Inventiones mathematicae (2024) 236:373–385
https://doi.org/10.1007/s00222-024-01244-6

The largest prime factor of n^2+1 and improvements on subexponential ABC

Hector Pasten[1]

Dedicado a la memoria de mi padre, quien siempre me apoyó en todo

Received: 27 December 2023 / Accepted: 9 February 2024 / Published online: 26 February 2024

Abstract
We combine transcendental methods and the modular approaches to the ABC conjecture to show that the largest prime factor of n^2+1 is at least of size $(\log_2 n)^2/\log_3 n$ where $\log_k$ is the k-th iterate of the logarithm. This gives a substantial improvement on the best available estimates, which are essentially of size $\log_2 n$ going back to work of Chowla in 1934. Using the same ideas, we also obtain significant progress on subexpoential bounds for the ABC conjecture, which in a case gives the first improvement on a result by Stewart and Yu dating back over two decades. Central to our approach is the connection between Shimura curves and the ABC conjecture developed by the author.

Mathematics Subject Classification Primary 11J25 · Secondary 11J86 · 11G18

1 Introduction

For a non-zero integer n let $\mathscr{P}(n)$ be the largest prime factor of n, with $\mathscr{P}(\pm 1)=1$. It is a classical problem to give lower bounds for $\mathscr{P}(f(n))$ where f is a non-linear polynomial with integer coefficients. In 1934 Chowla [2] proved that there is a positive constant κ such that

$$\mathscr{P}(n^2+1) \geq \kappa \cdot \log_2 n \tag{1.1}$$

as n grows, where $\log_k$ is the k-th iterate of the logarithm (for an iterated logarithm, we always assume that the argument is large enough for it to be defined.) Since then, this result has been generalized to all polynomials (see [9] and the references therein) but after 90 years only minor improvements on Chowla's theorem are available: to

✉ H. Pasten
hector.pasten@uc.cl

[1] Departamento de Matemáticas, Facultad de Matemáticas, Pontificia Universidad Católica de Chile, 4860 Av. Vicuña Mackenna, Macul, RM, Chile

the best of the author's knowledge, the sharpest available estimate is obtained by the theory of linear forms in logarithms and it takes the form

$$\mathscr{P}(n^2+1) \geq \kappa \cdot \frac{\log_3 n}{\log_4 n} \cdot \log_2 n,$$

see [9]. We prove a lower bound for $\mathscr{P}(n^2+1)$ which is nearly the square of the previous bounds:

Theorem 1.1 *There is a constant $\kappa > 0$ such that as n grows we have*

$$\mathscr{P}(n^2+1) \geq \kappa \cdot \frac{(\log_2 n)^2}{\log_3 n}.$$

For a positive integer n let $\mathrm{rad}(n)$ be its radical, that is, the largest squarefree divisor of n. The previous result is in fact a direct consequence of the next theorem:

Theorem 1.2 *There is a constant $\kappa > 0$ such that as n grows we have*

$$\mathrm{rad}(n^2+1) \geq \exp\left(\kappa \cdot \frac{(\log_2 n)^2}{\log_3 n}\right).$$

The proof of the previous theorems combines the theory of linear forms in logarithms with results from a modular approach to the ABC conjecture developed by the author using the theory of Shimura curves [7]. In particular, the methods pertain to both transcendental number theory and arithmetic geometry.

More precisely, when we apply linear forms in logarithms to the problem we will separate those primes with large exponent in the factorization of n^2+1 from those with small exponent. Then, for each n, we construct an elliptic curve and we apply our results from [7] to this elliptic curve in order to give a good bound for the number of prime divisors of n^2+1 with large exponent. After this point we return to the bounds provided by linear forms in logarithms using this new input to conclude.

The technique developed in this work is not limited to the previous two theorems. In fact, another application of our methods is that we can give improvements on the sharpest available subexponential bounds for the ABC conjecture. Let us recall the statement of the problem.

Conjecture 1.3 (The Masser–Oesterlé ABC conjecture) *Let $\epsilon > 0$. There is a number $\kappa_\epsilon > 0$ depending only on ϵ such that the following holds*:

Given a, b, c coprime positive integers with $a+b=c$, we have $c \leq \kappa_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}$.

