ALGEBRAIC CURVES, ARCS, AND CAPS OVER FINITE FIELDS

J.W.P.HIRSCHFELD

Mathematics Division

University of Sussex

Falmer

Brighton BN1 9QH

INGHILTERRA

INTRODUCTION

These notes give an account of a series of lectures at the University of Lecce as well as two at the University of Bari, all during April 1986.

§§1-15 are based on the thesis [18], of J.-F.Voloch, apart from some background remarks and classical interpolations. They deal with the number of points on an algebraic curve over a finite field. The main results of the thesis are also contained in [14], §16 records some classical results on elliptic curves and §17, following Voloch [19], proves the existence of complete k-arcs for many values of k by taking half the points on an elliptic curve. §§18-19 discusses the values of n(2,q), the size of the smallest k-arc in PG(2,q), and m'(2,q), the size of the second largest complete k-arc in PG(2,q), the main result of §19 follows a proof of Segre using an improved bound for the number of points on a curve from §§11 and 14. Finally, §20 summarizes the best, known estimates for $m_2(d,q)$, the largest size of k-cap in PG(d,q).

2. THE MAXIMUM NUMBER OF POINTS ON AN ALGEBRAIC CURVE

Let $\mathscr{C}$ be an algebraic curve defined over GF(q) of genus g, and let N_1 be the number of points, rational over GF(q), on a non-singular model of $\mathscr{C}$. Define $N_q(g) = \max N_1$, where $\mathscr{C}$ varies over all curves of genus g. We recall the following bounds.

(i) Hasse-Weil: $N_q(q) \leq q+1+2gq^{1/2}$

(ii) Serre: $N_q(g) \leq q+1+g[2q^{1/2}]$

(iii) Ihara: $N_q(g) \leq q+1 - \frac{1}{2}g + \{2(q+1/8)g^2+(q^2-q)g\}^{1/2}$

(iv) Manin: $N_2(q) \leq 2g - \sigma(g)$ as $g \to \infty$

$N_3(g) \leq 3g + \sigma(g)$ as $g \to \infty$

(v) Drinfeld-Vladut: $N_q(g) \leq g(q^{1/2}-1)+\sigma(g)$ as $g \to \infty$.

For a summary of results on $N_q(g)$ and references, see [9] Appendix IV.

The estimates (i) and (ii) are good for $g \leq \frac{1}{2}(q-q^{1/2})$, but not for $g > \frac{1}{2}(q-q^{1/2})$.

One of the aims of these notes is to describe improvements to (i), (ii), (iii). First, it is elementary that (ii) is sometimes better than (i) and never worse.

Let $m = [2q^{1/2}]$. Then $2q^{1/2} = m+\varepsilon$, where $0 \leq \varepsilon < 1$. So

$$[2gq^{1/2}] = [g(m+\varepsilon)] = [gm+g\varepsilon] = gm+[g\varepsilon].$$

3. THE DEDUCTION OF SERRE'S AND IHARA'S RESULTS FROM THE RIEMANN HYPOTHESIS.

(a) Serre's result

The Riemann hypothesis states that if N_i is the number of points of $\mathscr{C}$ rational over $GF(q^i)$, then

$$\mathscr{S}(\mathscr{C}) = \exp(\Sigma N_i\ x^i/i)$$
$$= f(x)/\{(1-x)(1-qx)\},$$

where $f(x) = 1+c_1x+\ldots+q^g x^{2g} \in \mathbb{Z}[x]$ has inverse roots $\alpha_1,\ldots,\alpha_{2g}$ satisfying

(i) $\alpha_i \alpha_{2g-i} = q$,

(ii) $|\alpha_i| = q^{1/2}$.

So $\alpha_i \bar{\alpha}_i = q$, whence $\alpha_{2g-i} = q/\alpha_i = \bar{\alpha}_i$ Thus, from the zeta function

$$N_1 = q + 1 - \sum_1^g (\alpha_i + \bar{\alpha}_i). \tag{3.1}$$

Since

$$\sum_{i=1}^{2g} \alpha_i^k = q^k + 1 - N_k , \tag{3.2}$$

the elementary symmetric functions of the α_i are integers and the α_i are algebraic integers.

As above, let $m = [2q^{1/2}]$ and let $x_i = m+1-\alpha_i-\bar{\alpha}_i$, $i=1,\ldots,g$.

(1) $x_i > 0$

Let $\alpha_i = c+d\sqrt{-1}$, $\bar{\alpha}_i = c-d\sqrt{-1}$. Then $c^2+d^2 = q$, whence $c \le \sqrt{q}$. So $\alpha_i + \bar{\alpha}_i = 2c \le 2\sqrt{q}$ and $[2\sqrt{q}]+1>\alpha_i+\bar{\alpha}_i$; thus $x_i>0$.

(2) The x_i are conjugate algebraic integers

To show that the elementary symmetric functions of the x_i are integers, it suffices to show that $\sum_1^g x_i^r$ is an integer for $r=1,\ldots,g$

or that $\Sigma(\alpha_i+\bar{\alpha}_i)^r$ is an integer. However,

$$\sum_1^g(\alpha_i+\bar{\alpha}_i)^r=\sum_1^g\alpha_i^r+\binom{r}{1}\sum_1^g\alpha_i^{r-1}\bar{\alpha}_i+\ldots+\binom{r}{1}\sum_1^g\alpha_i\bar{\alpha}_i^{r-1}+\sum_1^g\bar{\alpha}_i^r$$

$$=\sum_1^{2g}\alpha_i^r+\binom{r}{1}q\sum_1^{2g}\alpha_i^{r-2}+\binom{r}{2}q^2\sum_1^{2g}\alpha_i^{r-4}+\ldots,$$

which is an integer.

The classical inequality on arithmetic and geometric means gives

$$\frac{1}{g}\Sigma x_i \geq (\Pi x_i)^{1/g} \geq 1$$

by (1) and (2). So $\Sigma x_i \geq g$, whence $\Sigma(\alpha_i+\bar{\alpha}_i) \leq gm$. Applying the same argument with y_i for x_i with $y_i = m+1+\alpha_i+\bar{\alpha}_i$ gives $\Sigma(\alpha_i+\bar{\alpha}_i) \geq -gm$. Hence

$$|N_1 - (q+1)| \leq gm. \tag{3.3}$$

(b) Ihara's result

We use (3.1) and

$$N_2 = q^2+1-\Sigma(\alpha_i^2 + \bar{\alpha}_i^2). \tag{3.4}$$

Since $\alpha_i^2 + \bar{\alpha}_i^2 = (\alpha_i+\bar{\alpha}_i)^2 - 2q$, so

$$q+1-\Sigma(\alpha_i+\bar{\alpha}_i) = N_1 \leq N_2 = q^2+1+2qg-\Sigma(\alpha_i+\bar{\alpha}_i)^2.$$

However, $g\,\Sigma(\alpha_i+\bar{\alpha}_i)^2 \geq \{\Sigma(\alpha_i+\bar{\alpha}_i)\}^2$. Thus

$$N_1 \leq q^2 + 1 + 2qg - g^{-1}\{\Sigma(\alpha_i+\bar{\alpha}_i)\}^2$$

$$= q^2+1 + 2qg - g^{-1}(N_1-q-1)^2$$

and

$$N_1^2 - (2q+2-g)N_1+(q+1)^2-(q^2+1)g - 2qg^2 \leq 0,$$

from which the result follows.

For $g > \frac{1}{2}(q-\sqrt{q})$, Ihara's result is better than Serre's.

4. THE ESSENTIAL IDEA IN A PARTICULAR CASE

Let $\mathscr{C}$ be as in §2, but consider it as a curve over $\bar{K}$, the algebraic closure of $K = GF(q)$. Also suppose that $\mathscr{C}$ is embedded in the plane $PG(2,\bar{K})$ and let φ be the Frobenius map given by

$$P(x_o,x_1,x_2)\varphi = P(x_o^q,x_1^q,x_2^q)$$

where $P(x_o,x_1,x_2)$ is the point of the plane with coordinate vector (x_o,x_1,x_2). Then

$$\begin{aligned}\mathscr{C} &= V(F)\\ &= \{P(x_o,x_1,x_2) \mid F(x_o,x_1,x_2) = 0\}\end{aligned}$$

for some form F in $K[X_o,X_1,X_2]$. Also $\mathscr{C}\varphi = \mathscr{C}$ and the points of $\mathscr{C}$ rational over $GF(q)$ are exactly the fixed points of φ on $\mathscr{C}$.

For any non-singular point $P=P(x_o,x_1,x_2)$ the tangent T_p at P is

$$T_p = V\left(\frac{\partial F}{\partial x_o} X_o + \frac{\partial F}{\partial x_1} X_1 + \frac{\partial F}{\partial x_2} X_2\right) .$$

In affine coordinates,

$$T_p = V\left(\frac{\partial f}{\partial a} (x-a) + \frac{\partial f}{\partial b}(x-b)\right)$$

where $f(x,y) = F(x,y,1)$.

Instead of looking at fixed points of φ, let us look at the set of points such that $P\varphi \in T_p$. As $P \in T_p$, this set contains the GF(q)-rational points of $\mathscr{C}$. Let

$$h = (x^q - x)f_x + (y^q - y)f_y.$$

Then

$$\begin{aligned} h_x &= (qx^{q-1}-1)f_x + (x^q-x)f_{xx} + (y^q-y)f_{yx} \\ &= -f_x + (x^q-x)f_{xx} + (y^q-y)f_{yx} \end{aligned}$$

and

$$h_y = -f_y + (x^q-x)f_{xy} + (y^q-y)f_{yy}.$$

So V(h) and V(f) have a common tangent at any GF(q)-rational point of $\mathscr{C}$ that is non-singular. So, if N is the number of GF(q)-rational points of $\mathscr{C}$ and the degree of f is d, then Bézout's theorem implies, when f is not a component of h, that

$$\begin{aligned} (d+q-1)d &= \deg h \deg f \\ &= \text{sum of the intersection numbers at} \\ &\quad\ \text{the points of } V(f) \cap V(h) \\ &\geq 2N. \end{aligned}$$

Hence $N \leq \frac{1}{2}d(d+q-1)$.

