

Dilip Das

11/22/04

Thue's Theorem.

$$ax^3 + by^3 = c \quad a, b, c \in \mathbb{Z} \text{ nonzero.}$$

finitely many integer solutions.

\iff DAT

$$\beta = \sqrt[3]{b} \quad b \neq 0 \text{ integer not a perfect cube.}$$

Then there are finitely many p/q with

$$\left| \frac{p}{q} - \beta \right| \leq \frac{C}{q^3} \quad C \geq 0.$$

Want to construct $F(x, y)$ s.t.

$$F(\beta, \beta) = 0$$

F vanish to high order at (β, β) .

Today: Find F .

Siegel's Lemma: Let $N > M$ pos. integers.

Given a homogenous linear system of M equations in N unknowns:

$$A \bar{t} = \bar{0}$$

$$A = M \times N \text{ matrix. } \bar{t} = N \times 1 \quad \bar{0} = M \times 1$$

with integer coefficients

Then there exists a nonzero integer solution

$$\bar{t} = (t_1, \dots, t_N) \text{ satisfying}$$

$$\max_{1 \leq i \leq N} |t_i| < 2 \left(4N \prod_{i,j} |A_{ij}| \right)^{\frac{M}{N-M}}$$

$$F(x, y) = P(x) + Y Q(x)$$

$$\deg(P(x)), \deg(Q(x)) \leq m+n$$

Let n be a large positive integer.

$$\text{Let } m = \lfloor \frac{2n}{3} \rfloor$$

$$(X-\beta)^n \mid F(X, Y)$$

$$\frac{d^k}{dx^k} (x^n) = \frac{n!}{(n-k)!} x^{n-k}.$$

Notice $k! \mid \frac{n!}{(n-k)!}$ since $\binom{n}{k}$ is an integer.

$$F^{(k)}(X, Y) \equiv \frac{1}{k!} \frac{d^k}{dx^k} F(X, Y) = \frac{1}{k!} \left(\frac{d^k}{dx^k} P(X) + \frac{d^k}{dx^k} Q(X) Y \right)$$

If F has integer coefficients, so does $F^{(k)}$.

$$(X-\beta)^n \mid F(X, Y) \text{ iff } F^{(k)}(\beta, \beta) = 0 \quad 0 \leq k \leq n.$$

Write

$$P(X) = \sum_{i=0}^{m+n} u_i X^i \quad Q(X) = \sum_{i=0}^{m+n} v_i X^i$$

$$F^{(k)}(\beta, \beta) = \sum_{i=k}^{m+n} \binom{i}{k} (u_i \beta^{i-k} + v_i \beta^{i-k+1})$$

$$= \sum_{i=0}^{m+n-k} \binom{i+k}{k} \beta^i u_{i+k} + \sum_{i=0}^{m+n-k+1} \binom{i+k-1}{k} \beta^i v_{i+k-1}$$

$$\sum_{i=0}^{m+n-k+1} \left(\binom{i+k}{k} \beta^i u_{i+k} + \binom{i+k-1}{k} \beta^i v_{i+k-1} \right)$$

Note: $u_i, v_i = 0$ if $i < 0$ or $i > m+n$.

Want: $F^{(k)}(\beta, \beta) = 0$ for $0 \leq k < n$.

$$4 \cdot 2^{m+n+1} \leq 2^{m+n+3} \leq 4^{m+n}$$

(Assume $m \geq 3$)

$$\text{This gives us } \max \{ |u_i|, |v_i| \} \leq 2 \left((16b)^{m+n} \right)^{\frac{3n}{2(m+n)-3n}}$$

$$\frac{3n}{2(m+n)-3n} = \frac{3}{2 \frac{m+1}{n} - 1} \leq 9.$$

Auxiliary Polynomial Theorem

β as before, b as before. and ~~integers~~ m, n integers satisfying $m+1 \geq \frac{2n}{3} \geq m \geq 3$.

Then $\exists F(X, Y) = P(X) + Y Q(X)$
as before.

$$\max_{0 \leq i \leq m+n} \{ |u_i|, |v_i| \} \leq 2 \cdot (16b)^{9(m+n)}$$

Example on p. 164 of book $n=5, m=3$ $\beta = \sqrt[3]{2}$
 $3n=15$ equations in $2(m+n+1)=18$ unknowns. and
look at p. 164 for the matrix entries.

One of the polynomials they get is
 $-8 - 64x^3 - 20x^6 + Y(40x^2 + 32x^5 + x^8)$

$$\frac{29}{23} = 1.2608 \dots \quad \frac{635}{504} = 1.2599206 \dots$$

$$\sqrt[3]{2} \approx 1.2599210 \dots$$

$$F\left(\frac{29}{23}, \frac{635}{504}\right) \approx -0.00714$$

$\beta^3 = b$ is an integer. so $\beta^{3j+l} = b^j \beta^l$. $l=0,1,2$

$$F^k(\beta, \beta) = \sum_{l=0}^2 \left(\sum_j \binom{3j+l+k}{k} b^j u_{3j+l+k} + \binom{3j+l+k-1}{k} b^j v_{3j+l+k-1} \right) \beta^l$$

β has minimal poly. $x^3 - b$

So $a + c\beta + d\beta^2 = 0$, $a, c, d \in \mathbb{Q} \Rightarrow a=c=d=0$.

So we want

$$0 = \sum_j \left(\binom{3j+l+k}{k} b^j u_{3j+l+k} + \binom{3j+l+k-1}{k} b^j v_{3j+l+k-1} \right)$$

for every $l \in \{0,1,2\}$ and $k \in \{0,1, \dots, n-1\}$.

We have $3n$ equations (homogeneous linear) equations in $2(n+m+1)$ unknowns. u_i, v_i with integer coefficients.

Seigel says: there is an integer solution s.t.

$$\max_{0 \leq i \leq m+n} \{|u_i|, |v_i|\} \leq 2 \left(4 \cdot 2^{(m+n+1)n} \right)^{\frac{3n}{2(n+m+1)3n}}$$

want to estimate n . $\binom{N}{M} \leq 2^N$

$$\max_{\substack{j, k, l \\ 0 \leq 3j+l \leq m+n \\ 0 \leq k < n}} \binom{3j+l+k}{k} b^j \leq \max_{\substack{0 \leq i \leq m+n \\ 0 \leq k < n}} 2^{ik} b^{i/3}$$

$$= 2^{m+2n-1} \cdot b^{m+n/3} \leq (4b)^{m+n}$$