Interpolation determinants and the Lebesgue-Nagell equation $a^2 - D = b^p$

Davide Lombardo

August 31, 2024

Abstract

We solve the equation in the title for $D = 2, 3, 5, 37$ by obtaining sharp estimates on linear forms in two logarithms in special cases. The method can in principle be extended to higher values of D.

Contents

1 Introduction

The aim of this paper is to study the so-called *Lebesgue-Nagell equation*, that is, the diophantine equation

$$a^2 - D = b^p \tag{1}$$

where a, b, p are integer unknowns, with p prime, and D is a fixed integer. This equation has attracted an enormous amount of work, with hundreds of papers written on (1) and its variants: we refer the

reader to the recent paper [BS23b] for the state of the art, including a discussion of the known results and of the techniques that have been fruitfully applied to the problem. Here we will only review some of the main points.

The results of [Bug00] imply that there is an effective algorithm for solving Equation (1) for any fixed value of D, but so far, the algorithm is very far from being practical, and it is only through additional ideas and techniques that it has been possible to solve Equation (1) for certain concrete values of D. For negative D, the situation is reasonably – though not completely – well understood: several tools, in particular the modular method, the theory of primitive divisors in recurrence sequences, and techniques from Diophantine approximation, can be brought to bear on the problem to great effect. These techniques are especially powerful when b is odd, but the general case is not hopeless either: the beautiful paper [BMS06], for example, completes the solution of Equation (1) for all $D < 0$ with $|D| \leq 100$, while [BS23a] handles the cases $D = -q^\alpha$, where $2 \leq q < 100$ is a prime and α is any positive integer, under the additional assumption $(a, b) = 1$.

Much less is known for positive D, and this is the case we focus on in this paper. Some small values of D, including in particular $D = 2$, are widely regarded as being especially hard: see for example the comments at the beginning of [Coh07, §15.7.1], those after [BS23a, Theorem 2], and the introduction to [BS23b]. Two main obstacles have blocked all previous attempts at solving Equation (1) for $D = 2$. One is intrinsic: the existence of the *trivial solutions* $(a, b) = (\pm 1, -1)$ obstructs the application of many techniques, including in particular the modular method, even though Chen [Che12] has managed to adapt ideas related to this method to solve the equation when p lies in certain congruence classes modulo 24 (see Theorem 3.7 below). The other problem is, to a certain extent, 'merely' computational: linear forms in logarithms can be used to give an absolute bound for the exponent p, which leaves us with finitely many equations to solve. Each of these equations can be reduced to a finite number of Thue equations, and therefore, in principle, be solved effectively. However, even the best available estimates on linear forms in logarithms have, in the hands of experts, only led to bounds of the quality of $p \lesssim 10^3$ (see [Coh07, p. 520] for the bound $p \leq 1237$), while at present it seems that – from a computational point of view – the relevant Thue equations are solvable only for much smaller values of p. Experiments with the well-known computer algebra system GP suggest that even $p = 89$ may be out of reach, let alone $p = 1237$. Similar considerations apply to the next simplest positive values of D, namely $D = 3$ and $D = 5$, since we again have the obstructive solutions $2^2 - 3 = 1^p$ and $2^2 - 5 = (-1)^p$ for all odd primes p (the cases $D = 2^m$ with $m \geq 2$, including in particular $D = 4$, have all been solved; see [Coh07, Theorem 15.3.4] and [Sik03] for partial results, and [Ivo03] for the general case). The situation is somewhat reminiscent of the family of Thue equations $|(a + 1)x^n - ay^n| = 1$: these were solved for large values of n in [BdW98], which left only finitely many values of n to treat, but solving the remaining cases required extremely substantial additional work [Ben01]. The case of the Lebesgue-Nagell equation (1) is similar: for a fixed value of D it is not too hard to obtain an absolute bound for p, but the finitely many remaining equations can often prove intractable.

In this paper, we bridge the gap between what is computationally accessible and what the upper bounds can provide by obtaining refined estimates on certain linear forms in two logarithms. We use these results to show that (1) does not have any nontrivial solutions for any prime $p > 17$ when $D = 2, 3, 5$. Since it is not hard to solve directly the finitely many remaining Thue equations (for $D = 2$, this was already done in [Coh07, §15.7.3]), this provides a complete solution of (1) for these values of D:

Theorem 1.1. *Let $p \geq 3$ be a prime number and let $D \in \{2, 3, 5\}$. Every integral solution of the equation $a^2 - D = b^p$ satisfies $b \in \{\pm 1\}$.*

We will call solutions of Equation (1) with $|b| = 1$ the *trivial solutions*. Thus, Theorem 1.1 says that Equation (1) has only trivial solutions for $D \in \{2, 3, 5\}$ and $p \geq 3$. We emphasise that, to the best of our knowledge, this is the first time that the Lebesegue-Nagell equation is completely solved for positive prime values of D such that (1) admits solutions for every $p \geq 3$. It seems likely that the technique we develop can also solve Equation (1) for any positive squarefree value of D that is not a square modulo 8, provided that D is not too large: to keep the paper reasonably short, we have limited ourselves to a few interesting values, but the computations necessary to handle other small positive D should be feasible with current technology. As an example, in Section 4.7 we show how, at the cost of slightly more computation than is necessary to prove Theorem 1.1, we can also solve Equation (1) for $D = 37$, another prime for which the solutions of Equation (1) were not previously known. In this case, there are also a few non-trivial solutions, and we obtain the following:

Theorem 1.2. *Let $D = 37$. The solutions of Equation (1) with $p \geq 3$ are*

$$(a, b, p) \in \{(\pm 8, 3, 3), (\pm 3788, 3^5, 3), (\pm 3788, 3^3, 5)\},$$

together with the trivial solutions $(a, b, p) = (\pm 6, -1, p)$ for all $p \geq 3$.

We note that [BS23a, Theorem 2] solves Equation (1) when $D = q^\alpha$ is a prime power with $q \leq 100$, except for $q \in \{2, 3, 5, 17, 37, 41, 73, 89, 97\}$, with the primes $2, 3, 5, 17, 37$ being considered particularly hard (the main difficulties come from $\alpha = 1$, that is, the values we treat). We refer the reader to Section 4.8 for a discussion of the computational difficulties one faces when dealing with higher values of D, the role of the assumption that D is not a square modulo 8, and the case $D = 17$.

Our main contribution lies in a significant improvement of the upper bound for the exponent p, obtained as an application of the theory of linear forms in (complex) logarithms. We describe the main observations that allow us to gain such a large factor in the upper bound, focusing for simplicity on the case $D = 2$. As we will explain in Section 3, to a solution of Equation (1) we attach the linear form in logarithms

$$\Lambda := p \log \alpha_2 - \log \alpha_1,$$

where $\alpha_1 = (1+\sqrt{2})^2$ is the square of the fundamental unit of the field $\mathbb{Q}(\sqrt{2})$ and α_2 is a certain element of $\mathbb{Q}(\sqrt{2})$ constructed from the solution (a, b, p). Denoting by σ the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, the elements α_1, α_2 have the property $\sigma(\alpha_i) = 1/\alpha_i$. This implies that $\log \sigma(\alpha_1) = -\log \alpha_1$ and $\log \sigma(\alpha_2) = -\log \alpha_2$.

One can prove that – for nontrivial solutions of Equation (1) – $|\Lambda|$ is exponentially small in p (see Equation (27)), and therefore a good lower bound for $|\Lambda|$ gives an upper bound for p. The property $\sigma(\alpha_i) = 1/\alpha_i$ gives us another linear form in logarithms that is extremely small, namely,

$$\Lambda_\sigma := p \log \sigma(\alpha_2) - \log \sigma(\alpha_1) = -p \log \alpha_2 + \log \alpha_1 = -\Lambda.$$

In itself, this doesn't seem like much, since Λ_σ is obviously linearly dependent from Λ. However, revisiting the technique of *interpolation determinants* for establishing lower bounds for linear forms in logarithms, one sees that this extra piece of information can be used to get improved estimates. This is perhaps not so surprising if one thinks about the subspace theorem of Schmidt and Schlickewei, in which one considers the simultaneous smallness of several forms at once: the fact that Λ and Λ_σ are both small does contain some important arithmetic information, because it tells us that a certain number is small not just under one, but under *two* complex embeddings.

However, even the fact that two linear forms in logarithms are simultaneously extremely small turns out not to be enough for our purposes. A back-of-the-envelope calculation suggests that, when $D = 2$, one can use this observation – together with the fact that α_1 is an algebraic unit – to prove that (1) has no non-trivial solutions for $p > 100$: unfortunately, this would still leave open a few computationally intractable cases.

The other observation that comes to our rescue is again related to the fact that α_1 is an algebraic unit. Specifically, by plugging the information that α_1 is invertible into our variant of interpolation determinants, we can remove the dependence of the final estimate on both the *height* and the *degree* of α_1, and only make it depend on its *size* (that is, complex absolute value). The crucial remark is now that the same inequalities can then be applied to any fractional power of α_1, because (for any integer $k \geq 1$) the algebraic number $\alpha_1^{1/k}$ is still an algebraic unit, all of whose conjugates have only two possible absolute values, namely $\alpha_1^{\pm 1/k}$. As k tends to infinity, the absolute value of $\alpha_1^{1/k}$ tends to 1: since this absolute value – or rather its logarithm – is an important parameter in the estimates for linear forms, this leads to a further significant gain in the upper bound (even though, for technical reasons, we cannot quite take the limit $k \to \infty$; we will take h to be a large, but finite, value). Replacing α_1 with a fractional power is usually not convenient when working with linear forms in logarithms, because the known estimates all have rather bad dependence on the degree of the algebraic numbers involved. Our contribution is to completely get rid of this dependence for our linear form, which gives us one more degree of freedom – the parameter h – to play with. We believe that this idea is quite new, and hope that it can have applications to other diophantine problems as well.

Concretely, the technical tools we use to prove Theorem 1.1 are formalised in Theorem 2.16, which we do not repeat here due to the extensive notation that is necessary to state it. This result is a

lower bound for linear forms in two logarithms, obtained as a variant of a well-known theorem of Laurent [Lau08, Theorem 1]. It only applies to very special linear forms: as explained above, we have to assume that α_1 is an algebraic unit and that several linear forms are simultaneously small; moreover, the absolute values of the conjugates of α_1, α_2 need to be related to one another in a simple manner. However, when the theorem *does* apply, the lower bound it provides is vastly better than any previously available estimate on linear forms in two logarithms. We state Theorem 2.16 in a way that makes it easy to compare it with [Lau08, Theorem 1]; it will be clear that the hypotheses of our result are much more restrictive, but the bound we obtain is much sharper. As in the work of Laurent, it is not immediately obvious what lower bound the theorem implies for a given linear form, because its application requires choosing the values of several parameters. By arguments similar to those in Laurent's paper, one could deduce explicit lower bounds for the linear form $|b_1 \log \alpha_1 - b_2 \log \alpha_2|$ with a simple dependence on $b_1, b_2, \alpha_1, \alpha_2$. However, due to the restrictive hypotheses and the fact that any corollary of the main theorem would necessarily provide (much) worse bounds than a direct application of Theorem 2.16, we do not work out such consequences here. We hope that Theorem 2.16 can be applied directly to other diophantine problems; the present paper, and especially Section 4, should suffice to provide a blueprint of how to deal with any concrete linear form.

The structure of the paper is as follows. In Section 2 we derive our estimates for linear forms in logarithms. The results in this section are completely independent of their application to Equation (1). In Section 3 we first set some useful notation and reduce the resolution of Equation (1) to the study of a linear form in two logarithms of algebraic numbers. We then review some known results on Equation (1) for $D = 2$ and show how to adapt them to the cases $D = 3, 5, 37$. Specifically, combining estimates for linear forms in logarithms already available in the literature, ideas from the modular method, arithmetic considerations related to continued fractions, and the algorithmic techniques for the resolution of Thue equations, we show that for any non-trivial solution of Equation (1), neither b nor p can be too small. We also prove that a certain auxiliary parameter (called r and discussed in greater detail in Section 3) – which in principle can vary between 0 and $p-1$ – is uniquely determined, or at least severely constrained, by the value of D. While some of the results concerning the special case $D = 2$ have been obtained in a somewhat ad hoc manner, we develop techniques that can be applied to any squarefree D that is not a square modulo 8 (or even any D, if we restrict to solutions of Equation (1) in which b is odd and $(a, b) = 1$).

We point out that the work in this section is only necessary to solve Equation (1) for $D = 3, 5$ and 37, because the known results would suffice for the case $D = 2$. We include a discussion of the other values of D for two main reasons: first, because it shows that the method we propose is capable of handling Equation (1) for several values of D, including some of the most notoriously difficult ones; second, because the material in Section 3 provides a roadmap to solving Equation (1) for any fixed value of D, and it seems useful to gather all the necessary ingredients in one place.

In Section 4 we then deduce Theorems 1.1 and 1.2 from Theorem 2.16. This section also contains some intermediate general lemmas which should make the application of Theorem 2.16 to other linear forms fairly straightforward. Finally, Appendices A and B contain some elementary lemmas which we have chosen to isolate in order to streamline the main body of the paper.

Notation. All the notation in the paper is standard. For completeness, we recall the definition of the logarithmic height h of an algebraic number α. Let $p(x) = c_n x^n + \cdots + c_0$ be the minimal polynomial of α over $\mathbb{Z}$, so that $p(x)$ is irreducible, $p(\alpha) = 0$, $c_0, \ldots, c_n \in \mathbb{Z}$, and $(c_0, \ldots, c_n) = 1$. The height of α is by definition

$$h(\alpha) = \frac{1}{n} \left(\log |c_0| + \sum_{\beta \in \mathbb{C} : p(\beta) = 0} \log \max\{1, |\beta|\} \right).$$

Computations. We use computer-aided calculations at several points in the paper. To allow the reader to check these computations with minimal effort, MAGMA and GP scripts verifying them can be found in the online repository

https://github.com/DavideLombardoMath/LebesgueNagell.

We would like to point out that the final computations of Section 4.6, i.e., those necessary to apply Theorem 2.16, are in fact completely straightforward and would require nothing more than a pocket

calculator. More extensive computations (that still only take minutes on a modern laptop) are required only for the preliminary results in Section 3.

Acknowledgements. I would like to thank Angelos Koutsianas for many interesting discussions about Equation (1) over the years. I acknowledge financial support from the University of Pisa through grant PRA-2022-10 and from MUR through grant PRIN-2022HPSNCR (funded by the European Union project "Next Generation EU"). I am a member of the GNSAGA INdAM group.

2 The interpolation determinant

In this section, we prove a lower bound for certain linear forms in logarithms. The method of proof is based on interpolation determinants, for which we follow [Lau08]. The general structure of the proof mirrors closely the arguments in [Lau08], but the details are quite different; in particular, our lower bound for the size of the interpolation determinant is rooted in a very different application of Liouville's inequality. Apart from the details of the proof, the main innovation we introduce is the observation that assumptions like those in Condition 2.3 below can lead to significantly improved estimates on linear forms in logarithms.

The results we obtain hold in some generality, but in this paper, we will only use them for one specific linear form, and so we only prove an analogue in our context of [Lau08, Theorem 1], without deriving corollaries similar to [Lau08, Corollary 1 and 2]. The main reason for this is that we need very sharp estimates for the proof of Theorem 1.1, and in the derivation of the corollaries the sharpness of the inequalities would necessarily deteriorate. The second, related reason is that Theorem 2.16 is already quite easy to apply when combined with the calculations in Section 4, which we have tried to make as general as possible.

We will use the following notation.

Notation 2.1. We fix non-zero complex algebraic numbers α_1, α_2 and positive integers b_1, b_2, and we define

$$\Lambda := b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where $\log \alpha_1, \log \alpha_2$ are arbitrary determinations of the logarithms. We further fix an algebraic integer $\delta \in \mathbb{Q}(\alpha_1, \alpha_2)$ such that δ/α_2 is an algebraic integer, and write $\log \overline{|\delta|} := \max_\tau |\log |\tau(\delta)||$, as τ varies among the embeddings $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$.

Remark 2.2. The final lower bound for $|\Lambda|$ will depend on the quantity $\log \overline{|\delta|}$. One can systematically choose a δ_0 such that δ_0/α_2 is an algebraic integer with $\log \overline{|\delta_0|}$ bounded in terms of the height of α_2, but it seems more flexible to keep the extra parameter δ free: for example, if $1/\alpha_2$ is an algebraic integer, one can simply take $\delta = 1$, independently of the height of α_2.

We assume that these data satisfy the following:

Condition 2.3. *1. α_1 is an algebraic unit;*

2. for every $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$, there are determinations of $\log \tau(\alpha_1)$ and $\log \tau(\alpha_2)$ such that

$$\Lambda_\tau := b_2 \log \tau(\alpha_2) - b_1 \log \tau(\alpha_1)$$

has the same absolute value as $\Lambda_{\mathrm{id}} = \Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$;

3. for every $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$ we have

$$|\log |\tau(\alpha_i)|| = |\log |\alpha_i|| \quad \text{for } i = 1, 2.$$

2.1 Definition of Δ

We start by introducing several parameters that we will use to define the relevant interpolation determinant.

Notation 2.4. We let:

1. K, L, R_1, R_2, S_1, S_2 be positive integers with $K \geq 2$;

2. ρ, μ be real numbers with $\rho > 1$ and $\frac{1}{3} \le \mu \le 1$;

3. $R := R_1 + R_2 - 1$, $S := S_1 + S_2 - 1$, $N := KL$, $g = \frac{1}{4} - \frac{N}{12RS}$;

4. $\sigma := \frac{1+2\mu-\mu^2}{2}$, $\gamma := \frac{(R-1)b_2+(S-1)b_1}{2} \left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)}$.

Note that γ is denoted by b in [Lau08]. However, this notation would conflict with our notation for solutions of Equation (1).

We further impose that these parameters satisfy the following conditions.

Condition 2.5. *We have*

$$\#\{\alpha_1^r \alpha_2^s : 0 \le r < R_1, 0 \le s < S_1\} \ge L \tag{2}$$

and

$$\#\{rb_2 + sb_1 : 0 \le r < R_2, 0 \le s < S_2\} \ge (K-1)L. \tag{3}$$

Let $\mathcal{M}$ be the $KL \times RS$ matrix whose entries are

$$\binom{rb_2 + sb_1}{k} \alpha_1^{lr} \alpha_2^{ls},$$

where (k, l) with $0 \le k < K, 0 \le l < L$ is the row index and (r, s) with $0 \le r < R, 0 \le s < S$ is the column index. By [LMN95, Lemma 5], under Condition 2.5, the rank of $\mathcal{M}$ is $N = KL$.

Remark 2.6. The fact that the rank of $\mathcal{M}$ is KL implies that the number of its columns is at least KL, that is, Condition 2.5 implies $RS \ge KL$.

