J. Aust. Math. Soc. **109** (2020), 68–80
doi:10.1017/S144678871900003X

PERFECT TRIANGLES ON THE CURVE C_4

SHAHRINA ISMAIL

(Received 2 April 2018; accepted 26 January 2019; first published online 9 October 2019)

Communicated by I. Shparlinski

Abstract

A Heron triangle is a triangle that has three rational sides (a, b, c) and a rational area, whereas a perfect triangle is a Heron triangle that has three rational medians (k, l, m). Finding a perfect triangle was stated as an open problem by Richard Guy [*Unsolved Problems in Number Theory* (Springer, New York, 1981)]. Heron triangles with two rational medians are parametrized by the eight curves $C_1, \ldots, C_8$ mentioned in Buchholz and Rathbun ['An infinite set of heron triangles with two rational medians', *Amer. Math. Monthly* **104**(2) (1997), 106–115; 'Heron triangles and elliptic curves', *Bull. Aust. Math. Soc.* **58** (1998), 411–421] and Bácskái *et al.* [Symmetries of triangles with two rational medians, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.65.6533, 2003]. In this paper, we reveal results on the curve C_4 which has the property of satisfying conditions such that six of seven parameters given by three sides, two medians and area are rational. Our aim is to perform an extensive search to prove the nonexistence of a perfect triangle arising from this curve.

2010 *Mathematics subject classification*: primary 11Y05; secondary 11Y35.

Keywords and phrases: elliptic curve, perfect triangle, p-adic.

1. Introduction

Various authors have examined the problem of finding triangles with as many of their parameters as possible being simultaneously rational. A perfect triangle, as defined by Guy [13] in Problem D21, is a Heron triangle which also has three rational medians. Numerous research has been done in the past [9, 10, 14, 16] to find such a triangle; unfortunately, to date no one has found such a triangle, nor has anyone proved its nonexistence. However, on the bright side, there are partial results which show that triangles do exist in which five or six of the seven parameters are rational.

A triangle with sides denoted by (a, b, c) has medians (k, l, m) given by

$$k = \tfrac{1}{2}\sqrt{2b^2 + 2c^2 - a^2},$$
$$l = \tfrac{1}{2}\sqrt{2c^2 + 2a^2 - b^2},$$
$$m = \tfrac{1}{2}\sqrt{2a^2 + 2b^2 - c^2}.$$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

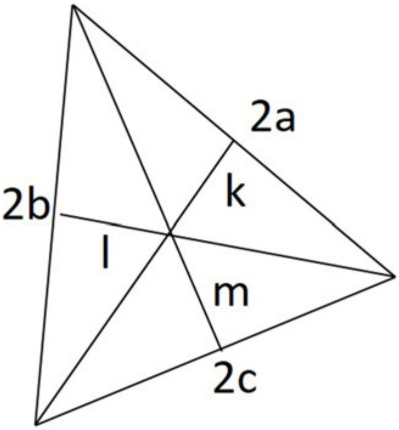

FIGURE 1. Triangles with sides $(2a, 2b, 2c)$ and medians (k, l, m).

All rational-sided triangles with two rational medians [2] are completely parametrized by equations given by

$$\begin{aligned} a &= (-2\phi\theta^2 - \phi^2\theta) + (2\theta\phi - \phi^2) + \theta + 1, \\ b &= (\phi\theta^2 + 2\phi^2\theta) + (2\theta\phi - \theta^2) - \phi + 1, \\ c &= (\phi\theta^2 - \phi^2\theta) + (\theta^2 + 2\theta\phi + \phi^2) + \theta - \phi, \end{aligned}$$

for rational ϕ and θ such that $\theta > 0$, $\phi < 1$, $\phi + 2\theta > 1$. Also, Heron's formula for the area, $\triangle$, of the triangle (a, b, c) is given by $\triangle = \sqrt{s(s-a)(s-b)(s-c)}$ where $s = (a + b + c)/2$ known as the semiperimeter, as illustrated in Figure 1.

Many interesting questions can be raised about these triangles, and there has been massive research on several properties of the Heron triangle, see for example [10, 16]. One interesting question is, of course, the existence of a perfect triangle arising from any known Heron triangle. The search for a perfect triangle requires one to find rational solutions to the equations defining the area and the medians in terms of the sides. There are partial results which show that triangles do exist in which six of the seven parameters are rational. In fact, we know of infinite families of triangles with three rational sides and one rational median [8]; three integral sides and three integral medians [11]; three rational sides, two rational medians and rational area [3]; and rational triangles with three rational sides and rational medians, but not the area [5].

The authors in [4] applied Schubert parameters to generate the values of θ and ϕ and plotted these parameters, considered as points corresponding to distinct Heron triangles with two rational medians, in the $\theta\phi$-plane. Rather than being randomly distributed in the region, the points seem to lie on five distinct curves. As a result, it was easy to isolate the rational coordinates of enough points on each curve to determine the corresponding equations for C_1, C_2, C_3, C_4 and C_5. Following on from that, in an attempt to find all Heron triangles with the property of having three rational medians,

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

Bácskái *et al.* [1] have uncovered additional three curves, C_6, C_7, C_8, apart from the one found in [4].

