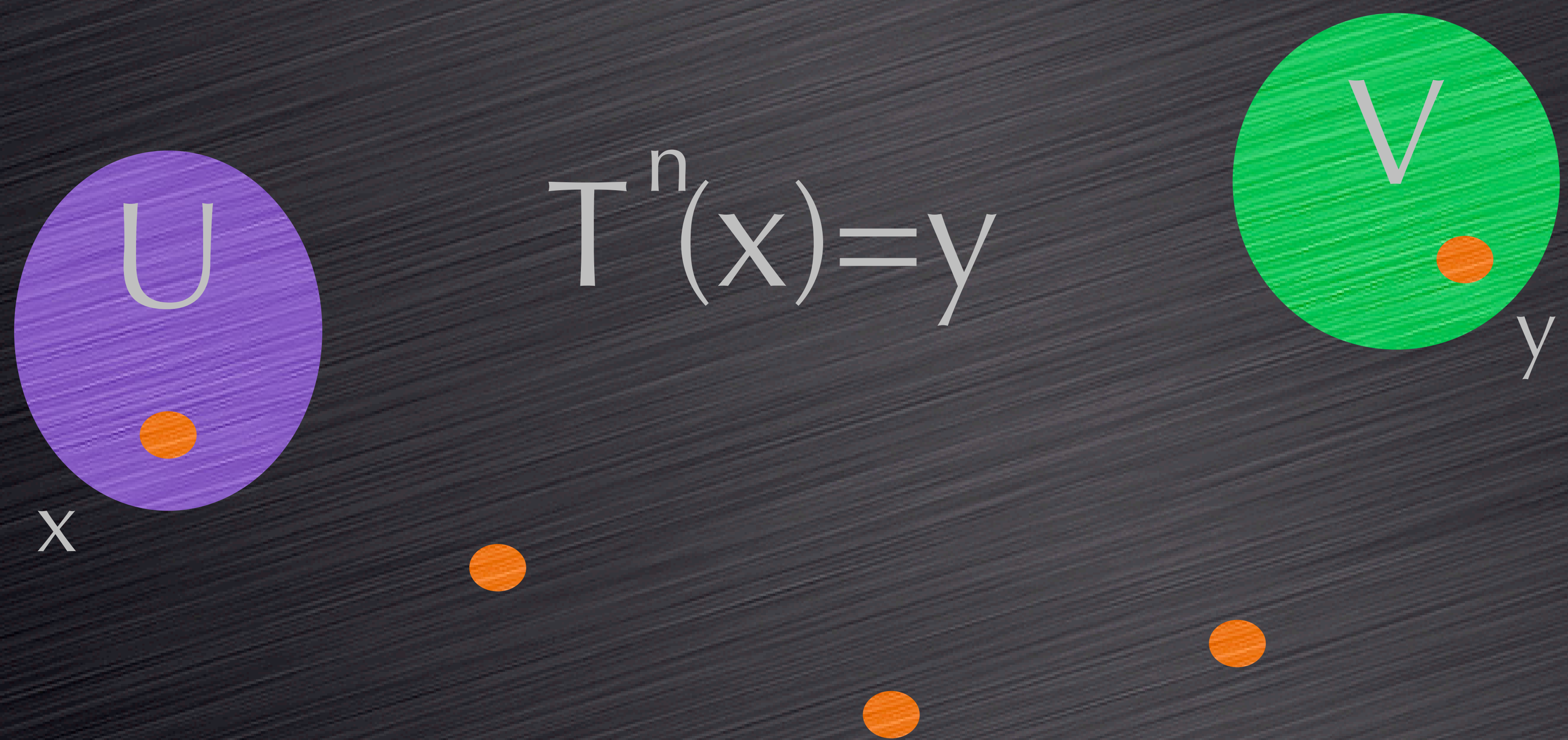
The Phase space



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

Usefulness of dyn log

- 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

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).

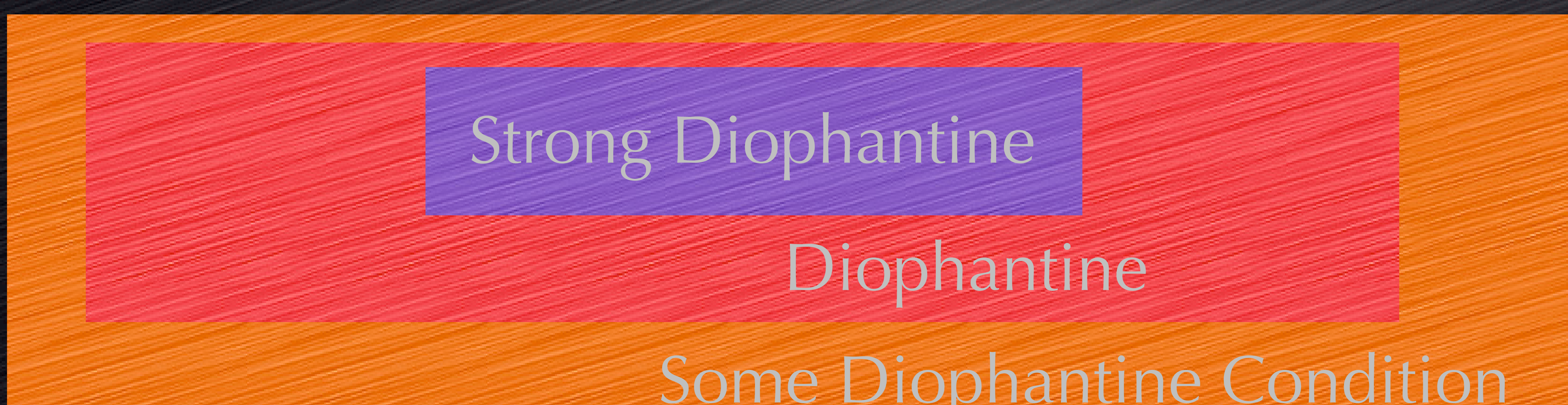
Diophantine vectors

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

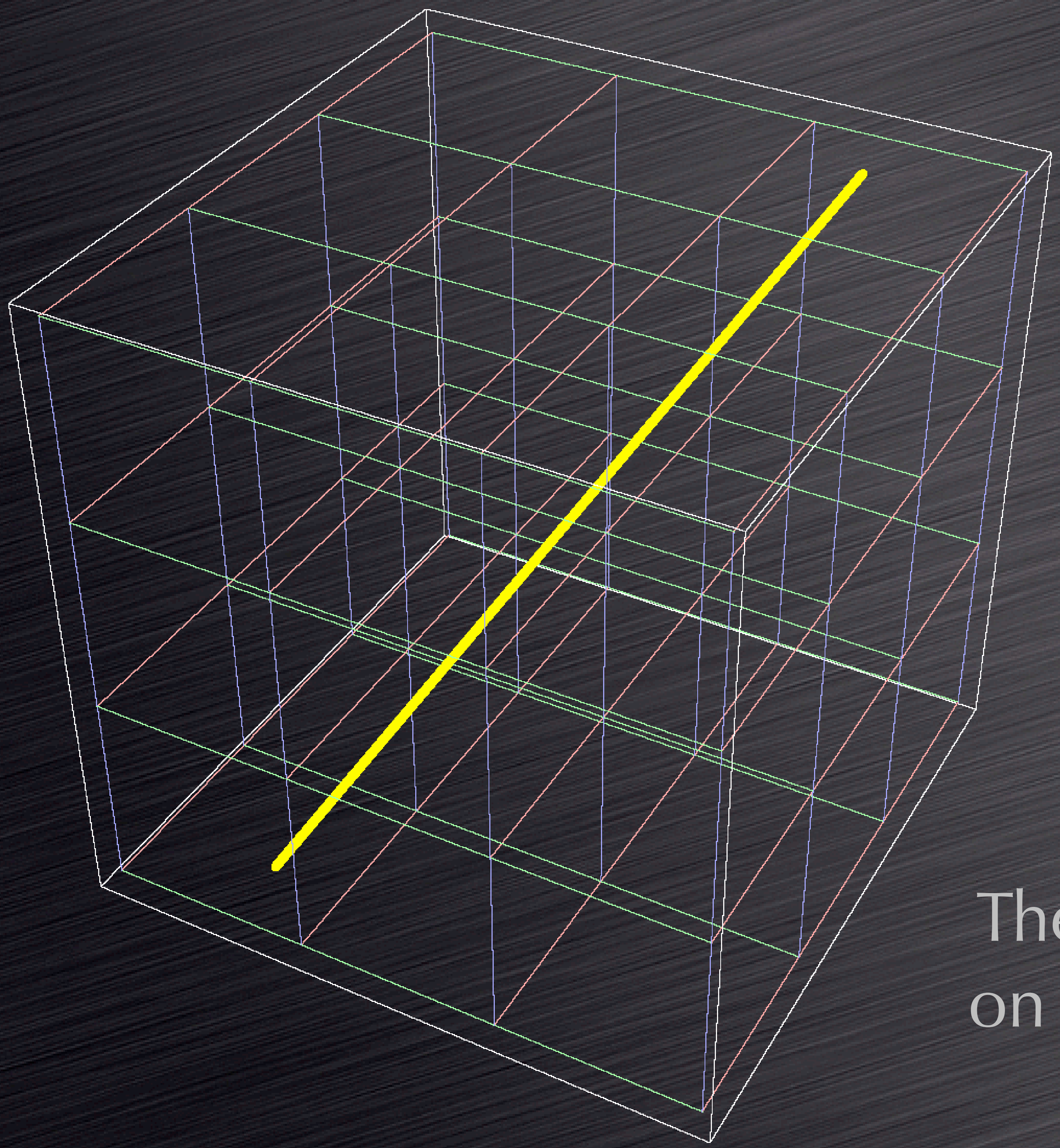
$$||a\alpha + b\beta|| \leq [\max(a,b)]^{-\delta}$$

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

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



Diophantine Slopes



produce extremal lines in the plane or in space.

The corresponding systems on tori are translations with Diophantine vectors.