Now, suppose that V(f) is a component of V(h), or equivalently that h=0 as a function an V(f). Therefore

$$(x^q-x)f_x/f_y + (y^q-y) = 0,$$
$$(x^q-x)\frac{dy}{dx} - (y^q-y) = 0.$$

Differentiating gives

$$(x^q-x)\frac{d^2y}{dx^2} - \frac{dy}{dx} - \frac{d}{dx}(y^q-y) = 0$$

Remembering that $\frac{d}{dx} = \frac{\partial}{\partial x} + \frac{dy}{dx}\frac{\partial}{\partial y}$, we obtain that

$$(x^q-x)\frac{d^2y}{dx^2} = 0$$

$$\frac{d^2y}{dx^2} = 0.$$

Since $\frac{dy}{dx} = -f_x/f_y$, it follows that

$$\frac{d^2y}{dx^2} = -f_y^{-2}\{f_{xx}f_y^2 - 2f_{xy}f_xf_y + f_{yy}f_x^2\}.$$

THEOREM 4.1: If $\frac{d^2y}{dx^2} \neq 0$, that is, $\mathscr{C}$ is not all inflexions and q is odd, then $N \leq \frac{1}{2}d(d+q-1)$.

In fact $\frac{d^2y}{dx^2} = 0$ can only occur when $\mathscr{C}$ is a line or the characteristic $p \leq d$. For example, when $f = x^{p^r+1} + y^{p^r+1}+1$, then $\mathscr{C}$ is all inflexions. A particular case of this phenomenon is the Hermitian curve $\mathcal{U}_{2,q} = V(X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1})$ when q is a square.

Since every curve of genus 3 can be embedded in the plane as a non-singular quartic, we can see how theorem 4.1 compares with Serre's bound for $N_q(3)$ and its actual value.

q	3	5	7	9	11	13	17	19
$2(q+3)$	12	16	20	24	28	32	40	44
$q+1+3[2\sqrt{q}]$	13	18	23	28	30	35	42	44
$N_q(3)$	10	16	20	28	28	32	40	44

Thus, for q odd with $q \leq 19$ and $q \neq 3$ or 9, the theorem gives the best possible result. A curve achieving $N_9(3)$ is $\mathcal{U}_{2,9}$.

5. WEIERSTRASS POINTS IN CHARACTERISTIC ZERO.

First consider the canonical curve $\mathscr{C}^{2g-2}$ of genus $g \geq 3$ in $PG(g-1,\mathbb{C})$. The <u>Weierstrass points</u>, W-points for short, are the points at which the osculating hyperplane has g coincident intersections. In this case, with w the number of W-points

$$w = g(g^2-1).$$

In any case,

$$2g + 2 \leq w \leq g(g^2-1)$$

with the lower bounded achieved only for hyperelliptic curves. A curve of genus $g > 1$ is <u>hyperelliptic</u> if it has a linear series γ^1_2 (a 2-sheeted covering) on it; for example, a plane quartic with a double point. It has equation

$$y^2 = f(x)$$

with genus $g = [\frac{1}{2}(d-1)]$ where $d = \deg f$.

Consider the case g=3 of the canonical curve $\mathscr{C}^4$, a non-singular plane quartic. The W-points are the 24 inflexions. We note that in characteristic $p > 0$, there is different behaviour; for example, $\mathscr{U}_{2,q}$ has 28 <u>undulations</u> (points where the tangent has 4-point contact). When g=4, the curve $\mathscr{C}^6 = \mathscr{F}^3 \cap \mathscr{F}^2$, the intersection of a cubic and a quadric surface, has 60 <u>stalls</u> where the osculating plane meets the curve at four coincident points.

More generally, still with characteristic zero, if $\mathscr{C}$ has genus $g \geq 1$ and $P \in \mathscr{C}$, there exist integers $n_1, n_2, \ldots, n_g$ such that no function has pole divisor precisely $n_i P$. Also $\{n_1, n_2, \ldots, n_g\} = \{1, 2, \ldots, g\}$ for all but a finite number of points. We elaborate this idea and make it more precise in §§8-10.

6. FUNDAMENTAL DEFINITIONS IN ALGEBRAIC GEOMETRY

Let $\mathscr{C} \subset A^n(K)$ be an irreducible non-singular algebraic curve defined over K, let $I(\mathscr{C}) \subset K[X_1, \ldots, X_n]$ be the ideal of polynomials wich are zero at all points of $\mathscr{C}$, let $\Gamma(\mathscr{C}) = K = [X_1, \ldots, X_n]/I(\mathscr{C})$; and $K(\mathscr{C})$ be the quotient field of $\Gamma(\mathscr{C})$; then $K(\mathscr{C})$ is called the <u>function field</u> of $\mathscr{C}$. Also, for P in $\mathscr{C}$, let $O_P = \{f/g \mid f, g \in \Gamma, g(P) \neq 0\}$, the <u>local ring</u> of $\mathscr{C}$ at P. Then, by natural inclusions, $K \subset \Gamma(\mathscr{C}) \subset O_P(\mathscr{C}) \subset K(\mathscr{C})$. Also $O_P \setminus \{\text{units}\} = M_P = \langle t \rangle$, the maximal ideal, and for any z in O_P there exist a unique unit u and a unique non-negative integer m such that $z = ut^m$; write $m = \mathrm{ord}_P(z)$. Hence, if $G \in K[X_1, \ldots, X_n]$ and g is the image of G in $\Gamma(\mathscr{C})$ with $G(P) \neq 0$, define $\mathrm{ord}_P(G) = \mathrm{ord}_P(g)$. In particular, if $\mathscr{C}$ is a plane curve and V(L) the tangent at P, then $\mathrm{ord}_P(L)$ gives the multiplicity of contact of the tangent with $\mathscr{C}$.

For the extension of these definitions to the projective case, see Fulton [3], p.182. This is the situation we now consider.

A <u>divisor</u> D on $\mathscr{C}$ is $D = \sum_{P\in\mathscr{C}} n_P P$, $n_P \in \mathbf{Z}$, with $n_P = 0$ for all but a finite number of points P; the <u>degree</u> of D is $\deg D = \Sigma n_P$. Then D is <u>effective</u> if $n_P \geq 0$ for all P. For z in $K(\mathscr{C})$, define

$$\begin{aligned} \mathrm{div}(z) &= \mathrm{ord}_P(z)P \\ &= (z)_0 - (z)_\infty \ , \end{aligned}$$

where

$$(z)_0 = \sum_{\mathrm{ord}(z)>0} \mathrm{ord}_P(z)P, \text{ the } \underline{\text{divisor of zeros}},$$

and

$$(z)_\infty = \sum_{\mathrm{ord}(z)<0} -\,\mathrm{ord}_P(z)P, \ \underline{\text{the divisor of poles}};$$

that is, div(z) is the difference of two effective divisors and $\deg \mathrm{div}(z) = 0$.

Given $D = \Sigma n_P P$, define

$$L(D) = \{ f\in K(\mathscr{C}) \mid \mathrm{ord}_P(f) \geq -\, n_P, \ \forall P \} \ ;$$

that is, poles of f are no worse than n_P. In other words, $f\in L(D)$ if $f=0$ or if $\mathrm{div}(f) + D$ is effective.

The set L(D) is a vector space and its dimension is denoted $\ell(D)$.

There is an important equivalence relation on the divisors given by $D \sim D'$ if there exists g in $K(\mathscr{C})$ such that $D - D' = \mathrm{div}(g)$.

7. THE CANONICAL SERIES

Let $\mathscr{C}$ be an irreducible curve in $PG(2,\bar{K})$ where $\bar{K}$ is the algebraic closure of K and let X be a non-singular model of $\mathscr{C}$ with $\Psi: X \to \mathscr{C}$ birational. Points of X are <u>places</u> or <u>branches</u> of $\mathscr{C}$. A place Q is <u>centred</u> at P if $Q\Psi = P$. Let $r_Q = m_P(\mathscr{C})$, the multiplicity of $\mathscr{C}$ at P, where $\mathscr{C}$ has only ordinary singular points. If $\mathscr{C}' = V(G)$ is any other plane curve such that $\mathrm{div}(G)-E$ is effective, where $E = \sum_{Q \in X} (r_Q - 1)Q$, then $\mathscr{C}'$ is an <u>adjoint</u> of $\mathscr{C}$; essentially, $\mathscr{C}'$ passes $m-1$ times through any point of $\mathscr{C}$ of multiplicity m. If $\deg\mathscr{C} = d$ and $\deg\mathscr{C}' = d-3$, then $\mathscr{C}'$ is a <u>special adjoint</u> of $\mathscr{C}$. In this case, $\mathrm{div}(G) - E$ is a <u>canonical</u> divisor. The <u>canonical series</u>, consisting of all canonical divisors, is therefore cut out by all the special adjoints of $\mathscr{C}$. The series is a γ^{g-1}_{2g-2} of (projective) dimension $g-1$ and order $2g-2$. For example,

$$\mathscr{C}^6 = V(z^2xy(x-y)(x+y)+x^6+y^6)$$

is a sextic with an ordinary quadruple point at $P(0,0,1)$ and no other singularity. So

$$g = \frac{1}{2}(6-1)(6-2) - \frac{1}{2}\,4(4-1) = 4 \ .$$

The special adjoints are cubics with a triple point at $P(0,0,1)$, that is triples of lines through the point. A special adjoint has equation $V((x-\lambda_1 y)(x-\lambda_2 y)(x-\lambda_3 y))$ and has freedom 3. It meets $\mathscr{C}^6$ in $6.3-4.3=6$ points other than $P(0,0,1)$. Hence the special adjoints cut out a γ^3_6, as expected.

The Riemann-Roch theorem says that if W is a canonical divisor on X and D is any divisor, then

$$\ell(D) = \deg D + 1 - g + \ell(W-D).$$

8. THE OSCULATING HYPERPLANE OF A CURVE

Let X be an irreducible, non-singular, projective, algebraic curve of genus g defined over K but viewed as the set of points defined over $\bar{K}$, and let $f : X \to \mathscr{C} \subset PG(n,\bar{K})$ be a suitable rational map. Then $\mathscr{C}$ is viewed as the set of branches of X.

