AHLFORS LECTURE II

INTEGER POINTS ON AFFINE CUBIC SURFACES

PETER SARNAK

NOV 1 2019

JOINT WORK WITH A. GHOSH AND WITH J. BOURGAIN / A. GAMBURD
Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial with integral coefficients and $f$ and $f - k$ irreducible over $\mathbb{Q}$ for all $k$.

$$f(x_1, x_2, \ldots, x_n) = k \quad (\star)$$

To be solved over $\mathbb{Z}$ (or $\mathbb{Q}_k$ when $k$ is a number field).

$$V_{f, k} = \{x : f(x) = k\}$$, affine hypersurface.

Local congruence obstructions / $\mathbb{Z}$:

**Nec. Cond. is that**

$$f(x) \equiv k \pmod{q}, q \geq 1 \text{ has solution.}$$

If the local condition is sufficient for solvability over $\mathbb{Z}$, we have a local to global or Hasse principle.

**Linear:**

$$f(x_1, \ldots, x_n) = a_1 x_1 + \ldots + a_n x_n = k$$

**Nec. Cond. is** $\gcd(a_1, \ldots, a_n) \mid k$

It is also sufficient.
\( \text{f QUADRATIC (HILBERT'S ELEVENTH PROBLEM):} \)

\( \text{TO SOLVE (\star) WITH} \)

(a) \( x, k \in K \)
(b) \( x, k \in \mathcal{O}_K \)

(\( \square \) HASSE-MINKOWSKI THEOREM:

(\( \star \)) IS SOLVABLE IN \( K \) IFF IT IS SOLVABLE OVER EVERY \( K_v \), FOR EVERY COMPLETION \( K_v \) OF \( K \).

(\( \square \)) OVER \( \mathcal{O}_K \) MUCH MORE DIFFICULT; FOR EXAMPLE WHICH NUMBERS ARE SUMS OF THREE SQUARES IN \( \mathcal{O}_K \)?

A STABLE LOCAL TO GLOBAL PRINCIPLE (THAT IS EXCEPT FOR FINITELY MANY EXCEPTIONS) HOLDS FOR \( M \geq 3 (\text{SIEGEL, KNESER, DUKE/IWANIEC, OGDELL/PIATETSKI, SHAPIRO IS}) \)

KEY: \( V_{f, k} \) IS A HOMOGENEOUS SPACE FOR AN ORTHOGONAL GROUP \( \rightarrow \) MODULAR FORMS.
CUBIC FORMS

· An affine cubic \( f \) is a polynomial in \( \mathbb{Z}[x_1, \ldots, x_n] \) with leading homogeneous part \( f_0 \) of degree 3 and non-degenerate, we also assume that \( f \) and \( f - k \) are irreducible.

\[
V_{k, f} = \{ x : f(x) = k \}
\]

\text{Affine hypersurface}

· \( k \) is admissible if there are no local congruence obstructions to \((***)\) (these have a simple description)

Richness of \( V_{k, f}(\mathbb{Z}) \):

- For \( k \) admissible is \( V_{k, f}(\mathbb{Z}) \) non-empty (i.e., has a Hasse principle), Zariski-dense in \( V_{k, f} \), satisfy a form of strong approximation?

\( n = 2 \) (super-critical) Thue/Siegel

\[
| V_{k, f}(\mathbb{Z}) | < \infty
\]

Schmidt shows that for very few admissible \( k \)'s is \( V_{k, f}(\mathbb{Z}) \neq \emptyset \).
\( n \geq 10 \) (Subcritical) Browning/Heath-Brown

- If nonsingular then for \( \mathbf{r} \) admissible, \( V_{k,\mathbf{r}}(\mathbb{Z}) \neq \emptyset \), it is Zariski dense and it satisfies strong approximation.

- \( n \geq 4 \) (Subcritical) Hooley

- Homogeneous nonsingular and assuming the Riemann hypothesis for certain associated Hasse-Weil zeta functions, \( V_{k,\mathbf{r}}(\mathbb{Z}) \neq \emptyset \) for almost all admissible \( \mathbf{r} \)'s.

