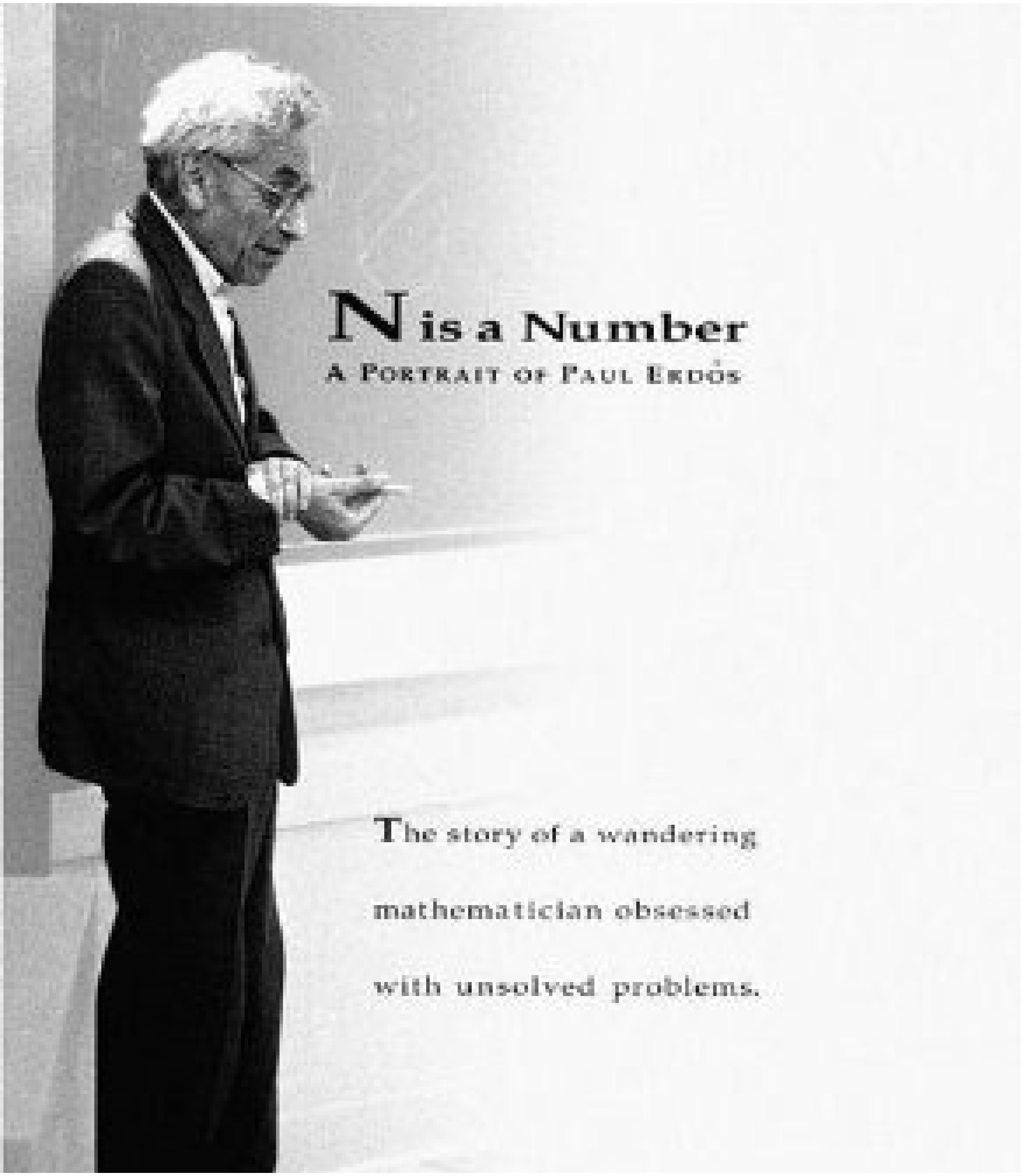
From Apollonian Circle Packings to Fibonacci Numbers

Jeff Lagarias,
University of Michigan

March 25, 2009



N is a Number

A Portrait of Paul Erdős

The story of a wandering mathematician obsessed with unsolved problems.

Credits

- Results on integer Apollonian packings are joint work with Ron Graham, Colin Mallows, Allan Wilks, Catherine Yan, ([GLMWY])

- Some of the work on Fibonacci numbers is an ongoing joint project with Jon Bober. ([BL])

- Work of J. L. was partially supported by NSF grant DMS-0801029.

Table of Contents

1. Exordium

2. Apollonian Circle Packings

3. Fibonacci Numbers

4. Peroratio

1. Exordium (Contents of Talk)-1

- The talk first discusses Apollonian circle packings. Then it discusses integral Apollonian packings - those with all circles of integer curvature.

- These integers are describable in terms of integer orbits of a group $\mathcal{A}$ of 4×4 integer matrices of determinant ± 1, the Apollonian group, which is of infinite index in $O(3,1,\mathbb{Z})$, an arithmetic group acting on Lorentzian space. [Technically $\mathcal{A}$ sits inside an integer group conjugate to $O(3,1,\mathbb{Z})$.]

Contents of Talk-2

- Much information on primality and factorization theory of integers in such orbits can be read off using a sieve method recently developed by Bourgain, Gamburd and Sarnak.

- They observe: The spectral geometry of the Apollonian group controls the number theory of such integers.

- One notable result: integer orbits contain infinitely many almost prime vectors.

Contents of Talk-3

- The talk next considers Fibonacci numbers and related quantities. These can be obtained an orbit of an integer subgroup $\mathcal{F}$ of 2×2 matrices of determinant ± 1, the Fibonacci group. This group is of infinite index in $GL(2, \mathbb{Z})$, an arithmetic group acting on the upper and lower half planes.

- Factorization behavior of these integers is analyzable heuristically. The behavior should be very different from the case above. In contrast to the integer Apollonian packings, there should be finitely many almost prime vectors in each integer orbit! We formulate conjectures to quantify this, and test them against data.

2. Circle Packings

A circle packing is a configuration of mutually tangent circles in the plane (Riemann sphere). Straight lines are allowed as circles of infinite radius. There can be finitely many circles, or countably many circles in the packing.

- Associated to each circle packing is a *planar graph*, whose vertices are the centers of circles, with edges connecting the centers of touching circles.

- The simplest such configuration consists of four mutually touching circles, a *Descartes configuration*.

Descartes Configurations

Three mutually touching circles is a simpler configuration than four mutually touching circles.

However...

any such arrangement "almost" determines a fourth circle. More precisely, there are exactly two ways to add a fourth circle touching the other three, yielding two possible Descartes configurations.

