University of California,
Santa Barbara

Senior Thesis

Moduli of Euclidean Triangle Curves

Author:
Jason Murphy

Supervisor:
Dr. Jordan Schettler

September 12, 2015

Abstract

We investigate an invariant, called k^2, associated to elliptic curves over the complex numbers. Like the well-known j-invariant, the k^2-invariant can be regarded as a function on the complex upper half plane, and, as such, it is modular with respect to the congruence subgroup $\Gamma_0(3)$. In fact, k^2 generates the function field of the associated modular curve $X_0(3)$. Certain rational values of k^2 come from curves which parameterize triangles having rational side lengths, fixed area, and fixed perimeter. There are many questions about what the analytic and algebraic properties of k^2 imply for the families of triangles, and we explore some of them in the following report.

FIGURE 1: The k^2-invariant as a function on the complex upper-half plane $\mathfrak{h}$.

Contents

Chapter 1

Curves Arising from Euclidean Triangles

1.1 Construction

We begin by posing a seemingly innocent question from Euclidean geometry: if two triangles have the same area and perimeter, are they necessarily congruent? The answer to this question is no, but the more interesting part of this answer is that all triangles sharing the same perimeter and the same area can be parametrized by points on a certain family of elliptic curves (over a suitably defined field), which we refer to as the family of **triangle curves**. In particular, we have the following:

Theorem 1.1. *(Brody-Schettler) Let $\mathscr{T}_{A,P}$ denote the set of all triples $(\ell_1, \ell_2, \ell_3) \in \mathbb{Q}^3$ representing side lengths of triangles with the same area A and perimeter P, and let $\mathscr{C}_{A,P}$ denote the set of rational points in the first quadrant on the triangle curve whose coefficients are determined by A and P. Then there exists a bijection*

$$\psi : \mathscr{C}_{s,r} \longleftrightarrow \mathscr{T}_{s,r}.$$

In order to prove this, we must first construct the family of triangle curves and make explicit the relationship between rational points on these curves and triangles with the same area and perimeter. To that end, consider the Euclidean triangle Δ in Figure 2.1.

The dashed blue lines represent the angle bisectors, which intersect in a point called the incenter. And the circle which is centered at this point is called the incircle, which lies tangent to the 3 sides of Δ. Connecting these points of tangency to the incenter, the dashed red lines determine the 3 central angles α, β and γ. Letting r denote the radius of the incircle, these central angles

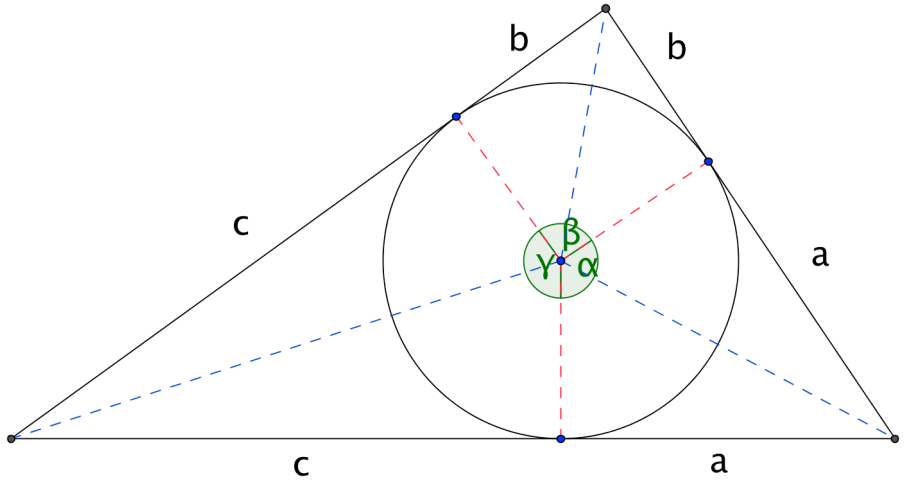

FIGURE 1.1: Partial side lengths a, b, c and central angles α, β, γ of a Euclidean triangle Δ.

then determine the partial side lengths a, b and c of Δ:

$$a = r\tan\left(\frac{\alpha}{2}\right) \qquad b = r\tan\left(\frac{\beta}{2}\right) \qquad c = r\tan\left(\frac{\gamma}{2}\right).$$

Using the triple tangent identity, we have

$$\frac{\alpha}{2} + \frac{\beta}{2} + \frac{\gamma}{2} = \pi \quad \Rightarrow \quad \tan\left(\frac{\alpha}{2}\right) + \tan\left(\frac{\beta}{2}\right) + \tan\left(\frac{\gamma}{2}\right) = \tan\left(\frac{\alpha}{2}\right)\tan\left(\frac{\beta}{2}\right)\tan\left(\frac{\gamma}{2}\right).$$

Thus, the triple tangent identity determines a relation for the side lengths:

$$abc = r^3\tan\left(\frac{\alpha}{2}\right)\tan\left(\frac{\beta}{2}\right)\tan\left(\frac{\gamma}{2}\right) = r^2\left(r\tan\left(\frac{\alpha}{2}\right) + r\tan\left(\frac{\beta}{2}\right) + r\tan\left(\frac{\gamma}{2}\right)\right) = r^2(a+b+c)$$

