Journal of Number Theory 133 (2013) 3739–3754

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Modular forms and effective Diophantine approximation

M. Ram Murty [1], Hector Pasten [*,2]

Department of Mathematics and Statistics, Queen's University, Jeffery Hall, University ave., Kingston, ON K7L 3N6, Canada

ARTICLE INFO

Article history:
Received 21 November 2012
Revised 21 May 2013
Accepted 25 May 2013
Available online 18 July 2013
Communicated by Michael A. Bennett

MSC:
primary 11F11, 11D75
secondary 11G05

Keywords:
Effective Diophantine approximation
Modular forms
Unit equation
ABC conjecture

ABSTRACT

After the work of G. Frey, it is known that an appropriate bound for the Faltings height of elliptic curves in terms of the conductor (Frey's height conjecture) would give a version of the ABC conjecture. In this paper we prove a partial result towards Frey's height conjecture which applies to all elliptic curves over $\mathbb{Q}$, not only Frey curves. Our bound is completely effective and the technique is based in the theory of modular forms. As a consequence, we prove effective explicit bounds towards the ABC conjecture of similar strength to what can be obtained by linear forms in logarithms, without using the latter technique. The main application is a new effective proof of the finiteness of solutions to the S-unit equation (that is, S-integral points of $\mathbb{P}^1 - \{0, 1, \infty\}$), with a completely explicit and effective bound, without using any variant of Baker's theory or the Thue–Bombieri method.

Contents

* Corresponding author.
E-mail addresses: murty@mast.queensu.ca (M.R. Murty), hpasten@gmail.com (H. Pasten).

[1] The author has been partially funded by an NSERC Discovery grant.
[2] The author has been partially supported by an Ontario Graduate Scholarship.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.05.006

1. Introduction

A central problem in number theory is to establish the finiteness of integral or rational solutions to a Diophantine equation. The proof of such finiteness results often gives an upper bound for the number of solutions, while obtaining upper bounds for the *size* (or more precisely, *height*) of the solutions is a much harder problem. Results of the latter type are called *effective* since, in theory, a bound for the height of the solutions reduces the search for solutions to a finite amount of computation. For later reference, we denote the (logarithmic) *height* of a rational number $q \in \mathbb{Q}$ by

$$h(q) = \log \max\{|a|, |b|\}$$

where a, b are coprime integers with $q = a/b$.

Effective results are difficult to obtain, and essentially the only general approaches are Baker's theory of linear forms in logarithms along with the p-adic and elliptic analogues of it, and Bombieri's improvement of Thue's method [2].

The purpose of this note is to introduce another approach for obtaining effective finiteness results. The technique that we present is based on the theory of modular forms, and it originates in the known approaches to attack the ABC conjecture using elliptic curves and modular forms, which we discuss below. Using this approach we provide an 'algebro-geometric proof' of the following effective version of Mahler's theorem [13, p. 724] on the S-unit equation, a topic classically studied by means of analytic techniques.

Theorem 1.1. *Let S be a finite set of primes in $\mathbb{Z}$ and let P be the product of the elements of S. If $U, V \in \mathbb{Z}_S^\times$ satisfy $U + V = 1$ then*

$$\max\{h(U), h(V)\} < 4.8P \log P + 13P + 25.$$

Here, $\mathbb{Z}_S^\times$ denotes the group of units of the ring $\mathbb{Z}_S$ of rational S-integers. Moreover, as we vary the set S we get

$$\max\{h(U), h(V)\} < 4P \log P + O(P \log\log P).$$

The S-unit equation is a relevant case of finiteness result since several Diophantine problems can be reduced to it. Although this is not the first 'algebro-geometric' proof of finiteness of $\mathbb{Z}_S$-solutions to the unit equation (see the important work of M. Kim [11], where the result is stated in terms of $\mathbb{Z}_S$-points of $\mathbb{P}^1 - \{0, 1, \infty\}$ and it is attributed to Siegel), our method is effective and gives explicit constants.

An equivalent way to state the previous theorem is the following partial result towards the ABC conjecture.

Theorem 1.2. *Let A, B, C be coprime non-zero integers with $A+B=C$. Let $R=\operatorname{rad}(ABC)$ be the radical of ABC, where $\operatorname{rad}(N)=\prod_{p|N}p$. Then*

$$\log\max\{|A|,|B|,|C|\}<4.8R\log R+13R+25.$$

Moreover, as we vary the triple A, B, C we have

$$\log\max\{|A|,|B|,|C|\}\leqslant 4R\log R+O(R\log\log R).$$

We remark that Theorems 1.1 and 1.2 do not give the sharpest effective bounds known today. However, our bounds have similar shape compared to the previous results on the ABC conjecture, all of them effective and obtained by means of the theory of linear forms in logarithms:

- $\log\max\{|A|,|B|,|C|\}\ll\operatorname{rad}(ABC)^{15}$ by Stewart and Tijdeman in 1986, see [19],
- $\log\max\{|A|,|B|,|C|\}\ll\operatorname{rad}(ABC)^{2/3+\epsilon}$ by Stewart and Yu in 1991, see [20],
- $\log\max\{|A|,|B|,|C|\}\ll\operatorname{rad}(ABC)^{1/3+\epsilon}$ by Stewart and Yu in 2001, see [21].

