17. k-ARCS ON ELLIPTIC CURVES

As in §16, the curve $\mathscr{C}$ is a non-singular cubic in PG(2,q) with inflexion O.

THEOREM 17.1: (Zirilli [22]) If $|\mathscr{C}| = 2k$, then there exists a k-arc K on $\mathscr{C}$.

Proof. Since $\mathscr{C}$ is an abelian group, the fundamental theorem says that $\mathscr{C}$ is a direct product of cyclic groups of prime power order. By taking a subgroup of order 2^{r-1} in a component of order 2^r, we obtain a subgroup G of $\mathscr{C}$ of index 2. Let $K = \mathscr{C} \setminus G$. Let $P_1, P_2 \in K$. Then $-P_1 \in K$ and $P_2 = -P_1 + Q$ for some Q in G. Hence $P_1 + P_2 = Q$ and $P_1 + P_2 - Q = 0$. Since $-Q$ is in G, no three points of K are collinear.

The remainder of §17 follows Voloch [19].

The object is now to show that $\mathscr{K}$ can be chosen to be complete. First we construct $\mathscr{K}$ in a different way.

Let $U_o = P(1,0,0)$, $U_1 = P(0,1,0)$, $U_2 = P(0,0,1)$.
Also, with K=GF(q), let $K_o = GF(q) \setminus \{0\}$ and $K_o^2 = \{t^2 \mid t \in K_o\}$.

Now, let $\mathscr{C}$ in PG(2,q), q odd, have equation

$$y^2 z = x^3 + a_2 x^2 z + a_1 x z^2 + a_o z^3.$$

Also suppose it is non-singular with 2k points. The point U_1 is an inflexion and we take this as the zero of $\mathscr{C}$ as an abelian group. Since $|\mathscr{C}|$ is even, so $\mathscr{C}$ has an element of order 2, which necessarily is a point of contact of a tangent through U_1. Choose the tangent as x=0 and the point of contact as U_2. Thus $a_o = 0$ and $\mathscr{C}$ has equation

$$y^2 z = x^3+a_2x^2z+a_1xz^2. \tag{17.1}$$

Define $\Theta : \mathscr{C} \to K_o/K_o^2$ by

$$U_1\Theta = K_o^2 \ ; \ U_2\Theta = a_1K_o^2, \ P(x,y,1)\Theta = xK_o^2 \text{ for } x\neq 0.$$

Write $K_o/K_o^2 = \{1,\nu \mid \nu^2=1\}$.

LEMMA 17.2: Θ is a homomorphism.

Proof. If $P = P(x,y,1)$, then $-P=P(x,-y,1)$.

So $P\Theta = (-P)\Theta$, this also holds for U_1 and U_2. Hence, if $P_1+P_2+P_3=0$, then $P_1+P_2=-P_3$ and $(P_1+P_2)\Theta = (-P_3)\Theta = P_3\Theta = 1/(P_3\Theta)$. If it is shown that $(P_1\Theta)(P_2\Theta)(P_3\Theta)=1$, then $(P_1+P_2)\Theta = (P_1\Theta)(P_2\Theta)$.

Let $P_i = P(x_i,y_i,1)$, $i=1,2,3$. Since $P_1+P_2+P_3=0$, so P_1,P_2,P_3 are collinear, whence there exist m and c in K such that $y_i=mx_i+c$, $i=1,2,3$. So

$$(mx+c)^2 - (x^3+a_2x^2+a_1x)=(x_1-x)(x_2-x)(x_3-x).$$

Thus $x_1x_2x_3 = c^2$ and so $(P_1\Theta)(P_2\Theta)(P_3\Theta) = 1$.

If $(P_1,P_2) = (U_1,P_2)$, then $(P_1+P_2)\Theta = P_2\Theta = (P_1\Theta)(P_2\Theta)$. If $(P_1,P_2) = (P_1,U_2)$ and $P_1 = P(x_1,y_1,1)$, then $P_1+U_2=P(x_2,y_2,1)$ with $x_1x_2=a_1$.

Hence $(P_1+U_2)\Theta = x_2=a_1/x_1$

$$= x_1^2(a_1/x_1) = x_1a_1 = (P_1\Theta)(U_2\Theta).$$

So the homomorphism is established in all cases.

LEMMA 17.3: Θ is surjective for $q \geq 7$.

