AGRA IV, 2021
Diophantine equations with few solutions

Hector Pasten

Compiled on 2021/08/14 at 16:01:41

Departamento de Matemáticas, PUC, Chile
Email address, H. Pasten: `hector.pasten@mat.uc.cl`

Contents

LECTURE 1

Warm-up: elliptic curves

1. The basics

Let k be a field. An *elliptic curve* over k is a smooth projective irreducible curve of genus 1 with a distinguished k-rational point.

For us, the most relevant example is given by elliptic curves in *Weierstrass form*

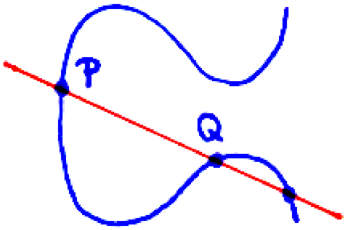
$$y^2 = x^3 + Ax^2 + Bx + C$$

where $\mathrm{Disc}(x^3 + Ax^2 + Bx + C) \neq 0$. This last condition ensures that the plane curve defined by the previous equation is smooth. It is not projective, but its projective closure in $\mathbb{P}^2$ in homogeneous coordinates $[x : y : z]$ is

$$y^2 z = x^3 + Ax^2 z + Bxz^2 + Cz^3.$$

At infinity (i.e. $z = 0$) there is only the point $[0 : 1 : 0]$ which is the distinguished point of an elliptic curve in Weierstrass form.

Given an elliptic curve $E \subseteq \mathbb{P}^2$ in Weierstrass form over k and k-rational points P, Q (possibly the same) we consider the line L through P and Q (if $P = Q$ we take the tangent to E). Since $\deg(L) = 1$ and $\deg(E) = 3$ there must be a third intersection point if we count with multiplicities. It is k-rational because P and Q are.



This method to get new points from known ones was already discussed by Diophantus in his book series *Arithmetica* in the III century.

Example 1.1. Let E over $\mathbb{Q}$ be given by $y^2 = x^3 + 1$. We have the trivial points $(x, y) = (-1, 0)$ and $(0, 1)$. The line L through them is $y = x + 1$. Let's intersect L and E:

$$\begin{cases} y^2 = x^3 + 1 \\ y = x + 1 \end{cases} \Rightarrow \begin{cases} x^2 + 2x + 1 = x^3 + 1 \\ y = x + 1 \end{cases} \Rightarrow \begin{cases} 0 = x^3 - x^2 - 2x = x(x+1)(x-2) \\ y = x + 1 \end{cases}$$

We find the two initial solutions and a new more interesting one: $(x, y) = (2, 3)$.

2. Group law

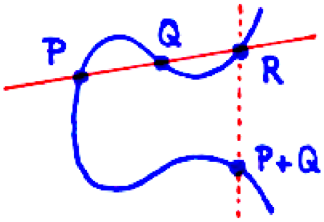
It is a theorem of Poincaré that a small modification of Diophantus's method yields much more algebraic structure:

THEOREM 1.2 (Poincare; group law). *Let k be a field and let E be an elliptic curve given in Weierstrass form over k. Given $P, Q \in E(k)$ define the point "$P + Q$" as follows:*

Suppose that $R = (a, b)$ is the third intersection with E of the line L through P and Q. Then $P + Q := (a, -b)$.

With this operation, $E(k)$ becomes an abelian group with neutral element $P_\infty = [0 : 1 : 0]$.

Pictorially, we have:



3. Integral points

Let us consider another example, only slightly different to the previous one. We'll focus on integral solutions.

EXAMPLE 1.3. Let E over $\mathbb{Q}$ be given by $y^2 = x^3 - 1$. We have the trivial point $(x, y) = (1, 0)$ and a quick search reveals no other integer solution. Is there any other integer solution?

First, we see that x must be odd and y must be even, by working modulo 4.

Now, working over the Euclidean domain $\mathbb{Z}[i]$ we have

$$x^3 = y^2 + 1 = (y + i)(y - i).$$

Notice that $(y + i) - (y - i) = 2i$ and recall that x is odd, so, $\gcd(y + i, y - i) = 1$.

Due to the equation $(y+i)(y-i) = x^3$ in $\mathbb{Z}[i]$ (which is UFD) we see that $y+i$ and $y-i$ are cubes up to units, but the only units are $\pm 1, \pm i$ which are cubes themselves. Therefore $y + i$ and $y - i$ are cubes in $\mathbb{Z}[i]$

In particular, $y + i = (a + bi)^3 = a^3 + 3a^2bi - 3ab^2 - b^3i$ for some $a, b \in \mathbb{Z}$. Separating real and imaginary parts, we find

$$\begin{cases} y = a^3 - 3ab^2 = a(a^2 - 3b^2) \\ 1 = 3a^2b - b^3 = b(3a^2 - b^2) \end{cases}$$

The second equation forces $b = \pm 1$ and $a = 0$, and the first equation gives $y = 0$. Hence, the only integral point in the elliptic curve $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.

Finiteness of integral points holds in much greater generality than this example:

THEOREM 1.4 (Siegel). *If E is an elliptic curve given by a Weierstrass equation with integer coefficients, then it has at most a finite number of integral points.*

4. Rational points

The main theorem for the rational solutions of an elliptic curve over $\mathbb{Q}$ is

Theorem 1.5 (Mordell). *Let E be an elliptic curve over $\mathbb{Q}$. With the group structure from Poincaré's theorem, the set of rational points $E(\mathbb{Q})$ is a finitely generated abelian group. In particular, $E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$ where T is a finite abelian group (the torsion part) and $r = \operatorname{rk} E(\mathbb{Q}) \geq 0$ is the rank.*

The torsion part is easy to compute with the aid of

Theorem 1.6 (Nagell-Lutz). *Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation*

$$y^2 = x^3 + Ax^2 + Bx + C$$

with integer coefficients, and let $\Delta = \operatorname{Disc}(x^3 + Ax^2 + Bx + C)$. All affine torsion points have integral coordinates. Points with $y = 0$ are precisely the 2-torsion points, and all other torsion points satisfy $y^2|\Delta$.

Computing the rank is harder. There is a method called *descent* which, at present, is not guaranteed to terminate. Nevertheless, descent often works in practice. It is slow to do by hand, but fortunately it is programmed in Sage and Magma (among other softwares).

