Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5)
Vol. VII (2008), 579-608

Diophantine triples with values in binary recurrences

CLEMENS FUCHS, FLORIAN LUCA AND LASZLO SZALAY

Abstract. In this paper, we study triples a, b and c of distinct positive integers such that $ab+1$, $ac+1$ and $bc+1$ are all three members of the same binary recurrence sequence.

Mathematics Subject Classification (2000): 11D72 (primary); 11D61, 11B37 (secondary).

1. Introduction

A *Diophantine m-tuple* is a set $\{a_1, \ldots, a_m\}$ of positive integers such that $a_i a_j + 1$ is a perfect square (*i.e.* a square of a number in $\mathbb{Z}$) for all $1 \leq i < j \leq m$. Finding such sets was already investigated by Diophantus and he found the *rational* quadruple $\{1/16, 33/16, 68/16, 105/16\}$. The first quadruple in integers, the set $\{1, 3, 8, 120\}$, was found by Fermat. Infinitely many Diophantine quadruples are known and it is conjectured that there is no Diophantine quintuple. This was almost proved by Dujella [7], who showed that there can be at most finitely many Diophantine quintuples and all of them are, at least in theory, effectively computable. Several variants of this problem have been studied in the past. For example, Bugeaud and Dujella [2], proved upper bounds for the size m of sets of positive integers with the property that the product of any two distinct elements plus one is a perfect k-th power for fixed k, namely m is bounded by 7 for $k = 3$, by 5 for $k = 4$, by 4 for $5 \leq k \leq 176$, and by 3 for $k \geq 177$. Another variant studied previously is concerned with perfect powers instead of squares or k-th powers for fixed k. The second author proved that the abc-conjecture implies that the size of such sets is bounded by an absolute constant, whereas unconditionally there are bounds depending on the largest element in the set (see [14] and the papers cited therein). For further results on Diophantine m-tuples and its variants, we refer to [8].

In this paper, we treat another variant of this problem. Let r and s be nonzero integers such that $\Delta = r^2 + 4s \neq 0$. Let $(u_n)_{n \geq 0}$ be a binary recurrence sequence

Received January 10, 2008; accepted in revised form May 26, 2008.

of integers satisfying the recurrence

$$u_{n+2} = ru_{n+1} + su_n \quad \text{for all} \quad n \geq 0.$$

It is well-known that if we write α and β for the two roots in $\mathbb{C}$ of the *characteristic equation* $x^2 - rx - s = 0$, then there exist constants $\gamma, \delta \in \mathbb{K} = \mathbb{Q}[\alpha]$ such that

$$u_n = \gamma\alpha^n + \delta\beta^n \tag{1.1}$$

holds for all $n \geq 0$. We shall assume in what follows that the sequence $(u_n)_{n\geq 0}$ is *nondegenerate*, which means that $\gamma\delta \neq 0$ and α/β is not root of unity. We shall also make the convention that $|\alpha| \geq |\beta|$. Note that $|\alpha| > 1$.

Here, we look for Diophantine triples with values in the set $\mathcal{U} = \{u_n : n \geq 0\}$, namely sets of three distinct positive integers $\{a, b, c\}$, such that $ab + 1$, $ac + 1$, $bc + 1$ are all in $\mathcal{U}$. Clearly, there are always such pairs as *e.g.* $\{1, u_n - 1\}$. Note that if $u_n = 2^n + 1$ for all $n \geq 0$, then there are infinitely many such triples (namely, take a, b, c to be any distinct powers of two); in this situation, we can even get arbitrarily large sets $\{a_1, \ldots, a_m\}$ with the property that $a_i a_j + 1 \in \mathcal{U}$ for all $1 \leq i < j \leq m$. Our main result is that the above example is representative for the sequences $(u_n)_{n\geq 0}$ with real roots for which there exist infinitely many Diophantine triples with values in $\mathcal{U}$. More precisely we prove the following.

Theorem 1.1. *Assume that $(u_n)_{n\geq 0}$ is a nondegenerate binary recurrence sequence with $\Delta > 0$ such that there exist infinitely many sextuples of nonnegative integers $(a, b, c; x, y, z)$ with $1 \leq a < b < c$ such that*

$$ab + 1 = u_x, \qquad ac + 1 = u_y, \qquad bc + 1 = u_z. \tag{1.2}$$

Then $\beta \in \{\pm 1\}$, $\delta \in \{\pm 1\}$, $\alpha, \gamma \in \mathbb{Z}$. Furthermore, for all but finitely many of the sextuples $(a, b, c; x, y, z)$ as above one has $\delta\beta^z = \delta\beta^y = 1$ and one of the following holds:

(i) $\delta\beta^x = 1$. *In this case, one of γ or $\gamma\alpha$ is a perfect square;*
(ii) $\delta\beta^x = -1$. *In this case, $x \in \{0, 1\}$.*

Theorem 1.1, of course, implies that there are only finitely many triples of positive integers such that the product of any two plus one is in $\mathcal{U}$, except in the cases described (and these cases really occur as we saw above). We mention that the problem can be reformulated as a Diophantine equation of polynomial-exponential type with three independent exponential variables and three additional polynomial variables, namely

$$(ab + 1 - u_x)^2 + (ac + 1 - u_y)^2 + (bc + 1 - u_z)^2 = 0.$$

It is well-known that the Subspace theorem is a powerful tool for such problems, *e.g.* it was also used to classify the solutions to the equation $Au_x + Bu_y + Cu_z = 0$ for fixed $A, B, C \in \mathbb{Z}$ in [18] (see [19] for a survey on such equations). A new

development in applying the Subspace theorem was started by Corvaja and Zannier (see [10, 23, 24]), and their techniques will also be used in our proof (especially we use [6, 11] and [5]). We could not prove any finiteness result for the case when $\Delta < 0$, the reason being that in this case there is no *dominant root* in the polynomial-exponential Diophantine equation, which is the main restriction in applying the Subspace theorem with these techniques at present. A simple example for a sequence with this property is given by $(u_n)_{n\geq 0}$ with $(r, s) = (1, -2)$, $u_0 = 0$, $u_1 = 1$, where $\Delta = -7$ and $\alpha = (1 + i\sqrt{7})/2$, $\beta = (1 - i\sqrt{7})/2$. We mention that the same condition also appears in [16].

For example, it follows for the particular case of the Fibonacci sequence $(F_n)_{n\geq 0}$, given by $(r, s) = (1, 1)$, $F_0 = 0$ and $F_1 = 1$, that there are at most finitely many triples of positive integers such the product of any two plus one is a Fibonacci number F_n. In the subsequent paper [17] the second and third author show that there is in fact no triple of distinct positive integers a, b and c such that $ab + 1$, $ac + 1$ and $bc + 1$ are all three Fibonacci numbers.

ACKNOWLEDGEMENTS. The authors thank an anonymous referee for the careful reading of the text.
During the preparation of this paper, F. L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508, and L. S. was supported in part by a János Bolyai Scholarship of HAS and the Hungarian National Foundation for Scientific Research Grants No. T 048945 MAT and K 61800 FT2.

2. A bird's-eye-view of the proof

For the convenience of the reader we will give an overview of the proof of the theorem, since the proof is rather long and becomes more and more technical towards the end. We mention that throughout the paper the symbols o, O, $\sim$, $\ll$, $\gg$, $\asymp$, are used with their usual meaning.

Since $\Delta > 0$, it follows that $|\alpha| > |\beta|$. We shall show that one may assume that both α and γ are positive. We assume that we have infinitely many solutions $(a, b, c; x, y, z)$ to equation (1.2). Then $z \to \infty$, $x < y < z$ if z is sufficiently large, and $c \mid \gcd(u_y - 1, u_z - 1)$. The case $\delta\beta^z = 1$ is not hard to handle. When $\delta\beta^z \neq 1$, results from Diophantine approximations relying on the Subspace theorem, as the finiteness of the number of solutions of nondegenerate unit equations with variables in a finitely generated multiplicative group and bounds for the greatest common divisors of values of rational functions at units points in the number fields setting, allow us to reduce the problem to elementary considerations concerning polynomials. By using unit equations, we first conclude that $\log b$ and $\log c$ have the same orders of magnitude, therefore $x \asymp y \asymp z$. Then we show that a is also large which will come in handy later on. These preliminaries can be found in the next two sections (see Section 3 and 4). Next, since the multi-recurrence $((u_x - 1)(u_y - 1)(u_z - 1))_{x<y<z}$ has a dominant root and comparable positive integer subscripts, a result of the first author from [11] tells us that

for infinitely many of our solutions, the positive integer abc is a linear combination of finitely many of the monomials in $\alpha^x,\ \beta^x,\ \alpha^y,\ \beta^y,\ \alpha^z,\ \beta^z$ appearing in the formal Puiseux expansion of $\sqrt{(u_x-1)(u_y-1)(u_z-1)}$. Hence, the relation $(abc)^2=(u_x-1)(u_y-1)(u_z-1)$, may now be regarded as a unit equation with unknowns in the multiplicative group generated by α and β, and it remains to deal with it (equivalently, it can be viewed as the problem of calculating the zeroes of a multi-recurrence; this is not an easy task, see *e.g.* Remark 5 in [11]). The proof now falls in two distinct cases depending on whether α and β are multiplicatively independent or dependent. In case α and β are multiplicatively independent (which together with the considerations outlined above is handled in Section 5), listing the first few dominant units on both sides of the equation and identifying them, one gets a few linear relations among the exponents x, y and z. It turns out that if one goes back to the original equations, these few linear relations are enough to get a contradiction in this case. In case when α and β are multiplicatively dependent (see Section 6), we argue without going back to the before mentioned multi-recurrence. Instead, we show first in an elementary way (using just the pigeon hole principle), that there are only finitely many lines in $\mathbb{Z}^3$ the union of which contain all possible triples (x, y, z) leading to a solution of our problem. Since we have infinitely many solutions, we may assume that for infinitely many of them we have $x=d_1t+e_1$, $y=d_2t+e_2$, $z=d_3t+e_3$, where $d_1, d_2, d_3, e_1, e_2, e_3$ are fixed integers with the first three positive and t is some positive integer variable. But in this case, since α and β are also multiplicatively dependent, it follows that $u_x-1,\ u_y-1,\ u_z-1$ are all polynomials in ρ^t, where ρ is some number such that $\alpha=\rho^i$ and $\beta=\pm\rho^j$ for some integers i and j. Since any two of these numbers have large greatest common divisors, it follows that any two of these three polynomials have a common root and the product of all three is the square of some other polynomial. The proof ends by a careful analysis of how these polynomials might share their roots with a view of getting a contradiction.

3. Preparations

Let $\mathbb{L}$ be any algebraic number field and $\mathcal{S}$ be a finitely generated multiplicative subgroup of $\mathbb{L}$. Given $N\geq 1$, a unit equation is an equation of the form

$$\sum_{i=1}^{N} a_i x_i = 1, \tag{3.1}$$

where $a_1,\ldots,a_N\in\mathbb{L}$ are fixed nonzero coefficients and $x_1,\ldots,x_N\in\mathcal{S}$. A solution $(x_1,\ldots,x_N)$ of the above unit equation is called *nondegenerate* if $\sum_{i\in I} a_i x_i\neq 0$ for all proper subsets $I\subseteq\{1,\ldots,N\}$. In such a case, we will call the unit equation (3.1) itself nondegenerate. We record the following result about unit equations. A proof can be found, for example, in [23].

Lemma 3.1. *There are only finitely many nondegenerate solutions* $\mathbf{x}=(x_1,\ldots,x_N)\in\mathcal{S}^N$ *to the unit equation* (3.1).

We will use Lemma 3.1 several times in what follows. In our case (and for the rest of the paper), $\mathcal{S}$ is the multiplicative group generated by α and β inside $\mathbb{K}$; *i.e.*, $\mathcal{S} = \{\alpha^n \beta^m : n, m \in \mathbb{Z}\}$. In this special case (3.1) can be rewritten as

$$\sum_{i=1}^{N} a_i \alpha^{n_i} \beta^{m_i} = 1 \tag{3.2}$$

to be solved in integers $n_1, \ldots, n_N, m_1, \ldots, m_N$. Lemma 3.1 tells us that there are only finitely many $(n_1, \ldots, n_N, m_1, \ldots, m_N) \in \mathbb{Z}^{2N}$ such that no subsum on the left of (3.2) vanishes. In the case when the right hand side of (3.2) is 0, then Lemma 3.1 implies that the differences $n_i - n_j, m_i - m_j$ are bounded for all $1 \leq i < j \leq N$ and for all $n_1, \ldots, n_N, m_1, \ldots, m_N$ such that no subsum on the left vanishes. We mention that the set of all $\mathbb{K}$-linear combinations of elements in $\mathcal{S}$ is easily understood: it is isomorphic to $\mathbb{K}[X^{\pm 1}, Y^{\pm 1}]$ in the case when α and β are multiplicatively independent and isomorphic to $\mathbb{K}[X^{\pm 1}]$ otherwise.

We will also need the following lemma. Assume that $(u_n)_{n \geq 0}$ is the nondegenerate binary recurrent sequence whose general term is given by the formula (1.1). Assume further that $\Delta > 0$, therefore that $|\alpha| > |\beta|$. We have the following result.