In what follows, let us write $R = \mathrm{rad}(abc)$ where a, b, c are triples as in the statement of the ABC conjecture and the term "absolute constant" refers to a number independent of all parameters. At present, the best unconditional bound is due to Stewart–Yu [12] and it is of the form

$$\log c \leq \kappa \cdot R^{1/3} (\log R)^3$$

for certain absolute constant κ. See also [5, 10, 11] for other unconditional bounds. While all these bounds are exponential on R, under certain circumstances one can do better obtaining subexponential bounds:

(i) (See [6] by the author.) Let $\epsilon > 0$. There is a number $\kappa_\epsilon > 0$ depending only on ϵ such that if $a \leq c^{1-\eta}$ for some number $\eta > 0$, then

$$\log c \leq \eta^{-1} \cdot \kappa_\epsilon \cdot \exp\left((1+\epsilon) \cdot \frac{\log_3 R}{\log_2 R} \cdot \log R\right).$$

(ii) (See [12] by Stewart and Yu.) Let $q = \min\{\mathscr{P}(a), \mathscr{P}(b), \mathscr{P}(c)\}$. Then for certain absolute constant $\kappa > 0$ we have

$$\log c \leq q \cdot \exp\left(\kappa \cdot \frac{\log_3 R}{\log_2 R} \cdot \log R\right).$$

Our method gives a substantial improvement on both bounds:

Theorem 1.4 *Let a, b, c vary over triples of coprime positive integers with $a+b=c$ and write $R = \mathrm{rad}(abc)$. Then we have the following bounds*:

(1) *There is an absolute constant $\kappa > 0$ such that if $a \leq c^{1-\eta}$ for a number $\eta > 0$, then*

$$\log c \leq \eta^{-1} \exp\left(\kappa \cdot \sqrt{(\log R)\log_2 R}\right).$$

(2) *Let $q = \min\{\mathscr{P}(a), \mathscr{P}(b), \mathscr{P}(c)\}$. There is an absolute constant $\kappa > 0$ for which we have*

$$\log c \leq q \cdot \exp\left(\kappa \cdot \sqrt{(\log R)\log_2 R}\right).$$

It is worth pointing out that item (2) of the previous theorem is the first improvement on Theorem 2 from [12] in more than two decades.

Using item (2) of Theorem 1.4 we also get the following improvement on the bound (7) of [12]:

Corollary 1.5 *There is an absolute constant $\kappa > 0$ such that as $x < y$ vary over coprime positive integers, we have*

$$\mathscr{P}(xy(x+y)) \geq \kappa \cdot \frac{(\log_2 y)^2}{\log_3 y}.$$

Namely, the bound (7) in [12] is

$$\mathscr{P}(xy(x+y)) \geq \kappa \cdot \frac{(\log_2 y)\log_3 y}{\log_4 y}$$

which in turn is an improvement of the earlier bound

$$\mathscr{P}(xy(x+y)) \geq \kappa \cdot \log_2 y$$

by van der Poorten, Schinzel, Shorey, and Tijdeman [14].

As the reader will see, with some bookkeeping one can get explicit values for κ in Theorems 1.1, 1.2, and 1.4 as well as Corollary 1.5 that work for large enough values of the variables. We leave this task to the interested reader.

2 Preliminaries

2.1 Bounds coming from linear forms in logarithms

We need estimates for approximation by finitely generated multiplicative groups due to Evertse and Győry (cf. Theorem 4.2.1 in [3]) that come from the theory of linear forms in logarithms and geometry of numbers.

Let us first introduce the notation. Let k be a number field of degree d over $\mathbb{Q}$. If v is an archimedean place of k associated to an embedding $\sigma : k \to \mathbb{C}$ (it could be real, or it could come in a complex conjugate pair), we define the v-adic norm on k

$$|x|_v = |\sigma(x)|^{\epsilon_v}$$

where $|-|$ is the usual complex absolute value and $\epsilon_v = 1$ if σ is real, and $\epsilon_v = 2$ if σ is complex. On the other hand, if v is a non-archimedean place of k associated to a prime ideal $\mathfrak{p}$ of O_k, we let $v_\mathfrak{p}$ be the $\mathfrak{p}$-adic valuation on k and define the v-adic norm

$$|x|_v = \mathrm{Norm}(\mathfrak{p})^{-v_\mathfrak{p}(x)}.$$

In the case of $k = \mathbb{Q}$ we simply write v_p for the p-adic valuation when p is a prime number.

