Integer Points on Cubic Curves

Irina Sofronova, Lorenzo Zegg

07.11.2023

Contents

1 How Many Integer Points?

Let

$$C : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

be a non-singular cubic curve with integer coefficients. As the title of the talk suggests, we will try to find which rational points on C have integer coordinates. Let us first recall a few results from the previous talks:

Theorem (Nagell-Lutz Theorem)**.** *Let $y^2 = f(x) = x^3 + ax^2 + bx + c$ be a non-singular cubic curve with integer coefficients a, b, c, let D be the discriminant of the cubic polynomial and $P = (x, y)$ be a rational point of finite order. Then x and y are integers, and either $y = 0$, in which case P has order two, or y divides D.*

Theorem (Mordell's Theorem)**.** *If a non-singular rational plane cubic curve has a rational point, then the group of rational points is finitely generated.*

The Nagell-Lutz Theorem gives us an answer to our question in the case of curves given by a Weierstrass equation and points of finite order. But is the converse also true? Are the integer points on such curves always of finite order? We can easily find examples where this is not true. For example, the curve $y^2 = x^3 + 3$ has no points of finite order but it has an integer point $(x, y) = (1, 2)$.

Can we expect to have infinitely many integer points on a non-singular cubic curve? By Mordell's Theorem, if we have $rank(C) = 0$, then $C(\mathbb{Q})$ is finite and by Nagell-Lutz Theorem the finitely many rational points are integers.

If $rank(C) > 0$, e.g. $rank(C) = 1$, then there are no non-trivial points of finite order and there is a generator P of $C(\mathbb{Q})$ such that every point has the form $nP = (x_n, y_n)$ for some $n \in \mathbb{Z}$. Now we can consider the points $P, 2P, 3P, ...$ It holds that $nP = (n-1)P + P$, therefore using the explicit formulas for the group law (Section 1.4 in [1]) we get for $n \geq 3$

$$x_n = \lambda^2 - a - x_1 - x_{n-1},$$

where $\lambda = \frac{y_{n-1} - y_1}{x_{n-1} - x_1}$. This means, even if P and $(n-1)P$ have integer coordinates, it is highly unlikely that nP will also have integer coordinates. Indeed,

Theorem (Siegel's Theorem)**.** *Let C be a non-singular cubic curve given by an equation $F(x, y) = 0$ with integer coefficients. Then C has only finitely many points with integer coordinates.*

Remark. C consists of the points (x, y) such that $F(x, y) = 0$, as well as one or more points at infinity. Therefore, for Siegel's Theorem we need the curve C to be non-singular at every point, including the ones at infinity.

Let us now compare Siegel's Theorem to the cases of linear, quadratic and singular cubic equations:

- If (x_0, y_0) is an integer solution to the linear equation $ax + b = c$ with $a, b, c \in \mathbb{Z}$, then there are infinitely many solutions $(x_n, y_n) = (x_0 + bn, y_0 - an)$ for $n \in \mathbb{Z}$.

- We know that Pell's equation $x^2 - Dy^2 = 1$ has infinitely many integer solutions for every D a positive square-free integer.
- The singular cubic curve $C_1 : y^2 = x^3 - x^2$ has infinitely many integer points: $(t^2 + 1, t^3 + t)$ for all $t \in \mathbb{Z}$.
- The singular cubic curve $C_2 : y^2 = x^3$ also has infinitely many integer points: (t^2, t^3) for all $t \in \mathbb{Z}$. In particular, the non-singularity condition in Siegel's Theorem is essential.

Proving Siegel's Theorem in the general case is quite complicated. However, in the next sections we will consider some special cases of this theorem in which the proofs are manageable.

2 Taxicab Numbers

In this section we will discuss the so-called *taxicab numbers*. Their name comes from the following anecdote of G.H. Hardy visiting Ramanujan in the hospital: *"I remember once going to see him [Ramanujan] when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."*

Indeed, we have $1729 = 9^3+10^3 = 1^3+12^3$ and the cubic curve $x^3+y^3 = 1729$ has four integer points: $(9, 10), (10, 9), (1, 12), (12, 1)$. We will now prove this as a special case of Siegel's Theorem.