Regardless of whether it terminates or not, descent always gives an upper bound for the rank. In the case of 2-descent in the presence of a 2-torsion point, we get the following simple upper bound (see [**1**], and see [**6**] for a more precise result)

Theorem 1.7. *Let E be an elliptic curve given by a Weiertrass equation of the form $y^2 = x^3 + Ax^2 + Bx$ with $A, B \in \mathbb{Z}$. Then*

$$\operatorname{rk} E(\mathbb{Q}) \leq \omega(B) + \omega(A^2 - 4B) - 1$$

where $\omega(n)$ is the number of different prime divisors of n.

The next example will use Sage. You can use a basic version for free here:
`https://sagecell.sagemath.org`

Example 1.8. After a change of variables, elliptic curves over $\mathbb{Q}$ can be written in the form $y^2 = x^3 + bx + c$ and Sage reads this as $[b, c]$. For instance, let us compute the rank of the elliptic curve $y^2 = x^3 + 1$ of Example 1.1:

```
>E=EllipticCurve([0,1]);
>[E, E.rank()]
Sage: [Elliptic Curve defined by y^2 = x^3 + 1 over Rational Field, 0]
```

This means that $E(\mathbb{Q})$ is just torsion. We leave it as an exercise to compute all the affine torsion points using the Nagell-Lutz theorem. Here, instead, let us simply use Sage:

```
>E=EllipticCurve([0,1]);
>E.torsion_order()
Sage: 6
```

This means that there are 6 torsion points. One is $\infty = [0 : 1 : 0]$ and we already know the points $(-1, 0), (0, 1), (0, -1), (2, 3), (2, -3)$ from Example 1.1. Thus, our list is complete and we found *all* the rational solutions of $y^2 = x^3 + 1$.

LECTURE 2

Rational approximations and integral points

1. Dirichlet: Good and cheap rational approximations exist

Every real number can be approximated by rational numbers. Naturally, one one would love to have control on the quality of such approximations. For instance, $\sqrt{2} = 1.4142...$ can be approximated by

$$\frac{17}{12} = 1.41\overline{6} \text{ and by } \frac{109}{77} = 1.\overline{415584}.$$

The second approximation has a slightly smaller error, but it is more complicated to write.

A classical result by Dirichlet provides a supply of rational approximations that are both good and not too expensive:

Theorem 2.1 (Dirichlet, 1840). *Let $\alpha \in \mathbb{R}$ be an irrational number. There are infinitely many rational numbers $q = a/b$ with a, b coprime integers and $b > 0$, such that*

$$|\alpha - q| < \frac{1}{b^2}.$$

If the reader has not seen the proof before, she should give it a try.

An example: Our first rational approximation of $\sqrt{2}$ is as provided by Dirichlet's theorem while the second one is not: it is too expensive for its quality:

$$\left|\sqrt{2} - \frac{17}{12}\right| = 0.0024... < \frac{1}{12^2} = 0.0069...; \quad \left|\sqrt{2} - \frac{109}{77}\right| = 0.0013... > \frac{1}{77^2} = 0.0001...$$

2. Liouville: Algebraic numbers cannot be approximated too well

Can we do better than what Dirichlet's theorem provides? The first result to address this problem is due to Liouville. It imposes a non-trivial restriction on the exponent on the approximation when α is *algebraic*.

Theorem 2.2 (Liouville, 1844). *Let $\alpha \in \mathbb{R}$ be an irrational algebraic number of degree d. There is a constant $c(\alpha) > 0$ depending only on α such that for every rational number $q = a/b$ with a, b coprime integers and $b > 0$ we have*

$$|\alpha - q| > \frac{c(\alpha)}{b^d}.$$

The proof is an easy exercise using the minimal polynomial of α.

We have two immediate consequences:

Corollary 2.3. *The exponent of b^2 in Dirichlet's theorem cannot be increased when α is real quadratic, e.g. for $\alpha = \sqrt{2}$. Thus, the exponent in Dirichlet's theorem is optimal.*

Corollary 2.4. *The real number $\lambda = \sum_{n=1}^{\infty} \frac{1}{2^{n!}}$ is transcendental.*

3. Approximation theorems beyond Liouville

Liouville's argument has served as a blueprint for more sophisticated arguments leading to stronger estimates. The first improvement was due to Thue:

THEOREM 2.5 (Thue's approximation bound, 1909). *Let $\alpha \in \mathbb{R}$ be an irrational algebraic number of degree d and let $\epsilon > 0$. For all but finitely many $q = a/b \in \mathbb{Q}$ (with a, b coprime integers) we have*

$$|\alpha - q| \geq \frac{1}{|b|^{d/2+1+\epsilon}}. \tag{3.1}$$

COMMENTS ABOUT THE PROOF. A gentle and detailed exposition of Thue's proof can be found in [**33**]. We will not repeat the details here. Let us simply say that it is a two-variables generalization of Liouville's proof. □

The method of proof initiated by Liouville and Thue (namely, constructing auxiliary polynomials, proving non-vanishing at rational points, and confronting upper and lower bounds) is nowadays called **Diophantine approximation method**.

The exponent $d/2 + 1 + \epsilon$ in Thue's theorem was improved by Siegel, Gelfond, Dyson, and finally by Roth [**31**] who obtained the exponent $2 + \epsilon$. Roth's theorem was generalized by Schmidt [**32**] to higher dimensions, in what is now called the *Subspace Theorem.*

4. Integral points in curves

Thue used his Diophantine approximation result to prove the following remarkable finiteness theorem for a special type of Diophantine equations.

THEOREM 2.6 (Thue's equation). *Let $F(x, y) \in \mathbb{Z}[x, y]$ be an irreducible homogeneous polynomial of degree $d \geq 3$. Let c be a non-zero integer. The Diophantine equation*

$$F(x, y) = c \tag{4.1}$$

has at most finitely many integer solutions.

PROOF. Let $\alpha_1, ..., \alpha_d$ be the roots of $F(x, 1)$ in $\mathbb{C}$ and let $\delta = \min\{|\alpha_i - \alpha_j| : i \neq j\}/3$. We can factor F as

$$F(x, y) = \prod_{j=1}^{d} (x - \alpha_j y).$$

We proceed by contradiction; assume that (4.1) has infinitely many integer solutions.