Assume that $\mathscr{C}$ is not contained in a hyperplane. The <u>degree</u> d of $\mathscr{C}$ is the number of points of intersection of $\mathscr{C}$ with a generic hyperplane. For any hyperplane H, if n_P is the intersection multiplicity of H and $\mathscr{C}$ at P, then

$$H \cdot \mathscr{C} = \sum_{P \in \mathscr{C}} n_P \, P$$

is a <u>divisor</u> of degree $d = \Sigma n_P$. Also

$$\mathscr{D} = \{H.\mathscr{C} \mid H \text{ a hyperplane}\}$$

is a <u>linear system</u>. In this case, $D \sim D'$ for any D, D' in $\mathscr{D}$. Hence $\mathscr{D}$ is contained in the <u>complete</u> linear system $|D| = \{D' \mid D' \sim D\}$, where D is some element of $\mathscr{D}$.

A complete linear system defines an embedding $f : X \to \mathscr{C}$ given by

$$f(Q) = P(f_0(Q), \ldots, f_n(Q))$$

where $\{f_0, \ldots, f_n\}$ is a basis of

$$L(D) = \{g \in \bar{K}(X) \mid \mathrm{div}(g) + D \geq 0\}.$$

Given a linear system $\mathscr{D}$, the complete system containing $\mathscr{D}$ has the same degree as $\mathscr{D}$ and possibly larger dimension. Hence, although not necessary, it is simpler to consider complete linear systems, and this we do.

Let $\mathscr{C}$ of degree d have associated complete linear system $\mathscr{D}$ and let P be a fixed point of $\mathscr{C}$. Let $\mathscr{D}_i$ be the set of hyperplanes passing through P with multiplicity at least i. Then

$$\mathscr{D} = \mathscr{D}_o \supset \mathscr{D}_1 \supset \ldots \supset \mathscr{D}_d \supset \mathscr{D}_{d+1} = \emptyset.$$

Each $\mathscr{D}_i$ is a projective space. If $\mathscr{D}_i \neq \mathscr{D}_{i+1}$, then $\mathscr{D}_{i+1}$ has codimension one in $\mathscr{D}_i$. Such an i is a $(\mathscr{D},P)$-<u>order</u>. So the $(\mathscr{D},P)$-orders are $j_o,\ldots,j_n$, where

$$0 = j_o < j_1 < j_2 < \ldots < j_n \leq d.$$

Note that $j_1 = 1$ if and only if P is non singular.

For example, let $\mathscr{C}$ be a plane cubic.
Then

$$(j_o,j_1,j_2) = \begin{cases} (0,1,2) & \text{if P is neither singular nor an inflexion,} \\ (0,1,3) & \text{if P is an inflexion,} \\ (0,2,3) & \text{if P is singular.} \end{cases}$$

Note that, as the points of $\mathscr{C}$ are viewed as branches, each branch has a unique tangent.

The <u>Hasse derivative</u>, satisfies the following properties:

(i) $D_t^{(i)}(\Sigma a_j t^j) = \Sigma a_j \binom{j}{i} t^{j-i}$;

(ii) $D_t^{(i)}(fg) = \sum_{j=o}^{i} D_t^{(j)}f \cdot D_t^{(i-j)}g$;

(iii) $D_t^{(i)} D_t^{(j)} = \binom{i+j}{i} D_t^{(i+j)}$.

The unique hyperplane with intersection multiplicity j_n at P is the <u>osculating hyperplane</u> H_P and has equation

$$\det \begin{bmatrix} x_o & \cdots & x_n \\ D^{(j_o)} f_o & & D^{(j_o)} f_n \\ \vdots & & \vdots \\ D^{(j_{n-1})} f_o & & D^{(j_{n-1})} f_n \end{bmatrix} = 0$$

For example, if $\mathscr{C}$ is the twisted cubic in PG(3,K),

$$(f_o, f_1, f_2, f_3) = (1, t, t^2, t^3),$$

$$(j_o, j_1, j_2, j_3) = (0, 1, 2, 3).$$

The osculating hyperplane at $P(1,t,t^2,t^3)$ is

$$\det \begin{bmatrix} x_o & x_1 & x_2 & x_3 \\ 1 & t & t^2 & t^3 \\ 0 & 1 & 2t & 3t^2 \\ 0 & 0 & 1 & 3t \end{bmatrix} = 0 ;$$

that is,

$$t^3 x_o - 3t^2 x_1 + 3t x_2 - x_3 = 0.$$

The point P on $\mathscr{C}$ is a <u>Weierstrass point</u>, W-point for short, if $(j_o, j_1, \ldots, j_n) \neq (0, 1, \ldots, n)$.

Since $\mathscr{D}$ is complete, the Riemann-Roch theorem gives that, if $d > 2g-2$, then

(i) $n = d-g$;

(ii) $\dim \mathscr{D}_i = d-g-i$ for $i \leq d - 2g + 1$;

(iii) $j_i = i$ for $i \leq d - 2g$.

Let $L_i = \cap$ hyperplanes meeting $\mathscr{C}$ at P with $n_P \geq j_i+1$. Then L_i is dual to $\mathscr{D}_i$ and

$$L_o \subset L_1 \subset L_2 \subset \ldots \subset L_{n-1}.$$

Also $L_o = \{P\}$, the set L_1 is the tangent line at P, and L_{n-1} is the osculating hyperplane at P.

The point P is a $\mathscr{D}$-<u>osculation point</u> if $j_n > n$, that is, there exists a hyperplane H such that $n_P > n$.

The integers j_i are characterized by the following result.

THEOREM 8.1 : (i) If $j_o,\ldots,j_{i-1}$ are known, then j_i is the smallest integer r such that $D^{(r)}f(Q)$ is linearly independent of $\{D^{(j_o)}f(Q),\ldots,D^{(j_{i-1})}f(Q)\}$; the latter set spans L_{i-1}.

(ii) If $0 \leq r_o < \ldots < r_s$ are integers such that $D^{(r_o)}f(Q),\ldots,D^{(r_s)}f(Q)$ are linearly independent, then $j_i \leq r_i$.

9. THE GENERALIZED WRONSKIAN

Consider the <u>generalized Wronskian</u>

$$W = \det \begin{bmatrix} D^{(\varepsilon_o)} f_o & \dots & D^{(\varepsilon_o)} f_n \\ \vdots & & \vdots \\ D^{(\varepsilon_n)} f_o & \dots & D^{(\varepsilon_n)} f_n \end{bmatrix}$$

Here the derivations are taken with respect to a separating variable t (dt is the image of t under the map d : $\bar{K}(\mathscr{C}) \to \Omega_{\bar{K}}$; see Fulton [3] p. 203).

The ε_i are required to satisfy the conditions:

(i) $0 = \varepsilon_o < \varepsilon_1 < \dots < \varepsilon_n$;

(ii) $W \neq 0$;

(iii) given $\varepsilon_o, \dots, \varepsilon_{i-1}$, then ε_i is chosen as small as possible such that $D^{(\varepsilon_o)} f, \dots, D^{(\varepsilon_i)} f$ are linearly independent.

Then

(iv) the ε_i are the $(\mathscr{D}, P)$-orders at a general point P;

(v) $\varepsilon_i \leq r_i$ for any $r_o < \dots < r_n$ with $\det (D^{(r_i)} f_j) \neq 0$;

(vi) $\varepsilon_i \leq j_i$ for any P in $\mathscr{C}$;

(vii) the ε_i are called the $\mathscr{D}$-<u>orders</u> of $\mathscr{C}$.

The divisor

$$R = \mathrm{div}(W) + (\sum_0^n \varepsilon_i)\,\mathrm{div}(dt) + (n+1)\sum_P e_P P,$$

where dt is the differential of t and $e_P = -\min_i \mathrm{ord}_P f_i$, is the ramification divisor of $\mathscr{D}$ and depends only on $\mathscr{D}$. Putting R = $= \Sigma\, r_P P$, we have

$$\deg R = \Sigma\, r_P = (2g-2)\Sigma\varepsilon_i + (n+1)d.$$

THEOREM 9.1: $r_P \geq \sum_{i=0}^{n}(j_i - \varepsilon_i)$ with equality if and only if det $C \neq 0 \pmod p$, where $C = (c_{is})$ and $c_{is} = \binom{j_i}{\varepsilon_s}$.

COROLLARY: (i) R is effective.

(ii) $r_P = 0$ if and only if $j_i = \varepsilon_i$ for $0 \leq i \leq n$.

The points P where $r_P = 0$ are called $\mathscr{D}$-ordinary; the others are called $\mathscr{D}$-Weierstrass. The number r_P is the weight of P. When $\mathscr{D}$ is the canonical series, the $\mathscr{D}$-Weierstrass points are simply the Weierstrass points. This coincides with the classical definition.

When $\varepsilon_i = i$, $0 \leq i \leq n$, then $\mathscr{D}$ is classical. Next, the estimate $\varepsilon_i \leq j_i$ is improved.

THEOREM 9.2: (i) Let P on $\mathscr{C}$ have $(\mathscr{D},P)$-orders $j_0,\dots,j_n$ and suppose that det $C' \not\equiv 0 \pmod p$, where $C' = (c'_{is})$ and $c'_{is} = \binom{j_i}{r_s}$, then $D^{(r_0)}f,\dots,D^{(r_n)}f$ are linearly independent and $\varepsilon_i \leq r_i$.

(ii) If $\prod_{i>s} (j_i - j_s)/(i-s) \not\equiv 0 \pmod p$, then $\mathscr{D}$ is classical and $r_P = \sum_{i=0}^{n} (j_i - i)$

(iii) If $p > d$ or $p=0$, then $r_p = \sum_0^n (j_i - i)$ for all P in $\mathscr{C}$.

(iv) If ε is a $\mathscr{D}$-order and μ is an integer with $\binom{\varepsilon}{\mu} \not\equiv 0 \pmod{p}$, then μ is also a $\mathscr{D}$-order.

(v) If ε is a $\mathscr{D}$-order and $\varepsilon < p$, then $0, 1, \ldots, \varepsilon - 1$ are also $\mathscr{D}$-orders.

Entering into this theorem is the classical result of Lucas.

LEMMA 9.3: Let $A = a_o + a_1 p + \ldots + a_m p^m$ and $B = b_o + b_1 p + \ldots + b_n p^m$ be p-adic expansions of A and B with respect to the prime p; that is, $0 \leq a_i, b_i \leq p-1$. Then

(i) $\binom{A}{B} \equiv \binom{a_o}{b_o}\binom{a_1}{b_1} \ldots \binom{a_m}{b_m} \pmod{p}$;

(ii) $\binom{A}{B} \not\equiv 0 \pmod{p}$ if and only if $a_i \geq b_i$, all i;

Proof:
$$(1+x)^A = (1+x)^{\Sigma a_i p^i}$$
$$= (1+x)^{a_o} (1+x^p)^{a_1} \ldots (1+x^{p^m})^{a_m}.$$

Now, the result follows by comparing the coefficient of x^B on both sides.