- \( n = 3 \) (Critical) Affine cubic surface, very little is known.

**Example**

\[
\mathbf{f} = S(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3
\]

\( \mathbf{r} \) is admissible iff \( \mathbf{r} \equiv 4, 5 \pmod{9} \)

- It is possible that for every admissible \( \mathbf{r} \), \( V_{k,\mathbf{r}}(\mathbb{Z}) \neq \emptyset \) and is Zariski dense in \( V_{k,\mathbf{r}} \).


\[
33 = (8866128975287528)^3 + (-8778405442862239)^3 + (-2736111468807040)^3
\]

\[
42 = (-80538738912075974)^3 + (80435758145817515)^3 + (12602123297335631)^3
\]

With D. Sutherland
Lehmer, Beukers show that $V_{S,1}(Z)$ is Zariski dense in $V_{S,1}$.

Using cubic reciprocity one can show that strong approximation fails for $V_{S,r}(Z)$.

E.g. $x \in V_{S,3}(Z) \Rightarrow x_1 \equiv x_2 \equiv x_3 \pmod{9}$

(Cassels, Heath-Brown, Colliot-Thélène/Wittenberg)

However in the slightly weaker form

$V_{S,r}(Z) \rightarrow V_{S,r}(Z/pZ)$, being onto for $p$ a large prime, may hold.

A diophantine theory for integral points on some special cubic surfaces can be developed.

A. Ghosh / S, J. Bourgain / A. Gamburd / S

These start with Markoff's surfaces.
MARKOFF’S CUBIC SURFACES

\[ M(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 x_3 \]

\[ V_k = V_{k, M} = \{ x : M(x) = k \} \]

\( k = 0 \) : IS MARKOFF’S SURFACE

\( k = 4 \) : IS THE CAYLEY CUBIC

( IT IS SPECIAL IN WHAT follows)

**V_k(\mathbb{Z}) ARISES IN MANY CONTEXTS**

- **DIOPHANTINE APPROXIMATION (MARKOFF)**
- **SIMPLE CLOSE GEODESICS ON THE MODULAR SURFACE (H. COHN)**
- **EXCEPTIONAL VECTOR BUNDLES OVER \( \mathbb{P}^2 \) (GORODENTSEV / RUDAKOV)**
- **SMOOTHABLE DEL-PEZZO SURFACES (HACKING / PROKHOROV)**
- **SYMPLECTIC 4-MANIFOLDS VIA LEFSCHETZ FIBRATIONS (AURoux)**

**V_k** is also the relative character variety of representations of \( \pi_1(\Sigma_{1,1}) \rightarrow \text{SL}_2 \)

It also arises as the non-linear monodromy group of Painlevé VI.
$V_0$ Markoff’s cubic surface

$V_4$ Cayley’s cubic surface

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

$k = 0$ and $k = 4$

$k = 2$ and $k = 8$
The reason one can study $V_k(Z)$ is that it is acted on by a non-linear group of morphisms allowing descent. $\Gamma$, the group in $\text{Aut}(\mathbb{A}^3)$ generated by permutations of the coordinates and switching the signs of two coordinates, and the Vieta involutions $R_1, R_3, R_3$

$$R_3(x_1, x_2, x_3) = (x_1, x_2, x_1x_2 - x_3)$$

preserves $V_k$ and $V_k(Z)$ ($\Gamma \cong \text{PGL}_2(\mathbb{Z})$).

• For $k \neq 4$, $V_k(Z)$ consists of a finite number $h(k)$ of $\Gamma$-orbits (Markoff, Hurwitz, Mordell).

**Classical Questions:**

(i) When is $V_k(Z) \neq \emptyset$ if $h(k) > 0$.

