Thue's Theorem 1909

Om Joglekar

November 2024

1 Introduction

The Thue-Siegel-Roth theorem [6] deals with rational approximations of algebraic numbers. In simple terms, it says that algebraic numbers cannot have many 'good' approximations.
We state the theorem in its other version below:

Theorem 1. *Suppose $p(x, y) \in \mathbb{Z}[x][y]$ is a homogeneous irreducible polynomial of degree at least 3, then there can only be finitely many solutions to $p(x, y) = A$ for every $A \in \mathbb{Z}$.*

Remark. All the three conditions of p in the hypothesis are crucial as shown below.

If the degree hypothesis is relaxed, one can simply choose $p(x, y) = y^2 - 2x^2$ and $y^2 - 2x^2 = 1$ is the famous Brahmagupta–Pell's equation [5] with $n = 2$ and this has infinite solutions as can be produced algorithmically (and beautifully) by the Chakravala method of Bhaskara II [4] (12th century).
If the homogeneity is relaxed, one can choose $p(x, y) = y - x^3$ and $y - x^3 = 1$ obviously has infinite solutions.
If the irreducibility is dropped, one chooses $p(x, y) = y^2 - x^4 - 4x^2 - 4$ and again, one can see infinitely many solutions with $\alpha = 0$

We now state Thue's original theorem statement. It should henceforth be noted that all rationals of the form $\frac{p}{q}$ will be considered only in their simplest form, that is, $p \in \mathbb{Z}, q \in \{1, 2, 3, ...\}$ and $\gcd(p, q) = 1$

Theorem 2. *Suppose $\beta \in \mathbb{R} \setminus \mathbb{Q}$ is an algebraic number of degree d, then there are at most finitely many rationals $\frac{p}{q} \in \mathbb{Q}$ in lowest form such that, for all $s > \frac{d+2}{2}$,*

$$\left|\beta - \frac{p}{q}\right| \leq \frac{1}{|q|^s}$$

2 Liouville's and Dirichlet's theorems

Theorem 3. [Liouville's Theorem] *Given β, an irrational algebraic number of degree d, $\exists C > 0$ (depending on β) such that for every $\frac{p}{q} \in \mathbb{Q}$, we have*

$$\left|\beta - \frac{p}{q}\right| \geq \frac{C}{|q|^d}$$

.

Theorem 4. [Dirichlet's Theorem] *Given $\beta \in \mathbb{Q}$, there are infinitely many rationals $\frac{p}{q} \in \mathbb{Q}$ such that*

$$\left|\beta - \frac{p}{q}\right| \leq \frac{1}{|q|^2}$$

.

In the first glance, one might feel that the statements contradict each other for irrational algebraic numbers but this is not the case given that we are able to choose our constant C and that the the degree d of our β might be very large. For $d = 2$, Dirichlet's theorem gives us an error of $|q|^{-2}$ where as Liouville's theorem tells us that

we can't get closer to β than $C|q|^{-2}$. One can now see that the C we choose is going to be smaller than 1. It must be noted that Dirichlet's theorem guarantees it for only some infinite sub-collection of the rationals.
We now prove theorems 3 and 4.

Proof. [proof of theorem 3]
Let $P(x) \in \mathbb{Z}[x]$ be the minimal polynomial of degree d that β satisfies. We then have that $P(\beta) = 0$ and $P'(\beta) \neq 0$.
By continuity of polynomials, pick $\delta > 0$ such that $|P'(\beta)| > 0$ on $I = [\beta - \delta, \beta + \delta]$
Choose $C = \sup_{x \in I} P'(x) = \max_{x \in I} P'(x)$.
By the mean value theorem, we have $\dfrac{P(x) - P(\beta)}{x - \beta} = P'(\xi)$ for some $\xi \in (x, \beta) or (\beta, x)$.
Thus, $P(x) = P'(\xi)(x - \beta)$ since $P(\beta) = 0$.
Hence,

$$\left| P\left(\frac{p}{q}\right) \right| = |P'(\xi)| \left| \frac{p}{q} - \beta \right| \leq C \left| \frac{p}{q} - \beta \right|$$