An auxiliary map. Let us ignore the finitely many solutions with $y = 0$. Given an integer solution $(a, b) \in \mathbb{Z}^2$ for (4.1) having $b \neq 0$, we construct the rational number $\phi(a, b) = a/b$. Since $F(a, b) = c$ we have $\gcd(a, b)^d | c$, thus, this construction is finite-to-one.

The auxiliary map gives good approximations. Let (a, b) be an integer solution of (4.1) with $b \neq 0$ and write $q = \phi(a, b)$. Then

$$\frac{c}{b^d} = F(q, 1) = \prod_{j=1}^{d} (q - \alpha_j).$$

By definition of δ, for at most one j we can have $|q-\alpha_j|<\delta$. This means that

$$|c|/|b|^d \geq \delta^{d-1} \cdot \min_{1\leq j\leq d} |\alpha_j - q|.$$

Since we have infinitely many (a,b) and ϕ is finite-to-one, we have infinitely many possible values of q. Passing to an infinite sub-sequence $q_i = \phi(a_i, b_i)$ and relabeling the α_j if necessary, we obtain

$$\delta^{1-d}|c|/|b_i|^d \geq |\alpha_1 - q_i| \quad \text{for each } i = 1, 2, ...$$

A posteriori, this α_1 must belong to $\mathbb{R}$ because it is the limit of a sequence in $\mathbb{Q}$.

Applying a Diophantine approximation estimate. Let $\epsilon > 0$. The algebraic number $\alpha_1 \in \mathbb{R}$ has degree $d \geq 3$. Hence, Thue's approximation theorem gives

$$|\alpha_1 - q| > \frac{1}{|b|^{d/2+1+\epsilon}}$$

for all but finitely many $q = \phi(a,b)$.

Confronting the bounds. Let $\epsilon = 1/4$. Discarding finitely many of the q_i, we get

$$\delta^{1-d}|c|/|b_i|^d \geq |\alpha_1 - q_i| > 1/|b_i|^{d/2+1+1/4}$$

for an infinite sequence $q_i = \phi(a_i, b_i)$. This gives

$$|b_i|^{1/4} \leq |b_i|^{d/2-1.25} < \delta^{1-d}|c|.$$

where we used $d \geq 3$. Hence, b_i is bounded, which is impossible because the sequence $q_i = \phi(a_i, b_i)$ was infinite. □

We remark that a Pell equation such as $x^2-2y^2=1$ has infinitely many integral solutions. This shows that the assumption $d \geq 3$ in Thue's theorem cannot be dropped.

The strategy in the previous proof is still in use today, to show that integral or rational points of certain algebraic varieties are Zariski degenerate, or even to show finiteness. See for instance [**9**].

Thue's theorem on finiteness of integral points in plane curves of the form $F(x,y) = c$ with $\deg F \geq 3$ was later generalized by Siegel using stronger Diophantine approximation bounds. For the moment we state a version over $\mathbb{Z}$, but the result actually holds over rings of S-integers of number fields.

Theorem 2.7 (Siegel's theorem on integral points). *Let C be a smooth, geometrically irreducible algebraic curve in affine space defined by equations over $\mathbb{Z}$. When C has geometric genus 0 we further assume that the smooth compactification of C has at least 3 complex points at infinity. Under these assumptions, the set $C(\mathbb{Z})$ of integral points of C is finite.*

We leave it to the reader to check that Thue's Theorem 2.6 is a direct consequence of Siegel's theorem: The equation $F(x,y) = c$ defines an affine plane curve and its projective closure in $\mathbb{P}^2_{\mathbb{C}}$ is smooth irreducible with $d \geq 3$ points at infinity.

Also, this version of Siegel's theorem implies the one about integral points in affine Weierstrass models of elliptic curves (cf. Theorem 1.4).

LECTURE 3

Chabauty's p-adic approach

1. Abelian varieties

Let k be a field. An *abelian variety* A over k is an algebraic group over k which is projective. Automatically, A is commutative.

Examples.

- A point. This is an abelian variety of dimension 0.
- The affine line $\mathbb{A}^1$ with addition is a group variety, it is commutative, but it is not an abelian variety: it is not projective.
- Abelian varieties of dimension 1 are precisely elliptic curves.
- Products of elliptic curves give examples of abelian varieties of any dimension.
- Jacobians of curves of genus g give examples of abelian varieties of dimension g. We'll say more about jacobians of curves below.
- Over $k = \mathbb{C}$ all abelian varieties are of the form $\mathbb{C}^g/\Lambda$ where $\Lambda \subseteq \mathbb{C}^g$ is a rank $2g$ lattice. (However, if $g \geq 2$ not every quotient of this form is algebraic.)

Weil generalized Mordell's theorem to abelian varieties over number fields. Here we state a version over $\mathbb{Q}$:

Theorem 3.1 (Mordell-Weil). *Let A be an abelian variety over $\mathbb{Q}$. The group of rational points $A(\mathbb{Q})$ is a finitely generated abelian group. In particular, $A(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r$ where T is a finite abelian group (the torsion part) and $r = \operatorname{rk} A(\mathbb{Q}) \geq 0$ is the rank of A.*

2. Jacobians

Now, let k be a perfect field and let C be a smooth, projective curve over k of genus g. Recall that the *jacobian* of C is an abelian variety $J = J_C$ over k of dimension g with the following property: For every L/k there is a functorial bijection between degree 0 divisors on $C \otimes L$ modulo linear equivalence, and the points of $J(L)$.

Example. All degree 0 divisors on $\mathbb{P}^1_k$ are linearly equivalent to each other, so $J_{\mathbb{P}^1_k}$ must be a point: the trivial abelian variety. This is correct and it coincides with the fact that the genus of $\mathbb{P}^1$ is 0.

Suppose that $C(k)$ is non-empty and fix $x_0 \in C(k)$. Then we get a function

$$j_{x_0} : C \to J, \quad x \mapsto [x - x_0].$$

This map is called the Abel-Jacobi map. Over $\mathbb{C}$ it has another expression using period integrals; we don't need that in these notes.

Theorem 3.2 (Properties of the Abel-Jacobi map). *We keep the previous notation. If $g \geq 1$ then $j_{x_0} : C \to J$ is an embedding defined over k. Moreover, the curve $j_{x_0}(C)$ generates J geometrically (i.e. over an algebraic closure of k).*

Therefore, every curve of genus $g \geq 1$ having a k-rational point can be embedded into an abelian variety over k —its own jacobian! This is an extremely useful construction to study rational points in curves, since rational points in abelian varieties have more structure.

