Counting curves and their rational points

Spelier, P.

Summary

A major focus of mathematics throughout the millennia has been studying the solutions of equations. For example, in roughly 1800BC the Babylonians [BPS11] studied integer solutions of

$$x^2 + y^2 = z^2,$$

now known as Pythagorean triplets. There are of course many, many examples of equations: one can consider the equation

$$y = x^2$$

whose solutions form a parabola, or $xy = z$, whose solutions give a surface in a 3-dimensional space. Or

$$y^2 = x^3 + x,$$

which gives a so-called elliptic curve, a concept originally from the 19th century that forms the basis of a large part of modern cryptography [Mil86, Kob87], and has many ties to number theory [Sil94, Sil09].

In this thesis we consider curves, *algebraic curves* to be precise. These are one-dimensional geometric objects given by polynomial equations. The study of spaces given by polynomial equations is called algebraic geometry, precisely because it combines the languages of algebra and geometry. Algebraically we have equations, whose set of solutions we interpret as geometric objects called *varieties*; algebraically we have solutions, which geometrically we see as points on the variety. For example, the equation $y = x^2$ corresponds to the parabola, a special case of a variety, and the solution $9 = 3^2$ corresponds to the point $(3, 9)$ on the parabola. For an introductory reference to algebraic curves, see for example [Sil09, Chapters 1-2].

We study two problems about curves. First of them, is *counting curves*, part of a field called *enumerative geometry*. The aim of this field is to count curves satisfying certain properties, such as curves passing through a fixed set of points. For example, there is a unique line through two points in the plane, and there is a unique conic (a curve given by a degree 2 polynomial equation in x and y) passing through five points in the plane. And there are exactly twelve cubics (a curve given by a degree 3 polynomial equation in x and y) that have one point of self-intersection and pass through eight points in the plane. This subject turns out to have deep connections to physics and to systems of partial differential equations [DZ01, BR21]. A general introduction to the subject can be read in [KV07] or [Vak08].

The second problem is actually solving the equations, that is, finding all points on the curve. We are interested in finding the rational points, i.e. the points with coordinates in $\mathbb{Q}$. This problem is a special instance of the very broad class of *diophantine* equations. Under some conditions on the curve, there are only finitely many rational points, but provably finding them all is a difficult task. Some introductory references to the subject can be found in [MP12, BM20, BDM$^+$21].

The following two sections of the summary deal with these two subjects. They are intended to be self-contained.

Counting curves

We first delve into a specific case, namely the case of a conic passing through 5 points in the plane. For any 5 points, there is a unique conic passing through them. Consider for example that we pick our five points to be

$$S_t = \{(1,t),(t,1),(-1,-t),(-t,-1),(\sqrt{t},\sqrt{t})\},$$

for some real number $t > 0$. Then the hyperbola

$$C_t : xy = t$$

passes through these five points, see Figure 1. An interesting phenomenon occurs if t gets closer and closer to 0: the hyperbola becomes sharper and sharper around $(0,0)$, and eventually becomes the curve

$$C_0 : xy = 0.$$

This degeneration is shown in Figure 2. This curve C_0 is not *smooth*, meaning that it does not locally look like a line, while C_t is smooth for $t \neq 0$. As it locally looks like the crossing of two lines, we say C_0 is a *nodal* curve.

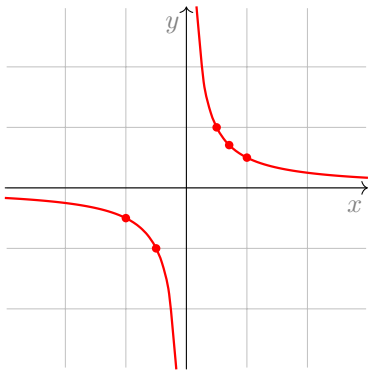

Figure 1: The hyperbola $xy = \frac{1}{2}$, passing through the five points $(1, \frac{1}{2})$, $(\frac{1}{2}, 1)$, $(-1, -\frac{1}{2})$, $(-\frac{1}{2}, -1)$, $(\sqrt{\frac{1}{2}}, \sqrt{\frac{1}{2}})$.