The authors show that these families correspond to eight elliptic curves, all isomorphic to each other. The subsequent exploration of these curves revealed that constraining the remaining median to be rational required one to find rational points on genus-seven curves, which by Faltings's theorem [12] leads to a finite number of possible solutions, which were left unresolved. Then, in [6], the authors disposed of the unresolved finite list of solutions in the sense that they found them all and verified that none of them correspond to a nontrivial Heron triangle with three rational medians, in other words, a perfect triangle.

In this paper we prove that there does not exist any perfect triangle arising from the curve C_4. The core theorem of this paper is as follows.

Theorem 1.1. *There does not exist any perfect triangle arising from the curve* C_4*:* $\theta\phi(\theta - \phi) + \theta\phi + 2(\theta - \phi) - 1$*, except possibly for* $n \equiv 3024 \bmod 6052$.

Here, the word 'except' indicates that there may exist one or more further points on the curve that is of enormous height which could possibly form a perfect triangle. We establish a new inductive method for applying the Mordell–Weil sieve [7, 15] to provably find all points on a (complicated) curve of high genus, without necessarily having to compute its Jacobian or a basis for its Mordell–Weil group. We illustrate with a difficult curve arising from the question in [13] of the existence of perfect triangles. We can show that any perfect triangle arising in this instance would have to have side lengths at least $10^{10^{10}}$. The reason why we know this is that we can prove n must be, say, $\{-4, -3, -2, -1, 0, 3\} \bmod 10^6$ by explicit calculations and so a counter-example would have n at least 10^6, which means the coordinates of (x, y) on the curve would be approximately $\exp(10^{12})$ in size.

2. A condition for the existence of a perfect triangle

It was shown in [4] that every rational point on C_4 such that $0 < \theta < 1, 0 < \phi < 1$ and $2\theta + \phi > 1$ corresponds to a triangle with rational sides, rational area and two rational medians. The sides of a triangle corresponding to a point $(\theta, \phi) \in C_4$ immediately imply that the sides and two medians are rational, thus it is only required to check the area $\triangle$ as to whether or not (a, b, c) form a proper triangle [2]. These inequalities exclude regions in which proper triangles cannot form.

The following theorem is one of our main results in this paper.

Theorem 2.1. *Finding a perfect triangle corresponding to an appropriate rational point on the curve* C_4 *is equivalent to finding an integer n such that* $Z(nP) = R(x) - S(x)y$ *where* $n \in \mathbb{Z}$*,* $(x_n, y_n) = nP$*,* $P = (-21, 324)$ *is an infinite-order generator of the curve*

$$E : y^2 = (x - 15)(x^2 + 15x - 3042)$$

and $R(x), S(x) \in \mathbb{Z}[x]$ *are polynomials of degree 16 and degree 14 defined below.*

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

Proof. Since the curve C_4 satisfies conditions such that six of seven parameters are rational (i.e. three rational sides (a, b, c), two rational medians, k and l, and area), we only need to check if the third median, m, of the equation

$$\begin{aligned}4m^2 &= 4 + 9\phi^2\theta^4 - 4\phi + 18\theta\phi + 4\theta + 6\phi\theta^2 - 6\phi^2\theta - 6\phi\theta^4 - 22\theta\phi^3 \\ &\quad + 6\phi^2\theta^2 + 6\phi^4\theta + 9\phi^4\theta^2 - 22\phi\theta^3 + 18\phi^3\theta^2 - 18\phi^2\theta^3 \\ &\quad + 18\phi^3\theta^3 - 3\phi^2 - 3\theta^2 + \phi^4 + \theta^4 - 2\theta^3 + 2\phi^3\end{aligned}$$

is rational. Since we are searching for rational points on C_4, the corresponding discriminant of C_4 with respect to θ, say C, is a square. Therefore all the rational points which force this correspond to rational points on the elliptic curve

$$C : v^2 = \phi^4 - 2\phi^3 + 5\phi^2 + 8\phi + 4.$$

We want to find rational values ϕ, θ and m that simultaneously satisfy the curve C_4 and the surface $4m^2 = f_4(\phi, \theta)$. Taking the resultant of C_4 and $f_4(\phi, \theta)$ with respect to θ gives

$$D_4 : 16\phi^4 m^4 - 8A(\phi)m^2 + B(\phi) = 0. \tag{2.1}$$

The curve D_4 is a curve of genus 7. Thus, by Faltings's theorem [12], D_4 consists of finitely many rational points. It contains the following 14 rational points:

$$(\phi, m) = \{\infty, (-1, 0), (-1, \pm 2), (-1/2, \pm 9/8), (0, \pm 9/8), (1, \pm 2), (1, \pm 18), (3, \pm 18)\}.$$

However, the factorization of D_4 using the curve C to replace the square root of a quartic in ϕ with v gives

$$\phi\bigg((16\phi^4 m^4 - 8Am^2 + B) - 16\phi^4\bigg(m^2 - \frac{A + 2Fv}{4\phi^4}\bigg)\bigg(m^2 - \frac{A - 2Fv}{4\phi^4}\bigg)\bigg) = 0.$$

Since $\phi \neq 0$, $D_4 = 0$ and $m \neq 0$ (otherwise it will form a degenerate triangle), one of the two factors on the left-hand side has to be zero. Thus, we have

$$[4\phi^4 m^2 - (A + 2Fv)][4\phi^4 m^2 - (A - 2Fv)] = 0,$$

which implies that either $A + 2Fv$ or $A - 2Fv$ is a nonzero square. Hence if $\phi \neq 0$, equation (2.1) has a rational root m if and only if one of $A \pm 2Fv$ is a nonzero square. Also, note that if (ϕ, v) is a point on C so is $(\phi, -v)$, thus without loss of generality the third median is rational if and only if $A + 2Fv$ is a square.

