UiO : Department of Mathematics
University of Oslo

Heron triangles and van Luijks Theorem

Martin Bråtelund

Master's Thesis, Spring 2018

This master's thesis is submitted under the master's programme *Lektorprogrammet*, with programme option *Mathematics*, at the Department of Mathematics, University of Oslo. The scope of the thesis is 30 credits.

The front page depicts a section of the root system of the exceptional Lie group E_8, projected into the plane. Lie groups were invented by the Norwegian mathematician Sophus Lie (1842–1899) to express symmetries in differential equations and today they play a central role in various parts of mathematics.

Abstract

A Heron triangle is a triangle with integer sides and integer area. A rational triangle is a triangle with rational sides and area. We will set out to prove van Luijks Theorem, that there exist infinitely many non-similar rational triangles with the same area and perimeter. Unlike the original proof, we will not use elliptic surfaces, using instead only elliptic curves. Hopefully making the proof a bit more accessible to readers without a background in algebraic geometry. We will also prove, as a corollary, that there exist arbitrarily many Heron triangles having the same area and perimeter, and construct a method for generating such triangles. This thesis will also provide a fix to a minor flaw in the original proof of the theorem.

Contents

1 Introduction

In this thesis, we will have a look at the main Theorem in van Luijks paper [8]. We will attempt to recreate the proof, only using elliptic curves, rather than taking the step up to elliptic surfaces, as is the case in the original paper. Hopefully, this will make the proof somewhat more accessible to the average reader. The main Theorem will be formally stated later in the thesis. For now, let us state (and later prove) an important corollary following directly from van Luijks Theorem. It involves Heron triangles, which are triangles with integer sides and integer area, and goes as follows:

Corollary 1.1. *For every positive integer N there exists an infinite family of N-tuples of Heron triangles with the same area and perimeter such that no two triangles will be similar regardless of whether the triangles are in the same N-tuple or not.*

1.1 Historical context

Heron triangles are named after Heron of Alexandria, the man who is credited with the proof of Herons formula. A formula which expresses the area A of a triangle using the sides a, b and c

$$A^2 = \frac{p}{2}(\frac{p}{2} - a)(\frac{p}{2} - b)(\frac{p}{2} - c). \tag{1}$$

Where $p = a + b + c$ is the perimeter of the triangle.

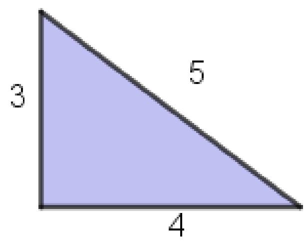

Figure 1: The (3,4,5) triangle has integer sides and integer area $A = 6$, making it a Heron triangle. This is the smallest Heron triangle, meaning no Heron triangle has a smaller area or perimeter.

Heron triangles are a field of study, both in geometry and number theory, and over time, many interesting properties of Heron triangles have been found.

It was proven early on that there exist an infinite number of non-similar Heron triangles. Proofs that there exists an infinite number of non-similar Pythagorean triangles (right-angled triangles with integer sides) date back to the days of Euclid, approximately 300 years before Heron. And it turns out that:

Theorem 1.2. *Every Pythagorean triangle is also Heron.*

Proof. All Pythagorean triangles are right-angled, so their area is given by $A = {c_1 c_2}/2$ where c_1, c_2 are the lengths of the catheti (or legs) of the triangle. Hence the only way for the area to

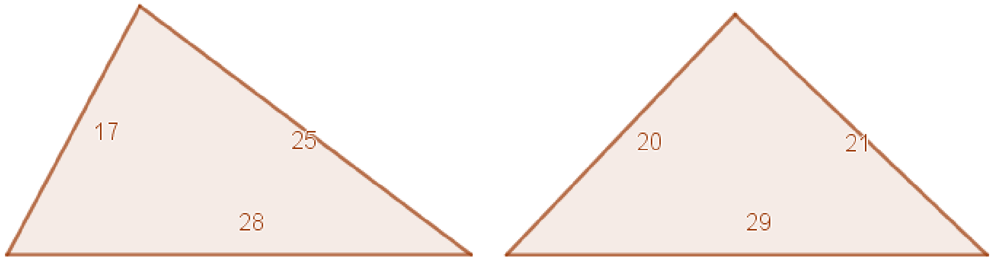

Figure 2: The triangles (17,25,28) and (20,21,29) both have area $A = 210$ and perimeter $p = 70$, making them the smallest pair of Heron triangles having the same area and perimeter.

not be an integer is if both the catheti have odd length.

So let us assume that c_1, c_2 are odd, in other words that $c_1 \equiv 1 \pmod 4$ or $c_1 \equiv 3 \pmod 4$, and same for c_2. Either way $c_1^2 \equiv 1 \pmod 4$, and $c_2^2 \equiv 1 \pmod 4$. It follows that the hypotenuse h must be such that $h^2 = c_1^2 + c_2^2 \equiv 2 \pmod 4$, but if $h^2 \equiv 2 \pmod 4$ it can not be a square number (square numbers are congruent to either 1 or 0 (mod 4)), so h is not an integer, so the triangle (c_1, c_2, h) is not Pythagorean.

From this it follows that for any Pythagorean triangle, at least one of the catheti must have even length, making the area an integer. Thus any Pythagorean triangle is also Heron. □

There also exist an infinite number of Heron triangles that are not Pythagorean. In the 7th century, a parametric solution was found by Brahmagupta, who showed that every Heron triangle would have sides on the form [1]:

$$\begin{aligned} a &= n(m^2 + k^2), \\ b &= m(n^2 + k^2), \\ c &= (m + n)(mn - k^2). \end{aligned}$$

The next question (leading up to van Luijks Theorem) was on the number of Heron triangles having the same area and perimeter. For example, the triangles (17,25,28) and (20,21,29) share the same area and perimeter (see Figure 2), so pairs of Heron triangles with common area and perimeter do indeed exist. However, finding out how many such triangles there are, took a long time.

It was not until the year 2000 that Kramer and Luca [4] proved that there exist an infinite family of such pairs, having the same area and perimeter. They were, however, unable to find a triple of Heron triangles where all three have the same area and perimeter. It was left as an unanswered question, and this is where van Luijks Theorem comes in.

Before van Luijk found the solution in 2006, computer searches had provided not only triples but gone as far as finding a 9-tuple of Heron triangles, all having the same area and perimeter. But the question remained: how big an N-tuple of Heron triangles can be found? Van Luijks Theorem proved that we, for any integer N, can find an infinite family of N-tuples of Heron triangles with the same area and perimeter [Corollary 1.1]. Not only that, but the paper also provided an explicit method for generating such triangles. A method for generating N-tuples will be given later in this thesis, in section 3.3, after the necessary theory has been introduced.

1.2 Our approach

A rational triangle is a triangle with rational sides and rational area. We are looking for Heron triangles, but it turns out that it is far easier to search for rational triangles. These can always be scaled up to form a Heron triangle, so we will try to find a method for generating rational triangles with the same area and perimeter instead, and then simply scale these up to Heron triangles.

Van Luijks proof uses elliptic K3 surfaces to find these triangles. In this thesis, however, we will aim to prove the theorem without the use of elliptic surfaces and fibers, instead relying simply on elliptic curves to prove the theorem. This will hopefully make the proof somewhat more accessible to readers without a background in algebraic geometry.

The thesis will start with a brief introduction to elliptic curves, providing the reader with all the theory needed to follow the proof. Next, we will construct an elliptic curve such that the rational points on the curve correspond to rational triangles and use this to prove van Luijks Theorem. Lastly, we will compute some examples of such tuples of triangles.

2 Elliptic curves

Many of the properties of Heron triangles can be proven by using arguments that rely on little more than high school geometry and algebra. Van Luijks Theorem, however, uses elliptic curves as a means of finding Heron triangles. Given the importance of elliptic curves in the proof of van Luijks Theorem, this section will contain a short introduction to elliptic curves.

Elliptic curves can be defined in several ways. Our definition will be that an elliptic curve E is a plane, projective, non-singular curve given by the zeros of a homogeneous equation on the form

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3. \tag{2}$$

The curve being non-singular means that it has no cusps or self-intersections. Figure 3 shows an example of a singular curve, with a self-intersection at (1,0). Over some fields, we might need a more general definition, where the equation will not be as simple as equation (2), but for the fields we are working over, like $\mathbb{R}$ and $\mathbb{Q}$, all elliptic curves can be written on the form above [6, p. 45].

The affine part of this curve, where $z = 1$, will be the curve given by

$$y^2 = x^3 + ax^2 + bx + c. \tag{3}$$

This equation describing the curve is called a Weierstrass equation. This is a curve in the affine plane, but not the whole elliptic curve, as we are missing the part where $z = 0$. Substituting $z = 0$ into equation (2), we get

$$x^3 = 0.$$

This means that we are missing the point (0:1:0) on the curve. But how can we interpret this point in the affine plane?

If we take a vertical line $x = k$ for some $k \in \mathbb{R}$, this line will correspond to the line given by the homogeneous equation $x = kz$ in the projective plane. However, we know that this line will intersect the elliptic curve E in the point (0:1:0) for any k. So in the affine plane, we are missing a point where all vertical lines intersect. This point, which we call O, is the only point on E that is not in the affine plane $z = 1$. We think of this point as the point at infinity on the y-axis. And because it is generally easier to visualize curves in the affine plane than in the projective plane, we will throughout this thesis, consider elliptic curves to be curves is the affine plane, on the form (3), plus this point O at infinity.

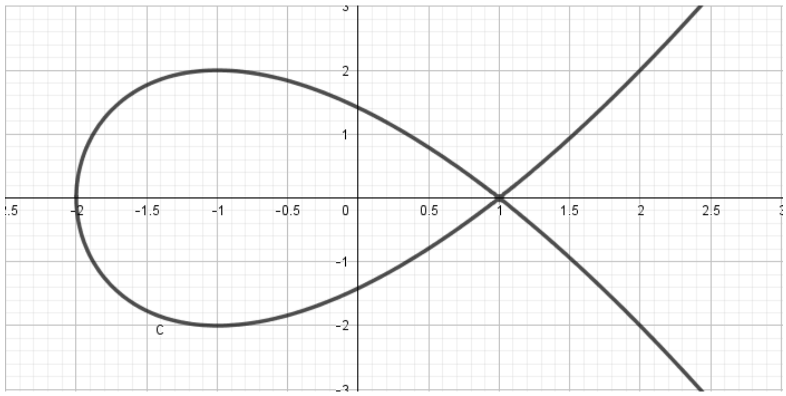

Figure 3: The curve given by $y^2 = x^3 - 3x + 2$. Despite the equation being on the form (3), it is not an elliptic curve. This is because it has discriminant $\Delta = 0$, meaning that it is singular. In this case, the singular point is a self intersection at (1,0).

2.1 Group structure of elliptic curves

One nice property of elliptic curves is that under the right operation their points will form a group with identity O. The group operation $+$ is defined as follows (use Figure 4 for reference):

Given two points P and Q on the elliptic curve

$$E = \{(x, y)|y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}. \tag{4}$$

Take l to be the straight line through these two points. This line will intersect the curve E at a third point R (this is not obvious, but will be proven as Lemma 2.4). Next, take a vertical line through R, this line will intersect E at a new point $-R$. We define $P + Q$ to be the point $-R$. In the event where one wishes to add a point to itself, take l to be the tangent line of E through P.

