Neuberg cubics over finite fields

N. J. Wildberger
School of Mathematics and Statistics
UNSW Sydney 2052 Australia

June 18, 2013

Abstract

The framework of universal geometry allows us to consider metrical properties of affine views of elliptic curves, even over finite fields. We show how the Neuberg cubic of triangle geometry extends to the finite field situation and provides interesting potential invariants for elliptic curves, focussing on an explicit example over $\mathbb{F}_{23}$. We also prove that tangent conics for a Weierstrass cubic are identical or disjoint.

Metrical views of cubics

This paper looks at the connection between modern Euclidean triangle geometry and the arithmetic of elliptic curves over finite fields using the framework of universal geometry (see [8]), a metrical view of algebraic geometry based on the algebraic notions of *quadrance* and *spread* rather than *distance* and *angle.* A good part of triangle geometry appears to extend to finite fields. In particular, the Neuberg cubic provides a rich organizational structure for many triangle centers and associated lines through the group law and related Desmic (linking) structure, even in a finite field. It and other triangle cubics have the potential to be useful geometrical tools for understanding elliptic curves. See [1], [2], [3], [4], [5] and [6] for background on triangle cubics.

For triangle geometers, finite fields hold potential applications to cryptography and also provide a laboratory for exploration that in many ways is more pleasant than the decimal numbers. A price to be paid, however, is that the usual tri-linear coordinate framework needs to be replaced by Cartesian or barycentric coordinates.

We begin with a brief review of the relevant notions from rational trigonometry, which allows the set-up of metrical algebraic geometry. Then we discuss the Neuberg cubic of a triangle and related centers, illustrated in a particular example over $\mathbb{F}_{23}$. We also prove that for affine cubics in Weierstrass form the tangent conics are all disjoint provided -3 is not a square in the field.

It should be noted that there is also a projective version of universal geometry (see [9]), but here we stick to the affine situation.

Laws of Rational Trigonometry

Fix a finite field $\mathbb{F}$ not of characteristic two, whose elements are called **numbers**. A **point** A is an ordered pair $[x, y]$ of numbers, that is an element of $\mathbb{F}^2$. The **quadrance** $Q(A_1, A_2)$ between points $A_1 \equiv [x_1, y_1]$ and $A_2 \equiv [x_2, y_2]$ is the number

$$Q(A_1, A_2) \equiv (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

A **line** l is an ordered proportion $\langle a : b : c \rangle$, where a and b are not both zero. This represents the equation $ax + by + c = 0$. Such a line is **null** precisely when

$$a^2 + b^2 = 0.$$

Null lines occur precisely when -1 is a square. For distinct points $A_1 = [x_1, y_1]$ and $A_2 = [x_2, y_2]$ the line passing through them both is

$$A_1A_2 = \langle y_1 - y_2 : x_2 - x_1 : x_1y_2 - x_2y_1 \rangle.$$

Two lines $l_1 \equiv \langle a_1 : b_1 : c_1 \rangle$ and $l_2 \equiv \langle a_2 : b_2 : c_2 \rangle$ are **perpendicular** precisely when

$$a_1a_2 + b_1b_2 = 0.$$

For any fixed line l and any point A, there is a unique line n passing through A and perpendicular to l, called the **altitude** from A to l. If l is a non-null line then the altitude n meets l at a unique point F, called the **foot** of the altitude. In this case we may define the **reflection of** A **in** l to be the point $\sigma_l(A)$ such that F is the midpoint of the side $\overline{A\sigma_l(A)}$. If m is another line, then the **reflection of** m **in** l is the line $\Sigma_l(m)$ with the property that the reflection in l of any point A on m lies on $\Sigma_l(m)$.

The **spread** $s(l_1, l_2)$ between non-null lines $l_1 \equiv \langle a_1 : b_1 : c_1 \rangle$ and $l_2 \equiv \langle a_2 : b_2 : c_2 \rangle$ is the number

$$s(l_1, l_2) \equiv \frac{(a_1b_2 - a_2b_1)^2}{(a_1^2 + b_1^2)(a_2^2 + b_2^2)} = 1 - \frac{(a_1a_2 + b_1b_2)^2}{(a_1^2 + b_1^2)(a_2^2 + b_2^2)}.$$

This number $s = s(l_1, l_2)$ is 0 precisely when the lines are parallel, and 1 precisely when the lines are perpendicular. It has the property that $s(1 - s)$ is a square in the field, and every such **spread number** s can be shown to be the spread between some two lines.

The spread between lines may alternatively be expressed as a ratio of quadrances: if l_1 and l_2 intersect at a point A, choose any other point B on l_1, and let C on l_2 be the foot of the altitude line from B to l_2, then

$$s(l_1, l_2) = \frac{Q(B, C)}{Q(A, B)}.$$

Reflection in a line preserves quadrance between points and spread between lines. Given three distinct points A_1, A_2 and A_3, we use the notation

$$Q_1 \equiv Q(A_2, A_3) \qquad Q_2 \equiv Q(A_1, A_3) \qquad Q_3 \equiv Q(A_1, A_2)$$

and

$$s_1 \equiv s\left(A_1A_2, A_1A_3\right) \qquad s_2 \equiv s\left(A_2A_1, A_2A_3\right) \qquad s_3 \equiv s\left(A_3A_1, A_3A_2\right).$$

A **triangle** $\overline{A_1A_2A_3}$ is a set of three non-collinear points, and is **non-null** precisely when its three lines A_1A_2, A_2A_3 and A_1A_3 are non-null. Here are the five main laws of rational trigonometry, which may be viewed as purely algebraic identities involving only rational functions.