3. Completions of $\mathbb{Q}$

A classical result of Ostrowski says that the only non-trivial absolute values on $\mathbb{Q}$ are (up to equivalence by taking powers) the usual archimedian one $|x|_\infty = |x|$ and for each prime number p, the p-adic one $|x|_p = p^{-\mathrm{ord}_p(x)}$. Note that $|-|_p$ is a non-archimedian absolute value, that is, it satisfies the strong triangle inequality

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}.$$

Hence, the set of places of $\mathbb{Q}$ is $M_{\mathbb{Q}} = \{\infty, 2, 3, 5, ...\}$ and for each $v \in M_{\mathbb{Q}}$ we have the corresponding absolute value $|-|_v$ we just mentioned. These absolute values satisfy:

Lemma 3.3 (Product formula on $\mathbb{Q}$). *For all $x \in \mathbb{Q}^\times$ we have*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1.$$

For each $v \in M_{\mathbb{Q}}$ we let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ with respect to $|-|_v$. Thus, $\mathbb{Q}_v$ is a field, it densely contains $\mathbb{Q}$, and $|-|_v$ extends to $\mathbb{Q}_v$. There are two cases:

- $v = \infty$. Then $\mathbb{Q}_v = \mathbb{Q}_\infty = \mathbb{R}$.
- $v = p$ is a prime. Then $\mathbb{Q}_v = \mathbb{Q}_p$ is the field of p-adic numbers.

We define $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$; this is the bordered unit ball in $\mathbb{Q}_p$. The proof of the following simple fact is left as an exercise (in case the reader does not already know it).

Lemma 3.4. *The set $\mathbb{Z}_p$ is a sub-ring of $\mathbb{Q}_p$, it contains $\mathbb{Z}$ and, in fact, $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. The ring $\mathbb{Z}_p$ is a complete DVR and its only maximal ideal is $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$.*

Furthermore, the distance $d_p(x,y) = |x-y|_p$ makes $\mathbb{Z}_p$ into a compact metric space.

The next example should help to get some familiarity p-adic numbers.

Example. The equation $x^2+1=0$ does not have solutions in $\mathbb{Q}_\infty = \mathbb{R}$.

Let $v = p$ be a prime $p \equiv 1 \bmod 4$. It is an exercise in elementary number theory to check that for all $n \geq 1$, the congruence $x^2+1 \equiv 0 \bmod p^n$ has a solution $a_n \in \mathbb{Z}$ (recall that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.) The sequence a_n in $\mathbb{Z} \subseteq \mathbb{Z}_p$ has a convergent subsequence $b_j = a_{n_j}$ by compactness of $\mathbb{Z}_p$ where $n_j \geq j$; let $b = \lim b_j \in \mathbb{Z}_p$. From $b_j^2 + 1 \equiv 0 \bmod p^j$ we get

$$|b_j^2+1|_p = p^{-\mathrm{ord}_p(b_j^2+1)} \leq p^{-j} \to 0$$

so, $b^2+1=0$ in $\mathbb{Z}_p$. This means that $\mathbb{Q}_p$ contains a root of x^2+1 when $p \equiv 1 \bmod 4$.

We leave it as an exercise to check that $x^2+1=0$ does not have solutions in $\mathbb{Q}_v$ for $v=2$ and for $v = p \equiv 3 \bmod 4$ (*Hint:* prove that if such a solution b exists, it must be in $\mathbb{Z}_p$. As $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, approximate b by $b' \in \mathbb{Z}$ and reduce b' modulo 4 or modulo p accordingly.)

4. The Chabauty-Coleman method

Mordell [**25**] formulated the following celebrated conjecture

Conjecture 3.5 (Mordell's conjecture). *Let C be a smooth projective curve of genus $g \geq 2$ over $\mathbb{Q}$. The set of rational points $C(\mathbb{Q})$ is finite.*

Obviously, the condition $g \geq 2$ is necessary in general. Mordell's conjecture was proved by Faltings in 1983 —we'll say more about Faltings's work in the next lecture.

In 1941, more than 40 years before Faltings's proof of Mordell's conjecture, Chabauty proved the following remarkable result in the direction of Mordell's conjecture:

Theorem 3.6 (Chabauty). *Let C be a smooth projective curve over $\mathbb{Q}$ of genus $g \geq 2$. Let J be the jacobian of C and assume that* $\operatorname{rk} J(\mathbb{Q}) \leq g-1$. *Then $C(\mathbb{Q})$ is finite.*

Sketch of proof. If $C(\mathbb{Q})$ is empty, we are done. Otherwise, embed C into J using a base point $x_0 \in C(\mathbb{Q})$ via the Abel-Jacobi map

$$C \to J, \quad x \mapsto [x - x_0].$$

Choose a prime p. There is a nice p-adic logarithm

$$\mathrm{Log} : J(\mathbb{Q}_p) \to T_e := \mathbb{Q}_p^g$$

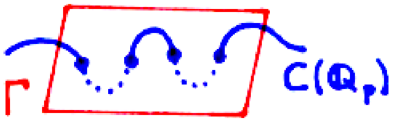
which is a p-adic analytic group morphism with finite kernel. Let Γ be the p-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$, then using Log one sees

$$\dim \Gamma = \dim \mathrm{Log}(\Gamma) = \dim \overline{\mathrm{Log} J(\mathbb{Q})} \leq \operatorname{rk} J(\mathbb{Q}) \leq g-1 < \dim J(\mathbb{Q}_p).$$

The p-adic analytic group Γ is important because

$$C(\mathbb{Q}) = C(\mathbb{Q}_p) \cap J(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap \Gamma.$$

The curve C generates J but Γ is an analytic subgroup of positive codimension, so, the p-adic manifolds $C(\mathbb{Q}_p)$ and Γ intersect properly.



Using the identity principle for p-adic analytic functions, a compactness argument shows that $C(\mathbb{Q}_p) \cap \Gamma$ is finite, hence $C(\mathbb{Q})$ is finite. □

In 1985, Coleman [**7**] discovered a way to make Chabauty's theorem more precise:

Theorem 3.7 (Coleman). *Let C be a smooth projective curve of genus $g \geq 2$ over $\mathbb{Q}$ and let $p > 2g$ be a prime of good reduction for C. Suppose that* $\operatorname{rk} J_C(\mathbb{Q}) \leq g-1$. *Then*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2.$$

This bound is quite small and in some cases it is attained. When that occurs, one knows that all the rational points of C have been found.