With a change of variables from C, we obtain the elliptic curve

$$\begin{aligned}E : y^2 &= x^3 - 3267x + 45630 \\ &= (x - 15)(x^2 + 15x - 3042)\end{aligned}$$

via the maps

$$C \to E : x = 3\frac{5\phi^2 + 24\phi + 12v + 24}{\phi^2}, \quad y = 108\frac{-\phi^3 + 5\phi^2 + 2\phi v + 12\phi + 4v + 8}{\phi^3},$$

$$E \to C : \phi = 12\frac{6 - x}{6x - y - 198}, \quad v = 2\frac{x^3 - 18x^2 + 3267x - 324y - 71658}{x^3 + 36x^2 - 12xy - 5643x + 396y + 84834}.$$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

The discriminant of E is $2^{14} \cdot 3^{14} \cdot 17$, which is zero upon reduction by the primes $2, 3, 17$. These are called the primes of bad reduction on E. Furthermore, $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with 2-torsion point $T = (15, 0)$ and generator $P = (-21, 324)$. The Cremona label of E is '102a1'. Also, E has points of order 2, $T' = [\frac{1}{2}(-15 + 27\beta), 0]$ and $T'' = [\frac{1}{2}(-15 - 27\beta), 0]$, where $\beta^2 = 17$. All the rational points on E can be written as $nP + \varepsilon T$ with $\varepsilon \in \{0, 1\}$. Rewriting $A + 2Fv$ in terms of x, y requires that

$$\frac{6^4}{(-12xy + 396y + x^3 + 36x^2 - 5643x + 84834)^2(6x - y - 198)^8}(R(x) - S(x) \cdot y) \tag{2.2}$$

is a square where

$$\begin{aligned} R(x) = {} & 81x^{16} + 40662x^{15} + 14353281x^{14} - 460241028x^{13} - 644722959186x^{12} \\ & + 39379675354740x^{11} + 5212980804862026x^{10} - 415546630058854656x^{9} \\ & - 8202010485984353739x^{8} + 1396767997483732402758x^{7} \\ & - 27550698906220673513787x^{6} - 1044392234943529703379852x^{5} \\ & + 60770398462922893831446348x^{4} - 1284453663719469166478575296x^{3} \\ & + 14183844641879715988450074288x^{2} \\ & - 81800517874945025246941522368x \\ & + 196162341839727571433321441856 \end{aligned}$$

and

$$\begin{aligned} S(x) = {} & 3240x^{14} + 456840x^{13} + 188268624x^{12} - 45834271200x^{11} \\ & - 2435651997264x^{10} + 682353767281968x^{9} - 7053953405575680x^{8} \\ & - 2553415737499629216x^{7} + 98906717445152189544x^{6} \\ & + 1348117411901578667784x^{5} - 162666175355778441465360x^{4} \\ & + 4276857451171442758058304x^{3} - 54456600108308451946891776x^{2} \\ & + 350065581968511893813480064x - 918312303919436410092339456. \end{aligned}$$

The numerator and denominator of the leading factor of (2.2) are both squares, hence we are only left to check if $R(x) - S(x) \cdot y$ is a square. For brevity, we denote $Z(nP) = R(x_n) - S(x_n) \cdot y_n$. This completes the proof of Theorem 2.1. □

We now have the following corollary.

Corollary 2.2. *Let*

$$\begin{aligned} X &= \{n \in \mathbb{N} \mid Z(nP) = R(x_n) - S(x_n) \cdot y_n = \square\}, \\ Y &= \{-4, -3, -2, -1, 0, 3\}. \end{aligned}$$

If $X = Y$, then there are no perfect triangles arising from C_4, and the set of rational points on D_4 is precisely

$$(\phi, m) = \{\infty, (-1, 0), (-1, \pm 2), (-1/2, \pm 9/8), (0, \pm 9/8), (1, \pm 2), (1, \pm 18), (3, \pm 18)\}.$$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

3. Elimination of lifted multiples of a point

For each of the five problematic values of $\mu \in Y \backslash \{-2\}$, we compute a corresponding integer $\delta(\mu)$ which represents the square-free part of $Z(\mu P \oplus T')$ (see Table 1) with the property that there exists a prime q such that $(\delta(\mu)/q) = -1$. These will be used to eliminate certain lifted multiples of P. We first have the following definition for the *indicator prime*, q.

Definition 3.1. Let $k \in \mathbb{Z}^+$. We say that q is a 2-torsion prime for k if $q \neq 2, 3, 17$ such that $k\widetilde{P} \neq O, T$ but $2k\widetilde{P} = O$ in $E(\mathbb{F}_q)$ where $\widetilde{P}$ is the reduction of P onto the curve $E(\mathbb{F}_q)$. This implies that $k\widetilde{P} = T'$ or T'' in $E(\mathbb{F}_q)$.

Definition 3.2. Let $k \in \mathbb{Z}^+$ and $\mu = Y \backslash \{-2\}$. We say q is an *indicator prime* for (k, μ) if q is a 2-torsion prime for k and $(\delta(\mu)/q) = -1$.