Triple quad formula The points A_1, A_2 and A_3 are collinear precisely when

$$\left(Q_1 + Q_2 + Q_3\right)^2 = 2\left(Q_1^2 + Q_2^2 + Q_3^2\right).$$

Pythagoras' theorem The lines A_1A_3 and A_2A_3 are perpendicular precisely when

$$Q_1 + Q_2 = Q_3.$$

Spread law For a non-null triangle $\overline{A_1A_2A_3}$

$$\frac{s_1}{Q_1} = \frac{s_2}{Q_2} = \frac{s_3}{Q_3}.$$

Cross law For a non-null triangle $\overline{A_1A_2A_3}$ define the **cross** $c_3 \equiv 1 - s_3$. Then

$$\left(Q_1 + Q_2 - Q_3\right)^2 = 4Q_1Q_2c_3.$$

Triple spread formula For a non-null triangle $\overline{A_1A_2A_3}$

$$\left(s_1 + s_2 + s_3\right)^2 = 2\left(s_1^2 + s_2^2 + s_3^2\right) + 4s_1s_2s_3.$$

See [8] for proofs, and many more facts about geometry in such a purely algebraic setting.

Neuberg cubics

Many interesting points, lines, circles, parabolas, hyperbolas and cubics have been associated to a triangle in the plane, such as the centroid G, orthocenter O, circumcenter C, incenter I, Euler line e (which passes through O, G and C), nine-point circle and so on. Perhaps the most remarkable of these is the *Neuberg cubic*, which in the earlier literature was called the 32 point cubic, but these days is known to pass through many more triangle centers (see [4], [5], [6]). Most such objects depend crucially on a metrical structure on the affine plane.

Figure 1 shows the Neuberg cubic for the triangle $\overline{A_1A_2A_3}$ with vertices $A_1 = [0,0]$, $A_2 = [1,0]$ and $A_3 = [3/4, 3/4]$. For this triangle the Euler line, which passes through the orthocenter O and the circumcenter C, is horizontal. Various incenters I_i are shown, as well as reflections of the vertices in the sides. These are just a few of the many points on the Neuberg cubic. Note that the

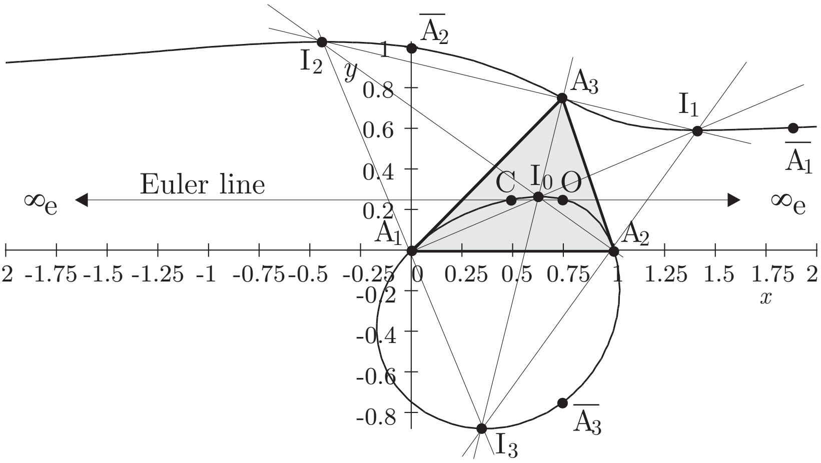

Figure 1: Neuberg cubic for $A_1 = [0, 0]$, $A_2 = [1, 0]$ and $A_3 = [3/4, 3/4]$

tangents to the four incenters are also horizontal, and it turns out that the asymptote of the cubic is also.

With the completely algebraic language of rational trigonometry, we consider such a picture for *triangles in finite fields.* For this it will be convenient to alter the usual point of view somewhat, elevating the quadrangle $\overline{I_0I_1I_2I_3}$ of *incenters* to a primary position. This ensures that the reference triangle $\overline{A_1A_2A_3}$ actually has vertex bisectors.

For a triangle $\overline{I_1I_2I_3}$ the altitudes from each point to the opposite side intersect at the orthocenter, which we here denote I_0. In terms of Cartesian coordinates $I_j = [x_j, y_j]$,

$$x_0 \equiv \frac{\begin{pmatrix} x_1x_2y_2 - x_1x_3y_3 + x_2x_3y_3 - x_3x_2y_2 + x_3x_1y_1 - x_2x_1y_1 \\ +y_1y_2^2 - y_1y_3^2 + y_2y_3^2 - y_3y_2^2 + y_3y_1^2 - y_2y_1^2 \end{pmatrix}}{x_1y_2 - x_1y_3 + x_2y_3 - x_3y_2 + x_3y_1 - x_2y_1}$$

and

$$y_0 \equiv \frac{\begin{pmatrix} x_1y_1y_2 - x_1y_1y_3 + x_2y_2y_3 - x_3y_3y_2 + x_3y_3y_1 - x_2y_2y_1 \\ +x_1^2x_2 - x_1^2x_3 + x_2^2x_3 - x_3^2x_2 + x_3^2x_1 - x_2^2x_1 \end{pmatrix}}{x_1y_2 - x_1y_3 + x_2y_3 - x_3y_2 + x_3y_1 - x_2y_1}.$$