Proof. Since $P(bx^2, y, 1)\Theta = bx^2 = b$, it suffices to find a point Q on $\mathscr{C}' = V(F(bx^2, y, z))$ where $\mathscr{C} = V(F(x,y,z))$. So $\mathscr{C}'$ has equation

$$y^2z^4 = (bx^2)^3 + a_2(bx^2)^2z^2 + a_1(bx^2)z^4.$$

However, we require Q not on $V(xz)$. But $V(z) \cap \mathscr{C}' = \{U_1\}$ and $V(x) \cap \mathscr{C}' = \{U_1, U_2\}$. If we put $y = tx$, we see that $\mathscr{C}'$ is also elliptic and so has at least $(\sqrt{q}-1)^2$ points. Since $(\sqrt{q}-1)^2 > 2$ for $q \geq 7$, there exists the required point Q.

LEMMA 17.4: $\mathscr{K} = \mathscr{C} \setminus \ker\Theta$ is a k-arc.

Proof. Let $G = \ker\Theta$. Then, from the previous two lemmas, $G < \mathscr{C}$ with $[\mathscr{C} : G] = 2$. Then, if $P \in G$, $P\Theta = 1$; if $P \in K$, $P\Theta = \nu$. Suppose P_1, P_2, P_3 in $\mathscr{K}$ are collinear. So $P_1+P_2+P_3 = 0$, whence $(P_1+P_2+P_3)\Theta = 0\Theta$. So $(P_1\Theta)(P_2\Theta)(P_3\Theta) = 1$, whence $\nu^3 = 1$, whence $\nu = 1$, a contradiction.

This lemma just repeats lemma 17.1 using the homomorphism Θ.

THEOREM 17.5: $\mathscr{K}$ is complete for $q \geq 311$.

Proof. Let $P_0 \in PG(2,q) \setminus \mathscr{K}$. It must be shown that $\mathscr{K} \cup \{P_0\}$ is not a (k+1)-arc. There are three cases: (a) $P_0 \in \mathscr{C} \setminus \mathscr{K}$, (b) $P_0 = P(x_0, y_0, 1)$, (c) $P_0 = P(1, y_0, 0)$.

Case (a). There are at most four tangents through P_0 with point of contact Q in $\mathscr{K}$. Since $k = \frac{1}{2}|\mathscr{C}| > \frac{1}{2}(\sqrt{q}-1)^2 > 4$, there exists Q in $\mathscr{K}$ which is not such a point of contact. So $2Q \neq -P_0$ and $Q \neq -(P_0+Q)$. Also $-(P_0+Q) \in \mathscr{K}$, as otherwise $Q \in G = \mathscr{C} \setminus \mathscr{K}$. So $P_0, Q, -(P_0+Q)$ are distinct collinear points of $\mathscr{K} \cup \{P_0\}$.

Case (b). Let $\mathscr{C}'$ be the elliptic curve with affine equation

$$y^2 = \nu^3 x^4 + \nu^2 a_2 x^2 + \nu a_1 \ . \tag{17.2}$$

Define the following functions on $\mathscr{C}'$:

$$U = \nu x^2, \quad Z = xy, \quad A = (y_o - Z)/(x_o - U),$$

$$B = A^2 - a_2, \quad C = 2AZ - a_1 - 2A^2 U,$$

$$D = (U-B)^2 + 4(C+BU - U^2).$$

Then there exists a double cover

$$\Psi : \mathscr{D} \to \mathscr{C}'$$

defined by $W^2 = D$; that is, for any point $P(x,y,1)$ of $\mathscr{C}'$, there are two points $P(x,y,W,1)$ of $\mathscr{D}$. Now, let $P(x,y,W,1)$ be a rational point of $\mathscr{D}$. Then, from the equation for $\mathscr{C}'$,

$$x^2 y^2 = \nu^3 x^6 + \nu^2 a_2 x^4 + \nu a_1 x^2,$$

whence

$$Z^2 = U^3 + a_2 U^2 + a_1 U \ . \tag{17.3}$$

Hence

(1) $P = P(U,Z,1) \in \mathscr{K}$;

(2) PP_o has equation $y - Z = A(x-U)$;

(3) PP_o meets $\mathscr{C}$ is two points other than P whose x-coordinates satisfy

$$x^2 - (B-U)x - (C+BU-U^2) = 0 \tag{17.4}$$

The last follows by substitution from (2) in (17.1), for we have

$$\{Z+A(x-U)\}^2 = x^3+a_2x^2+a_1x.$$

Then, from (17.3),

$$(U^3+a_2U^2+a_1U) - (x^3+a_2x^2+a_1x)$$
$$+ 2ZA(x-U) + A^2(x-U)^2 = 0.$$

Cancelling x-U gives (17.4).