10. CONSTRUCTION OF SOME LINEAR SYSTEMS

LEMMA 10.1: Let $|D|$ be a complete, non-special linear system and let $j_o,\dots,j_n$ be the $(|D|,P)$-orders, where $n=\dim|D|$. Then the $(|D+P|,P)$-orders are $0,\ j_o+1,\dots,j_n+1$.

THEOREM 10.2: If $|D|$ is a complete, non-special, classical, linear system and $|D'|$ is a complete, base-point-free, linear system, then $|D+D'|$ is classical.

Let $P\in\mathscr{C}$ and let $j_o,\dots,j_n$ be the $(\mathscr{D},P)$-orders for $\mathscr{D}$ canonical. Then $j_o+1=\alpha_1,\dots,j_{g-1}+1=\alpha_g$ are the <u>Weierstrass gaps</u> at P; that is, there does not exist f in $\bar{K}(\mathscr{C})$, regular outside P, such that $\mathrm{ord}_P(f)=-\alpha_i$.

THEOREM 10.3: Let $P\in\mathscr{C}$ and let $\alpha_1,\dots,\alpha_g$ be the Weierstrass gap sequence at P. If the linear system $\mathscr{D}=|dP|$ for some positive integer d, then the $(\mathscr{D},P)$-orders are $\{0,1,\dots,d\}\setminus\{d-\alpha_i \mid \alpha_i \le d\}$.

THEOREM 10.4: With P and $\alpha_1,\dots,\alpha_g$ as above, let V be a canonical divisor, $s\ge 2$ an integer, and $\mathscr{D}=|V+sP|$. Then the $(\mathscr{D},P)$-orders are

$$j_i = i \qquad \text{for } i=0,1,\dots,s-2,$$

$$j_{i+s-2} = s-1+\alpha_i \quad \text{for } i=1,\dots,g\ .$$

THEOREM 10.5: Let P in $\mathscr{C}$ be an ordinary point for the canonical linear system $|V|$ and assume that $|V|$ is classical. Then, for any n such that $0\le n\le g-1$, the linear system $\mathscr{D}=|V-nP|$ is a classical γ^{g-1-n}_{2g-2-n} without base points, and P is $\mathscr{D}$-ordinary.

An important result an linear series is also worth noting.

THEOREM 10.6: The generic curve of genus g has a γ_d^n if and only if

$$d \geq \frac{n}{n+1} g+n.$$

11. THE ESSENTIAL CONSTRUCTION

Given the curve $\mathscr{C}$ with its linear system of hyperplanes and with N the number of its GF(q)-rational points, consider the set $\mathscr{F} = \{P \mid P\varphi \subset H_p\}$; compare §4 for the plane. So $P \epsilon \mathscr{F} \iff$

$$\det \begin{bmatrix} f_o^q & \cdots\cdots & f_n^q \\ D_t^{(j_o)} f_o & \cdots & D_t^{(j_o)} f_n \\ \vdots & & \vdots \\ D_t^{(j_{n-1})} f_o & \cdots & D_t^{(j_{n-1})} f_n \end{bmatrix} = 0$$

To give an outline first, take the classical case in which $j_i = i$. So, let

$$W' = \det \begin{bmatrix} f_o^q & \cdots\cdots\cdots & f_n^q \\ f_o & \cdots\cdots\cdots & f_n \\ \vdots & & \vdots \\ D^{(n-1)} f_o \cdots & & D^{(n-1)} f_n \end{bmatrix}$$

If $W' \neq 0$, then W is a function of degree

$$n(n-1)(g-1) + d(q+n)$$

and the rational points are n-fold zeros of W'. Hence

$$N \leq (n-1)(g-1) + d(q+n)/n.$$

Since $\mathscr{D}$ is complete, $d \leq n+g$; hence

$$N \leq (n-1)(g-1)+(n+g)(q+n)/n$$

$$= q + 1 + g(n + q/n).$$

This has minimum value for $n = \sqrt{q}$, in which case

$$N \leq q + 1 + 2g\sqrt{q}$$

More carefully, let

$$W_t(v,f) = \det \begin{bmatrix} f_o^q & \cdots\cdots & f_n^q \\ D_t^{(v_o)} f_o & \cdots\cdots & D_t^{(v_o)} f_n \\ \vdots & & \vdots \\ D_t^{(v_{n-1})} f_o & & D_t^{(v_{n-1})} f_n \end{bmatrix}$$

where t is a separating variable on $\mathscr{C}$ and $v=(v_o,\ldots,v_{n-1})$ with $0 \leq v_o < \ldots < v_{n-1}$.

THEOREM 11.1: (i) There exist integers $v_o,\ldots,v_{n-1}$, such that $0 \leq v_o < \ldots < v_{n-1}$ and $W_t(v,f) \neq 0$.

(ii) If $v_o,\dots,v_{n-1}$ are chosen successively so that v_i is as small as possible to ensure the linear independence of $D^{(v_o)}f,\dots,D^{(v_i)}f$, then there exists an integer n_o with $0 < n_o \leq n$ such that

$$v_i = \varepsilon_i \quad \text{for} \quad i < n_o,$$

$$v_i = \varepsilon_{i+1} \quad \text{for } i \geq n_o \quad ,$$

where $\varepsilon_o,\dots,\varepsilon_n$ are the $\mathcal{D}$-orders; that is

$$(v_o,\dots,v_{n-1}) = (\varepsilon_o,\dots,\varepsilon_{n_o-1},\varepsilon_{n_o+1},\dots,\varepsilon_n).$$

(iii) If $v'=(v'_o,\dots,v'_{n-1})$ and $W_t(v',f) \neq 0$, then $v_i \leq v'_i$ for all i.

The integers v_i are the <u>Frobenius</u> <u>$\mathcal{D}$-orders</u>. They and S depend only on $\mathcal{D}$, where

$$S = \mathrm{div}(W_t(v,f)) + \mathrm{div}(dt)\,\Sigma\, v_i + (q+n)E,$$

$$\deg S = (2g-2)\,\Sigma\, v_i + (q+n)d.$$

THEOREM 11.2: If $v \leq q$ is a Frobenius $\mathcal{D}$-order, then each non-negative integer u such that $\binom{v}{u} \not\equiv 0 \pmod p$ is a Frobenius $\mathcal{D}$-order. In particular, if $v_i < p$, then $v_j = j$ for $j \leq i$.

THEOREM 11.3: (i) If P is a GF(q)-rational point of $\mathcal{C}$, then

$$m_P(S) \geq \sum_{i=1}^{n}(j_i - v_{i-1}),$$

with equality if and only if det $C \not\equiv 0 \pmod p$, where

$$C = (c_{ir}) \text{ and } c_{ir} = \binom{j_i}{v_{r-1}}, \quad i,r=1,\dots,n.$$

(ii) If $P \in \mathscr{C}$ but not GF(q)-rational, then

$$m_p(S) \geq \sum_{i=1}^{n-1}(j_i - v_i).$$

If det $C' \equiv 0 \pmod p$, the inequality is strict, where

$$C' = (c'_{ir}) \text{ and } c'_{ir} = \binom{j_i - 1}{v_{r-1}}, \quad i,r=1,\dots,n.$$

THEOREM 11.4: Let P be a GF(q)-rational point of $\mathscr{C}$. If $0 \leq m_0 < \dots < m_{n-1}$ and det $C'' \not\equiv 0 \pmod p$, then $v_i \leq m_i$ for all i, where $C'' = (c''_{ir})$ and

$$c''_{ir} = \binom{j_i - j_1}{m_{r-1}}, \quad i,r = 1,\dots,n.$$

COROLLARY 1: (i) If P is a GF(q)-rational point of $\mathscr{C}$, then $v_i \leq j_{i+1} - j_i$ for $i=0,\dots,n-1$ and $m_p(S) \geq nj_1$.

(ii) If (a) $\prod_{1 \leq i < r \leq n} (j_r - j_i)/(r-i) \not\equiv 0 \pmod p$, or (b) $j_i \not\equiv j_r \pmod p$ for $i \neq r$, or (c) $p \geq d$, then $v_i = i$ for $i=0,\dots,n-1$ and $m_p(S) = n + \sum_{i=1}^{n}(j_i - i)$.

COROLLARY 2: If $v_i \neq \varepsilon_i$ for some $i < n$, then each GF(q)-rational point of $\mathscr{C}$ a $\mathscr{D}$-Weierstrass point.

COROLLARY 3: If $\mathscr{C}$ has some GF(q)-rational point, then $v_i \leq i+d-n$, all i. If also $\mathscr{D}$ is complete, then $v_i = i$ for $i < d - 2g$.

THEOREM 11.5: (THE MAIN RESULT) Let X be an irreducible, non-singular, projective, algebraic curve of genus g defined over K = GF(q) with N rational points. If there exists on X a linear system γ_d^n without base points, and with order sequence $\varepsilon_o,\ldots,\varepsilon_n$ and Frobenius order sequence $v_o,\ldots,v_{n-1}$, then

$$N \leq \frac{1}{n}\{(2g-2)\sum_{o}^{n-1} v_i + (q+n)d\}.$$

If also $v_i = \varepsilon_i$ for $i < n$, then

$$\varepsilon_n N + \sum_P a_P + \sum_{P'} b_{P'} \leq (2g-2)\sum_{o}^{n-1}\varepsilon_i + (q+n)d,$$

where P is a K-rational point of X, where $P' \epsilon X$ but not K-rational and where

$$a_P = \sum_{i \leq n}(j_i - \varepsilon_i), \quad b_P = \sum_{i < n}(j_i - \varepsilon_i)$$

with $j_o,\ldots,j_n$ the $(\mathscr{D},P)$-orders.

COROLLARY: $|N-(q+1)| \leq 2g\sqrt{q}$.

THEOREM 11.6: If X is non-singular, $p \geq g \geq 3$ with $q = p^h$, and the canonical system is classical, then

$$N \leq 2q + g(g-1).$$

Notes: (1) If $p \geq 2g-1$, then the canonical system is classical.

