Journal of Number Theory 213 (2020) 232–253

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Heron triangles and their elliptic curves

Lorenz Halbeisen, Norbert Hungerbühler *

Department of Mathematics, ETH Zentrum, Rämistrasse 101, 8092 Zürich, Switzerland

ARTICLE INFO

Article history:
Received 17 July 2019
Received in revised form 2 December 2019
Accepted 9 December 2019
Available online 21 January 2020
Communicated by A. Pal

MSC:
11G05
11D09

Keywords:
Heron triangles
θ-triangles
Heronian elliptic curves
Congruent numbers

ABSTRACT

In geometry, a Heron triangle is a triangle with rational side lengths and integral area. We investigate Heron triangles and their elliptic curves. In particular, we provide some new results concerning Heron triangles and give elementary proofs for some results concerning Heronian elliptic curves.

1. Introduction

Motivated by Goins [2] and based on our research [4,5], we investigate Heron triangles and the corresponding elliptic curves. In particular, we give elementary proofs for some results in Goins and Maddox [3] and generalize the main results of [4] and [5].

* Corresponding author.
E-mail addresses: lorenz.halbeisen@math.ethz.ch (L. Halbeisen), norbert.hungerbuehler@math.ethz.ch (N. Hungerbühler).

https://doi.org/10.1016/j.jnt.2019.12.005
0022-314X/

In Section 2, we introduce and investigate H-triples: A rational triple $(a, b, \lambda) \in \mathbb{Q}^3$ is called an H-triple if a, b are non-zero and $c := \sqrt{a^2 - 2\lambda ab + b^2}$ is rational. This notion generalizes Heron triples, for which $\sqrt{1-\lambda^2}$ is a positive rational number, and for which a Heron triangle exists, *i.e.*, a triangle with integral area and rational sides $|a|, |b|, c$ such that the cosine of the angle opposite of side c is λ. We start by giving a relation between solutions of $(p^2 - q^2)(a^2 - b^2) = r^2 - s^2$ in positive integers and the existence of certain pairs of H-triples. In particular, in Proposition 2 we show that non-zero integers p, q, a, b, r, s are an integral solution for the Diophantine equation $(p^2 - q^2)(a^2 - b^2) = r^2 - s^2$ if and only if there is a rational $\lambda \in \mathbb{Q}$ such that both, (qa, pb, λ) and (pa, qb, λ), are H-triples.

Based on Section 2 we investigate families of Heron triangles sharing a given angle in Section 3. In particular, we first formulate an algorithm which generalizes a result of Fermat's, to produce infinitely many Heron triangles sharing the same angle and the same area. Then, we characterize isosceles Heron triangles by showing in Theorem 6 that there is an isosceles Heron triangle (a, b, c) with $a = b$ if and only if there are $u, v \in \mathbb{N}$ such that $\frac{v^2-u^2}{u^2+v^2} = \frac{a^2+b^2-c^2}{2ab}$ and u^2+v^2 is a square. Furthermore, we investigate pairs of integral isosceles Heron triangles and integral Pythagorean triangles of the same area, and show in Proposition 7 that every positive integral solution of the Diophantine equation $pq(p^2 - q^2) = 2mn(m^2 - n^2) \cdot \square$ (where $\square$ denotes a square) leads to such a pair. Non-trivial solutions of this Diophantine equation are given in Corollary 8. Finally, by generalizing a result from [5], we construct triples of integral Heron triangles of the same area and sharing an angle from positive solutions of the Diophantine equation $m = n^2 + nl + l^2$.

In Section 4, we investigate the torsion group and the rank of elliptic curves related to Heron triangles, so-called Heronian elliptic curves, which are curves of the form

$$E_{u,v,A}: \quad y^2 = x^3 + \frac{v^2 - u^2}{uv} Ax^2 - A^2 x\,, \quad \text{where } A \text{ is a positive integer.}$$

Here we use results from Section 3. In particular, we provide a new proof for Theorem 15 which states that the torsion group of a Heronian elliptic curve $E_{u,v,A}$ is isomorphic either to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or — in the case when there exists an isosceles Heron triangle with area A — to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The proof given by Goins and Maddox [3, Proposition 3.3] relies on Mazur's Theorem, which states that the torsion group of an elliptic curve is isomorphic to one of fifteen groups, and uses twice a symbolic computer package (e.g., MAGMA) in order to show that Heronian elliptic curves never have rational points of order 3 or of order 8. However, in the proof given below, we do not need computer assistance, and in the case when u and v are both odd, we do not even use Mazur's Theorem. At the end of this article, we show — by generalizing a result from [5] — under which conditions positive solutions of $m = n^2 + nl + l^2$ lead to Heronian elliptic curves of rank at least 2 and provide examples of Heronian elliptic curves of rank 5.

2. H-triples

2.1. A theorem of Sós

A rational triple $(a, b, \lambda) \in \mathbb{Q}^3$, where a, b are non-zero, is called a **H-triple** if

$$c := \sqrt{a^2 - 2\lambda ab + b^2} \quad \textit{is rational.}$$

Theorem 1 *(Sós). For every H-triple (a, b, λ) there are relatively prime integers $m, n \in \mathbb{Z}$ and a rational $\mu \in \mathbb{Q}$, such that*

$$\begin{aligned} a &= \mu(m^2 - n^2) \\ b &= \mu\big(2m(n + \lambda m)\big) \\ c &= \mu\big(m^2 + 2\lambda mn + n^2\big) \end{aligned} \tag{1}$$

For a proof see Sós [11, p. 189].

Notice that for $\lambda = 0$ the set of equations (1) corresponds to the well-known formula for rational Pythagorean triples. Notice also that for $-1 < \lambda < 1$, the values $|a|, |b|, |c|$ are the side lengths of a triangle with $\cos(\theta) = \lambda$, where $\theta := \sphericalangle ACB$.

2.2. The Diophantine equation $(p^2 - q^2)(a^2 - b^2) = r^2 - s^2$

The following proposition which will be used later on connects H-triples with the Diophantine equation $(p^2 - q^2)(a^2 - b^2) = r^2 - s^2$.

Proposition 2. *The non-zero integers p, q, a, b, r, s are an integral solution for the Diophantine equation $(p^2 - q^2)(a^2 - b^2) = r^2 - s^2$ if and only if there is a rational $\lambda \in \mathbb{Q}$ such that (qa, pb, λ) and (pa, qb, λ) are both H-triples with*

$$s^2 = (qa)^2 - 2\lambda(qa)(pb) + (pb)^2$$

and

$$r^2 = (pa)^2 - 2\lambda(pa)(qb) + (qb)^2.$$

Proof. Assume that the non-zero integers p, q, a, b, r, s are a solution for the equation $(p^2 - q^2)(a^2 - b^2) = r^2 - s^2$. Let $\bar{a} := qa$ and $\bar{b} := pb$ and

$$\lambda := \frac{\bar{a}^2 + \bar{b}^2 - s^2}{2\bar{a}\bar{b}}.$$

Then, $\lambda \in \mathbb{Q}$ and

$$\bar{a}^2 - 2\lambda\bar{a}\bar{b} + \bar{b}^2 = s^2,$$

which shows that (qa, pb, λ) is an H-triple.