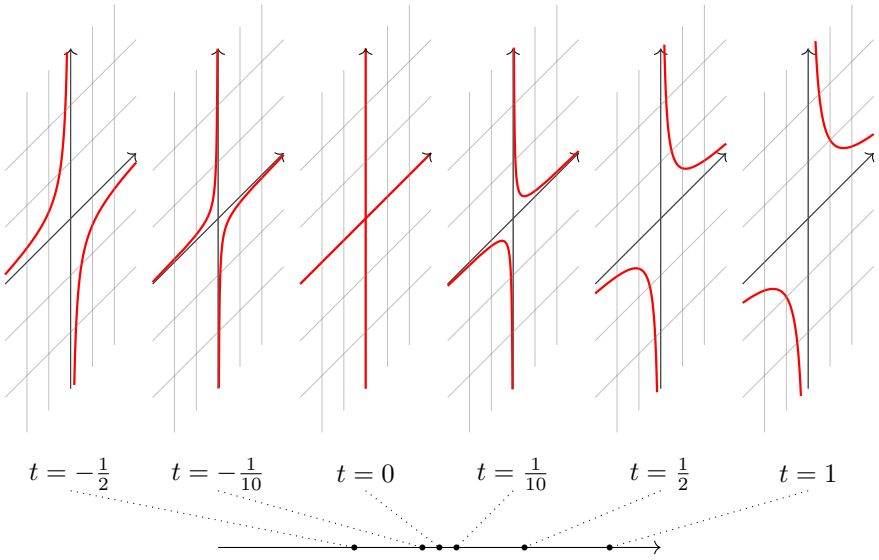

Figure 2: The curve $xy = t$ for various values of t. It is smooth for $t \neq 0$.

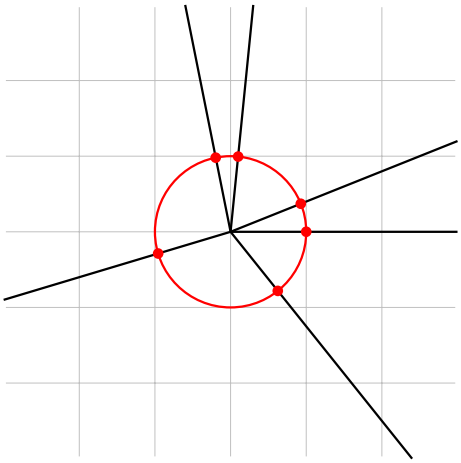

Figure 3: The set of rays starting in the origin can naturally be identified with a circle (red). Each ray corresponds to its intersection with the circle.

Many nice properties that smooth curves satisfy do not carry over to nodal curves. However, people do often study nodal curves, even if they want to count smooth curves. Why? The explanation lies in the notion of the *moduli space of curves*. This is a set containing all curves, and miraculously it itself is a geometric object.

For an example of this phenomenon, consider the set of rays starting at the origin, pictured in Figure 3. This is a set of geometric objects, but it itself is also a geometric object, namely a circle! For another example, we take a look at Figure 2 again. Here the set of curves naturally forms a line with coordinate t, and the set of smooth curves forms a line with a hole, as the point $t = 0$ is missing.

Studying moduli spaces is an incredibly powerful perspective for answering questions about curves. However, if these moduli spaces have holes in them, i.e., are not *compact*, then many of the geometric techniques cannot be applied. The moduli space of smooth curves $\mathcal{M}$ has many holes, and its *compactification* $\overline{\mathcal{M}}$ of nodal curves has none. Today, moduli spaces feature front and center in many areas in algebraic geometry. For a beautiful introduction to the subject via the moduli space of triangles, we recommend [Beh14]. For a more classical, algebraic version, see for example [Vak08] or [Sch20].

In Chapter 2 we use this moduli space perspective to study the *double rami-*

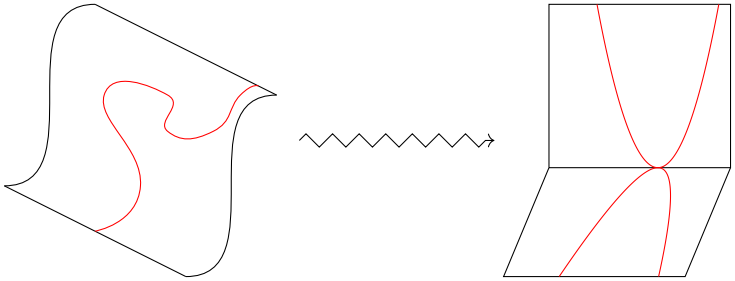

Figure 4: A degeneration of a variety. The curves inside the variety degenerate into curves tangent to the intersection.

fication cycle $\mathrm{DR}(A)$, which depends on a sequence $A \in \mathbb{Z}^n$ with sum 0 and counts curves with infinite symmetries and some extra conditions given by A. This object, defined in [GV03, MW20, Hol21] has many ties with other areas in mathematics [BR21, RK23]. In [JPPZ17] they conjectured that $\mathrm{DR}(A)$ is polynomial in A, and announced a proof of this fact. Recently Pixton gave a proof of this statement [Pix23]. We give an alternative proof, in Theorem A.