The height on k is defined by

$$h(x) = \frac{1}{d} \sum_v \log \max\{1, |x|_v\}.$$

Let Γ be a finitely generated multiplicative subgroup of k^* and let $\{\xi_1, \ldots, \xi_m\} \subseteq \Gamma$ be a system of generators for $\Gamma / \Gamma_{\mathrm{tor}}$ with $m \geq 1$. With these notation and assumptions, from Theorem 4.2.1 in [3] we get:

Theorem 2.1 (Approximation bound) *There is a number K_d depending only on d such that the following holds*:

(i) (*Archimedean bound*) *Let v be an archimedean place of k. For every $\xi \in \Gamma$ different from* 1 *we have*

$$-\log|1-\xi|_v < K_d^m \cdot (\log \max\{e, h(\xi)\}) \prod_{j=1}^m h(\xi_j).$$

(ii) (*Non-archimedean bound*) *Let v be a non-archimedean place of k associated with a prime ideal $\mathfrak{p}$ of O_k. For every $\xi \in \Gamma$ different from* 1 *we have*

$$-\log|1-\xi|_v < K_d^m \cdot \frac{\mathrm{Norm}(\mathfrak{p})}{\log \mathrm{Norm}(\mathfrak{p})} (\log \max\{e, \mathrm{Norm}(\mathfrak{p}) h(\xi)\}) \prod_{j=1}^m h(\xi_j).$$

2.2 Bounds coming from the classical modular approach to Szpiro's conjecture

In [5] Murty and the author showed an unconditional partial result for Szpiro's conjecture using classical modular forms.

Theorem 2.2 (Szpiro type bound, [5]) *There is an absolute constant $\kappa > 0$ such that for all elliptic curves E over $\mathbb{Q}$ one has*

$$\log \Delta \leq \kappa \cdot N \log N$$

where Δ and N are the minimal discriminant and the conductor of E.

The constant κ was made explicit in [5] and the result is strong enough to be useful in explicit computations with Diophantine equations; see [5] for the S-unit equation and [15] for other applications. See [7] for improvements.

From the previous theorem one in particular gets:

Corollary 2.3 (Bounds for exponents of the minimal discriminant) *There is an absolute constant $\kappa > 0$ such that for all elliptic curves E over $\mathbb{Q}$ and all primes p one has*

$$v_p(\Delta) \leq \kappa \cdot N \log N$$

where Δ and N are the minimal discriminant and the conductor of E.

2.3 Bounds coming from Shimura curves

In [7] the author developed a theory based on Shimura curve parametrizations of elliptic curves in order to obtain a new type of unconditional bounds for the ABC and Szpiro's conjecture. Let us state the results that we need.

Theorem 2.4 (Bound for elliptic curves, Corollary 16.3 in [7]) *Let S be a finite set of primes and let $\epsilon > 0$. There is a number $\kappa_{S,\epsilon}$ depending only on S and ϵ such that the following holds*:

Let E be an elliptic curve over $\mathbb{Q}$, semistable outside of S, with minimal discriminant Δ and conductor N. Then

$$\prod_{p|N^*} v_p(\Delta) \leq \kappa_{S,\epsilon} \cdot N^{11/2+\epsilon}$$

where N^* is the product of all the primes dividing N not in S.

Theorem 2.5 (Bound for ABC triples, Theorem 16.8 in [7]) *Let $\epsilon > 0$. There is a number κ_ϵ depending only on ϵ such that the following holds*:

For all coprime positive integers a, b, c with $a + b = c$ we have

$$\prod_{p|abc} v_p(abc) \leq \kappa_\epsilon \cdot \mathrm{rad}(abc)^{8/3+\epsilon}.$$

For the convenience of the reader let us briefly sketch the main ideas in the proof of the previous two results.

