

## CHAPTER EIGHT

### CURVES IN THE PLANE

#### §1. QUADRATICS

Algebraic curves are graphs of polynomials in two variables. Quadratic curves are either conic sections or pairs of straight lines. Their study can be unified by casting the situation into the projective plane by the use of homogeneous coordinates.

The general quadratic equation in the plane is given by

$$ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0 ,$$

and this can represent an ellipse (in particular, a circle), an hyperbola, a parabola, an intersecting or parallel pair of lines, or a degenerate locus. The first three of these, the conic sections are projectively related, and can be studied together as one phenomenon in the real projective plane consisting of equivalent classes of points  $(X, Y, Z)$  with  $X, Y, Z$  not all zero, and  $(X, Y, Z) \sim (U, V, W)$  when  $X : Y : Z = U : V : W$ . A regular affine point  $(x, y)$  corresponds to the equivalence class of  $(x, y, 1)$ , while  $(U, V, 0)$  is a “point at infinity” given by the vector direction  $(U, V)$  (*i.e.*, the set of parallel lines in the direction of  $(U, V)$  meet at the point of infinity). These lines are parallel to the line  $Uy = Vx$  and have slope  $V/U$ .

We can describe the locus in the projective plane by a homogeneous equation that, when satisfied by  $(X, Y, Z)$ , is satisfied also by all scalar multiples of this. The “homogenization” of the general quadratic is

$$aX^2 + 2hXY + bY^2 + 2gXZ + 2fYZ + cZ^2 = 0 .$$

The interplay between algebraic and geometric structure can be used to solve diophantine equations over  $\mathbf{Q}$ . Consider the Pythagorean diophantine equation  $x^2 + y^2 = 1$ . An obvious solution of this is  $(x, y) = (-1, 0)$ . Let  $m$  be an arbitrary rational. The line  $y = m(x + 1)$  passes through  $(-1, 0)$  and a second point on the circle  $x^2 + y^2 = 1$  whose abscissa satisfies the equation

$$0 = (m^2 + 1)x^2 + 2m^2x + (m^2 - 1) = (x + 1)[(m^2 + 1)x - (1 - m^2)] ,$$

so that the rational point

$$\left( \frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right)$$

also lies on the circle. (We know the coordinates of the point are rational, because one of the zeros and the sum of the zeros of the quadratic for the abscissae are both rational.)

Setting  $m = p/q$  and casting the situation in the projective plane, we obtain the generic solution

$$(X, Y, Z) = (q^2 - p^2, 2pq, q^2 + p^2)$$

for the Pythagorean equation. If we take  $m = \tan(\theta/2)$ , a rational number, we get the solution in the form  $(x, y) = (\cos \theta, \sin \theta)$  and the group structure of rotation through the angle  $\theta$  induces a group structure on the solutions of the Pythagorean equation.

A similar technique involving the sum or product of the roots can be used to solve other quadratic diophantine equations, even with more variables. For example, an obvious solution of the equation

$$x^2 + y^2 + z^2 = 3xyz$$

is  $(x, y, z) = (1, 1, 1)$ . If we fix two variables, the equation is quadratic in the third:

$$x^2 - (3yz)x + (y^2 + z^2) = 0 .$$

If  $y, z$  are integers, then either both roots of this equation are integers with the sum  $3yz$  or neither are integers. Using this, we can construct an infinite family of solutions including

$$(1, 1, 1), (1, 1, 2), (1, 5, 2), (1, 5, 13), (29, 5, 2) .$$

## §2. BEZOUT'S THEOREM

In complex projective space  $(X, Y, Z)$  any pair of lines either coincide or intersect in exactly one point; we do not have to make exception for parallel lines as in affine space. This is a simple instance of a very strong property in that the number of intersections of two algebraic curves is a product of the degrees of the equations that represent them.

If  $\mathcal{C}_1$  and  $\mathcal{C}_2$  are two projective curves given by homogeneous polynomials of respective degrees  $d_1$  and  $d_2$ , and  $P$  is a common point, we can define the multiplicity of  $P$  at an intersection point. Its value is 1 if the curves intersect transversally, *i.e.* their tangents have distinct directions, and greater than 2 otherwise. The exact value is given by a rather technical definition.