In terms of barycentric coordinates, if the quadrances of the triangle $\overline{I_1I_2I_3}$ are R_1, R_2 and R_3 and

$$\begin{aligned} \mathcal{A} &= (R_1 + R_2 + R_3)^2 - 2\left(R_1^2 + R_2^2 + R_3^3\right) \\ &= 4\left(x_1y_2 - x_1y_3 + x_2y_3 - x_3y_2 + x_3y_1 - x_2y_1\right)^2 \end{aligned}$$

is the **quadrea** of the triangle (sixteen times the square of the area in the decimal number situation), then $I_0 = \beta_1 I_1 + \beta_2 I_2 + \beta_3 I_3$ where

$$\begin{aligned}\beta_1 &\equiv \left(R_3 + R_1 - R_2\right)\left(R_1 + R_2 - R_3\right)/\mathcal{A} \\ \beta_2 &\equiv \left(R_1 + R_2 - R_3\right)\left(R_2 + R_3 - R_1\right)/\mathcal{A} \\ \beta_3 &\equiv \left(R_2 + R_3 - R_1\right)\left(R_3 + R_1 - R_2\right)/\mathcal{A}.\end{aligned}$$

If $\overline{I_1 I_2 I_3}$ is non-null, which we henceforth assume, then the feet of its altitudes exist and we call them respectively A_1, A_2 and A_3. Thus for example I_1, I_0 and A_1 are collinear points which lie on a line perpendicular to $I_2 I_3$. In the quadrangle $\overline{I_1 I_2 I_3 I_4}$ we have a complete symmetry between the four points I_0, I_1, I_2 and I_3. So we could have started with any three of these points, and the orthocenter of such a triangle would have been the fourth point, with the **orthic triangle** $\overline{A_1 A_2 A_3}$ obtained always the same.

Theorem 1 (Orthic triangle) *The lines $I_0 I_1$ and $I_2 I_3$ are bisectors of the vertex of $\overline{A_1 A_2 A_3}$ at A_1, in the sense that*

$$\begin{aligned}s\left(I_0 I_1, A_1 A_2\right) &= s\left(I_0 I_1, A_1 A_3\right) \\ s\left(I_2 I_3, A_1 A_2\right) &= s\left(I_2 I_3, A_1 A_3\right).\end{aligned}$$

The proof uses a computer, and one can further verify that the former spread is

$$\frac{\left(x_2 x_3 - x_1 x_3 - x_1 x_2 - y_1 y_2 - y_1 y_3 + y_2 y_3 + x_1^2 + y_1^2\right)^2}{R_2 R_3}$$

while the latter spread is

$$\frac{\left(x_1 y_2 - x_1 y_3 + x_2 y_3 - x_3 y_2 + x_3 y_1 - x_2 y_1 + x_3 y_2\right)^2}{R_2 R_3}.$$

These two spreads sum to 1, as they must since $I_0 I_1$ and $I_2 I_3$ are perpendicular. So the triangle $\overline{A_1 A_2 A_3}$ has a special property: each of its vertices has bisectors. Over the decimal numbers, every triangle has vertex bisectors, but in [8] it is shown that in general this amounts to the condition that the spreads of the triangle are *squares*.

For a point P, let P_1, P_2 and P_3 denote its reflections in the sides $A_2 A_3$, $A_1 A_3$ and $A_1 A_2$ respectively, and define the **Neuberg cubic** N_c of $\overline{A_1 A_2 A_3}$ to be the locus of points P such that P_1, P_2 and P_3 are perspective with A_1, A_2 and A_3 respectively: in other words that $P_1 A_1, P_2 A_2$ and $P_3 A_3$ are concurrent lines.

An example over $\mathbb{F}_{23}$

We work in the prime field $\mathbb{F}_{23}$, in which the squares are $1, 4, 9, 16, 2, 13, 3, 18, 12, 8$ and 6. Note that -1 is not a square, but that $3 = 7^2$ is a square. The latter fact implies that equilateral triangles exist in $\mathbb{F}_{23}^2$. Let

$$I_1 = [6, 4] \qquad I_2 = [22, 22] \qquad I_3 = [21, 12].$$

These points have been chosen so that the orthocenter of $\overline{I_1 I_2 I_3}$ is $I_0 = [0, 0]$. The feet of the altitudes are

$$A_1 = [13, 1] \qquad A_2 = [5, 5] \qquad A_3 = [2, 11] .$$

The lines of $\overline{A_1 A_2 A_3}$ are

$$A_1 A_2 = \langle 3 : 6 : 1 \rangle \qquad A_2 A_3 = \langle 6 : 3 : 1 \rangle \qquad A_1 A_2 = \langle 12 : 4 : 1 \rangle$$

and the spreads of the triangle $\overline{A_1 A_2 A_3}$ are

$$s_1 = 12 \qquad s_2 = 16 \qquad s_3 = 6.$$

Note that as expected these numbers are squares, and one can check that

$$\begin{aligned} s\left(A_1 I_0, A_1 A_2\right) &= s\left(A_1 I_0, A_1 A_3\right) = 5 \\ s\left(A_2 I_0, A_2 A_1\right) &= s\left(A_2 I_0, A_2 A_3\right) = -6 \\ s\left(A_3 I_0, A_3 A_1\right) &= s\left(A_3 I_0, A_3 A_2\right) = -7. \end{aligned}$$

The connection between for example the spread $s = 5$ and the spread of its 'double' $r = 12$ is given by the *second spread polynomial*,

$$r = S_2\left(s\right) = 4s\left(1 - s\right)$$

which in chaos theory is known as the *logistic map*. The spread polynomials have many remarkable properties that hold also over finite fields, see [8].

