On Ennola's Conjecture on Non-Galois Cubic Number Fields with Exceptional Units

Stéphane Louboutin

On Ennola's conjecture on non-Galois cubic number fields with exceptional units

Stéphane R. LOUBOUTIN
Aix Marseille Université, CNRS, Centrale Marseille, I2M,
Marseille, France
stephane.louboutin@univ-amu.fr

December 10, 2021

Abstract

Let ε be a non-Galois totally real cubic special unit, i.e. a unit such that $\varepsilon-1$ is also a unit. Then ε and $\varepsilon-1$ are multiplicatively independent and the unit index j_ε of the groups of units generated by -1, ε and $\varepsilon-1$ in the group of units of the ring of algebraic integers of $\mathbb{Q}(\varepsilon)$ is finite. It is known that $\{\varepsilon, \varepsilon-1\}$ is a system of fundamental units of the cubic order $\mathbb{Z}[\varepsilon]$. V. Ennola conjectured that $\{\varepsilon, \varepsilon-1\}$ is always a system of fundamental units of the maximal order of $\mathbb{Q}(\varepsilon)$, i.e. that j_ε is always equal to 1. Fix an algebraic closure of $\mathbb{Q}$. We prove that for any given prime p there are only finitely many cases for which p divides j_ε. We explain how this result makes Ennola's conjecture very reasonable for its possible exceptions would be few and far between. Our proof is conditional: we conjecture that the degrees of some explicit rational fractions that clearly are Laurent polynomials are always negative and given by conjectured explicit formulas. These degrees being easy to compute by using any formal language for algebraic computation, we checked enough of them to obtain that for any given prime $p \leq 1875$ there are only finitely many cases for which p divides j_ε. We also prove that under the assumption of the ABC conjecture there are only finitely many exceptions to Ennola's conjecture.

[0]2010 Mathematics Subject Classification. Primary. 11R16, 11R27.
Key words and phrases. Units. Exceptional units. Cubic number fields. Unit index. Thue's Lemma. The abc conjecture.

1 Introduction

Let $\varepsilon > 1$ with $\varepsilon \neq (3+\sqrt{5})/2$ be a real quadratic algebraic unit. It is not that difficult to prove that ε is a fundamental unit of the order $\mathbb{Z}[\epsilon]$, i.e. that the group of units of this order is generated by -1 and ε. (If $\varepsilon = (3+\sqrt{5})/2$, then $\varepsilon = (\varepsilon-1)^2$ and $\varepsilon - 1 = (1+\sqrt{5})/2 > 1$ is the fundamental unit of the order $\mathbb{Z}[\epsilon]$.) However, since $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\varepsilon^n)$ for any $n \geq 2$, we cannot expect a real quadratic algebraic unit to always be a fundamental unit of the maximal order of the real quadratic field it generates. In contrast to this situation, V. Ennola's conjectured that if ε is a non-Galois totally real cubic exceptional algebraic unit, i.e. a unit ε for which $\varepsilon - 1$ is also a unit, then not only is $\{\varepsilon, \varepsilon - 1\}$ a system of fundamental unit of the totally real cubic order $\mathbb{Z}[\varepsilon]$ (see [Tho, Proposition (3.6)]), but it always is a system of fundamental units of the maximal order of the non-Galois totally real cubic field $\mathbb{Q}(\varepsilon)$. The aim of this paper is to prove a weak form of Ennola's conjecture which we now expound.

Fix an algebraic closure of $\mathbb{Q}$. A totally real cubic algebraic unit ε is called an **exceptional unit** if $\varepsilon - 1$ is also a unit. In that situation, ε and $\varepsilon - 1$ are multiplicatively independent (see Theorem 22 below) and we let

$$j_\varepsilon = (\mathbb{U}_\varepsilon : \langle -1, \varepsilon, \varepsilon - 1\rangle) < \infty$$

denote the finite index of the group of units $\langle -1, \varepsilon, \varepsilon - 1\rangle$ generated by -1, ε and $\varepsilon - 1$ in the group $\mathbb{U}_\varepsilon$ of units of the ring of algebraic integers of the number field $\mathbb{Q}(\varepsilon)$. If ε is exceptional, then any $\eta \in V_\varepsilon$ is also exceptional and (i) $\mathbb{Q}(\eta) = \mathbb{Q}(\varepsilon)$, (ii) $\langle -1, \eta, \eta - 1\rangle = \langle -1, \varepsilon, \varepsilon - 1\rangle$ and (iii) $j_\eta = j_\varepsilon$ for

$$\eta \in V_\varepsilon := \{\varepsilon, 1/\varepsilon, 1-\varepsilon, 1/(1-\varepsilon), (\varepsilon-1)/\varepsilon, \varepsilon/(\varepsilon-1)\}.$$

Proposition 1. *(i). Let ε_l denote any of the three distinct real roots of the $\mathbb{Q}$-irreducible polynomial $P_l(X) := X^3 + (l-1)X^2 - lX - 1 \in \mathbb{Z}[X]$. Then ε is a totally real cubic exceptional unit with $\mathbb{Q}(\varepsilon)$ not normal if and only if ε is one of the three real conjugates of some $\eta \in V_{\varepsilon_l}$ for some $l \geq 3$. (ii). Let θ_m denote any of the three distinct real roots of the $\mathbb{Q}$-irreducible polynomial $Q_m(X) := X^3 + mX^2 - (m+3)X + 1 \in \mathbb{Z}[X]$. Then ε is a totally real cubic exceptional unit with $\mathbb{Q}(\varepsilon)$ normal if and only if ε is one of the three real conjugates of some $\eta \in V_{\theta_m}$ for some $m \geq -1$ or some $\eta \in V_{-\theta_{-1}}$.*

Proof. A cubic unit ε is exceptional if and only if $\mathrm{Irr}(\varepsilon, \mathbb{Q}, X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$, with $c = N_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(\varepsilon) \in \{\pm 1\}$ and $-(1-a+b-c) = -\mathrm{Irr}(\varepsilon, \mathbb{Q}, 1) = N_{\mathbb{Q}(\varepsilon)/\mathbb{Q}}(\varepsilon - 1) \in \{\pm 1\}$. It amounts to asking $c = 1$ and $b - a \in \{\pm 1\}$, or $c = -1$ and $b - a \in \{-1, -3\}$, i.e. to asking that

$$\mathrm{Irr}(\varepsilon, \mathbb{Q}, X) = X^3 - aX^2 + (a-1)X - 1 = P_{-a+1}(X) = \mathrm{Irr}(\varepsilon_{-a+1}, \mathbb{Q}, X),$$

$$\mathrm{Irr}(\varepsilon, \mathbb{Q}, X) = X^3 - aX^2 + (a+1)X - 1 = -X^3 P_{-a}(1/X) = \mathrm{Irr}(1/\varepsilon_{-a}, \mathbb{Q}, X),$$

$$\mathrm{Irr}(\varepsilon, \mathbb{Q}, X) = X^3 - aX^2 + (a-1)X + 1 = -P_{a-2}(1-X) = \mathrm{Irr}(1-\varepsilon_{a-2}, \mathbb{Q}, X)$$

in which cases ε is one of the three real conjugates of some $\eta \in V_{\varepsilon_l}$, or

$$\mathrm{Irr}(\varepsilon, \mathbb{Q}, X) = X^3 - aX^2 + (a-3)X + 1 = X^3 Q_{a-3}(1/X) = \mathrm{Irr}(1/\theta_{a-3}, \mathbb{Q}, X),$$

in which case ε is one of the three real conjugates of some $\eta \in V_{\theta_m}$.

Since $P_{-l-3}(X) = -(X-1)^3 P_l(X/(X-1))$, we have $\mathrm{Irr}(\varepsilon_{-l-3}, \mathbb{Q}, X) = \mathrm{Irr}(\varepsilon_l/(\varepsilon_l - 1), \mathbb{Q}, X)$, and we may assume that $l \geq -1$. Since the discriminant $(l^2+3l-1)^2 - 32$ of $P_l(X)$ is positive if and only if $l \leq -5$ or $l \geq 2$, we may moreover assume that $l \geq 2$. In that case, this discriminant is a square if and only if $l = 2$, in which case $P_2(X) = -Q_{-1}(-X)$. Since $Q_{-m-3}(X) = X^3 Q_m(1/X)$, we have $\mathrm{Irr}(\theta_{-m-3}, \mathbb{Q}, X) = \mathrm{Irr}(1/\theta_m, \mathbb{Q}, X)$ and we may assume that $m \geq -1$. Finally, the discriminant $(m^2 + 3m + 9)^2$ of $Q_m(X)$ is a square. □

