Irrationality of $\sqrt{2}$ and Arakelov Geometry

Jürg Kramer and Anna-Maria von Pippich

Summary of a talk given by the first named author at the occasion of a visit to the Indian Institute of Technology at Madras on August 17, 2010, as a member of a delegation of the German Science Foundation (DFG)

1 Introduction

We begin our exposition with the well-known example of the proof of the irrationality of $\sqrt{2}$ using a descent argument going back to Fermat. We assume that $\sqrt{2}$ is rational, so $\sqrt{2} = x/y$ with non-zero integers $x, y \in \mathbb{Z}_{\neq 0}$. Squaring both sides and clearing denominators yields $x^2 = 2y^2$, which shows that x^2 is even. But $2|x^2$ implies $2|x$, hence there exists $x_1 \in \mathbb{Z}_{\neq 0}$ with $x = 2x_1$. Substituting, we get $y^2 = 2x_1^2$, whence y^2 is even. But $2|y^2$ implies $2|y$, hence there exists $y_1 \in \mathbb{Z}_{\neq 0}$ with $y = 2y_1$. Substituting again, we find $x_1^2 = 2y_1^2$. In summary, this proves the following implication:

$$\exists\, x, y \in \mathbb{Z}_{\neq 0} : x^2 = 2y^2 \implies \exists\, x_1, y_1 \in \mathbb{Z}_{\neq 0} : x_1^2 = 2y_1^2 \text{ and } |x_1| < |x|,\ |y_1| < |y|.$$

From this it is evident that we can produce infinitely many non-zero integral solutions of the polynomial equation $X^2 = 2Y^2$, which become smaller and smaller in size. Of course, because of the discrete nature of the integers, this is not possible, which proves, by contradiction, that the equation $X^2 = 2Y^2$ has no non-zero integral solutions, whence $\sqrt{2} \notin \mathbb{Q}$.

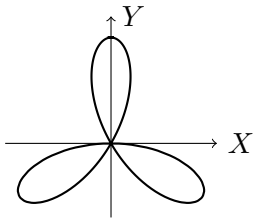
In general, we are faced with the following problem: Given a polynomial $P = P(X_1, \ldots, X_n)$ with integral or rational coefficients in the n variables $X_1, \ldots, X_n$ or, more generally, a system of such polynomials, we may ask the two questions:

(A) Is there a rational zero for the polynomial P, i.e., does there exist $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ such that $P(x_1, \ldots, x_n) = 0$?

and, in case the answer to question (A) is affirmative,

(B) Are there finitely many or infinitely many such rational solutions?

In general, it is very difficult to answer questions (A) and (B). In the next two sections, we will restrict ourselves to studying the case of two variables, i.e., we will investigate questions (A) and (B) for polynomials $P(X, Y) \in \mathbb{Z}[X, Y]$. The equation $P(X, Y) = 0$ then defines an affine (or projective) curve C in the affine (or projective) X, Y-plane.



$$P(X,Y) = (X^2+Y^2)^2 - 3X^2Y - Y^3$$

Question (A) now asks whether the set $C(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 \,|\, P(x,y) = 0\}$ of rational points on the curve C is empty or not, and question (B) asks, whether the set $C(\mathbb{Q})$ is finite or infinite.

2 Rational points on plane curves

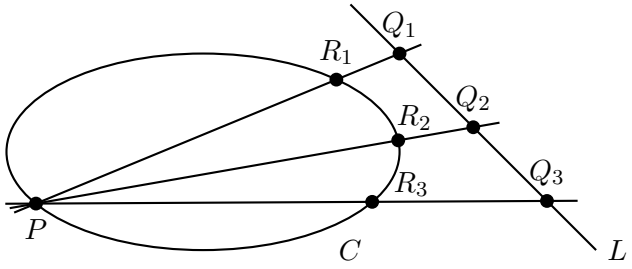
In this section we investigate questions (A) and (B) for plane curves C which are defined by an absolutely irreducible polynomial $P(X,Y) \in \mathbb{Z}[X,Y]$ of degree d. Without loss of generality, we may assume that the curves under consideration are smooth and projective.