Degenerating smooth curves to nodal curves can be useful in order to study smooth curves. But a curve is just a special case of a variety, as a variety is any geometric space defined by polynomial equations. In fact, we can degenerate any variety, and this can at times be a strong tool. One can degenerate a smooth variety into simpler building blocks, similarly to how we degenerated $xy = 1$ to $xy = 0$, the union of the two lines $x = 0$ and $y = 0$. The curves in the variety then deform to curves on the pieces. For an example, see Section 7.7.6. Often questions about the original variety can be translated into questions about the building blocks. For example, the *degeneration formula* tells us how to compute curve counts in a smooth variety X from curve counts of the building blocks of its degeneration [KLR18, ACGS20b, RK23].

The key to making the geometry and the combinatorics of the degenerations work together is the language of *logarithmic geometry*, an extension of algebraic geometry. A *log variety* is a variety with some more structure, a *log structure*. We mainly care about *log smooth* log varieties X, where the log structure is a representation of X as a degeneration from a smooth variety. For example, Figure 2 naturally induces a log smooth log structure on C_0, by representing it as the degeneration of $xy = t$ as t goes to 0.

It turns out that every nodal curve admits a canonical log smooth log struc-

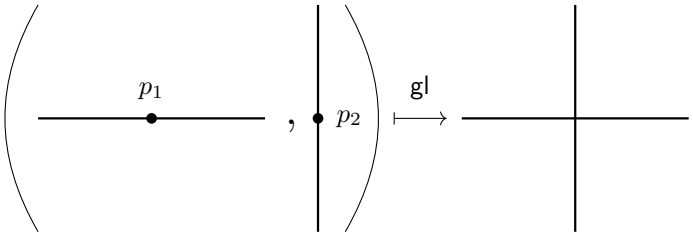

Figure 5: The gluing of two lines.

ture, and hence we can also interpret $\overline{\mathcal{M}}$ as the moduli space of log smooth curves. This also induces a log structure on $\overline{\mathcal{M}}$. All log curves being log smooth causes everything to behave similarly to the case of smooth curves, with the added advantage of still having a compact moduli space. Many results in algebraic geometry have been proven by considering a log analogue and proving statements about the log analogue and then deducing algebraic results [HPS19, HMOP23, RK23]. For some examples where *tropical geometry*, the combinatorial part of log geometry, is used to prove algebraic statements, see e.g. [KRZB16, FJP23]. However, finding the correct log analogue and proving the corresponding log statements is not an easy feat.

In Chapter 3 we show one example of this, where using logarithmic methods we simplify results from [BH19] and use that to answer some open questions from [BH19].

In Chapter 4, joint work with David Holmes, we study a different example, that of *gluing* curves. Classically, this works as follows. Let $\overline{\mathcal{M}}_1$ denote the moduli space of pairs (C, p) where C is a curve and p is a point on C. Then given two curves $(C_1, p_1), (C_2, p_2) \in \overline{\mathcal{M}}_1$, we can glue the points p_1 and p_2 together to get a different curve C^{gl}. Formally, we have

$$C^{\mathsf{gl}} = (C_1 \sqcup C_2)/\sim$$

where $p_1 \sim p_2$. As an example of this, see Figure 5 where we construct C_0 as the gluing of two lines.

This defines a gluing map

$$\mathsf{gl} : \overline{\mathcal{M}}_1 \times \overline{\mathcal{M}}_1 \to \overline{\mathcal{M}}.$$

The image lies in the boundary $\overline{\mathcal{M}} \setminus \mathcal{M}$ of nodal curves, and it is this gluing map that lets us recursively understand the boundary. These gluing maps

have laid the ground for many theories, theorems and formulas in classical algebraic geometry. For example, the curve counts mentioned above satisfy some recursive relations with respect to gluing maps.