Lemma 3.2. *There exist constants $\kappa_0 \in (0, 1)$ and z_0 such that if y and z are positive integers with $z > \max\{y, z_0\}$, $\delta\beta^z \neq 1$ and $u_y \neq 1$, then*

$$\gcd(u_y - 1, u_z - 1) < |\alpha|^{\kappa_0 z}.$$

Proof. We may assume that $u_y \neq 0$, since otherwise the assertion is trivially true. Then clearly, $|u_y - 1| \ll |u_y| \ll |\alpha|^y$. Thus, if for some small but fixed $\varepsilon > 0$ we have $y < (1 - \varepsilon)z$, then we can take $\kappa_0 = 1 - \varepsilon/2$ and the desired inequality holds for large z. From now on, we shall assume that the inequalities $(1 - \varepsilon)z < y < z$ hold with some small $\varepsilon > 0$ to be fixed later. Put $\lambda = z - y \in (0, \varepsilon z)$. Let $D = \gcd(u_y - 1, u_z - 1)$. Then

$$D \mid \gamma\alpha^y + \delta\beta^y - 1 \qquad \text{and} \qquad D \mid \gamma\alpha^{y+\lambda} + \delta\beta^{y+\lambda} - 1. \tag{3.3}$$

Multiplying the first divisibility relation in (3.3) by the algebraic integer α^λ, we also have that $D \mid \gamma\alpha^{y+\lambda} + \delta\beta^y\alpha^\lambda - \alpha^\lambda$. From this and the second relation in (3.3), we get

$$D \mid \delta\beta^y(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1). \tag{3.4}$$

Let us first assume that the algebraic integer appearing on the right hand side above is zero. We then get

$$1 = \alpha^\lambda + \delta\beta^z - \delta\beta^y\alpha^\lambda. \tag{3.5}$$

This is a unit equation in four terms. If it is nondegenerate, then it has only finitely many solutions. Thus, taking z_0 sufficiently large, it follows that if equation (3.5) holds, then it must be degenerate. In this case, one of α^λ, $\delta\beta^z$, or $-\delta\beta^y\alpha^\lambda$ equals 1. The case $\delta\beta^z = 1$ is excluded by hypothesis. The case $\alpha^\lambda = 1$ leads to $\lambda = 0$,

which is impossible. Finally, the case $-\delta\beta^y\alpha^\lambda = 1$ leads to $\delta\beta^z + \alpha^\lambda = 0$, or $|\alpha|^\lambda = |\delta||\beta|^z$. If $|\beta| \neq 1$, we then get that $z\log|\beta| + \log|\delta| = \lambda\log|\alpha|$. Since $\lambda < \varepsilon z$, it follows that the above relation is impossible for large z if we choose $\varepsilon < \log|\beta|/(2\log|\alpha|)$. Thus, if $z > z_0$, then we must have $|\beta| = 1$, therefore $|\alpha|^\lambda = |\delta|$. Now the relation $-\delta\beta^y\alpha^\lambda = 1$ leads to $|\alpha|^\lambda = |\delta|^{-1}$. Thus, $|\alpha|^\lambda = |\delta| = |\delta|^{-1}$, leading to $|\delta| = 1$. We next get $|\alpha|^\lambda = 1$, therefore $\lambda = 0$, which is a contradiction.

From now on, we may assume that z is sufficiently large, and therefore that relation (3.5) does not hold.

Assume first that $\mathbb{K} = \mathbb{Q}$. Then the nonzero integer appearing on the right hand side of (3.4) is of size

$$\begin{aligned}\left|\delta\beta^y(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1)\right| &\ll \exp(y\log|\beta| + \lambda\log|\alpha|)\\ &\leq \exp\left(z\left(\log|\beta| + \varepsilon\log|\alpha|\right)\right) < |\alpha|^{\kappa_0 z},\end{aligned}$$

for a certain $\kappa_0 < 1$ (depending on ε) provided that we first choose $\varepsilon < (\log|\alpha| - \log|\beta|)/\log|\alpha|$, and then we let z be sufficiently large. This finishes the proof of the lemma in this case.

Assume now that $\mathbb{K}$ is quadratic. Conjugating (3.4) by the nontrivial Galois automorphism of $\mathbb{K}$ over $\mathbb{Q}$, we get

$$D \mid \gamma\alpha^y(\beta^\lambda - \alpha^\lambda) - (\beta^\lambda - 1). \tag{3.6}$$

Multiplying relations (3.4) and (3.6), we get

$$D^2 \mid \left(\delta\beta^y(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1)\right)\left(\gamma\alpha^y(\beta^\lambda - \alpha^\lambda) - (\beta^\lambda - 1)\right),$$

and the right hand side above is a nonzero integer. Hence,

$$D^2 \ll \exp\left(y\log|\alpha\beta| + 2\lambda\log|\alpha|\right) \leq \exp\left(\left(\log|\alpha\beta| + 2\varepsilon\log|\alpha|\right)z\right).$$

Choosing $\varepsilon < (\log|\alpha| - \log|\beta|)/(2\log|\alpha|)$, one checks easily that the last inequality above leads to the conclusion that $D \leq |\alpha|^{\kappa_0 z}$ for a certain $\kappa_0 \in (0,1)$ (depending on ε) provided that z is sufficiently large. This completes the proof of Lemma 3.2. □

We mention that Bugeaud, Corvaja and Zannier (see [1]), showed by using the Subspace theorem that if $a > b > 1$ are multiplicatively independent integers, then for all $\varepsilon > 0$ there exists n_ε such that $\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n)$ if $n > n_\varepsilon$. Afterwards, this result was extended in various ways by various authors (see [5, 9, 15] and [21] for a sample of such extensions). The last lemma is a weak form of such a result, which is enough for our purpose, and admits an easier proof. Furthermore, we point out that a generalisation of these results to the number-field setting can be found in [5], which will also be used later.

4. Further preliminaries and the case $\delta\beta^z = 1$

In this section, we will prove some useful information on the solutions of our problem. Especially, we will handle the case when $\delta\beta^z = 1$, which gives the exceptional solutions in the theorem.

4.1. Both z and y are large

Assume that $1 \le a < b < c$ and that $ab + 1 = u_x$, $ac + 1 = u_y$ and $bc + 1 = u_z$. We may assume that there are infinitely many such triples, therefore that $c \to \infty$. Since $|\alpha| > |\beta|$, we have

$$|u_n| = |\gamma||\alpha|^n|1 - \delta\gamma^{-1}(\beta/\alpha)^n|,$$

and $(\beta/\alpha)^n$ tends to zero as $n \to \infty$. This shows that if $n > n_0$ is sufficiently large, then $|u_n| < |u_m|$ means $n < m$. Since

$$u_z = bc + 1 > \max\{u_x, u_y\} = \max\{|u_x|, |u_y|\},$$

we get that $z > \max\{x, y\}$. Further, since c is arbitrarily large and $u_y = ac+1 > c$, it follows that y is arbitrarily large. Since $u_y = ac + 1 > ab + 1 = u_x$, it follows that if c is sufficiently large, then $y > x$. Thus, we may assume that $x < y < z$. Clearly, z tends to infinity. We shall assume that $z > z_0$, where z_0 is a sufficiently large number, not necessarily the same at each occurrence. Note that

$$u_z = |\gamma||\alpha|^z|1 - \delta\gamma^{-1}(\beta/\alpha)^z| = bc + 1 \in [c, c^2],$$

showing that

$$\log c \le z \log|\alpha| + O(1) \le 2 \log c. \tag{4.1}$$

Since

$$u_y = |\gamma||\alpha^y||1 - \delta\gamma^{-1}(\beta/\alpha)^y| = ac + 1 > c,$$

we get that

$$\log c \le y \log|\alpha| + O(1). \tag{4.2}$$

Estimates (4.1) and (4.2) show that $z \le 2y + O(1)$.

4.2. The case when $\delta\beta^z = 1$

Since z is large, the above relation implies $\beta = \pm 1$, therefore $\delta = \pm 1$. Hence, $\alpha \in \mathbb{Z}$. Furthermore, since $\gamma = u_0 - \delta = u_0 \pm 1$, we get that $\gamma \in \mathbb{Z}$. Moreover, $\delta\beta^y$ and $\delta\beta^x$ are both in $\{\pm 1\}$. If $\delta\beta^y = -1$, we then have

$$bc = \gamma\alpha^z \qquad \text{and} \qquad ac = \gamma\alpha^y - 2.$$

It is easy to see that for large z we have $\gcd(\gamma\alpha^z, \gamma\alpha^y - 2) = O(1)$. This shows that $c = O(1)$, therefore that $z = O(1)$. This leads to only finitely many solutions. Thus, if z is sufficiently large, then $\delta\beta^y = 1$. If also $\delta\beta^x = 1$, then

$$ab = \gamma\alpha^x, \qquad ac = \gamma\alpha^y, \qquad bc = \gamma\alpha^z,$$

therefore $(abc)^2 = \gamma^3\alpha^{x+y+z}$, implying that either γ or $\gamma\alpha$ is a perfect square, according to whether $x + y + z$ is even or odd, respectively. Assume now that $\delta\beta^x = -1$. Then

$$ab = \gamma\alpha^x - 2, \qquad ac = \gamma\alpha^y, \qquad bc = \gamma\alpha^z.$$

Furthermore, since $\delta\beta^y = \delta\beta^z = 1$ but $\delta\beta^x = -1$, it follows that $\beta = -1$, y and z have the same parity, and x has opposite parity. Since $abc^2 = \gamma^2\alpha^{y+z}$ and y and z have the same parity, it follows that ab is a perfect square. Assume now that $x \geq 2$. Then

$$ab + 2 = \gamma\alpha^x. \tag{4.3}$$

But since a and b divide $\gamma\alpha^y$ and $\gamma\alpha^z$, respectively, it follows that all primes dividing ab divide $\gamma\alpha$. The last relation above (4.3) shows now that the only prime factor of ab is 2. Hence, ab is a power of 2 and since it is a square, it is ≥ 4. Thus, $2\|ab + 2$ (*i.e.* $2|ab + 2$, but 4 does not), therefore $2\|\gamma\alpha^x$, and since $x \geq 2$, we get that $2\|\gamma$ and α is odd. Now the relations $ac = \gamma\alpha^y$ and $bc = \gamma\alpha^z$ together with the fact that ab is a power of 2, show that $a \in \{1, 2\}$ and $b \in \{1, 2\}$. This is impossible since $1 \leq a < b$ and ab must be a perfect square. Thus, if $\delta\beta^x = -1$, then $x \in \{0, 1\}$. This takes care of the exceptions (i) and (ii) appearing in the text of Theorem 1.1.

4.3. All three x, y and z are large

From now on, we assume that $\delta\beta^z \neq 1$. Note that $u_y = ac + 1 > 1$. Lemma 3.2 shows that there exists a positive constant $\kappa_0 < 1$ such that the inequality

$$\gcd(u_z - 1, u_y - 1) < |\alpha|^{\kappa_0 z}$$

holds provided that z is sufficiently large. Thus, the fact that c divides $\gcd(ac, bc) = \gcd(u_z - 1, u_y - 1)$ shows that $c < |\alpha|^{\kappa_0 z}$, leading to

$$b = \frac{u_z - 1}{c} \gg |\alpha|^{(1-\kappa_0)z}.$$

Since $|\alpha|^x \gg u_x = ab + 1 > b \gg |\alpha|^{(1-\kappa_0)z}$, it follows that $x \geq (1 - \kappa_0)z + O(1)$. Thus, x tends to infinity with c also and, in fact,

$$x \asymp y \asymp z. \tag{4.4}$$

This will be essential when applying the Subspace theorem.

4.4. Signs of γ and α

Here, we comment on the signs of α and γ. Assume that $\alpha > 0$. Then the sign of u_n is the same as the sign of γ once $n > n_0$ is sufficiently large. Thus, if $\gamma < 0$, then there are only finitely many n such that u_n is positive, and we obtain a contradiction. Hence, $\gamma > 0$ when $\alpha > 0$.

Assume now that $\alpha < 0$. Then for large n, the sign of u_n alternates; namely, the sign of u_n is the sign of $\gamma(-1)^n$. Thus, if $\gamma > 0$, then for large c the three numbers $x,\ y,\ z$ are even, while if $\gamma < 0$, then for large c the three numbers $x,\ y,\ z$ are odd. Thus, we may replace the pair of roots (α, β) by the pair (α^2, β^2), and keep the pair of coefficients (γ, δ) (if $\gamma > 0$), or replace it by $(\gamma\alpha, \delta\beta)$ (if $\gamma < 0$), and consequently suppose again that both α and γ are positive. From now on, we work under this assumption, namely that α and γ are positive.

4.5. a is large

Here, we shall prove a fact that will turn out to be useful later.

Lemma 4.1. *We have $a \to \infty$ as $z \to \infty$ through integer values such that $\delta\beta^z \neq 1$. Furthermore, in case α and β are multiplicatively independent, there exists a positive constant κ_1 such that $a > |\alpha|^{\kappa_1 z}$ when $z > z_0$.*

Proof. We start by assuming that for each $\varepsilon > 0$ there are infinitely many solutions with $a < |\alpha|^{\varepsilon z}$. We will see that this condition with a sufficiently small $\varepsilon > 0$ and a sufficiently large z entails that $a = O(1)$ when α and β are multiplicatively independent. Then we shall show that this last condition leads to a contradiction without any assumption on α and β with regard to their multiplicative independence.

