CONTEMPORARY METHODS FOR SOLVING DIOPHANTINE EQUATIONS

MICHAEL BENNETT (UNIVERSITY OF BRITISH COLUMBIA)
NILS BRUIN (SIMON FRASER UNIVERSITY)
YANN BUGEAUD (UNIVERSITÉ DE STRASBOURG)
BJORN POONEN (MASSACHUSETTS INSTITUTE OF TECHNOLOGY)
SAMIR SIKSEK (UNIVERSITY OF WARWICK)

1. OVERVIEW OF THE FIELD

The topic of this summer school was Diophantine equations, which are among the oldest studied mathematical objects. A *Diophantine equation* is an equation where admissible solutions are restricted to the rationals or the integers, or appropriate mathematical generalizations of such objects. The equations themselves tend to be polynomial, exponential, or a mixture of both, where variables in the exponents are usually restricted to (positive) integers. A characteristic example is the equation that is central to Fermat's Last Theorem,

$$x^n + y^n = z^n, \text{ with } x, y, z \in \mathbb{Z} \text{ and } n \in \{3, 4, \ldots\}.$$

Because Diophantine equations concern themselves with objects so fundamental to mathematics, they tend to arise whenever one uses the mathematical language to formulate problems or theories. This supplies a dual motivation to the field.

On the one hand, there is an interest to understand theoretically the set of solutions to the equations and its relationship to the geometric objects defined by the equations.

On the other hand, there is a demand for practical methods that, given an explicit equation, provide a complete and explicit description of the set of solutions. In recent years, a combination of development of general theory, computational tools and computational techniques has greatly improved our ability to explicitly solve Diophantine equations. Some of the methods that have proved to be particularly relevant recently are the following.

- *The modular method (see Section 4).* The application of the ideas of Frey, Ribet, Wiles, and others, that led to the proof of Fermat's last theorem. The method only applies to a limited class of equations, but it is currently the only method that is able to handle statements about *rational* solutions to families of equations with varying exponents.
- *Linear Forms in Logarithms (See Section 5).* This method applies to a wide class of equations for which one wants to determine *integral* solutions. It provides explicit versions of results along the lines of Roth's theorem, which has been used to prove finiteness of integral points on affine hyperbolic curves.
- *Hypergeometric method (See Section 6).* This method applies to a subset of problems where linear forms in logarithms apply. When it does apply, it usually yields sharp results.
- *Cohomological obstructions (See Section 7).* One of the oldest and simplest methods to show that a Diophantine equation has no solutions is by showing that there is some *local obstruction* to having solutions. Equations that have no local obstructions to having solutions are said to have *solutions everywhere locally*. It is well known that local obstructions are not the only obstructions to having solutions. Various other obstructions have been identified, many of which were eventually shown to

Date: June 10 – 17, 2012 .

be part of the *Brauer-Manin obstruction*. This obstruction is, at least in theory, largely computable and is most conveniently formulated in the language of étale cohomology. The closely related *descent obstruction* is also most conveniently studied in a cohomological setting and translates the original question into one about solutions to finitely many other equations, which may have local obstructions even if the original equation does not.

- *Mordell-Weil Sieving and Chabauty's method (See Section 8)*. Many of the cohomological ideas lead in principle to computable criteria, but not necessarily in a practical way. At least for determining the rational points on curves, two methods have proven to be particularly practical and successful in recent years. Both methods rely on embedding the curve into an *abelian variety* and obtaining quite detailed information on the rational points on the latter. The first method then uses combinatorial arguments to arrive at detailed information on where rational points can lie. Under standard conjectures, one can show that the obstructions derived from this are also part of the Brauer-Manin obstruction, but the method is does not need to be formulated in that language and is much easier to use in practice.

  The second method uses p-adic analysis to prove that rational points need to be *isolated* in some sense. The method does not always apply, but if it does, it complements the first method almost perfectly and often allows the explicit determination of the rational points on curves.

2. Objective and format of the summer school

The objective of the workshop was to give the participants (primarily graduate students, ranging from starting master's students to finishing doctoral students) a working knowledge of current methods of solving Diophantine equations. Of course, one week is too short to expect that all participants become experts in all of the methods. So our goal was instead to bring them to the point where they would be aware of the general ideas, the range of application, and references for learning more, for each method.

We chose five main relevant methods and arranged for lecture series covering each method. We distributed these lecture over the days, such that every day started with 3 lectures.

In order for the participants to properly internalize the methods, we thought it would be important for them to see the methods in action. For that reason we arranged a rich set of assignments accompanying each lecture and ample time for the participants to work on these problems in groups. We closed every day with presentations of solutions to the problems, presented by participants. Not everybody would work on all problems, but at the end of the day they at least would see a solution presented by one of their peers, thus confirming to them that these problems are indeed doable.

Since this was a summer school, not a research meeting, we thought we would collect the best group of participants not by constructing our own invitation list but by having an open application and selection process. We sent out an announcement and collected letters of interest from candidates plus letters of recommendation from supervisors. We received more applications than we had places, so we did have to make a selection.

The timing of the summer school was kindly coordinated by BIRS to be adjacent to the twelfth meeting of the Canadian Number Theory Association in nearby Lethbridge. The CNTA conferences are important international meetings and is one of the most prominent number theory conferences in North America. Therefore, the opportunity for the participants to combine this relatively specialized summer school with a large number theory conference that allowed them to place the material just learned in the larger context of current number theoretic research was an exceptional opportunity.

3. Outcome of the meeting

We were extremely happy with the selection of participants. They formed an exceptionally motivated and talented group. We had no problem getting volunteers to present solutions and the participants worked very hard and successfully on the set problems.

