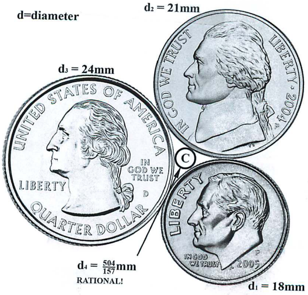
Number Theory and the Circle Packings of Apollonius

Peter Sarnak
Mahler Lectures 2011

Apollonius of Perga
lived from about 262 BC to about 190 BC
Apollonius was known as 'The Great Geometer'. His famous book *Conics* introduced the terms parabola, ellipse, and hyperbola.


UNITED STATES OF AMERICA
LIBERTY
IN GOD WE TRUST
QUARTER DOLLAR
IN GOD WE TRUST
LIBERTY · 2004
LIBERTY
IN GOD WE TRUST
2005


d=diameter
$d_2 = 21$mm
$d_3 = 24$mm
C
$d_4 = \frac{504}{157}$mm
RATIONAL!
$d_1 = 18$mm

Scale the picture by a factor of 252 and let
$a(c) =$ curvature of the circle $c = 1/\mathrm{radius}(c)$.

The curvatures are displayed. Note the outer one by convention has a negative sign.
By a theorem of Apollonius, place unique circles in the lines.

The Diophantine miracle is the curvatures are integers!

Repeat ad infnitum to get <u>an</u> integral Apollonian packing:

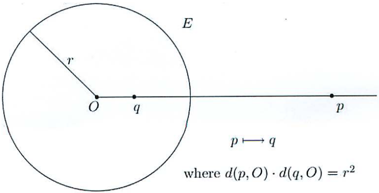
- There are infinitely many such P's.

Basic questions (Diophantine)
Which integers appear as curvatures?
Are there infinitely many prime curvatures, twin primes i.e. pairs of tangent circles with prime curvature?

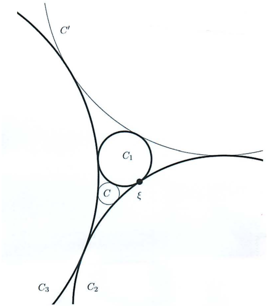
- The integral structure — F. Soddy (1936)
- Diophantine setup and questions — R. Graham–J. Lagarias–C. Mellows–L. Wilks–C. Yan (2000)
- Many of the problems are now solved
  Recent advances in modular forms, ergodic theory, hyperbolic geometry, and additive combinatorics.

Apollonius' Theorem

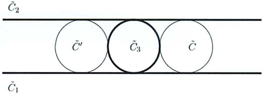
Given three mutually tangent circles c_1, c_2, c_3, there are exactly two circles c and c' tangent to all three.



Inversion in a circle takes circles to circles and preserves tangencies and angles.



c_1, c_2, c_3 given invert in ξ ($\xi \to \infty$) yields



Now the required unique circles $\widetilde{c}'$ and $\widetilde{c}$ are clear
$\longrightarrow$ invert back.

Descartes' Theorem

Given four mutually tangent circles whose curvatures are a_1, a_2, a_3, a_4 (with the sign convention), then

$$F(a_1, a_2, a_3, a_4) = 0,$$

where F is the quadratic form

$$F(a) = 2(a_1^2 + a_2^2 + a_3^2 + a_4^2) - (a_1 + a_2 + a_3 + a_4)^2.$$

I don't know of the proof "from the book". (If time permits, proof at end.)

Diophantine Property:

Given c_1, c_2, c_3, c_4 mutually tangent circles, a_1, a_2, a_3, a_4 curvatures. If c and c' are tangent to c_1, c_2, c_3, then

$$F(a_1, a_2, a_3, a_4) = 0$$
$$F(a_1, a_2, a_3, a_4') = 0$$

So a_4 and a_4' are roots of the same quadratic equation $\implies$

$$
\begin{aligned}
a_4 + a_4' &= 2a_1 + 2a_2 + 2a_3 \qquad (1)\\
a_4, a_4' &= a_1 + a_2 + a_3 \pm 2\sqrt{\Delta}\\
\Delta &= a_1 a_2 + a_1 a_3 + a_2 a_3
\end{aligned}
$$

(our example $(a_1, a_2, a_3) = (21, 24, 28)$, $\Delta = 1764 = 42^2$)
If c_1, c_2, c_3, c_4 have integral curvatures, then c_4' also does from (1)!
In this way, every curvature built is integral.