Let Δ be a non-zero $N \times N$ minor of $\mathcal{M}$. Numbering the rows and columns of the submatrix corresponding to Δ, we can write

$$\Delta = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} \alpha_1^{l_i r_j} \alpha_2^{l_i s_j}\right) \tag{4}$$

for certain sequences $(k_i, l_i)_{1 \le i \le N}$ and $(r_j, s_j)_{1 \le j \le N}$. We will need upper and lower bounds for $|\Delta|$. For the upper bound, we will use a modification of [Lau08, Lemma 2] that we will discuss in Section 2.3 below. In the next section we discuss instead our lower bound, which is rather different in nature than the corresponding lower bound in [Lau08, Lemma 1] (itself simply a restatement of [LMN95, Lemma 6]). Specifically, we do not give a lower bound for $|\Delta|$ itself, but rather for $|\tau(\Delta)|$ for *some* (unspecified) embedding $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$. The assumptions of Condition 2.3 will then be used to show that (independently of τ) one can obtain a good upper bound for $|\tau(\Delta)|$: combining these bounds will lead to the desired estimate for $|\Lambda|$.

To state and prove both the upper and the lower bound we need a final piece of notation:

Notation 2.7. We set

$$G_1 = gLRN/2, \quad G_2 = gLSN/2$$
$$M_1 = (L-1)(r_1 + \cdots + r_N)/2, \quad M_2 = (L-1)(s_1 + \cdots + s_N)/2.$$

We further let $V_1 = \lfloor M_1 + G_1 \rfloor$ (resp. $V_2 = \lfloor M_2 + G_2 \rfloor$) and $U_1 = \lceil M_1 - G_1 \rceil$ (resp. $U_2 = \lceil M_2 - G_2 \rceil$).

2.2 Lower bound for Δ

We continue with the notation of the previous section. In particular, (k_i, l_i) and (r_j, s_j) are sequences of pairs of positive integers that index the rows and columns of $\mathcal{M}$ giving the minor Δ. Consider the polynomial [LMN95, page 297]

$$P(X, Y) := \sum_{\sigma \in S_N} (-1)^\sigma \prod_{i=1}^{N} \binom{r_{\sigma(i)} b_2 + s_{\sigma(i)} b_1}{k_i} X^{\sum_{i=1}^N l_i r_{\sigma(i)}} Y^{\sum_{i=1}^N l_i s_{\sigma(i)}}.$$

By [LMN95, page 298] we have

$$\Delta = P(\alpha_1, \alpha_2) = \alpha_1^{V_1} \alpha_2^{V_2} \tilde{P}\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}\right),$$

where $\tilde{P}(X,Y)$ is a polynomial with integral coefficients whose degrees in X and Y are bounded above by $V_1 - U_1$ and $V_2 - U_2$ respectively. Let

$$d_Y := \text{exact degree in } Y \text{ of the polynomial } \tilde{P}. \tag{5}$$

Write

$$\tilde{P}(X,Y) = \sum_{q=0}^{d_Y} \tilde{P}_q(X) Y^q,$$

where each $\tilde{P}_q(X)$ is a polynomial with integer coefficients. From this expression, it is clear that

$$\omega := \delta^{d_Y} \tilde{P}\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}\right) = \delta^{d_Y} \sum_{q=0}^{d_Y} \tilde{P}_q\left(\frac{1}{\alpha_1}\right) \cdot \left(\frac{1}{\alpha_2}\right)^q = \sum_{q=0}^{d_Y} \tilde{P}_q\left(\frac{1}{\alpha_1}\right) (\delta/\alpha_2)^q \cdot \delta^{d_Y - q} \tag{6}$$

is an algebraic integer, because α_1 is an algebraic unit, $\tilde{P}_q$ has integer coefficients, and $\delta, \delta/\alpha_2$ are algebraic integers by assumption. We now use the following obvious fact:

Lemma 2.8. *Let $\omega \in \overline{\mathbb{Z}}$ be an algebraic integer and let $L = \mathbb{Q}(\omega)$. Suppose that $\omega \neq 0$. There exists an embedding $\tau : L \hookrightarrow \mathbb{C}$ such that $|\tau(\omega)| \geq 1$.*

Proof. The quantity $|N_{L/\mathbb{Q}}(\omega)|$ is an algebraic integer which lies in $\mathbb{Q}$ and is non-negative and non-zero, hence it is ≥ 1. Since

$$1 \leq |N_{L/\mathbb{Q}}(\omega)| = \prod_{\tau : L \hookrightarrow \mathbb{C}} |\tau(\omega)|,$$

at least one factor $|\tau(\omega)|$ must be greater than or equal to 1. □

Fix a τ such that $|\tau(\omega)| \geq 1$, as in Lemma 2.8 (which applies, because ω is nonzero; in turn, this is a consequence of the fact that $\Delta \neq 0$). We also extend τ to an embedding $\mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$ (note that $\omega \in \mathbb{Q}(\alpha_1, \alpha_2)$). We then obtain

$$\begin{aligned} \tau(\Delta) &= \tau \det\left(\binom{r_j b_2 + s_j b_1}{k_i} \alpha_1^{l_i r_j} \alpha_2^{l_i s_j}\right) \\ &= \det\left(\binom{r_j b_2 + s_j b_1}{k_i} \tau(\alpha_1)^{l_i r_j} \tau(\alpha_2)^{l_i s_j}\right) \end{aligned}$$

and at the same time

$$\tau(\Delta) = \tau(P(\alpha_1, \alpha_2)) = \tau(\alpha_1)^{V_1} \tau(\alpha_2)^{V_2} \tilde{P}(\tau(1/\alpha_1), \tau(1/\alpha_2)) = \tau(\alpha_1)^{V_1} \tau(\alpha_2)^{V_2} \tau\left(\delta^{-d_Y} \omega\right).$$

The second of these equations implies

$$|\tau(\Delta)| = |\tau(\alpha_1)|^{V_1} |\tau(\alpha_2)|^{V_2} |\tau(\delta)|^{-d_Y} |\tau(\omega)| \geq |\tau(\alpha_1)|^{V_1} |\tau(\alpha_2)|^{V_2} |\tau(\delta)|^{-d_Y},$$

and we have therefore proved the following lemma:

Lemma 2.9. *Using Notations 2.1, 2.4, and 2.7, assume that Conditions 2.3 and 2.5 are satisfied. There is an embedding $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$ such that*

$$\log|\tau(\Delta)| \geq V_1 \log|\tau(\alpha_1)| + V_2 \log|\tau(\alpha_2)| - d_Y \log|\tau(\delta)|,$$

for some $d_Y \leq V_2 - U_2$.

Remark 2.10. This statement should be contrasted with [Lau08, Lemma 1] and [LMN95, Lemma 5]. By definition, $V_i \leq M_i + G_i$ and $d_Y \leq V_2 - U_2 \leq 2G_2$, so – if $\log|\tau(\alpha_i)| \geq 1$ – the estimate in Lemma 2.9 can also be written as $\log|\Delta| \geq (M_1 + G_1)\log|\tau(\alpha_1)| + (M_2 + G_2)\log|\tau(\alpha_2)| - 2G_2 \log|\tau(\delta)|$. If we further suppose that δ is roughly of the same height as α_2 – which for generic α_2 is reasonable – then one can bound $\log|\tau(\delta)| \leq [\mathbb{Q}(\delta) : \mathbb{Q}]h(\delta) \approx [\mathbb{Q}(\alpha_2) : \mathbb{Q}]h(\alpha_2)$. Comparing with [Lau08, Lemma 1] we then see that – at the price of an unspecified embedding τ – we have completely removed the term $-2DG_1 h(\alpha_1)$, that is, we have removed the dependence on the degree and height of α_1.

2.3 Upper bound for Δ

We keep all the symbols introduced in Notations 2.4 and 2.7. We will apply [Lau08, Lemma 2]. Since that lemma is stated in a slightly less general context than what we need, we find it useful to state and prove precisely the version we will use, even at the cost of repeating some arguments already in the literature.

As in the whole section, we let α_1, α_2 be arbitrary nonzero complex numbers and b_1, b_2 be non-negative integers. In particular, α_1, α_2 need not be real, nor have absolute value greater than 1. We will eventually apply the result to $\tau(\alpha_1), \tau(\alpha_2)$, where τ is the embedding of Lemma 2.8, but since τ plays no role here, for simplicity we state and prove the lemma for general values $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \{0\}$.

As above, we consider the determinant Δ of a non-zero $N \times N$ minor of the $KL \times RS$ matrix whose entries are

$$\binom{rb_2 + sb_1}{k} \alpha_1^{lr} \alpha_2^{ls}.$$

We denote again by $(k_i, l_i)_{1 \le i \le N}$ and $(r_j, s_j)_{1 \le j \le N}$ the sequences indexing the rows and columns of Δ. Since we have assumed $RS \ge KL$ (see Remark 2.6), the pairs (k_i, ℓ_i) are a permutation of the $N = KL$ pairs (k, ℓ) with $0 \le k < K$ and $0 \le \ell < L$. In particular, we can assume $l_i = \lfloor \frac{i}{K} \rfloor$ and (independently of the numbering) we have

$$\sum_{i=1}^{N} k_i = L \sum_{k=0}^{K-1} k = (K-1)K/2 \cdot L = N(K-1)/2. \tag{7}$$

The following is essentially [Lau08, Lemma 2].

Lemma 2.11. *Recall Notations 2.4 and 2.7. Let Λ be the linear form in logarithms*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

for certain determinations of $\log \alpha_1, \log \alpha_2$. Assume that

$$|\Lambda'| \le \rho^{-\mu N}, \tag{8}$$

where

$$\Lambda' := \Lambda \max\left\{ \frac{LSe^{LS|\Lambda|/2b_2}}{2b_2}, \frac{LRe^{LR|\Lambda|/2b_1}}{2b_1} \right\}. \tag{9}$$

We have

$$\begin{aligned} |\Delta| \le & \rho^{-(\sigma N^2 - N)/2} N (e^N + (e-1)^N) \cdot N! \cdot (\rho\gamma)^{(K-1)N/2} \\ & \times |\alpha_1|^{M_1} |\alpha_2|^{M_2} e^{\rho(G_1 |\log|\alpha_1|| + G_2 |\log|\alpha_2||)}. \end{aligned}$$

The rest of this subsection is dedicated to proving Lemma 2.11. As already pointed out, the proof only requires minor modifications with respect to [Lau08], so we only give limited details. We set

$$\lambda_i := \ell_i - \frac{L-1}{2}, \tag{10}$$

so that the λ_i sum to 0. We further introduce

$$\beta = b_1/b_2 \quad \text{and} \quad \eta := \frac{(R-1) + \beta(S-1)}{2}. \tag{11}$$

Since the statement of Lemma 2.11 is clearly symmetric in (α_1, b_1) and (α_2, b_2), up to exchanging α_1 with α_2 and b_1 with b_2, we may assume

$$b_1 |\log|\alpha_1|| \le b_2 |\log|\alpha_2||. \tag{12}$$

It is then certainly enough to prove the desired upper bound assuming

$$\Lambda'' \le \rho^{-\mu N},$$

where $\Lambda'' := \left(\frac{LS\Lambda}{2b_2}\right) e^{LS|\Lambda|/(2b_2)}$. As in [Lau94, p. 191, next to last displayed equation] or [Lau08, p. 331, next to last displayed equation] we have

$$\Delta = \alpha_1^{M_1}\alpha_2^{M_2} \det\left(\frac{b_2^{k_i}}{k_i!}(r_j + s_j\beta - \eta)^{k_i}\alpha_1^{\ell_i r_j}\alpha_2^{\ell_i s_j}\right). \tag{13}$$

By definition of Λ we have $\log\alpha_2 = \beta\log\alpha_1 + \Lambda/b_2$ and we may therefore write

$$\alpha_1^{\lambda_i r_j}\alpha_2^{\lambda_i s_j} = \alpha_1^{\lambda_i(r_j+s_j\beta-\eta)}\alpha_1^{\lambda_i\eta}e^{\lambda_i s_j\Lambda/b_2}, \tag{14}$$

where for $x \in \mathbb{C}$ the exponentiation α_1^x is defined to be $\exp(x\log\alpha_1)$ for the given determination of $\log\alpha_1$.

Remark 2.12. Notice that this convention is irrelevant for the left-hand side of the above equality, which only involves integral exponents. It is however essential to make sense of the right-hand side. This point is not stressed in [Lau08, last formula on p. 331], where one finds the same identity. We also remark that, *since the exponents* $\lambda_i(r_j + s_j\beta - \eta)$ *and* $\lambda_i\eta$ *are real numbers*, we have the equalities

$$|\alpha_1^{\lambda_i(r_j+s_j\beta-\eta)}| = |\alpha_1|^{\lambda_i(r_j+s_j\beta-\eta)}, \quad |\alpha_1^{\lambda_i\eta}| = |\alpha_1|^{\lambda_i\eta}.$$

Replacing (14) in (13) and factoring out of the determinant the product $\prod_{i=1}^N \alpha_1^{\lambda_i\eta} = \alpha_1^{\eta\sum_{i=1}^N\lambda_i} = \alpha_1^0 = 1$, we find

$$\Delta = \alpha_1^{M_1}\alpha_2^{M_2}\det\left(\varphi_i(z_j)e^{\lambda_i s_j\Lambda/b_2}\right),$$

where

$$\varphi_i(x) = \frac{b_2^{k_i}}{k_i!}x^{k_i}\alpha_1^{\lambda_i x} \quad \text{and} \quad z_j = r_j + s_j\beta - \eta,$$

see [Lau08, p. 332, first displayed equation]. Still following [Lau08, p. 332], we develop the determinant Δ as

$$\Delta = \alpha_1^{M_1}\alpha_2^{M_2}\sum_{n_1\geq 0}\cdots\sum_{n_N\geq 0}\Delta_{\underline{n}},$$

where $\underline{n} = (n_1, \ldots, n_N)$ and

$$\Delta_{\underline{n}} = \det\left(\varphi_i(z_j)\frac{(\lambda_i s_j\Lambda/b_2)^{n_i}}{n_i!}\right).$$

Now fix a tuple $\underline{n}$ and let $m_1, \ldots, m_l$ be the distinct values taken by the n_i in the N-tuple $\underline{n}$. Arrange these values in ascending order as $m_1 < m_2 < \cdots < m_l$. For each integer t with $1 \leq t \leq l$ we denote by I_t the subset of indices i for which $n_i = m_t$ and by $\nu_t = \#I_t$ the number of occurrences of the value m_t in the sequence $\underline{n}$.

Our next two lemmas are slight variants of the arguments in [Lau94, Lemma 8] (see also [LMN95, Lemme 7]) and [Lau08, Lemma 4] respectively. Notice however that in our statements we have $|\log|\alpha_i||$ where [Lau08] has $|\log\alpha_i|$. This difference will be crucial for us.

Lemma 2.13 (cf. the proof of [Lau94, Lemma 8])**.** *Let* ψ *be any permutation of* $\{1, \ldots, N\}$*. We have*

$$\prod_{i=1}^N |\varphi_i(xz_{\psi(i)})| \leq (|x|\gamma)^{(K-1)N/2}\exp\left(|x|(G_1|\log|\alpha_1|| + G_2|\log|\alpha_2||)\right).$$

Proof. By definition and Remark 2.12 we have

$$\prod_{i=1}^N |\varphi_i(xz_{\psi(i)})| = \prod_{i=1}^N \left|\frac{(b_2 xz_{\psi(i)})^{k_i}}{k_i!}\right| |\alpha_1|^{(\sum_{i=1}^N\lambda_i z_{\psi(i)})x},$$

and using $\sum_{i=1}^N \lambda_i = 0$ we obtain

$$\begin{aligned}\sum_{i=1}^N \lambda_i z_{\psi(i)} &= \sum_{i=1}^N \lambda_i (r_{\psi(i)} + \beta s_{\psi(i)} - \eta) \\ &= \sum_{i=1}^N \lambda_i r_{\psi(i)} + \beta \sum_{i=1}^N \lambda_i s_{\psi(i)} - \eta \sum_{i=1}^N \lambda_i \\ &= \sum_{i=1}^N \lambda_i r_{\psi(i)} + \beta \sum_{i=1}^N \lambda_i s_{\psi(i)}.\end{aligned}$$

By [LMN95, Lemma 4] we have

$$|\sum_{i=1}^N \lambda_i r_{\psi(i)}| \le G_1, \quad \beta|\sum_{i=1}^N \lambda_i s_{\psi(i)}| \le \beta G_2,$$

and therefore (independently of whether $|\alpha_1| \ge 1$ or $|\alpha_1| < 1$) we obtain

$$\left|\alpha_1^{(\sum_{i=1}^N \lambda_i z_{\psi(i)})x}\right| = |\alpha_1|^{(\sum_{i=1}^N \lambda_i z_{\psi(i)})x} \le \exp(|\log|\alpha_1||(G_1 + \beta G_2)|x|).$$

Assumption (12) gives $\beta|\log|\alpha_1|| \le |\log|\alpha_2||$, and therefore

$$\left|\alpha_1^{(\sum_{i=1}^N \lambda_i z_{\psi(i)})x}\right| \le \exp(|\log|\alpha_1||(G_1 + \beta G_2)|x|) \le \exp((G_1|\log|\alpha_1|| + G_2|\log|\alpha_2||)|x|).$$

It remains to treat the product

$$\prod_{i=1}^N \left|\frac{(b_2 x z_{\psi(i)})^{k_i}}{k_i!}\right|.$$

We bound this from above using the trivial estimate

$$\begin{aligned}|b_2 z_{\psi(i)}| &= |b_2(r_{\psi(i)} + \beta s_{\psi(i)} - \eta)| \\ &= |b_2 r_{\psi(i)} + b_1 s_{\psi(i)} - \frac{b_2(R-1) + b_1(S-1)}{2}| \\ &= \left|b_2\left(r_{\psi(i)} - \frac{R-1}{2}\right) + b_1\left(s_{\psi(i)} - \frac{S-1}{2}\right)\right| \\ &\le \frac{b_2(R-1) + b_1(S-1)}{2},\end{aligned}$$

which gives

$$\prod_{i=1}^N \left|\frac{(b_2 x z_{\psi(i)})^{k_i}}{k_i!}\right| \le \left(\frac{b_2(R-1) + b_1(S-1)}{2}\right)^{\sum_{i=1}^N k_i} |x|^{\sum_{i=1}^N k_i} \left(\prod_{i=1}^N k_i!\right)^{-1}.$$

It now suffices to use the identities $\sum_{i=1}^N k_i = (K-1)N/2$ (see (7)) and

$$\left(\prod_{i=1}^N k_i!\right)^{-1} = \left(\prod_{k=1}^K k!\right)^{-L} = \left(\prod_{k=1}^K k!\right)^{\frac{N(K-1)}{2} \cdot \frac{-2}{K^2-K}}$$

to obtain

$$\begin{aligned}\prod_{i=1}^N \left|\frac{(b_2 x z_{\psi(i)})^{k_i}}{k_i!}\right| &\le |x|^{(K-1)N/2} \left(\frac{b_2(R-1) + b_1(S-1)}{2} \cdot \left(\prod_{k=1}^K k!\right)^{-\frac{2}{K^2-K}}\right)^{(K-1)N/2} \\ &= (|x|\gamma)^{(K-1)N/2}.\end{aligned}$$

This concludes the proof. □

Lemma 2.14 (cf. [Lau08, Lemma 4]). *For any N-tuple $\underline{n} = (n_1, \dots, n_N)$ of non-negative integers and any real number $\rho > 1$, we have the upper bound*

$$|\Delta_{\underline{n}}| \leq \Omega \rho^{-\sum_{t=1}^{\ell} \binom{\nu_t}{2}} \left(\frac{LS|\Lambda|}{2b_2}\right)^{\sum_{i=1}^{N} n_i} \left(\prod_{i=1}^{N} n_i!\right)^{-1}$$

with

$$\Omega = N!(\rho\gamma)^{(K-1)N/2} e^{\rho(G_1|\log|\alpha_1||+G_2|\log|\alpha_2||)}.$$

Proof. The proof is virtually identical to that of [Lau08, Lemma 4], simply replacing [Lau94, Lemma 8] with Lemma 2.13. □

At this point, the rest of the proof of [Lau08, Lemma 2] goes through and shows Lemma 2.11: one simply needs to apply Lemma 2.14 instead of [Lau08, Lemma 4].