(ii) If $h(k) > 0$, is $V_k(Z)$ infinite, Zariski dense, satisfy a form of strong approximation?
HASSE PRINCIPLE

LOCAL CONGRUENCE OBSTRUCTIONS:

\[ V_k(\mathbb{Z}_p) \neq \emptyset \text{ for all } p \text{ iff } k \not\equiv 3(4) \text{ or } \equiv 3 \pmod{9} . \]

We restrict to \( k \)'s which have local integral points and say that \( V_k \) fails HASSE'S PRINCIPLE if \( V_k(\mathbb{Z}) = \emptyset \).

For \( |k| \geq 5 \), call \( k \) special if \( V_k(\mathbb{Z}) \) contains a point \( x \) with \( |x_j| = 0,1,2 \). The special \( k \)'s are easy to describe and analyze, they are of zero density. Remaining \( k \)'s are called generic.

- For \( k > 0 \) generic a point \( x \in V_k(\mathbb{Z}) \) is GHOSH reduced if it is of the form

\[ (x_1, x_2, x_3) \text{ with } 3 \leq x_1 \leq x_2 \leq x_3 \text{ and } x_1^2 + x_2^2 + x_3^2 + x_1 x_2 x_3 = k \]

- (GHOSH) For \( k > 0 \) generic

\[ \prod V_k(\mathbb{Z}) \cong \text{GHOSH reduced points}. \]
COR: \( h(k) \ll |k|^\frac{1}{3} \)

(1) \[ \sum_{0 < k \leq K} h(k) \sim \frac{K(\log K)^2}{36}, \quad K \to \infty \]

\[ \sum_{-K \leq k < 0} h(k) \sim \frac{K(\log K)^2}{48}, \quad K \to \infty. \]

The explicit fundamental domains allow for the numerical computations of the \( h(k) \)'s and these indicate that

\[ \left| \sum_{1 \leq |k| \leq K : V_k \text{ fails Hasse}} \right| \sim CK^\Theta \]

with \( C \neq 0 \) and \( \Theta \approx 0.887... \).
Figure: Lattice points and fundamental set (triangular) for $k = 3685$. 
THEOREM 1 (GHOSH 15 2017)

(i) There are infinitely many $k$'s which fail the Hasse principle. The number of such with $|\mathfrak{a}| \leq k$ is at least $k^{3/2}/\log k$.

(ii) Fix $t \geq 0$

$$\left| \{ k \mid k \text{ admissible, } h(k) = t \} \right| = o(k)$$

As $k \to \infty$

$\Rightarrow$ Almost all $k$'s satisfy Hasse and also these $V_k(\mathbb{Q})$'s are Zariski dense.

COMMENTS:

(\sigma) The Hasse failures are produced by an obstruction via quadratic reciprocity. They come in two types: one direct use of reciprocity and the second which also incorporates the descent group.

Recently Loughran and Mitnanskii; and independently Colliot-Thélène, D. Sheng and F. Xu have shown that the obstructions of the first (but not second) can be be explained in terms of an integral Brauer-Manin obstruction.
For example if

\[ k = 4 + 2y^2 \]

with \( y \) having all of its prime factors \( \equiv \pm 1 \pmod{8} \) and \( y \equiv 0, \pm 3, \pm 4 \pmod{9} \), then \( k \) is admissible but \( V_k(\mathbb{Z}) = \emptyset \).

(b) Is proved by comparing the number of points on \( V_k(\mathbb{Z}) \) in certain tentacled regions gotten by special plane sections, with the expected number of solutions according to a product of local densities. The key is that the variance of this comparison goes to zero on averaging \( \|V_k\| \). This moving plane quadric method applies to more general cubic surfaces including ones that don't carry morphisms.
2 \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_0 - 1)^2 - \frac{\Theta_x^2 t}{W^2} + \frac{\Theta_y^2 (t-1)}{(W-1)^2} + \frac{(1-\Theta_z^2)t(t-1)}{(W-t)^2} \right)

Here \( \Theta_0, \Theta_x, \Theta_y, \Theta_z \) are parameters defining P-VI. Using appropriate co-ordinates the non-linear monodromy of solutions reduces the problem of determining finite orbits of a nonlinear action on \( \mathbb{A}^3 \).