Our bound $\log\max\{|A|,|B|,|C|\}\ll\operatorname{rad}(ABC)^{1+\epsilon}$ is better than the first bound obtained by transcendental methods, but it is certainly worse than the subsequent improvements.

Let us now discuss in more detail our approach. After the work of G. Frey (see [7]) one knows that the following conjecture implies a version of the ABC conjecture.

Conjecture 1.3 *(Height conjecture). For all elliptic curves $E/\mathbb{Q}$ one has $h_F(E)\ll\log N_E$. Here h_F denotes the Faltings height, and N_E is the conductor of E.*

Conversely, the ABC conjecture implies the Height conjecture (see for instance Exercises F.4 and F.5 in [8]). By looking at proofs of these implications, it is clear that any bound towards the Height conjecture would give a bound in the spirit of the ABC conjecture. However the converse is not known to hold, for instance, it is not clear if one can deduce from [21] a partial result for the Height conjecture for *all* elliptic curves over $\mathbb{Q}$. Nevertheless, the computations in the proof of Theorem 1 (ii) in [16] show that a partial result for the ABC conjecture would give a partial result for the Height conjecture restricted to Frey curves (that is, elliptic curves of the form $y^2=x(x-A)(x+B)$ with A, B coprime integers). In particular, *for Frey curves* one knows that $h_F(E)\ll N_E^{1/3+\epsilon}$ thanks to the results in [21]. No such bound is known to hold for the height of all elliptic curves over $\mathbb{Q}$.

In this paper we prove a partial result towards the Height conjecture, which holds for all elliptic curves over $\mathbb{Q}$. Namely, we prove $h_F(E)\ll N_E\log N_E$. We also work out explicit values of the involved constants, obtaining Theorem 7.1. To the best of

our knowledge, this is the first unconditional result for the Height conjecture for all elliptic curves over $\mathbb{Q}$, not only Frey curves. From it, we deduce a partial result for the Szpiro conjecture, from which our effective bounds on the ABC conjecture and the S-unit equation follow (after making explicit the constants involved at various steps of the reduction from the Height conjecture to the ABC conjecture).

More precisely, since all elliptic curves over $\mathbb{Q}$ are modular (see [23] and [22] for the semi-stable case) well-known arguments of [7] and [16] show that for our purposes of bounding the Faltings height in terms of the conductor, it suffices to bound the *modular degree*. To bound the latter in terms of the conductor, it is enough to bound certain number called the *congruence number* of a modular form in terms of the *level* (here, we perform these arguments in a slightly different and more careful way in order to get explicit constants). However, it is not clear how to bound the congruence number in terms of the level with a bound of the expected order of magnitude, namely, polynomial. Instead, we prove a bound for the congruence number which is exponential on the level. The technique that we use to get this bound originates in ideas of [16] (however our proof is different, it corrects some imprecisions of [16] and has better dependence on the level). Namely, we show that the congruence number divides certain index i_N related to the Hecke algebra, and finally we bound the latter by the covolume of a specific lattice which can be estimated in terms of the level. This last bound follows from classical estimates related to the Fourier coefficients of modular forms. It is this relation to the index of the Hecke algebra what allows us to give a partial result for the Height conjecture.

Let us remark that when we prove that the congruence number divides the index i_N, a new invariant n'_f arises in a natural way. We discuss this in Section 4. The invariant n'_f is related to the coprime Hecke algebra $\mathbb{T}'_N$ in the same way that the congruence number (resp. the modular degree) is related to the Hecke algebra $\mathbb{T}_N$ (resp. the endomorphism ring $\operatorname{End} J_0(N)$). This analogy leads us to formulate a conjectural bound for n'_f which, if true, would imply the ABC conjecture.

Finally, to make clear the approach in this work, note that the way in which the known partial results for the Height conjecture have been proved goes as follows: apply linear forms in logarithms to the equation $A + B = C$ which gives an effective result for the ABC conjecture, and then apply the resulting bound on Frey elliptic curves. Our approach, instead, goes the other way around: we apply the theory of modular forms to get a result for the Height conjecture on all elliptic curves over $\mathbb{Q}$ (and this bound turns out to be effective), then we use it in the special case of Frey curves, and an effective bound for the ABC conjecture and the S-unit equation follow.

2. The index of the coprime Hecke algebra

Let N be a positive integer such that the space of weight two modular forms for $\Gamma_0(N)$, denoted by $S_2(\Gamma_0(N))$, is non-trivial. Let $\mathbb{T}'_N$ be the *coprime Hecke algebra* generated over $\mathbb{Z}$ by the Hecke operators T_n with $(n, N) = 1$ acting on $S_2(\Gamma_0(N))$.

Let $\mathcal{N}(N)$ denote the set of normalized newforms of weight 2 for $\Gamma_0(N)$, and let $\mathcal{N}^*(N) = \bigcup_{d|N} \mathcal{N}(d)$. For $f \in \mathcal{N}^*(N)$ let K_f be the number field generated over $\mathbb{Q}$ by the Fourier coefficients of f. We adopt the following notation valid for all the remaining sections.

