LECTURE 3

STRONG APPROXIMATION FOR INTEGRAL POINTS ON MARKOFF SURFACES AND MARKOFF NUMBERS

PETER SARNAK

BRISTOL 2016

JOINT WORK WITH
J. BOURGAIN AND A. GAMBURD.

IN GENERAL THE PROBLEM OF THE HASSE PRINCIPLE (I.E. THERE BEING A GLOBAL INTEGRAL POINT AS LONG AS THERE ARE NO LOCAL OBSTUCTIONS) AND OF STRONG APPROXIMATION FOR $X_k(\mathbb{Z})$

$$X_k : \quad F(x_1, \dots, x_n) = k$$

AND F GENERAL IS WELL KNOWN TO BE HOPELESS.

THE ONLY ROBUST METHOD KNOWN TO PRODUCE A RICH SET OF INTEGRAL POINTS IS THE HARDY-LITTLEWOOD CIRCLE METHOD. HOWEVER IT REQUIRES MANY VARIABLES COMPARED TO THE DEGREE OF F. REDUCING THE NUMBER OF VARIABLES IS THE HOLY GRAIL. IF F IS HOMOGENEOUS AND DIAGONAL MUCH PROGRESS HAS BEEN MADE

(VINOGRADOV, WOOLEY, ...)

THE FIRST LECTURE WAS CONCERNED WITH QUADRIC, WE TURN TO <u>CUBICS</u>:

FOR HOMOGENEOUS CUBIC FORMS

$$X : F(x_1, \ldots, x_n) = 0 \quad \text{(PROJECTIVE)}$$

THE SEARCH FOR <u>RATIONAL</u> POINTS AND STRONG APPROXIMATION IS VERY ACTIVE. THERE ARE RESULTS FOR $n = 10$ (NON-SINGULAR) AND SPECIAL FORMS WITH $n \geq 7$ AND EVEN $n = 4$ (HEATH-BROWN, HOOLEY, VAUGHAN, SWINNERTON-DYER, SKOROBOGATOV, BROWNING, ...) SEE BROWNING'S 2014 SURVEY.

OUR INTEREST IS IN INTEGRAL POINTS ON AFFINE CUBIC SURFACES IN A^3. (IN A^2 THERE ARE ONLY FINITELY MANY INTEGRAL POINTS - SIEGEL, IN A^3 WE EXPECT FEW INTEGRAL POINTS IN GENERAL - VOJTA)

<u>EG</u>: $$X_m : x_1^3 + x_2^3 + x_3^3 = m$$

IF $m \not\equiv 4, 5 \pmod 9$ "EXPECT" $|X_m(\mathbb{Z})| = \infty$? HOWEVER THE STRONGEST FORM OF STRONG APPROXIMATION FAILS (CASSELS, HEATH-BROWN, COLLIOTE-THELENE / WITTENBERG)

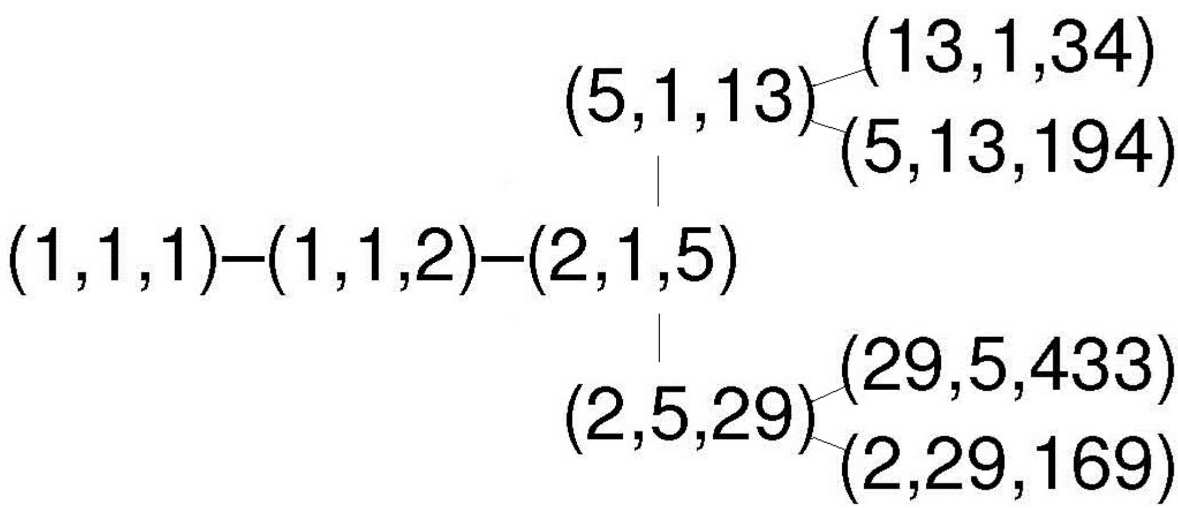
Markoff's Surface X:

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

$$X : \Phi(x) = 0. \qquad \text{——}(1)$$

An affine cubic surface in $\mathbb{A}^3$.

- The positive integer solutions to (1) are called Markoff Triples denoted by M
- The coordinates of $x \in M$ are Markoff numbers denoted by $\mathbb{M}$.



$$\mathbb{M} : 1, 2, 5, 13, 29, 34, 89, 169, 194, \ldots$$

The process of producing new solutions from a given one is repeated applications of the group Γ of affine polynomial maps of $\mathbb{A}^3$ generated by

- Permutations of the coordinates

- 'Vieta Transformations' switching the roots of the quadratic on fixing two coordinates.

$$x_1^2+x_2^2+x_3^2-3x_1x_2x_3=0$$

$$R_1:(x_1,x_2,x_3)\to(x_1,x_2,3x_1x_2-x_3).$$

Similarly for R_2,R_3

Markoff (Simple Descent):

$$M=\Gamma\cdot(1,1,1)$$

The Γ orbit of $(1,1,1)$ yields all elements of M.

M and $\mathbb{M}$ arise in many different contexts.

- Diophantine approximation (Markoff)
- Simple closed geodesics on once punctured hyperbolic surfaces (H. Cohn)
- Algebraic geometry of surfaces classifications of:
  Exceptional vector bundles over $\mathbb{P}^2$ (Gorodentsev + Rudakov)
  Smoothable del Pezzo surfaces with singularities (Hacking + Prokhorov)

.

.

.

Little is known about the diophantine properties of $\mathbb{M}$ or M and $X(\mathbb{Z})$.

- Strong approximation concerns the reduction of $X(\mathbb{Z})$ mod q and the extent to which this covers $X(\mathbb{Z}/q\mathbb{Z})$.
- For $\mathbb{M}$ mod q, Frobenius noted that $m \in \mathbb{M} \Rightarrow m \not\equiv 0, \pm 2/3$ (mod p), for $p \equiv 3(4)$ a prime.

Note that Γ acts on $X(\mathbb{Z}/q\mathbb{Z})$ and the strong approximation problem is connected to

Main Conjecture (MC) (for primes.)

Γ acts as permutations of $X(\mathbb{Z}/p\mathbb{Z})$ with two orbits $\{(0,0,0)\}$ and $X^*(\mathbb{Z}/p\mathbb{Z}) = X(\mathbb{Z}/p\mathbb{Z})|\{0\}$.

Note that if MC is true then $M \xrightarrow{mod\ p} X^*(\mathbb{Z}/p\mathbb{Z})$ is onto, i.e. we have strong approximation and Frobenius' congruence obstruction is the only one for $\mathbb{M}$.

Theorem 1 (Giant Orbit)

For $\varepsilon > 0$ and p large there is a Γ-orbit $\mathscr{C}(p)$ in $X^*(\mathbb{Z}/p\mathbb{Z})$ for which

$$|X^*(\mathbb{Z}/p\mathbb{Z}) \setminus \mathscr{C}(p)| \leq p^{\varepsilon} (\text{note} \quad |X^*(\mathbb{Z}/p\mathbb{Z})| \sim p^2)$$

and all Γ-orbits $\mathscr{D}(p)$ satisfy $|\mathscr{D}(p)| \gg \log p$.

We can prove MC as long as p^2-1 is not very "smooth" (that is it does not have a very large number of small prime factors)

Theorem 2 (Few exceptions to MC)

The set E of primes for which MC fails satisfies

$$|\{p \in E; p \leq T\}| \underset{\varepsilon}{\ll} T^{\varepsilon}, \text{ for any } \varepsilon > 0.$$

An extension of Theorem 2 to composite moduli q together with a basic sieve allows us to show that most Markoff numbers are composite.

