Integral points on $\mathbb{P}^1 \setminus \{f(u,v)=0\}$ following Skolem

Nils Bruin

1. Introduction

In these notes, we will be concerned with the problem of finding the set of rational points on projective curves. Oddly enough, it is instructive to realize that this is the same as determining the *integral* points on a projective curve over $\mathbb{Z}$. In order to see this, one should realize that, for any ring R, we have

$$\mathbb{P}^n(R) = \{(a_0, \ldots, a_n) : a_i \in R \text{ and not all } 0\}/\sim$$

where $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ if the two are linearly dependent over R, i.e., there exist $\lambda, \mu \in R$ such that $\lambda a_i = \mu b_i$ for $i = 0, \ldots, n$.

In particular, by clearing denominators, one sees that $\mathbb{P}^n(\mathbb{Q}) = \mathbb{P}^n(\mathbb{Z})$. Thus, finding *rational* points is the same as finding *integral* points on projective varieties.

Thanks to Baker's explicit results on linear forms in logarithms, finding the integral points on affine curves in general can be done effectively. In these lectures, however, we will discuss some ineffective methods for this as well, going back to Skolem. These methods are not generally applicable and even when they are, there is no proof that they really work (although there are some pretty good heuristic reasons why we should expect them to). If they do work, however, the obtained proof is much easier to check and much more satisfying than one based on effective bounds. There is an additional benefit: Once we have the appropriate dictionary in place, the methods we will discuss will carry over directly between affine and projective curves.

2. $\mathbb{P}^1$ minus points

Consider the affine curve:

$$x^2y - xy^2 + 3xy + 1 = 0$$

What are the integral points on this curve? That's the points with integral x, y. In order to get a better grip on the geometry of this curve, consider the projective closure

$$C : X^2Y - XY^2 + 3XYZ + 1 = 0$$

This is a rational curve, as can be readily illustrated by the parametrization

$$\begin{array}{ccc} \mathbb{P}^1 & \to & C \\ (u:v) & \mapsto & (u^3 : v^3 : uv(u-v)) \end{array}$$

In order for $(u : v)$ to map to an *integral* point on C, we need that

$$\left(\frac{u^3}{uv(u-v)}, \frac{v^3}{uv(u-v)} \right)$$

is integral, which amounts to $f(u,v) = uv(u-v)$ taking a unit value (i.e., ± 1). Hence

$$(\mathbb{P}^1 \setminus \{f(u,v) = 0\})(\mathbb{Z})$$

consists of points represented by

$$\{(u:v) : u, v \in \mathbb{Z} \text{ and } f(u,v) \in \mathbb{Z}^*\}$$

In our example, $f(u,v) = uv(u-v)$ and indeed, the points $(1:0), (0:1), (1:1)$ get mapped to the line at infinity.

Thus, we see that if $f(u,v)$ is of degree 1, then

$$\mathbb{P}^1 \setminus \{f(u,v)=0\} \simeq \mathbb{A}^1,$$

modulo some subtleties about non-minimal models over $\mathbb{Z}$.

If $f(u,v)$ is of degree 2, then we are essentially solving an equation of the type $f_2u^2+f_1uv+f_0v^2=\pm 1$, i.e., a Pell-type equation. The solution set is empty or has the structure of a finitely generated group.

Remains the case of $f(u,v)$ of degree at least 3. Siegel's theorem gives that there are only finitely many integral points on $\mathbb{P}^1 \setminus \{f(u,v)=0\}$.

3. The trichotomy

As it turns out, the geometry of a curve has a profound influence on the nature of the set of integral points on the curve. There is a 3-way split, both for projective and for affine curves.

	Projective	Affine
"Rational"	Conics, $\mathbb{P}^1$	$\mathbb{A}^1$ ($\mathbb{P}^1$ minus one point)
"Group"	Genus 1, Elliptic curves	$\mathbb{P}^1$ minus 2 points
Hyperbolic	Higher genus curves	$\mathbb{P}^1$ minus at least 3 points, elliptic curves minus point.

In the rational case, there are either no integral points or infinitely many. Furthermore, the height of the points grows polynomially if one enumerates the points.

In the "Group" case, there are either no integral points or the points form a finitely generated abelian group (For elliptic curves, this is a theorem of Mordell (and Weil if we also include other base rings than $\mathbb{Z}$). For tori, this is a result of Dirichlet. The height of points grows exponentially.

In the "hyperbolic" case, there are only finitely many points. This is a result of Faltings for projective curves and of Siegel for affine curves.

There remains a central question: how do we find the set of rational points, in particular in the hyperbolic case?

4. Overview of the methods

Let's consider a hyperbolic curve C, either a projective or affine. We are interested in determining $C(\mathbb{Z})$. We will explain a couple of complimentary methods.