2.4 The linear form in logarithms

We now have all the tools to prove our lower bound for linear forms in logarithms.

Proposition 2.15. *Using Notations 2.1, 2.4, and 2.7, assume that Conditions 2.3 and 2.5 are satisfied. Let τ be the embedding of Lemma 2.9. Set*

$$\Lambda' := \Lambda \max\left\{\frac{LSe^{LS|\Lambda|/2b_2}}{2b_2}, \frac{LRe^{LR|\Lambda|/2b_1}}{2b_1}\right\}. \tag{15}$$

At least one of the following holds (recall that d_Y has been introduced in Equation (5)):

1. $|\Lambda'| > \rho^{-\mu N}$;
2. $V_1 \log|\tau(\alpha_1)| + V_2 \log|\tau(\alpha_2)| - d_Y \log|\tau(\delta)| \leq \log|\tau(\Delta)|$ *and simultaneously*

$$\begin{aligned}\log|\tau(\Delta)| \leq &-\frac{\sigma N^2 - N}{2}\log\rho + \log\left(N(e^N + (e-1)^N)N!\right) + \frac{(K-1)N}{2}\log(\rho\gamma)\\ &+ M_1\log|\tau(\alpha_1)| + M_2\log|\tau(\alpha_2)| + \rho(G_1|\log|\tau(\alpha_1)|| + G_2|\log|\tau(\alpha_2)||).\end{aligned}$$

Proof. The lower bound in (2) always holds, by Lemma 2.9. Suppose that the inequality in (1) does not hold: then the upper bound in (2) follows from Lemma 2.11, applied to $\tau(\alpha_1), \tau(\alpha_2)$ in place of α_1, α_2. We note explicitly that here we use the second part of Condition 2.3 to deduce the equality between

$$|\Lambda'_\tau| := |\Lambda_\tau| \max\left\{\frac{LSe^{LS|\Lambda_\tau|/2b_2}}{2b_2}, \frac{LRe^{LR|\Lambda_\tau|/2b_1}}{2b_1}\right\},$$

which is the quantity appearing in the hypothesis of Lemma 2.11, and the original linear form $|\Lambda'|$. □

We now manipulate the inequalities in case (2) of this statement. More precisely, we show that they imply a slightly less sharp, but more manageable, inequality. Assume that both inequalities in case (2) of Proposition 2.15 hold. Then we have

$$\begin{aligned}V_1\log|\tau(\alpha_1)| + V_2\log|\tau(\alpha_2)| - d_Y|\log|\tau(\delta)|| &\leq V_1\log|\tau(\alpha_1)| + V_2\log|\tau(\alpha_2)| - d_Y\log|\tau(\delta)|\\ &\leq \log|\tau(\Delta)|\\ &\leq -\frac{\sigma N^2 - N}{2}\log\rho + \log\left(N(e^N + (e-1)^N)N!\right) + \frac{(K-1)N}{2}\log(\rho\gamma)\\ &\quad + M_1\log|\tau(\alpha_1)| + M_2\log|\tau(\alpha_2)| + \rho(G_1|\log|\tau(\alpha_1)|| + G_2|\log|\tau(\alpha_2)||);\end{aligned}$$

rearranging we get

$$\begin{aligned}\left(\frac{\sigma N^2 - N}{2} - \frac{N(K-1)}{2}\right)\log\rho \leq\ & d_Y|\log|\tau(\delta)|| + \log\left(N(e^N + (e-1)^N)N!\right) + \frac{(K-1)N}{2}\log\gamma\\ &+ (M_1 - V_1)\log|\tau(\alpha_1)| + (M_2 - V_2)\log|\tau(\alpha_2)|\\ &+ \rho(G_1|\log|\tau(\alpha_1)|| + G_2|\log|\tau(\alpha_2)||).\end{aligned} \tag{16}$$

Now we recall that by definition (see Notation 2.7) we have $V_i = \lfloor M_i + G_i \rfloor$, $U_i = \lceil M_i - G_i \rceil$, and by construction $d_Y \leq V_2 - U_2 \leq 2G_2$. In particular, for $i = 1, 2$ we have the following trivial estimates for $M_i - V_i$:

$$-G_i \leq M_i - (M_i + G_i) \leq M_i - V_i \leq M_i - (M_i + G_i - 1) = -G_i + 1.$$

It follows that $|M_i - V_i| \leq G_i$. Plugging these estimates into (16) and using Condition 2.3 to replace $|\log|\tau(\alpha_1)||$ with $|\log|\alpha_1||$, we arrive at

$$\begin{aligned}\left(\frac{\sigma N^2 - NK}{2}\right) \log \rho &\leq 2G_2 |\log|\tau(\delta)|| + \log\left(N(e^N + (e-1)^N)N!\right) + \frac{(K-1)N}{2} \log \gamma \\ &\quad + G_1 |\log|\tau(\alpha_1)|| + G_2 |\log|\tau(\alpha_2)|| + \rho(G_1 |\log|\tau(\alpha_1)|| + G_2 |\log|\tau(\alpha_2)||) \\ &= 2G_2 |\log|\tau(\delta)|| + \log\left(N(e^N + (e-1)^N)N!\right) + \frac{(K-1)N}{2} \log \gamma \\ &\quad + (\rho+1)(G_1 |\log|\alpha_1|| + G_2 |\log|\alpha_2||).\end{aligned}$$

We now replace G_1, G_2, as well as the first occurrence of N, with their definitions (see Notations 2.4 and 2.7) and divide by $N/2$ to get

$$\begin{aligned}K(\sigma L - 1) \log \rho &\leq 2gLS |\log|\tau(\delta)|| + \frac{2}{N} \log\left(N(e^N + (e-1)^N)N!\right) + (K-1) \log \gamma \\ &\quad + (\rho+1) gL(R |\log|\alpha_1|| + S |\log|\alpha_2||).\end{aligned}$$

We finally use the trivial bound $|\log|\tau(\delta)|| \leq \log \overline{|\delta|}$ to arrive at the final form of our inequality:

Theorem 2.16. *Notations and assumptions as in Proposition 2.15. Set for simplicity* $a_1 := (\rho+1)|\log|\alpha_1||$, $a_2 := (\rho+1)|\log|\alpha_2|| + 2\log\overline{|\delta|}$. *At least one of the following holds:*

1. $|\Lambda'| > \rho^{-\mu N}$;
2. $$K(\sigma L - 1) \log \rho \leq h(N) + (K-1) \log \gamma + gL(Ra_1 + Sa_2), \tag{17}$$

   where

   $$h(N) = \frac{2}{N} \log\left(N(e^N + (e-1)^N)N!\right).$$

As already pointed out, this result should be compared with [Lau08, Theorem]. If we assume that (2) in the theorem does not hold, then (1) does, so Theorem 2.16 is indeed a lower bound for linear forms in logarithms. The assumptions we listed as Condition 2.5 are very similar to those of [Lau08, Theorem], but it is quite apparent that (the negation of) inequality (2) is a much weaker condition than the corresponding inequality (2) in [Lau08, Theorem]. On the other hand, this gain comes at the cost of the very restrictive extra assumptions of Condition 2.3.

To prove Theorem 1.1, we will apply Theorem 2.16 to bound the exponent p in a putative non-trivial solution to Equation (1). The main task will be to choose parameters K, L, R, S such that the inequality (2) is *not* satisfied: this implies that (1) holds, which will provide us with the desired sharp lower bound for the linear form in logarithms $|\Lambda|$. We will carry out this program in Section 4; in the next section we start instead with more algebraic considerations about the solutions of Equation (1).

3 Estimates for solutions of Equation (1)

In this section, we obtain some preliminary results on the non-trivial solutions of Equation (1), including in particular an upper bound for the values of p for which Equation (1) admits non-trivial solutions, and a lower bound for $|b|$ for any non-trivial solution (a, b). These are the two main inputs needed to apply Theorem 2.16 to the resolution of Equation (1).

We start with some algebraic considerations about the solutions of Equation (1). Solving (1) for $p = 2$ (and any value of D) is an easy exercise, so we will assume that $p \geq 3$ throughout. The following is [Bug97b, Lemma 3]:

Lemma 3.1. *Let $D > 1$ be a squarefree integer and let k be a positive odd integer coprime to D. Denote by $\eta > 1$ the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D})$. Let X, Y, Z be positive integers satisfying*

$$X^2 - DY^2 = \pm k^Z.$$

There exist positive integers t and v and an algebraic integer $\pi \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that

$$X + Y\sqrt{D} = \eta^{-t}\pi^v.$$

Moreover, $0 < t \leq v$ and the integer Z/v divides h_D, the class number of $\mathbb{Q}(\sqrt{D})$.

To apply this lemma (with $X = a, Y = 1, k = b, Z = p$), we note that if (a, b) is a solution of Equation (1) for some $D \in \{2, 3, 5\}$ and $p \geq 3$, then b is odd, for otherwise – taking (1) modulo 8 – we get $a^2 \equiv D \pmod 8$, which is impossible for all the values of D under consideration. Moreover, suppose $(k, D) = (b, D)$ is divisible by some prime q. Then we have $q \mid X = a$, and considering the equation modulo q^2 we get $0 - D \equiv 0 \pmod{q^2}$, contradicting the fact that D is squarefree.

Remark 3.2. The same argument shows that Lemma 3.1 can be applied whenever D is squarefree and not a square modulo 8.

Let (a, b) be a solution of Equation (1) for certain values of D and p. For the rest of this discussion, we will assume that the exponent p does not divide the class number h_D of $\mathbb{Q}(\sqrt{D})$: in practice, this is a very mild constraint (and for $D \in \{2, 3, 5\}$ it only excludes $p = 2$). Under this assumption, Lemma 3.1, applied to the identity $a^2 - D \cdot 1^2 = b^p$ with b odd, yields

$$a + \sqrt{D} = \eta^t \pi^p$$

for some $\pi \in \mathcal{O}_{\sqrt{D}}$, because the condition $\frac{p}{v} \mid h_D$ implies $p \mid v$ under our assumption $p \nmid h_D$. Multiplying π by (powers of) η^{-1} if necessary, we can then assume that

$$a + \sqrt{D} = \eta^r \pi^p \tag{18}$$

with $-\frac{p-1}{2} \leq r \leq \frac{p-1}{2}$.

We denote by σ the generator of the group $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ and write $\overline{\pi} = \sigma(\pi), \overline{\eta} = \sigma(\eta)$. Note that $\eta\overline{\eta} = N_{K/\mathbb{Q}}(\eta) = \pm 1$, hence $\overline{\eta} = \pm\eta^{-1}$. We denote the sign appearing in this equation by $\pm_D$. Our next remarks are well-known, see for example the beginning of [Coh07, §15.7.1]. Applying σ to (18) we get

$$a - \sqrt{D} = \overline{\eta}^r \overline{\pi}^p, \tag{19}$$

which implies

$$b^p = a^2 - D = (a + \sqrt{D})(a - \sqrt{D}) = \eta^r \pi^p \cdot \pm_D \eta^{-r} \overline{\pi}^p = \pm_D (\pi\overline{\pi})^p,$$

hence (since p is odd)

$$\pi\overline{\pi} = (\pm_D 1)^r b. \tag{20}$$

Subtracting (19) from (18) we get

$$2\sqrt{D} = (a + \sqrt{D}) - (a - \sqrt{D}) = \eta^r \pi^p - \overline{\eta}^r \overline{\pi}^p, \tag{21}$$

and dividing by $\overline{\eta}^r \overline{\pi}^p = \eta^{-r} (\pm_D 1)^r \cdot \overline{\pi}^p$ we obtain

$$(\pm_D 1)^r \frac{2\sqrt{D}\eta^r}{|\overline{\pi}|^p} = (\pm_D 1)^r \eta^{2r} \left(\frac{\pi}{\overline{\pi}}\right)^p - 1. \tag{22}$$

Remark 3.3. If (a, b) is a solution of Equation (1) with a certain exponent $r = -r_0$, that is,

$$a + \sqrt{D} = \eta^{-r_0} \pi^p,$$

then conjugating we find

$$a - \sqrt{D} = \overline{\eta}^{-r_0} \overline{\pi}^p = \left((\pm_D 1)\eta^{-1}\right)^{-r_0} \overline{\pi}^p = \eta^{r_0} ((\pm_D 1)^{r_0} \overline{\pi})^p,$$

and therefore

$$-a+\sqrt{D}=-(a-\sqrt{D})=\eta^{r_0}((\mp_D 1)^{r_0}\overline{\pi})^p,$$

which means that $(-a,b)$ is a solution with the opposite value of $r=r_0$. Thus, we may (and usually will) assume that r satisfies $0\le r\le\frac{p-1}{2}$. When $r=0$, changing a into $-a$ if necessary (which in this case does not alter the value of r), we can assume $|\overline{\pi}|\ge|\pi|$. This inequality is strict if D is not a perfect p-th power: to see this, notice that $|\overline{\pi}|=|\pi|$ with $r=0$ implies $|a+\sqrt{D}|=|a-\sqrt{D}|$, hence $a=0$, which is not a solution of Equation (1) unless $D=b^p$ for some b.

Note that for fixed D there are only finitely many solutions to Equation (1) with $b\le 0$, and these can be trivially enumerated. This is obvious if $D<0$, in which case there are no solutions at all, while if $D>0$ we have $a^2-D=b^p\le 0$, hence $a\le\sqrt{D}$ and $|b^p|\le|D|$. At least for moderate values of D, such solutions can easily be found (this is certainly the case for the small values of D we are interested in: for $D\in\{2,3,5\}$, the only solutions with $b<0$ are the trivial ones for $D=2,5$). The case $b=1$ is equally easy. Suppose now that $b>1$. In this case, Equation (20) implies that the sign of $\pi/\overline{\pi}$ is $(\pm_D 1)^r$, hence from (22) we obtain

$$1+(\pm_D 1)^r\frac{2\sqrt{D}\eta^r}{|\overline{\pi}|^p}=\eta^{2r}\left(\frac{|\pi|}{|\overline{\pi}|}\right)^p. \tag{23}$$

Set $\beta_1=\eta$ and $\beta_2=|\overline{\pi}|/|\pi|$. Suppose first that

$$\left|(\pm 1)^r\frac{2\sqrt{D}\eta^r}{|\overline{\pi}|^p}\right|\ge\frac{1}{2}:$$

this implies

$$|\overline{\pi}|^p/\eta^r\le 4\sqrt{D},$$

and hence $|a-\sqrt{D}|=|\overline{\pi}^p/\eta^r|\le 4\sqrt{D}\eta$, which gives an absolute (and quite manageable) upper bound for a.

Remark 3.4. For $D\in\{2,3,5\}$, the values of a in this range only lead to trivial solutions.

We may therefore assume $\left|(\pm 1)^r\frac{2\sqrt{D}\eta^r}{|\overline{\pi}|^p}\right|<\frac{1}{2}$: Equation (23), together with the fact that $|\log(1+x)|\le 2|x|$ for $|x|<\frac{1}{2}$, then yields the following. Let Λ_β be the linear form in logarithms

$$\Lambda_\beta:=2r\log\beta_1-p\log\beta_2: \tag{24}$$

then we have

$$|\Lambda_\beta|\le\frac{4\sqrt{D}\eta^r}{|\overline{\pi}|^p}. \tag{25}$$

Most of the rest of the paper is dedicated to obtaining good lower bounds on $|\Lambda_\beta|$. We now set the following notation.

Notation 3.5. We set

$$\begin{aligned}&\alpha_1:=\beta_1^{2/k}=\eta^{2/k},\quad \alpha_2:=\beta_2=\frac{|\overline{\pi}|}{|\pi|}>0,\\ &b_1=kr,\quad b_2:=p,\\ &\Lambda:=b_2\log\alpha_2-b_1\log\alpha_1=p\log\beta_2-2r\log\beta_1,\end{aligned} \tag{26}$$

where $k\ge 1$ is in principle any positive integer (we will fix its value at the very end). Note that we define $\eta^{2/k}$ to be $\exp\left(\frac{2}{k}\log_{\mathbb{R}}(\eta)\right)$, where $\log_{\mathbb{R}}$ is the usual real logarithm.

The form $|\Lambda|$ coincides with the linear form $|\Lambda_\beta|$ considered above, and we will write (25) as

$$|\Lambda|\le\varepsilon:=\frac{4\sqrt{D}\eta^r}{|\overline{\pi}|^p}. \tag{27}$$

Remark 3.6. Consider Equation (21) for fixed values of D, p and r. Suppose for simplicity $D \equiv 2, 3 \pmod 4$, so that $\{1, \sqrt{D}\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Writing $\pi = u + v\sqrt{D}$, $\overline{\pi} = u - v\sqrt{D}$ with $u, v \in \mathbb{Z}$, expanding both sides of (21), and matching coefficients of $\sqrt{D}$ on both sides, we get a Thue equation of degree p. Thus, for every fixed value of $p \geq 3$ one can (in principle) solve Equation (21) and therefore Equation (1) (note that for fixed p there are only finitely many values of r to consider). The same applies, with minimal changes, also for $D = 5$ (and other values congruent to 1 modulo 4): simply write $\pi = u + v\frac{1+\sqrt{5}}{2}, \overline{\pi} = u + v\frac{1-\sqrt{5}}{2}$.