Theorem 2.1. *(E,+) is an abelian group with identity O.*

Proof. One can easily check that the operation is indeed commutative, that O is the identity and that the group is closed under $+$. Also if P has coordinates (x, y) then the inverse, $-P$, will have coordinates $(x, -y)$, and because of symmetry around the x-axis, this point will also lie on E. Hence, every element will have an inverse. The only remaining group axiom is associativity. It is not obvious that $+$ is associative, but it turns out that it is. Proof of this can be found in

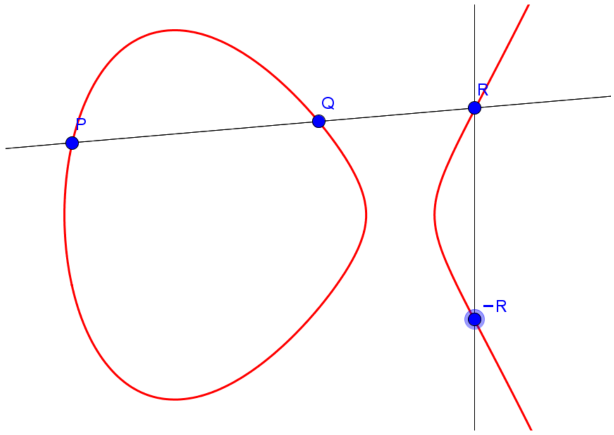

Figure 4: Illustrating the group operation on an elliptic curve. The sum of P and Q will be the point $-R$.

Silvermans book [6, p. 53]. □

An explicit formula for the sum of two points can easily be derived, using regular algebra. It can also be found in Silvermans book [6, p. 54]. The formula is as follows: given $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, the coordinates of $-R = P + Q$, will be:

$$-R = (x_{-R}, y_{-R}),$$

where

$$\begin{aligned} x_{-R} &= \lambda^2 - x_P - x_Q - a, \\ y_{-R} &= -\lambda(x_{-R} - x_P) - y_P. \end{aligned} \tag{5}$$

Where λ is the slope of the line l, given by

$$\lambda = \begin{cases} \dfrac{y_P - y_Q}{x_P - x_Q} & \text{if } x_P \neq x_Q, \\ \\ \dfrac{3x_P{}^2 + 2ax_p + b}{2y_P} & \text{if } P = Q. \end{cases}$$

There is one more possibility. One can have $x_P = x_Q$ but $P \neq Q$, in this case, you will not have a slope, because the line is vertical. Then you have $Q = -P$, so $P + Q = P - P = O$.

Having a look at these formulas, we observe that the sum of two points with rational coordinates will itself have rational coordinates. Thus $E(\mathbb{Q}) = \{(x, y) \in E | x, y \in \mathbb{Q}\}$ forms a subgroup of E. Not only that, but we also have the following theorem:

Theorem 2.2 (Mordell-Weil Theorem). *The group $E(\mathbb{Q})$ is finitely generated.*

Proof. See the original proof by Weil [5, p. 179–192], or for the general theorem over any field, see the proof in Silvermans book [6], starting on page 207. □

The Mordell–Weil Theorem dates back to 1922, and is one of the fundamental theorems on the arithmetic of elliptic curves.

2.2 Positive discriminants

Next, we want some information about the shape of the elliptic curve. The *discriminant* Δ provides us with the information we need. An elliptic curve given by the equation

$$y^2 = x^3 + ax^2 + bx + c,$$

will have discriminant

$$\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.$$

This is the same as the discriminant of the polynomial

$$f(x) = x^3 + ax^2 + bx + c.$$

The sign of Δ tells us much about the shape of the curve. The discriminant being zero means that the curve is singular, and thus not an elliptic curve. See Figure 3 for a curve with $\Delta = 0$. Hence all elliptic curves have $\Delta \neq 0$.

Lemma 2.3. *Let E be an elliptic curve given by an equation on the form $y^2 = x^3 + ax^2 + bx + c$, and let E have discriminant Δ. Then the following is true:*

1. *If $\Delta > 0$, then E will consist of two separate components, one bounded and one unbounded.*
2. *If $\Delta < 0$, then E will consist of one unbounded component.*

Figure 5 shows two examples of elliptic curves, one with $\Delta < 0$ and one with $\Delta > 0$.

Proof. We define

$$f(x) = x^3 + ax^2 + bx + c.$$

From the equation for E, it is clear that for every x such that $f(x) \geq 0$, there will be points on E with x as first coordinate, and vice versa. In mathematical terms:

$$f(x) \text{ is non-negative} \Leftrightarrow \text{There exists a point on } E \text{ with first coordinate } x.$$

With this, we can move on to looking at the zeros of $f(x)$.

1. The discriminant being positive means that $f(x)$ has three distinct roots. Let us call these x_0, x_1 and x_2, and let them be such that $x_0 < x_1 < x_2$.

   Because $f(x)$ tends to $+\infty$ as x increases, $f(x)$ is positive where $x \in [x_0, x_1] \cup [x_2, \infty)$. Hence this is also the two intervals in which E lies, and as such, E must consist of two separate parts. The part lying where $x \geq x_2$ is clearly unbounded, because it has no bound in x. The part lying where $x_0 < x < x_1$ must be bounded because $f(x)$ is bounded on this interval[1].

[1] **Boundedness Theorem:** a continuous function on a closed interval is always bounded.

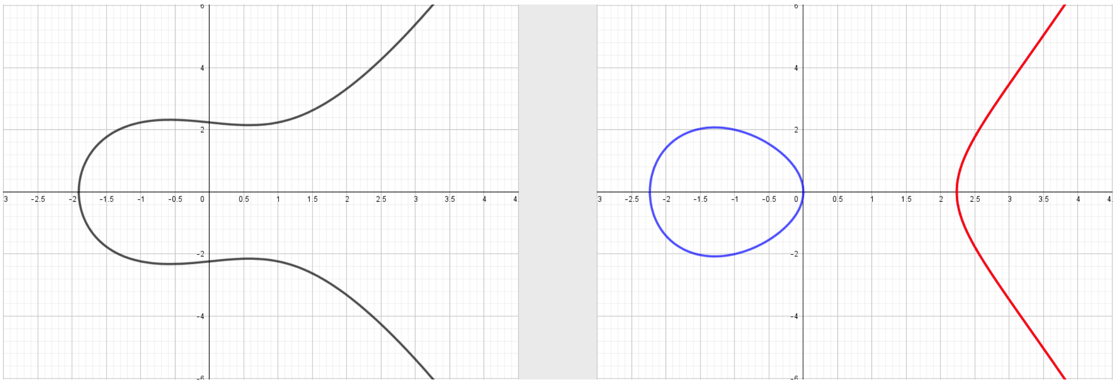

Figure 5: Two examples of elliptic curves. $\Delta = -671$ for the left one, and $\Delta = 500$ for the one to the right. The right curve consists of two parts, the bounded part in blue, and the unbounded part in red.

2. The discriminant being negative means that $f(x)$ has exactly one zero, let the zero be at $x = x_0$.

   Then $f(x)$ will be positive for all $x \geq x_0$, so this is the interval in which E lies. Because there is only one interval, E will now consist of one component. This component cannot be bounded, because it is not bounded in x.

□

When we later use elliptic curves to find Heron triangles, we will be using curves with $\Delta > 0$, so we will focus a bit more on them. As mentioned before, these curves will consist of two separate components. One will be unbounded and thus contain O, while the other one will be bounded, and form a closed curve. One of the properties we will use is that when we have a bounded part, that part of the curve will be a convex curve, that is, it will be the boundary of a convex set. No litterature stating this could be found, so it will be proven here. This can be proven in several ways, for example using calculus, by computing the double derivative of $g(x) = \sqrt{f(x)}$. We will, however, give a geometric argument. For this, we first need a lemma that, on its own, is very useful in the study of elliptic curves.

Lemma 2.4. *For every elliptic curve E, any line l will intersect E in exactly one or three points.*

Note here that a tangent line to the curve is counted as intersecting twice.

Proof. Let us first deal with the special case, when l is vertical. Let us assume that l is given by the equation $x = x_0$. First off, all vertical lines intersect E at O, thus giving us one point of intersection between E and l. If $f(x_0) \geq 0$ we get two more points of intersection, namely $(x_0, \pm\sqrt{f(x_0)})$. If $f(x) < 0$, we only have O as a point of intersection. Meaning that a vertical line does indeed intersect E exactly once or thrice.

Now, let's consider the case where l is non-vertical, and instead given by an equation on the form $y = \alpha x + \beta$. If we substitute this into equation (3) we get a third-degree equation in one variable. From calculus, we know that such an equation will have either one or three real roots, each of them corresponding to a point of intersection. Meaning that non-vertical lines also intersect E exactly once or thrice. Hence, all lines do indeed intersect an elliptic curve in exactly one or three points. □

This result is used, among other things, when defining the group operation on E. For the operation to make sense, we need to be sure that any line going through two points, also goes through a third one. This follows directly from Lemma (2.4).

Now we can move on to prove the convexity of the bounded part.

Proposition 2.5. *An elliptic curve E with $\Delta > 0$ will consist of two parts, one of these parts will be a closed curve that is bounded and convex.*

Proof. Let E be an elliptic curve with $\Delta > 0$. From Lemma (2.3) we know that E will consist of two parts, where one is bounded and one is unbounded. Let us call the bounded part E_B.

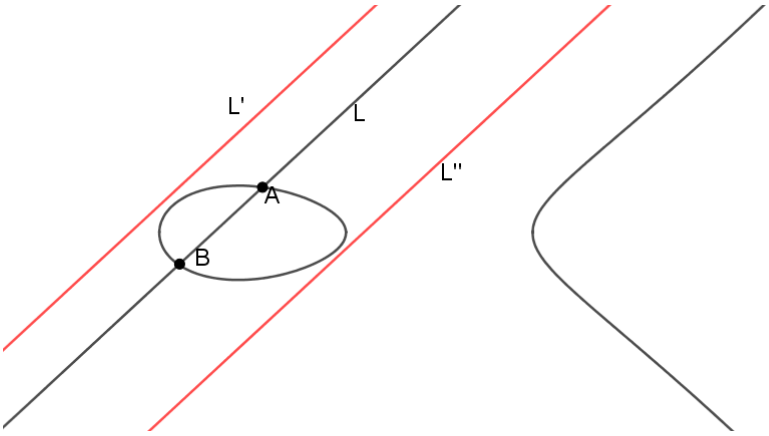

Figure 6: Illustration of the proof of Proposition 2.5, the curve is given by $y^2 = x^3 - 5x$. It is not clear from the figure that the lines will cut the unbouded part of E, but from Lemma (2.4) it follows that they will.