Hence, as in [Enn1], [Lou17] and [Lou20], consider the non-Galois totally real cubic number fields $\mathbb{Q}(\varepsilon_l)$, where

$$\mathrm{Irr}(\varepsilon_l, \mathbb{Q}) = X^3 + (l-1)X^2 - lX - 1 \qquad (l \geq 3)$$

is of positive and non-square discriminant

$$D_l = (l^2 + 3l - 1)^2 - 32.$$

Then ε_l is an exceptional unit, ε_l and $\varepsilon_l - 1$ are multiplicativily independent and the set $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of the totally real cubic order $\mathbb{Z}[\varepsilon_l]$, by [Tho, Proposition (3.6)]. Moreover, $\mathbb{Z}[\varepsilon_l]$ is equal to the ring of algebraic integers of $\mathbb{Q}(\varepsilon_l)$ whenever D_l is square-free. By the usual conjecture on square-free values of polynomials, see for example [Gr, Theorem 1], this should happen infinitely often with positive probability

$$\rho = \prod_p \left(1 - \frac{\omega(p^2)}{p^2}\right) = \frac{6}{7} \prod_{p \equiv \pm 1 \pmod 8} \left(1 - \frac{\omega(p)}{p^2}\right) = 0.839\cdots .$$

Here, $\omega(p^2)$ and $\omega(p)$ are the number of solutions mod p^2, respectively mod p, to the congruence $F(l) := (l^2 + 3l - 1)^2 - 32 \equiv 0 \pmod{p^2}$, respectively $F(l) \equiv 0 \pmod p$. Hence $\omega(p^2) \neq 0$ implies $p \equiv \pm 1 \pmod 8$, $\omega(7^2) = 7 \neq 1 = \omega(7)$ and $\omega(p^2) = \omega(p) \in \{0, 2, 4\}$ for $p > 7$, as $F(l)$ is of discriminant $-2^{14}7^3$ (Hensel's Lemma).

In [Enn1], V. Ennola conjectured that $\{\varepsilon_l, \varepsilon_l - 1\}$ is always a fundamental pair of units for the maximal order of $\mathbb{Q}(\varepsilon_l)$. He checked numerically that this conjecture holds true for $3 \leq l \leq 500$ and supported it by proving that the unit index

$$j_l := (\mathbb{U}_l : \langle -1, \varepsilon_l, \varepsilon_l - 1 \rangle)$$

of the groups of units generated by -1, ε_l and $\varepsilon_l - 1$ in the group of units $\mathbb{U}_l$ of the ring of algebraic integers of $\mathbb{Q}(\varepsilon_l)$ is always coprime to 2, 3 and 5. In [Lou17], we added a lot more credit to Ennola's conjecture by proving (i) that $\gcd(j_l, 19!) = 1$ for $l \geq 3$ and (ii) that $j_l = 1$ for $3 \leq l \leq 5 \cdot 10^7$ (not by using softwares for numerical computation with number fields like Pari GP, but by using Proposition 4 below). In [Lou20] we introduced new tools that enabled us to prove that for l effectively large enough, we have $\gcd(j_l, N!) = 1$ with $N = 97$. However, proving that $j_l = 1$ for l effectively large enough seems intractable at the moment.

The aim of this paper is to prove a weak form of Ennola's conjecture:

Theorem 2. *Assume that Conjectures 12 and 20 below hold true. Then for any given prime $p \geq 3$ there are only finitely many $l \geq 3$ for which p divides the unit index j_l. Hence, for any given integer $N \geq 2$ we have $\gcd(j_l, N!) = 1$ for $l \geq l_N$ effectively large enough.*

Conjectures 12 and 20 below assert that the explicit identities of Tables 1 and 2 in the ring of the Laurent polynomials

$$\mathbb{Q}[T,T^{-1}] := \left\{ \sum_{n\in\mathbb{Z}} q_n T^n;\ q_n \in \mathbb{Q} \text{ and } q_n = 0 \text{ for } |n| \text{ large enough} \right\}.$$

always hold true.
Notice that we do not need the full of these conjectures to be proved. The only part we need is the one on the expected degrees $N_{a,b}$ and $N_{a,b,m_{a,b}}$ of the $G_{a,b}(T)$'s and $G_{a,b,m_{a,b}}$'s as conjectured in Tables 1 and 3, where for $G(T) = \sum_{n\in\mathbb{Z}} q_n T^n \in \mathbb{Q}[T,T^{-1}]$ we set

$$\deg G(T) := \max\{n \in \mathbb{Z};\ q_n \neq 0\}.$$

This should not be that difficult to prove (see Conjecture 14). Maybe it could even be proved by using a formal language for algebraic computation. It is just that at the moment we have no brighter idea than to use the trinomial expansion formula

$$(x+y+z)^n = \sum_{i+j+k=n} \frac{n!}{i!j!k!} x^i y^j z^k$$

to expand each term $R_{a,b}(T)^u R_{-a,-b}(T)^v$ (or $S_{a,b}(T)^u S_{a,b}(1/T)^v$) and then collect all the terms in $G_{a,b}(T)$ of a given degree to check that those of non-negative degree cancel out and that it remains only few terms of negative degree. Nobody would want to read in extenso such a proof. Moreover, whereas it would enable us to check our formulae in Table 1, it would not explain why we end up with such simple results for the $G_{a,b}(T)$'s.

At least, for a given p is is rather easy to check that Conjectures 12 and 20 hold true. The hardest one to check is Conjecture 20 because the number of non-zero coefficients of $G_{a,b,p}(X,Y)$ increases rapidly with p and the computation of $G_{a,b,p}(X,Y)$ in the ring $\mathbb{Q}[T,T^{-1}]$ becomes slow and requires a lot of memory (see the proof of Theorem 21 for details). We stopped our computation at $p \leq 1875$ and obtain:

Theorem 3. *For any given odd prime $p \leq 1875$ there are only finitely many $l \geq 3$ for which p divides the unit index j_l.*

2 Ennola's conjecture follows from the ABC conjecture

Theorem 4 below makes Ennola's conjecture asserting that $j_l = 1$ for $l \geq 3$ a very reasonable conjecture, for its possible exceptions should be few and far between. We also used it in [Lou17, Proposition 5] with $p_0 = 7$ to prove that $j_l = 1$ for $3 \leq l \leq 5{\cdot}10^7$. We will finally use it with $p_0 = 5$ to prove Theorem 6, which asserts that Ennola's conjecture holds true for l large enough under the assumption of the ABC conjecture which asserts that

$$\mathrm{rad}(ABC) := \prod_{p|ABC} p \gg_\epsilon C^{1-\epsilon}$$

for any triples (A, B, C) of coprime positive integers satisfying $A + B = C$.

To begin with, let ε be a totally real cubic exceptional unit. Let D_ε be the discriminant of $\mathrm{Irrr}(\varepsilon, \mathbb{Q}, X)$ and I_ε be the index of $\mathbb{Z}[\varepsilon]$ in the ring of algebraic integers of $\mathbb{Q}(\varepsilon)$. Hence, $D_\varepsilon = I_\varepsilon^2 d_{\mathbb{Q}(\varepsilon)}$. Using [Cus] we obtained in [Lou17, proof of Theorem 2] that

$$j_\varepsilon \leq \frac{\mathrm{Reg}(\varepsilon, \varepsilon - 1)}{\frac{1}{16}\log^2(d_{\mathbb{Q}(\varepsilon)}/4)} = \frac{\mathrm{Reg}(\varepsilon, \varepsilon - 1)}{\frac{1}{16}\log^2(D_\varepsilon/4I_\varepsilon^2)}. \tag{1}$$

Now, (i) the ABC conjecture yields lower bounds on $d_{\mathbb{Q}(\varepsilon)}$ and upper bounds on I_ε for the parametrized families of exceptional units given in Proposition 1 and (ii) asymptotics for the regulators $\mathrm{Reg}(\varepsilon, \varepsilon - 1)$ are easy to obtain. Hence the ABC conjecture yields conditional upper bounds on j_ε. If we know beforehand that the primes p less than or equal to this conditional upper bound do not divide j_ε, at least for the parameter large enough, then we get that $j_\varepsilon = 1$, except possibly for finitely many cases.