Notation 2.1. The cardinal of $\mathcal{N}^*(N)$ is $r = r(N)$, and the elements of $\mathcal{N}^*(N)$ are $f_1, \ldots, f_r$ where the indices are arranged in such a way that $f_1, \ldots, f_c$ (for some $c \leqslant r$) form a set of representatives of Galois conjugacy classes in $\mathcal{N}^*(N)$. Whenever we focus our attention into a single rational newform f, we will implicitly assume that it is $f = f_1$.

One has a $\mathbb{Q}$-vector space isomorphism

$$\mathbb{T}'_N \otimes \mathbb{Q} \to \prod_{i=1}^{c} K_{f_i}$$

given by $T_n \mapsto (a_n(f_i))_i$. Moreover, the image $\mathcal{T}'_N$ of $\mathbb{T}'_N$ is a full-rank subgroup of $\mathcal{O}'_N := \prod \mathcal{O}_i$, where $\mathcal{O}_i$ is the ring of integers of $K_i = K_{f_i}$. The *coprime Hecke index* is defined by

$$i_N = \big[\mathcal{O}'_N : \mathcal{T}'_N\big].$$

The fields K_i are totally real, so the canonical embedding from algebraic number theory is

$$K_i \to \mathbb{R}^{[K_i:\mathbb{Q}]} =: E_i.$$

Let $E = \prod_{i=1}^{c} E_i$, then $E = \mathbb{R}^r$ with r as defined above. We have an embedding $\prod_{i=1}^{c} K_i \to E$ which allows us to see $\mathcal{T}'_N$ and $\mathcal{O}'_N$ as full-rank sub-lattices of E.

We put the usual Lebesgue measure on E and we write Covol_V for the covolume of a full-rank lattice in a given real vector space V.

Lemma 2.2. *We have* $i_N \cdot \mathrm{Covol}_E(\mathcal{O}'_N) = \mathrm{Covol}_E(\mathcal{T}'_N)$ *and* $\mathrm{Covol}_E(\mathcal{O}'_N) \geqslant 1$. *In particular*

$$i_N \leqslant \mathrm{Covol}_E\big(\mathcal{T}'_N\big).$$

Proof. We only need to justify the assertion $\mathrm{Covol}_E(\mathcal{O}'_N) \geqslant 1$. The covolume of $\mathcal{O}_i$ in E_i is $\sqrt{|\Delta_i|}$ where Δ_i is the discriminant of $\mathcal{O}_i$. Thus $\mathrm{Covol}_E(\mathcal{O}'_N) = \prod_{i=1}^{c} \sqrt{|\Delta_i|} \geqslant 1$. □

We want to bound $\mathrm{Covol}_E(\mathcal{T}'_N)$. For this, let $I = \{1, \ldots, r\}$ and for any J set of r positive integers coprime to N define the square matrix $A_J = [a_j(f_i)]_{(i,j)\in I\times J}$. Then we have

Lemma 2.3. *If J is a set of r positive integers coprime to N such that $\det A_J \neq 0$ then*

$$\operatorname{Covol}_E\big(\mathcal{T}'_N\big) \leqslant |\det A_J|.$$

Proof. Up to reordering the rows of A_J, we see that the columns of A_J are elements of $\mathcal{T}'_N \subseteq E$ because $\mathcal{N}^*(N)$ is stable under the Galois action on Fourier coefficients. On the other hand, the condition $\det A_J \neq 0$ implies that these columns form an $\mathbb{R}$-basis for E. The result follows. □

In the next section we study $\det A_J$ more closely.

3. Bounding $\det A_J$

Let $\operatorname{sf}(N)$ be the square-free part of N, which is the product of the primes dividing N with exponent exactly 1. By properties of the killing operators (see pp. 142–143 in [1]) we know that the rule

$$f = \sum_{n\geqslant 1} a_n q^n \mapsto t(f) = \sum_{(n,N)=1} a_n q^n$$

defines a linear map

$$t : S_2\big(\Gamma_0(N)\big) \to S_2\big(\Gamma_0\big(N \operatorname{sf}(N)\big)\big).$$

Define the following subspaces of $S_2(\Gamma_0(N))$

$$H(N) = \bigoplus_{d|N} S_2\big(\Gamma_0(N/d)\big)^{\text{new}} \subseteq S_2\big(\Gamma_0(N)\big),$$

$$K(N) = \left\{ \sum_{p|N} g_p(pz) \in S_2\big(\Gamma_0(N)\big) \colon\ g_p \in S_2\big(\Gamma_0(N/p)\big) \right\}.$$

Note that $\dim H(N) = r$; indeed, the set $\mathcal{N}^*(N)$ is a basis for $H(N)$.

Proposition 3.1. *The kernel of t is $K(N)$, which is equal to the set of all $f \in S_2(\Gamma_0(N))$ with $a_n(f) = 0$ for $(n, N) = 1$. Moreover, $S_2(\Gamma_0(N)) = H(N) \oplus K(N)$. In particular, t is injective on $H(N)$.*

Proof. The inclusion $\ker t \supseteq K(N)$ is clear. The reciprocal inclusion follows from Atkin–Lehner theory (more precisely, Theorem 1 in [1]). That $S_2(\Gamma_0(N)) = H(N) \oplus K(N)$ also follows from Atkin–Lehner theory. □

In particular, if $f \in S_2(\Gamma_0(N))$ has $a_n(f) = 0$ for *all* n coprime to the level N, then $f \in K(N)$. For our purposes, the following effective version is needed.