Claim. The cubic curve $x^3 + y^3 = 1729$ has only finitely many points with integer coordinates.

Proof. We will use the polynomial factorization of $x^3 + y^3$ as

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2).$$

Then for $x, y \in \mathbb{Z}$

$$(x + y)(x^2 - xy + y^2) = 1729 = 7 \cdot 13 \cdot 19$$

and we have to look at all possible factorizations of $1729 = A \cdot B$.

$$x + y = A, x^2 - xy + y^2 = B \Rightarrow B = (x + y)^2 - 3xy = A^2 - 3xy$$

Then

$$x + y = A, xy = \frac{A^2 - B}{3}$$

and x, y are the solutions of the quadratic equation $t^2 - At + \frac{A^2-B}{3} = 0$. Using the quadratic formula we have

$$t_{1,2} = \frac{3A \pm \sqrt{12B - 3A^2}}{6}$$

and for each A, B checking if $t_{1,2} \in \mathbb{Z}$ gives the pairs $(A, B) = (13, 133), (19, 91)$. Then we get the four solutions $(9, 10), (10, 9), (1, 12), (12, 1)$. □

We can also prove that cubic equations of the type

$$(ax + by + c)(dx^2 + exy + fy^2 + gx + hy + i) = j \text{ with } j \neq 0$$

have finitely many integer solutions (again using the factorization method).

Let's go back to the taxicab equations

$$x^3 + y^3 = m \qquad (*)$$

(with finitely many integer solutions) and try to answer some questions about them.

- **Can we bound how large the integer solutions are?**
  Yes. We have the following

Proposition. *Let $m \geq 1$ be an integer. Then every solution to the equation $x^3 + y^3 = m$ in integers x, y satisfies*

$$max\{|x|, |y|\} \leq 2\sqrt{\frac{m}{3}}.$$

Proof. Again we can use the factorization $x^3+y^3 = (x+y)(x^2-xy+y^2) = A \cdot B = m$. Then

$$m \geq |B| = |x^2 - xy + y^2| = \frac{3}{4}x^2 + (\frac{1}{2}x - y)^2 \geq \frac{3}{4}x^2$$

$\Rightarrow |x| \leq 2\sqrt{\frac{m}{3}}$. Similarly, $|y| \leq 2\sqrt{\frac{m}{3}}$. □

- **How many integer solutions are there?**
  We consider two solutions (x, y) and (y, x) as the same. Ramanujan observed that $m = 1729$ is the smallest positive integer such that $(*)$ has two solutions. But is there an integer m for which we have three solutions? Or four? The following proposition answers this question

  Proposition. *For any integer $N \geq 1$ we can find an $m \in \mathbb{N}$ such that the equation $(*)$ has at least N points with integer coordinates.*

  We omit the proof here, it can be found in [1], Section 5.2.

- **What is the smallest m such that $(*)$ has N integer solutions?**
  Let us define the N-th Taxicab Number $Taxi(N)$ as

  $Taxi(N) = min\{m \geq 1 : x^3+y^3 = m$ has at least N integer solutions with $x \geq y > 0\}$.

  We have

  $$\begin{aligned} Taxi(1) &= 2 \\ Taxi(2) &= 1729 \\ Taxi(3) &= 87539319 \\ Taxi(4) &= 6963472309248 \\ Taxi(5) &= 48988659276962496 \\ Taxi(6) &= 24153319581254312065344 \end{aligned}$$

  However, for $N \geq 7$ the taxicab numbers are still not known.

