The Proof of Thue's Theorem

Lin Feng

July 4, 2024

In this talk, our goal is to complete the proof of Thue's theorem.

Theorem 1 (Thue's theorem)**.** *Suppose that β is an algebraic number of degree $d \geq 3$, and suppose that $s > (d+2)/2$. Then there are only finitely many rational numbers p/q that satisfy the inequality*

$$\left|\beta - \frac{p}{q}\right| \leq q^{-s}.$$

1 Outline of the proof

WLOG, we assume that $(d+2)/2 < s \leq d$ in this talk (since we have Liouville's theorem).

Recall the outline of the proof:

Suppose that the algebraic number β has infinitely many good rational approximation p/q, then it has two very good rational approximations $r_1 = p_1/q_1$ and $r_2 = p_2/q_2$.

(1) Find a non-zero polynomial $P \in \mathbb{Z}[x_1, x_2]$ with controlled degree and coefficients that vanishes to high order at (β, β). (Use parameter counting.)

(2) Because r_1 and r_2 are good approximations of β, the polynomial must also vanish to high order at (r_1, r_2).

(3) The polynomial P vanishes too much at (r_1, r_2), and so its coefficients have a lower bound.

(4) Compare the lower and upper bound. Contradiction.

2 Step 1: Parameter counting

Firstly, we give the parameter counting lemma for linear map $L : \mathbb{Z}^M \to \mathbb{Z}^N$ given by a matrix with integer coefficients. Denote $|x|_\infty = \max_i |x_i|$ for $x = (x_1, \ldots, x_k) \in \mathbb{Z}^k$.

Lemma 2 (Siegel's lemma)**.** *If $L : \mathbb{Z}^M \to \mathbb{Z}^N$ is a linear map, given by a matrix with integer coefficients, with $M > N$, then there exists a nonzero $x \in \mathbb{Z}^M$ with $|x|_\infty \leq |L|_{op}^{N/(M-N)}$ such that $Lx = 0$, where*

$$|L|_{op} = \sup_{x \in \mathbb{Z}^M \setminus \{0\}} \frac{|Lx|_\infty}{|x|_\infty}$$

Remark. *If $L = (a_{ij})_{i,j}$, then*

$$|L|_{op} = \max_{1 \leq i \leq N} \sum_{j=1}^{M} |a_{ij}|.$$

If we assume further that $|a_{ij}| \leq B$, then $|L|_{op} \leq MB$.

Next we will use this parameter counting argument to find an integer polynomial $P(x_1, x_2)$ that vanishes at (β, β) to high order, with a bound on the degree of P and the size of the coefficients of P. We write $|P|$ for the maximum of the absolute value of the coefficients of P.

Proposition 3. *Let $\beta \in \mathbb{R}$ be an algebraic number of degree d. Suppose $\varepsilon > 0$. For any sufficiently large integer m, there is a polynomial $P \in \mathbb{Z}[x_1, x_2]$ with the form $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$ such that*

- $\partial_1^j P(\beta, \beta) = 0$ *for* $0 \le j \le m-1$.
- $\deg P \le (1+\varepsilon)dm/2 + 2$.
- $|P| \le C(\beta)^{m/\varepsilon}$.

Remark. *The reason that we consider polynomial P with such form dates back to the original paper by Thue, where we want to extend the method used in the proof of Liouville's theorem.*

The proof of this proposition need the following lemma which gives an upper bound of the coefficients of the expansion of β^e $(e \ge d)$.

Lemma 4. *Suppose $Q(\beta) = 0$, where $Q \in \mathbb{Z}[x]$ with degree d and leading coefficient q_d. Then for any $e \ge d$, we can write*

$$q_d^e \beta^e = \sum_{k=0}^{d-1} c_{ke} \beta^k,$$

where $c_{ke} \in \mathbb{Z}$ and $|c_{ke}| \le (2|Q|)^e$.

3 Step 2: Taylor approximation

Recall Taylor's theorem.