2.1 The totally real non-normal cubic case

Theorem 4. *Assume that $p \nmid j_l$ for $2 \leq p < p_0$ and $l \geq 3$ (e.g. take $p_0 = 5$ by Proposition 8 or $p_0 = 23$ by [Lou17]), respectively for $2 \leq p < p_0$ and l large enough (e.g. take $p_0 = 101$ by [Lou20] or $p_0 = 1877$ by Theorem 3). Write the discriminant of $\mathrm{Irr}(\mathbb{Q}, \varepsilon_l, X)$ as $D_l = (l^2+3l-1)^2-32 = a_l b_l^2$, with $a_l > 1$ square-free and $1 \leq b_l \leq l^2$. If $b_l \leq l^{2-2/\sqrt{p_0}}/2$ then $j_l = 1$ and $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of the ring of algebraic integers of $\mathbb{Q}(\varepsilon_l)$ for $l \geq 3$, respectively for l large enough.*

Proof. Since $D_l = I_{\varepsilon_l}^2 d_{\mathbb{Q}(\varepsilon_l)} = a_l b_l^2$ and a_l is square-free, it follows that I_{ε_l} divides b_l. Hence, $I_{\varepsilon_l} \leq b_l$. Now, $j_l = 1$ if $I_{\varepsilon_l} \leq l^{2-2/\sqrt{p_0}}/2$, by [Lou17, Theorem 2] (notice that [Enn2] gives $j_l = 1$ only if $I_{\varepsilon_l} \leq l/3$). □

Lemma 5. *Assume that the ABC conjecture holds true. Let $g(X) \in \mathbb{Z}[X]$ be of non-zero discriminant. Fix $\epsilon > 0$. Then $b_l \ll_\epsilon |l|^{1+\epsilon}$, where $g(l) = a_l b_l^2$ with a_l square-free.*

Proof. First, $a_l \ll |l|^d/b_l^2$, where $d = \deg g(X)$. By [Gr, Corollary 1], under the assumption of ABC conjecture, we have $a_l b_l \geq \prod_{p|g(l)} p \gg |l|^{d-1-\epsilon}$. Hence, $|l|^d/b_l \gg |l|^{d-1-\epsilon}$ and the desired first result follows. □

Theorem 6. *Assume that the ABC conjecture holds true. Fix an algebraic closure of $\mathbb{Q}$. Then, $j_l = 1$ for l large enough. Hence, by Proposition 1, if ε is a non-normal totally real cubic exceptional unit then $\{\varepsilon, \varepsilon - 1\}$ is a system of fundamental units of the cubic number field $\mathbb{Q}(\varepsilon)$, except possibly for finitely many cases.*

Proof. Now, take $g(X) = (X^2 + 3X - 1)^2 - 32$ and $\epsilon < 1 - 2/\sqrt{5}$. We have $1 + \epsilon < 2 - 2/\sqrt{5}$. Therefore, for l large enough we have $b_l \leq l^{2-2/\sqrt{5}}/2$ and $j_l = 1$, by Theorem 4 applied with $p_0 = 5$. (Notice that since Lemma 5 does not yield $b_l \ll |l|$, [Enn2] is not good enough to prove this Theorem 6). □

2.2 The totally real normal cubic case

According to Proposition 1, consider

$$\mathrm{Irr}(\theta_m, \mathbb{Q}, X) = X^3 + mX^2 - (m+3)X + 1 \qquad (m \geq -1),$$

of discriminant $D_m = f_m^2$ with $f_m = m^2 + 3m + 9$. Write $f_m = b_m c_m^3$, with b_m cube-free. Then $d_{\mathbb{Q}(\theta_m)} \geq \mathrm{rad}(b_m)^2$, with $\mathrm{rad}(b_m) := \prod_{p|b_m} p$, by [Was, Proposition 1 and its proof]. Fix $\epsilon > 0$ By [Gr, Corollary 1], under the assumption of ABC conjecture, we have

$$\begin{aligned} m^{1-\epsilon/6} &\ll \mathrm{rad}(f_m) \\ &= \mathrm{rad}(b_m c_m) \leq \mathrm{rad}(b_m)\mathrm{rad}(c_m) \ll \mathrm{rad}(b_m)\left(m^2/\mathrm{rad}(b_m)\right)^{1/3} \end{aligned}$$

and $\mathrm{rad}(b_m) \gg m^{(1-\epsilon)/2}$, by using $\mathrm{rad}(b_m)\mathrm{rad}(c_m)^3 \leq b_m c_m^3 = f_m \ll m^2$. Hence, $d_{\mathbb{Q}(\theta_m)} \geq \mathrm{rad}(b_m)^2 \gg m^{1-\epsilon}$. Now, as in [Lou17, proof of Theorem 2] it is readily seen that $\mathrm{Reg}(\theta_m, \theta_m - 1) \leq \left(\log m + \frac{2}{m}\right)^2$ for $m \geq 1$. Hence, by (1) we obtain $j_{\theta_m} < p_0 = 17$ for m large enough. Now, by [Lou20, Lemmas 12, 13], we know that if $p < 17$ divides j_{θ_m} for some $m \geq -1$, then $p \in \{3, 7, 13\}$. By [Lou20, Theorems 17, 18] we know that neither 3 nor 7 divides j_{θ_m} for $m > 5$. Finally, by [Lou20, Remark 20] we know that 13 does not divide j_{θ_m} for m large enough. Hence we have:

Theorem 7. *Assume that the ABC conjecture holds true. Fix an algebraic closure of $\mathbb{Q}$. If ε is a normal totally real cubic exceptional unit then $\{\varepsilon, \varepsilon - 1\}$ is a system of fundamental units of the cubic number field $\mathbb{Q}(\varepsilon)$, except possibly for finitely many cases.*

Notice that contrary to the non-normal cubic case where no example of $j_{\varepsilon_l} > 1$ are known, here 7 values of m for which $j_{\theta_m} > 1$ are known:

m	3	5	12	54	66	1259	2389
j_{θ_m}	3	7	13	19	13	97	31

3 How to prove that p does not divide j_l

To begin with, recall (see [Lou17, Proposition 10] or [Lou20, Proposition 3]):

Proposition 8. *Assume that $l \geq 3$. The prime numbers 2 and 3 never divide the unit index j_l and an odd prime number $p \geq 5$ divides j_l if and only if one of the $p-4$ units $\varepsilon_l^k(\varepsilon_l - 1)$ is a pth power in $\mathbb{Q}(\varepsilon_l)$, where $2 \leq k \leq p-3$.*

Corollary 9. *Let $p \geq 5$ a prime. Let*

$$E_p := \{(a_n, b_n);\ 1 \leq n \leq p-4\} \subseteq \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}$$

be a set of pairs of coprime rational integers with $p \nmid b$ such that

$$\mathbb{Z}/p\mathbb{Z} \setminus \{0, 1, p-2, p-1\} = \{a_n/b_n;\ 1 \leq n \leq p-4\}.$$

Then, p divides j_l if and only if one of the $p-4$ units

$$\varepsilon_{a,b} = (-1)^{a+b}\varepsilon_l^a(\varepsilon_l - 1)^b$$

is a pth power in $\mathbb{Q}(\varepsilon_l)$, where $(a, b) \in E_p$.

Proof. The unit $\varepsilon_l^k(\varepsilon_l - 1)$ is a pth power if and only so is any $\varepsilon_l^{kb}(\varepsilon_l - 1)^b$ for b not divisible by p, hence if and only if so is $\varepsilon_l^a(\varepsilon_l - 1)^b$ for b not divisible by p and any a verifying $a \equiv kb \pmod{p}$. Since $-1 = (-1)^p$ is a pth power, the desired result follows. □

According to the following result known as Thue's Lemma, we can find a set E_p such that $(a, b) \in E_p$ implies $\max(|a|, |b|) \leq \sqrt{p}$:

Lemma 10. *(See also [LM]). For any k not divisible by a prime $p \geq 3$, there exist a and $b \neq 0$ such that $a \equiv kb \pmod{p}$ and $0 < \max(|a|, |b|) \leq \sqrt{p}$.*

Proof. The set $F_p := \{(x, y) \in \mathbb{Z}^2;\ 0 \leq x, y \leq g := \lfloor\sqrt{p}\rfloor\}$ contains $(g+1)^2 > p$ elements. Thus, 2 of the $(g+1)^2$ elements $x - yk$'s are equal mod p when (x, y) range over F_p, say $x - yk \equiv x' - y'k \pmod{p}$ with $(x, y) \neq (x', y')$. Then $x - x' \equiv (y - y')k \pmod{p}$, with $|x - x'| \leq g < p$ and $|y - y'| \leq g < p$. Hence, $b = y - y' \neq 0$ and the desired result follows. □

In the present paper we will need to prove that we can find a set E_p such that $(a, b) \in E_p$ implies $a^2 + ab + b^2 \leq p$ (Proposition 16). The number of points $(a, b) \in \mathbb{Z}^2$ satisfying $\max(|a|, |b|) \leq \sqrt{p}$ is asymptotic to $4p$. The number of those satisfying $a^2 + ab + b^2 \leq p$ is asymptotic to $\frac{2\pi}{\sqrt{3}}p$, where $\frac{2\pi}{\sqrt{3}} < 4$. Hence, Proposition 16 below is stronger than Thue's Lemma.

We now explain how we prove that a given unit $\varepsilon_{a,b} = (-1)^{a+b}\varepsilon_l^a(\varepsilon_l - 1)^b$ is not a pth power in $\mathbb{Q}(\varepsilon_l)$ for $p \geq B_{a,b}$ and $l \geq l_{a,b,p}$ effectively large enough. Notice that the rational fractions $R_{a,b}(T)$, $G_{a,b}(T)$, $R_{a,b,m}(T)$ and $G_{a,b,m}(T)$ that crop up in this paper are in the ring $\mathbb{Q}[T, T^{-1}]$ of Laurent polynomials.