Apollonian Group:
(1) above $\implies$ that in forming a new curvature when inserting a new circle

$$a_4' = -a_4 + 2a_1 + 2a_2 + 2a_3$$

Set

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

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

$$a' = aS_4, \qquad a' = (a_1, a_2, a_3, a_4') \in \mathbb{Z}^4$$

Similarly with generating $c_1, c_2, c_4, \ldots$.

$$S_j^2 = I, \quad S_j \in \mathrm{GL}_4(\mathbb{Z}), \quad j = 1, 2, 3, 4.$$

Definition

A is the subgroup of $\mathrm{GL}_4(\mathbb{Z})$ generated by S_1, S_2, S_3, S_4; called the Apollonian group.

- It is the symmetry group for any integral Apollonian packing.

If $a \in \mathbb{Z}^4$ is a fourtuple of curvatures of 4 mutually tangent circles in P, then the orbit

$$\mathcal{O}_a = aA \subset \mathbb{Z}^4$$

gives all such 4-tuples in P.

Any a as above satisfies

$$F(a) = 0 \qquad \text{(i.e. we are on a cone)}$$

Not surprisingly,

$$F(xS_j) = F(x)$$

F as a real quadratic form has signature $3, 1$ and S_j and hence A are all orthogonal!

O_F the orthogonal group of F.
$\mathrm{O}_F(\mathbb{Z})$ the orthogonal matrices whose entries are integers.

$$A \leq \mathrm{O}_F(\mathbb{Z}).$$

Key feature: (defines our problem)

(i) A is "thin"; it is of infinite index in $\mathrm{O}_F(\mathbb{Z})$

(ii) A is not too small — it is "Zariski dense" in O_F.

The group $\mathrm{O}_F(\mathbb{Z})$ is an arithmetic group. It appears in the modern theory of integral quadratic equations.

- Hilbert's 11-th problem concerns solvability of such equations — solved only recently (2000).

To put Hilbert's 11th problem in context: it is a generalization of the following classical result:
Which numbers are sums of three squares?

$$n = x^2 + y^2 + z^2, \quad x, y, z \in \mathbb{Z}.$$

"Local obstruction": if

$$n = 4^a(8b + 7)$$

then n is not a sum of three squares (consider arithmetic on dividing by 8).

- Gauss/Legendre (1800) (local to global principle): n is a sum of three squares iff $n \neq 4^a(8b + 7)$.

$$V = \{x : F(x) = 0\} \qquad \text{cone in } \mathbb{R}^4$$

$V^{\mathrm{prim}}(\mathbb{Z})$ = points with integer coordinates and $\gcd(a_1, a_2, a_3, a_4) = 1$.

Then

$$V^{\mathrm{prim}}(\mathbb{Z}) = a\mathrm{O}_F(\mathbb{Z})$$

(i.e. one orbit for all points)
$V^{\mathrm{prim}}(\mathbb{Z})$ has infinitely many orbits under A — each corresponding to a different Apollonian packing.

Such "thin groups" come up in many places in number theory. While the powerful modern theory of automorphic forms says nothing about them, there is a flourishing theory of thin groups. It allows for the solution of many related problems.

<u>Counting:</u> $x \geq 1$,

$$N_P(x) := |\{c \in P : a(c) \leq x\}|$$

Theorem (D. Boyd)

$$\lim_{x \to \infty} \frac{\log N_P(x)}{\log x} = \delta = 1.305\ldots$$

"Hausdorff dimension of limit set of the Apollonian Gasket" — elementary arguments

Using tools from hyperbolic 3 manifolds — Laplacians

Theorem (A. Kontorovich–H. Oh 2009)

There is $b = b(P) > 0$ such that

$$N_P(x) \sim bx^{\delta} \quad \text{as } x \to \infty.$$

$$b(P_o) \approx 0.0458\ldots$$

$b(P)$ is determined in terms of the base eigenfunction of the infinite volume "drum" $A \setminus \mathrm{O}_F(\mathbb{R})$.

Diophantine Analysis of P:

Which integers occur as curvatures?

- There are congruence restrictions — that is, in arithmetic on dividing by q, "mod q".

For P_0 for example,

$$\text{every } a(c) \equiv 0, 4, 12, 13, 16, 21 \pmod{24}$$

Theorem (E. Fuchs 2010)

The above is the only congruence obstruction for P_0.