$\mathbb{M}^S$; the Markoff sequence, consists of the x_3's where $(x_1,x_2,x_3) \in M$ and $x_1 \leq x_2 \leq x_3$.

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

Markoff Numbers are very sparse:

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

<u>Theorem 3</u> (Almost all composite)

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

Our methods apply to more general affine cubic surfaces S:

$$S_k : \Phi(x_1, x_2, x_3) = k.$$

$$S_{A,B,C,D} : x_1^2 + x_2^2 + x_3^2 + x_1 x_2 x_3 = A x_1 + B x_2 + C x_3 + D$$

$$S_{gen} : \sum_{i,j=1}^{3} A_{ij} x_i x_j + \sum_{j=1}^{3} B_j x_j + C = D x_1 x_2 x_3$$

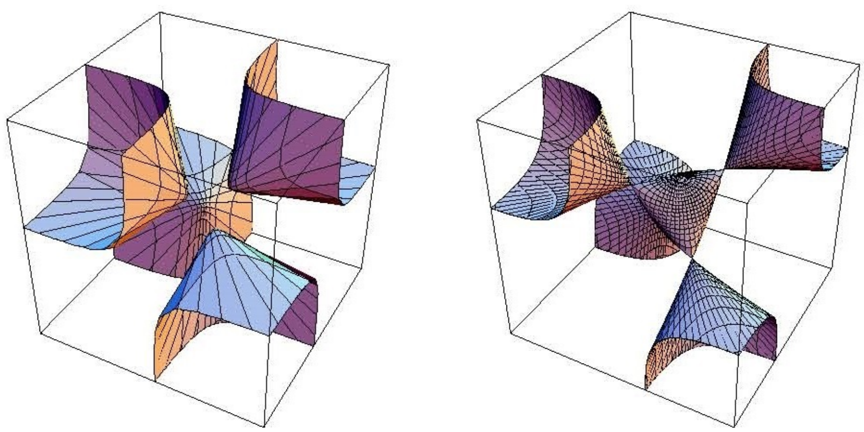
A_{ij}, B_j, C, D integers (non degenerate).

In all cases we have the group $\Gamma = \Gamma_S$ of affine polynomial morphisms generated by the Vieta transformations, acting on S and $S(\mathbb{Z})$, $(p\ large)$.

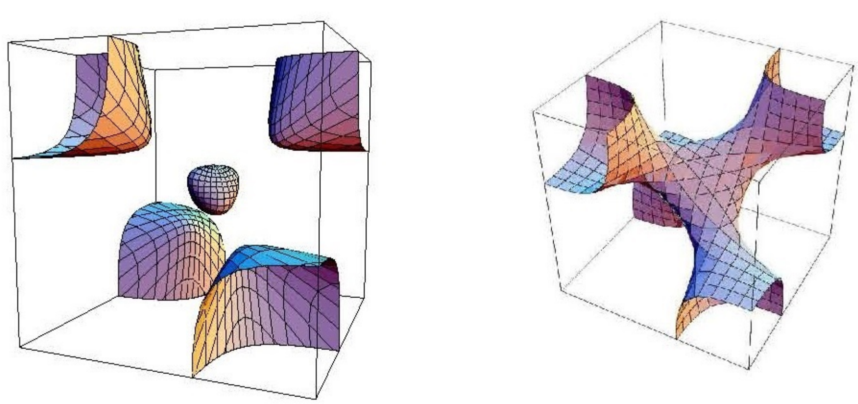
S_0 Markoff's cubic surface

S_4 Cayley's cubic surface

$S_k(\mathbb{R})$ for different k:



$k = 0$ and $k = 4$



$k = 2$ and $k = 8$

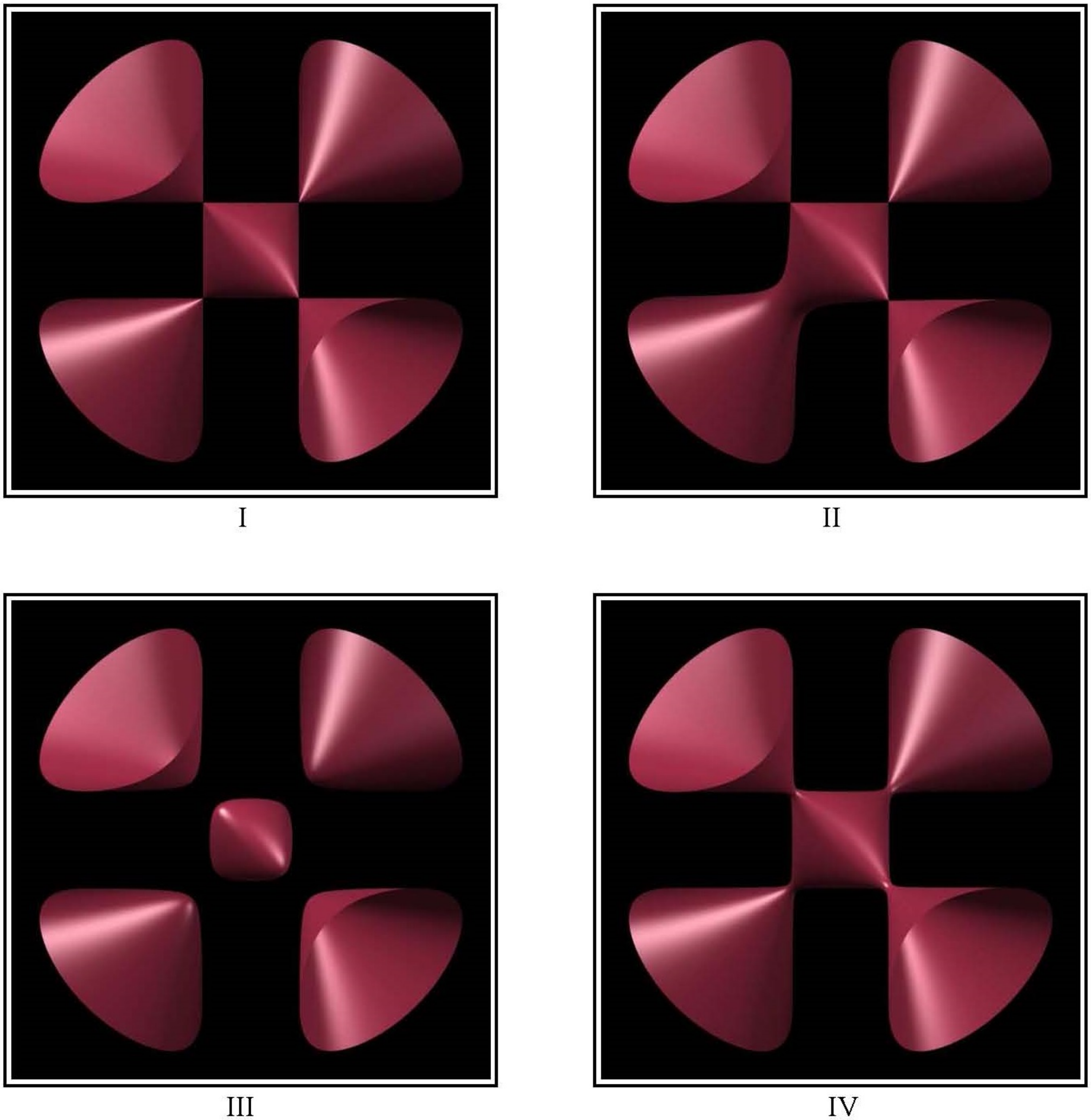


FIGURE 2. Four examples. I. The Cayley cubic S_C ; II. $S_{(-0.2,-0.2,-0.2,4.39)}$; III. $S_{(0,0,0,3)}$; IV. $S_{(0,0,0,4.1)}$.

In order to formulate the analogue of MC for the surfaces S we need.

<u>Theorem 4</u>: There are finitely many finite Γ_S orbits on $S(\overline{\mathbb{Q}})$ and these orbits may be determined effectively.

Remarkably this determination has been carried out for $S_{A,B,C,D}$ by Dubrovin/Mazzocco and Lisovyy/Tykhyy.

For these the finite Γ-orbits correspond exactly to the solutions $y(z) = y(\alpha, \beta, \gamma, \delta; z)$ of Painlevé VI, which are algebraic functions of z!

$$\frac{d^2y}{dz^2} = \frac{1}{2}\Big(\frac{1}{y} + \frac{1}{y-1} + \frac{1}{y-z}\Big)\Big(\frac{dy}{dz}\Big)^2 - \Big(\frac{1}{z} + \frac{1}{z-1} + \frac{1}{y-z}\Big)\frac{dy}{dz} +$$

$$+ \frac{y(y-1)(y-z)}{z^2(z-1)^2}\left[\alpha + \frac{\beta z}{y^2} + \frac{\gamma(z-1)}{(y-1)^2} + \frac{\delta(z-1)z}{(y-z)^2}\right]$$

$\Gamma_{A,B,C} \Longleftrightarrow$ nonlinear monodromy group of the Painlave VI.

