A Remark on Prime Divisors of Lengths of Sides of Heron Triangles

István Gaál, István Járási, and Florian Luca

CONTENTS

A *Heron* triangle is a triangle having the property that the lengths of its sides as well as its area are positive integers. Let $\mathcal{P}$ be a fixed set of primes; let S denote the set of integers divisible only by primes in $\mathcal{P}$. We prove that there are only finitely many Heron triangles whose sides $a, b, c \in S$ and are reduced, that is $\gcd(a, b, c) = 1$. If $\mathcal{P}$ contains only one prime $\equiv 1 \pmod 4$, then all these triangles can be effectively determined. In case $\mathcal{P} = \{2, 3, 5, 7, 11\}$, all such triangles are explicitly given.

2000 AMS Subject Classification: Primary 11Y50, 11D57

Keywords: Heron triangle, S-unit equation, reduction

1. INTRODUCTION

There are several open questions concerning the existence of Heron triangles with certain properties. For example (see [Guy 94]), it is not known whether there exist Heron triangles having the property that the lengths of all their medians are positive integers, and it is not known (see [Harborth and Kemnitz 90] and [Harborth et al. 96]) whether there exist Heron triangles having the property that the lengths of all their sides are Fibonacci numbers. A different unsolved problem which asks for the existence of a perfect cuboid, i.e., a rectangular box having the lengths of all the sides, face diagonals, and main diagonal integers has been related (see [Luca 00]) to the existence of a Heron triangle having the lengths of its sides perfect squares and the lengths of its bisectors positive integers.

Let $a,\ b,\ c$ be three positive integers which can be the sides of an arbitrary triangle and let $d := \gcd(a, b, c)$. It is then easy to see that the triangle whose sides have lengths $a,\ b,\ c$ is Heron (i.e., its area is an integer), if and only if the triangle whose sides have lengths $\frac{a}{d},\ \frac{b}{d},\ \frac{c}{d}$ is Heron as well. Thus, we will restrict our analysis to the Heron triangles which are *reduced*, i.e., for which the greatest common divisor of the lengths of all its sides is 1.

Let $a,\ b,\ c$ be the sides of a reduced Heron triangle and let A be its area. Set $s := \dfrac{a+b+c}{2}$ to be its semiperimeter. By the Heron formula, we get

$$A = \sqrt{s(s-a)(s-b)(s-c)}, \tag{1–1}$$

which is equivalent to

$$(4A)^2 = -a^4 - b^4 - c^4 + 2a^2b^2 + 2a^2c^2 + 2b^2c^2. \tag{1–2}$$

It is easy to see that precisely one of the three numbers $a,\ b,\ c$ is even and the other two are odd. Notice that the point $(x, y, z, t) = (a, b, c, 4A)$ lies on the surface

$$-x^4 - y^4 - z^4 + 2x^2y^2 + 2x^2z^2 + 2y^2z^2 = t^2. \tag{1–3}$$

But conversely, if (x, y, z, t) are positive integers satisfying Equation (1–3), then $x,\ y,\ z$ are the sides of a triangle whose area is an integer. Clearly, we may assume that $\gcd(x,\ y,\ z) = 1$, because with $d := \gcd(x, y, z)$, we get that $d^2 \mid t$ and that the positive integer point $(x_1, y_1, z_1, t_1) = \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}, \frac{t}{d^2}\right)$ satisfies Equation (1–3) as well. Since $x,\ y,$ and z have no nontrivial common divisor, by looking at Equation (1–3) modulo 8, it follows immediately that exactly one of the three numbers $x,\ y,$ and z is even and the other two are odd. In particular, all four numbers $x + y + z,\ x + y - z,\ x + z - y,$ and $y + z - x$ are even, and now rewriting Equation (1–3) as

$$(x + y + z)(x + y - z)(x + z - y)(y + z - x) = t^2, \tag{1–4}$$

we get that $4 \mid t$. Moreover, since $x,\ y,$ and z are positive, from Equation (1–4), we also read that $x,\ y,$ and z form a triangle (i.e., the largest one is smaller than the sum of the other two), and the area of this triangle is $t/4$, therefore an integer. Thus, the study of Heron triangles reduces to the study of the positive integer solutions of Equation (1–3).

For any nonzero integer k, let $P(k)$ be the largest prime divisor of k with the convention that $P(\pm 1) = 1$. In [Kramer and Luca 00], it is shown that $P(A) \to \infty$ when $\max(a, b, c)$ tends to infinity over all the triples (a, b, c) which are the sides of reduced Heron triangles and all Heron triangles having $P(A) < 5$ were computed. In [Luca 03], all the Heron triangles whose sides are prime powers were found. In this note, we prove the following theorem.

Theorem 1.1. *$P(abc) \to \infty$ when $\max(a, b, c)$ tends to infinity over the triples of positive integers (a, b, c) which are the sides of reduced Heron triangles.*

Very few results of this kind have been proved so far. Until recently, it was not even known that for distinct positive integers $a,\ b,\ c$ the number $P((ab+1)(ac+1)(bc+1))$ tends to infinity when $\max(a, b, c)$ tends to infinity, although partial results concerning this problem appeared in [Bugeaud 98], [Győry et al. 96], [Győry and Sárközy 97], and [Stewart and Tijdeman 97]. The fact that this is indeed the case has been shown in [Corvaja and Zannier 03] and [Hernández and Luca 03]. The proof of Theorem 1.1 is based on the finiteness of number of solutions of an $\mathcal{S}$-unit equation and as such is ineffective. We can obtain an effective result at the cost of assuming that the prime divisors of abc have a certain shape.

