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 \( C \) 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 \( C \). Define \( N_q(g) = \max N_1 \), where \( C \) 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: \[ N_2(q) \leq 2g - \sigma(g) \text{ as } g \to \infty \]
\[ N_3(g) \leq 3g + \sigma(g) \text{ as } g \to \infty \]

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

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 \( m = \lfloor 2q^{1/2} \rfloor \). Then \( 2q^{1/2} = m+\varepsilon \), where \( 0 \leq \varepsilon < 1 \). So
\[ \lfloor 2q^{1/2} \rfloor = \lfloor g(m+\varepsilon) \rfloor = \lfloor gm+g\varepsilon \rfloor = gm+\lfloor g\varepsilon \rfloor. \]

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

(a) Serre's result
The Riemann hypothesis states that if \( N_1 \) is the number of points of \( \mathbb{F} \) rational over \( GF(q^i) \), then

\[
\mathcal{F}(\mathbb{F}) = \exp(\sum_{i=1}^{N_1} x^i/i) = f(x)/(1-x)(1-qx),
\]

where \( f(x) = 1+c_1x+\ldots+q^{g-2g}x^{2g} \) and \( \mathbb{F}[x] \) 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

\[
N_1 = q + 1 - \frac{g}{2} (\alpha_i + \bar{\alpha}_i).
\]

Since

\[
\sum_{i=1}^{2g} \alpha_i^k = q^k + 1 - N_k,
\]

the elementary symmetric functions of the \( \alpha_i \) are integers and the \( \alpha_i \) are algebraic integers.

As above, let \( m = \lceil 2q^{1/2} \rceil \) and let \( x_i = m+1-\alpha_i-\bar{\alpha}_i, \quad i=1, \ldots, g \).

(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 \( c \leq \sqrt{q} \).

So \( \alpha_i + \bar{\alpha}_i = 2c \leq 2\sqrt{q} \) and \( \lceil 2\sqrt{q} \rceil > \alpha_i + \bar{\alpha}_i \); 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 \( \frac{g}{1}x_i \) is an integer for \( r=1, \ldots, g \).
or that $\Sigma (\alpha_1 + \bar{\alpha}_1)^r$ is an integer. However,

$$
\frac{g}{1}(\alpha_1 + \bar{\alpha}_1) \cdot r = \frac{g}{1} \cdot \alpha_1 \cdot r + \left( \frac{r}{1} \right) \cdot \frac{g}{1} \cdot r - 1 \cdot \bar{\alpha}_1 + \ldots + \left( \frac{r}{1} \right) \cdot \frac{g}{1} \cdot \bar{\alpha}_1 \cdot r - 1 + \frac{g}{1} \cdot \bar{\alpha}_1 \cdot r
$$

$$
= \frac{2g}{1} \cdot \alpha_1 \cdot r + \left( \frac{r}{1} \right) \cdot q \cdot \frac{2g}{1} \cdot \alpha_1 \cdot r - 2 + \left( \frac{r}{2} \right) \cdot q \cdot 2 \cdot \frac{2g}{1} \cdot \alpha_1 \cdot r - 4 + \ldots
$$

which is an integer.

The classical inequality on arithmetic and geometric means gives

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

by (1) and (2). So $\Sigma \cdot x_i \geq g$, whence $\Sigma (\alpha_1 + \bar{\alpha}_1) \leq g m$. Applying the same argument with $y_i$ for $x_i$ with $y_i = m+\alpha_i + \bar{\alpha}_i$ gives

$$
\Sigma (\alpha_i + \bar{\alpha}_i) \geq -g m. \text{ Hence}
$$

$$
|N_1 - (q+1)| \leq g m. \quad (3.3)
$$

(b) Ihara's result

We use (3.1) and

$$
N_2 = q^2 + 1 - \Sigma (\alpha_1^2 + \bar{\alpha}_1^2).
$$

(3.4)

Since $\alpha_1^2 + \bar{\alpha}_1^2 = (\alpha_1 + \bar{\alpha}_1)^2 - 2q$, so

$$q + 1 - \Sigma (\alpha_1 + \bar{\alpha}_1) = N_1 \leq N_2 = q^2 + 1 + 2 q g - \Sigma (\alpha_1 + \bar{\alpha}_1)^2.$$

However, $g \Sigma (\alpha_1 + \bar{\alpha}_1)^2 \geq \Sigma \Sigma (\alpha_1 + \bar{\alpha}_1)^2$. Thus

$$
N_1 \leq q^2 + 1 + 2 q g - g^{-1}(\Sigma (\alpha_1 + \bar{\alpha}_1)^2)^2
$$

$$
= q^2 + 1 + 2 q g - g^{-1}(N_1 - q - 1)^2
$$
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 \( \mathcal{C} \) be as in §2, but consider it as a curve over \( \bar{K} \), the algebraic closure of \( K = GF(q) \). Also suppose that \( \mathcal{C} \) is embedded in the plane \( PG(2, \bar{K}) \) and let \( \varphi \) be the Frobenius map given by

\[
P(x_0, x_1, x_2) \varphi = P(x_0^q, x_1^q, x_2^q)
\]

where \( P(x_0, x_1, x_2) \) is the point of the plane with coordinate vector \((x_0, x_1, x_2)\). Then

\[
\mathcal{C} = V(F) = \{ P(x_0, x_1, x_2) \mid F(x_0, x_1, x_2) = 0 \}
\]

for some form \( F \) in \( K[X_0, X_1, X_2] \). Also \( \mathcal{C} \varphi = \mathcal{C} \) and the points of \( \mathcal{C} \) rational over \( GF(q) \) are exactly the fixed points of \( \varphi \) on \( \mathcal{C} \).

For any non-singular point \( P = P(x_0, x_1, x_2) \), the tangent \( T_P \) at \( P \) is

\[
T_P = V( \frac{\partial F}{\partial x_0} X_0 + \frac{\partial F}{\partial x_1} X_1 + \frac{\partial F}{\partial x_2} X_2 )
\]

In affine coordinates,

\[
T_P = V( \frac{\partial f}{\partial a} (x-a) + \frac{\partial f}{\partial b} (x-b) )
\]
where \( f(x,y) = F(x,y,1) \).