Liouville slope

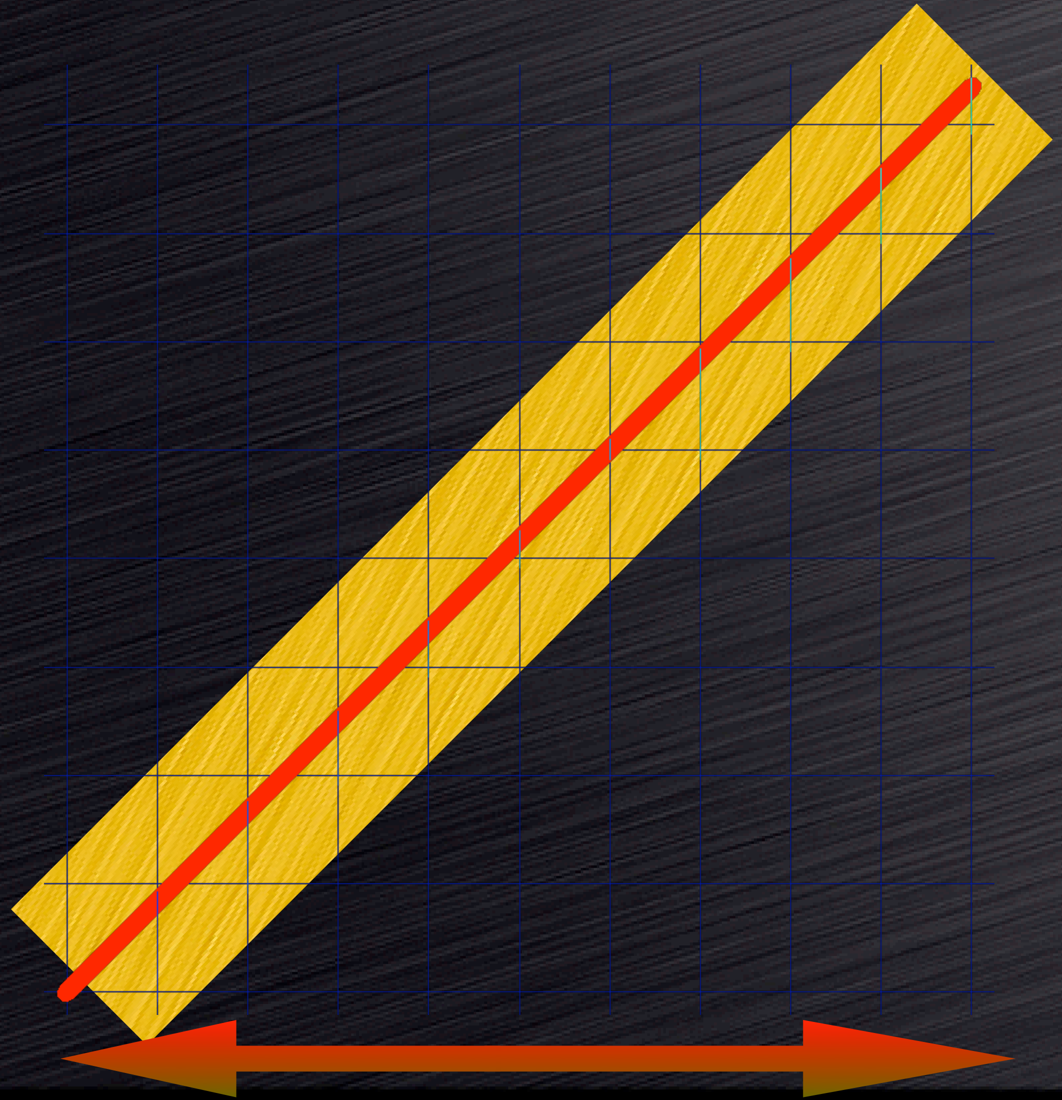
for all m there are irreducible fractions p_n/q_n

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

"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

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**

About the convergence

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

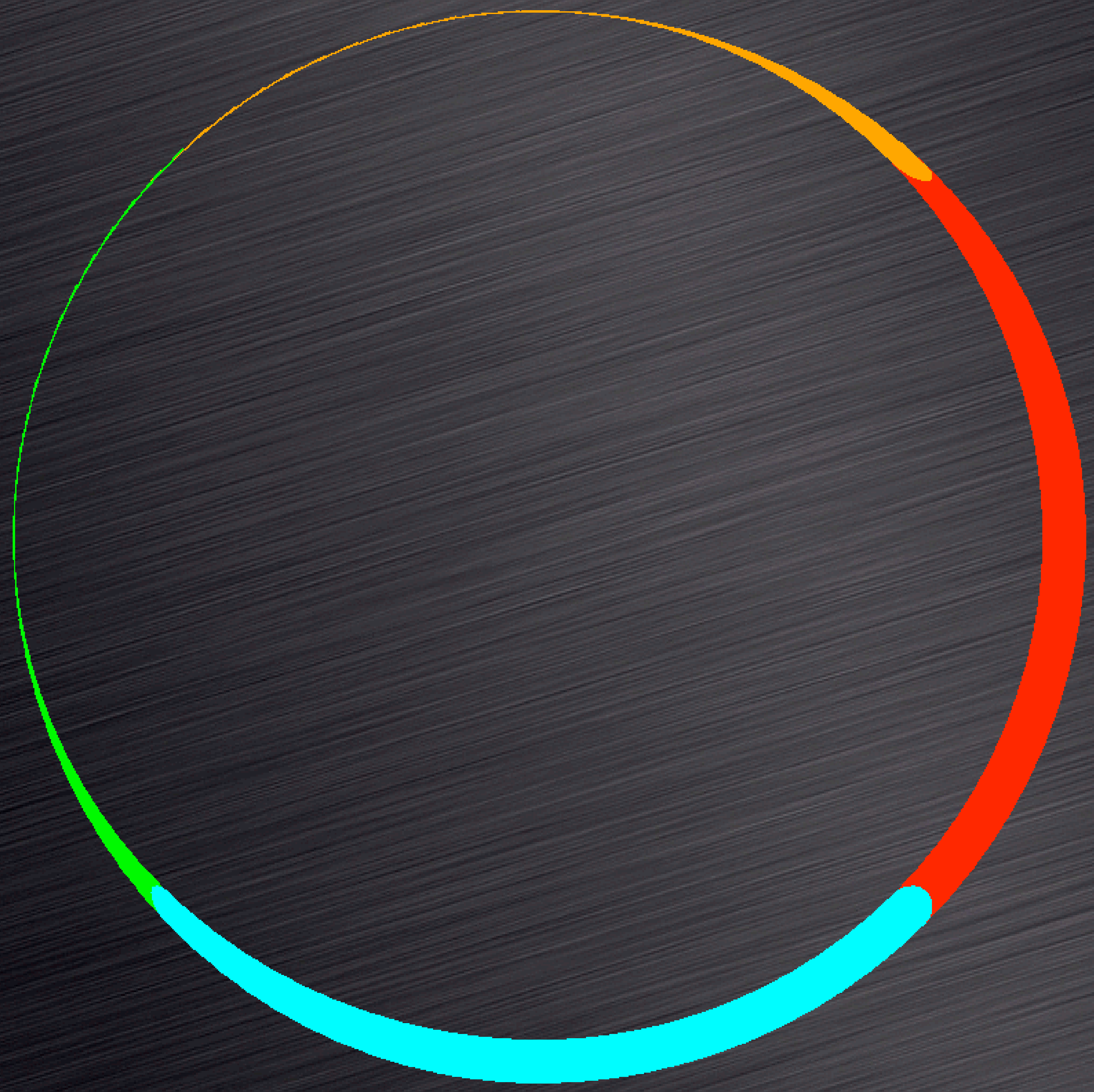
$$\frac{1}{n^{1-\theta}} \sum_{k=1}^{n} 1_{A_n}(x + k\alpha) = 1 + O(\frac{\log(n)^{2+\epsilon}}{n^{(1-\theta)/2}}) \, .$$

Paul Erdoes, Wolfgang Schmidt 1959/1960

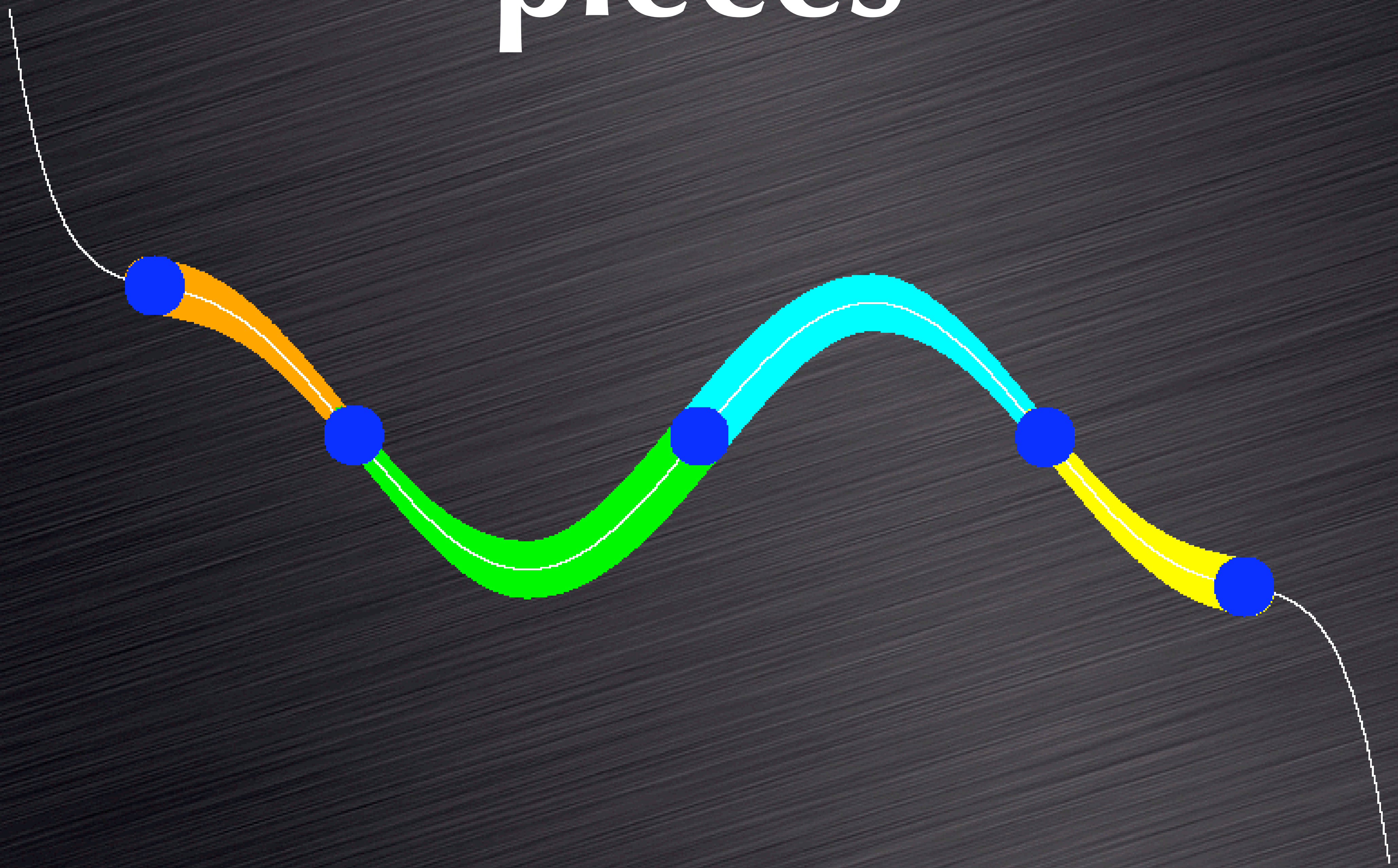
Elementary proof of the curve approximation result

- 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.