In the rest of the paper, although we will try to frame the discussion in the most general way possible, we focus in particular on the cases $D = 2, 3, 5$. It therefore seems useful to recall that for these values of D the fundamental unit $\eta = \eta_D > 1$ of the ring of integers of $\mathbb{Q}(\sqrt{D})$ is given by

$$\eta_2 = 1 + \sqrt{2}, \quad \eta_3 = 2 + \sqrt{3}, \quad \eta_5 = \frac{1 + \sqrt{5}}{2}.$$

To motivate the rest of this section, we now briefly review some partial results towards the resolution of Equation (1) for $D = 2$. Our objective will then be to obtain analogues of these results also for $D = 3, 5$. We start with a result by Chen which, although we will not use it, shows what can be achieved with the modular method:

Theorem 3.7 ([Che12, Theorem 5])**.** *The equation $a^2 - 2 = b^p$ has no non-trivial solutions for $p \equiv 1, 5, 7, 11 \pmod{24}$ and $p \neq 5, 7$.*

We will, on the other hand, make use of the following estimate, again obtained by the modular method (much weaker estimates would suffice, and later in Section 3.5 we explain how to obtain even stronger lower bounds on b using different techniques):

Lemma 3.8 ([Che12, Corollary 25])**.** *For every non-trivial solution (a, b) of Equation (1) with $D = 2$ we have $b > 10^{102}$.*

Other partial results have been obtained by Bugeaud, Mignotte, and Siksek by combining linear forms in logarithms, ideas related to the modular method, and the computational resolution of Thue equations. Specifically, they prove:

Theorem 3.9 (Bugeaud, Mignotte, Siksek)**.** *The following hold:*

1. *For $p > 1237$, Equation (1) has no non-trivial solutions for $D = 2$ [Coh07, p. 520].*
2. *For $p \leq 10^6$, if (a, b) is a non-trivial solution of Equation (1) for $D = 2$, then – in the notation of Equation (18) – we have $r = \pm 1$ [Coh07, Proposition 15.7.1].*
3. *For $5 \leq p \leq 37$, Equation (1) has no non-trivial solutions for $D = 2$ [Coh07, Lemma 15.7.3].*

In the next subsections, we will derive similar results for $D = 3$ and 5. Since the details of the proof of part 1 of Theorem 3.9 do not seem to appear in print, we will derive a (much weaker) upper bound for p also for $D = 2$, sufficient to allow us to apply Theorem 3.9 (2). Specifically, in Section 3.1 we prove an analogue of Theorem 3.9 (1) for $D = 3, 5$ using linear forms in logarithms. In the next two sections, we first recall some facts about the theory of Frey curves, and then (Section 3.3) apply ideas from the modular method to extend Theorem 3.9 (2) to the cases $D = 3, 5$. In Section 3.4 we explain a variant of the same idea that avoids computations with modular forms, at the cost of slightly less precise results. In Section 3.5 we discuss a technique, based on continued fractions, to obtain good lower bounds on the size of non-trivial solutions (a, b) of Equation (1). Finally, in Proposition 3.18 we explain how to solve Equation (1) for a fixed (small) value of p, thus extending Theorem 3.9 (3) to $D = 3, 5$, in the slightly larger range $3 \leq p \leq 43$ (we solve the Thue equations in this range as an extra check, but we would only need $p \leq 23$).

We point out that – if we only wanted to solve Equation (1) for $D = 2$ – Lemma 3.8 and Theorem 3.9 would be more than sufficient, but we have decided to also treat $D = 3, 5$ to show that our method can handle Equation (1) in a certain generality. The rest of this section is therefore intended as a guide to the steps necessary to solve Equation (1) for any given value of D: one needs an upper bound for p (which can be obtained using linear forms in logarithms), some control over the parameter r of

Equation (18) (provided by the modular method), and a lower bound for b (which, as we shall see, can be obtained by Diophantine approximation techniques). We point out that the determination of the parameter r is useful to speed up later calculations, but not strictly necessary, especially if the bound for p is good enough. The material in this section is largely based on known ideas, but it still seems useful to collect all the details in one place and have statements that are adapted to the resolution of Equation (1).

3.1 A preliminary bound for p

We will need an absolute upper bound $p \le p_0$ on the exponent p for a non-trivial solution of Equation (1). It is well-known that linear forms in logarithms can be used to provide such a bound. In fact, Theorems 1 and 2 in [Bug97b] and the main result of [Bug97a] would give us an absolute upper bound for p, but one that is a bit too large for our purposes (especially for use in Section 3.3). We will instead prove the following estimate, which, while still quite weak, will be enough for us. We focus in particular on the cases $D \in \{2, 3, 5\}$, but, with a view towards future applications, we also obtain a reasonable upper bound for other squarefree values of $D > 0$.

Proposition 3.10. *Let $D = 2, 3$ or 5. Equation (1) has no non-trivial solution with $p > p_0(D)$, where*

$$p_0(D) = \begin{cases} 2.4 \cdot 10^4, & \text{if } D = 2 \\ 8.5 \cdot 10^4, & \text{if } D = 3 \\ 3.1 \cdot 10^4, & \text{if } D = 5. \end{cases}$$

For general squarefree $D > 0$ such that D is not a square modulo 8, Equation (1) has no solutions with $|b| > 1$ for $p > p_0(D) = \max\{h_D, 3950(\log \eta)^2 \cdot \log\left(1411(\log \eta)^2\right)^2\}$, where h_D is the class number of $\mathbb{Q}(\sqrt{D})$.

Remark 3.11. Note that $\log \eta$, being the regulator of $\mathbb{Q}(\sqrt{D})$, is $\ll D^{1/2+\varepsilon}$, and we also have $h_D \ll D^{1/2+\varepsilon}$. The value of $p_0(D)$ given in Proposition 3.10 is thus $\ll D^{1+\varepsilon}$, while the (more general) results of [Bug97b] give $p_0(D) \ll D^{2+\varepsilon}$ when $D = p$ is prime.

As recalled above, in the case $D = 2$, Bugeaud, Mignotte, and Siksek, in [Coh07, Chapter 15], give the bounds $p < 8200$ [Coh07, Proof of Proposition 15.7.1] and even $p < 1237$ [Coh07, p. 520], but – to the best of our knowledge – the details of the proofs have not appeared in print. Since we will only need a much looser upper bound for p, and also need it for $D = 3, 5$, we prefer to provide details on how to obtain this weaker bound to make the exposition as self-contained as possible. Before proving Proposition 3.10, we make the following elementary observation.

Lemma 3.12. *Let $D \in \{2, 3, 5\}$. For every non-trivial solution of Equation (1) with $p \ge 3$ we have $b \ge 11$. If $D = 2$, we even have $b \ge \exp(234)$.*

Proof. The case $D = 2$ is covered by Lemma 3.8, so assume $D \in \{3, 5\}$. Clearly there are no solutions of Equation (1) with $b \le -2$, because this would contradict $b^p + D = a^2 \ge 0$, and the solutions with $|b| \le 1$ are trivial by definition. Suppose then $b > 1$ and let q be a prime dividing b. Since $p \ge 3$, considering Equation (1) modulo q^3 we find $a^2 - D \equiv 0 \pmod{q^3}$, hence D is a square modulo q^3. Since neither 3 nor 5 are squares modulo $2^3, 3^3, 5^3$, or 7^3, we deduce $b \ge q \ge 11$. □

Proof of Proposition 3.10. We consider again the linear form in logarithms

$$\Lambda_\beta := 2r \log \beta_1 - p \log \beta_2 \tag{28}$$

and the inequality (25). We assume $0 \le r \le \frac{p-1}{2}$ and, if $r = 0$, $\log|\overline{\pi}| \ge \log|\pi|$, see Remark 3.3. We first treat the case $D \in \{2, 3, 5\}$. Lemma A.2 implies that β_1, β_2 are multiplicatively independent. We can therefore apply [Lau08, Corollary 1]. We set

$$d = [\mathbb{Q}(\beta_1, \beta_2) : \mathbb{R}(\beta_1, \beta_2)] = 2,$$

$$\log A_1 = \max\{h(\beta_1), |\log \beta_1|/2, 1/2\} \quad \text{and} \quad \log A_2 = \max\{h(\beta_2), |\log \beta_2|/2, 1/2\}.$$

By Lemma A.4 we have

$$\log A_1 = \begin{cases} \frac{1}{2}, \text{ for } D = 2, 5 \\ \frac{1}{2}\log\eta, \text{ for } D = 3. \end{cases}$$

As for $\log A_2$, note first that Lemma A.4 gives $h(\beta_2) = \log|\overline{\pi}|$. We claim that this realises the maximum. If $\log|\overline{\pi}| \leq 1/2$, then by Lemma A.3 we get $\log|\pi| \leq 1/2$, and Equation (20) implies $|b| \leq \exp(1)$, which contradicts Lemma 3.12. If $\log|\overline{\pi}| \leq \frac{1}{2}|\log\beta_2|$, then using $\log\beta_2 \geq 0$ (Lemma A.3) and $|b| = |\pi\overline{\pi}|$ (Equation (20)) we obtain

$$2\log|\overline{\pi}| \leq \log|\overline{\pi}| - \log|\pi| \iff \log|b| = \log|\overline{\pi}| + \log|\pi| \leq 0,$$

hence $|b| = 1$ and we again have a trivial solution. We further set

$$b' = \frac{2r}{d\log A_2} + \frac{p}{d\log A_1} \leq \frac{2r}{2\log|\overline{\pi}|} + p < \frac{3}{2}p,$$

where the last inequality follows immediately from $r \leq \frac{p-1}{2}$ together with $\log|\overline{\pi}| \geq \frac{1}{2}\log b$ (Lemma A.3) and $\log b \geq \log(11)$ (Lemma 3.12). We can then apply [Lau08, Corollary 1] with $m = 20$ and $C_1(m) = 25.2$ (see [Lau08, Table 1]): it gives

$$\log|\Lambda_\beta| \geq -25.2 \cdot 2^4 \cdot (\max\{\log b' + 0.21, 10\})^2 \cdot \log A_1 \cdot \log A_2.$$

We distinguish two cases: if the maximum in the above formula is 10, then $\log b' + 0.21 \leq 10$, hence

$$\frac{p}{\max\{1, \log\eta\}} \leq b' \leq \exp(10 - 0.21) \leq 1.8 \cdot 10^4 \Rightarrow p \leq 1.8 \cdot 10^4 \cdot \max\{1, \log\eta\} < p_0(D).$$

Otherwise, we obtain

$$\begin{aligned} \log|\Lambda_\beta| &\geq -25.2 \cdot 2^4 \cdot (\log b' + 0.21)^2 \cdot \log A_1 \cdot \log|\overline{\pi}| \\ &\geq -201.6 \cdot \max\{1, \log\eta\} \cdot \left(\log\left(\frac{3}{2}p\right) + 0.21\right)^2 \cdot \log|\overline{\pi}|. \end{aligned}$$

Comparing with Equation (25) we then obtain

$$-201.6 \cdot (\log p + 0.62)^2 \cdot \max\{1, \log\eta\} \cdot \log|\overline{\pi}| < \log|\Lambda_\beta| \leq -p(\log|\overline{\pi}| - \frac{1}{2}\log\eta) + \log(4\sqrt{D}),$$

that is,

$$p < \frac{\log(4\sqrt{D})}{\log|\overline{\pi}| - \frac{1}{2}\log\eta} + 201.6 \cdot (\log p + 0.62)^2 \cdot \max\{1, \log\eta\} \cdot \frac{\log|\overline{\pi}|}{\log|\overline{\pi}| - \frac{1}{2}\log\eta}.$$

Using the lower bound for $\log|\overline{\pi}|$ provided by Lemma 3.12, and plugging in the values of D and η, we immediately obtain the inequalities in the statement.

In the general case, we proceed similarly. Suppose first that $a \leq (4\eta+1)\sqrt{D}$. Then $|b^p| = |a^2 - D| \leq (16\eta^2+8\eta)D$, hence $p \leq \frac{\log|a^2-D|}{\log 2} \leq \frac{\log((16\eta^2+8\eta)D)}{\log 2}$. Since $\eta = \frac{u+v\sqrt{D}}{2} \geq \frac{1+\sqrt{D}}{2}$ (here u, v are positive), it is easy to see that $\frac{\log((16\eta^2+8\eta)D)}{\log 2}$ is much smaller than the bound given in the statement. We can then suppose $a > (4\eta+1)\sqrt{D}$.

Since D is not a square modulo 8, every solution of $a^2 - D = b^p$ has b odd, so Lemma 3.1 applies and we can repeat the discussion at the beginning of Section 3. The assumptions $p \nmid h_D$ (which follows from $p > p_0(D)$) and $a > (4\eta+1)\sqrt{D}$ then imply that inequality (25) holds. We consider again the linear form Λ_β and the numbers

$$\log A_1 = \max\{h(\beta_1), |\log\beta_1|/2, 1/2\} \quad \text{and} \quad \log A_2 = \max\{\log|\overline{\pi}|, |\log\beta_2|/2, 1/2\}.$$

By Lemma A.4 we have $\log|\overline{\pi}| \geq h(\beta_2)$ and $\log A_1 = \frac{1}{2}\max(1, \log\eta)$. As above, we can easily show $\log|\overline{\pi}| > \frac{1}{2}|\log\beta_2|$. Note that the assumption $a > (4\eta+1)\sqrt{D} \geq \sqrt{D+4} + 2$ implies that β_1, β_2 are multiplicatively independent (Lemma A.2) and also $b = (a^2 - D)^{1/p} \geq 4^{1/p} > 1$, hence $b \geq 2$.

Since $\log A_2 \geq \frac{1}{2}$,we have

$$b' = \frac{2r}{d \log A_2} + \frac{p}{d \log A_1} \leq p - 1 + \frac{p}{\max\{1, \eta\}} \leq 2p.$$

We apply [Lau08, Corollary 1] as above. If $\max\{\log b' + 0.21, 10\} = 10$, then exactly as before we obtain $p \leq 1.8 \cdot 10^4 \cdot \max\{1, \log \eta\} < p_0(D)$. Otherwise, comparing with Equation (25) we obtain

$$-201.6 \cdot (\log 2p + 0.21)^2 \cdot \max\{1, \log \eta\} \cdot \log |\overline{\pi}| < \log |\Lambda_\beta| \leq -p \left(\log |\overline{\pi}| - \frac{r}{p} \log \eta \right) + \log(4\sqrt{D}). \quad (29)$$

We distinguish two cases: if $\log |\overline{\pi}| \geq 2 \log \eta$, we have $\log |\overline{\pi}| - \frac{r}{p} \log \eta \geq \frac{3}{4} \log |\overline{\pi}|$, and dividing by $\log |\overline{\pi}| \geq 2 \log \eta$ the above inequality we get

$$-201.6 \cdot (\log 2p + 0.21)^2 \cdot \max\{1, \log \eta\} < -\frac{3}{4} p + \frac{\log(4\sqrt{D})}{2 \log \eta}. \quad (30)$$

Otherwise, suppose $\log |\overline{\pi}| < 2 \log \eta$. The equality $a^2 - D = b^p$ gives $a \geq \sqrt{b^p + D} \geq b^{p/2}$, and therefore (using (19), $a \geq 2\sqrt{D}$ and $b \geq 2$) we have

$$p \log |\overline{\pi}| - r \log \eta = \log \left(a - \sqrt{D} \right) \geq \log(a/2) = \log a - \log 2 \geq \frac{p}{2} \log b - \log 2 \geq \left(\frac{p}{2} - 1 \right) \log 2,$$

which implies $\log |\overline{\pi}| - \frac{r}{p} \log \eta \geq \left(\frac{1}{2} - \frac{1}{p} \right) \log 2$. Since we can assume $p > 10^4$ (otherwise, the upper bound in the statement is obviously satisfied), we get $\log |\overline{\pi}| - \frac{r}{p} \log \eta \geq 0.346$. Using this inequality and $\log |\overline{\pi}| < 2 \log \eta$ in Equation (29) we obtain

$$-201.6 \cdot (\log 2p + 0.21)^2 \cdot \max\{1, \log \eta\} < -\frac{0.346}{2 \log \eta} p + \frac{\log(4\sqrt{D})}{2 \log \eta}. \quad (31)$$

This inequality is weaker than (30), so in every case we get that Equation (31) is satisfied. Rearranging, we arrive at the inequality

$$p < 1165.4 \cdot (\log p + 0.91)^2 \cdot \max\{1, \log \eta\} \cdot \log \eta + 2.9 \log(4\sqrt{D}). \quad (32)$$

Since we can assume $p \geq 10^4$, we have $\log p + 0.91 \leq 1.1 \log p$. Moreover, it is easy to see that $\log \eta \leq 1$ only for $D = 2, 5$, which we have already treated, so we can also assume $\max\{1, \log \eta\} = \log \eta$. Moreover, since $\eta = \frac{u + \sqrt{D}}{2}$ with u, v positive integers, we have $\eta \geq \frac{1}{2}\sqrt{D}$, which also allows us to absorb $2.9 \log(4\sqrt{D}) \leq 2.9 \log(8\eta) < 0.1 (\log p)^2 \log \eta$ into the first term. Thus, we get the inequality

$$p < 1410.24 \cdot (\log \eta)^2 \cdot (\log p)^2. \quad (33)$$

Note that $\log \eta \geq \log \left(\frac{3 + \sqrt{13}}{2} \right)$, hence $1410.24 \cdot (\log \eta)^2 \geq 2000$. Lemma B.2, applied with $A = 1410.24 (\log \eta)^2$, yields $p < 2.8 \cdot 1410.24 (\log \eta)^2 \cdot \log \left(1410.24 (\log \eta)^2 \right)^2$, which concludes the proof. □

3.2 Frey curves

We briefly review some relevant theory of Frey curves, for use in the next section. Given a solution (a, b) of Equation (1) for a prime $p \geq 7$ and $D = 3$, we consider the following elliptic curve over $\mathbb{Q}$ (see [BS23a, Equation (69)], and [BS23a, §3] and [BS04] for general background on Frey curves for ternary diophantine equations of signature $(n, n, 2)$)

$$E : Y^2 = X^3 + 2aX^2 + DX. \quad (34)$$

Let N_E be the conductor of E. By [BS04, Lemma 2.1] (see also [BS23a, p. 1821]) we have $N_E = 2^5 \prod_{q | bD} q = 2^5 \operatorname{rad}(3b)$. By standard level-lowering arguments, the modulo-p representation attached to E arises from a weight 2 newform f of level $N := 2^5 \cdot D = 96$ and trivial Nebentypus ([BS04, Lemmas 3.2 and 3.3] and [BS23a, p. 1821]). The situation is very similar, though not identical, for

$D = 5$; the difference arises because of the different congruence class of D modulo 4. In this case, the Frey curve we take is (see [BS23a, Equation (70)])

$$E : Y^2 = X^3 + 2aX^2 + b^pX = X^3 + 2aX^2 + (a^2 - 5)X, \tag{35}$$

which – again by [BS04, Lemma 2.1] – has conductor $N_E = 2^5 \prod_{q|bD} q = 2^5 \operatorname{rad}(5b)$. The results of [BS04] show that the mod-p representation attached to E arises from a weight 2 eigenform f of level $N := 2^5 \cdot D = 160$. We will write $E \sim_p f$ to denote this fact. The implications of the property $E \sim_p f$ that we need are summarised in Proposition 3.13. Both in the case $D = 3$ and $D = 5$, write

$$f = q + \sum_{m=2}^{\infty} a_m(f) q^m$$

for the normalised q-expansion of the eigenform f introduced above and let $K_f = \mathbb{Q}(a_2(f), a_3(f), \ldots)$ be its Hecke eigenfield. The condition $E \sim_p f$ implies in particular the following (see [KO92], [Sik12] or [BS23a, Lemma 7.1]):

Proposition 3.13. *There is a prime $\mathfrak{p}$ of the ring of integers $\mathcal{O}_f$ of K_f, lying over p, such that the following holds. Let $\ell \neq p$ be a rational prime and denote by $a_\ell(E)$ the ℓ-th coefficient of the L-function of $E/\mathbb{Q}$.*

1. *If $\ell \nmid N_E N$, then $a_\ell(E) \equiv a_\ell(f) \pmod{\mathfrak{p}}$;*
2. *If $\ell \nmid N$ but $\ell \,||\, N_E$, then $\ell + 1 \equiv \pm a_\ell(f) \pmod{\mathfrak{p}}$.*

Furthermore, if $K_f = \mathbb{Q}$, then these properties also hold for $\ell = p$.