Method 0: Local solvability Once should always first test if $C(\mathbb{Z})$ is empty for an obvious reason, for instance because $C(\mathbb{Z}_p)$ or $C(\mathbb{R})$ is already empty. If this is the case, then we are easily done. Otherwise, if C does have points over all completions, then there are some consequences that will come in handy later.

The other methods are all based on the fact that a hyperbolic curve can be mapped into a semiabelian variety – a semidirect product of an algebraic torus (twist of $\mathbb{G}_m^n$) and an Abelian variety. We will consider the situation

$$C \to J$$

where J is either a torus or an abelian variety. In both cases (either by Dirichlet or by Mordell-Weil), the integral points of J form a finitely generated group.

Method 1: Mordell-Weil or Dirichlet Sieving This methods allows us, given a finite index subgroup $\Lambda \subset J(\mathbb{Z})$, to derive information on the image of $C(\mathbb{Z}) \to$

$J(\mathbb{Z})/\Lambda$, i.e., we can compute a list of cosets modulo Λ that might contain points from $C(\mathbb{Z})$. We cannot prove that we will always be able to exclude cosets that do not contain points from $C(\mathbb{Z})$ but a heuristic argument by Poonen does suggest that we should be able to.

Method 2: Skolem's method or Chabauty's method Provided that $J(\mathbb{Z})$ is of free rank strictly smaller than the dimension of J, this method uses p-adic analytic methods to provide a bound on the number of points from $C(\mathbb{Z})$ that can land in a coset $J(\mathbb{Z})/\Lambda_p$.

Method 3: Chevalley-Weil descent (unramified Galois covers) As you can see, Method2 has a restriction on rank. This is a very real restriction: The rank of J can easily be too high. One solution is to use a result by Chelley and Weil: If D/C is an unramified Galois cover of nonsingular curves then there is a finite extension k of $\mathbb{Q}$ such that $D(k)$ cover $C(\mathbb{Q})$. Furthermore, this extension is unramified outside the primes of bad reduction of D/C. This result can be formulated differently too: There exists a finite number of twists D_δ/C such that $\bigcup D_\delta(\mathbb{Q})$ covers $C(\mathbb{Q})$.

The dimension of the generalised Jacobians of D_δ are generally of higher dimension than of C. It is unknown if the ranks of these Jacobians tend to grow slower than their dimensions.

Method 4: Subcovers

This is a very simple observation that often alleviates the computational complexities introduced by Method 4: Given a cover D/E (ramified or not, galois or not(, if we can find the rational points on E then we can also find the rational points on D.

5. The generalized Jacobian of $\mathbb{P}^1 \setminus \{f(u,v) = 0\}$

First let's consider the simplest case of $\mathbb{P}^1 \setminus \{f(u,v) = 0\}$. We take $f(u,v) = uv(u-v)$, i.e., we remove the points $(0:1), (1:0), (1,1)$. Because we remove 3 points, we can now construct some functions that do not have poles or zeros! Given the functions

$$g_0 = \frac{u^3}{uv(u-v)},\ g_1 = \frac{(u-v)^3}{uv(u-v)},\ g_\infty = \frac{v^3}{uv(u-v)}$$

We have a map:

$$\begin{array}{ccc} \mathbb{P}^1 \setminus \{0,1,\infty\} & \to & \mathbb{G}_m^3 \\ (u:v) & \mapsto & (g_0(u,v), g_1(u,v), g_\infty(u,v)) \end{array}$$

Note that $g_0 g_1 g_\infty = 1$, so although the map is defined as a map into a 3-dimensional torus, we are really mapping into a 2-dimensional subtorus.

More generally, suppose that $f(u,v) = u^n + \cdots$, and consider $A = \mathbb{Q}[\theta] = Q[x]/f(x,1)$. If f is square-free then A is a direct product of number fields. We consider the torus obtained by taking the *Weil restriction* of $\mathbb{G}_m$ with respect to $A/\mathbb{Q}$. This means that we take $T = \mathbb{A}^n \setminus \{N_{A/\mathbb{Q}}(a_0 + \theta a_1 + \cdots \theta^{n-1} a_{n-1}) = 0\}$ with the group operation

$$(a_0, \ldots, a_{n-1}) \cdot (b_0, \ldots b_{n-1}) = (c_0, \ldots, c_{n-1})$$

given by

$$(a_0 + \cdots + a_{n-1}\theta^{n-1}) \cdot (b_0 + \cdots + b_{n-1}\theta^{n-1}) = (c_0 + \cdots + c_{n-1}\theta^{n-1})$$

i.e., we write out $\mathbb{G}_m$ with respect to a basis of A over $\mathbb{Q}$. As you can see $A^* = \mathbb{G}_m(A) = T(\mathbb{Q})$, so we can work with T as if it were A^*. Later on, we need that we can consider it as an n-dimensional variety over $\mathbb{Q}$, though. That is something you won't get from A.