(2) This gives a better bound than $S_g = q+1 + g[2\sqrt{q}]$ when $|\sqrt{q}-g|<\sqrt{g+1}$.

THEOREM 11.7: If X is non-singular and not hyperelliptic, with $\frac{1}{2}(p+3) \geq g \geq 3$, then

$$N \leq \left(\frac{2g-3}{g-2}\right)q + g(q-2).$$

Note : This is better than S_g when

$$\left|\sqrt{q} - \frac{g(g-2)}{g-1}\right|<\{(g-2)(g^2-g-1)\}^{\frac{1}{2}}/(g-1).$$

THEOREM 11.8: If X is non-singular with classical canonical system and a K-rational point, then

$$N \leq (g-n-2)(g-1)+(2g-n-2)(q+g-n-1)(g-n-1)^{-1}$$

for $0 \leq n \leq g - 1$.

12. ELLIPTIC CURVES

The number of elements of a γ_d^n on a curve of genus g with n+1 coincident points, that is $\mathscr{D}$-Weierstrass points, is $(n+1)(d+ng-n)$. When $g=1$, this number is $d(n+1)$. If $\mathscr{D}$ consists of all curves of degree r and $\mathscr{C}$ is a plane non-singular cubic, then $n=\frac{1}{2}r(r+3)$, $d = 3r$. The condition for a γ_d^n to exist is, from Theorem 10.6, that $d \geq n/(n+1)+n$. So this only allows γ_3^2 and γ_6^5, whence $d=n+1$ and the number of $\mathscr{D}$-Weierstrass points is $(n+1)^2$. From the Riemann-Roch theorem, as every series is non-special on $\mathscr{C}$, a complete series γ_d^n satisfies d = n+1.

For n=2, the $\mathcal{D}$-Weierstrass points are the 9 inflexions. For n=5, they are the 9 inflexions (repeated) plus the 27 sextactic points (6-fold contact points of conics = points of contact of tangents through the inflexions).

The above holds for the complex numbers; for finite fields, the result is the following.

THEOREM 12.1: (i) If $p \nmid (n+1)$, the $\mathcal{D}$-W-points have multiplicity one .

(ii) If $p^k | (n+1)$, $p^{k+1} \nmid (n+1)$ with $k \geq 1$, then one of the following holds:

(a) $\mathcal{C}$ is ordinary and there are $(n+1)^2/p^k$ $\mathcal{D}$-W-points with multiplicity p^k;

(b) $\mathcal{C}$ is supersingular and there are $(n+1)^2/p^{2k}$ $\mathcal{D}$-W-points with multiplicity p^{2k}.

THEOREM 12.2: If $\mathcal{C}$ is elliptic with origin 0 and $\mathcal{D}$ is a complete linear system on $\mathcal{C}$, then

(i) $\mathcal{D}$ is classical;

(ii) $\mathcal{D}$ is Frobenius classical except perhaps when $\mathcal{D} = |(\sqrt{q}+1)0|$;

(iii) $|(\sqrt{q}+1)0|$ is Frobenius classical if and only if $N < (\sqrt{q}+1)^2$.

13. HYPERELLIPTIC CURVES

As in §5, if $p \neq 2$, then $\mathcal{C}$ has homogeneous equation $y^2z^{d-2}=z^d f(x/z)$ with $g=[\frac{1}{2}(d-1)]$. Let $g > 1$ and let $P_1,\ldots,P_n$ be the ramification points of the double cover (= double points of the γ_2^1 on $\mathcal{C}$);

then $n=2(g+1)$ from the formula beginning §12. When d is even, they are the points with $y=0$; when d is odd, they are these plus $P(0,1,0)$. Let n_o be the number of K-rational P_i.

THEOREM 13.1: Let $\mathscr{C}$ be hyperelliptic with a complete $\gamma_2^1 = |D|$ and n,n_o as above. If there is a positive integer n_1 such that $|(n_1+g)D|$ is Frobenius classical, then

$$|N-(q+1)| \leq g(2n_1+g)+(2n_1+g)^{-1}\{g(q-n_o)-g^3-g\}.$$

Note: If $p \geq 2(n_1+g)$, then the hypothesis is fulfilled.

COROLLARY: Let $p \geq 5$ with $p=c^2+1$ or $p=c^2+c+1$ for some positive integer c and let $\mathscr{C}$ be hyperelliptic with $g>1$ over $GF(p)$. Then

$$|N-(p+1)| \leq g[2\sqrt{p}] - 1.$$

14. PLANE CURVES

Let $\mathscr{C}$ be a non-singular, plane curve of degree d over $K=GF(q)$; then $g = \frac{1}{2}(d-1)(d-2)$. Let D be a divisor cut out by a line, which can be taken as $z=0$.

Let x,y be affine coordinates. The monomials $x^i y^j$, $i,j\geq 0$, $i+j\leq m$ span $L(mD)$ and are linearly independent for $m < d$. Hence $\dim|mD| = \frac{1}{2}m(m+3)$ for $m < d$. Also, mD is a special divisor for $m \leq d-3$. Thus $|mD|$ is cut out by all curves of degree m.

THEOREM 14.1: Let $\mathscr{C}$ be a plane curve of degree d and let D be a divisor cut out by a line. If m is a positive integer with $m \leq d - 3$ such that $|mD|$ is Frobenius classical, then

$$N \leq \tfrac{1}{2}(m^2+3m-2)(g-1)+2d(m+3)^{-1}\{q+\tfrac{1}{2}m(m+3)\}.$$

Proof. Put (i) $\frac{1}{2}m(m+3)$ for n, (ii) $\frac{1}{2}(d-1)(d-2)$ for g, (iii) md for d, (iv) i for v_i, in theorem 11.5.

Notes: (1) When $m \leq p/d$, then $|mD|$ is Frobeinius classical.

(2) For m=1, we have that $4 \leq d \leq p$ implies that

$$N \leq \frac{1}{2}d(d+q-1),$$

as in theorem 4.1.

(3) For m=2, we have that $5 \leq d \leq \frac{1}{2}p$ implies that

$$N \leq \frac{2d}{5}\{5(d-2)+q\} \quad ,$$

which is required in theorem 19.1.

Let f(x,y) be homogeneous of degree d with f(x,1) having distinct roots in $\bar{K}$. A <u>Thue curve</u> is given by

$$\mathscr{C}_d \ : \ f(x,y) = z^d.$$

It is non-singular.

THEOREM 14.2: Let D be a divisor cut out by a line on $\mathscr{C}_d$. If m is a positive integer such that $|mD|$ is Frobenius classical, then

$$N \leq (n-1)(g-1) + \frac{1}{n}\{md(q+n)-d\ A_m-d_oB_m\} \quad ,$$

where n is the dimension of $|mD|$;

$$n=\begin{cases} \frac{1}{2}m(m+3) \text{ for } m \leq d-3 \\ \\ dm - g \quad \text{for } m > d-3 \ , \end{cases}$$

$g = \frac{1}{2}(d-1)(d-2)$,

d_o = number of K-rational roots of $f(x,1)$,

$$A_m = \begin{cases} \frac{1}{24}m(m-1)\{4(d-m-1)(m+4)+(m-2)(m-5)\} & \text{for } m \leq d-3 \\ \frac{1}{24}(d-1)(d-2)(d-3)(d+4) & \text{for } m > d-3, \end{cases}$$

$$B_m = \begin{cases} dm - \frac{1}{2}m(m+3) & \text{for } m \leq d-3 \\ g & \text{for } m > d-3. \end{cases}$$

Note: When $m \leq p/d$, then $|mD|$ is Frobenius classical.

A <u>Fermat curve</u> is a special case of a Thue curve given by

$$\mathscr{F}_d : ax^d + by^d = z^d$$

with $a,b \in K\setminus\{0\}$.

THEOREM 14.3: For $\mathscr{F}_d$ with the same conditions as above,

$$N \leq (n-1)(g-1) + \frac{1}{n}\{md(q+n)-3d\, A_m - d_1\, B_m\}$$

with n,g,A_m,B_m as above, but d_1 is the number of points of $\mathscr{F}_d$ with $xyz = 0$.

15. THE MAXIMUM NUMBER OF POINTS ON AN ALGEBRAIC CURVE

In Table 1, we give the value of $N_q(g)$ or the best, known bound for $g \leq 5$ and $q \leq 49$ arising from results of Serre [12],[13] and the preceding sections. Also included in the table is the bound $S_g = q+1+g[2\sqrt{q}]$; see §2.

TABLE 1

The maximum number points on an algebraic curve

q	$[2\sqrt{q}]$	$N_q(1)$	$N_q(2)$	S_2	$N_q(3)$	S_3	$N_q(4)$	S_4	$N_q(5)$	S_5
2	2	5	6	7	7	9	8	11	9	13
3	3	7	8	10	10	13	12	16	≤ 15	19
4	4	9	10	13	14	17	15	21	≤ 18	25
5	4	10	12	14	16	18	18	22	≤ 22	26
7	5	13	7	18	20	23	24-25	28	≤ 29	33
8	5	14	18	19	24	24		29	≤ 32	34
9	6	16	20	22	28	28	26-30	34	≤ 36	40
11	6	18	24	24	28	30	32-34	36	≤ 40	42
13	7	21	26	28	32	35	36-38	42	≤ 45	49
16	8	25	33	33	38	41		49		57
17	8	26	32	34	40	42	≤ 46	50	≤ 54	58
19	8	28	36	36	44	44	≤ 50	52	≤ 58	60
23	9	33	42	42	≤ 48	51	≤ 58	60	≤ 66	69
25	10	36	46	46	56	56	66	66		76
27	10	38	48	48		58		68		78
29	10	40	50	50		60		70	≤ 78	80
31	11	43	52	54		65	≤ 74	76	≤ 82	87
32	11	44	53	55		66		77		88
37	12	50	60	62		74		86	≤ 94	98
41	13	54	66	68		81		94	≤ 102	107
43	13	57	68	70		83		96	≤ 106	109
47	13	61	74	74		87		100		113
49	14	64	78	78	92	92		106		120

16. ELLIPTIC CURVES: FUNDAMENTAL ASPECTS.

The theory of elliptic curves over an arbitrary field K offers an appealing mixture of geometric and algebraic arguments. Let $\mathscr{C}$ be a non-singular cubic in PG(2,q). For the projective classification when K = GF(q), see [6] Chapter 11. Although $\mathscr{C}$ may have no inflexion, up to isomorphism it may be assumed to have one, O.

