A tale of three curves

———

Jennifer S. Balakrishnan [1]

In this snapshot, we give a survey of some problems
in the study of rational points on higher genus curves,
discussing questions ranging from the era of the an-
cient Greeks to a few posed by mathematicians of the
20th century. To answer these questions, we describe
a selection of techniques in modern number theory
that can be used to determine the set of rational
points on a curve.

1 Introduction

Here's a question to think about: do there exist a rational right triangle and a
rational isosceles triangle that have the same perimeter and the same area? By
a *rational* triangle, we mean one whose lengths are rational numbers: that is,
ratios $\frac{a}{b}$ of integers a and b.

This feels like a very classical question – indeed, one that may have been
studied by the ancient Greeks thousands of years ago – but the answer is
somewhat surprising and uses some beautiful 20th century number theory. The
answer was very recently given by Hirakawa and Matsumura [9]. We describe
their proof below and use it to frame some recent advances in studying *rational
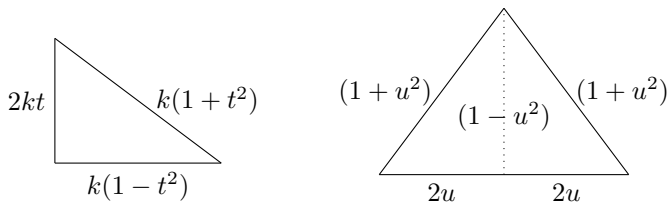points* on curves.

Figure 1: Can these two triangles have the same perimeter and same area while having rational side lengths?

Suppose that there exists such a pair of triangles (see Figure 1). It turns out that for them to be rational, their side lengths must have the following form:

$$(k(1 + t^2), k(1 - t^2), 2kt) \quad \text{and} \quad ((1 + u^2), (1 + u^2), 4u),$$

respectively, for the right triangle and isosceles triangle, for some rational numbers t, u, and k, where $0 < t < 1$, $0 < u < 1$, and $k > 0$. Then by equating the corresponding perimeters and areas of the two triangles, we have the system of equations

$$k(1 + t) = (1 + u)^2 \quad \text{and} \quad k^2 t(1 - t^2) = 2u(1 - u^2).$$

Changing coordinates shows that solving this system of equations is equivalent to computing the set of rational points $X(\mathbb{Q})$ on the curve X with equation

$$y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6. \tag{1}$$

The set of rational points on X is the set of those points $(x, y) \in \mathbb{Q}^2$ that satisfy the equation above (see Figure 2), along with points "at infinity."

Before we go on, let us say a little about the types of curves we are considering and recall some of the main results about them.

We will assume that our curve is algebraic and defined over $\mathbb{Q}$, meaning that we can write down a set of polynomial equations with coefficients in $\mathbb{Q}$ whose zero locus – the set of points that make the polynomials equal zero – is our curve. In fact, in all of the problems we discuss, our curve will be described by just one equation. We will further assume our curves are *smooth* (meaning that they do not have any *singular points*, for instance, a point where the curve crosses itself or where it has a sharp corner), and that they are *geometrically irreducible*: if $f(x, y) = 0$ is the equation describing the curve, then the polynomial $f(x, y)$ cannot be written as a product of smaller factors using only coefficients in the
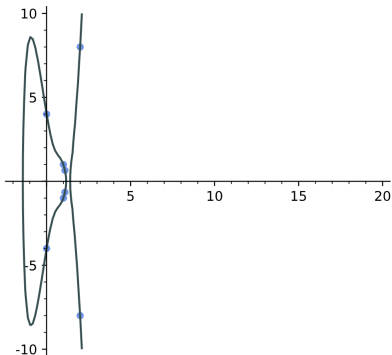
Figure 2: A plot of the curve $y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6$ and its rational points (in blue).

algebraic numbers [2]. Finally, our curves are required to be *projective*: we think of them as living in a plane with added "points at infinity" (the "projective plane"), where they are given by homogeneous polynomials.

Given a curve C, we would like to determine the set of its rational points $C(\mathbb{Q})$. Note that we don't just want to find some rational points, but rather, we want to prove that we've found *all* rational points – in other words, we would like to have an algorithm that determines $C(\mathbb{Q})$ – and this is the challenge.