Proposition 11. *Let $a, b \in \mathbb{Z}$ not both equal to 0 be given.*
Set $s = \max(a+b, -a, -b) \geq 0$, $t = \max(-a-b, a, b) \geq 0$ and

$$R_{a,b}(T) := T^{-a} + (-1)^{a+b} T^{-b} + T^{a+b} \in \mathbb{Q}(T).$$

Suppose there exists $0 \neq F_{a,b}(X,Y) = \sum_{u,v} f_{u,v} X^u Y^v \in \mathbb{Z}[X,Y]$ such that

$$G_{a,b}(T) := F_{a,b}\left(R_{a,b}(T), R_{-a,-b}(T)\right) = F_{a,b}\left(R_{a,b}(T), R_{a,b}(1/T)\right) \in \mathbb{Z}[T, T^{-1}]$$

is of negative degree. Set

$$M_{a,b} = \max\{us + vt;\ f_{u,v} \neq 0\}$$

and

$$N_{a,b} = -\deg G_{a,b}(T) \geq 1.$$

Then for any given odd prime

$$p \geq B_{a,b} := M_{a,b} + N_{a,b} + 1$$

the unit $\varepsilon_l^a (\varepsilon_l - 1)^b$ is not a pth power in $\mathbb{Q}(\varepsilon_l)$ for $l \geq l_{a,b,p} := w_{a,b}^p$ effectively large enough, for some effective $w_{a,b} > 1$ not depending on p.

Proof. If α, α' and α'' are the three conjugates of a totally real cubic algebraic number α and $m \geq 3$ is an odd integer, we set

$$S_m(\alpha) = \alpha^{1/m} + \alpha'^{1/m} + \alpha''^{1/m} \in \mathbb{R}. \tag{2}$$

Hence, $S_m(\alpha) \in \mathbb{Z}$ if α in a mth power in $\mathbb{Q}(\alpha)$. Set $\varepsilon = (-1)^{a+b} \varepsilon_l^a (\varepsilon_l - 1)^b$. Let $p \geq 3$ be given. Set $w := l^{1/p} > 1$. Letting θ stand for an effective real number such that $0 \leq \theta \leq 1$, not necessarily the same at different places, the three conjugates of ε_l satisfy

$$\begin{array}{ll} \varepsilon_l = -l(1 - \theta l^{-1}) & \varepsilon_l - 1 = -l\,(1 + \theta l^{-1}) \\ \varepsilon_l' = -l^{-1}(1 - \theta l^{-1}) & \varepsilon_l' - 1 = -(1 + \theta l^{-1}) \\ \varepsilon_l'' = 1 + \theta l^{-1} & \varepsilon_l'' - 1 = l^{-1}(1 - 2\theta l^{-1}) \end{array}$$

(evaluate $\mathrm{Irr}(\varepsilon_l, \mathbb{Q}) = X^3 + (l-1)X^2 - lX - 1$ at $-l$ and $-l+1$, at $-l^{-1}$ and $-l^{-1} + l^{-2}$ and at 1 and $1 + l^{-1}$ to check sign changes and do the same for $\mathrm{Irr}(\varepsilon_l - 1, \mathbb{Q}) = X^3 + (l+2)X^2 + (l+1)X - 1$).
Hence, with the notation in (2), as l goes to infinity we have

$$S_p(\varepsilon) = R_{a,b}(w) + O(w^{s-p}) \text{ and } S_p(1/\varepsilon) = R_{-a,-b}(w) + O(w^{t-p}).$$

For $P(X,Y) = X^u Y^v$ with $u, v \geq 0$ we thus have

$$P(S_p(\varepsilon), S_p(1/\varepsilon)) = P(R_{a,b}(w), R_{-a,-b}(w)) + O(w^{us+vt-p}).$$

Hence,

$$\begin{aligned} F_{a,b}(S_p(\varepsilon), S_p(1/\varepsilon)) &= G_{a,b}(w) + O(w^{M_{a,b}-p}) \\ &= q_{N_{a,b}} w^{-N_{a,b}} + O(w^{-N_{a,b}-1}) + O(w^{M_{a,b}-p}), \end{aligned}$$

where $q_{N_{a,b}} \neq 0$. Now assume that $p \geq M_{a,b} + N_{a,b} + 1$. We obtain

$$0 < |F_{a,b}(S_p(\varepsilon), S_p(1/\varepsilon))| < 1$$

if $w \geq w_{a,b} > 1$ is effectively large enough, i.e. if $l = w^p \geq w_{a,b}^p = l_p$ is effectively large enough. Since $S_p(\varepsilon) \in \mathbb{Z}$ and $S_p(1/\varepsilon) \in \mathbb{Z}$ and hence $F_{a,b}(S_p(\varepsilon), S_p(1/\varepsilon)) \in \mathbb{Z}$ whenever $\varepsilon = \eta^p$ is a pth power in $\mathbb{Q}(\varepsilon_l)$, we get the desired result. □

4 Conjectural suitable polynomials $F_{a,b}(X, Y)$

In [Enn1] and [Lou17] the authors laboriously constructed some such suitable polynomials $F_{a,b}(X, Y) \in \mathbb{Z}[X, Y]$ for small values of a, b. After that, we wrote an (unpublished) algorithm which for given a and b yields such a $F_{a,b}(X, Y) \in \mathbb{Z}[X, Y]$. After the computation of a lot of them for various choices of a and b and a lengthly research of some pattern in those $F_{a,b}(X, Y)$'s, we came up in [Lou20, Table 1] with a guess for an explicit formula for such $F_{a,b}(X, Y)$'s. Finally, after the acceptance for publication of [Lou20], we realized that when we computed the $B_{a,b}$'s defined in Proposition 11 for these $F_{a,b}(X, Y)$'s in Table 1, we almost always got $B_{a,b} = a^2 + ab + b^2 + 1$. We have also just now realized that with the notation of [Lou20, Lemma 8] we have $V_d(X, Y) = -P_d(-Y, X)$!! Hence, we have now Conjecture 12 which is much clearer and more complete than [Lou20, Conjecture 7] and from which we will deduce Theorem 18. Conjecture 12 can be checked easily on a given pair (a, b) by using any formal language for computation (we checked it on a MacBook Air laptop computer using Maple in 3120 seconds for $\max(|a|, b) \leq 50$):

Conjecture 12. *Let $(a, b) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}$, with $a + b \neq 0$. For $d \geq 1$, set*

$$P_d(X, Y) = d \sum_{\substack{k,l \geq 0 \\ 0 \leq 2k+3l \leq d}} (-1)^{k-1} \binom{k+l}{k} \binom{d-k-2l}{k+l} \frac{X^k Y^{d-2k-3l}}{d-k-2l} \in \mathbb{Z}[X, Y].$$

(with the convention $0! = 1$). Let $F_{a,b}(X, Y) \in \mathbb{Z}[X, Y]$ be as in Table 1. Keep the notation of Proposition 11. Then, $M_{a,b}$ and

$$G_{a,b}(T) := F_{a,b}(R_{a,b}(T), R_{-a,-b}(T)) = F_{a,b}\left(R_{a,b}(T), R_{a,b}(1/T)\right) \in \mathbb{Z}[T, T^{-1}]$$

are as in Table 1. In particular, $G_{a,b}(T)$ is of negative degree and

$$B_{a,b} = a^2 + ab + b^2 + 1,$$

except if $a = -2b$ with $b \geq 1$ odd, in which case $B_{a,b} = B_{-2b,b} = 6b^2 + 1$.

The fact that $P_d(X, Y)$ is in $\mathbb{Z}[X, Y]$ follows from the identity

$$\frac{k+2l}{d-k-2l} \binom{k+l}{k} \binom{d-k-2l}{k+l} = \left\{ \binom{k-1+l}{l} + 2 \binom{k+l-1}{k} \right\} \times \binom{d-k-2l-1}{k+l-1}.$$

Notice that with the notation of Proposition 11, we have $s = \deg R_{a,b}(T)$ and $t = \deg R_{-a,-b}(T)$, except in the case that $a = -2b$ with $b \geq 1$ odd, in which case $s = 2b = \deg R_{a,b}(T)$ but $t = b \neq -2b = \deg R_{-a,-b}(T)$.

Table 1: Conjecture for $F_{a,b}(X,Y)$,
for $a \neq 0$, $b \geq 1$ and $c := a + b \neq 0$

1. $a \geq 1$ odd and $b \geq 1$ odd $F_{a,b}(X,Y) = -P_a(Y,X) - P_b(Y,X) + P_c(X,Y)$, $M_{a,b} = c\max(a,b)$, $G_{a,b}(T) = T^{-a^2} + T^{-b^2} - T^{-c^2} + 2T^{-ab}$ for which $N_{a,b} = \min(a,b)^2$.
2. $a \leq -1$ odd, $b \geq 1$ odd and $c > 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(X,Y) - P_b(Y,X) + P_c(X,Y)$, $M_{a,b} = b\max(\lvert a\rvert, c)$, $G_{a,b}(T) = -T^{-a^2} + T^{-b^2} - T^{-c^2} - 2T^{-\lvert a\rvert c}$ for which $N_{a,b} = \min(\lvert a\rvert, c)^2$.
3. $a \leq -1$ odd, $b \geq 1$ odd and $c < 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(X,Y) - P_b(Y,X) - P_{\lvert c\rvert}(Y,X)$, $M_{a,b} = \lvert a\rvert\max(b,\lvert c\rvert)$, $G_{a,b}(T) = -T^{-a^2} + T^{-b^2} + T^{-c^2} + 2T^{-b\lvert c\rvert}$ for which $N_{a,b} = \min(b,\lvert c\rvert)^2$.

