A positive proportion of quartic binary forms does not represent 1

Shabnam Akhtari

University of Oregon

akhtari@uoregon.edu

June 25, 2020

Binary Forms

We are interested in forms of the shape

$$F(x, y) = a_0x^d + a_1x^{d-1}y + \ldots + a_dy^d,$$

with $a_i \in \mathbb{Z}$ of degree $d \geq 3$.

We will mostly talk about quartic forms; i.e., forms of degree $d = 4$.

Thue Equations

Let

$$F(x, y) = a_0 x^d + a_1 x^{d-1} y + \ldots + a_d y^d,$$

with $a_i \in \mathbb{Z}$, be a form of degree $d \geq 3$ which is irreducible over $\mathbb{Q}$.

Thue (1909)

The equation

$$F(x, y) = m$$

has only finitely many solutions in integers x and y.

The Proof of Finiteness

If $(x, y) \in \mathbb{Z}^2$ satisfies

$$\begin{aligned} F(x, y) &= a_0 x^d + a_1 x^{d-1} y + \ldots + a_d y^d \\ &= a_0 (x - \alpha_1 y) \ldots (x - \alpha_d y) = m, \end{aligned}$$

then $\frac{x}{y}$ is a good rational approximation for one of the algebraic numbers α_i.

Two Types of Questions

How many solutions a Thue equation can have?

How often do Thue equations have solutions?

Discriminants of Binary Forms

Let

$$\begin{aligned} F(x,y) &= a_0x^d + a_1x^{d-1}y + \ldots + a_dy^d \\ &= a_0(x-\alpha_1 y)\ldots(x-\alpha_d y). \end{aligned}$$

The discriminant $D = D(F)$ of $F(x,y)$ is

$$D := a_0^{2(d-1)} \prod_{i \neq j} (\alpha_i - \alpha_j)^2 .$$

Properties of Discriminant

The discriminant of $F(x, y) = a_0(x - \alpha_1 y) \ldots (x - \alpha_d y)$ is

$$a_0^{2(d-1)} \prod_{i \neq j} (\alpha_i - \alpha_j)^2 .$$

The discriminant of $F(x, y) = a_0 x^d + a_1 x^{d-1} y + \ldots + a_d y^d$ is a homogeneous polynomial in $\mathbb{Z}[a_0, \ldots, a_d]$ of degree $2d - 2$.

Properties of Discriminant

For $\begin{pmatrix} \mathfrak{a} & \mathfrak{b} \\ \mathfrak{c} & \mathfrak{d} \end{pmatrix}$, we define

$$F_A(x,y) = F(\mathfrak{a}x + \mathfrak{b}y, \mathfrak{c}x + \mathfrak{d}y).$$

The discriminant of $F_A(x,y) = F(\mathfrak{a}x + \mathfrak{b}y, \mathfrak{c}x + \mathfrak{d}y)$ equals

$$(\det(A))^{d(d-1)} D(F).$$

Invariants of Binary Forms

An invariant of a binary form is a polynomial in the coefficients of the binary form that remains invariant under $\mathrm{SL}_2(\mathbb{Z})$.

Invariants of Quartic Binary Forms

The discriminant D of F is given by

$$D = D_F = a_0^6(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_1-\alpha_4)^2(\alpha_2-\alpha_3)^2(\alpha_2-\alpha_4)^2(\alpha_3-\alpha_4)^2,$$

where α_1 , α_2, α_3 and α_4 are the roots of

$$F(x,1) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4.$$

The invariants of F form a ring, generated by two invariants I and J of weights 4 and 6.

The invariants of F form a ring, generated by two invariants

$$I = I_F = a_2^2 - 3a_1a_3 + 12a_0a_4$$

and

$$J = J_F = 2a_2^3 - 9a_1a_2a_3 + 27a_1^2a_4 - 72a_0a_2a_4 + 27a_0a_3^2.$$

I and J These are algebraically independent.

Every invariant is a polynomial in I and J.

For the invariant D, we have

$$27D = 4I^3 - J^2.$$

Equivalent Binary Forms

If $A \in \mathrm{GL}_2(\mathbb{Z})$, then we say that F_A is *equivalent* to F.

We will need to work with one binary form from each class.