THEOREM 16.1: If $\mathscr{C}'$, $\mathscr{C}''$ are cubic curves in PG(2,K) such that the divisors $\mathscr{C}.\mathscr{C}' = \sum_{i=1}^{9} P_i$ and $\mathscr{C}.\mathscr{C}'' = \sum_{i=1}^{8} P_i + Q$, then $Q = P_9$.

Proof. (Outline) Through $P_1,\dots,P_8$ there is a pencil $\mathscr{F}$ of cubic curves to which $\mathscr{C}$, $\mathscr{C}'$, $\mathscr{C}''$ belong. Any curve of $\mathscr{F}$ has the form $V(F+\lambda G)$ and so contains $V(F)\cap V(G)$. By Bézout's theorem $|V(F)\cap V(G)|=9$. Hence $Q = P_9$.

For a detailed proof, see [3], Chapter 5.

Theorem 16.1 is known as the theorem of the nine associated points. It has numerous corollaries of which we give a variety before the important theorem 16.7.

THEOREM 16.2: Any two inflexions of $\mathscr{C}$ are collinear with a third.

Proof. Let P_1, P_2 be inflexions of $\mathscr{C}$ with corresponding tangents ℓ_1, ℓ_2. Let $\ell = P_1P_2$ meet $\mathscr{C}$ again at P_3, and let ℓ_3 be the tangent at P_3 meeting $\mathscr{C}$ again at Q. Then

$$\mathscr{C}.\ell_1 = 3P_1 \quad , \quad \mathscr{C}.\ell_2 = 3P_2, \quad \mathscr{C}.\ell_3 = 2P_3+Q$$

$$\mathscr{C}.\ell = P_1 + P_2 + P_3 .$$

Hence

$$\mathscr{C}.\ell_1\ell_2\ell_3 = 3P_1 + 3P_2 + 2P_3 + Q$$

$$\mathscr{C}.\ell^3 = 3P_1 + 3P_2 + 3P_3 \quad .$$

By the previous theorem, $Q = P_3$; so P_3 is an inflexion.

THEOREM 16.3. If P_1 and Q_1 are any two points of $\mathscr{C}$, the cross-ratio of the four tangents through P_1 is the same as the cross-ratio of the four tangents through Q_1.

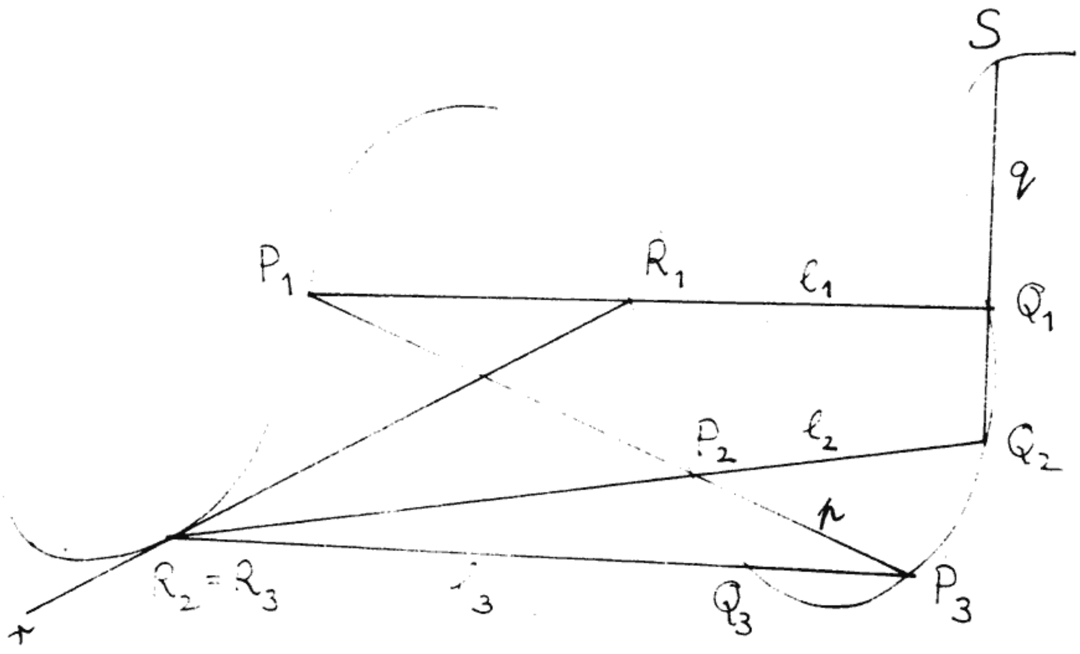
Proof. Let P_1Q_1 meet $\mathscr{C}$ again at R_1. Let r be a tangent to through R_1 with point of contact $R_2=R_3$. Let $P_1\ P_2\ P_3$ be any line through P_1 with P_2,P_3 on $\mathscr{C}$. Let R_2P_2 meet $\mathscr{C}$ again at Q_2 and let R_3P_3 meet $\mathscr{C}$ again at Q_3. We use the previous theorem to show that Q_1,Q_2,Q_3 are collinear.

Write $\ell_i = P_iR_iQ_i$, $i=1,2,3$; let $p=P_1P_2P_3$, $r=R_1R_2$, $q=Q_1Q_2S$ with S the third point of Q on $\mathscr{C}$.

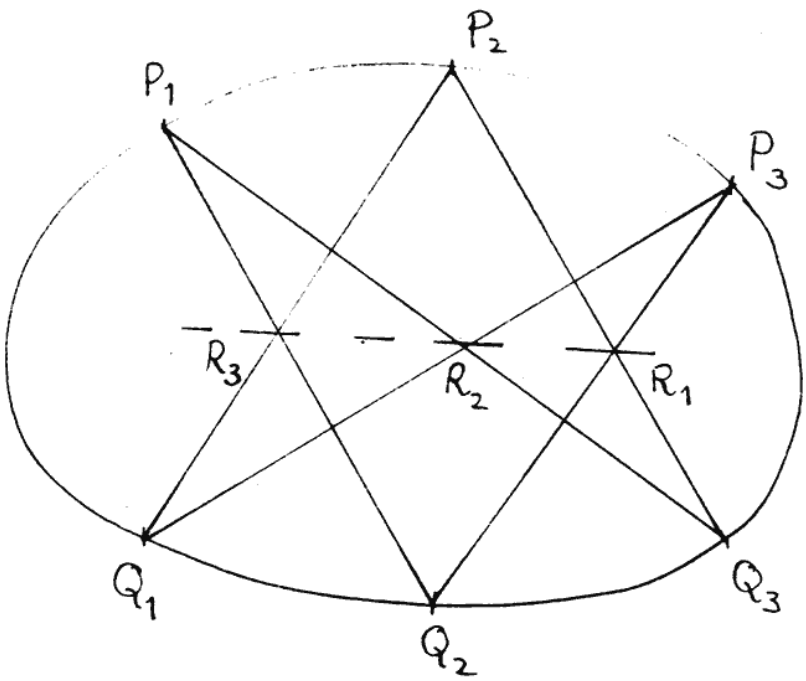
Then $\mathscr{C}.\ell_1\ell_2\ell_3 = \sum_{i=1}^{3}(P_i+Q_i+R_i)$

$$\mathscr{C}.\ prq = \sum_{i=1}^{3} (P_i+R_i) + Q_1+Q_2+S.$$

Again by theorem 16.1, $S = Q_3$. When P_2 and P_3 coincide, so do Q_2 and Q_3. So there is an algebraic bijection τ from the pencil $\mathscr{F}$ through P_1 and the pencil G through Q_1 in which the tangents correspond. Hence τ is projective and the cross-ratios of the tangents are equal.



THEOREM 16.4. (Pascal's Theorem)



If $P_1Q_2P_3Q_1P_2Q_3$ is a hexagon inscribed in a conic $\mathscr{P}$,then the intersections of opposite sides, that is R_1,R_2,R_3, are collinear.

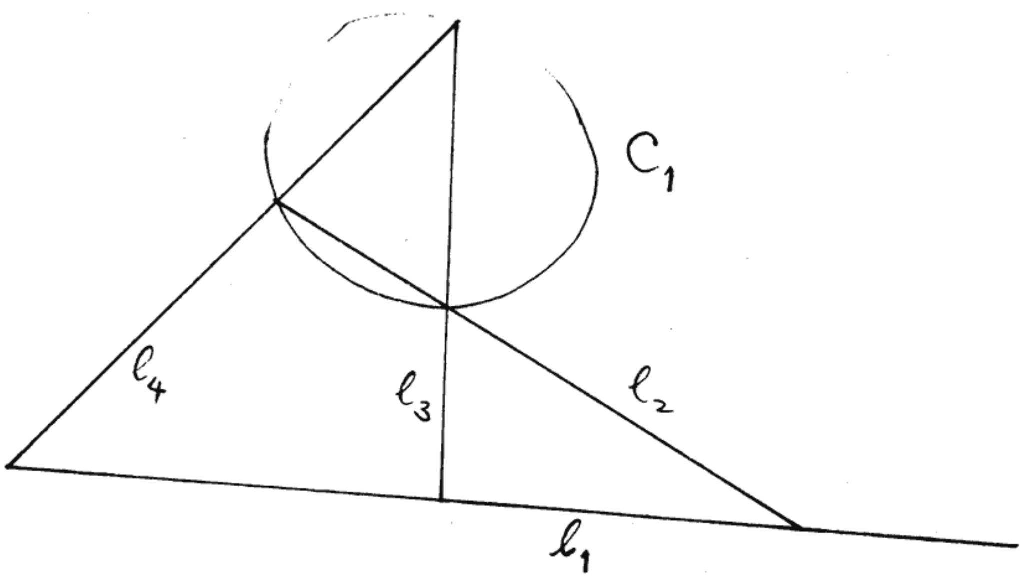
Proof. The two sets of three lines

$$P_1Q_2)(P_3Q_1)(P_2Q_3) \quad \text{and} \quad (Q_1P_2)(Q_3P_1)(Q_2P_3)$$

are cubics through the nine points P_i, Q_i, R_i, $i=1,2,3$; there is an irreducible cubic $\mathscr{C}$ in the pencil they determine. Also in the pencil is the cubic consisting of $\mathscr{P}$ and the line R_3R_2. So, by theorem 16.1, this cubic contains the ninth point R_1, which cannot lie on $\mathscr{P}$. So $R_3R_2R_1$ is a line.