Table 1 (continued)

4. $a \geq 1$ odd, $b \geq 1$ even $F_{a,b}(X,Y) = -P_a(-Y,-X) - P_b(-Y,-X) + P_c(-X,-Y)$, $M_{a,b} = c\max(a,b)$, $G_{a,b}(T) = -T^{-a^2} + T^{-b^2} + T^{-c^2} + 2T^{-ab}$ for which $N_{a,b} = \min(a,b)^2$.
5. $a \leq -1$ odd, $b \geq 1$ even and $c > 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(-X,-Y) - P_b(-Y,-X) + P_c(-X,-Y)$, $M_{a,b} = b\max(\lvert a\rvert, c)$, $G_{a,b}(T) = T^{-a^2} + T^{-b^2} + T^{-c^2} + 2T^{-\lvert a\rvert c}$ for which $N_{a,b} = \min(\lvert a\rvert, c)^2$.
6. $a \leq -1$ odd, $b \geq 1$ even and $c < 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(-X,-Y) - P_b(-Y,-X) - P_{\lvert c\rvert}(-Y,-X)$, $M_{a,b} = \lvert a\rvert\max(b,\lvert c\rvert)$, $G_{a,b}(T) = T^{-a^2} + T^{-b^2} - T^{-c^2} + 2T^{-b\lvert c\rvert}$ for which $N_{a,b} = \min(b,\lvert c\rvert)^2$.

Table 1 (continued)

7. $a \geq 2$ even, $b \geq 1$ odd $F_{a,b}(X,Y) = -P_a(-Y,-X) - P_b(-Y,-X) - P_c(-X,-Y)$, $M_{a,b} = c\max(a,b)$, $G_{a,b}(T) = T^{-a^2} + T^{-b^2} - T^{-c^2}$ for which $N_{a,b} = \min(a,b)^2$.
8. $a \leq -2$ even, $b \geq 1$ odd and $c > 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(-X,-Y) + P_b(-Y,-X) + P_c(-X,-Y)$, $M_{a,b} = b\max(\lvert a\rvert, c)$, $G_{a,b}(T) = -T^{-a^2} - T^{-b^2} + T^{-c^2}$ for which $N_{a,b} = \min(\lvert a\rvert, c)^2$.
9. $a \leq -2$ even, $b \geq 1$ odd and $c < 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(-X,-Y) + P_b(-Y,-X) + P_{\lvert c\rvert}(-Y,-X)$, $M_{a,b} = \lvert a\rvert\max(b,\lvert c\rvert)$, $G_{a,b}(T) = -T^{-a^2} - T^{-b^2} + T^{-c^2}$ for which $N_{a,b} = \begin{cases} \min(b,\lvert c\rvert)^2 & \text{if } a \neq -2b, \\ 4b^2 & \text{if } a = -2b. \end{cases}$

Table 1 (continued)

10. $a \geq 2$ even, $b \geq 1$ even $F_{a,b}(X,Y) = -P_a(Y,X) - P_b(Y,X) + P_c(X,Y)$, $M_{a,b} = c\max(a,b)$, $G_{a,b}(T) = T^{-a^2} + T^{-b^2} - T^{-c^2} + 2T^{-ab}$ for which $N_{a,b} = \min(a,b)^2$.
11. $a \leq -2$ even, $b \geq 1$ even and $c > 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(X,Y) - P_b(Y,X) + P_c(X,Y)$, $M_{a,b} = b\max(\lvert a\rvert, c)$, $G_{a,b}(T) = -T^{-a^2} + T^{-b^2} - T^{-c^2} - 2T^{-\lvert a\rvert c}$ for which $N_{a,b} = \min(\lvert a\rvert, c)^2$.
12. $a \leq -2$ even, $b \geq 1$ even and $c < 0$ $F_{a,b}(X,Y) = P_{\lvert a\rvert}(X,Y) - P_b(Y,X) - P_{\lvert c\rvert}(Y,X)$, $M_{a,b} = \lvert a\rvert\max(b,\lvert c\rvert)$, $G_{a,b}(T) = -T^{-a^2} + T^{-b^2} + T^{-c^2} + 2T^{-b\lvert c\rvert}$ for which $N_{a,b} = \min(b,\lvert c\rvert)^2$.

Remark 13. *Cases* **11** *and* **12** *in Table 1 correct the awkward last two cases in [Lou20, Table 1]. This awkwardness has in fact no impact on the results obtained in [Lou20] where one deals only with coprime integers a and b.*
In fact, here again we deal with pairs of coprime integers, by Corollary 9. Hence, we do not even need cases **10-11-12** *of the present Table 1.*

Conjecture 12 would be a consequence of the behavior of the $P_d(X,Y)$'s:

Conjecture 14. *Let $a, b \in \mathbb{Z}$ be such that $a \neq 0$, $b \neq 0$ and $c := a + b \neq 0$. Set $S_{a,b}(T) := T^{-a} + T^{-b} + T^{a+b}$. Let $P_d(X,Y) \in \mathbb{Z}[X,Y]$ be as in Conjecture 12. Then*

$$P_{|d|}(S_{a,b}(T), S_{a,b}(1/T)) = -S_{a,b}(1/T^{|d|}) \text{ for } d \in \{a,b,c\}.$$

Moreover, if a is even and b is odd, then with $R_{a,b}(T) := T^{-a} - T^{-b} + T^{a+b}$ we have

$$P_{|d|}(-R_{a,b}(T), -R_{a,b}(1/T)) = \begin{cases} -S_{a,b}(1/T^{|d|}) & \text{if } d = a, \\ R_{a,b}(1/T^{|d|}) & \text{if } d \in \{b,c\}. \end{cases}$$

Proposition 15. *Assume that Conjecture 14 holds true. Let the $F_{a,b}(X,Y)$'s be as in Table 1. Then $G_{a,b}(T) := F_{a,b}(R_{a,b}(T), R_{a,b}(1/T))$ is as Table 1.*

Proof. For example, in case **1** of Table 1, we have $R_{a,b}(T) = S_{a,b}(T)$ and taking $F_{a,b}(X,Y)$ as given in Table 1 and using Conjecture 14 we do obtain

$$\begin{aligned} G_{a,b}(T) &= F_{a,b}\left(R_{a,b}(T), R_{a,b}(1/T)\right) \\ &= -P_a(R_{a,b}(1/T), R_{a,b}(T)) - P_b(R_{a,b}(1/T), R_{a,b}(T)) + P_c(R_{a,b}(T), R_{a,b}(1/T)) \\ &= -P_a(S_{a,b}(1/T), S_{a,b}(T)) - P_b(S_{a,b}(1/T), S_{a,b}(T)) + P_c(S_{a,b}(T), S_{a,b}(1/T)) \\ &= S_{a,b}(T^a) + S_{a,b}(T^b) - S_{a,b}(T^{-c}) \\ &= (T^{-a^2} + T^{-ab} + T^{ac}) + (T^{-ab} + T^{-b^2} + T^{bc}) - (T^{ac} + T^{bc} + T^{-c^2}) \\ &= T^{-a^2} + T^{-b^2} - T^{-c^2} + 2T^{-ab}. \end{aligned}$$

In the same way, as a second example, in case **9** of Table 1, taking $F_{a,b}(X,Y)$ as given in Table 1 and using Conjecture 14 we do obtain

$$\begin{aligned} G_{a,b}(T) &= F_{a,b}\left(R_{a,b}(T), R_{a,b}(1/T)\right) \\ &= P_{|a|}(-R_{a,b}(T), -R_{a,b}(1/T)) + P_b(-R_{a,b}(1/T), -R_{a,b}(T)) + P_{|c|}(-R_{a,b}(1/T), -R_{a,b}(T)) \\ &= -S_{a,b}(1/T^{|a|}) + R_{a,b}(T^b) + R_{a,b}(T^{|c|}) \\ &= -S_{a,b}(T^a) + R_{a,b}(T^b) + R_{a,b}(T^{-c}) \\ &= -(T^{-a^2} + T^{-ab} + T^{ac}) + (T^{-ab} - T^{-b^2} + T^{bc}) + (T^{ac} - T^{bc} + T^{-c^2}) \\ &= -T^{-a^2} - T^{-b^2} + T^{-c^2}. \end{aligned}$$

Cases -2-8 being treated in the same way we obtain the following Table:

Cases	$G_{a,b}(T)$
1 and 10	$S_{a,b}(T^a) + S_{a,b}(T^b) - S_{a,b}(T^{-c})$
2 and 11	$-S_{a,b}(T^a) + S_{a,b}(T^b) - S_{a,b}(T^{-c})$
3 and 12	$-S_{a,b}(T^a) + S_{a,b}(T^b) + S_{a,b}(T^{-c})$
4	$S_{a,b}(-T^a) + S_{a,b}(T^b) - S_{a,b}(-T^{-c})$
5	$-S_{a,b}(-T^a) + S_{a,b}(T^b) - S_{a,b}(-T^{-c})$
6	$-S_{a,b}(-T^a) + S_{a,b}(T^b) + S_{a,b}(-T^{-c})$
7	$S_{a,b}(T^a) - R_{a,b}(T^b) - R_{a,b}(T^{-c})$
8	$-S_{a,b}(T^a) + R_{a,b}(T^b) + R_{a,b}(T^{-c})$
9	$-S_{a,b}(T^a) + R_{a,b}(T^b) + R_{a,b}(T^{-c})$

The desired result follows. □

5 Proof of Theorem 2

Theorem 2 will follow from Theorems 18 and 21 below. Theorem 18 is a consequence of Proposition 11, Conjecture 12 and the first point of Corollary 17. Theorem 21 is a consequence of Proposition 11 and Conjecture 12, Proposition 19, and Conjecture 20 and the second point of Corollary 17.