Descartes Circle Theorem

Theorem (Descartes 1643) *Given four mutually touching circles (tangent externally), their radii* d, e, f, x *satisfy*

$$\begin{aligned} ddeeff + ddeexx + ddffxx + eeffxx &= \\ + 2deffxx &+ 2deeffx + 2deefxx \\ + 2ddeffx &+ 2ddefxx + 2ddeefx. \end{aligned}$$

Remark. Rename the circle *radii* r_i, so the circles have curvatures $c_i = \frac{1}{r_i}$. Then the Descartes relation can be rewritten

$$c_1^2 + c_2^2 + c_3^2 + c_4^2 = \frac{1}{2}(c_1 + c_2 + c_3 + c_4)^2.$$

“The square of the sum of the bends is twice the sum of the squares” (Soddy 1936).

Beyond Descartes: Curvature-Center Coordinates

- Given a Descartes configuration $\mathcal{D}$, with circle C_i of radius r_i and center (x_i, y_i), and with dual circle $\bar{C}_i$ of radius $\bar{r_i}$, obtained using the anti-holomorphic map $z \to 1/\bar{z}$. The curvatures of C_i and $\bar{C}_i$ are $c_i = 1/r_i$ and $\bar{c_i} = 1/\bar{r_i}$.

- Assign to $\mathcal{D}$ the following 4×4 matrix of (augmented) curvature-center coordinates

$$M_{\mathcal{D}} = \begin{bmatrix} c_1 & \bar{c}_1 & c_1x_1 & c_1y_1 \\ c_2 & \bar{c}_2 & c_2x_2 & c_2y_2 \\ c_3 & \bar{c}_3 & c_3x_3 & c_3y_3 \\ c_3 & \bar{c}_4 & c_4x_4 & c_4y_4 \end{bmatrix}$$

Curvature-Center Coordinates- 1

• The Lorentz group $O(3,1,\mathbb{R})$ consists of the real automorphs of the Lorentz form $Q_L = -w^2 + x^2 + y^2 + z^2$. That is $O(3,1,\mathbb{R}) = \{U : U^T Q_L U = Q_L\}$, where

$$Q_L = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

• Characterization of Curvature-center coordinates M: They satisfy an intertwining relation

$$M^T Q_D M = Q_W$$

where Q_D and Q_W are certain integer quadratic forms equivalent to the Lorentz form. (Gives: moduli space!)

Curvature-Center Coordinates-2

- Characterization implies: Curvature-center coordinates of all ordered, oriented Descartes configurations are identified (non-canonically) with the group of

  Lorentz transformations $O(3,1,\mathbb{R})$!

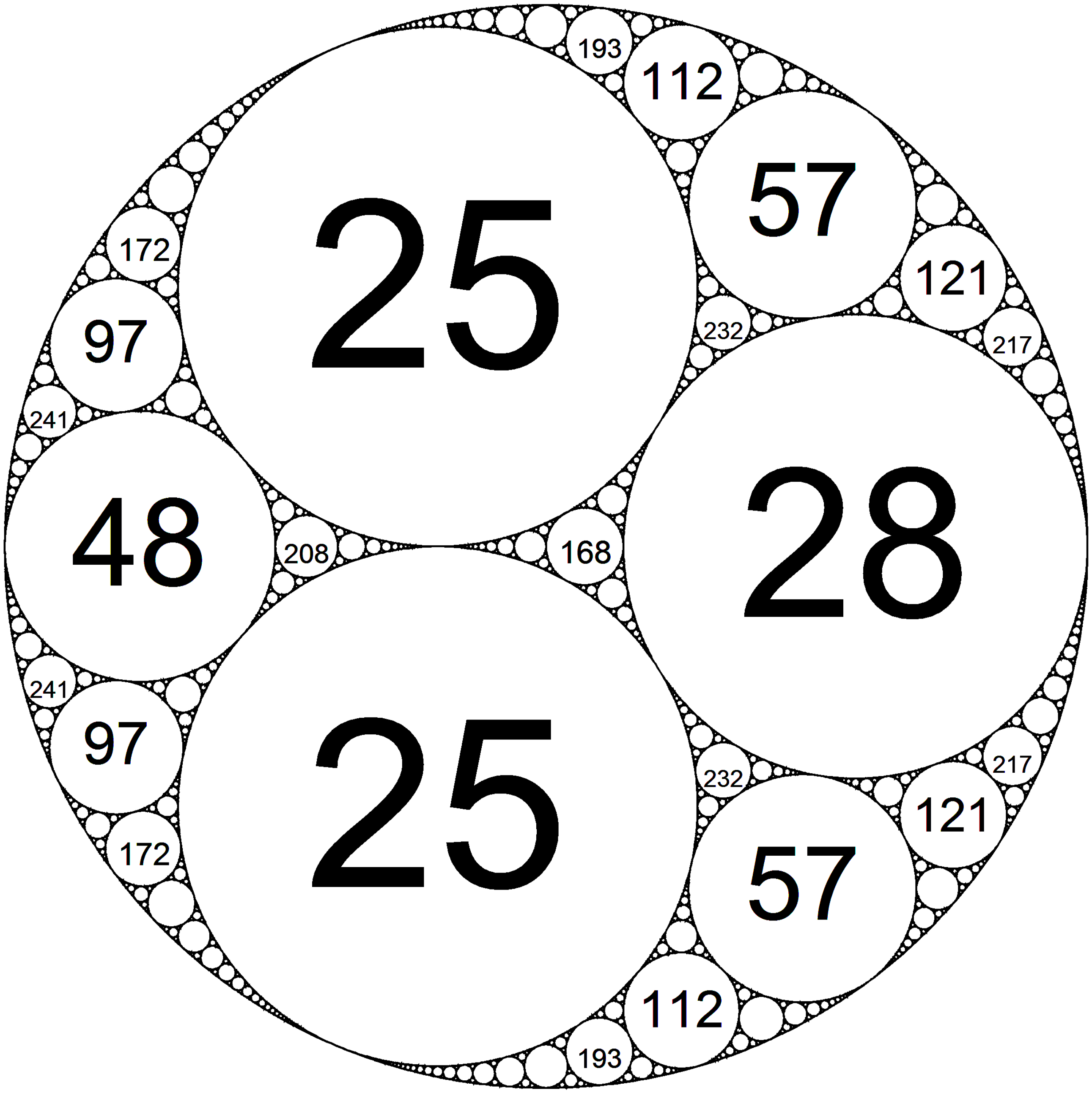
  Thus: “Descartes configurations parametrize the Lorentz group.”

