rec 3/13/86 - HFM

Rational Points on Curves over Finite Fields

Part I: "q large"

Jean-Pierre Serre

Lectures given at Harvard University, September to December 1985.

Notes by Fernando Q. Gouvêa

Contents - Part I

The case $g=3$

Curves over Finite Fields

Jean-Pierre Serre

Let C be a complete non singular curve of genus g over a finite field F_q. Let $N(C)$ be the number of rational points of C. By a well-known theorem of Weil, we have

$$|N(C) - (q+1)| \leqslant 2g\sqrt{q} .$$

For a given pair (q,g), let $N_q(g) = \operatorname{Sup}_C N(C)$. Weil's inequality implies :

$$N_q(g) \leqslant q + 1 + 2g\sqrt{q} .$$

I shall discuss several improvements of this bound. Namely :

(a) $N_q(g) \leqslant q + 1 + g[2\sqrt{q}]$.

(b) (Asymptotic result - due to Drinfeld-Vladut) :
for fixed q (and $g \to \infty$) $\text{lim.sup.}\ N_q(g)/g \leqslant \sqrt{q} - 1$,
with equality when q is a square (Ihara-Zink).

(c) Explicit computation of $N_q(g)$ when $g = 1$ or 2.

(d) Numerical results :

Table of values of $N_q(g)$

g \ q	2	3	4	5	7	8	9	11	13	16	17	19	23	25
1	5	7	9	10	13	14	16	18	21	25	26	28	33	36
2	6	8	10	12	16	18	20	24	26	33	32	36	42	46
3	7	10	14	16	20	24	28	28	32	38	40	44		56
4	8	12	15	18										
5	9													66
6	10													
7	10									65				

Curves over $\mathbb{F}_q$

$q = p^e$, p prime, $e \geq 1$

X = curve (smooth, complete, abs. irreducible).

genus of $X = g$ is well-defined

$N(X)$ = nber of pts of X rat'l $/\mathbb{F}_q$

$= \# X(\mathbb{F}_q)$

One knows:

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

If one wants $|\# X(\mathbb{F}_{q^n}) - (q^n+1)| \leq 2g q^{n/2}$ as a fct. of n, then $2g$ is optimal.

But for any given n, one doesn't know.

Want: upper bound, so curves with "many" pts.

Def: $N_q(g) = \sup_X N(X)$ (given g, q).

So Weil is: $\boxed{N_q(g) \leq 1 + q + 2g\sqrt{q}}$.

E.g., $q=2$, $g=50$; then Weil is $N \le 1+2+100\sqrt{2} = 144.\dots$
so $N \le 144$ (Weil's bound).

It's easy to see ≤ 103 (later: ≤ 40; then we'll show ≥ 40.).

So in this case $N_q(g) = 40$.

If $g = 1, 2, 3$ (small): $g=1$ is in the literature; $g=2$ known; $g=3$ known only for $q < 23$] Tuesday

AG. Varieties

---

g large, q small [asymptotic results]
(Thursday)

(see Part II)

analogy:

curves w/ many pts $\longleftrightarrow$ fields w/ small discriminan[t]

rel. to $\updownarrow$ ... $\updownarrow$ rel. to

coding theory $\longleftrightarrow$ geom. of #s

Y. Ihara: some modular curves have lots of pts, over $\mathbb{F}_{p^2}$.

Coding theory: Goppa: curves w/ many pts

$\updownarrow$ connection

codes.

Connection w/ codes

A Linear Code over $\mathbb{F}_q$ is a vector subspace $V \subset \mathbb{F}_q^n$

(Think as $V \subset W$ together w/ a basis of W (basis must be fixed, except by scalars).)

Element $(x_1, -, x_n) \in \mathbb{F}_q^n$ is a word of length n (letters $\leftrightarrow \mathbb{F}_q$).

If $q = 2$, this is a sequence of 0's and 1's.

$V \subset \mathbb{F}_q^n$ are the code-words.

message is 01001111 $\in V$

might be sent as 01100111 0

$>$ H-d = 2

two errors.

So we want an error-correcting code.

H-distance of two words = nbr of coords where they differ.

Suppose H-d ≥ 5 (for words in V)

then the wrong word $\notin V$, and the correct one is the unique closest word in V (as long as ≤ 2 errors)

Parameters are : $\begin{cases} n = \text{length of word} \\ v = \dim V \\ d = \text{min nber of non-zero coords in an element of } V, \neq 0 \text{ (since } V \text{ is subspace).} \end{cases}$

Want d large, but also v large.