Bezout's Theorem says that the number of intersection points counting multiplicity of the two curves is equal to the product of the degrees, provided the two curves do not have a common component (given by a common factor of their polynomials). The affine version of this theorem says that the number of intersection points does not exceed the product of the degrees.

For example, if  $\mathcal{C}_1$  and  $\mathcal{C}_2$  are both conic sections, then they have at most four points in common unless they intersect in a line or coincide. (See [5, Chapter 1] for further details.)

## §3. CUBIC CURVES.

Suppose that  $\mathcal{C}_1$  and  $\mathcal{C}_2$  are both cubic curves. By Bezout's Theorem, they intersect in 9 points. However, if  $\mathcal{D}$  is a curve that goes through 8 of these points, it will in fact go through the ninth point as well. This can be seen as follows.

Each cubic curve can be described by an equation of the form  $\sum a_{ij} X^i Y^j Z^{3-i-j} = 0$ , where there are ten parameters  $a_{ij}$  corresponding to the conditions  $0 \leq i, j \leq 3, i + j \leq 3$ . Every point on the curve imposes a linear restriction on these parameters, so that nine points lead to nine homogeneous linear equations for these ten coefficients  $a_{ij}$ . Normally, this system will have a unique solution up to a multiple of the vector of coefficients. However, in the situation of Bezout's Theorem, the nine points would be the set of intersection points of two distinct curves.

To find a cubic such as  $\mathcal{D}$  containing eight of the intersection points, we have to solve 8 homogenous linear equations for the vector of 10 coefficients. The space of solutions is 2-dimensional. The coefficient vectors for  $\mathcal{C}_1$  and  $\mathcal{C}_2$  constitute a basis for this space, and so the coefficient vector for  $\mathcal{D}$  must be a linear combination of them. Since  $\mathcal{C}_1$  and  $\mathcal{C}_2$  pass through the ninth point, so also must  $\mathcal{D}$ . ♣

A cubic curve is *irreducible* if and only if, having integer or rational coefficients, its polynomial does not factor nontrivially over  $\mathbf{Q}$ . It is *nonsingular* at a point if and only if its affine realization in  $(x, y)$  does not have both its partial derivatives vanishing at the point. Basically, the curve does not intersect itself nor have a cusp at a nonsingular point. A *flex* of  $\mathcal{C}$  is a point at which  $\mathcal{C}$  is nonsingular and intersects its tangent at least three times (think of  $y = x^3$  at the origin). A projective transformation can be found that removes the flex to the point at infinity and renders the equation of the curve into the form

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

an *elliptic curve*.

We can define a group operation on the points of a cubic curve  $\mathfrak{C}$  as follows. We note that, as the coordinates of the points on the curve belong to a particular field, say the rationals, then the “sum” of the points under the group operations will have coordinates in the same field.

Begin by specifying a point  $O$ , which is generally a flex point of the curve; this is going to be the identity. In the complex projective plane, each line passing through two points of  $\mathfrak{C}$  passes through a third. (If we are in the affine plane, one of these points may be at infinity.) For  $P$  and  $Q$  on the cubic curve, let  $P * Q$  be the third point of intersection of the line  $PQ$  with the curve; note that if these two points coincide, the line  $PQ$  is the tangent. Define  $P + Q$  to be the intersection of the cubic curve with the line that passes through  $O$  and  $P * Q$ .

It is straightforward to see that the group operation  $+$  is commutative.  $O$  is the identity, since  $O, O * P$  and  $P$  are collinear and so  $P = P + O$ . Let  $S$  be the point where the tangent at  $O$  intersects  $\mathfrak{C}$ . Then  $-P$  is the third point of intersection of  $\mathfrak{C}$  and the line that passes through  $P$  and  $S$ . Since  $P * (-P) = S$ , it follows that  $P + (-P) = O$ .

Proving that the group law is associative is more interesting and delicate. We have to show that  $(P + Q) + R = P + (Q + R)$ ; it is sufficient to show that  $(P + Q) * R = P * (Q + R)$ .