However, one can prove that log curves cannot be glued. That means that many classical construction involving the gluing map could not be generalised to the logarithmic case. Joint with David Holmes we have solved this issue, by defining *log pointed curves*. This defines a log moduli space $\mathbb{M}_1$, again with some log structure. We proved the following theorem.

Theorem (Theorem F)**.** *The underlying variety of* $\mathbb{M}_1$ *is* $\overline{\mathcal{M}}_1$*. There is a natural logarithmic gluing map*

$$\mathsf{gl} : \mathbb{M}_1 \times \mathbb{M}_1 \to \overline{\mathcal{M}}.$$

This enabled us to produce log analogues of several classical constructions, most notably logarithmic cohomological field theories, which are collections of functions satisfying some compatibility with respect to the logarithmic gluing maps. We generalised an important theorem [BR21] in the classical world to the log setting, obtaining Theorem G. This paper also opens up a new research line, on what constructions and theorems concerning the classical gluing map can be generalised to the log setting.

Rational points

One of the first abstract mathematical problems was that of *diophantine* equations, polynomial equations where the goal is to find all rational solutions. For example, the equation $x^2+y^2 = 1$, describing a circle, has the rational solution $(x, y) = (\frac{3}{5}, \frac{4}{5})$.

Throughout the millenia, there have been many tricks and theorems used to solve all kinds of diophantine equations, but we focus on the specific case of curves. Given a polynomial in x, y, for example $x^2 + y^2 = 1$, or

$$y^2 + (x^3 + x + 1)y = x^5 - x$$

the set of all complex solutions forms a geometric curve that is easy to describe. The rational solutions then correspond to rational points on the curve, and they form a subset that is often difficult to find. For a curve C we denote this set of rational points by $C(\mathbb{Q})$. Perhaps most famous is the Fermat curve F_n, given by $x^n + y^n = 1$ for a fixed $n \geq 3$, which has been shown by Andrew Wiles to only have rational points (x, y) of the form $(0, \pm 1)$ and $(\pm 1, 0)$, thereby

proving Fermat's Last Theorem on the integer solutions of $a^n+b^n = c^n$ [Wil95, TW95].

A curve C has an important invariant called the genus $g \in \mathbb{Z}_{\geq 0}$, and the behaviour of the curve C and of the rational points $C(\mathbb{Q})$ is strongly dependent on the genus. There is only one curve of genus $g = 0$, namely the line, and it has infinitely many rational points[12].

Curves of genus 1 are called *elliptic curves*. This is a very special kind of curve that naturally has the structure of an abelian group, meaning that you can add two points on it to get a third point. The rational points form a subgroup, and this is even a finitely generated group. For any specific elliptic curve, finding generators and relations for this group is usually doable.

For curves of genus $g \geq 2$, the topic of the second half of this thesis, Mordell conjectured in 1922 that there are always only finitely many rational points. Though there was partial progress, this conjecture was only proven in 1983 by Faltings, and is now known as Faltings' theorem. This was a breakthrough result, but unfortunately this result is not *effective*, i.e., it does not help in actually computing the set of rational points.

One way to make it effective in certain cases, is by a theorem of Chabauty proven in 1941 [Cha41], that was partial progress towards Faltings' theorem. To every curve C of genus g there is an associated space of dimension g called its Jacobian, which we denote by $J = J(C)$. Like an elliptic curve, this geometric space is an abelian group. It comes with a natural map $C \to J$, the Abel–Jacobi map, that is an embedding if $g \geq 1$, and one can think of J as the abelian groupification of C. As one incarnation of this, the fundamental group of J is the abelianisation of the fundamental group of C. For an example of what the embedding might look like for $g = 2$, see Figure 6.

For an elliptic curve C, the Jacobian J is equal to C, and the map to the Jacobian is simply the identity. In general, J has similar properties to an elliptic curve. For example, its set of rational points $J(\mathbb{Q})$ forms an abelian group that is finitely generated, of some rank r. See Figure 7 for an example where $r = 1$ and where we have plotted the line containing $J(\mathbb{Q})$.

Now we can see Chabauty's trick appearing, if we overlay these two embeddings $C \to J$ and $J(\mathbb{Q}) \to J$, as in Figure 8. We know the rational points in $C(\mathbb{Q})$ both lie in C and map to $J(\mathbb{Q})$ under the Abel–Jacobi map, and hence lie in the intersection $J(\mathbb{Q}) \cap C \subset J$. And under the crucial assumption $r < g$, we

[12]Throughout this section, we make the technical assumption that C has at least one rational point to simplify the exposition.