Nowadays, the Chabauty-Coleman method and its non-abelian extensions (after Kim [**20**]) are the most powerful tools for computing the set of all rational points of a curve.

Very recently, Caro and yours truly extended the Chabauty-Coleman method to surfaces, obtaining explicit bounds for the number of rational points. See [**5**] for details.

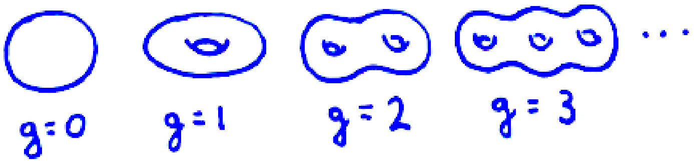
LECTURE 4

The theorems of Faltings

1. Faltings's theorem for curves

We have the following fundamental finiteness result by Faltings [**12**] which proves a conjecture formulated by Mordell [**25**] in 1922.

THEOREM 4.1 (Faltings's theorem; conjectured by Mordell). *Let X be a smooth, projective, geometrically irreducible curve over a number field K (e.g. $K = \mathbb{Q}$) of genus $g \geq 2$. Then $X(K)$ is finite.*



The original proof by Faltings uses the method of *moduli spaces*: To each $P \in X(K)$ one associates an abelian variety A_P and finiteness is proved by studying the moduli space of such abelian varieties as well as their ℓ-adic Galois representations. The details go far beyond the modest goals of these lecture notes and we refer the interested reader to [**8**] for a full account of the proof and the necessary background.

There is another proof by Vojta [**34**] which uses the method of Diophantine approximation in the language of Arakelov geometry. It was later simplified and presented in classical terms by Bombieri [**3**]. This approach to Mordell's conjecture was generalized by Faltings [**13, 14**] to study rational points in subvarieties of abelian varieties; see [**11**] for an exposition.

There is yet another more recent proof of Mordell's conjecture by Lawrence and Venkatesh [**22**] which is inspired by Faltings's original proof, but which directly works with Galois representations attached to points of $X(K)$, not with the abelian varieties A_P mentioned above.

2. Examples

EXAMPLE 4.2. Let $f(x) \in \mathbb{Z}[x]$ be a squarefree polynomial of degree $r \geq 5$. Then $\{f(t) : t \in \mathbb{Q}\}$ can only contain finitely many squares.

Indeed, the equation $y^2 = f(x)$ defines a hyperelliptic curve of genus $g = \lfloor (r-1)/2 \rfloor \geq 2$.

EXAMPLE 4.3. Let $n \geq 4$. The Fermat equation $x^n + y^n = z^n$ has finitely many coprime integer solutions.

Indeed, the equation defines a smooth plane curve X_n in the projective plane $\mathbb{P}^2$ in the homogeneous coordinates $[x:y:z]$. The genus of this curve is

$$g = \frac{(n-1)(n-2)}{2} \geq 3.$$

Example 4.4. This example comes from complex analysis. A *uniqueness polynomial* $P(x) \in \mathbb{C}[x]$ is one with the following property: If $f, g \in \mathscr{M}$ are non-constant complex meromorphic functions on $\mathbb{C}$ with $P(f) = P(g)$, then $f = g$.

For instance, $P(x) = x^n - x$ is a uniqueness polynomial for each integer $n \geq 5$ (cf. Theorem 2 in [**19**]).

Proposition 4.5. *If $P(x) \in \mathbb{Q}[x]$ is a uniqueness polynomial, then the map $P : \mathbb{Q} \to \mathbb{Q}$ is injective, up to finitely many points.*

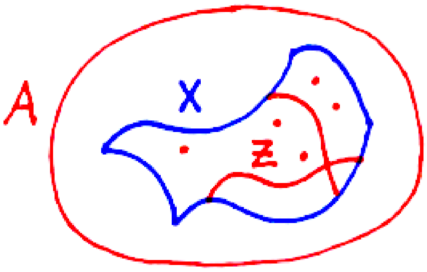
Proof. Let X be the affine plane curve $P(x) = P(y)$ and let C be an irreducible component of X over $\mathbb{C}$ of geometric genus $g \leq 1$. Then there is a complex holomorphic map $f : \mathbb{C} \to \overline{C}$ where $\overline{C}$ is the projective closure of C. Concretely, $f = (f_1, f_2)$ with f_j non-constant meromorphic on $\mathbb{C}$. Since $C \subseteq X$ we have $P(f_1) = P(f_2)$, so in fact $f_1 = f_2$ because P is a uniqueness polynomial. Therefore, $C = \{x = y\}$.

Thus, the only geometric component of X with geometric genus $g \leq 1$ is the diagonal, and Faltings's theorem gives that all but finitely many rational points of X satisfy $x = y$. □

3. Faltings's "big" theorem

The aforementioned result of Faltings for subvarieties of abelian varieties is the following (stated over $\mathbb{Q}$ for simplicity):

Theorem 4.6. *Let A be an abelian variety over $\mathbb{Q}$ and let $X \subseteq A$ be a subvariety defined over $\mathbb{Q}$. Let $Z \subseteq X$ be the Zariski closure of $X(\mathbb{Q})$. Then Z is the union of finitely many translates of abelian subvarieties of A.*



For instance, if $X \subseteq A$ contains no abelian variety of positive dimension, then $X(\mathbb{Q})$ is finite. For the sake of exposition, let us discuss one of many possible applications:

Theorem 4.7 (cf [**28**]). *Let E be an elliptic curve over $\mathbb{Q}$ of positive rank. There is a non-empty affine Zariski open set $U \subseteq E \times E$ and a polynomial function F on the surface U such that the map $F : U(\mathbb{Q}) \to \mathbb{Q}$ is injective.*

Idea of proof. Upon a suitable construction of f, one needs to consider the variety X defined by $F(x) = F(y)$ in $U \times U \subseteq A = E^4$. It turns out that $\dim X = 3$ and one has to apply Faltings's theorem to it. This is not enough: one has to explicitly find the abelian varieties contained in X. The computation is simplified by the choice of F. The basic idea is to use uniqueness functions as in Example 4.4 to construct F. See the details in [**28**]. □