If $d = 1$, the polynomial is of the form $P(X,Y) = aX + bY + c$ with $a, b, c \in \mathbb{Z}$; without loss of generality, we may assume $a \neq 0$. The polynomial then defines a straight line C with rational slope. The set of rational points on C is given by

$$C(\mathbb{Q}) = \big\{\big(-(b\lambda + c)/a, \lambda\big) \,\big|\, \lambda \in \mathbb{Q}\big\},$$

which shows that there exist always infinitely many rational points in case $d = 1$.

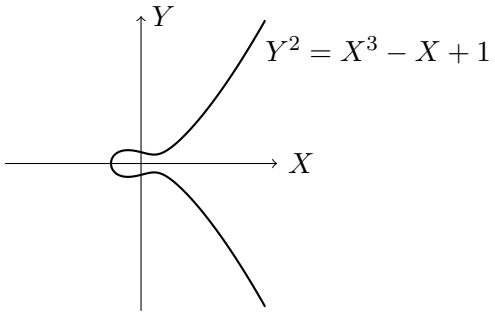
If $d = 2$, we may assume without loss of generality that $P(X,Y) = aX^2 + bY^2 + c$ with $a, b, c \in \mathbb{Z}$ and $a \neq 0$. The curve C defined by $P(X,Y) = 0$ is a quadric. Such curves might have no rational point as the example $P(X,Y) = X^2 + Y^2 - 3$ shows. However, question (A) can be effectively decided using the Hasse-Minkowski Theorem, which states that set $C(\mathbb{Q})$ is non-empty if and only if the equation $P(X,Y) = 0$ has solutions in the p-adic rational numbers $\mathbb{Q}_p$ for each prime p (including the archimedean prime $p = \infty$). This is the first instance of a so-called "local-global principle", nowadays a fundamental technique in arithmetic geometry. However, if $C(\mathbb{Q})$ is non-empty, that is, if there exists a rational point $P \in C(\mathbb{Q})$, then $C(\mathbb{Q})$ is always infinite as the following argument shows: We choose a straight line L with rational slope so that L admits infinitely many rational points $Q_j \in L$ $(j = 1, 2, 3, \dots)$. The line through P and Q_j (which has obviously rational slope) intersects the curve C in a point R_j $(j = 1, 2, 3, \dots)$, which can be shown to be rational using Vieta's theorem. Hence, the curve C has infinitely many rational points.



If $d > 3$, the curve C defined by $P(X, Y) = 0$ is a quartic, quintic, etc. The theorem of Faltings (see [4]), formerly known as Mordell's conjecture, then shows, in contrast to the case $d < 3$, that the set $C(\mathbb{Q})$ of rational points on C is always finite.

3 Rational points on elliptic curves

This section is devoted to studying the remaining case $d = 3$. As for $d = 2$, the set $C(\mathbb{Q})$ may be empty, however this time the answer to question (A) is more involved, since there is no "local-global principle" in this situation. For example the cubical equation $3X^3 + 4Y^3 + 5 = 0$ has no rational solution, but for every prime p it has solutions in $\mathbb{Q}_p$. To investigate question (B), we suppose that the curve C admits at least one rational point. We choose this point to be the "point at infinity" and we may assume without loss of generality that the curve is given in Weierstraß normal form, i.e., it is defined by $P(X, Y) = Y^2 - X^3 - aX^2 - bX - c$ with $a, b, c \in \mathbb{Z}$. If C is smooth, then C is called an *elliptic curve*.



We first note that the set $C(\mathbb{Q})$ has the structure of an abelian group. The sum $P + Q$ of two points $P, Q \in C(\mathbb{Q})$ is given by the following rational point: The line joining P and Q has rational slope and intersects the elliptic curve C in a third rational point R. Reflecting R about the X-axis yields the desired point $P+Q \in C(\mathbb{Q})$. The main result of this section states that the abelian group $\big(C(\mathbb{Q}), +\big)$ of rational points on an elliptic curve is finitely generated. In order to prove this result, we need the following crucial lemma mimicking Fermat's descent argument for the proof of the irrationality of $\sqrt{2}$ presented in section1.