Binary Forms with Bounded Discriminant

Birch and Merrimann (1972)

There are finitely many classes of integral binary forms of degree d with bounded discriminant.

Davenport-Heilbronn's theorem

The number of equivalence classes of irreducible binary cubic forms per discriminant is a positive constant on average.

Quartic Forms with Bounded I and J

Borel and Harish-Chandra (1962)

The number of equivalence classes of integral binary quartic forms, having any given fixed values of I and J (so long as I and J are not both equal to zero), is finite.

Bhargava and Shankar (2015)

Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves

Ordering Binary Forms

Naive heights

Discriminant

The generators of the ring of invariants

What Is a Good Upper Bound for the Number of Solutions of a Thue Equation?

$$x^d + c(x-y)(2x-y)\dots(dx-y) = 1.$$

This equation has at least d solutions, namely $(1,1)$, $(1,2)$, …, $(1,d)$.

the best possible upper bound

$$C\,d.$$

Upper Bounds

Bombieri-Schmidt (1987)

The Thue equation

$$|F(x, y)| = 1$$

has at most $215d$ solutions, provided that d is sufficiently large.

A. (2011), using linear forms in logs

The Thue equation

$$|F(x, y)| = 1$$

has at most $11d$ solutions, provided that the discriminant of F is large in terms of d.

How about $F(x, y) = m$?

Bombieri-Schmidt (1987)

If

$$\max_F \#\{(x, y) | F(x, y) = 1\} \leq N_d$$

then

$$\#\{(x, y) | F(x, y) = m\} \leq N_d d^{\omega(m)}.$$

Here $\omega(m)$ denotes the number of distinct prime factors of m.

Therefore,

$$F(x, y) = m$$

has at most $11d^{1+\omega(m)}$ integral solutions.

p-adic reductions

Consider

$$F(x, y) = p.$$

If

$$F(x, y) \equiv a_0 \prod (x - a_i y) \pmod{p},$$

then

$$F_i(x, y) := F(px + a_i y, y).$$

p divides all coefficients of F_i.

$$\tilde{F}_i(x, y) := \frac{1}{p} F(px + a_i y, y).$$

If (x_0, y_0) is a solution of

$$F(x, y) = p,$$

then

$$p | F(x_0, y_0).$$

So

$$p | (x_0 - a_i y_0)$$

for some i.

So $x_0 = pX_0 + a_i y_0$. And (X_0, y_0) is a solution to

$$\tilde{F}_i(x, y) = \frac{1}{p} F(px + a_i y, y) = 1.$$

Constructing New Binary Forms

The integral solutions of

$$F(x, y) = pm'$$

are in correspondence with integral solutions of up to d equations

$$G_i(x, y) = m', \qquad 1 \leq i \leq d,$$

provided that $\gcd(p, m') = 1$.

Each form $G_i(x, y)$ has degree d.

Each form $G_i(x, y)$ is obtained from $F(x, y)$ under the action of a 2×2 rational matrix with determinant p.

Bombieri-Schmidt (1987)

If

$$\max_F \#\{(x,y) | F(x,y) = 1\} \le N_d$$

then

$$\#\{(x,y) | F(x,y) = m\} \le N_d d^{\omega(m)}.$$

Here $\omega(m)$ denotes the number of distinct prime factors of m.

A. (2015)

Let $F(x,y) \in \mathbb{Z}[x,y]$ be an irreducible binary form of degree $d \geq 3$ and discriminant D. Let m be an integer with

$$0 < m \leq \frac{|D|^{\frac{1}{2(d-1)}-\epsilon}}{(3.5)^{d/2} d^{\frac{d}{2(d-1)}}},$$

where $0 < \epsilon < \frac{1}{2(d-1)}$. Then the equation $|F(x,y)| = m$ has at most

$$\begin{cases} 7d + \frac{d}{(d-1)\epsilon} & \text{if } d \geq 5 \\ 9d + \frac{d}{(d-1)\epsilon} & \text{if } d = 3, 4 \end{cases}$$

primitive solutions.

Constructing Quartic Thue Equations with no Solutions

Let $m = 5.7.11$.

Choose $F(x, y)$ with large enough discriminant. So that $F(x, y) = m$ has at most $4 \times 13 = 52$ solutions.

Choose F such that it splits completely modulo every prime factor of m.