Now, let $\mathscr{C} \cap PP_0 = \{P,Q,R\}$. The discriminant of (17.4) is

$$(B-U)^2 + 4(C+BU-U^2) = D = W^2.$$

So Q and R are rational points of $\mathscr{C}$. Since P,Q,R are collinear $(P\Theta)(Q\Theta)(R\Theta) = 1$. As $P \in \mathscr{K}$, so $P\Theta = \nu$, whence $(Q\Theta)(R\Theta) = \nu$. So one of Q and R, say Q, is in $\mathscr{K}$. Hence, if $P \neq Q$, there are three collinear points P, P_0, Q of $\mathscr{K} \cup \{P_0\}$.

it remains to examine the condition that $P \neq Q$. There are at most six tangents to $\mathscr{C}$ through P_0 ([6] p.252). So, if P=Q or P=R, there are at most six choices for P, hence 12 choices for (x,y) and 24 choices for P(x,y,W,1) on $\mathscr{D}$. As $|\mathscr{C}' \cap V(x)| \leq 2$ and $|\mathscr{C} \cap V(z)| = 0$, so $|\mathscr{D} \cap V(x)| \leq 4$ and $|\mathscr{D} \cap V(z)| = 0$. So we require that $\mathscr{D}$ has at least 24+4+1 = 29 rational points.

By the Hurwitz formula ([5] p.301 or [3] p.215),

$$2g(\mathscr{D})-2 = 2\{2g(\mathscr{C}')-2\} + \deg E \qquad (17.5)$$
$$= \deg E.$$

Here, E is the ramification divisor (cf. §9) and

$$\begin{aligned} \deg E &= \#\text{ points of ramification} \\ &= \#\text{ points with } D = 0 \\ &= \#\text{ points such that } Q \text{ and } R \text{ have} \\ &\quad \text{the same x-coordinate}. \end{aligned}$$

If $Q = P(x_1,y_1,1)$ and $R = P(x_1,y_2,1)$, then $y_2=\pm y_1$; if $y_2 = - y_1$, then Q,R,U_1 are collinear. So either $Q=R$ or $Q=-R$. If $Q = -R$, then $P = U_1$ and this gives at most two points on $\mathscr{C}'$. If $Q=R$, then PP_o is a tangent to $\mathscr{C}$ at Q. Hence there are at most six choices for P and hence at most 12 such points on $\mathscr{C}'$. Hence $2g(\mathscr{D}) -2 \leq 12 + 2 = 14$, whence $g(\mathscr{D}) \leq 8$. Thus by the corollary to theorem 11.5,

$$|\mathscr{D}| \geq q+1 - 16\sqrt{q} .$$

So, when $q+1-16\sqrt{q} \geq 29$, we obtain the desired contradiction; this occurs for $q \geq 311$.

Case (c). This is similar to case (b). Here, among the functions on $\mathscr{C}'$, one takes $A = y_o$.

Notes: (1) The result certainly holds for some but not all k with $q < 311$.

(2) A similar technique can be applied for q even. Here $\mathscr{C}$ is taken in the form

$$(y^2+xy)z = x^3+a_1xz^2+a_oz^3.$$

Instead of Θ as above, we define $\Theta : \mathscr{C} \to K/C_o$ where $C_o=\{t\in K|T(t)=0\}$ and $T(t) = t+t^2+\dots t^{q/2}$; here C_o in the set of elements of category (= trace) zero. Take $P(x,y,1)\Theta = xC_o$. Then $\mathscr{K}$ is complete for $q\geq 256$.

COROLLARY : In PG(2,q) there exists a complete k-arc with $k=\frac{1}{2}(q+1-t)$ for every t satisfying 16.8 when either (a) q is odd, $q \geq 311$, t is even; or (b) q is even, $q \geq 256$, t is odd.

18. k-ARCS IN PG(2,q).

Let $\mathcal{K}$ be a complete k-arc in PG(2,q); that is, $\mathcal{K}$ has no three points collinear and is not contained in a (k+1)-arc. We define three constants m(2,q), n(2,q), m'(2,q).

$$m(2,q) = \max k = \begin{cases} q+2, & q \text{ even} \\ q+1, & q \text{ odd}, \end{cases}$$

$$n(2,q) = \min k.$$

If $m(2,q) \neq n(2,q)$,

$$m'(2,q) = \text{second largest } k;$$

if $m(2,q) = n(2,q)$, let $m'(2,q) = m(2,q)$. So, if a k-arc has $k > m'(2,q)$, then it is contained in an m(2,q)-arc. For q odd, every (q+1)-arc is a conic. For q even, the (q+2)-arcs have been classified for $q \leq 16$; see [4], [6].

The value of n(2,q) seems to be a difficult problem. By elementary considerations ([6] p.205),

$$n(2,q) \geq \sim \sqrt{2q}.$$

Constructions have been given for complete k-arcs with k having the following values (up to an added constant):

$\frac{1}{2}q$, see [6], §9.4;

$\frac{1}{3}q$, [1];