Descent lemma. Let G be an abelian group satisfying $|G/2G| < \infty$. Then, G is finitely generated, provided that there is a "height function" $h : G \to \mathbb{R}$ having the following properties:

(i) For all $c \in \mathbb{R}$, we have $\#\{x \in G \,|\, h(x) \leq c\} < \infty$.

(ii) For every $x_0 \in G$, there is a constant $c_0 = c(x_0) > 0$ such that $h(x+x_0) \leq 2h(x)+c_0$.

(iii) There is a constant $c_1 > 0$ such that $h(2x) \geq 4h(x) - c_1$.

Sketch of proof: Let $\mathcal{R} = \{x_1, \ldots, x_m\} \subseteq G$ be a complete set of representatives of the cosets of G mod $2G$. Now, for arbitrary $x \in G$, there exist $x_{i_1} \in \mathcal{R}$ and $y_1 \in G$ with $x = x_{i_1}+2\cdot y_1$. Iterating this process, we find after n steps that $x = d_1\cdot x_1+\ldots+d_m\cdot x_m+2^n\cdot y_n$

with integers $d_j \in \mathbb{Z}$. Using properties (ii), (iii), we find that $h(y_n) \sim 4^{-n} \cdot h(x) < 1$ for n sufficiently large. The claim now follows using property (i). $\square$

In order to prove the finite generatedness of $C(\mathbb{Q})$, we apply the descent lemma. We have to show that $C(\mathbb{Q})/2C(\mathbb{Q})$ is finite. Furthermore, we have to show that the function $h : C(\mathbb{Q}) \to \mathbb{R}$, given by

$$(x, y) \mapsto \max\big\{ \log|N(x)|, \log|D(x)| \big\},$$

where $N(x)$ denotes the numerator and $D(x)$ the denominator of x, defines a height function on $C(\mathbb{Q})$. This can be done with not too much effort, and we arrive at

Theorem (Mordell [7]). The group $C(\mathbb{Q})$ of rational points on an elliptic curve C defined over $\mathbb{Q}$ is finitely generated, i.e., we have $C(\mathbb{Q}) \cong \mathbb{Z}^{r_C} \oplus C(\mathbb{Q})_{\mathrm{tor}}$ with $r_C \in \mathbb{N}$, the rank of C, and $C(\mathbb{Q})_{\mathrm{tor}}$ the torsion part of C.

For example, we have $C(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ for C given by $Y^2 = X^3 + 4X$, and $C(\mathbb{Q}) \cong \mathbb{Z}$ for C given by $Y^2 = X^3 + X + 1$.

4 Weil heights

In this section we generalize the notion of a "height function", which occurred in the previous section in the context of rational points on elliptic curves. We emphasize that the height of a rational point should be seen as a tool which measures the arithmetic complexity of the rational point. We start by looking at rational points $x = (x_0 : \ldots : x_n)$ in projective space $\mathbb{P}^n(\mathbb{Q})$ and define the *Weil height*, respectively *logarithmic Weil height*, of x by

$$H(x) := \max\big\{|x_0|, \ldots, |x_n|\big\}, \text{ respectively } h(x) := \max\big\{ \log|x_0|, \ldots, \log|x_n| \big\}.$$