We need the following formula for a reflection.

Theorem 2 (Reflection of a point in a line) *If $l \equiv \langle a : b : c \rangle$ is a non-null line and $A \equiv [x, y]$, then*

$$\sigma_l\left(A\right) = \left[\frac{\left(b^2 - a^2\right)x - 2aby - 2ac}{a^2 + b^2}, \frac{-2abx + \left(a^2 - b^2\right)y - 2bc}{a^2 + b^2}\right].$$

Using this, the reflections of $P = [x, y]$ in the sides of $\overline{A_1 A_2 A_3}$ are

$$\begin{aligned} P_1 &= [4x + 13y + 12, 13x + 19y + 6] \\ P_2 &= [13x + 4y + 1, 4x + 10y + 8] \\ P_3 &= [19x + 13y + 6, 13x + 4y + 12] . \end{aligned}$$

The lines $P_1 A_1, P_2 A_2$ and $P_3 A_3$ are then

$$\begin{aligned} &\langle 13x + 19y + 5 : 19x + 10y + 1 : 19x + 19y + 3 \rangle \\ &\langle 4x + 10y + 3; 10x + 19y + 4 : 22x + 16y + 11 \rangle \\ &\langle 13x + 4y + 1 : 4x + 10y + 19 : 22x + 20y + 19 \rangle \end{aligned}$$

and these are concurrent precisely when

$$\begin{vmatrix} 13x+19y+5 & 19x+10y+1 & 19x+19y+3 \\ 4x+10y+3 & 10x+19y+4 & 22x+16y+11 \\ 13x+4y+1 & 4x+10y+19 & 22x+20y+19 \end{vmatrix} = 0.$$

Expanding gives the Neuberg cubic $\overline{A_1A_2A_3}$: an affine curve over $\mathbb{F}_{23}$ with equation

$$y^3 + x^2y + 22y^2 + 7xy + 9x^2 + 13y = 0. \tag{1}$$

The tangent line to a point $[a, b]$ on the curve has equation

$$x\left(18a + 7b + 2ab\right) + y\left(7a + 21b + a^2 + 3b^2 + 13\right) + 3b + 7ab + 9a^2 + 22b^2 = 0.$$

There is another revealing way to obtain the Neuberg cubic.

Theorem 3 (Reflection of a line in a line) *The reflection in the non-null line $l \equiv \langle a : b : c \rangle$ sends $\langle a_1 : b_1 : c_1 \rangle$ to*

$$\left\langle \left(a^2 - b^2\right) a_1 + 2abb_1 : 2aba_1 - \left(a^2 - b^2\right) b_1 : 2aca_1 + 2bcb_1 - \left(a^2 + b^2\right) c_1 \right\rangle.$$

In a triangle with vertex bisectors, the reflection of a line through a given vertex in either of the vertex bisectors at that vertex is the same.

Theorem 4 (Isogonal conjugates) *If a triangle $\overline{A_1A_2A_3}$ has vertex bisectors at each vertex, then for any point P the reflections of A_1P, A_2P and A_3P in the vertex bisectors at A_1, A_2 and A_3 respectively are concurrent.*

The point of concurrence of these lines is P^*, the **isogonal conjugate** of $P = [x, y]$. The proof again is a calculation using coordinates. We may use the reflection of a line in a line theorem to establish a precise formula for P^* in the special case of our example reference triangle $\overline{A_1A_2A_3}$:

$$P^* = \left[\frac{2x + 22xy + 2x^2 + 17y^2}{4x + 20y + 5x^2 + 5y^2 + 21}, \frac{2y + 15xy + x^2 + 2y^2}{4x + 20y + 5x^2 + 5y^2 + 21}\right].$$

Over the decimal numbers, the Neuberg cubic is *also* the locus of those $P = [x, y]$ such that PP^* is parallel to the Euler line. We can verify this also in our finite example, since this condition amounts to

$$y = \frac{2y + 15xy + x^2 + 2y^2}{4x + 20y + 5x^2 + 5y^2 + 21}$$

which in turn is equivalent to the equation (1) of N_c. It follows that if P lies on N_c, then so does P^*—this is a useful way to obtain new points from old ones. In fact the Euler line is parallel to the tangent to N_c at the infinite point ∞_e.

The cubic (1) is nonsingular, has 27 points lying on it, and its projective extension has one more point at infinity, namely $\infty_e = [1:0:0]$. Here are all the points, the notation will be explained more fully below:

$[0,0] = I_0$	$[0,8] = E_3'$	$[0,16] = S'$	$[2,11] = A_3$
$[3,13] = S = \overline{A_3}$	$[4,5]$	$[5,5] = A_2$	$[5,14] = \infty_e^*$
$[6,4] = I_1$	$[7,1]$	$[7,2] = E_2'$	$[7,21] = O$
$[8,10] = \overline{A_1} = E_2$	$[13,1] = A_1$	$[13,7]$	$[13,16] = F'$
$[14,9]$	$[16,11]$	$[17,7] = E_1'$	$[17,8]$
$[17,9] = \overline{A_2} = E_1$	$[18,21] = C = E_3$	$[19,13] = F$	$[21,2]$
$[21,10]$	$[21,12] = I_3$	$[22,22] = I_2$	$[1:0:0] = \infty_e$

