Number Theory and the Circle Packings of Apollonius

Peter Sarnak

Johannesburg, July 2014

- Number Theory is concerned with the study of whole numbers, diophantine equations, prime numbers . . .

- Easy to state questions - often every difficult to answer

- We highlight some examples coming from elementary geometry.

A classical result:

Sums of Three Squares

$$x_1^2 + x_2^2 + x_3^2 = n$$

to be solved in integers

$$x_1, x_2, x_3.$$

Local Obstructions:

If $n \equiv 7(mod 8)$

(that is it gives remainder 7 when divided by 8)
then

$$x_j^2 \equiv 0, 1, 4(mod 8)$$

so 7 is impossible.

Similarly if

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

then n is not a sum of three squares.

Theorem (Gauss 1800)

If $0 < n \neq 4^a(8b+7)$ then there are integers x_1, x_2, x_3 such that

$$x_1^2 + x_2^2 + x_3^2 = n$$

That is our congruence obstruction is the only one!

- Such local to global principle are rare and much sought.

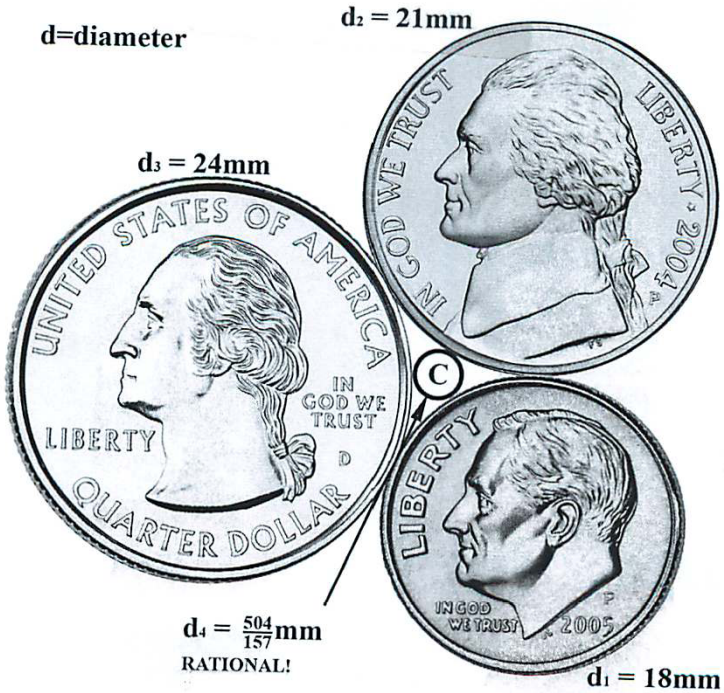
Comment:
The general question of representation of integers by integral quadratic forms (local to global principles) over number fields is Hilbert's 11-th problem. It was resolved completely relatively recently (2001) using the theory of automorphic forms. In general for forms in 3 variables the local to global is valid with finitely many exceptions.

A Diophamtine Problem from Geometry

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
IN GOD WE TRUST
LIBERTY
D
QUARTER DOLLAR
IN GOD WE TRUST
LIBERTY
2004
LIBERTY
IN GOD WE TRUST
2005

d=diameter


$d_2 = 21mm$
$d_3 = 24mm$
UNITED STATES OF AMERICA
IN GOD WE TRUST
LIBERTY
D
QUARTER DOLLAR
IN GOD WE TRUST
LIBERTY
2004
LIBERTY
IN GOD WE TRUST
2005
C
$d_4 = \frac{504}{157}mm$
RATIONAL!
$d_1 = 18mm$

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

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

The Diophantine miracle is the curvatures are integers!

Repeat ad infnitum to get an integral Apollonian packing:

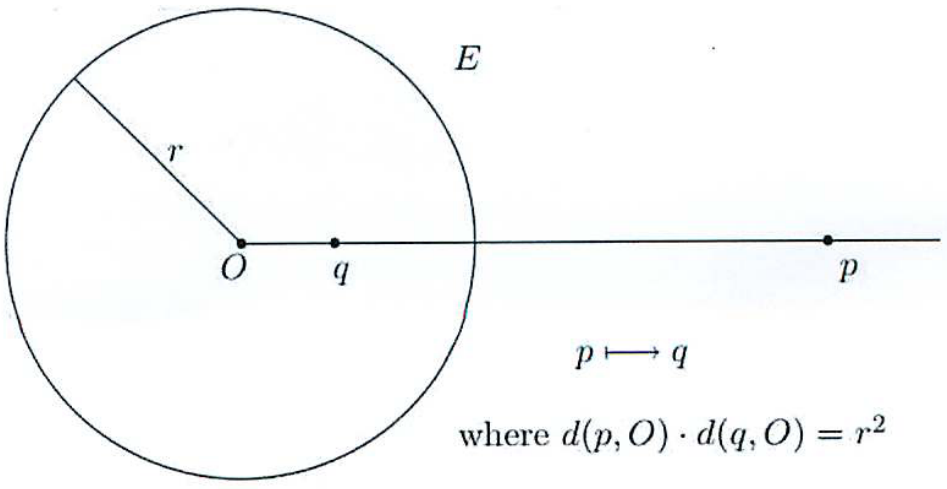
- There are infinitely many such P's.

