The Affine Sieve Markoff Triples and Strong Approximation

Peter Sarnak

GHYS Conference, June 2015

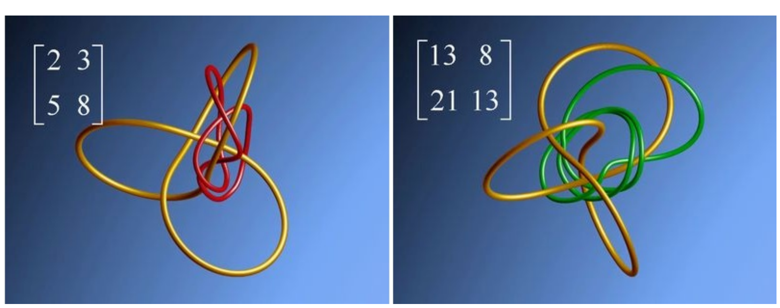
The Modular Flow on the Space of Lattices

Guest post by Bruce Bartlett

The following is the greatest math talk I've ever watched!

- Etienne Ghys (with pictures and videos by Jos Leys), Knots and Dynamics, ICM Madrid 2006.

"I wasn't actually at the ICM; I watched the online version a few years ago, and the story has haunted me ever since. Simon and I have been playing around with some of this stuff, so let me share some of my enthusiasm for it!"



Affine Sieve

Γ a group of affine polynomial maps of affine n-space $\mathbb{A}^n$ which preserve $\mathbb{Z}^n$. Fix a $\in \mathbb{Z}^n$.

$$O := \Gamma \cdot a \text{ , the orbit of } a \text{ under } \Gamma.$$

$O \subset \mathbb{Z}^n$, $V := Zcl(O)$, the Zariski closure of O.

V is defined over $\mathbb{Q}$.

Diophantine analysis of O:

- Strong Approximation; for $q \geqslant 1$

$$O \xrightarrow{red\ mod\ q} \quad V(\mathbb{Z}/q\mathbb{Z}).$$

What is the image?

• Sieving for primes or almost primes.

If $f \in \mathbb{Z}[x_1, x_2, \dots x_n]$, not constant on O; is the set of $x \in O$ for which $f(x)$ is prime (or has at most a fixed number r prime factors) Zariski dense in V?

Examples of Γ and Orbits:

(1) Classical (automorphic forms)

$\Gamma \leqslant GL_3(\mathbb{Z})$ generated by

$$\begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix},$$

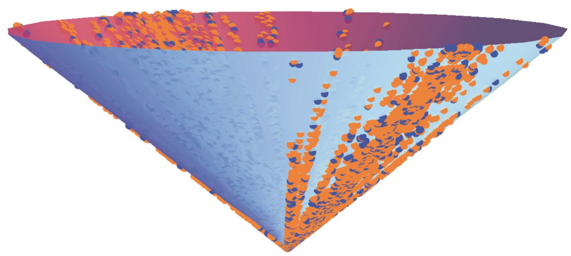
Γ is a finite index subgroup of $O_f(\mathbb{Z})$, where

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$$

Γ is an arithmetic group

$$O = \Gamma \cdot (3,4,5)$$

yields all (primitive) Pythagorean triples.



(2) Γ linear and "thin", not so classical:

$\Gamma = A \subset GL_4(\mathbb{Z})$ the Apollonian Group generated by the involutions S_1, S_2, S_3, S_4

$$\begin{bmatrix} -1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 2 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & -1 \end{bmatrix}$$

S_j corresponds to switching the root x_j to its conjugate on the cone

$$F(x) = 0 \text{ , where}$$

$$F(x_1, x_2, x_3, x_4) = 2(x_1^2 + x_2^2 + x_3^2 + x_4^2) - (x_1 + x_2 + x_3 + x_4)^2.$$

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

but while $Zcl(A) = O_F$, A is of infinite index in $O_F(\mathbb{Z})$, i.e. “thin".