Furthermore, we obtain

$$\begin{aligned}(pa)^2 - 2\lambda(pa)(qb) + (qb)^2 &= (pa)^2 - \big((qa)^2 + (pb)^2 - s^2\big) + (qb)^2\\ &= (p^2 - q^2)(a^2 - b^2) + s^2\\ &= r^2,\end{aligned}$$

which shows that (pa, qb, λ) is an H-triple.

For the other implication, assume that (qa, pb, λ) and (pa, qb, λ) are both H-triples, and that $s^2 = (qa)^2 - 2\lambda(qa)(pb) + (pb)^2$ and $r^2 = (pa)^2 - 2\lambda(pa)(qb) + (qb)^2$ are both integers. Then

$$r^2 - s^2 = (pa)^2 - (qa)^2 - \big((pb)^2 - (qb)^2\big) = (p^2 - q^2)(a^2 - b^2)\,,$$

which completes the proof. *q.e.d.*

3. Heron triples and Heron triangles

3.1. Heron triples

An H-triple $(a, b, \lambda) \in \mathbb{Q}^3$ is called a **Heron triple** if

$$\bar{\lambda} := \sqrt{1 - \lambda^2} \in \mathbb{Q}^+ \qquad \textit{and} \qquad A := \bar{\lambda}\frac{|ab|}{2} \in \mathbb{N}\,.$$

Notice that if (a, b, λ) is a Heron triple, then

$$\lambda = \frac{1 - \tau^2}{1 + \tau^2}$$

for some $\tau \in \mathbb{Q}$. If we set $\tau = \frac{u}{v}$, where we always assume that u and v are relatively prime, then

$$\lambda = \frac{v^2 - u^2}{u^2 + v^2} \qquad \textit{and} \qquad \bar{\lambda} = \frac{2uv}{u^2 + v^2}\,.$$

In particular we obtain

$$A = \frac{uv}{u^2 + v^2}\,ab\,,$$

and since $(u, v) = 1$ and A is integral, we have that $u^2 + v^2$ divides ab. In the sequel we will write $Q := ab$. In particular, it follows that λQ is integral.

3.2. Heron triangles

If $(a, b, \lambda) \in \mathbb{Q}^3$ is a Heron triple and $c := \sqrt{a^2 - 2\lambda ab + b^2}$, then $|a|, |b|, c$ are the lengths of the sides of a triangle with integral area A and $\lambda = \cos(\theta)$, where θ is the angle opposite to the side c. In abuse of notation, the triple (a, b, c) is called a **Heron Triangle**.

In the case $\lambda = 0$ (*i.e.*, for right-angled triangles), Fermat stated in [1] without proof a formula which generates for a given rational Pythagorean triangle a new rational Pythagorean triangle with the same area. The following two results generalize Fermat's formula to Heron triangles (for a proof of Fermat's formula see [4, Thm. 3]).

Lemma 3. *Let (a, b, λ) be a Heron triple and let (a, b, c) be the corresponding Heron triangle. Then*

$$(a^2 - b^2)^2 = c^4 + 4\lambda Q c^2 - 16A^2.$$

In particular,

$$|a^2 - b^2| = \sqrt{c^4 + 4\lambda Q c^2 - 16A^2}.$$

Proof. First notice that

$$c^4 - 16A^2 = (a^2 - 2\lambda Q + b^2)^2 - 4(1 - \lambda^2)Q^2 = (a^2 - b^2)^2 - 4\lambda Q(a^2 + b^2) + 8\lambda^2 Q^2,$$

and since $a^2 + b^2 = c^2 + 2\lambda Q$, we obtain

$$(a^2 - b^2)^2 = c^4 + 4\lambda Q c^2 - 16A^2. \quad q.e.d.$$

Theorem 4 *(Generalized Fermat Algorithm). Let (a_0, b_0, λ) be a Heron triple with $a_0 \neq b_0$, and let (a_0, b_0, c_0) be the corresponding Heron triangle with integral area A. Further assume that $\lambda = \frac{v^2 - u^2}{u^2 + v^2}$ where u, v are both odd and relatively prime.*

Then the algorithm $(a_n, b_n, c_n) \mapsto (a_{n+1}, b_{n+1}, c_{n+1})$, where

$$\begin{aligned} a_{n+1} &= \frac{\sqrt{c_n^4 + 4\lambda Q c_n^2 - 16A^2}}{2c_n} = \frac{|a_n^2 - b_n^2|}{2c_n} \\ b_{n+1} &= \frac{2a_n b_n c_n}{\sqrt{c_n^4 + 4\lambda Q c_n^2 - 16A^2}} = \frac{2a_n b_n c_n}{|a_n^2 - b_n^2|} \\ c_{n+1} &= \frac{c_n^4 + 16A^2}{2c_n\sqrt{c_n^4 + 4\lambda Q c_n^2 - 16A^2}} = \frac{c_n^4 + 16A^2}{2c_n|a_n^2 - b_n^2|} \end{aligned} \tag{2}$$

generates an infinite sequence of pairwise distinct Heron triangles with area A. Moreover, the Heron triangles (a_n, b_n, c_n) and $(a_{n+1}, b_{n+1}, c_{n+1})$ share the same angle $\theta = \arccos(\lambda)$, opposite the side c_n and c_{n+1} respectively.

Proof. First we show that if (a_n, b_n, λ) is a Heron triple, then $(a_{n+1}, b_{n+1}, \lambda)$ is also a Heron triple: Notice that $a_n b_n = a_{n+1} b_{n+1}$. Under the assumption that

$$c_n^2 = a_n^2 - 2\lambda a_n b_n + b_n^2,$$

we have to show that

$$c_{n+1}^2 = a_{n+1}^2 - 2\lambda a_{n+1} b_{n+1} + b_{n+1}^2.$$

In particular, we have to check that

$$(c_n^4 + 16A^2)^2 = (a_n^2 - b_n^2)^4 - 2\lambda(a_n^2 - b_n^2)^2(4a_n b_n c_n^2) + (4a_n b_n c_n^2)^2,$$

where $16A^2 = 4(1-\lambda^2)(a_n b_n)^2$, but this is just a simple calculation.

Now we show that the Heron triangles (a_n, b_n, c_n) obtained by Fermat's Algorithm are pairwise distinct: Let (a_0, b_0, c_0) be a Heron triangle. Without loss of generality, we may assume that a_0, b_0, c_0 are integral. Since u and v are both odd, $v^2 - u^2 \equiv 0 \pmod 8$ and $u^2 + v^2 \equiv 2 \pmod 4$, say $v^2 - u^2 = 8s$, $u^2 - v^2 = 4t + 2$. Hence we have

$$\frac{v^2 - u^2}{u^2 + v^2} = \frac{4s}{2t+1} = \frac{2^k \cdot \nu}{\eta}$$

for some odd integers ν, η (or $\nu = 0$) and $k \geq 2$. Furthermore, since $u^2 + v^2$ divides $a_0 b_0$, we have that $\eta \mid a_0 b_0$, in particular, $\frac{\nu}{\eta} \cdot a_0 b_0$ is integral. Now,

$$c_0^2 = a_0^2 + b_0^2 - 2^{k+1} \cdot \tfrac{\nu}{\eta} \cdot a_0 b_0 \,.$$

Let 2^l be the greatest common power of 2 which divides both a_0 and b_0 and let $a := \frac{a_0}{2^l}$, $b := \frac{b_0}{2^l}$, and $c := \frac{c_0}{2^l}$. Since η is odd and $\eta \mid a_0 b_0$, we have $\eta \mid ab$. Now, we show that c is an odd integer. For this, we consider the following two cases:

a and b are both odd: In this case we have $a^2 + b^2 \equiv 2 \pmod 4$, and therefore we have

$$a^2 + b^2 - 4\big(2^{k-1} \cdot \tfrac{\nu}{\eta} \cdot ab\big) \equiv 2 \pmod 4,$$

which implies that $a^2 + b^2 - 4\big(2^{k-1} \cdot \frac{\nu}{\eta} \cdot ab\big)$ is not a square, and therefore,

$$a^2 + b^2 - 2^{k+1} \cdot \tfrac{\nu}{\eta} \cdot ab \neq c^2,$$

which is a contraction to our assumption that (a_0, b_0, c_0) are the lengths of the sides of a Heron triangle.