We are claiming that the only small values of n that make $Z(nP)$ a square are $\mu \in Y = \{-4, -3, -2, -1, 0, 3\}$. We now have the following theorem that provides conditions applied to each of the cases in $\mu \in Y \backslash \{-2\}$ to ensure the lifting of $n \equiv Y \backslash \{-2\} \bmod 2^t k$ to $n \equiv Y \backslash \{-2\} \bmod 2^{t+1} k$ eliminating the five so-called problematic values, namely $n \equiv k + \mu \bmod 2^{t+1} k$ for $\mu \in Y \backslash \{-2\}$. The indicator primes, q, satisfying the hypothesis of the theorem are precisely the q occurring in the denominator of $2k\widetilde{P}$ but not the denominator of $k\widetilde{P}$ and satisfying $x(k\widetilde{P}) \neq 15$.

Theorem 3.3. *Suppose there exists an indicator prime, q. Then for every $\mu \in Y \backslash \{-2\}$ there exists $\delta(\mu) \in \mathbb{Z}$ as defined in Table 1 such that $(\delta(\mu)/q) = -1$, which implies $Z((2k \oplus \mu)P) \neq \square$.*

Proof. Suppose $q \neq 2, 3, 17$. Let $W = k\widetilde{P} = (x_W, y_W)$. This has exact order 2 and $W \neq T$. So $y_W = 0$ and x_W is a root of $(x - 15)(x^2 + 15x - 3042)$ which is $x_W = \frac{3}{2}(-5 \pm 9\beta)$ where $\beta^2 = 17$. The quadratic polynomial $x^2 + 15x - 3042$ has discriminant $3^6 \cdot 17$ and hence splits over $\mathbb{F}_q$ for $q \neq 2, 3, 17$ if and only if $(17/q) = 1$, which implies $\pm q = 1, 2, 4, 8 \bmod 17$.

Let $\mu \in \mathbb{Z}$ and $\mu \neq 0$. Let $\mu P = (r, s)$ and $Q = (k \oplus \mu)P = (x_Q, y_Q)$. Then $2\widetilde{Q} = 2\mu\widetilde{P}$ but $\widetilde{Q} \neq \mu\widetilde{P}$ or $\mu\widetilde{P} \oplus \widetilde{T}$ or else $k\widetilde{P} = O$ or $\widetilde{T}$. We let $T' = (\frac{3}{2}(-5 - 9\beta), 0)$ and $T'' = (\frac{3}{2}(-5 + 9\beta), 0)$ be the other 2-torsion points. Thus

$$\widetilde{Q} = \mu\widetilde{P} \oplus T' = (r, s) \oplus (\tfrac{3}{2}(-5 - 9\beta), 0).$$

Adding this on the curve gives us

$$x_{\widetilde{Q}} = \frac{3}{2(r^2 + 15r - 3042)}((-5r^2 + 4056r - 46755) + 9(r^2 - 30r + 2817)\beta)$$

and

$$y_{\widetilde{Q}} = \frac{-243s}{2(r^2 + 15r - 3042)^2}(51(r^2 - 30r + 2817) - (5r^2 - 1302r + 5445)\beta).$$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

TABLE 1. Conditions following from lifting the multiplier.

$\mu \in Y$	$\delta(\mu)$	Condition applied on $\delta(\mu)$	Implication upon lifting
-4	$13 \cdot 1789$	$\left(\frac{13\cdot1789}{q}\right) = -1$	$n \not\equiv k - 4 \bmod 2k$
-3	$5 \cdot 29$	$\left(\frac{5\cdot29}{q}\right) = -1$	$n \not\equiv k - 3 \bmod 2k$
-2	—	—	—
-1	$5 \cdot 29$	$\left(\frac{5\cdot29}{q}\right) = -1$	$n \not\equiv k - 1 \bmod 2k$
0	$13 \cdot 1789$	$\left(\frac{13\cdot1789}{q}\right) = -1$	$n \not\equiv k \bmod 2k$
3	$5333 \cdot 97324757$	$\left(\frac{5333\cdot97324757}{q}\right) = -1$	$n \not\equiv k + 3 \bmod 2k$

TABLE 2. $Z(\widetilde{Q})$ a square for $\mu \in Y$.

$\mu \in Y$	$\mu P \oplus T'$	$Z(nP)$
-4	$\left(\frac{4482}{361}\beta + \frac{3489}{361}, \frac{-52002}{6859}\beta + \frac{2057238}{6859}\right)$	$2^{22} \cdot 3^{44} \cdot 19^{-32} \cdot \mathbf{13} \cdot \mathbf{1789} \cdot [-469311139\beta + 24250687120]^2$
-3	$\left(\frac{-99}{8}\beta + \frac{93}{8}, \frac{-81}{16}\beta - \frac{5049}{16}\right)$	$2^{-32} \cdot 3^{34} \cdot \mathbf{5} \cdot \mathbf{29} \cdot \left[\frac{-143654012463}{2}\beta + \frac{596091741497}{2}\right]^2$
-2	$(162\beta + 681, -5994\beta - 24786)$	$[2^{13} \cdot 3^{22} \cdot 5 \cdot 19 \cdot 379 \cdot 1433 \cdot 1481\beta + 2^{13} \cdot 3^{23} \cdot 199 \cdot 527732929]^2$
-1	$(-18\beta + 69, -162\beta + 918)$	$2^{24} \cdot 3^{34} \cdot \mathbf{5} \cdot \mathbf{29} \cdot [95293 + 23052\beta]^2$
0	$(\frac{3}{2}(-5 - 9\beta), 0)$	$2^{10} \cdot 3^{44} \cdot \mathbf{13} \cdot \mathbf{1789} \cdot [21\beta + 7]^2$
3	$\left(\frac{-99}{8}\beta + \frac{93}{8}, \frac{81}{16}\beta + \frac{5049}{16}\right)$	$2^{-32} \cdot 3^{34} \cdot \mathbf{5333} \cdot \mathbf{97324757} \cdot \left[\frac{2188485}{2}\beta + \frac{12121421}{2}\right]^2$