Theorem 1.2. *Let $\mathcal{P}$ be a finite set of prime numbers containing only one prime $p \equiv 1 \pmod 4$. Let $\mathcal{S}$ be the set of all positive integers whose prime factors belong to $\mathcal{P}$. Then there are only finitely many effectively computable reduced Heron triangles whose sides have lengths $a,\ b,\ c$ such that $abc \in \mathcal{S}$.*

By noticing that the second largest prime number which is congruent to 1 modulo 4 is 13, by Theorem 1.2 it follows that there are only finitely many effectively computable reduced Heron triangles whose sides have lengths $a,\ b,\ c$ and for which $P(abc) < 13$. All these triangles are listed below.

Theorem 1.3. *The only reduced Heron triangles whose sides have lengths $a \leq b \leq c$ and such that $P(abc) < 13$ are:*

3	4	5
5	5	6
5	5	8
7	15	20
7	24	25
11	25	30
14	25	25
25	25	48
35	44	75
55	84	125
88	125	125
625	625	672

Note that in the above theorem, we only list the nondegenerate solutions for which $a < b+c,\ b < a+c,\ c < a+b$ hold.

2. PROOF OF THEOREM 1.1

Let $\mathcal{P}$ be any finite set of prime numbers. Without loss of generality we may assume that $2 \in \mathcal{P}$. Let $\mathcal{S}$ be the set of all positive integers whose prime factors belong to $\mathcal{P}$. To prove Theorem 1.1, it suffices to show that there are only finitely many reduced Heron triangles whose sides have lengths $a,\ b,\ c$ such that $abc \in \mathcal{S}$. We distinguish two cases.

2.1 The Triangle Is Isosceles

Assume that $a = b$. In this case, c is even and if we denote by h_c the length of the altitude perpendicular to the side of length c, then $(a, h_c, c/2)$ is a reduced Pythagorean triple. In particular, we get

$$h_c^2 = a^2 - \left(\frac{c}{2}\right)^2. \tag{2–1}$$

With $y := a^2 \in \mathcal{S}$ and $z := \left(\frac{c}{2}\right)^2 \in \mathcal{S}$, Equation (2–1) is a particular case of an equation of the form

$$x^2 = y - z \qquad \gcd(x, y, z) = 1 \text{ and } yz \in \mathcal{S}, \tag{2–2}$$

and by work of [de Weger 90], we know that the above equation has only finitely many, even effectively computable, positive solutions $(x,\ y,\ z)$.

2.2 The Triangle Is Not Isosceles

We begin with Formula (1–4)

$$(a+b+c)(a+b-c)(a+c-b)(b+c-a) = (4A)^2. \tag{2–3}$$

We notice that

$$\begin{aligned} &\gcd(a+b+c, a+b-c) \mid 2c, \\ &\gcd(a+b+c, a+c-b) \mid 2b, \\ &\gcd(a+b+c, b+c-a) \mid 2a, \end{aligned} \tag{2–4}$$

therefore

$$\gcd(a+b+c, (a+b-c)(a+c-b)(b+c-a)) \in \mathcal{S}. \tag{2–5}$$

With (2–3) and (2–5), it follows that there exists a square-free number $d_1 \in \mathcal{S}$ such that

$$a + b + c = d_1 x_1^2 \tag{2–6}$$

holds with some positive integer x_1. In a similar way, we also get that there exist six positive integers $d_2,\ d_3,\ d_4,\ x_2,\ x_3,\ x_4$ such that $d_2,\ d_3,\ d_4$ are square-free integers in $\mathcal{S}$ and such that

$$a+b-c = d_2x_2^2,\ \ a+c-b = d_3x_3^2,\ \ b+c-a = d_4x_4^2. \tag{2–7}$$

Let $p_1 < p_2 < \cdots < p_t$ be all the prime numbers in $\mathcal{P}$ and let $\mathbf{K} := \mathbf{Q}[\sqrt{p_i} \mid i = 1, \ldots, t]$. Let $h := h_{\mathbf{K}}$ be the class number of $\mathbf{K}$, and let $\mathcal{O} := \mathcal{O}_{\mathbf{K}}$ be the ring of algebraic integers in $\mathbf{K}$. Let $\pi_1, \ldots, \pi_l$ be all the prime ideals in $\mathcal{O}$ whose norms sit above prime numbers in $\mathcal{P}$. Let a_i be a generator of the principal ideal $[\pi_i]^h$. It is then well known that there exists a positive integer u and some computable algebraic numbers $b_1, \ldots, b_u$ in $\mathcal{O}$ such that if $c \in \mathcal{O}$ has the property that the norm of c in $\mathbf{K}$ is an element of $\mathcal{S}$, then c can be written in the form

