Elliptic Curves Seminar: Integral Points on Elliptic Curves

Dominik Schlagenhauf, Silvan Suter

November 3, 2020

The set of integer points on a non-singular cubic curve with integer coefficients is not in general a subgroup of the group of rational points $C(\mathbb{Q})$, as the following example shows.

Example 1. Let C: $y^2 = x^3 + 17$. Then $P = (-1, 4) \in C(\mathbb{Q})$. But, by a short computation one sees that $Q = 2P = (\frac{137}{64}, \frac{-2651}{512})$ does not have integer coordinates.

The Nagel-Lutz Theorem says that points of finite order on an elliptic curve have integer coordinates (as seen in the presentation about points of finite order). The converse, however, is not true, as the following example shows.

Example 2. Let C, P and Q as in Example 1. Then if we suppose that the converse of Nagel-Lutz holds then, we have that P must have finite order. This implies that Q has finite order and then by Nagel-Lutz we have that Q has integer coordinates. But this is clearly not the case, as seen in Example 1.

Nevertheless, integer points on non-singular cubic curves with integer coefficients have a nice property.

Theorem 1. (Siegel's Theorem). *A non-singular cubic curve with integer coefficients has only finitely many points with integer coordinates.*

Remark 1. The condtion of the cubic curve being non-singular in Siegel's Theorem is necessary. Indeed, $y^2 = x^3$ is a singular cubic curve, for which each (t^2, t^3), $t \in \mathbb{Z}$, is an integer solution.

A proof of Siegel's Theorem can be found in [2], [3]. For the sake of simplicity, we restrict ourselves to the special case of Thue's Theorem, as stated for example in the book of Silverman and Tate [1]. Our proof follows closely their proof.

Theorem 2. (Thue's Theorem). *Let a, b, c be non-zero integers. Then the equation*

$$ax^3 + by^3 = c \tag{1}$$

has only finitely many solutions in integers x, y.

After making a variable shift of x to ax and possibly replacing x with $-x$, y with $-y$ and/or b with $-b$, we can assume that (1) is of the form

$$x^3 - by^3 = c, \text{ where } b, c > 0. \tag{2}$$

Proof. Note that we can factorize

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

If $\beta = \sqrt[3]{b}$ is an integer, this splitting gives rise to a product of two integers. Let

$$A = (x - \beta),$$
$$B = (x^2 + \beta xy + \beta^2 y^2).$$

Solving the first equation for x and insert it into the second equation, we get a quadratic equation for y. Thus there are only two possibilities for the value y, each of which determines x uniquely. So for any factorization of $c = AB$ we can only have a finite number of solutions. Thus, since there are only finitely many ways to factorize $c = AB$, we have that there are also only finitely many solutions $x, y \in \mathbb{Z}$ of (2).

From now on suppose, that β is not an integer. If $y = 0$ we get only one possibility for x, so we may assume $y \neq 0$. We observe

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

Thus, by using (3) we get the inequality

$$c \geq \frac{3}{4}\beta^2 |y|^3 \Big| \frac{x}{y} - \beta \Big|$$

That is,

$$\Big| \frac{x}{y} - \beta \Big| \leq \frac{4c}{3\beta^2} \frac{1}{|y|^3}$$

The result hence follows from the following theorem, since by symmetry, if $y < 0$, then $-y > 0$ and we can apply the following theorem with $-x$ and $-y$.

□

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

$$\Big| \frac{p}{q} - \beta \Big| \leq \frac{C}{q^3} \tag{4}$$

The proof can be divided into four steps:

1. Construct an auxiliary polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ with "bounded" coefficients such that F vanishes at high order with respect to X at the point (β, β).
2. Find an upper bound for the derivatives of F.
3. Show that there is a derivative of F, which does not vanish.
4. Assume that the Diophantine Approximation Theorem does not hold and find solutions, so that the auxiliary polynomial evaluated at those solutions has contradicting upper and lower bounds.