Exactly one of a and b is odd: In this case we have that a^2+b^2 and $a^2+b^2-2^{k+1}\cdot\frac{\nu}{\eta}\cdot ab$ are both odd, which implies that c is an odd integer.

So, without loss of generality we may assume that a_0, b_0, c_0 are positive integers, one of a_0 and b_0 is even and the other is odd, and c_0 is odd. In particular, c_0 is of the form

$$c_0 = \frac{r}{2^k \cdot s} \quad \text{where } r \text{ is odd, } s = 1, \text{ and } k = 0.$$

Now, we can follow the corresponding proof for $\lambda = 0$ (*i.e.*, $u = v = 1$), given in [4]: Assume that c_n is of the form

$$c_n = \frac{r}{2^k \cdot s}\,,$$

where r and s are both odd and $k \geq 0$. Since $a_{n+1}, b_{n+1}, c_{n+1}$ are rational, $|a_{n+1}^2 - b_{n+1}^2| = \sqrt{c_n^4 + 4\lambda Q c_n^2 - 16A^2}$ is rational. In particular, there are some odd integers $\bar{r}, \tilde{r}, \bar{s}, \tilde{s}$, such that

$$c_n^4 + 16A^2 = \frac{\bar{r}}{2^{4k}\bar{s}} \qquad \text{and} \qquad \sqrt{c_n^4 + 4\lambda Q c_n^2 - 16A^2} = \frac{\tilde{r}}{2^{2k}\tilde{s}}.$$

Therefore,

$$|c_{n+1}| = \frac{c_n^4 + 16A^2}{2c_n\sqrt{c_n^4 + 4\lambda Q c_n^2 - 16A^2}} = \frac{\frac{\bar{r}}{2^{4k}\bar{s}}}{2 \cdot \frac{r}{2^k s} \cdot \frac{\tilde{r}}{2^{2k}\tilde{s}}} = \frac{2^{3k} s\tilde{s}\bar{r}}{2^{4k+1} r\tilde{r}\bar{s}} = \frac{r'}{2^{k+1}s'}$$

for some odd integers r' and s'. This shows that

$$c_n = \frac{r}{2^k \cdot s} \quad \Rightarrow \quad |c_{n+1}| = \frac{r'}{2^{k+1} \cdot s'}$$

where r, s, r', s' are odd. *q.e.d.*

Notice that in the case when u and v are both odd, we always have $a_n \neq b_n$. On the other hand, if $u + v$ is odd, it may happen that $a_0 = b_0$, in which case the algorithm breaks down. However, one can show that if $u + v$ is odd and $a_0 \neq b_0$, then Fermat's Algorithm generates an infinite sequence of pairwise distinct Heron triangles with area A and the same angle θ (see Corollary 16).

3.3. A decoupled version of the Fermat formulas

The recursion (2) consists of three coupled formulas. Only c_{n+1} can be computed from c_n alone, whereas the formulas for a_{n+1} and b_{n+1} require a_n, b_n and c_n as input. Here we give a decoupled version of the recursion, which is most easily formulated in terms of the squares of the sides:

Proposition 5. *Let (a_n, b_n, c_n) be the sequence generated by Fermat's Algorithm in Theorem 4. Consider the squares*

$$X_n := a_n^2, \quad Y_n := b_n^2, \quad Z_n := c_n^2,$$

and the quantities

$$\mu := X_0 Y_0, \quad \nu := Z_0 - X_0 - Y_0.$$

Then, there holds:

$$X_{n+1} = \frac{(X_n^2 - \mu)^2}{4X_n(X_n^2 + X_n\nu + \mu)}$$

$$Y_{n+1} = \frac{4Y_n\mu(Y_n^2 + Y_n\nu + \mu)}{(Y_n^2 - \mu)^2}$$

$$Z_{n+1} = \frac{(Z_n^2 - \nu^2 + 4\mu)^2}{4Z_n((Z_n - \nu)^2 - 4\mu)}$$

Proof. We replace in the formulas for $X_{n+1}, Y_{n+1}, Z_{n+1}$ the expressions for μ and ν and subtract the corresponding expressions from Theorem 4 for $a_{n+1}^2, b_{n+1}^2, c_{n+1}^2$. Observe that $A^2 = \frac{\mu}{4} - \frac{\nu^2}{16}$. Short calculations show that the result reduces to zero in all three cases. *q.e.d.*

3.4. Isosceles Heron-triangles

The following result gives a characterization for values of λ, such that corresponding Heron triangle (a, b, c) is isosceles with $a = b$.

Theorem 6. *Let $\cos(\theta) = \lambda$, where $\lambda = \frac{v^2-u^2}{u^2+v^2}$. Then there is an isosceles Heron triangle (a, b, c), with $a = b$ and a corresponding Heron triple (a, b, λ), if and only if $u^2 + v^2 = \square$ (i.e., $u^2 + v^2$ is a square).*

Proof. If $(u, v) = 1$ and $u^2 + v^2 = \square$, then there are relatively prime, positive integers m and n such that $\{u, v\} = \{m^2 - n^2, 2mn\}$. Without loss of generality, let us assume that $u = m^2 - n^2$ and $v = 2mn$. Then

$$1 - \lambda = \frac{(u^2 + v^2) - (v^2 - u^2)}{u^2 + v^2} = \frac{2u^2}{u^2 + v^2}.$$

Let $a = b = m^2 + n^2$ and let $c = 2(m^2 - n^2)$. Then, we have $c^2 = 4(m^2 - n^2)^2$ and

$$a^2 - 2\lambda ab + b^2 = 2a^2(1 - \lambda) = 2(m^2 + n^2)^2 \frac{2(m^2 - n^2)^2}{(m^2 + n^2)^2} = 4(m^2 - n^2)^2,$$

which shows that (a, b, c) is an isosceles Heron triangle.