The equation

$$a^2 = \frac{(u_x - 1)(u_y - 1)}{(u_z - 1)} \tag{4.5}$$

implies

$$|a^2\alpha^z - \gamma\alpha^{x+y}| \ll a^2 \max\{|\alpha|^y|\beta|^x, |\alpha|^y, |\beta|^z\}. \tag{4.6}$$

By estimate (4.4), it follows easily that there exists a constant $\kappa_2 \in (0, 1)$ such that if $\varepsilon > 0$ is sufficiently small, then

$$|a^2\alpha^z - \gamma\alpha^{x+y}| < |\alpha|^{\kappa_2 \max\{x+y,z\}}. \tag{4.7}$$

Indeed, putting κ_3 for a positive constant such that $\min\{x/z, x/(x + y)\} > \kappa_3$, a little calculation shows that the estimate (4.7) is implied by the estimate (4.6) for large z when

$$\varepsilon < 2^{-1}\kappa_3 \min\{\log|\alpha|, \log|\alpha/\beta|\}$$

with some constant κ_2 (depending on ε) provided that $z > z_0$ (here, z_0 also depends on ε). Assume that $x + y \geq z$ since the other case can be dealt with similarly. Then

$$|a^2\alpha^{z-x-y} - \gamma| < \frac{1}{|\alpha|^{(1-\kappa_2)(x+y)}}. \tag{4.8}$$

This shows that $z - x - y = O(\varepsilon z)$. Our next aim is to deduce for $z > z_0$ that the left hand side of (4.8) has to be zero. Indeed, if $\mathbb{K} = \mathbb{Q}$, and the left hand side is not zero, then its naïve height is $\exp(O(\varepsilon z))$. By the Liouville principle, if ε is sufficiently small and z is large, then inequality (4.8) cannot hold. If $\mathbb{K}$ is quadratic, and the right hand side is not zero, then the conjugate of $a^2\alpha^{z-x-y} - \gamma$ in $\mathbb{K}$ is $a^2\beta^{z-x-y} - \delta$. Thus, the height of this number is again $\exp(O(\varepsilon z))$. By the Liouville principle again, we arrive at a contradiction in inequality (4.8) for small $\varepsilon > 0$, assuming that its left hand side is nonzero.

Hence, for $z > z_0$, it follows that $a = \pm\gamma^{1/2}\alpha^{(x+y-z)/2}$. Now equation (4.5) is

$$\begin{aligned} a^2\delta\beta^z - a^2 = \gamma\delta(\alpha^x\beta^y + \alpha^y\beta^x) + \delta^2\beta^{x+y} - \gamma\alpha^x \\ - \gamma\alpha^y - \delta\beta^x - \delta\beta^y + 1. \end{aligned} \tag{4.9}$$

This is a unit equation. Let $\mathcal{E}$ be some nondegenerate subequation containing the variable 1. Then any unit in $\mathcal{E}$ can take only finitely many values. If α and β are multiplicatively independent, it then follows that either $\mathcal{E}$ contains $a^2 = \gamma\alpha^{x+y-z}$, or one of the other units. In the first case, $x + y - z = O(1)$, so $a = O(1)$. In the second case, one checks using the fact that α and β are multiplicatively independent, that $x = O(1)$; hence there are only finitely many possibilities for x.

From now on, we assume that a is bounded for infinitely many solutions. Thus, infinitely many of these solutions will therefore have the same value for a. Now rewrite equation (4.5) (keeping in mind again that $a^2\gamma\alpha^z = \gamma^2\alpha^{x+y}$ as we did for (4.9)), as

$$\begin{aligned} a^2 + 1 = a^2\delta\beta^z + \delta\beta^x + \delta\beta^y - \delta^2\beta^{x+y} \\ + \gamma\alpha^x + \gamma\alpha^y - \gamma\delta\alpha^x\beta^y - \gamma\delta\alpha^y\beta^x. \end{aligned} \tag{4.10}$$

This is again a unit equation. In order to discuss its degeneracies, we distinguish several cases.

Assume first that α and β are multiplicatively independent. Then there must be a nondegenerate subequation containing the left side ($a^2 + 1 \neq 0$) and some member from the right hand side. There are only finitely many such subequations, and each one of them has only finitely many solutions. In each one of the cases, we get that $x = O(1)$; hence, only finitely many possibilities.

Assume now that α and β are multiplicatively dependent. In this case, there exists $\rho > 1$ and coprime integers $i > j$ such that $\alpha = \rho^i$ and $\beta = \pm\rho^j$.

If $j > 0$, then again there must be some non-degenerate subequation of equation (4.10) containing the fixed nonzero number $a^2 + 1$ from the left hand side and some variable from the right hand side. This leads to $x = O(1)$; hence, only finitely many possibilities.

If $j = 0$, then $\beta = \pm 1$, $\alpha > 1$ and $\gamma,\ \delta$ are all integers. We may also assume that the class of (x, y, z) in $(\mathbb{Z}/2\mathbb{Z})^3$ is fixed. Thus, the three numbers $\delta\beta^x,\ \delta\beta^y$ and $\delta\beta^z$ are fixed in $\{\pm\delta\}$. We rewrite equation (4.10) as

$$a^2 + 1 - a^2\delta\beta^z - \delta\beta^x - \delta\beta^y + \delta^2\beta^{x+y} = \gamma(1 - \delta\beta^y)\alpha^x + \gamma(1 - \delta\beta^x)\alpha^y.$$

The left hand side as well as the coefficients $\gamma(1-\delta\beta^y)$ and $\gamma(1-\delta\beta^x)$ from the right hand side of α^x and α^y, respectively, are fixed. Assume first that these coefficients are zero. Then $\delta\beta^x = \delta\beta^y = 1$ and the left hand side must also be zero. This leads to $a^2(1-\delta\beta^z) = 0$, therefore $\delta\beta^z = 1$, which is not allowed. Thus, at least one of the two coefficients $\gamma(1-\delta\beta^y)$ and $\gamma(1-\delta\beta^x)$ from the right hand side is nonzero. Note that the left hand side is a fixed integer. Thus, if the left hand side is nonzero, then equation (4.10) is a unit equation (3.1) with $N = 1$ or 2 according to whether one or none of the coefficients of α^x and α^y from the right hand side vanishes. This leads again to $x = O(1)$; hence, only finitely many possibilities. Assume now that the right hand side is zero. Then

$$\alpha^{y-x} = -\frac{1-\delta\beta^y}{1-\delta\beta^x}, \qquad a^2 = -\frac{(1-\delta\beta^x)(1-\delta\beta^y)}{1-\delta\beta^z}.$$

Since $\alpha > 1$, it follows from the first of the above two equations that the cases $\beta = 1$, or $\beta = -1$ and $x \equiv y \pmod 2$ are impossible. Thus, up to replacing δ by $-\delta$ if needed, we may assume that

$$\alpha^{y-x} = -\frac{(1-\delta)}{(1+\delta)}.$$

Since $y > x$ and α is an integer, we get that $1+\delta \mid 1-\delta$. Thus, $1+\delta \mid 2$ leading to $1+\delta = -2,\ -1,\ 1,\ 2$. The cases $1+\delta = 1,\ 2$ lead to $\delta = 0$, which is not allowed, and $\alpha = 0$, which is not allowed either. The cases $1+\delta = -2,\ -1$ give $\alpha^{y-x} = 2,\ 3$, respectively. Thus, $\alpha = 2,\ 3$, respectively, and $y = x+1$. Now

$$a^2 = -\frac{(1-\delta\beta^x)(1-\delta\beta^y)}{(1-\delta\beta^z)} = -\frac{1-\delta^2}{1\pm\delta} \in \{-4, -3, 2, 1\},$$

so the only possibility is that $a = 1$. This happens if $\delta = -2$ and $a^2 = -(1+\delta)$, therefore $1-\delta\beta^z = 1-\delta$, so z is even. On the other hand, $1 = a = \gamma^{1/2}\alpha^{(x+y-z)/2}$ and γ and α are positive integers, therefore $\gamma = 1$ and $z = x+y = 2x+1$ is odd. This contradiction shows that it is not possible that the left hand side of equation (4.10) is zero and not both of the coefficients $\gamma(1-\delta\beta^y)$ and $\gamma(1-\delta\beta^x)$ of α^y and α^x, respectively, from its right-hand side are zero. Hence, if $j = 0$, then there are only finitely many possibilities for $x,\ y$ and z.

Finally, assume that $j < 0$. Since $\rho > 1$, it follows that $|\beta| < 1$, therefore β cannot be rational. Hence, α and β are quadratic conjugates. Now $\alpha^j = \rho^{ij} = \pm\beta^i$. Conjugating this relation in $\mathbb{K}$, we also get $\alpha^i = \pm\beta^j$. Thus,

$$\alpha^{i^2} = (\alpha^i)^i = \pm(\beta^j)^i = \pm(\beta^i)^j = (\alpha^j)^j = \alpha^{j^2},$$

so $i^2 = j^2$. Since $i > 0$ and $j < 0$, we get that $j = -i$, and since i and j are coprime, we get that $i = 1,\ j = -1$. Thus, $\beta = \pm\alpha^{-1}$. Rewrite equation (4.10) as

$$a^2 + 1 - a^2\delta\beta^z - \delta\beta^x - \delta\beta^y + \delta^2\beta^{x+y} + \gamma\delta(\alpha^x\beta^y + \alpha^y\beta^x) = \gamma(\alpha^x + \alpha^y).$$

Its right hand side is $\gg \alpha^y$. Its left hand side is in absolute value $\ll \alpha^{y-x}$, since $\beta = \pm\alpha^{-1}$. Thus, $\alpha^{y-x} \gg \alpha^y$, leading to $\alpha^x \ll 1$, therefore $x = O(1)$; hence, finitely many possibilities.

Having analyzed all the possible scenarios and having arrived to only finitely many possibilities in each case, we conclude that $a = O(1)$ leads to only finitely many possibilities. Thus, it must be the case that $a \to \infty$ as $z \to \infty$. Furthermore, in case α and β are multiplicatively independent, we have $a > |\alpha|^{\kappa_1 z}$ when $z > z_0$, where $\kappa_1 > 0$ is some constant. □

We saw that $\delta\beta^z \neq 1$. For future use, we also record that $\delta\beta^y \neq 1$ and $\delta\beta^x \neq 1$. Indeed, if say $\delta\beta^x = 1$, then $\beta = \pm 1$ and $b \mid \gcd(\gamma\alpha^z + (\delta\beta^z - 1), \gamma\alpha^x)$. Since $\delta\beta^z - 1 = O(1)$ is nonzero, it follows easily that b is bounded, which is a contradiction. The similar contradiction that $c = O(1)$ is obtained if one assumes that $\delta\beta^y = 1$.

5. The case α and β multiplicatively independent

In this section we will finish the proof of the theorem in the case when α and β are multiplicatively independent. This will be done by applying Theorem 1 of [11], which follows from the general result from [6] (see also [3, 4, 10], or [12]). We will indicate the proof to see that we get an additional piece of information which is not stated explicitly, although well-known, in [11, Theorem 1]. Then we show that the assumption of α and β being multiplicatively independent leads to a contradiction. As a first independent step we show that $\min\{y - x, y - 2x, z - 2x\} = O(1)$ in this case. Afterwards, the contradiction is derived.

5.1. An application of the Subspace theorem

The three relations (1.2) yield

$$(u_x - 1)(u_y - 1)(u_z - 1) = (abc)^2. \tag{5.1}$$

Note that

$$(u_x - 1)(u_y - 1)(u_z - 1) = \gamma^3\alpha^{x+y+z}(1 + \eta),$$

where

$$\eta = \prod_{t\in\{x,y,z\}} \left(\gamma_1\left(\frac{\beta}{\alpha}\right)^t + \delta_1\left(\frac{1}{\alpha}\right)^t\right),$$

with $\gamma_1 = \delta/\gamma$ and $\delta_1 = -1/\gamma$. Thus,

$$abc = \gamma^{3/2}\alpha^{(x+y+z)/2}(1 + \eta)^{1/2} = \gamma^{3/2}\alpha^{(x+y+z)/2}\sum_{k\geq 0}\binom{1/2}{k}\eta^k.$$

Furthermore, using the binomial formulae, for each k we have

$$\eta^k = \sum_{(\mathbf{i},\mathbf{j})\in\Gamma_k} c_{(\mathbf{i},\mathbf{j})}\alpha^{-i_1x-i_2y-i_3z}\beta^{j_1x+j_2y+j_3z},$$

where Γ_k is the set of all sextuples $(\mathbf{i},\mathbf{j})$ with $\mathbf{i}=(i_1,i_2,i_3)$, $\mathbf{j}=(j_1,j_2,j_3)$ fulfilling $i_1+i_2+i_3=k$, and $0\le j_\ell\le i_\ell$ for all $\ell=1,2,3$, while $c_{(\mathbf{i},\mathbf{j})}$ are certain coefficients in $\mathbb{K}$ indexed over the members of Γ_k.

Since x, y and z have the same order of magnitude, the arguments from [11] show that there exists a finite set Λ of sextuples $(\mathbf{i},\mathbf{j})$ (note that if $(\mathbf{i},\mathbf{j})$ is given, then k is the sum of the entries in $\mathbf{i}$), and nonzero coefficients $d_{(\mathbf{i},\mathbf{j})}\in\overline{\mathbb{Q}}$ for $(\mathbf{i},\mathbf{j})\in\Lambda$, such that infinitely many of the solutions $(a,b,c;x,y,z)$ have the property that

$$abc=\alpha^{(x+y+z)/2}\sum_{(\mathbf{i},\mathbf{j})\in\Lambda} d_{(\mathbf{i},\mathbf{j})}\alpha^{-i_1x-i_2y-i_3z}\beta^{j_1x+j_2y+j_3z}. \tag{5.2}$$

From now on, we work only with such solutions. We insert abc given by formula (5.2) into formula (5.1) and we end up with

$$(u_x-1)(u_y-1)(u_z-1)=\alpha^{x+y+z}\left(\sum_{(\mathbf{i},\mathbf{j})\in\Lambda} d_{(\mathbf{i},\mathbf{j})}\alpha^{-i_1x-i_2y-i_3z}\beta^{j_1x+j_2y+j_3z}\right)^2 \tag{5.3}$$

which upon expansion of both sides above leads to an $\mathcal{S}$-unit equation with infinitely many solutions. We now study this equation.