$$c = b_j \zeta a_1^{m_1} \ldots a_l^{m_l}$$

for some $j \in \{1,\ \ldots,\ u\}$, a unit ζ in $\mathbf{K}$, and nonnegative integers m_i for $i = 1,\ \ldots,\ l$ (see [Shorey and Tijdeman 86]). Let $\widehat{\mathcal{S}}$ be the set of all algebraic integers in $\mathcal{O}$ which can be written in the form $\zeta a_1^{m_1} \ldots a_l^{m_l}$ with some unit ζ in $\mathbf{K}$ and some nonnegative integers m_i for $i = 1,\ \ldots,\ l$. In particular, if $c \in \mathcal{O}$ is such that the norm of c is an element of $\mathcal{S}$, then c can be written in the form $c = b_j s$ for some $j = 1,\ \ldots,\ u$, and some $s \in \widehat{\mathcal{S}}$. We now return to Equations (2–6) and (2–7) and notice that

$$2c = d_1x_1^2 - d_2x_2^2 = (\sqrt{d_1}x_1 - \sqrt{d_2}x_2)(\sqrt{d_1}x_1 + \sqrt{d_2}x_2)$$

and

$$2b = d_1x_1^2 - d_3x_3^2 = (\sqrt{d_1}x_1 - \sqrt{d_3}x_3)(\sqrt{d_1}x_1 + \sqrt{d_3}x_3).$$

By taking norms in $\mathbf{K}$ in the above equations, we get that $N_{\mathbf{K}}(\sqrt{d_1}x_1 \pm \sqrt{d_i}x_i)$ are all elements of $\mathcal{S}$ for $i = 1,\ 2$. Thus, there exist four indices $i_1,\ i_2,\ i_3,\ i_4$ in $\{1,\ \ldots,\ u\}$ and four numbers $s_1,\ s_2,\ s_3,\ s_4$ in $\widehat{\mathcal{S}}$ such that

$$\sqrt{d_1}x_1 - \sqrt{d_2}x_2 = b_{i_1}s_1,\ \ \sqrt{d_1}x_1 + \sqrt{d_2}x_2 = b_{i_2}s_2$$

and

$$\sqrt{d_1}x_1 - \sqrt{d_3}x_3 = b_{i_3}s_3,\ \ \sqrt{d_1}x_1 + \sqrt{d_3}x_3 = b_{i_4}s_4.$$

From the four equations above, we get that

$$\sqrt{d_3}x_3 - \sqrt{d_2}x_2 = b_{i_1}s_1 - b_{i_3}s_3 = b_{i_4}s_4 - b_{i_2}s_2.$$

Thus,

$$b_{i_1}s_1 + b_{i_2}s_2 - b_{i_3}s_3 - b_{i_4}s_4 = 0. \tag{2–8}$$

Suppose now that there are infinitely many reduced Heron triangles which are not isosceles and for which $abc \in \mathcal{S}$. Each one of these triangles will lead to an equation of the form (2–8) in $\mathcal{O}$. Since there are only finitely many choices for the quadruple of indices (i_1, i_2, i_3, i_4) from $\{1,\ \ldots,\ u\}$, it follows that there is a fixed quadruple of indices (i_1, i_2, i_3, i_4) for which Equation (2–8) admits infinitely many solutions $(s_1, s_2, s_3, s_4) \in \widehat{\mathcal{S}}^4$. Write $\beta_1 := b_{i_1},\ \beta_2 := b_{i_2},\ \beta_3 := -b_{i_3}$, and $\beta_4 := -b_{i_4}$. We first check that the equation

$$\beta_1 s_1 + \beta_2 s_2 + \beta_3 s_3 + \beta_4 s_4 = 0 \tag{2–9}$$

is nondegenerate, that is, no proper subsum is zero. Since $\beta_i s_i \neq 0$, it follows that the only way that some proper subsum of (2–9) is zero is when

$$\beta_1 s_1 + \beta_2 s_2 = \beta_3 s_3 + \beta_4 s_4 = 0, \tag{2–10}$$

or when

$$\beta_1 s_1 + \beta_3 s_3 = \beta_2 s_2 + \beta_4 s_4 = 0, \tag{2–11}$$

or when

$$\beta_1 s_1 + \beta_4 s_4 = \beta_2 s_2 + \beta_3 s_3 = 0. \tag{2–12}$$

If (2–10) holds, we get $0 = \beta_1 s_1 + \beta_2 s_2 = b_{i_1} s_1 + b_{i_2} s_2 = 2\sqrt{d_1}x_1$, which is impossible. If (2–11) holds, we get $0 = \beta_1 s_1 + \beta_3 s_3 = b_{i_1} s_1 - b_{i_3} s_3 = \sqrt{d_3}x_3 - \sqrt{d_2}x_2$, therefore $d_3 x_3^2 = d_2 x_2^2$, or, equivalently $b = c$, which is impossible because we are assuming that the triangle is not isosceles. Finally, if (2–12) holds, we then get $0 = \beta_1 s_1 + \beta_4 s_4 = b_{i_1} s_1 - b_{i_4} s_4 = -\sqrt{d_2}x_2 - \sqrt{d_3}x_3$, leading again to $d_2 x_2^2 = d_3 x_3^2$, which is impossible as we have seen. Thus, Equation (2–9) is nondegenerate. It follows, from the classical results on nondegenerate S-unit equations (see [Evertse et al. 88]), that there exist finitely many quadruples of solutions (S_1, S_2, S_3, S_4) with $S_i \in \widehat{\mathcal{S}}$ for $i = 1, \ldots, 4$, so that for every solution (s_1, s_2, s_3, s_4) with $s_i \in \widehat{\mathcal{S}}$ of Equation (2–8), there exist a number $\rho \in \widehat{\mathcal{S}}$ and one of these finitely many quadruples of solutions, say (S_1, S_2, S_3, S_4), so that