- The Lorentz group is a 6-dimensional real Lie group with four connected components. It is closely related to the Möbius group $PSL(2,\mathbb{C}) = SL(2,\mathbb{C})/\{\pm I\}$. (But it allows holomorphic and anti-holomorphic transformations.)

Apollonian Packings-1

- An Apollonian Packing $\mathcal{P}_{\mathcal{D}}$ is an infinite configuration of circles, formed by starting with an initial Descartes configuration $\mathcal{D}$, and then filling in circles recursively in each triangular lune left uncovered by the circles.

- We initially add 4 new circles to the Descartes configuration, then 12 new circles at the second stage, and $2 \cdot 3^{n-1}$ circles at the n-th stage of the construction.


193
112
57
25
172
121
97
232
217
241
48
28
208
168
241
217
232
97
121
172
25
57
112
193

Apollonian Packings-2

- An *Apollonian Packing* is unique up to a Möbius transformation of the Riemann sphere. There is exactly one Apollonian packing in the sense of *conformal geometry*! However, Apollonian packings are not unique in the sense of *Euclidean geometry*: there are uncountably many different Euclidean packings.

- Each Apollonian packing $\mathcal{P}_{\mathcal{D}}$ has a limit set of uncovered points. This limit set is a fractal. It has Hausdorff dimension about 1.305686729 (according to physicists). [Mathematicians know fewer digits.]

Apollonian Packing Characterizations

- Geometric Characterization of Apollonian Packings An Apollonian packing has a large group of Möbius transformations preserving the packing. This group acts transitively on Descartes configurations in the packing.

- Algebraic Characterization of Apollonian Packings The set of Descartes configurations is identifiable with the real Lorentz group. $O(3, 1, \mathbb{R})$. There is a subgroup, the *Apollonian group*, such that the set of Descartes configurations in the packing is an orbit of the Apollonian group!

- Holographic Characterization of Apollonian Packings For each Apollonian packing there is a geometrically finite Kleinian group acting on hyperbolic 3-space $\mathbb{H}^3$, such that the circles in the Apollonian packing are the complement of the limit set of this group on the ideal boundary $\hat{\mathbb{C}}$ of $\mathbb{H}^3$, identified with the Riemann sphere.

Apollonian Packing Characterization-1

Geometric Characterization of Apollonian Packings

(i) An Apollonian packing $\mathcal{P}_{\mathcal{D}}$ is a set of circles in the Riemann sphere $\widehat{\mathbb{C}} = \mathbb{R} \cup \{\infty\}$, which consist of the orbits of the four circles in $\mathcal{D}$ under the action of a discrete group $G_{\mathcal{A}}(\mathcal{D})$ of Möbius transformations inside the conformal group $Mob(2)$.

(ii) The group $G_{\mathcal{A}}(\mathcal{D})$ depends on the initial Descartes configuration $\mathcal{D}$.

Note. Möbius transformations move individual circles to individual circles in the packing. They also move Descartes configurations to other Descartes configurations.

Apollonian Packing-Characterization-1a

- The group of Möbius transformations is

$$G_{\mathcal{A}}(\mathcal{D}) = \langle \mathfrak{s}_1, \mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4 \rangle,$$

  in which $\mathfrak{s}_i$ is inversion in the circle that passes through those three of the six intersection points in $\mathcal{D}$ that touch circle C_i.

- The group $G_{\mathcal{A}}(\mathcal{D})$ can be identified with a certain group of right-automorphisms of the moduli space of Descartes configurations, given in curvature-center coordinates. These are a group 4×4 real matrices multiplying the coordinate matrix $M_{\mathcal{D}}$ on the right.

Apollonian Packing-Characterization-2

Algebraic Characterization of Apollonian Packings

(i) The collection of all (ordered, oriented) Descartes configurations in the Apollonian acking $\mathcal{P}_{\mathcal{D}}$ form 48 orbits of a discrete group $\mathcal{A}$, the Apollonian group, that acts on a moduli space of Descartes configurations.

(ii) The Apollonian group is contained the group $Aut(Q_D) \sim O(3,1,\mathbb{R})$ of left-automorphisms of the moduli space of Descartes configurations given in curvature-center coordinates.

Apollonian Packing-Characterization-2a

(1) The Apollonian group $\mathcal{A}$ is *independent* of the initial Descartes configuration $\mathcal{D}$. However the particular orbit under $\mathcal{A}$ giving the configurations depends on the initial Descartes configuration $\mathcal{D}$.

(2) The Apollonian group action moves Descartes configurations as a whole , "mixing together" the four circles to make a new Descartes configuration.

Apollonian Packing-Characterization-2b

The *Apollonian group* is a subgroup of $GL(4, \mathbb{Z})$, acting on curvature-center coordinates on the left, given by

$$\mathcal{A} := \langle S_1, S_2, S_3, S_4 \rangle$$

- Here

$$S_1 = \begin{bmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad S_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$S_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad S_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{bmatrix},$$

- These generators satisfy

$$S_1^2 = S_2^2 = S_3^2 = S_4^2 = I$$

Properties of the Apollonian group

- The *Apollonian group* $\mathcal{A}$ is of infinite index in the integer Lorentz group $O(3,1,\mathbb{Z})$. In particular, the quotient manifold

  $$X = O(3,1,\mathbb{R})/\mathcal{A}$$

  is a Riemannian manifold of infinite volume.

- *FACT.*([GLMWY]) The Apollonian group is a hyperbolic Coxeter group.

Apollonian Packing-Characterization-3

Holographic Characterization of Apollonian Packings

The open disks comprising the interiors of the circles in an Apollonian packing $\mathcal{P}_{\mathcal{D}}$ *are the complement* $\hat{\mathbb{C}} \smallsetminus \Lambda_{\mathcal{D}}$ *of the limit set* $\Lambda_{\mathcal{D}}$ *of a certain Kleinian group* $\mathcal{S}_{\mathcal{D}}$ *acting on hyperbolic* 3*-space* $\mathbb{H}^3$*, with the Riemann sphere* $\hat{\mathbb{C}}$ *identified with the ideal boundary of* $\mathbb{H}^3$*. The group* $\mathcal{S}_{\mathcal{D}}$ *depends on the Descartes configuration* $\mathcal{D}$*.*

Apollonian Group and Integer Packings

Theorem. [Söderberg (1992)]
The circle curvatures of the four circles in all Descartes configurations in an Apollonian packing $\mathcal{P}_{\mathcal{D}}$ starting with the Descartes configuration $\mathcal{D}$ with curvatures $\{c_1, c_2, c_3, c_4\}$ comprise a (vector) orbit of the Apollonian group

$$\mathcal{O}_{\mathcal{A}}([c_1, c_2, c_3, c_4]^T) := \{A \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} : \quad A \in \mathcal{A}\}$$

