Rational Points on elliptic curves

Integer points on cubic curves

Ajay Prajapati
170063

Dept. of Mathematics and Statistics
Indian Institute of Technology, Kanpur

End-Semester Exam presentation

How many integer points?

- Let C be non-singular cubic with integer coefficients given by

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \quad (1)$$

- Natural Number theoretic problem is to describe all solutions (x, y) to cubic equation with x, y $\in \mathbb{Z}$.

How many integer points?

- Let C be non-singular cubic with integer coefficients given by

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \quad (1)$$

- Natural Number theoretic problem is to describe all solutions (x, y) to cubic equation with x, y $\in \mathbb{Z}$.
- If curve given by Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ then Nagell-Lutz theorem tells that points of finite order have integer coordinates.
- Converse? $y^2 = x^3 + 3$ have integer point P=(1, 2) and 2P=$(\frac{-23}{16}, \frac{11}{16})$. So P is not finite order point.

How many integer points to expect?

- If rank of C is 0 then by Nagell-Lutz theorem all rational points(finitely many) on C are integer points.
- Suppose C is of rank 1 having trivial torsion. Let P be generator of $C(\mathbb{Q})$ then any point in $C(\mathbb{Q})$ is of form nP, for some n$\in \mathbb{Z}$. If $nP = (x_n, y_n)$ then for n$\geq$3,

$$x_n = \left(\frac{y_{n-1} - y_1}{x_{n-1} - x_1}\right)^2 - a - x_{n-1} - x_1 \tag{2}$$

How many integer points to expect?

- If rank of C is 0 then by Nagell-Lutz theorem all rational points(finitely many) on C are integer points.
- Suppose C is of rank 1 having trivial torsion. Let P be generator of $C(\mathbb{Q})$ then any point in $C(\mathbb{Q})$ is of form nP, for some n$\in \mathbb{Z}$. If $nP = (x_n, y_n)$ then for n$\geq$3,

$$x_n = \left(\frac{y_{n-1} - y_1}{x_{n-1} - x_1}\right)^2 - a - x_{n-1} - x_1 \tag{2}$$

Siegel's Theorem(1929)

A smooth affine algebraic curve C of genus g defined over a number field K, there are only finitely many points on C with coordinates in the ring of integers $\mathcal{O}$ of K, provided $g > 0$.

Taxicabs and sum of two cubes

- Famous story? 1729 is the smallest number expressible as a sum of two cubes in two different ways: $1729 = 9^3 + 10^3 = 1^3 + 12^3$.

Taxicabs and sum of two cubes

- Famous story? 1729 is the smallest number expressible as a sum of two cubes in two different ways: $1729 = 9^3 + 10^3 = 1^3 + 12^3$.
- Means cubic curve $x^3 + y^3 = 1729$ has two integer points upto ordering of x and y, How to prove? Factorize $x^3 + y^3$.

Taxicabs and sum of two cubes

- Famous story? 1729 is the smallest number expressible as a sum of two cubes in two different ways: $1729 = 9^3 + 10^3 = 1^3 + 12^3$.
- Means cubic curve $x^3 + y^3 = 1729$ has two integer points upto ordering of x and y, How to prove? Factorize $x^3 + y^3$.
- Taxicab Equation: $x^3 + y^3 = m$. Bound on solutions?

Theorem

Let m ≥ 1 be an integer. Then every solution to the equation $x^3 + y^3 = m$ in integers x, y $\in \mathbb{Z}$ satisfies $\max\{|x|, |y|\} \leq \sqrt{2m/3}$.

Taxicabs and sum of two cubes

- Famous story? 1729 is the smallest number expressible as a sum of two cubes in two different ways: $1729 = 9^3 + 10^3 = 1^3 + 12^3$.
- Means cubic curve $x^3 + y^3 = 1729$ has two integer points upto ordering of x and y, How to prove? Factorize $x^3 + y^3$.
- Taxicab Equation: $x^3 + y^3 = m$. Bound on solutions?

Theorem

Let m $\geq$ 1 be an integer. Then every solution to the equation $x^3 + y^3 = m$ in integers x, y $\in \mathbb{Z}$ satisfies $\max\{|x|, |y|\} \leq \sqrt{2m/3}$.

Theorem

For every N $\geq$ 1, there is an integer m $\geq$ 1 such that the cubic curve $x^3 + y^3 = m$ has at least N points with integer coordinates.