$$s_i = S_i \rho \qquad \text{for } i = 1, \ldots, 4. \tag{2–13}$$

Let us call the collection of finitely many such solutions (S_1, S_2, S_3, S_4) of equation (2–8) as the collection of *reduced* solutions. Let C be an upper bound for $N_{\mathbf{K}}(b_j)$ for $j = 1, \ldots, u$ and for $N_{\mathbf{K}}(S_i)$ for $i = 1, \ldots, 4$ over all the finitely many reduced solutions. With equation (2–13), we get

$$2\sqrt{d_1}x_1 = b_{i_1} s_1 + b_{i_2} s_2 = \rho(b_{i_1} S_1 + b_{i_2} S_2),$$

therefore ρ divides $2\sqrt{d_1}x_1$. In particular, ρ^2 divides $4(a + b + c)$. In a similar way, we get that ρ^2 divides $4(a + b - c)$ and $4(a + c - b)$. Since $\gcd(a, b, c) = 1$, and precisely one of the numbers $a,\ b,\ c$ is even and the other two are odd, we get that $\gcd(a+b+c, a+b-c, a+c-b) = 2$. Thus, ρ^2 divides 8, therefore ρ divides 4. Thus, $N_{\mathbf{K}}(\rho)$ divides $N_{\mathbf{K}}(4) = 4^{2^t}$, and in particular $N_{\mathbf{K}}(\rho)$ is bounded. Since

$$\begin{aligned}2c = d_1 x_1^2 - d_2 x_2^2 &= (\sqrt{d_1}x_1 - \sqrt{d_2}x_2)(\sqrt{d_1}x_1 + \sqrt{d_2}x_2)\\ &= b_{i_1} b_{i_2} S_1 S_2 \rho^2,\end{aligned}$$

and

$$\begin{aligned}2b = d_1 x_1^2 - d_3 x_3^2 &= (\sqrt{d_1}x_1 - \sqrt{d_3}x_3)(\sqrt{d_1}x_1 + \sqrt{d_3}x_3)\\ &= b_{i_3} b_{i_4} S_3 S_4 \rho^2,\end{aligned}$$

we get that $b^{2^t} = N_{\mathbf{K}}(b)$ and $c^{2^t} = N_{\mathbf{K}}(c)$ are both bounded. So, b and c can take only finitely many values. Since instead of b and c, we could have used the same argument for any other two lengths of sides of our triangle, we get that there are indeed only finitely many reduced Heron triangles with $abc \in \mathcal{S}$. □

3. PROOF OF THEOREM 1.2

The following lemma has already appeared in [Luca 03], but we shall include it here for the completeness of the argument.

Lemma 3.1. *Assume that a, b, c are the lengths of sides of a nonisosceles Heron triangle. Suppose that p is a prime number, $p \not\equiv 1 \pmod 4$ such that $p^\alpha \mid a$. Then, $p^{\alpha+1} \mid (b^2 - c^2)$ if $p = 2$ and $p^\alpha \mid (b^2 - c^2)$ if $p > 2$.*

Proof: We treat only the case $p > 2$ since the case $p = 2$ can be dealt with similarly. We rewrite Equation (1–2) as

$$2a^2(b^2 + c^2) - a^4 - (b^2 - c^2)^2 = (4A)^2. \tag{3–1}$$

One may reduce Equation (3–1) modulo $p^{2\alpha}$ and get

$$-(b^2 - c^2)^2 \equiv (4A)^2 \pmod{p^{2\alpha}}. \tag{3–2}$$

All that is left to notice is that Equation (3–2) forces $p^\alpha \mid (b^2 - c^2)$. Indeed, assume that this is not the case. It then follows that if $p^\delta \,||\, (b^2 - c^2)$, then $\delta < \alpha$. Simplifying both sides of equation (3–2) by $p^{2\delta}$, we get

$$-\Big(\frac{b^2 - c^2}{p^\delta}\Big)^2 \equiv \Big(\frac{4A}{p^\delta}\Big)^2 \pmod{p^{2(\alpha-\delta)}}. \tag{3–3}$$

However, notice that congruence (3–3) is impossible because -1 is not a quadratic residue modulo p. Hence, p^α divides both $(b^2 - c^2)$ and A. The lemma is therefore proved. □