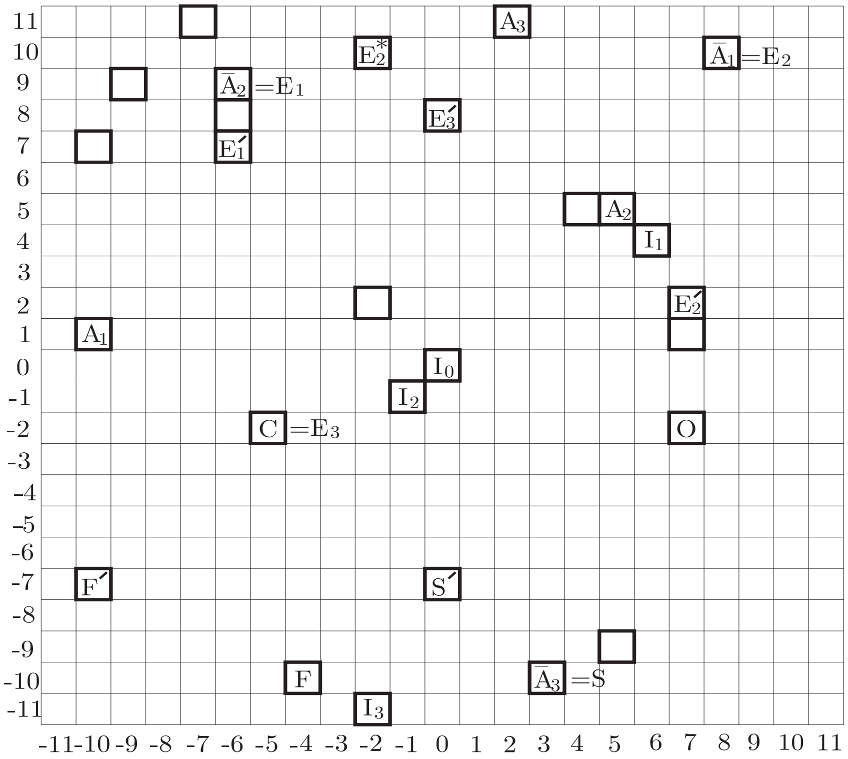

Figure 2: The Neuberg cubic for $A_1 = [13,1]$, $A_2 = [5,5,]$ and $A_3 = [2,11]$

To define the group structure on the cubic, define $X \star Y$ to be the (third) intersection of the line XY with the (projective) cubic, so that for example

$$I_0 \star I_0 = \infty_e.$$

We choose the base point of the group structure to be the point I_0. Then define

$$X \cdot Y = (X \star Y) \star I_0$$

with inverse

$$X^{-1} = X \star (I_0 \star I_0) = X \star \infty_e = X^*.$$

So we are writing the group multiplicatively, and note that I_0 is not a flex, so that X, Y and Z collinear is equivalent to $X \cdot Y \cdot Z = \infty_e$, not $X \cdot Y \cdot Z = I_0$. Furthermore X is of order two when $X \star X = \infty_e$ and X is not I_0, which happens when X is I_1, I_2 or I_3, and the four incenters form a Klein 4-group.

The triangle $\overline{A_1A_2A_3}$ can be recovered from the Neuberg cubic by first finding the asymptote (tangent to the point at infinity), then finding the four points $\overline{I_0I_1I_2I_3}$ on the cubic with a tangent parallel to this asymptote, and then taking the orthic triangle of any three of them. This can all be done algebraically using the group law, since $I_j \star I_j = \infty_e$ and $A_1 = I_2 \star I_3$ etc.

Points on the Neuberg cubic

Not only is the Neuberg cubic defined metrically, but it also has many points on it that are metrical in nature. More than a hundred are known, we will illustrate some of these for our example. The Neuberg cubic N_c of $\overline{A_1A_2A_3}$ first of all passes through A_1, A_2 and A_3. It also passes through the reflections of these points in the sides of the triangle, in this case

$$\overline{A_1} = [8, 10] \qquad \overline{A_2} = [17, 9] \qquad \overline{A_3} = [3, 13].$$

It also passes through the four incenters I_0, I_1, I_2 and I_3 of $\overline{A_1A_2A_3}$. In a general field there is no notion of 'interior point', so these four incenters should be regarded symmetrically. The Neuberg cubic passes through the orthocenter $O = [7, 21]$ and the circumcenter $C = [18, 21]$ of $\overline{A_1A_2A_3}$, and these are isogonal conjugates, that is

$$O^* = C.$$

The line OC is the Euler line e of $\overline{A_1A_2A_3}$ and it has equation $y = 21$, so that it is horizontal and passes through the infinite point $\infty_e = [1 : 0 : 0]$. Note that

$$\infty_e^* = [5, 14].$$

Since $3 = 7^2$ is a square, on any side of $\overline{A_1A_2A_3}$ we may create two equilateral triangles, for example on the side containing $A_1 = [13, 1]$ and $A_3 = [2, 11]$ we can choose a third point

$$[13 + 2, 1 + 11]/2 \pm \frac{7}{2}[1 - 11, 2 - 13]$$

namely

$$E_2 = [8, 10] \qquad \text{or} \qquad E_2' = [7, 2].$$

Thus $\overline{A_1A_3E_2}$ and $\overline{A_1A_3E_2'}$ are equilateral triangles with