Next, we wish to prove that E_B is convex. Take any two points A and B on E_B, and let L be the line through these points. If we can show that L will not intersect E_B in any other points than A and B we will have shown that E_B is convex. Take two new lines L' and L'' parallel to L but not intersecting E_B, such lines will exist since E_B is bounded. From Lemma (2.4) we know that these two lines will intersect the curve, and will hence do so at the unbounded part. But because the unbounded part is connected, and L lies between L' and L'', L too must intersect the unbounded part, and because it can intersect the curve no more than three times, it will not intersect E_B more than twice. Hence E_B must be convex. □

With this, we have covered the properties of elliptic curves that we will be using in this thesis. We can now move on to the main part: van Luijks Theorem and the existence of an infinite number of Heron triangles.

3 An infinite number of Heron triangles

In this section, we will aim to prove van Luijks Theorem, as well as Corollary 1.1. We do this by first constructing an elliptic curve on which the points correspond to solutions to Herons equation. Then we develop a method for finding an infinite number of points on the curve that correspond to actual Heron triangles. With this method in place, we will see that van Luijks Theorem follows rather straightforwardly.

Proving that the method actually gives us Heron triangles will be the main part of this section. But first, let us state van Luijks Theorem, and prove Corollary 1.1.

3.1 van Luijks Theorem

In his paper [8], van Luijk proves the following Theorem:

Theorem 3.1. (van Luijks Theorem) *There exists a sequence $\{(a_n(s), b_n(s), c_n(s))\}_{n\geq 1}$ of triples of elements in $\mathbb{Q}(s)$ such that*

(1) for all $n\geq 1$ and all $s \in \mathbb{R}$ with $s > 1$ there exists a triangle $\triangle_n(s)$ with sides $a_n(s)$, $b_n(s)$ and $c_n(s)$, inradius $s-1$, perimeter $2s(s+1)$ and area $s(s^2-1)$, and

(2) for all m, $n \geq 1$ and $s_1, s_2 \in \mathbb{Q}$ with $s_1, s_2 > 1$, the rational triangles $\triangle_m(s_1)$ and $\triangle_n(s_2)$ are similar if and only if $m = n$ and $s_1 = s_2$.

This theorem tells us, among other things, that there exists an infinite number of non-similar rational triangles, with the same area and perimeter. We can use these rational triangles to produce Heron triangles, thus proving Corollary 1.1.

Corollary 1.1. *For every positive integer N there exists an infinite family of N-tuples of Heron triangles with the same area and perimeter such that no two triangles will be similar regardless of whether the triangles are in the same N-tuple or not.*

Proof. First off, take some integer s, for example $s = 3$. Then according to Theorem 3.1 there exist a sequence of rational triangles with area $s(s^2-1)$ and perimeter $2s(s+1)$. Take the first N triangles in the sequence and multiply them with the common denominator to get a collection of N Heron triangles, all having the same area and perimeter.

The same thing can be done for ($s = 4, 5, 6, ...$), each time giving a new N-tuple. Hence we get an infinite family of N-tuples of triangles with integer sides, with each family consisting of triangles with the same area and perimeter. Furthermore, because we chose integer values of s, the area is an integer, making the triangles Heron. Finally, it follows from part 2 of Theorem 3.1 that no two triangles are similar, meaning our proof is complete. □

With the proof of Corollary 1.1 in place we can now move on to the main part of this section, namely proving van Luijks Theorem. Note again that the proof we will provide, is largely based upon the original proof by van Luijk.

3.2 Constructing the curve

First, we aim to find an elliptic curve on which each point corresponds to a solution to Herons formula

$$A^2 = \frac{p}{2}(\frac{p}{2} - a)(\frac{p}{2} - b)(\frac{p}{2} - c), \tag{1}$$

where a, b and c are the sides of the triangle, and A and p are its area and perimeter, respectively. The search for rational triangles is the search for rational solutions (a, b, c, A) to this equation. Let us make some changes to make it easier to solve. First of, we set:

$$x = \frac{p}{2} - a, \quad y = \frac{p}{2} - b, \quad z = \frac{p}{2} - c. \tag{6}$$

This gives us $p = a + b + c = 2(x + y + z)$. Putting this into Herons formula, we get

$$A^2 = (x + y + z)xyz.$$

We can also use the relation $A = rp/2 = r(x + y + z)$ where r is the inradius of the triangle. This allows us to write Herons formula as

$$r^2(x + y + z) = xyz.$$

Now we are looking for rational solutions (x, y, z, r) to this equation, an infinite number of such solutions in fact. But even with this change of variables, there is no obvious way to find an infinite number of solutions[2]. If we can rewrite it to be the equation of an elliptic curve, however, we get a method for generating solutions. In order to do this, let us first set $r = \tau(x + y + z)$, so that we get the equation

$$\tau^2(x + y + z)^3 = xyz, \tag{7}$$

where $\tau = \frac{r}{(x+y+z)} = \frac{4A}{p^2}$, so for any non-degenerate triangle (x, y, z, r) we can find a τ. Hence, we have not lost any interesting solutions by making this change of variables. Let us consider τ as a fixed positive value. Then we get a family of equations in three variables, with one equation for each choice of τ. We take τ to be positive in order to keep the ratio between area and perimeter positive.

Since equation (7) is homogeneous, we can look for solutions $[x : y : z] \in \mathbb{P}^2$ instead of solutions $(x, y, z) \in \mathbb{R}^3$. This is the same as saying that two solutions where one is simply a scaling of the other are equivalent. Which is exactly what we want, because we are looking for non-similar solutions. Now, because we chose to work in the projective plane we can fix one of the coordinates. Let us try with $z = 1$, then we get

$$\tau^2(x + y + 1)^3 = xy.$$

We are now missing the solutions where $z = 0$, but these solutions correspond to degenerate triangles with zero area, and are not the solutions we were looking for anyway. We also observe

[2]This is not, in fact, true, if (x, y, z, r) is a rational solution, so is (nx, ny, nz, nr) for any $n \in \mathbb{Q}$. This is the same as saying that if we scale a triangle is remains a triangle. But since we are looking for an infinite number of non-similar triangles, scaling triangles will get us nowhere.

that for each choice of τ, this turns out to be the equation for an elliptic curve. It might not be obvious that this is the case, considering we have, among other things, cross-terms. But an equation on this form can always be rewritten to the form

$$y^2 = x^3 + ax^2 + bx + c, \tag{3}$$

with a simple change of variables [6, p. 42]. We will soon give such a change of variables. We will also fix z at a different value than 1 and set $\tau(s) = \frac{s-1}{s(s+1)}$[3], thus changing the parameter for the curves from τ to s. We do this to make the computations we do later easier, and to get the same Weierstrass equation as the one van Luijk uses in his proof.

Now, we change coordinates to (α, β), by applying the following change of variables

$$\begin{aligned} x &= -s(s+1)\alpha + \beta, \\ y &= -s(s+1)\alpha - \beta, \\ z &= 8(s-1)^2 s(s+1), \end{aligned} \tag{8}$$

to equation (7), then we get the Weierstrass equation:

$$\beta^2 = (\alpha - 4(s-1)^2)^3 + (s(s+1)\alpha)^2. \tag{9}$$

This is still not on the form $\beta^2 = \alpha^3 + a\alpha^2 + b\alpha + c$, but now we can get there by simply expanding the parentheses. Doing this will give us a longer and more confusing equation, so we will stick to the form above. Here we can again consider s to be a fixed variable, meaning that for each choice of s we get an elliptic curve E_s, given by equation (9). In order to keep $0 < \tau = \frac{s-1}{s(s+1)}$ we need to set the condition that $s > 1$.

Now we have constructed a family of elliptic curves, with one curve for each s. The points on these curves correspond, under the change of variables (8) and (6), to solutions to Herons equation. The next step will be to find an infinite number of rational points on this curve. Recall that the rational points on an elliptic curve form a group, so if we can find a rational point of infinite order, we can use this point to generate the points we need. The point we will use as a generator will be the point $R(s) = (8 - 8s, 8s^2 - 8)$, which is rational if we take s to be rational.

Lemma 3.2. *The point $R(s) = (8 - 8s, 8s^2 - 8)$ is a point of infinite order on E_s.*

Proof. One can easily check that $R(s)$ satisfies equation (9), and thus lies on the curve E_s. Furthermore, form van Luijks article, we have that for any s, $R(s)$ will always lie in a subgroup of E_s that is isomorphic to $\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ [8, Theorem 5.6.]. Hence $R(s)$ must either have order 1, 3 or have infinite order. Knowing this, we only need to show that it does not have order 1 or 3. It can not have order 1, because it is not the identity. Computation also shows that

$$2R(s) = (s^6 - 4s^5 + 3s^4 + 4s^3 - s^2 - 8s + 5, s^9 - 6s^8 + 11s^7 + s^6 - 21s^5 + 11s^4 + 9s^3 - 5s^2 - 1)$$

which is definitely not $-R(s) = (8 - 8s, 8 - 8s^2)$. Hence, $R(s)$ does not have order 3 either, and must therefore have infinite order. $\square$

[3]Note that this function is not injective, so two different values of s can give us the same elliptic curve. We will come back to this problem in section 3.3.

Now that we have found an elliptic curve on which the points correspond to solutions to Herons equation, and a rational point of infinite order, we have all that we need to start generating triangles.

3.3 An explicit method for generating rational triangles

In this subsection, we will construct a method for generating solutions to Herons equation, and prove that the solutions correspond to non-similar rational triangles.

Method 3.3. *First of all we choose some rational $s > 1$, and look at the curve E_s given by*

$$\beta^2 = (\alpha - 4(s-1)^2)^3 + (s(s+1)\alpha)^2. \tag{9}$$

From Lemma (3.2) we know that $R(s) = (8 - 8s, 8s^2 - 8)$ lies on E_s and has infinite order.

Next, compute $(3R(s), 5R(s), 7R(s), ...)$[4]*, and let (α_n, β_n) be the coordinates of $(2n-1)R(s)$, this will give us an infinite number of points lying on E_s . Now that we have N points on E_s, we can change their coordinates from (α_n, β_n)*[5] *to (x_n, y_n, z_n) using*

$$\begin{aligned} x_n &= -s(s+1)\alpha_n + \beta_n, \\ y_n &= -s(s+1)\alpha_n - \beta_n, \\ z_n &= 8(s-1)^2 s(s+1). \end{aligned} \tag{8}$$

And finally, apply

$$a_n = \frac{y_n + z_n}{x_n + y_n + z_n}, \quad b_n = \frac{x_n + z_n}{x_n + y_n + z_n}, \quad c_n = \frac{x_n + y_n}{x_n + y_n + z_n} \tag{10}$$

to change coordinates to (a_n, b_n, c_n).

The triples (a_n, b_n, c_n) generated by this method will sometimes be referred to as $\triangle_n(s)$, when we are talking about the triangle with sides a_n, b_n and c_n. In section 5.1 we will demonstrate the method step-by-step, by computing a 4-tuple of rational triangles.

Now we have a method that will generate triples (a_n, b_n, c_n) satisfying Herons equation. But for all we know these triples might not even satisfy the triangle inequality, far less correspond to rational triangles. So the next step is to prove that the method does indeed produce rational triangles.