We are now ready to prove Theorem 1.2. Let p_1 be the unique prime number in $\mathcal{P}$ which is congruent to 1 modulo 4 and assume that $p_2 < p_3 < \cdots < p_t$ are the other prime numbers belonging to $\mathcal{P}$. Since $\gcd(a, b, c) = 1$, it follows that at least one of the three numbers $a,\ b,$

and c is not a multiple of p_1. Assume that a is coprime to p_1 and write

$$a = p_2^{\alpha_2} \cdots \cdot p_t^{\alpha_t}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots \cdot p_t^{\beta_t}, \quad c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots \cdot p_t^{\gamma_t}. \tag{3–4}$$

We may restrict ourselves to treating the case of the nonisosceles triangles by Theorem 1.1. Write $b_1 = \dfrac{b}{p_1^{\beta_1}}$, $c_1 = \dfrac{c}{p_1^{\gamma_1}}$, and set $X := \max\{\alpha_i, \beta_i, \gamma_i \mid i = 1, \ldots, t\}$, where we assume that $X > e$. Repeated applications of Lemma 3.1 give

$$a \mid b^2 - c^2, \qquad b_1 \mid a^2 - c^2, \qquad c_1 \mid a^2 - b^2. \tag{3–5}$$

For every prime number p and every nonzero rational number r, let $\mathrm{ord}_p(r)$ denote the order at which the prime number p divides r (r is written in reduced form). We use the divisibility relations (3–5) and lower bounds for linear forms in p-adic logarithms to bound $\max\{\alpha_i, \beta_i, \gamma_i \mid i = 2, \ldots, t\}$ linearly in $\log X$. Let us take the first divisibility relation (3–5) and let $i \in \{2, \ldots, t\}$. If $\alpha_i = 0$, then we are done. If not, then since $\gcd(a, b, c) = 1$, it follows that bc is not a multiple of p_i and that

$$\begin{aligned} \alpha_i &= \mathrm{ord}_{p_i}(a) \le \mathrm{ord}_{p_i}(b^2 - c^2) = \mathrm{ord}_{p_i}(1 - b^{-2}c^2) \\ &= \mathrm{ord}_{p_i}\big(1 - p_1^{2(\gamma_1 - \beta_1)} p_2^{2(\gamma_2 - \beta_2)} \cdots p_t^{2(\gamma_t - \beta_t)}\big) \end{aligned} \tag{3–6}$$

We use standard lower bounds for linear forms in p-adic logarithms (see, for example, [Yu 99]) to deduce that inequality (3–6) implies that

$$\alpha_i < C_1 \log X, \tag{3–7}$$

where C_1 is an effectively computable constant depending only on P, the largest prime number in $\mathcal{P}$, and t, the number of elements of $\mathcal{P}$. Similar arguments show that

$$\max\{\alpha_i, \beta_i, \gamma_i \mid i = 2, \ldots, t\} < C_1 \log X. \tag{3–8}$$

It remains to bound β_1 and γ_1. Assume that $\beta_1 \le \gamma_1$. From the triangular inequality, we have

$$0 < |b - c| < a$$

and p^{β_1} divides $b - c$. So,

$$p_1^{\beta_1} < a, \tag{3–9}$$

therefore

$$\beta_1 \log p_1 < \log a.$$

In particular,

$$\beta_1 < \frac{C_1 t \log P}{\log p_1} \log X, \tag{3–10}$$

and

$$\log b = \beta_1 \log p_1 + \sum_{i=2}^{t} \beta_i \log p_i < \sum_{i=2}^{t} (\alpha_i + \beta_i) \log p_i < C_2 \log X,$$

where $C_2 = 2C_1 t \log P$. Finally, we use the triangular inequality again to get

$$p_1^{\gamma_1} \le c \le a + b < 2\max(a, b), \tag{3–11}$$

therefore

$$\gamma_1 \log p_1 < \log 2 + \max(\log a, \log b) < \log 2 + C_2 \log X,$$

which implies that

$$\gamma_1 < \frac{\log 2}{\log p_1} + \frac{C_2}{\log p_1} \log X. \tag{3–12}$$

Since X was the maximum of all the exponents $\alpha_i,\ \beta_i,\ \gamma_i$ with $i = 1, \ldots, t$, we get, from inequalities (3–8)–(3–12), that

$$X < \frac{\log 2}{\log p_1} + \frac{2C_1 t \log P}{\log p_1} \log X,$$

which implies that $X < C_3$. Theorem 1.2 is therefore proved. □

4. PROOF OF THEOREM 1.3

4.1 Isosceles Triangles

We denote by S the set of positive integers divisible by 2, 3, 5, 7, 11 only. We assume that in our isosceles triangle $a = b$, and we denote by h_c the altitude perpendicular to c. In this case, c is even. By (2–1), we have

$$\left(\frac{c}{2}\right)^2 = (a + h_c)(a - h_c),$$

which implies that $(a + h_c), (a - h_c) \in S$. Further,

$$X + Y = Z \quad (X, Y, Z \in S) \tag{4–1}$$

holds for $X = (a + h_c),\ Y = (a - h_c),\ Z = 2a$. Using Equation (2–1) and $\gcd(a, c) = 1$, we obtain that $\gcd((a + h_c), (a - h_c), 2a)$ is 1 or 2. Hence, the values of $(a + h_c)$, $(a - h_c)$, $2a$, that is, the values of $a = b$ and c, can be obtained from the primitive solutions of Equation (4–1).