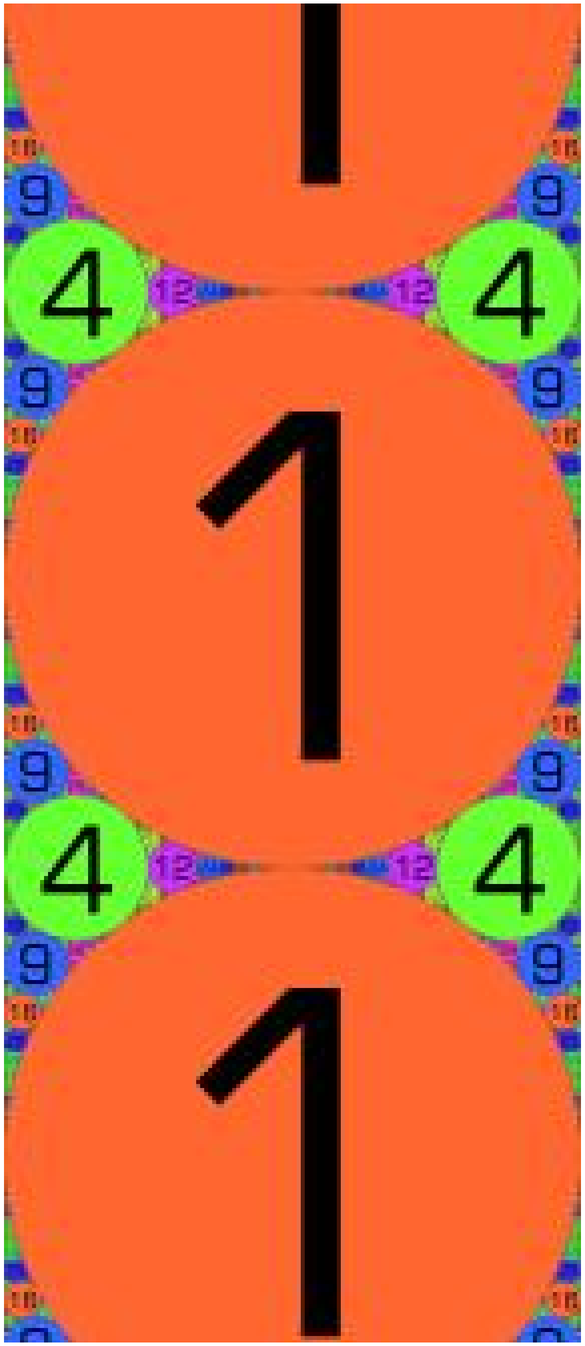
Consequence: If the initial curvatures are integers, then all circles in the packing have integer curvatures. Call these integer Apollonian circle packings.

Root Quadruples

- To tell integral packings apart, can classify them by the "smallest" (curvature) Descartes configuration they contain. We call the resulting curvatures (c_1, c_2, c_3, c_4) the root quadruple of such a packing.

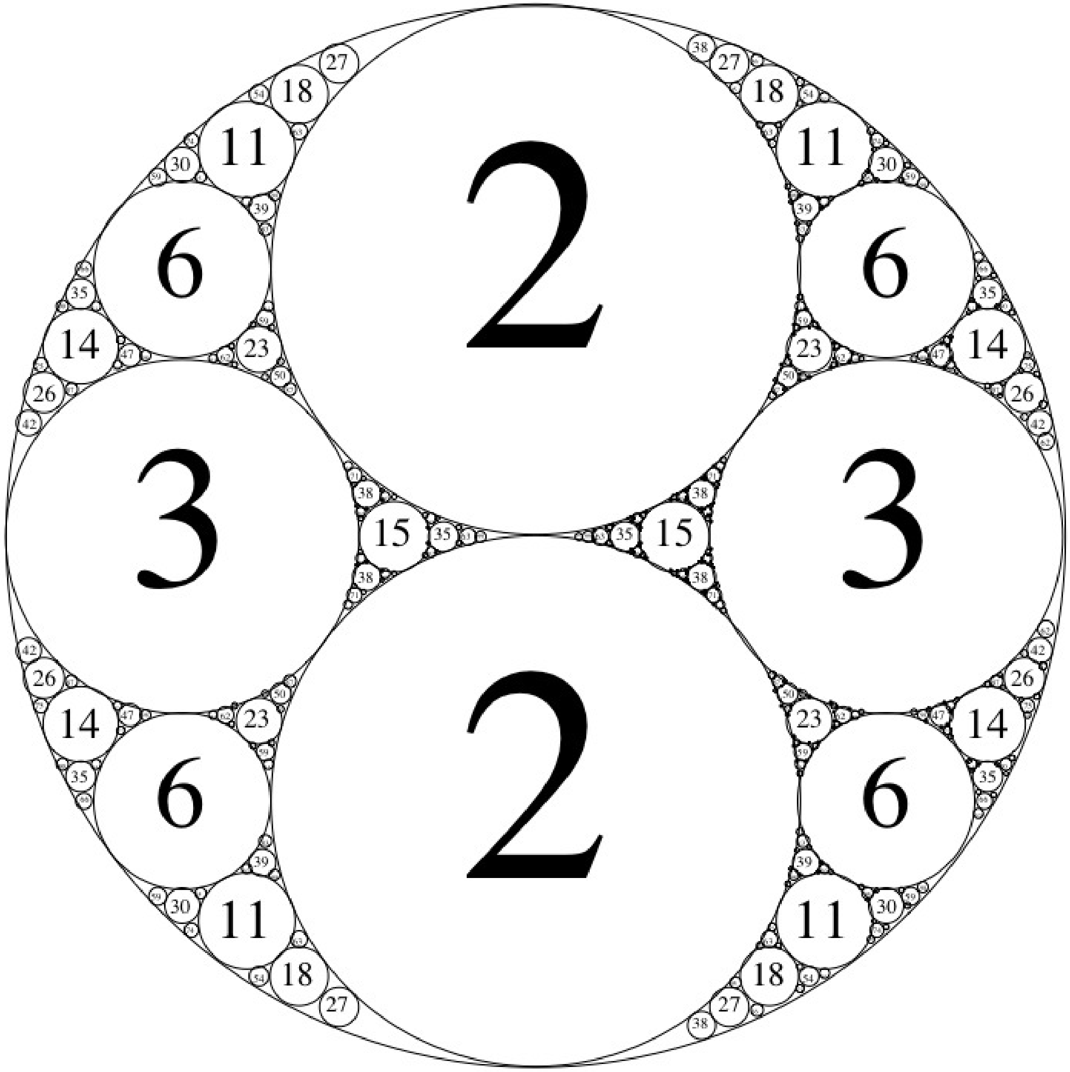
- The root quadruple is unique. One value in the root quadruple will be negative, and the other three values strictly positive, with one exception!