Theorem 5 (Taylor's theorem)**.** *If f is a smooth function on an interval, then $f(x+h)$ can be approximated by its Taylor expansion around x:*

$$f(x+h) = \sum_{j=0}^{m-1} \frac{1}{j!} \partial^j f(x) h^j + E,$$

where the error term E is bounded by

$$|E| \le \frac{1}{m!} \sup_{y \in [x, x+h]} |\partial^m f(y)| \, h^m.$$

Corollary 6. *If Q is a polynomial of one variable, and Q vanishes at x to order $m \ge 1$, and if $|h| \le 1$, then*

$$|Q(x+h)| \le C(x)^{\deg Q} |Q| \, h^m.$$

Next, we can choose suitable ε to make P in Proposition 3 vanishes at (r_1, r_2) to high order.

Proposition 7. *Suppose that β is an algebraic number of degree $d \ge 3$. Suppose that $s > (d+2)/2$. There is a small constant $c(\beta, s) > 0$ so that the following holds. Suppose that $r_1 = p_1/q_1, r_2 = p_2/q_2$ such that*

$$|\beta - r_i| \le q_i^{-s}.$$

We assume that $q_1 < q_2$, and we let m be the integer so that

$$q_1^m \le q_2 < q_1^{m+1}.$$

Given β and s, we also assume that q_1 is sufficiently large and that m is sufficiently large. Then there exists a polynomial $P \in \mathbb{Z}[x_1, x_2]$ with the form $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$ such that

- $\partial_1^j P(r_1, r_2) = 0$ *for* $0 \le j < c(\beta, s)m$.
- $\deg P \le C(\beta)m$.
- $|P| \le C(\beta)^m$.

Remark. *The assumptions for q_1, q_2, m make sense, because if there exist infinitely many rational numbers p/q such that $|\beta - p/q| \le q^{-s}$, then we can find a sequence of such q with $q_i \to \infty$.*

4 Step 3: Gauss's lemma

Recall that, in last talk, we have proved the next proposition, which could give us a lower bound of the polynomial P.

Proposition 8. *If $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1) \in \mathbb{Z}[x_1, x_2]$, and $(r_1, r_2) = (p_1/q_1, p_2/q_2) \in \mathbb{Q}^2$, and $\partial_1^j P(r_1, r_2) = 0$ for $j = 0, \ldots, l-1$, and if $l \geq 2$, then*

$$|P| \geq \min\left\{(2\deg P)^{-1} q_1^{(l-1)/2}, q_2\right\}.$$

5 Conclusion

We are ready to complete the proof of Thue's theorem.

We have to show that there are only finitely many rational solutions to the inequality

$$\left|\beta - \frac{p}{q}\right| \leq q^{-s}.$$

Suppose that there are infinitely many such rational numbers p/q. Let p_1/q_1 be one rational solution, where q_1 is large enough. Then let p_2/q_2 be another rational solution, with q_2 much larger than q_1. We define m to be the integer so that $q_1^m \leq q_2 < q_1^{m+1}$.

By Proposition 7, there is a polynomial $P \in \mathbb{Z}[x_1, x_2]$ with the form $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$ such that

- $\partial_1^j P(r_1, r_2) = 0$ for $0 \leq j \leq l-1$, where $l = c(\beta, s)m$.
- $\deg P \leq C(\beta)m$.
- $|P| \leq C(\beta)^m$.

On the other hand, Proposition 8 gives a lower bound for $|P|$:

$$|P| \geq \min\left\{(2C(\beta)m)^{-1} q_1^{(l-1)/2}, q_2\right\} \geq q_1^{\tilde{c}(\beta,s)m}.$$

Hence, we get

$$q_1^{\tilde{c}(\beta,s)m} \leq C(\beta, s)^m,$$

and so

$$q_1 \leq C(\beta, s)^{1/\tilde{c}(\beta,s)}.$$

Since q_1 could be arbitrarily large, this is a contradiction.

References

[1] L. Guth. Polynomial methods in combinatorics. Vol. 64. American Mathematical Soc., 2016.

[2] A. Thue. Über Annäherungswerte algebraischer Zahlen. Journal für die reine und angewandte Mathematik. 1909 (135): 284–305.