Now suppose $P(x) = a_0 + a_1 x + ... + a_d x^d$,then

$$\left| P\left(\frac{p}{q}\right) \right| = \frac{\left| a_0 q^d + a_1 q^{d-1} p + ... + a_d p^d \right|}{|q|^d} \geq \frac{1}{|q|^d}$$

and we are done.
To see why the last inequality holds, it suffices to prove that the polynomial P does not vanish at $\frac{p}{q}$. This follows because if $\frac{p}{q}$ were to be a root, then the polynomial wouldnt be minimal for β. □

Proof. [proof of theorem 4]
Consider for each positive integer n, the partition of $[0, 1]$ given by
$\left\{0, \frac{1}{n}, \frac{2}{n}, ..., \frac{n-1}{n}, 1\right\}$. Now consider the $n + 1$ numbers $\{\beta\}, \{2\beta\}, \{3\beta\}, ..., \{(n+1)\beta\}$
where $\{x\} = x - \lfloor x \rfloor$ denotes the integer part function.
By noting that none of these $n + 1$ values could possibly fall on the boundary of intervals and using the pigeonhole principle, we obtain i and j so that
$i\beta, j\beta \in \left(\frac{k}{n}, \frac{k+1}{n}\right)$. Without loss of generality suppose that $i > j$
Now, $|\{i\beta\} - \{j\beta\}| < 1/n$ i.e. $|(i - j)\beta - (\lfloor i\beta \rfloor - \lfloor j\beta \rfloor)| < 1/n$.
Denoting by $(\lfloor i\beta \rfloor - \lfloor j\beta \rfloor)$ by p, we can say that

$$\left| \beta - \frac{p}{i - j} \right| < \frac{1}{n(i - j)} \leq \frac{1}{(j - i)^2}$$

which is what we wanted. □

3 Proof of Thue's theorem - Theorem 1

We now provide a proof of Theorem 1 using Theorem 2. Theorem 2 shall be proved in the next section independently.

Proof. Let $P(x, y) = a_d y^d + a_{d-1} y^{d-1} x + ... + a_0 x^d$. For a fixed $A \in \mathbb{Z}$ we consider $P(x, y) = A$. Dividing throughout by x^d and letting $Q(z) = a_d z^d + ... + a_0$, we have $Q\left(\frac{y}{x}\right) = \frac{A}{x^d}$.
One can observe easily that reducibility of Q implies that of P and hence Q is irreducible.
Suppose, if possible, for the sake of contradiction, P has infinitely many solutions, then so does Q and if (m, n) denotes a solution of P, one can choose m, n arbitrarily large. This is so because if m and n are both bounded, we only have finitely many solutions and without loss of generality if n is bounded, then each $P(x, n) = A$ has at most d many solutions again leading to finiteness when multiplied by bound on n.
Clearly the limit $\lim_{m,n \to \infty} \frac{n}{m}$ approaches a root of Q since
$x^d Q(y/x) - A = P(x, y) - A$.

Let $\{\beta_i\}_{i=1}^{d}$ be the roots of Q. By irreducibility of Q, $Q(\beta_i) \neq 0$ and hence by continuity of Q' and using MVT, one obtains a $\delta > 0$ so that the following holds on $[\beta_i - \delta, \beta_i + \delta]$

$$\frac{|Q'(\beta_i)|}{2} |x - \beta_i| \leq |Q(x) - Q(\beta_i)|$$

Choose m, n large enough so that $\frac{n}{m}$ falls in the δ-interval. Since $\left|Q\left(\frac{n}{m}\right)\right| = \frac{|A|}{|m|^d}$.