Instead of looking at fixed points of \( \varphi \), 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 \( \mathcal{C} \). Let

\[
h = (x^q-x)f_x + (y^q-y)f_y.
\]

Then

\[
h_x = (qx^{q-1}-1)f_x + (x^q-x)f_{xx} + (y^q-y)f_{yx}
\]

\[
= -f_x + (x^q-x)f_{xx} + (y^q-y)f_{yx}
\]

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 \( \mathcal{C} \) that is non-singular. So, if \( N \) is the number of GF(q)-rational points of \( \mathcal{C} \) and the degree of \( f \) is \( d \), then Bézout's theorem implies, when \( f \) is not a component of \( h \), that

\[
(d+q-1)d = \deg h \deg f
\]

\[
= \text{sum of the intersection numbers at the points of } V(f) \cap V(h)
\]

\[
\geq 2N.
\]

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 on \( V(f) \). 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 \(\frac{dy}{dx} = -\frac{f_x}{f_y}\), it follows that

\[\frac{d^2y}{dx^2} = -f_y^{-2} \left( f_{xx}f_y^2 - 2f_{xy}f_x f_y + f_{yy}f_x^2 \right).\]

**THEOREM 4.1**: If \(\frac{d^2y}{dx^2} \neq 0\), that is, \(\wp\) 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 \(\wp\) is a line or the characteristic \(p \leq d\). For example, when \(f = x^{p+1} + y^{p+1}+1\), then \(\wp\) is all inflexions. A particular case of this phenomenon is the Hermitian curve \(\omega_{2,q} = V(x_0^{q+1} + x_1^{q+1} + x_2^{q+1})\) 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.
Thus, for $q$ odd with $q \leq 19$ and $q \neq 3$ or 9, the theorem gives the best possible result. A curve achieving $N_q(3)$ is $\mathcal{W}_{2,9}$.

5. WEIERSTRASS POINTS IN CHARACTERISTIC ZERO.

First consider the canonical curve $\mathcal{C}^{2g-2}$ of genus $g \geq 3$ in $\mathbb{P}G(g-1, \mathbb{C})$. The Weierstrass points, 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 hyperelliptic if it has a linear series $\mathcal{Y}_2^1$ (a 2-sheeted covering) on it; for example, a plane quartic with a double point. It has equation

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

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

Consider the case $g=3$ of the canonical curve $\mathcal{C}^4$, 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, \( \mathcal{C}_2, q \) has 28 undulations (points where the tangent has 4-point contact). When \( g=4 \), the curve \( \mathcal{C}^6 = \mathcal{F}^3 \cap \mathcal{F}^2 \), the intersection of a cubic and a quadric surface, has 60 stalls where the osculating plane meets the curve at four coincident points.

More generally, still with characteristic zero, if \( \mathcal{C} \) has genus \( g \geq 1 \) and \( P \in \mathcal{C} \), there exist integers \( n_1, n_2, \ldots, n_g \) such that no function has pole divisor precisely \( n_1 P \). 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 \( \mathfrak{c} \subseteq \mathcal{A}^n(K) \) be an irreducible non-singular algebraic curve defined over \( K \), let \( I(\mathfrak{c}) \subseteq K[X_1, \ldots, X_n] \) be the ideal of polynomials which are zero at all points of \( \mathfrak{c} \), let \( \Gamma(\mathfrak{c}) = K = [X_1, \ldots, X_n]/I(\mathfrak{c}) \); and \( K(\mathfrak{c}) \) be the quotient field of \( \Gamma(\mathfrak{c}) \); then \( K(\mathfrak{c}) \) is called the function field of \( \mathfrak{c} \). Also, for \( P \) in \( \mathfrak{c} \) let \( \mathcal{O}_P = \{ f/g | f, g \in \Gamma, g(P) \neq 0 \} \), the local ring of \( \mathfrak{c} \) at \( P \). Then, by natural inclusions, \( K \subseteq \Gamma(\mathfrak{c}) \subseteq \mathcal{O}_P(\mathfrak{c}) \subseteq K(\mathfrak{c}) \). Also \( \mathcal{O}_P \setminus \{ \text{units} \} = \mathcal{M}_P = \langle t \rangle \), the maximal ideal, and for any \( z \) in \( \mathcal{O}_P \) there exist a unique unit \( u \) and a unique non-negative integer \( m \) such that \( z = ut^m \); write \( m = \text{ord}_P(z) \). Hence, if \( g \in K[X_1, \ldots, X_n] \) and \( g \) is the image of \( G \) in \( \Gamma(\mathfrak{c}) \) with \( G(P) \neq 0 \), define \( \text{ord}_P(G) = \text{ord}_P(g) \). In particular, if \( \mathfrak{c} \) is a plane curve and \( V(L) \) the tangent at \( P \), then \( \text{ord}_P(L) \) gives the multiplicity of contact of the tangent with \( \mathfrak{c} \).
For the extension of these definitions to the projective case, see Fulton [3], p.182. This is the situation we now consider.

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

$$\text{div}(z) = \text{ord}_p(z)P,$$

$$= (z)_o - (z)_\infty,$$

where

$$(z)_o = \sum_{\text{ord}(z) > 0} \text{ord}_p(z)P, \text{ the divisor of zeros,}$$

and

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

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

Given $D = \Sigma n_p P$, define

$$L(D) = \{ f \in K(\mathbb{P}) | \text{ord}_P(f) \geq -n_p, \forall P \};$$

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

The set $L(D)$ is a vector space and its dimension is denoted $\mathfrak{g}(D)$.

There is an important equivalence relation on the divisors given by $D \sim D'$ if there exists $g$ in $K(\mathbb{P})$ such that $D - D' = \text{div}(g)$. 
7. THE CANONICAL SERIES

Let \( \mathcal{C} \) be an irreducible curve in \( \mathbb{P}G(2, \overline{K}) \) where \( \overline{K} \) is the algebraic closure of \( K \) and let \( X \) be a non-singular model of \( \mathcal{C} \) with \( \psi : X \rightarrow \mathcal{C} \) birational. Points of \( X \) are places or branches of \( \mathcal{C} \). A place \( Q \) is centred at \( P \) if \( Q\psi = P \). Let \( r_Q = \mu_p(\mathcal{C}) \), the multiplicity of \( \mathcal{C} \) at \( P \), where \( \mathcal{C} \) has only ordinary singular points. If \( \mathcal{C}' = V(G) \) is any other plane curve such that \( \text{div}(G) - E \) is effective, where \( E = \sum (r_Q - 1)Q \), then \( \mathcal{C}' \) is an adjoint of \( \mathcal{C} \); essentially, \( \mathcal{C}' \) passes \( m-1 \) times through any point of \( \mathcal{C} \) of multiplicity \( m \). If \( \deg \mathcal{C} = d \) and \( \deg \mathcal{C}' = d - 3 \), then \( \mathcal{C}' \) is a special adjoint of \( \mathcal{C} \). In this case, \( \text{div}(G) - E \) is a canonical divisor. The canonical series, consisting of all canonical divisors, is therefore cut out by all the special adjoints of \( \mathcal{C} \). The series is a \( \gamma \frac{g-1}{2g-2} \) of (projective) dimension \( g-1 \) and order \( 2g-2 \). For example,

\[
\mathcal{C}^6 = V(z^2 xy(x-y)(x+y)+x^6+y^6)
\]

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 \( \mathcal{C}^6 \) in \( 6.3-4.3=6 \) points other than \( P(0,0,1) \). Hence the special adjoints cut out a \( \gamma_5^3 \), as expected.