Proposition 3.4. *Let $s > 1$ be a rational number and let the triples (a_n, b_n, c_n) be generated by method 3.3. Then for every $n \in \mathbb{N}$ there is a rational triangle $\triangle_n(s)$ with sides a_n, b_n, c_n. All these triangles will have perimeter $p = 2$ and area $A = \frac{s-1}{s(s+1)}$.*

[4]We choose to use the odd multiples because it turns out that only they produce triangles, the reason behind this will become clear in the proof of Proposition 3.4.

[5]Seeing as we are now working with a specific value of s, we will write $\alpha_n, \beta_n, x_n, y_n, z_n, a_n, b_n, c_n$ instead of $\alpha_n(s), \beta_n(s), x_n(s), y_n(s), z_n(s), a_n(s), b_n(s), c_n(s)$ despite the fact that they depend on the choice of s, this is done to make the expressions here, and later, less messy.

Proof. Before we show that the triangles we produce are rational, we must first show that method 3.3 actually produces triangles $\triangle_n$. Specifically, we want to show that a_n, b_n and c_n are positive, and that they satisfy the triangle inequality.

Starting with the triangle inequality for a_n, we get:

$$
\begin{gathered}
a_n < b_n + c_n \\
\Updownarrow \\
\frac{y_n + z_n}{x_n + y_n + z_n} < \frac{x_n + z_n}{x_n + y_n + z_n} + \frac{x_n + y_n}{x_n + y_n + z_n} \\
\Updownarrow \\
y_n + z_n < x_n + z_n + x_n + y_n \\
\Updownarrow \\
0 < 2x_n
\end{gathered}
$$

Doing the same for b_n and c_n we get $0 \leq 2y_n$ and $0 \leq 2z_n$ respectively. That means that if we can prove that x_n, y_n and z_n are positive, we will have shown that a_n, b_n and c_n satisfy the triangle inequality. Furthermore, if x_n, y_n and z_n are positive, so are a_n, b_n and c_n, because of how they are defined in (10).

Next, we want to find out what points (α_n, β_n) on E_s we can use to make $x_n, y_n, z_n > 0$. We know that the value of z_n does not depend on α_n or β_n, and will always be positive for $s > 1$. On the other hand, x_n and y_n might not be positive. However, if we take the points on E_s where $\alpha_n < 0$ and therefore also $\alpha_n < 4(s-1)^2$ and substitute into equation (9), we get

$$
\begin{gathered}
(s(s+1)\alpha_n)^2 = \beta_n^2 - (\alpha_n - 4(s-1)^2)^3 > \beta_n^2 \\
\Downarrow \\
-s(s+1)\alpha_n > |\beta_n| \\
\Downarrow \\
x_n = -s(s+1)\alpha_n + \beta_n > 0, \\
y_n = -s(s+1)\alpha_n - \beta_n > 0.
\end{gathered}
$$

This means that the points on E_s that have first coordinate $\alpha < 0$ will make $x_n, y_n, z_n > 0$, and hence produce triangles. Now it remains to show that the odd multiples of $R(s)$ (those are the ones we use to generate triangles) lie on the part where $\alpha < 0$.

Now, for the next step, we will need to use some of the properties of elliptic curves. Our elliptic curve, E_s has discriminant

$$
\Delta(s) = 2^{12}(s-1)^6 s^4 (s+1)^4 (s^4 + 2s^3 - 26s^2 + 54s - 27). \tag{11}
$$

For $s > 1$, the discriminant will be positive, meaning that according to Lemma (2.3), the elliptic curve will consist of two separate components, one that is bounded, and one that is not (see Figure 7 for reference). Our starting point $R(s)$ (R_1 on Figure 7) lies on the bounded part. We call this part B (for bounded), and the other part, the unbounded one, U (for unbounded).

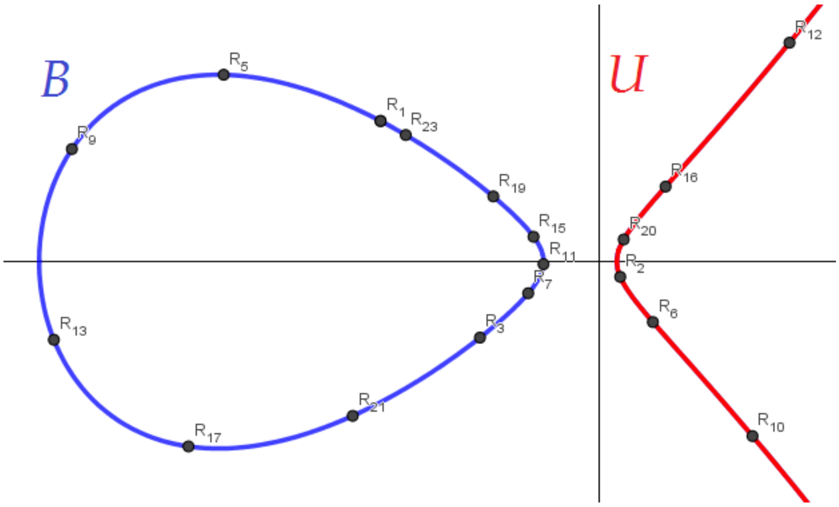

Figure 7: The curve E_s for $s = 7/4$, with the first 23 multiples of R. The bounded part B is coloured blue, and the unbounded part U is coloured red. Note that the the graph tool we use, uses the notation R_n for $nR(s)$.

From Proposition 2.5 we know that part B is convex, so any line intersecting B will intersect it in exactly two points (recall that tangents are counted as intersecting E_s twice). This, combined with the fact that any non-vertical line intersects E_s either once or thrice [Lemma 2.4], gives us the following results:

- Any line through two points on B will intersect U. This is because it has already intersected B twice, so it can not do so again. It follows that the sum of two points on B will lie on U.
- Any line through one point on B and another one on U will intersect E_s in a third point lying on B. This is because any line intersecting B does so twice. It follows that the sum of two points, one on B and one on U, will lie on B.

Combining these two results, we get this useful property of points on B:

- When taking the multiples of any point on B, all the odd multiples will be lying on B, and all the even ones will be on U.

Now, because R lies on B, we know that all its odd multiples do so as well. We wanted to show that all odd multiples of R had first coordinate $\alpha < 0$, so now, for the final step, we need to show that B lies entirely in the half-plane where $\alpha < 0$.

Recall the equation defining E_s:

$$\beta^2 = (\alpha - 4(s-1)^2)^3 + (s(s+1)\alpha)^2. \tag{9}$$

If we set $\alpha = 0$, we get $\beta^2 = -64(s-1)^6 < 0$, meaning that no point on E_s has α-coordinate equal to zero. Hence, the line $\alpha = 0$ either lies between B and U, or to the left of both. Or, equivalently: either the whole curve E_s will lie in the half plane where $\alpha > 0$, or the entire connected component B will lie where $\alpha < 0$. We do, however, know that the point $R = (8-8s, 8s-8)$

has $\alpha < 0$, and that it lies on B meaning that all of B does indeed lie where $\alpha < 0$.

Thus, because all the odd multiples of $R(s)$ lie where $\alpha < 0$, we know that x_n, y_n and z_n are all positive. And because they are all positive, the triple (a_n, b_n, c_n) does indeed form a triangle.

Next, we need to show that the triangle is, in fact, rational.

First, we want to show that a_n, b_n, c_n are rational, in order to prove this, it suffices to show that $x_n, y_n, z_n \in \mathbb{Q}$. Recall from section 2.1 that the rational points on E_s form a subgroup of E_s, hence adding two points with rational coordinates will yield a new point with rational coordinates. Our starting point $R(s)$ has coordinates $(8-8s, 8s^2-8)$. We have chosen s to be rational, so $R(s)$, will have rational coordinates, and only generate points with rational coordinates. In turn x_n, y_n, z_n will be rational, and so will a_n, b_n, c_n. Thus, the triangle, will indeed have rational sides.

In order for $\triangle_n$ to be a rational triangle, we also need to show that it has rational area. We can do this by simply computing the area A, using Herons formula:

$$A^2 = \frac{p}{2}(\frac{p}{2} - a_n)(\frac{p}{2} - b_n)(\frac{p}{2} - c_n), \tag{1}$$

where p is the perimeter of the triangle. We substitute $p = a_n + b_n + c_n = 2$ into equation (1), and get:

$$A^2 = (1-a_n)(1-b_n)(1-c_n)$$

Changing variables to x, y, z using (6), and then to α, β using (8) gives us:

$$A^2 = \frac{x_n y_n z_n}{(x_n + y_n + z_n)^3}$$

$$A^2 = \frac{(s^2(s+1)^2\alpha_n^2 - \beta_n^2)(8(s-1)^2 s(s+1))}{(-2s(s+1)\alpha_n + 8(s-1)^2 s(s+1))^3}$$

$$A^2 = \frac{(s^2(s+1)^2\alpha_n^2 - \beta_n^2)(8(s-1)^2 s(s+1))}{(2s(s+1))^3(4(s-1)^2 - \alpha_n)^3}$$

$$A^2 = \frac{(s-1)^2}{s^2(s+1)^2}\,\frac{s^2(s+1)^2\alpha_n^2 - \beta_n^2}{4(s-1)^2 - \alpha_n)^3}.$$

Now, because α_n and β_n satisfy equation (9), we have $\frac{s^2(s+1)^2\alpha_n^2 - \beta_n^2}{4(s-1)^2 - \alpha_n)^3} = 1$, we are left with

$$A^2 = \frac{(s-1)^2}{s^2(s+1)^2}$$
$$\Downarrow$$
$$A = \frac{s-1}{s(s+1)}.$$

Now, it is easy to see that A is rational when $s \in \mathbb{Q}$. We have already shown that the sides are rational, so the triangle with sides a_n, b_n and c_n is indeed a rational triangle.

At the same time, we have shown that all the triangles have the same area $A = \frac{s-1}{s(s+1)}$, and the same perimeter $p = 2$, regardless of the choice of n. With this, our proof is finally complete. Method 3.3 does indeed produce rational triangles, all having the same area and perimeter. □

Before we move on to the next proposition, let us have a closer look at A. We have found that the area of our triangles is

$$A = \frac{s-1}{s(s+1)} = \tau(s). \tag{12}$$

The graph of τ is shown in Figure 8. It has a maximal point at $(s_0, \tau(s_0))$ where

$$s_0 = 1 + \sqrt{2},$$
$$\tau(s_0) = (\sqrt{8} + 3)^{-1}.$$

This means that none of the triangles we generate will have an area greater than $\tau(s_0) \approx 0.172$, but we know the largest area a triangle with perimeter 2 can have is when it is equilateral, then it will have area $A = (3\sqrt{3})^{-1} \approx 0.192$. Method 3.3 will hence generate far from all rational triangles, as it is missing out on, for example, the $(6/8, 5/8, 5/8)$ triangle, which has area $A = 3/16 \approx 0.188$.