Thus, $\frac{|Q'(\beta_i)|}{2} \left|\frac{n}{m} - \beta_i\right| \leq \frac{|A|}{|m|^d}$.

By theorem 2 ,there are only finitely many rationals so that $\left|\beta - \frac{n}{m}\right| \leq \frac{1}{|m|^s}$ for every $s > \frac{d+2}{2}$. Thus choosing m sufficiently large, one can obtain m, n such that $\left|\beta - \frac{n}{m}\right| > \frac{1}{|m|^s}$. But as we have just seen, $\frac{|Q'(\beta_i)|}{2} \left|\frac{n}{m} - \beta_i\right| \leq \frac{|A|}{|m|^d}$.

Thus, absorbing the derivative into a constant, say $\tilde{A}$, and picking s such that $\frac{d+2}{2} < s < d$ (such an s exists because $d > 3$), we get $|m|^d < |\tilde{A}||m|^s$. This equation clearly has finitely many solutions for q.

Once there are only finitely many values possible for m it is clear that n must also have only finitely many values. This leads to a contradiction since we had infinitely many solutions (m, n) to $P(x, y)$. □

4 Proof of Thue's theorem - Theorem 2

In this section, we prove the Theorem 2 stated initially. This is the original statement of Thue's theorem.

It is important to note beforehand - owing to Liouville's theorem, it suffices to prove this statement for all s satisfying $\frac{d+2}{2} < s < d$.

We need additional machinery for this proof which is outlined below.

Lemma 1. [Siegel's Lemma] *If $L \in \mathbb{M}_{n\times m}(\mathbb{Z})$ then $\exists\, \vec{x} \in \mathbb{Z}^m \setminus 0$ satisfying (i) $L(\vec{x}) = 0$ and (ii) $\|\vec{x}\|_\infty \leq |L|_{op}^{n/(m-n)}$*

Remark. *Note that we use the following definition of the operator norm.*

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

It is also to be noted that if $L = (\ell_{ij})$, then $|L|_{0p} = \max_{1\leq i\leq N} S_i$ where S_i denotes sum of absolute values of entries of the i-th column.

Proof. We begin by restricting $\vec{x}$ to the cube in $\mathbb{Z}^m$ given by $[-s, s]^m$ where $2s = |L|_{op}^{n/(m-n)}$.

By definition, $\|L(\vec{x})\|_\infty \leq \|L\|_{op} \|\vec{x}\|_\infty \leq s \|L\|_{op}$.

The above inequality says that a set of $(2s+1)^m$ number of vectors we had in our cube, get mapped into a set having at most $(2s\|L\|_{op} + 1)^n$.

Now, supposing that the latter number is smaller than the former, then by the pigeonhole principle, we obtain two vectors which map to the same vector and hence the required $\vec{x}$ is just the difference if the vectors.

The claim is true because of the following calculations.

$$2s + 1 \geq 2s = |L|_{op}^{n/(m-n)} \implies (2s+1)^m \geq (|L|_{op}(2s+1))^n \geq (2s|L|_{op} + 1))^n$$

The last inequality follows because the $(|L|_{op}(2s+1))^n$ is an integer which is non-negative. Although, if it is zero, one can conclude the lemma trivially.

Also, condition (ii) is satisfied because the norm of the difference of two vectors with $\|\cdot\|_\infty \leq s$ is at most $2s = |L|_{op}^{n/(m-n)}$. This is what we wanted when we said that the number of vectors in range is smaller than number of vectors in the domain (we are talking about vectors in $\mathbb{Z}^n$). □

Lemma 2. *Let β be algebraic of degree d. Suppose $Q(x) = q_n x^n + ... + q_0 \in \mathbb{Z}[x]$ has a root as β. Then for any $m \geq n$, we can write $q_n^m \beta^m = \sum_{i=0}^{n-1} c_{i,m}\beta^i$ where $c_{k,m} \in \mathbb{Z}$ and $|c_{i,m}| \leq (2|Q|)^m$ where $|Q|$ denotes maximum value among absolute values of coefficients of Q*

Proof. The proof proceeds by induction on m. Since $Q(\beta) = 0$, we may write $q_n\beta^n = \sum_{i=0}^{n-1}(-q_i)\beta^i$ and clearly, our requirement holds for the base case $m = n$.