If (a, b, λ) is a Heron triple with $a = b$, then, by Theorem 1, there are relatively prime integers $m, n \in \mathbb{Z}$ and a rational $\mu \in \mathbb{Q}$, such that $a = \mu(m^2-n^2)$ and $b = \mu\big(2m(n+\lambda m)\big)$. Now, since $a = b$, we obtain

$$n = m\Big(\frac{\pm 2u}{\sqrt{u^2+v^2}} - 1\Big),$$

and since $n \in \mathbb{Z}$, this implies $u^2 + v^2 = \square$. *q.e.d.*

3.5. When Heron meets Pythagoras

A pair $(a_0, b_0, 0)$, (a_1, a_1, λ) of Heron triples is a **Heron-Pythagoras Pair** if $\lambda \neq 0$ and

$$\frac{a_0 b_0}{2} = \bar{\lambda}\frac{a_1^2}{2}\,.$$

By definition, if $(a_0, b_0, 0)$, (a_1, a_1, λ) is a pair of Heron triples, then, for

$$c_0 := \sqrt{a_0^2 + b_0^2} \qquad \text{and} \qquad c_1 := \sqrt{2a_1^2(1-\lambda)},$$

the Heron triangles (a_0, b_0, c_0) and (a_1, a_1, c_1) have the same area and in addition, the triangle (a_0, b_0, c_0) is a right-angled triangle and the triangle (a_1, a_1, c_1) is isosceles. We call (a_0, b_0, c_0) and (a_1, a_1, c_1) a **Pair of Heron-Pythagoras Triangles**.

The following result shows how we can construct integral pairs of Heron-Pythagoras triangles.

Proposition 7. *Every positive integral solution of the Diophantine equation*

$$pq(p^2 - q^2) = 2mn(m^2 - n^2) \cdot \square \tag{3}$$

leads to an integral pair of Heron-Pythagoras triangles.

Proof. Let p, q, m, n be a positive integral solution of (3). Let $a_0 := p^2 - q^2$, $b_0 := 2pq$, and $c_0 := p^2 + q^2$. Then (a_0, b_0, c_0) is a right-angled triangle with area $pq(p^2 - q^2)$. Now, let $u := m^2 - n^2$ and $v := 2mn$. Then $u^2 + v^2 = \square$. Furthermore, we have

$$\lambda = \frac{6m^2n^2 - m^4 - n^4}{(m^2+n^2)^2} \qquad \text{and} \qquad \bar{\lambda} = \frac{4mn(m^2-n^2)}{(m^2+n^2)^2}$$

which implies

$$2 - 2\lambda = \left(\frac{2(m^2-n^2)}{(m^2+n^2)}\right)^2.$$

Since $pq(p^2-q^2) = 2mn(m^2-n^2)\cdot\square$,

$$\sqrt{\frac{pq(p^2-q^2)}{2mn(m^2-n^2)}} = s$$

for some integer s. Finally, let $a_1 = s(m^2+n^2)$ and let $b_1 = a_1$. Then

$$a_1^2 - 2\lambda a_1 b_1 + b_1^2 = a_1^2(2-2\lambda) = s^2\big((2(m^2-n^2)\big)^2.$$

So, for $c_1 := 2s(m^2-n^2)$, (a_1, a_1, c_1) is a Heron triangle with area

$$\frac{\bar{\lambda}}{2}\,a_1^2 = \frac{2mn(m^2-n^2)}{(m^2+n^2)^2}\cdot s^2(m^2+n^2)^2 = pq(p^2-q^2).$$

Hence, (a_0, b_0, c_0) and (a_1, a_1, c_1) is an integral pair of Heron-Pythagoras triangles. *q.e.d.*

A positive integer A is called a **congruent number** if there exists a Heron triple $(a, b, 0)$ such that the corresponding right-angled Heron triangle is of area A.

Corollary 8. *If the integer $m > 1$ is such that $3m+1 = \square$, then $A := m(m^2-1)$ and $2A$ are both congruent numbers.*

Proof. It is easy to show that if $A\cdot\square$ is a congruent number, then also A is a congruent number. It is also easy to see that for any distinct positive integers r and s, $rs(r^2-s^2)$ is a congruent number. In particular,

$$pq(p^2-q^2), \quad mn(m^2-n^2), \quad mn(m^2-n^2)\cdot\square,$$

are congruent numbers. Hence,

$$pq(p^2-q^2) = 2mn(m^2-n^2)\cdot\square$$

implies that also $2mn(m^2-n^2)\cdot\square$ is a congruent number. Let $n := 1$, $p := 2m$, and $q := m+1$. Then

$$\frac{pq(p^2-q^2)}{2mn(m^2-n^2)} = \frac{2m(m+1)\big(4m^2-(m+1)^2\big)}{2m(m^2-1)} = 3m+1.$$

So, if $3m+1 = \square$, then $pq(p^2-q^2) = 2m(m^2-1)\cdot\square$ is a congruent number. This implies that $2m(m^2-1)$ is a congruent number, and since $m(m^2-1)$ is of the form $mn(m^2-n^2)$, also $m(m^2-1)$ is a congruent number. *q.e.d.*

Notice that for all positive integers k, if $k \not\equiv 0 \pmod 3$, then $k^2 \equiv 1 \pmod 3$, *i.e.*, $k^2 = 3m + 1$ for some integer m.

As a matter of fact we would like to mention that up to similitude, there exists a unique pair of Heron-Pythagoras triangles which have the same perimeter. The unique such pair consists of the right-angled triangle with sides of lengths $(377, 135, 352)$ and the isosceles triangle with sides of lengths $(366, 366, 132)$ (see Hirakawa and Matsumura [6, Thm. 1.1]).

3.6. Integral Heron triangles related to $m = n^2 + nl + l^2$

In this section we show how one can construct with each integral solution of the Diophantine equation

$$m = n^2 + nl + l^2 \tag{4}$$

and for every $\lambda = \frac{v^2-u^2}{u^2+v^2}$ a triple of integral Heron triangles which share the area and an angle. The ideas are similar to the ones in [5], where we constructed integral right-angled triangles with integral solutions of (4) in the case when $m = \square$.

Theorem 9. *Let m, n, l be a positive, integral solution of (4) and let $k = n + l$. Further, let $\lambda = \frac{v^2-u^2}{u^2+v^2}$, where $(u, v) = 1$, and let*

$$\alpha = ku^2 + lv^2, \qquad \beta = nu^2 + kv^2, \qquad \gamma = nv^2 - lu^2, \qquad \delta = u^2 + v^2.$$

Assume that $\gamma \neq 0$. Finally, let

$$\begin{aligned}
a_1 &= nl\alpha\beta, & b_1 &= mk\gamma\delta, & c_1 &= k^2l^2u^4 + \big(l^4 - l^2n^2 + n^4\big)u^2v^2 + n^2k^2v^4,\\
a_2 &= nk\alpha\gamma, & b_2 &= ml\beta\delta, & c_2 &= l^2n^2u^4 + \big(n^4 - n^2k^2 + k^4\big)u^2v^2 + k^2l^2v^4,\\
a_3 &= lk\beta\gamma, & b_3 &= mn\alpha\delta, & c_3 &= n^2k^2u^4 + \big(k^4 - k^2l^2 + l^4\big)u^2v^2 + l^2n^2v^4.
\end{aligned}$$

Then (a_1, b_1, λ), (a_2, b_2, λ), (a_3, b_3, λ) are Heron triples and (a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3) are the corresponding integral Heron triangles which share the area and the angle opposite the side c_i.