The participants have provided feedback on the workshop, see
`http://www.birs.ca/events/2012/summer-schools/12ss131/testimonials`.

Many report not only on the relevance of the material they learned, but also on the contacts they made with other young researchers.

Another noteworthy resource was the availability of online recording of all lectures. One participant was unable to attend the first few days of the workshop due to outside circumstances. However, he was able to download recordings of all the lectures he missed and to watch them on the way to BIRS. By the time he arrived, he was fully up to date.

4. The Modular Method

The modular approach is a method for associating Galois representations having very little ramification to (non-trivial) solutions of certain Diophantine equations via Frey curves. Occassionaly, the method proves the non-existence of such solutions—this was the case with Wiles' proof of Fermat's Last Theorem. More commonly, it provides a vast amount of local data about the solutions; to completely solve the equations it is often necessary to combine this data with global information obtained via other methods such as linear forms in logarithms.

The approach rests of three major theoretical pillars. Theses are the Modularity Theorem (due to Wiles and others), the Level-Lowering Theorem (Ribet) and Mazur's criteria for the irreducibility of Galois representations (introduced here as statements about the non-existence of isogenies).

4.1. **Modularity.**

Theorem 1. *(The Modularity Theorem for Elliptic Curves) Associated to any* **rational** *newform $f = q + \sum_{n\geq 2} c_n q^n$ of level N and weight 2 is an elliptic curve $E_f/\mathbb{Q}$ of conductor N so that for all primes $l \nmid N$*

$$c_l = a_l(E_f)$$

where c_l is the l-th coefficient in the q-expansion of f and $a_l(E_f) = l + 1 - \#E_f(\mathbb{F}_l)$. For any given positive integer N, the association $f \mapsto E_f$ is a bijection between rational newforms of level N and isogeny classes of elliptic curves of conductor N.

The association $f \mapsto E_f$ is due to Shimura. The fact that this association is surjective was previously known as the Modularity Conjecture, and first proved for squarefree N (the semi-stable case) by Wiles [25], [24]. The proof was completed in a series of papers by Diamond [9], Conrad, Diamond and Taylor [7], and finally Breuil, Conrad, Diamond and Taylor [4].

4.2. **Level-Lowering.**

4.2.1. *'Arises From'.*

Definition 1. *Let E be an elliptic curve over the rationals of conductor N, and suppose that f is a newform of weight 2 and level N' with q-expansion $f = q + \sum_{i\geq 2} c_i q^i$, and coefficients c_i generating the number field $K/\mathbb{Q}$. We shall say that the curve E arises modulo p from the newform f (and write $E \sim_p f$) if there is some prime ideal $\mathfrak{P} \mid p$ of K such that for almost all primes l, we have $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$.*

In fact we can be a little more precise.

Proposition 2. *Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of K such that for all primes l*

(i) *if $l \nmid pNN'$ then $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$, and*
(ii) *if $l \nmid pN'$ and $l \,||\, N$ then $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$.*

If f is a rational newform, then we know that f corresponds to some elliptic curve F say (this is E_f in the notation of Theorem 1). If E arises modulo p from f then we shall also say that E arises modulo p from F (and write $E \sim_p F$).

Proposition 3. *(Kraus and Oesterlé* [14]*) Suppose that E, F are elliptic curves over $\mathbb{Q}$ with conductors N and N' respectively. Suppose that E arises modulo p from F. Then for all primes l*

(i) *if $l \nmid NN'$ then $a_l(E) \equiv a_l(F) \pmod{p}$, and*
(ii) *if $l \nmid N'$ and $l \,||\, N$ then $l + 1 \equiv \pm a_l(F) \pmod{p}$.*

4.2.2. *Ribet's Level-Lowering Theorem.* Let E be an elliptic curve over $\mathbb{Q}$. Let $\Delta = \Delta_{\min}$ be the discriminant for a minimal model of E, and N be the conductor of E. Suppose p is a prime, and let

$$N_p = N \Big/ \prod_{\substack{q||N, \\ p \mid \mathrm{ord}_q(\Delta)}} q. \tag{1}$$

Theorem 4. *(A simplified special case of Ribet's Level-Lowering Theorem) Suppose E is an elliptic curve over $\mathbb{Q}$ and $p \geq 5$ is prime. Suppose further that E does not have any p-isogenies. Let N_p be as defined above. Then there exists a newform f of level N_p such that $E \sim_p f$.*

4.3. **Absence of Isogenies.** To be able to apply Ribet's Theorem we must know that our elliptic curve E does not have a p-isogeny.

Theorem 5. *(Mazur* [18]*) Suppose $E/\mathbb{Q}$ is an elliptic curve and that* **at least one** *of the following conditions holds.*

- *$p \geq 17$ and $j(E) \notin \mathbb{Z}[\frac{1}{2}]$,*
- *or $p \geq 11$ and E is a semi-stable elliptic curve,*
- *or $p \geq 5$, $\#E(\mathbb{Q})[2] = 4$, and E is a semi-stable elliptic curve,*

Then E does not have any p-isogenies.

4.4. **Fermat's Last Theorem.**

Theorem 6. *(Wiles) Suppose $p \geq 5$ is prime. The equation*

$$x^p + y^p + z^p = 0 \tag{2}$$

has no solutions with $xyz \neq 0$.