Now suppose that the statement holds for some $m \geq n$. We have $q_n^m\beta^m = \sum_{i=0}^{n-1} c_{i,m}\beta^i$.

Multiplying by $q_n\beta$, we get

$$q_n^{m+1}\beta^{m+1} = \sum_{i=0}^{n-1} c_{i,m}q_n\beta^{i+1} = \sum_{i=0}^{n-2} c_{i,m}q_n\beta^{i+1} + c_{n-1,m}q_n\beta^n = \sum_{i=1}^{n-1} c_{i-1,m}q_n\beta^i + \sum_{i=0}^{n-1} c_{n-1,m}(-q_i)\beta^i.$$

Thus, $q_n^{m+1}\beta^{m+1} = -c_{n-1,m}q_0 + \sum_{i=1}^{n-1}[c_{i-1,m}q_n - c_{n-1,m}q_i]\beta^i$.
We have that $|-c_{n-1,m}q_0| \leq (2|Q|)^m|Q| \leq (2|Q|)^{m+1}$ and
$|c_{i-1,m}q_n - c_{n-1,m}q_i| \leq |q_n||c_{i-1,m}| + |q_i||c_{n-1,m} \leq |Q|(2|Q|)^m + |Q|(2|Q|)^m = (2|Q|)^{m+1}$
and hence the statement holds by induction. □

Lemma 3. *Let β be an algebraic number of degree d. Suppose $\varepsilon > 0$. For any sufficiently large integer m, there is a polynomial $P \in \mathbb{Z}[x, y]$ of the form $P(x, y) = P_1(x)y + P_0(x)$ such that*
(i) $\frac{\partial^j P}{\partial x^j}(\beta, \beta) = 0$ *for* $0 \leq j \leq m - 1$
(ii) $\deg P \leq (1 + \varepsilon)dm/2 + 2$
(iii) $|P| \leq C^{m/\varepsilon}$ *(C is some constant depending only on β)*

Proof. Let D be a degree to be decided later. Write $P_0(x) = \sum_{i=0}^{D} a_i x^i$ and $P_1(x) = \sum_{i=0}^{D} b_i x^i$.
Letting $P(x, y) = P_0(x) + P_1(x)y$, we have a system of m equations in $2D + 2$ variables

$$0 = \frac{\partial^j P}{\partial x^j}(\beta, \beta) = \sum_{i=0}^{D} a_i \frac{i!}{(i-j)!}\beta^{i-j} + \sum_{i=0}^{D} b_i \frac{i!}{(i-j)!}\beta^{i-j+1} \qquad (\star)$$

Since β is algebraic, it satisfies a minimal polynomial $Q(\beta) = 0 = \sum_{i=0}^{d} q_i\beta^i$. Thus, $\{1, \beta, \beta^2, ..., \beta^{d-1}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}[\beta]$ and hence we can write for any $e \geq d$, $\beta^e = \sum_{i=0}^{d-1} C_{i,e}\beta^i$ where the coefficients are in $\mathbb{Q}$.
We now have $0 = \sum_{k=0}^{d-1} \beta^k \left[\sum_{i=0}^{D-1} b_i B_{ijk} + \sum_{i=0}^{D-1} a_i A_{ijk}\right] = 0$ where the constants A_{ijk} and $B_{i,j,k}$ are rationals. Using the linear independency of the β's, we have d new equations for each $0 \leq j \leq m - 1$.
We thus have dm linear equations in $2D + 2$ variables with integer coefficients (after clearing out denominators).
We choose D so that $\frac{dm-2}{2} < D \leq \frac{dm+2}{2}$ so that by the first inequality, we can apply Siegel's lemma to find a particular integer solution and this will recover our polynomial P. By construction, P satisfies the first two conditions described in the lemma.
Dividing equation $(\star)$ throughout by $j!$, we get

$$0 = \frac{1}{j!}\frac{\partial^j P}{\partial x^j}(\beta, \beta) = \sum_{i=0}^{D} a_i \binom{i}{j}\beta^{i-j} + \sum_{i=0}^{D} b_i \binom{i}{j}\beta^{i-j+1}$$