One important characterization of a curve is by its *genus*. The genus can be defined in a few different ways, but perhaps the easiest one to visualize is the following: we consider the curve over the complex numbers, so that it looks like a 2-dimensional surface. The genus is the number of holes in that surface (after adding some points at infinity): see Figure 3.

The genus of a curve already tells us quite a bit about the behavior of the set of its rational points. Curves of genus 0 either have no rational points at all or infinitely many. They further satisfy a "local-to-global" principle: a genus 0 curve has a rational point if and only if has a rational point in every *completion* of the rational numbers $\mathbb{Q}$.

What is a completion of the rational numbers? The best known is a very familiar one: the set of real numbers $\mathbb{R}$. But there are more, and they are called the *p-adic numbers*. Since the p-adic numbers $\mathbb{Q}_p$ are an important part of the discussion to follow, let us pause for a moment and say a bit about these numbers. Perhaps the first way of looking at a p-adic number is through its

---

[2] For example, integers, roots of integers, and rational numbers are algebraic numbers. But some irrational numbers are not, such as π.
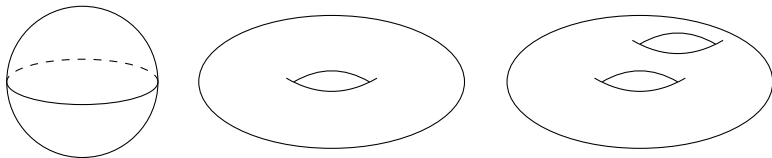
"base p" expansion. While a real number can be represented by infinitely many digits to the right (for example, we have the following expression for π:

$$\pi = 3.1415\ldots = 3 \cdot 10^0 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 1 \cdot 10^{-3} + 5 \cdot 10^{-4} + \cdots$$

in base 10), a p-adic number can be thought of as a sequence of infinitely many digits to the left. That is, we may write it in the form

$$c_{-n} \cdot p^{-n} + c_{-n+1} \cdot p^{-n+1} + \cdots + c_0 + c_1 \cdot p + c_2 \cdot p^2 + \cdots,$$

where p is a prime, with some $n \in \mathbb{N}$ and $c_{-n}, c_{-n+1}, \ldots \in \{0, 1, \ldots, p-1\}$. One also needs a new absolute value for expressions of this form: if only high powers of p show up in a p-adic number, the p-adic number is considered "small" – similar to how a real number is small if its only nonzero digits are far to the right after the decimal point. More precisely, if $q = p^n \frac{u}{v}$, where u and v are integers not divisible by p, then the p-adic absolute value of q is given by $|q|_p = p^{-n}$.

We can write some familiar numbers p-adically: the 5-adic expansion of 2 is just 2, since $2 \cdot 5^0 = 2$, whereas the 5-adic expansion of $-\frac{1}{2}$ is the infinite series

$$2 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + \cdots.$$

This might at first seem counterintuitive, but calculating that

$$-\frac{1}{2} - 2 \cdot 5^0 = -\frac{1}{2} \cdot 5^1,$$

$$-\frac{1}{2} - (2 \cdot 5^0 + 2 \cdot 5^1) = -\frac{1}{2} \cdot 5^2,$$

$$-\frac{1}{2} - (2 \cdot 5^0 + 2 \cdot 5^1 + 2 \cdot 5^2) = -\frac{1}{2} \cdot 5^3,$$

$$\vdots$$

one can see that the p-adic absolute value of the first line is 5^{-1}, of the second line 5^{-2}, of the third 5^{-3}, etc. Thus the series $2 + 2 \cdot 5 + 2 \cdot 5^2 + \cdots$ converges 5-adically to $-\frac{1}{2}$. In fact, every rational number has a p-adic expansion as above, for every prime p!

The real numbers include not only the rational numbers but also limits of sequences of rational numbers whose terms eventually get arbitrarily close under the usual absolute value; one says that the set of real numbers is a completion of the rational numbers. Likewise, for any prime p, the set of p-adic numbers is a completion of the rational numbers, but the closeness between numbers is now measured by the p-adic absolute value.