Theorem 4 (Step 1; Auxiliary Polynomial Theorem)**.** *Let b be a non-negative integer, $\beta = \sqrt[3]{b}$, $n \in \mathbb{N}$. Choose $m \in \mathbb{N}$ such that*

$$3 \leq m \leq \frac{2}{3}n < m + 1 \tag{5}$$

Then there is a non-zero polynomial $F(X, Y) \in \mathbb{Z}[X, Y]$ with $deg_X(F) \leq m + n$ of the form

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

which satisfies the following properties

1. *for any $k \in \{1, \ldots, n-1\}$*

$$\frac{\partial^k F}{\partial X^k}(\beta, \beta) = 0$$

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

Proof. Let $F(X, Y) = \sum_{i=0}^{n+m} u_i X^i + v_i X^i Y$ for some later to be defined coefficients $u_i, v_i \in \mathbb{Z}$. Observe that for any $0 \leq k \leq n$ we have $\frac{d^k(x^n)}{dx^k} = \frac{n!}{(n-k)!}x^{n-k}$ and hence

$$F^{(k)}(X, Y) = \frac{1}{k!}\frac{\partial^k F}{\partial X^k}(X, Y)$$

has integer coefficients for any $k \in \mathbb{N}$. By taking derivatives and doing an index shift in the summation, we may compute for $k \in \{1, \ldots, n-1\}$

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

where we set $u_{m+n+1} = v_{-1} = 0$ and $\binom{l}{r} = 0$ if $l < r$. Noting that β^i is an integer times 1, β or β^2 and writing $i = 3j + l$, we get

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

We want to have $F^{(k)}(\beta, \beta) = 0$. Note that $1, \beta, \beta^2$ are linearly independent over $\mathbb{Q}$, hence we want the following equations to hold for any $l \in \{0, 1, 2\}$ and any $k \in \{0, \ldots, n-1\}$

$$\sum_j \binom{3j+l+k}{k} b^j u_{3j+l+k} + \binom{3j+l+k-1}{k} b^j v_{3j+k+l-1} = 0.$$

This yields $3n$ linear equations in $2(m+n+1)$ variables $u_0, \ldots, u_{n+m}, v_0, \ldots, v_{n+m}$. The result thus follows from the next lemma. □

Lemma 1 (Siegel's Lemma)**.** *Let $N < M$ be positive integers and let*

$$\begin{array}{ccc} a_{11}T_1 + \ldots a_{1N}T_N = 0 \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \\ a_{M1}T_1 + \ldots a_{MN}T_N = 0 \end{array}$$

be a nontrivial system of linear equations with $a_{ij} \in \mathbb{Z}$. Then there exist a solution $0 \neq (t_1, \ldots, t_N) \in \mathbb{Z}^N$ with

$$\max_{i=1,\ldots,N} |t_i| < 2(4N \max_{i,j} |a_{ij}|)^{\frac{M}{N-M}}$$

The proof Siegel's Lemma is a result of elementary techniques in linear algebra. For a proof, see [1]. The constructed auxiliary polynomial F(X,Y) satisfies the following properties:

Theorem 5 (Step 2; Smallness Theorem)**.** *Let b, β, n, m and $F(X, Y)$ as in Theorem 4. Then there exists a constant $c_1 = c_1(b) > 0$ depending only on b such that for any $x, y \in \mathbb{R}$ with $|x - \beta| \leq 1$ there holds*

$$|F^{(t)}(x, y)| \leq c_1^n(|x - \beta|^{n-t} + |y - \beta|), \quad \forall t \in \{0, \ldots, n\}.$$

Theorem 6 (Step 3; Non-Vanishing Theorem)**.** *Let b, β, n, m and $F(X, Y)$ as in Theorem 4, and let $(\frac{p_1}{q_1}), (\frac{p_2}{q_2}) \in \mathbb{Q}$ be in lowest terms. Then there exists a constant $c_2 = c_2(b) > 0$ depending only on b and there is a $t \in \mathbb{N}_0$ with $0 \leq t \leq 1 + \frac{c_2 n}{\log q_1}$ such that*

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

The Proofs of Theorems 5 and 6 are rather technical. We therefore refer to the literature, see [1].

Now we have all we need to give the proof of Theorem 3, which will also complete the proof of Theorem 2.