Proof. To show that (a_i, b_i, λ) is a Heron triple with corresponding Heron triangle (a_i, b_i, c_i), we have to show that for each $i \in \{1, 2, 3\}$, $c_i^2 = a_i^2 - 2\lambda a_i b_i + b_i^2$. This can be easily checked by using the equations

$$m^2 - 2mk^2 + k^4 = l^2n^2, \qquad m^2 - 2ml^2 + l^4 = n^2k^2, \qquad m^2 - 2mn^2 + n^4 = k^2l^2.$$

For $i \in \{1, 2, 3\}$, the area of the Heron triangle (a_i, b_i, c_i) is

$$A = \frac{uv}{u^2+v^2}\, a_i b_i = uv \cdot klmn \cdot \alpha\beta\gamma.$$

In particular, the area A does not depend on i. *q.e.d.*

As a matter of fact we would like to mention that, in contrast to the case studied in [5], the Heron triangles (a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3) are not necessarily pairwise distinct. For example, for $u = 1$, $v = 2$, $l = 1$, $n = 2$, we obtain $a_2 = a_3 = 294$, $b_2 = b_3 = 490$, and $c_2 = c_3 = 392$. However, with each integral solution of the Diophantine equation (4) and for every λ, we obtain at least two different integral Heron triangles (see Corollary 17). Moreover, the following proposition tells exactly when we actually have three pairwise distinct Heron triangles: It turns out that for each given solution n, l of (4) at most three values of $\frac{u}{v}$ do *not* lead to a triple of different triangles.

Proposition 10. *The Heron triangles (a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3) in Theorem 9 are pairwise distinct if and only if*

1. $\frac{u}{v} < \sqrt{\frac{n}{l}}$ *and* $\frac{u}{v} \notin \left\{\sqrt{\frac{n^2-l^2}{k^2-n^2}}, \frac{l}{n}, \frac{n}{k}\right\}$, *or*
2. $\frac{u}{v} > \sqrt{\frac{n}{l}}$ *and* $\frac{u}{v} \notin \left\{\sqrt{\frac{k^2-l^2}{l^2-n^2}}, \frac{l}{n}, \frac{k}{l}\right\}$

Proof. First observe, that two triangles are congruent if and only if they have the same area, the same perimeter and an angle in common: To see this, recall from elementary geometry that the perimeter $p = 2|CP|$ together with the angle θ define the excircle e_c (see Fig. 1). On the other hand, the area is given by $A = \frac{p}{2} r_i$, where r_i is the radius of the incircle i. Hence the incircle is also determined. Therefore, the side c of such a triangle is one of the two common inner tangents of i and e_c.

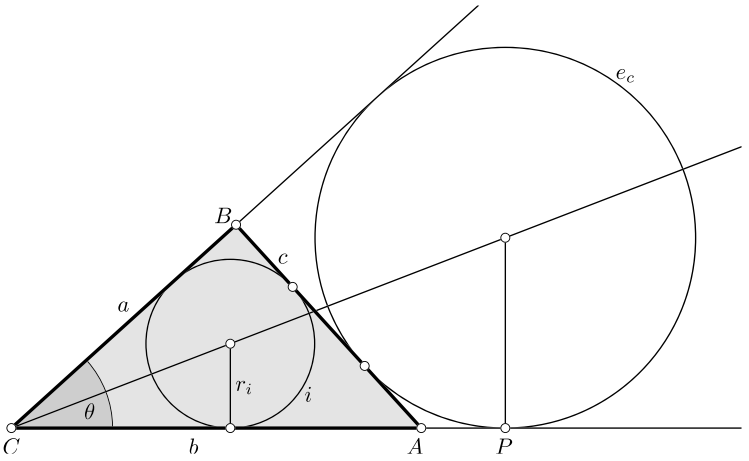

Fig. 1. Triangle given by angle θ, perimeter $p = 2|CP|$ and area $A = \frac{p}{2} r_i$.

This elementary observation allows now to conclude that two of the triangles (a_i, b_i, c_i) are different if and only if they have different perimeter. Suppose first, that $\gamma > 0$, *i.e.*, $\frac{u}{v} < \sqrt{\frac{n}{l}}$. In this case, the perimeters of the triangles are $p_i = a_i + b_i + c_i$ and a short computation shows that

$$p_1 \neq p_2 \iff u^2(k^2 - n^2) \neq v^2(n^2 - l^2), \quad p_2 \neq p_3 \iff lv \neq nu,$$
$$p_3 \neq p_1 \iff ku \neq nv.$$

If, on the other hand, $\gamma < 0$, *i.e.*, $\frac{u}{v} > \sqrt{\frac{n}{l}}$, the perimeters are

$$p_1 = a_1 - b_1 + c_1, \quad p_2 = -a_2 + b_2 + c_2, \quad p_3 = -a_3 + b_3 + c_3.$$

Similarly as above, one finds that

$$p_1 \neq p_2 \iff lu \neq kv, \quad p_2 \neq p_3 \iff nu \neq lv,$$
$$p_3 \neq p_1 \iff u^2(l^2 - n^2) \neq v^2(k^2 - l^2). \quad \textit{q.e.d.}$$

The phenomenon that, for a given angle θ of θ-triangles, finitely many exceptional values for the crucial parameter exist can also be observed in other contexts (see, for example, Lalín and Ma [7, Theorem 1 & 2, and Sec. 4]).

4. Heronian elliptic curves

It is well known that the rational points on an elliptic curve form an abelian group. Moreover, by Mordell's Theorem, this group is finitely generated (see, for example, Mordell [9, Ch. 16]). Therefore, by the *Fundamental Theorem of Finitely Generated Abelian Groups*, the group of rational points on an elliptic curve is isomorphic to some group of the form

$$\underbrace{\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}}_{\text{torsion group}} \times \mathbb{Z}^r,$$

where $n_1, \ldots, n_k$ are positive integers with $n_i \mid n_{i+1}$, and r is a non-negative integer. The group $\mathbb{Z}/\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}/\mathbb{Z}_{n_k}$, which is generated by rational points of finite order, is the so-called **torsion group**, and r is called the **rank** of the curve. Surprisingly, there are just a few possible types of groups for the torsion group of an elliptic curve. More precisely, by Mazur's Theorem (see Mazur [8]), the torsion group of an elliptic curve is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/m\mathbb{Z} \quad \text{for } m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{for } n \in \{1, 2, 3, 4\}.$$

4.1. Elliptic curves related to Heron-triangles

In Goins and Maddox [3, Thm. 2.1] it is shown that a positive integer A can be expressed as the area of a triangle with rational sides if and only if for some non-zero rational $\tau = \frac{u}{v}$ the elliptic curve

$$E_{\tau,A}: \quad y^2 = x(x - A\tau)(x + A\tau^{-1})$$

has a rational point (x, y) with $y \neq 0$.

In particular, A is a congruent number if and only if the elliptic curve $y^2 = x^3 - A^2x$ has a rational point (x, y) with $y \neq 0$.

In our setting we have $\lambda = \frac{v^2-u^2}{u^2+v^2}$, $\bar{\lambda} = \frac{2uv}{u^2+v^2}$, and

$$Q = \frac{2A}{\bar{\lambda}} = \frac{u^2 + v^2}{uv}\, A.$$

With respect to this terminology, the elliptic curve $E_{\tau,A}$ becomes

$$E_{u,v,A}: \quad y^2 = x^3 + \frac{v^2 - u^2}{uv} Ax^2 - A^2x\,.$$

This curve can also be written with λ and Q as

$$E_{\lambda,Q,A}: \quad y^2 = x^3 + \lambda Q x^2 - A^2 x\,,$$

which is called **Heronian elliptic curve**.