Substituting $x_{\widetilde{Q}}$ and $y_{\widetilde{Q}}$ into the expression for $Z(\widetilde{Q})$ gives Table 2. We define $\delta(\mu)$ to be the square-free part of $Z(\widetilde{Q})$. For each of the five problematic values of $\mu \in Y\{-2\}$ we compute a corresponding integer $\delta(\mu)$ (see Table 2) with the property that there exists a prime q such that $(\delta(\mu)/q) = -1$. These will be used to eliminate certain lifted multiples of P. Note that $\mu = -2$ does not possess a square-free part.

Now, for every $\mu \in Y \backslash \{-2\}$, we have the implications from $\delta(\mu)$ as in Table 1. Note that the conditions of $\mu = -1$ and $\mu = 0$ are similar to $\mu = -3$ and $\mu = -4$. Thus, we need only look at the conditions of $(\delta(\mu)/q) = -1$ for $\mu \in \{-1, 0, 3\}$, which implies that $Z((2k + \mu)P) \neq \square$. □

We ultimately obtain congruence conditions on $n \in X$ and $\mu \in Y \backslash \{-2\}$ from the following theorem.

THEOREM 3.4. *Let $k \in \mathbb{Z}^+$. If there exists an indicator prime, q, for (k, μ) then*

$$n \in X, \mu \in Y \backslash \{-2\} \text{ implies } n \equiv k + \mu \bmod 2k.$$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

Proof. Let $k \in \mathbb{Z}^+$. Then for $n \in X$, $\mu \in Y \backslash \{-2\}$ we have $n \equiv \mu \bmod 2^t k$. Conditions imposed on $(\delta(\mu)/q) = -1$ as per Table 1 imply that upon lifting we will have $n \equiv \mu \bmod 2^{t+1}k$, eliminating $n \equiv 2^t + \mu \bmod 2^{t+1}k$. □

4. Cases of $\mu \in \{-1, 0, 3\}$

In this section, we will take a look at the conditions applied on $(\delta(\mu)/q) = -1$ as in Table 1. In order to find an indicator prime, q, satisfying Theorem 3.3 we need to examine the numerator and denominator of $x(kP)$. We let $kP = (s_k/d_k^2, t_k/d_k^3)$ and let $\mathcal{B}_k$ denote the square-free part of the quadratic univariate part of the elliptic curve E, namely $\mathcal{B}_k = s_k^2 + 15s_kd_k^2 - 3042d_k^4$. To find the primes occurring we can use p-adic methods. We first have the following lemma which states the form of $\mathcal{B}_k$.

Lemma 4.1. *Let $\mathcal{B}_k = s_k^2 + 15s_kd_k^2 - 3042d_k^4$ with $\gcd(s_k, d_k) = 1$. Then $\mathcal{B}_k = (-1)^k \cdot 2^{\alpha_k} \cdot 3^{\beta_k} \cdot w_k^2$ where w_k is a positive integer with $\gcd(w_k, 2 \cdot 3 \cdot 17) = 1$ and α_k, β_k are given by*

(1)
$$\alpha_k = \operatorname{ord}_2(\mathcal{B}_k) = \begin{cases} 2 & \textit{if } 6 \nmid k, \\ 0 & \textit{otherwise}; \end{cases}$$

(2)
$$\beta_k = \operatorname{ord}_3(\mathcal{B}_k) = \begin{cases} 0 & \textit{if } 8 \mid k, \\ 4 & \textit{if } 2 \mid k \textit{ but } 8 \nmid k, \\ 6 & \textit{if } k \textit{ is odd}; \end{cases}$$

(3)
$$\operatorname{ord}_{17}(\mathcal{B}_k) = 0.$$

Note that the sign of $\mathcal{B}_k$ is $(-1)^k$, as can be seen by looking at the $\mathbb{R}$-connected components of elliptic curve E which has two connected components.

We apply this lemma to prove the following theorems for the case $\mu = \{-1, 0, 3\} \in Y$. From Table 1, we have the conditions that $5 \cdot 29 \neq \square$, $13 \cdot 1789 \neq \square$ and $5333 \cdot 97324757 \neq \square$, where $5, 29, 13, 1789, 5333, 97324757 \equiv 1 \bmod 4$ (the open square symbol represents a square number). We have the following lemma to show that there always exists a prime number, p, such that product of two primes q_1, q_2 congruent to 1 modulo 4 is not a square.