For example if \( \Theta_x = \Theta_y = \Theta_z \) this group \( G \) is generated by involutions \( R_1, R_2, R_3 \) and permutations of the co-ords

\[ R_3 : (x_1, x_2, x_3) \rightarrow (x_1, x_2, x_1 x_2 - x_3) \]

and similarly for \( R_1 \) and \( R_2 \).
The transformation

\[ \Sigma_{2,3} R_3 : (x_1, x_2, x_3) \rightarrow (x_1, x_4 x_2 - x_3, x_2) \]

is in \( G \) and if fixes \( x_1 \), and induces the linear transf \( A \) on \( (x_2, x_3) \).

\[ A = \begin{bmatrix} x_1 & -1 \\ 1 & 0 \end{bmatrix} \]

so if \((x_1, x_2, x_3)\) is on a finite orbit then

\[ x_1 = \text{trace}(A) = 2 \cos(2\pi t_1) \quad \text{with} \quad t_1 \in \mathbb{Q} \]

Similarly for \( x_2 \) and \( x_3 \) and with a suitably chosen element of \( G \) one finds that if \((x_1, x_2, x_3)\) is in a finite orbit it gives rise to a solution of

\[ \cos 2\pi \phi_1 + \cos 2\pi \phi_2 + \cos 2\pi \phi_3 + \cos 2\pi \phi_4 = 0 \]

with the \( \phi_j \)'s in \( \mathbb{Q} \) and related to \( t_1, t_2, t_3 \).

By Lang's \( G_{\text{m}} \) we can parametrize all the solutions of \((*)\) and then check directly which correspond to finite orbits of \( G \) acting on \( \mathbb{A}^3 \).
STONG APPROXIMATION

When $V_r(Z) \neq \emptyset$ how rich is it beyond Zariski density?

We discuss the Markoff case $k = 0$.

The general case is similar but first requires a study of all the finite $\Gamma$-orbits in $\mathbb{A}^3(\mathbb{Q})$.

This is closely related to the determination (Dubrovin–Mazzocco) of the algebraic Painlevé VI's.

Our treatment of the latter uses the resolution (effective) of Lang's $G_0$ conjecture.

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

$\Gamma$ as before except that the $R_j$'s are

$R_3((x_1, x_2, x_3)) = (x_1, x_2, 3x_1x_2 - x_3)$

$p = 2$, with one orbit being $\{0\}$ and the other $Y^*(Z) = \Gamma(1, 1, 1, 1)$. 
Strong Approximation Conjecture for $y$:

Reduction mod $p$

$Y^* (\mathbb{Z}) \rightarrow Y^* (\mathbb{Z}/p\mathbb{Z})$ is onto for all primes $p$.

- $\Gamma$ acts on reduction mod $p$ as a permutation group on $Y^* (\mathbb{Z}/p\mathbb{Z})$.

- Strong approximation $\iff \Gamma$ acting transitively on $Y^* (\mathbb{Z}/p\mathbb{Z})$.

Note: $|Y^* (\mathbb{Z}/p\mathbb{Z})| \sim p^2$ as $p \to \infty$.

As long as $p^2 - 1$ is not very smooth (eg. $p = k!$) we can prove strong approximation.
**Theorem 2 (Bourgain-Gamburd-S, 2014)**

For $\epsilon > 0$ and $p$ large there is a $\Gamma$-orbit $\Theta(p)$ in $Y^*(\mathbb{Z}/p\mathbb{Z})$ such that

$$|\Theta(p)| = |Y^*(\mathbb{Z}/p\mathbb{Z})| \Theta(p) | \lesssim \epsilon^p$$

And every $\Gamma$-orbit $t(p)$ in $Y^*(\mathbb{Z}/p\mathbb{Z})$ satisfies

$$|t(p)| \gg (\log p)^{1/3}.$$ 

These have been recently improved by Konyagin-Makarychev-Shparlinski-Mugnian (2017)

To

$$|\Theta(p)| \leq \exp\left((\log p)^{2+o(1)}\right)$$

$$|t(p)| \gg (\log p)^{4/9}.$$ 

**Theorem 3 (BG-S, 2015)**

$$|\{p \leq T: \text{strong approximation fails for } p\}| \lesssim T^\epsilon$$

$\epsilon > 0$.