One can examine the reduction

$$A \longrightarrow \mathrm{GL}_4(\mathbb{Z}/q\mathbb{Z}) \quad \text{for } q \geq 1 \text{ (finite group).}$$

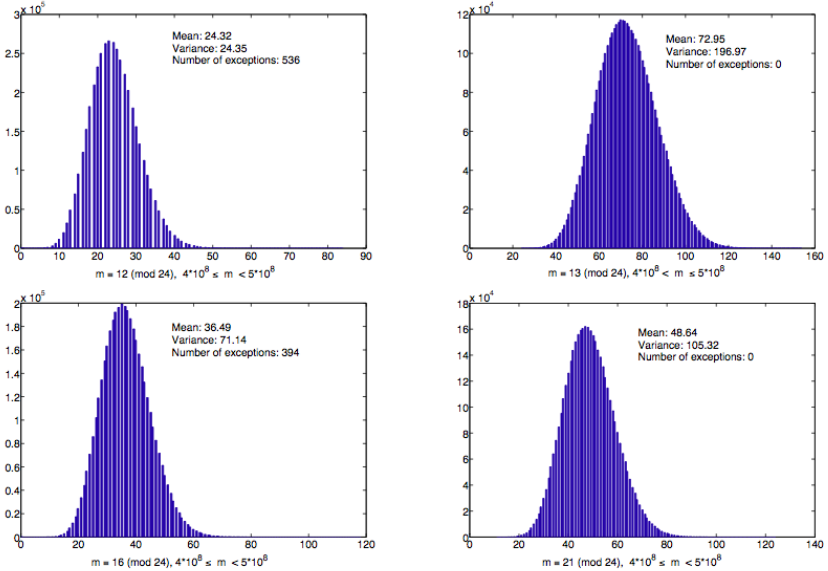
Fuchs determines the precise image.
[Here the "Zariski density" is used; Weisfeiller's work.]

$\#$ of integers $\leq x$ that are hit with multiplicity is $\sim x^{1.3\cdots}$.
So we might hope that a positive density (proportion) of integers are curvatures.

Theorem (J. Bourgain, E. Fuchs 2010)

There is $C > 0$ such that the number of integers $< x$ which are curvatures is at least Cx.

Much more ambitious is the local to global principle: that except for a finite number of integers, every integer satisfying the congruence (mod 24) is a curvature.


x 10^5
Mean: 24.32
Variance: 24.35
Number of exceptions: 536
m ≡ 12 (mod 24), 4*10^8 ≤ m < 5*10^8
x 10^4
Mean: 72.95
Variance: 196.97
Number of exceptions: 0
m ≡ 13 (mod 24), 4*10^8 < m ≤ 5*10^8
x 10^5
Mean: 36.49
Variance: 71.14
Number of exceptions: 394
m ≡ 16 (mod 24), 4*10^8 ≤ m < 5*10^8
x 10^4
Mean: 48.64
Variance: 105.32
Number of exceptions: 0
m ≡ 21 (mod 24), 4*10^8 ≤ m < 5*10^8

Primes:

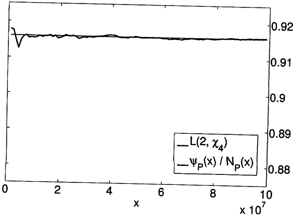
Are there infinitely many prime $a(c)$'s in P_0? Or twins such as 157 and 397 in the middle?

Theorem (S. '07)

In any integral Apollonian packing, there are infinitely many c's with $A(c)$ prime and, better still, infinitely many pairs c, c' with $a(c)$ and $a(c')$ prime.

Is there a prime number theorem? Möbius heuristics suggest yes.

$$\Psi_P(x) := \sum_{\substack{c \in P \\ a(c) \text{ prime} \\ a(c) \le x}} \log a(c), \qquad \frac{\Psi_P(x)}{N_P(x)} \longrightarrow L(2, \chi_4) = 0.9159\ldots ??$$



Using the "affine sieve" for thin groups

Theorem (Kontorovich–Oh 2009)

x large,

$$\pi_P(x) = |\{c \in P : a(c) \le x; a(c) \text{ prime}\}| \le \frac{CN_P(x)}{\log x}$$

Some references:

- J. Bourgain and E. Fuchs, JAMS **24** (2011), 945–967.
- D. Boyd, Math. Comp. **39** (1982), 249–254.
- J. Cogdell, "On sums of three squares", J. Théor. No. Bordeaux **15** (2003), 33–44.
- H. Coxeter, Aequationes Math. **1** (1968), 104–121.
- W. Duke, Notices AMS **44**(2) (1997), 190–196.
- E. Fuchs, "Arithmetic properties of Apollonian circle packings", Ph.D. thesis, Princeton (2010).
- E. Fuchs and K. Sanden, "Some experiments with integral Apollonian circle packings", arXiv, January 2010.
- R. Graham, J. Lagarias, C. Mallows, R. Wilks, and C. Yan, J. Number Theory **100** (2003), 1–43.

- A. Kontorovich and H. Oh, JAMS **24** (2011), 603–648.
- P. Sarnak, letter to J. Lagarias on integral Apollonian packings, www.math.princeton.edu/sarnak/ (2007).
- P. Sarnak, "Integral Apollonian packings", Amer. Math. Monthly 118.04.291 (2011).
- F. Soddy, Nature **137** (1936), 1021.