Lemma 4.2. *Let $q_1, q_2 \equiv 1 \bmod 4$ be distinct primes. Suppose $N \in \mathbb{Z}$ satisfies $\gcd(N, 2q_1q_2) = 1$ and the Legendre symbol $(N/q_1) \neq (N/q_2)$. Then there exists a prime number, p, such that $p \mid N$ and $(q_1 \cdot q_2/p) = -1$.*

This lemma above is handy in proving the following cases of $\mu \in Y \backslash \{-2\}$ in the following theorems. Also, recall that we have $\mathcal{B}_k = (-1)^k \cdot 2^{\alpha_k} \cdot 3^{\beta_k} \cdot w_k^2$, where $w_k \in \mathbb{Z}^+$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

with $\gcd(w_k, 2\cdot 3\cdot 17) = 1$. Let $P_{\mathcal{M}_i}(w_k)$ denote the period of w_k in $\mathbb{Z}/\mathcal{N}\mathbb{Z}$. We define

$$\begin{aligned}
A_5 &= \{k \in \mathbb{Z}/\mathcal{M}_1\mathbb{Z} \mid w_k = \text{square mod } 5 \ \&\ \mathcal{M}_1 = P_5(w_k)\},\\
A_{29} &= \{k \in \mathbb{Z}/\mathcal{M}_2\mathbb{Z} \mid w_k = \text{square mod } 29 \ \&\ \mathcal{M}_2 = P_{29}(w_k)\},\\
A_{13} &= \{k \in \mathbb{Z}/\mathcal{M}_3\mathbb{Z} \mid w_k = \text{square mod } 13 \ \&\ \mathcal{M}_3 = P_{13}(w_k)\},\\
A_{1789} &= \{k \in \mathbb{Z}/\mathcal{M}_4\mathbb{Z} \mid w_k = \text{square mod } 1789 \ \&\ \mathcal{M}_4 = P_{1789}(w_k)\},\\
A_{5333} &= \{k \in \mathbb{Z}/\mathcal{M}_5\mathbb{Z} \mid w_k = \text{square mod } 5333 \ \&\ \mathcal{M}_5 = P_{5333}(w_k)\},\\
A_{97324757} &= \{k \in \mathbb{Z}/\mathcal{M}_6\mathbb{Z} \mid w_k = \text{square mod } 97324757 \ \&\ \mathcal{M}_6 = P_{97324757}(w_k)\}.
\end{aligned}$$

It follows that the complement set is given by

$$\begin{aligned}
A^*_5 &= \{k \in \mathbb{Z}/\mathcal{M}_1\mathbb{Z}\backslash A_5\},\\
A^*_{29} &= \{k \in \mathbb{Z}/\mathcal{M}_2\mathbb{Z}\backslash A_{29}\},\\
A^*_{13} &= \{k \in \mathbb{Z}/\mathcal{M}_3\mathbb{Z}\backslash A_{13}\},\\
A^*_{1789} &= \{k \in \mathbb{Z}/\mathcal{M}_4\mathbb{Z}\backslash A_{1789}\},\\
A^*_{5333} &= \{k \in \mathbb{Z}/\mathcal{M}_5\mathbb{Z}\backslash A_{5333}\},\\
A^*_{97324757} &= \{k \in \mathbb{Z}/\mathcal{M}_6\mathbb{Z}\backslash A_{97324757}\}.
\end{aligned}$$

By building C++ code we have checked that the periods $\mathcal{M}_1 = 30$, $\mathcal{M}_2 = 102$, $\mathcal{M}_3 = 30$, $\mathcal{M}_4 = 2670$, $\mathcal{M}_5 = 750$ and $\mathcal{M}_6 = 97306362$. We now have the following theorem.

THEOREM 4.3. *Let $k \in \mathbb{Z}^+$ satisfying the following congruence condition*

$$\begin{gathered}
\{k \equiv A_5 \bmod 30 \textit{ and } k \equiv A^*_{29} \bmod 102\\
\textit{or}\\
k \equiv A^*_5 \bmod 30 \textit{ and } k \equiv A_{29} \bmod 102\},\\
\textit{and}\\
\{k \equiv A_{13} \bmod 30 \textit{ and } k \equiv A^*_{1789} \bmod 2670\\
\textit{or}\\
k \equiv A^*_{13} \bmod 30 \textit{ and } k \equiv A_{1789} \bmod 2670\},\\
\textit{and}\\
\{k \equiv A_{5333} \bmod 750 \textit{ and } k \equiv A^*_{97324757} \bmod 97306362\\
\textit{or}\\
k \equiv A^*_{5333} \bmod 750 \textit{ and } k \equiv A_{97324757} \bmod 97306362\}.
\end{gathered}$$

Then there exists an indicator prime $q \neq 2, 3, 17$ and $\{5\cdot 29 \neq \square \bmod q, 13\cdot 1789 \neq \square \bmod q, 5333\cdot 97324757 \neq \square \bmod q$ such that $\mu = \{-4, -3, -1, 0, 3\} \in Y$ implies $n \not\equiv k-1 \bmod 2k, n \not\equiv k-3 \bmod 2k, n \not\equiv k-4 \bmod 2k$ and $n \not\equiv k \bmod 2k$ and $n \not\equiv k+3 \bmod 2k$.

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

5. Existence of a suitable pair (M, k_0)

In this section, we will show the existence of a suitable pair (M, k_0) based on the congruence condition as per Theorem 4.3. We now find an initial value, k_0, that satisfies the following definition.