The Riemann-Roch theorem says that, if \( \mathcal{W} \) is a canonical divisor
on $X$ and $D$ is any divisor, then

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

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 $\overline{K}$, and let $f : X \to \mathbb{C} \subset \mathbb{P}(n, \overline{K})$ be a suitable rational map. Then $\mathbb{C}$ is viewed as the set of branches of $X$.

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

$$H \cdot \mathbb{C} = \sum_{P \in \mathbb{C}} n_p P$$

is a divisor of degree $d = \Sigma n_p$. Also

$$\mathcal{D} = \{ H \cdot \mathbb{C} | H \text{ a hyperplane} \}$$

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

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

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

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

$$L(D) = \{ g \in K(X) | \text{div}(g) + D \geq 0 \}.$$
Given a linear system \( \mathcal{D} \), the complete system containing \( \mathcal{D} \) has the same degree as \( \mathcal{D} \) and possibly larger dimension. Hence, although not necessary, it is simpler to consider complete linear systems, and this we do.

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

\[
\mathcal{D} = \mathcal{D}_0 \supset \mathcal{D}_1 \supset \ldots \supset \mathcal{D}_d \supset \mathcal{D}_{d+1} = \emptyset.
\]

Each \( \mathcal{D}_i \) is a projective space. If \( \mathcal{D}_i \neq \mathcal{D}_{i+1} \), then \( \mathcal{D}_{i+1} \) has codimension one in \( \mathcal{D}_i \). Such an \( i \) is a \((\mathcal{D}, P)\text{-order}\). So the \((\mathcal{D}, P)\text{-orders}\) are \( j_0, \ldots, j_n \), where

\[
0 = j_0 < j_1 < j_2 < \ldots < j_n < d.
\]

Note that \( j_1 = 1 \) if and only if \( P \) is non singular.

For example, let \( \mathcal{C} \) be a plane cubic.

Then

\[
(j_0, j_1, j_2) = \begin{cases} 
(0, 1, 2) & \text{if } P \text{ is neither singular nor an inflexion}, \\
(0, 1, 3) & \text{if } P \text{ is an inflexion}, \\
(0, 2, 5) & \text{if } P \text{ is singular}.
\end{cases}
\]

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

The Hasse derivative, satisfies the following properties:

(i) \( D_t^{(i)}(\Sigma a_j t^j) = \Sigma a_j (^{(i)} t^{j-1}) \); 

(ii) \( D_t^{(i)}(fg) = \sum_{j=0}^{i} D_t^{(j)} f \cdot D_t^{(i-j)} g \).
(iii) \( D_t^{(i)} D_t^{(j)} = \binom{i+j}{i} D_t^{(i+j)} \).

The unique hyperplane with intersection multiplicity \( j \) at \( P \) is the osculating hyperplane \( H_P \) and has equation

\[
\det \begin{bmatrix}
    x_0 & \ldots & x_n \\
    (j_0 f_0) & \ldots & (j_n f_n) \\
    \vdots & \ddots & \vdots \\
    (j_{n-1} f_0) & \ldots & (j_{n-1} f_n)
\end{bmatrix} = 0
\]

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

\[
(f_0, f_1, f_2, f_3) = (1, t, t^2, t^3),
\]

\[
(j_0, j_1, j_2, j_3) = (0, 1, 2, 3).
\]

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

\[
\det \begin{bmatrix}
    x_0 & x_1 & x_2 & x_3 \\
    1 & t & t^2 & t^3 \\
    0 & 1 & 2t & 3t^2 \\
    0 & 0 & 1 & 3t
\end{bmatrix} = 0,
\]

that is,

\[
t^3 x_0 - 3t^2 x_1 + 3tx_2 - x_3 = 0.
\]

The point \( P \) on \( \mathcal{C} \) is a Weierstrass point, W-point for short, if \( (j_0, j_1, \ldots, j_n) \neq (0, 1, \ldots, n) \).
Since $\mathcal{O}$ is complete, the Riemann-Roch theorem gives that, if $d > 2g - 2$, then

(i) $n = d - g$;

(ii) $\dim \mathcal{O}_i = d - g - i$ for $i < d - 2g + 1$;

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

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

$$L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_{n-1}.$$  

Also $L_0 = \{P\}$, 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 $\mathcal{O}$-osculation point if $j_n > n$, that is, there exists a hyperplane $H$ such that $n_H > n$.

The integers $j_i$ are characterized by the following result.

**THEOREM 8.1:** (i) If $j_0, \ldots, j_{i-1}$ are known, then $j_i$ is the smallest integer $r$ such that $D^{(r)}f(Q)$ is linearly independent of $\{D^{(j_0)}f(Q), \ldots, D^{(j_{i-1})}f(Q)\}$; the latter set spans $L_{i-1}$.

(ii) If $0 < r_0 < \ldots < r_s$ are integers such that $D^{(r_0)}f(Q), \ldots, D^{(r_s)}f(Q)$ are linearly independent, then $j_i \leq r_i$. 
9. THE GENERALIZED WRONSKIAN

Consider the generalized Wronskian

\[ W = \det \begin{bmatrix} (\epsilon_0) & (\epsilon_0) & \cdots & (\epsilon_0) \\ D^{(\epsilon_0)}f_0 & D^{(\epsilon_0)}f_1 & \cdots & D^{(\epsilon_0)}f_n \\ \vdots & \vdots & & \vdots \\ (\epsilon_n) & (\epsilon_n) & \cdots & (\epsilon_n) \\ D^{(\epsilon_n)}f_0 & D^{(\epsilon_n)}f_1 & \cdots & D^{(\epsilon_n)}f_n \end{bmatrix} \]

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

The \( \epsilon_i \) are required to satisfy the conditions:

(i) \( 0 = \epsilon_0 < \epsilon_1 < \ldots < \epsilon_n \);

(ii) \( W \neq 0 \);

(iii) given \( \epsilon_0, \ldots, \epsilon_{i-1} \), then \( \epsilon_i \) is chosen as small as possible such that \( D^{(\epsilon_i)}f_i, \ldots, D^{(\epsilon_i)}f_n \) are linearly independent.

Then

(iv) the \( \epsilon_i \) are the \( (\mathcal{E}, P) \)-orders at a general point \( P \);

(v) \( \epsilon_i < r_i \) for any \( r_0 < \ldots < r_n \) with \( \det (D^{(r_i)}f_j) \neq 0 \);

(vi) \( \epsilon_i < j_i \) for any \( P \) in \( \mathcal{E} \);

(vii) the \( \epsilon_i \) are called the \( \mathcal{E} \)-orders of \( \mathcal{E} \).