Proof. Suppose $xyz \neq 0$. Without loss of generality: x, y, z are coprime, and

$$2 \mid y, \qquad x^p \equiv -1 \pmod 4, \qquad z^p \equiv 1 \pmod 4.$$

Associate to this solution the elliptic curve (called a Frey curve)

$$E : \quad Y^2 = X(X - x^p)(X + y^p).$$

So

$$\Delta = 16x^{2p}y^{2p}(x^p + y^p)^2 = 16x^{2p}y^{2p}z^{2p}$$

using $x^p + y^p + z^p = 0$. Also

$$c_4 = 16(z^{2p} - x^p y^p), \qquad \gcd(c_4, \Delta) = 16.$$

Applying Tate's algorithm to compute the minimal discriminant and conductor:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \qquad N = \prod_{\ell \mid xyz} \ell.$$

Moreover, $N_2 = 2$. Since $E(\mathbb{Q})[2] = 4$ and N squarefree, we know by Mazur's Theorem that E has no p-isogenies.

By Ribet, there is a newform f of level $N_p = 2$ and weight 2 such that $E \sim_p f$. However, there are no newforms of level 2 and weight 2. This gives a contradiction. □

The bibliography below provides some references for further study.

REFERENCES

[1] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[2] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine Equations of Signature* $(p, p, 3)$, Compositio Mathematica **140** (2004), 1399-1416.

[3] M. A. Bennett, *Recipes for ternary Diophantine equations of signature* (p, p, k), Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55

[4] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14 No.4** (2001), 843–939.

[5] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Mathematics **163** (2006), 969–1018.

[6] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell Equation*, Compositio Mathematica **142** (2006), 31–62.

[7] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[8] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.

[9] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. **144** (1996), no. 1, 137–166.

[10] E. Halberstadt and A. Kraus, *Sur les modules de torsion des courbes elliptiques*, Math. Ann. **310** (1998), 47–54.

[11] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. reine angew. Math. **548** (2002), 167âĂŤ234.

[12] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^p = z^2$ *et* $x^p + 2^\beta y^p = 2z^2$, Acta Arith. **108** (2003), 327–338.

[13] W. Ivorra and I. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$, Canad. J. Math. **58** (2006), 115–153.

[14] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

[15] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.

[16] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experimental Mathematics **7** (1998), No. 1, 1–13.

[17] A. Kraus, *On the Equation* $x^p + y^q = z^r$*: A Survey*, The Ramanujan Journal **3** (1999), 315–333.

[18] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[19] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[20] K. Ribet, *On the equation* $a^p + 2b^p + c^p = 0$, Acta Arith. **LXXIX.1** (1997), 7–15.

[21] J.-P. Serre, *Abelian* l*-adic representations and elliptic curves*, W. A. Benjamin, New York, 1968.

[22] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[23] S. Siksek and J. E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$, Acta Arith. **109.2** (2003), 143–149.

[24] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[25] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

5. LINEAR FORMS IN LOGARITHMS AND APPLICATIONS

A Diophantine equation (E) being given, our aim is to determine the complete list of its solutions, say, in rational integers. The first question is to decide whether (E) has only finitely many solutions or infinitely many. In the former situation, a refined information would be a bound for the total number N of solutions. Note that such a result cannot always be obtained: for instance, if one is able to show that the largest solution of (E) has no more than twice as many decimal digits as the smallest one, this gives no information on N. Furthermore, the knowledge of N is in general far from being sufficient for solving completely (E), since it is unlikely that (E) has exactly N solutions. In order to determine all the solutions to (E), we thus need an explicit upper bound B for the size (the absolute value) of the largest one. Then, at least in principle, it is possible to complete the resolution of (E) by simply checking which integers between $-B$ and B are solutions.

The first family of Diophantine equations on which a general result has been proved are the Thue equations, named after the Norwegian mathematician Axel Thue, who established in 1909 the following result.

Theorem 7. *Let* $F(X, Y)$ *be an irreducible, homogeneous, integer polynomial of degree at least* 3*. Let* b *be a non-zero integer. Then, the equation*

$$F(x, y) = b \qquad (T)$$

has only finitely many solutions in integers x *and* y*.*

Unfortunately, the method developed by Thue does not enable him to explicitly bound from above the absolute values of the solutions x and y to (T).

Such a result was obtained more than half a century after the publication of Thue's paper, by means of the theory of linear forms in the logarithms of algebraic numbers developed by Alan Baker at the end of the 60's and which can be presented as follows.

Let $n \geq 2$ be an integer. For $1 \leq i \leq n$, let x_i/y_i be a non-zero rational number and b_i a positive integer. Set

$$B := \max\{3, b_1, \ldots, b_n\}$$

and, for $1 \leq i \leq n$, set

$$A_i := \max\{3, |x_i|, |y_i|\}.$$

We assume that the rational number

$$\Lambda := \left(\frac{x_1}{y_1}\right)^{b_1} \cdots \left(\frac{x_n}{y_n}\right)^{b_n} - 1 \tag{1}$$

is non-zero. We wish to bound $|\Lambda|$ from below, thus we may assume that $|\Lambda| \leq 1/2$ and we get the *linear form in logarithms*

$$|\Lambda| \geq \frac{|\log(1+\Lambda)|}{2} = \frac{1}{2}\left|b_1 \log \frac{x_1}{y_1} + \cdots + b_n \log \frac{x_n}{y_n}\right|.$$

A trivial estimate of the denominator of (1) gives

$$\log|\Lambda| \geq -\sum_{i=1}^{n} b_i \log|y_i| \geq -B\sum_{i=1}^{n} \log A_i.$$

The dependence on the A_i's is very satisfactory, unlike the dependence on B. However, for applications to Diophantine problems, a better estimate in terms of B is needed, even if it comes with a weaker dependence in terms of the A_i's.

Alan Baker [1, 2] was the first to prove such a result, and we are now able to show that, under the above assumptions, there exists an effectively computable constant $c(n)$, depending only on the number n of rational numbers involved, such that the lower estimate

$$\log|\Lambda| \geq -c(n)\, \log A_1 \ldots \log A_n \log B$$

holds.