Letting s denote the semiperimeter of Δ (i.e. 1/2 the perimeter), we have the following two relations on the partial side lengths:

$$s = a + b + c \tag{1.1}$$

$$abc = r^2(a+b+c) \tag{1.2}$$

Solving relation (2.2) for c and plugging it into (2.1) yields

$$s = a + b + \frac{r^2(a+b)}{ab - r^2} \quad \Rightarrow \quad s(ab - r^2) = a^2b + ab^2. \tag{1.3}$$

In other words, the pair (a, b) is a point on the degree 3 curve

$$C_{r,s} : s(xy - r^2) = x^2y + xy^2.$$

We will find that this degree 3 curve will be an elliptic curve before we begin to discuss the

relationship between rational points on a family of elliptic curves and triangles with the same area and perimeter, we must first consider the following definitions and basic observations.

Definition 1.2. *A Euclidean triangle Δ is a **rational triangle** if its side lengths $\ell_1, \ell_2, \ell_3 \in \mathbb{Q}$.*

Definition 1.3. *The curve*

$$C_{r,s} : s(xy - r^2) = x^2y + xy^2$$

*will be called a **triangle curve** whenever $s > 3\sqrt{3}r > 0$.*

Remark 1.4. We can determine a Weierstrass form for $C_{r,s}$

$$E_{r,s} : Y^2 + sXY + sr^2Y = X^3$$

which is given explicitly by

$$(X, Y) = \left(\frac{sr^2}{x}, \frac{sr^2y}{x}\right).$$

The curve $E_{r,s}$ has discriminant equal to

$$\Delta_{E_{r,s}} = s^3r^6(s^3 - 27sr^2),$$

and, thus, is singular if and only if $s = 0$, $r = 0$ or $s^2 - 27r^2 = 0$ (i.e. $s = 3\sqrt{3}r$). In other words, $C_{r,s}$ is an **elliptic curve** (thus, a **triangle curve**) whenever s and r arise as the semiperimeter and inradius, respectively, of a non-equilateral triangle. In the case that s and r parametrize an equilateral triangle, then $\frac{s}{r} = 3\sqrt{3}$ and $\Delta_{E_{r,s}} = 0$; thus, $E_{r,s}$ is singular.

Definition 1.5. *Let $C_{r,s}$ be a triangle curve and define*

$$E_{r,s} : Y^2 + sXY + sr^2Y = X^3$$

*to be its **auxiliary elliptic curve**, which is in Weierstrass form.*

With the following proposition, one can more readily see the relationship between the semiperimeter s and the inraidius r of a Euclidean triangle.

Proposition 1.6. *If s and r parametrize a Euclidean triangle, then $s \geq 3\sqrt{3}r$.*

Proof: Let Δ be a Euclidean triangle with semiperimeter s, inradius r, area A and side lengths ℓ_1, ℓ_2, ℓ_3. Using the geometric-arithmetic mean inequality $\sqrt[3]{xyz} \leq \frac{x+y+z}{3}$ with $x = s - \ell_1$, $y = s - \ell_2$ and $z = s - \ell_3$, we find that

$$(s - a)(s - b)(s - c) \leq \frac{(3s - 2s)^3}{27} = \frac{s^3}{27}. \tag{1.4}$$

From **Heron's Forumula**

$$A^2 = s(s-\ell_1)(s-\ell_2)(s-\ell_3) = s^2r^2,$$

we can multiply both sides of (2.4) by s and deduce that

$$s^2r^2 = A^2 \leq \frac{s^4}{27} \quad \Rightarrow \quad 27r^2 \leq s^2,$$

as desired. □

Remark 1.7. Note that Heron's formula gives an equivalence between triangles parametrized by area A and perimeter P and triangles parametrized by semiperimeter s and inradius r. In other words, if $A = sr$ and $P = \frac{s}{2}$, then $\mathscr{T}_{A,P} = \mathscr{T}_{r,s}$. Moreover, the set $\mathscr{C}_{A,P}$ from the statement of Theorem 2.1 can be regarded as the set of rational points in the first quadrant of $C_{r,s}$.

Now suppose that Δ is a rational Euclidean triangle with semiperimeter s and inradius r satisfying $s > 3\sqrt{3}r$.

Proposition 1.8. *For any rational triangle Δ' with semiperimeter s, inradius r and side lengths ℓ_1, ℓ_2 and ℓ_3, the pair*

$$(a', b') = (s-\ell_2, s-\ell_3)$$

is a rational point on the cubic curve

$$C_{r,s} : s(xy - r^2) = x^2y + xy^2.$$

Proof: It is clear from Figure 1.1 that the partial side lengths a', b', c' of Δ' satisfy

$$a' + b' = \ell_1 \qquad b' + c' = \ell_2 \qquad c' + a' = \ell_3 \tag{1.5}$$

and so

$$a' = \frac{\ell_1 - \ell_2 + \ell_3}{2} \qquad b' = \frac{\ell_1 + \ell_2 - \ell_3}{2} \qquad c' = \frac{-\ell_1 + \ell_2 + \ell_3}{2}. \tag{1.6}$$