- **Given an integer N, is it possible to find an integer $m \geq 1$ so that the equation $x^3 + y^3 = m$ has at least N integer solutions with $x \geq y > 0$ and $gcd(x, y) = 1$?**
  These are the so-called cubefree taxicab numbers. Only the first four of them are known so far:

  - for $N = 1$ or 2 we have that $Taxi(1) = 2$ and $Taxi(2)$ are cubefree.
  - for $N = 3$ Paul Vojta found the following example in 1981:

    $$15170835645 = 2468^3 + 517^3 = 2456^3 + 709^3 = 2152^3 + 1733^3.$$

– for $N = 4$ Stuart Gascoigne and Duncan Moore discovered in 2003 independently that 1801049058342701083 is the 4-th cubefree taxicab number.
– for $N \geq 5$ finding the cubefree taxicab numbers is an open problem. Some mathematicians believe that there aren't any such numbers.

3 Thue's Theorem and Diophantine Approximation

Let us now consider a polynomial that does not factor, e.g.

$$x^3 + 2y^3 = m. \tag{$\star$}$$

The fact that $x^3 + y^3 = m$ has infinitely many integer solutions does not give us any information about the number of integer solutions of ($\star$): in the case of quadratic equations we had that $x^2 - y^2 = 1$ has finitely many solutions and $x^2 - 2y^2 = 1$ has infinitely many.

In fact, we have the following general result for cubic curves of the type $ax^3 + by^3 = c$:

Theorem (Thue)**.** *Let a, b, c be non-zero integers. Then the equation*

$$ax^3 + by^3 = c \tag{$\dagger$}$$

has only finitely many solutions in integers x, y.

Remark.
1. If $(x, y) \in \mathbb{Z}^2$ is a solution to ($\dagger$), then we have $a^3x^3+a^2by^3 = a^2c$ and (ax, y) is a solution to the equation $x^3 + a^2by^3 = a^2c$. This means it is enough to prove Thue's Theorem for $a = 1$.
2. It is enough to consider equations of the form $x^3 - by^3 = c$ with $b, c \in \mathbb{Z}, b > 0$ and $c > 0$ (otherwise we can replace y by $-y$, b by $-b$ if needed).

We will prove that the equation

$$x^3 - by^3 = c$$

with $b, c \in \mathbb{Z}_{>0}$ has only finitely many integer points.

Proof. We will use once again the factorization method. Let $\beta := \sqrt[3]{b}$ (not necessarily rational), then we have

$$x^3 - by^3 = x^3 - (\beta y)^3 = (x - \beta y)(x^2 + \beta xy + \beta^2 y^2) = c.$$

However, we cannot continue in the same way as we did in the previous section. Instead, we will try to approximate β.

- If (x, y) is a solution to $x^3-by^3 = c$ with x, y large $\Rightarrow |x-\beta y| = |y|\cdot|x/y-\beta|$ must be quite small:
  We have

  $$x^2 + \beta xy + \beta^2 y^2 = (x + \frac{1}{2}\beta y)^2 + \frac{3}{4}\beta^2 y^2 \geq \frac{3}{4}\beta^2 y^2$$

  then

  $$\begin{aligned} |c| = |x^3 - by^3| &= |x - \beta y| \cdot |x^2 + \beta xy + \beta^2 y^2| \\ \Rightarrow |c| \geq |x - \beta y| \cdot \frac{3}{4}\beta^2 y^2 &\qquad \Big| : \frac{3}{4}\beta^2|y|^3 \\ \Rightarrow \left|\frac{x}{y} - \beta\right| \leq \frac{4|c|}{3\beta^2} \cdot \frac{1}{|y|^3} &\qquad (*) \end{aligned}$$

  i.e.: if (x, y) is an integer solution of $x^3 - by^3 = c$ with $|y|$ large then the rational number $\frac{x}{y}$ is a good approximation of the irrational β.