The divisor
\[
\text{R} = \text{div}(W) + \sum_{i=0}^{n} (\text{p}_i \text{p}_i) \text{div}(dt) + (n+1) \sum_{p \neq p} \text{p}_p \text{p},
\]

where \(dt\) is the differential of \(t\) and \(\text{e}_p = \text{sign} \text{ord}_p f_i\), is the ramification divisor of \(\mathcal{O}\) and depends only on \(\mathcal{O}\). Putting \(R = \sum_{p \neq p} \text{p}_p \text{p}\), we have

\[
\text{deg} R = \sum_{p \neq p} \text{p}_p = (2g-2) \sum_{i=1}^{n} \text{c}_i + (n+1)d.
\]

**Theorem 9.1:** \(r_p \geq \sum_{i=0}^{n} (j_i - \text{c}_i)\) with equality if and only if \(\det C \equiv 0 \pmod{p}\), where \(C = (c_{is})\) and \(c_{is} = (j_i)\).

**Corollary:**

(i) \(R\) is effective.

(ii) \(r_p = 0\) if and only if \(j_i = \text{c}_i\) for \(0 \leq i \leq n\).

The points \(P\) where \(r_p = 0\) are called \(\mathcal{O}\)-ordinary; the others are called \(\mathcal{O}\)-Weierstrass. The number \(r_p\) is the weight of \(P\). When \(\mathcal{O}\) is the canonical series, the \(\mathcal{O}\)-Weierstrass points are simply the Weierstrass points. This coincides with the classical definition.

When \(\text{c}_i = i\), \(0 \leq i \leq n\), then \(\mathcal{O}\) is classical. Next, the estimate \(\epsilon_i \leq j_i\) is improved.

**Theorem 9.2:**

(i) Let \(P\) on \(\mathcal{O}\) have \((\mathcal{O},P)\)-orders \(j_0, \ldots, j_n\) and suppose that \(\det C' \neq 0 \pmod{p}\), where \(C' = (c_{is}')\) and \(c_{is}' = (j_i)\).

\[
D^{(r_0)}, \ldots, D^{(r_n)} f \text{ are linearly independent and } \epsilon_i \leq r_i.
\]

(ii) If \(\prod_{i=s}^{n} (j_i - j_s)(i-s) \neq 0 \pmod{p}\), then \(\mathcal{O}\) is classical and \(r_p = \sum_{i=0}^{n} (j_i - i)\).
(iii) If \( p > d \) or \( p = 0 \), then \( r_p = \sum_{i=0}^{n}(j_i - 1) \) for all \( p \) in \( \mathcal{C} \).

(iv) If \( \epsilon \) is a \( \mathbb{Q} \)-order and \( \mu \) is an integer with \( (\epsilon^\mu) \neq 0 \) (mod \( p \)), then \( \mu \) is also a \( \mathbb{Q} \)-order.

(v) If \( \epsilon \) is a \( \mathbb{Q} \)-order and \( \epsilon < p \), then 0, 1, ..., \( \epsilon - 1 \) are also \( \mathbb{Q} \)-orders.

Entering into this theorem is the classical result of Lucas.

**Lemma 9.3:** Let \( a = a_0 + a_1p + ... + a_mp^m \) and \( b = b_0 + b_1p + ... + b_mp^m \) 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

\[
\begin{align*}
(i) \ A & \equiv B \\
\text{mod } p & \equiv \frac{a_0}{b_0} \left( \frac{a_1}{b_1} \right) \ldots \left( \frac{a_m}{b_m} \right) \text{ (mod } p) ;
\end{align*}
\]

\[
(ii) \ A \neq B \text{ (mod } p) \text{ if and only if } a_i > b_i, \text{ all } i;
\]

**Proof:** \((1+x)^A = \sum_{i=0}^{\sum a_i p^i}
\]

\[
= (1+x)^a_0 (1+x^p)^a_1 \ldots (1+x^p)^a_m .
\]

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 $j_0, \ldots, j_n$ be the $(|D|, P)$-orders, where $n=\dim |D|$. Then the $(|D+P|, P)$-orders are $0, j_0 + 1, \ldots, j_n + 1$.

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 $\mathcal{D}$ and let $j_0, \ldots, j_n$ be the $(\mathcal{D}, P)$-orders for $\mathcal{D}$ canonical. Then $j_0 + 1 = a_1, \ldots, j_{g-1} + 1 = a_g$ are the Weierstrass gaps at $P$; that is, there does not exist $f$ in $\mathbb{K}(\mathcal{D})$, regular outside $P$, such that $\ord_P(f) = -a_i$.

THEOREM 10.3: Let $\mathcal{D}$ and let $a_1, \ldots, a_g$ be the Weierstrass gap sequence at $P$. If the linear system $\mathcal{D} = |dP|$ for some positive integer $d$, then the $(\mathcal{D}, P)$-orders are $\{0, 1, \ldots, d\} \setminus \{d-a_1 \mid a_1 < d\}$.

THEOREM 10.4: With $P$ and $a_1, \ldots, a_g$ as above, let $V$ be a canonical divisor, $s \geq 2$ an integer, and $\mathcal{D} = |V+sP|$. Then the $(\mathcal{D}, P)$-orders are

$$j_i = i$$

for $i = 0, 1, \ldots, s-2$,

$$j_i = s-1+a_i$$

for $i = 1, \ldots, g$.

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

An important result an linear series is also worth noting.
THEOREM 10.6: The generic curve of genus \( g \) has a \( \gamma_d \) if and only if
\[
d > \frac{n}{n+1} g + n.
\]

11. THE ESSENTIAL CONSTRUCTION

Given the curve \( \mathcal{C} \) with its linear system of hyperplanes and with \( N \) the number of its GF(q)-rational points, consider the set
\[ \mathcal{F} = \{ P | P \in \mathcal{C} \} \] ; compare §4 for the plane. So \( \text{Pe} \mathcal{F} \iff \det \left[ \begin{array}{cccc}
  f_0^q & \cdots & f_0^q \\
  (j_0) & \cdots & (j_0) \\
  D_t f_0 & \cdots & D_t f_n \\
  \vdots & \ddots & \vdots \\
  (j_{n-1}) & \cdots & (j_{n-1}) \\
  D_t f_0 & \cdots & D_t f_n
  \end{array} \right] = 0
\]

To give an outline first, take the classical case in which \( j_1 = 1 \). So, let
\[ W' = \det \left[ \begin{array}{cccc}
  f_0^q & \cdots & f_0^q \\
  f_0 & \cdots & f_n \\
  \vdots & \ddots & \vdots \\
  D^{(n-1)} f_0 & \cdots & D^{(n-1)} f_n
  \end{array} \right]
\]
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

\[ N \leq (n-1)(g-1) + \frac{d(q+n)}{n}. \]

Since \( \mathcal{O} \) is complete, \( d \leq n + g \); hence

\[ N \leq (n-1)(g-1) + \frac{(n+g)(q+n)}{n} \]

\[ = q + 1 + g(n + q/n). \]

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

\[ N \leq q + 1 + 2g\sqrt{q} \]

More carefully, let

\[
W_t(v,f) = \det \begin{bmatrix}
f^q_0 & \cdots & f^q_n \\
(D_t v_0 f_0) & \cdots & (D_t v_0 f_n) \\
\vdots & \ddots & \vdots \\
(D_t v_{n-1} f_0) & \cdots & (D_t v_{n-1} f_n)
\end{bmatrix}
\]

where \( t \) is a separating variable on \( \mathcal{O} \) and \( v=(v_0,\ldots,v_{n-1}) \) with \( 0 \leq v_0 < \cdots < v_{n-1} \).