5.2. $\min\{y-x, y-2x, z-2x\} = O(1)$ when α and β are multiplicatively independent

We order the units appearing on the left hand side of the unit equation (5.3) according to their sizes of their absolute values.

5.2.1. *The case* $|\beta|>1$

It is then easy to see that

$$\begin{aligned}(u_x-1)(u_y-1)(u_z-1) = {}& \gamma^3\alpha^{x+y+z}+\gamma^2\delta\alpha^{z+y}\beta^x+\gamma^2\delta\alpha^{z+x}\beta^y\\ &+\gamma^2\delta\alpha^{x+y}\beta^z+\gamma\delta^2\alpha^z\beta^{x+y}+\text{smaller units.}\end{aligned} \tag{5.4}$$

We claim that for large z, we have

$$\alpha^{z+y}|\beta|^x>\alpha^{z+x}|\beta|^y>\alpha^{x+y}|\beta|^z>\alpha^z|\beta|^{x+y}.$$

Indeed, the ratios of any two consecutive expressions above are

$$\left(\frac{\alpha}{|\beta|}\right)^{y-x},\quad \left(\frac{\alpha}{|\beta|}\right)^{z-y},\quad \left(\frac{\alpha}{|\beta|}\right)^{x+y-z}.$$

The first two expressions are certainly > 1 and they remain bounded only when $y - x = O(1)$ and $z - y = O(1)$, and the fact that the third one tends to infinity as $z \to \infty$ is a consequence of Lemma 4.1 and of the fact that $\alpha^{x+y-z} \gg a^2 \geq \alpha^{\kappa_1 z}$. Especially, it follows that $x + y - z \to \infty$ as $z \to \infty$, which will be used later on.

We now insert the right hand side of (5.4) in (5.3) and use Lemma 3.1 (see also the remarks made below Lemma 3.1). We may assume that α^{x+y+z} cancels from both sides of equation (5.3). Indeed, if not, then $(\mathbf{0}, \mathbf{0}) \notin \Lambda$, and the largest unit present on the right hand side is $\leq \alpha^{y+z-x}|\beta|^{2x}$. Let $\mathcal{E}$ be some nondegenerate subequation containing α^{x+y+z}. If $\mathcal{E}$ contains some unit from the right hand side of (5.3), we deduce that the ratio of α^{x+y+z} to $\alpha^{y+z-x}|\beta|^{2x}$ is bounded; hence, $(\alpha/|\beta|)^{2x} = O(1)$, leading to $x = O(1)$; thus, only finitely many possibilities. If on the other hand $\mathcal{E}$ contains some other unit from the left hand side of equation (5.3), then the ratio of α^{x+y+z} to $\alpha^{y+z}|\beta|^x$ is bounded. Thus, again $(\alpha/|\beta|)^x = O(1)$, which leads to only finitely many possibilities. From now on, we assume that α^{x+y+z} cancels from both sides of equation (5.3), so in particular that $(\mathbf{0}, \mathbf{0}) \in \Lambda$.

Let $\mathcal{E}$ be some nondegenerate subequation containing $\alpha^{z+y}\beta^x$.

If $\mathcal{E}$ contains either $\alpha^z\beta^{x+y}$ or one of the smaller units, then the ratio of $\alpha^{z+y}\beta^x$ to $\alpha^z\beta^{z+y}$ stays bounded. This gives $(\alpha/|\beta|)^y = O(1)$, therefore $y = O(1)$; thus, only finitely many possibilities.

If $\mathcal{E}$ contains either $\alpha^{z+x}\beta^y$, or $\alpha^{x+y}\beta^z$, we then get that $(\alpha/|\beta|)^{y-x} = O(1)$, which is what we are after.

If $\mathcal{E}$ does not contain any unit from the left hand side of (5.3), then it must contain one from the right hand side. Hence, the ratio of

$$\alpha^{y+z}\beta^x \qquad \text{to} \qquad \alpha^{x+y+z}\frac{\beta^{j_1x+j_2y+j_3z}}{\alpha^{i_1x+i_2y+i_3z}}$$

is bounded for some $(\mathbf{i}, \mathbf{j}) \in \Lambda$ with $i_1 + i_1 + i_3 = k \neq 0$. Thus,

$$\alpha^{(i_1-1)x+i_2y+i_3z} \ll |\beta|^{(j_1-1)x+j_2y+j_3z}. \tag{5.5}$$

Since $j_\ell \leq i_\ell$ for $\ell = 1, 2, 3$, it follows that $(\alpha/|\beta|)^{(i_1-1)x+i_2y+i_3z} \ll 1$. If $i_2 + i_3 > 0$, we then get $y - x \ll 1$, which is what we want. Thus, $i_2 = i_3 = 0$, and since $k > 0$, we get that $i_1 \geq 1$. If $i_1 \geq 2$, we then get $x = O(1)$, so we get only finitely many possibilities. Thus, infinitely many of the solutions will have $\mathbf{i}_0 = (1, 0, 0)$. If $i_1 = 1$, $j_1 = 0$, then estimate (5.5) shows that $|\beta|^x \asymp 1$, therefore again $x = O(1)$. Hence, $j_1 = 1$ for infinitely many solutions. This shows that for $\mathbf{i}_0 = (1, 0, 0)$ and $\mathbf{j}_0 = (1, 0, 0)$ we have that $(\mathbf{i}_0, \mathbf{j}_0) \in \Lambda$. In particular, $\alpha^{x+y+z}(\beta/\alpha)^{2x}$ appears in the formula for $(abc)^2$. Let $\mathcal{F}$ be some nondegenerate equation that contains this variable.

If $\mathcal{F}$ contains a unit from the left hand side equal to $\alpha^z\beta^{x+y}$ or smaller, we then get that the ratio of

$$\alpha^{x+y+z}\left(\frac{\beta}{\alpha}\right)^{2x} \qquad \text{to} \qquad \alpha^z\beta^{x+y}$$

is $O(1)$. This implies that $(\alpha/|\beta|)^{y-x} \ll 1$, or $y - x = O(1)$, which is what we want.

If $\mathcal{F}$ contains a unit from the left hand side which is in

$$\{\alpha^{y+z}\beta^x,\ \alpha^{z+x}\beta^y,\ \alpha^{x+y}\beta^z\},$$

we then get that the ratio of $\alpha^{y+z-x}\beta^{2x}$ to one of these three units belongs to a fixed finite set of numbers. Thus, one of

$$\left(\frac{\alpha}{\beta}\right)^x, \qquad \left(\frac{\alpha}{\beta}\right)^{y-2x}, \qquad \left(\frac{\alpha}{\beta}\right)^{z-2x}$$

belongs to a fixed finite set of numbers. The first possibility gives $x = O(1)$, so only finitely many possibilities. The second and third show that $y - 2x = O(1)$, or $z - 2x = O(1)$, which is what we wanted.

Assume now that $\mathcal{F}$ does not contain any unit from the left hand side of equation (5.3). Then it must contain some unit from the right hand side. Thus, there must exist $(\mathbf{i}_1, \mathbf{j}_1) \neq (2\mathbf{i}_0, 2\mathbf{j}_0)$ such that the ratio of $(\beta/\alpha)^{2x}$ to $\beta^{j_1'x+j_2'y+j_3'z}/\alpha^{i_1'x+i_2'y+i_3'z}$ belongs to a finite set of numbers. Here, $\mathbf{i}_1 = (i_1', i_2', i_3')$ and $\mathbf{j}_1 = (j_1', j_2', j_3')$. Put $k = i_1' + i_2' + i_3'$. If $k \geq 3$, then

$$\frac{|\beta|^{j_1'x+j_2'y+j_3'z}}{\alpha^{i_1'x+i_2'y+i_3'z}} \ll \left(\frac{|\beta|}{\alpha}\right)^{3x},$$

and so we get that $(\alpha/|\beta|)^x \ll 1$, showing that $x = O(1)$; hence, again only finitely many possibilities. If $k = 2$, then it is easy to see that units of this shape of maximal absolute value not equal to $(\beta/\alpha)^{2x}$ have maximal value at most $(|\beta|/\alpha)^{x+y}$. So, the ratio of $(\beta/\alpha)^{2x}$ to such a unit is $\gg (\alpha/|\beta|)^{y-x}$. Hence, $(\alpha/|\beta|)^{y-x} \ll 1$, showing that $y - x = O(1)$, which is what we want.

The only elements in $\mathcal{F}$ with $k = 1$ are

$$\frac{1}{\alpha^x}, \quad \frac{1}{\alpha^y}, \quad \frac{1}{\alpha^z}, \quad \left(\frac{\beta}{\alpha}\right)^x, \quad \left(\frac{\beta}{\alpha}\right)^y, \quad \left(\frac{\beta}{\alpha}\right)^z.$$

Thus, the ratio of $(\beta/\alpha)^{2x}$ to one of the above six units belongs to some finite set of numbers. If one of these six units is one of the first four, then we get that one of $\beta^{2x}\alpha^{-x}$, $\beta^{2x}\alpha^{y-x}$, $\beta^{2x}\alpha^{z-x}$, or $(\beta/\alpha)^x$ belongs to a finite list of numbers. Since α and β are multiplicatively independent, we get that $x = O(1)$; hence, there are only finitely many possibilities. Finally, if one of these six units is one of the last two, we then get that one of $(\beta/\alpha)^{2x-y}$ or $(\beta/\alpha)^{2x-z}$ belongs to a fixed finite set of numbers. Thus, $y - 2x = O(1)$ or $z - 2x = O(1)$, as we wanted.

This finishes the case when $|\beta| > 1$.

5.2.2. *The case* $|\beta| < 1$

Here, we just sketch the main steps since the argument is very similar to the previous one. Instead of (5.4), we have

$$(u_x - 1)(u_y - 1)(u_z - 1) = \gamma^3\alpha^{x+y+z} - \gamma^2\alpha^{z+y} - \gamma^2\alpha^{z+x} - \gamma^2\alpha^{x+y} + \gamma\alpha^z + \text{smaller units}. \tag{5.6}$$

The main roots are, in decreasing order of their absolute values,

$$\alpha^{x+y+z},\ \alpha^{y+z},\ \alpha^{z+x},\ \alpha^{x+y},\ \alpha^z,$$

and the ratio between any two consecutive ones is

$$\alpha^x,\ \alpha^{y-x},\ \alpha^{z-y},\ \alpha^{x+y-z},$$

respectively. The last one tends to infinity with z by Lemma 4.1. The same argument as the one used in the case $|\beta| > 1$ shows that one may assume that the unit α^{x+y+z} cancels from both sides of the unit equation (5.3), for otherwise we get $x = O(1)$; hence, only finitely many possibilities. Thus, $(\mathbf{0}, \mathbf{0}) \in \Lambda$.

Let $\mathcal{E}$ be again some nondegenerate subequation of (5.3) containing α^{y+z} on the left hand side. If it contains some other unit from the left hand side which is α^z or smaller in absolute value, we get that $\alpha^y = (\alpha^{y+z})/\alpha^z = O(1)$. Thus, we have only finitely many possibilities. If $\mathcal{E}$ contains one of the units α^{z+x} or α^{x+y} from the left hand side, we then get $\alpha^{y-x} = O(1)$, which is what we want. Suppose now $\mathcal{E}$ contains some unit from the left hand side, say of the form

$$\alpha^{x+y+z}\frac{\beta^{j_1x+j_2y+j_3z}}{\alpha^{i_1x+i_2y+i_3z}}, \tag{5.7}$$

where $k = i_1 + i_2 + i_3 > 0$. Then

$$\alpha^{(i_1-1)x+i_2y+i_3z} \ll \beta^{j_1x+j_2y+j_3z}.$$

Since $|\beta| < 1$, the above inequality leads easily to the conclusion that $x = O(1)$, unless $\mathbf{i}_0 = (i_1, i_2, i_3) = (1, 0, 0)$ and $\mathbf{j}_0 = (j_1, j_2, j_3) = (0, 0, 0)$. Thus, $(\mathbf{i}_0, \mathbf{j}_0) \in \Lambda$, which shows that the square of (5.7) appears on the right hand side of equation (5.3). Let $\mathcal{F}$ be some subequation containing α^{y+z-x} from the right hand side of (5.3). Assume that $\mathcal{F}$ contains some unit from the left hand side of (5.3). If this is α^z or some unit of a smaller absolute value, we get that $\alpha^{y-x} \ll O(1)$. Thus, $y - x = O(1)$, which is what we want. If it contains one of α^{y+z}, α^{x+z}, or α^{x+y}, then one of the numbers α^x, α^{y-2x} or α^{z-2x} belongs to a finite list. Thus, either $x = O(1)$, which happens for only finitely many possibilities, or $\min\{y - 2x,\ z - 2x\} = O(1)$, which is what we want.

Finally, assume that $\mathcal{F}$ contains some other unit from the right hand side of equation (5.3) of the form $\alpha^{x+y+z}\beta^{j_1'x+j_2'y+j_3'z}/\alpha^{i_1'x+i_2'y+i_3'z}$. We scale everything

by α^{x+y+z}. If $k \geq 3$, then the largest such unit in absolute value is $1/\alpha^{3x}$. The ratio of $1/\alpha^{2x}$ to this unit is $\gg \alpha^x$, so if this ratio is in a finite set of numbers, we then get $x = O(1)$; hence, only finitely many possibilities. If $k = 2$, then the largest such unit in absolute value which is not $1/\alpha^{2x}$ is $\leq 1/\alpha^{x+y}$. The ratio of $1/\alpha^{2x}$ to such a unit is $\gg \alpha^{y-x}$. So, if this ratio is in a finite set, we get $y - x = O(1)$, as desired. Finally, the only possibilities when $k = 1$ are

$$\frac{1}{\alpha^x}, \quad \frac{1}{\alpha^y}, \quad \frac{1}{\alpha^z}, \quad \left(\frac{\beta}{\alpha}\right)^x, \quad \left(\frac{\beta}{\alpha}\right)^y, \quad \left(\frac{\beta}{\alpha}\right)^z.$$

If $\mathcal{F}$ contains one of these units, we then get that one of

$$\alpha^x, \ \alpha^{y-x}, \ \alpha^{z-x}, \ (\alpha\beta)^x, \ \alpha^{y-2x}\beta^{-y}, \ \alpha^{z-2x}\beta^{-z}$$

belongs to a finite list. In the first case, we get $x = O(1)$. In the next two, we get $y - x = O(1)$, as desired. Finally, since α and β are multiplicatively independent, in the last three cases we get $x = O(1)$; hence, finitely many possibilities also.