Remark 3.14. We note a consequence of part 2 of this proposition and the fact that $N_E = 2^5 \prod_{q|bD} q$: if ℓ is a prime different from $2, D$, and p, and $a_\ell(f) \not\equiv \pm(\ell + 1) \pmod{\mathfrak{p}}$, then $\ell \nmid N_E$, hence $\ell \nmid b$. If $K_f = \mathbb{Q}$, the same conclusion holds also for $\ell = p$.

From the LMFDB [LMF24], we find that there are two weight-2 normalised eigenforms at level 96 and four at level 160. The forms at level 160 form three Galois orbits. We give some information about these newform that we will need in what follows.

1. Level 96: let $F_1 = q - q^3 + 2q^5 + 4q^7 + \cdots$ be the form [LMF24, Newform orbit 96.2.a.a] and $F_2 = q + q^3 + 2q^5 - 4q^7 + \cdots$ be the form [LMF24, Newform orbit 96.2.a.b]. They are quadratic twists of each other, and they both have Hecke eigenfield equal to $\mathbb{Q}$, hence they correspond to (isogeny classes of) elliptic curves over $\mathbb{Q}$. We can take as representatives of the isogeny classes respectively the curves $y^2 = x^3 - x^2 - 32x - 60$ and its quadratic twist $y^2 = x^3 + x^2 - 32x + 60$.
2. Level 160: let $G_1 = q - 2q^3 - q^5 - 2q^7 + \cdots$ be the form [LMF24, Newform orbit 160.2.a.a], $G_2 = q + 2q^3 - q^5 + 2q^7 + \cdots$ be the form [LMF24, Newform orbit 160.2.a.b], and $G_3 = q + \beta q^3 + q^5 - \beta q^7 + \cdots$, where $\beta = 2\sqrt{2}$, be the form [LMF24, Newform orbit 160.2.a.c]. The forms G_1 and G_2 are quadratic twists of each other and have Hecke eigenfield equal to $\mathbb{Q}$, hence they correspond to (isogeny classes of) elliptic curves over $\mathbb{Q}$. We can take as representatives of the isogeny classes respectively the curves $y^2 = x^3 + x^2 - 6x + 4$ and its quadratic twist $y^2 = x^3 - x^2 - 6x - 4$. The form G_3 has Hecke eigenfield $\mathbb{Q}(\sqrt{2})$. One knows that GL_2-type varieties are modular (this follows from [Rib92], since Serre's conjecture is a theorem by work of Khare and Wintenberger [KW09a, KW09b]), hence one can show unconditionally that the L-function of the Jacobian of the genus-2 curve $y^2 = 2x^5 - 5x^4 - x^3 + 5x^2 + 2x$ [LMF24, Curve 25600.f.512000.1] agrees with the product of the L-functions of G_3 and of its Galois conjugate.

3.3 The value of r

We now explain how we can prove (computationally) that – for any non-trivial solution of Equation (1) for $D \in \{2, 3\}$ (resp. $D = 5$) – we have $r = \pm 1$ in Equation (18) (resp. $r = \pm 3$). For $D = 2$ this is the statement of [Coh07, Proposition 15.7.1]. For $D = 3, 5$ one can generalise the argument of that proposition; we give some details for completeness, and because the computation is slightly more involved for $D = 5$. Let $D = 3$ and let (a, b) be a solution of Equation (1), for some prime p. Suppose that the modulo p representation attached to the Frey curve of Equation (34) arises from the newform f. Note that, thanks to Proposition 3.10, we only have finitely many primes p to consider. We can therefore assume that p is fixed. Let $\ell > 2$ be a prime that satisfies all of the following conditions:

Condition 3.15. *1. $\ell = np + 1$ for some positive integer n;*

2. D is a square modulo ℓ, say $D \equiv \theta^2 \pmod{\ell}$;

3. $a_\ell(f) \not\equiv \pm(\ell + 1) \pmod{p}$;

4. $(2 + \theta)^n \not\equiv 1 \pmod{\ell}$.

Denote by $x \mapsto \overline{x}$ reduction modulo ℓ. Condition (3) implies that $\ell \nmid b$ (see Remark 3.14). Thus, b^p reduces modulo ℓ to a non-zero p-th power, which is in particular an n-th root of unity in $\mathbb{F}_\ell$. Let $\mu_n(\mathbb{F}_\ell) = \{\delta \in \mathbb{F}_\ell \mid \delta^n = 1\}$, so that $\overline{b}^p \in \mu_n(\mathbb{F}_\ell)$. Setting

$$\mathcal{X}'_\ell = \{\delta \in \mathbb{F}_\ell : \delta^2 - D \in \mu_n(\mathbb{F}_\ell)\}, \tag{36}$$

it is clear that $\overline{a}$ belongs to $\mathcal{X}'_\ell$. For $\delta \in \mathcal{X}'_\ell$ let E_δ be the elliptic curve over $\mathbb{F}_\ell$ with equation

$$E_\delta : Y^2 = X(X^2 + 2\delta X + D).$$

Further let

$$\mathcal{X}_\ell = \{\delta \in \mathcal{X}'_\ell \mid a_\ell(E_\delta) \equiv a_\ell(f) \pmod{p}\}.$$

By the fact that $E \sim_p f$, we have $a_\ell(E) \equiv a_\ell(f) \pmod{p}$ (see Proposition 3.13 (1)), hence $\overline{a}$ belongs to $\mathcal{X}_\ell$ (because for $\delta = \overline{a}$ we have $a_\ell(E_\delta) = a_\ell(E) \equiv a_\ell(f) \pmod{p}$). Finally, let $\mathfrak{l}$ be the prime $(\ell, \sqrt{D} - \vartheta)$ of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Reducing Equation (18) modulo $\mathfrak{l}$ we obtain

$$a + \theta \equiv \eta^r \pi^p \equiv (2 + \theta)^r \pi^p \pmod{\mathfrak{l}}.$$

Let $\Phi : \mathbb{F}_\ell^\times \to \mathbb{Z}/p\mathbb{Z}$ be the map obtained as the composition of the discrete logarithm $\mathbb{F}_\ell^\times \to \mathbb{Z}/(\ell-1)\mathbb{Z}$ (with respect to any fixed generator g of $\mathbb{F}_\ell^\times$) and of the natural projection $\mathbb{Z}/(\ell - 1)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Note that $\Phi(2 + \theta) \neq 0$, since otherwise $2 + \theta$ would be of the form g^{pk} for some k, and therefore $(2+\theta)^n \equiv g^{npk} \equiv 1 \pmod{\ell}$, contradicting assumption 4. Applying Φ to the identity $a+\theta \equiv (2 + \theta)^r \pi^p \pmod{\mathfrak{l}}$ we obtain

$$\Phi(a + \theta) \equiv r\Phi(2 + \theta) \pmod{p}.$$

This implies that

$$r \bmod p \in \left\{ \frac{\Phi(\delta + \theta)}{\Phi(2 + \theta)} : \delta \in \mathcal{X}_\ell \right\} =: \mathcal{R}_\ell(f).$$

Note that since $|r| < p/2$ the equality $r = \pm 1$ is equivalent to the congruence $r \equiv \pm 1 \pmod{p}$. Thus, if, for a fixed newform f, we find a collection of primes $\ell_1, \ldots, \ell_k$ satisfying the above assumptions and such that $\bigcap_{i=1}^k \mathcal{R}_{\ell_i}(f) \subseteq \{\pm 1\}$, then we have proved that for that specific f we can only have $r = \pm 1$. If we do this for all newforms f of weight 2 and level $2^5 \cdot 3$, then we have proven $r = \pm 1$. As we saw above, there are only two weight-2 newforms at level 96, and both have rational coefficients. A simple MAGMA script (which can be found in the repository associated with this paper) finds, for every $p \leq 10^5$ and every relevant newform of level $2^5 \cdot 3$, a collection of primes $\{\ell_j\}$ as above.

The same argument extends with trivial modifications also to $D = 5$: in this case, we replace $2 + \theta$ by $\frac{1+\theta}{2}$ (this plays the role of η), we use the Frey curve of Equation (35), and we obtain $r = \pm 3$.

Conceptually, this is all that is needed. However, computationally there is a small hiccup which we will now explain how to overcome. Specifically, the approach outlined above requires the ability to compute the coefficients $a_\ell(f)$ with reasonable efficiency. This is not completely straightforward, especially at level $2^5 \cdot 5$, where we also find the non-rational newform G_3 with Hecke eigenfield $\mathbb{Q}(\sqrt{2})$. In all cases, what we do is work with elliptic curves instead: if $f \in \{F_1, F_2, G_1, G_2\}$ is a *rational* newform, then by modularity we know that there is an associated elliptic curve $E_f/\mathbb{Q}$ that satisfies $a_\ell(f) = a_\ell(E_f)$. We have explicit representatives for these elliptic curves, given in Section 3.2. Since point-counting on elliptic curves over finite fields is very fast, this allows us to quickly compute $a_\ell(f)$ when f is a rational newform.

For the unique non-rational newform G_3, we consider the genus-2 curve $C/\mathbb{Q}$ with equation $y^2 = 2x^5 - 5x^4 - x^3 + 5x^2 + 2x$. As already explained, the L-function of $\operatorname{Jac} C$ agrees with the product of the L-functions of G_3 and of its Galois conjugate. Moreover, over the field $\mathbb{Q}(i)$, the Jacobian of C splits as the square of the $\mathbb{Q}$-curve $E_{G_3} : y^2 = x^3 + (i - 1)\,x^2 + (6i + 3)\,x - i + 5$ [LMF24, Elliptic curve 1600.2-b3]. As a consequence, for $\ell \equiv 1 \pmod{4}$ (that is, for the primes that split in $\mathbb{Q}(i)$), the

trace $a_\ell(G_3)$ is equal to the Frobenius trace of the reduction of E_{G_3} modulo $\mathfrak{l}$, where $\mathfrak{l}$ is any prime of $\mathbb{Z}[i]$ lying over ℓ (since E_{G_3} is a $\mathbb{Q}$-curve, hence it has the same L-function as its Galois conjugate, it does not matter which prime above ℓ we take). Note that this implies in particular $a_\ell(G_3) \in \mathbb{Z}$, so that the congruence $a_\ell(G_3) \equiv a_\ell(E_\delta) \pmod{\mathfrak{p}}$ of Proposition 3.13 (1) is actually a congruence modulo p (again when $\ell \equiv 1 \pmod 4$). Thus, for primes $\ell \equiv 1 \pmod 4$ we can again compute $a_\ell(G_3)$ by counting points on elliptic curves, which gives a much faster method than computing the coefficients of the modular form directly. In particular, for the unique irrational newform G_3, we limit ourselves to using primes ℓ that are congruent to 1 modulo 4.

The above discussion, together with the corresponding computation, shows:

Proposition 3.16. *Let (a, b) be a solution of Equation (1) for $D = 2$ or 3 (resp. $D = 5$) and for $11 \leq p < 10^5$. In the notation of Equation (18) we have $r = \pm 1$ (resp. $r = \pm 3$).*

Combining Remark 3.3, Proposition 3.10 and Proposition 3.16, we see that it suffices to solve Equation (1) under the further assumption that $r = 1$ or 3 in Equation (18):

Corollary 3.17. *Suppose that for some $D \in \{2, 3\}$ (resp. for $D = 5$) and some prime $p \geq 11$ Equation (1) admits a non-trivial solution. Then it also admits a non-trivial solution (for the same prime p and the same value of D) such that, in the notation of Equation (18), we have $r = 1$ (resp. $r = 3$).*

We also note that a direct computation allows us to handle the cases when p is sufficiently small (this takes care in particular of the cases $p < 11$ that are not covered by the previous corollary). We will only use the result of the next proposition for $p \leq 17$.

Proposition 3.18. *Equation (1) has no non-trivial solutions for $D \in \{2, 3, 5\}$ and $3 \leq p \leq 43$.*

Proof. As in Remark 3.6, each of the finitely many equations to be considered reduces to a Thue equation. These can easily be handled by GP's Thue equation solver. Note that, using Corollary 3.17, for a fixed value of D we only need to consider a single value of r, unless $p \leq 7$, in which case we test all $r \in \{0, \ldots, \frac{p-1}{2}\}$. □

3.4 The value of r: a variant without modular forms

In this section, we discuss a slightly different method to determine the value of r for given D and p. The procedure of the previous section is very effective, but it relies on the ability to quickly compute coefficients of modular forms. This has already caused some difficulties for $D = 5$, and one can only assume matters get worse for larger D. We now explain how we can obtain weaker, but still very useful, results using only arithmetic in finite fields.

Suppose that (a, b, p) is a solution of Equation (1) and use the notation of Equations (18) and (19). Write the fundamental unit of $\mathbb{Q}(\sqrt{D})$ as $\eta = \frac{u+v\sqrt{D}}{2}$, where u, v are integers (possibly both even).

Let ℓ be a prime that satisfies the following conditions (cf. Condition 3.15):

1. $\ell = np + 1$ for some positive integer n;
2. D is a square modulo ℓ, say $D \equiv \theta^2 \pmod{\ell}$;
3. $\ell \nmid 2D$;
4. $\left(\frac{u+v\theta}{2}\right)^n \not\equiv 1 \pmod{\ell}$.

Define $\mathcal{X}'_\ell$ as in Equation (36) and let Φ be the same map as in the previous section (discrete logarithm $\mathbb{F}_\ell^\times \to \mathbb{Z}/(\ell-1)\mathbb{Z}$ composed with the projection $\mathbb{Z}/(\ell-1)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$). We set by definition $\Phi(\eta) = \Phi\left(\frac{u+v\theta}{2}\right)$; note that by definition $\ell > 2$, so it makes sense to divide by 2 in $\mathbb{F}_\ell$. As in the previous section, assumption 4 implies that $\Phi(\eta) \not\equiv 0 \pmod p$. We point out that – having replaced Condition 3.15 (3) with the condition $\ell \nmid D$ – we no longer know that $\ell \nmid b$.

We claim that $r \bmod p$ belongs to the set

$$\left\{ \frac{\Phi(\delta + \theta)}{\Phi(\eta)} : \delta \in \mathcal{X}'_\ell \right\} \cup \left\{ \frac{\Phi(2\theta)}{\Phi(\eta)}, -\frac{\Phi(-2\theta)}{\Phi(\eta)} \right\}.$$

To see this, consider the prime $\mathfrak{l} = (\ell, \sqrt{D} - \theta)$ of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, write $\pi = \frac{c+d\sqrt{D}}{2}, \overline{\pi} = \frac{c-d\sqrt{D}}{2}$, and reduce Equations (18) and (19) modulo $\mathfrak{l}$. We obtain

$$a + \theta = \left(\frac{u + v\theta}{2}\right)^r \cdot \left(\frac{c + d\theta}{2}\right)^p, \quad a - \theta = \left(\frac{u - v\theta}{2}\right)^r \cdot \left(\frac{c - d\theta}{2}\right)^p.$$

We now distinguish two cases. If a is not congruent to θ, nor to $-\theta$, modulo ℓ, then we can apply Φ to the first equation to obtain (as in the previous section) $r \equiv \frac{\Phi(a+\theta)}{\Phi(\eta)} \bmod p$. Note that in this case we have $\ell \nmid a^2 - \theta^2 \equiv a^2 - D$, hence $\ell \nmid b$, and therefore we deduce that $a \in \mathcal{X}'_\ell$. On the other hand, if $a \equiv \theta \pmod{\ell}$, then we *cannot* have $a \equiv -\theta \pmod{\ell}$, for otherwise we would get $2\theta \equiv 0 \pmod{\ell}$ and hence $4D \equiv (2\theta)^2 \equiv 0 \pmod{\ell}$, which contradicts $\ell \nmid 2D$. Applying Φ to the equation $a + \theta = \left(\frac{u+v\theta}{2}\right)^r \cdot \left(\frac{c+d\theta}{2}\right)^p$ we then get $r \equiv \frac{\Phi(a+\theta)}{\Phi(\eta)} \equiv \frac{\Phi(2\theta)}{\Phi(\eta)} \pmod{p}$. The case $a \equiv -\theta \pmod{\ell}$ is completely analogous.

As in the previous section, given p we can then loop over a few primes ℓ that satisfy the above conditions. This restricts the list of exponents r that are possible for a given prime p.

Remark 3.19. Note that $\#\mathcal{X}'_\ell \leq 2n$ and that (for a given prime ℓ) the above procedure restricts the list of possible r to at most $2n + 2$ candidates. In practice, we expect to find a prime $\ell = np + 1$ with n not too large (in particular, much smaller than p, if p is large), so even after testing just the first prime ℓ that satisfies the conditions given above, we expect to have much fewer than $p - 1$ candidate values of r.

As we will see in Section 4.7, this procedure is less precise than that of the previous section, in the sense that (especially for small primes p) it tends to leave us with several possibilities for r. On the other hand, when p gets large, it seems to be equally effective as the approach of the previous section, with the advantage that it avoids computing coefficients of modular forms.

Remark 3.20. When Equation (1) does not have solutions for a certain p, the method of this section can often be used to prove this fact. For example, for $D = 6$, a relatively short computation with the above method shows that Equation (1) has no solutions for $59 < p < 1.5 \cdot 10^5$. By the method of Proposition 3.10, one can show that there are no solutions for $p > 1.5 \cdot 10^5$. Together, we get the excellent absolute upper bound $p \leq 59$ for solutions of Equation (1) with $D = 6$.

Remark 3.21. We could have used the technique in this section to prove a weaker version of Proposition 3.16: for example, for $D = 5$ we would get the result for all primes $p > 61$. This weaker version, apart from being less clean, would also make it much harder to solve the Thue equations that lead to Proposition 3.18. On the other hand, one can fruitfully combine the two approaches: use the algorithm in this section to (hopefully) determine the value of r when p is sufficiently large, and only use the more precise – but more computationally expensive – algorithm of Section 3.3 for the remaining small primes.

3.5 A lower bound for b via continued fractions

We now describe a way to obtain a good lower bound for b. The basic observation is that – by Remark 3.6 – the coefficients u, v in a basis representation $\pi = \frac{u+v\sqrt{D}}{2}$ are solutions of a Thue equation $F(u, v) = 2$. As is well known, this implies that (for u large enough) the fraction v/u is a convergent of the continued fraction of a root of the polynomial $F(1, x)$. By testing the first convergents of the continued fraction, one can show that any solution of the Thue equation must have u very large, and from this, it follows that b itself must be very large. We now make this observation quantitative.