**THEOREM 11.1**: (i) There exist integers \( v_0,\ldots,v_{n-1} \), such that \( 0 \leq v_0 < \cdots < v_{n-1} \) and \( W_t(v,f) \neq 0 \).
(ii) If \( v_0, \ldots, v_{n-1} \) are chosen successively so that \( v_i \) is as small as possible to ensure the linear independence of \( D(v_0)f, \ldots, D(v_i)f \), then there exists an integer \( n_0 \) with \( 0 < n_0 \leq n \) such that

\[
\begin{align*}
  v_i &= \varepsilon_i \quad \text{for } i < n_0, \\
  v_i &= \varepsilon_{i+1} \quad \text{for } i \geq n_0,
\end{align*}
\]

where \( \varepsilon_0, \ldots, \varepsilon_n \) are the \( \mathcal{D} \)-orders; that is

\[
(v_0, \ldots, v_{n-1}) = (\varepsilon_0, \ldots, \varepsilon_{n_0-1}, \varepsilon_{n_0+1}, \ldots, \varepsilon_n).
\]

(iii) If \( v' = (v'_0, \ldots, v'_{n-1}) \) and \( W_t(v', f) \neq 0 \), then \( v_i \leq v'_i \) for all \( i \).

The integers \( v_i \) are the Frobenius \( \mathcal{D} \)-orders. They and \( S \) depend only on \( \mathcal{D} \), where

\[
S = \text{div}(W_t(v, f)) + \text{div}(dt) + (q+n)E,
\]

\[
\deg S = (2g-2) \sum v_i + (q+n)d.
\]

**Theorem 11.2:** If \( v \leq q \) is a Frobenius \( \mathcal{D} \)-order, then each non-negative integer \( u \) such that \( \binom{v}{u} \neq 0 \) (mod \( p \)) 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

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

(ii) If $P \in \mathbb{G}$ but not $\text{GF}(q)$-rational, then

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

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

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

THEOREM 11.4: Let $P$ be a $\text{GF}(q)$-rational point of $\mathbb{G}$. If

$$0 \leq m_0 < \ldots < m_{n-1} \text{ and } \det C'' \not\equiv 0 \pmod{p},$$

then $v_i \leq m_i$ for all $i$, where $C'' = (c''_{ir})$ and

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

COROLLARY 1: (i) If $P$ is a $\text{GF}(q)$-rational point of $\mathbb{G}$, then

$$v_i \leq j_{i+1} - j_i \quad \text{for } i = 0, \ldots, n-1 \text{ and } m_p(S) \geq \sum_{i=1}^{n} j_i.$$  

(ii) If (a) $\sum_{1 \leq i < r \leq n} (j_r - j_i)/(r - i) \not\equiv 0 \pmod{p}$, or (b) $j_i \equiv j_r \pmod{p}$ for $i \neq r$, or (c) $p \geq d$, then $v_i = 1$ for $i = 0, \ldots, n-1$ 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 $\text{GF}(q)$-rational
point of $\mathcal{C}$ a $\mathcal{D}$-Weierstrass point.

COROLLARY 3: If $\mathcal{C}$ has some GF(q)-rational point, then $v_i \leq i+d-n$, all $i$. If also $\mathcal{D}$ 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 $K = \text{GF}(q)$ with $N$ rational points. If there exists on $X$ a linear system $\gamma_d^n$ without base points, and with order sequence $\epsilon_0, \ldots, \epsilon_n$ and Frobenius order sequence $v_0, \ldots, v_{n-1}$, then

$$N \leq \frac{1}{n} \left\{ (2g-2) \sum_{i=0}^{n-1} v_i + (q+n)d \right\}.$$ 

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

$$\epsilon^N \sum_{p} a_p + \sum_{p'} b_p' \leq (2g-2) \sum_{i=0}^{n-1} \epsilon_i + (q+n)d,$$

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

$$a_p = i_{\leq n}(j_i - \epsilon_i), \quad b_p' = i_{\leq n}(j_i - \epsilon_i)$$

with $j_0, \ldots, j_n$ the $(\mathcal{D}, P)$-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

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

Note: This is better than $S_g$ when

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

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 $\gamma_d^n$ on a curve of genus $g$ with $n+1$ coincident points, that is $C$-Weierstrass points, is $(n+1)(d+ng-n)$.

When $g=1$, this number is $d(n+1)$. If $C$ consists of all curves of degree $r$ and $C$ is a plane non-singular cubic, then $n=\frac{1}{2}r(r+3)$, $d=3r$. The condition for a $\gamma_d^n$ to exist is, from Theorem 10.6, that $d \geq n/(n+1)+n$. So this only allows $\gamma_3^2$ and $\gamma_6^5$, whence $d=n+1$ and the number of $C$-Weierstrass points is $(n+1)^2$. From the Riemann-Roch theorem, as every series is non-special on $C$, a complete
series $\gamma_d^n$ satisfies $d = n+1$.

For $n=2$, the $\mathcal{E}$-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 $p^k | (n+1)$, the $\mathcal{E}$-W-points have multiplicity one.

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

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

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

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

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

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

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

13. HYPERELLIPTIC CURVES

As in §5, if $p \neq 2$, then $\mathcal{E}$ has homogeneous equation $y^2 z^{d-2} = z^d f(x/z)$ 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 $\gamma_2^1$ on $\mathcal{E}$);
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 $n_0$ be the number of $K$-rational $P_i$.

**THEOREM 13.1:** Let $\mathcal{C}$ be hyperelliptic with a complete $\gamma_2^1 = |D|$ and $n, n_0$ as above. If there is a positive integer $n_1$ such that $|(n_1 + g)D|$ is Frobenius classical, then

$$|N-(q+1)| \leq g(2n_1 + g) + (2n_1 + g)^{-1} \{g(q-n_0) - g^3 - g \}.$$  

**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 $\mathcal{C}$ be hyperelliptic with $g > 1$ over $GF(p)$. Then

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

14. **PLANE CURVES**

Let $\mathcal{C}$ 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 $x^iy^j, i, j \geq 0, i + j \leq m$ 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 $\mathcal{C}$ 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

$$N \leq \frac{1}{2}(m^2 + 3m - 2)(g-1) + 2d(m+3)^{-1} \{q + \frac{1}{2}m(m+3) \}.$$
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 $v_1$, in theorem 11.5.