Proposition 3.2. *Let $g_1, \dots, g_r \in S_2(\Gamma_0(N))$ be a basis for $H(N)$, and let*

$$I = \{1, \dots, r\}, \qquad J' = \big\{j\colon\ 1 \leqslant j \leqslant \rho(N) \text{ and } (j, N) = 1\big\}$$

where

$$\rho(N) = \frac{N \operatorname{sf}(N)}{6} \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

Then the matrix $[a_j(g_i)]_{(i,j)\in I\times J'}$ has rank r.

Proof. By Proposition 3.1 we know that $t(g_i)$ are linearly independent elements in $S_2(\Gamma_0(N \operatorname{sf}(N)))$. Hence, if $\beta_1, \dots, \beta_r$ are complex numbers not all zero then $h = \sum_{1\leqslant j\leqslant r} \beta_j t(g_j) \in S_2(\Gamma_0(N \operatorname{sf}(N)))$ is a non-zero element, so that its order of vanishing at $i\infty$ is at most $2g(N \operatorname{sf}(N)) - 2$, where (see Theorem 9.10 in [12])

$$g(m) := \dim_{\mathbb{C}} S_2\big(\Gamma_0(m)\big) \leqslant 1 + \frac{m}{12} \prod_{p \mid m} \left(1 + \frac{1}{p}\right).$$

With $m = N \operatorname{sf}(N)$ we get

$$2g\big(N \operatorname{sf}(N)\big) - 2 \leqslant \frac{N \operatorname{sf}(N)}{6} \prod_{p \mid N \operatorname{sf}(N)} \left(1 + \frac{1}{p}\right) = \rho(N).$$

Therefore $(a_j(h))_{j\in J}$ is not the zero vector, which shows that the rows of $[a_j(g_i)]_{(i,j)\in I\times J'}$ are linearly independent. □

We will also need a bound for $r = \dim H(N)$. From Theorem 4 in [14] one deduces

Proposition 3.3. *We have*

$$\dim H(N) \leqslant \frac{N + 4}{12}.$$

Now we can bound $\det A_J$ for suitable J.

Proposition 3.4. *There exists a set J of r positive integers coprime to N such that $\det A_J \neq 0$ and*

$$\log|\det A_J| < \frac{1}{5} N \log N.$$

Moreover, as $N \to \infty$ this choice of J (depending on N) gives

$$\log|\det A_J| \leqslant \frac{1}{6} N \log N + O(N \log\log N).$$

Proof. We need a suitable set J such that the determinant of the matrix $A_J = [a_j(f_i)]_{(i,j)\in I\times J}$ is not zero and we can estimate it. Proposition 3.2 applied to the basis $\mathcal{N}^*(N)$ implies that there is a subset $J \subseteq \{1, 2, \ldots, \rho\}$ such that $\det A_J \neq 0$, where $\rho := \rho(N)$. Consider such a set J.

Since f_i are normalized eigenforms of weight 2, one has the bound $|a_j(f_i)| \leqslant j^{1/2}\sigma_0(j)$ where σ_0 is the number of divisors. Therefore

$$|\det A_J| \leqslant r \prod_{j\in J} j^{1/2}\sigma_0(j) \leqslant r\rho^{r/2} \prod_{j\in J} \sigma_0(j).$$

The trivial upper bound $\sigma_0(j) \leqslant 2\sqrt{j}$ is sufficient for our purposes, and we obtain

$$|\det A_J| \leqslant r\rho^{r/2}(2\rho)^{r/2}. \tag{1}$$

On the other hand, it is easily seen from the definition of $\rho = \rho(N)$ that

$$\rho \leqslant \frac{1}{6} N \operatorname{sf}(N)(1 + \log N) \leqslant \frac{1}{6} N^2(1 + \log N).$$

Plugging this bound and the bound for r given by Proposition 3.3 into (1) one gets

$$\begin{aligned} \log|\det A_J| &\leqslant r \log \rho + \frac{\log 2}{2} r + \log r \\ &\leqslant \frac{N+4}{12}\left(2\log N + \log(1 + \log N) - \frac{\log 18}{2}\right) + \log\frac{N+4}{12}. \end{aligned}$$

It is a calculus exercise to check that the last expression is strictly less than $0.2N \log N$ when $N > 30$.

Finally, for $N \leqslant 30$ with $S_2(N) \neq (0)$ one can directly check the existence of a set of indices J with the desired properties by looking at tables of modular forms. Namely, the following table gives suitable sets J for such N, along with the related quantities:

N	J	$\log\lvert\det A_J\rvert$	$0.2N \log N$
11, 14, 15, 17, 19, 20, 21, 22, 24, 27, 28	$\{1\}$	$\log 1 = 0$	$\geqslant 5.27$
23	$\{1, 2\}$	$\log\sqrt{5} < 0.81$	$\geqslant 14.42$
26	$\{1, 3\}$	$\log 4 < 1.39$	$\geqslant 16.94$
29	$\{1, 2\}$	$\log 2^{3/2} < 1.04$	$\geqslant 19.53$
30	$\{1, 7\}$	$\log 4 < 1.39$	$\geqslant 20.4$

The Fourier coefficients necessary for computing this table have been obtained using Sage. □

From Proposition 3.4 and Lemmas 2.2 and 2.3 we conclude

Theorem 3.5. *We have*

$$\log i_N \leqslant \frac{1}{5} N \log N.$$

Moreover, as $N \to \infty$

$$\log i_N \leqslant \frac{1}{6} N \log N + O(N \log\log N).$$

4. The congruence number and the modular degree

Let f be a rational newform in $S_2(\Gamma_0(N))$. The congruence number of f, denoted by n_f, is the largest positive integer M satisfying the following: there is a cusp form $g \in S_{\mathbb{Z}}$ such that $(f,g) = 0$ and $f \equiv g \bmod M$. Here, $(\,,)$ denotes the Petersson inner product and $f \equiv g \bmod M$ means that for each $n \geqslant 1$ one has $a_n(f) \equiv a_n(g) \bmod M$.

