J. P. Serre  Nov. 1982  Number of points on curves

\[ \frac{\mathbb{F}_q}{\mathbb{F}_q^*} \]

curve \( \mathcal{X} \) of genus \( g \) / \( \mathbb{F}_q \) \( (\text{proj. n.s.}) \)

\( N = \text{number of rational pts.} \quad \)  
\( g = 0 \quad \mathcal{X} = \mathbb{P}^1 \)

\[ N(g, \mathbb{F}_q) = \text{stays} \quad N(X) \quad \text{for} \quad g \]

\( N = g + 1 \quad \text{only possibility} \)

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

We are interested in \( g \) small \( \quad g \) large. First \( g = 2 \)

<table>
<thead>
<tr>
<th>( g )</th>
<th>( N(g, \mathbb{F}_2) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>11</td>
</tr>
</tbody>
</table>

Direct attack on low genus by genus method

\( g = 1 \quad \) all. curve

\[ y^2 + y = x^3 + x \]

\( \leq 5 \quad \text{clear} \)

the bound 5 achieved by

\( g = 2 \quad \text{hyperelliptic} \)

\[ y^2 + y = \frac{x^2 + x}{x^3 + x + 1} \quad \text{works.} \]
$g = 3$ \quad \text{hyperellip.} \quad N \leq 6

\text{non-hyperell.} \quad X \to P_2 \quad \text{non-sing. quartic}

7 \text{ points} \quad \therefore \quad N \leq 7

$g = 4$ \quad \text{hyperell.} \quad N \leq 6

\text{intersection of a quadric in } P_3 \quad \text{cubic}

\text{get } N \leq 9 \quad \text{instead of 8}

\text{D. Mumford, Curves and their Jacobians - for high } g
\text{no systematic description of curves of genus } g

\text{Game started 2 years ago with remark by Goppa (Russian in coding theory)}

\text{linear code } (F_2)^N \supset V \text{ subspace}

V \text{ "large"}

2 \text{ words in } V \text{ not too similar}

\text{if } u \neq v \in V \quad d(u) = \text{no. of zeroes in } u \quad \forall \text{ all } v

d(v) \leq \delta

\mathbb{F}_2^N \rightarrow V' \quad \text{auto}

P_1, \ldots, P_N \in \mathbb{P}_{d-1} (F_2)

\text{no hyperplane contains more than } \delta \text{ pts.}

\text{C \quad N rational pt.}

\text{C} \rightarrow \mathbb{P}_{d-1}

\text{so can construct codes from curves}

\text{if could realize Weil bound, then you would}
\text{get improved codes. e.g. over } F_{47}

\text{Interest: asymptotic properties as } g \to \infty

\limsup_{g \to \infty} \frac{N(g)}{g} = A(g)
Weil
\[ N(g, g) \leq 1 + g + 2g\sqrt{g} \]
\[ \Rightarrow A(g) \leq 2\sqrt{g} \quad \text{8.9} \]

Drinfeld
\[ V h a l d u t \quad \Rightarrow \quad A(g) = \sqrt{g} - 1 \quad \text{0.91} \]

Vladut
\[ \Rightarrow \quad A(g) = \sqrt{g} - 1 \]
when \( g \) is square curves you take if \( g = p^2 \) are modular curves \( X_0(N) \) and use \( \exists \) "supersingular" pts which are all over \( \mathbb{F}_{p^2} \) (Shimura curves)

In general for \( g \) not square, here we can prove
\[
\begin{align*}
A(g) & > 0 \\
A(g) & > c \log g \quad \text{for} \quad c > 0 \\
A(2) & = \sqrt{2} - 1 = 0.414.. \\
A(2) & > 0.205.. 
\end{align*}
\]

Ideas of the proof. Assume it has \( N \) rdl pts.

To prove \( g \geq \ldots ? \)

Analogy with number fields
disc. \( \geq \ldots \)

Minkowski, Rogers, Stark, Odlyzko
disc. \( \geq \) degree
genus \( \leftrightarrow \) discriminant
\( \# \) rdl pts. \( \leftrightarrow \) degree
galois theory \( \leftrightarrow \) genus of nos.

Geometry of nos. involves \( \ldots \), but Stark, Odlyzko use \( f \) and get better story.
\[ N_n = \text{no. of pts over } \mathbb{F}_q^n = 1 + q^n - \sum_{i=1}^{3^n} \omega_i \cdot n \]

Pfaff's formula

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

How to use this to see Weil not optimal

\[ \text{over } \mathbb{F}_q \]

\[ \text{over } \mathbb{F}_q^2 \]

Thus Weil's idea realized: \[ N_{2n} = 1 + q^2 - 2g \cdot q^2 < 0 \]

for \( g \) large

(This same as Hadamard that \( f(s) \neq 0 \) \( \text{Res } s = 1 \))

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

1. \( f(q) > 0 \) for all \( \varphi \)
2. \( c_n > 0 \) for all \( n \)

\[ c_n = \left\{ \begin{array}{ll}
1 + \cos \varphi \\
\frac{1}{2} (\alpha_0 + \alpha_1 \cos \varphi + \cdots + \alpha_n \cos^n \varphi) \\
(1+\cos \varphi)^{n-1}
\end{array} \right. \]

Thus: If \( f \) as above, then \( g \geq \sum c_n g^{-\frac{n}{2}} - \sum_{n=1}^{N_n} q^{n/2} \)

Lef: \( g \geq 2 \sum \cos(n \varphi_\alpha) > 0 \)

\[ g + \sum c_n g^{n/2} - \sum c_n (N_n - 1) g^{-n/2} \]
\[ g > \sum c_n (N_n - 1) f^{-n/2} - \sum c_n g^{-n/2} \]

But \( N_n - 1 > N - 1 \).

The above is an analogue of an explicit formula.

Take \( f = 1 \), \( c_n > 0 \) \( \Rightarrow \) \( g > 0 \)

\( f = 1 + c_n \phi \) \( \Rightarrow \) Weil's bound

J. Costerlé found optimal \( f \) \( (N, g \text{ fixed}) \).

This handles \( g = 2 \), \( N \leq 10 \) but not for \( g = 7 \).

This method uses by Drinfel'd Vladut.

Other direction: Make fields with small discriminant

Class field this is a very efficient way to construct fields without wanting generator. To construct a \( g = 50 \) with 40 pts.

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

\[ \times \]

+ deg \( 8 \) group \( (2, 2, 2) \)

Choose pt, with deg \( d = 7 \). Look for abelian covering type \( 2, 2, 2 \) ramified only at \( \mathbb{Q} \) with conductor = 2. Get one with \( [\mathbb{Q} : \mathbb{Q}(2, \ldots, 2)] = 8 \) copies. Then \( \phi_i \mapsto \phi_i \) for \( i = 1, \ldots, 5 \), so you can take quotient to get covering \( (2, 2, 2) \).

Compute \( g \) using Hurwitz

\[ d^g - 2 = 2d((d - 1)(d - 7) - 1) \]

\[ d = 50. \]