Proof of Theorem 3. For a contradiction assume that there are infinitely many pairs (p, q), which satisfy (4). For the given b in the hypothesis, let c_1 and c_2 be the constants from the Smallness Theorem and the Non-Vanishing Theorem respectively (remember those constants are independent of the choice of $n \in \mathbb{N}$). Multiplying both sides of (4) and using that $q \geq 1$, we get

$$|p - q\beta| \leq C.$$

Hence, if the denominators q of the solutions were bounded, then also the nominators p were bounded, which would contradict the assumption that there are infinitely many solutions. Therefore, there are integer solutions for (4), where the denominator q is arbitrarily large.

We can now use this fact to find integer solutions for which some auxiliary polynomial $F(X, Y)$ has contradicting upper and lower bounds.

Choose integer solutions (p_1, q_1), (p_2, q_2) to (4), so that

$$q_1 > max\{e^{9c_2}, (2c_1C)^{18}\} \tag{6}$$

$$q_2 > q_1^{65}. \tag{7}$$

Let $n \in N$, satisfying

$$n \leq \frac{9}{8}\frac{log(q_2)}{log(q_1)} < n+1.$$

Exponentiating shows, that

$$q_1^{\frac{9}{8}n} \leq q_2 < q_1^{\frac{8}{9}(n+1)}. \tag{8}$$

Using (7), we see that n satisfies

$$n > 72.$$

Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be the polynomial from the Auxiliary Polynomial Theorem with parameters b and n. By the Non-Vanishing Theorem, there exists a $t \in \mathbb{N}$, so that

$$t \leq 1 + \frac{c_2 m}{log(q_1)} \text{ and } F^{(t)}\big(\frac{p_1}{q_1}, \frac{p_2}{q_2}\big) \neq 0.$$

Then, by (6)

$$t \leq 1 + \frac{n}{9}.$$

Since $F^{(t)}(X,Y)$ has degree at most $m+n$ in X and degree 1 in Y, we have

$$F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \frac{N}{q_1^{m+n}q_2}$$

for some integer $N \in \mathbb{N}$. Thus using (8) and $m \leq \frac{2}{3}n$, we find

$$\big|F^{(t)}\big(\frac{p_1,q_1}{p_2,q_2}\big)\big| \geq \frac{1}{q_1^{m+n}q_2} \geq \frac{1}{q_2^{\frac{23}{9}n+\frac{8}{9}}}.$$

For an upper bound, using the Smallness Theorem and the fact that (p_1,q_1) and (p_2,q_2) are solutions to (4), we calculate, that

$$\begin{aligned}
\big|F^{(t)}\big(\frac{p_1}{q_1}, \frac{p_2}{q_2}\big)\big| &\leq c_1^n\left(\big|\frac{p_1}{q_1} - \beta\big|^{n-t} + \big|\frac{p_2}{q_2} - \beta\big|\right) \\
&\leq c_1^n\left(\big(\frac{C}{q_1^3}\big)^{n-t} + \frac{C}{q_2^3}\right) \\
&\leq c_1^n\left(\big(\frac{C}{q_1^3}\big)^{\frac{8}{9}n-1} + \frac{C}{q_1^{\frac{8}{3}n}}\right) \\
&\leq \frac{(2c_1C)^n}{q_1^{\frac{8}{3}n-3}} \\
&\leq \frac{1}{q_1^{\frac{47}{18}n-3}}.
\end{aligned}$$

We therefore have

$$\frac{1}{q_1^{\frac{23}{9}n+\frac{8}{9}}} \leq \big|F^{(t)}\big(\frac{p_1}{q_1}, \frac{p_2}{q_2}\big)\big| \leq \frac{1}{q_1^{\frac{47}{18}n-3}}.$$

Multiplying both sides by $q_1^{\frac{47}{18}n-33}$ and using $n \geq 72$, we find

$$q_1^{\frac{1}{9}} \leq 1.$$

But this contradicts $q_1 \geq (2c_1C)^{18} \geq 2$. Thus (4) can only have finitely many solutions. This proves the theorem. $\square$

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).

[2] C.L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. Lond. Math. Soc. (1926).

[3] C.L. Siegel, *Über einige Anwendungen diophantischer Approximationen (1929), in Collected Works*, Springer (1966).