Set $Q_{-3}(x,y) = x^2 + xy + y^2$. After having proved Proposition 11 and formulated Conjecture 12, we wrote a program which for a given prime p and for any $k \in \{2, \cdots, p-3\}$ computes some $(a_k, b_k) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}$ such that

$$Q_{-3}(a_k, b_k) = \min\{Q_{-3}(a,b); (a,b) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1},\ p \nmid b,\ a \equiv kb \pmod{b}\}.$$

We then computed $Bound(p) = \max\{Q_{-3}(a_k, b_k);\ 2 \leq k \leq p-3\}$ for various p's. We hoped that we would always have $Bound(p) \leq p-1$, in which case, by Corollary 9, Proposition 11 and Conjecture 12, we would have conditionally proved Theorem 2. We readily guessed Proposition 16 (which does not always hold true with the better bound $a^2 + ab + b^2 \leq p-1$, by Corollary 17):

Proposition 16. *For any k not divisible by a prime $p \geq 5$, there exist a and $b \geq 1$ such that $a \equiv kb \pmod{p}$ and $0 < a^2 + ab + b^2 \leq p$, which implies $p \nmid b$.*

Proof. Consider the quadratic form $Q_{-3}(X,Y) = X^2 + XY + Y^2$ and the lattice $L_k = \{(a,b) \in \mathbb{Z}^2;\ a \equiv kb \pmod{p}\} = \mathbb{Z}e_1 + \mathbb{Z}e_2$, where $e_1 = (k,1)$ and $e_2 = (p,0)$. We want to find $0 \neq e \in L_k$ such that $Q_{-3}(e) \leq p$.
Consider the quadratic form $Q(e) = Q(x,y) = Q_{-3}(kx+py, x) = Ax^2 + Bxy + Cy^2 = (k^2+k+1)x^2 + (2k+1)pxy + p^2y^2$ of discriminant $\Delta = B^2 - 4AC = -3p^2$, where $e = xe_1 + ye_2 = (kx+py, x) \in L_k$.
Let $e_1' \in L_k$ be such that $Q(e_1') = \min\{Q(e);\ 0 \neq e \in L_k\}$ and $e_2' \in L_k$ be such that $Q(e_2') = \min\{Q(e);\ e \in L_k \setminus \mathbb{Z}e_1'\}$. Then $\{e_1', e_2'\}$ is a $\mathbb{Z}$-basis of L_k and if $e = xe_1 + ye_2 = x'e_1' + y'e_2' \in L_k$, then $Q(e) = Q(x,y) = Q'(x',y') = A'x'^2 + B'x'y' + C'y'^2$ is a quadratic form in x', y' of the same discriminant $\Delta' = B'^2 - 4A'C' = -3p^2 = \Delta$ as the quadratic form Q.
The key point is that Q' is reduced, i.e. that $0 \leq |B'| \leq A' \leq C'$. Indeed, $A' =$

$Q'(1,0) = Q(e'_1) \leq Q(e'_2) = Q'(0,1) = C'$ yields $A' \leq C'$ and $C' = Q(e'_2) \leq Q(e'_1 \pm e'_2) = A' \pm B' + C'$ yields $|B'| \leq A'$.
Hence, $3p^2 = 4B'C' - A'^2 \geq 4A'^2 - A'^2 = 3A'^2 = 3Q'(1,0)^2 = 3Q(e'_1)^2$ and $0 < Q(e'_1) \leq p$. The desired result follows. □

Corollary 17. *Let $p \geq 5$ be a prime integer.*

1. *Assume that $p \equiv 5 \pmod 6$. For any k not divisible by p there exist a and b not divisible by p such that $a \equiv kb \pmod p$ and $0 < a^2 + ab + b^2 \leq p - 1$. Hence, there exists a set $E_p \subseteq \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}$ as defined in Corollary 9 such that $(a, b) \in E_p$ implies $0 < a^2 + ab + b^2 \leq p - 1$.*

2. *Assume that $p \equiv 1 \pmod 6$. Write $p = A^2 + AB + B^2$, with $A > B \geq 1$ (in a unique way). Let k_1 and k_2 be such that $A \equiv k_1 B \pmod p$ and $B \equiv k_2 A \pmod p$. (i.e. k_1 mod p and k_2 mod p are the two non trivial cubic roots of unity mod p). Then k_1 mod p and k_2 mod p are the only k mod p not divisible by p for which there do not exist a and b not divisible by p such that $kb \equiv a \pmod p$ and $0 < a^2 + ab + b^2 \leq p - 1$. Hence, there exists a set $E_p \subseteq \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}$ with $p - 4$ elements as defined in Corollary 9 such that $(a, b) \in E_p$ implies $0 < a^2 + ab + b^2 \leq p - 1$ for $p - 6$ of its elements and $a^2 + ab + b^2 = p$ for its remaining 2 elements $(a, b) \in \{(A, B), (B, A)\}$.*

Proof. Suppose there exists some k not divisible by p for which there do not exist a and b not divisible by p such that $kb \equiv a \pmod p$ and $a^2 + ab + b^2 \leq p - 1$. By Proposition 16, there exist a and b not divisible by p such that $kb \equiv a \pmod p$ and $a^2 + ab + b^2 = p$. Then $b^2(k^2 + k + 1) \equiv a^2 + ab + b^2 \equiv 0 \pmod p$, hence $k^2 + k + 1 \equiv 0 \pmod p$ and the image of k in $(\mathbb{Z}/p\mathbb{Z})^*$ is of order 3 in this multiplicative group of order $p - 1$. Hence, 3 divides $p - 1$ and $p \equiv 1 \pmod 6$, which proves the first assertion. Conversely, suppose that $p \equiv 1 \pmod 6$ and k is a solution of the congruence $k^2 + k + 1 \equiv 0 \pmod p$. Then p does not divide k and if $kb \equiv a \pmod b$ with a and b not divisible by p, then $a^2 + ab + b^2 \equiv b^2(k^2 + k + 1) \equiv 0 \pmod p$ and hence $a^2 + ab + b^2 \geq p$ (notice that for a and b not both equal to 0 we have $a^2 + ab + b^2 > 0$). □

5.1 Proof of Theorem 2 for $p \equiv 5 \pmod 6$

The first point of Corollary 17 and Proposition 11 yield:

Theorem 18. *Let $p \equiv 5 \pmod 6$ be a given prime. Assume that Conjecture 12 holds true for the $p - 4$ pairs (a, b) in a set E_p as in the first point of Corollary 17. Then p does not divide the unit index j_l for l effectively large enough. In particular, if $p \equiv 5 \pmod 6$ is a prime less than 1875, then p does not divide the unit index j_l for l effectively large enough.*

Proof. We checked that Conjecture 12 holds true in the range $1 \leq \max(|a|, b) \leq 50$ on a MacBook Air laptop computer, using Maple. This computation took 52 minutes. Since $a^2 + ab + b^2 \leq p$ implies $\max(|a|, |b|) \leq \sqrt{4p/3}$, Theorem 18 holds true for all the primes $p \equiv 5 \pmod 6$ less than 1875. □

5.2 Proof of Theorem 2 for $p \equiv 1 \pmod 6$

Let $p \equiv 1 \pmod 6$ be a prime. By the second point of Corollary 17 and Proposition 11, it remains to prove that $\epsilon_{a,b}$ is not pth powers in $\mathbb{Q}(\varepsilon_l)$, where a and b are such that $p = a^2 + ab + b^2$. For dealing with such occurrences we will use the following modification of Proposition 11 (notice that for given a and b, Proposition 11 deals with all the odd integers large enough, whereas Proposition 19 deals with only one odd integer at a time):

Proposition 19. *Let $a, b \in \mathbb{Z}$ not both equal to 0 be given. Let $m \geq 3$ be odd. Let the notation be as in Proposition 11. Set*

$$R_{a,b,m}(T) = R_{a,b}(T) + \frac{b-a}{m}T^{-a-m} + (-1)^{a+b}\frac{a-2b}{m}T^{-b-m} + \frac{b}{m}T^{a+b-m}.$$

Assume that

$$G_{a,b,m}(T) = F_{a,b}\left(R_{a,b,m}(T), R_{-a,-b,m}(T)\right) \in \mathbb{Q}[T, T^{-1}]$$

is of negative degree. Set $N_{a,b,m} = -\deg G_{a,b,m}(T) \geq 1$ and

$$B_{a,b,m} := (M_{a,b} + N_{a,b,m} + 1)/2.$$

If $B_{a,b,m} \leq m$, then the unit $\varepsilon_{a,b} = (-1)^{a+b}\varepsilon_l^a(\varepsilon_l - 1)^b$ is not a mth power in $\mathbb{Q}(\varepsilon_l)$ for $l \geq l_m$ effectively large enough.