The partial side lengths also satisfy relations (2.1) and (2.2) and so we get the point $(a', b') = (s-\ell_2, s-\ell_3)$ on $C_{r,s}$, as desired. Furthermore, as $\ell_1, \ell_2, \ell_3 \in \mathbb{Q}$, it follows that $s, r^2 \in \mathbb{Q}$. □

Thus far, we have shown that any Euclidean triangle Δ with semiperimeter s and inradius r (or, equivalently, perimeter P and area A) can be realized as a point on the cubic curve $C_{r,s}$. However, the converse is clearly not true:

Corollary 1.9. *If $(a, b) \in \mathbb{R}^2$ is a point on $C_{r,s}$ corresponding to a Euclidean triangle Δ with semiperimeter s and inradius r, then it must be the case that $a, b > 0$.*

But if we restrict $C_{r,s}$ to the first quadrant, we can show that the converse is true.

Lemma 1.10. *Suppose $s, r^2 \in \mathbb{Q}$ with $s \geq 3\sqrt{3}r > 0$ and suppose $(x_0, y_0) \in C_{r,s}(\mathbb{Q})$ with $x_0, y_0 > 0$. Then $(x_0 + y_0, s - x_0, s - y_0)$ is a sequence of rational side lengths of a Euclidean triangle having semiperimeter s and inradius r.*

Proof: [**Bro**, p. 5] It suffices to check that

$$(x_0 + y_0) + (s - x_0) = s + y_0 > s - y_0$$

$$(x_0 + y_0) + (s - y_0) = s + x_0 > s - x_0$$

$$(s - x_0) + (s - y_0) = 2s - (x_0 + y_0) > x_0 + y_0$$

where the last inequality follows from

$$\frac{s}{x_0 + y_0} = \frac{x_0 y_0}{x_0 y_0 - r^2} > 1.$$

□

We are now in a position to prove Theorem 2.1.

Proof of Theorem 2.1: Let $s, r^2 \in \mathbb{Q}$ with $s > 3\sqrt{3}r$. In light of Remark 2.7, we have $\mathscr{T}_{A,P} = \mathscr{T}_{r,s}$ and $\mathscr{C}_{A,P} = \{(x, y) \in C_{r,s} : x, y > 0\} = \mathscr{C}_{r,s}$, so it suffices to exhibit a bijection $\mathscr{C}_{r,s} \longrightarrow \mathscr{T}_{r,s}$. Consider the assignment

$$\psi : \mathscr{C}_{r,s} \longrightarrow \mathscr{T}_{r,s}$$

$$(x_0, y_0) \longmapsto (x_0 + y_0, s - x_0, s - y_0).$$

Lemma 2.10 implies that ψ does, in fact, map into $\mathscr{T}_{r,s}$ and Proposition 2.7 implies that ψ is surjective. To see that ψ is injective, simply observe that

$$(x_0 + y_0, s - x_0, s - y_0) = (x_0' + y_0', s - x_0', s - y_0') \quad \Rightarrow \quad (x_0, y_0) = (x_0', y_0').$$

□

1.2 Basic Properties

In order to talk about the family of triangle curves as a family of elliptic curves, we must first specify a designated point at infinity O. From there, we can begin to explore such questions as what the torsion subgroups of triangle curves look like and how they might be related to the geometry of the triangles from which they arise.

1.2.1 Points at Infinity and the Group Law

We can homogenize $C_{r,s}$ to view it as a curve in $\mathbb{P}^2(\mathbb{C})$ with projective coordinates $[X : Y : Z]$:

$$C_{r,s} : X^2Y + XY^2 = s(XYZ - r^2Z^3).$$

In this regime the points at infinity on $C_{r,s}$ correspond to the points on $C_{r,s}$ with $Z = 0$, which is to say the points $[X : Y : 0] \in \mathbb{P}^2(\mathbb{C})$ satisfying

$$X^2Y + XY^2 = XY(X + Y) = 0.$$

Clearly, these points are $[1 : 0 : 0]$, $[0 : 1 : 0]$ and $[1 : -1 : 0]$.

Corollary 1.11. *Points at infinity on the curve $C_{r,s}$ correspond, in projective coordinates to* $[1 : 0 : 0]$, $[0 : 1 : 0]$ *and* $[1 : -1 : 0]$.