Consider the following ten points:

$$O, P, Q, R, P * Q, P + Q, Q * R, Q + R, (P + Q) * R, P * (Q + R)$$

in the given cubic curve,  $\mathfrak{C}$ . Let  $\mathfrak{D}$  be the cubic curve consisting of the union of the three lines:

$$\mathfrak{L}_1 \text{ through } P, Q, P * Q$$

$$\mathfrak{L}_2 \text{ through } O, Q * R, Q + R$$

$$\mathfrak{L}_3 \text{ through } P + Q, R, (P + Q) * R$$

and let  $\mathfrak{E}$  be the cubic curve consisting of the union of the three lines:

$$\mathfrak{M}_1 \text{ through } Q, R, Q * R$$

$$\mathfrak{M}_2 \text{ through } O, P * Q, P + Q$$

$$\mathfrak{M}_3 \text{ through } P, Q + R, P * (Q + R) .$$

The curve  $\mathfrak{E}$  passes through eight of the nine intersection points of  $\mathfrak{C}$  and  $\mathfrak{D}$  (all but possibly  $(P + Q) * R$ ), so it must pass through the ninth, namely  $(P + Q) * R$ . Since  $\mathfrak{C}$  and  $\mathfrak{E}$  cannot have more than nine intersection points, we must have  $(P + Q) * R = P * (Q + R)$ .

#### §4. THE LYNNESS RECURSION

It is readily checked that, except for some anomalous cases, the recursion  $\{x_n\}$  defined by

$$x_{n+1} = \frac{x_n + 1}{x_{n-1}}$$

is periodic with period 5. In fact, if you start with initial terms (called *seeds*)  $x$  and  $y$  unequal to  $-1$  or  $0$ , the sequence cycles through  $x, y, (y + 1)/x, (x + y + 1)/(xy), (x + 1)/y$ . It is natural to consider the generalization of this recursion

$$x_{n+1} = \frac{x_n + c}{x_{n-1}}$$

where  $c \geq 0$ . We suppose that the seeds  $x_0$  and  $x_1$  are given, so that every other  $x_n$  can be determined, with division by 0 never occurring. When  $c = 0$ , we find that the recursion has period 6. However, for other values of  $c$  the situation is more complicated. We can conveniently analyze the sequence by plotting points  $(x_n, x_{n+1})$ , where  $n$  ranges over the integers. We are looking for orbits under the planar transformation

$$T_c : (x, y) \longrightarrow \left( y, \frac{y+c}{x} \right).$$

Peter Harrison of Toronto, ON observed that, when  $c$  is positive and unequal to 0 or 1, the orbits appear to fill up loops in the positive quadrant. Perhaps these loops can be described by an algebraic equation. So we can ask, given  $c$  and any  $(x_0, x_1)$ , is there a function  $f_c(x, y)$  for which

$$f_c(x_n, x_{n+1}) = f_c(x_0, x_1)$$

for each  $n$ . Such a function should satisfy the identity

$$f_c(x, y) = f_c\left(y, \frac{y+c}{x}\right).$$

Fortunately, we can get an idea of what such a function might be by looking at the  $c = 0$  and  $c = 1$  cases; here we can construct such a function by adding together the finite number of entries in a general orbit. Thus,

$$\begin{aligned} f_1(x, y) &= x + y + \frac{y+1}{x} + \frac{x+y+1}{xy} + \frac{x+1}{y} \\ &= \frac{x^2y + xy^2 + x^2 + 2x + y^2 + 2y + 1}{xy}, \end{aligned}$$

and

$$\begin{aligned} f_0(x, y) &= x + y + \frac{y}{x} + \frac{1}{x} + \frac{1}{y} + \frac{x}{y} \\ &= \frac{x^2y + xy^2 + x^2 + x + y^2 + y}{xy}. \end{aligned}$$

These examples lead to a successful conjecture for the function, namely

$$\begin{aligned} f_c(x, y) &= \frac{x^2y + xy^2 + x^2 + (c+1)x + y^2 + (c+1)y + c}{xy} \\ &= \frac{(x+1)(y+1)(x+y+c)}{xy} - (c+2), \end{aligned}$$

and we can check by substitution that  $f_c(x, y) = f_c(y, (y+c)/x)$ . In the positive quadrant, the function  $f_c(x, y)$  achieves a global minimum at  $(\alpha, \alpha)$ , where  $\alpha = \frac{1}{2}(1 + \sqrt{1+4c})$ . This is a fixed point for the mapping  $T_c$ .