So in general there is always a giant component and the strong approximation conjecture holds except perhaps for very few $p$'s.
**Theorem 4 (Meiri-Puder 2019):**

If \( p \equiv 1(4) \) and \( p \) satisfies strong approximation for \( \hat{\gamma}^*(\mathbb{Z}/p\mathbb{Z})/\pm 1 \) then the action of \( \Gamma \) on the latter is either the full alternating or symmetric group.

Under the same assumptions on \( p \), the orbit of every point in \( \hat{\gamma}^*(\mathbb{Z}_p) \) is dense; here \( \mathbb{Z}_p \) is the \( p \)-adic integers.

**Theorem 4 allows one to show that:**

\[ \hat{\gamma}^*(\mathbb{Z}) \to \hat{\gamma}^*(\mathbb{Z}/q\mathbb{Z}) \text{ is one-to-one} \]

for \( q = p_1 p_2 \ldots p_k \), \( p_j \equiv 1(4) \) and satisfying strong approximation (Goursat-Lemma).

With these we can execute some simple sieving and couple it with some Teichmüller dynamics (Mirzakhani) to answer some old questions about Markoff numbers.
$M$: MARKOFF NUMBERS, THAT IS
COORDINATES OF A MARKOFF TRIPLE
$X \in \mathcal{Y}(\mathbb{Z})$ WITH $x_j > 0$.

$M$: 1, 2, 5, 13, 29, 34, 89, 169, 194, 

- FROBENIUS: $m \in M \Rightarrow m \neq 0, \pm 2/3 \mod p$,
  IF $p \equiv 3(4)$ AND $p \neq 3$.
- STRONG APPROXIMATION $\Rightarrow$ THESE ARE THE ONLY CONGRUENCE
  OBSTRUCTIONS.

$M$ IS LACUNARY:

$$\left| \left\{ m \leq T : m \in M \right\} \right| \sim c \left( \log T \right)^2,$$

ZAGIER (1982)
MIRZAKHANI (2016)

**THEOREM 5:** (B-G-S 2015)

ALMOST ALL $m \in M$ ARE COMPOSITE

$$\left| \left\{ p \leq T : p \in M, p \text{ prime} \right\} \right| = o\left( \left| \left\{ m \in M : m \leq T \right\} \right| \right),$$

AS $T \to \infty$. 
**Remarks**

Tools are elementary coming from analytic number theory, curves over finite fields and combinatorics. One interesting feature being:

\[
C_A : \begin{cases} 
  y + y^{-1} = x + 2x^{-1}, & x, y \in \mathbb{F}_p \\
  x \in H_1, & y \in H_2 \\
  H_1, H_2 \leq \mathbb{F}_p^{\times}, & |H_1| \leq |H_2|.
\end{cases}
\]

Need an upper bound for \(|C|\) of the form

\[
|C| \leq |H_2|^s
\]

for some \(s < 1\) independent of \(p\).

• If \(|H_2| \geq \sqrt{p}\) one can use the Riemann hypothesis for curves over finite fields to prove this.

• For \(|H_2|\) small this is of no use and we use Stepanov's elementary proof of Weil's theorem (specifically auxiliary polynomials) to establish such a bound.
\[ V_k \text{ is the relative character variety of representations of the fundamental group of a surface of genus one with one puncture, to } \text{SL}_2. \text{ The action of the mapping class group is that of } \Gamma. \]

More generally the (affine) relative character variety \( X_k \) of representations of \( \pi_1(\Sigma_{g,n}) \) into \( \text{SL}_2 \) is defined over \( \mathbb{Z}. \) \( \Sigma_{g,n} \) is a surface of genus \( g \) with \( n \) punctures.