More generally, if $X/\mathbb{Q}$ is a projective variety, i.e., the variety X is defined over $\mathbb{Q}$ and there is an embedding $\varphi : X \hookrightarrow \mathbb{P}^n$ also defined over $\mathbb{Q}$, and $x \in X(\mathbb{Q})$, then the *logarithmic Weil height* of x is given by

$$h_\varphi(x) := h\big(\varphi(x)\big).$$

Of course, we note that the latter definition depends on the choice of an embedding of X into $\mathbb{P}^n$. However, one can show that if ψ is another projective embedding, then the difference $|h_\varphi(x) - h_\psi(x)|$ is bounded for $x \in X(\mathbb{Q})$, in short

$$h_\varphi - h_\psi = O(1) \text{ on } X(\mathbb{Q}).$$

We note that the definition of the (logarithmic) Weil height and the above mentioned consequences can be carried over to points $x \in X(\overline{\mathbb{Q}})$, where X is a projective variety defined over a number field. Another aspect to be mentioned is the following: Since the logarithmic Weil height only makes sense up to functions which are bounded on $X(\overline{\mathbb{Q}})$, and since it is equivalent to giving projective embeddings φ for X or a very ample line bundle L on X, we allow ourselves to write h_L instead of h_φ. The second statement of the subsequent theorem allows us to generalize this definition to any line bundle on X.

Theorem "height machine" (Weil). Let $f : Y \longrightarrow X$ be a morphism of projective varieties defined over $\overline{\mathbb{Q}}$ and let L, M be line bundles on X. Then, we have the following statements:

(i) For all $c \in \mathbb{R}$, we have $\#\{x \in X(\overline{\mathbb{Q}}) \mid \deg(x) \leq c,\, h_L(x) \leq c\} < \infty$.

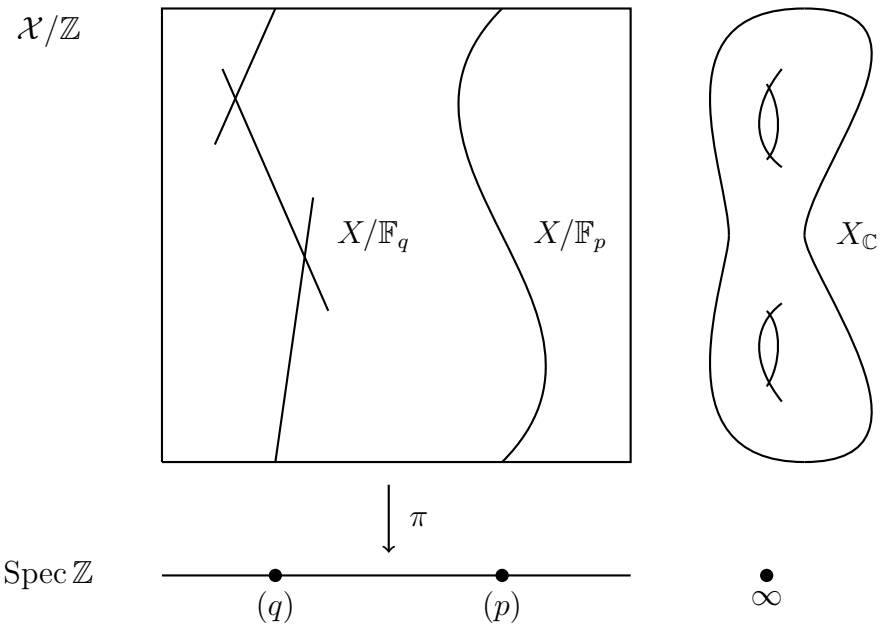
(ii) $h_{L\otimes M} = h_L + h_M + O(1)$ on $X(\overline{\mathbb{Q}})$.

(iii) $h_{f^*L} = h_L \circ f + O(1)$ on $X(\overline{\mathbb{Q}})$.

We end this section by mentioning that the above theorem plays an important role in Bombieri's elementarized proof of Mordell's conjecture, i.e., the theorem of Faltings; an excellent reference for this proof is the book of E. Bombieri and W. Gubler [1].