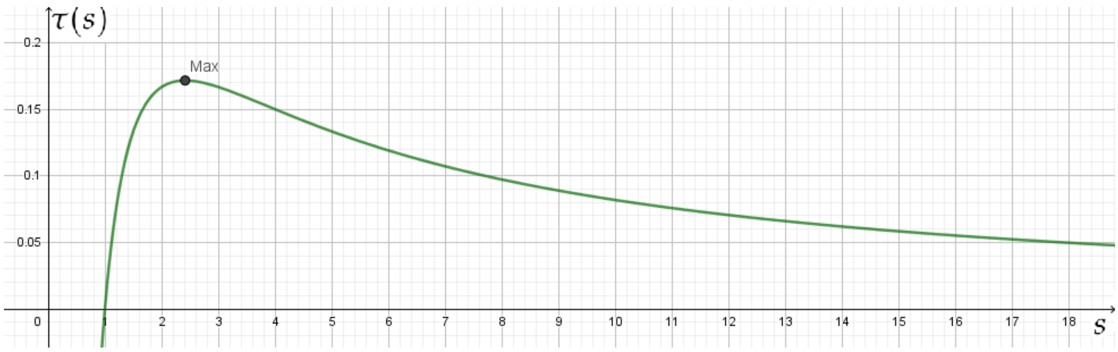

Figure 8: The function $\tau(s)$, with its maximal point at $s = s_0$. It is clearly not injective for $s > 1$. It is however, injective on both sides of s_0.

Figure 8 also shows that, as we briefly mentioned in section 3.2, $\tau(s)$ is not injective for $s \in [1, \infty)$, meaning that two different choices of s can generate triangles with the same area. Hence, we can not know whether method 3.3 generates a unique family of triangles for each s. In his paper, van Luijk seems to overlook this fact, which in turn causes a flaw in his proof. We will return to this once we complete the proof of our main theorem. For now, all we need to note is that the function $\tau(s)$ is injective for $s > s_0$, as this will be an important point in the proof of Proposition 3.6 later.

From Proposition 3.4 it is clear that there exists a sequence of Heron triangles, all with the same area and perimeter. Meaning that we are well on our way to proving van Luijks Theorem: *"for each $s > 1$, there exist a sequence of Heron triangles, all having the same area and perimeter, and all being non-similar"*. We only need to show that the triangles will be non-similar. In order to do this, we first need a lemma:

Let us define a point P on E_s given by $P = (4(s-1)^2, 4s(s+1)(s-1)^2)$.

Lemma 3.5. *For any odd multiple R' of R with corresponding triangle (a_n, b_n, c_n)*

1. *$-R'$ will correspond to the triangle (b_n, a_n, c_n), and*
2. *$R' + P$ will correspond to the triangle (b_n, c_n, a_n).*

These two operations generate all possible permutations of (a_n, b_n, c_n).

Figure (9) shows these operations applied to R.

Proof. Let R' have coordinates (α_n, β_n), and let that correspond to (x_n, y_n, z_n), under the change of variables in (8). We prove 1. and 2. separately.

1. The coordinates of $-R'$ will be $(\alpha_n, -\beta_n)$, corresponding to (y_n, x_n, z_n) under (8). So taking the inverse of a point will be the same as switching around x_n and y_n, which, under (10) will correspond to switching the sides a_n and b_n of the triangle, giving us (b_n, a_n, c_n).
2. From van Luijks paper [8], the automorphism induced by the 3-cycle (xyz) corresponds to translation by P [8, see Lemma 5.5]. In other words, adding P to R' will give us a point that corresponds to (z_n, x_n, y_n), which in turn corresponds to the triangle (c_n, a_n, b_n).

There exist 6 possible permutations of (a_n, b_n, c_n), it is simple to check that these two operations generate all of them. □

With this lemma, we can move on to prove that the triangles given by method 3.3 will indeed be non-similar, not only for different n, but also for different s.

Proposition 3.6. *Let the triangles $\triangle_n(s)$ be given by method 3.3 described in the beginning of the chapter. Then for all $n_1, n_2 \in \mathbb{N}$ and $s_1, s_2 \in \mathbb{Q}$ with $s_1, s_2 > s_0$ the triangles $\triangle_{n_1}(s_1)$ and $\triangle_{n_2}(s_2)$ are similar if and only if $n_1 = n_2$ and $s_1 = s_2$.*

Proof. If $n_1 = n_2$ and $s_1 = s_2$ the triangles will obviously be similar, no proof of this will be given. The implication the other way, however, is less trivial.

Let us first assume that $s_1 \neq s_2$. Because $s_1, s_2 > s_0$ we know that $\tau(s_1) \neq \tau(s_2)$ because $\tau(s)$ is injective for $s > s_0$. Hence the two triangles will have different areas (recall that $A = \tau(s)$). We already know that they will have the same perimeter because our method only produces

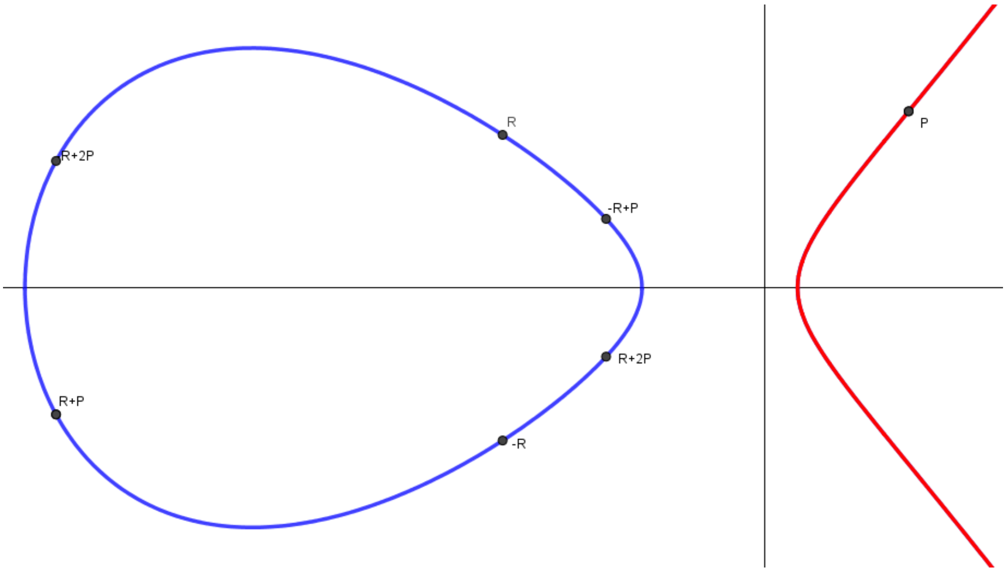

Figure 9: This shows the 6 point we get by applying the operations in Lemma 3.5 to R, on the curve E_s for $s = 2.1$

triangles with $p = 2$, but then they can not be similar, because a scaling that makes the areas equal will make the perimeters different. As such, the two triangles will be similar only if they have the same s.

For the next part, we assume that $s_1 = s_2$ and that the triangles are similar, and use this to show that $n_1 = n_2$. Because $s_1 = s_2$, the two triangles will have the same area and perimeter. But if two triangles with the same area and perimeter are similar, they must be congruent. Hence, we know that the sides of $\triangle_{n_1}(s_1)$ are just a permutation of the sides of $\triangle_{n_2}(s_2)$.

From Lemma 3.5 we have that any permutation can be obtained by inversions and translations by P. So we can write

$$(2n_1 - 1)R = \pm(2n_2 - 1)R + kP$$

for some $k \in \{0, 1, 2\}$. We multiply by 3 on both sides to get

$$3(2n_1 - 1)R = \pm 3(2n_2 - 1)R + 3kP.$$

Because P has order 3, we know that $3kP = O$, and we get

$$3(2n_1 - 1)R = \pm 3(2n_2 - 1)R.$$

Because R has infinite order, $nR = mR \Rightarrow n = m$, so

$$3(2n_1 - 1) = \pm 3(2n_2 - 1)$$

Since $n_1, n_2 \geq 1$, and we only have positive multiples of R, we get

$$6n_1 - 3 = 6n_2 - 3$$
$$\Downarrow$$
$$n_1 = n_2$$

This means that if $\triangle_{n_1}(s_1)$ and $\triangle_{n_2}(s_2)$ are similar, then $n_1 = n_2$ and $s_1 = s_2$. □

3.4 Our main theorem, and the error in the original proof

With these two propositions in place, we can construct a theorem of our own, analogue to the main theorem in van Luijsks paper [8].

Theorem 3.7 (Main Theorem). *There exists a sequence* $\{(a_n(s), b_n(s), c_n(s))\}_{n\in\mathbb{N}}$ *of triples of elements in* $\mathbb{Q}(s)$ *such that*

(1) *for all* $n\in \mathbb{N}$ *and all* $s \in \mathbb{Q}$ *with* $s > 1$ *there exists a triangle* $\triangle_n(s)$ *with sides* $a_n(s)$, $b_n(s)$ *and* $c_n(s)$, *perimeter* 2, *and area* $\frac{s-1}{s(s+1)}$, *and*

(2) *for all* $n_1, n_2 \in \mathbb{N}$ *and* $s_1, s_2 \in \mathbb{Q}$ *with* $s_1, s_2 > s_0$, *the rational triangles* $\triangle_{n_1}(s_1)$ *and* $\triangle_{n_2}(s_2)$ *are similar if and only if* $n_1 = n_2$ *and* $s_1 = s_2$.

Proof. We want to show the existence of such a sequence with these properties. If we take $\{(a_n(s), b_n(s), c_n(s))\}_{n\in\mathbb{N}}$ to be the sequence generated by method 3.3, then by Proposition 3.4 and 3.6 it will satisfy (1) and (2) respectively. □

Now, that we have proven our main theorem, let us compare it to the main theorem in van Luijks paper:

Theorem 3.1. (van Luijks Theorem) *There exists a sequence* $\{(a_n(s), b_n(s), c_n(s))\}_{n\geq 1}$ *of triples of elements in* $\mathbb{Q}(s)$ *such that*

(1) *for all* $n\geq 1$ *and all* $s \in \mathbb{R}$ *with* $s > 1$ *there exists a triangle* $\triangle_n(s)$ *with sides* $a_n(s)$, $b_n(s)$ *and* $c_n(s)$, *inradius* $s - 1$, *perimeter* $2s(s + 1)$ *and area* $s(s^2 - 1)$, *and*

(2) *for all* m, $n \geq 1$ *and* $s_1, s_2 \in \mathbb{Q}$ *with* $s_1, s_2 > 1$, *the rational triangles* $\triangle_m(s_1)$ *and* $\triangle_n(s_2)$ *are similar if and only if* $m = n$ *and* $s_1 = s_2$.

Remark. Van Luijks proof of this theorem is, as we will soon see, flawed. He only proves it for $s_1, s_2 > s_0$, not for $s_1, s_2 > 1$. The theorem itself will, however, turn out to be true.

Van Luijks method for generating triangles is similar to ours, the main difference is the final step, when going from x, y, z to a, b, c. Whereas we choose to scale the triangles so that they have $p = 2$, van Luijks scaling is a bit different. This is the reason why the two theorems give triangles with different areas and perimeters. It is simple to check that if we scale our triangles up by a factor of $s(s + 1)$ we get the same areas and perimeters as van Luijk.