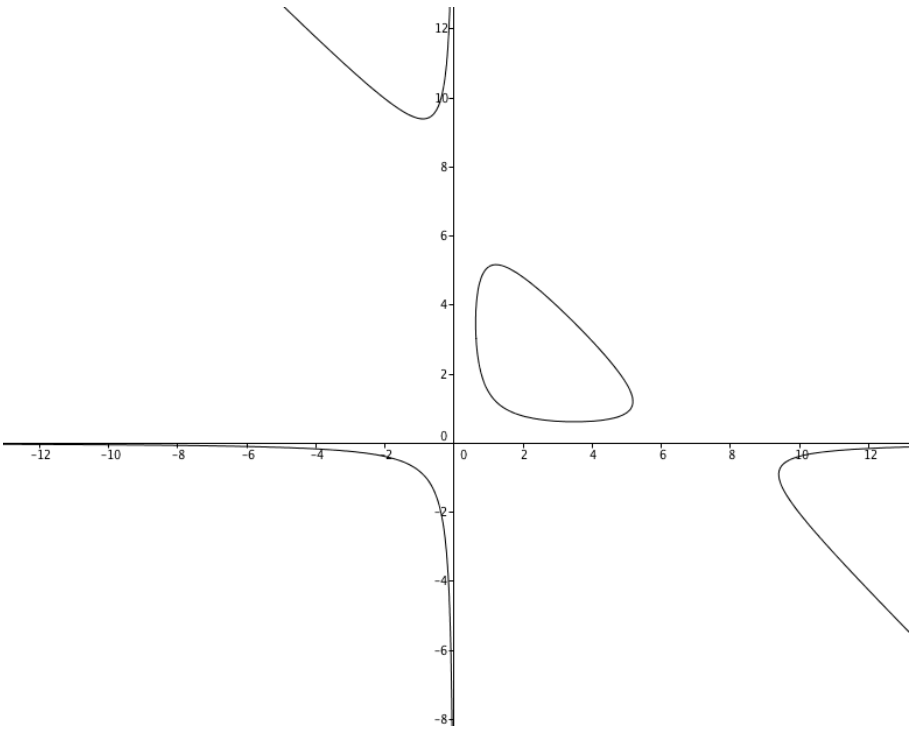

FIGURE 1.2: Graph of generic $C_{r,s}$ with $s > 3\sqrt{3}r > 0$.

In Figure 1.2, one can see what these points at infinity look like with respect to the graph of $C_{r,s}$: the projective point $[1 : 0 : 0]$ corresponds to the line $y = 0$ in the affine real plane, the point $[0 : 1 : 0]$ to the line $x = 0$ and the point $[1 : -1 : 0]$ to the line $y = -x$.

If we choose the point $O = [1 : -1 : 0]$, then we have a natural group law on the points of $C_{r,s}$ in the affine real plane using a tangent/chord construction not unlike that of a real elliptic curve in Weierstrass form:

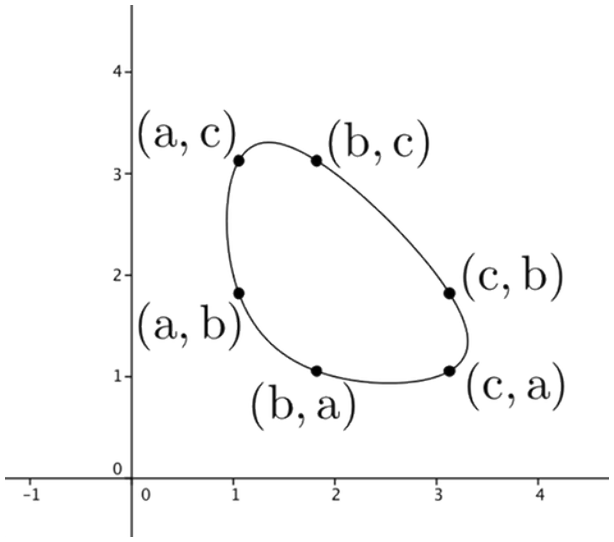

FIGURE 1.3: The (up to) six points on $C_{r,s}$ coming from Δ

- **Case 1:** Take any two distinct points $P, Q \in C_{r,s}(\mathbb{R})$ and draw the line line between them, which will be secant to $C_{r,s}$. By Bezout's Theorem, this line will intersect the curve in precisely one more point, which we call $P * Q \in C_{r,s}(\mathbb{R})$. Reflecting this point over the line $y = x$ in the affine real plane then yields the point $P + Q$.

- **Case 2:** Take a point $P \in C_{r,s}(\mathbb{R})$ and draw the line tangent to P on $C_{r,s}$. By Bezout's Theorem, this line will intersect the curve in precisely one more point, $P * P \in C_{r,s}(\mathbb{R})$. Reflecting this point over the line $y = x$ in the affine real plane then yields the point $P + P$.

Using this group law for a triangle curve $C_{r,s}$, we note that we always have the identity:

$$[1 : 0 : 0] + [0 : 1 : 0] = [1 : -1 : 0].$$

Which is to say that whenever $C_{r,s}$ is a triangle curve, we automatically have a subgroup of order 3. Moreover, for any rational Euclidean triangle Δ with partial side lengths $a, b, c \in \mathbb{Q}$ we can get up to 6 points on $C_{r,s}$:

And, from the tangent/chord group law, one can easily deduce the following relations:

$$-[a : b : 1] = [b : a : 1] \tag{1.7}$$

$$[a : b : 1] + [c : b : 1] = [1 : 0 : 0] \tag{1.8}$$

$$[a : b : 1] + [a : c : 1] = [0 : 1 : 0] \tag{1.9}$$

However, the for the case when Δ is an isosceles triangle, the story is slightly different.

1.2.2 Torsion Subgroups and Isosceles Triangles

Suppose Δ is a (not necessarily rational) Euclidean triangle which is isosceles with semiperimeter s and inradius r satisfying $s > 3\sqrt{3}r$. Then there are only three points on $C_{r,s}(\mathbb{R})$ arising from Δ (say, for example, $a = b$ in Figure 1.1, representing the base leg of Δ). In this case, we find that $P = (a, a) = -(a, a) = -P \in C_{r,s}(\mathbb{R})$, which is to say that the base leg of Δ will be parametrized by a point of order 2 on $C_{r,s}$.