Taxicabs and sum of two cubes

- Ramanujan's observation was also that 1729 is the **smallest** m with two positive solutions. Based on this, people have defined Nth taxicab number: **Taxi**(N)=min$\{$m $\geq$ 1: $x^3 + y^3 = m$ has atleast N solutions with $x \geq y \geq 1\}$.

Taxicabs and sum of two cubes

- Ramanujan's observation was also that 1729 is the **smallest** m with two positive solutions. Based on this, people have defined Nth taxicab number: **Taxi**(N)=min$\{$m ≥ 1: $x^3 + y^3 = m$ has atleast N solutions with $x \geq y \geq 1\}$.
- **Taxi**(1)=2
  Taxi(2)=1729
  Taxi(3)=87539319
  Taxi(4)=6963472309248
  Taxi(5)=48988659276962496
  Taxi(6)= 24153319581254312065344
- Till now only 6 taxicab numbers are known. Although upper bounds on next 6 taxicab numbers have been obtained.

Relationship between number of integer point and rank of group of rational points

- There is an interesting relationship between the number of integer points and the rank of the group of rational points.

Relationship between number of integer point and rank of group of rational points

- There is an interesting relationship between the number of integer points and the rank of the group of rational points.
- Serge Lang made a general conjecture that has been proven for certain types of cubic curves, including the taxicab curves studied in this section.

Theorem(Silverman)

There is a constant $K > 1$ with the following property. For every integer $m \geq 1$, the number of relatively prime integer points on the cubic curve

$$C_m : x^3 + y^3 = m \tag{3}$$

is bounded by the rank of C_m via the estimate

$$\#\{(x, y) \in C_m(\mathbb{Q}) : x, y \in \mathbb{Z}, gcd(x, y) = 1\} \leq K^{1+rank(C_m(\mathbb{Q}))} \tag{4}$$

Diophantine Approximation

Diophantine Approximation

This is a branch of mathematics which deals with approximating real numbers with rational numbers.

Diophantine Approximation

This is a branch of mathematics which deals with approximating real numbers with rational numbers.

1. The first problem was how "well" a real number can be approximated by a rational number. This was solved in 18th century by using **continued fractions**.

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}} \tag{5}$$

2. The first few convergents are 3, 22/7, 333/106, 355/113.

Diophantine Approximation

Diophantine Approximation

This is a branch of mathematics which deals with approximating real numbers with rational numbers.

1. The first problem was how "well" a real number can be approximated by a rational number. This was solved in 18th century by using **continued fractions**.

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}} \tag{5}$$

2. The first few convergents are 3, 22/7, 333/106, 355/113.
3. Now the main problem is to find sharp upper bound on above approximation. The first result is due to Liouville who used it to prove existence of **transcendental numbers** by giving an explicit example.

Thue's Theorem

Thue's Theorem(1909)(Special case)

Let b be a positive integer that is not a perfect cube, and let $\beta = \sqrt[3]{b}$ Let C be any fixed positive constant. Then there are only finitely many pairs of integers (p, q) with q $>$0 that satisfy the inequality

$$\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^3} \tag{6}$$

Thue's Theorem

Thue's Theorem(1909)(Special case)

Let b be a positive integer that is not a perfect cube, and let $\beta = \sqrt[3]{b}$ Let C be any fixed positive constant. Then there are only finitely many pairs of integers (p, q) with q $>$0 that satisfy the inequality

$$\left| \frac{p}{q} - \beta \right| \leq \frac{C}{q^3} \tag{6}$$

1. The above theorem is special case of more general theorem. The proof is complicated like proof of Mordell's Theorem. So I am going to give only outline and main results that are required in proof.

Thue's Theorem

Thue's Theorem(1909)(Special case)

Let b be a positive integer that is not a perfect cube, and let $\beta = \sqrt[3]{b}$ Let C be any fixed positive constant. Then there are only finitely many pairs of integers (p, q) with q $>$0 that satisfy the inequality

$$\left| \frac{p}{q} - \beta \right| \leq \frac{C}{q^3} \tag{6}$$

1. The above theorem is special case of more general theorem. The proof is complicated like proof of Mordell's Theorem. So I am going to give only outline and main results that are required in proof.

Corollary

Let a, b, c be non-zero integers. Then the equation $ax^3 + by^3$= c has only finitely many solutions in integers x, y.