Secondly, and more importantly, we require $s > s_0$ in order to avoid similar triangles, while van Luijks Theorem only requires $s > 1$, and here the theorems are somewhat less compatible. It turns out that neither mine nor van Luijks method is sure to generate non-similar triangles if we don't require $s > s_0$. In his paper [8, Remark 1.2.], van Luijk gives an example of a sequence of triangles parameterized by s and states that all the triangles will be non-similar. However, both the triangle $(3, 4, 5)$ and the triangle $(6, 8, 10)$ appear in the sequence, for $s = 2$ and $s = 3$ respectively, and these two triangles are obviously similar.

Indeed, not only the example but also the proof itself is flawed, as it fails to recognize that $\tau(s) = \frac{s-1}{s(s+1)}$ is not injective. Van Luijk himself stated, in an email [7], that

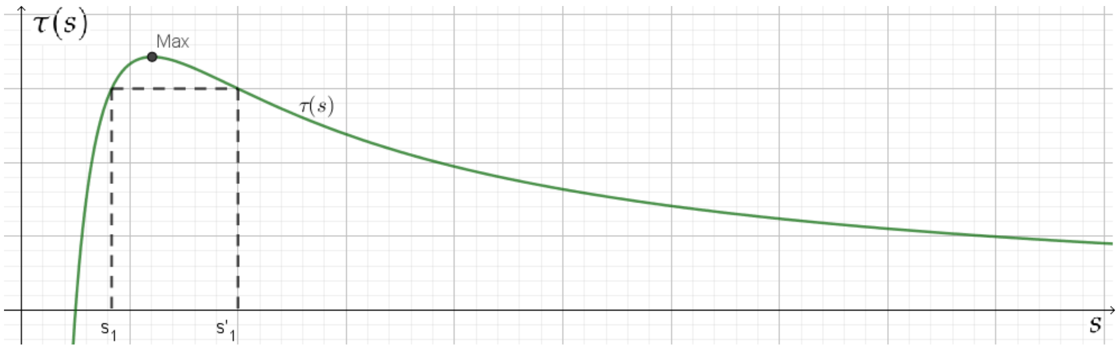

Figure 10: The function $\tau(s)$, with its maximal point at $s = s_0$. For each value of s, there will be another value $s' = \frac{s+1}{s-1}$ such that $\tau(s) = \tau(s')$.

> "The idea was that the ratio 2s(s+1)/(s-1) between the perimeter and the inradius depends on s and is therefore different for different values, but I somehow overlooked the fact that there are usually two values that give the same, namely s and s' = (s+1)/(s-1). Or phrased differently, when (s-1)(s'-1) = 2."

Figure 10 illustrates the point in the e-mail, that there are usually two values of s giving the same area. This, however, does not mean that the theorem is false, in fact, it turns out that such a sequence still exists and that the theorem remains true. Even better, we can still find such a sequence explicitly, based on our current method. Let us construct this new sequence in order to prove van Luijks Theorem.

Proof. (van Luijks Theorem)
We simply define a new sequence $\blacktriangle_n(s)$ for $n \in \mathbb{N}$ and $s > 1$:

$$\blacktriangle_n(s) = \begin{cases} \triangle_{2n}(s) & \text{if } s < s_0, \\ \triangle_{2n-1}(s) & \text{if } s > s_0, \end{cases}$$

where $\triangle_n(s)$ are the triangles generated by method 3.3.

Now, two triangles $\blacktriangle_{n_1}(s_1)$ and $\blacktriangle_{n_2}(s_2)$ will be similar only if $n_1 = n_2$ and $s_1 = s_2$, because even if we take s_1 and s_2 such that they have the same area, they will be non-similar because they correspond to $\triangle_n(s)$ with different n which we know to be non-similar from Proposition 3.6. □

As such, van Luijks Theorem remains true. In the next section we will see what this implies, and what problems on Herons triangles that still remain to be solved .

4 The next step - rational medians

Since we concluded that van Luijks Theorem was indeed true, it follows that one can find an N-tuple of non-similar Heron triangles all having the same area and perimeter for any $N \in \mathbb{N}$[6].

[6]see section 3.1 if you forgot why this follows from van Luijks Theorem.

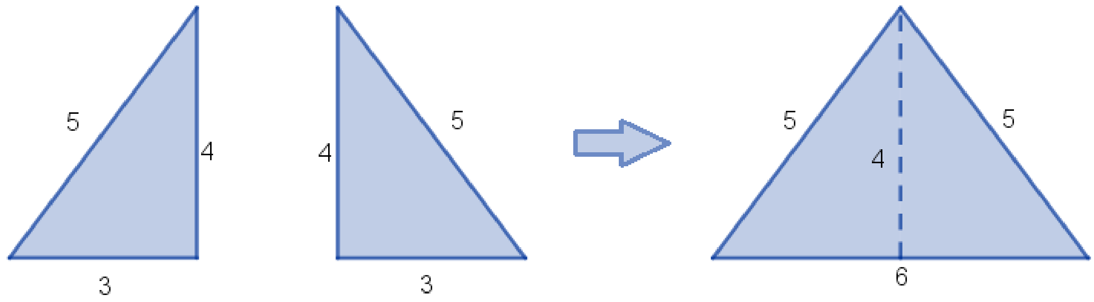

Figure 11: By combining two Pythagorean triangles, one can obtain a Heron triangle with one integer median.

Now that this problem on Heron triangles has been solved, what will be the next step? Some might wonder whether it is possible to find an infinite (not just an arbitrarily large) number of non-similar Heron triangles having the same area and perimeter. But it is simple to show that this is impossible. Given any natural number, there exists only a finite number of ways to write it as the sum of three natural numbers. Equivalently, for any finite perimeter, there exist only a finite number of triangles with integer sides, having this perimeter. Even fewer of these will be Heron triangles, so we cannot find infinitely many having the same area and perimeter

We can also start looking for Heron triangles with integer altitudes or medians. But because the altitude h_a is given by $h_a = \frac{A}{a}$ for side a and similar for the other sides, the altitude of a Heron triangle is always rational, and can be scaled up to be an integer. The medians however, are more interesting.

Now, first of all, does there even exist Heron triangles with integer medians? The triangle (5,5,6) will have one median of length 4, so the answer is yes. This is because the triangle (5,5,6) can be formed by joining two (3,4,5) triangles along the side with length 4. So, because (3,4,5) is Pythagorean, the resulting triangle must be Heron, and have median 4 (see Figure 11). This process can be done with any Pythagorean triple, and because we know there exist infinitely many primitive Pythagorean triples, we know that there also exists an infinite number of Heron triangles with one integral median.

There also exists an infinite number of Heron triangles with two rational medians, this was proven in 1997, by Buchholz and Rathbun [2]. However, a Heron triangle with three rational medians has not yet been found. Several "proofs" have been given that no such triangle can exist, but they have all turned out to be flawed [3]. This remains an open problem to this day (see D21 in [3]).

In this thesis we have found an infinite number of integer solutions (A, a, b, c) to Herons equation

$$A^2 = \frac{p}{2}(\frac{p}{2} - a)(\frac{p}{2} - b)(\frac{p}{2} - c), \tag{1}$$

where $p = a + b + c$. If we are to find a Heron triangles with rational medians, we will also need to find integer solutions to the equations

$$4m_a^2 = 2b^2 + 2c^2 - a^2, \qquad 4m_b^2 = 2a^2 + 2c^2 - b^2, \qquad 4m_c^2 = 2a^2 + 2b^2 - c^2,$$

where m_a, m_b, m_c is the length of the medians from the midpoints of a, b and c respectively. Under the same changes of variables we used on Herons formula in section 3.2, these equation do not turn out to be elliptic curves, but rather to be quadratic equations, which are generally easier to work with. We also know that each of these equations have a countably infinite number of rational solutions. Still, finding a 7-tuple of integers $(A, a, b, c, m_a, m_b, m_c)$ that solves all four equations simultaneously is difficult, if not impossible, as finding integer solutions to even one of these equations is far from trivial.

We will not seek to find a triangle with rational medians, sides, and area, as this is beyond the scope of this thesis, but to give an idea of how rare these triangles are: The next section contains examples of Heron triangles computed using method 3.3, and among these only one triangle (up to similarity) has one rational median, while the others have only irrational medians. So among the solutions to Herons equation, very few will also be solutions to even one of the three other equations.

5 Computing examples

Now that we have constructed a method and proven that it works, the reader is probably eager to see the actual Heron triangles generated by it. In this section, we will use the method to generate some examples of triangles sharing the same area and perimeter. We will start with a simple example where we do every step in method 3.3, in order to clarify how it works. Then we will see what happens with bigger tuples of triangles. Finally, we prove the result of Kramer and Luca, that there exists an infinite parameterized family of *pairs* of Heron triangles with the same area and perimeter, by giving an example of such a family.

5.1 Applying the method for $s = 2$ and $N = 4$

In this example we will try to find $N = 4$ Heron triangles, all having the same area and perimeter. We start of by setting $s = 2$[7] into (9) to get the curve E_2: $\beta^2 = (\alpha - 4)^3 + 36\alpha^2$, we also get the point $R_2 = (-8, 24)$ lying on the curve.

Next we want to compute the first $(2n - 1)$ multiples of R. In section 2.1 we gave the formula for addition of points on an elliptic curve. Recall equation (5):

Given $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, the coordinates of $-R = P + Q$, will be:

$$-R = (x_{-R}, y_{-R}),$$

where

$$\begin{aligned} x_{-R} &= \lambda^2 - x_P - x_Q - a, \\ y_{-R} &= -\lambda(x_{-R} - x_P) - y_P, \end{aligned} \tag{5}$$

Here λ is the slope of the line l, given by

[7]Here we choose $s < s_0$. But this does not cause any problems with similarity because we are only looking at one 4-tuple of triangles, and not a family of such.

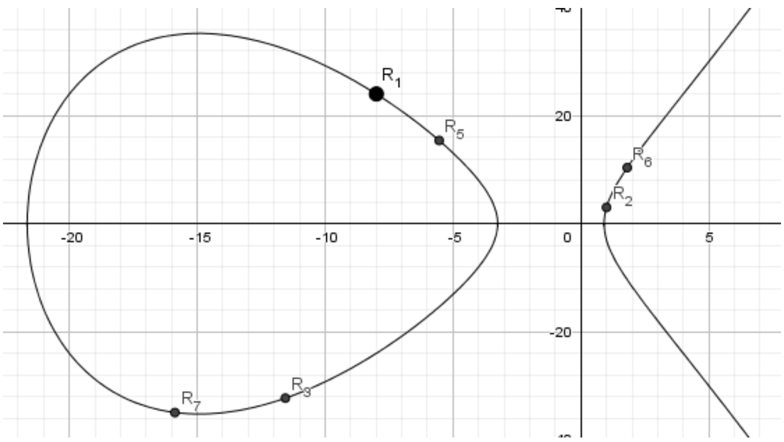

Figure 12: This shows E_2 with the the seven first multiples of R.

$$\lambda = \begin{cases} \dfrac{y_P - y_Q}{x_P - x_Q} & \text{if } x_P \neq x_Q, \\ \\ \dfrac{3{x_P}^2 + 2ax_p + b}{2y_P} & \text{if } P = Q. \end{cases}$$

We proceed use equation (5) over and over to compute the first 7 multiples of R. The odd multiples are given in Table (1).

