J.P. Serre   Nov 1982   Number of points on curves of finite fields.   1

$\mathbb{F}_q$ curve X of genus g / $\mathbb{F}_q$ (proj. n.s. abs. irred.)

$N =$ number of rational pts.   If $g=0$, $X = \mathbb{P}^1$

$N(g,q) = \sup\limits_{g(X)=g} N(X)$ $N = q+1$ only possibility

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

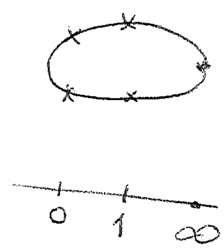
Serre interested in q small g large.   First $q=2$

g	$N(g,2)$
0	3
1	5
2	6
3	7
4	8
5	9
6	10
7	10
8	11

g	N	
9	12	
10	12 or 13	
21	21	
50	40	144 Weil bound
100	≤ 70	
1000	≤ 543	

Direct attack on low genus by geom. method

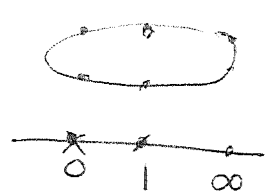
$g = 1$ ell. curve



≤ 5 clear

the bound 5 achieved by $y^2 + y = x^3 + x$

$g = 2$ hyperelliptic



≤ 6

$$y^2 + y = \frac{x^2 + x}{x^3 + x + 1}$$ works.

$g = 3$ | hyperellip. — $N \leq 6$
| non-hypell. — $X \hookrightarrow \mathbb{P}_2$ non-sing. quartic
7 points $\therefore N \leq 7$.

$g = 4$ hyperell. $N \leq 6$
intersection of a | quadric / cubic in $\mathbb{P}_3$ get $N \leq 9$ instead of 8

D. Mumford Curves and their Jacobians - for high g
no systematic description of curves of genus g

Game ~~started~~ 2 years ago with remark by Goppa (Russian in coding theory)

linear code $(\mathbb{F}_2)^N \supset V$ subspace

V "large"

2 words in V not too similar

$0 \neq v \in V$ $d(v)$ = no. of zeroes in v $\qquad \underset{\text{all } v}{d(v) \leq \delta}$

$$\mathbb{F}_2^{\,N} \xrightarrow[\text{onto}]{} V'$$

$$P_1, \ldots, P_N \in \mathbb{P}_{d-1}(\mathbb{F}_2)$$

no hyperplane contains more than δ pts.

C N rational pt.

$C \hookrightarrow \mathbb{P}_{d-1}$

so can construct codes from curves

If could realize Weil bound, then you would get improved codes. e.g. over $\mathbb{F}_{49}$

Interest: asymptotic properties as $g \nearrow \infty$

$$\limsup_{g \nearrow \infty} \frac{N(g, q)}{g} = A(q)$$

Weil $\quad N(g,q) \leq 1+q+2g\sqrt{q}$

$\Longrightarrow \quad A(q) \leq 2\sqrt{q} \qquad 2.8$

Drinfeld Vladut $\Big| \Longrightarrow \quad A(q) \leq \sqrt{q} - 1 \qquad 0.41$

Ihara Vladut $\Longrightarrow \quad A(q) = \sqrt{q} - 1$
when q is a square

curves you take if $q = p^2$ are modular curves $X_0(M)$ and use $\exists$ "supersingular" pts which are rtl over $\mathbb{F}_{p^2}$ (Shimura curves)

In general for q not square, Serre can prove

$A(q) > 0$
$A(q) > c \log q \qquad c > 0$

$A(2) \leq \sqrt{2} - 1 = 0.414..$
$A(2) \geq 0.205..$

Ideas of the proof. Assume it has N rtl pts.
to prove $g \geq \cdots$?

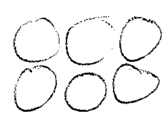
Analogy with number fields

disc. $\geq$ ....

Minkowski, Rogers, Stark
Odlyzko

disc. $\geq$ degree

genus	$\longleftrightarrow$	discriminant
# rtl pts.	$\longleftrightarrow$	degree
coding theory	$\longleftrightarrow$	geom. of nos.

geometry of nos. involves 

But Stark, Odlyzko use $\int$ and get better bds. than geom. of nos.