So, we obtain the following

Fact 11. *There exists a Heron triple (a, b, λ) such that the corresponding Heron triangle is of area A, if and only if the Heronian elliptic curve $E_{\lambda,Q,A}$ has a rational point (x, y) with $y \neq 0$.*

The correspondence between Heron triangles (a, b, c) with $\cos(\theta) = \lambda$ and area A and rational points (x, y) with $x, y \neq 0$ on the Heronian elliptic curve $E_{\lambda,Q,A}$ is given by the following functions:

$$\Psi_{\lambda,Q,A}\big((a, b, c)\big) \mapsto \left(\frac{(a + c)^2 - b^2}{4},\ a \cdot \frac{(a + c)^2 - b^2}{4}\right)$$

$$\Psi^{-1}_{\lambda,Q,A}\big((x, y)\big) \mapsto \left(\frac{y}{x},\ \frac{Qx}{y},\ \frac{x^2 + A^2}{y}\right)$$

4.2. Fermat's algorithm revisited

In order to state the next result, we first introduce the function which corresponds to the generalized Fermat Algorithm 4:

$$\Phi_{\lambda,Q,A}\big((a,b,c)\big) \mapsto \left(\frac{|a^2-b^2|}{2c},\ \frac{2abc}{|a^2-b^2|},\ \frac{c^4+16A^2}{2c|a^2-b^2|}\right)$$

Let (a,b,c) be a right-angled Heron triangle of area A. Further, let $(x_1,y_1) := \Psi_{0,Q,A}\big((a,b,c)\big)$, and let $(x_2,y_2) := 2*(x_1,y_1)$, *i.e.*, $(x_2,y_2) = (x_1,y_1)+(x_1,y_1)$ on the elliptic curve. Finally, let

$$(x_2',y_2') := \Psi_{0,Q,A} \circ \Phi_{0,Q,A}\big((a,b,c)\big).$$

In [4, Lem. 5] it is shown that $(x_2,y_2) = (x_2',-y_2')$. In other words, the two points $(x_2,y_2) = 2*(x_1,y_1)$ and (x_2',y_2') just differ in the sign of their y-coordinate.

Now, by the same arguments as in the proof of [4, Lem. 5], by a simple calculation, one can show that this result also holds for $\lambda \neq 0$.

Fact 12. *Let (a,b,λ) be a Heron triple with $a \neq b$ and with corresponding Heron triangle (a,b,c) of area A. Further, let $(x_1,y_1) := \Psi_{\lambda,Q,A}\big((a,b,c)\big)$, let $(x_2,y_2) := 2*(x_1,y_1)$, and let $(x_2',y_2') := \Psi_{\lambda,Q,A} \circ \Phi_{\lambda,Q,A}\big((a,b,c)\big)$. Then*

$$(x_2,y_2) = (x_2',-y_2')\,.$$

So, the generalized Fermat Algorithm 4 is essentially doubling points on the curve $E_{\lambda,Q,A}$.

As an immediate consequence we obtain the following

Corollary 13. *Let (a,b,λ) be a Heron triple with corresponding Heron triangle (a,b,c) of area A. Then, up to the sign of their y-coordinate, the two points*

$$2*\Psi_{\lambda,Q,A}\big((a,b,c)\big) \qquad \text{and} \qquad \left(\frac{c^2}{4},\ \frac{c(a^2-b^2)}{8}\right)$$

are equal.

4.3. On the torsion group of Heronian elliptic curves

We first prove the following

Lemma 14. *Let A be a positive integer and let $\lambda = \frac{v^2-u^2}{u^2+v^2}$ for some integers u,v with $(u,v)=1$. Then $E_{\lambda,Q,A}$ contains a point of order 4 if and only if there exists an isosceles Heron triangle (a,a,c) with $\cos(\theta)=\lambda$ and area A.*

Proof. ($\Rightarrow$) Let (a,a,c) be an isosceles Heron triangle with $\cos(\theta)=\lambda$ and area A, and let (x_0,y_0) be the corresponding rational point on the curve $E_{\lambda,Q,A}$. Then, by Corollary 13,

$$2*(x_0,y_0)=2*\Psi_{\lambda,Q,A}\big((a,a,c)\big)=\left(\frac{c^2}{4},\ \frac{c(a^2-a^2)}{8}\right)=\Big(\frac{c^2}{4},\ 0\Big).$$

Thus, the point (x_0,y_0) is of order 4.

($\Leftarrow$) Let (x_0,y_0) be a rational point on $E_{\lambda,Q,A}$ of order 4 and let (a,b,c) be the corresponding Heron triangle with $\cos(\theta)=\lambda$ and area A. Further, let $(x_1,y_1):=2*(x_0,y_0)$. Then, since (x_0,y_0) is of order 4, $y_1=0$, and since

$$(x_1,0)=2*\Psi_{\lambda,Q,A}\big((a,b,c)\big)=\left(\frac{c^2}{4},\ \frac{c(a^2-b^2)}{8}\right)=\Big(\frac{c^2}{4},\ 0\Big),$$

we have $a=b$. *q.e.d.*

The following theorem was first proved by Goins and Maddox (see [3, Proposition 3.3]).

Theorem 15. *Let A be a positive integer and let $\lambda=\frac{v^2-u^2}{u^2+v^2}$ for some integers u,v with $(u,v)=1$. Then, for the torsion group $T_{\lambda,Q,A}$ of the Heronian elliptic curve $E_{\lambda,Q,A}$, we have*

$$T_{\lambda,Q,A}\cong\begin{cases}\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} & \text{if there exists an isosceles Heron triangle } (a,a,c)\\ & \text{with } \cos(\theta)=\lambda \text{ and area } A,\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & \text{otherwise.}\end{cases}$$

Proof. For $\tau:=\frac{u}{v}$, the three points $(A\tau,0)$, $(-A\tau^{-1},0)$, and $(0,0)$ are on the curve $E_{\lambda,Q,A}$ and have all order 2, and since $(A\tau,0)+(-A\tau^{-1},0)=(0,0)$, $T_{\lambda,Q,A}$ always contains $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ as a subgroup. We consider first the following case:

u and v are both odd: In this case, we can just follow the proof of [4, Thm. 1]. First notice that since $u^2+v^2\neq\square$, by Theorem 6, there is no isosceles Heron triangle (a,a,c) with corresponding Heron triple (a,a,λ). Let (x_0,y_0) be a rational point on the curve $E_{\lambda,Q,A}$ with $y_0\neq 0$ and let $(a_0,b_0,c_0):=\Psi^{-1}_{\lambda,Q,A}\big((x_0,y_0)\big)$. Since $a_0\neq b_0$, by Fermat's Algorithm 4 we obtain infinitely many pairwise distinct Heron triangle (a_n,b_n,c_n) of the same area A, and by Fact 12, the corresponding points $2^n*(x_0,y_0)$ are also pairwise distinct, which shows that the order of (x_0,y_0) is infinite.

If exactly one of u and v is odd (*i.e.*, u^2+v^2 is odd), then we proceed as follows.