- Then, in order to prove that there are only finitely many integer points it is enough to prove that there are only finitely many rational numbers with denominator > 0 that satisfy $(*)$. Let us first assume that this claim is true and finish the proof.
  - if $b = \beta^3$ for some $\beta \in \mathbb{Z}$ then the factorization argument from before works
  - if $y = 0$ we have $x^3 = c$ and there is at most one solution
  - if b is not a perfect cube and (x, y) is a solution with $y \neq 0$ then $(*)$ is fulfilled and by the claim there are only finitely many pairs $(x, y) \in \mathbb{Z}^2$ with $y > 0$. In the case where $y < 0$ we just use that $x/y = -x/-y$ and apply the claim again.

□

Our remaining goal is to prove the following

Theorem (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*

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

3.1 Motivation of Proof

Let us first try the factorization method once again. As before, we have

$$x^3 - by^3 = (x - \beta y)(x^2 + \beta xy + \beta^2 y^2).$$

If we suppose that the rational number p/q satisfies $|p/q - \beta| \leq C/|q|^3$, then we have using the triangle inequality and that $\beta > 0, q > 0$:

$$\left|\frac{p}{q}\right| \leq \left|\frac{p}{q} - \beta\right| + |\beta| \leq \beta + \frac{C}{q^3} \leq \beta + C. \tag{$\star_1$}$$

Our plan is to bound $|\frac{p}{q} - \beta|$ on both sides. First we can use the factorization to write

$$p^3 - bq^3 = (p - \beta q)(p^2 + \beta pq + \beta^2 q^2) \qquad \Big| : q^3$$

$$f\left(\frac{p}{q}\right) := \frac{p^3 - bq^3}{q^3} = \left(\frac{p}{q} - \beta\right) \cdot \left(\frac{p^2}{q^2} + \beta\frac{p}{q} + \beta^2\right). \tag{$\star_2$}$$

Here $f(x)$ is the polynomial $f(x) = x^3 - b$. Because $b \in \mathbb{Z}_{>0}$ is not a perfect cube, $p^3 - bq^3 \in \mathbb{Z}$ can't be zero $\Rightarrow |p^3 - bq^3| \geq 1$ and since $q > 0$ we have

$$\left|\frac{p^3 - bq^3}{q^3}\right| = \frac{|p^3 - bq^3|}{|q|^3} \geq \frac{1}{q^3}. \tag{$\star_3$}$$

On the other hand, using $(\star_1)$ and again the triangle inequality, we have

$$\left|\frac{p^2}{q^2} + \beta\frac{p}{q} + \beta^2\right| \leq \left|\frac{p}{q}\right|^2 + \beta \cdot \left|\frac{p}{q}\right| + \beta^2 \leq (\beta + C)^2 + \beta(\beta + C) + \beta^2 =: C' \tag{$\star_4$}$$

for some constant C' depending on β and C. Plugging $(\star_3)$ and $(\star_4)$ in $(\star_2)$ we get

$$\left|\frac{p}{q}-\beta\right| = \frac{\left|\frac{p^3-bq^3}{q^3}\right|}{\left|\frac{p^2}{q^2}+\beta\frac{p}{q}+\beta^2\right|} \geq \frac{\frac{1}{q^3}}{C'} = \frac{1}{C'q^3}.$$

Therefore,

$$\frac{1}{C'q^3} \leq \left|\frac{p}{q}-\beta\right| \leq \frac{C}{q^3} \Rightarrow C' \geq \frac{1}{C}.$$

This inequality doesn't really help us, because we already have that $C' = (\beta+C)^2+\beta(\beta+C)+\beta^2$ is rather large. If we were to find a stronger lower bound for $|p/q-\beta|$, say

$$\frac{1}{C'q^{2.9}} \leq \left|\frac{p}{q}-\beta\right|,$$

then we would have

$$\frac{1}{C'q^{2.9}} \leq \left|\frac{p}{q}-\beta\right| \leq \frac{C}{q^3} \Rightarrow q \leq (CC')^{10}$$

and the denominators q of the rationals $\frac{p}{q}$ will be bounded. Using $|p/q-\beta| \leq C/q^3$ it follows that the nominators p also will be bounded, which gives us the desired result that there are only finitely many rationals p/q that satisfy $|p/q-\beta| \leq C/q^3$.