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

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

which is required in theorem 19.1.

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

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

It is non-singular.

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

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

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

$$n = \begin{cases} 
\frac{1}{2}m(m+3) & \text{for } m \leq d - 3 \\
md - g & \text{for } m > d - 3.
\end{cases}$$
\begin{align*}
g &= \frac{1}{2}(d-1)(d-2), \\
d_0 &= \text{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}
\end{align*}

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

A Fermat curve is a special case of a Thue curve given by

\[ F_d : ax^d + by^d = z^d \]

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

**THEOREM 14.3:** For \( F_d \) 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 \( F_d \) 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

<table>
<thead>
<tr>
<th>q</th>
<th>$[2\sqrt{q}]$</th>
<th>$N_q(1)$</th>
<th>$N_q(2)$</th>
<th>$N_q(3)$</th>
<th>$N_q(4)$</th>
<th>$N_q(5)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>7</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>9</td>
<td>10</td>
<td>13</td>
<td>15</td>
<td>21</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>10</td>
<td>12</td>
<td>14</td>
<td>18</td>
<td>22</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>13</td>
<td>7</td>
<td>18</td>
<td>20</td>
<td>23</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>14</td>
<td>18</td>
<td>19</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>16</td>
<td>20</td>
<td>22</td>
<td>28</td>
<td>28</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>18</td>
<td>24</td>
<td>24</td>
<td>28</td>
<td>30</td>
</tr>
<tr>
<td>13</td>
<td>7</td>
<td>21</td>
<td>26</td>
<td>28</td>
<td>32</td>
<td>35</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
<td>25</td>
<td>33</td>
<td>33</td>
<td>38</td>
<td>41</td>
</tr>
<tr>
<td>17</td>
<td>8</td>
<td>26</td>
<td>32</td>
<td>34</td>
<td>40</td>
<td>42</td>
</tr>
<tr>
<td>19</td>
<td>8</td>
<td>28</td>
<td>36</td>
<td>36</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>23</td>
<td>9</td>
<td>33</td>
<td>42</td>
<td>42</td>
<td>48</td>
<td>51</td>
</tr>
<tr>
<td>25</td>
<td>10</td>
<td>36</td>
<td>46</td>
<td>46</td>
<td>56</td>
<td>56</td>
</tr>
<tr>
<td>27</td>
<td>10</td>
<td>38</td>
<td>48</td>
<td>48</td>
<td>58</td>
<td>66</td>
</tr>
<tr>
<td>29</td>
<td>10</td>
<td>40</td>
<td>50</td>
<td>50</td>
<td>60</td>
<td>70</td>
</tr>
<tr>
<td>31</td>
<td>11</td>
<td>43</td>
<td>52</td>
<td>54</td>
<td>65</td>
<td>74</td>
</tr>
<tr>
<td>32</td>
<td>11</td>
<td>44</td>
<td>53</td>
<td>55</td>
<td>66</td>
<td>77</td>
</tr>
<tr>
<td>37</td>
<td>12</td>
<td>50</td>
<td>60</td>
<td>62</td>
<td>74</td>
<td>86</td>
</tr>
<tr>
<td>41</td>
<td>13</td>
<td>54</td>
<td>66</td>
<td>68</td>
<td>81</td>
<td>94</td>
</tr>
<tr>
<td>43</td>
<td>13</td>
<td>57</td>
<td>68</td>
<td>70</td>
<td>83</td>
<td>96</td>
</tr>
<tr>
<td>47</td>
<td>13</td>
<td>61</td>
<td>74</td>
<td>74</td>
<td>87</td>
<td>100</td>
</tr>
<tr>
<td>49</td>
<td>14</td>
<td>64</td>
<td>78</td>
<td>78</td>
<td>92</td>
<td>92</td>
</tr>
</tbody>
</table>
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 \( \mathcal{C} \) be a non-singular cubic in \( \mathbb{P}G(2,q) \). For the projective classification when \( K = GF(q) \), see [6] Chapter 11. Although \( \mathcal{C} \) may have no inflexion, up to isomorphism it may be assumed to have one, 0.

**THEOREM 16.1:** If \( \mathcal{C}', \mathcal{C}'' \) are cubic curves in \( \mathbb{P}G(2,K) \) such that the divisors \( \mathcal{C} \cdot \mathcal{C}' = \sum_{i=1}^{9} P_i \) and \( \mathcal{C} \cdot \mathcal{C}'' = \sum_{i \neq 1}^{8} P_i + Q \), then \( Q = P_9 \).

**Proof.** (Outline) Through \( P_1, \ldots, P_8 \) there is a pencil \( \mathcal{F} \) of cubic curves to which \( \mathcal{C}, \mathcal{C}', \mathcal{C}'' \) belong. Any curve of \( \mathcal{F} \) 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 \( \mathcal{C} \) are collinear with a third.

**Proof.** Let \( P_1, P_2 \) be inflexions of \( \mathcal{C} \) with corresponding tangents \( \ell_1, \ell_2 \). Let \( \ell = P_1 P_2 \) meet \( \mathcal{C} \) again at \( P_3 \), and let \( \ell_3 \) be the tangent at \( P_3 \) meeting \( \mathcal{C} \) again at \( Q \). Then

\[
\mathcal{C} \cdot \ell_1 = 3P_1, \quad \mathcal{C} \cdot \ell_2 = 3P_2, \quad \mathcal{C} \cdot \ell_3 = 2P_3 + Q
\]

\[
\mathcal{C} \cdot \ell = P_1 + P_2 + P_3.
\]
Hence

\[ \mathcal{C} \cdot l_1 l_2 l_3 = 3P_1 + 3P_2 + 2P_3 + Q \]

\[ \mathcal{C} \cdot l^3 = 3P_1 + 3P_2 + 3P_3 \]

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 \( \mathcal{C} \), 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 \( P_1 Q_1 \) meet \( \mathcal{C} \) again at \( R_1 \). Let \( r \) be a tangent to \( \mathcal{C} \) 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 \( \mathcal{C} \). Let \( R_2 P_2 \) meet \( \mathcal{C} \) again at \( Q_2 \) and let \( R_3 P_3 \) meet \( \mathcal{C} \) again at \( Q_3 \). We use the previous theorem to show that \( Q_1, Q_2, Q_3 \) are collinear.

Write \( l_i = P_i R_i Q_i \), \( i = 1, 2, 3 \); let \( p = P_1 P_2 P_3 \), \( r = R_1 R_2 \), \( q = Q_1 Q_2 S \) with \( S \) the third point of \( Q \) on \( \mathcal{C} \).