We have a ring homomorphism $\mathbb{T}_N \to \mathbb{Z}$ defined by $T \mapsto a_1(Tf)$. Let $\mathbb{I}_f$ be the kernel, then one constructs the Shimura quotient

$$q_f : J_0(N) \to E_f = J_0(N)/\mathbb{I}_f J_0(N)$$

where $J_0(N)$ is the Jacobian of the modular curve $X_0(N)$. Here we are using the canonical rational model of $X_0(N)$ and we take the embedding $j_\infty : X_0(N) \to J_0(N)$ using the cusp at infinity which is $\mathbb{Q}$-rational. One gets that E_f is an elliptic curve defined over $\mathbb{Q}$ and q_f is a morphism of abelian varieties defined over $\mathbb{Q}$. Let $\phi_f = q_f \circ j_\infty : X_0(N) \to E_f$ be the modular parametrization. The *modular degree* m_f is defined as $m_f = \deg \phi_f$.

The integers m_f and n_f are related by the following result attributed to Ribet (see [3]):

Theorem 4.1. *If f is a rational newform, then $m_f | n_f$.*

Following an approach similar to [16] we prove

Theorem 4.2. *We have $n_f | i_N$. In particular $m_f | i_N$.*

Proof. We assume $f = f_1 \in \mathcal{N}^*(N)$. By definition of i_N we know that $i_N e_1 \in \mathcal{T}'_N$ where $e_1 = (1,0,\ldots,0) \in \mathcal{O}'_N$. Let $T \in \mathbb{T}'_N$ be such that $T = i_N e_1$ in $\prod_i K_i$. This means that $T(f) = i_N f$ and $T(f_i) = 0$ for $i = 2,\ldots,c$. The Hecke action commutes with the Galois action on Fourier coefficients and therefore $T(f_i) = 0$ for $i = 2,\ldots,r$. Moreover, since $T \in \mathbb{T}'_N$ we know (by Atkin–Lehner theory) that the action of T on $S_2(\Gamma_0(N))$ is diagonalizable and the eigenvalues of T on $S_2(\Gamma_0(N))$ are the same (with possible repetitions) as the eigenvalues of the $f_i \in \mathcal{N}^*(N)$ with respect to T. Therefore $T(f) = i_N f$ and T annihilates the orthogonal complement of f in $S_2(\Gamma_0(N))$.

Let $g \in S_2(\Gamma_0(N))$ be a cusp form with integral Fourier coefficients which is orthogonal to $f = f_1$, and such that $a_j(f) \equiv a_j(g) \bmod n_f$ for all $j \geqslant 1$. In particular $T(g) = 0$.

The n-th Fourier coefficient of $T(g)$ (which is 0) satisfies

$$a_n\big(T(g)\big) \equiv a_n\big(T(f)\big) \bmod n_f$$

because $T \in \mathbb{T}'_N$ and $g \equiv f \bmod n_f$. Since $T(f) = i_N f$ we get $a_n(T(f)) = a_n(i_N f) = i_N a_n(f)$ from which we conclude that $n_f | i_N a_n(f)$ for all n. In particular, with $n = 1$ we get $n_f | i_N$. □

From Theorem 3.5 we deduce the following bound for the modular degree and the congruence number.

Theorem 4.3. *We have*

$$\log m_f \leqslant \log n_f \leqslant \frac{1}{5} N \log N.$$

Moreover, as $N \to \infty$ *one has*

$$\log m_f \leqslant \log n_f \leqslant \frac{1}{6} N \log N + O(N \log\log N).$$

The rest of the discussion in this section will not be used in other parts of the paper, but it can be of independent interest. Looking at the proof of Theorem 4.2 it is natural to define n'_f as the least positive integer n such that $ne_1 \in \mathcal{T}'_N$ (from the proof, it follows that n'_f exists). Equivalently, let p_f be the orthogonal projection from $S_2(\Gamma_0(N))$ onto $\mathbb{C} \cdot f$, then n'_f is the least positive integer n such that $np_f \in \mathbb{T}'_N$; that is, n'_f is the denominator of p_f with respect to $\mathbb{T}'_N$. This quantity n'_f satisfies $n_f | n'_f$ and $n'_f | i_N$. We conjecture

Conjecture 4.4. *The quantity* n'_f *satisfies* $\log n'_f \ll \log N$.