THEOREM 16.5: Let $\ell_1, \ell_2, \ell_3, \ell_4$ be the sides of a complete quadrilateral in an affine plane and let C_i be the circumcircle of the triangle obtained by deleting ℓ_i. Then $C_1 \cap C_2 \cap C_3 \cap C_4 = \{P\}$.

Proof.



There is a pencil of cubics through the vertices of the quadrilateral and the two circular points at infinity. The four cubics $C_i + \ell_i$, $i=1,2,3,4$, contain these eight points and therefore the ninth associated point P. As each ℓ_i contains three of the eight initial points, it does not contain P. Hence P lies on each C_i.

Now we show that an elliptic curve $\mathscr{C}$ is an abelian group. As above we take O as an inflexion.

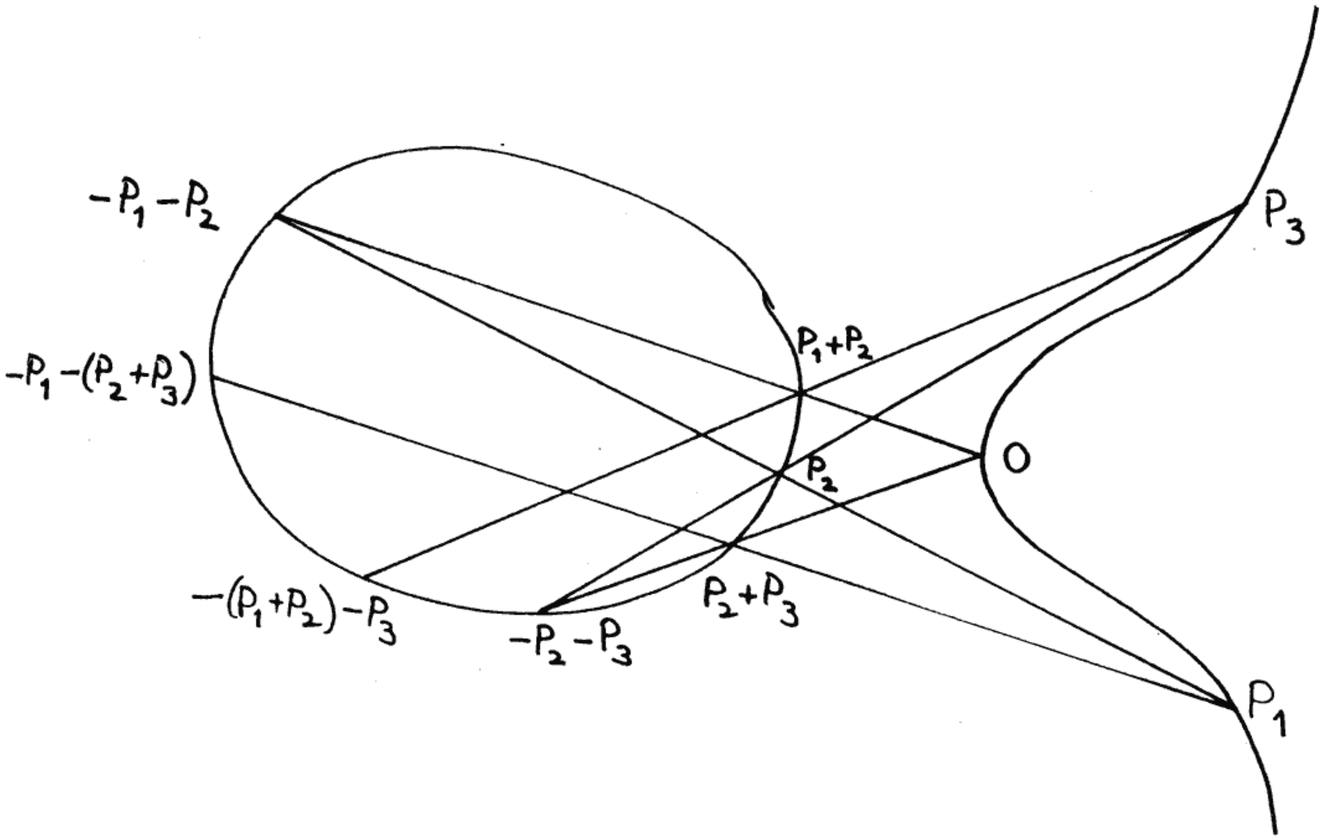
Definition: For P,Q on $\mathscr{C}$, let $\mathscr{C}.PQ=P+Q+R$ and let $\mathscr{C}.OR=O+R+S$; define $S = P+Q$.

LEMMA 16.6: (i) On $\mathscr{C}$, the points $O,P,-P$ are collinear.

(ii) P,Q,R are collinear on $\mathscr{C}$ if and only if $P+Q+R=O$.

THEOREM 16.7: Under the additive operation, $\mathscr{C}$ is an abelian group.

Proof. The only non-trivial property to verify is the associative law.



Apart from $\mathscr{C}$, consider the two cubics consisting of three lines given by the rows and columns of the array

$$\begin{array}{ccc} P_1 & P_2 & -P_1-P_2 \\ P_2+P_3 & P_2-P_3 & 0 \\ X & P_3 & P_1+P_2 \end{array}$$

Again, by theorem 16.1, X lies on both these cubics. So, $X = -P_1-(P_2+P_3) = -(P_1+P_2)-P_3$; hence, if Y is the third point of $\mathscr{C}$ on OX, then

$$Y = P_1+(P_2+P_3) = (P_1+P_2)+P_3.$$

Note: $\mathscr{C}$ has been drawn as $y^2=(x-a)(x-b)(x-c)$ with $a<b<c$, but the point of inflexion natural to this picture is at infinity.

THEOREM 16.8: (Waterhouse [21]). For any integer $N=q+1-t$ with $|t| \leq 2\sqrt{q}$, there exists an elliptic cubic in $PG(2,q)$, $q= p^h$, with precisely N rational points if and only if one of the following conditions on t and q is satisfied:

(i)	$(t,p) = 1$	
(ii)	$t = 0$	h odd or $p \not\equiv 1 \pmod 4$
(iii)	$t = \pm\sqrt{q}$	h even and $p \not\equiv 1 \pmod 3$
(iv)	$t = \pm 2\sqrt{q}$	h even
(v)	$t = \pm\sqrt{2q}$	h odd and $p = 2$
(vi)	$t = \pm\sqrt{3q}$	h odd and $p = 3$

COROLLARY: $N_q(1) = \begin{cases} q + [2\sqrt{q}] & \text{if } p \text{ divides } [2\sqrt{q}], \\ & h \text{ is odd and } h \geq 3; \\ q+1+[2\sqrt{q}] & \text{otherwise.} \end{cases}$

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 $U_0 = P(1,0,0)$, $U_1 = P(0,1,0)$, $U_2 = P(0,0,1)$.
Also, with $K = GF(q)$, let $K_0 = GF(q) \setminus \{0\}$ and $K_0^2 = \{t^2 \mid t \in K_0\}$.

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

$$y^2 z = x^3 + a_2 x^2 z + a_1 x z^2 + a_0 z^3.$$

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 $a_0 = 0$ and $\mathscr{C}$ has equation

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

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

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

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

$$y^2 = \nu^3 x^4 + \nu^2 a_2 x^2 + \nu a_1 \ . \qquad (17.2)$$

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

$$U = \nu x^2, \quad Z = xy, \quad A = (y_0 - Z)/(x_0 - U),$$

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

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

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

$$Z^2 = U^3 + a_2 U^2 + a_1 U \ . \qquad (17.3)$$

Hence

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

(2) PP_0 has equation $y-Z = A(x-U)$;

(3) PP_0 meets $\mathscr{C}$ is two points other than P whose x-coordinates satisfy

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

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 a nd 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_0 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 $A = y_0$.

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

$$(y^2+xy)z = x^3+a_1xz^2+a_0z^3.$$

Instead of Θ as above, we define $\Theta : \mathscr{C} \to K/C_0$ where $C_0=\{t\in K|T(t)=0\}$ and $T(t) = t+t^2+\ldots t^{q/2}$; here C_0 in the set of elements of category (= trace) zero. Take $P(x,y,1)\Theta = xC_0$. 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];

$\frac{1}{4}q$, [11]

$2q^{9/10}$, q large, [15];

cq, $c \leq \frac{1}{2}$, q large [16];

These examples all lie an rational curves, namely conics or singular cubics; to be precise the k-arcs of order $\frac{1}{2}q$ have one point off a conic. The examples of §17 are the only other ones known.

Conjecture: For each k such that

$$n(2,q) \leq k \leq m'(2,q),$$

these exists a complete k-arc in PG(2,q).

In fact, although the conjecture is true for $q \leq 13$, it is probably more realistic to ask for the smallest value of q for which the conjecture is false.

In Table 2, we give m, m' and n for $q \leq 13$.

q	2	3	4	5	7	8	9	11	13
m	4	4	6	6	8	10	10	12	14
m'	4	4	6	6	6	6	8	10	12
n	4	4	6	6	6	6	6	7	8

Upper bounds for m'(2,q) are as follows:

$m'(2,q) \leq q - \frac{1}{4}\sqrt{q} + \frac{25}{16}$, q odd, [17];

$m'(2,q) \leq q - \sqrt{q} + 1$, $q = 2^h$, [6], theorem 10.3.3.

$m'(2,q) = q - \sqrt{q} + 1$, $q = 2^{2r}$, [2].

19. AN IMPROVEMENT ON THE BOUND FOR m'(2,q) WHEN q IS PRIME

THEOREM 19.1: (Voloch [20]). For a prime $p \geq 7$,

$$m'(2,p) \leq \frac{44}{45}p + \frac{8}{9}.$$

Proof. A theorem of Segre (see [6], theorem 10.4.4) says that, for q odd with $q \geq 7$, we have $m'(2,q) \leq q - \frac{1}{4}\sqrt{q} + \frac{7}{4}$ and we follow the structure of this proof.