IN MORE DETAIL AND DIFFERENT COORDS

$$\frac{d^2w}{dt^2} = \frac{1}{2}\left(\frac{1}{w}+\frac{1}{w-1}+\frac{1}{w-t}\right)\left(\frac{dw}{dt}\right)^2 - \left(\frac{1}{t}+\frac{1}{t-1}+\frac{1}{w-t}\right)\frac{dw}{dt}$$

$$+ \frac{w(w-1)(w-t)}{2t^2(t-1)^2}\left((\theta_\infty - 1)^2 - \frac{\theta_x t}{w^2} + \frac{\theta_y^2(t-1)}{(w-1)^2} + \frac{(1-\theta_z^2)\,t(t-1)}{(w-t)^2}\right) \quad \text{—}(*)$$

$$\Theta = (\theta_x, \theta_y, \theta_z, \theta_\infty)$$

$$p_\nu = 2\cos\pi\theta_\nu \qquad \nu = x, y, z, \infty$$

$$\omega_x = p_x p_\infty + p_y p_z \ , \omega_y = p_y p_\infty + p_z p_x , \omega_z = p_z p_\infty + p_x p_y$$

$$\omega_4 = p_x^2 + p_y^2 + p_z^2 + p_\infty^2 + p_x p_y p_z p_\infty$$

$$S_\Theta = S_\omega \ : \quad xyz + x^2 + y^2 + z^2 - \omega_x x - \omega_y y - \omega_z z + \omega_4 = 0$$

THE NONLINEAR MONODROMY GROUP OF $(*)$ ACTS ON PARAMETERS PRESERVING THE SURFACES S, AND ~~ACTUS~~ THE ACTION IS THE MARKOFF / VIETA Γ ACTION ON THESE CUBIC SURFACES.

FINITE ORBIT CORRESPONDS TO W BEING ALGEBRAIC (IWASAKI).

EXAMPLES $(\overline{L-T})$:

1) $\Theta = \left(\frac{2}{5}, \frac{1}{5}, \frac{1}{3}, \frac{2}{3}\right)$

$r = (x, y, z) = \left(2\cos\frac{2\pi}{3}, 2\cos\frac{\pi}{3}, 2\cos\frac{\pi}{3}\right)$

$|\Gamma . r| = 5$

$$W = \frac{2(s^2+s+7)(5s-2)}{s(s+5)(4s^2-5s+10)}, \quad t = \frac{2s^3(s^2-5)}{(s-2)^2(s+3)^3}$$

genus $= 0$.

2) $\Theta = \left(\frac{2}{5}, \frac{2}{5}, \frac{2}{5}, \frac{2}{3}\right)$

$r = \left(2\cos\frac{4\pi}{5}, 2\cos\frac{3\pi}{5}, 2\cos\frac{3\pi}{5}\right)$

$|\Gamma . r| = 9$

$$W = \frac{1}{2} + \frac{350s^3+63s^2-6s-2}{30s(2s+1)u}$$

$$t = \frac{1}{2} + \frac{(25s^4+170s^3+42s^2+8s-2)u}{54s^3(5s+4)}$$

$u^2 = s(8s+1)(5s+4)$; genus $= 1$.

With this we have the general MC.

MC (general): Fix S and Γ_S as above. For p large the Γ orbits in $S(\mathbb{Z}/p\mathbb{Z})$ consist of the finitely many finite $S(\overline{\mathbb{Q}})$ orbits which occur in $\mathbb{Z}/p\mathbb{Z}$ and the complement of these, $S^*(\mathbb{Z}/p\mathbb{Z})$, which is the big orbit.

- For the surfaces S_k this conjecture is equivalent to $SL_2(\mathbb{F}_p)$ t-systems for pairs of generators under Nielsen moves put forth recently by Mccullough/Wanderley.

- Our methods lead to the anologues of Theorem 1 and 2 for these S_{gen}'s.