$$Q(A_1, A_3) = Q(A_1, E_2) = Q(A_3, E_2) = Q(A_1, E_2') = Q(A_3, E_2') = 14.$$

As opposed to the case over the decimal numbers, there seems to be no obvious notion of these triangles being either 'exterior' or 'interior' to $\overline{A_1A_2A_3}$. Using all three sides gives the six points

$$\begin{array}{ccc} E_1 = [17,9] & E_2 = [8,10] & E_3 = [18,21] \\ E_1' = [13,7] & E_2' = [7,2] & E_3' = [0,8] \end{array}$$

and their isogonal conjugates

$$\begin{array}{ccc} E_1^* = [14,9] & E_2^* = [21,10] & E_3^* = [7,21] \\ E_1'^* = [17,7] & E_2'^* = [21,2] & E_3'^* = [17,8]\,. \end{array}$$

All twelve of these points lie on the Neuberg cubic. Yet the centroids of the six equilateral triangles thus formed are

$$\begin{array}{ccc} G_1 = [8,16] & G_2 = [0,15] & G_3 = [12,9] \\ G_1' = [22,0] & G_2' = [15,20] & G_3' = [6,20] \end{array}$$

and you may check that

$$\begin{aligned} Q\left(G_1,G_2\right) &= Q\left(G_2,G_3\right) = Q\left(G_1,G_3\right) = 19 \\ Q\left(G_1',G_2'\right) &= Q\left(G_2',G_3'\right) = Q\left(G_1',G_3'\right) = 12 \end{aligned}$$

so that Napolean's theorem that the centroids of both 'external' and 'internal' equilateral triangles themselves form an equilateral triangle seems to hold. It seems curious that the six points E_i and E_j' are thereby divided naturally into two groups.

The Fermat points of a triangle may be defined over the decimal numbers as the perspectors of the 'external and internal equilateral triangles', and with the above interpretation, these points exist also in this field. There is another approach to their definition. The vertex bisectors at A_1 of $\overline{A_1A_2A_3}$ intersect A_2A_3 at the points $X_1 = [20,21]$ and $Y_1 = [12,14]$. The circle through these points with center the midpoint of $\overline{X_1Y_1}$ has equation $(x-16)^2 + (y-6)^2 = 11$ and is called an **Apollonius circle** of $\overline{A_1A_2A_3}$. There is also such a circle starting with A_2, with equation $(x-1)^2 + (y-14)^2 = 5$ and one starting with A_3, with equation $(x-4)^2 + (y-17)^2 = 17$. These three Appollonius circles intersect at two points, called the **isodynamic points** of $\overline{A_1A_2A_3}$, given by

$$S = [3,13] \qquad \text{and} \qquad S' = [0,16]\,.$$

The Neuberg cubic passes through the two isodynamic points. The centres of the three Appollonius circles are collinear, and lie on the **Lemoine line** with equation $16x + 7y + 1 = 0$.

The isogonal conjugates of the isodynamic points are the **Fermat points**

$$F = S^* = [19,13] \qquad \text{and} \qquad F' = (S')^* = [13,16]\,.$$

It may be checked that F is also the centre of perspectivity between $\overline{A_1A_2A_3}$ and $\overline{E_1E_2E_3}$, while F' is the centre of perspectivity between $\overline{A_1A_2A_3}$ and $\overline{E_1'E_2'E_3'}$.

It may be remarked that in the decimal number plane, the Fermat points also have an interpretation in terms of minimizing the sum of the distances to the vertices of the triangle, but this kind of statement cannot be expected to have a simple analog in universal geometry.

The **Brocard line** with equation $10x + 10y + 1 = 0$ passes through the circumcenter $C = [18, 21]$, the **symmedian point** $K = G^* = [10, 6]$ and the two isodynamic points S and S'. It is perpendicular to the Lemoine line.

Quadrangles and Desmic structure

Elliptic curves naturally give rise to interesting configurations of 12 points and 16 lines, called by John Conway *Desmic (or linking) structure,* where each line passes through three points and each point lies on four lines (see [7]). To describe this situation, begin with a triangle ABC and two generic points P and Q. Then define

$$\begin{array}{lll} A' = (BP)\,(CQ) & B' = (CP)\,(AQ) & C' = (AP)\,(BQ) \\ A'' = (BQ)\,(CP) & B'' = (CQ)\,(AP) & C'' = (AQ)\,(BP) \end{array}$$

This insures that $\overline{ABC}$ and $\overline{A'B'C'}$ are perspective from some perspector D'', that $\overline{A'B'C'}$ and $\overline{A''B''C''}$ are perspective from some perspector D and that $\overline{A''B''C''}$ and $\overline{ABC}$ are perspective from some perspector D'. Furthermore the points D, D' and D'' are collinear.