In conclusion, we proved that both when $|\beta| > 1$ and $|\beta| < 1$, assuming that α and β are multiplicatively independent, infinitely many of the solutions will have one of $y - x$, $y - 2x$, or $z - 2x$ bounded.

5.3. Proof of the theorem for α and β multiplicatively independent

Suppose first that $y - x = \lambda$ is a fixed number for infinitely many of our solutions. Then

$$a \mid \gamma\alpha^x + \delta\beta^x - 1 \qquad \text{and} \qquad a \mid \gamma\alpha^{x+\lambda} + \delta\beta^{x+\lambda} - 1.$$

Multiplying the first relation above by α^λ and subtracting them, we get that

$$a \mid \delta\beta^x(\alpha^\lambda - \beta^\lambda) - (\alpha^\lambda - 1), \tag{5.8}$$

and, as in the proof of Lemma 3.2, the right hand side above is nonzero for $z > z_0$. Note further that $\alpha^\lambda - \beta^\lambda \neq 0$ because $\lambda \neq 0$ and α/β is not a root of 1. Put $\zeta = \delta^{-1}(\alpha^\lambda - 1)/(\alpha^\lambda - \beta^\lambda)$. Note that $\zeta \neq 0$. Relation (5.8) shows that

$$a \mid \kappa_4(\beta^x - \zeta),$$

where we can take κ_4 to be some fixed positive integer which is divisible by the norm of $|\alpha^\lambda - \beta^\lambda|$ with respect to $\mathbb{K}$. The same argument (interchanging α with β) shows that

$$a \mid \kappa_4(\alpha^x - \eta),$$

where $\eta = \gamma^{-1}(\beta^\lambda - 1)/(\beta^\lambda - \alpha^\lambda)$. The fact that $\eta \neq 0$ follows because $\beta \neq \pm 1$ and $\lambda \neq 0$. Furthermore, both $\alpha^x - \eta$ and $\beta^x - \zeta$ are nonzero. Hence,

$$a \ll N_{\mathbb{K}}\left(\gcd(\alpha^x - \eta, \beta^x - \zeta)\right),$$

where the last expression is to be interpreted as the norm of the ideal greatest common divisor of the two algebraic numbers in $\mathbb{K}$ (see also [21]). Since α and β are multiplicatively independent, the Main Theorem from [5, page 205] shows that $a = \exp(o(x))$ as $x \to \infty$. This contradicts Lemma 4.1 for large values of x.

Suppose now that $y - 2x = \lambda$ for some fixed value of λ. We will get the contradiction by a similar argument as in the first case. It follows

$$a \mid \gamma\alpha^x + (\delta\beta^x - 1) \mid (\gamma\alpha^x)^2 - (\delta\beta^x - 1)^2.$$

Thus,

$$a \mid \gamma^2\alpha^{2x} - \delta^2\beta^{2x} + 2\delta\beta^x - 1 \qquad \text{and} \qquad a \mid \gamma\alpha^{2x+\lambda} + \delta\beta^{2x+\lambda} - 1.$$

Multiplying the first relation above by α^λ, the second by γ, and subtracting them, we get

$$a \mid \beta^{2x}\delta(\gamma\beta^\lambda + \delta\alpha^\lambda) - 2\delta\alpha^\lambda\beta^x + \alpha^\lambda - \gamma.$$

The last expression above is nonzero for large x. Indeed, this expression is a polynomial of degree at most 2 in β^x. If it were zero, then it must happen that all three coefficients $\delta(\gamma\beta^\lambda + \delta\alpha^\lambda)$, $-2\delta\alpha^\lambda$ and $\alpha^\lambda - \gamma$ are zero, which is not the case since $\delta\alpha \neq 0$. Thus,

$$a \mid \kappa_4 P(\beta^x),$$

where $P(X) \in \mathbb{K}[X]$ is a nonzero monic polynomial of degree at most 2. Interchanging β to α in the previous argument, we get that

$$a \mid \kappa_4 Q(\alpha^x),$$

where $Q(X) \in \mathbb{K}[X]$ is some nonzero polynomial of degree at most 2. Hence, at the level of ideals,

$$a \mid \kappa_4 \prod_{\substack{\zeta,\eta \\ P(\zeta)=0,\ Q(\eta)=0}} N_{\mathbb{L}}\left(\gcd(\beta^x - \zeta, \alpha^x - \eta)\right),$$

where $\mathbb{L}$ is the splitting field over $\mathbb{K}$ of $P(X)Q(X)$ and where the roots ζ and η of $P(X)$ and $Q(X)$ in $\mathbb{L}$, respectively, are counted with their multiplicities. If $\zeta\eta \neq 0$, then $N_{\mathbb{K}}(\gcd(\beta^x - \zeta, \alpha^x - \eta)) = |\alpha|^{o(x)}$ as $x \to \infty$ by [5, Main Theorem, page 205]. It remains to deal with the case when one of ζ or η is zero. Assume say that $\zeta = 0$. Let π be any prime ideal dividing β in $\mathbb{K}$. All we need to understand is an upper bound for $\mu_\pi(a)$, where for a number $\omega \in \mathbb{K}$ we use $\mu_\pi(\omega)$ for the exponent of π in the factorization of ω in prime ideals inside $\mathbb{K}$. If π divides also α, then π does not divide $u_x - 1$ for large x. Thus, $\mu_\pi(a) = 0$ in this case. If π does not divide α, then

$$\mu_\pi(u_x - 1) = \mu_\pi(\gamma\alpha^x + \delta\beta^x - 1) \leq \min\{x\mu_\pi(\beta), \mu_\pi(\gamma\alpha^x - 1)\}.$$

By linear forms in π-adic logarithms (see, for example, [22]),

$$\mu_\pi(\gamma\alpha^x - 1) \ll \log x.$$

Thus, for large x, $\mu_\pi(a) \leq \mu_\pi(u_x - 1) \ll \log x$. A similar argument applies to the ideals dividing α. This argument shows that the roots with $\zeta\eta = 0$ contribute a factor of size $|\alpha|^{O(\log x)} = |\alpha|^{o(x)}$ as $x \to \infty$ in a. Consequently,

$$a \leq |\alpha|^{o(x)}$$

holds as $x \to \infty$, contradicting again Lemma 4.1.

The same argument works also in the case $z - 2x = O(1)$, the role of a being played by b. We give no further details.

6. The case α and β multiplicatively dependent

We begin with some remarks about the case when α and β are multiplicatively dependent. Since they are also either rational or quadratic integers, there exist $\rho > 1$, coprime integers $i > 0$ and j, and $\eta \in \{\pm 1\}$, such that $\alpha = \rho^i$ and $\beta = \eta\rho^j$. If $j \geq 0$, then ρ is a rational integer. Otherwise, $i = 1$, $j = -1$, and ρ is a quadratic unit (compare with the arguments in Section 4.5).

Observe now that if $j \geq 0$, then

$$u_n - 1 = \gamma(\rho^n)^i + \eta^n\delta(\rho^n)^j - 1$$

is a polynomial in ρ^n when $\eta = 1$, and one of two polynomials when $\eta = -1$ according to whether n is even or odd. When $j = -1$, then

$$u_n - 1 = \rho^{-n}(\gamma(\rho^n)^2 - \rho^n + \eta^n\delta)$$

is associated (because ρ^{-n} is a unit) to one (if $\eta = 1$), or one of the two (if $\eta = -1$) polynomials of degree 2 in ρ^n with coefficients in $\mathbb{K}$. The following result is very important in what follows.

Lemma 6.1. *All solutions* (x, y, z) *of equation* (1.2) *are contained in the union of finitely many lines in* $\mathbb{Z}^3$.

Proof. We let b_1 and c_1 be the largest divisors of b and c, respectively, which are free of primes dividing ρ. Note that both b/b_1 and c/c_1 are $O(1)$. Indeed, if $j > 0$, then $\rho > 1$ is in $\mathbb{Z}$ and $u_n - 1$ is coprime to ρ for all n sufficiently large. If $j < 0$, then ρ is a unit, so $b_1 = b$ and $c_1 = c$. Finally, if $j = 0$, then, since $\delta\beta^z \neq 1$ and $\delta\beta^y \neq 1$, we get that $\delta\beta^z - 1 = O(1)$ and $\delta\beta^y - 1 = O(1)$ are both nonzero. This justifies that $b/b_1 = O(1)$ and $c/c_1 = O(1)$.

We now fix the class of (x, y, z) modulo $(\mathbb{Z}/2\mathbb{Z})^3$. For $j \geq 0$, we may write

$$bc = u_z - 1 = \gamma P(\rho^z) = \gamma \prod_{i=1}^{\ell} (\rho^z - \mu_i)^{\sigma_i},$$

$$ac = u_y - 1 = \gamma Q(\rho^y) = \gamma \prod_{j=1}^{\ell'} (\rho^y - \mu'_j)^{\sigma'_j}.$$

In the above formulae, $\mu_1, \ldots, \mu_\ell$ are all the distinct roots of $P(X)$ having multiplicities $\sigma_1, \ldots, \sigma_\ell$, respectively. Similarly, $\mu'_1, \ldots, \mu'_{\ell'}$ are the distinct roots of $Q(X)$ of multiplicities $\sigma'_1, \ldots, \sigma'_{\ell'}$, respectively. Note that $\mu_1, \ldots, \mu_\ell, \mu'_1, \ldots, \mu'_{\ell'}$ are all nonzero. Note also that $P(X)$ and $Q(X)$ have degrees i. When $j < 0$, then we write

$$bc = u_z - 1 = \gamma \rho^{-z} P(\rho^z), \qquad \text{and} \qquad ac = u_y - 1 = \gamma \rho^{-y} Q(\rho^y),$$

where now $P(X)$ and $Q(X)$ are monic quadratic polynomials. We keep the notations $\mu_i,\ \sigma_i$ and $\mu'_j,\ \sigma'_j$ with $1 \leq i \leq \ell,\ 1 \leq j \leq \ell'$ for the distinct roots with their corresponding multiplicities of $P(X)$ and $Q(X)$, respectively.

In all cases, we put d for the common degree of $P(X)$ and $Q(X)$.

We now write $\sigma = \max\{\sigma_i, \sigma'_j : 1 \leq i \leq \ell,\ 1 \leq j \leq \ell'\}$, $\mathbb{L}$ for the splitting field of $P(X)Q(X)$ over $\mathbb{K}$, and κ_5 for a positive integer divisible by the denominators of γ, μ_i and μ'_j for all $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$. We then get that

$$\begin{aligned} c_1 \mid \gcd(u_z - 1, u_y - 1) &\mid \gcd(\gamma P(\rho^z), \gamma Q(\rho^y)) \\ &\mid \kappa_5^{d^3+1} \gamma \prod_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq \ell'}} \gcd\left(\rho^z - \mu_i, \rho^y - \mu'_j\right)^{\sigma}. \end{aligned} \tag{6.1}$$

The last product above is to be interpreted as a product of ideals in $\mathbb{L}$.

Now let $T > 2$ be a large positive integer. Consider the set of numbers $\mathcal{T} = \{pz + qy : 1 \leq p \leq T,\ 1 \leq q \leq T\}$. Clearly, all numbers in $\mathcal{T}$ are $\leq 2zT$ for large z. Since there are T^2 pairs of positive integers $(p, q) \in [1, T]^2$, it follows, by the pigeon hole principle, that there there exist $(p, q) \neq (p', q')$ such that $|pz + qy - (p'z + q'y)| \leq 2Tz/(T^2 - 1) < 3z/T$. Write $u = p - p'$ and $v = q - q'$ and assume that $uz + vy \geq 0$ (otherwise, we replace the pair (u, v) by the pair $(-u, -v)$). For $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$, put $c_{1,i,j}$ for the ideal $\gcd(c_1, \rho^z - \mu_i, \rho^y - \mu'_j)$ in $\mathbb{L}$. Since

$$\rho^z \equiv \mu_i \pmod{c_{1,i,j}} \qquad \text{and} \qquad \rho^y \equiv \mu'_j \pmod{c_{1,i,j}},$$

and ρ is invertible modulo c_1, we get that $\rho^{uz+vy} \equiv \mu_i^u \mu_j'^v \pmod{c_{1,i,j}}$. We thus get, using relation (6.1), that

$$c_1 \mid \kappa_5^{2T(d^3+1)} \gamma \prod_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq \ell'}} \left(\rho^{uz+vy} - \mu_i^u \mu_j'^v\right). \tag{6.2}$$

Assume that the right hand side above is nonzero. Then, taking norms in $\mathbb{L}$ and using the fact that $0 \le uz + vy \ll z/T$, we get that

$$c_1 \le \exp(O(z/T + T)).$$

The constant implied by the above O depends on the sequence $(u_n)_{n\ge 0}$. Since $c_1 \gg c \gg \alpha^{z/2}$, we get that

$$\alpha^{z/2} \le \exp(O(z/T + T)),$$

therefore $z \ll z/T + T$. This inequality is false if we first choose $T > 2\kappa_6^{-1}$, where κ_6 is the constant implied by the above O, and then make z large. The contradiction comes from the fact that we have assumed that the right hand side of (6.2) is nonzero for $T = \lfloor \kappa_6^{-1} \rfloor + 1$ once z is large. If the right hand side of (6.2) is zero with this value for T, then $\rho^{uz+vy} = \mu_i^u \mu_j'^v$ for some i, j, u, v, and since ρ is not a root of 1, we get that $uz + vy$ is uniquely determined once i, j, u, v have been fixed.