Let E be an elliptic curve defined over $\mathbb{Q}$. By the modularity theorem [1, 13, 16] there is a modular parametrization $\varphi : X_0(N) \to E$. By the Jacquet–Langlands correspondence, for each admissible factorization $N = DM$ there is a Shimura curve parametrization $\varphi_{D,M} : X_0^D(M) \to E$ where in particular $X_0(N) = X_0^1(N)$ and $\varphi = \varphi_{1,N}$. We assume that these parametrizations have minimal degree.

The starting point is to prove a generalization of the Ribet–Takahashi formula [8] to obtain the formula

$$\prod_{p|D} \nu_p(\Delta) = \gamma_{D,M} \cdot \frac{\deg \varphi}{\deg \varphi_{D,M}}$$

with an error factor $\gamma_{D,M}$ of controlled height (in the worst case, $h(\gamma_{D,M}) \leq (1 + \epsilon) \log D$ for any $\epsilon > 0$, provided that N is large enough) where Δ is the minimal discriminant of E. It is important that this formula is *global*: the contribution of every prime is taken into account.

If $h(E)$ denotes the Faltings height of E and c is the Manin constant of φ, then pulling back a Néron differential of E via the parametrizations of E one deduces

$$\frac{\deg \varphi}{\deg \varphi_{D,M}} = \frac{c^2 \| f \|^2 e^{2h(E)}}{\| f_{D,M} \|_2^2 e^{2h(E)}} = \frac{c^2 \| f \|^2}{\| f_{D,M} \|_2^2}$$

where $\| - \|_2$ is the Petersson norm, f is the Fourier normalized newform attached to E, and $f_{D,M}$ is a quaternionic modular form defined on an integral model of $X_0^D(M)$ which is Jacquet–Langlands correspondent associated to f.

An important part of the work is to prove a uniform upper bound for the Manin constant c (fixing the set of primes of additive reduction). On the other hand, the upper bound $\| f \|_2^2 \ll_\epsilon N^{1+\epsilon}$ is known [4]. Since $f_{D,M}$ extends to an integral model of $X_0^D(M)$ one can use Arakelov theory to give a polynomial lower bound $\| f_{D,M} \|_2^2 \gg_\epsilon N^{-(5/3+\epsilon)} M^{-1}$. For this it is crucial to have bounds for the Arakelov height of Heegner points in terms of L-functions (extensions of the Chowla–Selberg formula due to Yuan–Zhang [17] in the context of Colmez's conjecture) and suitable zero-free regions for the relevant L-functions. Putting it all together one finally arrives at

$$\prod_{p|D} \nu_p(\Delta) \ll_\epsilon N^{8/3+\epsilon} DM = N^{11/3+\epsilon}.$$

Theorem 2.4 follows by varying the choice of M. Theorem 2.5 follows by choosing E as a Frey–Hellegouarch elliptic curve in which case one shows the stronger bound $h(\gamma_{D,M}) \leq \epsilon \log D$.

3 The largest prime factor of $n^2 + 1$

The following simple observation will be used a couple of times.

Lemma 3.1 *Consider a number $A > e$. The real function $t \mapsto t\log(A/t)$ is increasing in the range $1 \le t \le A/e$.*

The next lemma does not give the best bound that the method allows, but it is enough for our purposes.

Lemma 3.2 *There is an absolute constant $K > 0$ such that for all positive integers n we have*

$$\prod_{p|n^2+1} v_p(n^2+1) \le K \cdot \mathrm{rad}(n^2+1)^8.$$

Proof Let n be a positive integer and consider the elliptic curve

$$E: \quad y^2 = x^3 + 3x + 2n.$$

Let Δ and N be the minimal discriminant and the conductor of E. This Weierstrass equation is minimal except perhaps at 2 and 3 and it has (not necessarily minimal) discriminant

$$-16(4 \cdot 3^3 + 27(2n)^2) = -1728(n^2+1).$$

One checks that E has multiplicative reduction away from 2 and 3 (thus, N is square-free except for uniformly bounded powers of 2 and 3) and that the minimal discriminant is

$$\Delta = -2^s \cdot 3^t \cdot (n^2+1)$$

where s and t are integers of uniformly bounded absolute value.