We now observe two things - by choice of D, $D < dm$ (m is large). Also, $\binom{i}{j} \leq 2^i \leq 2^D$.
Coming back to our equation with A_{ijk} and B_{ijk}, by using lemma 2, the bound on these integers coefficients is $|Q|^D 2^D (2|Q|)^D \leq C^D \leq C^d m \leq C^m$ (The $|Q|^D$ term comes from q_i^D, the next one comes from the binomial coefficients and the last one comes from lemma 2) where the the constant C depends only on β (note that we have abused notation for the last inequality).
Finishing up with Siegel's lemma, P is chosen so that $|P| \leq (C^m)^{\frac{N}{M-N}}$ where $M = 2D + 2$ and $N = md$. Since m can be taken large enough, we choose a D so that $D \leq \frac{dm+2}{2} + \frac{dm\varepsilon}{2}$. This gives the desired bound on P and we are done. □

We quickly recall Taylor's theorem whose proof can be found easily. One such reference is Mathematical Analysis by Apostol[1]

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

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

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

$$|Q(x+h)| \leq C(x)^{\deg Q} |Q| h^m$$

Proof. Essentially, by Taylor's theorem, we have to estimate the size of the coefficients of $\frac{1}{m!} \frac{d^m}{dx^m} Q$. Now $\frac{1}{m!} \frac{d^m}{dx^m} x^i = \binom{i}{m} x^{i-m}$ and so the coefficients have norm at most $2^{\deg Q} |Q|$. Therefore, we get

$$\sup_{|y-x| \leq 1} \frac{1}{m!} \left| \frac{d^m}{dx^m} Q(y) \right| \leq 2^{\deg Q} |Q| (\deg Q)(|x|+1)^{\deg Q} \leq C(x)^{\deg Q} |Q|.$$

Plugging this estimate into Taylor's theorem finishes the proof. □

Lemma 4. *Suppose that β is an algebraic number of degree $d \geq 3$. Suppose that $s > (d+2)/2$. There is a small constant $c > 0$ depending only on β and s, so that the following holds. Suppose that $r_1 = p_1/q_1, r_2 = p_2/q_2$ such that $|\beta - r_i| \leq q_i^{-s}$. We assume that $q_1 < q_2$, and we let m be the integer so that $q_1^m \leq q_2 < q_1^{m+1}$ Given β and s, we also assume that q_1 is sufficiently large and that m is sufficiently large. Then there exists a polynomial $P \in \mathbb{Z}[x, y]$ with the form $P(x, y) = P_1(x) y + P_0(x)$ such that*
(i) $\frac{\partial^j P}{\partial x^j}(r_1, r_2) = 0$ *for* $0 \leq j < cm$
(ii) $\deg P \leq Km$
(iii) $|P| \leq K^m$
(K is some constant depending only on β)

Proof. Let us obtain P using Lemma 3 with the choice of $\varepsilon = \frac{1}{10d}\left(s - \frac{d+2}{2}\right)$. Then the second and third conclusions follow through readily. We now only need to check the first point of the conclusion.
Consider $\tilde{P}(x, y) = \frac{1}{j!} \frac{\partial^j P}{\partial x^j}(r_1, r_2)$ and observe that this new polynomial also has integer coefficients and that $\deg(\tilde{P}) \leq \deg(P)$. Further, $|\tilde{P}| \leq q^{\deg(P)} |P| \leq (K(\beta, s))^m$ (K is some constant depending on those two parameters).
Let $Q(x) = \tilde{P}(x, \beta)$. Then, Q vanishes at β to order $(1-c)m$ and coefficients of Q satisfy $|Q| \leq K^m$.