Frame Title

Proof of corollary

1. It is sufficient to prove corollary for the equation $x^3 - by^3 = c$ with $b, c \in \mathbb{Z}, b > 0, c > 0$.

Frame Title

Proof of corollary

1. It is sufficient to prove corollary for the equation $x^3 - by^3 = c$ with $b, c \in \mathbb{Z}, b > 0, c > 0$.
2. Let $\beta = \sqrt[3]{b}$. Then $x^3 - by^3 = (x - \beta y)(x^2 + \beta xy + \beta^2 y^2)$. Now $x^2 + \beta xy + \beta^2 y^2 \geq 3/4\beta^2$.

Frame Title

Proof of corollary

1. It is sufficient to prove corollary for the equation $x^3 - by^3 = c$ with $b, c \in \mathbb{Z}, b > 0, c > 0$.
2. Let $\beta = \sqrt[3]{b}$. Then $x^3 - by^3 = (x - \beta y)(x^2 + \beta xy + \beta^2 y^2)$. Now $x^2 + \beta xy + \beta^2 y^2 \geq 3/4\beta^2$.
3. Hence we get,
$$\left|\frac{x}{y} - \beta\right| \leq \frac{4|c|}{3\beta^2} . \frac{1}{|y|^3} \tag{7}$$
4. Then Thue's Theorem says there are only finitely many (x, y) with $y > 0$. To deal with $y < 0$ rewrite the equation as following and again apply Thue's Theorem.

$$\left|\frac{-x}{-y} - \beta\right| \leq \frac{4|c|}{3\beta^2} . \frac{1}{|y|^3} \tag{8}$$

Possible proof of Diophantine equation

1. It can be proved that $\exists$ a constant C' s.t. for every rational number p/q,

$$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C' q^3} \tag{9}$$

Possible proof of Diophantine equation

1. It can be proved that $\exists$ a constant C' s.t. for every rational number p/q,

$$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C'q^3} \tag{9}$$

2. Recall we were trying to prove that for every constant C, there are only finitely many rationals p/q satisfying the inequality

$$\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^3} \tag{10}$$

3. Suppose we could prove stronger version of (1) with exponent < 3.

$$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C'q^{2.9}} \tag{11}$$

Possible proof of Diophantine equation

1. It can be proved that $\exists$ a constant C' s.t. for every rational number p/q,
$$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C'q^3} \tag{9}$$
2. Recall we were trying to prove that for every constant C, there are only finitely many rationals p/q satisfying the inequality
$$\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^3} \tag{10}$$
3. Suppose we could prove stronger version of (1) with exponent < 3.
$$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C'q^{2.9}} \tag{11}$$
4. Then combining (8) and (9), we get $q \leq (CC')^{10}$ and we are done.

Possible proof of Diophantine equation

1. How to improve (7)? Let's summarize how we proved it.
   1. Took polynomial $f(X) = X^3 - b \in \mathbb{Z}[\mathbb{X}]$ which has β as a root.
   2. Noted $|f(p/q)| \geq 1/q^3$. Factoring f(X) we saw that $|f(p/q)|$ is $|p/q - \beta|$ times something bounded hence we get (7).

Possible proof of Diophantine equation

1. How to improve (7)? Let's summarize how we proved it.
    1. Took polynomial $f(X) = X^3 - b \in \mathbb{Z}[\mathbb{X}]$ which has β as a root.
    2. Noted $|f(p/q)| \geq 1/q^3$. Factoring f(X) we saw that $|f(p/q)|$ is $|p/q - \beta|$ times something bounded hence we get (7).
2. One way to improve (7) might be to use some other polynomial $f(X) \in \mathbb{Z}[X]$ instead of $X^3 - b$.
    1. Suppose we are able to find $f(X) \in \mathbb{Z}[\mathbb{X}]$ which is divisible by $(X^3 - b)^n$ for some n.
    2. Then f(X) factors as

$$f(X) = (X - \beta)^n g(X) \text{ with } g(X) \in \mathbb{R}[X] \tag{12}$$

Possible proof of Diophantine equation

1. How to improve (7)? Let's summarize how we proved it.
    1. Took polynomial $f(X) = X^3 - b \in \mathbb{Z}[\mathbb{X}]$ which has β as a root.
    2. Noted $|f(p/q)| \geq 1/q^3$. Factoring f(X) we saw that $|f(p/q)|$ is $|p/q - \beta|$ times something bounded hence we get (7).
2. One way to improve (7) might be to use some other polynomial $f(X) \in \mathbb{Z}[X]$ instead of $X^3 - b$.
    1. Suppose we are able to find $f(X) \in \mathbb{Z}[\mathbb{X}]$ which is divisible by $(X^3 - b)^n$ for some n.
    2. Then f(X) factors as

