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 O 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 $\mathcal{D} = |(\sqrt{q}+1)O|$;

(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 $\mathcal{C}$ 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 $\mathcal{C}$);