From the corollary above it follows that $\left|\tilde{P}(r_1,\beta)\right| \leq K^m \left|\beta - r_1\right|^{(1-c)m}$.
Using the MVT, we have $\left|\tilde{P}(r_1,r_2) - \tilde{P}(r_1,\beta)\right| \leq K^m \left|\beta - r_2\right|$
Combining the above two lines, we have $\left|\tilde{P}(r_1,r_2)\right| \leq K^m \left[\left|\beta - r_1\right|^{(1-c)m} + \left|\beta - r_2\right|\right]$
Using the fact that $|\beta - r_i| \leq |q_i|^{-s}$, we have $\left|\tilde{P}(r_1,r_2)\right| \leq K^m \left[\left|q_1\right|^{(-s)(1-c)m} + \left|q_2\right|^{-s}\right]$
Using the hypothesis, we have $q_1^m \leq q_2$ and hence the second term is dominated by the first one and hence we have the bound $K^m q_1^{-(1-c)sm}$ (q_i is positive anyways).
On the other hand, $\tilde{P}$ has integer coefficients and hence when we substitute (r_1, r_2), we get a maximum denominator of $q_1^{\deg_x(P)} q_2$. But from the way P was obtained using lemma 2, $\deg(P) \leq (1+\varepsilon)(1/2)dm$. Also, $q_2 \leq q_1^{m+1}$.
Hence, we conclude that the denominator of $\tilde{P}(r_1, r_2)$ is at most $q_1^{(1+\varepsilon)(d/2)m+m+1}$.
Thus, if we show that $(1-c)sm > (1+\varepsilon)(d/2)m + m + 1$, we shall be done because we would have shown that $|\tilde{P}(r_1, r_2)|$ is "small" (since q_1 can be taken arbitrarily large. But this holds by choice of ε, choosing m large, and choosing c significantly smaller than ε. □

Lemma 5. [Gauss Lemma] *If $r = p/q \in \mathbb{Q}$ is a zero of $P \in \mathbb{Z}[x]$ of order ℓ, then $P(x) = (qx-p)^\ell P_1(x)$ for some $P_1(x) \in \mathbb{Z}[x]$*

Remark. *This is just a slightly generalised version of the usual Gauss Lemma for UFD's*

Proof. We can safely say $P(x) = (qx-p)^\ell P_2(x)$ for some $P_2(x) \in \mathbb{Q}[x]$. We write $MP(x) = (qx-p)^\ell \tilde{P}_2(x)$ as an equation in $\mathbb{Z}[x]$ after clearing out the denominator. We readily get a contradiction when we consider this equation modulo p_1 where p_1 is some prime dividing M since p_1 cannot possibly divide any of the coefficients of the the right hand side. □

Lemma 6. [Generalised Gauss Lemma] *If $P(x,y) = P_1(x)y + P_0(x) \in \mathbb{Z}[x,y]$ and $(r_1, r_2) = (p_1/q_1, p_2/q_2) \in \mathbb{Q}^2$ is such that $\dfrac{\partial^j P}{\partial x^j}(r_1, r_2) = 0$ for $0 \leq j < l$ for some $l > 2$, then $|P| \geq \min\left(q_2, \dfrac{q_1^{\frac{l-1}{2}}}{2\deg(P)}\right)$*