The orbits of A in $\mathbb{Z}^4$ corresponds to the curvatures of 4 mutually tangent circles in an integral Apollonian packing.

For example $O = A.(-11, 21, 24, 28)$

corresponds to:

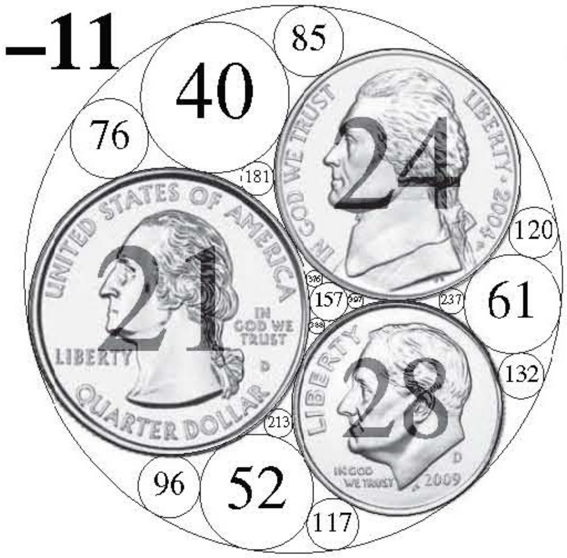


Figure 5.

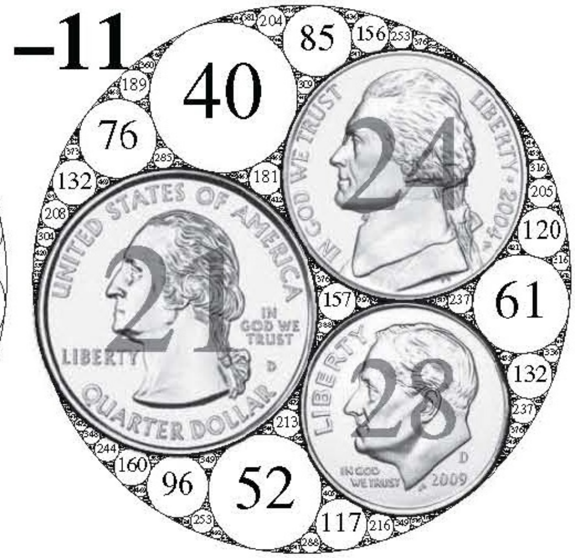


Figure 6.

(3) Markoff Equation (Nonlinear Action)

Γ acts on $\mathbb{A}^3$ and is generated by:

- Permutations of x_1, x_2, x_3

- The quadratic involutions R_1, R_2, R_3 where

$$R_1 : (x_1, x_2, x_3) \to (3x_2x_3 - x_1, x_2, x_3)$$

and R_2, R_3 defined similarly.

Γ preserves

$$\Phi(x_1,x_2,x_3) := x_1^2+x_2^2+x_3^2-3x_1x_2x_3$$

The R_j's correspond to x_j replaced by its conjugate.

$V : \Phi(x)=0$ is the Markoff cubic affine surface.

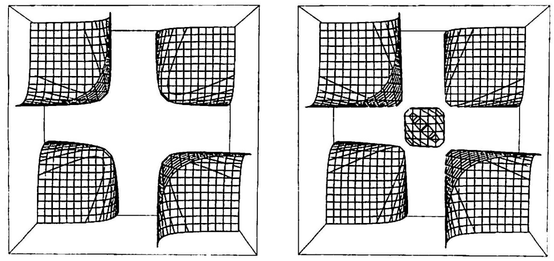
- Solutions to $\Phi(x)=0$ with $x_j \in \mathbb{N}$ are called Markoff triples denoted M.
- The coordinates of M are called Markoff numbers $\mathbb{M}$.

M corresponds to the Markoff spectrum in diophantine approximation.