$$f(X) = (X - \beta)^n g(X) \text{ with } g(X) \in \mathbb{R}[X] \tag{12}$$

    3. As before, we can show that

$$|F(p/q)| \leq C''|p/q - \beta|^n \tag{13}$$

continued

1. Proof continued...
   1. Since F(p/q) $\neq$ 0, this implies
   $$|F(p/q)| \geq 1/q^d \text{ where } d = deg(f) \tag{14}$$
   2. Comparing upper and lower bounds and taking nth roots, we get
   $$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C''} \cdot \frac{1}{q^{d/n}} \tag{15}$$

continued

1. Proof continued...
   1. Since F(p/q) $\neq$ 0, this implies
   $$|F(p/q)| \geq 1/q^d \text{ where } d = deg(f) \tag{14}$$
   2. Comparing upper and lower bounds and taking nth roots, we get
   $$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C''} \cdot \frac{1}{q^{d/n}} \tag{15}$$
   3. If $d < 3n$ we are done. But $d \geq 3n$ because $(X^3 - b)^n | f(X)$. So using this method, we achieve nothing.

continued

1. Proof continued...
   1. Since F(p/q) $\neq$ 0, this implies
   $$|F(p/q)| \geq 1/q^d \text{ where } d = deg(f) \tag{14}$$
   2. Comparing upper and lower bounds and taking nth roots, we get
   $$\left|\frac{p}{q} - \beta\right| \geq \frac{1}{C''} \cdot \frac{1}{q^{d/n}} \tag{15}$$
   3. If $d < 3n$ we are done. But $d \geq 3n$ because $(X^3 - b)^n | f(X)$. So using this method, we achieve nothing.
2. Thue's brilliant idea which enabled him to prove (8) is to use a two variable polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$. He chose the polynomial that vanishes to high order of (β, β) and then compared the upper and lower bound of for the value $|F(p_1/q_1, p_2/q_2)|$ where p_1/q_1 and p_2/q_2 are solutions of (7).
3. Thue's theorem proof naturally breaks into three parts of which we give outline.

Outline of proof

Construction of auxiliary polynomial

We construct $F(X, Y) \in \mathbb{Z}[X, Y]$ with reasonably small coefficients that vanishes to high order of (β, β).

Outline of proof

Construction of auxiliary polynomial

We construct $F(X, Y) \in \mathbb{Z}[X, Y]$ with reasonably small coefficients that vanishes to high order of (β, β).

The auxilary polynomial is small

1. We assume that there are infinitely many pairs of integers (p, q) that satisfy the inequality (8).
2. Under this assumption, we can find a rational p_1/q_1 satisfying (8) and with q_1 quite large. Then we can find a second rational number p_2/q_2 satisfying (8) with q_2 much larger than q_1.

Outline of proof

Construction of auxiliary polynomial

We construct $F(X, Y) \in \mathbb{Z}[X, Y]$ with reasonably small coefficients that vanishes to high order of (β, β).

The auxilary polynomial is small

1. We assume that there are infinitely many pairs of integers (p, q) that satisfy the inequality (8).
2. Under this assumption, we can find a rational p_1/q_1 satisfying (8) and with q_1 quite large. Then we can find a second rational number p_2/q_2 satisfying (8) with q_2 much larger than q_1.
3. We consider the value of the polynomial F(X, Y) at the point $(p_1/q_1, p_2/q_2)$. Since F(X, Y) vanishes to high order at (β, β) and since (8) says that each p_i/q_i is close to β, gives $F(p_1/q_1, p_2/q_2)$ very small.

Outline of Proof

The Auxilary polynomial does not vanish

1. This is the subtlest part of the proof. We want to show that $F(p_1/q_1, p_2/q_2)$ is not zero. Hence,

$$\left| F\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \right| \geq \frac{1}{q_1^d q_2^e} \tag{16}$$

Outline of Proof

The Auxilary polynomial does not vanish

1. This is the subtlest part of the proof. We want to show that $F(p_1/q_1, p_2/q_2)$ is not zero. Hence,

$$\left| F\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \right| \geq \frac{1}{q_1^d q_2^e} \tag{16}$$

2. Hope that this lower bound contradicts the upper bound in step 2.
3. Unfortunately, we will not be able to show that $F(p_1/q_1, p_2/q_2) \neq 0$.