Pieces of Graphs

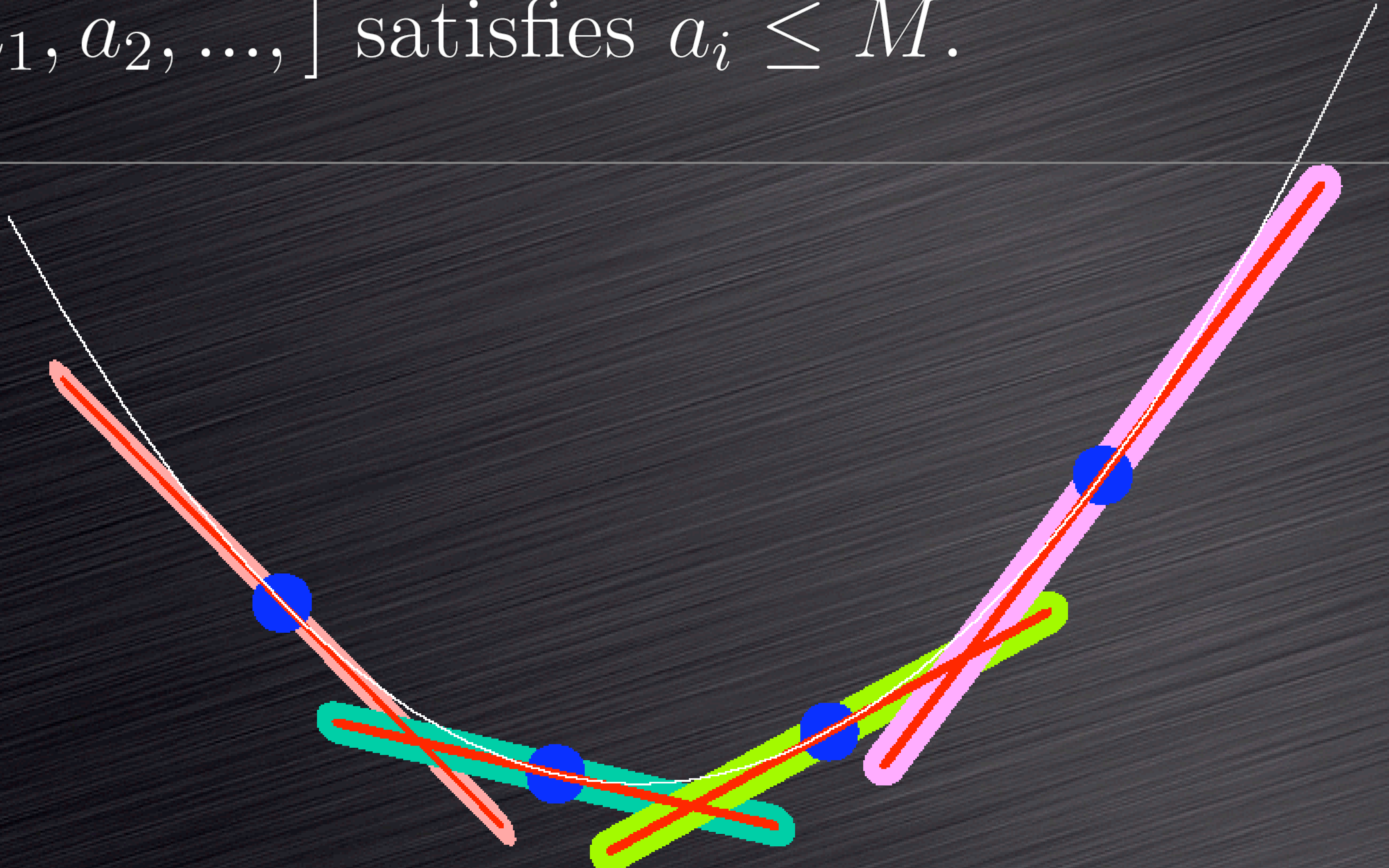


Concave or Convex pieces

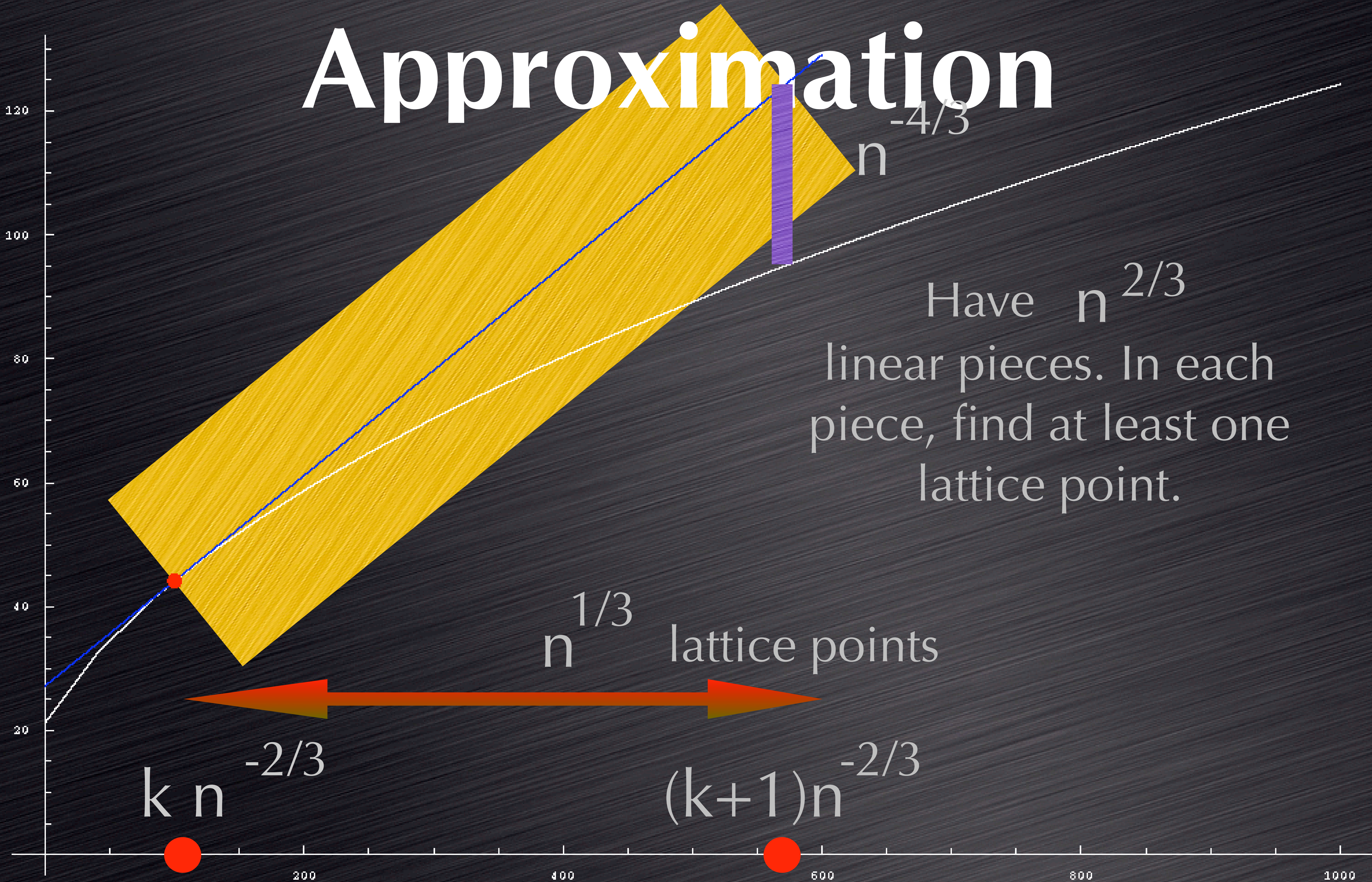


Diophantine Spline approximation

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 $a_i \leq M$.