More generally, one can get analogous lower bounds if the rational numbers x_i/y_i are replaced by algebraic numbers α_i, the quantity $\log A_i$ being then essentially the absolute logarithmic height of α_i. Further information, including precise estimates and detailled proofs, can be found in the textbook of Waldschmidt [5].

Quantities like (1) occur naturally when one studies certain families of Diophantine equations, like the Thue equations or the superelliptic and hyperelliptic equations $f(x) = y^m$, where $f(X)$ is an integer polynomial and $m \geq 2$ is a fixed integer. Baker's theory can then be applied to get upper bounds for the size of the solutions to these equations (under some necessary assumptions: one must e.g. exclude the Pell equations like $x^2 - dy^2 = 1$). It also applies to the more general equation $f(x) = y^z$ in the three unknowns x, y, z (again, under some necessary assumptions).

The most striking application of Baker's theory is Tijdeman's theorem on Catalan's problem, which was posed in 1844 and is the following: do there exist consecutive positive integers other than 8 and 9 which are both pure powers? This corresponds to the exponential Diophantine equation

$$x^m - y^n = 1,$$

which has been solved completely only in 2002, by Mihăilescu. In 1976, Tijdeman used Baker's theory to prove the finiteness of the number of pairs of consecutive integers which are both perfect powers.

Theorem 8. *Let x, y, $m \geq 2$, and $n \geq 2$ be strictly positive integers such that $x^m - y^n = 1$. There exists an effectively computable, absolute constant C such that $\max\{x, y, m, n\} < C$.*

We direct the reader to the monographs [3, 4] for many applications of Baker's theory to Diophantine equations.

REFERENCES

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 12 (1966), 204–216.
[2] A. Baker, *A sharpening of the bounds for linear forms in logarithms I–III*, Acta Arith. 21 (1972), 117–129; 24 (1973), 33–36; 27 (1975), 247–252.
[3] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics 87, Cambridge University Press, Cambridge, 1986.
[4] V. G. Sprindžuk, Classical Diophantine Equations, Lecture Notes in Math. 1559, Springer-Verlag, Berlin, 1993.
[5] M. Waldschmidt, Diophantine Approximation on Linear Algebraic Groups. Transcendence Properties of the Exponential Function in Several Variables, Grundlehren Math. Wiss. 326, Springer, Berlin, 2000.

6. THE HYPERGEOMETRIC METHOD

Bennett's lecture was an overview of the most classical version of the hypergeometric method and its applications to Diophantine equations. In this context, this method behaves in a similar fashion to lower bounds for linear forms in two logarithms (archimedean or otherwise), with the (substantial) drawback that it is not generally applicable, but with the advantage that, when it can be applied, the results are typically extremely sharp. Combined with gap principles (usually of an elementary nature), this technique can often be applied to bound the number of rational of integral points on certain specific curves or surfaces.

6.1. **Rational approximation.** While the hypergeometric method in general relates to approximation to special values of hypergeometric series, typically via special values of Padé approximations, in its most classical sense (at least from the viewpoint of Diophantine equations), it concerns rational approximation to irrational numbers. Bennett discussed the case of rational approximations to π and to algebraic number of the form $(a/b)^{m/n}$, via specialization of Padé approximants (in the latter case, to the binomial function $(1-z)^{m/n}$). By extending these ideas to working over imaginary quadratic fields, one is able to give an alternative proof of an old theorem of Ljunggren, to the effect that the positive integral solutions to the Diophantine equation $x^2-2y^4=-1$ are given by $(x,y)=(1,1)$ and $(239,13)$. This apparently unmotivated equation arises in a surprising number of places, including in Machin's formula for computing digits of π.

6.1.1. *Some details.* The underlying principle of the hypergeometric method, as it applies to rational approximation, is the following.

Suppose that we are given a real number θ that we wish to prove to be irrational. One way to do this is to find a sequence of distinct rational approximations p_n/q_n to θ (here, p_n and q_n are integers) with the property that there exist positive real numbers α, β, a and b with $\alpha, \beta > 1$,

$$|q_n| < a \cdot \alpha^n, \quad \text{and} \quad |q_n\theta - p_n| < b \cdot \beta^{-n},$$

for all $n \in \mathbb{N}$. If we can construct such a sequence, we in fact get rather more. Namely, we obtain the inequality

$$\left|\theta - \frac{p}{q}\right| > \left(2\,a\,\alpha\,(2\,b\,\beta)^{\lambda}\right)^{-1} |q|^{-1-\lambda} \quad \text{for} \quad \lambda = \frac{\log\alpha}{\log\beta}, \tag{3}$$

valid for *all* integers p and $q \neq 0$ (at least provided $|q| > 1/2b$). To see this, note that

$$\left|\theta - \frac{p}{q}\right| \geq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| - \left|\theta - \frac{p_n}{q_n}\right|,$$

and hence if $p/q \neq p_n/q_n$, we have

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{|q_n|}\left(\frac{1}{|q|} - \frac{b}{\beta^n}\right).$$

Now we choose n minimal such that $\beta^n \geq 2\,b\,|q|$ (since we assume $|q| > 1/2b$, n is a positive integer). Then

$$\beta^{n-1} < 2\,b\,|q| \leq \beta^n$$

and so

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{2\,|q\,q_n|} > \frac{1}{2\,|q|\,a\,\alpha^n} = \frac{1}{2\,|q|\,a\,\beta^{\lambda n}} < \frac{1}{2\,|q|\,a\,(2|q|\,b\,\beta)^{\lambda}}.$$

If instead we have $p/q = p_n/q_n$ for our desired choice of n, we argue similarly, only with n replaced by $n+1$ (whereby the fact that our approximations are distinct guarantees that $p/q \neq p_{n+1}/q_{n+1}$). The slightly weaker constant in (3) results from this case.