We now repeat the argument but with x instead of y and with b instead of c. The similar argument leads to the conclusion that unless some equality of the form $\rho^{u'z+v'x} = \mu_i^{u'} \mu_j''^{v'}$ holds with some integers u', v' of absolute values at most T' and not both zero, then $b \le \exp(O(z/T' + T'))$. Here, $\mu_1'', \ldots, \mu_{\ell''}''$ are the roots of the polynomial $R(X)$ such that $u_x - 1$ is associated to $\gamma R(\rho^x)$ in the same way as $u_z - 1$ and $u_y - 1$ were associated to $\gamma P(\rho^z)$ and $\gamma Q(\rho^y)$, respectively. Since $b \gg \alpha^{(1-\kappa_0)z}$ for some constant $\kappa_0 \in (0, 1)$, we get again that $z \ll z/T' + T'$, which is a contradiction if T' is first chosen to be sufficiently large, and then z is allowed to be large. In conclusion, there must exist a relation of the form $\rho^{u'z+v'x} = \mu_i^{u'} \mu_j''^{v'}$, with exponents $u',\ v'$ of sizes $O(1)$, which are not both zero, leading again to the fact that $u'z + v'x = O(1)$. Since we also have $uz + vy = O(1)$, we get that (x, y, z) belongs to one of finitely many effectively computable lines in $\mathbb{Z}^3$. □

Since we have infinitely many solutions (x, y, z) and only finitely many possibilities for the lines in $\mathbb{Z}^3$ on which they might lie, it follows that infinitely many of the x, y and z are of the form

$$x = d_1 t + e_1, \qquad y = d_2 t + e_2, \qquad z = d_3 t + e_3,$$

where $d_1, d_2, d_3, e_1, e_2, e_3$ are fixed integers with the first three positive and t is a positive integer which may be arbitrarily large. Note that $d_3 \ge d_2 \ge d_1 > 0$. We may also fix the parity of t, therefore the signs of $\beta^x,\ \beta^y,\ \beta^z$ are all determined by η and the parities of $e_1,\ e_2$ and e_3. We now distinguish the following cases.

6.1. The case $j > 0$

This is the easiest case. We have

$$ab = u_x - 1 = (\gamma\rho^{ie_1})(\rho^t)^{id_1} + \zeta_1(\delta\rho^{je_1})(\rho^t)^{jd_1} - 1,$$

$$ac = u_y - 1 = (\gamma\rho^{ie_2})(\rho^t)^{id_2} + \zeta_2(\delta\rho^{je_2})(\rho^t)^{jd_2} - 1,$$

$$bc = u_z - 1 = (\gamma\rho^{ie_3})(\rho^t)^{id_3} + \zeta_3(\delta\rho^{je_3})(\rho^t)^{jd_3} - 1,$$

where $\zeta_i = \eta^{e_i} \in \{\pm 1\}$ for $i = 1, 2, 3$. Multiplying the three relations above we get a polynomial with rational coefficients in ρ^t which is a perfect square for infinitely many values of t. It follows easily that this polynomial must be the perfect square of a polynomial with rational coefficients (see, for example, [13]). However, this is impossible because its constant term is -1, which is not a perfect square.

6.2. The case $j = 0$

In this case, $\alpha \in \mathbb{Z}$, $\beta = \pm 1$. We mention that below we will use i and j without the meaning from above. We have

$$ab = u_x - 1 = \gamma_1(\rho^t)^{d_1} + \delta_1,$$
$$ac = u_y - 1 = \gamma_2(\rho^t)^{d_2} + \delta_2,$$
$$bc = u_z - 1 = \gamma_3(\rho^t)^{d_3} + \delta_3,$$

where $\delta_1, \delta_2, \delta_3 \in \{-\delta - 1, \delta - 1\}$ are nonzero and $\gamma_i = \gamma\rho^{e_i}$ for $i = 1, 2, 3$. Let us put $P_i(X) = \gamma_i X^{d_i} + \delta_i$. Then

$$a \mid \gcd(P_1(\rho^t), P_2(\rho^t)),\ b \mid \gcd(P_1(\rho^t), P_3(\rho^t)),\ c \mid \gcd(P_2(\rho^t), P_3(\rho^t)).$$

We now look at $\gcd(P_i(X), P_j(X))$ for $i \neq j$. The roots of $P_i(X)$ in $\mathbb{C}$ are $e^{2\pi i\mu/d_i}\eta_i$, for $\mu = 0, 1, \ldots, d_i - 1$, where η_i is any fixed determination of $(-\delta_i/\gamma_i)^{1/d_i}$. It now follows easily that $\gcd(P_i(X), P_j(X))$ is a polynomial of degree at most $\gcd(d_i, d_j)$. In particular, $\gcd(P_3(X), P_1(X))\cdot \gcd(P_3(X), P_2(X))$ is a polynomial of degree at most $\gcd(d_3, d_3) + \gcd(d_3, d_2)$. Since

$$P_3(\rho^t) = bc \mid \gcd(P_1(\rho^t), P_3(\rho^t))\gcd(P_2(\rho^t), P_3(\rho^t))$$

holds for infinitely many positive integers t, we get that $d_3 \leq \gcd(d_3,d_1)+\gcd(d_3,d_2)$. Since $d_1 \leq d_2 \leq d_3$, the above inequality shows that either $d_3 = d_2$, or $d_1 = d_2 = d_3/2$. We treat only the case $d_1 = d_2$, since the case when $d_2 = d_3$ is similar. Since $d_1 = d_2$ and $y > x$, we get that $e_2 > e_1$. Putting $d = d_1$, we get that $P_1(X)$ is associated to $X^d + \delta_1/\gamma_1$ and $P_2(X)$ is associated to $X^d + \delta_2/\gamma_2$. They have a common root if and only if $\delta_1/\gamma_1 = \delta_2/\gamma_2$. This leads to $\rho^{e_2-e_1} = \delta_2/\delta_1$. If $\delta_2 = \delta_1$, then $e_2 = e_1$, therefore $x = y$, which is a contradiction. This shows that $\delta_2 \neq \delta_1$, therefore δ_2/δ_1 equals either $(\delta - 1)/(-\delta - 1)$, or $(-\delta - 1)/(\delta - 1)$. Changing δ to $-\delta$, if necessary, we may assume that

$$\rho^{e_2-e_1} = -\frac{\delta - 1}{\delta + 1}.$$

Since ρ is an integer, we get that $1 + \delta \mid \delta - 1$, therefore $1 + \delta \mid 2$. Thus, $1 + \delta = -2, -1, 1, 2$. The cases $1+\delta = -2,\ -1,\ 2$ give $\rho^{e_2-e_1} = -2,\ -3,\ 0$, respectively, which are impossible because ρ is positive, while the case $1 + \delta = 1$ gives $\delta = 0$, which is not allowed. This completes the analysis of this case.

6.3. The case $j = -1$

This is by far the most technical one. Again we will use the indices i, j without referring to $\alpha = \rho^i = \rho$, $\beta = \eta\rho^j = \pm\rho^{-1}$. We have that

$$u_x - 1 = \gamma\rho^{x+e_1}((\rho^t)^{2d_1} - \gamma_1(\rho^t)^{d_1} + \delta_1),$$
$$u_y - 1 = \gamma\rho^{y+e_2}((\rho^t)^{2d_2} - \gamma_2(\rho^t)^{d_2} + \delta_2),$$
$$u_z - 1 = \gamma\rho^{z+e_3}((\rho^t)^{2d_3} - \gamma_3(\rho^t)^{d_3} + \delta_3),$$

where $\gamma_i = \gamma^{-1}\rho^{-e_i}$, $\delta_i = \eta_i\delta\gamma^{-1}\rho^{-2e_i}$ and $\eta_i = \eta^{e_i} \in \{\pm 1\}$ for $i = 1, 2, 3$. We put

$$P_i(X) = X^{2d_i} - \gamma_i X^{d_i} + \delta_i = Q_i(X^{d_i}) \qquad \text{for all } i = 1, 2, 3,$$

where $Q_i(X) = X^2 - \gamma_i X + \delta_i$ for $i = 1, 2, 3$. Note that $P(\rho^t) = \prod_{i=1}^3 P_i(\rho^t)$ is associated to a perfect square in $\mathbb{K}$ for infinitely many t. Since $P(X) = \prod_{i=1}^t P_i(X)$ does not have just two simple roots, it follows, again by [13], that $P(X)$ is a square of a polynomial in $\mathbb{K}[X]$. In particular, all roots of $P(X)$ have even multiplicities.

We now fix $i \in \{1, 2, 3\}$ and take a closer look at $P_i(X)$. Let $z_{i,1}$ and $z_{i,2}$ be the roots of $Q_i(X)$. Since $P_i(X) = Q_i(X^{d_i})$, it follows that all roots of $P_i(X)$ are $e^{2\pi i\ell/d_i} z_{i,j}^{1/d_i}$ for $\ell = 0, 1, \ldots, d_i - 1$ and $j = 1, 2$, where $z_{i,1}^{1/d_i}$ and $z_{i,2}^{1/d_i}$ are two fixed determinations of these complex nonzero numbers. Thus, if $P_i(X)$ has a double root, then it must be the case that $e^{2\pi i\ell/d_i} z_{i,1}^{1/d_i} = e^{2\pi i\ell'/d_i} z_{i,2}^{1/d_i}$ for some $\ell, \ell' \in \{0, 1, \ldots, d_i - 1\}$. Upon exponentiating this last relation to the power d_i, we get $z_{i,1} = z_{i,2}$. Thus, $Q_i(X)$ has a double root. This happens if and only if $\gamma_i^2 - 4\delta_i = 0$, which leads to $\eta^{e_i}\gamma\delta = 1/4$. Furthermore, if this is the case, then $z_{i,1} = z_{i,2} = \gamma_i/2$ is an algebraic integer and $P_i(X) = (X^{d_i} - \gamma_i/2)^2$ is the square of a polynomial whose coefficients are algebraic integers in $\mathbb{K}$.

6.3.1. *The case of double roots*

Assume that $P_i(X)$ has a double root for some $i \in \{1, 2, 3\}$. Then writing $\{1, 2, 3\} = \{i, j, k\}$, we get, from the fact that $P(X)$ and $P_i(X)$ are both squares of other polynomials with coefficients in $\mathbb{K}$, that $P_j(X)P_\ell(X)$ is a square of a polynomial with coefficients in $\mathbb{K}$. If $P_j(X)$ has a double root, then again $z_{j,1} = z_{j,2} = \gamma_j/2$ and $P_j(X) = (X^{d_j} - \gamma_j/2)^2$. This leads to the fact that $P_\ell(X)$ is also the square of a polynomial with coefficients in $\mathbb{K}$, therefore $P_\ell(X) = (X^{d_\ell} - \gamma_\ell/2)^2$.

Put $R(X) = \prod_{i=1}^3 (X^{d_i} - \gamma_i/2)$. Thus, $R(X)$ is monic and $P(X) = R^2(X)$. For a fixed t even, we have that abc is associated in $\mathbb{K}$ to $\gamma^{1/2}R(\rho^t)$. Indeed, note that $(abc)^2 = \gamma^3\rho^{x+y+z+e_1+e_2+e_3} \cdot R^2(\rho^t)$, and

$$x + y + z + e_1 + e_2 + e_3 = t(d_1 + d_2 + d_3) + 2(e_1 + e_2 + e_3)$$

is even, therefore $\gamma^{1/2}$ must be a member of $\mathbb{K}$. Since bc is associated to $\gamma^2 P_3(\rho^t) =$

$\gamma^2((\rho^t)^{d_3} - \gamma_3/2)^2$, we have that a is associated to $H(\rho^t)$, where

$$H(X) = \gamma^{1/2}\gamma^{-2}\frac{(X^{d_1} - \gamma_1/2)(X^{d_2} - \gamma_2/2)}{(X^{d_3} - \gamma_3/2)}.$$

We now show that $H(X)$ is a polynomial. Assume that this is not so and let $H(X) = F(X)/G(X)$, where $G(X)$ is of positive degree and $F(X)$ and $G(X)$ are coprime. Then the algebraic integer $G(\rho^t)$ in $\mathbb{K}$ divides the resultant $\mathrm{Res}_X(F(X), G(X))$ evaluated at $X = \rho^t$, which is a nonzero algebraic integer in $\mathbb{K}$, since $H(\rho^t)$ is associated to a and thus $G(\rho^t)$ divides $F(\rho^t)$. Thus, $G(\rho^t)$ is associated to some element from a finite list in $\mathbb{K}$. However, since $G(X)$ is of positive degree and does not have zero as a root, this resulting Diophantine equation has only finitely many positive integer solutions t. In fact, by the classical theory of Diophantine equations (see [20], for example), this Diophantine equation can be immediately reduced to a unit equation in three terms in $\mathbb{K}[(\gamma_3/2)^{1/d_3}]$. This contradiction shows that $H(X)$ is a polynomial, therefore that $X^{d_3} - \gamma_3/2$ divides $(X^{d_1} - \gamma_1/2)(X^{d_2} - \gamma_2/2)$. The polynomials $X^{d_3} - \gamma_3/2$ and $X^{d_i} - \gamma_i/2$ can have at most $\gcd(d_3, d_i)$ roots in common for $i = 1, 2$. Thus, $d_3 \le \gcd(d_3, d_1) + \gcd(d_3, d_1)$. Since $d_3 \ge d_2 \ge d_1$, it follows that either $d_3 = d_2$, or $d_1 = d_2 = d_3/2$. If $d_3 = d_2$, then by putting $d = d_3$ and using the fact that $X^d - \gamma_3/2$ and $X^d - \gamma_2/2$ have a root in common, we also get $\gamma_3 = \gamma_2$, therefore $\rho^{e_2} = \rho^{e_3}$. Thus, $z = y$ which is not allowed. Finally, if $d_1 = d_2$, then using the fact that also $X^{d_1} - \gamma_1/2$ and $X^{d_2} - \gamma_2/2$ have a root in common (because a becomes arbitrarily large), we get that $\gamma_1 = \gamma_2$, therefore $e_1 = e_2$, leading to $x = y$, which is again not allowed.