Theorem 1.12. *The points of order 2 on $C_{r,s}$ are precisely the roots of the polynomial*

$$2x^3 - sx^2 + sr^2 = 0,$$

which are:

$$\mathbb{R} \cap \overline{\mathbb{Q}} \ni \alpha = \frac{s}{6}\left(e^{\frac{i\theta}{3}} + 1 + e^{-\frac{i\theta}{3}}\right) > 0$$

$$\mathbb{R} \cap \overline{\mathbb{Q}} \ni \beta = \frac{s}{6}\left(\omega e^{\frac{i\theta}{3}} + 1 + \omega e^{-\frac{i\theta}{3}}\right) < 0$$

$$\mathbb{R} \cap \overline{\mathbb{Q}} \ni \gamma = \frac{s}{6}\left(\omega^2 e^{\frac{i\theta}{3}} + 1 + \omega^2 e^{-\frac{i\theta}{3}}\right) > 0$$

where $\theta = \cos^{-1}\left(1 - \frac{54r^2}{s^2}\right)$ and $\omega = \frac{-1+\sqrt{-3}}{2}$. Furthermore, when $s > 3\sqrt{3}r$, the roots α and γ parametrize the isosceles triangles with semiperimeter s and inradius r.

Proof: Let $C_{r,s}$ be a triangle curve. We have that $P \in C_{r,s}(\mathbb{C})$ is a point of order 2 if and only if $P = -P$; which is to say that if $P = (x, y)$ in affine coordinates, then $-P = (y, x)$ so that $y = x$. Substituting $y = x$ in the affine equation for $C_{r,s}$ yields

$$\psi : 2x^3 - sx^2 + sr^2 = 0$$

and dividing by 2 yields the desired cubic. Taking the discriminant of the cubic yields

$$\Delta_\psi = 4s^2r^2(s^2 - 27r^2) > 0,$$

since $C_{r,s}$ is a triangle curve. Thus, ψ has 3 distinct, real roots: $\alpha, \beta, \gamma \in \mathbb{R}$. Following the approach in [**Nic**] to solving the cubic, we make the substitution $x = \frac{s}{6}(2\cos\theta + 1)$ yielding the trigonometric polynomial

$$\psi' : \frac{s^3}{54}\left(4\cos^3\theta - 3\cos\theta - \frac{54r^2}{s^2} - 1\right) = 0 \quad \Rightarrow \quad \cos 3\theta = 1 - \frac{54r^2}{s^2}.$$

Figure 1.4[1] gives a geometric description of the roots of ψ in trigonometric terms, where the angle corresponding to the first maximum on ψ is always $2\pi/3$. Thus, the three roots of the

[1] [**Nic**, p.6]

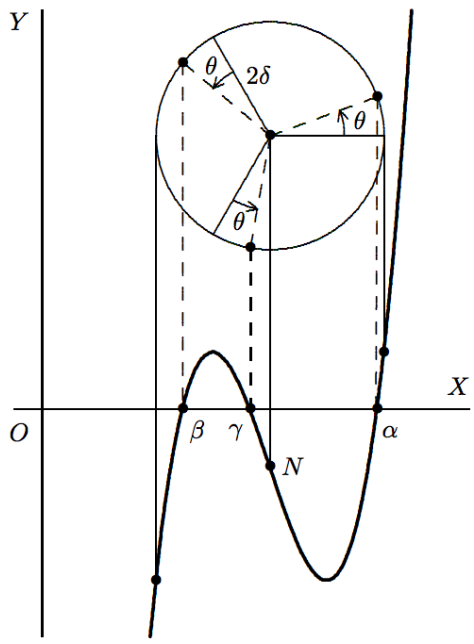

FIGURE 1.4: Geometric depiction of roots of ψ in terms of θ with $\delta = N = \frac{s}{6}$.

cubic can be parametrized by the angles $\theta, \theta + 2\pi/3, \theta - 2\pi/3$, as tripling each angle and taking its cosine will yield the same answer (namely, $1 - 54r^2/s^2$). Working backwards, we get the three roots

$$\alpha = \frac{s}{6}(2\cos\theta + 1) = \frac{s}{6}\left(e^{\frac{i\theta}{3}} + 1 + e^{-\frac{i\theta}{3}}\right),$$

$$\beta = \frac{s}{6}(2\cos(\theta + 2\pi/3) + 1) = \frac{s}{6}\left(\omega e^{\frac{i\theta}{3}} + 1 + \omega e^{-\frac{i\theta}{3}}\right),$$

$$\gamma = \frac{s}{6}(2\cos(\theta - 2\pi/3) + 1) = \frac{s}{6}\left(\omega^2 e^{\frac{i\theta}{3}} + 1 + \omega^2 e^{-\frac{i\theta}{3}}\right).$$

Moreover, the x-coordinate of the first maximum for ψ always occurs at 0, so that $\beta < 0$ and $\alpha, \gamma > 0$. Thus, α, γ always parametrize the base legs of the two isosceles triangles with semiperimeter s and inradius r. □