Let $\mathscr{K}$ be a complete k-arc with $k > \frac{44}{45}p+\frac{8}{9}$. Through each point P of $\mathscr{K}$ there are $t = p+2-k$ unisecants. The kt unisecants of $\mathscr{K}$ belong to an algebraic envelope Δ_{2t} of class 2t, which has a simple component Γ_n with $n \leq 2t$. For t=1, the envelope Δ_2 is the dual of a conic, $\mathscr{K}$ is a (q+1)-arc and so a conic. When $t \geq 2$, four cases are d stinguished.

(i) Γ_n <u>is a regular (rational) linear component</u>.

Here Γ_n is a pencil with vertex Q not in $\mathscr{K}$. Then $\mathscr{K} \cup \{Q\}$ is a (k+1)-arc and $\mathscr{K}$ is not complete.

(ii) Γ_n <u>is regular of class two.</u>

Here Γ_n is the dual of a conic $\mathscr{C}$, and $\mathscr{K}$ is contained in $\mathscr{C}$, [6] theorem 10.4.3.

(iii) Γ_n is irregular.

Suppose that Γ_n has M simple lines and d double lines, and let N=M+d. Then, by [6] lemma 10.1.1, it follows that $N \leq n^2$. Also by the definition of Δ_{2t} and Γ_n, there are at least $\frac{1}{2}n$ distinct lines of Γ_n through P; so $N \geq \frac{1}{k}$ kn. Therefore $k \leq 2N/n \leq 2n \leq 4t=$

$= 4(p+2-k)$. Thus $k \leq \frac{4}{5}(p+2) < \frac{44}{45}p + \frac{8}{9}$, a contradiction for $p \geq 5$.

(iv) Γ_n is regular with $n \geq 3$.

Either $n=2t \leq \frac{1}{2}p$ or $t > \frac{1}{4}p$. When $t > \frac{1}{4}p$, then $k=p+2-t < \frac{3}{4}p+2 < \frac{44}{45}p+\frac{8}{9}$ for $p \geq 5$.

When $n \leq \frac{1}{2}p$, then

$$N \leq \frac{2n}{5}\{5(n-2)+p\}$$

for $n \geq 5$ by theorem 14.1, note (3); for $n \geq 3$ it follows from theorem 11.5 when we note that $n \leq \frac{1}{2}p$ implies $v_i = i$ by theorem 11.4, corollary 1 (ii).

As in (iii), $N \geq \frac{1}{2}kn$. So

$$\frac{1}{2}kn \leq N \leq \frac{2n}{5}\{5(n-2) + p\},$$

$$k \leq \frac{4}{5}\{5(n-2)+p\},$$

$$k \leq \frac{4}{5}\{5(2t-2)+p\}.$$

Substituting $t = p+2-k$ gives

$$k \leq \frac{4}{5}\{10(p+1-k)+p\},$$

$$k \leq \frac{4}{45}(11p + 10),$$

the required contradiction.

COROLLARY: For any prime $p \geq 311$,

$$\frac{1}{2}(p+[2\sqrt{p}]) \leq m'(2,p) \leq \frac{4}{45}(11p+10).$$

Notes: (1) $\frac{4}{45}(11p+10) < p - \frac{1}{4}\sqrt{p} + \frac{25}{16}$ for $p \geq 47$.

(2) $\frac{4}{45}(11p+10) < p - \sqrt{p}+1$ for $p \geq 2017$.

20. k-CAPS IN PG(n,q), $n \geq 3$.

A k-cap in PG(n,q) is a set of k points no 3 collinear. Let $m_2(n,q)$ be the maximum value that k can attain. From §19, $m(2,q) = m_2(2,q)$. For $n \geq 3$, the only values known are as follows:

$$m_2(3,q) = q^2+1, \qquad q > 2;$$

$$m_2(d,2) = 2^d;$$

$$m_2(4,3) = 20;$$

$$m_2(5,3) = 56.$$

See [8] for a survey on these and similar numbers. The sets corresponding to these values for $m_2(d,q)$ have been classified apart from (q^2+1)-caps for q even with $q \geq 16$.

As for the plane, let $m_2(n,q)$ be the size of the second largest complete k-cap. Then, from [9], chapter 18,

$$m_2'(3,2) = 5 \quad , \; m_2'(3,3) = 8.$$

We now summarize the best known upper bounds for $m_2'(n,q)$ and $m_2(n,q)$.

THEOREM 20.1: ([7]) For q odd with $q \geq 67$,

$$m_2'(3,q) \leq q^2 - \frac{1}{4}q\sqrt{q} + 2q.$$

THEOREM 20.2: ([10]) For q even with $q > 2$,

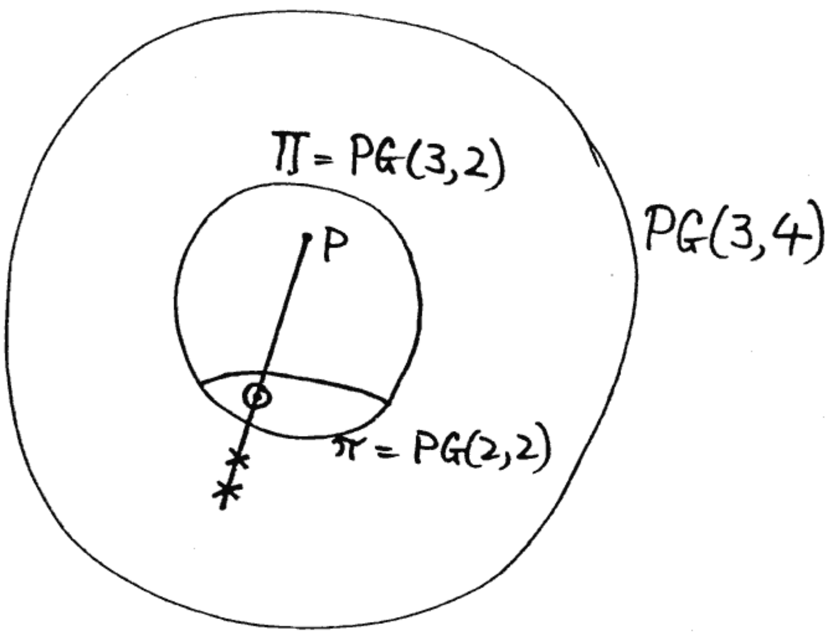
$$m_2'(3,q) \leq q^2 - \frac{1}{2}q - \frac{1}{2}\sqrt{q} + 2.$$

This gives that $m_2'(3,4) \leq 15$.

THEOREM 20.3: ([10]) $m_2'(3,4) = 14$.

In fact, a complete 14-cap in PG(3,4) is projectively unique and is obtained as follows.

Let π be a PG(2,2) in PG(3,4), let P be a point not in π, and let Π be a PG(3,2) containing P and π. Each of the seven lines joining P to a point of π contains three points in π and two points not in Π. The 14 points on the lines through P not in Π form the desired cap.



THEOREM 20.4: ([7]) For q odd, $q \geq 121$, $n \geq 4$,

$$m_2(n,q) < q^{n-1} - \frac{1}{4}q^{n-3/2} + 3q^{n-2}.$$

THEOREM 20.5: ([10]) For even, $q \geq 4$, $n \geq 4$,

$$m_2(n,q) \leq q^{n-1} - \frac{1}{2}q^{n-2} + \frac{5}{2}q^{n-3}.$$

REFERENCES

[1] V.ABATANGELO, A class of complete $[(q+8)/3]$-arcs of PG(2,q); with $q=2^h$ and $h(\geq 6)$ even, **Ars Combin.** 16(1983), 103-111.

[2] J.C.FISHER, J.W.P.HIRSCHFELD, and J.A.THAS, Complete arcs in planes of sequence order, **Ann.Discrete Math.** 30(1986), 243-250.

[3] W.FULTON, **Algebraic curves**, Benjamin, 1969.

[4] D.G.GLYNN, Two new sequences of ovals in finite Desarguesian planes of even order, **Combinatorial Mathematics X**, Lecture Notes in Math. 1036, Springer, 1983, 217-229.

[5] R.HARTSHORNE, **Algebraic geometry**, Springer, 1977.

[6] J.W.P.HIRSCHFELD, **Projective geometries over finite fields**, Oxford, 1979.

[7] J.W.P.HIRSCHFELD, Caps in elliptic quadrics, **Ann. Discrete Math.** 18 (1983), 449-466.

[8] J.W.P.HIRSCHFELD, Maximum sets in finite projective spaces, **London Math.Soc. Lecture Note Series** 82(1983), 55-76.

[9] J.W.P.HIRSCHELD, **Finite projective spaces of three dimensions**, Oxford, 1985.

[10] J.W.P.HIRSCHFELD and J.A.THAS, Linear independence in finite spaces. **Geom. Dedicata**, to appear.

[11] G.KORCHMAROS, New examples of complete k-arcs in PG(2,q), **European J.Combin.** 4(1983), 329-334.

[12] J.-P.SERRE, Nombres de points des courbes algébriques sur F_q, Seminaire de Théorie des Nombres de Boudeaux (1983) exposé no.22.

[13] J.-P.SERRE, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C.R.Acad.Sci. Paris Sér I 296(1983), 397-402.

[14] K.-O.STOHR and J.F.VOLOCH, Weierstass points and curves over finite fields. **Proc. London Math.Soc.** 52(1986), 1-19.

[15] T.SZONYI, Small complete arcs in Galois planes, **Geom. Dedicata** 18 (1985), 161-172.

[16] T.SZONYI, On the order of magnitude of k for complete k-arcs in PG(2,q), preprint.

[17] J.A.THAS, Complete arcs and algebraic curves in PG(2,q), **J.Algebra**, to appear.

[18] J.F.VOLOCH, Curves over finite fields, Ph.D.thesis, University of Cambridge, 1985.

[19] J.F.VOLOCH, On the completeness of certain plane arcs, **European J.Combin**, to appear.

[20] J.F.VOLOCH, Arcs in projective planes over prime fields, **J.Geom.**, to appear.

[21] W.G.WATERHOUSE, Abelian varieties over finite fields, **Ann.Sci. École Norm. Sup.** 2(1969), 521-560.

[22] F.ZIRILLI, Su una classe di k-archi di un piano di Galois, **Atti Acad. Naz.Lincei Rend.** 54(1973), 393-397.