We now return to the situation where $P_i(X) = (X^{d_i} - \gamma_i/2)^2$ but $P_j(X)$ does not have a double root. Then $P_\ell(X)$ does not have a double root either, and since $P_j(X)P_\ell(X)$ is a square, we get that $P_j(X) = P_\ell(X)$. By identifying degrees and coefficients, we get $d_j = d_\ell$ and $\gamma_j = \gamma_\ell$. The last equation implies that $\rho^{e_j} = \rho^{e_\ell}$; hence, $e_j = e_j$. Since $(d_j, e_j) = (d_\ell, e_\ell)$, we get again that the two of the three variables $\{x, y, z\}$ corresponding to j and ℓ are equal, which is impossible.

6.3.2. *Bounding the number of common roots*

From now on, we can assume that all three polynomials $P_1(X)$, $P_2(X)$ and $P_3(X)$ have only simple roots. We look at

$$P_3(X) = (X^{d_3} - z_{3,1})(X^{d_3} - z_{3,2}),$$

and count the number of common roots that $P_3(X)$ can have with $P_i(X)$ for some $i = 1, 2$. Let

$$P_i(X) = (X^{d_i} - z_{i,1})(X^{d_i} - z_{i,2}).$$

Note that both $P_3(X)$ and $P_i(X)$ are product of two binomial polynomials. Our aim is to show that $P_3(X)$ has $\le 2\gcd(d_3, d_1)$ roots in common with each of $P_i(X)$ for $i = 1, 2$.

Assume say that $z_{3,1}/z_{3,2}$ is not a root of 1. Suppose that $z_{i,1}/z_{i,2}$ is not a root of 1 either. Then, since all roots of $X^{d_3} - z_{3,1}$ differ one from another multiplicatively by roots of unity, it follows that if $X^{d_3} - z_{3,1}$ has a root in common

with $X^{d_i} - z_{i,j}$, then it will not have a root in common with $X^{d_i} - z_{i,\ell}$, where $\{j, \ell\} = \{1, 2\}$. Thus, in this case there exists at most one $j \in \{1, 2\}$ such that $X^{d_3} - z_{3,1}$ has a common root with $X^{d_i} - z_{i,j}$, and clearly the number of such roots is $\leq \gcd(d_3, d_i)$. Hence, $X^{d_3} - z_{3,1}$ has at most $\gcd(d_3, d_i)$ common roots with $P_i(X)$. The same is true for $X^{d_3} - z_{3,2}$. Hence, in this case the number of common roots of $P_3(X)$ and $P_i(X)$ is $\leq 2\gcd(d_3, d_i)$.

Assume now that still $z_{3,1}/z_{3,2}$ is not a root of 1, but that $z_{i,1}/z_{i,2}$ is a root of 1. If each of $X^{d_3} - z_{3,i}$ for $i = 1, 2$ has common roots with at most one of the two binomials $X^{d_i} - z_{i,j}$ for $j = 1, 2$, then the above argument shows again that the number of common roots of $P_3(X)$ and $P_i(X)$ is at most $2\gcd(d_3, d_i)$. If say $X^{d_3} - z_{3,1}$ has common roots with both $X^{d_i} - z_{i,1}$ and $X^{d_i} - z_{i,2}$, then it has at most $\gcd(d_3, d_i)$ common roots with each one of them, while $X^{d_3} - z_{3,2}$ does not have common roots neither with $X^{d_i} - z_{i,1}$, nor with $X^{d_i} - d_{i,2}$, since otherwise $z_{3,1}/z_{3,2}$ will end up being a root of 1, which is not the case. Hence, again $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_3, d_i)$ roots in common.

Assume next that $z_{3,1}/z_{3,2}$ is a root of 1, but that $z_{i,1}/z_{i,2}$ is not. If both $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ have common roots with $P_i(X)$, then these common roots will be roots of $X^{d_i} - z_{i,j}$ for the same value of j. Thus, each of $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ will have at most $\gcd(d_3, d_i)$ common roots with $X^{d_i} - z_{i,j}$ (and none common with $X^{d_i} - z_{i,\ell}$, where ℓ is such that $\{j, \ell\} = \{1, 2\}$), so again $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_3, d_i)$ roots in common. Of course, if only one of $X^{d_3} - z_{3,j}$ for $j = 1, 2$ has common roots with $P_i(X)$, then again it will have common roots with only one of $X^{d_i} - z_{i,\ell}$ for $\ell = 1, 2$, and the number of such is $\leq \gcd(d_3, d_i)$, so in this case $P_3(X)$ and $P_i(X)$ have at most $\gcd(d_3, d_i) < 2\gcd(d_3, d_i)$ common roots.

So far, we have always obtained that $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_i, d_3)$ roots in common.

Assume now finally that both $z_{3,1}/z_{3,2}$ and $z_{i,1}/z_{i,2}$ are roots of 1.

Note that by definition we have $Q_i(X) = (X - z_{i,1})(X - z_{i,2}) = X^2 - \gamma_i X + \delta_i$ with $\gamma_i = \gamma^{-1}\rho^{-e_i}$, $\delta_i = \eta^{e_i}\delta\gamma^{-1}\rho^{-2e_i}$. Therefore, it follows that $(z_{i,1}\gamma\rho^{e_i}, z_{i,2}\gamma\rho^{e_i})$ are the roots of $X^2 - X + \eta^{e_i}\gamma\delta$, and $\gamma\delta \in \mathbb{Q}^*$ because γ and δ are conjugates in $\mathbb{K}$. Thus, while $z_{i,1}$, $z_{i,2}$ might belong to a quadratic field over $\mathbb{K}$ (hence, a field of degree 4 over $\mathbb{Q}$), their ratio belongs to a quadratic field. Thus, if $z_{i,1}/z_{i,2} \neq 1$ is a root of 1, then its order is one of 2, 3, 4, or 6. Note next that the order cannot be 2 (*i.e.*, $z_{i,1} = -z_{i,2}$), because the coefficient of X in the quadratic polynomial $X^2 - X + \eta^{e_i}\gamma\delta$ is not zero. Hence, $z_{i,1}/z_{i,2}$ is a root of unity of order 3, 4, or 6. One checks easily that $z_{i,1}/z_{i,2}$ is a root of 1 of order 3, 4, 6, respectively, if and only if $\eta^{e_i}\gamma\delta = 1$, $1/2$, or $1/3$, respectively. Since we are discussing the case when both $z_{3,1}/z_{3,2}$ and $z_{i,1}/z_{i,2}$ are roots of unity, we deduce that either $\eta = 1$, or $\eta = -1$ and $e_i \equiv e_3 \pmod 2$, and in any case these two roots of unity have the same order. Let this order be $k \in \{3, 4, 6\}$, and put $\varepsilon = e^{2\pi i/k}$.

If each of $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ has common roots with at most one of two polynomials $X^{d_i} - z_{i,1}$ and $X^{d_i} - z_{i,2}$, then the previous argument shows that $P_3(X)$ and $P_i(X)$ have at most $2\gcd(d_3, d_i)$ roots in common. Further, if at most one of

the two polynomials $X^{d_3} - z_{3,1}$ and $X^{d_3} - z_{3,2}$ has common roots with $P_i(X)$, then again the previous argument shows that the number of common roots of $P_3(X)$ and $P_i(X)$ is at most $2\gcd(d_3, d_i)$.

We now look at the remaining cases. Here, we shall show that the number of common roots of $P_3(X)$ and $P_i(X)$ is $< d_3$.

We start by noting that up to relabeling the roots of $P_i(X)$, we may assume that $z_{i,1} = z_i$, that $z_{i,2} = z_i\varepsilon$, and that $X^{d_3} - z_{3,1}$ has a root in common with $X^{d_i} - z_i$, and another root in common with $X^{d_i} - z_i\varepsilon$. Certainly, $z_{3,2} = z_{3,1}\varepsilon^{\pm 1}$, and $X^{d_3} - z_{3,2}$ has a root in common with at least one of $X^{d_i} - z_i$ or $X^{d_i} - z_i\varepsilon$.

Since $X^{d_3} - z_{3,1}$ has a root in common with $X^{d_i} - z_i$, we get that there is a number ν such that $\nu^{d_3} = z_{3,1}$ and $\nu^{d_i} = z_i$. Thus,

$$P_i(X) = (X^{d_i} - \nu^{d_i})(X^{d_i} - \nu^{d_i}\varepsilon).$$

Since $X^{d_3} - \nu^{d_3}$ has also a root in common with $X^{d_i} - \nu^{d_i}\varepsilon$, it follows that for some integers j and ℓ we have

$$\nu e^{2\pi i j/d_3} = \nu e^{2\pi i/(kd_i) + 2\pi i \ell/d_i}.$$

Thus,

$$\frac{1}{kd_i} \in \frac{\ell}{d_i} - \frac{j}{d_3} + \mathbb{Z},$$

implying that $\mathrm{lcm}[d_3, d_i]$ is a multiple of kd_i. Thus,

$$kd_i \le \mathrm{lcm}[d_3, d_i] = d_3 d_i / \gcd(d_3, d_i),$$

giving $\gcd(d_3, d_i) \le d_3/k$.

Suppose first that $X^{d_3} - z_{3,2}$ does not have a common root with both of $X^{d_i} - z_i$ and $X^{d_i} - z_i\varepsilon$. Then $P_3(X)$ and $P_i(X)$ have at most $3\gcd(d_3, d_i) \le 3d_3/k$ roots in common. Note that $3d_3/k \le d_3$. Thus, $P_3(X)$ and $P_i(X)$ have at most d_3 roots in common. Let us show that in fact the inequality is strict. From the above arguments, the inequality is strict unless $k = 3$ and $\gcd(d_3, d_i) = d_3/3$. Put $\gcd(d_3, d_i) = \lambda$. Then $d_3 = 3\lambda$ and $d_i \in \{\lambda, 2\lambda\}$. If $d_i = \lambda$, then $P_i(X)$ has a totality of $2\lambda < d_3$ roots, and we obtain a contradiction. Thus, $d_i = 2\lambda$. Hence,

$$P_3(X) = (X^{3\lambda} - \nu^{3\lambda})(X^{3\lambda} - \nu^{3\lambda}\varepsilon^{\pm 1}), \qquad P_i(X) = (X^{2\lambda} - \nu^{2\lambda})(X^{2\lambda} - \nu^{2\lambda}\varepsilon).$$

However, it is now easy to see that $X^{3\lambda} - \nu^{3\lambda}\varepsilon^{\pm 1}$ cannot have a common root with $P_i(X)$. Indeed, any such common root x will satisfy $x^{3\lambda} = \nu^{3\lambda}\varepsilon^{\pm 1}$ and either $x^{2\lambda} = \nu^{2\lambda}$ (leading to $\nu^{6\lambda}\varepsilon^{\pm 2} = x^{6\lambda} = \nu^{6\lambda}$, which is false since $\varepsilon^{\pm 2} \ne 1$), or $x^{2\lambda} = \nu^{2\lambda}\varepsilon$ (leading to $\nu^{6\lambda}\varepsilon^{\pm 2} = x^{6\lambda} = \nu^{6\lambda}\varepsilon^3$, which is again false since $\varepsilon^3 = 1$ and $\varepsilon^{\pm 2} \ne 1$).

So, it remains to treat the case when also $X^{d_3} - z_{1,3}\varepsilon^{\pm 1}$ has a root in common with both $X^{d_i} - z_i$ and $X^{d_i} - z_i\varepsilon$. With the previous notations, since $X^{d_3} - \nu^{d_3}\varepsilon^{\pm 1}$

and $X^{d_i} - \nu^{d_i}$ have a root in common, we get that for some integers j and ℓ we have $\nu e^{\pm 2\pi i/(kd_3)+2\pi ij/d_3} = \nu e^{2\pi i\ell/d_i}$. This leads to

$$\pm\frac{1}{kd_3} \in \frac{\ell}{d_i} - \frac{j}{d_3} + \mathbb{Z},$$

so $\operatorname{lcm}[d_3, d_i]$ is a multiple of kd_3. Thus, $kd_3 \le \operatorname{lcm}[d_3, d_i]$, leading to $\gcd(d_3, d_i) \le d_i/k$. In particular, $d_i \ne d_3$. Write $\lambda = \gcd(d_3, d_i)$. Then $d_i \ge k\lambda$, therefore $d_3 \ge (k+1)\lambda$. Thus, $\lambda \le d_3/(k+1)$. Since $P_3(X)$ and $P_i(X)$ have at most 4λ roots in common anyway, we get that the number of common roots of these two polynomials is $\le 4d_3/(k+1) \le d_3$. Equality is obtained if and only if $k = 3$ and $d_3 = 4\lambda$. Clearly, d_i cannot be λ (otherwise $P_i(X)$ and $P_3(X)$ will have at most $2d_i \le 2\lambda < d_3$ roots in common), and $d_i \ne 2\lambda$, for otherwise $\lambda = \gcd(d_3, d_i) = 2\lambda$, which is a contradiction. So, it must be the case that $d_i = 3\lambda$. Hence,

$$P_3(X) = (X^{4\lambda} - \nu^{4\lambda})(X^{4\lambda} - \nu^{4\lambda}\varepsilon^{\pm 1}), \qquad P_i(X) = (X^{3\lambda} - \nu^{3\lambda})(X^{3\lambda} - \nu^{3\lambda}\varepsilon).$$

Note now that the second factor of $P_i(X)$ above cannot have a common root x with the first factor of $P_3(X)$ above, for if not, we would have $\nu^{12\lambda} = x^{12\lambda} = \nu^{12\lambda}\varepsilon^4$, therefore $\varepsilon^4 = 1$, which is false.

