series γ_d^n satisfies $d = n+1$.

For $n=2$, the $\mathscr{D}$-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 $\mathscr{D}$-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) $\mathscr{C}$ is ordinary and there are $(n+1)^2/p^k$ $\mathscr{D}$-W-points with multiplicity p^k;

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

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

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

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

(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 $\mathscr{C}$ 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 γ_2^1 on $\mathscr{C}$);

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

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