By Corollary 2.3 there is an absolute constant $\kappa > 0$ such that

$$v_2(n^2+1)v_3(n^2+1) \le \kappa \cdot N^2(\log N)^2.$$

Letting $\epsilon > 0$ and choosing $S = \{2, 3\}$ we apply Theorem 2.4 we get a number $\kappa_{S,\epsilon}$ depending only on S and ϵ such that

$$\prod_{p|N^*} v_p(n^2+1) \le \kappa_{S,\epsilon} \cdot N^{11/2+\epsilon}$$

where N^* is the product of the primes dividing N other than 2 and 3. For a prime $p \neq 2, 3$ we have that p divides N if and only if it divides Δ, hence, if and only if it divides n^2+1. It follows that

$$\prod_{p|n^2+1} v_p(n^2+1) \le \kappa \cdot \kappa_{S,\epsilon} \cdot N^{15/2+\epsilon}.$$

As S is fixed, one can choose $\epsilon = 1/2$ to obtain

$$\prod_{p|n^2+1} v_p(n^2+1) \le K \cdot \mathrm{rad}(n^2+1)^8$$

for certain absolute constant $K > 0$, because $\mathrm{rad}(n^2+1)$ and N agree except, perhaps, by a bounded power of 2 and 3 (this is because of the semi-stable reduction at primes $p \neq 2, 3$). □

Proof of Theorem 1.2 Let n be a sufficiently large positive integer and write $i = \sqrt{-1} \in \mathbb{C}$. We consider the equation

$$(n+i) - (n-i) = 2i$$

in $\mathbb{Z}[i]$. This gives the equation

$$1 - \frac{n-i}{n+i} = \frac{2i}{n+i}$$

in the quadratic number field $k = \mathbb{Q}(i)$.

Consider a factorization $n+i = u \cdot \gamma_1^{e_1} \cdots \gamma_r^{e_r}$ with γ_j non-associated irreducible elements of $\mathbb{Z}[i]$ and $u \in \{\pm 1, \pm i\}$. Then we have $n - i = \bar{u} \cdot \bar{\gamma}_1^{e_1} \cdots \bar{\gamma}_r^{e_r}$ where the bar denotes complex conjugation.

Let

$$B = \exp\left(\sqrt{(\log R)\log_2 R}\right)$$

where $R = \mathrm{rad}(n^2+1)$. In what follows we will use the fact that R grows as n grows—for instance, by Chowla's result, although we don't need a precise rate of growth.

Define $J = \{1, \ldots, r\}$ and let $I \subseteq J$ be the set of indices such that $e_j > B$. Let $\xi_j = \bar{\gamma}_j/\gamma_j$ for $j \in J$ and let $\xi_0 = \prod_{j \in J-I} \xi_j^{e_j}$. Let $w = \bar{u}/u$. Then we have

$$\frac{n-i}{n+i} = w \cdot \xi_0 \cdot \prod_{j \in I} \xi_j^{e_j}.$$

Let $I_0 = I \cup \{0\}$ and let Γ be the subgroup of $k^\times$ generated by w and the ξ_j for $j \in I_0$. Let $m = 1 + \#I = \#I_0$. Then the elements ξ_j for $j \in I_0$ generate $\Gamma/\Gamma_{\mathrm{tor}}$ and we can write

$$\frac{2i}{n+i} = 1 - \xi$$

where $(n-i)/(n+i) = \xi = w \cdot \xi_0 \cdot \prod_{j \in I} \xi_j^{e_j} \in \Gamma$. Item (i) in Theorem 2.1 (with $d = 2$) gives an absolute constant K such that

$$\log n \leq -2 \log \frac{2}{|n+i|} = -\log|1-\xi|^2 \leq K^m \cdot (\log \max\{e, h(\xi)\}) \prod_{j \in I_0} h(\xi_j) \quad (3.1)$$

where $|-|$ is the usual absolute value on $\mathbb{C}$. Let us estimate the terms on the right of (3.1). First we have

$$h(\xi) = h\left(\frac{n-i}{n+i}\right) \leq \frac{1}{2}\log|n+i|^2 = \log|n+i|$$

so that

$$K^m \cdot (\log \max\{e, h(\xi)\}) \le (2K)^m \log_2 n. \tag{3.2}$$

On the other hand $e_j \le B$ for each $j \in J - I$, and recalling that the γ_j are non-associated irreducibles we get