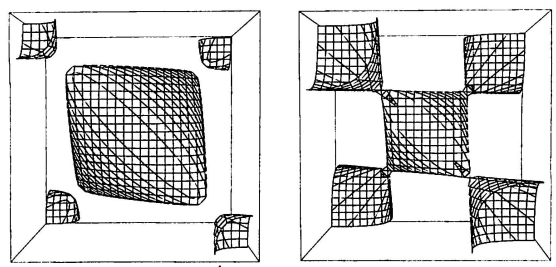
Markoff(1879):

$$M = O_{(1,1,1)} = \Gamma \cdot (1,1,1)$$

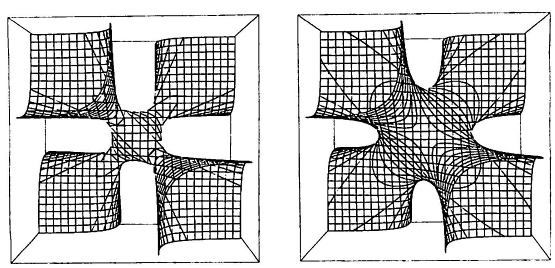
Real Surfaces $\Phi(x) = k$ (Goldman)



(a) Level set $\kappa = -2.1$ (b) Level set $\kappa = 1.9$



(a) Level set $\kappa = 1.9$ (b) Level set $\kappa = 2.1$



(a) Level set $\kappa = 4$ (b) Level set $\kappa = 19$

The affine linear theory has been developed over the last 10 years:

Let $G = Zcl(\Gamma)$.

It is a linear algebraic group $/\mathbb{Q}$

$V = Zcl(O)$ is a G-homogeneous space.

Strong approximation:

(i) If Γ is finite index in $G(\mathbb{Z})$, i.e. arithmetic, this is classical.

(ii) If Γ is thin and G is say semisimple simply connected, then

$$\Gamma \xrightarrow{mod\ q} G(\mathbb{Z}/q\mathbb{Z})$$

is still onto for q prime to a fixed set of ramified primes!

(Matthews-Vaserstein-Weisfeiler, Nori)

To do anything diophantine one needs to show that in these cases the congruence graphs associated with $G(\mathbb{Z}/q\mathbb{Z})$ are “expanders".

(S-Xue, Gamburd, Helfgott, Bourgain-Gamburd, Bourgain-Gamburd-S, Pyber-Szabo,

Breulliard-Green-Tao, Varju, Salehi-Varju)

The affine linear sieve has been developed by a number of people leading to:

Fundamental Theorem of the Affine Linear

Sieve (Salehi-S, 2012) “Brun-Sieve"

Let (O, f) be a pair as above, $G = Zcl(\Gamma)$. If radical(G) contains no tori (“levi semisimple") there is $r < \infty$ such that

$$\{x \in O : f(x) \text{ is } r \text{ almost prime}\}$$

is Zariski dense in $V = Zcl(O)$, we say “ (O, f) saturates".

Tori pose fundamnetal difficulties from all points of view. Heuristics suggest that saturation fails for them. Even a problem like $2^n + 5$ being composite for almost all n is very problematic (Hooley).

Markoff Equation (all of what follows is joint work with Bougain and Gamburd)

- M Markoff triples

- $\mathbb{M}$ Markoff numbers

- $\mathbb{M}^S$ the Markoff sequence consists of the largest coordinate of a Markoff triple counted with multiplicity.

Conjecture(Frobenius 1913): $\mathbb{M}^S = \mathbb{M}$.

Theorem(Zagier 1982): $\mathbb{M}$ is very sparse

$$\sum_{\substack{m \leq T \\ m \in \mathbb{M}^S}} 1 \sim c(logT)^2, \text{as } T \to \infty (c > 0).$$

$X^*(p) = V(\mathbb{Z}/p\mathbb{Z}) | \{(0,0,0)\}$. Γ acts on $X^*(p)$, by joining $x \in X^*(p)$ to its permutations and to $R_j(x), j = 1,2,3$ we get Markoff graphs $X^*(p)$.

Strong Approximation Conjecture*
(Mccullough-Wanderley 2013)

$M \xrightarrow{mod\ p} X^*(p)$ is onto, equivalently the Markoff graphs are connected.