- The exceptional configuration is the $(0, 0, 1, 1)$ packing, which is the only unbounded integer Apollonian packing.

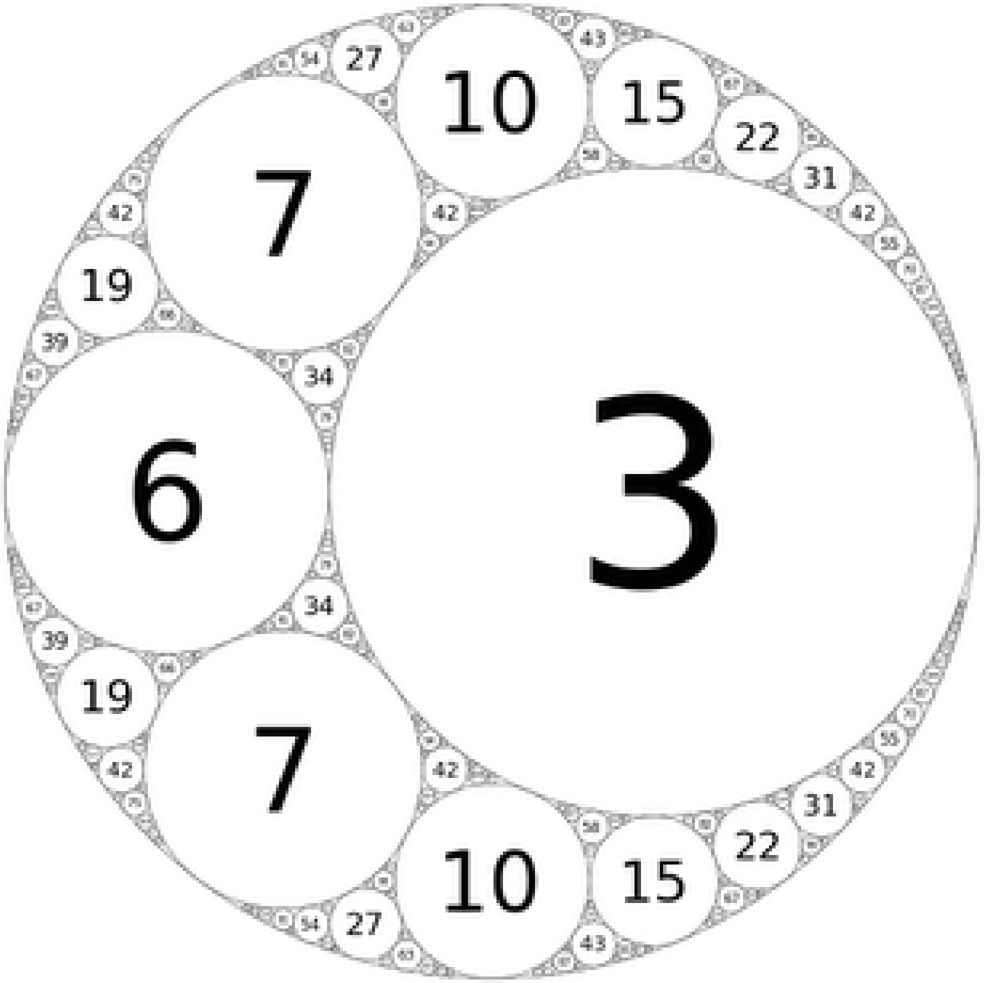

1
18
9
4
12
1
4
12
9
1

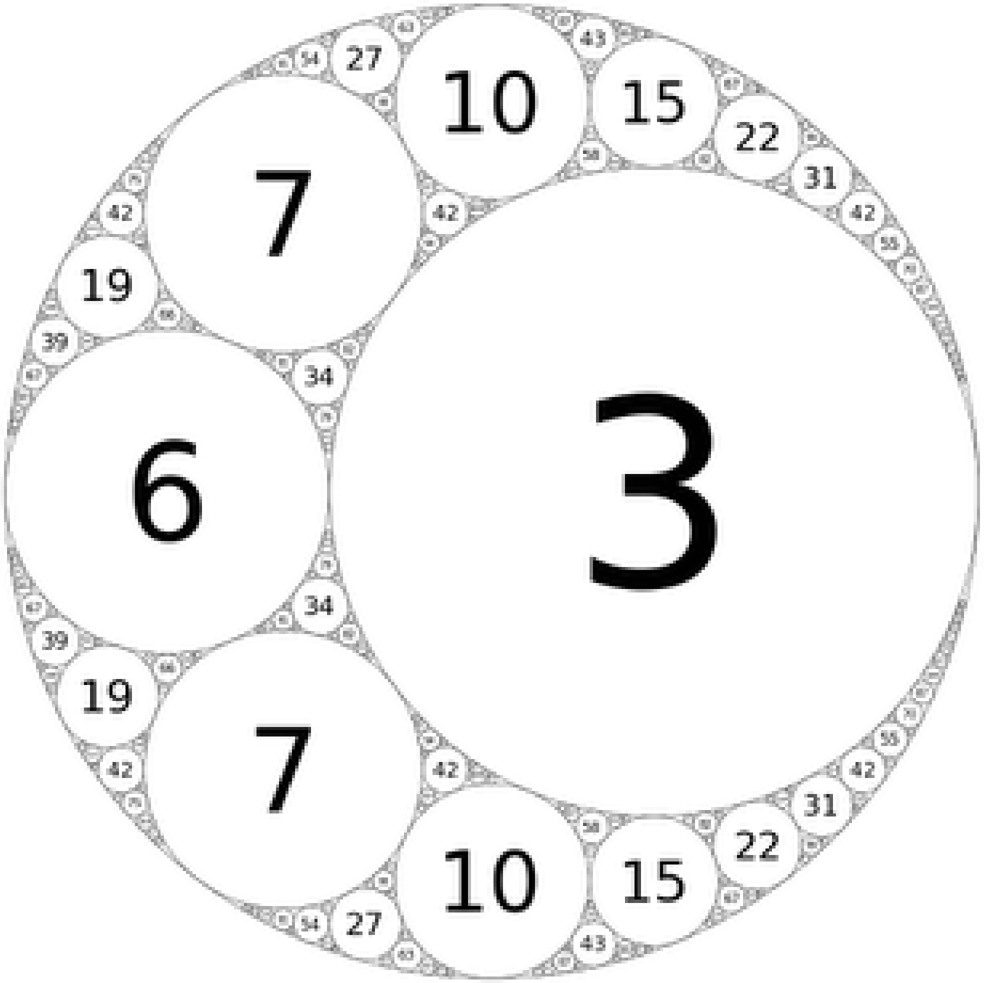
Bounded Integer Packings- Root Quadruples

The largest bounded packing is the $(-1, 2, 2, 3)$ packing, enclosed in a bounding circle of radius 1. The next largest is the $(-2, 3, 6, 7)$ packing, with bounding circle of radius $1/2$.