$$h(\xi_0) \le B \cdot h\left(\prod_{j\in J-I} \gamma_j\right) \le \frac{B}{2} \log \prod_{j\in J} \mathrm{Norm}(\gamma_j) \le B \log \prod_{p|n^2+1} p$$

which gives

$$h(\xi_0) \le B \cdot \log R. \tag{3.3}$$

At this point we note from (3.1), (3.2), and (3.3) that if $m = 1$ (i.e. $I = \emptyset$) then

$$\sqrt{\log n} \le \frac{\log n}{\log_2 n} \le 2KB \log R < \exp\left(K' \cdot \sqrt{(\log R)\log_2 R}\right)$$

for a suitable absolute constant $K' > 0$, and the result is proved. So we may assume $m \ge 2$.

Let p_j be the prime number below the irreducible γ_j. Noticing that for $j \in I$ we have $h(\xi_j) \le \log p_j$ we get

$$\prod_{j\in I} h(\xi_j) \le \prod_{j\in I} \log p_j \le \left(\frac{\log R}{m-1}\right)^{m-1}$$

where we used the arithmetic-geometric mean inequality. Putting this together with (3.1), (3.2), and (3.3) we deduce

$$\begin{aligned} \sqrt{\log n} \le \frac{\log n}{\log_2 n} &\le (2K)^m B(\log R)\left(\frac{\log R}{m-1}\right)^{m-1} \\ &= 2KB(\log R)\left(\frac{2K\cdot \log R}{m-1}\right)^{m-1}. \end{aligned} \tag{3.4}$$

Next, we note that

$$e_j = v_{(\gamma_j)}(n+i) \le 2v_{p_j}(n^2+1).$$

Therefore the condition $e_j > B$ implies $v_{p_j}(n^2+1) > B/2$ and the number of indices j satisfying the former condition is $m - 1 = \#I$. This gives

$$\prod_{j\in I} v_{p_j}(n^2+1) > (B/2)^{m-1}.$$

On the other hand, by Lemma 3.2 we have

$$\prod_{p|n^2+1} v_p(n^2+1) \le \kappa \cdot R^8$$

for some absolute constant κ. This yields

$$m-1<\frac{8\log R+\log\kappa}{\log(B/2)}<\kappa'\cdot\frac{\log R}{\sqrt{(\log R)\log_2 R}}=\kappa'\cdot\sqrt{\frac{\log R}{\log_2 R}}$$

for a suitable absolute constant κ'.

Using Lemma 3.1 with $A=2K\log R$, and since

$$\kappa'\cdot\sqrt{\frac{\log R}{\log_2 R}}<\frac{2K}{e}\log R$$

for R large enough, we deduce

$$\begin{aligned}\left(\frac{2K\cdot\log R}{m-1}\right)^{m-1}&\leq\left(\frac{2K}{\kappa'}\sqrt{(\log R)\log_2 R}\right)^{\kappa'\sqrt{(\log R)/\log_2 R}}\\&\leq\exp\left(K''\cdot\sqrt{(\log R)\log_2 R}\right)\end{aligned}$$

for a suitable absolute constant K''. Using this in (3.4) we obtain

$$\sqrt{\log n}\leq 2KB(\log R)B^{K''}.$$

Thus, for a suitable absolute constant $M>0$ we obtain

$$\log n\leq\exp\left(M\cdot\sqrt{(\log R)\log_2 R}\right)$$

and the result follows. □

Proof of Theorem 1.1 Write $R=\mathrm{rad}(n^2+1)$. By Theorem 1.2 we have

$$R\geq\exp\left(\kappa\cdot\frac{(\log_2 n)^2}{\log_3 n}\right).$$

Write $P=\mathscr{P}(n^2+1)$. By Chebyshev's bound for the function $\theta(x)=\sum_{p\leq x}\log p$, we have

$$R\leq\prod_{p\leq P}p\leq\exp(4P)$$

which proves the result. □

4 Subexponential ABC, case 1

Proof of Theorem 1.4 item (1) We keep the notation from the statement and assume that c is large enough. Note that R grows as c grows —for instance, by the finiteness of solutions of the S-unit equation. We can write