As a preliminary observation, note that – for a fixed value of p – it is easy to test if b corresponds to a solution of Equation (1), even if b is very large: if we suspect that $b^p + D$ is not a square (which is usually the case), this can be shown by finding an auxiliary prime q such that $b^p + D$ is not a square in $\mathbb{F}_q$. Chebotarev's theorem tells us that the density of such primes q is $\frac{1}{2}$, so one can quickly rule out any given value of b (such that $b^p + D$ is not a square) with this technique. This is what we will mean when we say that we *test* a value of b.

Fix both a prime $p \geq 3$ and an exponent $r \in \{0, \ldots, \frac{p-1}{2}\}$ (in the sense of Equation (18)). By the method of the previous section, for every prime p we typically only have one value of r to consider (by Corollary 3.17, this is the case for $D \in \{2, 3, 5\}$), but in principle, one could also loop over all possible values of r for a given p. We explain how to use continued fractions to quickly compute a lower bound

for the values of b in a non-trivial solution of Equation (1) with exponent p and with the given value of r. We assume as usual $0 \le r \le \frac{p-1}{2}$ and $|\overline{\pi}| \ge |\pi|$ (Remark 3.3).

We start from Equation (21) and divide both sides by $\overline{\eta}^r \pi^p$ to obtain

$$\left(\frac{\eta}{\overline{\eta}}\right)^r - \left(\frac{\overline{\pi}}{\pi}\right)^p = \frac{2\sqrt{D}}{\overline{\eta}^r \pi^p}.$$

Thanks to Equation (20), the real numbers $\frac{\eta}{\overline{\eta}}$ and $\frac{\overline{\pi}}{\pi}$ have the same sign (equal to $\pm_D$), so we have

$$\left|\left|\frac{\eta}{\overline{\eta}}\right|^r - \left|\frac{\overline{\pi}}{\pi}\right|^p\right| = \frac{2\sqrt{D}}{|\overline{\eta}|^r |\pi|^p}.$$

Let $x := |\eta/\overline{\eta}|^{r/p} = \eta^{2r/p} \ge 1$ and $y := |\overline{\pi}/\pi| \ge 1$. Using the identity $x^p - y^p = (x-y)\sum_{i=0}^{p-1} x^i y^{p-1-i}$ and $x \ge 1, y \ge 1$ we obtain

$$\frac{2\sqrt{D}\eta^r}{|\pi|^p} = |x^p - y^p| = |x-y| \sum_{i=0}^{p-1} x^i y^{p-1-i} \ge p|x-y|.$$

Multiplying by $|\pi|$ and taking into account that the sign of $\pi\overline{\pi}$ is $(-1)^r$, we arrive at

$$|\pi x - (-1)^r \overline{\pi}| = ||\pi|x - |\overline{\pi}|| = ||\pi|x - |\pi|y| \le \frac{2\sqrt{D}\eta^r}{p|\pi|^{p-1}}. \tag{37}$$

We now write $\pi = \frac{u+v\sqrt{D}}{2}, \overline{\pi} = \frac{u-v\sqrt{D}}{2}$ with $u, v \in \mathbb{Z}$. Note that, with this notation, the equation we are trying to solve is

$$\eta^r \left(\frac{u+v\sqrt{D}}{2}\right)^p - \overline{\eta}^r \left(\frac{u-v\sqrt{D}}{2}\right)^p = 2\sqrt{D}. \tag{38}$$

We can then rewrite (37) as

$$|u(x-(-1)^r) + v\sqrt{D}(x+(-1)^r)| = |(u+v\sqrt{D})x - (-1)^r(u-v\sqrt{D})| \le \frac{4\sqrt{D}\eta^r}{p|\pi|^{p-1}}.$$

Dividing both sides by $|\sqrt{D}u(x+(-1)^r)|$ we obtain

$$\left|\frac{x-(-1)^r}{(x+(-1)^r)\sqrt{D}} + \frac{v}{u}\right| \le \frac{4\eta^r}{p|\pi|^{p-1}(x+(-1)^r)|u|}. \tag{39}$$

The idea is now that v/u is an excellent rational approximation of the real number $\tau := -\frac{x-(-1)^r}{(x+(-1)^r)\sqrt{D}}$, and therefore we expect $-v/u$ to be a convergent of the continued fraction of τ. To exploit this connection, we need to compare $|\pi|$ with $|u|$. We have

$$|u| = |\pi + \overline{\pi}| \le 2|\overline{\pi}| = 2y|\pi| \quad \text{and} \quad |v| = \frac{1}{\sqrt{D}}|\pi - \overline{\pi}| \le \frac{2}{\sqrt{D}}|\overline{\pi}| = \frac{2}{\sqrt{D}}y|\pi|. \tag{40}$$

We note for later use that we also have $|b| = |\pi\overline{\pi}| = |\overline{\pi}|^2/y \ge |u|^2/4y$. Using (40) in (39) we obtain

$$\left|\frac{x-(-1)^r}{(x+(-1)^r)\sqrt{D}} + \frac{v}{u}\right| \le \frac{4\eta^r(2y)^{p-1}}{p(x+(-1)^r)|u|^p}. \tag{41}$$

Before continuing, we observe that (at the cost of a short computation) we can obtain good bounds on y.

Lemma 3.22. *Let (a,b) be a solution of Equation (1) for some prime p. If $|b| > (4\sqrt{D})^{2/p}\eta$, then $y \le \eta^{2r/p} \cdot 2^{1/p} \le \eta \cdot 2^{1/p}$.*

Proof. Start again from Equation (21) and divide both sides by $\eta^r\overline{\pi}^p$. We get

$$(\pi/\overline{\pi})^p - (\overline{\eta}/\eta)^r = \frac{2\sqrt{D}}{\eta^r\overline{\pi}^p} \Rightarrow (\pi/\overline{\pi})^p = (\overline{\eta}/\eta)^r\left(1 + \frac{2\sqrt{D}}{\overline{\pi}^p\overline{\eta}^r}\right).$$

Since $|\overline{\pi}|^p > b^{p/2} > (4\sqrt{D})\eta^{p/2} \geq 2\cdot 2\sqrt{D}/|\overline{\eta}^r|$ (see Lemma A.3 for the inequality $|\overline{\pi}| \geq b^{1/2}$), in the above equality we have $\left|1 + \frac{2\sqrt{D}}{\overline{\pi}^p\overline{\eta}^r}\right| \geq \frac{1}{2}$, and therefore

$$|\pi/\overline{\pi}| \geq |\overline{\eta}/\eta|^{r/p}2^{-1/p} \Rightarrow y = |\pi/\overline{\pi}|^{-1} \leq \eta^{2r/p}2^{1/p} \leq \eta 2^{1/p}.$$

□

We can easily test all values of b with $|b| \leq \left(4\sqrt{D}\eta^r\right)^{2/p}$. As p is fixed, this is trivial, especially given that the upper bound $(4\sqrt{D}\eta^r)^{2/p}$ will usually be quite small (and when it is < 2, there is nothing to test). Also note that, if r is fixed and p tends to infinity, the upper bound in the lemma tends to 1, while $y \geq 1$ holds by assumption. Now we distinguish two complementary cases, depending on the size of the right-hand side of Equation (41):

1. We first assume $\frac{4\eta^r}{p|\pi|^{p-1}(x+(-1)^r)|u|} \geq \frac{1}{2|u|^2}$. Rearranging and using (40) we get

$$\frac{8\eta^r}{p|\pi|^{p-1}(x+(-1)^r)} \geq \frac{1}{|u|} \geq \frac{1}{2y|\pi|} \Rightarrow |\pi| \leq \left(\frac{16\eta^r y}{p(x+(-1)^r)}\right)^{1/(p-2)}.$$

   Using (40) again, this leads to $|b| = |\pi\overline{\pi}| = |\frac{u^2-Dv^2}{4}| \leq \frac{\max\{|u|^2,D|v|^2\}}{4} \leq \frac{\max\{4y^2|\pi|^2,4y^2|\pi|^2\}}{4} = y^2|\pi|^2$. Since we have upper bounds on both y and $|\pi|$, we have thus obtained an upper bound for b, and we can simply test all b up to this bound to see if they lead to solutions of Equation (1). In practice, this will be quite fast if D is not too large. Once these values of b have been tested, we can assume that we are in the next case.

2. We now assume the opposite inequality,

$$\frac{4\eta^r}{p|\pi|^{p-1}(x+(-1)^r)|u|} < \frac{1}{2|u|^2}: \tag{42}$$

   by Legendre's theorem on continued fractions, this inequality – together with (41) – implies that $\frac{v}{u}$ is a convergent of the continued fraction of τ. Let v_k/u_k be the sequence of convergents of τ. Note that if (u,v) is a solution of Equation (38), then $(u,v) \mid 2$, because we know from Lemma A.1 that $\pi = \frac{u+v\sqrt{D}}{2}, \overline{\pi} = \frac{u-v\sqrt{D}}{2}$ are relatively prime. Hence, writing the fraction v/u in reduced form as v'/u', we have either $(u,v) = (u',v')$ or $(u,v) = (2u',2v')$.

   For each pair (u_k,v_k), we can test whether $b = \frac{u_k^2-Dv_k^2}{4}$ or $b = \frac{(2u_k)^2-D(2v_k)^2}{4}$ is a solution to Equation (1). If we test the pairs $(u_1,v_1),\ldots,(u_n,v_n)$, we will have shown that all other solutions of Equation (38) that satisfy (42) have $|u| \geq |u_n|$. As remarked above, $|u| \geq |u_n|$ implies $|b| \geq |u|^2/4y \geq |u_n|^2/4y$, which – using the upper bound for y obtained above – gives an explicit lower bound for $|b|$.

Since the convergents of the continued fraction of τ grow exponentially fast, the above procedure gives a quick way to prove good lower bounds on b for fixed p. Combined with an absolute upper bound for p, this leads to a small list of solutions together with an absolute lower bound for b for the remaining solutions of Equation (1).

Applying this strategy for $D \in \{2,3,5\}$ and for all $5 \leq p \leq p_0(D)$ (see Proposition 3.10), we obtain:

Proposition 3.23. *Let $D \in \{2,3,5\}$, let $p \geq 5$, and let (a,b) be a non-trivial solution of Equation (1). We have $b > b_0 = \exp(400)$.*

Remark 3.24. We briefly discuss other possible strategies for obtaining lower bounds on b, which – as we will see in Section 4 – are quite important for the application of our method. First of all, suppose that we already know that the exponent p is bounded above by some $p_{\max}$: then we can simply *test*

all pairs (b,p) where $b \leq b_0$ and $p \leq p_{\max}$; all remaining solutions will have $b > b_0$. Of course, as b_0 grows, this approach quickly becomes impractical. Another possible technique is the argument in the proof of [Che12, Corollary 25], which is based on the modular method. Finally, the idea of [Coh07, Lemma 15.7.2] (which is similar to [BS23a, Lemma 15.3]) can often be used to show that b must grow with the exponent p.

4 Proof of Theorems 1.1 and 1.2

Suppose now that (a,b) is a non-trivial solution of (1) for some $D \in \{2,3\}$ (resp. $D = 5$). By Corollary 3.17 we may assume that $r = 1$ (resp. $r = 3$) in Equation (18), and by Proposition 3.18 we may also assume $p > 43$ (in fact, $p > 17$ will suffice). We aim to use Theorem 2.16 to find a good lower bound for the form Λ introduced in Notation 3.5. By Remark 3.4, we may assume that the inequality in (27) holds.

The next subsections are organised as follows. First of all, in Section 4.1 we fix the values of most parameters in Theorem 2.16 in terms of a single free variable, called $\tilde{K}$. Then, in Sections 4.2 and 4.3 we check that these parameters satisfy the hypotheses of Theorem 2.16. In Section 4.4 we estimate the size of various terms in inequality (17). This gives an easily testable criterion on $\tilde{K}$ that ensures that (17) is *not* satisfied. When this is the case, the first inequality in Theorem 2.16 holds, and this implies an upper bound for p. We work out this upper bound in Section 4.5. Finally, in Section 4.6 we apply this upper bound to show that Equation (1) has no solutions for $p > 17$. Combined with Proposition 3.18, this concludes the proof of Theorem 1.1. In Section 4.7 we then prove Theorem 1.2 by a similar method, and in Section 4.8 we highlight some strengths and weaknesses of our approach.

4.1 Choice of parameters

We could proceed analytically, estimating the optimal parameters for Theorem 2.16 in terms of the data, but – since we are dealing with a specific linear form in logarithms – it is both easier and more effective to apply Theorem 2.16 with fixed parameters. Specifically, we take the following values, where $\tilde{K} \geq 0.1$ will be fixed below.

1. $b_1 = kr = k$ or $3k$, where $k = 2^t$ for some $t \in \mathbb{N}$ (we take $t = 10$), $b_2 = p$, $\alpha_1 = \eta^{2/k}$, $\alpha_2 = \frac{|\overline{\pi}|}{|\pi|}$, $\delta = |\overline{\pi}|$ (note that $\delta = |\overline{\pi}|$ is an algebraic integer, and so is $\delta/\alpha_2 = |\pi|$);
2. $R_1 = 3$, $S_1 = 2$, $L = R_1 S_1$, $\mu = 1$ (hence $\sigma = 1$), $\rho = 35$;
3. $K = \lfloor \tilde{K} \cdot a_2 \rfloor$, $R_2 = \lceil \sqrt{\tilde{K} L / a_1} \cdot a_2 \rceil$, $S_2 = \lceil \sqrt{\tilde{K} L a_1} \rceil$.

Even though we have fixed some relations among these values, we will keep using the symbols R_1, R_2, S_1, etc., to keep the discussion more general. Notice in particular that these choices fix the value of the number a_1 appearing in the statement of Theorem 2.16. We also remark explicitly that with this choice of parameters the linear form Λ of Notation 2.1 is obviously the same as the form Λ of Notation 3.5.

We further assume to know that $a_2 = (\rho+1)\log\alpha_2 + 2\log|\overline{\pi}|$ is not too small. Specifically, we fix $a_{2,\min} \geq e$ and assume

$$\log|\overline{\pi}| \geq \frac{1}{2} a_{2,\min} \Rightarrow a_2 \geq a_{2,\min}. \tag{43}$$

The condition $a_{2,\min} \geq e$ ensures that the function $x \mapsto \frac{\log x}{x}$ is decreasing for $x \geq a_{2,\min}$. The bound $a_{2,\min}$ we will use is provided by Lemma A.3 and Proposition 3.23: together, these results imply $a_2 \geq \log 2|\overline{\pi}| \geq \log b \geq 400$. We will also choose $k = 2^t$ large enough that

$$a_1 = (\rho+1)\log\eta^{2/k} = \frac{2}{k}(\rho+1)\log\eta \leq 1. \tag{44}$$

This implies in particular $S_2 \leq R_2$ and $S \leq R$. It is also useful to introduce the parameter λ defined by the equality

$$K - 1 = \lfloor \tilde{K} a_2 \rfloor - 1 = \lambda \tilde{K} a_2.$$

As a_2 (hence K) tends to infinity, λ obviously tends to 1, and we always have $\lambda = \frac{\lfloor \tilde{K} a_2 \rfloor - 1}{\tilde{K} a_2} \geq \frac{\tilde{K} a_2 - 2}{\tilde{K} a_2} \geq 1 - \frac{2}{\tilde{K} a_{2,\min}}$.

Remark 4.1. The definitions imply

$$K - 1 = \lambda \tilde{K} a_2,$$

$$R = R_1 + R_2 - 1 \leq R_1 + \sqrt{\tilde{K} L / a_1}\, a_2 \leq \left(\sqrt{\tilde{K} L / a_1} + \frac{R_1}{a_{2,\min}} \right) a_2,$$

$$S = S_1 + S_2 - 1 \leq \sqrt{\tilde{K} L a_1} + S_1.$$

4.2 Checking Condition 2.3

It is clear that $\alpha_1 = \eta^{2/k}$ is an algebraic unit, because $\alpha_1^k = \eta^2$ is an algebraic unit by definition. The following lemma implies parts (2) and (3) of Condition 2.3:

Lemma 4.2. *Let (a, b) be a non-trivial solution of Equation (1) and assume that in the notation of Equation (18) we have $0 \leq r \leq \frac{p-1}{2}$ and $\log|\overline{\pi}| \leq \log|\pi|$ (see Remark 3.3). The following hold.*

1. *The quantities $|\log|\tau(\alpha_i)||$ for $i = 1, 2$ are independent of the embedding $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$ (this is Condition 2.3 (3));*
2. *For suitable determinations of the various logarithms, the quantity*

$$|b_2 \log \tau(\alpha_2) - b_1 \log \tau(\alpha_1)|$$

   is independent of the embedding $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$ (this is Condition 2.3 (2));
3. *$|\log|\tau(\overline{\pi})|| \leq \log|\overline{\pi}|$ for all $\tau : \mathbb{Q}(\alpha_1, \alpha_2) \hookrightarrow \mathbb{C}$.*

Proof. By definition, $\alpha_1^k = \eta^2$, so α_1 is a root of the polynomial

$$\left(x^k - \eta^2\right)\left(x^k - \overline{\eta}^2\right) \in \mathbb{Q}[x].$$

Since $\overline{\eta} = \pm_D \eta^{-1}$, the conjugates of α_1 over $\mathbb{Q}$ are contained in the set

$$\left\{ \eta^{2/k} \zeta_k^j, (\pm_D \eta)^{-2/k} \zeta_k^j = \eta^{-2/k} \zeta' \zeta_k^j = \eta^{-2/k} \zeta_k^j : j = 0, \ldots, k-1 \right\},$$

where ζ' is a root of unity such that $(\zeta')^{k/2} = \pm_D 1$. Notice that ζ' has multiplicative order dividing k, hence it can be reabsorbed in the factor ζ_k^j. Thus, $|\log|\tau(\alpha_1)|| = |\log \eta^{\pm 2/k}| = \left|\pm \frac{2}{k} \log \eta\right| = \frac{2}{k} \log \eta$ is independent of τ. Similarly, the absolute value of the only conjugate of $\alpha_2 = |\overline{\pi}|/|\pi|$ is $|\alpha_2|^{-1} = |\pi|/|\overline{\pi}|$, so the absolute value of $\log|\tau(\alpha_2)|$ is independent of τ. This proves part 1.