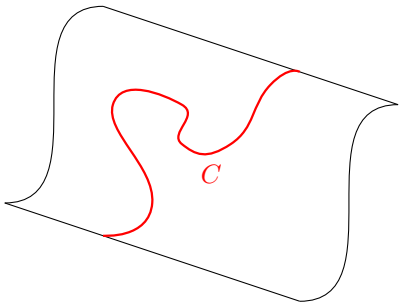

Figure 6: An embedding of the genus 2 curve C (red) into its Jacobian (black), a surface.

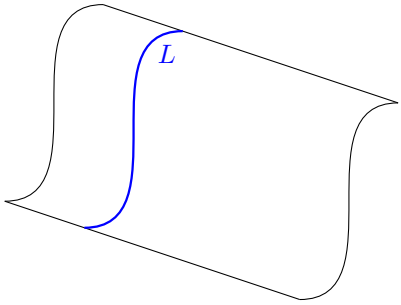

Figure 7: A line L (blue) containing all rational points of the Jacobian (black).

expect this intersection to be finite for dimension reasons. Indeed, this is what Chabauty proved: if $r < g$, then $C(\mathbb{Q})$ is finite.

A small technical note: the picture suggests that we are taking this intersection inside the $\mathbb{R}$-points of J. In fact, this won't work, and we instead take the intersection $C(\mathbb{Q}_p) \cap J(\mathbb{Q})$ inside $J(\mathbb{Q}_p)$, where $\mathbb{Q}_p$ are the p-adic numbers for some prime p. This is a different, non-archimedic completion of $\mathbb{Q}$ that does not have many of the convergence issues that $\mathbb{R}$ has.

It took another 44 years for an effective version of Chabauty's method to come out. In 1985 Coleman [Col85a] gave a method to compute (a slightly larger set than) $\overline{J(\mathbb{Q})} \cap C \subset J$ where $\overline{J(\mathbb{Q})}$ is the closure of $J(\mathbb{Q})$ inside J. He did this by studying some vector spaces associated to C and J, called *cohomology* groups.

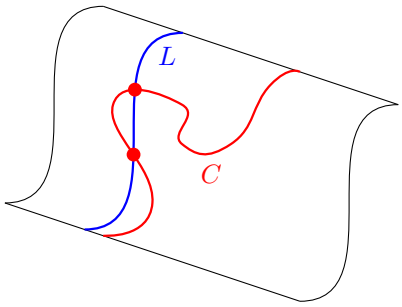

Figure 8: Chabauty's method: the intersection of L (blue) and C (red) contains all rational points of C and is finite.

Currently, there are many variations of this method, and the name of the game is to find methods that work on ever more curves and produce ever smaller sets of points (still containing all the rational points).

In 2009 Kim vastly generated the Chabauty–Coleman method [Kim09]. Instead of working with the abelianisation of the fundamental group $G = \pi_1(C)$, Kim worked with non-abelian quotients of the fundamental group G. Kim defined a sequence of successive quotients

$$G \to \cdots \to G_n \to G_{n-1} \to \cdots \to G_2 \to G_1 = G^{\mathrm{ab}} = \pi_1(J)$$

and for each G_n they defined a subset C_n of C (not necessarily finite) containing the rational points, such that we get a sequence

$$C(\mathbb{Q}) \subset \cdots \subset C_n \subset C_{n-1} \subset \cdots \subset C_2 \subset C_1.$$

Like Coleman, they defined these sets using cohomology groups. And indeed, for the abelianisation G_1 they recover the same set Coleman finds. This generalisation could have massive implications: it is conjectured that for any curve C of genus at least 2, no matter what r is, the sequence $C_1, C_2, \cdots$ is eventually finite and even that there is always some n with $C_n = C(\mathbb{Q})$. However, actually computing any of these sets C_n beyond $n = 1$ has proven difficult. The best method so far is *(cohomological) quadratic Chabauty*. This uses a group G_{Coh} with $G_2 \to G_{\mathrm{Coh}} \to G_1$, and produces a set of points C_{Coh} with $C_2 \subset C_{\mathrm{Coh}} \subset C_1$. If we let ρ be the Néron–Severi rank of J (some integer in $\mathbb{Z}_{\geq 1}$ associated to J), then C_{Coh} is finite if $r < g + \rho - 1$. This method was first developed by Balakrishnan, Dogra and Müller for $r = g, \rho > 1$

[BBM16, BD18, BD21, BDM$^+$21]. One of its crowning achievements has been computing the rational points on the "cursed curve" $X_{\mathrm{s}}(13)$ [BDM$^+$19].