$$\frac{a}{c}=1-\xi$$

where $\xi = b/c$. Let $\xi_1, \ldots, \xi_r$ be the different prime divisors of bc and let $e_j = v_{\xi_j}(b/c)$ (possibly negative). Let

$$B = \exp\left(\sqrt{(\log R)\log_2 R}\right)$$

and define $J = \{1, 2, \ldots, r\}$ and $I = \{j \in J : |e_j| > B\}$. Let $\xi_0 = \prod_{j \in J-I} \xi_j^{e_j}$, let $I_0 = I \cup \{0\}$, and let $m = \#I_0$. Let Γ be the subgroup of $\mathbb{Q}^\times$ generated by ξ_j for $j \in I_0$; in particular, $\xi = b/c \in \Gamma$.

By item (1) in Theorem 2.1 we have

$$\eta \cdot \log c \le \log(c/a) = -\log|1-\xi| \le K^m \cdot (\log \max\{e, h(\xi)\}) \prod_{j \in I_0} h(\xi_j)$$

where $|-|$ is the archimedean absolute value on $\mathbb{Q}$ and K is an absolute constant.

We have $h(\xi) = h(b/c) = \log c \le R^{K'}$ for some absolute constant K', by applying any exponential bound for the ABC conjecture (such as the one in [10] which gives $K' = 15$.) On the other hand, we have $h(\xi_0) \le B \log R$, so we obtain

$$\eta \cdot \log c \le K' \cdot K^m B (\log R)^2 \prod_{j \in I} h(\xi_j). \tag{4.1}$$

If $m = 1$ we have $I = \emptyset$ thus obtaining

$$\eta \cdot \log c \le K' K B (\log R)^2 \le \exp\left(2\sqrt{(\log R)\log_2 R}\right)$$

and the result follows. So we may assume that $m \ge 2$. From (4.1) we get

$$\begin{aligned} \eta \cdot \log c &\le K' \cdot K^m B (\log R)^2 \left(\frac{1}{m-1}\log R\right)^{m-1} \\ &\le K' K B^2 \left(\frac{K}{m-1}\log R\right)^{m-1} \end{aligned} \tag{4.2}$$

by applying the arithmetic-geometric mean inequality.

Let us bound m. Fixing a small $\epsilon > 0$, from Theorem 2.5 we get

$$B^{m-1} \le \prod_{j \in I} |e_j| \le \prod_{p|R} v_p(abc) \le R^3$$

from which it follows that

$$m - 1 \le \frac{3\log R}{\log B} = 3\sqrt{\frac{\log R}{\log_2 R}}.$$

From Lemma 3.1 we deduce

$$\left(\frac{K}{m-1}\log R\right)^{m-1} \le \left(\frac{K}{3}\sqrt{(\log R)\log_2 R}\right)^{3\sqrt{(\log R)/\log_2 R}} \le B^{K''}$$

for some absolute constant K''. Putting this together with (4.2) we get

$$\eta \cdot \log c \leq K' K B^{2+K''}.$$

The result follows from the definition of B. □

5 Subexponential ABC, case 2

Proof of Theorem 1.4 item (2) By Theorem 1.4 item (1) it suffices to assume $c^{1/2} \leq a < b < c$. For the sake of having a more symmetric formulation of the problem, let $x, y, z \in \mathbb{Z}$ be the same numbers a, b, c up to sign and in some order, such that $x + y + z = 0$. We may assume that q divides x and let us write the equation $x + y + z = 0$ as

$$-\frac{x}{z} = 1 - \xi$$

where $\xi = -y/z$. Let p_0 be a prime divisor of x (in particular, $p_0 \leq q$) such that $v_{p_0}(x)$ is maximal among the prime divisors of x. Then, since $c^{1/2} \leq a < b < c$ we see that

$$\frac{\log c}{2 \log R} \leq v_{p_0}(x) \leq 2 v_{p_0}(x) \log p_0 \leq -2 \log |1 - \xi|_{p_0}.$$

Let

$$B = \exp\left(\sqrt{(\log R) \log_2 R}\right).$$

As in the proof of Theorem 1.2 item (1), we may use Theorem 2.5 to bound the number of prime divisors of xz with exponent larger than B. Then, using an argument very similar to that in the proof of Theorem 1.2 item (1), but applying item (ii) of Theorem 2.1 (with $v = p_0$) instead of item (i), we deduce that there is some absolute constant K such that

$$-\log |1 - \xi|_{p_0} \leq p_0 \cdot B^K \leq q \cdot B^K$$

and the result follows. □

Proof of Corollary 1.5 We take $a = x$, $b = y$ and $c = x + y$. Since $c < 2b = 2y$ we may express the desired lower bound for $\mathscr{P}(xy(x + y))$ in terms of c.