38
27
27
18
18
54
54
11
11
30
30
59
59
39
39
2
6
6
35
35
14
14
47
47
23
23
62
62
50
50
26
26
42
42
3
3
38
38
15
15
35
35
38
38
2
42
42
26
26
14
14
47
47
23
23
50
50
35
35
6
6
39
39
30
30
11
11
18
18
54
54
27
27
38


54
27
10
43
15
22
31
58
7
42
42
42
55
19
39
34
6
3
34
39
19
7
42
42
42
55
31
22
58
15
10
54
27
43


3
6
7
7
10
10
15
15
19
19
22
22
27
27
31
31
34
34
39
39
42
42
42
42
42
42
43
43
54
54
55
55
58
58

Root Quadruples and Number Theory

Theorem ([GLMWY 2003])

(1) For each $n \geq 1$ *there are finitely many primitive integral Apollonian circle packings having a root quadruple with smallest element equal to* $-n$*.*

(2) The number of such packings $N_{root}(-n)$ *is given by the (Legendre) class number counting primitive binary quadratic form classes of discriminant* $-4n^2$ *under the action of* $GL(2, \mathbb{Z})$*-equivalence.*

Remark. Thus, there is at least one root quadruple for every such $n \geq 1$.

Counting Curvatures of a Packing

Theorem (A. Kontorovich, H. Oh 2008) *Given any bounded Apollonian circle packing $\mathcal{P}$. The number $N(x)$ of circles in the packing having curvatures no larger than x satisfies*

$$N(x) \sim c(\mathcal{P}) x^{\alpha_0}$$

where $\alpha_0 \approx 1.3056$ is the Hausdorff dimension of the limit set of the packing, for a constant $c(\mathcal{P})$ depending on the packing.

Remark. For details, attend the talk of A. Kontorovich tomorrow.

Counting Curvatures of an Integer Packing

The Kontorovich-Oh result above says that the number of circles with curvatures smaller than x is proportional to $x^{1.3056}$.

Since there are only x positive integers smaller than x, that means: in an integer packing, on average, each integer is hit many times, about $x^{0.3056}$ times.

So we might expect a lot of different integers to occur in a packing. Maybe all of them, past some point...

Congruence Conditions

Theorem ([GLMWY 2003])
Let $\mathcal{P}$ be a primitive integer Apollonian circle packing $\mathcal{P}$. Then all integers in certain congruence classes

$$(\mathrm{mod}\ 24),$$

will be excluded as curvatures in such a packing. The excluded classes depend on $\mathcal{P}$, and there are at least 16 excluded classes in all cases.

Example. For the packing with $(0, 0, 1, 1)$ root quadruple, the allowed congruence classes are $0, 1, 4, 9, 12, 16$ (mod 24) and the remaining 18 residue classes are excluded.

Density of Integers in Integral Apollonian Packing

Positive Density Conjecture ([GLMWY 2003])

Let $\mathcal{P}$ be a bounded integer Apollonian circle packing. Then there is a constant C depending on $\mathcal{P}$ such that:

The number of different integer circle curvatures $N_{\mathcal{P}}^{(0)}(x)$ less than x satisfies

$$N_{\mathcal{P}}^{(0)}(x) > Cx$$

for all sufficiently large x.

Note added January 2012: This conjecture has been proved by J. Bourgain and E. Fuchs, JAMS **24** (2011), no.4, 945–967.

Density of Integers in Integral Apollonian Packings-2

Remarks. (1) Stronger conjecture: every sufficiently large integer occurs in each allowed congruence class (mod 24).

(2) The stronger conjecture is supported by computer evidence showing a dwindling number of exceptions in such congruence classes, with apparent extinction of exceptions in many classes.

(3) Theorem. (Sarnak 2007) *There are at least* $Cx/(\log x)$ *distinct curvatures smaller than* x.

Almost-Prime Descartes Configurations in an Integer Apollonian Packing

C- almost prime Descartes configurations are those integer Descartes configurations with curvatures (c_1, c_2, c_3, c_4) such that $c_1c_2c_3c_4$ has at most C distinct prime factors, i.e.

$$\omega(c_1c_2c_3c_4) \leq C.$$

Theorem. (J. Bourgain, A. Gamburd, P. Sarnak 2008) *Let $\mathcal{P}$ be an integer Apollonian circle packing. Then:*

there is a constant $C = C(\mathcal{P})$, such that the set of C- almost prime Descartes configurations it contains is infinite.

Remarks on Proofs

- Spectral gap is used by Bourgain, Gamburd, and Sarnak. They also use a sieve argument (Brun's sieve, Selberg sieve).

- The holographic structure (Kleinian group) is used by Kontorovich and Oh.

3. Fibonacci Numbers

- The Fibonacci numbers F_n satisfy $F_n = F_{n-1} + F_{n-2}$, initial conditions $F_0 = 0, F_1 = 1$, giving

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55 \cdots$$

- The Lucas numbers L_n satisfy $L_n = L_{n-1} + L_{n-2}$, $L_0 = 2, L_1 = 1$, giving

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \cdots$$

- They are cousins:

$$F_{2n} = F_n L_n.$$

Fibonacci Group

- The Fibonacci Group $\mathcal{F}$ is

$$\mathcal{F} = \{M^n : \quad n \in \mathbb{Z}\}$$

  with

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

- This group is an infinite cyclic subgroup of $GL(2, \mathbb{Z})$. It is of infinite index in $GL(2, \mathbb{Z})$.

Fibonacci Group Orbits-1

- Fibonacci and Lucas numbers are given by orbits of the Fibonacci group:

$$\begin{aligned}\mathcal{O}([1,0]^T) &:= \{M^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} : \ n \in \mathbb{Z}\} \\ &= \{\begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} \ n \in \mathbb{Z}\}.\end{aligned}$$

$$\mathcal{O}([1,2]^T) := \{\begin{bmatrix} L_{n+1} \\ L_n \end{bmatrix} \ n \in \mathbb{Z}\}$$

Fibonacci Group Orbit Divisibility

Problem. *Let*

$$\mathcal{O}([a,b]^T) = \{\left[\begin{array}{c} G_n \\ G_{n-1} \end{array}\right] \; n \in \mathbb{Z}\}$$

be an integer orbit of the Fibonacci group $\mathcal{F}$. How do the number of distinct prime divisors $\omega(G_n G_{n-1})$ behave as $n \to \infty$?