The primitive solutions of Equation (4–1) were described by [de Weger 89] (see Theorem 6.3 on page 123) for an even larger set of primes including also 13. To list the primitive solutions of (4–1), we just had to select the solutions not divisible by 13 from the list of de Weger's theorem. We tested these candidates against the condition that they be the sides of a triangle whose area is an integer. This yielded the solutions (5,5,6), (5,5,8), (14,25,25), (25,25,48), (88,125,125), (625,625, 672).

4.2 Nonisosceles Triangles

4.2.1 Explicit upper bounds. Set $p_1 = 5$, $p_2 = 2$, $p_3 = 3$, $p_4 = 7$, $p_5 = 11$. These are all the primes less than 13, and p_1 is the only one congruent to 1 mod 4. We keep the notation of the proof of Theorem 1.2, see (3–4). We shall use

$$\tilde{X} := \max_{2 \le i \le 5} \{\alpha_i, \beta_i, \gamma_i\}$$

and

$$X := \max\{\beta_1, \gamma_1, \tilde{X}\}$$

will be the same as before.

We first make explicit the estimates of the proof of Theorem 1.2. Let $t = 5$. For $2 \le i \le 5$, consider α_i. If $\alpha_i > 0$, then (3–6) holds. Note that by the remark before (3–6), it follows that if $\alpha_i > 0$, then the i-th factor of the last product in (3–6) does not appear because of $\beta_i = \gamma_i = 0$ $(i = 2, \ldots, 5)$. We apply the estimates of [Yu 99] (a more explicit formulation can be found in the book [Smart 98], page 225). We obtain

$$\begin{aligned} \alpha_i &\le \operatorname{ord}_{p_i}\left(1 - p_1^{2(\gamma_1-\beta_1)} p_2^{2(\gamma_2-\beta_2)} \cdot \cdots \cdot p_5^{2(\gamma_5-\beta_5)}\right) \\ &\le C_1 \log X, \end{aligned} \tag{4–2}$$

where the values of C_1 are different for the different primes, but all of them satisfy

$$C_1 \le 1.4 \cdot 10^{25}.$$

We obtain similar estimates for β_i, γ_i $(2 \le i \le 5)$, that is, we infer

$$\tilde{X} < C_1 \cdot \log X. \tag{4–3}$$

We only have to bound β_1 and γ_1. Similarly as in (3–9), we have

$$\beta_1 \log p_1 < \log a = \alpha_2 \log p_2 + \ldots + \alpha_5 \log p_5 \le \tilde{X} \log 462,$$

that is, by (4–3),

$$\beta_1 < \frac{\log 462}{\log 5} \cdot \tilde{X} \le 3.82 \cdot \tilde{X} \le 3.82 \cdot C_1 \cdot \log X. \tag{4–4}$$

By (3–11) and the above inequalities, we obtain

$$\gamma_1 \le \frac{\log(a+b)}{\log p_1} \le \frac{1}{\log 5} \cdot \log\left(5^{3.82\tilde{X}} \cdot 462^{\tilde{X}} + 462^{\tilde{X}}\right) \tag{4–5}$$

whence

$$\begin{aligned} \gamma_1 &\le \frac{\log 2 + 3.82\tilde{X} \log 5 + \tilde{X} \log 462}{\log 5} \\ &\le 8.07 \cdot \tilde{X} < 8.07 \cdot C_1 \log X, \end{aligned} \tag{4–6}$$

which finally implies

$$X < 1.13 \cdot 10^{26} \cdot \log X,$$

whence

$$X < 10^{28}. \tag{4–7}$$

4.2.2 Reduction. Let again $2 \le i \le 5$, then if $\alpha_i > 0$, we have (see (4–2))

$$0 < \alpha_i \le \operatorname{ord}_{p_i}(2(\gamma_1-\beta_1)\log_{p_i} p_1 + \ldots + 2(\gamma_5-\beta_5)\log_{p_i} p_5), \tag{4–8}$$

where in the above sum the term with index i does not occur. We are now going to reduce the bound (4–7). For this purpose, we apply the following statement.

Lemma 4.1. *Let p be a prime, $\vartheta_1, \ldots, \vartheta_n \in \Omega_p$, $\Lambda = \sum_{i=1}^n x_i \vartheta_i$ with coefficients $x_1, \ldots, x_n \in \mathbb{Z}$, $X := \max |x_i|$ and c_1, c_2 be positive constants. Assume that $\operatorname{ord}_p(\vartheta_i)$ is minimal for $i = n$, let*

$$\vartheta'_i = -\vartheta_i/\vartheta_n \quad (i = 1, \ldots, n-1),$$

and

$$\Lambda' = \Lambda/\vartheta_n = -\sum_{i=1}^{n-1} x_i \vartheta'_i + x_n.$$

Let $0 < \mu \in \mathbb{Z}$, and for any $\vartheta \in \Omega_p$ let $\vartheta^{(\mu)}$ be a rational integer with $\operatorname{ord}_p(\vartheta - \vartheta^{(\mu)}) \ge \mu$. Denote by Γ_μ the lattice spanned by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \vartheta'_1 & \vartheta'_2 & \cdots & \vartheta'_{n-1} & p^\mu \end{pmatrix}.$$