In applications, its is often useful to have the following more precise version due to Rémond [**30**]

Theorem 4.8 (Rémond). *Let A be an abelian variety of dimension n defined over $\mathbb{Q}^{alg}$, and let $\mathscr{L}$ be a symmetric ample invertible sheaf on A. There is an effectively computable number $c(A,\mathscr{L}) > 0$ such that the following holds:*

Let X be a closed subvariety of A of dimension m, and let Λ be a subgroup of $A(\mathbb{Q}^{alg})$ such that its rank $r = \dim_{\mathbb{Q}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})$ is finite. There is a non-negative integer

$$R \leq (c(A,\mathscr{L}) \deg_{\mathscr{L}} X)^{(r+1)n^{5(m+1)^2}}$$

and there exist points $x_1, \dots, x_R$ in $X(\mathbb{Q}^{alg}) \cap \Lambda$ and abelian subvarieties $T_1, \dots, T_R$ of A satisfying that $x_i + T_i \subseteq X$ for each $1 \leq i \leq R$, and

$$X(\mathbb{Q}^{alg}) \cap \Lambda = \bigcup_{i=1}^{R} (x_i + T_i)(\mathbb{Q}^{alg}) \cap \Lambda.$$

The statement is complicated but the important lesson is that there is aversion of Faltings's big theorem with control on the number of rational points, although it is not as sharp as what one can get from the Chabauty-Coleman approach (when it applies).

4. Hyperbolicity

Let M be a complex compact manifold. M is *hyperbolic* if every complex holomorphic map $f : \mathbb{C} \to M$ is constant. For instance:

- Hyperbolic curves are precisely those of genus $g \geq 2$ (Picard)
- Products of hyperbolic manifolds are hyperbolic.
- Abelian varieties of positive dimension are not hyperbolic: over $\mathbb{C}$ they are of the form $\mathbb{C}^g/\Lambda$ for a suitable lattice Λ so, they admit holomorphic maps from $\mathbb{C}$.

We immediately deduce the following from Faltings's theorem

Corollary 4.9. *Let A be an abelian variety over $\mathbb{Q}$ and let $X \subseteq A$ be a subvariety defined over $\mathbb{Q}$. If $X(\mathbb{C})$ is a hyperbolic manifold, then $X(\mathbb{Q})$ is finite.*

This can be seen as strong evidence for the following conjecture of Lang, which is a higher dimensional generalization of Mordell's conjecture (thanks to Picard's theorem):

Conjecture 4.10 (Lang). *Let X over $\mathbb{Q}$ be a smooth projective variety. If $X(\mathbb{C})$ is hyperbolic, then $X(\mathbb{Q})$ is finite.*

LECTURE 5

Conjectures of Bombieri and Lang

1. Kodaira-Iitaka dimension

Let k be a field and let X be a smooth, irreducible, projective variety over k.

Given a line sheaf $\mathscr{L}$ on X, its **semigroup** is $\mathbb{N}(\mathscr{L}) = \{m \geq 0 : h^0(\mathscr{L}^{\otimes m}) > 0\}$. This is indeed an additive semigroup because $0 \in \mathbb{N}(\mathscr{L})$ since $\mathscr{L}^{\otimes 0} = \mathscr{O}_X$, and we also have the maps of multiplication of sections $H^0(X, \mathscr{L}^{\otimes a}) \otimes H^0(X, \mathscr{L}^{\otimes b}) \to H^0(X, \mathscr{L}^{\otimes (a+b)})$.

It is a standard fact that if $\mathbb{N}(\mathscr{L})$ is non-trivial, there is an integer $\kappa(\mathscr{L}) \in \{0, 1, ..., \dim(X)\}$ and some constants $A > a > 0$ such that for all large enough $m \in \mathbb{N}(\mathscr{L})$ we have

$$a \cdot m^{\kappa(\mathscr{L})} < h^0(\mathscr{L}^{\otimes m}) < A \cdot m^{\kappa(\mathscr{L})}.$$

Furthermore, if $\mathbb{N}(\mathscr{L}) = \{0\}$ we define $\kappa(\mathscr{L}) = -\infty$. The quantity $\kappa(\mathscr{L})$ is called the **Kodaira-Iitaka dimension of $\mathscr{L}$**.

2. Big line sheaves

A line sheaf $\mathscr{L}$ is called **big** if there is some $N \geq 1$ such that $\mathscr{L}^{\otimes N}$ is effective (i.e. $h^0(\mathscr{L}^{\otimes N}) \geq 1$) and the rational map $\phi_{\mathscr{L}^{\otimes N}} : X \dashrightarrow \mathbb{P}^d_k$ (with $d+1 = h^0(\mathscr{L}^{\otimes N})$) is birational onto its image. This extends to divisors via the construction $\mathscr{O}_X(D)$. Note that if $\mathscr{L}$ is ample, then it is big. We have the following classical characterization of bigness:

Lemma 5.1. *Let $\mathscr{L}$ be a line sheaf on X. The following are equivalent:*

(i) *$\mathscr{L}$ is big.*
(ii) *$\kappa(\mathscr{L}) = \dim(X)$.*
(iii) *(Kodaira's lemma) There are an ample line sheaf $\mathscr{A}$ and an effective line sheaf $\mathscr{E}$ on X with $\mathscr{L}^{\otimes N} \simeq \mathscr{A} \otimes \mathscr{E}$ for certain integer $N > 0$.*

Let $\mathscr{K}_X = \Omega^{\dim(X)}_{X/k}$ be the canonical sheaf of X, which is invertible since X is smooth. The **Kodaira dimension of** X is $\kappa(X) := \kappa(\mathscr{K}_X)$. A smooth, irreducible, projective variety X is of **general type** if $\kappa(X) = \dim(X)$, i.e. when $\mathscr{K}_X$ is big. In particular, if $\mathscr{K}_X$ is ample then X is of general type. The following example is left as an exercise.