Having covered all the possibilities, we get that $P_3(X)$ has $< d_3$ common roots with $P_i(X)$. If this is true for both i, $j \in \{1, 2\}$, it follows that there is a root of $P_3(X)$ which is not a root of $P_1(X)P_2(X)$, and this is a contradiction because $P_1(X)P_2(X)P_3(X)$ has the property that all its roots are double.

So, there could be at most one $i \in \{1, 2\}$ such that $P_3(X)$ has $< d_3$ roots in common with $P_i(X)$, and for $j \notin \{i, 3\}$, $P_3(X)$ and $P_j(X)$ have at most $2\gcd(d_3, d_j)$ roots in common. If $\gcd(d_3, d_j) \ne d_3$, it follows that $\gcd(d_3, d_j) \le d_3/2$, so $P_3(X)$ has $< 2d_3$ roots in common with $P_1(X)P_2(X)$, which is false. So, it must be the case that $\gcd(d_3, d_j) = d_3$, so $d_j = d_3$. Write $d = d_3$. Thus,

$$P_3(X) = (X^d - z_{3,1})(X^d - z_{3,2}), \qquad P_j(X) = (X^d - z_{j,1})(X^d - z_{j,2}).$$

But it is clear that if the above polynomials have more than d roots in common, then they will have all roots in common so they will coincide. In particular, $d_3 = d_j$ and $\gamma_3 = \gamma_j$, leading to $e_3 = e_j$, so we get again the contradiction that two of the positive integer unknowns x, y and z are equal. Hence, $P_3(X)$ and $P_j(X)$ have at most d_3 roots in common, therefore $P_3(X)$ and $P_1(X)P_2(X)$ have less than $2d_3$ roots in common, which is false.

In conclusion, it must be the case that $P_3(X)$ has $\le 2\gcd(d_3, d_i)$ roots in common with each of $P_i(X)$ for $i = 1, 2$. Thus, $2d_3 \le 2\gcd(d_3, d_1) + 2\gcd(d_3, d_2)$, therefore either $d_2 = d_3$, or $d_1 = d_2 = d_3/2$. Assume that $d_1 = d_2 = d_3/2$. Then $P_3(X)$ has at most d_3 roots in common with each of $P_1(X)$ and $P_2(X)$. Since all its roots are common to either $P_1(X)$ or $P_2(X)$, we get that $P_3(X)$ and $P_1(X)P_2(X)$ are monic and have the same roots which are all simple for each of these two polynomials. Hence, $P_3(X) = P_1(X)P_2(X)$. Evaluating this in $X = \rho^t$ with large t, we get that $a = O(1)$, which is a contradiction.

6.3.3. *The case $d_1 < d_2 = d_3$*

Let $d = d_2 = d_3$. Then the two polynomials

$$P_3(X) = (X^d - z_{3,1})(X^d - z_{3,2}), \qquad P_2(X) = (X^d - z_{2,1})(X^d - z_{2,3})$$

cannot have more than d root in common, for otherwise, by an argument already used before, we would get that they coincide, therefore $z = y$, which is a contradiction. Thus, $P_3(X)$ and $P_2(X)$ have exactly d roots in common, therefore $P_3(X)$ and $P_1(X)$ also have d roots in common. Since the number of such roots is $\leq 2\gcd(d_3, d_1)$, we get that either $d_1 = d$, or $d_1 = d/2$. Assume that $d_1 = d/2$. Then $P_1(X)$ divides $P_3(X)$. Furthermore, up to relabeling the roots of $Q_2(X)$, it follows that we may assume that $\gcd(P_3(X), P_2(X)) = X^d - z_{2,1}$. Then $P_1(X)P_2(X)P_3(X) = P_1(X)^2(X^d - z_{2,1})^2(X^d - z_{2,2})$, and since this must be the square of a polynomial with coefficients in $\mathbb{K}$, we get that $X^d - z_{2,2}$ is a square of a polynomial with coefficients in $\mathbb{K}$, and this is false again.

6.3.4. *The case $d = d_1 = d_2 = d_3$*

It now follows immediately that $Q_1(X)Q_2(X)Q_3(X)$ must be a perfect square of a polynomial of degree 3 with coefficients in $\mathbb{K}[X]$. Furthermore, $Q_i(X)$ and $Q_j(X)$ have precisely one root in common for all $i \neq j \in \{1, 2, 3\}$. We now analyze this last situation.

Assume first that either $\eta = 1$, or $\eta = -1$ but that $e_1,\ e_2,\ e_3$ are all congruent modulo 2. Let us write u and v for the roots of $X^2 - X + \eta^e\gamma\delta$, where the value of e modulo 2 is congruent to e_i ($i = 1, 2, 3$) in case $\eta = -1$. It then follows that $Q_i(X)$ has roots $u\gamma^{-1}\rho^{-e_i}$ and $v\gamma^{-1}\rho^{-e_i}$. Note that since $Q_i(X) \in \mathbb{K}[X]$ for all $i \in \{1, 2, 3\}$, and any two of them have precisely one root in common, it follows that $u,\ v \in \mathbb{K}$. Furthermore, since $u/v \neq \pm 1$, and $\mathbb{K}$ is real, it follows, up to interchanging u and v, that we may assume $|u| > |v|$. Since the root $u\gamma^{-1}\rho^{-e_i}$ is also a root of $Q_j(X)$ for some $j \in \{1, 2, 3\}\backslash\{i\}$, we get that either $u\gamma^{-1}\rho^{-e_i} = u\gamma^{-1}\rho^{-e_j}$, leading to $e_i = e_j$, therefore two of the positive integer unknowns $x,\ y$ and z are equal, which is impossible, or for each i there is $j \neq i$ such that $u\gamma^{-1}\rho^{-e_i} = v\gamma^{-1}\rho^{-e_j}$. Thus, $u/v = \rho^{e_i - e_j}$, and since $|u| > |v|$ and $\rho > 1$, we get that $e_i > e_j$. Thus, for each $i \in \{1, 2, 3\}$, there is $j \neq i$ in the same set such that $e_i > e_j$. This is of course impossible because there must be some index i such that $e_i = \min\{e_j : j \in \{1, 2, 3\}\}$.

Finally, we assume that $\eta = -1$ and that not all e_i are congruent modulo 2 for $i = 1, 2, 3$. Thus, there are two of them, say i and j such that $e_i \equiv e_j \pmod 2$, and the third one ℓ is such that $e_\ell \not\equiv e_i \pmod 2$. Let $e \equiv e_i \pmod 2$, and we assume that u and v are the roots of $X^2 - X + (-1)^e\gamma\delta$, and that u_1 and v_1 are the roots of $X^2 - X - (-1)^e\gamma\delta$. An argument used previously shows that u, v, u_1, v_1 are all in $\mathbb{K}$. In particular, they are real. Then the pairs of roots of $Q_i(X),\ Q_j(X)$ and $Q_\ell(X)$ are $(u\gamma^{-1}\rho^{-e_i}, v\gamma^{-1}\rho^{-e_i})$, $(u\gamma^{-1}\rho^{-e_j}, v\gamma^{-1}\rho^{-e_j})$, and $(u_1\gamma^{-1}\rho^{-e_\ell}, v_1\gamma^{-1}\rho^{-e_\ell})$, respectively. Up to interchanging u and v, we may assume that $u\gamma^{-1}\rho^{-e_i}$ is also a root of $Q_j(X)$. If $u\gamma^{-1}\rho^{-e_i} = u\gamma^{-1}\rho^{-e_j}$, we

then get again $e_i = e_j$, which leads again to the conclusion that two of the three positive integer unknowns x, y and z coincide, which is false. Thus, $u\gamma^{-1}\rho^{-e_i} = v\gamma^{-1}\rho^{-e_j}$, so $u/v = \rho^{e_i - e_j}$. In particular, $(-1)^e\delta\gamma = uv = v^2(u/v) = v^2\rho^{e_i-e_j}$ is a positive number. Now each of the roots of $Q_\ell(X)$ is also a root of $Q_i(X)$ or $Q_j(X)$. In particular, $u_1\gamma^{-1}\rho^{-e_\ell} = w_1\gamma^{-1}\rho^{-e_m}$ and $v_1\gamma^{-1}\rho^{-e_\ell} = w_2\gamma^{-1}\rho^{-e_n}$, where w_1, $w_2 \in \{u, v\}$, and m, $n \in \{i, j\}$. Hence, $(-1)^{e+1}\delta\gamma = u_1v_1 = w_1w_2\rho^{2e_\ell - e_m - e_n}$, but this last number is positive since $\rho > 1$ and $w_1w_2 \in \{u^2, v^2, uv\}$. This contradicts the fact that $(-1)^e\gamma\delta > 0$, and completes the proof of Theorem 1.1.

References

[1] Y. BUGEAUD, P. CORVAJA and U. ZANNIER, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z. **243** (2003), 79–84.

[2] Y. BUGEAUD and A. DUJELLA, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. **135** (2003), 1–10.

[3] Y. BUGEAUD and F. LUCA, *On the period of the continued fraction expansion of square root of $2^{2n+1} + 1$*, Indag. Math. (N.S.) **16** (2005), 21–35.

[4] P. CORVAJA and U. ZANNIER, *Diophantine equations with power sums and Universal Hilbert Sets*, Indag. Math. (N.S.) **9** (1998), 317–332.

[5] P. CORVAJA and U. ZANNIER, *A lower bound for the height of a rational function at S-unit points*, Monatsh. Math. **144** (2005), 203–224.

[6] P. CORVAJA and U. ZANNIER, *S-unit points on analytic hypersurfaces*, Ann. Sci. École Norm. Sup. (4) **38** (2005), 76–92.

[7] A. DUJELLA, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[8] A. DUJELLA, *Diophantine m-tuples*, webpage available at http://web.math.hr/∼duje/dtuples.html.

[9] C. FUCHS, *An upper bound for the G.C.D. of two linear recurring sequences*, Math. Slovaca **53** (2003), 21–42.

[10] C. FUCHS, *Diophantine problems with linear recurrences via the Subspace Theorem*, Integers **5** (2005), #A08.

[11] C. FUCHS, *Polynomial-exponential equations involving multirecurrences*, Studia Sci. Math. Hungar., to appear.

[12] C. FUCHS and A. SCREMIN, *Polynomial-exponential equations involving several linear recurrences*, Publ. Math. Debrecen **65** (2004), 149–172.

[13] W. J. LEVEQUE, *On the equation $y^m = f(x)$*, Acta Arith. **9** (1964), 209–219.

[14] F. LUCA, *On shifted products which are powers*, Glas. Mat. Ser. III **40** (2005), 13–20.

[15] F. LUCA, *On the greatest common divisor of $u - 1$ and $v - 1$ with u and v near $\mathcal{S}$-units*, Monatsh. Math. **146** (2005), 239–256.

[16] F. LUCA and T. N. SHOREY, *Diophantine equations with products of consecutive terms in Lucas sequences, II*, Acta Arith., to appear.

[17] F. LUCA and L. SZALAY, *Fibonacci Diophantine triples*, Glas. Mat. Ser. III **43** (2008), 252–264.

[18] H. P. SCHLICKEWEI and W. M. SCHMIDT, *Linear equations in members of recurrence sequences*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **20** (1993), 219–246.

[19] W. M. SCHMIDT, *Linear Recurrence Sequences and Polynomial-Exponential Equations*, In: "Diophantine Approximation, Proc. of the C.I.M.E. Conference, Cetraro (Italy) 2000", F. Amoroso, U. Zannier (eds.), Springer-Verlag, LN **1819**, 2003, 171–247.

[20] T. N. SHOREY and R. TIJDEMAN, "Exponential Diophantine Equations", Cambridge Univ. Press, Cambridge, 1986.

[21] J. SILVERMAN, *Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups*, Monats. Math. **145** (2005), 333–350.
[22] K. R. YU, *p-adic logarithmic forms and group varieties, II*, Acta Arith. **89** (1999), 337–378.
[23] U. ZANNIER, "Some applications of Diophantine Approximation to Diophantine Equations (with special emphasis on the Schmidt Subspace Theorem)", Forum, Udine, 2003.
[24] U. ZANNIER, *Diophantine equations with linear recurrences. An overview of some recent progress*, J. Théor. Nombres Bordeaux **17** (2005), 423–435.

Department of Mathematics
ETH Zürich, Rämistrasse 101
8092 Zürich, Switzerland
clemens.fuchs@math.ethz.ch

Instituto de Matemáticas
Universidad Nacional
Autónoma de México
C.P. 58180
Morelia, Michoacán, México
fluca@matmor.unam.mx

Department of Mathematics
and Statistics
University of West Hungary
9400, Sopron
Bajcsi-Zs. út 4, Hungary
laszalay@ktk.nyme.hu