$(*)$ the graphs appear to be expanders!

Theorem 1:

$X^*(p)$ has a giant connected component $C(p)$ namely

$$|X^*(p) \backslash C(p)| \underset{\varepsilon}{\ll} p^{\varepsilon} \ , \ \varepsilon > 0$$

(note that $|X^*(p)| \sim p^2$) and each component has size at least $c_1 log p$, c_1 fixed).

Theorem 2 If E is the set of primes p for which the strong approximation conjecture fails then $|E \cap [0,T]| \underset{\varepsilon}{\ll} T^{\varepsilon}$, $\varepsilon > 0$.

In fact we prove the conjecture unless $p^2 - 1$ is not very “smooth".

Concerning primality and divisibility of Markoff numbers little is known.

Theorem (Corvaja-Zannier 2006)

As $x = (x_1, x_2, x_3) \in M$ goes to infinity the biggest prime factor of $x_1 x_2$ goes to infinity (should be true for x_1 alone!).

Theorem 3

Almost all Markoff numbers are composite; precisely

$$\sum_{\substack{p \leq T \\ p \text{ prime}, p \in M^S}} 1 = o\Big(\sum_{\substack{m \leq T \\ m \in M^S}}\Big), \quad \text{as} \quad T \to \infty.$$

Much of the above extends to the diophantine analysis of Cayley's general (affine) cubic surface $S_{A,B,C,D}$:

$$x^2+y^2+z^2 = Ax+By+Cz+D$$

$\Gamma_{A,B,C,D}$ is generated by the switching of roots S_x, S_y, S_z

$$S_x : x \to -x-yz+A, y \to y, z \to z$$

and S_y and S_z defined similarly. Up to finite index $\Gamma_{A,B,C,D}$ is the automorphism group of $S_{A,B,C,D}$.

The complex dynamics of $\Gamma_{A,B,C,D}$ on $\mathbb{A}^3$ has been studied in depth by Cantat and Loray and is closely connected to the (nonlinear) Painlave VI equation.

Some points in the proofs which are related to other works:

If $x = (x_1, x_2, x_3) \in X^*(p)$,

want to connect x to many points. The plane section $y_1 = x_1$ of $X^*(p)$ yeilds a conic section in the y_2, y_3 plane containing x and $(x_1, R^j(x_2, x_3)), j = 1, 2, \ldots$ where

$$R(x_2, x_3) = [x_2, x_3]\begin{bmatrix} 3x_1 & 1 \\ -1 & 0 \end{bmatrix}$$

If t_1 is the order of R in $SL_2(\mathbb{F}_p)$ then x is joined to these t_1 points.

If t_1 is maximal (i.e. $t_1 = p-1$ or $p+1$[in $\mathbb{F}_p^*, \mathbb{F}_{p^2}^*$]) then the t_1 points cover the full conic section. We are then in good shape to connect things up via intersections of these conics in different planes.

Otherwise we seek among these t_1 points one for which the corresponding operation yields a rotation of order $t_2 > t_1$, and to repeat. To realize this we are led to

$$b \neq 1, \quad \xi + \frac{b}{\xi} = \eta + \frac{1}{\eta} \qquad \text{——}(*)$$

with $\xi \in H_1(|H_1| = t_1)$ a subgroup of $\mathbb{F}_p^*$ or $(\mathbb{F}_{p^2}^*)$ and we want η of large order.

- If $t_1 > p^{1/2+\delta}(\delta > 0)$ then using Weil's R.H. for curves over finite fields, one can show that there is an η of maximal order.

- If $t_1 \leq p^{1/2}$ then the genus of the corresponding curve is too large for R.H. to be of use. In this case we need a nontrivial(exponent saving) upper bound for solutions to $(*)$ with $\xi \in H_1, \eta \in H_2, |H_2| \leq t_1$.

