Solving S-unit and Mordell equations via Shimura–Taniyama conjecuture

Benjamin Matschke
(joint work with Rafael von Känel)

In this talk certain geometry of numbers (discrete geometry) aspects of the project [5] have been presented. The plan of the present abstract is as follows. We first summarize the content of [5]. Then we briefly discuss S-unit and Mordell equations and we state parts of the results of [5]. Finally we mention two problems related to non-convex polytopes, which are motivated by [5].

Summary. Mordell and S-unit equations are classical Diophantine equations. In [5] we construct two types of practical algorithms that solve S-unit and Mordell equations. The first type builds on Cremona's algorithm using modular symbols. The second type combines explicit height bounds with sieving and enumeration algorithms. Here we conduct some effort to work out optimized height bounds and to construct refined enumeration algorithms (e.g. we develop a refined de Weger sieve and we obtain a global elliptic logarithm sieve). To illustrate the utility of our algorithm we solved large classes of S-unit and Mordell equations, and we used the resulting data to motivate various questions (e.g. Baker's explicit *abc*-conjecture) related to these fundamental Diophantine equations. Furthermore we establish new results for Mordell equations, which for example directly imply improved versions of two old theorems of Coates on the difference of coprime squares and cubes. Our results and algorithms all crucially rely on the Shimura–Taniyama conjecture [8, 6, 2] combined with the method of Faltings [3] (Arakelov, Paršin, Szpiro) and they do not use the theory of logarithmic forms.

Mordell and S-unit equations. Let S be a finite set of rational primes and let $N_S = \prod_{p\in S} p$. Denote by $\mathcal{O} = \mathbb{Z}[1/N_S]$ the ring of S-integers and by $\mathcal{O}^\times$ their units, the S-units. We consider the classical S-unit equation

$$x + y = 1, \quad x, y \in \mathcal{O}^\times. \tag{1}$$

Many important Diophantine problems can be reduced to the study of S-unit equations. For example, the *abc*-conjecture of Masser–Oesterlé is equivalent to a certain height bound for the solutions of S-unit equations. On using Diophantine approximations à la Thue–Siegel, Mahler (1933) showed that (1) has only finitely many solutions. Furthermore there already exists a practical algorithm of de Weger [7] which solves the S-unit equation (1) using the theory of logarithmic forms [1]. Next we take a non-zero $a \in \mathcal{O}$ and we consider the Mordell equation

$$y^2 = x^3 + a, \quad x, y \in \mathcal{O}. \tag{2}$$

This equation is a priori more difficult than (1). The simplest case $\mathcal{O} = \mathbb{Z}$ of equation (2) goes back at least to Bachet (1621). For this case, using a Diophantine approximation result of Thue, Mordell (1923) showed that (2) has only finitely many solutions. Furthermore there already exist practical algorithms which resolve Mordell equations (2) by using the theory of logarithmic forms [1].

Algorithm for S-unit equation. We first describe the main ingredients for our algorithm solving the S-unit equation (1) by using height bounds. The Shimura–Taniyama conjecture together with Faltings' method leads to explicit height bounds for the S-unit equation (1). For practical purposes, these bounds are the actual best ones. However they are still too large to check all candidates with height below this bound. A method of de Weger [7], using Diophantine approximation and the LLL lattice reduction algorithm, can considerably reduce these bounds in practice. In [5] we refined the reduction method, we worked out a refined sieve which is very efficient for sets S of cardinality at least 6, and we developed an improved enumeration of solutions with very small height. Here we used ideas and methods from geometry of numbers (discrete geometry).

We now discuss some results which we obtained by using the above described algorithm. To solve the S-unit equation (1), it is natural to consider the set $\Sigma(S)$ of solutions of (1) modulo symmetry. Here two solutions (x, y) and (x', y') are called symmetric if x' or y' lies in $\{x, \frac{1}{x}, \frac{1}{1-x}\}$. Previously, de Weger [7] computed the set $\Sigma(S)$ in the case $S = \{2, 3, 5, 7, 11, 13\}$. We obtained the following theorem.

Theorem 1. *Let $n \in \{1, 2, \ldots, 16\}$ and let $S(n)$ be the set of the n smallest rational primes. The cardinality $\#$ of $\Sigma(S(n))$ is given in the following table.*

n	1	2	3	4	5	6	7	8
$\#$	1	4	17	63	190	545	1433	3649
n	9	10	11	12	13	14	15	16
$\#$	8828	20015	44641	95358	199081	412791	839638	1663449

Let $N \in \{1, 10, \ldots, 10^7\}$. If $\Sigma(N) = \cup_S \Sigma(S)$ with the union taken over all sets S with $N_S \leq N$, then the cardinality $\#$ of $\Sigma(N)$ is given in the following table.