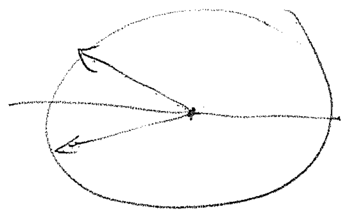
$$N_n = \text{no. of pts over } \mathbb{F}_{q^n} = 1 + q^n - \sum_{1}^{2g} \omega_i^n$$

$$|\omega_i| = \sqrt{q}$$

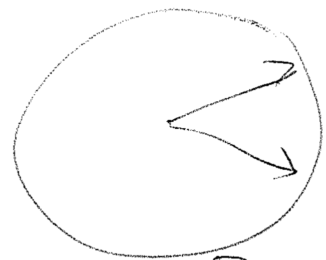
Lefschetz formula

$$N_n = 1 + q^n - q^{n/2} \sum_{\alpha=1}^{g} 2\cos(n\varphi_\alpha)$$

How to use this to see Weil not optimal



over $\mathbb{F}_q$



over $\mathbb{F}_{q^2}$

Thus Weil bds realized $\Rightarrow$ $N_{2n} = 1 + q^2 - 2gq \underset{<0}{}$ for g large

a contradiction

(This same as Hadamard that $\zeta(s) \neq 0$ $\operatorname{Re} s = 1$)

Let $f(\varphi) = 1 + 2 \sum_{n=1}^{t} c_n \cos n\varphi$

① $f(\varphi) \geq 0$ for all φ

② $c_n \geq 0$ for all n

Ex.
$$\begin{cases} 1 \\ 1 + \cos\varphi \\ \frac{1}{2}(\alpha_0 + \alpha_1 \cos\varphi + \dots + \alpha_n \cos n\varphi)^2 \qquad a_n \geq 0. \\ (1+\cos\varphi) \times \underline{\qquad\qquad} \end{cases}$$

Thm: If f as above, then
$$g \geq (N-1) \sum_{n\geq 1} c_n q^{-n/2} - \sum_{n \geq 1} c_n q^{n/2}$$

Pf: $g + c_n 2 \sum \cos(n\varphi_\alpha) \geq 0$ sum of values of f

$$\parallel$$

$$g + \sum c_n q^{n/2} - \sum c_n (N_n - 1) q^{-n/2}$$

$$g \geq \sum c_n (N_n - 1) q^{-n/2} - \sum c_n q^{n/2}$$

But $N_n - 1 \geq N - 1$.

The above is an analogue of an explicit fmla

Take $f = 1 \quad c_n = 0 \implies g \geq 0$

$f = 1 + \cos\varphi \implies$ Weil's bound

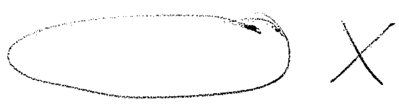
J. Oesterlé found optimal f (N, g fixed, $g \geq 3$)

This handles $g = 2$ $N \leq 10$ but not for $g = 7$.

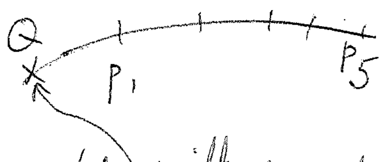
This method uses by Drinfeld Vladut

Other direction: Make fields with small discriminant class field this is a very efficient way to construct fields without writing generator. To construct a $g = 50$ with 40 pts.

Start with $g = 1$, $N = 5$ ell. curve $\qquad y^2 + y = x^3 + x$



$\downarrow$ deg 8 $\quad$ group $(2,2,2)$



$P_1 \cdots P_5$ split completely

Choose pt with deg $d = 7$. Look for abelian coverings type $2,2,2$ ramified only at Q with conductor $= 2$. Get one with gp. $(2, \ldots 2)$, $d+1 = 8$ copies. Then $P_i \mapsto \sigma_i$ for $i = 1, \ldots, 5$, so you can take ~~quotient~~ to get covering $(2,2,2)$. Compute g using Hurwitz

$$2g - 2 = 2d(2^{d-4} - 1) \qquad d = 50.$$

$A(q) > 0$ analogue of unramified class field. Make towers

$$\begin{array}{l} X_n \\ \downarrow \\ \downarrow \\ X_0 \end{array}$$

rtl $S \subset X_0$
$\neq \phi$

$$g_n - 1 = [X_n : X_0](g_0 - 1)$$

$$N_n \geq \text{———} \quad |S|$$

$$\overline{\lim} \frac{N_n}{g_n} \geq \frac{|S|}{g_0 - 1} > 0$$