For each value of  $k$ , the equation  $f_c(x, y) = k$  can be recast as  $h_{c,k}(x, y) = 0$ , where

$$\begin{aligned} h_{c,k}(x, y) &= x^2y + xy^2 + x^2 + y^2 - kxy + (c+1)(x+y) + c \\ &= xy(x+y) + (x+y)^2 - (k+2)xy + (c+1)(x+y) + c \\ &= xy(x+y-k-2) + (x+y+c)(x+y+1) \\ &= (y+1)x^2 + (y^2 - ky + (c+1))x + (y+1)(y+c) \\ &= (x+1)y^2 + (x^2 - kx + (c+1))y + (x+1)(x+c) \\ &= (x+1)(y+1)(x+y+c) - Kxy, \end{aligned}$$

with  $K = k + c + 2$ . Observe that  $h_{c,k}$  is symmetric in  $x$  and  $y$ , so that  $h_{c,k}(x_{n-1}, x_n) = h_{c,k}(x_n, x_{n+1}) = h_{c,k}(x_{n+1}, x_n)$  with the result that  $x_{n-1}$  and  $x_{n+1}$  are the two roots of the quadratic equation  $h_{c,k}(x, x_n) = 0$ .

**Proposition 8.1.** *There is no value of  $c$ , save 0 and 1, for which every sequence obtained and defined is periodic with fixed period  $N$ .*

*Proof.* The sequence with seed  $-1, t$  is

$$\dots, -1, t, -t - c, -1, \frac{1 - c}{t + c}, \dots .$$

Since every third element is  $-1$ , the issue turns on whether the real mapping  $\phi_c : t \rightarrow (1 - c)/(t + c)$  has a universal period independent of  $t$ .

When  $c \neq 0, 1, 2$ ,  $\phi_c$  has two fixed points,  $-1$  and  $1 - c$ , one attractive and one repellent, so that there is a neighbourhood of each free of periodic points. When  $c = 2$ , the fixed point  $-1$  is attractive from the right and repellent from the left, so again there is a neighbourhood free of fixed points. ♠

It may happen, when  $c \neq 0, 1$  that there are particular values of  $x_0$  and  $x_1$  yielding periodic sequences. First, if the seeds are  $-1$  and  $t$ , then  $f_c(-1, t) = -(c + 2)$  and

$$h_{c, -(c+2)}(x, y) = (y + 1)(x + 1)(x + y + c)$$

with the result that each point  $(-1, t)$  lies on a degenerate cubic locus consisting of the union of three straight lines  $y = -1$ ,  $x = -1$  and  $x + y = -c$ . Since the quadratic equation  $h_{c, -(c+2)}(-1, t) = 0$  is degenerate, there is no restriction on  $t$  (unless the sequence leads to a term with 0 denominator). If there are two consecutive terms  $u, v$ , in the sequence for which  $u + v + c = 0$ , then the next term is  $-1$ . Thus, the sequences that contain  $-1$  are precisely those that satisfy  $f_c(x_n, x_{n+1}) = -(c + 2)$  for all  $n$ .

When  $y \neq -1$ , the quadratic  $h_{c, -(c+2)}$  in  $x$  has precisely two roots, whose product is  $y + c$ . Suppose  $x_0 = u$  and  $x_1 = v$ . Then we obtain

$$\begin{aligned} x_{-4} &= \frac{c(u^2v + uv^2) + cv^2 + (c^2 + 1)uv + cv}{cuv + u^2 + 2cu + c^2v + c^2} \\ x_{-3} &= \frac{cuv + cv + u + c}{u^2 + cu} \\ x_{-2} &= \frac{cv + u + c}{uv} \\ x_{-1} &= \frac{u + c}{v} \\ x_0 &= u \\ x_1 &= v \\ x_2 &= \frac{v + c}{u} \\ x_3 &= \frac{cu + v + c}{uv} \\ x_4 &= \frac{cuv + cu + v + c}{v^2 + cv} \\ x_5 &= \frac{c(u^2v + uv^2) + cu^2 + (c^2 + 1)uv + cu}{cuv + v^2 + 2cv + c^2u + c^2} . \end{aligned}$$

**Proposition 8.2.** *Suppose that the sequence  $\{x_n\}$  does not contain  $-1$ .*

(a) *If  $x_0 = x_1$ , then  $x_{-n} = x_{n+1}$  for each positive integer  $n$ .*

(b) *If, for some positive integer  $m$ ,  $x_{m+1} = x_{-m}$ , then either  $x_0 = x_1$  or the sequence  $\{x_n\}$  has period  $2m + 1$ .*

(c) If, for some positive integer  $m$ ,  $x_0 = x_1$  and the sequence is periodic with period  $2m + 1$ , then for  $2 \leq r \leq m$ ,  $x_r = x_{2m+2-r}$ . Thus, the sequence is “symmetric” about the term  $x_{m+1}$ .