We have two methods to achieve this

(A) Stepanov's transcendence method (auxiliary polynomials) for proving R.H. for curves yields nontrivial bounds for these curves (Corvaja and Zannier give quite sharp bounds using a somewhat different method of hyper-Wronskians).

(B) For the specific eqn$(*)$ one can use the finite field projective "Szemeredi-Trotter Theorem" of Bourgain. This gives a nontrivial upper bound for the number of incindences $x = gy$, x and y in a subset of $\mathbb{P}^1(\mathbb{F}_p)$ and g a subset of $PGL_2(\mathbb{F}_p)$.

The above leads to the existence of a very large component $C(p)$ and the connectness of $X^*(p)$ as long as $p^2 - 1$ is not very smooth.

With one caveat: that there may be components of bounded size as $p \to \infty$. To deal with these, we lift to characteristic 0 and face the problem of determining the finite orbits of Γ on $V(\mathbb{C})$.

Remarkably this exact problem for the surfaces $S_{A,B,C,D}$ arises in determining the Painlave VI's which have finite monodromy or equivalently are algebraic functions (Dubrovin-Mazzacca and Lisouyy and Tykhyy)!

Our method is to apply Lang's G_m torsion conjecture (Laurent's theorem) which handles such finiteness questions for groups generated by linear and quadratic morphisms.

Lang G_m:

Let $V \subset (\mathbb{C}^*)^m$ be an algebraic set (i.e. one defined as the zero set of Laurent polynomials) then there are (effectively computable) multiplicative subtori $T_1, \ldots, T_l$ contained in V such that

$$TOR \cap V = TOR \cap (\bigcup_{j=1}^{l} T_j),$$

where TOR = all torsion points in $(\mathbb{C}^*)^m$.

If $p^2 - 1$ is very smooth our methods fall short of proving $X^*(p)$ is connected. The following variant of a conjecture of M. C. Chang and B. Poonen would suffice.

Conjecture:

Given $\delta > 0$ and $d \in \mathbb{N}$ there is a $K = K(\delta, d)$ such that for p large and $f(x,y)$ absolutely irreducible over $\mathbb{F}_p$ and of degree $d (f(x,y) = 0$ not a subtorus), then the set of (x,y) in $\mathbb{F}_p^2$ for which $f(x,y) = 0$ and max$(ordx, ordy) \leq p^\delta$, has size at most K.

Some References

E. Bombieri, *Continued fractions and the Markoff tree*, Expo. Math. 25 (2007), no 3, 187-213

J. Bourgain, *A modular Szemeredi-Trotter theorem for hyperbolas*, C.R. Acad. Sci. Paris Ser 1, 350 (2012), 793-796.

W. Goldman, *The modular group action on real* $SL(2)$*-characters of a one-holed torus*, Geom. and Top. Vol. 7 (2003), 443-486.

M. Laurent, *Exponential diophantine equations*, C.R. Acad. Sci. 296 (1983), 945-947.

C. Matthews, L. Vaserstein and B. Weisfeiler, *Congruence properties of Zariski dense groups*, Proc. London Math. Soc. 48, 514-532 (1984).

D. Mccullough and M. Wanderley, *Nielsen equivalence of generating pairs in* $SL(2,q)$, Glasgow Math. J. 55 (2013), 481-509.

P. Sarnak and A. Salehi, *The affine sieve*, JAMS (2013), no 4, 1085-1105.

S.A. Stepanov, *The number of points of a hyperelliptic curve over a prime field*, MATH USSR-IZV 3:5 (1969), 1103-1114.

D. Zagier, *On the number of Markoff numbers below a given bound*, Math of Comp. 39, 160 (1982), 709-723.

J. Bourgain, A. Gamburd and P. Sarnak, arXiv 1505.06411 (2015).

S. Cantat and F. Loray, Ann. Inst. Fourier. Grenoble 59,7 (2009), 2957-2978.

P. Corvaja and U. Zannier, JEMS 15 (2013), 1927-1942.

B. Dubrovin and M. Mazzocco, Invent. Math 141 (2000), 55-147.