Remark 1.13. When $s = 6\sqrt{3}r$, then the cubic parametrizing the base legs of the isosceles triangles is a Ramanujan cubic polynomial, and the angle parametrizing the roots is $\theta = \pi/3$. In other words, the roots satisfy some very weird, albeit neat, identities (via eq. 4 in **[Wit]**):

$$\left(\cos\left(\frac{\pi}{9}\right)\right)^{1/3} + \left(\cos\left(\frac{2\pi}{9}\right)\right)^{1/3} + \left(\cos\left(\frac{5\pi}{9}\right)\right)^{1/3} = \left(\frac{3\sqrt[3]{9} + 6}{2}\right)^{1/3} \tag{1.10}$$

These are the only values for s, r for which the 2-torsion polynomial of $C_{r,s}$ is a Ramanujan cubic polynomial.

Theorem 1.14. *The point* $[1 : 0 : 0] \in C_{r,s}(\mathbb{Q})$ *is always a rational point of order 3.*

Proof: Clear from §1.2.1. □

1.2.3 Isomorphism Classes of Triangle Curves: The Parameter

Thus far, we have discussed properties of the torsion subgroups of triangle curves, relating them to the geometric properties of triangles when possible. So it makes sense at this point to talk about when two triangle curves are isomorphic as elliptic curves and try to relate that property to geometric properties of the triangles themselves.

Proposition 1.15. *Let Δ and Δ' be Euclidean triangles with semiperimeter s and s' and inradii r and r'. Then*

$$\frac{s}{r} = \frac{s'}{r'} \quad \Rightarrow \quad C_{r,s} \cong C_{r',s'}.$$

Proof: Consider the map

$$\varphi : C_{r,s} \longrightarrow C_{r',s'}$$

$$[x : y : z] \longmapsto [rx : ry : r'z].$$

□

Remark 1.16. In 1.5, we defined the auxiliary elliptic curve for $C_{r,s}$ which is nonsingular whenever $C_{r,s}$ is a triangle curve. Viewing the objects as complex projective curves, the map

$$\varphi : C_{r,s} \longrightarrow E_{r,s}$$

$$[x : y : z] \longmapsto [-sr^2 z : sr^2 y : x]$$

is an isomorphism of projective curves but not of groups:

$$\varphi\left(O_{C_{r,s}}\right) = [0 : -sr^2 : 1] \neq [0 : 1 : 0] = O_{E_{r,s}}.$$

However, if we define the translation-by-Q map

$$\tau_Q : E_{r,s} \longrightarrow E_{r,s}$$

$$[x : y : z] \longmapsto [sr^2 x : -sr^2(y + sx + sr^2 z) : y]$$

where $Q = [0 : 0 : 1]$, then the composition

$$\tau_Q \circ \varphi : C_{r,s} \longrightarrow E_{r,s}$$

satisfies

$$(\tau_Q \circ \varphi)([1 : -1 : 0]) = \tau_Q([0 : -sr^2 : 1]) = [0 : 1 : 0] = O_{E_{r,s}},$$

so that $\tau_Q \circ \varphi$ is an isogeny with trivial kerne, which is to say that we have an isomorphism of the group structure on $C_{r,s}$ with that of $E_{r,s}$ (over an algebraically closed field).

Remark 1.17. We see that Euclidean triangles will define isomorphic curves. Thus, for the purpose of constructing a moduli space for the family of triangle curves, it is enough to consider curves defined by the single parameter $k = \frac{s}{r}$. Such curves take the form

$$C_k : x^2y + xy^2 = k(xy - 1).$$

We would, ideally, like more than a sufficient condition to define the isomorphism classes of triangle curves. And this leads us to compute the j-invariant of the triangle curves C_k in Weierstrass form as a function of the parameter k.

Remark 1.18. Suppose we have a triangle curve of the form

$$x^2y + xy^2 = k(xy - 1),$$

where $k = \frac{s}{r}$. In order to transform the curve into its Weierstrass normal form, we take the homogenized curve:

$$X^2Y + XY^2 = kXYZ - kZ^3,$$

and make the substitutions

$$Y' \mapsto \frac{Y}{X} \qquad Z' \mapsto \frac{Z}{X}$$

which yields the following curve:

$$Y^2 + Y = kYZ - kZ^3.$$

We can further simplify the form this curve takes by making the substitutions

$$y' \mapsto kY' \qquad z' \mapsto -kZ',$$

which gives us the following curve:

$$y^2 + kzy + ky = z^3.$$

We can put the equation into it's final Weierstrass Normal Form by completing the square

$$y'^2 + (kz' + k)y' = \left(y' + \frac{kz' + k}{2}\right)^2 - \frac{(kz' + k)^2}{4}$$

and making the substitution $y'' \mapsto 2y' + kz' + k$:

$$y''^2 = 4z'^3 + k^2z'^2 + 2k^2z' + k^2.$$

Now that our triangle curve is in Weierstrass Normal form, we may compute its j-invariant as a rational function of k. To do this, we start by making the substitution