Remark. The values given from now on, have been computed using Python. The script we use can be found in appendix A.

n	$(2n-1)$R
1	(-8,24)
2	$(-\frac{104}{9}, -\frac{872}{27})$
3	$(-\frac{70760}{12769}, \frac{22205688}{1442897})$
4	$(-\frac{1367100104}{86136961}, -\frac{27943556883288}{799437135041})$

Table 1: The first 4 odd multiples of R for $s = 2$.

Now we have 4 points on E_2 that will correspond to rational triangles. first of, we apply equation

$$\begin{aligned} x &= -s(s+1)\alpha + \beta, \\ y &= -s(s+1)\alpha - \beta, \\ z &= 8(s-1)^2 s(s+1), \end{aligned} \tag{8}$$

to change coordinates to x, y, z and then apply

$$a_n = \frac{y_n + z_n}{x_n + y_n + z_n}, \quad b_n = \frac{x_n + z_n}{x_n + y_n + z_n}, \quad c_n = \frac{x_n + y_n}{x_n + y_n + z_n} \tag{10}$$

to change to a, b, c. By doing this we get the four rational triangles in Table (2).

a	b	c	A
$\frac{1}{2}$	$\frac{5}{6}$	$\frac{2}{3}$	$\frac{1}{6}$
$\frac{101}{126}$	$\frac{41}{90}$	$\frac{26}{35}$	$\frac{1}{6}$
$\frac{27689}{48138}$	$\frac{27277}{32318}$	$\frac{17690}{30459}$	$\frac{1}{6}$
$\frac{226180525}{302690534}$	$\frac{221167193}{487085442}$	$\frac{341775026}{427911987}$	$\frac{1}{6}$

Table 2: Four rational triangles with sides a, b, c and area A. Note that the first triangle is similar to (3,4,5), the smalle st Heron triangle.

With this we have completed every step in method 3.3, but because we are looking to find Heron triangles, and not rational triangles, we want to multiply with the lowest common denominator[8] in order to make the sides integers . We find this to be 956844466195327139430, and multiplying with this gives us the following Heron triangles:

a'	b'	c'
478422233097663569715	797370388496105949525	637896310796884759620
766994373696254294305	435895812377871252407	710798746316528732148
550377382202883650415	807594730627202747145	555716819560567881300
714986295895873126125	434467110856505321595	764235525638275831140

Table 3: Four Heron triangles with sides a', b', c', each of them will have area and perimeter:
$A = 152591888748103423480760746692984443454150$,
$p = 956844466195327139430$.

We have now generated a quadruple of Heron triangles having the same area and perimeter. These are shown in Figure 13.

Now we have shown how method 3.3 works step by step. We will move on to finding some bigger tuples soon. But first, let us return to the problem with $\tau(s)$ not being injective.

[8]We multiply with the lowest common denominator of the sides in ALL the triangles, rather than simply scaling up each triangle. We do this to ensure all the triangles have the same area and perimeter.

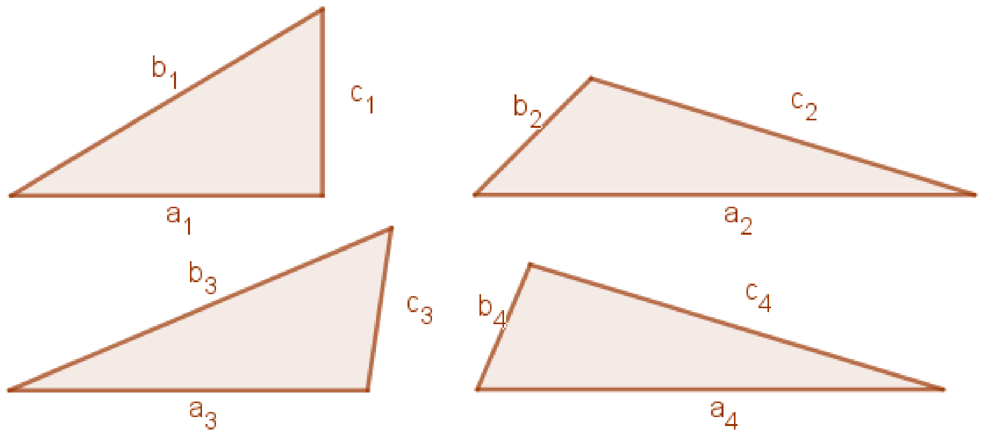

Figure 13: The first four triangles on the elliptic curve E_2.

5.2 When different values of s give the same τ

As we have discussed before, there are usually two different values of s that give the same value of τ and hence the same elliptic curve. Earlier we chose to only use $s > s_0$ to be certain to avoid similar triangles. We have, however, not checked whether this was actually necessary. For all we know, the triangles produced will still be non-similar, despite having the same area. After all, the starting point R will have different coordinates, and so will all its multiples. In this section, we will see what happens when we take two different values of s that give the same τ.

In the previous section, we were using using $s = 2$. Seeing as $s < s_0$ there should exist some $s' > s_0$ that will give triangles similar to these. In this case $s' = 3$ is such that $\tau(s') = \tau(s) = 1/6$. So let us have a look at the first four triangles generated by method 3.3 when we choose $s = 3$, and see whether these are the same as the ones we generated with $s = 2$. The first four odd multiples of $R(s')$ turn out to be:

n	$(2n-1)$R
1	(-16,64)
2	$(-\frac{416}{9}, \frac{6976}{27})$
3	$(-\frac{436432}{5041}, \frac{2458432}{357911})$
4	$(-\frac{3618888400}{76510009}, -\frac{175197095447104}{669233048723})$

Table 4: The first 4 odd multiples of R for $s = 3$.

These are not at all similar to the first four multiples we got when we chose $s = 2$. However, after applying (8) and (10) to change coordinates back to (a, b, c) we get the following rational triangles:

a	b	c
$\frac{2}{3}$	$\frac{5}{6}$	$\frac{1}{2}$
$\frac{41}{90}$	$\frac{101}{126}$	$\frac{26}{35}$
$\frac{27689}{48138}$	$\frac{17690}{30459}$	$\frac{27277}{32318}$
$\frac{341775026}{427911987}$	$\frac{221167193}{487085442}$	$\frac{226180525}{302690534}$

Table 5: The first four rational triangles given by method 3.3 for $s = 3$. Note that these are just permutations of the values in Table 2.

These rational triangles are not only similar to the ones generated when $s = 2$, they are congruent. While this is the case, the sides do seem to have been permuted, it is not as simple as two of the columns (a, b, c) simply having been switched either. For example, $n = 1, s = 2$ gave $(1/2, 5/6, 2/3)$, while $n = 1, s = 3$ gave $(2/3, 5/6, 1/2)$ meaning a and c has been switched. For $n = 2$ however, it is a and b that have been switched. It seems to be a pattern that for each n, one of the values a, b and c will always be unchanged, while the other two are switched around. This means that the triangles generated when $s = 2$ will have opposite orientation of those generated when $s = 3$.

This example shows that we can not take families of triangles generated by $s < s_0$ and $s > s_0$ without running a risk of generating similar triangles. Having shown this, we move on to computing some more examples.

5.3 Larger examples

In theory, method 3.3 can provide us with arbitrarily many Heron triangles with the same area and perimeter. But when we actually try to use the method, we quickly encounter a problem as the number of triangles N increases. Namely that the sides of the triangles start to become increasingly large. While this is hardly a surprise, the numbers of digits needed to represent each of the sides quickly increase beyond what can fit on this page. The least number of digits needed to represent the sides in each triangle, when we generate N triangles, can be found in Table 6.

We can attempt to reduce the number of digits needed by picking the right value of s, as the number of digits needed is largely dependent on both s and N. For example, if we had used $s = 4$ instead of $s = 2$ when computing our 4-tuple in the previous section, we would have gotten 38 digits for each side length, instead of 21. In an attempt to find the optimal s we have tested all rational values of s on the form $s = \frac{a}{b}$ with $b \leq 60$ and $a < 4b$ as well as for integral s up to $s = 100$. The s that gave the least number of digits are given in Table 6. But even after trying all these values of s we still seem unable to push the number of digits down to a manageable amount for the larger N. As such, we will not give examples of N-tuples of triangles

N	Digits needed	Optimal s	N	Digits needed	Optimal s
1	1	2	13	167	2
2	3	2	14	182	2
3	9	2	15	195	2
4	21	2	16	210	2
5	38	2	17	224	3
6	49	2	18	239	2
7	64	2	19	254	2
8	78	2	20	269	3
9	92	2	30	418	111/32
10	108	2	40	563	103/32
11	124	2	50	709	11
12	152	3	100	1429	67/32

Table 6: This table shows the number of digits we need to represent each of the sides in the triangle, when we generate N Heron triangles with the same area and perimeter, as well as showing what s minimizes the number of digits needed.

for $N > 6$, simply because my pages are not large enough to contain numbers with more than 40-50 digits. We will, however, give an example of a 6-tuple. This can be found in appendix B.

The values of s in Table 6 are the ones minimizing digits among the s that we have checked, but it is quite possible that there exists some value of s making the number of digits far lower. In fact, van Luijk gives an example of a 20-tuple of such triangles, where each of the sides are 22-digit numbers. Luckily, we know that $\tau = \frac{s-1}{s(s+1)} = \frac{4A}{p^2}$, so we can use this to compute s when the area and perimeter is known. It turns out that van Luijk has used $\tau = 28/195$ when computing the triangles, this does not, however, correspond to a rational value of s. Unfortunately, irrational numbers are always prone to round-off errors, and all of our attempts to implement the script with $\tau = 28/195$ ends up giving triangles that don't have the same area and perimeter, although being very close. This is most likely due to round off errors.

Even when s is rational we get some round-off errors. In fact, the 6-tuple given in the appendix does not contain only Heron triangles. Due to round off errors, only the first four are Heron. Using Herons formula

$$A^2 = \frac{p}{2}(\frac{p}{2} - a)(\frac{p}{2} - b)(\frac{p}{2} - c)$$

to compute A^2 and then checking whether A^2 is a perfect square, shows that the last two triangles given in the 6-tuple are not Heron, because their A^2 is not a perfect square. Their area is very close to being a square though, but for our purpose, approximations are not sufficient, as we are working with a problem in number theory. So while method 3.3 does give us an arbitrarily large number of Heron triangles, the actual triangles it produces are not that easy to compute. It is, however, likely that a reader with more computational experience can do a better job than me on this problem.

Finally, we will use method 3.3 to give a proof of the result of Kramer and Luca [4]:

Theorem 5.1 (Kramer and Luca). *There exists an infinite family, parametrized by s, of pairs of Heron triangles.*

This actually follows from Corollary 1.1, by taking $N = 2$. But because we are in the computational section of the thesis, we will instead give proof by example.