5 Arakelov geometry

In this section we want to generalize the notion of height for a rational point to higher dimensional subvarieties defined over $\mathbb{Q}$ or, more generally, over a number field, so-called algebraic cycles. For this we have to summarize the basics of Arakelov geometry as developed by H. Gillet and C. Soulé in [8]. We start with a smooth, projective variety $X/\mathbb{Q}$, for which we assume that it extends to a regular scheme $\mathcal{X}/\mathbb{Z}$, which is projective and flat over $\operatorname{Spec}\mathbb{Z}$. In general, this is a quite restrictive assumption; however, in the case of curves or abelian varieties one is always able to find such a regular model. By an arithmetic variety we mean a regular scheme $\mathcal{X}/\mathbb{Z}$ as above together with its associated complex manifold $X_{\mathbb{C}}$. In the case of a curve $X/\mathbb{Q}$, its associated arithmetic surface can be represented as shown in the figure below: the vertical fiber over a prime p is the reduction of the original curve modulo p, if the reduction is smooth, or a suitable desingularization of this reduction in case it is singular; the fiber over the point ∞ is the compact Riemann surface $X_{\mathbb{C}}$.



We denote by $\mathrm{Z}^p(\mathcal{X})$ the free abelian group generated by the p-codimensional, integral subvarieties $\mathcal{Z}$ of $\mathcal{X}$. The p-th Chow group $\mathrm{CH}^p(\mathcal{X})$ is then defined as the quotient of $\mathrm{Z}^p(\mathcal{X})$ modulo algebraic equivalence. Intersection theory on $\mathcal{X}$ asserts the validity of the intersection pairing

$$\mathrm{CH}^p(\mathcal{X}) \times \mathrm{CH}^q(\mathcal{X}) \longrightarrow \mathrm{CH}^{p+q}(\mathcal{X}) \otimes_{\mathbb{Z}} \mathbb{Q},$$

induced by the assignment $(\mathcal{Z}, \mathcal{W}) \mapsto \mathcal{Z} \cap \mathcal{W}$, provided that the cyles $\mathcal{Z}, \mathcal{W}$ intersect properly. We note that there are the "usual" functorialities such as push-forward maps and pull-back maps on the level of Chow groups with respect to flat and proper morphisms between arithmetic varieties, respectively. As an example, we note

$$\mathrm{CH}^0(\operatorname{Spec}\mathbb{Z}) \cong \mathbb{Z}.$$

So far we have not yet made use of the underlying analytical data. This will now be necessary for the definition of arithmetic Chow groups. To do this we start by defining $\widehat{\mathrm{Z}}^p(\mathcal{X})$ as the free abelian group generated by pairs $(\mathcal{Z}, g_{\mathcal{Z}})$, where $\mathcal{Z} \in \mathrm{Z}^p(\mathcal{X})$ and $g_{\mathcal{Z}}$ is a so-called Green's current, i.e., a current of type $(p-1, p-1)$ on $X_{\mathbb{C}}$ such that the current $\mathrm{d}\mathrm{d}^c g_{\mathcal{Z}} + \delta_{\mathcal{Z}}$ is a current arising from a smooth differential form of type (p,p) via integration. The p-th arithmetic Chow group $\widehat{\mathrm{CH}}^p(\mathcal{X})$ is now defined as the quotient of $\widehat{\mathrm{Z}}^p(\mathcal{X})$ by a suitable equivalence relation extending algebraic equivalence to the present setting. The main achievement of Arakelov geometry consists in extending geometric intersection theory to an arithmetic intersection pairing

$$\widehat{\mathrm{CH}}^p(\mathcal{X}) \times \widehat{\mathrm{CH}}^q(\mathcal{X}) \stackrel{\cdot}{\longrightarrow} \widehat{\mathrm{CH}}^{p+q}(\mathcal{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$$

with functorialities analogous to the geometric setting. As a useful example we mention the isomorphism

$$\widehat{\deg} : \widehat{\mathrm{CH}}^1(\operatorname{Spec}\mathbb{Z}) \stackrel{\cong}{\longrightarrow} \mathbb{R}.$$