For part 2, notice that $\tau(\alpha_1)$ is of the form $\eta^{2/k} \zeta_k^j$ for some j if and only if $\tau(\alpha_2) = \alpha_2$ (to see this, raise to the k-th power), and $\tau(\alpha_1)$ is of the form $\eta^{-2/k} \zeta_k^j$ for some j if and only if $|\tau(\alpha_2)| = |1/\alpha_2|$. We discuss only the first case, the second being completely analogous. The logarithms of $\eta^{2/k} \zeta_k^j$ are $\frac{2}{k} \log_{\mathbb{R}}(\eta) + \frac{2\pi i}{k} j + 2\pi i k_1$ for $k_1 \in \mathbb{Z}$. The logarithms of α_2 are $\log_{\mathbb{R}}(\alpha_2) + 2\pi i k_2$ for $k_2 \in \mathbb{Z}$, where in both cases $\log_{\mathbb{R}}$ denotes the real logarithm of a positive real number. For these determinations,

$$\begin{aligned}
\Lambda_\tau &= b_2 \log(\alpha_2) - b_1 \log\left(\eta^{2/k} \zeta_k^j\right) \\
&= b_2 \log_{\mathbb{R}}(\alpha_2) + b_2 \cdot 2\pi i k_2 - b_1 \left(\frac{2}{k} \log_{\mathbb{R}}(\eta) + \frac{2\pi i}{k} j + 2\pi i k_1 \right) \\
&= b_2 \log_{\mathbb{R}}(\alpha_2) - 2r \log_{\mathbb{R}}(\eta) + 2\pi i \left(k_2 b_2 - rj - k_1 b_1\right) \\
&= \Lambda + 2\pi i \left(k_2 b_2 - rj - k_1 b_1\right).
\end{aligned}$$

Since $b_2 = p$ and $b_1 = kr = 2^t r$ are relatively prime (recall that $|r| \leq \frac{p-1}{2}$ and p is odd), Bézout's identity allows us to find integers k_1, k_2 such that $k_2 b_2 - k_1 b_1 = rj$. For these values of k_1, k_2 (that is, for the corresponding determinations of the logarithms), the above calculation shows $\Lambda_\tau = \Lambda$, as desired. A completely analogous calculation shows that when $\tau(\sqrt{D}) = -\sqrt{D}$ we can find determinations for which $\Lambda_\tau = -\Lambda$.

Finally, the only conjugates of $\overline{\pi}$ over $\mathbb{Q}$ are π and $\overline{\pi}$ itself. By the assumptions and Lemma A.3 we have $|\overline{\pi}| > |\pi|$, and the claim follows. □

4.3 Checking Condition 2.5

We check that our parameters satisfy Condition 2.5.

1. We know from Lemma A.2 that α_1, α_2 are multiplicatively independent. We then obtain
$$\#\{\alpha_1^r \alpha_2^s : 0 \le r < R_1, 0 \le s < S_1\} = R_1 S_1 = L,$$
so that (2) is satisfied.

2. We now have to show that
$$\#\{rb_2 + sb_1 : 0 \le r < R_2, 0 \le s < S_2\} \ge (K-1)L.$$
We prove this under the assumption
$$S_2 < p; \tag{45}$$
if (45) is not satisfied, we get a good upper bound $p \le S_2$. On the other hand, if (45) holds, then the numbers $pr + b_1 s$ are all distinct because $pr_1 + b_1 s_1 = pr_2 + b_1 s_2$ implies $s_1 = s_2$ by considering the equality modulo p (we find $b_1 s_1 \equiv b_1 s_2 \pmod p$; since p is coprime to $b_1 = kr = 2^t$ or $2^t \cdot 3$, this implies $s_1 \equiv s_2 \pmod p$. Given that $|s_1 - s_2| < S_2 < p$, we finally conclude $s_1 = s_2$). Hence the cardinality of the above set is
$$R_2 S_2 \ge \left(\sqrt{\frac{\tilde{K}L}{a_1}} a_2\right) \cdot \left(\sqrt{\tilde{K} L a_1}\right) = L \cdot \tilde{K} a_2 > L \cdot (K-1).$$

4.4 Estimating the terms in (17)

With the above choice of parameters we have the following estimates for the various terms in (17):

1. We give an upper bound for $\log \gamma$. By definition we have
$$\log \gamma = \log\left(\frac{(R-1)b_2 + (S-1)b_1}{2}\right) - \frac{2}{K^2-K} \log\left(\prod_{k=1}^{K-1} k!\right).$$
By [LMN95, p. 307] we have the inequality
$$-\frac{2}{K^2-K} \log\left(\prod_{k=1}^{K-1} k!\right) \le -\log(K-1) + \frac{3}{2} - \frac{\log\left(2\pi(K-1)/\sqrt{e}\right)}{K-1} + \frac{\log K}{6K(K-1)},$$
and it is easy to see that the sum of the last two terms is negative. We then have
$$\begin{aligned}\log \gamma &\le \log\left(\frac{(R-1)b_2 + (S-1)b_1}{2}\right) - \log(K-1) + \frac{3}{2} = \frac{3}{2} + \log\left(\frac{(R-1)p + (S-1)b_1}{2(K-1)}\right) \\ &= \frac{3}{2} + \log\left(\frac{(R-1) + (S-1)(rk/p)}{2(K-1)} \cdot p\right).\end{aligned}$$
Recall that $r = 1$ or 3 (Corollary 3.17). Using Remark 4.1, we obtain
$$(K-1)\log\gamma \le \left(\frac{3}{2} + \log\left(\frac{\sqrt{\tilde{K}L/a_1} + R_1/a_{2,\min} + (S-1)/(pa_{2,\min}) \cdot rk}{\lambda \tilde{K}} \cdot \frac{p}{2}\right)\right) \tilde{K} \cdot a_2.$$
Remark 4.3. Note that, even if we didn't know that r is fixed, the ratio r/p would still be bounded by $1/2$. This gives a weaker, but still useful, bound.

2. By the inequalities in Remark 4.1 we have
$$\begin{aligned}Ra_1 + Sa_2 &\le \left(\sqrt{\tilde{K}L/a_1} + \frac{R_1}{a_{2,\min}}\right) a_1 a_2 + \left(\sqrt{\tilde{K} L a_1} + S_1\right) a_2 \\ &= \left(2\sqrt{\tilde{K} L a_1} + \frac{R_1 a_1}{a_{2,\min}} + S_1\right) a_2.\end{aligned}$$
One could also give precise bounds on the factor g, but it will be enough to observe that by definition $g < \frac{1}{4}$.

To simplify the next inequality we use our explicit lower bound for $a_{2,\min}$: combining Lemma A.3 and Proposition 3.23 we know that in all cases $a_2 \geq a_{2,\min} \geq 400$, hence $K \geq \tilde{K}a_2 - 1 > 0.1a_2 - 1 > 6$. We can then use Lemma B.1 to estimate

$$h(N) \leq 2 \cdot 1.41 \log N \leq 3 \log(\tilde{K}La_2) = \frac{3\log(\tilde{K}L) + 3\log(a_2)}{a_2} a_2 \leq \frac{3\log(\tilde{K}L) + 3\log(a_{2,\min})}{a_{2,\min}} a_2.$$

Putting everything together, we see that, if $p_{\min} \leq p \leq p_0$, the right-hand side of (17) is at most $g(\tilde{K}, p_0) \cdot a_2$, where

$$\begin{aligned} g(\tilde{K}, p_0) = \frac{3\log(\tilde{K}L)}{a_{2,\min}} + \frac{3\log a_{2,\min}}{a_{2,\min}} + \frac{1}{4}L\left(2\sqrt{\tilde{K}La_1} + \frac{R_1}{a_{2,\min}}a_1 + S_1\right) \\ + \log\left(e^{3/2} \cdot \frac{\sqrt{\tilde{K}L/a_1} + R_1/a_{2,\min} + (S-1)/(p_{\min}a_{2,\min}) \cdot rk}{\lambda\tilde{K}} \cdot \frac{p_0}{2}\right)\tilde{K}. \end{aligned} \tag{46}$$

On the other hand, it is clear that the left-hand side of (17) is at least $f(\tilde{K}) \cdot a_2$, where

$$f(\tilde{K}) = \lambda\tilde{K} \cdot (L-1) \cdot \log(\rho). \tag{47}$$

In particular, if $f(\tilde{K}) > g(\tilde{K}, p_0)$, then the inequality in the second case of Theorem 2.16 does not hold, and thus we obtain the lower bound in case 1 of this theorem. In the next section we compute this lower bound more explicitly.

4.5 Applying Theorem 2.16

We have now checked that our choice of parameters satisfies all the assumptions of Theorem 2.16 and we have estimated the various summands in Equation (17). We obtain the following corollary:

Corollary 4.4. *Let $f(\tilde{K})$ and $g(\tilde{K}, p_0)$ be as in Equations (47) and (46). Fix p_0. Suppose that Equation (1) admits a non-trivial solution with $p \geq p_{\min}$ and $p \leq p_0$. Suppose that $\tilde{K}$ satisfies $f(\tilde{K}) > g(\tilde{K}, p_0)$. Assume in addition that the following inequalities hold:*

1. $L(\sqrt{\tilde{K}L/a_1} + \frac{R_1}{a_{2,\min}}) < 2b_1 < 10^{10}$;
2. $LS \leq 2pa_{2,\min}$.

Then we have

$$p \leq \max\left\{\lceil\sqrt{\tilde{K}L(\rho+1) \cdot \frac{2}{k}\log\eta}\rceil,\ 2L\tilde{K}\log\rho + 2\delta\right\},$$

where, using the notation $c_2(D)$ of Lemma A.6, we have set

$$\delta := \frac{\log(4\sqrt{D}\eta^r)}{a_{2,\min}} + \frac{c_2(D)(\rho+1)}{2a_{2,\min}} + 10^{-1000} + \frac{\log a_{2,\min}}{a_{2,\min}}.$$

Remark 4.5. The additional assumptions 1-2 are only included to obtain a simpler bound, but they are somewhat arbitrary. In any case, they will be largely met by our final choice of parameters.

Proof. From the analysis in the previous section, it follows that either the inequality (45) is not satisfied, that is,

$$p \leq S_2 = \lceil\sqrt{\tilde{K}La_1}\rceil = \lceil\sqrt{\tilde{K}L(\rho+1) \cdot \frac{2}{k}\log\eta}\rceil$$

or all assumptions of Theorem 2.16 hold. Moreover, the first inequality in Theorem 2.16 holds, because the assumption $f(\tilde{K}) > g(\tilde{K}, p_0)$ implies that the inequality in case (2) of Theorem 2.16 does *not* hold. Applying the theorem we then obtain

$$\log|\Lambda'| \geq -\mu N \log\rho = -LK\log\rho \geq -L\tilde{K}\log\rho \cdot a_2, \tag{48}$$

where (see (15))

$$\Lambda' = \Lambda \max\left\{\frac{LSe^{LS|\Lambda|/2b_2}}{2b_2}, \frac{LRe^{LR|\Lambda|/2b_1}}{2b_1}\right\}.$$

The correction term given by the maximum in this formula is very small: we estimate it as follows. For the exponential part, we have

$$\log\max\left\{e^{LS|\Lambda|/2b_2}, e^{LR|\Lambda|/2b_1}\right\} \leq LR|\Lambda| < 10^{-1000}a_2,$$

where we have used $S \leq R$ (which follows from Equation (44)), $LR < 10^4 a_2$ (see Remark 4.1 and use assumption 1) and $|\Lambda| < 10^{-1010}$ (see Lemma A.5). For the rest, we simply write

$$\log\max\{\frac{LS}{2b_2}, \frac{LR}{2b_1}\} \leq \log a_2 + \log\max\left\{\frac{LS}{2pa_2}, \frac{L\left(\sqrt{\tilde{K}L/a_1} + R_1/a_{2,\min}\right)}{2b_1}\right\} \leq \log a_2,$$

where we have used the assumptions in the statement. From Equation (27) we know that

$$\log|\Lambda| \leq \log(4\sqrt{D}\eta^r) - p\log|\overline{\pi}| = \log(4\sqrt{D}\eta^r) - p\frac{a_2 - (\rho+1)\log\alpha_2}{2}.$$

Further using $\log(\alpha_2) < \frac{c_2(D)}{p} = \frac{c_2(D)}{pa_2}a_2 \leq \frac{c_2(D)}{a_{2,\min}p}a_2$ (Lemma A.6), we arrive at

$$\begin{aligned}\log|\Lambda'| &\leq \log(4\sqrt{D}\eta^r) - p\frac{a_2 - (\rho+1)\log\alpha_2}{2} + 10^{-1000}a_2 + \log a_2 \\ &\leq \log(4\sqrt{D}\eta^r) - \frac{p}{2}a_2 + \frac{\rho+1}{2}p\cdot\frac{c_2(D)}{pa_{2,\min}}a_2 + 10^{-1000}a_2 + \log a_2 \\ &\leq -\left(\frac{p}{2} - \frac{\log(4\sqrt{D}\eta^r)}{a_{2,\min}} - \frac{c_2(D)(\rho+1)}{2a_{2,\min}} - 10^{-1000} - \frac{\log a_{2,\min}}{a_{2,\min}}\right)a_2.\end{aligned} \tag{49}$$

Combining Equations (48) and (49) we obtain

$$(-\frac{p}{2} + \delta)a_2 \geq -L\tilde{K}\log\rho\cdot a_2,$$

hence

$$p \leq 2\left(L\tilde{K}\log\rho + \delta\right),$$

as desired. □

4.6 Conclusion of the proof of Theorem 1.1

Fix $D \in \{2,3,5\}$. From Proposition 3.10 we know that Equation (1) has no non-trivial solutions for $p > p_0 = 10^5$, so we can assume $p \leq p_0$. We find a $\tilde{K}_0$ such that $f(\tilde{K}_0) > g(\tilde{K}_0, p_0)$ and all conditions of Corollary 4.4 are satisfied. This gives us a new bound $p \leq p_1$ (notice that p is an integer, so we can take the floor of the bound in Corollary 4.4). If this bound is smaller than p_0, we can iterate this procedure, obtaining sharper and sharper estimates on p. We denote by $p_0, p_1, \ldots$ the successive upper bounds obtained in this way. Tables 1 to 3 give the result of this procedure for $D = 2, 3, 5$, starting from $p < p_0 = 10^5$, and assuming $p > 17$ (so $p \geq 19$: we take $p_{\min} = 19$). For the third and fourth columns, we give four significant digits, which in each case are enough to check the inequality $f(\tilde{K}) > g(\tilde{K}, p_i)$. Note that all the values of $\tilde{K}_i$ employed in the reduction process are ≥ 0.1.

From the last line of each table, we obtain $p \leq 17$. Since we had assumed from the beginning that $p > 17$, we have reached a contradiction. This proves that Equation (1) does not have any non-trivial solutions for $p > 17$, hence for any $p \geq 3$ since the cases $3 \leq p \leq 17$ are taken care of by Proposition 3.18. This concludes the proof of Theorem 1.1.

i	p_i	$\tilde{K}_i$	$f(\tilde{K}_i)$	$g(\tilde{K}_i, p_i)$	p_{i+1}
0	10^5	1.623	28.77	28.73	69
1	69	0.4365	7.670	7.655	18
2	18	0.3797	6.661	6.649	16

Table 1: Reduction process for $D = 2$

i	p_i	$\tilde{K}_i$	$f(\tilde{K}_i)$	$g(\tilde{K}_i, p_i)$	p_{i+1}
0	10^5	1.689	29.94	29.89	72
1	72	0.4587	8.065	8.053	19
2	19	0.3991	7.005	6.994	17

Table 2: Reduction process for $D = 3$

i	p_i	$\tilde{K}_i$	$f(\tilde{K}_i)$	$g(\tilde{K}_i, p_i)$	p_{i+1}
0	10^5	1.591	28.20	28.16	68
1	68	0.4153	7.293	7.292	17
2	17	0.3613	6.333	6.321	15

Table 3: Reduction process for $D = 5$

4.7 Solving Equation (1) for $D = 37$

In this section, we quickly prove Theorem 1.2. We do not give many details, because the arguments are simple variants of those already presented in detail for $D = 2, 3, 5$. We do point out, however, that the calculations required are somewhat more extensive than those for $D \in \{2, 3, 5\}$, and the intermediate results are slightly less clean: for example, we only get an analogue of Proposition 3.16 for $p > 157$. Nevertheless, the total computation time is of the order of ten minutes on an ordinary laptop.

For this section, set $D = 37$. The fundamental unit of $\mathbb{Q}(\sqrt{D})$ is $\eta = 6 + \sqrt{D}$ and the class number h_{37} is 1. By Proposition 3.10, Equation (1) has no solutions for $p > p_0 := 2.1 \cdot 10^6$. Note that in every solution of Equation (1) with $p \geq 3$ the variable b is odd, because 37 is not a square modulo 8. By testing directly all pairs (b, p) with odd $b \leq 200$ and $p \leq p_0$, we find the small solutions $(a, b, p) = (8, 3, 3), (3788, 27, 5)$. We can then assume $b \geq 201$; by a computation very similar to the proof of Proposition 3.10 for $D \in \{2, 3, 5\}$, using this lower bound we find $p < 1.5 \cdot 10^5$ (we omit the details).

By the procedure explained in Section 3.4, we find that, for all p with $157 < p < 1.5 \cdot 10^5$, we must have $r \in \{\pm 1\}$. We can then apply the technique of Section 3.5, where we consider all pairs $(r, p) = (1, p)$ for $p \in (157, 1.5 \cdot 10^5)$, as well as all pairs (r, p) with $p \leq 157$ and $0 \leq r \leq \frac{p-1}{2}$. The outcome is that, for $p \geq 7$, all non-trivial solutions of Equation (1) satisfy $b \geq \exp(400)$. Applying the reduction process of Section 4.6 (with the same parameters) we then get $p \leq 17$. We note that we use Remark 4.3, as well as the estimate $|r| \leq 59$ that comes from our previous examination of the possible values of r.

There only remains to consider the Thue equations of Remark 3.6 for $p \leq 17$ and $r \in \{0, \ldots, \frac{p-1}{2}\}$. Thanks to the previous results, we can even avoid testing certain values of r. Solving these Thue equations explicitly, we find one more non-trivial solution, namely $(\pm 3788)^2 = (3^5)^3 + 37$. This concludes the proof of Theorem 1.2.

4.8 Final comments

We conclude with a few remarks.

1. The computations necessary to obtain Tables 1 to 3 are completely straightforward and can be checked with a pocket calculator. In general, the final reduction process is simple enough that it can almost be carried out by hand.

2. The reduction process converges very quickly, and the size of the initial upper bound has very little effect on it: for $D = 2, 3, 5$, if we start with the much weaker upper bound $p_0 \leq 10^6$, the p_i converge to the same estimates in the same number of steps. The other side of the coin is that

iteration beyond a few steps does not lead to any further improvement of the upper bound p_i (in particular, the values given in the tables are stable: further applications of Corollary 4.4 yield $p_{i+1} = p_i$).

3. There are two reasons why having a larger value of $a_{2,\min}$ helps in obtaining better estimates. The first is that this parameter appears as a denominator in many error terms (see Corollary 4.4), which therefore go to zero as $a_{2,\min} \to \infty$. The other reason is that if $a_{2,\min}$ is very large, one can take h to be large (see Equation (46), which involves the ratio $h/a_{2,\min}$), and as a consequence, we can also take a large value of ρ while ensuring $a_1 \leq 1$. In general, larger values of ρ lead to better upper bounds. More precisely: in the limit where $a_{2,\min}, k = 2^t$ and ρ all go to infinity, with $\frac{1}{2} \leq a_1 \leq 1$ and $a_{2,\min}$ being much larger than any other parameter in play, one can check that asymptotically the optimal value of $\tilde{K}$ is $\frac{9}{10 \log \rho}$, which leads to an upper bound $p \lesssim 2 \cdot 6 \cdot \frac{9}{10 \log \rho} \cdot \log \rho < 12$.