Let give some justification for this conjecture. Recall from [3] that m_f (resp. n_f) is the denominator of p_f with respect to $\operatorname{End} J_0(N)$ (resp. $\mathbb{T}_N$) acting on $S_2(\Gamma_0(N))$. One has the chain of inclusions $\mathbb{T}'_N \subseteq \mathbb{T}_N \subseteq \operatorname{End} J_0(N)$ and therefore $m_f | n_f$ and $n_f | n'_f$. The conjecture $\log m_f \ll \log N$ is due to Frey (see [7]), and Murty formulated the conjecture $\log n_f \ll \log N$ (see [16]); both of these conjectures imply a version of the ABC conjecture. Therefore, after the analogous characterizations of m_f, n_f, n'_f as denominators, we think that it is natural to formulate Conjecture 4.4.

Since $m_f | n'_f$ and $n'_f | i_N$ we obtain the following result about Conjecture 4.4.

Theorem 4.5. *Conjecture 4.4 implies Frey's modular degree conjecture, hence, the Height conjecture, the Szpiro conjecture and a version of the ABC conjecture. Unconditionally, the estimate* $\log n'_f \ll N \log N$ *holds.*

We do not know if a sufficiently strong version of the ABC conjecture implies Conjecture 4.4, and we believe that the invariant n'_f deserves a more detailed study.

5. The height and minimal discriminant of elliptic curves

Let $\Delta(z)$ be the Ramanujan cusp form, which is given by

$$\Delta(z) = q \prod_{n \geqslant 1} \left(1 - q^n\right)^{24}, \quad q = e^{2i\pi z}.$$

Given E an elliptic curve defined over $\mathbb{Q}$, we denote its minimal discriminant by Δ_E and we let τ_E be a point in the upper half plane $\mathfrak{h}$ such that $E(\mathbb{C})$ is biholomorphic to the torus $\mathbb{C}/(\mathbb{Z}+\tau_E\mathbb{Z})$. Of course there are infinitely many choices for τ_E, all of them $\mathrm{SL}_2(\mathbb{Z})$-equivalent, but in the discussion below the choice of τ_E is irrelevant as we will be concerned with the quantity $|\Delta(\tau_E)|(\Im\tau_E)^6$ which is $\mathrm{SL}_2(\mathbb{Z})$-invariant.

In his solution to the Mordell conjecture [6], Faltings introduced a notion of height for an abelian variety defined over a number field (which we call *Faltings height*). The precise definition is better understood in terms of Arakelov geometry and we do not recall it here. For our purposes we will only need the Faltings height $h_F(E)$ of an elliptic curve E defined over $\mathbb{Q}$, and the following fact (cf. [17]):

Theorem 5.1. *If E is an elliptic curve defined over $\mathbb{Q}$, then its Faltings height satisfies*

$$12h_F(E) = \log|\Delta_E| - \log\big(\big|\Delta(\tau_E)\big|(\Im\tau_E)^6\big) + 12\log(2\pi).$$

Since $\Delta(z)$ is a weight 12 cusp for $\mathrm{SL}_2(\mathbb{Z})$ it is a standard fact that the quantity $|\Delta(\tau_E)|(\Im\tau_E)^6$ has a uniform upper bound on $\mathfrak{h}$. From the next two lemmas we get an explicit such bound.

Lemma 5.2. *Let $0<r<1$. If $|q|\leqslant r$ then we have*

$$\big|\Delta(\tau)/q\big| < \left(\frac{1}{1-r}\right)^{1/(1-r)}.$$

Proof. Since $\Delta(\tau) = q\prod_{n\geqslant 1}(1-q^n)^{24}$, we find (for the branch of log with $\log 1 = 0$)

$$\log q - \log\Delta(\tau) = -24\sum_{n\geqslant 1}\log\big(1-q^n\big) = \sum_{n\geqslant 1}\sum_{k\geqslant 1}\frac{q^{kn}}{k} = \sum_{k\geqslant 1}\sum_{n\geqslant 1}\frac{q^{kn}}{k}$$

thus

$$\big|\log\Delta(\tau) - \log q\big| \leqslant \sum_{k\geqslant 1}\sum_{n\geqslant 1}\frac{r^{kn}}{k} = \sum_{k\geqslant 1}\frac{1}{k}\frac{r^k}{1-r^k} < \frac{1}{1-r}\sum_{k\geqslant 1}\frac{r^k}{k} = \frac{1}{1-r}\log\frac{1}{1-r}. \qquad \square$$

Lemma 5.3. *If $\tau\in\mathcal{F}$ then*

$$\log\big|\Delta(\tau)\Im(\tau)^6\big| < -6.272.$$

Proof. Observe that if $\tau\in\mathcal{F}$ then $|q| = e^{-2\pi\Im(\tau)} \leqslant r := e^{-\pi\sqrt{3}}$ so that the previous lemma gives

$$\big|\Delta(\tau)\Im(\tau)^6\big| < \left(\frac{1}{1-r}\right)^{1/(1-r)} e^{-2\pi\Im(\tau)}\Im(\tau)^6.$$