For a p-codimensional cycle Z on a d-dimensional variety $X/\mathbb{Q}$, the height $h_L(Z)$ with respect to a line bundle L can now be defined via the formula

$$h_L(Z) := \widehat{\deg}\big(\pi_*\big(\widehat{\mathrm{c}}_1(\overline{\mathcal{L}})^{d+1-p} \cdot [\mathcal{Z}, g_{\mathcal{Z}}^{(H)}]\big)\big) \in \mathbb{R},$$

where $\mathcal{Z} \in \mathrm{Z}^p(\mathcal{X})$ and $\mathcal{L} \in \mathrm{Pic}(\mathcal{X})$ denote the extension of Z and L to $\mathcal{X}$, respectively; furthermore, $\pi : \mathcal{X} \to \operatorname{Spec}\mathbb{Z}$ denotes the structural morphism, $\overline{\mathcal{L}} = (\mathcal{L}, \|\cdot\|)$ refers to the line bundle $\mathcal{L}$ together with a smooth hermitian metric $\|\cdot\|$ on the holomorphic line bundle $L_{\mathbb{C}}$, and $\widehat{\mathrm{c}}_1(\overline{\mathcal{L}}) = [\operatorname{div}(s), -\log\|s\|^2] \in \widehat{\mathrm{CH}}^1(\mathcal{X})$ is the first arithmetic Chern class of $\overline{\mathcal{L}}$. We note that there is a distinguished choice $g_{\mathcal{Z}}^{(H)}$ for a Green's current characterized by some harmonicity conditions.

By means of the generalized height notion, one is able to prove a theorem which is analogous to the "height machine" mentioned above. It states, roughly speaking, that there are only finitely many cycles $Z \in \mathrm{Z}^p(X)$ defined over $\mathbb{Q}$ of bounded height. A striking application is the following generalization of Mordell's conjecture, namely a part of Lang's conjectures:

Theorem (Faltings [5]). Let $A/\mathbb{Q}$ be an abelian variety and X a closed, geometrically irreducible subvariety of A, which is not a translate of an abelian subvariety of A. Then, the intersection $X \cap A(\mathbb{Q})$ is not Zariski dense in X.

By the recent work of J. Burgos, J. Kramer, and U. Kühn (see [2, 3]), it has been made possible to extend the basic constructions of Arakelov geometry to the setting where the hermitian metrics $\|\cdot\|$ of the line bundles or, more generally, of the vector bundles under consideration allow logarithmic singularities along a fixed divisor. This is of particular interest in order to be able to apply Arakelov geometry to automorphic vector bundles on Shimura varieties of non-compact type. Also in this setting an analogue of the "height machine" has been established in the thesis of G. Freixas i Montplet [6]; in fact, for the case of points such a result has been anticipated in G. Faltings' proof of Mordell's conjecture.

References

[1] E. Bombieri, W. Gubler: *Heights in Diophantine Geometry*. New Mathematical Monographs. Cambridge University Press, Cambridge, 2006.

[2] J. I. Burgos Gil, J. Kramer, U. Kühn: *Arithmetic characteristic classes of automorphic vector bundles*. Doc. Math. 10 (2005), 619–716.

[3] J. I. Burgos Gil, J. Kramer, U. Kühn: *Cohomological arithmetic Chow rings*. J. Inst. Math. Jussieu 6 (2007), 1–172.

[4] G. Faltings: *Endlichkeitssätze für abelsche Varietäten*. Invent. Math. 73 (1983), 349–366.

[5] 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, CA, 1994, 175–182.

[6] G. Freixas i Montplet: *Heights and metrics with logarithmic singularities*. J. Reine Angew. Math. 627 (2009), 97–153.

[7] L.J. Mordell: *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc. Cambridge Philos. Soc. 21 (1922), 179–192.

[8] C. Soulé, D. Abramovich, J.-F. Burnol, J. Kramer: *Lectures on Arakelov geometry*. Cambridge Studies in Advanced Mathematics 33. Cambridge University Press, Cambridge, 1992 & 1994.

Jürg Kramer
Institut für Mathematik
Humboldt-Universität zu Berlin
Unter den Linden 6
D-10099 Berlin
e-mail: kramer@math.hu-berlin.de

Anna-Maria von Pippich
Departement Mathematik
Universität Basel
Rheinsprung 21
CH-4051 Basel
e-mail: anna.vonpippich@unibas.ch