Now we return to our discussion about curves of genus 0. Here the problem about determining the set of rational points is solved, as the local-to-global principle is a nice criterion that is checked with a finite amount of computation.

Curves of genus 1 can have no rational points, finitely many rational points, or infinitely many rational points. A genus 1 curve with a specified rational point is an *elliptic curve*, and it is a theorem of Mordell from the 1920s that the set of rational points on an elliptic curve E forms a *finitely generated Abelian group*[3] $E(\mathbb{Q})$. Elliptic curves figure prominently in modern number theory, ranging from the theoretical (for example, the proof of Fermat's Last Theorem) to the applied (for example, modern cryptosystems, which are sets of cryptographic algorithms used for data encryption). There are still many open questions about rational points on elliptic curves.

One remarkable property of curves of genus 2 or larger is that they have only *finitely* many rational points. This was conjectured by Mordell in the 1920s, and Faltings [8] proved this landmark result in the 1980s.

Now returning to the curve in the triangle problem: it turns out that our curve X has genus[4] 2. In fact, we know even more: the "Chabauty–Coleman bound" [6] on the size of the set of rational points for this particular curve yields the following bound on the number of rational points: $\#X(\mathbb{Q}) \leq 10$. By searching for points with bounded numerator and denominator, we find a collection of rational points: $\{(0, \pm 4), (1, \pm 1), (2, \pm 8), (12/11, \pm 868/11^3)\} \subset X(\mathbb{Q})$.

Moreover, as X is a projective curve, we must also consider its rational points at infinity: here X has a pair of such points, which we will denote as $\infty^{\pm}$. We have managed to find 10 rational points, which is the upper bound given by

---

[3] We will not give a formal definition here; simply imagine a set (for example, the integers $\mathbb{Z}$) equipped with an operation (like addition $+$) and some extra properties. But we will come back to this idea, in the more general context of *Jacobians of curves*, momentarily.

[4] The genus of any *hyperelliptic* curve, that is, any smooth algebraic curve with an equation of the form $y^2 = f(x)$ can be read off from the degree of the polynomial f: if $\deg f = 2g + 2$ or $2g + 1$, then the genus is g. For the curve we are considering here (see Figure 2), $\deg f = 6 = 2 \cdot 2 + 2$, so $g = 2$.

Chabauty–Coleman! So we have provably determined the set of rational points on this curve. Furthermore, only $(12/11, 868/11^3)$ satisfies the inequalities necessary to correspond to a pair of triangles. This yields the following:

Theorem 1 (Hirakawa–Matsumura) *Up to similitude, there exists a unique pair of a rational right triangle and a rational isosceles triangle that have the same perimeter and the same area. The unique pair consists of the right triangle with sides of lengths* $(377, 135, 352)$ *and the isosceles triangle with sides of lengths* $(366, 366, 132)$.

2 The Chabauty–Coleman method

What allowed us to compute the set of rational points $X(\mathbb{Q})$ in the previous example? We mentioned that the Chabauty–Coleman bound applied to our curve. This upper bound existed since the rank of the *Mordell–Weil group of the Jacobian* of this curve was less than its genus. Let us first give some idea about the objects involved and then discuss the ingredients of the Chabauty–Coleman method.

For starters, when the genus g of X is 2 or larger, the set of its rational points $X(\mathbb{Q})$ is just that: a set. It does not have any obvious additional structure. So it is helpful to embed our curve X into other objects that have more structure.

One such object is the *Jacobian variety J of X*. The Jacobian is a g-dimensional "Abelian variety" associated to the genus g curve X.

The set $J(\mathbb{Q})$, called the Mordell–Weil group, is an Abelian group, and the Mordell–Weil Theorem states that it is finitely generated, which means that it has finitely many points from which all others can be generated by repeated addition and subtraction.

The rank[5] r of the Mordell–Weil group measures the complexity of the group. Computing the rank r and finding a basis captures all of the information about rational points on the Jacobian. Unfortunately, computing the rank and finding a basis of the Mordell–Weil group are very difficult problems: in general, there is no known algorithm! The situation in smaller dimension is no easier: the case of elliptic curves, when $g = 1$, is famously difficult as well, and figures prominently in the Birch and Swinnerton-Dyer conjecture, one of the Clay Mathematics Institute's Millennium Prize Problems.