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?

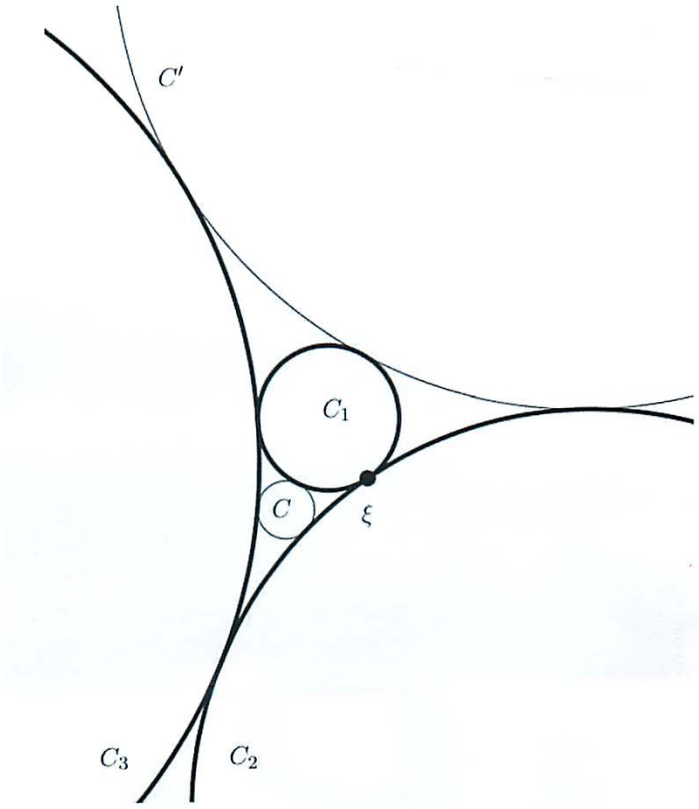
- The integral structure - F. Soddy (1936)

- Diophantine setup and questions - R. Graham - J. Lagarias - C. Mellows - L. Wilks - C. Yan (2000)

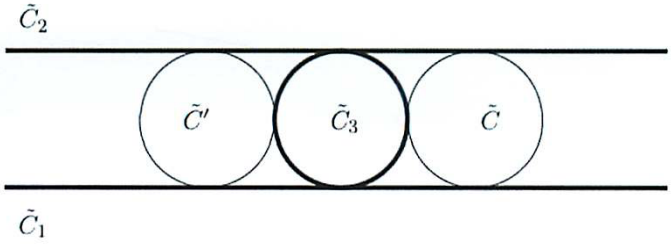
Apollonius' Theorem
Given three mutually tangent circles c_1, c_2, c_3, there are exactly two circles c and c' tangent to all three.



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



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



Now the required unique circles $\tilde{c}'$ and $\tilde{c}$ are clear $\to$ 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".

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 $\Longrightarrow$

$$a_4 + a_4^{'} = 2a_1 + 2a_2 + 2a_3 \qquad (1)$$
$$a_4, a_4^{'} = a_1 + a_2 + a_3 \pm 2\sqrt{\Delta}$$
$$\Delta = a_1a_2 + a_1a_3 + a_2a_3$$

(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 $\Longrightarrow$ that in forming a new curvature when inserting a new circle

$$a_4^{'} = -a_4 + 2a_1 + 2a_2 + 2a_3$$

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

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

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

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

$$S_j^2 = I, \quad S_j \in GL_4(\mathbb{Z}), \quad j = 1,2,3,4.$$

"GL_4" consists of all 4×4 invertible matrices.

Definition
A is the subgroup of $GL_4(\mathbb{Z})$ generated by S_1, S_2, S_3, S_4; called the Apollonian group.

- It is the symmetry group (Galois group) of 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

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

gives all such 4-tuples in P.

Any a as above satisfies

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

Not surprisingly,

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

F as a real quadratic form has signature (3,1) and S_j and hence A all preserve F!

- O_F : The orthogonal group of F, that is all 4×4 matrices preserving F

- $O_F(\mathbb{Z})$ The orthogonal matrices whose entries are integers

- $A \leq O_F(\mathbb{Z})$

Key Feature (Defines our problem)

(i) A is "thin" it is of infinite index in $O_F(\mathbb{Z})$.