Diophantine Spline Approximation

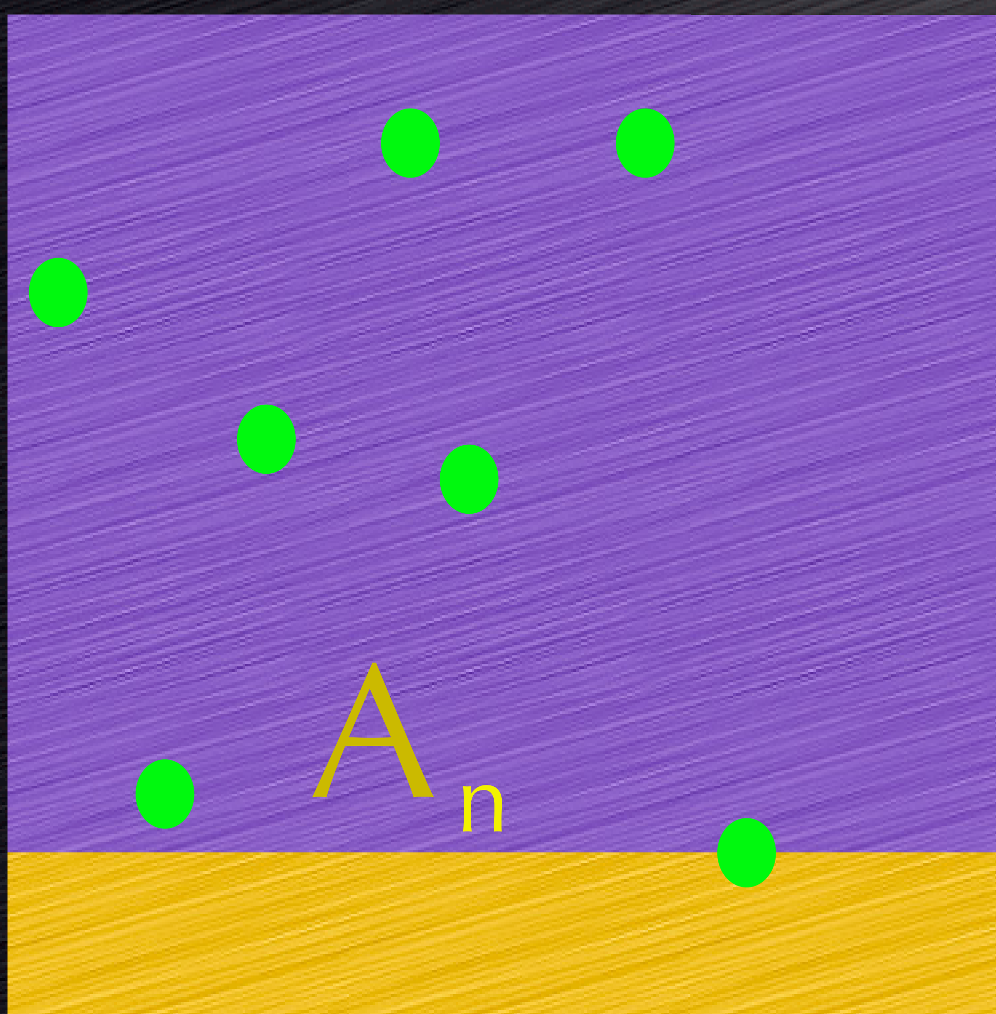


For larger delta?

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

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

???

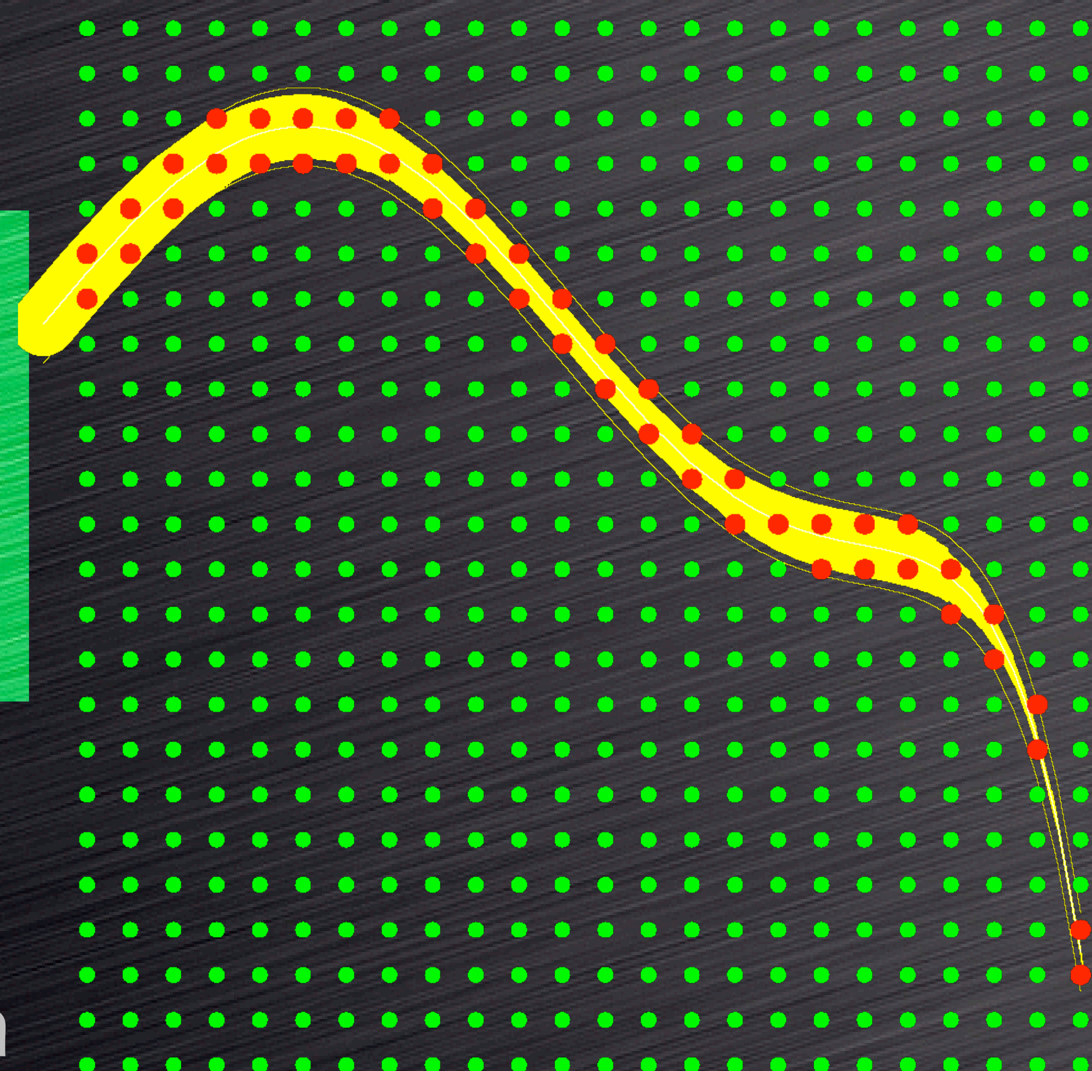


$$T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x+a \\ x+y \end{bmatrix}$$

Numerical experiments indicate limit exists.

Constructive Proof

The proof is constructive. Lattice points close to the curve are obtained by drawing tangents and computing lattice points close to that tangent using a continued fraction expansion.

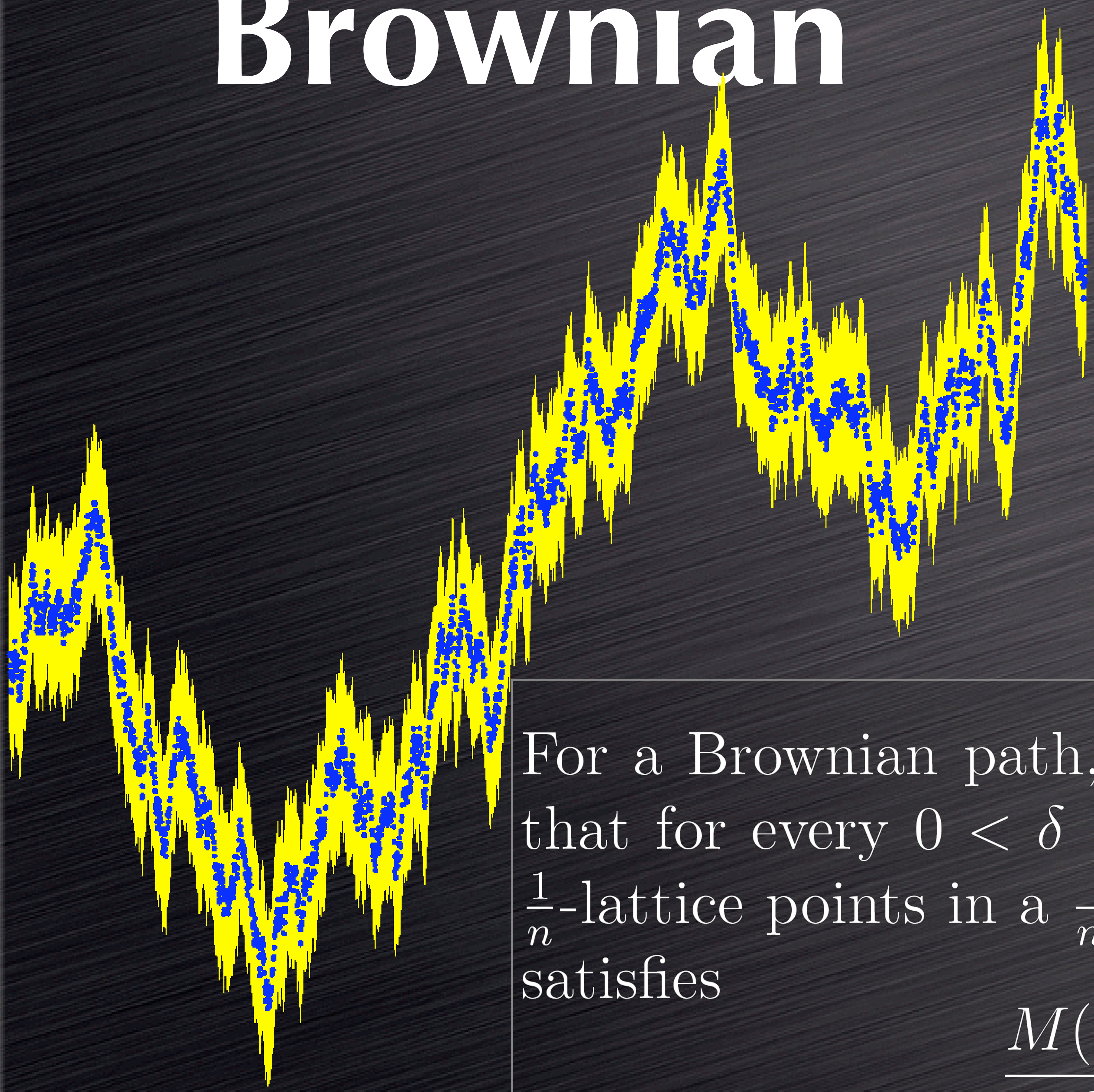


Existence and construction

Complexity and efficient computation

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.