Proof. To prove this we simply use method 3.3 without choosing a value of s, and compute the first two triangles. We get

$$a_1 = \frac{s-1}{s}, \qquad b_1 = \frac{s^2+1}{s(s+1)}, \qquad c_1 = \frac{2}{s+1}$$

$$a_2 = \frac{s^{10} - 8s^9 + 21s^8 - 8s^7 - 46s^6 + 48s^5 + 26s^4 - 40s^3 + 29s^2 + 8s + 1}{s(s^9 - 7s^8 + 16s^7 - 4s^6 - 26s^5 + 10s^4 + 16s^3 + 20s^2 + 9s - 3)},$$

$$b_2 = \frac{s^{10} - 6s^9 + 13s^8 - 16s^7 + 26s^6 - 20s^5 - 46s^4 + 48s^3 + 37s^2 - 6s + 1}{s(s^9 - 5s^8 + 4s^7 + 16s^6 - 22s^5 - 14s^4 + 12s^3 + 16s^2 + 21s + 3)},$$

$$c_2 = \frac{2(s^7 - 7s^6 + 21s^5 - 31s^4 + 19s^3 + 3s^2 - s - 5)}{s^8 - 6s^7 + 10s^6 + 10s^5 - 40s^4 + 14s^3 + 30s^2 - 2s - 1}.$$

Let $\triangle_1(s)$ have sides (a_1, b_1, c_1), and let $\triangle_2(s)$ have sides (a_2, b_2, c_2). Then $\triangle_1(s)$ and $\triangle_2(s)$ are rational triangles having the same area and perimeter. If we multiply with the common denominator and substitute integral $s > 2$ we will get a family of pairs of Heron triangles having the same area and perimeter with no triangles being similar to one another. Hence such a family does indeed exist. □

This concludes the computational part of the thesis.

Acknowledgements

First, I would like to thank my supervisor, professor Kristian Ranestad, for suggesting such an interesting topic for my thesis, and for his continuous support. Without his help and guidance, I would still be struggling with the initial parts of the thesis.

I would also like to thank my fellow students, for providing me with help, motivation, and support in these last five years. They have made my time here at the University of Oslo truly enjoyable, and have given me fond memories that will stay with me for the rest of my life.

Finally, I would like to thank my family for always supporting and encouraging me. For this, I am truly grateful. For without them, I would never have gotten to where I am today.

Martin Bråtelund

Oslo, May 2018

A Script used to compute examples

This is the script used to generate the triangles given in section 5. We have used Python, rather than MATLAB, because Python appears to be better at handling large integers.

This script can be somewhat hard to understand for readers without computational experience, and any reader with experience, will probably frown upon such a needlessly complicated script. As such we recommend any reader to create their own script based on method 3.3, rather than trying to use or understand this one.

Python code

```python
from pylab import*
import numpy as np
from fractions import gcd #We import the gcd function

#First off, we define som function we will need later

#A function to compute the least common multiple of two numbers
def lcm(x,y):
    g=gcd(long(x),long(y))
    prod=long(x)*long(y)
    lcm=prod/g
    return lcm

#A function for adding fractions
def add(a,b):
    if type(a)==long:
        a=(a,1)
    if type(a)==int:
        a=(a,1)
    if type(b)==long:
        b=(b,1)
    if type(b)==int:
        b=(b,1)
    D=lcm(abs(long(a[1])),abs(long(b[1])))
    N=a[0]*(D/a[1])+b[0]*(D/b[1])
    G=gcd(abs(N),abs(D))
    n=N/G
    d=D/G
    add=(n,d)
    return add

#A function for subtracting b from a (fractions)
def sub(a,b):
    if type(a)==long:
        a=(a,1)
    if type(a)==int:
        a=(a,1)
    if type(b)==long:
        b=(b,1)
    if type(b)==int:
        b=(b,1)
    D=lcm(abs(long(a[1])),abs(long(b[1])))
    N=a[0]*(D/a[1])-b[0]*(D/b[1])
    G=gcd(abs(N),abs(D))
    n=N/G
    d=D/G
    sub=(n,d)
    return sub

```

```python
#A function for multiplying fractions
def mult(a,b):
    if type(a)==long:
        a=(a,1)
    if type(a)==int:
        a=(a,1)
    if type(b)==long:
        b=(b,1)
    if type(b)==int:
        b=(b,1)
    D=b[1]*a[1]
    N=long(a[0])*long(b[0])
    G=gcd(abs(N),abs(D))
    n=N/G
    d=D/G
    mult=(n,d)
    return mult

#A function for dividing a by b (fractions)
def div(a,b):
    if type(a)==long:
        a=(a,1)
    if type(a)==int:
        a=(a,1)
    if type(b)==long:
        b=(b,1)
    if type(b)==int:
        b=(b,1)
    D=long(a[1])*long(b[0])
    N=long(a[0])*long(b[1])
    G=gcd(abs(N),abs(D))
    n=N/G
    d=D/G
    mult=(n,d)
    return mult

#Now we can start the actual computation
#Most of the values here are fractions represented by 2-tuples on the form (nominator,denominator)

n=4   #Number of triangles we want to generate
s=(2,1)   #Choose s>1 (nominator,denominator)

#Define variables
Rx = zeros((2*n-1,2))       #The x values of nR
Ry = zeros((2*n-1,2))       #The y values of nR
lambdaa = zeros((2*n-1,2))  #The lambda used when adding polongs on the curve
x=  zeros((n,2),dtype=long)
y=  zeros((n,2),dtype=long)     #x,y and z as in the thesis
z=  zeros((n,2),dtype=long)
p_2 = zeros((n,2),dtype=long)   #the sum of x,y and z, for scaling
an= zeros((n,2),dtype=long)
bn= zeros((n,2),dtype=long)     #an,bn,cn are the sides of a rational triangle
cn= zeros((n,2),dtype=long)
l=  [0] * n                 #helping variable when computing common divisor
aa= [0] * n
bb= [0] * n                 #aa,bb,cc are the sides of a Heron triangle
cc= [0] * n

#Define R
Rx[0,:]=sub(8,mult(8,s))
Ry[0,:]=sub(mult(mult(8,s),s),8)
```

```

#Define a and b in the polynomial y^2=x^3+ax^2+bx+c
a= sub(mult(mult(s,s),mult(add(s,1),add(s,1))),mult(12,mult(sub(s,1),sub(s,1))))
b= mult(48,mult(mult(mult(sub(s,1),sub(s,1)),sub(s,1)),sub(s,1)))

#Computing (2n-1)R by repedeatley adding R
for i in range(0,2*n-2):
    if i==0:
        lambdaa[i,:]=div(add(add(mult(3,mult(Rx[0,:],Rx[0,:])),mult(mult(2,a),\
               Rx[0,:])),b),mult(2,Ry[0,:]))
        Rx[i+1,:]=sub(mult(lambdaa[i,:],lambdaa[i,:]),add(mult(2,Rx[0,:]),a))
    else:
        lambdaa[i,:]=div(sub(Ry[i,:],Ry[0,:]),sub(Rx[i,:],Rx[0,:]))
        Rx[i+1,:]=sub(sub(sub(mult(lambdaa[i,:],lambdaa[i,:]),Rx[i,:]),Rx[0,:]),a)

    Ry[i+1,:]=sub(0,add(mult(lambdaa[i,:],sub(Rx[i+1,:],Rx[0,:])),Ry[0,:]))
    i = i+1

#Changing the odd multiples of R to (x,y,z) and then to (an,bn,cn)
for i in range(0,n):
    x[i,:]=add(mult(mult(mult(-1,s),add(s,1)),Rx[2*i,:]),Ry[2*i,:])  #computing x
    y[i,:]=sub(mult(mult(mult(-1,s),add(s,1)),Rx[2*i,:]),Ry[2*i,:])  #computing y
    z[i,:]=mult(mult(mult(8,mult(sub(s,1),sub(s,1))),s),add(s,1))    #computing z
    p_2[i,:]=add(add(x[i,:],y[i,:]),z[i,:])          #computing x+y+z for scaling
    an[i,:]=div(sub(p_2[i,:],x[i,:]),(p_2[i,:]))     #computing an
    bn[i,:]=div(sub(p_2[i,:],y[i,:]),(p_2[i,:]))     #computing bn
    cn[i,:]=div(sub(p_2[i,:],z[i,:]),(p_2[i,:]))     #computing cn

#Compute the common divisor of all an,bn and cn.
for i in range(0,n):
    l[i]=lcm(lcm(an[i,1],bn[i,1]),cn[i,1])
    L=1
for i in range(0,n):
    L=lcm(L,l[i])
L=long(L)

#Multiplying the rational sides (an,bn,cn) with the common divior to get integer sides (aa,bb,cc)
for i in range(0,n):
    aa[i]=long(an[i,0])*(L/long(an[i,1]))
    bb[i]=long(bn[i,0])*(L/long(bn[i,1]))
    cc[i]=long(cn[i,0])*(L/long(cn[i,1]))
```

B An example of a 6-tuple

This table shows us the Heron triangles generated by our script for $s = 2$. Only the first four are actually Heron, while the last two have irrational area. This is due to round off errors when using a script for computing the triangles. This page has a sideways layout, so that the table can fit on a single page. Our script can be used to generate larger tuples, but then the the results will no longer fit on this page. It is also likely that the round-off errors will only get larger as we generate larger tuples.

a	b	c
227923701560191955421494599620372336899202081323306385	379872835933653259035824332700620561498670135538843975	303898268746922607228659466160496449198936108431075180
365401489802847420596364358121549302013006511327840395	207663816977063781606250635209672573619273007427901373	338629499460856619483363405150267471964528806537483772
262203638393790978173823755406892252956167951712203685	384743784111476945852596583566117719759857365694401155	264747383735499897659558059508479374880783007886620700
340624477399927779558578761678755476742714384552231375	206983173569114288255624328278308984512195083284929705	364087155271725753871775308524424886341898857456064460
301370687544486355257600240988786205307804281116146510	380481399370835746272657477547085501071562437514931510	229842719325445720155720679945617641217441606662147520
306405002032704575981208756247674685967399162572168050	226067242569808406851646604197087346342525084868131570	379222561638254838853123038036727315286884077852925920

References

[1] Andrew Bremner. On heron triangles. In *Annales Mathematicae et Informaticae*, volume 33, pages 15–21. Eszterházy Károly College, Institute of Mathematics and Computer Science, 2006.

[2] Ralph H Buchholz and Randall L Rathbun. An infinite set of heron triangles with two rational medians. *The American mathematical monthly*, 104(2):107–115, 1997.

[3] Richard Guy. *Unsolved problems in number theory*, volume 1. Springer Science & Business Media, 2013.

[4] Alpar-Vajk Kramer and Florian Luca. Some remarks on heron triangles. *Acta Acad. Paedagog. Agriensis, Sect. Mat.(NS)*, 27:25–38, 2000.

[5] Louis Joel Mordell. On the rational resolutions of the indeterminate equations of the third and fourth degree. In *Proc. Cambridge Phil. Soc.*, volume 21, pages 179–192, 1922.

[6] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[7] Ronald van Luijk. Private communication, 7th march, 2018.

[8] Ronald van Luijk. An elliptic K3 surface associated to Heron triangles. *Journal of Number Theory*, 123(1):92–119, mar 2007.