We may assume $q < (\log_2 c)^2 / \log_3 c$ for otherwise the result directly holds. By item (2) of Theorem 1.4 we get

$$\log c \leq \exp\left(K \cdot \sqrt{(\log R) \log_2 R}\right)$$

for certain absolute constant $K > 0$, where $R = \mathrm{rad}(abc)$. This gives

$$\log R \geq K' \cdot \frac{(\log_2 c)^2}{\log_3 c}$$

for certain absolute constant K'. By Chebyshev's bound we have $\exp(4\mathscr{P}(abc)) \geq R$ and the result follows. □

Acknowledgements I thank Kálmán Győry and Cameron L. Stewart for valuable comments on these results. And I am particularly indebted to Samuel Le Fourn and M. Ram Murty for carefully reading an earlier version of this manuscript and suggesting several changes and corrections. The comments and suggestions of the referee are gratefully acknowledged.

Funding Supported by ANID Fondecyt Regular grant 1230507 from Chile.

References

1. Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Am. Math. Soc. **14**(4), 843–939 (2001)
2. Chowla, S.: The greatest prime factor of $x^2 + 1$. J. Lond. Math. Soc. **10**(2), 117–120 (1935)
3. Evertse, J.-H., Győry, K.: Unit Equations in Diophantine Number Theory. Cambridge Studies in Advanced Mathematics, vol. 146. Cambridge University Press, Cambridge (2015)
4. Murty, M.R.: Bounds for congruence primes. In: Automorphic Forms, Automorphic Representations, and Arithmetic (Fort Worth, TX, 1996). Proc. Sympos. Pure Math., Part 1, vol. 66, pp. 177–192. Am. Math. Soc., Providence (1999)
5. Murty, M.R., Pasten, H.: Modular forms and effective Diophantine approximation. J. Number Theory **133**(11), 3739–3754 (2013)
6. Pasten, H.: On the arithmetic case of Vojta's conjecture with truncated counting functions. Preprint (2022). arXiv:2205.07841
7. Pasten, H.: Shimura curves and the abc conjecture. J. Number Theory **254**, 214–335 (2024)
8. Ribet, K., Takahashi, S.: Parametrizations of elliptic curves by Shimura curves and by classical modular curves. Proc. Natl. Acad. Sci. USA **94**(21), 11110–11114 (1997)
9. Shorey, T., Tijdeman, R.: On the greatest prime factors of polynomials at integer points. Compos. Math. **33**(2), 187–195 (1976)
10. Stewart, C., Tijdeman, R.: On the Oesterlé-Masser conjecture. Monatshefte Math. **102**(3), 251–257 (1986)
11. Stewart, C., Yu, K.: On the *abc* conjecture. Math. Ann. **291**(2), 225–230 (1991)
12. Stewart, C., Yu, K.: On the *abc* conjecture. II. Duke Math. J. **108**(1), 169–181 (2001)
13. Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. Ann. Math. (2) **141**(3), 553–572 (1995)
14. van der Poorten, A., Schinzel, A., Shorey, T., Tijdeman, R.: Applications of the Gel'fond-Baker Method to Diophantine Equations. Transcendence Theory: Advances and Applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), pp. 59–77. Academic Press, London (1977)
15. von Känel, R., Matschke, B.: Solving *S*-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via the Shimura-Taniyama conjecture. Mem. Am. Math. Soc. **286**, 1419 (2023)
16. Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. Math. (2) **141**(3), 443–551 (1995)
17. Yuan, X., Zhang, S.-W.: On the averaged Colmez conjecture. Ann. Math. (2) **187**(2), 533–638 (2018)