Given a representative (u, v) on $\mathbb{P}^1 \setminus \{f(u, v) = 0\}$, we can get a point on T by taking $u - \theta v$, i.e.,

$$(a_0, a_1, \ldots, a_{n-1}) = (u, -v, 0, \ldots, 0)$$

Of course, this map is dependent on the representative chosen. We need to quotient out by $\mathbb{G}_m \subset T$, being the subtorus corresponding to points of the form $(a, 0, \ldots, 0)$. This gives us the generalised Jacobian $J = T/\mathbb{G}_m$ and we end up with the map I will denote by

$$\begin{array}{ccc} \mathbb{P}^1 \setminus \{f(u, v) = 0\} & \to & J \\ (u : v) & \mapsto & \text{“}u - \theta v\text{”} \end{array}$$

This map actually gives us an embedding and allows us to consider $\mathbb{P}^1 \setminus \{f(u, v) = 0\}$ as a subvariety of J. The way to think of $J(\mathbb{Q})$ is really just as $T(\mathbb{Q})$ modulo scalars, i.e., $A^*/\mathbb{Q}^*$.

6. A finitely generated subgroup

As we saw before, an *integral* point on $\mathbb{P}^1 \setminus \{f(u, v) = 0\}$ is a point $(u : v)$ that we can represent by integers u, v such that $f(u, v)$ is a unit in $\mathbb{Z}$. If $f(u, v) = N_{A/\mathbb{Q}}(u - \theta v)$ then that means that $u - \theta v$ must be (almost) a unit in the ring of integers of A, say $\mathcal{O}_A$ (which is just the direct product of rings of integers of the number fields that make up K. This is what we'll consider to be the integral points of J, so $J(\mathbb{Z}) \simeq \mathcal{O}_A^*/\mathbb{Q}^*$. Hence, we obtain a map

$$\mathbb{P}^1 \setminus \{f(u, v) = 0\} \to J(\mathbb{Z})$$

7. An example

Let us consider $f(u, v) = u^3 - 2v^3$, so essentially we are trying to solve the equation $u^3 - 2v^3 = \pm 1$. We know that the unit group of the algebraic integers of $A = \mathbb{Q}(\sqrt[3]{2})$ is $\langle -1, \theta \rangle$, where $\theta = \sqrt[3]{2}$.

Thus, we are looking at the mapping

$$\mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\} \to \langle -1, \theta \rangle / \mathbb{Z}^*$$

given by $(u, v) \mapsto u - \theta v$. Our problem translates into: Which units can be written in the form $u - \theta v$?

There's the obvious ones $1, -1, \theta - 1, 1 - \theta$, which gives rise to two integral points on $\mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\}$.

8. Information from reduction mod p

Let p be a prime such that $f(u,v) \mod p$ has good reduction, i.e., $f(u,v) \in \mathbb{F}_p[u,v]$ still has no repeated roots. Then we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{P}^1 \setminus \{u^3 - 2v^3\}(\mathbb{Z}) & \xrightarrow{u-\theta v} & J(\mathbb{Z}) \\ \downarrow & & \downarrow \rho_p \\ \mathbb{P}^1 \setminus \{u^3 - 2v^3\}(\mathbb{F}_p) & \xrightarrow{\alpha_p} & J_p(\mathbb{F}_p) \end{array}$$

where $J_p = J \otimes_{\mathbb{Z}} \mathbb{F}_p$. We define Λ_p by the exact sequence

$$0 \to \Lambda_p \to T(\mathbb{Z}) \to^{\rho_p} T_p(\mathbb{F}_p)$$

where ρ_p is a group homomorphism from a finitely generated abelian group to a finite group $J_p(\mathbb{F}_p)$, so Λ_p is some finite index subgroup of $J(\mathbb{Z})$.

We know that $\mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\}(\mathbb{Z})$ lands inside $\mathrm{im}(\alpha_p) \cap \mathrm{im}(\rho_p)$, so computing this intersection gives us the cosets in $J(\mathbb{Z})$ modulo Λ_p that may contain points from $\mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\}(\mathbb{Z})$. For $p = 5$ we obtain:

n	$(\theta-1)^n$
0	1
1	$\theta + 4$
2	$\theta^2 + 3\theta + 1$
3	$2\theta^2 + 3\theta + 1$
4	$\theta^2 + 3\theta + 3$
5	$2\theta^2 + 4$
6	$3\theta^2 + 4\theta$
7	$\theta^2 + \theta + 1$
8	1

