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

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

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_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

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

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

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

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.