An inequality of the shape

$$\left|\theta - \frac{p}{q}\right| > |q|^{-\kappa},$$

valid for suitably large integers p and q is termed an *irrationality measure*. For real transcendental θ, any such measure is in some sense nontrivial. For algebraic θ, say of degree n, however, Liouville's theorem provides a "trivial" lower bound of n for κ.

6.1.2. *Padé approximants to* $(1-z)^{1/m}$. Given a formal power series $f(z)$ and positive integers r and s, it is an exercise in linear algebra to deduce, for fixed integer n, the existence of nonzero polynomials $P_{r,s}(z)$ and $Q_{r,s}(z)$ with rational integer coefficients and degrees r and s, respectively, such that

$$P_{r,s}(z) - f(z)\, Q_{r,s}(z) = z^{r+s+1} E_{r,s}(z)$$

where $E_{r,s}(z)$ is a power series in z. In certain situations, these *Padé approximants* (which are unique up to scaling) can be written down in explicit fashion. Such is the case for $f(z) = (1-z)^{1/m}$. Indeed, if we define, taking $r = s = n$ for simplicity,

$$P_n(z) = \sum_{k=0}^{n} \binom{n+1/m}{k} \binom{2n-k}{n} (-z)^k$$

and

$$Q_n(z) = \sum_{k=0}^{n} \binom{n-1/m}{k} \binom{2n-k}{n} (-z)^k,$$

then there exists a power series $E_n(z)$ such that for all complex z with $|z| < 1$,

$$P_n(z) - (1-z)^{1/m}\, Q_n(z) = z^{2n+1} E_n(z). \tag{4}$$

How could we go about discovering these polynomials for ourselves? Let us write

$$I_n(z) = \frac{1}{2\pi i} \int_\gamma \frac{(1-wz)^{n+1/m}}{(w(w-1))^{n+1}} dw,$$

where γ is a closed counter-clockwise contour enclosing 0 and 1. Here, by $(1+t)^{1/m}$ for t a complex number with $|t| < 1$, we mean

$$(1+t)^{1/m} = \sum_{k=0}^{\infty} \binom{1/m}{k} t^k.$$

In fact, expanding the binomial series, we may write

$$I_n(z) = \sum_{h=0}^{\infty} \binom{n+1/m}{h} (-z)^h J_h,$$

where

$$J_h = \frac{1}{2\pi i} \int_\gamma \frac{w^{h-n-1}}{(w-1)^{n+1}} dw.$$

As is well-known, the integral of a rational function $P(w)/Q(w)$ over a closed contour enclosing its poles vanishes, provided the degree of the polynomial Q exceeds that of P by at least 2. We thus have $J_h = 0$ for $0 \le h \le 2n$. To find the shape of the coefficients of $P_n(z)$ and $Q_n(z)$ involves a residue calculation.

To actually apply the hypergeometric method, we need some inequalities.

Lemma 9. *Let n be a positive integer and suppose that z is a complex number with $|1-z| \le 1$. Then*

(i) *We have*

$$|P_n(z)| < 4^n,\ |Q_n(z)| < 4^n \ \text{ and } \ |E_n(z)| < 4^{-n}(1-|z|)^{-\frac{1}{2}(2n+1)}.$$

(ii) *For all complex numbers $z \neq 0$, we have*

$$P_n(z) Q_{n+1}(z) \neq P_{n+1}(z) Q_n(z).$$

(iii) *If we define*

$$\sigma_{k,m} = \prod_{p|m} p^{[k/(p-1)]},$$

then

$$\sigma_{k,m} m^k \binom{n \pm 1/m}{k} \in \mathbb{Z}.$$

(iv) *If we define $G_{n,m}$ to be the largest positive integer such that*

$$\frac{\sigma_{n,m} m^n P_n(z)}{G_{n,m}} \text{ and } \frac{\sigma_{n,m} m^n Q_n(z)}{G_{n,m}}$$

are both polynomials with integer coefficients, then

$$G_{n,3} > \frac{1}{42}\, 2^n \text{ and } G_{n,4} > (3/2)^n,$$

for all $n \in \mathbb{N}$.

6.1.3. *Consequences.* Arguing carefully with the results of the preceding subsection, we can prove, by way of example, inequalities of the shape

$$\left|x^3 - 2y^3\right| \geq \sqrt{|x|},$$

valid for all integers x and y.

Combining this machinery with various gap principles, leads one (after, it must be confessed, a certain amount of work) to conclude that the general equation $|ax^n - by^n| = 1$ has, for fixed nonzero integers a, b and $n \geq 3$, at most one solution in positive integers x and y.

More generally, we can apply these methods to bound solutions to the number of solutions to S-unit equation, Thue equations and Thue-Mahler equations, as well as to wide classes of exponential equations.

REFERENCES

[1] A. BAKER, "Rational approximations to certain algebraic numbers", *Proc. London Math. Soc. (3)* **14** (1964), 385–398.
[2] A. BAKER, "Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers", *Quart. J. Math. Oxford Ser. (2)* **15** (1964), 375–383.
[3] M. BENNETT, "Simultaneous rational approximation to binomial functions", *Trans. Amer. Math. Soc.* **348** (1996), 1717–1738.
[4] M. BENNETT, "Effective measures of irrationality for certain algebraic numbers", *J. Austral. Math. Soc.* **62** (1997), 329–344.
[5] M. BENNETT, "Explicit lower bounds for rational approximation to algebraic numbers", *Proc. London Math. Soc.* **75** (1997), 63–78.
[6] F. BEUKERS, " A note on the irrationality of $\zeta(2)$ and $\zeta(3)$", *Bull. London Math. Soc.* **11** (1979), no. 3, 268–272.
[7] J.H. CHEN, "A new solution of the Diophantine equation $X^2 + 1 = 2Y^4$", *J. Number Theory* **48** (1994), no. 1, 62–74.
[8] G.V. CHUDNOVSKY, "On the method of Thue-Siegel", *Ann. Math. II Ser.* **117** (1983), 325–382.
[9] C.L. SIEGEL, "Die Gleichung $ax^n - by^n = c$", *Math. Ann.* **114** (1937), 57–68.
[10] A. THUE, "Berechnung aller Lösungen gewisser Gleichungen von der form", *Vid. Skrifter I Mat.-Naturv. Klasse* (1918), 1–9.