Lemma 5.2. *Let X be a smooth, projective, geometrically irreducible curve of genus g over a perfect field k. Then X is of general type if and only if $g \geq 2$. More precisely:*

$$\kappa(X) = \begin{cases} -\infty & \text{if } g = 0, \\ 0 & \text{if } g = 1, \\ 1 & \text{if } g \geq 2. \end{cases}$$

The Enriques-Kodaira classification of complex projective surfaces (see for instance [**2**]) gives a full description of smooth, projective, irreducible surfaces X over $\mathbb{C}$ up to birational equivalence in the cases of Kodaira dimension $-\infty$, 0, and 1. However, the classification of surfaces of general type is not yet fully understood.

3. Mordell, Bombieri, and Lang

The question is how to generalize Mordell's conjecture to higher dimensional varieties. A first hint is given by Lemma 5.2. During a lecture in 1980, Bombieri asked [**26**] the following:

Question 5.3 (Bombieri). *Let X be a smooth, projective variety of general type defined over $\mathbb{Q}$. Is there a non-empty Zariski-open set $U \subseteq X$ such that $U(\mathbb{Q}) = \emptyset$?*

Motivated by the Enriques-Kodaira classification and by a theorem of Bogomolov regarding curves of bounded genus in surfaces of general type, Bombieri expects a positive answer when X is a surface. Lang [**21**] proposed the following daring conjecture often referred to as the **Bombieri-Lang conjecture** to distinguish it from other conjectures of Lang:

Conjecture 5.4 (Lang's conjecture; "Bombieri-Lang"). *Let X be a smooth, projective variety of general type defined over $\mathbb{Q}$. There is a proper Zariski closed subset $Z \subseteq X$ such that $(X - Z)(\mathbb{Q})$ is finite.*

There is yet another way to generalize Mordell's conjecture. A compact complex manifold M is called **hyperbolic** if every complex holomorphic map $f : \mathbb{C} \to M$ is constant. For instance, it is a theorem of Picard that the hyperbolic compact Riemann surfaces are precisely those of genus $g \geq 2$. In view of Mordell's conjecture, this suggests:

Conjecture 5.5 (Lang [**21**]). *Let X be a smooth projective irreducible variety over $\mathbb{Q}$. Suppose that $X(\mathbb{C})$ is hyperbolic. Then for every number field L we have that $X(L)$ is finite.*

The aforementioned results of Faltings [**13, 14**] prove Conjectures 5.4 and 5.5 when X is contained in an abelian variety. Up to cases that can be reduced to this one, Faltings's results are all we know unconditionally about these conjectures as of today.

While we are enthusiastic about sparsity of rational points, in all fairness, we must point out that there are some doubts about the Bombieri-Lang conjecture for varieties of higher dimension. First, even the geometric picture is unclear and, at present, there is no analogue of the Enriques-Kodaira classification for higher dimensional varieties. Moreover, the Bombieri-Lang conjecture applied to higher dimensional varieties has rather strong and surprising consequences, such as the following uniform version of Mordell's conjecture:

Theorem 5.6 (cf. [**4**]). *If Conjecture 5.4 holds, then for each $g \geq 2$ there is a constant $M(g)$ such that for every smooth, projective, geometrically irreducible curve X of genus $g \geq 2$ over $\mathbb{Q}$ we have $\#X(\mathbb{Q}) \leq M(g)$.*

4. Büchi's problem

We would like to conclude by discussing a concrete and classical-looking problem which has been very useful for testing the results and conjectures we have presented so far.

Notice that for a sequence of squares of consecutive integers, the second differences are always $2, 2, ..., 2$. For instance

1		0		1		4		9
	-1		1		3		5	
		2		2		2		

Examples of this sort will be called **trivial**. Are there examples with non-trivial sequences of squares with second differences equal to $2, ..., 2$? Yes, such as

0		49		100
	49		51	
		2		

and

6^2		23^2		32^2		39^2
	493		495		497	
		2		2		

Motivated by a problem in logic, Büchi proposed the following problem in the early 70's:

Problem 5.7 (Büchi's problem). *Is there some constant M such that every sequence of integer squares $x_1^2, ..., x_M^2$ having second differences equal to $2, ..., 2$ is necessarily trivial?*

In fact, Büchi asked for the value $M = 5$, but any uniform value of M would suffice for the intended applications in logic. More precisely, Büchi proved the following (see [**23, 24**]):

Theorem 5.8. *If Büchi's Problem 5.7 has a positive answer for some M, then there is no algorithm for deciding existence of integer solutions for systems of diagonal quadratic equations of the form $a_1x_1^2 + ... + a_mx_m^2 = b$ with $a_j, b \in \mathbb{Z}$.*

In the 90's, Vojta proved (cf. [**24, 35**]) that a positive solution to Büchi's problem would follow from the Bombieri-Lang conjecture for surfaces.

Basically, Vojta considers certain algebraic surfaces X_n attached to the problem, and upon invoking the Bombieri-Lang conjecture, the problem becomes that of computing the exceptional Zariski closed set $Z \subseteq X_n$ containing all but finitely many rational points. Since X_n is a surface, Z consists of finitely many curves. Vojta's computation of Z involved a study of symmetric differentials on surfaces. This approach originates in ideas of Bogomolov [**10**] and it has been generalized and applied to other elementary-looking Diophantine problems by Garcia-Fritz [**15, 16, 17**], such as the Perfect Cuboid Problem and Mohanty's conjecture.

The result we would like to prove is

Theorem 5.9. *Suppose that there is a bound B such that every smooth projective curve C over $\mathbb{Q}$ of genus $g = 2$ has $\#C(\mathbb{Q}) \leq B$ (in particular, this would hold if the Bombieri-Lang conjecture holds, see Theorem 5.6). Then Büchi's Problem 5.7 has a positive answer with $M = (B + 1)^3 + 1$.*

Proof. It suffices to show that given $a, b \in \mathbb{Z}$ with $a \neq 0$, not all the integers $(j + b)^2 - a$ for $j = 1, ..., M$ are squares. For the sake of contradiction, assume they are.

The polynomials $f_1(x) = (x^3 + b)^2 - a$ and $f_2(x) = (x^3 + 1 + b)^2 - a$ have discriminants $46656a^3(a - b^2)^2$ and $46656a^3(a - (b + 1)^2)^2$ respectively. As $a \neq 0$, at least one of them is non-zero. Thus, at least one of the two equations

$$y^2 = f_1(x), \quad y^2 = f_2(x)$$

defines a smooth hyperelliptic curve; let us call it C. It has genus $g = \lfloor (6-1)/2 \rfloor = 2$. Thus, $\#C(\mathbb{Q}) \leq B$.