So, let's see how we can improve the lower bound. In our unsuccessful first attempt we used the polynomial $f(x) = x^3 - b$. So one possible way to improve would be to use some "better" polynomial $F(x)$. Suppose we found a polynomial $F(x) \in \mathbb{Z}[x]$ such that $(x^3-b)^n | F(x)$ for some (large) $n \in \mathbb{Z}$. Then $F(x)$ has the factorization $F(x) = (x-\beta)^n G(x)$ for some $G(x) \in \mathbb{R}[x]$ and again we can show that $|F(p/q)| \leq \bar{C}|p/q-\beta|^n$ for some constant $\bar{C}$ depending only on $F(x)$ and C. If $F(p/q) \neq 0$ we get the lower bound for $|F(p/q)|$:

$$\left|F\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d},$$

where $d = deg(F)$.
(because $F(p/q) = A_d(p/q)^d +$ (some polyn. of degree $< d$) $= A_d p^d (1/q)^d +$ $(\dots)$, $A_d p^d \in \mathbb{Z}$ and again we use the triangle inequality)
Then, we have

$$\frac{1}{q^d} \leq \left|F\left(\frac{p}{q}\right)\right| \leq \bar{C}\left|\frac{p}{q}-\beta\right|^n \Rightarrow \left|\frac{p}{q}-\beta\right| \geq \frac{1}{\sqrt[n]{\bar{C}}} \cdot \frac{1}{q^{d/n}}$$

If $d < 3n$ we are done. However, $d \geq 3n$, because $(x-\beta)^n | F(x)$ and $F(x) \in \mathbb{Z}[x]$ then $F(x)$ is divisible by the n-th power of the minimal polynomial of $\beta \Rightarrow (x^3-\beta) | F(x) \Rightarrow deg(F(x)) \geq deg((x^3-b)^n) = 3n$. So we need to improve the lower bound differently.

3.2 Actual Proof

The key idea of Thue was to use a two-variable polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$. He chose a polynomial that vanishes to high order at the point (β,β) and he then compared upper and lower bounds for the value $F(p_1/p_2, p_2/q_2)$, where p_1/q_1 and p_2/q_2 are solutions to

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

Thue's proof naturally divides into three parts:

1. Find a suitable polynomial $F(X,Y)$.
2. Compute a good upper bound for $|F(p_1/p_2, p_2/q_2)|$ in terms of the quantities $|p_1/q_1 - \beta|$ and $|p_2/q_2 - \beta|$.
3. Derive a lower bound for $|F(p_1/p_2, p_2/q_2)|$, and in particular, show that this value is not zero. This is the technically hardest part of the proof.

Since the proof is rather long and somewhat technical, we decided to not go into much detail of the proof. Instead we give an outline of each step and for those who want to see the full proof, we encourage them to just read through it in the main reference [1].

3.2.1 Construction of Auxiliary Polynomial

We begin by constructing a polynomial $F(X,Y)$ with integer coefficients so that $F(X,Y)$ vanishes to very high order at the point $\beta,\beta)$. Further we will need to find an F whose coefficients are not too large. This is achieved by using *Siegel's Lemma*

Lemma (Siegel)**.** *Let $N > M$ be positive integers and let*

$$\begin{array}{ccccc} a_{11}T_1 + & \cdots & +a_{1N}T_N = & 0 \\ \vdots & \ddots & \vdots & \vdots \\ a_{M1}T_1 + & \cdots & +a_{MN}T_N = & 0 \end{array}$$

be a non-trivial system of linear equations with integer coefficients. Then there is a solution $(t_1,\ldots,t_N)$ to this system with $t_1,\ldots,t_N$ integers, not all zero, and satisfying

$$\max_{1\leq i\leq N} |t_i| < \left(4N \max_{\substack{1\leq i\leq M \\ 1\leq j\leq M}} |a_{ij}|\right)^{\frac{M}{N-M}}$$

The statement of Siegel's lemma says: *The system of homogeneous equations has more variables than equations, so we know that it has non-trivial solutions in rational numbers and clearing denominators, we can create integer solutions. So it is obvious that there are non-zero integer solutions. The last part of the lemma says that we can find a solution whose coordinates are not too large. More precisely, we can find a solution whose coordinates are bounded explicitly in terms of the number of equations M, the number of variables N, and the size of the coefficients a_{ij}.*
In fact, Siegel's lemma is the precise form of the bound we are looking for.
We can now state the goal of the first step.