Put another way, two triangles which are doubly perspective are triply perspective (essentially a consequence of Pappus' theorem). The various collinear-

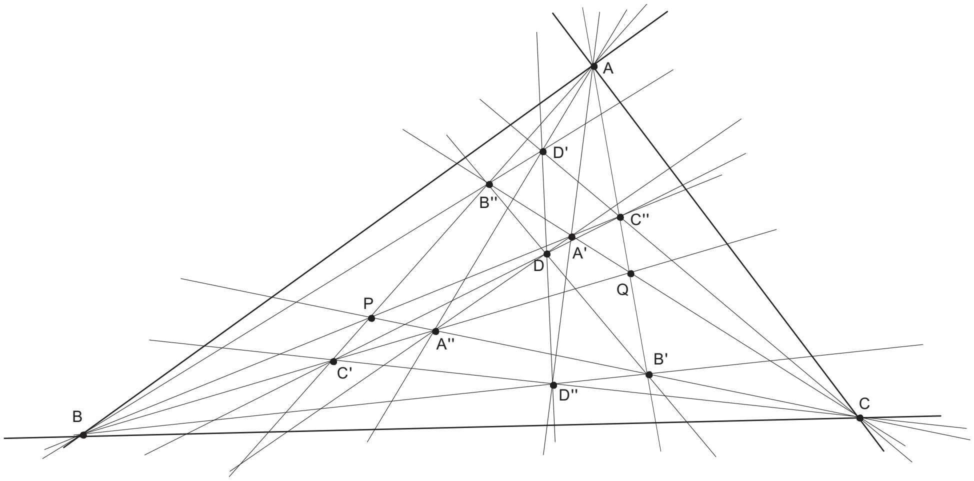

Figure 3: Desmic $16 - 12$ structure

ities can be recorded in terms of the array

A	B	C	D
A'	B'	C'	D'
A''	B''	C''	D''

A triple of points from the array is collinear precisely when a) each is from a different row, and b) if no D is involved each is from a different column, and c) if a D is involved, then the other two are both from the same column. An example of the former would be A, B'' and C', or C, B' and A''. An example of the latter would be D', B and B'' or D, D' and D''. There are then exactly 16 such collinearities among these 12 points.

Given a point P on a cubic, there are in general four points X_1, X_2, X_3 and X_4 on the cubic, other than P, whose tangents pass through P. Call these four points a **quadrangle** of the Neuberg cubic, and more specifically the **quadrangle to** P. To illustrate this, we write $X_1, X_2, X_3, X_4 : P$.

Here are some quadrangles for our cubic:

$$\begin{aligned} A_1, A_2, A_3, \infty_e &: \infty_e^* \\ I_1, I_2, I_3, I_o &: \infty_e \\ \overline{A_1}, \overline{A_2}, \overline{A_3}, C &: [0,8] \\ \overline{A_1}^*, \overline{A_2}^*, \overline{A_3}^*, O &: [17,8] \end{aligned}$$

Given three collinear points on a cubic, the associated quadrangles form a Desmic structure. Here are some examples for our cubic

A_1	A_2	A_3	∞_e
I_1	I_2	I_3	I_0
I_1	I_2	I_3	I_0

A_1	A_2	A_3	∞_e
E_1	E_2	E_3	$[3,13]$
E_1^*	E_2^*	E_3^*	$[19,13]$

A_1	A_2	A_3	∞_e
E_1'	E_2'	E_3'	$[0,16]$
$E_1'^*$	$E_2'^*$	$E_3'^*$	$[13,16]$.

We see that having recognized an (affine) cubic curve as a Neuberg cubic of a triangle, we have lots of natural and deep geometry that connects to the group multiplication. A natural question is: given an elliptic curve can we find an affine view of it which is a Neuberg cubic? And if so, how can we classify such views, and use them to understand elliptic curves?

Such an approach ought to be especially useful in the convenient laboratory provided by finite fields.

Tangent conics to an affine cubic

Here is a quite different use of affine coordinates in the study of an elliptic curve. For more information and examples involving tangent conics, see [8]. Different metrical interpretations of tangent conics thus allows one to distinguish points on an affine curve from the nature of the tangent conic. Figure 4 gives a view of some tangent conics to $[x_0, y_0]$ for the curve $y^2 = x^3 - x$ over the decimal numbers. Tangent conics to points on the 'egg' are ellipses, while others are either hyperbolas opening horizontally, a pair of lines, or hyperbolas opening vertically depending respectively on whether x_0 is less than, equal to, or greater than $\sqrt{\frac{2}{3}\sqrt{3}+1}$. Rather remarkably, these tangent conics nowhere intersect.

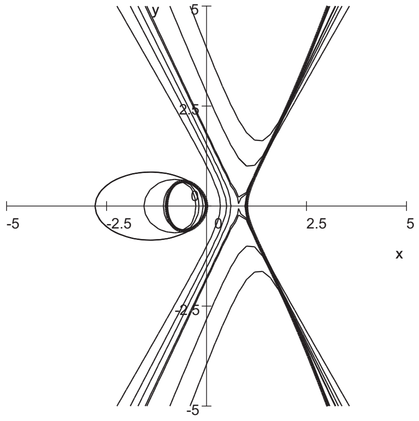

Figure 4: Tangent conics to $y^2 = x^3 - x$

Theorem 5 *Over a field in which -3 is not a square, any two tangent conics of the affine curve $y^2 = ax^3 + bx + c$ are either identical or disjoint.*