In the 1940s, Chabauty [5] proved that for curves X of genus at least 2, if the rank r of the Jacobian is less than g, then $X(\mathbb{Q})$ is finite. Then 40 years

---

[5] The rank of an Abelian group is analogous to the dimension of a vector space. For example, the rank of the group $(\mathbb{Z}^3, +)$ is 3. Abelian just means that commutativity holds.

later, Coleman made Chabauty's theorem effective [6], using his theory of p-adic integration [7], giving the bound

$$\#X(\mathbb{Q}) \leq \#\overline{X}(\mathbb{F}_p) + 2g - 2, \tag{2}$$

where $p > 2g$ is a prime of good reduction [6] for X, where $\overline{X}$ denotes the reduction modulo p of X and $\mathbb{F}_p$ is the finite field with p elements. Computing $\#\overline{X}(\mathbb{F}_p)$ means to compute the number of "$\mathbb{F}_p$-rational" points on $\overline{X}$. We will now explain in more detail what all of this means.

Let us take $p = 5$. The field $\mathbb{F}_5$ has 5 elements: $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, which are the remainders of integers upon division by 5. Essentially, we are taking the integers *modulo 5* and identifying numbers that have the same remainder:

$$\cdots = \overline{-5} = \overline{0} = \overline{5} = \overline{10} = \cdots$$
$$\cdots = \overline{-6} = \overline{1} = \overline{6} = \overline{11} = \cdots$$
$$\cdots = \overline{-7} = \overline{2} = \overline{7} = \overline{12} = \cdots$$
$$\cdots = \overline{-8} = \overline{3} = \overline{8} = \overline{13} = \cdots$$
$$\cdots = \overline{-9} = \overline{4} = \overline{9} = \overline{14} = \cdots$$

So if we start with the curve X, which has equation

$$y^2 = (3x^3 + 2x^2 - 6x + 4)^2 - 8x^6 = x^6 + 12x^5 - 32x^4 + 52x^2 - 48x + 16,$$

and reduce modulo 5, we obtain the curve

$$\overline{X} : y^2 = x^6 + \overline{2}x^5 + \overline{3}x^4 + \overline{2}x^2 + \overline{2}x + \overline{1} \quad \text{over } \mathbb{F}_5,$$

which has the following $\mathbb{F}_5$-rational points:

$$\{\overline{\infty^{\pm}}, (\overline{0}, \overline{1}), (\overline{0}, \overline{4}), (\overline{1}, \overline{1}), (\overline{1}, \overline{4}), (\overline{2}, \overline{2}), (\overline{2}, \overline{3})\}.$$

We see that $\#\overline{X}(\mathbb{F}_5) = 8$ and $g = 2$, so Inequality (2) becomes $\#X(\mathbb{Q}) \leq 10$.

Now we briefly give an overview of the ideas behind Inequality (2). The goal is to give an upper bound on the size of the set of rational points by embedding the set of rational points inside a finite set of p-adic points and carrying out some p-adic analysis to bound the size of this auxiliary set. This set of p-adic points is the zero set of a "p-adic integral".

The theorem of Hirakawa–Matsumura is a striking application of the Chabauty–Coleman method: since the upper bound on the size of the set of rational points is matched just by searching for rational points within a

---

[6] *Good reduction* means that if one were to look at the equations for X modulo p (the reduction of X modulo p), this would also give a smooth curve.

small bounded box, this Diophantine equation (1) is solved without needing to compute any p-adic integrals.

Nevertheless, in many other interesting examples of curves, the upper bound (2) does not match the size of the set of known rational points. In such a scenario, one needs to compute the zero sets of the relevant p-adic integrals and figure out which points in this set are truly rational or merely p-adic. To do this, it often helps to carry out the Chabauty–Coleman method for several different primes and to use this information, together with the structure of the Mordell–Weil group of the Jacobian, to sieve out the merely p-adic points. This process is known as the Mordell–Weil sieve [4].