First assume that there exists an isosceles Heron triangle (a,a,c) with $\cos(\theta)=\lambda$ and area A, and let (x_0,y_0) be the corresponding rational point on the curve $E_{\lambda,Q,A}$. Then, by Lemma 14, the point (x_0,y_0) is of order 4, which implies that the torsion group $T_{\lambda,Q,A}$ contains $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ as a subgroup. By Mazur's Theorem, in order to show that $T_{\lambda,Q,A}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, it is enough to show that $E_{\lambda,Q,A}$ does not have a point

of order 8. For this, assume towards a contradiction that the rational point (x_0, y_0) on $E_{\lambda,Q,A}$ is of order 8. Let

$$(a_0, b_0, c_0) := \Psi^{-1}_{\lambda,Q,A}\big((x_0, y_0)\big)$$

be the corresponding Heron triangle. Without loss of generality, we may assume that a_0, b_0, c_0 are positive integers. Furthermore, let

$$(a_1, b_1, c_1) := \Phi_{\lambda,Q,A}\big((a_0, b_0, c_0)\big) \qquad \text{and} \qquad (x_2, y_2) := \left(\frac{c_1^2}{4},\ \frac{c_1(a_1^2 - b_1^2)}{8}\right).$$

Then, by Corollary 13, up to the sign of their y-coordinate, the two points (x_2, y_2) and $4 * (x_0, y_0)$ are equal. Since (x_2, y_2) is of order 2, we have $y_2 = 0$, *i.e.*,

$$\frac{c_1(a_1^2 - b_1^2)}{8} = 0$$

which implies $a_1 = b_1$. Now,

$$a_1 = \frac{|a_0^2 - b_0^2|}{2c_0} \qquad \text{and} \qquad b_1 = \frac{2a_0b_0c_0}{|a_0^2 - b_0^2|},$$

and thus, $a_1 = b_1$ implies that

$$(a_0^2 - b_0^2)^2 = (2c_0)^2 \cdot a_0b_0, \tag{5}$$

and therefore we have $a_0b_0 = \square$. For $d := \gcd(a_0, b_0)$, we have $a_0 = d\alpha^2$ and $b_0 = d\beta^2$ for some integers α and β. Since

$$c_0^2 = d^2\big(\alpha^4 - 2\lambda\alpha^2\beta^2 + \beta^4\big),$$

equation (5) becomes

$$d^4\big(\alpha^8 - 2\alpha^4\beta^4 + \beta^8\big) = 4d^4\alpha^2\beta^2\big(\alpha^4 - 2\lambda\alpha^2\beta^2 + \beta^4\big),$$

and after dividing through d^4, we obtain

$$(\alpha^2 - \beta^2)^4 = 8\alpha^4\beta^4 \cdot (1 - \lambda).$$

Now, since $1 - \lambda = \frac{2u^2}{u^2+v^2}$, this leads to

$$(\alpha^2 - \beta^2)^4 = (2\alpha\beta)^4 \cdot \frac{u^2}{u^2 + v^2}$$

and consequently we have

$$\left(\frac{\alpha^2-\beta^2}{2\alpha\beta}\right)^4 = \frac{u^2}{u^2+v^2}. \tag{6}$$

Since $(u,v)=1$, equation (6) implies that u^2 as well as u^2+v^2 is a forth power, say $u^2=\nu^4$ and $u^2+v^2=\eta^4$. So, we have $\nu^4+v^2=\eta^4$, or equivalently, $\eta^4-\nu^4=v^2$, which does not have a solution in positive integers. Hence, the point (x_0,y_0) on $E_{\lambda,Q,A}$ is not a point of order 8.

Finally, assume that there exists no isosceles Heron triangle (a,a,c) with $\cos(\theta)=\lambda$ and area A. Then, by Lemma 14, $E_{\lambda,Q,A}$ does not have a point of order 4. So, by Mazur's Theorem, in order to show that $T_{\lambda,Q,A}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, it is enough to show that $E_{\lambda,Q,A}$ does not have a point of order 3, or equivalently, we have to show that $E_{\lambda,Q,A}$ does not have a rational point of inflection. Assume towards a contradiction that the rational point (x_0,y_0) on $E_{\lambda,Q,A}$ is of order 3 and let $(x_1,y_1):=2*(x_0,y_0)$. Then $x_1=x_0$ and $y_1=-y_0$. Let

$$(a_0,b_0,c_0) := \Psi^{-1}_{\lambda,Q,A}\big((x_0,y_0)\big)$$

be the corresponding Heron triangle. Without loss of generality, we may assume that a_0,b_0,c_0 are positive integers, and that c_0 is even and both a_0 and b_0 are odd — otherwise, we can apply Fermat's Algorithm 4 and can proceed as in the case when u and v are both odd. By Corollary 13,

$$\frac{c_0^2}{4} \;=\; x_1 \;=\; x_0 = \frac{(a_0+c_0)^2-b_0^2}{4}. \tag{7}$$

Equation (7) implies that $a_0^2+2a_0c_0-b_0^2=0$ and therefore, for the positive integer a_0 we have

$$a_0 \;=\; \sqrt{c_0^2+b_0^2}-c_0.$$

Thus, we have $c_0^2+b_0^2=(a_0+c_0)^2$, which implies that (c_0,b_0,a_0+c_0) is a Pythagorean triple, and hence, we find some positive integers k,m,n with $(m,n)=1$, such that $a_0+c_0=k(m^2+n^2)$, $b_0=k\cdot(m^2-n^2)$, and $c_0=k\cdot 2mn$ (recall that c_0 is even). So, on the one hand we have $a_0=k(m-n)^2$, and on the other hand we have $c_0^2=a_0^2-2\lambda a_0b_0+b_0^2$. Hence,

$$0=a_0^2-2\lambda a_0b_0+b_0^2-c_0^2=\frac{4m^3(m-2n)u^2+4n^3(-2m+n)v^2}{u^2+v^2}$$

which implies that

$$m^3(m-2n)u^2=n^3(2m-n)v^2.$$

Thus,

$$u = \pm v \cdot \frac{n}{m} \cdot \sqrt{\frac{n(2m-n)}{m(m-2n)}}\,,$$

and since u is an integer, this implies that both $n(2m-n)$ and $m(m-2n)$ are squares, say $n(2m-n) = p^2$ and $m(m-2n) = q^2$. This gives us

$$m = \pm \sqrt{\frac{2p^2 + q^2 - 2\sqrt{p^4 + p^2q^2 + q^4}}{3}}.$$

Now, since m is an integer, this implies that

$$p^4 + p^2q^2 + q^4 = \square\,,$$

which is not solvable in positive integers p and q (see, for example, Mordell [9, p. 19]). Hence, the point (x_0, y_0) on $E_{\lambda,Q,A}$ is a not a point of order 3. *q.e.d.*

Remark 1. The proof of Theorem 15 given by Goins and Maddox relies on Mazur's Theorem and uses twice a symbolic computer package (e.g., MAGMA) in order to show that Heronian elliptic curves never have rational points of order 3 or of order 8. On the other hand, in the proof given above, we do not need computer assistance, and in the case when u and v are both odd, we do not even use Mazur's Theorem. Moreover, it might be that there is a proof of Theorem 15 which does not rely on Mazur's Theorem even in the case when exactly one of u and v is odd.