This is an analogue of the problem considered by Bourgain, Gamburd and Sarnak, for integer orbits of the Apollonian group, where this number is bounded by C infinitely often.

Fibonacci Quarterly

- Fibonacci numbers have their own journal: The Fibonacci Quarterly, now on volume 46.

- P. Erdős was an author or co-author of 4 papers in the Fibonacci Quarterly, as were Leonard Carlitz (18 papers), Doug Lind (13), Ron Graham (3) (two with Erdős), Don Knuth (3), D. H. Lehmer (2) , Emma Lehmer (2), Carl Pomerance (1) Andrew Granville (1), Andrew Odlyzko (1), myself (1).

Binary Quadratic Diophantine Equation (Non-Split Torus)

- Fibonacci and Lucas numbers (L_n, F_n) form the complete set of integer solutions to the Diophantine equation
$$X^2 - 5Y^2 = \pm 4.$$
with $\pm = (-1)^n$.

- This Diophantine equation identifies (F_n, L_n) as integer points on a anisotropic (non-split) algebraic torus over $\mathbb{Q}$, that splits over a quadratic extension $\mathbb{Q}(\sqrt{5})$.

- "Tori are poison" to the Bourgain-Gamburd-Sarnak theory.

Fibonacci Divisibility Problems

- Problem 1: What is the extreme minimal behavior of $\omega(F_n)$, the number of distinct prime factors of F_n (counted without multiplicity)?

- Problem 2: What is the extreme minimal behavior of $\omega(F_nF_{n-1})$, the number of prime factors of F_nF_{n-1} (counted without multiplicity)?

Probabilistic Number Theory

Paul Erdős was one of the founders of the subject of probabilistic number theory.

This is a subject that uses probability theory to answer questions in number theory. One idea is that different prime numbers behave in some sense like independent random variables. It can also supply heuristics, that suggest answers where they cannot be proved.

Fibonacci Prime Heuristic-1

- Fibonacci and Lucas numbers F_n, L_n grow exponentially, with growth rate $c = \frac{1}{2}(1 + \sqrt{5}) \sim 1.618$.

- The probability a random number below x is prime is $\approx \frac{1}{\log x}$. Applied to Fibonacci numbers, the heuristic predicts:

$$Prob[F_n \text{ is } \quad \text{prime}] \sim \frac{1}{n \log c} = \frac{C}{n}.$$

Fibonacci Prime Heuristic-2

- Since $\sum \frac{1}{n}$ diverges, the heuristic predicts infinitely many Fibonacci primes (resp. Lucas primes). The density of such primes having $n \le x$ is predicted to grow like

$$\sum_{n \le x} \frac{1}{n} \sim \log x.$$

- Thus supports: Conjecture 1 :

$$\liminf_{n \to \infty} \omega(F_n) = 1,$$

as an answer to Problem 1. [Same heuristic for infinitely many Mersenne primes $M_n = 2^n - 1$.]

Expected Number of Prime Factors

Approach to Problem 2: estimate the number of prime divisors of a random integer.

Theorem (Hardy-Ramanujan 1917) *The number of distinct prime factors of a large integer* m *is usually near* $\log\log m$. *In fact for any* $\epsilon > 0$ *almost all integers satisfy*

$$|\omega(m) - \log\log m| \leq (\log\log m)^{1/2+\epsilon}$$

An Aside: Erdős-Kac Theorem

Erdős-Kac Theorem (1939)

Assign to each integer n the scaled value

$$x_m := \frac{\omega(m) - \log\log m}{\sqrt{\log\log m}}$$

Then as $N \to \infty$ the cumulative distribution function of such sample values $\{x_m : 1 \le m \le N\}$ approaches that of the standard normal distribution $N(0,1)$, which is

$$Prob[x \le \lambda] = \frac{1}{2\pi}\int_{-\infty}^{\lambda} e^{-\frac{1}{2}t^2} dt.$$

Erdős Pal

Fibonacci Product Heuristic-1

- What is the minimal expected number of prime factors $\omega(F_n F_{n-1})$?

- Assume, as a heuristic, that F_n, F_{n-1} factor like independent random integers drawn uniformly from $[1, 2^n]$. Want to find that value of λ such that

$$Prob[\omega(F_n F_{n-1}) < \lambda \log\log(F_n F_{n-1})] \sim \frac{1}{n^{1+o(1)}}.$$

- This gives the threshold value for infinitely many occurrences of solutions.

Fibonacci Product Heuristic-2

- One finds threshold value

$$\lambda := \beta_2 \sqrt{\log \log x}$$

with $\beta_2 \approx 0.3734$ given as the unique solution with $0 < \beta_2 < 2$ to

$$\beta_2 (1 + \log 2 - \log \beta_2) = 1.$$

[Tail of distribution: Erdös-Kac theorem not valid!]

- This suggests: $\omega(F_n F_{n-1}) \to \infty$, with

$$\liminf_{n \to \infty} \frac{\omega(F_n F_{n-1})}{\log \log (F_n F_{n-1})} \geq \beta_2 \approx 0.3734.$$

as an answer to Problem 2.

Fibonacci Product Heuristic-3

- The heuristic can be improved by noting that at least one of $n, n+1$ is even and $F_{2m} = F_m L_m$. Thus $F_n F_{n+1} = F_m L_m F_{2m \pm 1}$ has three "independent" factors. One now predicts threshold value:

$$\lambda := \beta_3 \sqrt{\log \log x}$$

with $\beta_3 \approx 0.9137$, given as the unique solution with $0 < \beta_3 < 3$ to $\beta_3(1 + \log 3 - \log \beta_3) = 2$.

- This suggests: Conjecture 2: $\omega(F_n F_{n-1}) \to \infty$, with

$$\liminf_{n \to \infty} \frac{\omega(F_n F_{n-1})}{\log \log(F_n F_{n-1})} \geq \beta_3 \approx 0.9137.$$

Difficulty of these Problems

- Difficulty of conjectures 1 and 2:
  "Hopeless. Absolutely hopeless".

- What one can do: Test the conjectures against empirical data.

Aside: Perfect Numbers

A number is perfect if it is the sum of its proper divisors. For example $6 = 1 + 2 + 3$ is perfect.

Theorem (Euclid, Book IX, Prop. 36)
If $2^n - 1$ is a prime, then

$$N = 2^{n-1}(2^n - 1)$$

is a perfect number.

Note. If $2^n - 1$ is prime, then it is called a Mersenne prime.