7. COHOMOLOGICAL OBSTRUCTIONS TO RATIONAL POINTS

Poonen's four lectures focused on the problem of deciding whether a variety has a rational point, in particular on the use of cohomological methods to prove that a variety has no rational point. He presented introductions to the Brauer–Manin obstruction and the descent obstruction, starting from the basic definitions, and working up to the statements of recent results comparing their relative strengths.

7.1. **Testing for local points.** Let k be a number field. For each place v of k, let k_v be the completion. For nonarchimedean v, let $\mathcal{O}_v$ be the valuation ring of k_v. The adele ring $\mathbf{A}$ of k is the restricted direct product $\prod_v'(k_v, \mathcal{O}_v)$. Let X be a nice k-variety, by which we mean a smooth projective geometrically integral variety over k.

If X is over $\mathbb{Q}$, for instance, sometimes one can prove that X has no $\mathbb{Q}$-point by proving that X has no $\mathbb{R}$-point. More generally, one can test all the completions. This can be summarized by the observation that $X(k)$ embeds diagonally into $X(\mathbf{A}) = \prod_v X(k_v)$ (equality holds since X is projective), so if $X(\mathbf{A}) = \emptyset$, then $X(k) = \emptyset$. Moreover, it is usually easy to decide whether $X(\mathbf{A})$ is empty or not, since one can compute in advance a finite set S of places such that $X(k_v)$ is nonempty for $v \notin S$, and then using real algebraic geometry or Hensel's lemma to treat the finitely many $v \in S$.

Since the 1940s, however, it has been known that there exist examples of nice varieties X such that $X(\mathbf{A}) \neq \emptyset$ but $X(k) = \emptyset$ [10, 13]. Many such examples can be explained in a systematic way by defining

subsets $X(\mathbf{A})^{\mathrm{Br}}$ and $X(\mathbf{A})^{\mathrm{descent}}$ of $X(\mathbf{A})$ known to contain $X(k)$. The emptiness of such a subset is an obstruction to the existence of a k-point.

7.2. **Brauer groups of fields.** The first of the obstructions is defined by using the Brauer group. For a field k, with separable closure k^{sep}, one defines an Azumaya algebra over k to be a twist of a matrix algebra, i.e., a k-algebra A (associative with 1) such that $A \otimes_k k^{\mathrm{sep}} \simeq M_n(k^{\mathrm{sep}})$ for some $n > 0$. An example is the quaternion algebra (a, b) over a field k of characteristic not 2 defined by $a, b \in k^\times$: it is the associative k-algebra generated by i and j modulo the 2-sided ideal generated by the relations $i^2 = a$, $j^2 = b$, $ji = -ij$. Two Azumaya algebras A and B are called equivalent if $M_n(A) \simeq M_m(B)$ for some $m, n > 0$. The Brauer group $\mathrm{Br}\, k$ is the set of equivalence classes of Azumaya algebras over k, with group law given by tensor product. Alternatively, $\mathrm{Br}\, k$ can be defined as the Galois cohomology group $H^2(k, \mathbb{G}_m)$. For example, if k is a local field, then there is an injection $\mathrm{Br}\, k \overset{\mathrm{inv}}{\hookrightarrow} \mathbb{Q}/\mathbb{Z}$ that is an isomorphism if k is nonarchimedean.

7.3. **Brauer groups of schemes.** Either definition can be extended to an arbitrary scheme X, by replacing the extension k^{sep} of k by an étale cover of X, and by replacing Galois cohomology by étale cohomology. In this way one obtains an Azumaya Brauer group and a cohomological Brauer group of X. A theorem of Gabber and de Jong [6] shows that they coincide for reasonable schemes X, e.g., any scheme X that is quasi-projective over a noetherian ring.

If X is a regular integral variety with function field K, then $\mathrm{Br}\, X$ can be understood as a subgroup of $\mathrm{Br}\, K$. More precisely, if X is a regular integral variety over a field k of characteristic 0, then there is an exact sequence

$$0 \to \mathrm{Br}\, X \to \mathrm{Br}\, K \overset{\mathrm{res}}{\to} \prod_D H^1(k(D), \mathbb{Q}/\mathbb{Z}),$$

where D ranges over irreducible divisors on X, and $k(D)$ is its function field. Another way to try to understand $\mathrm{Br}\, X$ concretely is to use the Hochschild–Serre spectral sequence in étale cohomology, which yields the exact sequence

$$0 \to \mathrm{Pic}\, X \to (\mathrm{Pic}\, X^{\mathrm{sep}})^G \to \mathrm{Br}\, k \to \ker(\mathrm{Br}\, X \to \mathrm{Br}\, X^{\mathrm{sep}}) \to H^1(k, \mathrm{Pic}\, X^{\mathrm{sep}}) \to H^3(k, \mathbb{G}_m).$$

7.4. **The Brauer–Manin obstruction.** Suppose that X is a nice variety over a global field k. Given $A \in \mathrm{Br}\, X$, one constructs a diagram

$$\begin{array}{ccccccccc} & & X(k) & \hookrightarrow & X(\mathbf{A}_k) & & & & \\ & & \downarrow{\scriptstyle \mathrm{ev}_A} & & \downarrow{\scriptstyle \mathrm{ev}_A} & \searrow^{\phi_A} & & & \\ 0 & \to & \mathrm{Br}\, k & \to & \bigoplus_v \mathrm{Br}\, k_v & \xrightarrow{\sum \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} & \to & 0, \end{array}$$

which shows that the set $X(\mathbf{A})^A := \phi_A^{-1}(0)$ contains $X(k)$. Define the Brauer set $X(\mathbf{A})^{\mathrm{Br}} := \bigcap_{A \in \mathrm{Br}\, X} X(\mathbf{A})^A$; it too contains $X(k)$.