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

The group $O_F(\mathbb{Z})$ is an "arithmetic" group. These appear in the modern theory of quadratic and automorphic forms.

$V = \{x : F(x) = 0\}$, cone in affine space

$V^{prim}(\mathbb{Z}) =$ points with integer coordinates

and $gcd(a_1, a_2, a_3, a_4) = 1$

Then $V^{prim}(\mathbb{Z}) = a.O_F(\mathbb{Z})$

However $V^{prim}(\mathbb{Z})$ has infinitely many orbits under A and there is no algebraic description of these.
Note: Solving $x_1 = t$ for $x \in V(\mathbb{Z})$ becomes a ternary integral quadratic equation - which has a local to global principle according to Hilbert's 11-th problem. Our problem is similar but for the thin group A!

Local Obstructions for P (E. Fuchs 2010)
For any c in P

$a(c) \equiv 0, 4, 12, 13, 16, 21 (mod 24)$

and these are the only such.

Local to Global Conjecture:
Graham-Lagarius-Mellows-Wilks-Yan 2003,
Fuchs-Sanden 2011
There is an N_0 such that if $n \geqslant N_0$ satisfies the necessary congruence above, then n is a curvature of a circle, $c \in P$.

The last 8 years have seen the development of a Diophantine theory of thin matrix groups. Some examples of what can be proven for integral Apollonian packings are:

Theorem 1(2007)

(i) There are infinitely many circles $c \in \underline{P}$ for which $a(c)$ is a prime number.

(ii) "Twin primes" there are infinitely many pairs of mutually tangent circles c and d in P such that $a(c)$ and $a(d)$ are prime.

More generally one can answer questions connected with the "affine-sieve".

Aside: How about the real twin primes?

- J. Chen's result from the 70's is still the best known towards the twin prime conjecture:

Striking progress on the gaps between primes:

1. Breakthrough by Goldston-Pinte-Yildirim (2005)

2. Y. Zhang (May 2013): There is $k < \infty$ such that x and $x+k$ are both prime for infinitely many x.

3. J. Maynard (Nov 2013) Given $m \geqslant 1$ there are $0 < k_1 < k_2 \ldots < k_m$ such that $x, x+k_1, \ldots, x+k_m$ are all prime for infinitely many x.

Back to our integral packings

<u>Theorem 2</u> (Bourgain - Kontorovich 2012)

Let E be the set of n's satisfying the necessary congruence conditions for being a curvature, but for which there is no $c \in \underline{P}$ such that $a(c) = n($ so E is the exceptional set to the local to global conjecture and should be finite), then E has zero density

$$\lim_{x\to\infty} \frac{|\{n \in E : n \leq x\}|}{x} = 0$$

One can also count asymptotically the number $N_{\underline{P}}(T)$ of circles in $\underline{P}$ whose curvature is at most T (Boyd, Kontorovich-Oh, Oh-Shah ...).

$$N_{\underline{P}}(T) \sim C_{\underline{P}} T^{\delta} \quad \text{as} \quad T \to \infty, \delta = 1.305\ldots.$$

Thin Matrix Groups

$GL_n(\mathbb{Z})$ is the group of $n \times n$ integral matrices of determinant ± 1.

$\Gamma \leqslant GL_n(\mathbb{Z})$ a subgroup

$G = Zc\ell(\Gamma)$, the Zariski closure of Γ, that is the smallest algebraic subgroup (defined by polynomial equations) to contain Γ.

Γ is "arithmetic" if Γ is finite index in $G(\mathbb{Z})$ and it is "thin" otherwise.

These arise naturally as soon as Γ is given in terms of generators such as for:

- Geometrically defined groups such as the Apollonian group

- Monodromy groups of differential equations and of families of algebraic varieties.

Note: Recognizing if a given Γ is thin or not has no decision procedure !

The Diophantine theory of thin matrix groups is concerned with techniques to study Diophantine problems on orbits of such groups. Among the novel tools used are expander graphs from combinatorics.

Some references:

1. "Apollonian Circle Packings: Number Theory" R. Graham, J. Lagarias, C. Mallows, A. Wilks, C. Yan, J. Number Theory 100 (2003), 1 - 45.

2. "Integral Apollonian Packings" P. Sarnak, American Math Monthly, 118 (2011), 291 - 306.

3. "From Apollonius to Zaremba, Local-Global Phenomena in Thin Orbits" A. Kontorovich, BAMS, 50 (2013), 187 - 228.

4. "Counting Problems in Apollonian Packings" E. Fuchs, BAMS, 50 (2013), 229 - 266.

5. "Notes on Thin Matrix Groups" P. Sarnak, in MSRI Publications Vol 61 (2014), 343 - 362.

6. "Apollonian Circle Packings: Dynamics and Number Theory" H. Oh, Japanese JNL of Math Vol 9 (2014), 69 - 97.