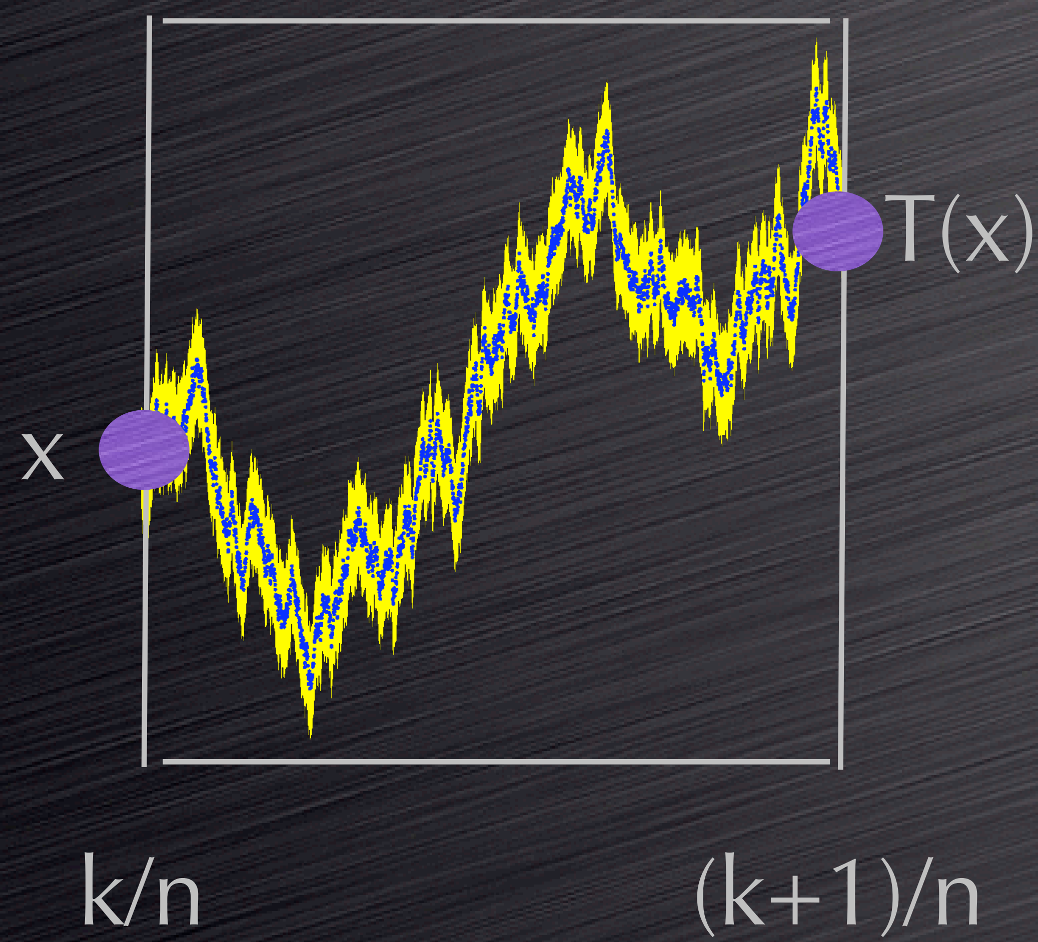
A random version

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

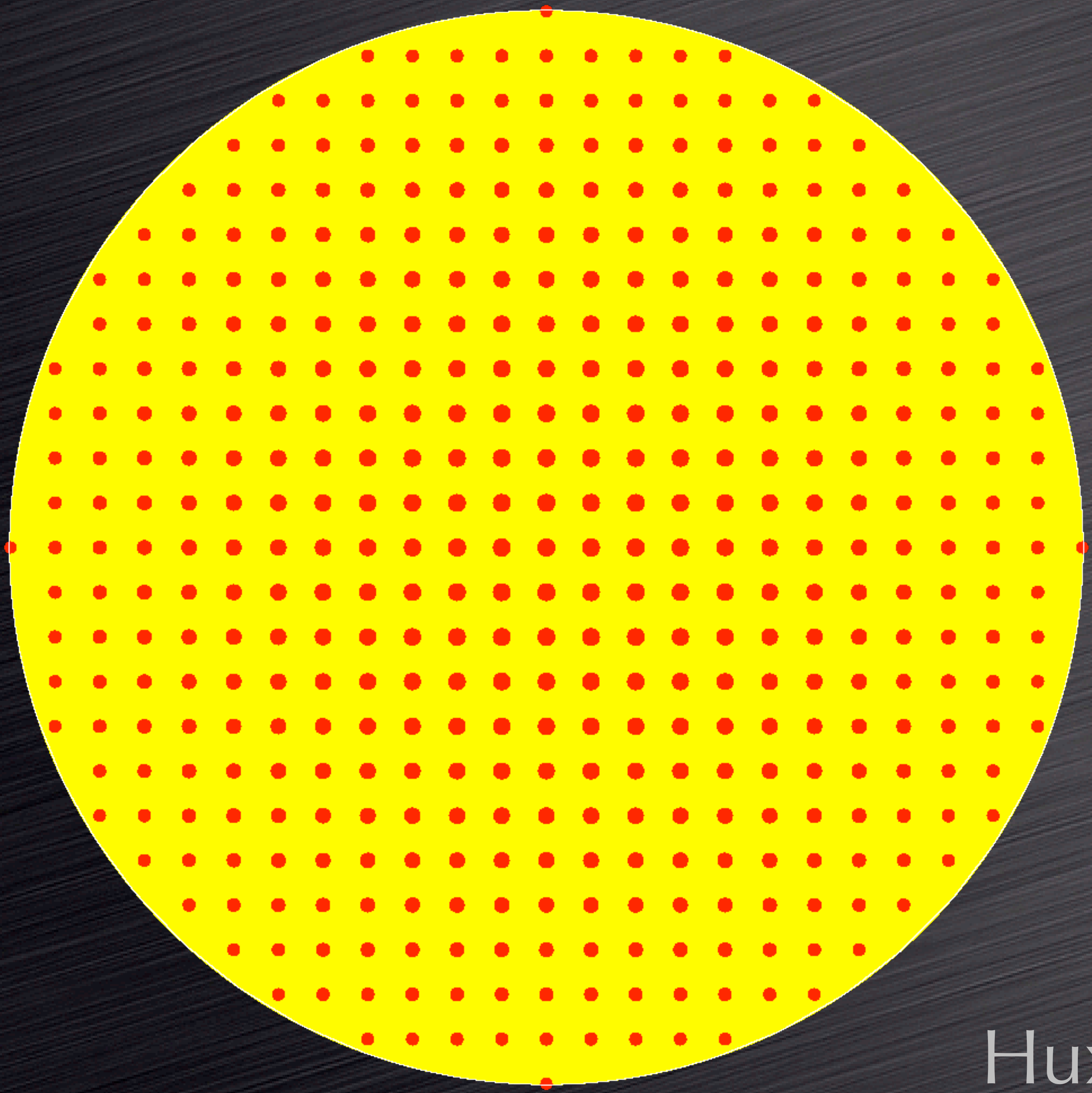
$$B_n = \{|\frac{S_n(x)}{n^{1-\delta}} - 1| > \epsilon\}$$

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.

Relation with Gauss problem



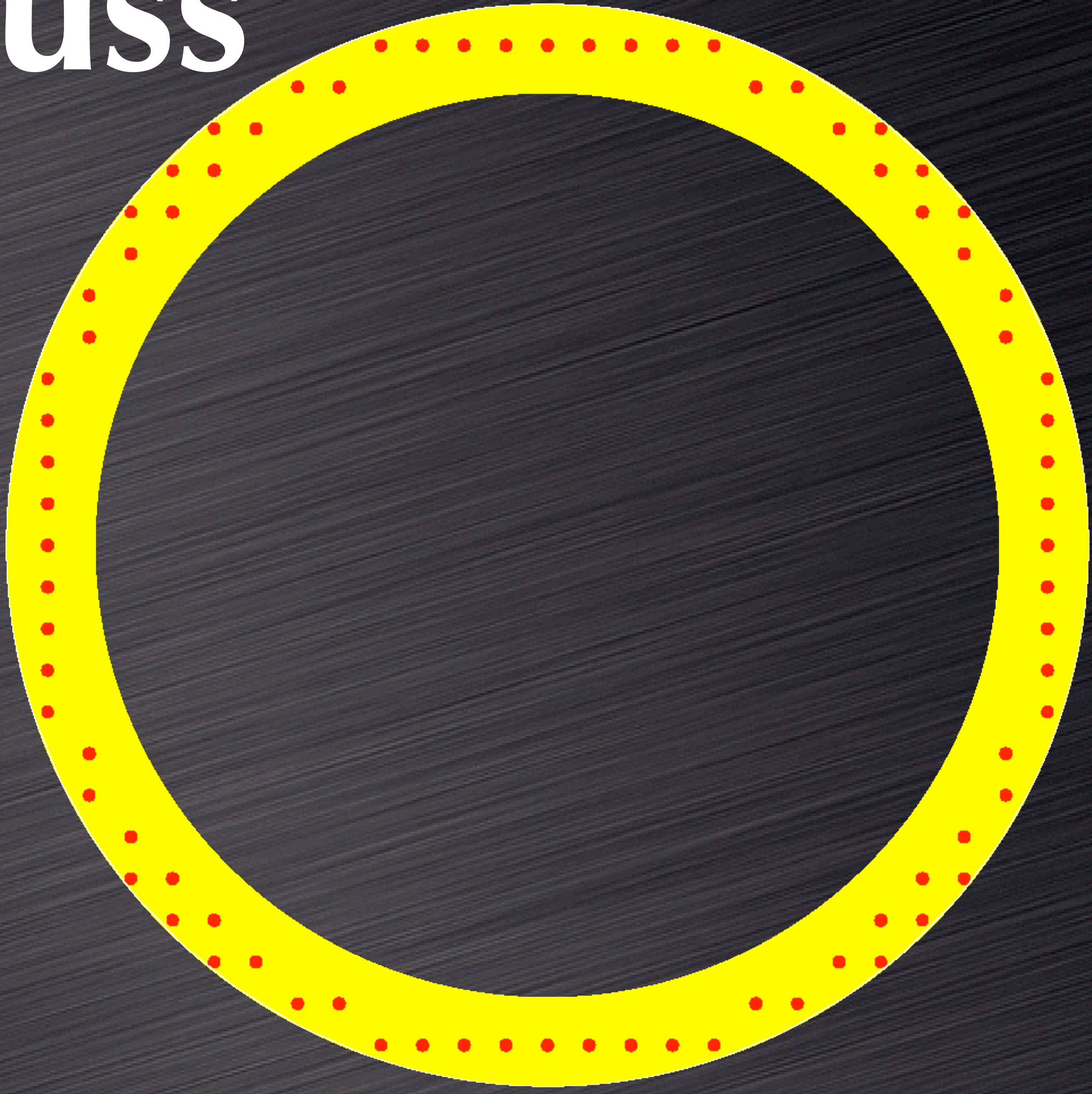
Gauss Circle Problem

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:

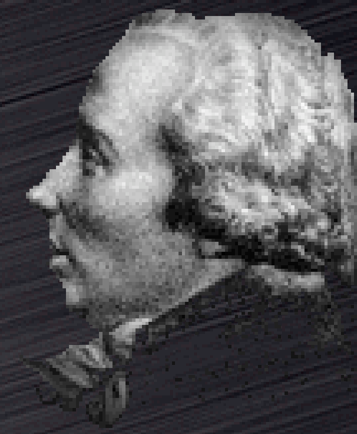
Assume Gauss lattice problem:

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

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

Relation 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

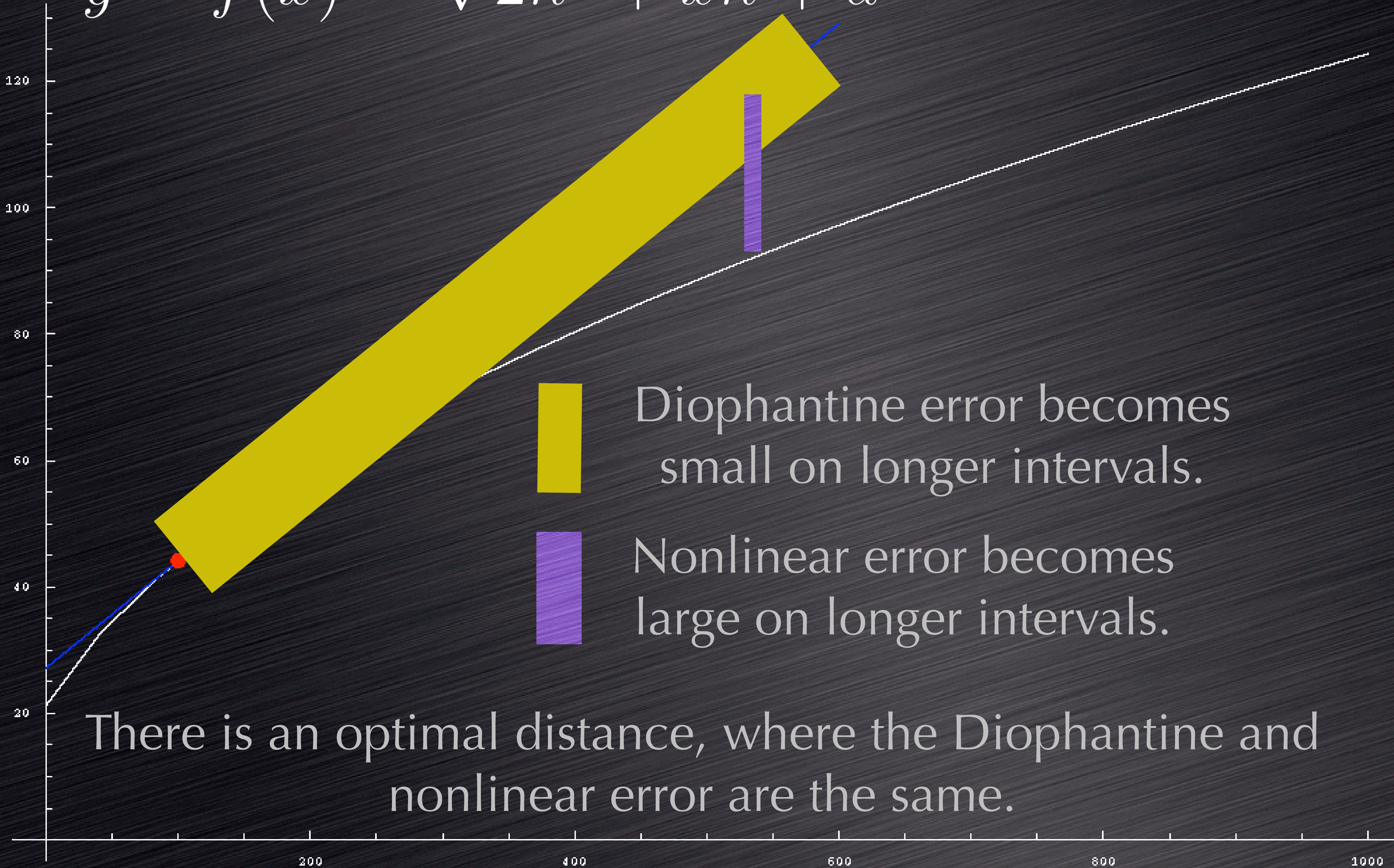
$$y^2 = 1 \bmod n$$

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.

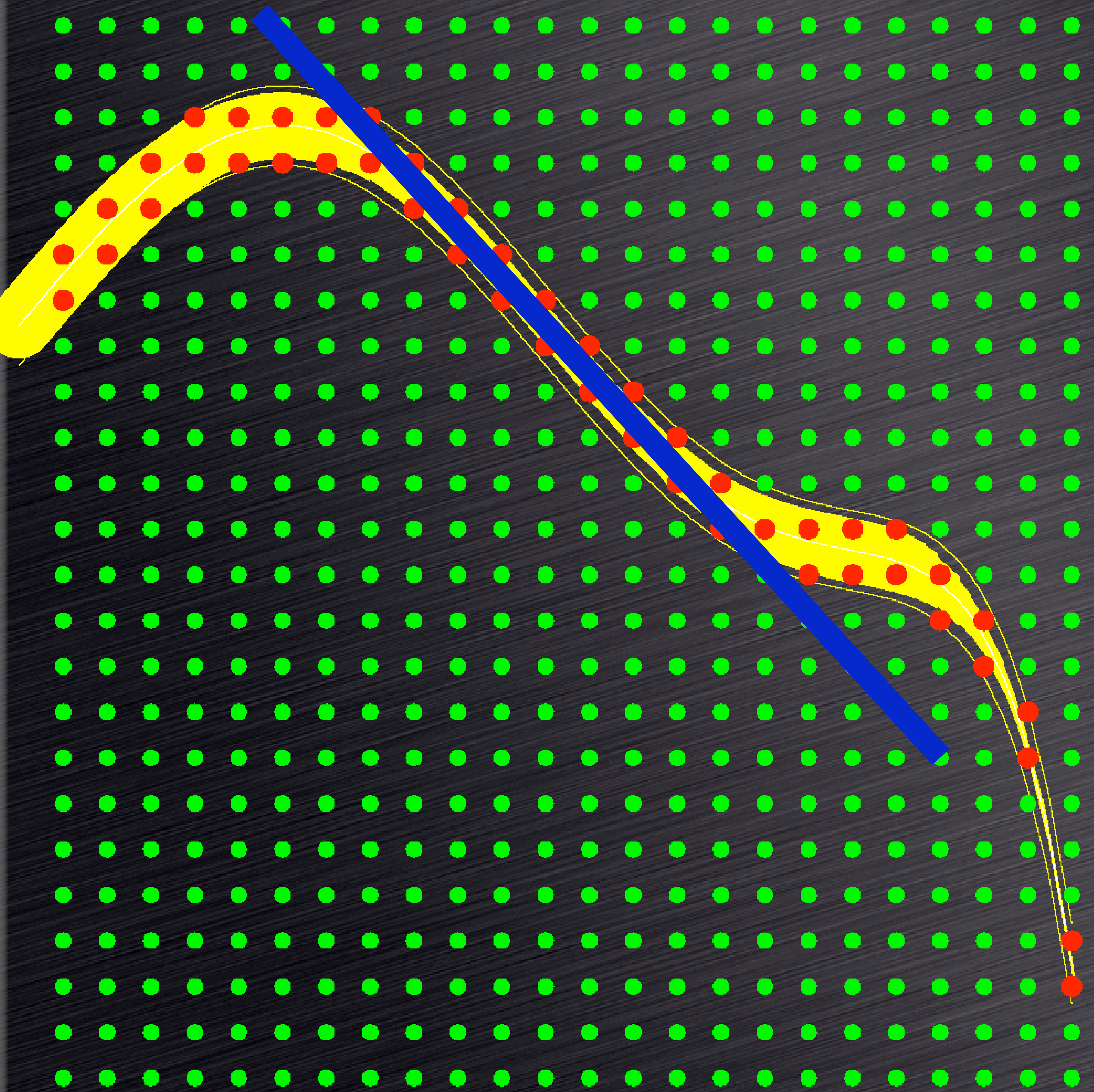
Estimate

$y = \sqrt{2n^2 + nx}$ 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?