Aside: Perfect Numbers-2

Theorem (Euler, 1732ff)

If an even number N is perfect, then it has Euclid's form

$$N = 2^{n-1}(2^n - 1),$$

with $2^n - 1$ a prime.

- This theorem gives an incentive to factor Mersenne numbers: those of form $2^n - 1$. Much effort has been expended on this.

- Cunningham factoring project. Factoring Fibonacci numbers is a spinoff.

Factoring Fibonacci Numbers

- Factoring Fibonacci and Lucas numbers has been carried out on a large scale. J. Brillhart, P. L. Montgomery, R. D. Silverman, (Math. Comp. 1988), and much since. Web pages of current records are maintained by Blair Kelly.

- Fibonacci numbers F_n have been completely factored for $n \leq 1000$, and partially factored for $n \leq 10000$. Fibonacci primes have been determined up to $n \leq 50000$ and have been searched somewhat further, to at least $n = 200000$, without rigorous proofs of primality.

- Lucas numbers L_n and primes determined similarly.

Test Heuristic

Test of $\omega(F_nF_{n+1}) = k$ for $n \leq 10000$. Empirically there appear to be cutoff values. [Heuristic cutoff: $0.9137 \log n = k$.]

- For $k = 2$, largest solution $n = 2$ (unconditionally proved).
- For $k = 3$, largest solution $n = 6$. [Heuristic: $n = 26$]
- For $k = 4$, largest solution $n = 22$. [Heuristic: $n = 79$.]
- For $k = 5$, largest solution $n = 226$. [Heuristic: $n = 238$.]
- For $k = 6$, largest solution $n = 586$. [Heuristic: $n = 711$.]

Simultaeous Prime Heuristic

- *Question 3*: How many Fibonacci and Lucas numbers F_n and L_n are simultaneously primes? (That is, that $\Omega(F_n L_n) = 2$.)

- Know that $gcd(F_n, L_n) = 1$. This leads to similar heuristic prediction:
$$\liminf_{n \to \infty} \frac{\omega(F_n L_n)}{\log \log (F_n L_n)} = \beta_2 \approx 0.3734.$$
This leads to prediction that finitely many F_n, L_n are simultaneously primes. and heuristic that largest n has $0.3734 \log n \approx 2$ so $n \approx 220$.

Fibonacci Primes

- For any Fibonacci prime, n must be a prime or a power of 2, up to 4.

- *Fibonacci Prime List to* $n < 50,000$ [N=32]

$$\begin{aligned} n \;=\; & 3,4,5,7,11,13,17,23,29,43,47,83,131,137,359,431 \\ & 31,433,449,509,569,571,2971,4723,5387,9311,9677, \\ & 14431,25561,30757,35999,37511,50833,81839 \end{aligned}$$

- *Probable Fibonacci Primes* $50,000 < n < 200,000$ [N=5]

$$n = 81839^{*}, 104911, 130021, 148091, 201107$$

Lucas Primes

- For any Lucas prime, n must be a prime or a power of 2, up to 16.

- *Lucas Prime List to* $n < 50,000$ [N=41]

$$\begin{aligned} n \;=\; & 0,2,4,5,7,8,11,13,16,17,19,31,37,41,47,53,61,71, \\ & 79,113,313,353,503,613,617,863,1097,1361,4787, \\ & 4793,5851,7741,8467,10691,12251,13963,14449, \\ & 19469,35449,36779,44507 \end{aligned}$$

- *Probable Lucas Primes* $50,000 < n < 200,000$ [N=10]

$$\begin{aligned} n \;=\; & 51169^{*},56003,81671,89849,94823,140057,148091, \\ & 159521,183089,193201 \end{aligned}$$

Simultaneous Fibonacci and Lucas Primes

- The simultaneous Fibonacci and Lucas primes $F_n =$ prime, $L_n =$ prime, are, for $n < 50,000$,

$$n = 2, 4, 5, 7, 11, 13, 47$$

- This is consistent with the heuristic above, which predicts a cutoff value $n \approx 220$.

An Outlier!

- The simultaneous Fibonacci and Lucas probable primes $F_n =$ prime, $L_n =$ prime, are, for $n < 200,000$ includes an outlier

  $$n = 148091$$

  Here F_n has 30949 decimal digits, and L_n has 30950 digits.

- These F_n, L_n are not certified to be primes. However they have both passed many pseudoprimality tests. (Probable primality for F_n noted by T. D. Noe and L_n by de Water.)

An Outlier-2

- The heuristic suggests (very roughly) that $F_n L_n$ should have about 4.5 prime factors between them.

- This provides some incentive to implement the full Miller primality test (valid on GRH) on F_{148091} and L_{148091}. (Two years of computer time.)

- Should one believe:

  (a) These are both primes? or:

  (b) Is at least one composite, the Miller test is passed, and the GRH false?

Explaining Away the Outlier

- *Question.* What is the expected size of the maximal n such that $\omega(F_n L_n) = 2$?

- *Probabilistic Model.* Draw pairs of integers (x_n, y_n), independently and uniformly from $2^n \le x_n \le 2^{n+1}$, for each $n \ge 1$. Estimate the expected value

$$E[\ \max\{n : \omega(x_n y_n) \le 2\}\ ].$$

- *Answer.* For any fixed $k \ge 2$,

$$E[\ \max\{n : \omega(x_n y_n) \le k\}\ ] = +\infty!$$

3. Peroratio: What is mathematics?

Thesis: Mathematics has a Fractal structure

- There is a ”structural core” of well-organized theories, illustrating the science of symmetry and pattern.
- On the fringes, the structure dissolves. There are pockets of order, surrounded by fractal tendrils, easy-to-state, difficult (or unsolvable) problems.
- On the fringes, conjectures formulating “unifying principles” turn out to be false.

What is mathematics-2?

Number theory is a fertile source of "fringe" problems.

- $3x + 1$ *Problem*: Iterate $C(n) = n/2$ if n even, $C(n) = 3n + 1$ if n odd. Do all positive numbers n iterate to 1? [Conjecture: Yes.]

- *Aliquot Divisors*: Iterate the function
$$\sigma^*(n) = \sigma(n) - n,$$
the sum of proper divisors of n, e.g. $\sigma^*(6) = 1 + 2 + 3 = 6$. Are all iteration orbits bounded?
[Conjecture: Yes. But some say: No]

What is mathematics-3?

- The “fringe” moves over time.

  What was once unfashionable, or disconnected from “core mathematics”, may become related to it through new discoveries. New islands of order may emerge.

- Erdös was a leader in bringing several new islands of order into mathematics. One such island was: ”Probabilistic Number Theory.” Another was: “Random Graphs”.

Thank you for your attention!