As an immediate consequence of Theorem 15 we get the following two results:

Corollary 16. *If (a_0, b_0, c_0) is a Heron triangle with $a_0 \neq b_0$, then Fermat's Algorithm 4 generates an infinite sequence of pairwise distinct Heron triangles with the same area A and the same angle θ.*

Proof. If the sequence of Heron triangles is finite, then (a_0, b_0, c_0) must be an isosceles triangle with $a_0 = b_0$, which contradicts our assumption. *q.e.d.*

Corollary 17. *Among the three Heron triangles we obtained in Theorem 9 from a positive, integral solution of (4), at least two are distinct.*

Proof. The three Heron triangles correspond to three rational points with non-zero y-coordinate on the curve $E_{\lambda,Q,A}$. If we obtain just one point, then a continuity argument would give us a rational point of inflection on the curve $E_{\lambda,Q,A}$, which is impossible. *q.e.d.*

4.4. A family of Heronian elliptic curves of rank at least 2

In this section we show how one can construct with integral solutions of the Diophantine equation

$$m = n^2 + nl + l^2 \tag{8}$$

Heronian elliptic curves $E_{\lambda,Q,A}$ of rank at least 2. Notice that by Mazur's Theorem, in order to show that an elliptic curve has positive rank, it is enough to find 17 generically different rational points on the curve (see, for example, Lalín and Ma [7, Lem. 5]). However, to show that the rank of an elliptic curve is at least 2, we have to proceed differently.

The construction we use is the same as in the proof of [5, Thm. 3], where we constructed congruent number elliptic curves $E_{0,0,A}$ of rank at least 2.

Proposition 18. *Let m, n, l be a positive, integral solution of (8) and let $k = n+l$. Further, let $\lambda = \frac{v^2-u^2}{u^2+v^2}$, where $(u, v) = 1$, let*

$$\alpha = ku^2 + lv^2, \qquad \beta = nu^2 + kv^2, \qquad \gamma = nv^2 - lu^2,$$

and let

$$A = uv \cdot klmn \cdot \alpha\beta\gamma.$$

Finally, for $i \in \{1, 2, 3\}$, let (a_i, b_i, c_i) be the three integral Heron triangles we obtain from Theorem 9.

Then, under the assumption that $A \neq 0$ and that the following twelve values

$$\frac{(a_i \pm c_i)^2 - b_i^2}{4} \qquad \text{and} \qquad \frac{(b_i \pm c_i)^2 - a_i^2}{4}$$

are pairwise distinct modulo squares, the rank of the Heronian elliptic curve $E_{\lambda,Q,A}$ is at least 2.

Proof. As a consequence of a well-known result, which can be found in Silverman and Tate [10, Chapter III.6.], a sufficient condition for an elliptic curve E to have rank at least 2 is that we find at least 9 rational points (x_j, y_j) $(1 \leq j \leq 9)$ on E, such that for any distinct $j, j' \in \{1, \ldots, 12\}$,

$$x_j \neq x_{j'} \cdot \square\,.$$

Now, since the twelve values given above are x-coordinates of rational points on the Heronian elliptic curve $E_{\lambda,Q,A}$ (see [5, Thm. 3]), the rank of $E_{\lambda,Q,A}$ is at least 2. *q.e.d.*

As a matter of fact we would like to mention that in all cases we considered, in order to satisfy the assumption in Proposition 18, it is enough that the three Heron triangles (a_i, b_i, c_i) obtain from Theorem 9 are pairwise distinct.

5. Odds and ends

1. Theorem 4 was just formulated for u and v both odd, which implies that $c_n = \frac{r}{2^k \cdot s}$, where r and s are both odd and $k \geq 0$, and includes the case when $u = v = 1$ (*i.e.*, $\lambda = 0$). If either u or v is even, then c_n may be of the form $2^k \cdot \frac{r}{s}$ where r and s are both odd and $k > 0$. Moreover, for $u = 32$, $v = 9$, $a_0 = 663$, $b_0 = 575$, $c_0 = 1192 = 2^3 \cdot 149$, we get $c_1 = 2^4 \cdot \frac{531448501}{1014541}$, and in general, for all $n \geq 1$, we have $c_n = 2^4 \cdot \frac{r}{s}$ for some odd integers r and s.

2. The three points on the curve $E_{\lambda,Q,A}$ which correspond to the three Heron triangles we obtained in Theorem 9 from a positive, integral solution of (4), are the intersection points of a straight line with the curve $E_{\lambda,Q,A}$ (see [5] for a similar result in the case when $\lambda = 0$). In particular, when two of the three points are equal, the straight line is a tangent to the curve $E_{\lambda,Q,A}$.

3. As in the case when $\lambda = 0$ (see [5, Sec. 3]), it seems that the Heronian elliptic curves $E_{\lambda,Q,A}$ obtained from Proposition 18 are good candidates for having high rank. For example, the following parameters lead to Heronian elliptic curves of rank 5:

u	v	l	n	λQ	A
1	5	1	8	198863240832	41429841840
1	5	1	10	748641009600	155966877000
1	6	1	9	1571587863300	269415062280
1	6	1	10	2927534679300	501863087880
1	6	2	9	7726084373700	1324471606920
2	5	3	8	3693500328672	1758809680320
2	7	1	12	44530908645600	13854060467520
2	9	1	14	690932437064100	161516673599400
2	9	6	13	29713050037586916	6945907800994344
3	5	12	23	45580866675926400	42732062508681000
4	9	2	9	323225487971100	179017193337840
5	12	1	3	1200153466512	605119394880
5	12	8	9	146025707565431232	73626407175847680

However, with this method we did not find any Heronian elliptic curve of rank 6 or higher (for a similar phenomenon see [5, Sec. 3]).

Acknowledgment

We would like to thank the referee for his or her thorough review and highly appreciate the comments and suggestions, which helped to improve the quality of the article.

References

[1] Pierre de Fermat, Fermat's Diophanti Alex. Arith., 1670, in: Ministère de l'instruction publique (Ed.), Œuvres III, Gauthier-Villars et fils, Paris, 1896, pp. 254–256.
[2] Edray Herber Goins, The ubiquity of elliptic curves, Not. Am. Math. Soc. 66 (2019) 169–174.
[3] Edray Herber Goins, Maddox Davin, Heron triangles via elliptic curves, Rocky Mt. J. Math. 36 (2006) 1511–1526.
[4] Lorenz Halbeisen, Norbert Hungerbühler, A theorem of Fermat on congruent number curves, Hardy-Ramanujan J. 41 (2018) 15–21.
[5] Lorenz Halbeisen, Norbert Hungerbühler, Congruent number elliptic curves related to integral solutions of $x^2 + xy + y^2 = m^2$, J. Integer Seq. 22 (3) (2019) 19.3.1.
[6] Yoshinosuke Hirakawa, Hideki Matsumura, A unique pair of triangles, J. Number Theory 194 (2019) 297–302.
[7] Matilde Lalín, Xinchun Ma, θ-triangle and ω-parallelogram pairs with common area and common perimeter, J. Number Theory 202 (2019) 1–26.
[8] Barry Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (1978) 129–162.
[9] Louis Joel Mordell, Diophantine Equations, Academic Press, London–New York, 1969.
[10] Joseph H. Silverman, John Tate, Rational Points on Elliptic Curves, 2nd edition, Springer-Verlag, New York, 2015.
[11] Ernst Sós, Zwei diophantische Gleichungen, Z. Math. Naturwiss. Unterr. 37 (1906) 186–190.