Outline of Proof

The Auxilary polynomial does not vanish

1. This is the subtlest part of the proof. We want to show that $F(p_1/q_1, p_2/q_2)$ is not zero. Hence,

$$\left| F\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \right| \geq \frac{1}{q_1^d q_2^e} \tag{16}$$

2. Hope that this lower bound contradicts the upper bound in step 2.
3. Unfortunately, we will not be able to show that $F(p_1/q_1, p_2/q_2) \neq 0$.
4. Instead we show that some derivative of F does not vanish at $(p_1/q_1, p_2/q_2)$. This means in step 2, we need to give upper bound on the values of the derivatives of F.

Construction of auxilary polynomial

We will build F is by solving a system of linear equations with integer coefficients. Siegel was first person to study integer solution of linear system with integer coefficients.

Construction of auxilary polynomial

We will build F is by solving a system of linear equations with integer coefficients. Siegel was first person to study integer solution of linear system with integer coefficients.

Siegel's Lemma(1929)

Let $N > M$ be $+$ve integers and let

$$\begin{gathered} a_{11}T_1 + ... + a_{1N}T_N = 0 \\ .. \; .... \; ... \; =0 \\ a_{M1}T_1 + ... + a_{MN}T_N = 0 \end{gathered}$$

be a system of linear equations with integer coefficients. Then there is a non-trivial solution $T = (t_1, ...t_N)$ satisfying

$$max_{1\leq i\leq N}|t_i| < 2(4Nmax_{i.j}|a_{ij}|)^{\frac{N}{N-M}} \tag{17}$$

Construction of auxilary polynomial

Auxiliary Polynomial Theorem

Let $b \in \mathbb{Z}$ and $\beta = \sqrt[3]{b}$ and let $m, n \in \mathbb{Z}$ s.t. $m \geq 3$ and $m = \left\lfloor \frac{2}{3} n \right\rfloor$. Then there is a non-zero polynomial

$$F(X, Y) = P(X) + YQ(X) = \sum_{i=0}^{m+n} (u_i + v_i Y) X^i \tag{18}$$

of degree atmost m+n and having the following properties:

- $F^k(\beta, \beta) = 0$ for all $0 \leq k < n$
- $max_{0 \leq i \leq m+n} \{|u_i|, |v_i|\} \leq 2(16b)^{9(m+n)}$

Auxilary polynomial is small

Smallness Theorem

Let F (X, Y) be a polynomial as described in previous theorem. Then there is a constant $c_1 > 0$, depending only on b, so that for any x, y $\in \mathbb{R}$ with $|x - \beta| \leq 1$ and for any integer $0 \leq t \leq n$, we have

$$|F^{(t)}(x, y)| \leq c_1^n(|x - \beta|^{n-t} + |y - \beta|) \tag{19}$$

Auxilary polynomial does not vanish

Now, we want that if x and y are rational numbers, then F(x, y) is not zero. Unfortunately, it is not possible to prove such a strong result. Instead, it is shown that some derivative $F^{(t)}(X, Y)$, with t not too large, does not vanish.

Auxilary polynomial does not vanish

Now, we want that if x and y are rational numbers, then F(x, y) is not zero. Unfortunately, it is not possible to prove such a strong result. Instead, it is shown that some derivative $F^{(t)}(X, Y)$, with t not too large, does not vanish.

Non-vanishing theorem

Let F(X, Y) be an auxiliary polynomial as above. Let $p_1/q_1, p_2/q_2 \in \mathbb{Q}$ in lowest terms. Then there is a constant c_2, depending only on b, and an integer t satisfying

$$0 \leq t \leq 1 + \frac{c_2 n}{log q_1} \tag{20}$$

so that

$$F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0 \tag{21}$$

Main result

Diophantine Approximation Theorem

Let b be a positive integer that is not a perfect cube, and let $\beta = \sqrt[3]{b}$ Let C be any fixed positive constant. Then there are only finitely many pairs of integers (p, q) with q $>$0 that satisfy the inequality

$$\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^3} \tag{22}$$

Proof

1. Assume above inequality has infinitely many solutions.
2. We can find a solution (p_1, q_1) s.t. $q_1 > e^{9c_2}$ and $q_1 > (2c_1C)^{18}$
3. We can find a solution (p_2, q_2) satisfying $q_2 > q_1^{65}$.
4. Let n be the integer satisfying $n = \left\lfloor \frac{9}{8} . \frac{logq_2}{logq_1} \right\rfloor$. Exponentiating this becomes, $q_1^{\frac{8}{9}n} \leq q_2 < q_1^{\frac{8}{9}(n+1}$.