Example: Birch and Swinnerton-Dyer [1] proved that the nice variety X defined by

$$uv = x^2 - 5y^2$$
$$(u + v)(u + 2v) = x^2 - 5z^2$$

in $\mathbb{P}^4_{\mathbb{Q}}$ has a $\mathbb{Q}_p$-point for all $p \leq \infty$ but no $\mathbb{Q}$-point. The nonexistence of a $\mathbb{Q}$-point can be explained by using the quaternion algebra $(5, (u + v)/u)$ to show that $X(\mathbf{A})^{\mathrm{Br}} = \emptyset$.

7.5. **The Brauer–Manin obstruction for abelian varieties and curves.** If A is an abelian variety over a global field, let $A(\mathbf{A})_\bullet$ be the quotient of $A(\mathbf{A})$ by its connected component; one may then define $A(\mathbf{A})^{\mathrm{Br}}_\bullet$. Work of Manin [11] implies that if the Shafarevich-Tate group $Ш(A)$ is finite, then $A(\mathbf{A})^{\mathrm{Br}}_\bullet$ equals the closure of $A(k)$ in $A(\mathbf{A})_\bullet$.

Scharaschkin [14] used this to show that if X is a nice curve of genus $g \geq 2$ over a number field with a Galois-stable divisor class of degree 1, which lets one embed X in its Jacobian A, and if $Ш(A)$ is finite, then $X(\mathbf{A})^{\mathrm{Br}}_\bullet = X(\mathbf{A})_\bullet \cap \overline{A(k)}$; conjecturally this equals the closure of $X(k)$ in $A(\mathbf{A})_\bullet$. This result suggests the Mordell-Weil sieve, a practical method for proving $X(k)$ empty.

7.6. **Torsors.** Let G be a linear algebraic group (smooth affine group scheme of finite type over a field k). The trivial G-torsor is G equipped with the right translation action of G. A G-torsor is a twist of this: a k-scheme Y equipped with a right action of G such that the base extension Y^{sep} is isomorphic to G^{sep} as k^{sep}-scheme with right G^{sep}-action. Examples: $Y\colon x^2+y^2=-3$ with the action of $G\colon x^2+y^2=1$, or any genus 1 curve with the action of its Jacobian. One can show that a G-torsor is trivial if and only if it has a k-point. The set of isomorphism classes of G-torsors is in bijection with $H^1(k,G)$.

One can generalize and define a G-torsor over a base variety X instead of just $\operatorname{Spec} k$. This is a scheme $Y\to X$ with right G-action such that its pullback $Y'\to X'$ by some étale surjective morphism $X'\to X$ isomorphic to $X'\times_k G$ with the obvious right G-action. Example: $Y=X=E$ and $G=E[2]$ for some elliptic curve E over a field k of characteristic not 2, and $Y\to X$ is the multiplication-by-2 map.

7.7. **Descent obstruction.** We present the theory of [9], generalizing [2, 3, 4]. Let k be a number field. Let $f\colon Y\to X$ be a G-torsor over X as above. There is a map $X(k)\to H^1(k,G)$ sending x to the class of the G-torsor $f^{-1}(x)$ over k. For each 1-cocycle $\sigma\in Z^1(k,G)$, one defines a twisted torsor $f^\sigma\colon Y^\sigma\to X$. Then

$$\begin{aligned} X(k) &= \coprod_{[\sigma]\in H^1(k,G)} \{x\in X(k) : (\text{class of } f^{-1}(x)) = [\sigma]\} \\ &= \coprod_{[\sigma]} f^\sigma(Y^\sigma(k)) \\ &\subseteq \bigcup_{[\sigma]} f^\sigma(Y^\sigma(\mathbf{A})) \\ &=: X(\mathbf{A})^f. \end{aligned}$$

Define $X(\mathbf{A})^{\mathrm{descent}}=\bigcap X(\mathbf{A})^f$ where f ranges over all G-torsors for all linear algebraic groups G over k. If one restricts the possibilities for G to connected algebraic groups, one obtains $X(\mathbf{A})^{\mathrm{connected}}$, which Harari [8] proved was equal to $X(\mathbf{A})^{\mathrm{Br}}$. In particular, $X(\mathbf{A})^{\mathrm{descent}}\subseteq X(\mathbf{A})^{\mathrm{Br}}$.

One can also define variants, by replacing $Y^\sigma(\mathbf{A})$ in the definition of $X(\mathbf{A})^f$ by a subset such as $Y^\sigma(\mathbf{A})^{\mathrm{Br}}$. Doing this and letting G range over finite étale groups leads to the étale-Brauer set $X(\mathbf{A})^{\mathrm{et,Br}}$, which was proved by Demarche [7] and Skorobogatov [15] to equal $X(\mathbf{A})^{\mathrm{descent}}$.

Example: Using ideas of Darmon [5], the proof of Fermat's last theorem can be reinterpreted using the descent obstruction.