The function $x \mapsto e^{-2\pi x}x^6$ attains its maximum on the interval $[\sqrt{3}/2, \infty)$ at the point $x = 3/\pi$ so that for $\tau \in \mathcal{F}$ we get

$$\left|\Delta(\tau)\Im(\tau)^6\right| < \left(\frac{1}{1-r}\right)^{1/(1-r)} e^{-6}\left(\frac{3}{\pi}\right)^6$$

that is

$$\log\left|\Delta(\tau)\Im(\tau)^6\right| < \frac{1}{1-r}\log\frac{1}{1-r} + 6\log\left(\frac{3}{e\pi}\right) = -6.272343\ldots$$

giving the claimed bound. □

Plugging this result into Theorem 5.1 we obtain

Theorem 5.4. *If E is an elliptic curve defined over $\mathbb{Q}$, then its Faltings height satisfies*

$$12h_F(E) > \log|\Delta_E| + 28.326.$$

6. The height and modular degree of elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. By the modularity theorem, there is a rational newform $f \in S_2(\Gamma_0(N))$ such that E is isogenous to E_f over $\mathbb{Q}$ (we use the notation from Section 4). By results of Mazur [15] and Kenku [10] we know that there is an isogeny $\psi : E_f \to E$ defined over $\mathbb{Q}$ of degree at most 163. Let $p_E = \psi \circ \phi_f : X_0(N) \to E$. We can assume that $\phi_f(\infty) = 0$ and $\psi(0) = 0$, then the same argument as in Proposition 1 of [5] gives the following result (which does not need our assumption on the degree of ψ).

Theorem 6.1. *Let ω be a minimal differential on E with respect to a global minimal Weierstrass form. Let f be the newform associated to E and denote the composition $\mathfrak{h} \to \Gamma_0(N)\backslash\mathfrak{h} \hookrightarrow X_0(N)$ by u. Then $u^* p_E^* \omega = 2\pi i c_E f dz$ on $\mathfrak{h}$, where c_E is a non-zero integer. In particular $|c_E| \geqslant 1$.*

The integer c_E is the *Manin constant* of the modular parameterization p_E (this is a slight abuse of notation; c_E depends on p_E not only on E) and we can assume it is *positive* by changing ω to $-\omega$ if necessary; we keep this assumption during the present section. It is conjectured that if p_E induces an optimal quotient $J_0(N) \to E$ (i.e. p_E is a strong parameterization) then $c_E = 1$, but for general p_E this does not need to be the case.

The Faltings height $h_F(E)$ is related to modular parameterizations by (cf. [17] where the hypothesis of p_E being strong is unnecessary for this formula):

Proposition 6.2. *With the above notation, we have*

$$\frac{1}{2}\log\deg p_E = h_F(E) + \log\|f\| + \log c_E$$

where $\|f\|$ denotes the Petersson norm of f.

It is easily seen that

$$\|f\| \geqslant \frac{e^{-2\pi}}{2\sqrt{\pi}}, \quad \text{hence} \quad \log\|f\| > -7.549.$$

This estimate is far from optimal with respect to the dependence on the level (see [9]), but it is sufficient for our purposes since it is explicit. Also, we have $c_E \geqslant 1$ by Theorem 6.1, and the results of Mazur and Kenku mentioned above give

$$\frac{1}{2}\log\deg\phi_f \geqslant \frac{1}{2}\log\deg p_E - \frac{1}{2}\log 163 > \frac{1}{2}\log\deg p_E - 2.547.$$

Plugging these estimates into Proposition 6.2 yields

Proposition 6.3. *With the above notation, we have*

$$\frac{1}{2}\log\deg\phi_f > h_F(E) - 10.096.$$

7. A bound for the Szpiro conjecture and the Height conjecture

In this section we put together the various results of the previous sections in order to get an explicit effective bound towards the Szpiro conjecture and Frey's height conjecture. We remark that such bounds can be obtained by other means, for example, using results from [21] (at least in the case when E has rational 2-torsion, i.e. Frey curves). However, our approach gives an effective result with explicit constants without using results from the theory of linear forms in logarithms (which is the goal of the present work).

Theorem 7.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ with minimal discriminant Δ_E, conductor N and Faltings height $h_F(E)$. Then we have*

$$h_F(E) < 0.1N\log N + 11$$

and

$$\log|\Delta_E| < 1.2N\log N + 93.$$

Moreover, as we let E vary, we have

$$h_F(E) < \frac{1}{12} N \log N + O(N \log\log N)$$

and

$$\log|\Delta_E| < N \log N + O(N \log\log N).$$

Proof. Using Proposition 6.3 and Theorem 4.3, we get

$$h_F(E) < \frac{1}{2} \log m_f + 10.096 \leqslant \frac{1}{10} N \log N + 10.096.$$

Using this bound and Theorem 5.4 we conclude

$$\log|\Delta_E| < \frac{12}{10} N \log N + 92.826$$

and the first part of the result follows. The second part is proved in the same way. □

8. Effective bounds for the ABC conjecture and the *S*-unit equation

Finally, using Frey elliptic curves we derive the explicit effective bound for the ABC conjecture and the S-unit equation stated in the introduction.