Proof. We begin with the hypothesis of the lemma which states that
$r_2 \dfrac{\partial^j P_1}{\partial x^j}(r_1) + \dfrac{\partial^j P_0}{\partial x^j}(r_1) = 0, 0 \leq j \leq l-1$.
Let $V(x)$ denote the vector $(P_1(x), P_0(x))$. In terms of this vector, the above line reads - All the j^{th} order derivatives lie on the line given by $V(x) \cdot (r_2, 1) = 0$.
In particular, any two of them are linearly dependent. In terms of determinants, $\det\left[\partial^{j_1} V, \partial^{j_2} V\right] = 0$ for any $0 \leq j_1, j_2 < l$.
Using the property $\partial \det[V, W] = \det[\partial V, W] + \det[V, \partial W]$ of derivatives of determinants, we have that $\partial^j \det[V, \partial V](r_1) = 0$ for any $0 \leq j < l$ If the polynomial $\det[V, \partial V] \in \mathbb{Z}[x]$ is non zero, using lemma 5, taking the size of coefficients, we get $|\det[V, \partial V]| \geq q_1^{l-1}$
On the other hand, expanding out the determinant, we get
$|\det[V, \partial V]| = |P_1 \partial P_0 - \partial P_1 P_0| \leq 2(\deg(P))^2 |P|^2$.
Thus, $|P| \geq (2\deg(P))^{-1} q_1^{\frac{l-1}{2}}$. However, if the polynomial $|\det[V, \partial V]|$ is identically 0, then P_1 may be identically zero in which case $P(x,y) = P_0(x)$ and by lemma 5 $|P| > q_1^l$.
If on the other hand, P_1 is not identically 0, then the derivative if P_0/P_1 must be identically 0 as the numerator of this derivative gives us $|\det[V, \partial V]|$.
Thus, $P(x,y) = (y + A) P_1(x)$ for some constant A. Then either $r_2 + A = 0$ or $\frac{\partial^j P_1}{\partial x^j}(r_1) = 0$ for all $0 \leq j < l$.
Again in the second case by lemma 5, $|P_1| \geq q_1^l$. In the first case $A = -r_2 = -p_2/q_2$.
Thus, $P(x,y) = (q_2 x_2 - p_2)\tilde{P}_1(x)$ where $P_1 \in \mathbb{Q}[x]$. But by same argument as in lemma 5 $\tilde{P}_1$ actually has integer coefficients and we get $|P| \geq q_2$. □

We are finally equipped with everything we need to prove theorem 2

Proof. [proof of theorem 2]
Suppose for the sake of contradiction there were infinitely many rationals satisfying the inequality $\left|\beta - \frac{p}{q}\right| \leq |q|^{-s}$ for some fixed $s > (d+2)/2$.
Choose $r_1 = p_1/q_1$ and $r_2 = p_2/q_2$ with $q_2 > q_1 >> 0$. Let m be an integer so that $q_1^m \leq q_2 \leq q_1^{m+1}$. Using lemma 4, obtain the polynomial P satisfying the conclusions of lemma 4. The generalised Gauss lemma gives $|P| \geq \min(m^{-1}q_1^{\frac{l-1}{2}}, q_2) \geq m^{-1}q_1^{cm}$. Comparing the bounds coming from Gauss lemma and point (iii) of lemma 4, we get $m^{-1}q_1^{cm} \leq K^m$ which implies that $q_1 \leq K$ which is a contradiction since q_1 can be considered very large. □

References

[1] Tom Apostol. *Mathematical Analysis*. 2nd. Theorem 12.14: Taylor's Theorem. Reading, Massachusetts: Addison-Wesley, 1974. Chap. 12, pp. 361–362.

[2] Larry Guth. *Polynomial Method in Combinatorics*. American Mathematical Society, 2016, pp. 265–278.

[3] A. Thue. "Über Annäherungswerte algebraischer Zahlen". In: *Journal für die reine und angewandte Mathematik* 135 (1909), pp. 284–305.

[4] Wikipedia. *Chakravala method*. Accessed: 2024-11-15.

[5] Wikipedia. *Pell's equation*. Accessed: 2024-11-15.

[6] Wikipedia. *Thue-Siegel-Roth theorem*. Accessed: 2024-11-15.