3 A question of Diophantus

Now for a question that does indeed date from the era of the ancient Greeks. Diophantus of Alexandria was a Greek mathematician who lived in the third century. In Problem 17 of book VI of the Arabic manuscript of the *Arithmetica*, Diophantus poses the following problem:

> Find three squares which when added give a square, and such that the first one is the side [the square root] of the second, and the second is the side of the third.

In other words, Diophantus asked if one can find positive rational x and y such that the equation
$$y^2 = x^8 + x^4 + x^2$$
is satisfied. He gave the solution $x = 1/2, y = 9/16$. Are there any others?

Removing the singularity of the curve at $(0,0)$ shows that this amounts to determining the set of all rational points on the genus 2 curve Y with equation

$$y^2 = x^6 + x^2 + 1.$$

This problem was solved in the 1990s by Wetherell [18], who showed that the set of rational points $Y(\mathbb{Q})$ is precisely

$$\left\{ (0, \pm 1), \left(\pm \frac{1}{2}, \pm \frac{9}{8} \right), \infty^\pm \right\}.$$

This curve is interesting because it is the only curve of genus 2 and higher considered in the 10 known books of the *Arithmetica*. Moreover, this curve is of interest because it lies just beyond the boundary of what is feasible using the Chabauty–Coleman method. It turns out that the rank of the Mordell–Weil group of its Jacobian is two.

Nevertheless, one special property of the curve Y is that it has extra symmetries and is said to be *bielliptic*: indeed, these extra symmetries (automorphisms) of the curve result in a nice decomposition of its Jacobian into a product of two elliptic curves. Wetherell gave a solution to Diophantus' problem by considering a collection of *covering curves*[7] $\{F_i\}$ of Y, and applying the Chabauty–Coleman method on the covers F_i, from which the result about $Y(\mathbb{Q})$ follows.

4 The cursed curve

Many curves of interest in modern Diophantine geometry come from *moduli problems*, which capture information about a family of geometric objects. There are several families of modular curves that are of interest. One such family comes to us from a question posed by Serre, on possible images of "residual Galois representations" attached to elliptic curves – if they are "uniformly bounded" in some sense. Following extensive work by Mazur [13, 14], Serre [16], and Bilu–Parent [2] and Bilu–Parent–Rebolledo [3], many cases of Serre's uniformity question were answered.

In particular, after the work of Bilu–Parent and Bilu–Parent–Rebolledo on the "split Cartan case of Serre uniformity", the set of rational points on the "split Cartan modular curves" $X_s(p)$ at prime level p were determined – except for the split Cartan curve at level $p = 13$, the so-called "cursed" level. An equation and plot of the modular curve $X_s(13)$ can be seen in Figure 4.

$$y^4 + 5x^4 - 6x^2y^2 + 6x^3z + 26x^2yz + 10xy^2z - 10y^3z$$
$$- 32x^2z^2 - 40xyz^2 + 24y^2z^2 + 32xz^3 - 16yz^3 = 0$$

Figure 4: A projective visualization of the cursed curve.

Here again, as in Diophantus' problem, the method of Chabauty–Coleman does not apply, since the genus of the curve is 3 and the rank of the Mordell–Weil group of its Jacobian is 3. However, the Jacobian of this curve does not decompose into a product of Abelian varieties of smaller dimension. Also, there

---

[7] Informally, the idea is that one tries to construct a finite collection of covering curves $\{F_i\}$ of Y such that every rational point on Y comes from a rational point on one of the F_i. Then one can consequently compute the set of rational points $Y(\mathbb{Q})$ by computing the sets $F_i(\mathbb{Q})$.

are no obvious covers to consider, which means that we cannot simply repeat the procedure used to solve Diophantus' problem.

Nevertheless, the "non-Abelian Chabauty" program of Kim [10, 11, 12] suggests that one can use further non-Abelian geometric objects – beyond the Jacobian (an Abelian variety) – to study rational points on curves, without restriction on rank. Indeed, one very striking aspect of Kim's program is that it is conjectured to give an effective resolution of Mordell's conjecture for all curves of genus at least 2.