Then \[ \mathcal{C} \cdot l_1 l_2 l_3 = 3 \sum_{i=1}^{3} (P_i + Q_i + R_i) \]

\[ \mathcal{C} \cdot prq = 3 \sum_{i=1}^{3} (P_i + R_i) + Q_1 + Q_2 + S. \]

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 \( \tau \) from the pencil \( \mathcal{C} \) through \( P_1 \) and the pencil \( Q \) through \( Q_1 \) in which the tangents correspond. Hence \( \tau \) 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 $\mathcal{P}$, 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 $P_1, Q_1, R_1$, $i=1,2,3$; there is an irreducible cubic $\$ in the pencil they determine. Also in the pencil is the cubic consisting of $\$ and the line $R_3R_2$. So, by theorem 16.1, this cubic contains the ninth point $R_1$, which cannot lie on $\$. So $R_3R_2R_1$ is a line.

**THEOREM 16.5:** Let $l_1, l_2, l_3, l_4$ be the sides of a complete quadrilateral in an affine plane and let $C_1$ be the circumcircle of the triangle obtained by deleting $l_1$. 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 $C_i + l_i$, $i=1,2,3,4$, 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 $\$ is an abelian group. As above we take $0$ as an inflexion.
Definition: For $P, Q$ on $\mathcal{C}$, let $\mathcal{C}.PQ = P + Q + R$ and let $\mathcal{C}.OR = O + R + S$; define $S = P + Q$.

**Lemma 16.6:**
(i) On $\mathcal{C}$, the points $O, P, -P$ are collinear.
(ii) $P, Q, R$ are collinear on $\mathcal{C}$ if and only if $P + Q + R = O$.

**Theorem 16.7:** Under the additive operation, $\mathcal{C}$ is an abelian group.

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

Apart from $\mathcal{C}$, consider the two cubics consisting of three lines given by the rows and columns of the 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 $C$ on $OX$, then

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

Note: $C$ 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) $t = 0$ \hspace{1cm} $h$ odd or $p \not\equiv 1 \pmod{4}$

(iii) $t = \pm \sqrt{q}$ \hspace{1cm} $h$ even and $p \not\equiv 1 \pmod{3}$

(iv) $t = \pm 2\sqrt{q}$ \hspace{1cm} $h$ even

(v) $t = \pm \sqrt{2q}$ \hspace{1cm} $h$ odd and $p = 2$

(vi) $t = \pm \sqrt{3q}$ \hspace{1cm} $h$ odd and $p = 3$

**Corollary:** $N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } p \text{ divides } \lfloor 2\sqrt{q} \rfloor, \\ q + 1 + \lfloor 2\sqrt{q} \rfloor & \text{otherwise.} \end{cases}$
17. k-ARCS ON ELLIPTIC CURVES

As in §16, the curve $\mathcal{C}$ is a non-singular cubic in $\text{PG}(2,q)$ with inflexion $0$.

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

**Proof.** Since $\mathcal{C}$ is an abelian group, the fundamental theorem says that $\mathcal{C}$ 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 $\mathcal{C}$ of index 2. Let $K = \mathcal{C} \setminus G$. 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 $\mathcal{X}$ can be chosen to be complete. First we construct $\mathcal{X}$ 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 $K = \text{GF}(q)$, let $K_0 = \text{GF}(q) \setminus \{0\}$ and $K_0^2 = \{t^2 | t \in K_0 \}$.

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

$$y^2z = x^3 + a_2x^2z + a_1xz^2 + a_0z^3.$$  

Also suppose it is non-singular with $2k$ points. The point $U_1$ is an inflexion and we take this as the zero of $\mathcal{C}$ as an abelian group. Since $|\mathcal{C}|$ is even, so $\mathcal{C}$ 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 $\mathcal{C}$ has equation
Define \( \theta : \mathcal{E} \to K_0/K_0^2 \) by

\[ U_1 \theta = K_0^2; \quad U_2 \theta = a_1 K_0^2, \quad P(x,y,1) \theta = x K_0^2 \] for \( x \neq 0 \).

Write \( K_0/K_0^2 = \{1, \nu | \nu^2 = 1\} \).

**Lemma 17.2:** \( \theta \) 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

\[
(mx+c)^2 - (x^3 + a_2 x^2 + a_1 x) = (x_1 - x)(x_2 - x)(x_3 - x).
\]

Thus \( x_1 x_2 x_3 = c^2 \) 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 \( x_1 x_2 = a_1 \).

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

\[
= x_1^2 (a_1 / x_1) = x_1 a_1 = (P_1 \theta)(U_2 \theta).
\]

So the homomorphism is established in all cases.
LEMMA 17.3: $\theta$ 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 $\mathcal{G}' = V(F(bx^2, y, z))$ where $\mathcal{G} = V(F(x, y, z))$. So $\mathcal{G}'$ 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 $V(z) \cap \mathcal{G}' = \{U_1\}$ and $V(x) \cap \mathcal{G}' = \{U_1, U_2\}$. If we put $y = tx$, we see that $\mathcal{G}'$ 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: $\mathcal{A} = \mathcal{G} \setminus \ker \theta$ is a $k$-arc.

Proof. Let $G = \ker \theta$. Then, from the previous two lemmas, $G \subset \mathcal{G}$ with $[\mathcal{G}: G] = 2$. Then, if $P \in G$, $P\theta = 1$; if $P \in \mathcal{K}$, $P\theta = \nu$. Suppose $P_1, P_2, P_3$ in $\mathcal{K}$ are collinear. So $P_1 + P_2 + P_3 = 0$, whence $(P_1 + P_2 + P_3)\theta = \theta$. 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 $\theta$.

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

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

Case (a). There are at most four tangents through $P_o$ with point of contact $Q$ in $\mathcal{K}$. Since $k = \frac{1}{2}|\mathcal{G}| > \frac{1}{2}(\sqrt{q} - 1)^2 > 4$, there exists $Q$ in $\mathcal{K}$ which is not such a point of contact. So $2Q \neq P_o$ and $Q \neq (P_o + Q)$. Also $-(P_o + Q) \in \mathcal{K}$, as otherwise $Q \in G = \mathcal{G} \setminus \mathcal{K}$. So $P_o, Q, -(P_o + Q)$ are distinct collinear points of $\mathcal{K} \cup \{P_o\}$. 
Case (b). Let \( C' \) be the elliptic curve with affine equation
\[
y^2 = v^3 x^4 + v^2 a_2 x^2 + v a_1.
\] (17.2)
Define the following functions on \( C' \):
\[
U = v x^2, \quad Z = xy, \quad A = (y_0 - Z)/(x_0 - U),
\]
\[
B = A^2 - a_2, \quad C = 2A a_1 - 2A^2 U,
\]
\[
D = (U - B)^2 + 4(C + B U - U^2).
\]
Then there exists a double cover
\[
\Psi : \mathcal{D} \to C'
\]
defined by \( W^2 = D \); that is, for any point \( P(x, y, 1) \) of \( C' \), there are two points \( P(x, y, W, 1) \) of \( \mathcal{D} \). Now, let \( P(x, y, W, 1) \) be a rational point of \( \mathcal{D} \). Then, from the equation for \( C' \),
\[
x^2 y^2 = v^3 x^6 + v^2 a_2 x^4 + v a_1 x^2,
\]
whence
\[
Z^2 = U^3 + a_2 U^2 + a_1 U .
\] (17.3)
Hence