Definition 5.1. Let $M \in \mathbb{N}$. Let $\emptyset \neq \mathcal{S} \subseteq \{0, 1, \ldots, M-1\}$. We say that (M, k_0) is a suitable pair if

(1) $2\mathcal{S} \equiv \mathcal{S} \bmod M$,

(2) $X \equiv Y \bmod k_0$ where $k_0 = \min(\mathcal{S})$, and

(3) for every $k \in \mathcal{S}$ there exists a universal indicator prime.

We now have the following theorem.

Theorem 5.2. *Let* $M = 2 \cdot 3^2 \cdot 5^3 \cdot 17 \cdot 89 \cdot 829 \cdot 6521 = 18403065713250$, *and let* $k_0 = 2 \cdot 17 \cdot 89 = 3026$. *Then there exists a suitable pair* (M, k_0).

The following theorem follows from the doubling closed set, $\mathcal{S}$, that we obtained above.

Theorem 5.3. *If* $k \equiv 3026 \bmod 18403065713250$ *then there exists a universal indicator prime, q, in kP satisfying all conditions such that* $(\delta(\mu)/q) = -1$ *for* $\delta(\mu)$ *values as per Table 1.*

Note that there could be more than one indicator prime apart from $q = 248840234180189$ in the denominator of $6052P$ that satisfies conditions of $(\delta(\mu)/q) = -1$ for $\delta(\mu)$ as per Table 1. Unfortunately, due to the limitations of large number factorization, we only found one such indicator prime, $q = 248840234180189$.
In the next section, we look for the prime divisors, p, of the denominator, dP, where $d \mid 3026$. Then, we find $Z(nP)$ not a square modulo p to perform the elimination.

6. Reducing sets to show $n \equiv \{-4, -3, -1, 0, 3\} \bmod 3026$

We work with the prime divisors of $3026P$ to show that $Z(nP)$ is not a square modulo p, which will eliminate certain congruence classes. Our aim is to show that the only elements that will survive are $\{3, 3022, 3023, 3024, 3025, 3026\} \bmod 3026$, eliminating the rest of the elements, which is achieved upon looking at multiples of 2 and 3. We have eliminated all elements, leaving only possible solutions given by $n \equiv -4, -3, -2, -1, 0, 3 \bmod 3026$. This huge calculation leads us to show that for all $n \in X$, $X \equiv Y \bmod 3026$. We now have the following theorem.

Theorem 6.1. *If there exists a suitable pair* (M, k_0) *then* $X = Y$.

Proof. We prove by induction that $X \equiv Y \bmod 2^r k_0$ for every nonnegative integer r. The case $r = 0$ is part (2) of Definition 5.1. Suppose inductively that $X \equiv Y \bmod 2^r k_0$. Thus

$$n \in X \text{ implies } n \equiv \mu \bmod 2^r k_0 \text{ for some } \mu \in Y.$$

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

Let $n \in X$. Let $k = 2^r k_0$. Then there exists $\mu \in Y$ such that $n \equiv \mu$ or $\mu + k \bmod 2k$. By (1) of Definition 5.1, $k \in \mathcal{S}$ and by (3) there exists an indicator prime q for (k, μ). Theorem 3.4 rules out $n \equiv \mu + k \bmod 2k$, so $n \equiv \mu \bmod 2k$. Since $n \in X$ was arbitrary, $X \equiv Y \bmod 2k$ which completes the induction. □

Table 1 indicated that there is no condition imposed on $(\delta(-2)/q) = -1$ from which we were unable to eliminate the lifting of $n \equiv 2^t k - 2 \bmod 2^{t+1}k$ for $k \in \mathbb{Z}^+$ values. Because we were unable to eliminate this case by applying the methodology introduced in this paper, numerous other independent methods and ideas were exploited, but unfortunately they were not strong enough to give a subtle argument to eliminate the lifting of $n \equiv 2^t k - 2 \bmod 2^{t+1}k$. This implies that a 'second ascent' would be needed to deal with this case. This would be a fundamental base for future work as it could possibly indicate the existence of one or more further points on the curve, of enormous height which comes from the congruence $n \equiv 3024 \bmod 3026$ that could possibly give us a perfect triangle, though it seems highly unlikely.

7. Proving Theorem 1.1

We now prove the core theorem of this paper. First, we have the following lemma which proves that the sets X and $Y \backslash \{-2\}$ are the same.

LEMMA 7.1. *Let $t \in \mathbb{Z}$. Then $X \equiv Y \backslash \{-2\} \bmod 3026 \cdot 2^t$ implies $X \equiv Y \backslash \{-2\} \bmod 3026 \cdot 2^{t+1}$. Thus by induction $X = \{-4, -3, -1, 0, 3\}$.*

PROOF. We have $X \equiv Y \backslash \{-2\} \bmod 3026$. The existence of an indicator prime, q, which gives $(\delta(\mu)/q) = -1$ for $\delta(\mu)$ as in Table 1, implies that $X \equiv Y \backslash \{-2\} \bmod 2 \cdot 3026$, eliminating $X \equiv \{3022, 3023, 3025, 3026, 3029\} \bmod 2^t \cdot 3026$. Since $k_0 = 3026 \in \mathcal{S}$, the closed doubling set, we will have $X \equiv Y \backslash \{-2\} \bmod 2^{t+1} \cdot 3026$ every time k_0 lifts. Thus by induction $X = Y \backslash \{-2\}$. □

Since we have proved that the set X and $Y \backslash \{-2\}$ are the same, consisting of only five elements, we conclude by proving the main result of this paper.