$$(x, y) \mapsto \left(\frac{z' - 3k^2}{36}, \frac{y''}{108}\right)$$

yielding the simpler equation

$$E : y^2 = x^3 - 27(k^4 - 24k^2)x - 54(-k^6 + 36k^4 - 216k^2).$$

Letting

$$A = -27(k^4 - 24k^2) \qquad B = 54(k^6 - 36k^4 + 216k^2)$$

we define

$$\Delta = -16(4A^3 + 27B^2)$$

and, thus, compute the j-invariant of the triangle curve E as a rational function of k to be

$$j(k) = -1728\frac{(4A)^3}{\Delta} = \frac{k^2(k^2 - 24)^3}{k^2 - 27}.$$

Remark 1.19. Now consider the following curve:

$$E_1 : y^2 = x^3 + x.$$

We can compute the j-invariant of this curve and find that it is $j_{E_1} = 1728$. We want to know what values of k in the triangle curve will produce an elliptic curve isomorphic to this one. Since all curves of the form $y^2 = x^3 + \alpha x$ will have the same j-invariant for all $\alpha \in \mathbb{Q}$, it follows that a triangle curve will be isomorphic to E_1 if and only if

$$k^4 - 36k^2 + 216 = 0$$

which implies that

$$k^2 = \frac{36 \pm \sqrt{1296 - 864}}{2} \quad \Rightarrow \quad k = \pm\sqrt{6(3 \pm \sqrt{3})}$$

Interestingly, there is only one value of k that will produce an elliptic curve isomorphic to E_1.

Chapter 2

Moduli of Euclidean Triangle Curves

In the previous chapter, we defined a family of elliptic curves arising from the parametrization of triangles with the same area and the same perimeter. Our goal in this chapter is to provide a description of the space of isomorphism classes of curves given by the parameter k^2. This collection of results is far from exhaustive, and there are also hyperbolic generalizations of $C_{r,s}$ which have yet to receive a treatment such as that presented in this chapter. Thus, we end with a brief discussion on what might be some future directions in which to take this work. We have also made extensive use of the computer algebra system Sage, and can provide any of the code written to break ground on the analysis of curves parametrizing hyperbolic triangles (such as a function to add triangles together on the hyperbolic curve and to determine linearly independent points on a Weierstrass form of the hyperbolic curves in [**Bro**]).

2.1 Hauptmoduln

Let

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \ c \equiv 0 \bmod N \right\}$$

be the principal congruence subgroups of level N and let $\mathfrak{h}$ denote the complex upper half plane and define the (left) action of the group Γ on $\mathfrak{h}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

Then the quotient $\Gamma_0(N) \setminus \mathfrak{h}$ defines a compact Riemann surface $X_0(N)$, called the principal modular curve of level N. The non-cuspidal points of this curve parametrize isomorphism classes of elliptic curves together with a cyclic subgroup of order N. In the case where $N \leq 12$,

we have that the genus of $X_0(N)$ is zero and so its function field will be generated by a single transcendental function, which is called a Hauptmodul. In this section we prove some basic properties about Hauptmoduln and the function fields which they generate.

Theorem 2.1. *A Hauptmodul will have exactly one simple zero and is uniquely determined by the location of its pole, its zero, and its (nonzero) value at another prescribed point.*

Proof: Let X be a compact, connected Riemann surface of genus 0 and let $\mathfrak{M}_X$ denote the field of meromorphic functions on X, which is of transcendence degree 1 over $\mathbb{C}$. Then X is isomorphic, as compact Riemann surfaces, to the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. Let

$$\varphi : X \longrightarrow \mathbb{P}^1(\mathbb{C})$$

denote such an isomorphism. Clearly, ψ has only one simple zero. For the second statement, let P, Q, R denote the zero, pole and nonzero value of another prescribed point on X mapped by φ and suppose $\psi : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ is any other isomorphism. Then there exists a unique linear fractional transformation γ mapping $\psi(P), \psi(Q)\psi(R)$ to $0, \infty, \varphi(R)$ and so the composition $\gamma \circ \psi \circ \varphi^{-1}$ is an automorphism of the Riemann sphere fixing the points $0, \infty, \varphi(R)$ and so is equal to the identity, which is to say $\varphi = \gamma \circ \psi$. □

Proposition 2.2. *Let f be a nonconstant meromorphic function on an algebraic curve X. Then*

$$[\mathscr{M}(X) : \mathbb{C}(f)] = deg(D),$$

where D is the divisor $div_\infty(f)$ of poles of f.

Proof: If $f \in \mathscr{M}(X)$ is a Hauptmodul then we know that $\mathbb{C}(f) = \mathscr{M}(X)$ so that the degree $[\mathscr{M}(X) : \mathbb{C}(f)] = 1 = deg(D)$, from which it follows that the number of poles of f is exactly 1. Moreover, for any meromorphic function the number of zeros equals the number of poles, so we see that f has exactly one simple zero. To see the uniqueness, suppose that we have 2 functions $f, g \in \mathscr{M}(X)$ such that $\mathbb{C}(g) = \mathscr{M}(X) = \mathbb{C}(f)$. So then there exists polynomials h_1, h_2 such that $g = h_2(f)$, $f = h_1(g)$; but then

$$g = h_2(f) = h_2(h_1(g)) \quad \Rightarrow \quad h_2 = h_1^{-1}.$$

Let $h_1 = p_1/q_1$ for polynomials p_1, q_1; then by Lüroth's Theorem we see that

$$[\mathbb{C}(x) : \mathbb{C}(h_1(x))] = 1 = \max\{deg(p_1), deg(q_1)\}$$

so that WLOG, h_1 and h_2 are Mobius transformations.