Denote by b_1 the first vector of the LLL-reduced basis of Γ_μ. If

$$||b_1|| > 2^{\frac{n-1}{2}} \sqrt{n}\, X_0,$$

then the inequality

$$\operatorname{ord}_p(\Lambda) \ge c_1 + c_2 x_j, \quad X \le X_0$$

has no solutions $x_1, \ldots, x_n$ with

$$\frac{\mu - 1 + \operatorname{ord}_p(\vartheta_n) - c_1}{c_2} \le X \le X_0.$$

Proof: This is Lemma 3.14 of [de Weger 89] combined with the well-known estimate for the shortest lattice vector in terms of b_1. The formulation of the statement in terms of b_1 makes it easier to apply. □

In view of (4–7), we have the initial bound $X_0 = 10^{28}$ for X. Note that in our case, $n = 4$ (the term with index i does not occur in the linear form (4–8)), and the constants in the above lemma are $c_1 = 0,\ c_2 = 1$. Having the bound X_0 for X, the coefficients of (4–8) can be bounded (in absolute value) by $2X_0$ (each prime occurs in exactly one of $a,\ b_1,\ c_1$). In order to perform the reduction, we must have

$$||b_1|| > 2^{\frac{3}{2}}\ 2\ (2X_0) = 2^{\frac{7}{2}}\ X_0. \tag{4–9}$$

Note that the value of $\mathrm{ord}_p(\vartheta_n)$ was 2 in case of $p = 2$ and 1 for $p = 3, 7, 11$. If (4–9) is satisfied for a certain μ, then by Lemma 4.1, we conclude

$$\alpha_i \le \mu - 1 + 2 = \mu + 1. \tag{4–10}$$

For $2 \le i \le 5$, we perform reductions for α_i and similarly for β_i and γ_i just interchanging the roles of $a,\ b,\ c$. The reductions for β_i and γ_i are formally the same as for α_i. That is, we have to perform reductions for the following linear forms:

p	ϑ_1	ϑ_2	ϑ_3	ϑ_4
2	$\log_2 3$	$\log_2 5$	$\log_2 7$	$\log_2 11$
3	$\log_3 2$	$\log_3 5$	$\log_3 7$	$\log_3 11$
7	$\log_7 2$	$\log_7 3$	$\log_7 5$	$\log_7 11$
11	$\log_{11} 2$	$\log_{11} 3$	$\log_{11} 5$	$\log_{11} 7$

If for a certain μ, (4–9) is satisfied for all linear forms, then by (4–10) we get $\tilde{X} \le \mu+1$. Then by (4–4) and (4–5), we derive a new bound for X. Using this new bound, the reduction can be repeated, as long as the new bound for X is less then the previous one. The following table gives a summary of the reduction process:

Step	X	$\lvert\lvert b_1\rvert\rvert >$	μ	new bound for $\tilde{X}$	new bound for X
I.	10^{28}	$1.131 \cdot 10^{29}$	390	391	2984
II.	2984	33749.04	61	62	473
III.	473	5349.63	51	52	396
IV.	396	4478.76	$p = 2:$ 50	51	
IV.	396	4478.76	$p = 3:$ 32	32	
IV.	396	4478.76	$p = 7:$ 20	20	
IV.	396	4478.76	$p = 11:$ 15	15	

In Step IV, we used different values for μ in order to get the best possible bounds for the exponents of 2, 3, 7, and 11, respectively.

4.2.3 Enumeration.

Using the reduced bounds, we have the following possibilities for a, b, c:

$$\begin{aligned} a &= 2^{\alpha_2}3^{\alpha_3}7^{\alpha_4}11^{\alpha_5} \\ b_1 &= 2^{\beta_2}3^{\beta_3}7^{\beta_4}11^{\beta_5} \\ c_1 &= 2^{\gamma_2}3^{\gamma_3}7^{\gamma_4}11^{\gamma_5}, \end{aligned}$$

where

$$\begin{aligned} &0 \le \alpha_2,\ \beta_2,\ \gamma_2 \le 51 \\ &0 \le \alpha_3,\ \beta_3,\ \gamma_3 \le 32 \\ &0 \le \alpha_4,\ \beta_4,\ \gamma_4 \le 20 \\ &0 \le \alpha_5,\ \beta_5,\ \gamma_5 \le 15, \end{aligned}$$

where in addition for all i $(1 \le i \le 4)$ at most one of $\alpha_i,\ \beta_i,\ \gamma_i$ can be nonzero. We enumerate all these values of $a,\ b_1,\ c_1$. For all these triples, we let β_1 run through the interval

$$0 \le \beta_1 \le \frac{\log a}{\log 5}.$$

We then set $b := 5^{\beta_1} \cdot b_1$ and test if $c_1 | a^2 - b^2$ (see (3–5)). If so, we then let γ_1 run through the interval

$$0 \le \gamma_1 \le \frac{\log(a+b) - \log c_1}{\log 5}$$

(remember that $c \le a + b$ must hold). Finally, we set $c := 5^{\gamma_1} \cdot c_1$, test if the three sides are distinct, and if $b_1 | a^2 - c^2$ and $a | b^2 - c^2$ (see (3–5)). We further test the surviving triples to see if they can be sides of a triangle whose area is an integer.