THEOREM 7.2. *There does not exist any perfect triangle arising from the curve C_4: $\theta\phi(\theta - \phi) + \theta\phi + 2(\theta - \phi) - 1$ except possibly for $n \equiv 3024 \bmod 6052$.*

Here, the word 'except' indicates that there may exist one or more further points on the curve that is of enormous height which could possibly form a perfect triangle.

PROOF. From Theorem 2.1, we proved that there exists a perfect triangle on the curve C_4 with $\phi \neq 0$ if and only if $Z(nP)$ is a square, which is true only for $n \in X = \{-4, -3, -1, 0, 3\}$. We now have the following table of $n \in X$ and the corresponding value of ϕ and m.

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press

n	nP=(x, y) on E	corresp. ϕ	m
-4	$(339, -6156)$	$-\frac{1}{2}$	$\pm\frac{9}{8}$, $\pm\frac{1}{4}\sqrt{949}$
-3	$(6, 162)$	0	$\pm\frac{9}{8}$
-2	$(51, 108)$	undefined	undefined
-1	$(-21, -324)$	undefined	undefined
0	$(0, 0)$	$-\frac{4}{11}$	$\frac{1}{10648}\sqrt{\pm\frac{391779925}{2}\sqrt{6829}+\frac{32625600067}{2}}$ $\frac{-1}{10648}\sqrt{\pm\frac{391779925}{2}\sqrt{6829}+\frac{32625600067}{2}}$
3	$(6, -162)$	0	$\pm\frac{9}{8}$

In [4] it is proven that a Heron triangle with two rational medians lies only on the region defined by $0 < \theta < 1$, $0 < \phi < 1$ and $2\theta + \phi > 1$. These inequalities exclude regions in which a proper triangle cannot form. It is clear from the table above that the corresponding values of ϕ in each case either lie outside the region defined or are undefined. This implies that there does not exist any perfect triangle arising from curve C_4 except possibly for the case $\mu = -2$ that gives $n \equiv 3024 \bmod 3026$. □

Acknowledgements

I am grateful to my supervisor Victor Scharaschkin who provided expertise that greatly assisted the research provided in this paper. I am also grateful to Ralph Buchholz who moderated this paper, and in so doing improved the manuscript by providing feedback. Finally, I am grateful to Ivan P. who provided expertise in advanced C++ software used to obtain some of the results in this research.

References

[1] Z. F. Bácskái, R. H. Buchholz, R. L. Rathbun and M. J. Smith, Symmetries of triangles with two rational medians, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.65.6533, (2003).

[2] R. H. Buchholz, 'On triangles with rational altitudes, angle bisectors and medians', PhD Thesis, University of Newcastle, Australia, 1989.

[3] R. H. Buchholz and R. L. Rathbun, 'An infinite set of heron triangles with two rational medians', *Amer. Math. Monthly* **104**(2) (1997), 106–115.

[4] R. H. Buchholz and R. L. Rathbun, 'Heron triangles and elliptic curves', *Bull. Aust. Math. Soc.* **58** (1998), 411–421.

[5] R. H. Buchholz, 'Triangles with three rational medians', *J. Number Theory* **97**(1) (2002), 113–131.

[6] R. H. Buchholz and R. P. Stingley, Heron triangles with three rational medians, https://ca827bd0-a-62cb3a1a-s-sites.googlegroups.com/site/teufelpi/papers/D21.pdf?attachauth=ANoY7cpsOhPDAmImchFC8BEi, (2013).

[7] H. Cohen, *Number Theory: Volume II: Analytic and Modern Tools*, 2nd edn (Springer, New York, 2007).

[8] L. E. Dickson, *History of the Theory of Numbers* (Carnegie Institution, Washington, 1919).

[9] A. Dujella and J. C. Peral, ‘Elliptic curves and triangles with three rational medians’, *J. Number Theory* **133** (2013), 2083–2091.

[10] A. Dujella and J. C. Peral, ‘Elliptic curves coming from heron triangles’, *Rocky Mountain J. Math.* **44**(4) (2014), 1145–1160.

[11] L. Euler, ‘Solutio facilior problematis Diophantei circa triangulum in quo rectae ex angulis latera opposita bisecantes rationaliter exprimantur’, *Mem. Acad. Sci. St. Petersburg* **2** (1810), 10–16; [See L. Euler, *Opera Omnia, Commentationes Arithmeticae* **3**, paper 732 (1911)].

[12] G. Faltings, ‘Endlichkeitsästze für abelsche Varietten ber Zahlkörpern’, *Invent. Math.* **73**(3) (1983), 349–366.

[13] R. Guy, *Unsolved Problems in Number Theory* (Springer, New York, 1981).

[14] R. Rathbun, Perfect rational triangle, https://www.ics.uci.edu/~eppstein/junkyard/q-triangle.html, (1987).

[15] J. H. Silverman, *Graduate Texts in Mathematics: The Arithmetic of Elliptic Curves*, 2nd edn (Springer, New York, 2009).

[16] P. Stanica, S. Sarkar, S. S. Gupta, S. Maitra and N. Kar, ‘Counting Heron triangles with constraints’, *J. Integers* **13** (2013), A3.

SHAHRINA ISMAIL, School of Mathematics and Physics,
The University of Queensland, St Lucia, Qld 4072, Australia
e-mail: s.ismail1@uq.edu.au

https://doi.org/10.1017/S144678871900003X Published online by Cambridge University Press