N	1	10	10^2	10^3	10^4	10^5	10^6	10^7
$\#$	0	5	42	354	2362	13902	79125	432408

In fact our algorithm completely determined the sets $\Sigma(S(n))$ and $\Sigma(N)$ appearing in the above theorem. Further we remark that given the set $\Sigma(S)$, one can directly write down all solutions of the S-unit equation (1).

Mordell equations and primitive solutions. To discuss some results for Mordell equations (2), we need to introduce more notation. Following Bombieri–Gubler, we say that $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is primitive if ± 1 are the only $n \in \mathbb{Z}$ with n^6 dividing $\gcd(x^3, y^2)$. In particular $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is primitive if x, y are coprime. To measure the finite set S and $a \in \mathcal{O}$, we take

$$a_S = 1728 N_S^2 \prod p^{\min(2, \mathrm{ord}_p(a))}$$

with the product taken over all rational primes $p \notin S$. Let h be the usual logarithmic Weil height with $h(n) = \log |n|$ for $n \in \mathbb{Z} - \{0\}$. Building on the arguments of [4, Cor 7.4], we establish the following result.

Theorem 2. *Let $a \in \mathbb{Z}$ be nonzero. Assume that $y^2 = x^3 + a$ has a solution in $\mathbb{Z} \times \mathbb{Z}$ which is primitive. Then any $(x, y) \in \mathcal{O} \times \mathcal{O}$ with $y^2 = x^3 + a$ satisfies*

$$\max\big(h(x), \tfrac{2}{3}h(y)\big) \leq a_S \log a_S.$$

We now discuss several aspects of this result. A useful feature of Theorem 2 is that it does not involve $|a|$. To illustrate this we take $n \in \mathbb{Z}_{\geq 1}$, we let $\mathcal{F}_n$ be the infinite family of integers a with radical $\mathrm{rad}(a)$ at most n, and we put $a_* = a_S$ for S empty. Then it holds $a_* \leq 1728\mathrm{rad}(a)^2$ and we obtain the following corollary.

Corollary. *For any $n \in \mathbb{Z}_{\geq 1}$, the set of primitive $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $y^2 - x^3 \in \mathcal{F}_n$ is finite and can in principle be determined. Furthermore if $a \in \mathbb{Z}$ satisfies $\log |a| \geq a_* \log a_*$, then there are no primitive $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $y^2 - x^3 = a$.*

Two problems in discrete geometry. The following problem is motivated by the global elliptic logarithm sieve constructed in [5]. This sieve is applied in our algorithm, which solves the Mordell equation (2) by using height bounds.

Problem. *Let $A := \mathbb{R}^n_{\geq 0}$. Given $k \geq n$, how does one choose $x_1, \ldots, x_k \in A$ with $||x_1||_1 = \ldots = ||x_k||_1 = 1$ such that $\sup\{||a||_1 \ : \ a \in A \backslash \bigcup_i (x_i + A)\}$ is minimal?*

In [5] we chose some reasonable x_i, but they are probably not yet optimal. In practice, approximately optimal solutions are good enough. Our refined sieve for the S-unit equation (1) motivates a similar but a bit more technical problem.

Problem. *Let $[n] = \{1, \ldots, n\}$. For any $X = (J, x)$ with $J \subseteq [n]$ and $x \in \mathbb{R}^J_{\geq 0}$ with $||x||_1 = 1$, define $A(X) = \{a \in \mathbb{R}^{[n]} \ : \ a_j \leq x_j \text{ for some } j \in J\}$ and $B(X) = A(X) \cap (-A(X))$. Given $k \geq n$, how does one choose k such pairs $X_1, \ldots, X_k$ such that $\sup\{||a||_1 \ : \ a \in \bigcap_i B(X_i)\}$ is minimal?*

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, volume 9 of *New Mathematical Monographs*. Cambridge University Press, 2007.

[2] 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(4) (2001), 843–939.

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73(3) (1983), 349–366.

[4] R. von Känel, *Integral points on moduli schemes of elliptic curves*, Trans. London Math. Soc. 1(1) (2014), 85–115.

[5] R. von Känel, B. Matschke, *Solving S-unit and Mordell equations via Shimura–Taniyama conjecture*, preprint.

[6] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2), 141(3) (1995), 553–572.

[7] B. M. M. de Weger, *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[8] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2), 141(3) (1995), 443–551.