Proof

Proof

1. Clearly, $n > \frac{9}{8}.65 - 1 > 72$.
2. Use Auxilary Polynomial Theorem and above value of n to find polynomial F(X, Y). Use non-vanishing theorem to find integer t s.t. $0 \leq t \leq 1 + \frac{c_2 n}{log q_1} < 1 + \frac{1}{9}n$ and $F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0$.

Proof

Proof

1. Clearly, $n > \frac{9}{8}.65 - 1 > 72$.
2. Use Auxilary Polynomial Theorem and above value of n to find polynomial F(X, Y). Use non-vanishing theorem to find integer t s.t. $0 \leq t \leq 1 + \frac{c_2 n}{log q_1} < 1 + \frac{1}{9}n$ and $F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0$.
3. This means that $\left|F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)\right| \geq \frac{1}{q_1^{m+n} q_2} \geq \frac{1}{q_1^{23n/9+8/9}}$.

Proof

Proof

1. Clearly, $n > \frac{9}{8}.65 - 1 > 72$.
2. Use Auxilary Polynomial Theorem and above value of n to find polynomial F(X, Y). Use non-vanishing theorem to find integer t s.t. $0 \leq t \leq 1 + \frac{c_2 n}{log q_1} < 1 + \frac{1}{9}n$ and $F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0$.
3. This means that $\left|F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)\right| \geq \frac{1}{q_1^{m+n} q_2} \geq \frac{1}{q_1^{23n/9+8/9}}$.
4. To find upper bound, we use Smallness theorem,

$$\left|F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)\right| \leq c_1^n \left(\left|\frac{p_1}{q_1} - \beta\right|^{n-t} + \left|\frac{p_2}{q_2} - \beta\right|\right) \leq \frac{1}{q_1^{\frac{47}{18}n-3}} \tag{23}$$

Proof

1. Combining the above 2, we get

$$\frac{1}{q_1^{23n/9+8/9}} \leq \left| F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \right| \leq \frac{1}{q_1^{47n/18-3}} \tag{24}$$

Proof

1. Combining the above 2, we get
$$\frac{1}{q_1^{23n/9+8/9}} \leq \left| F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \right| \leq \frac{1}{q_1^{47n/18-3}} \tag{24}$$
2. This means $q_1^{\frac{1}{18}n-\frac{35}{9}} \leq 1$.

Proof

1. Combining the above 2, we get
$$\frac{1}{q_1^{23n/9+8/9}} \leq \left| F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \right| \leq \frac{1}{q_1^{47n/18-3}} \tag{24}$$
2. This means $q_1^{\frac{1}{18}n - \frac{35}{9}} \leq 1$.
3. As $n \geq 72$ was chosen, this means $q_1^{\frac{1}{9}} \leq 1$. This is absurd because integer q_1 is certainly ≥ 2. This completes the proof.

Results in Diophantine approximation

Thue's Theorem (1909)

Let $\beta \in \mathbb{R}$ be the root of an irreducible polynomial $f[X] \in \mathbb{Q}[X]$ with d $=$ deg(f) $\geq$ 3. Let $\epsilon > 0$ and C $>$0 be positive numbers. Then there are only finitely many pairs of integers (p, q) with q $>$0 that satisfy the inequality

$$\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^{1+d/2+\epsilon}} \tag{25}$$

Results in Diophantine approximation

Thue's Theorem (1909)

Let $\beta \in \mathbb{R}$ be the root of an irreducible polynomial $f[X] \in \mathbb{Q}[X]$ with d $=$ deg(f) $\geq$ 3. Let $\epsilon > 0$ and C $>$0 be positive numbers. Then there are only finitely many pairs of integers (p, q) with q $>$0 that satisfy the inequality

$$\left| \frac{p}{q} - \beta \right| \leq \frac{C}{q^{1+d/2+\epsilon}} \tag{25}$$