Use Bombieri-Schmidt's p-adic reduction to obtain 4^3 equations

$$G(x, y) = 1$$

$4^3 > 52$.

Splitting Behavior

The p-adic density of quartic forms that split completely mod p is

$$\frac{(p-1)(p+1)p(p-1)(p-2)}{p^5}.$$

The equation $F(x, y) = 5.7.11$ has at most 52 solutions

Construction of Binary Forms that Locally Represent 1

$x^2y(x+y) = 1$ has no solution.

Construction of Binary Forms that Locally Represent 1

$$F(x, y) \equiv L_1(x, y) L_2^3(x, y) \mod p.$$

p-adic density:

$$\frac{(p+1)p(p-1)}{p^5}.$$

Construction of Binary Forms that Locally Represent 1

For larger p, we assume

$$F(x,y) \not\equiv Q(x,y)^2 \qquad \mod p.$$

p-adic density:

$$1 - \frac{(p-1)(p+1)p}{2p^5} - \frac{(p-1)(p+1)}{p^5}.$$

Ordering Quartic Binary Forms

Let F be a quartic form with the invariants I and J.

Bhargava-Shankar Height:

$$H(F) = H(I, J) := \max\left\{\left|I^3\right|, \frac{J^2}{4}\right\}.$$

A. (2020)

A positive proportion of integral quartic binary forms (that locally represent 1) does not represent 1 globally.

Bhargava and Shankar

Let $h^{(i)}(I, J)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary quartic forms having $4 - 2i$ real roots in $\mathbb{P}^1$ and invariants equal to I and J. Then

$$\begin{aligned}
\text{(a)} \quad \sum_{H(I,J)<X} h^{(0)}(I, J) &= \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}); \\
\text{(b)} \quad \sum_{H(I,J)<X} h^{(1)}(I, J) &= \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}); \\
\text{(c)} \quad \sum_{H(I,J)<X} h^{(2)}(I, J) &= \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}).
\end{aligned}$$

Eligible Invariants

We need to know which pairs (I, J) can actually occur as the invariants of an integral binary quartic form.

Eligible Invariants

In the binary quartic case, Bhargava and Shanker prove that an (I, J) is *eligible* (i.e., it occurs as the invariants of some binary quartic forms) if and only if it satisfies any one of a certain specific finite set of congruence modulo 27.

Bhargava and Shankar (2013)

A pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ occurs as the invariants of an integral binary quartic form if and only if it satisfies one of the following congruence conditions:

$$
\begin{aligned}
&\text{(a) } I \equiv 0 \pmod 3 \quad \text{and} \quad J \equiv 0 \pmod{27},\\
&\text{(b) } I \equiv 1 \pmod 9 \quad \text{and} \quad J \equiv \pm 2 \pmod{27},\\
&\text{(c) } I \equiv 4 \pmod 9 \quad \text{and} \quad J \equiv \pm 16 \pmod{27},\\
&\text{(d) } I \equiv 7 \pmod 9 \quad \text{and} \quad J \equiv \pm 7 \pmod{27}.
\end{aligned}
$$

It follows that the number of eligible (I, J), with $H(I, J) < X$, is a constant times $X^{5/6}$.

And therefore the number of classes of binary quartic forms per eligible (I, J) is a finite constant on average.

The number of equivalence classes of binary quartic forms per eligible (I, J), having a given number of real roots, is a constant on average. This constant is either $\zeta(2)/2$ or $\zeta(2)$, depending on whether the given number of real roots is 4 or less than 4, respectively.

Construction of Binary Forms that Locally Represent 1

In fact, Bhargava and Shankar obtain the asymptotic count of binary quartic forms, having bounded invariants, satisfying any specified finite set of congruence conditions.

Such a modification is crucial in application to ordering quartic forms by their *Bhargava-Shankar heights* in order to avoid construction of Thue equations that have no solutions because of local obstructions.

Construction of Binary Forms that are not Equivalent

Bhargava-Shankar

The number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of integral binary quartic forms $F \in V_{\mathbb{Z}}$ with non-zero discriminant and $H(I, J) < X$ whose stabilizer in $\mathrm{GL}_2(\mathbb{Q})$ has size greater than 2 is $O(X^{3/4+\epsilon})$.

Thank you!

Questions?