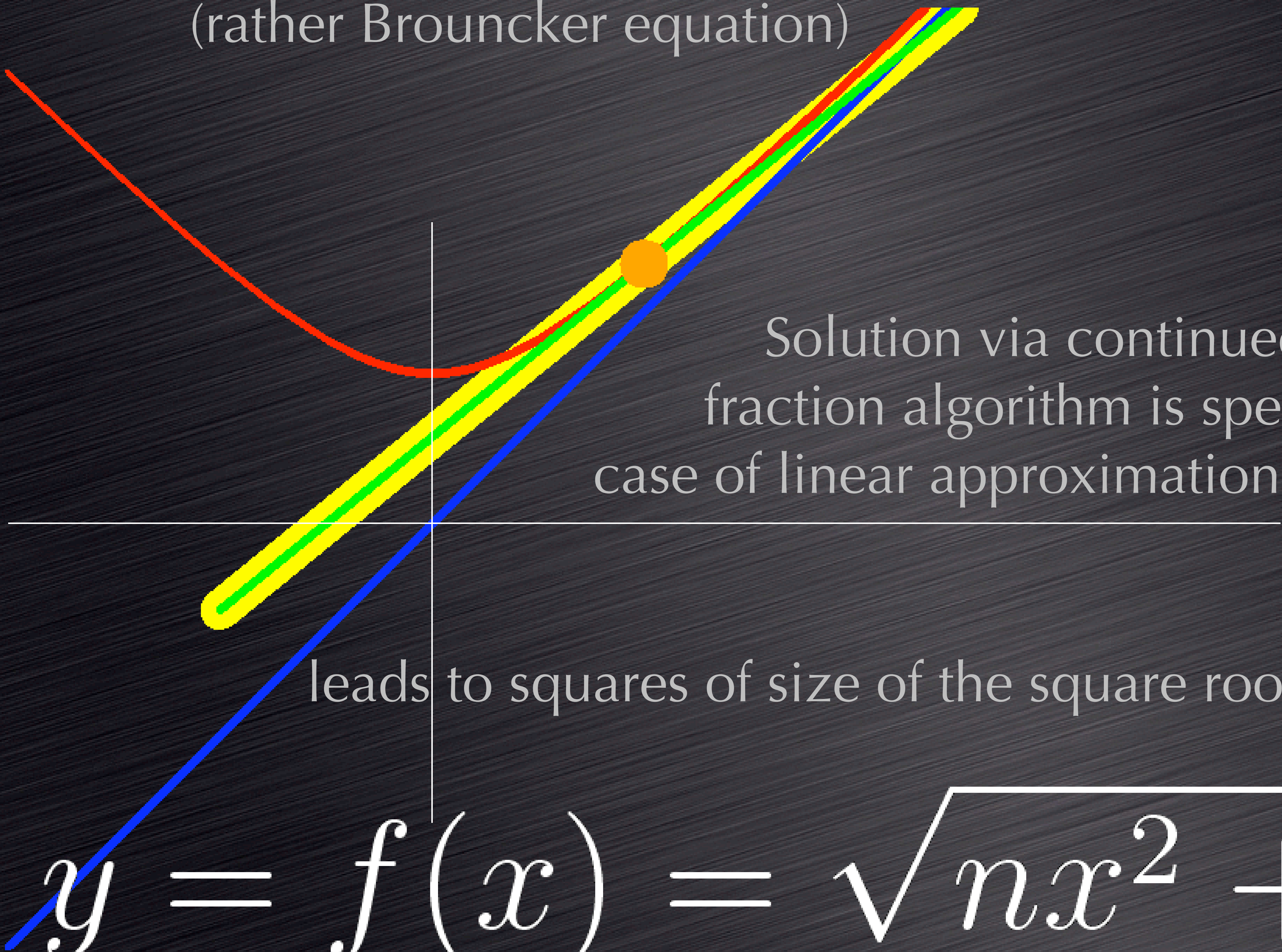


i.e near
inflection points

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

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

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

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

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

The quest for pi

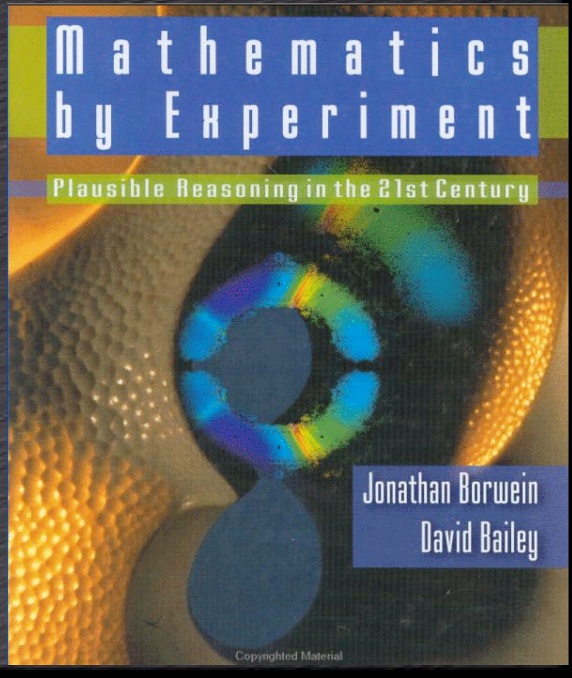
$$
\begin{aligned}
x &= 31415926535897932384626433832795028\ldots \\
T(x) &= 14159265358979323846264338327950288\ldots \\
T^2(x) &= 41592653589793238462643383279502884\ldots \\
T^3(x) &= 15926535897932384626433832795028841\ldots \\
\ldots & \quad \ldots
\end{aligned}
$$

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.

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].

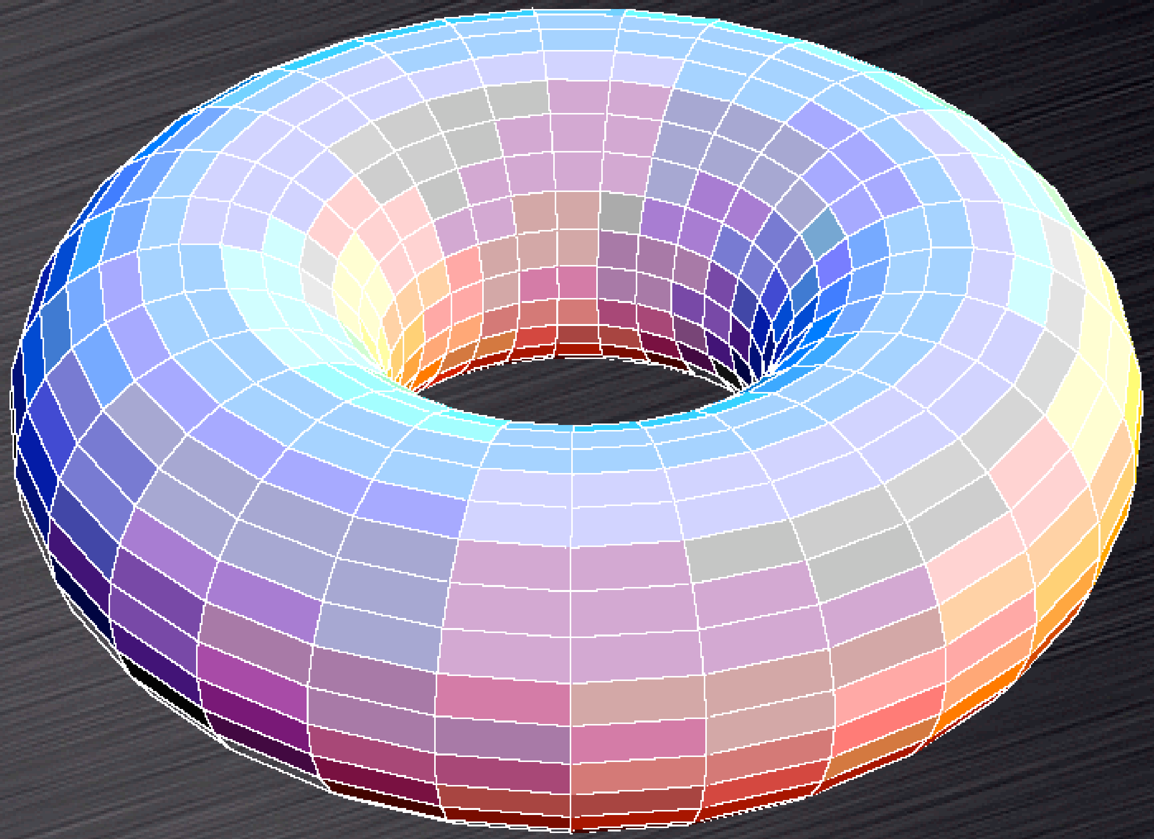
Spectral Theory of flows

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

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 $T_1(x)_n = x_{n+1}, T_2(x) = x_{n+2}, ..., T_l(x) = x_{n+l}$.

Literature

METRIC THEORY OF DIOPHANTINE APPROXIMATIONS

Vladimir G. Sprindžuk
Institute of Mathematics
Belorussian Academy of Sciences, Minsk

Translated and edited by
Richard A. Silverman

1979

V. H. WINSTON & SONS
Washington, D.C.

A HALSTED PRESS BOOK

JOHN WILEY & SONS
New York Toronto London Sydney

Metric Number Theory

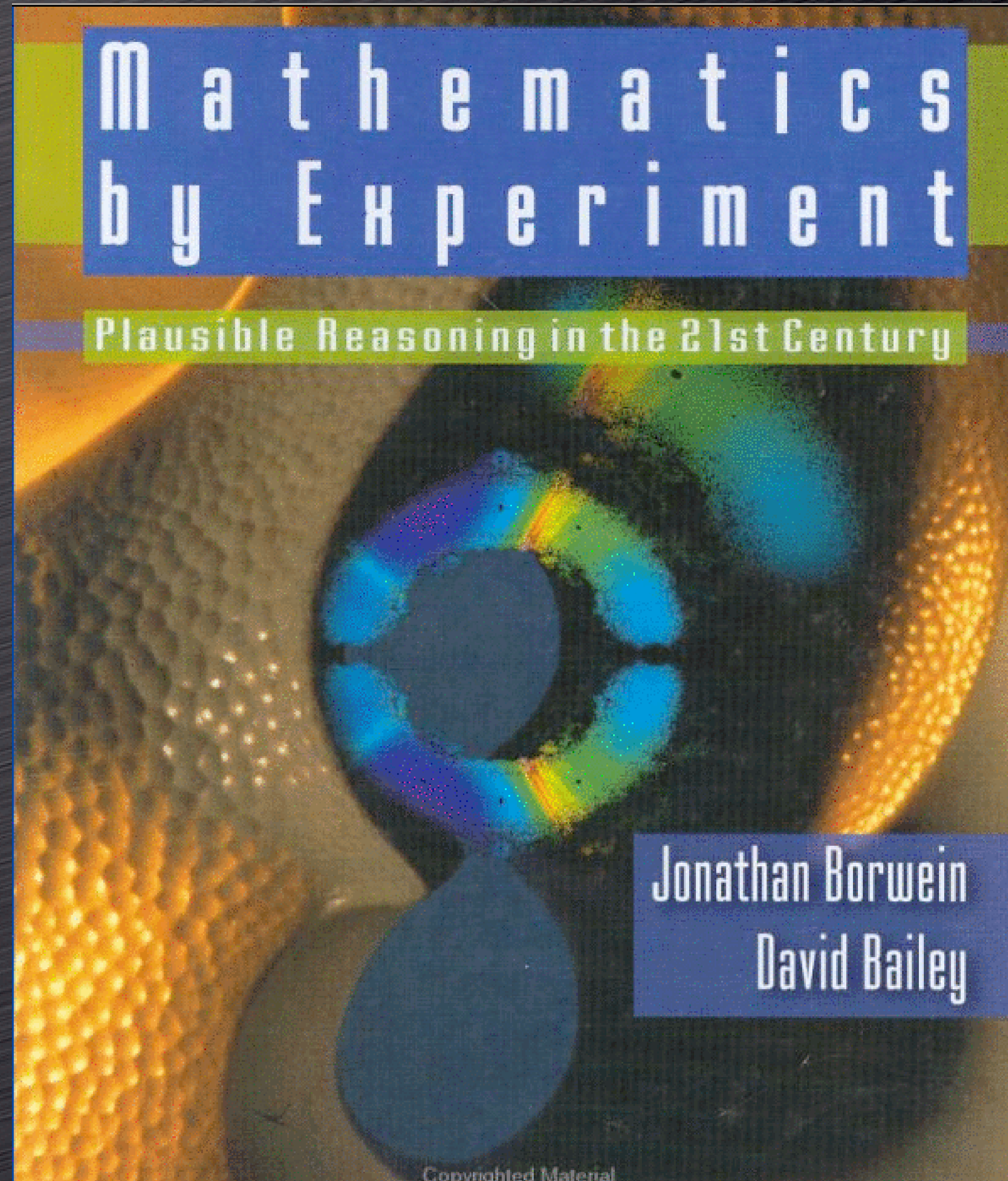
Glyn Harman
School of Mathematics
University of Wales Cardiff