2.2 The Modular Interpretation of k^2

Recall that the set of elliptic curves which arise from Euclidean triangles and parametrized by k always contains a cyclic subgroup of order 3, namely the three points at infinity. Thus, it is natural to consider the moduli space of elliptic curves with cyclic 3-torsion subgroup, i.e. the non-cuspidal points of the principal modular curve of level 3, and compare its hauptmodul to that of k.

In the case of $X_0(3)$, we know via [**Shi**] that its field of meromorphic functions will be generated by $\mathbb{C}(j, j_3)$. A formula for $j_3(\tau)$ is known in terms of a cannonical parameter t_3 from [**Mai**], which is written in terms of the Dedekind eta function

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \qquad q = e^{2\pi i \tau}.$$

We relate these parameters to the parameter k^2 in the following

Theorem 2.3. *As a function on $\mathfrak{h}$, k^2 can be expressed as*

$$k^2 = 27 + 729q \frac{\prod_{n=1}^{\infty}(1 - q^{3n})^{12}}{\prod_{n=1}^{\infty}(1 - q^n)^{12}}$$

Proof: Let $\eta(\tau) = q^{1/24} \prod (1 - q^n)$ denote the Dedekind eta function where $q = e^{2\pi i \tau}$ and define $t = \frac{1}{27}\left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{12}$. Then the j-invariant may be written in terms of the variable t as

$$j(\tau) = \frac{27(t+1)(t+9)^3}{t^3} = \frac{\left(\left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{12} + 27\right)\left(\left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{12} + 3^5\right)^3}{\left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{36}}.$$

With a bit of algebra, we see that this expression is equivalent to

$$j(\tau) = \left(\left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{12} + 27\right)\left(1 + 3^5\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)^3$$

$$= \left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{12}\left(1 + 27\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)\left(1 + 3^5\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)^3$$

$$= \frac{\left(1 + 27\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)\left(1 + 3^5\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)^3}{\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}}$$

$$= \frac{\left(27 + 3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)\left(3 + 3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)^3}{3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}}.$$

Since we know that as a function of k,

$$j(\tau) = j(k) = \frac{k^2(k^2-24)^3}{k^2-27} = \frac{\left(27 + 3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)\left(3 + 3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}\right)^3}{3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}}$$

then it follows that we may write k^2 as a function of τ:

$$k^2(\tau) = 27 + 3^6\left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}$$

Corollary 2.4. *k^2 is a Hauptmodul for $\Gamma_0(3)$, which has index 4 in $PSL(2,\mathbb{Z})$.*

Proof: Another brute force calculation can show that

Corollary 2.5. *k^2 parametrizes all elliptic curves, up to $\mathbb{C}$-isomorphism, with a cyclic subgroup of order 3.*

Theorem 2.6. *The extension $\mathbb{C}(k^2)/\mathbb{C}(j)$ is not Galois.*

Proof: Since $\mathbb{C}(k^2)$ is a Hauptmodul for the congruence subgroup $\Gamma_0(3)$, it suffices to examine the fixed field of F_3, the field of modular functions of level 3, by $\Gamma_0(3)$. We know via Lang's Elliptic Functions that F_3 is Galois over $\mathbb{C}(j)$ (it is the splitting field of $\Phi_3(j, j(3\tau))$)and its Galois group is isomorphic to A_4, which has order 24. Since $[\mathbb{C}(k^2) : \mathbb{C}(j)] = 4$, it follows that $Gal(F_3/\mathbb{C}(k^2))$ is isomorphic to $\mathbb{Z}_3$. It is easily shown that $N_{A_4}(\mathbb{Z}_3) = \mathbb{Z}_3$ and the normal closure of $\mathbb{Z}_3$ in A_4 is all of A_4 (from which it follows that the extension $\mathbb{C}(k^2)/\mathbb{C}(j)$ is not Galois).

2.3 Conclusion

We have seen that a seeminly innocent question from high school geometry has actually some rather deep connections with several areas of mathematics all at once. Although the approach taken here is nowhere near exhaustive, we hope that we can inspire future students to think about these objects no matter what field of mathematics they may be partial to.

Appendix A

References

[Cox] D. A. Cox, Primes of the form x2 + ny2. Fermat, class field theory and complex multiplication. John Wiley and Sons, Inc., New York, 1989.

[Sil] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[Shi] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Princeton University Press, Princeton, NJ, 1994.

[Lan] Lang, S. Elliptic Functions. Addison-Wesley, Reading MA. 1973.

[Mai] Maier, Robert. On Rationally Parametrized Modular Equations. J Ramanujan Math Soc. 24 (2009), 1-73.

[Nic] A new approach to solving the cubic: Cardan's solution revealed. 1. RWD Nickalls2. The Mathematical Gazette (1993); 77 (Nov, No 480), 354?359 (jstor).

[Bro] Brody, Nicholas. Rational Hyperbolic Triangles and a Quartic Model of Elliptic Curves. (In revision) 2014.