Theorem (Auxiliary Polynomial)**.** *Let b be an integer, and let $\beta = \sqrt[3]{b}$, and let m, n be integers satisfying*

$$m + 1 > \frac{2}{3}n \geq m \geq 3$$

Then there is a non-zero polynomial

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

having the following properties:

$$F^{(k)}(\beta, \beta) = 0 \qquad \forall 0 \leq k < n \tag{1}$$

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

The theorem is by no means a trivial corollary of Siegel's Lemma, but one can imagine if done correctly we can apply Siegel's Lemma. (i.e. condition (1) and maximal degree $m + n$ yield a system of linear equations and Siegel then provides the bound). Further since $1, \beta, \beta^2$ are linearly independent over $\mathbb{Q}$, we get that

$$A + B\beta + C\beta^2 = 0 \qquad \Longrightarrow \qquad A = B = C = 0.$$

By expressing every power of β in (1) in terms of $1, \beta, \beta^2$ we get more constraints on our v_i, u_i and end up with $3n$ homogeneous linear equations .

Example. Suppose we take

$$n = 5, \qquad m = 3, \qquad b = 2, \qquad \beta = \sqrt[3]{2}.$$

So we are looking for a polynomial

$$F(X, Y) = \sum_{i=0}^{8} (u_i X^i + v_i X^i Y)$$

satisfying $F^{(k)}(\beta, \beta) = 0$ for all $0 \leq k < 4$. Writing this out explicitly leads to 15 homogeneous linear equations in 18 variables $\{u_0, \ldots, u_8, v_0, \ldots, v_8\}$. Solving for the first 15 variables in terms of the last 3, we can substitute small integer values for v_6, v_7, v_8 to find non-zero integer solutions. For example, $v_6 = v_7 = 0$ and $v_8 = 1$ gives the polynomial

$$F(X, Y) = -8 - 64X^3 - 20X^6 + 40X^2Y + 32X^5Y + X^8Y$$

We observe that the largest coefficient of this F has magnitude 64, while the theorem only guarantees a polynomial whose coefficients are no larger than

$$2 \cdot (16b)^{9(m+n)} = 2 \cdot 32^{72}.$$

It is obvious that the estimate in the theorem is far from optimal.
We now use F to illustrate a further point. The rational numbers

$$\frac{29}{23} \approx 1.2608 \qquad\qquad \frac{635}{504} \approx 1.2599206$$

are quite close to

$$\sqrt[3]{2} \approx 1.259921.$$

So we expect that F evaluated at these rational numbers should be quite small, and indeed we find that

$$F(\frac{29}{23}, \frac{635}{504}) \approx -0.0000714.$$

This serves to illustrate the Smallness Theorem, which would be the next step.

3.2.2 Auxiliary Polynomial is Small

The auxiliary polynomial $F(X, Y)$ that we constructed in the last section vanishes to high order at the point (β, β). So if p_1/q_1 and p_2/q_2 are close to β, then we expect $F(p_1/q_1, p_2/q_2)$ to be small. We formulate the following theorem.

Theorem (Smallness)**.** *Let $F(X, Y)$ be a polynomial as described in the Auxiliary Polynomial Theorem. Then there is a constant $c_1 > 0$, depending only on b, so that for any rational numbers x, y with $|x - \beta| \leq 1$ and for any integer $0 \leq t \leq n$ we have*

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

Where c_1 only depends on b and does not depend on n, t, F, x, y.