Proof of Theorem 1.2. Given A, B, C non-zero coprime integers with $A+B+C=0$ we can assume that $A \equiv -1(4)$ and B is even. As usual, we consider the Frey–Hellegouarch curve

$$E: \quad y^2 = x(x-A)(x+B).$$

Then E the minimal discriminant of E satisfies $2^8|\Delta_E| \geqslant (ABC)^2$ (see p. 257 in [18]) and the conductor of E satisfies $N_E|2^4 \operatorname{rad}(ABC)$ (see [4]). Write $R = \operatorname{rad}(ABC)$, then applying Theorem 7.1 to E we get

$$\log(ABC)^2 - 8\log 2 < 1.2 \cdot 2^4 R \log\left(2^4 R\right) + 93$$

hence

$$2\log|ABC| < 19.2R \log R + 53.234R + 98.546.$$

Now, say that $1 \leqslant |A| \leqslant |B| \leqslant |C|$, then $\max\{|A|,|B|,|C|\} = |C| \leqslant |C \cdot 2B|^{1/2} \leqslant |2ABC|^{1/2}$ and we have

$$4\log\max\left\{|A|,|B|,|C|\right\} - 2\log 2 < 19.2R \log R + 53.234R + 98.546$$

from which the first part of the result follows. For the second part one does the same computation using the second part of Theorem 7.1 instead. □

Proof of Theorem 1.1. Let $U, V \in \mathbb{Z}_S^\times$ with $U + V = 1$, then we can write $U = -A/C$, $V = -B/C$ for A, B, C non-zero coprime integers whose prime factors belong to S (in particular $\mathrm{rad}(ABC)$ divides the product of the primes in S) and $A + B + C = 0$. Then one concludes by observing that

$$\max\{h(U), h(V)\} = \log \max\{|A|, |B|, |C|\}. \qquad \square$$

Acknowledgments

The second author presented this work at the Workshop on Algebraic Varieties held at the Fields Institute, Toronto, November of 2012. He would like to thank Noriko Yui for inviting him to present at this workshop, and acknowledges the generous support from the Fields Institute.

The authors would like to thank the anonymous referee for suggesting several changes that improved the presentation and some of the results. Also, it was after the referee's comments that we included a discussion on the invariant n'_f and its relation with the ABC conjecture.

References

[1] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.
[2] E. Bombieri, Effective Diophantine approximation on $\mathbb{G}_m$, Ann. Sc. Norm. Super. Pisa Cl. Sci. (4) 20 (1) (1993) 61–89.
[3] A. Cojocaru, E. Kani, The modular degree and the congruence number of a weight 2 cusp form, Acta Arith. 114 (2) (2004) 159–167.
[4] F. Diamond, K. Kramer, Modularity of a family of elliptic curves, Math. Res. Lett. 2 (3) (1995) 299–304.
[5] B. Edixhoven, On the Manin constants of modular elliptic curves, in: Arithmetic Algebraic Geometry, Texel, 1989, in: Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.
[6] G. Faltings, Finiteness theorems for abelian varieties over number fields, in: Arithmetic Geometry, Storrs, CT, 1984, Springer, New York, 1986, pp. 9–27, translated from the German original by Edward Shipz, Invent. Math. 73 (3) (1983) 349–366, Invent. Math. 75 (2) (1984) 381.
[7] G. Frey, Links between solutions of $A - B = C$ and elliptic curves, in: Number Theory, Ulm, 1987, in: Lecture Notes in Math., vol. 1380, Springer, New York, 1989, pp. 31–62.
[8] M. Hindry, J. Silverman, Diophantine Geometry. An Introduction, Grad. Texts in Math., vol. 201, Springer-Verlag, New York, 2000.
[9] J. Hoffstein, P. Lockhart, Coefficients of Maass forms and the Siegel zero, Ann. of Math. (2) 140 (1) (1994) 161–181, with an appendix by Dorian Goldfeld, Hoffstein and Daniel Lieman.
[10] M.A. Kenku, On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class, J. Number Theory 15 (2) (1982) 199–202.
[11] M. Kim, The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel, Invent. Math. 161 (3) (2005) 629–656.
[12] A.W. Knapp, Elliptic Curves, Math. Notes, vol. 40, Princeton University Press, Princeton, NJ, ISBN 0-691-08559-5, 1992, xvi+427 pp.
[13] K. Mahler, Zur Approximation algebraischer Zahlen. I, Math. Ann. 107 (1) (1933) 691–730 (in German).
[14] G. Martin, Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$, J. Number Theory 112 (2) (2005) 298–331 (English summary).
[15] B. Mazur, Rational isogenies of prime degree, Invent. Math. 44 (2) (1978) 129–162, with an appendix by D. Goldfeld.

[16] M.R. Murty, Bounds for congruence primes, in: Automorphic Forms, Automorphic Representations, and Arithmetic, Fort Worth, TX, 1996, Amer. Math. Soc., Providence, RI, 1999, pp. 177–192.
[17] J. Silverman, Heights and elliptic curves, in: Arithmetic Geometry, Storrs, CT, 1984, Springer, New York, 1986, pp. 253–265.
[18] J. Silverman, The Arithmetic of Elliptic Curves, second ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, ISBN 978-0-387-09493-9, 2009, xx+513 pp.
[19] C.L. Stewart, R. Tijdeman, On the Oesterlé–Masser conjecture, Monatsh. Math. 102 (3) (1986) 251–257.
[20] C.L. Stewart, Kun Rui Yu, On the abc conjecture, Math. Ann. 291 (2) (1991) 225–230.
[21] C.L. Stewart, Kun Rui Yu, On the abc conjecture. II, Duke Math. J. 108 (1) (2001) 169–181.
[22] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) 141 (3) (1995) 553–572.
[23] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) 141 (3) (1995) 443–551.