(d) If, for some positive integer  $m$ ,  $x_m = x_{-m}$  and  $x_{m+1} = x_{-(m-1)}$ , then  $x_n$  is periodic with period  $2m$ .

(e) If  $x_0 = x_1$  and for some positive integer  $m$ ,  $x_m = x_{m+1}$ , then the sequence  $\{x_n\}$  is periodic with period  $2m$ .

(f) If, for some positive integer  $m$ ,  $x_0 = x_1 = x_{2m} = x_{2m+1}$ , then  $x_m = x_{m+1}$ .

*Proof.* (a) This is established by induction.

(b) Let  $z$  be the common value of  $x_{m+1}$  and  $x_{-m}$ . If  $k = f_c(x_0, x_1)$ , the roots of the quadratic equation  $h_{c,k}(z, t) = 0$  are  $x_{m+2}$  and  $x_m$ , as well as  $x_{-m+1}$  and  $x_{-m-1}$ . If  $x_m = x_{-m-1}$ , then the consecutive pair  $x_m, x_{m+1}$  equals the consecutive pair  $x_{-m-1}, x_{-m}$  and the sequence has period  $2m + 1$ . The remaining possibility is that  $x_m = x_{-m+1}$ . This leads in turn to  $x_k = x_{-k+1}$  where  $k$  takes the values  $m, m-1, \dots, 1$ , i.e., to  $x_1 = x_0$ .

(c) By an argument similar to that used in (b), we note that if  $u = x_0 = x_1$ , then  $u = x_{2m+2}$  and  $x_2 = x_{2m}$  are the roots of a quadratic equation  $h_{c,k}(u, t) = 0$ . This leads to the result.

(d) This is clear.

(e) Since  $x_0 = x_1$ , it follows that  $x_{-m+1} = x_m$  and  $x_{-m} = x_{m+1}$ . Hence, the consecutive pair  $x_{-m}, x_{-m+1}$  is equal to the consecutive pair  $x_m, x_{m+1}$ .

(f) The hypothesis implies that  $\{x_n\}$  is  $2m$ -periodic. Hence  $x_m = x_{-m} = x_{m+1}$  as desired. ♠

We now examine the periodic behaviour of the mapping  $T_c$ .

**Period 1.**  $T_c$  has the fixed points  $(r, r)$  where  $r$  is one of the roots of the quadratic equation  $t^2 = t + c$ . The Jacobean matrix of the  $T_c$  has the characteristic equation  $t^2 - (1/r)t + 1 = 0$ . When  $r \leq \frac{1}{2}$ , this has two roots of the form  $\cos \theta + i \sin \theta$ , and  $T_c$  behaves roughly like a rotation. In fact,  $T_c$  takes nearby loops into themselves; we can refer to a rotation number, which is the limit as  $n \rightarrow \infty$  of the number of times we move clockwise around the loop in the first  $n$  points divided by  $n$ .

**Period 2.** For a sequence  $\{\dots, p, q, p, q, \dots\}$  of prime period 2, we have that  $p^2 = q + c$  and  $q^2 = p + c$ , whence  $p + q = -1$  and  $p$  and  $q$  are the roots of the quadratic equation  $t^2 + t + 1 = c$ . It happens that  $f_c(p, q) = -3$ , independently of  $c$ . Thus,  $(p, q)$  and  $(q, p)$  lie on the locus of  $h_{c,-3}(x, y) = 0$  where

$$h_{c,-3}(x, y) = (x + y + 1)(xy + x + y + c) .$$

They lie at the intersection of the straight line  $x + y = -1$  and the hyperbola  $(x + 1)(y + 1) = 1 - c$ .