Remarks: The passage from MC(general) to strong approximation is that if $S(\mathbb{Z})$ has a point with an infinite Γ-orbit then $S(\mathbb{Z}) \xrightarrow{mod\ p} S(\mathbb{Z}/p\mathbb{Z})$ contains $S^*(\mathbb{Z}/p\mathbb{Z})$.

According to Vojta's Conjectures integral points on affine cubic surfaces are typically rare (depending on the geometry of the divisor at infinity).

The familiar cases for which the integral points are Zariski dense for example tori, do not obey strong approximation.

These Markoff like affine cubic surfaces are remarkable in having only lacunary set of integral points but which are apparently rich enough for strong approximation.

The story with rational points on (projective) cubic surfaces is very different, once there are any such points there is an abundance of them.

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

$$X : x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 0$$

If $x = (x_1, x_2, x_3) \in X^*(\mathbb{Z}/p\mathbb{Z})$,

want to connect x via Γ to many points. The plane section $y_1 = x_1$ of $X^*(p)$ yields 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 is the rotation

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

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 $\xi \in H_1, \eta \in H_2, |H_2| \leq t_1$.

P LARGE

$$
(*) \quad \begin{cases} x + \dfrac{b}{x} = y + \dfrac{1}{y}, \quad b \neq 1 \\ x \in H_1, \; y \in H_2, \; H_1, H_2 \text{ subgroups of } \mathbb{F}_p \text{ or } \mathbb{F}_{p^2}. \\ |H_2| \leq |H_1| \leq p^{1/2}. \end{cases}
$$

THERE IS $\tau < 1$ AND $C < \infty$ SUCH THAT THE NUMBER OF SOLUTIONS TO $(*)$ ~~SATISFIES~~ IS AT MOST

$$C \, |H_1|^{\tau}.$$

(THE TRIVIAL BOUND IF $|H_2|$ AND $|H_1|$ ARE ROUGHLY THE SAME IS $|H_1|$)

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 and their technique to estimate $gcd(u-1, v-1)$).

(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 in a subset of $PGL_2(\mathbb{F}_p)$.

The above leads to the existence of a very large connected 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 $X(\overline{\mathbb{Q}})$. That is to Theorem 4. If $(x_1, x_2, x_3) \in X(\overline{\mathbb{Q}})$ and the rotations corresponding to x_1, x_2, and x_3 are of finite order say dividing n, then we have a solutions to (for S_k)

$$\begin{aligned} k = (\varphi_1 + \varphi_1^{-1})^2 + (\varphi_2 + \varphi_2^{-1})^2 + (\varphi_3 + \varphi_3^{-1})^2 - \\ (\varphi_1 + \varphi_1^{-1})(\varphi_2 + \varphi_2^{-1})(\varphi_3 + \varphi_3^{-1}) \end{aligned}$$

with φ_j an n th root of 1.

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 vieta 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 finitely many (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 $(\mathbb{C}^*)^m$, that is points whose coordinates are roots of unity.

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$(ord x, ord y) \leq p^\delta$, has size at most K.

Theorem 2, namely that MC is true for all but very few exceptions exploits firstly that for most p, p^2-1 is not smooth.

Erdös and Pomerance show that if $3 \leq y \leq x$, for most primes $p \leqslant x$, $p \pm 1$ has loglog y prime factors less than y.

Our stronger bounds for the exceptional set of primes exploit the specific structure of our problem and involve extending work of M.C. Chang.

The proof of Theorem 3 (“almost all $m \in \mathbb{M}$ composite") requires an extension of Zagier’s count to m’s satisfying congruences. This can be proven either by extending McShane and Rivin’s treatment of simple closed geodesics on a once punctured hyperbolic torus, or using recent work of Athraya, Befetov, Eskin and Mirzakhani.

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, *Markoff Triples and Strong Approximation*, 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.

O. Lisovyy and Y. Tykhyy, arXiv 0809.4873 (2008).

G. McShane and I. Rivin, IMRN (1995), 2, 61-69.

H. Cohn, Acta Arith. (1971), 18, 125-136.

P. Hacking and Y. Prokhorov, Compositio Math. 146 (2010), 169-192.

J. Athreya, A. Bufetov, A. Eskin and M. Mirzakhani, arXiv 061071 (2011).

A. Gorodentsev and A. Rudakov, DMJ 54 (1987), 115-130.

M.C. Chang, Bull Aust. Math. Soc. 88 (2013), 169-176.