Proof. The proof is similar to that of Proposition 11, except that we now use

$$\begin{array}{ll} \varepsilon_l = -l(1-\theta l^{-2}) & \varepsilon_l - 1 = -l\left(1 + l^{-1} - \theta l^{-2}\right)) \\ \varepsilon_l' = -l^{-1}(1 - l^{-1} + 3\theta l^{-2}) & \varepsilon_l' - 1 = -(1 + l^{-1} - \theta l^{-2}) \\ \varepsilon_l'' = 1 + l^{-1} - 2\theta l^{-2} & \varepsilon_l'' - 1 = l^{-1}(1 - 2l^{-1} + 4\theta l^{-2}). \end{array}$$

We obtain

$$S_p(\varepsilon) = R_{a,b,m}(w) + O(w^{s-2m}) \text{ and } S_m(1/\varepsilon) = R_{-a,-b,m}(w) + O(w^{t-2m})$$

(see [Lou17, Lemma 8]). For $P(X, Y) = X^u Y^v$ with $u, v \geq 0$ we thus have

$$P(S_m(\varepsilon), S_m(1/\varepsilon)) = P(R_{a,b,m}(w), R_{-a,-b,m}(w)) + O(w^{us+vt-2m}).$$

Hence,

$$\begin{aligned} F_{a,b}(S_m(\varepsilon), S_m(1/\varepsilon)) &= G_{a,b,m}(w) + O(w^{M_{a,b}-2m}) \\ &= q_{N_{a,b,m}} w^{-N_{a,b,m}} + O(w^{-N_{a,b,m}-1}) + O(w^{M_{a,b}-2m}), \end{aligned}$$

where $q_{N_{a,b,m}} \neq 0$. Now, assume that $m \geq (M_{a,b} + N_{a,b,m} + 1)/2$. We obtain

$$0 < |F_{a,b}(S_m(\varepsilon), S_m(1/\varepsilon))| < 1$$

if w is effectively large enough, i.e. if $l = w^m$ is effectively large enough. Since $S_m(\varepsilon) \in \mathbb{Z}$ and $S_m(1/\varepsilon) \in \mathbb{Z}$ and hence $F_{a,b}(S_m(\varepsilon), S_m(1/\varepsilon)) \in \mathbb{Z}$ whenever ε is a mth power in $\mathbb{Q}(\varepsilon_l)$, we get the desired result. □

Conjecture 20. *Let $(a,b) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1}$ be such that $m_{a,b} = a^2+ab+b^2$ is odd and $m_{a,b} \geq 5$. Assume that the pair (a,b) is not of the form $(-2b,b)$ with $b \geq 1$ odd, (b,b) with $b \geq 1$ odd, or $(-b/2,b)$ with $b \geq 2$ even.*
Then Proposition 19 is satisfied for $m = m_{a,b}$ with $M_{a,b}$ and $N_{a,b,m_{a,b}}$ as in Table 2, hence with

$$B_{a,b,m_{a,b}} := (M_{a,b} + N_{a,b,m_{a,b}} + 1)/2 = (a^2+ab+b^2+1)/2 = (m_{a,b}+1)/2 \leq m_{a,b}.$$

Notice that there is some cancelation between the 3 terms of $R_{a,b}(T)$ if and only if we are in one of the 3 cases excluded in Conjecture 20.

Since an explicit formula for

$$G_{a,b,m_{a,b}}(T) = \sum_{n \leq -N_{a,b,m_{a,b}}} q_n T^n$$

would be very complicated, contrary to Table 1, in Table 2 we only give a formula for the non zero coefficient $q_{N_{a,b,m_{a,b}}}$ of the leading term.

Table 2: Conjecture for $G_{a,b,m_{a,b}}(T)$,
for $a \neq 0$, $b \geq 1$, a or b odd and $c := a+b \neq 0$

1. $a \geq 1$ odd and $b \geq 1$ odd: $M_{a,b} = c\max(a,b)$, $N_{a,b,m_{a,b}} = \min(a,b)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2\min(a,b)}{N_{a,b,m_{a,b}}} \times \begin{cases} a & \text{if } a<b \\ c & \text{if } a>b. \end{cases}$
2. $a \leq -1$ odd, $b \geq 1$ odd and $c>0$: $M_{a,b} = b\max(\lvert a\rvert, c)$, $N_{a,b,m_{a,b}} = \min(\lvert a\rvert, c)^2$, $q_{N_{a,b,m_{a,b}}} = -\frac{2}{N_{a,b,m_{a,b}}} \times \begin{cases} bc & \text{if } b>-2a \\ a^2 & \text{if } b<-2a. \end{cases}$
3. $a \leq -1$ odd, $b \geq 1$ odd and $c<0$: $M_{a,b} = \lvert a\rvert\max(b,\lvert c\rvert)$, $N_{a,b,m_{a,b}} = \min(b,\lvert c\rvert)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2}{N_{a,b,m_{a,b}}} \times \begin{cases} bc & \text{if } a>-2b \\ a^2 & \text{if } a<-2b. \end{cases}$

Table 2 (continued)

4. $a \geq 1$ odd, $b \geq 1$ even: $M_{a,b} = c\max(a,b)$, $N_{a,b,m_{a,b}} = \min(a,b)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2}{N_{a,b,m_{a,b}}} \times \begin{cases} -bc & \text{if } a<b \\ a^2 & \text{if } a>b. \end{cases}$
5. $a \leq -1$ odd, $b \geq 1$ even and $c>0$: $M_{a,b} = b\max(\lvert a\rvert, c)$, $N_{a,b,m_{a,b}} = \min(\lvert a\rvert, c)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2}{N_{a,b,m_{a,b}}} \times \begin{cases} a^2 & \text{if } b>-2a \\ bc & \text{if } b<-2a. \end{cases}$
6. $a \leq -1$ odd, $b \geq 1$ even and $c<0$: $M_{a,b} = \lvert a\rvert\max(b,\lvert c\rvert)$, $N_{a,b,m_{a,b}} = \min(b,\lvert c\rvert)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2}{N_{a,b,m_{a,b}}} \times \begin{cases} -a^2 & \text{if } a>-2b \\ bc & \text{if } a<-2b. \end{cases}$

Table 2 (continued)

7. $a \geq 2$ even, $b \geq 1$ odd: $M_{a,b} = c\max(a,b)$, $N_{a,b,m_{a,b}} = \min(a,b)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2bc}{N_{a,b,m_{a,b}}}$.
8. $a \leq -2$ even, $b \geq 1$ odd and $c > 0$: $M_{a,b} = b\max(\lvert a\rvert, c)$, $N_{a,b,m_{a,b}} = \min(\lvert a\rvert, c)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2bc}{N_{a,b,m_{a,b}}} \times \begin{cases} -1 & \text{if } b > -2a \\ +1 & \text{if } b < -2a. \end{cases}$
9. $a \leq -2$ even, $b \geq 1$ odd and $c < 0$: $M_{a,b} = \lvert a\rvert\max(b, \lvert c\rvert)$, $N_{a,b,m_{a,b}} = \min(b, \lvert c\rvert)^2$, $q_{N_{a,b,m_{a,b}}} = \frac{2bc}{N_{a,b,m_{a,b}}} \times \begin{cases} +1 & \text{if } a > -2b \\ -1 & \text{if } a < -2b. \end{cases}$

Notice that for $1 \leq k \leq 9$, the value of $N_{a,b,m_{a,b}}$ for the kth case in Table 2 is equal to the value of $N_{a,b}$ for the similar kth case in Table 1.

In fact, since we will only deal with pairs of positive coprime integers (a,b) such that $m_{a,b}$ is a prime greater than 3 (see Theorem 21), we need only 3 cases out of the 12 ones in Table 1, those given in Table 3.

Table 3: Conjecture for $G_{a,b,m_{a,b}}(T)$, with $a \geq 1$ and $b \geq 1$ and $c := a + b$

1. $a \geq 1$ odd and $b \geq 1$ odd: $M_{a,b} = c\max(a,b)$ and $N_{a,b,m_{a,b}} = \min(a,b)^2$,
4. $a \geq 1$ odd and $b \geq 1$ even: $M_{a,b} = c\max(a,b)$ and $N_{a,b,m_{a,b}} = \min(a,b)^2$,
7. $a \geq 2$ even and $b \geq 1$ odd: $M_{a,b} = c\max(a,b)$ and $N_{a,b,m_{a,b}} = \min(a,b)^2$.