Again we omit the proof, since it doesn't provide any insight and again is mostly technical (Finding bounds for certain expressions to get the desired constant).

3.2.3 Auxiliary Polynomial does not vanish

So far we have obtained an auxiliary polynomial $F(X, Y)$ that vanishes to high order at the point (β, β) and for rational numbers x, y close to β we have that $F(x, y)$ is small. The last step is to show that for rational numbers x, y, $F(x, y)$ is not zero. Unfortunately, we are not able to prove such a strong result. Instead, we will show that some derivative $F^{(t)}(X, Y)$, with t not too large, does not vanish.

Theorem (Non-Vanishing)**.** *Let $F(X, Y)$ be an auxiliary polynomial as described in the Auxiliary Polynomial Theorem. Let $p_1/q_1, p_2/q_2$ be rational numbers in lowest terms. Then there is a constant c_2, depending only on b, and an integer t satisfying*

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

so that

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

By the same reasoning as in the previous section we've omitted the proof of this theorem.

3.3 Diophantine Approximation Theorem (Thue)

We have now assembled all of the tools needed to prove the *Diophantine Approximation Theorem*, which is the main goal of the talk.

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

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

Even though the above theorem is the main goal of the talk, we again omit the proof. But we mention the rough idea of the proof:

- By contradiction assume infinitely many such pairs.
- This implies that q values tend toward infinity, since otherwise both p, q bounded and therefore only finitely many pairs, since both are integers.
- Take larger solution (p_1, q_1) and even larger solution (p_2, q_2) (large in second coordinate). Where we get our bounds from the previous theorems (Smallness and Non Vanishing). Here we mention, that these bounds only depend on our fixed b.
- Then we get a bound for n in terms of q_1, q_2 and therefore by the Auxiliary Polynomial Theorem a polynomial $F(X, Y)$.
- Next we apply the Non Vanishing Theorem to get t i.e. bound for derivatives.
- Lastly computing lower and upper bounds gives the desired contradiction.

3.4 Further Developments

We have proven that an equation of the form

$$ax^3 + by^3 = c$$

has only finitely many integer solutions. The proof depends on a Diophantine Approximation Theorem which says, roughly, that it is not possible to use rational numbers p/q to very closely approximate a cube root $\sqrt[3]{b}$. Roth proved an even stronger result.

Theorem (Roth)**.** *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 $\varepsilon > 0$ and $C > 0$ be positive numbers. Then there are only finitely many pairs of integers (p, q) with $q > 0$ that satisfy the inequality*

$$\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^{2+\varepsilon}}$$

Further we wanted to mention that in our concentration on proving the Diophantine Approximation Theorem, we ignored the problem of *effectivity*. That is, we proved that there are only finitely many pairs of integers (p, q) satisfying the inequality

$$\left|\frac{p}{q} - \sqrt[3]{b}\right| \leq \frac{1}{q^3}.$$

But for any particular value of b, for example $b = 2$, does our proof give us a method for finding all such pairs?
The answer is no. If one looks at the proof, one will find that it says the following. If we can find a solution (p_1, q_2) to our inequality with q_1 very large(where this depends on b), then we can bound the coordinates of every other solution in terms of b, q_1. So if we can find that first large solution, then we can find all of them. But suppose that there are no large solutions? Then one could assume that we just take the small solutions and we are done. However, nothing in our proof gives us a way of verifying that there are no large solutions. So if we find one large solution, we can find all solutions, but if we cannot find a large solution, then we have no way of proving that the set of solutions that we already have is complete.
We therefore mention the following weaker but more effective theorem.

Theorem. *Let $a, b, c \in \mathbb{Z}$ and let*

$$H = \max\{|a|, |b|, |c|\}.$$

Then every point (x, y) on the elliptic curve

$$y^2 = x^3 + ax^2 + bx + c$$

with integer coordinates x, y satisfies

$$\max\{|x|, |y|\} \leq \exp\left((10^6 H)^{10^6}\right).$$

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (2015).