**Period 3.** Letting  $x_0 = u$  and  $x_1 = v$  and equating  $x_{-1} = x_2$  and  $x_0 = x_3$  leads to

$$u^2 + cu = v^2 + cv \iff (u - v)(u + v + c) = 0$$

and

$$u^2v = cu + v + c .$$

Taking  $c \neq 1$  to avoid a degenerate case, we find that the only possibility for a sequence of period 3 is

$$\{\dots, -1, -1, 1 - c, \dots\}$$

and the points of the 3-orbit on which  $T_c$  acts are the points where the lines  $x = -1$ ,  $y = -1$  and  $x + y = -c$  intersect in pairs.

**Period 4.** When  $x_0 = u$  and  $x_1 = v$ , we set  $x_{-2} = x_2$  and  $x_{-1} = x_3$  leads to  $0 = (u - v)(u + v + 1)$ . We pick up sequences of period 1 and period 2, and there are no sequences of prime period 4.

**Period 6.** Equating  $x_3 = x_{-3}$  and  $x_4 = x_{-2}$  leads to  $(v+1)(u^2 - v - c) = 0$  and  $(u+1)(v^2 - u - c) = 0$ . We pick up sequences of periods 1, 2, 3 and find there are no sequences of prime period 6, when  $c \neq 0$ .

**Period 7.** Suppose, to begin with, we have a sequence of period 7 with adjacent equal entries  $x_0 = x_1 = u$ . Then  $x_4 = x_{-3}$  holds automatically, and  $x_5 = x_{-2}$  leads to

$$0 = (u^2 - u - c)[2cu^3 + (1 + 3c + c^2)u^2 + (2c + 2c^2)u + c^2] .$$

The first factor picks up the constant sequence. From the second factor, we get a sequence for which  $f_c(u, v) = -((1/c) + 1 + c)$ . In the case that  $x_0 = u \neq x_1 = v$ , the condition  $x_4 = x_{-3}$  leads to the equation

$$0 = c(u - v)h_{c, -(1/c+1+c)}(u, v) .$$

Thus, a point of smallest period 7 must lie on the curve  $h_{c,k}(x, y) = 0$  where  $k = -(1/c + 1 + c)$  and so cannot lie in the positive quadrant.

**Period 8.** Every sequence of period 8 returns to adjacent equal values at every fourth term so we can take  $x_0 = x_1 = u$  and  $x_4 = x_5 = v$ . The latter equation leads to  $2cu^2 + (1 + 2c)u + c = 0$ , so  $v = \frac{1}{2}u$ . If  $c = (1 - \sqrt{2})/2$ , the quadratic has coincident roots and we get sequences with constant term  $1/\sqrt{2}$  or  $-1/\sqrt{2}$ . Noting that  $x_5 - x_{-3}$  has numerator  $c(u^2 - v - c)h_{c,k}(u, v)$  where  $k = -(2c^2 + 1)/c$ , we find that  $(u, v)$  is of period 8 if and only if  $h_{c,k}(u, v) = 0$  where  $k = -(2c^2 + 1)/c$ .

**Period 9.**  $(u, v)$  is of smallest period 9 for  $T_c$  if and only if  $h_{c,k}(u, v) = 0$  for  $k = (c^3 - 3c^2 - 1)/c$ . This gives the first case of periodic points in the positive quadrant when  $c$  is sufficiently large.

**Period 10.** When  $c = 2 \pm \sqrt{5}$ , there are no sequences with smallest period 10, as they collapse into constant sequences. Otherwise (excluding  $c = 0, 1$ ), we find that  $(u, v)$  has smallest period 10 if and only if  $h_{c,k}(u, v) = 0$  with  $k = -(1 + c + 3c^2 + c^3)/(c^2 + c)$ .

Numerical investigation led to the conjecture: *Let  $c > 1$  and  $r$  be a positive real for which  $c = r^2 - r$ . If  $p/q$  is a rational in lowest terms with  $1/5 < p/q < (1/2\pi) \arccos(1/2r)$ , there is a unique value of  $k$  for which the points of period  $q$  for  $T_c$ , for which one traverses clockwise around the loop on average  $p$  times to first return to the initial point of the orbit, is coincident with the set of points on the curve  $f_c(x, y) = k$ . On each loop  $f_c(x, y) = k$ ,  $T_c$  is conjugate to a rotation of the circle.*

This situation can be tackled using the theory of elliptic curves. Consider the curve  $\mathfrak{C}_k$ :

$$0 = (y + 1)x^2 + (y^2 - ky + (c + 1))x + (y + 1)(y + c) = h_{c,k}(x, y) .$$

It has an asymptote  $y + 1 = 0$ . Its rendition in the projective plane has the form  $(X + T)(Y + T)(X + Y + cT) - KXYT = 0$ . It contains the points  $P \sim (1, 0, 0)$  and  $O \sim (1, -1, 0)$  at infinity as well as  $A \sim (-c, 0, 1)$  and  $B \sim (-1, 0, 1)$ . A group law can be defined on this elliptic curve with identity  $O$ . The action of  $T_c$  can be defined as follows.