4.2.4 Remarks on CPU times.

The reduction procedure took just some minutes of CPU time. On the other hand, the enumeration of the possible exponents was a hard task, taking about a week of CPU time. Our programs were written in Maple and were executed on a PC with a 350Mhz processor.

Note that by omitting one prime, the same computation took just 20 minutes. This shows that it is not feasible to extend the present computation for more primes.

$\square$

ACKNOWLEDGMENTS

István Gaál's research was supported in part by Grants T 037367 and T 042985 from the Hungarian National Foundation for Scientific Research. István Járási's research was supported in part by Grant T 037367 from the Hungarian National Foundation for Scientific Research. Florian Luca's research was supported in part by Grant SEP-CONACYT 37259-E.

REFERENCES

[Bugeaud 98] Y. Bugeaud. "On the Greatest Prime Factor of $(ab+1)(bc+1)(ca+1)$." *Acta Arith.* 86 (1998), 45–49.

[Corvaja and Zannier 03] P. Corvaja and U. Zannier. "On the Greatest Prime Factor of $(ab+1)(ac+1)$." *Proc. Amer. Math. Soc.* 131 (2003), 1705–1709.

[Evertse et al. 88] J.-H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman. "S-Unit Equations and Their Applications." In *New Advances in Transcendence Theory (Durham, 1986)*, pp. 110–174. Cambridge, UK: Cambridge Univ. Press, Cambridge, 1988.

[Guy 94] R. K. Guy. *Unsolved Problems in Number Theory,* Second edition, Problem Books in Mathematics, Unsolved Problems in Intuitive Mathematics, I. New York: Springer-Verlag, 1994.

[Győry et al. 96] K. Győry, A. Sárközy, and C. L. Stewart. "On the Number of Prime Factors of Integers of the Form $ab+1$." *Acta Arith.* 74 (1996), 365–385.

[Győry and Sárközy 97] K. Győry and A. Sárközy. "On Prime Factors of Integers of the Form $(ab+1)(bc+1)(ca+1)$." *Acta Arith.* 79 (1997), 163–171.

[Hernández and Luca 03] S. Hernández and F. Luca. "On the Largest Prime Factor of $(ab+1)(ac+1)(bc+1)$." To appear in *Bol. Soc. Math. Mexicana.*

[Harborth and Kemnitz 90] H. Harborth and A. Kemnitz. "Fibonacci Triangles." In *Applications of Fibonacci Numbers*, Volume 3 (Pisa, 1988), pp. 129–132. Dordrecht: Kluwer Acad. Publ., 1990.

[Harborth et al. 96] H. Harborth, A. Kemnitz, and N. Robbins. "Non-Existence of Fibonacci Triangles." *Congr. Numer.* 114 (1996), 29–31.

[Kramer and Luca 00] A. -V. Kramer and F. Luca. "Some Remarks on Heron Triangles." *Acta Acad. Paedagog. Agriensis, Sect. Mat. (N.S.)* 27 (2000), 25–38.

[Luca 00] F. Luca. "Perfect Cuboids and Perfect Square Triangles." *Math. Mag.* 73 (2000), 400–401.

[Luca 03] F. Luca. "Fermat Primes and Heron Triangles with Prime Power Sides." *Am. Math. Monthly* 110:1 (2003), 46–49.

[Shorey and Tijdeman 86] T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations,* Cambridge Tracts in Mathematics, 87. Cambridge, UK: Cambridge University Press, 1986.

[Smart 98] N. Smart. *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc. Student Texts, 41. Cambridge, UK: Cambridge Univ. Press, 1998.

[Stewart and Tijdeman 97] C. L. Stewart and R. Tijdeman. "On the Greatest Prime Factor of $(ab+1)(ac+1)(bc+1)$." *Acta Arith.* 79 (1997), 93–101.

[de Weger 89] B. M. M. de Weger. *Algorithms for Diophantine Equations*, CWI Tracts, 65. Amsterdam: Centrum voor Wiskunde en Informatica, 1989.

[de Weger 90] B. M. M. de Weger. "The Weighted Sum of Two S-Units Being a Square." *Indag. Math. (N.S.)* 1 (1990), 243–262.

[Yu 99] K. Yu. "p-Adic Logarithmic Forms and Group Varieties. II." *Acta Arith.* 89 (1999), 337–378.

István Gaál, University of Debrecen, Mathematical Institute, H–4010 Debrecen Pf.12., Hungary (igaal@math.klte.hu)

István Járási, University of Debrecen, Mathematical Institute, H–4010 Debrecen Pf.12., Hungary (ijarasi@math.klte.hu)

Florian Luca, Mathematical Institute, UNAM, Ap. Postal 61-3 (Xangari), CP 58 089, Morelia, Michoacán, Mexico (fluca@matmor.unam.mx)

Received September 14, 2002; accepted in revised form September 2, 2003.