The second point of Corollary 17, Propositions 11 and 19 yield:

Theorem 21. *Let $p \equiv 1 \pmod 6$ be a given prime. Write $p = A^2 + AB + B^2$, with $A > B \geq 1$ (in a unique way). Let E_p be a set of $p - 4$ pairs (a,b) as in the second point of Corollary 17. Assume that Conjecture 12 holds true for the $p - 6$ pairs (a,b) in E_p satisfying $a^2 + ab + b^2 \leq p$ and that Conjecture 20 holds true for the remaining 2 pairs of positive coprime integers $(a,b) \in \{(A,B),(B,A)\}$ satisfying $a^2 + ab + b^2 = p$. Then p does not divide the unit index j_l for l effectively large enough. In particular, if $p \equiv 1 \pmod 6$ is a prime less than 1875, then p does not divide the unit index j_l for l effectively large enough.*

Proof. First, we checked Conjecture 12 in the range $1 \leq \max(\lvert a\rvert, b) \leq 50$ on a MacBook Air laptop computer using Maple. This computation took 52 minutes. (To show that the time needed to check this conjecture increases fast with the bound on a and b, we also did the computation using Maple on a not that new IMac computer with a 2,66 Intel Core 2 Duo processor. for $1 \leq \max(\lvert a\rvert, b) \leq 50$ the computation took 78 minutes, for $1 \leq \max(\lvert a\rvert, b) \leq 60$ the computation took 4 hours, for $1 \leq \max(\lvert a\rvert, b) \leq 70$ the computation took 11 hours and for $1 \leq \max(\lvert a\rvert, b) \leq 80$ the computation took 28 hours).
Second, we checked that Conjecture 20 as given in Table 2 holds true (i) in the range $\max(\lvert a\rvert, b) \leq 25$ (on a MacBook Air laptop computer using Maple, this computation took 8 hours and 30 minutes) and also (ii) in the range $7 \leq p \leq 1875$ for the 2 pairs $(a,b) \in \{(A,B),(B,A)\}$ satisfying $a^2 + ab + b^2 = p$ (on a MacBook Air laptop computer using Maple, this computation took 14 hours). □

6 Remarks on totally real exceptional units

Let ε be a totally real exceptional unit. If ε is quadratic, then the rank of the group of units of the number field $\mathbb{Q}(\varepsilon)$ is equal to 1 and ε and $\varepsilon-1$ are therefore multiplicatively dependent. The following Theorem 22 shows that this is the only such situation:

Theorem 22. *Let ε be a totally real exceptional unit. Then ε and $\varepsilon-1$ are multiplicatively dependent if and only if ε is quadratic, i.e. if and only if*

$$\varepsilon \in V_{(1+\sqrt{5})/2} = \{(1\pm\sqrt{5})/2, (-1\pm\sqrt{5})/2, (3\pm\sqrt{5})/2\}.$$

Proof. Let ε be a totally real exceptional unit. Assume that ε and $\varepsilon-1$ are multiplicatively dependent, i.e. that that

$$\varepsilon^a(\varepsilon-1)^b = \pm 1,$$

with $a, b \in \mathbb{Z}$ not both equal to 0. Clearly, $a \neq 0$ and $b \neq 0$. To begin with, it is easy to see that the only exceptional totally real quadratic units are (i) $\varepsilon = (1\pm\sqrt{5})/2$, in which case $\varepsilon(\varepsilon-1) = 1$; (ii) $\varepsilon = (-1\pm\sqrt{5})/2$, in which case $\varepsilon^2(\varepsilon-1)^{-1} = -1$; and (iii) $\varepsilon = (3\pm\sqrt{5})/2$, in which case $\varepsilon(\varepsilon-1)^{-2} = 1$. Now, assume that $\mathbb{K} := \mathbb{Q}(\varepsilon)$ is a totally real number field of degree $d := (\mathbb{K}:\mathbb{Q}) \geq 3$. Since ± 1 are the only complex roots of unity in the totally real number field $\mathbb{K}$, we may assume that $\gcd(a,b) = 1$. Let $u, v \in \mathbb{Z}$ be such that $au + bv = 1$. Then

$$1-\varepsilon = -(\pm 1)^u \left(\frac{(\varepsilon-1)^u}{\varepsilon^v}\right)^a \text{ and } \varepsilon = (\pm 1)^u \left(\frac{\varepsilon^v}{(\varepsilon-1)^u}\right)^b.$$

By [Enn1, Lemma 4.1], the totally real exceptional units $1-\varepsilon$ and ε are not n-powers in $\mathbb{Q}(\varepsilon)$, where $\pm 1 \neq n \in \mathbb{Z}$ is odd. Hence $a, b \in \{\pm 2^n;\ n \in \mathbb{Z}_{\geq 0}\}$. Since $\gcd(a,b) = 1$ we have $a = \pm 1$ or $b = \pm 1$. Since $d \geq 3$ we have $a \neq \pm 1$ or $b \neq \pm 1$. Hence, either $\varepsilon = \pm(\varepsilon-1)^{\pm 2^n}$ if $a = \pm 1$, or $1-\varepsilon = \pm\varepsilon^{\pm 2^n}$ if $b = \pm 1$, where $n \in \mathbb{Z}_{n\geq 1}$. Moreover, the sign is necessarily the plus sign. Indeed, otherwise we would have $\xi = -\eta^2$ in $\mathbb{K}$ for one of the two totally real exceptional units $\xi = \varepsilon$ or $\xi = 1-\varepsilon$, which would give the contradiction $1 = |N_{\mathbb{K}/\mathbb{Q}}(\xi-1)| = N_{\mathbb{K}/\mathbb{Q}}(1+\eta^2) > 1$, as η^2 is totally positive. Therefore, one of the two totally real exceptional units $\xi = \varepsilon$ or $\xi = 1-\varepsilon$ satisfies $\xi = (\xi-1)^{\pm m}$ for some $m = 2^n \geq 2$. Consequently, ξ is an algebraic integer of degree $d = (\mathbb{K}:\mathbb{Q}) \geq 3$ and the $d \geq 3$ conjugates of ξ are real roots of either $P_m(x) = (x-1)^m - x$ with $m \geq 4$ even or $Q_m(x) = x(x-1)^m - 1$ with $m \geq 2$ even. This can never happen. Indeed, let $m \geq 4$ be even. Then $x \mapsto P_m'(x) = m(x-1)^{m-1} - 1$ is strictly increasing, and $P_m'(x)$ has only one real root $x_m = 1 + m^{-1/(m-1)}$. Since

$$P_m(x_m) = \frac{1}{m \cdot m^{\frac{1}{m-1}}} - 1 - \frac{1}{m^{\frac{1}{m-1}}} < -1 < 0,$$

it follows that $P_m(x)$ has exactly 2 real roots. In the same way, let $m \geq 2$ be even. Then $Q_m'(x) = (x-1)^{m-1}((m+1)x-1)$ and we have the following table of sense of variation:

x	$-\infty$		$\frac{1}{m+1}$		1		$+\infty$
$Q_n'(x)$		$+$	0	$-$	0	$+$	
$Q_n(x)$		$\nearrow$	$\frac{1}{m+1}\left(\frac{m}{m+1}\right)^m - 1 < 0$	$\searrow$	-1	$\nearrow$	

It follows that $Q_m(x)$ has exactly 1 real root, which is greater than 1. □

7 Acknowledgements

We thank Prof. A. Granville who on October 23rd (2019) sent us the proof of Lemma 5, Lemma which we needed to prove Theorem 6.
We thank Prof. H. Lenstra who on October 25th (2019) sent us the proof of Proposition 16.

References

[Cus] T. W. Cusick. Lower bounds for regulators. *Lecture Notes in Math.* **1068** (1984), 63-73.

[Enn1] V. Ennola. Cubic number fields with exceptional units. *Computational number theory (Debrecen, 1989),* 103–128*, de Gruyter, Berlin,* 1991.

[Enn2] V. Ennola. Fundamental units in a family of cubic fields. *J. Théor. Nombres Bordeaux* **16** (2004), 569–575.

[Gr] A. Granville. ABC means we can count squarefrees. *International Mathematical Research Notices* **19** (1998), 991–1009

[LM] S. Louboutin and A. Murchio. Representation of the elements of the finite field $\mathbb{F}_p$ by fractions. *Period. Math. Hungar.* **79** (2019), 218–220.

[Lou17] S. Louboutin. Non-Galois cubic number fields with exceptional units. *Publ. Math. Debrecen* **91** (2017), 153–170.

[Lou20] S. Louboutin. Non-Galois cubic number fields with exceptional units. Part II. *J. Number Theory* **206** (2020), 62–80.

[Tho] E. Thomas. Fundamental units for orders in certain cubic number fields. *J. Reine Angew. Math.* **310** (1979), 33–55.

[Was] L. C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.* **48** (1987), 371–384.