One can study the Diophantine properties of \( X_k(\mathbb{Z}). \)
J.H. WHANG (PRINCETON THESIS 2018) has made big steps in this direction.

(i) $X_k$ has a projective compactification relative to which $X_k$ is "log Calabi Yau". According to conjectures of Vojta this places $X_k$ as being in the same threshold setting as affine cubic surfaces.

(ii) $X_k(Z)$ has a full descent in that the mapping class group acts via non-linear morphisms on $X_k(Z)$ with finitely many orbits.

These and more general character varieties connected with higher Teichmüller theory offer a rich family of threshold affine varieties for which one can approach the study of integral points.
There is a rich study of the action of \( \Gamma \) on \( X_k(R) \) (Thurston, Goldman...) and on \( X_k(\mathbb{Q}) \) (Canatat, McMullen... Entropy).

Since \( X_k \) is defined over \( \mathbb{Z} \), one can examine the orbit closures of \( \Gamma \) in \( X_k(\mathbb{Q}_p) \). The basic compact invariant set is \( X_k(\mathbb{Z}_p) \) and we expect as with \( g=1, n=1 \) the action of \( \Gamma \) on \( X_k(\mathbb{Z}_p) \) is minimal (closure of orbits are as large as possible).

Biswas | Gupta | MJ Whang (2019): classify finite (even bounded) orbits of \( \Gamma \) on \( X_k(\mathbb{Q}) \) for \( g \geq 1, n \geq 0 \) in terms of their lift \( \Gamma \) to a representation of \( \Sigma_{g,n} \) into \( \text{SL}_2(\mathbb{Q}) \), basically it should be finite.
If one replaces \( \mathbb{Z} \) by a larger ring \( D \), such as \( \mathbb{Z}[\frac{1}{5}] \) or \( \mathbb{Z}[\sqrt{2}] \), which contain infinitely many units, then the action of \( \Gamma \) on \( \Gamma_{M,K}(D) \) need no longer consist of finitely many orbits (first observed by Silverman).

This makes our Diophantine analysis much more challenging.

It appears that there are fewer (if any) exceptions to the Hasse principle.

For the Markoff surfaces this has bearing through Fricke's trace identities on commutators in \( SL_2(D) \).
Aner Shalev Question

Is every element in $\text{SL}_3(\mathbb{Z})$ a one commutator, i.e., can one solve for every $B$ in $\text{SL}_3(\mathbb{Z})$ for

$$XYX^{-1}Y^{-1} = B$$

Agni-Gelander-Kassabov-Shalev show that essentially there is no local obstruction to this in that it is true in every finite quotient of $\text{SL}_3(\mathbb{Z})$. 
REFERENCES CAN BE FOUND IN

"INTEGRAL POINTS ON MARKOFF TYPE CUBIC SURFACES"

A. GHOSH + P. SARNAK

arXiv: 1706.06712

AND

"NONLINEAR DESCENT ON MODULI OF LOCAL SYSTEMS"

THE RICHNESS RESULTS FOR MARKOFF SURFACES EXTEND TO OTHER CUBIC SURFACES, THOUGH STILL SPECIAL TO THE HOMOGENEOUS CUBIC PART SHOULD BE REDUCIBLE.

UNIVERSAL PERFECT FORMS

A CUBIC FORM IN THREE VARIABLES IS UNIVERSAL AND PERFECT IF IT REPRESENTS EVERY \( k \) AND RICHLY (\( V_k(\mathbb{Z}) \) IS ZARISKI DENSE AND A FORM OF STRONG APPROXIMATION HOLDS)

A POSSIBLE EXAMPLE ?:

EACH \( k \) IS ADMISSIBLE FOR

\[ x_1^3 + x_2^3 + 2x_3^3 \]

AND PERHAPS IT IS UNIVERSAL AND PERFECT.

GHOSH / S (2017):

\[ U(x_1, x_2, x_3) = x_2(x_3 - x_1) + x_1^2 x_2 + x_3^2 - x_1 x_2 x_3 \]

IS UNIVERSAL AND PERFECT.