(1) \( P = P(U, Z, 1) \in \mathcal{D} \);

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

(3) \( PP_0 \) meets \( C \) is two points other than \( P \) whose \( x \)-coordinates satisfy
\[
x^2 - (B - U)x - (C + B U - U^2) = 0 \] (17.4)
The last follows by substitution from (2) in (17.1), for we have
\[
\{ z + A(x-u) \}^2 = x^3 + a_2 x^2 + a_1 x.
\]

Then, from (17.3),
\[
(U^3 + a_2 U^2 + a_1 U) - (x^3 + a_2 x^2 + a_1 x)
+ 2 z A(x-u) + A^2(x-u)^2 = 0.
\]

Cancelling \( x-u \) gives (17.4).

Now, let \( \mathcal{E} \cap PP_o = \{ P,Q,R \} \). 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 \( \mathcal{E} \). Since \( P,Q,R \) are collinear
\( (P\theta)(Q\theta)(R\theta) = 1 \). As \( P \in \mathcal{E} \), so \( P\theta = \nu \), whence \( (Q\theta)(R\theta) = \nu \). So one
of \( Q \) and \( R \), say \( Q \), is in \( \mathcal{E} \). Hence, if \( P \neq Q \), there are three collinear
points \( P,P_o,Q \) of \( \mathcal{E} \cup \{ P_o \} \).

It remains to examine the condition that \( P \neq Q \). There are at
most six tangents to \( \mathcal{E} \) through \( P_o \) ([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 \( \mathcal{D} \). As \( |\mathcal{E} \cap V(x)| \leq 2 \) and \( |\mathcal{E} \cap V(z)| = 0 \),
so \( |\mathcal{D} \cap V(x)| \leq 4 \) and \( |\mathcal{D} \cap V(z)| = 0 \). So we require that \( \mathcal{D} \) has at least
\( 24 + 4 + 1 = 29 \) rational points.

\[
2g(\mathcal{D}) - 2 = 2 \{ 2g(\mathcal{E}) - 2 \} + \deg E \\
= \deg E.
\]

Here, \( E \) is the ramification divisor (cf. §9) and
\[ \text{deg } E = \# \text{ points of ramification} \]
\[ = \# \text{ points with } D = 0 \]
\[ = \# \text{ points such that } Q \text{ and } R \text{ have the same } x\text{-coordinate}. \]

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 \( \mathcal{C}' \). If \( Q = R \), then \( PP_0 \) is a tangent to \( \mathcal{C} \) at \( Q \). Hence there are at most six choices for \( P \) and hence at most 12 such points on \( \mathcal{C}' \). Hence \( 2g(\mathcal{D}) - 2 \leq 12 + 2 = 14 \), whence \( g(\mathcal{D}) \leq 8 \). Thus by the corollary to theorem 11.5,

\[ |\mathcal{D}| \geq q + 1 - 16\sqrt{q}. \]

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 \( \mathcal{C}' \), one takes \( A = \gamma_0 \).

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 \( \mathcal{C} \) is taken in the form

\[ (y^2 + xy)z = x^3 + a_1xz^2 + a_6z^3. \]

Instead of \( \Theta \) as above, we define \( \Theta : \mathcal{C} \to K/\mathcal{C}_0 \) where \( C_0 = \{ t \in K | T(t) = 0 \} \) and \( T(t) = t + t^2 + \ldots t^{q/2} \); here \( \mathcal{C}_0 \) in the set of elements of category (= trace) zero. Take \( P(x, y, 1) \theta = xC_0 \). Then \( \mathcal{X} \) is complete for \( q \geq 256 \).
COROLLARY: In $\text{PG}(2,q)$ 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 $\text{PG}(2,q)$.

Let $\mathcal{A}$ be a complete $k$-arc in $\text{PG}(2,q)$; that is, $\mathcal{A}$ 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),

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

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];
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 $q \leq 13$.

<table>
<thead>
<tr>
<th>$q$</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>11</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>$m'$</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>$n$</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

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

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

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

$$m'(2,q) = q - \sqrt{q} + 1, \text{ q = } 2^{2r}, [2].$$
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 $\mathcal{X}$ be a complete $k$-arc with $k > \frac{44}{45}p + \frac{8}{9}$. Through each point $P$ of $\mathcal{X}$ there are $t = p+2-k$ unisecants. The $kt$ unisecants of $\mathcal{X}$ belong to an algebraic envelope $\Delta_{2t}$ of class $2t$, which has a simple component $\Gamma_n$ with $n < 2t$. For $t=1$, the envelope $\Delta_2$ is the dual of a conic, $\mathcal{X}$ is a $(q+1)$-arc and so a conic. When $t \geq 2$, four cases are distinguished.

(i) $\Gamma_n$ is a regular (rational) linear component.

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

(ii) $\Gamma_n$ is regular of class two.

Here $\Gamma_n$ is the dual of a conic $\mathcal{C}$, and $\mathcal{X}$ is contained in $\mathcal{C}$, [6] theorem 10.4.3.

(iii) $\Gamma_n$ is irregular.

Suppose that $\Gamma_n$ 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 $\Delta_{2t}$ and $\Gamma_n$, there are at least $\frac{1}{2}n$ distinct lines of $\Gamma_n$ through $P$; so $N \geq \frac{1}{k} kn$. Therefore $k < 2N/n < 2n < 4t = \ldots$
= 4(p+2-k). Thus $k \leq \frac{4}{3}(p+2) < \frac{44}{45}p + \frac{8}{9}$, a contradiction for $p \geq 5$.

(iv) $\Gamma_n$ is regular with $n \geq 3$.

Either $n=2t < \frac{1}{2}p$ 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:

\[
\begin{align*}
m_2(3,q) &= q^2 + 1, \quad q > 2; \\
m_2(4,3) &= 20; \\
m_2(5,3) &= 56. \\
\end{align*}
\]

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

**Theorem 20.4:** ([7]) For odd, \( q \geq 121, n \geq 4 \).

\[
m_2(n,q) \leq q^{n-1} - \frac{1}{4}q^{n-3/2} + 3q^{n-2}.
\]

**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.


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