Choosing $j = x^3$ or $j = x^3 + 1$ accordingly, with $x = 1, 2, ..., B+1$ we obtain at least $B+1$ rational points on C because $(j+b)^2 - a$ is a square for each $j = 1, ..., M$. Contradiction. $\square$

For a more general application of these ideas, see [**29**]. Büchi's problem would also follow from the *abc* conjecture, see [**27**].

Bibliography

[1] J. Aguirre, A. Lozano-Robledo, J. Peral, Elliptic curves of maximal rank. Proceedings of the"Segundas Jornadas de Teoría de Números", 1-28, Bibl. Rev. Mat. Iberoamericana, Rev. Mat. Iberoamericana, Madrid, 2008.

[2] A. Beauville, *Complex algebraic surfaces.* London Mathematical Society Student Texts, 34 (2nd ed.), Cambridge University Press (1996)

[3] E. Bombieri, *The Mordell conjecture revisited.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 17 (1990), no. 4, 615-640.

[4] L. Caporaso, J. Harris, B. Mazur, *Uniformity of rational points.* J. Amer. Math. Soc. 10 (1997), no. 1, 1-35.

[5] J. Caro, H. Pasten, *A Chabauty-Coleman bound for surfaces.* Preprint arXiv:2102.01055

[6] J. Caro, H. Pasten, *Watkins's conjecture for elliptic curves with non-split multiplicative reduction.* Preprint 2021.

[7] R. Coleman, *Effective Chabauty.* Duke Math. J. 52 (1985), no. 3, 765-770.

[8] G. Cornell, J. Silverman (Eds.), *Arithmetic geometry.* Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30-August 10, 1984. Edited by Gary Cornell and Joseph H. Silverman. Springer-Verlag, New York, 1986. xvi+353 pp. ISBN: 0-387-96311-1

[9] P. Corvaja, U. Zannier, *A subspace theorem approach to integral points on curves*, C. R. Math. Acad. Sci. Paris 334 (2002), 267-271.

[10] M. Deschamps, *Courbes de genre géométrique borné sur une surface de type général (d'après F. A. Bogomolov).* Séminaire Bourbaki 30e année, 1977/78, Lecture Notes in Mathematics 710, Springer, 1978, No. 519.

[11] B. Edixhoven, J.-H. Evertse, *Diophantine Approximation and Abelian Varieties, Introductory Lectures.* LNM 1566, Springer Verlag, 1993.

[12] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* (German) [Finiteness theorems for abelian varieties over number fields] Invent. Math. 73 (1983), no. 3, 349-366.

[13] G. Faltings, *Diophantine approximation on abelian varieties.* Ann. Math., 133 (1991), 549-576.

[14] G. Faltings, *The general case of S. Lang's conjecture.* Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991). Perspect. Math. 15. Academic Press. San Diego. 1994. p. 175-182

[15] N. Garcia-Fritz, *Curves of low genus on surfaces and applications to Diophantine problems.* PhD Thesis, Queen's University, 2015.

[16] N. Garcia-Fritz, *Sequences of powers with second differences equal to two and hyperbolicity.* Trans. Am. Math. Soc. 370(5), 3441-3466 (2018)

[17] N. Garcia-Fritz, *Quadratic sequences of powers and Mohanty's conjecture.* International Journal of Number Theory 14.02 (2018), 479-507.

[18] R. Hartshorne. *Algebraic geometry.* Graduate texts in Math. vol. 52., Springer Science & Business Media, 2013.

[19] X.-H. Hua, C.-C. Yang *Unique polynomials of entire and meromorphic functions.* Mat. Fiz. Anal. Geom., 1997, Volume 4, Number 3, 391-398.

[20] M. Kim, *The motivic fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$ *and the theorem of Siegel.* Inventiones Mathematicae, 161, (2005) 629-656.

[21] S. Lang, *Hyperbolic and Diophantine analysis.* Bull. Amer. Math. Soc. (N.S.) 14 (1986), no. 2, 159-205.

[22] B. Lawrence, A. Venkatesh, *Diophantine problems and p-adic period mappings.* (English summary) Invent. Math. 221 (2020), no. 3, 893-999.

[23] L. Lipshitz. *Quadratic forms, the five square problem, and diophantine equations.* In Collected Works of J. Richard Büchi. Edited by Saunders Mac Lane and Dirk Siefkes. Springer, New York (1990)

[24] B. Mazur, *Questions of decidability and undecidability in number theory.* The Journal of Symbolic Logic Vol. 59, No. 2 (Jun., 1994), pp. 353-371.

[25] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.* Proc. Camb. Phil. Soc. 21. pp. 179-192. (1922)

[26] J. Noguchi, *A higher-dimensional analogue of Mordell's conjecture over function fields.* Math. Ann. 258 (1981/82), no. 2, 207-212.

[27] H. Pasten, *Powerful values of polynomials and a conjecture of Vojta.* Journal of Number Theory, 133 (2013), no. 9, 2964-2998.

[28] H. Pasten, *Bivariate polynomial injections and elliptic curves.* Selecta Math. (N.S.) 26 (2020), no. 2, Paper No. 22, 13 pp

[29] H. Pasten, X. Vidaux, *Positive existential definability of multiplication from addition and the range of a polynomial.* Israel Journal of Mathematics, 216 (2016), no. 1, 273-306.

[30] G. Rémond, *Décompte dans une conjecture de Lang.* Invent. Math. 142 (2000), no. 3, 513-545.

[31] K. Roth, *Rational approximations to algebraic numbers.* Mathematika 2 (1955), 1-20; corrigendum, 168.

[32] W. Schmidt. *Norm form equations.* Annals of Mathematics. Second Series. 96 (3): 526-551. (1972)

[33] T. N. Shorey, *Approximations of algebraic numbers by rationals: A theorem of Thue.* Elliptic curves, modular forms and cryptography (Allahabad, 2000), 119-137, Hindustan Book Agency, New Delhi, 2003.

[34] P. Vojta, *Siegel's theorem in the compact case.* Ann. Math., 1991, p. 509-548.

[35] P. Vojta, *Diagonal quadratic forms and Hilbert's tenth problem.* Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 261-274, Contemp. Math., 270, Amer. Math. Soc., Providence, RI, 2000.