1. A number of mathematicians have strengthened the Thue's result.
2. We might ask for what value of $\tau(d)$ is it true that there are only finitely many rational numbers satisfying

$$\left| \frac{p}{q} - \beta \right| \leq \frac{C}{q^{\tau(d)+\epsilon}} \tag{26}$$

Results in Diophantine approximation

1. The following traces the history of the problem:
   - Liouville (1851) $\tau(d) = d$
   - Thue (1909) $\tau(d) = 1 + d/2$
   - Siegel (1921) $\tau(d) = 2\sqrt{d}$
   - Gelfond, Dyson (1947) $\tau(d) = \sqrt{2d}$
   - Roth (1955) $\tau(d) = 2$

Results in Diophantine approximation

1. The following traces the history of the problem:
   - Liouville (1851) $\tau(d) = d$
   - Thue (1909) $\tau(d) = 1 + d/2$
   - Siegel (1921) $\tau(d) = 2\sqrt{d}$
   - Gelfond, Dyson (1947) $\tau(d) = \sqrt{2d}$
   - Roth (1955) $\tau(d) = 2$
2. Roth theorem is somewhat surprising, says for every degree d, we can take $\tau(d) = 2$. It is the strongest theorem of this form because any $\tau(d) < 2$ would not work. **Roth won Field's medal in 1958 for this work**.

Results in Diophantine approximation

1. The following traces the history of the problem:
   - Liouville (1851) $\tau(d) = d$
   - Thue (1909) $\tau(d) = 1 + d/2$
   - Siegel (1921) $\tau(d) = 2\sqrt{d}$
   - Gelfond, Dyson (1947) $\tau(d) = \sqrt{2d}$
   - Roth (1955) $\tau(d) = 2$
2. Roth theorem is somewhat surprising, says for every degree d, we can take $\tau(d) = 2$. It is the strongest theorem of this form because any $\tau(d) < 2$ would not work. **Roth won Field's medal in 1958 for this work**.
3. There are higher dimensional generalisation (both proven and conjectural) due to Schmidt, Vojta and Faltings.

1. The proof that we gave for our **special case** of Thue's theorem contains all of the ingredients that appear in general.

1. The proof that we gave for our **special case** of Thue's theorem contains all of the ingredients that appear in general.
2. One constructs an auxiliary polynomial, evaluates it at some rational numbers, shows that it (or a small derivative) does not vanish, and derives a contradiction by giving upper and lower bounds for its magnitude.

1. The proof that we gave for our **special case** of Thue's theorem contains all of the ingredients that appear in general.
2. One constructs an auxiliary polynomial, evaluates it at some rational numbers, shows that it (or a small derivative) does not vanish, and derives a contradiction by giving upper and lower bounds for its magnitude.
3. Siegel, Gelfond, and Dyson obtain their stronger results by using a general polynomial $F(X, Y)$, rather than a polynomial of the form $P(X)+YQ(X)$ as used by Thue.

1. The proof that we gave for our **special case** of Thue's theorem contains all of the ingredients that appear in general.
2. One constructs an auxiliary polynomial, evaluates it at some rational numbers, shows that it (or a small derivative) does not vanish, and derives a contradiction by giving upper and lower bounds for its magnitude.
3. Siegel, Gelfond, and Dyson obtain their stronger results by using a general polynomial $F(X, Y)$, rather than a polynomial of the form $P(X)+YQ(X)$ as used by Thue.
4. The proof of Siegel theorem can be found in book: **Arithmetic on Elliptic curves** by Silverman. There he proves the theorem for general number fields (not only for rationals) and for general absolute value (not just for usual absolute value).

1. The proof that we gave for our **special case** of Thue's theorem contains all of the ingredients that appear in general.
2. One constructs an auxiliary polynomial, evaluates it at some rational numbers, shows that it (or a small derivative) does not vanish, and derives a contradiction by giving upper and lower bounds for its magnitude.
3. Siegel, Gelfond, and Dyson obtain their stronger results by using a general polynomial F(X, Y), rather than a polynomial of the form P(X)+YQ(X) as used by Thue.
4. The proof of Siegel theorem can be found in book: **Arithmetic on Elliptic curves** by Silverman. There he proves the theorem for general number fields (not only for rationals) and for general absolute value (not just for usual absolute value).
5. Roth improves this by using an auxiliary polynomial $F(X_1, ..., X_r)$ of many variables.

Frame Title

Thank You