CLARENDON PRESS • OXFORD
1998

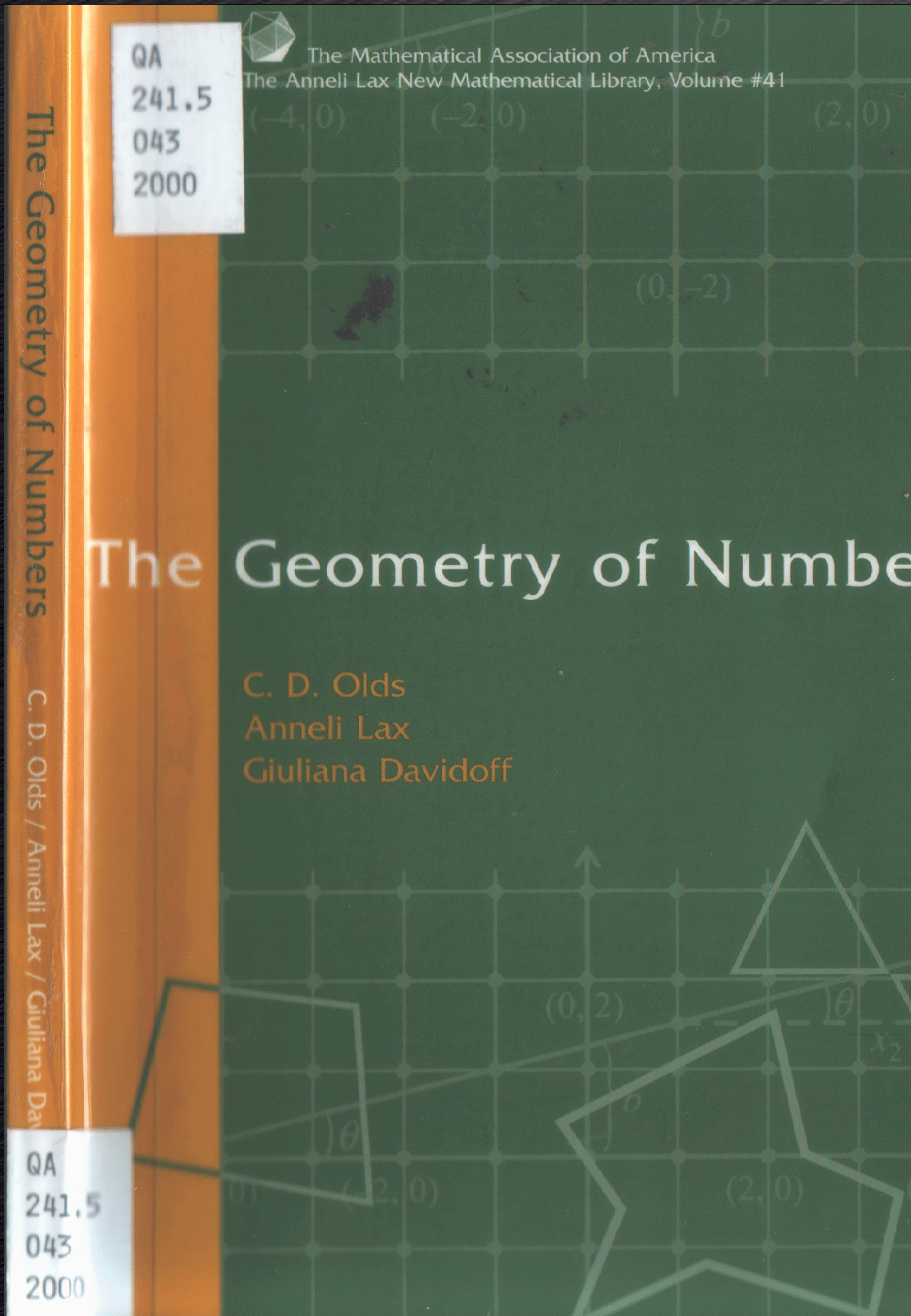
Area, Lattice Points, and Exponential Sums

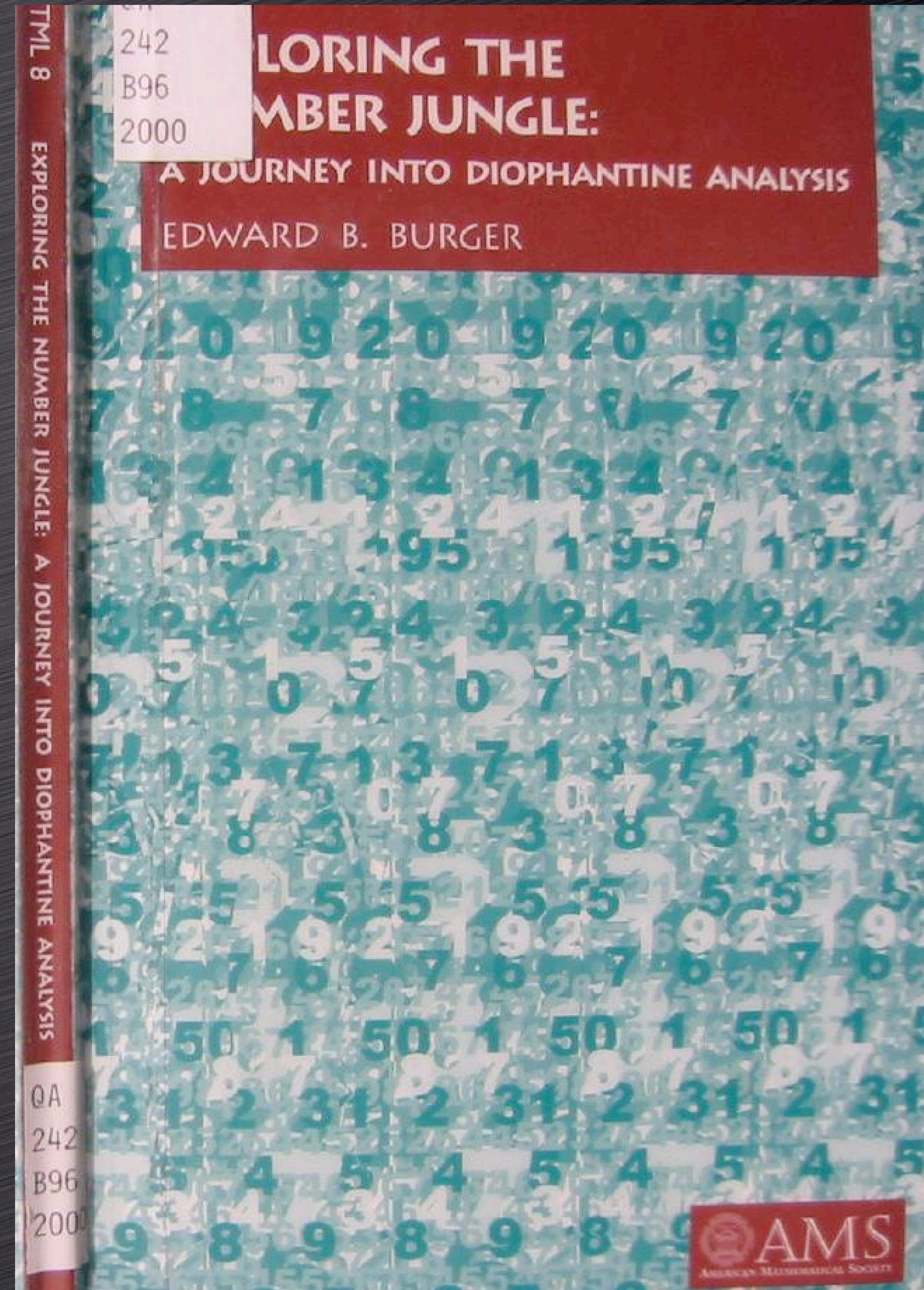
M. N. Huxley
College of Cardiff
University of Wales

CLARENDON PRESS • OXFORD
1996



Finally: Two nice introductions to Diophantine approximation and geometry of numbers:


QA
241.5
043
2000
The Mathematical Association of America
The Anneli Lax New Mathematical Library, Volume #41
The Geometry of Numbers
The Geometry of Numbe
C. D. Olds
Anneli Lax
Giuliana Davidoff
C. D. Olds / Anneli Lax / Giuliana Dav
QA
241.5
043
2000


242
B96
2000
LORING THE
MBER JUNGLE:
A JOURNEY INTO DIOPHANTINE ANALYSIS
EDWARD B. BURGER
TML 8
EXPLORING THE NUMBER JUNGLE: A JOURNEY INTO DIOPHANTINE ANALYSIS
QA
242
B96
200
AMS