Recently, Edixhoven and Lido have introduced a more geometric approach to effective Chabauty computations; their method is known as *geometric quadratic Chabauty* [EL21]. They replace the Abel–Jacobi map $C \to J$ with a different embedding $C \to T$, and they prove the intersection $C \cap T(\mathbb{Q}) \subset T$ is finite if $r < g + \rho - 1$. A visualisation for $r = g = \rho = 2$ is shown in Figure 9. The geometric quadratic Chabauty method was conjectured to be comparable to the cohomological quadratic Chabauty method, but this was an open problem.

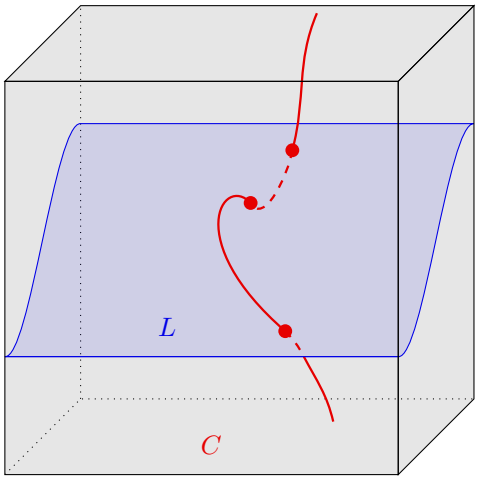

Figure 9: A visualisation of the geometric quadratic Chabauty method for $r = g = \rho = 2$: the rational points $T(\mathbb{Q})$ lie on a surface (blue) in T (black), and the curve C (red) intersects it in a finite set. This intersection $C \cap T(\mathbb{Q})$ contains the rational points of C, and hence the set of rational points $C(\mathbb{Q})$ is finite.

In my master's thesis [Spe20] I used the geometric methods from [EL21] to study the map $C \to J$, in a method called *geometric linear Chabauty*. This was conjectured to be comparable to the Chabauty–Coleman method.

Joint with Sachi Hashimoto in Chapter 5 we proved the following comparison theorem.

Theorem (Theorem 5.5.1)**.** *The geometric linear Chabauty method outperforms the Chabauty–Coleman method, in the following sense. Let* C_{CC} *be the*

set of points found by the Chabauty–Coleman method, and C_{GLC} *the set of points found by the geometric linear Chabauty method. Then we have inclusions*

$$C(\mathbb{Q}) \subset C_{\mathrm{CC}} \subset C_{\mathrm{GLC}},$$

and there is an explicit characterisation of $C_{\mathrm{GLC}} \setminus C_{\mathrm{CC}}$.

And joint with Juanita Duque-Rosero and Sachi Hashimoto in Chapter 6 we proved the following comparison theorem on quadratic Chabauty.

Theorem (Theorem H)**.** *The geometric quadratic Chabauty method outperforms the cohomological quadratic Chabauty method, in the following sense. Let* C_{Coh} *be the set of points found by the Chabauty–Coleman method, and* C_{Geo} *the set of points found by the geometric linear Chabauty method. Then we have inclusions*

$$C(\mathbb{Q}) \subset C_{\mathrm{Coh}} \subset C_{\mathrm{Geo}},$$

and there is an explicit characterisation of $C_{\mathrm{Geo}} \setminus C_{\mathrm{Coh}}$.

In Chapter 7 we focus on a specific ingredient needed for quadratic Chabauty, both cohomological and geometric, namely *local heights* (to be precise, the local heights away from p if we are considering the p-adic numbers $\mathbb{Q}_p$). These form a finite set of numbers associated to the curve. In literature, many examples are chosen such that the local heights are 0, in order to avoid having to compute non-vanishing local heights. In joint work with Alex Betts, Juanita Duque-Rosero and Sachi Hashimoto we give an algorithm for computing these local heights. We use this to prove the curve given by the equation

$$y^2 = x^6 + 18/5x^4 + 6/5x^3 + 9/5x^2 + 6/5x + 1/5$$

has exactly 10 rational points (Theorem I). This is the first example of the quadratic Chabauty method applied to a curve with two non-vanishing local heights.