All these obstructions are insufficient to answer the question of whether a $\mathbb{Q}$-variety has a rational point: there is a nice $\mathbb{Q}$-variety for which $X(\mathbf{A})^{\mathrm{et,Br}}\neq\emptyset$ but nevertheless $X(\mathbb{Q})=\emptyset$ [12].

REFERENCES

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. The Hasse problem for rational surfaces. *J. Reine Angew. Math.*, 274/275:164–174, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

[2] C. Chevalley and A. Weil. Un théorème d'arithmétique sur les courbes algébriques. *Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris*, 195:570– 572, 1930.

[3] J.-L. Colliot-Thélène and J.-J. Sansuc. *La descente sur les variétés rationnelles*. 1980.

[4] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. La descente sur les variétés rationnelles. ii. *Duke Math. J.*, 54(2):375–492, 1987.

[5] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1):3– 14, 1997.

[6] A. J. De Jong. A result of Gabber. Preprint.

[7] Cyril Demarche. Obstruction de descente et obstruction de brauer-manin étale. *Algebra Number Theory*, 3(2):237–254, 2009.

[8] David Harari. Groupes algébriques et points rationnels. *Math. Ann.*, 322(4):811–826, 2002.

[9] David Harari and Alexei N. Skorobogatov. Non-abelian cohomology and rational points. *Compositio Math.*, 130(3):241–273, 2002.

[10] Carl-Erik Lind. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom geschlecht Eins. *Thesis, University of Uppsala,*, 1940:97, 1940.

[11] Y. I. Manin. *Le groupe de Brauer-Grothendieck en géométrie diophantienne*. Gauthier-Villars, 1971.

[12] Bjorn Poonen. Insufficiency of the Brauer-Manin obstruction applied to étale covers. *Ann. of Math. (2)*, 171(3):2157–2169, 2010.

[13] Hans Reichardt. Einige im kleinen überall lösbare, im grossen unlösbare diophantische gleichungen. *J. reine angew. Math.*, 184:12–18, 1942.

[14] Victor Scharaschkin. *Local-global problems and the Brauer-Manin obstruction*. 1999. Ph.D. thesis, University of Michigan.

[15] Alexei Skorobogatov. Descent obstruction is equivalent to étale Brauer-Manin obstruction. *Math. Ann.*, 344(3):501–510, 2009.

8. MORDELL-WEIL SIEVING AND CHABAUTY'S METHOD

Bruin's lectures mainly covered methods that in practice often allow the explicit determination of integral and rational points on curves. Heuristically one expects that these methods should work always work eventually. This is in stark contrast with the negative results proved by Matyasevitch and Davis-Putnam-Robinson, that there is no general method to decide whether a polynomial equation has any integral solutions. The key difference here is that the class of equations describing curves is restricted and does not include the type of equations that provide the counterexamples.

The method of Mordell-Weil sieving considers a curve C embedded in a group variety J. For integer points, J can be a semiabelian variety; for rational points J is an abelian variety. The group of integral points on J in either case forms a finitely generated abelian group (and in the case where J is an abelian variety, this is the same as the group of rational points, because J is projective). Mordell-Weil sieving (which, in the case when J is a multiplicative group is more appropriately named Dirichlet sieving), is based on considering the following commutative diagram for an appropriate constant $B \in \mathbb{Z}_{>1}$ and an appropriate finite set of primes S.

$$\begin{array}{ccc} C(\mathbb{Z}) & \xrightarrow{\iota} & J(\mathbb{Z})/BJ(\mathbb{Z}) \\ \downarrow & & \downarrow \prod \rho_p \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\iota_S} & \prod_{p\in S} \dfrac{J(\mathbb{F}_p)}{B \operatorname{im} \rho_p} \end{array}$$

If C is hyperbolic, then all sets in the above diagram are finite and if B is appropriately chosen, then ι is injective. With appropriately chosen B, S, we have that $J(\mathbb{Z})/BJ(\mathbb{Z})$ and $\prod_{p\in S} C(\mathbb{F}_p)$ are so small compared to the set they are mapped into, that one expects the intersection of the images of $\prod \rho_p$ and ι_S to be extremely small [5]. In particular, for appropriate B, S one expects that $(\operatorname{im} \prod \rho_p) \cap (\operatorname{im} \iota_S)$ is in bijection with $C(\mathbb{Z})$. See [3] for details. Subject to standard conjectures, obstructions arising from this construction can be interpreted as part of the Brauer-Manin obstruction [6].

A method almost perfectly complementing sieving is the observation that if $J(\mathbb{Z})$ is of sufficiently low rank then one can construct a p-adic analytic function

$$\Theta_p : C(\mathbb{Z}_p) \to \mathbb{Q}_p$$

that vanishes on $C(\mathbb{Z})$. This gives us a way to prove that integral points cannot lie p-adically too close to one another. In particular, this usually is capable of proving that there can be at most one integer point in a fiber of the composition $C(\mathbb{Z}) \to J(\mathbb{F}_p)$. Together with Mordell-Weil sieving, this can usually determine a sharp bound on the number of integral or rational points. See [1] for evidence. This method is originally due to observations by Chabauty [4], building on ideas of Skolem for determining integral solutions.

In all cases, one needs to find an embedding of C into some appropriate group variety. This is always possible if $C(\mathbb{Z})$ is non-empty. Obstructions to this can be determined via *descent obstructions* (see Section 7.7). These can also be made relatively efficiently computable [2].

REFERENCES

[1] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[2] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Math. Comp.*, 78(268):2347–2370, 2009.

[3] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[4] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[5] Bjorn Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15:415–420, 2006.

[6] Victor Scharaschkin. *Local-global problems and the Brauer-Manin obstruction*. 1999. Ph.D. thesis, University of Michigan.