In joint work with Dogra, Müller, Tuitman, and Vonk [1], we used the first non-Abelian step of this program – quadratic Chabauty – to show that the curve $X_s(13)$ has exactly seven rational points:

$$(1:1:1), (1:1:2), (0:0:1), (-3:3:2), (1:1:0), (0:2:1), (-1:1:0).$$

One key idea behind quadratic Chabauty is to move beyond the linear relations among p-adic integrals to "bilinear relations" and to further study "p-adic heights", which can also be described in terms of p-adic integrals. It turns out that the Jacobian of the curve $X_s(13)$ does have some additional structure: it has extra symmetries (endomorphisms), and this allows us to apply quadratic Chabauty to compute rational points in this particular case of higher rank.

5 Going forward

In the study of these seemingly-simple equations, one pulls together ideas from several facets of mathematics – number theory, (algebraic) geometry, and (p-adic) analysis – to name a few. Moreover, for each of the three curves discussed, one has to translate these techniques into computer code that can be run to carry out some of the key steps: for instance, finding the Mordell–Weil rank of the Jacobian and doing the p-adic integration are steps for which one typically uses computer algebra packages such as `SageMath` or `Magma`.

There are still many curves whose rational points we would like to understand. And here is where we confess that really, this is a tale not just of three but of four curves. Our last curve is the genus 2 curve with equation

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 +$$
$$567207969x^2 - 985905640x + 247747600.$$

It has at least 642 rational points. This curve was found by Elkies and Stoll [17] in 2008 and is the current record-holder for the size of the set of rational points in genus 2. Conditional on a very important conjecture in mathematics, the Generalized Riemann Hypothesis, Müller and Stoll [15] proved that the

Jacobian of this curve has rank 22, so it is currently out of reach using the methods we have described so far.

Indeed, the tale of this fourth curve is not yet finished! Dear reader, perhaps you can definitively compute its set of rational points?

Image credits

Figure 4 Courtesy of the author and Sachi Hashimoto.

References

[1] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty–Kim for the split Cartan modular curve of level 13*, Annals of Mathematics (2) **189** (2019), no. 3, 885–944.

[2] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Annals of Mathematics (2) **173** (2011), no. 1, 569–584.

[3] Y. Bilu, P. Parent, and M. Rebolledo, *Rational points on $X_0^+(p^r)$*, Annales de l'Institut Fourier **63** (2013), no. 3, 957–984.

[4] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS Journal of Computations and Mathematics **13** (2010), 272–306.

[5] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, Comptes Rendus de l'Académie des Sciences de Paris **212** (1941), 882–885.

[6] R. F. Coleman, *Effective Chabauty*, Duke Mathematical Journal **52** (1985), no. 3, 765–770.

[7] R. F. Coleman, *Torsion points on curves and p-adic Abelian integrals*, Annals of Mathematics (2) **121** (1985), no. 1, 111–168.

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Mathematicae **73** (1983), no. 3, 349–366.

[9] Y. Hirakawa and H. Matsumura, *A unique pair of triangles*, Journal of Number Theory **194** (2019), 297–302.

[10] M. Kim, *The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel*, Inventiones Mathematicae **161** (2005), no. 3, 629–656.

[11] M. Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publications of the Research Institute for Mathematical Sciences **45** (2009), no. 1, 89–133.

[12] M. Kim, *Massey products for elliptic curves of rank 1*, Journal of the American Mathematical Society **23** (2010), 725–747.

[13] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques (1977), no. 47, 33–186 (1978).

[14] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Inventiones Mathematicae **44** (1978), no. 2, 129–162.

[15] J. S. Müller and M. Stoll, *Canonical heights on genus-2 Jacobians*, Algebra & Number Theory **10** (2016), no. 10, 2153–2234.

[16] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae **15** (1972), no. 4, 259–331.

[17] M. Stoll, *Rational points on curves of genus 2: Experiments and speculations*, Algorithms and Number Theory, Dagstuhl Seminar Proceedings, no. 09221, 2009.

[18] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, UC Berkeley Ph.D. thesis (1997).

―――――

Snapshots of modern mathematics from Oberwolfach provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

―――――