Suppose that  $(u, v) \in \mathfrak{C}_k$ . The line  $y = v$  intersects the curve  $\mathfrak{C}_k$  at the point  $(u', v)$ , where  $u$  and  $u'$  are the roots of the equation

$$0 = (v + 1)x^2 + (v^2 - kv + (c + 1))x + (v + 1)(v + c) .$$

The root  $u'$  is equal to  $(v + c)/u$ , so that the second point of intersection is  $((v + c)/u, v)$ . But then we flip this over the line  $y = x$  to arrive at  $T_c(u, v) = (v, (v + c)/u)$ .

Thus, if  $M$  is a point on  $\mathfrak{C}_k$ ,  $T_c(M) = M + P$ , and  $M$  is a  $n$ -periodic point on  $\mathfrak{C}_k$  if and only if  $nP = 0$ . If  $n = 2k$ , then  $kP = -kP$  and the two coordinates of  $kP$  are equal (there are three possibilities). If  $n = 2k + 1$ , then  $-kP = kP + P$ , so that, if  $kP = (u, v)$ , then  $(v, u) = (v, (v + c)/u)$  and  $v + c = u^2$ . Also  $-2(kP) = P$ , so that the tangent to the cubic at  $kP$  is horizontal.

An integer  $n \geq 2$  is an *algebraic minimum period* if  $nP = 0$  for at least one value of  $(c, k)$  with  $c > 0$ . It is *acceptable* if  $nP = 0$  occurs for at least one  $(c, k)$  with  $c > 0$  and  $k > f_c(r, r)$ , where  $(r, r)$  is the positive quadrant fixed point. Thus,  $n = 7, 8$  are algebraic but not acceptable, but  $n = 9$  is algebraic and acceptable.

From a theorem of Mazur, for  $c$  rational, there is no minimum period  $n$  with  $n = 11$  or  $n \geq 13$  among rational points. For a fixed  $c > 0$  and  $k > f_c(r, r)$ , the mapping  $T_c$  is conjugate to a rotation on a circle with rotation number in the interval bounded by  $1/5$  and  $\arccos(1/2r)/2\pi$ , which is contained in the interval  $[1/6, 1/4]$ . The integer  $n$  is a minimal acceptable period only if there is a positive quadrant loop acted on by  $T_c$  with rotation number  $m/n \in [1/6, 1/4]$ . This excludes the following numbers as minimal acceptable periods 2, 3, 4, 6, 7, 8, 10, 12, 15, 18, 20 and possibly 42.

## References

1. Ed Barbeau, Boas Gelbord & Steve Tanny, Periodicities of solutions of the generalized Lyness recursion. *Journal of Difference Equations and Applications* 1 (1995), 291-306
2. G. Bastien, M. Rogalski, *Global behaviour of the solutions of Lyness' difference equation  $u_{n+2}u_n = u_{n+1} + a$* . *Journal of Difference Equations and Applications* 10 (2004), 977-1003
3. G. Bastien, M. Rogalski, *On some algebraic difference equations  $u_{n+2}u_n = \psi(u_{n+1})$  in  $\mathbf{R}_*^+$  related to families of conics and cubic; generalizations of the Lyness sequences*. *Journal of Mathematical Analysis and Applications* 300 (2004), 303-333
4. Robert Bix, *Conics and cubics: concrete introduction to algebraic curves* Springer, 1998,2006
5. Terry Sheil-Small, *Complex polynomials* Cambridge, 2002
6. Joseph H. Silverman, John Tate, *Rational points on elliptic curves* Springer, 1992
7. John Stillwell, (The evolution of) Elliptic curves. *American Mathematical Monthly* 102:9 (November, 1995), 831-837