4. It seems that the main obstacle to generalising the arguments in this paper to larger values of $D > 0$ lies in extending Propositions 3.23 and 3.16. The two are closely connected: the computation necessary for Proposition 3.23 is much faster if one has a result analogous to Proposition 3.16. We have explained in Section 3.4 how to obtain results similar to Proposition 3.16 while avoiding computations with modular forms. However, there is no guarantee that this procedure will uniquely determine r (up to sign) for all values of p. In fact, it seems typical that for intermediate p – say, p up to a few hundred – we are unable to pin down the value of r using this method (this seems less of a problem if we also take into account the restrictions imposed by modular forms, which is why we included the discussion of Section 3.3). If the value of r cannot be determined, the resolution of the relevant Thue equations can become quite slow, both because the number of Thue equations to solve increases, and especially because the size of their coefficients grows rapidly with r. For example, we almost ran into this problem for $D = 37$. To check the result, we wanted to extend the resolution of the Thue equations a bit beyond our upper bound of 17. However, by the method of Section 3.4 we were unable to rule out the pair $p = 19, r = 8$, and the GP algebra system could not solve the corresponding Thue equation within a few hours, so we gave up on the computation. We note that we could not solve the Thue equation even after reducing the binary form using MAGMA's MinRedBinaryForm.

5. Finally, we discuss the situation for squarefree values of D that are squares modulo 8 (that is, $D \equiv 1 \pmod 8$). Nothing changes if we assume that b is odd: in this case, Lemma 3.1 applies, and the whole discussion of Section 3 can be repeated verbatim. Otherwise, the factors $a \pm \sqrt{D}$ have divisors that are primes of $\mathcal{O}_{\sqrt{D}}$ lying above 2, and are no longer relatively prime. In particular, $a \pm \sqrt{D}$ need not be p-th powers, even as ideals (an example is given by $a = 7, D = 17$, which corresponds to the solution $7^2 - 17 = 2^5$ of Equation (1) with $D = 17$). One is then naturally led to consider linear forms in *three* logarithms, so it seems that for $D \equiv 1 \pmod 8$ and $b \equiv 0 \pmod 2$ the situation is genuinely more complicated.

   On the other hand, trying to extend our technique to cover this situation may not be the right approach. The modular method can often handle ternary diophantine equations without solutions, and – when D is fixed – we expect infinite sequences of solutions of Equation (1) only for $b = \pm 1$ (or, in the exceptional case when D is a square, $b = 0$; but the situation is quite different when D is a square, so we will not focus on this case). The values $b = \pm 1$ are odd, and can therefore be treated with our method. The hope is then to use the modular method to deal with the complementary case when b is an even number. For example, Equation (1) for $D = 17$ can probably be solved by a combination of the techniques of this paper and [BS23a]: see the comments after [BS23a, Theorem 2], where it is (implicitly) claimed that the case $D = 17$ and b even can be treated with the methods of that paper. As already explained, we can handle the case where b is odd (specifically, with calculations almost identical to those of Section 4.7 we can prove that every solution of $a^2 - 17 = b^p$ with b odd and $p \geq 3$ is either trivial or $(a, b, p) = (282, 43, 3)$), so it seems likely that the resolution of Equation (1) for $D = 17$ is well within reach.

A Basic properties of solutions of Equation (1)

To avoid cluttering the main discussion, we collect here some numerical estimates and other basic facts about solutions of Equation (1). The results in this section are all elementary.

Lemma A.1. *Let $D \in \{2,3,5\}$ and let $\pi, \overline{\pi}$ be as in Equations (18) and (19). The algebraic numbers $\pi, \overline{\pi}$ are relatively prime in the ring of integers of $\mathbb{Q}(\sqrt{D})$.*

Proof. If $\mathfrak{q}$ is a prime of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ that divides both, then Equation (21) shows that $\mathfrak{q}$ divides $2\sqrt{D}$, hence $\mathfrak{q}$ is either a prime above 2 or the prime $(\sqrt{D})$. If $(\sqrt{D})$ divides π, then – taking the norm down to $\mathbb{Q}$ – we find that D divides b, which is easily seen to be impossible by considering Equation (1) modulo D^2. If a prime above 2 divides π, we similarly find that b must be even. When $D = 2$ this is ruled out as above. For $D = 3, 5$, considering Equation (1) modulo 8 shows that if b is even we have $a^2 \equiv D \pmod 8$, which is impossible both for $D = 3$ and $D = 5$.

□

Lemma A.2. *Suppose (a, b) is a non-trivial solution to Equation (1) with $D \in \{2,3,5\}$. With notation as in Equations (18) and (19), the numbers η and $\pm\overline{\pi}/\pi$ are multiplicatively independent. For general squarefree $D > 0$, not a square modulo 8, the same conclusion holds if $|a| > \sqrt{D+4} + 2$.*

Proof. Note that we are in the situation of Remark 3.2, so the discussion of Section 3 applies. If $\eta, \pm\overline{\pi}/\pi$ were multiplicatively dependent, a power of $\frac{\overline{\pi}}{\pi}$ would be equal to a power of η. Since η is an algebraic unit, $\pm\frac{\overline{\pi}}{\pi}$ would also be an algebraic unit. Since $\pi, \overline{\pi}$ are relatively prime (Lemma A.1), this implies that $\pi, \overline{\pi}$ are algebraic units. But then so is $b = \pm\pi\overline{\pi}$ (see Equation (20)), hence $b = \pm 1$, contradicting the non-triviality of the solution (a, b).

For general D we can proceed as follows: as above, if by contradiction η and $\pm\overline{\pi}/\pi$ are multiplicatively dependent, we obtain that $\overline{\pi}/\pi$ is an algebraic unit. Taking the ratio of Equations (18) and (19) we get that $\frac{a-\sqrt{D}}{a+\sqrt{D}}$ is an algebraic integer (in fact, a unit). We rewrite this ratio as $\frac{a^2+D-2a\sqrt{D}}{a^2-D}$. For any algebraic integer in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, the coefficient of $\sqrt{D}$ in the $\mathbb{Q}$-basis $\{1, \sqrt{D}\}$ is a half-integer, hence $a^2 - D \mid 4a$. Assuming without loss of generality $a \geq 0$, this implies $a = 0$ or $a^2 - D \leq |a^2 - D| \leq 4a$, and therefore $(a-2)^2 \leq D + 4$, which is the opposite of the inequality in the statement. □

Lemma A.3. *Let (a, b) be a non-trivial solution of Equation (1) for some prime p and some $D \in \{2,3,5\}$. With notation as in Equations (18) and (19), and under the assumption $r > 0$ (see Remark 3.3), we have $|\overline{\pi}| > |\pi|$ and $\log|\overline{\pi}| > \frac{1}{2}\log b$. For general squarefree $D > 0$, not a square modulo 8, the same conclusions hold for $|a| > \frac{\eta^2+1}{\eta^2-1}\sqrt{D}$. If $r = 0$, then (possibly up to replacing (a, b) with $(-a, b)$) we have $|\overline{\pi}| \geq |\pi|$ and $\log|\overline{\pi}| \geq \frac{1}{2}\log b$, with strict inequalities unless D is a perfect p-th power.*

Proof. We are in the situation of Remark 3.2, so the discussion of Section 3 applies. By Equations (18) and (19) we have

$$|\pi|^p = \frac{|a + \sqrt{D}|}{\eta^r}, \quad |\overline{\pi}|^p = \eta^r \cdot |a - \sqrt{D}|,$$

where we assume $0 < r \leq \frac{p-1}{2}$. If $|\pi| \geq |\overline{\pi}|$, then

$$|a| + \sqrt{D} \geq \eta^r |\pi|^p \geq \eta^r |\overline{\pi}|^p \geq \eta^{2r}(|a| - \sqrt{D}),$$

hence $(1+\eta^{2r})\sqrt{D} \geq (\eta^{2r}-1)|a|$. This gives the absolute upper bound $|a| \leq \frac{1+\eta^{2r}}{\eta^{2r}-1}\sqrt{D} = \frac{1+\eta^{-2r}}{1-\eta^{-2r}}\sqrt{D} \leq \frac{1+\eta^{-2}}{1-\eta^{-2}}\sqrt{D}$. For $D \in \{2,3,5\}$ these values of a only lead to trivial solutions, contradiction. Hence $|\pi| < |\overline{\pi}|$. Writing $|b| = |\pi\overline{\pi}| = |\overline{\pi}|^2 \cdot \frac{|\pi|}{|\overline{\pi}|} < |\overline{\pi}|^2$ then gives the other statement. For the case $r = 0$, see Remark 3.3. □

Lemma A.4. *Let (a, b) be a non-trivial solution of Equation (1) for some $D \in \{2,3,5\}$. With notation as in Equations (18) and (19), and under the assumption $r \geq 0$, or $r = 0$ and $|\overline{\pi}| \geq |\pi|$ (see Remark 3.3), the heights of η and $\overline{\pi}/\pi$ are given by*

$$h(\eta) = \frac{1}{2}\log(\eta) \quad \text{and} \quad h(\overline{\pi}/\pi) = \log\max\{|\pi|, |\overline{\pi}|\} = \log|\overline{\pi}|,$$

hence the heights of $\alpha_1 = \eta^{2/k}$ *and* $\alpha_2 = |\overline{\pi}|/|\pi|$ *are*

$$h(\alpha_1) = h(\eta^{2/k}) = \frac{1}{k}\log(\eta) \quad \text{and} \quad h(\alpha_2) = h(\overline{\pi}/\pi) = \log|\overline{\pi}|.$$

For general squarefree $D > 0$*, not a square modulo* 8*, we have* $h(\eta) = \frac{1}{2}\log\eta$ *and* $h(\overline{\pi}/\pi) \leq \log|\overline{\pi}|$.

Proof. The minimal polynomials of $\eta, \overline{\pi}/\pi$ are respectively

$$(x-\eta)(x-\overline{\eta}) \quad \text{and} \quad \left(x - \frac{\overline{\pi}}{\pi}\right)\left(x - \frac{\pi}{\overline{\pi}}\right) = x^2 - \left(\frac{\pi}{\overline{\pi}} + \frac{\overline{\pi}}{\pi}\right)x + 1.$$

Using $\pi\overline{\pi} = \pm b$ (see Equation (20)), we can rewrite the second of these polynomials as

$$x^2 \mp \frac{\pi^2 + \overline{\pi}^2}{b}x + 1;$$

in particular, $\overline{\pi}/\pi$ is a root of the polynomial with integer coefficients

$$bx^2 \mp (\pi^2 + \overline{\pi}^2)x + b.$$

Note that this polynomial is primitive: if there is a prime of $\mathbb{Z}$ that divides both b and $\pi^2 + \overline{\pi}^2$, then there is a prime of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ that divides both $b = \pm\pi\overline{\pi}$ and $\pi^2 + \overline{\pi}^2$, and this contradicts Lemma A.1.

Note that since $|\eta\overline{\eta}| = 1$ and $|\eta| > 1$ we have $|\overline{\eta}| < 1$, so the only conjugate of η with absolute value greater than 1 is η itself. Similarly, at most one of $|\overline{\pi}/\pi|$ and $|\pi/\overline{\pi}|$ is strictly greater than 1. We can then immediately compute the desired heights: since both η and $\pi/\overline{\pi}$ are of degree 2, we get

$$h(\eta) = \frac{1}{2}\log(\eta), \quad h(\overline{\pi}/\pi) = \frac{1}{2}\left(\log|b| + \log\max\{|\pi/\overline{\pi}|, |\overline{\pi}/\pi|\}\right).$$

Taking into account that $\log(|b|) = \log(|\pi\overline{\pi}|)$ by Equation (20), we get $h(\pi) = \log\max\{|\pi|, |\overline{\pi}|\}$. We conclude by applying Lemma A.3.

The proof for general $D > 0$ is the same, except that we do not necessarily know that the polynomial $bx^2 \mp (\pi^2 + \overline{\pi}^2)x + b$ is primitive, hence we only get an upper bound for the height. □

Lemma A.5. *Let* (a, b) *be a non-trivial solution of Equation* (1) *with* $D \in \{2, 3, 5\}$ *and* $p \geq 17$*. Let* $\pi, \overline{\pi}$ *be as in Equations* (18) *and* (19)*. Set*

$$\varepsilon := \frac{4\sqrt{D}\cdot\eta^r}{|\overline{\pi}|^p} > 0.$$

We have $\varepsilon < 4\sqrt{D}\eta^r b^{-p/2}$*, hence in particular* $\varepsilon < 4\sqrt{5}(2+\sqrt{3})^r\exp(-200p) < 10^{-1400}$.

Proof. We have $|\overline{\pi}| \geq |b|^{1/2}$ by Lemma A.3 and $|b| > \exp(400)$ by Proposition 3.23. □

Lemma A.6. *Let* (a, b) *be a non-trivial solution of Equation* (1) *for* $D \in \{2, 3, 5\}$ *and* $p \geq 17$*. Suppose that, in the notation of Equation* (18)*, we have* $r = 1$ *if* $D = 2, 3$ *and* $r = 3$ *if* $D = 5$*. With* α_2 *as in Notation 3.5, we have*

$$0 < \log\alpha_2 < \frac{c_2(D)}{p},$$

where

$$c_2(D) = \begin{cases} 1.77, & \text{for } D = 2 \\ 2.64, & \text{for } D = 3 \\ 0.97, & \text{for } D = 5. \end{cases}$$

Proof. We already know that $\log\alpha_2 = \log(|\overline{\pi}|/|\pi|) > 0$ by Lemma A.3. By (25) with $r = 1$ or $r = 3$ and Lemma A.5 we obtain

$$\left|\frac{2}{p}\log\beta_1 - \log\beta_2\right| < \frac{4\sqrt{D}\eta^r}{pb^{p/2}},$$

hence (using the lower bound for b provided by Proposition 3.23) we have

$$|\log\alpha_2| = |\log\beta_2| < \frac{4\sqrt{D}\eta^r}{pb^{p/2}} + \frac{2}{p}|\log\beta_1| < \frac{2\log\beta_1 + 10^{-4}}{p} < \frac{c_2(D)}{p}.$$

□

B Elementary inequalities

We prove two elementary inequalities needed in the rest of the paper.

Lemma B.1. *Let $N \geq 6$ be an integer. We have*

$$\frac{1}{N}\left(\log(e^N + (e-1)^N) + \log(N!) + \log N\right) < 1.41 \log N.$$

Proof. We bound $\log(e^N + (e-1)^N) < \log(2e^N) = N + \log 2$ and use Stirling's approximation,

$$N! \leq \sqrt{2\pi N}\left(\frac{N}{e}\right)^N e^{\frac{1}{12N}},$$

to get $\log(N!) \leq \frac{1}{2}\log(2\pi) + \frac{1}{12N} + (N+\frac{1}{2})\log N - N \leq 1 + (N+\frac{1}{2})\log N - N$ (the last inequality holds for all $N \geq 2$). We then obtain

$$\begin{aligned}\frac{\log(N)}{N} + \frac{\log\left(e^N + (e-1)^N\right)}{N} + \frac{\log(N!)}{N} \leq \\ \leq \frac{\log N}{N} + \frac{\log 2 + N}{N} + \frac{1 + (N+1/2)\log N - N}{N} \\ \leq \frac{N\log N + 3/2 \log N + \log(2e)}{N} < 1.41 \log N,\end{aligned}$$

where it is easy to test numerically that the last inequality holds for all $N \geq 6$. □

Lemma B.2. *Let $A \geq 2000$ be a real number. The inequality $x < A(\log x)^2$ implies $x < \gamma_0 A(\log A)^2$, where $\gamma_0 = 2.8$.*

Proof. It suffices to check that, for every $\gamma \geq \gamma_0$, the number $x = \gamma A(\log A)^2$ does not satisfy the inequality $x < A(\log x)^2$, that is, that we have

$$\begin{aligned}\gamma A(\log A)^2 \geq A\left(\log(\gamma A(\log A)^2)\right)^2 &\iff \gamma(\log A)^2 \geq (\log(\gamma) + \log A + 2\log\log A)^2 \\ &\iff \sqrt{\gamma} \geq 1 + \frac{\log\gamma + 2\log\log A}{\log A}.\end{aligned}$$

The right-hand side is a decreasing function of A, so it suffices to check this inequality for $A = 2000$. Once A is fixed, the derivative of the left-hand side is greater than the derivative of the right-hand side for $\gamma \geq 1$, so it suffices to check the inequality for $\gamma = \gamma_0$. A numerical verification concludes the proof. □

References

[BdW98] Michael A. Bennett and Benjamin M. M. de Weger. On the Diophantine equation $|ax^n - by^n| = 1$. *Math. Comp.*, 67(221):413–438, 1998.

[Ben01] Michael A. Bennett. Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$. *J. Reine Angew. Math.*, 535:1–49, 2001.

[BMS06] Yann Bugeaud, Maurice Mignotte, and Samir Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[BS04] Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[BS23a] Michael A. Bennett and Samir Siksek. Differences between perfect powers: prime power gaps. *Algebra Number Theory*, 17(10):1789–1846, 2023.

[BS23b] Michael A. Bennett and Samir Siksek. Differences between perfect powers: the Lebesgue-Nagell equation. *Trans. Amer. Math. Soc.*, 376(1):335–370, 2023.

[Bug97a] Yann Bugeaud. On the Diophantine equation $x^2 - 2^m = \pm y^n$. *Proc. Amer. Math. Soc.*, 125(11):3203–3208, 1997.

[Bug97b] Yann Bugeaud. On the Diophantine equation $x^2 - p^m = \pm y^n$. *Acta Arith.*, 80(3):213–223, 1997.

[Bug00] Yann Bugeaud. On the greatest prime factor of $ax^m + by^n$. II. *Bull. London Math. Soc.*, 32(6):673–678, 2000.

[Che12] Imin Chen. On the equations $a^2 - 2b^6 = c^p$ and $a^2 - 2 = c^p$. *LMS J. Comput. Math.*, 15:158–171, 2012.

[Coh07] Henri Cohen. *Number theory. Vol. II. Analytic and modern tools*, volume 240 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Ivo03] Wilfrid Ivorra. Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$. *Acta Arith.*, 108(4):327–338, 2003.

[KO92] Alain Kraus and Joseph Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lau94] Michel Laurent. Linear forms in two logarithms and interpolation determinants. *Acta Arith.*, 66(2):181–199, 1994.

[Lau08] Michel Laurent. Linear forms in two logarithms and interpolation determinants. II. *Acta Arith.*, 133(4):325–348, 2008.

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online; accessed 23 August 2024].

[LMN95] Michel Laurent, Maurice Mignotte, and Yuri Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory*, 55(2):285–321, 1995.

[Rib92] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[Sik03] Samir Siksek. On the Diophantine equation $x^2 = y^p + 2^k z^p$. *J. Théor. Nombres Bordeaux*, 15(3):839–846, 2003.

[Sik12] Samir Siksek. The modular approach to Diophantine equations. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 151–179. Soc. Math. France, Paris, 2012.

Davide Lombardo, Università di Pisa, Dipartimento di matematica, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy
E-mail address: davide.lombardo@unipi.it