Thus, we see that $\Lambda_5 = \langle(\theta-1)^8\rangle$ if $(u:v) \in \mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\}(\mathbb{Z})$ then $u - \theta v = \pm(\theta-1)^{8n}$ or $u - \theta v = \pm(\theta-1)(\theta-1)^{8n}$

9. Dirichlet sieving (method 1)

In general, one should not expect to get sharp results from a single prime p. However, we can combine results from distinct primes! For instance, if we look at $p = 11$, we obtain that if $u - \theta v = \pm(1-\theta)^n$ then $n \in \{0, 1, 14, 19\} + 40\mathbb{Z}$. On the other hand, from $p = 17$ we obtain $n \in \{0, 1, 44, 64, 81\} + 96\mathbb{Z}$ Combining these two together, we see that the first yields $n \in \{0, 1, 6, 3\}+8\mathbb{Z}$ and the second yields $n \in \{0, 1, 4, 0, 1\}+8\mathbb{Z}$.

10. Skolem's method (method 2)

Let's assume that Dirichlet sieving always works. Then, given any finite index subgroup $\Lambda \subset J(\mathbb{Z})$, we can determine the residue classes in $J(\mathbb{Z})/\Lambda$ that contain images of integral points. In order to establish finiteness, we have to be able to give an upper bound of the number of integral points that land in a residue class. We describe the problem in the following way:

Let $P_0(u_0 : v_0)$ be an integral point on $\mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\}(\mathbb{Z})$ Can there be another integral point $P_t(u : v)$ that reduces to the same point at P_t modulo p? We

formulate this p-adically and require the looser requirement, is there another point in $\mathbb{P}^1 \setminus \{u^3 - 2v^3 = 0\}(\mathbb{Z}_p)$ that reduces to P_0 and lands in $J(\mathbb{Z})$?

If we're working over $\mathbb{Z}_p$, then WLOG $(u_0 : v_0) = (u_0 : 1)$ or $(u_0 : v_0) = (1 : v_0)$ and a point that reduces to $(u_0 : v_0)$ is necessarily of the form $(u_0 + pt : 1)$ or $(1 : v_0 + pt)$ for some $t \in \mathbb{Z}_p$. So, we're asking if $(u_0 + pt : 1) = \pm(\theta - 1)^n$.

For $p = 5$ and $(u_0 : v_0) = (1 : 1)$ we see that $n = 1 + 8N$, so we obtain

$$1 + 5t - \theta = (1 - \theta) \cdot (\theta - 1)^{8N}$$

i.e.,

$$1 + 5(\theta^2 + \theta + 1)t = (-80\theta^2 + 100\theta + 1)^N$$

Note that both sides are close to 1 (they are congruent to 1 modulo 5. We can use

$$\mathrm{Log}(1 + z) = 1 - z + z^2/2 - z^3/3 + z^4/4 - z^5/5 + \cdots$$

which converges for $z \in 5\mathbb{Z}_5$.In fact, if $z \in 5\mathbb{Z}_5$ then

$$\mathrm{Log}(1 + z) \equiv 1 - z + z^2/2 \mod 5^3$$

so we find:

$$(-100\theta^2 - 50\theta + 0)t^2 + (5\theta^2 + 5\theta + 5)t \equiv N(45\theta^2 + 75\theta) \mod 5^3$$

Looking at this modulo 5^2, we see that we need

$$5t\theta^2 + 5t\theta + 5t \equiv N(20\theta^2 + 0\theta + 0) \mod 5^2$$

So, we see that if we have

$$a_0\theta^2 + a_1\theta + a_2 \equiv N(20\theta^2 + 0\theta + 0) \mod 5^2$$

we are going to have $a_2 = a_1 = 5a_0 \mod 5^2$, so we would get $5t \equiv 0 \mod 5^2$. In general, we see that $\mathrm{Log}(5(\theta^2 + \theta + 1)t$ would give rise to

$$H_2(t)\theta^2 + H_1(t)\theta + H_0(t) = N(u_2\theta^2 + u_1\theta + u_0)$$

where $h_i(t) \in \mathbb{Z}_p[[t]]$ and the $u_i \in \mathbb{Z}_p$. Eliminating N yields some power series equation

$$H(t) = u_1H_2(t) - u_2H_1(t) = 0$$

or similar.

Theorem (Strassman) Given a power series $h_0 + h_1t + h_2t^2 + \cdots = H(t) \in \mathbb{Z}_p[[t]]$ such that $\mathrm{ord}_p(h_i) > \mathrm{ord}_p(h_n)$ for all $i > n$ then $H(t)$ has at most n zeroes in $\mathbb{Z}_p$.

By this theorem, we see that the only value for $t \in \mathbb{Z}_5$ that works is indeed $t = 0$.