Proof. Recall that the tangent conic to an affine curve is the part of the Taylor expansion of degree two or less (see [8, Chapter 19]). More specifically, to find the tangent conic to $y^2 = ax^3 + bx + c$ at a point $A = [x_0, y_0]$ on it, first translate the curve by $-A$, yielding the equation

$$(y + y_0)^2 = a(x + x_0)^3 + b(x + x_0) + c$$

or, after simplification using the fact that A lies on the original curve,

$$y^2 + 2yy_0 - ax^3 - 3ax^2x_0 + x\left(-b - 3ax_0^2\right) = 0.$$

Then take the quadratic part:

$$y^2 + 2yy_0 - 3ax^2x_0 + x\left(-b - 3ax_0^2\right) = 0$$

and translate this conic back by A, yielding

$$(y-y_0)^2+2(y-y_0)y_0-3a(x-x_0)^2x_0+(x-x_0)\left(-b-3ax_0^2\right)=0$$

or after simplification

$$y^2-3ax^2x_0+x\left(3ax_0^2-b\right)-ax_0^3-c=0.$$

To find the intersection between two such tangent conics

$$\begin{aligned}y^2-3ax^2x_0+x\left(3ax_0^2-b\right)-ax_0^3-c=0\\ y^2-3ax^2x_1+x\left(3ax_1^2-b\right)-ax_1^3-c=0\end{aligned}$$

take the difference between the two equations, which factors as

$$a(x_1-x_0)\left(3x^2-3x(x_0+x_1)+x_0^2+x_0x_1+x_1^2\right).$$

If $x_0=x_1$ then the tangent conics coincide. Otherwise we get an intersection when the second quadratic factor has a zero. But its discriminant is

$$9(x_0+x_1)^2-4\times 3\left(x_0^2+x_0x_1+x_1^2\right)=(-3)(x_1-x_0)^2$$

and so if -3 is not a square then there is no solution and so the tangent conics are disjoint. ■

Note that the equation of the tangent conic

$$y^2-3ax^2x_0+x\left(3ax_0^2-b\right)-ax_0^3-c=0.$$

can be rewritten as

$$y^2-\left(ax^3+bx+c\right)+a(x-x_0)^3=0.$$

Figure 5 gives a view of some tangent conics for the curve $y^2=x^3+x$. The tangent conic to $[0,0]$ is a parabola, and otherwise they are either hyperbolas opening horizontally, a pair of lines, or hyperbolas opening vertically depending respectively on whether x_0 is less than, equal to, or greater than$\frac{1}{3}\sqrt{3}\sqrt{2\sqrt{3}-3}$.

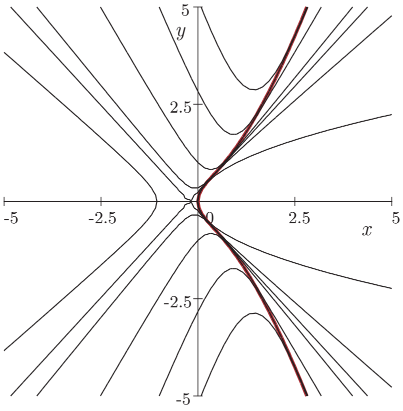

Figure 5: Tangent conics to $y^2=x^3+x$

Figure 6 shows the nodal cubic $y^2 = x^3 + x^2$ with tangent conic at $[x_0, y_0]$ given by

$$y^2 + 3xx_0^2 + x^2(-3x_0 - 1) - x_0^3 = 0.$$

We get a parabola when $x_0 = -1/3$, ellipses for x_0 less than that, hyperbolas opening horizontally till $x_0 = 0$, when we get the pair of lines $y = \pm x$, then hyperbolas opening upwards.

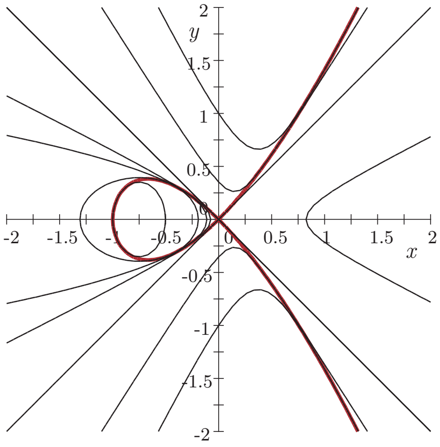

Figure 6: Tangent conics to $y^2 = x^3 + x^2$

References

[1] H. M. Cundy and C. F. Parry, *Geometrical properties of some Euler and circular cubics, Part 1*, J. Geom. 66 (1999), 72-103.

[2] H. M. Cundy and C. F. Parry, *Geometrical properties of some Euler and circular cubics, Part 2*, J. Geom. **68** (2000), 58-75.

[3] H. M. Cundy and C. F. Parry, *Some cubic curves associated with a triangle*, J. Geom. 53 (1995), 41-66.

[4] J-P. Ehrmann and B. Gibert, *Special Isocubics in the Triangle Plane*, available from http://perso.wanadoo.fr/bernard.gibert/downloads.html.

[5] C. Kimberling, *Triangle Centers and Central Triangles*, vol **129** of Congressus Numerantium, Utilitas Mathematica Publishing, Inc, Winnipeg, Manitoba, 1998.

[6] C. Kimberling, *Encyclopedia of Triangle Centers*, available at http://faculty.evansville.edu/ck6/encyclopedia/ETC.html

[7] W. Stothers, 'Grassmann cubics and Desmic structures', Forum Geometricorum **6** (2006) 117-138.

[8] N. J. Wildberger, *Divine Proportions: Rational Trigonometry to Universal Geometry*, Wild Egg Books (http://wildegg.com), Sydney, 2005.

[9] N. J. Wildberger, ‘Affine and projective universal geometry’, arXiv:math.MG/0612499v1, 18 Dec., 2006.