[Sloane, Coding Theory]

Dual point of view

(*) Assume : for every i, $1 \leq i \leq n$, there is an $x = (x_1, -, x_n) \in V$ with $x_i \neq 0$.

Then consider the fct.

$$x = (x_1, —, x_n) \longmapsto x_i \in \mathbb{F}_q$$

non-zero linear form.

This defines an elt. $P_i \in \mathbb{P}(V^*)$

(have $V \xrightarrow[\text{inj}]{} \mathbb{F}_q^n$; by duality $\mathbb{F}_q^n \xrightarrow[\text{surj}]{} V^*$).

So find $P_1, \ldots, P_n \in \mathbb{P}(V^*)$ which generate.

$v - 1 = \dim \mathbb{P}(V^*)$

$n = \#$ of pts

What is H-d ? Let $m = \max. \#$ of P_i lying on a hyperplane.

Claim: m determines d; in fact $m = n - d$.

So we want many pts in proj. space, but not too many on a hyperplane.

Now suppose $X \hookrightarrow \mathbb{P}_{r-1}$, and take $P_1, -, P_n$ = rat'l pts of X.

Then $m \leq \deg X$.

For $g = 0$, have $\mathbb{P}_1 \hookrightarrow \mathbb{P}_{r-1}$ by standard embedding and this gives Reed-Solomon code.

Suppose X, L line bundle, $P_1, -, P_n$ rat'l pts of X.

Then take $V = H^0(X, \underline{L}) = \Gamma(L)$.

And map

$$\begin{array}{ccc} V & \longrightarrow & \mathbb{F}_q^{\,n} \\ & \searrow & \| 2 \\ & & L_{P_1} \times \cdots \times L_{P_n} \end{array}$$

$$s \longmapsto (s(P_1), \ldots, s(P_n))$$

If injective, have a code, and $d \geq \deg(L)$ since sections cannot vanish at more than $\deg(L)$ pts.

For $q = p^2$, $p \geq 7$ modular curves give better codes than the previously known ones.

Refined Weil bound

Claim: $|N - (q+1)| \leq g\,[2\sqrt{q}]$. $[\ ]$ = integral part of

Example: 1) If q is a square, ref. Weil = Weil

2) If $q = 2$, $[2\sqrt{2}] = [2.8] = 2$

so $|N-3| \leq 2g$

When $g = 50$, this gives $|N-3| \leq 100$, so $N \leq 103$.

Pf: Weil comes from:

N = nber of fixed pts of Frob $= \pi : X \to X$
$(x_0, -, x_d) \mapsto (x_0^p, -, x_d^p)$.

So shd have N = Trace π on "$H^0(X)$" $\rightsquigarrow 1$

$-$ Trace π on $H^1(X)$ $\rightsquigarrow \pi_1, \dots, \pi_{2g}$

$+$ Trace π on $H^2(X)$. $\rightsquigarrow q$

So we get $N = 1 + q - \sum_{i=1}^{2g} \pi_i$

Then he proved
- $|\pi_i| = q^{1/2}$ (R.H. for X)
- π_i is an alg. integer
- family of π_i (mult. included) is stable under $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, i.e.,

$$\prod (T - \pi_i) \in \mathbb{Z}[T].$$

Finally,

The eigenvalues of π^n (Frob. rel to $\mathbb{F}_{q^n}$) are the π_i^n.

Then we have $\quad \# X(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{i=1}^{2g} \pi_i^n$

And then this determines the π_i.

We know $\quad \pi_i \bar{\pi}_i = q \quad$ and $\bar{\pi}_i = \pi_j$, some j.

Claim: One can write the π_i in such a way that $\pi_{g+1}, \dots, \pi_{2g}$ are $\bar{\pi}_1, \dots, \bar{\pi}_g$.

Note: [$Jac(X) = A/\mathbb{F}_q$ ab. var.
Then π_i = eigenvals of the Frob. on $Jac(X)$
And the same properties hold for any ab. variety.

Claim is equiv to : if $q = q_0^2$ is a square, then q_0 and $-q_0$ occur both with even multiplicities as eigenvalues.

(Note: it's clear for all the other cases.)

Pf: ① (for curves only) if these mult. were odd, the const. in the fct'l eqn of Z would be -1, but it is $+1$ ⚡.

② Can assume the ab. variety is <u>simple</u> over $\mathbb{F}_q$.
Suppose q_0 is eigenv. with mult ≥ 1.
Then the endom. $\pi - q_0$ has a kernel and

$$\dim(\mathrm{Ker}(\pi - q_0)) \geq 1$$

Simplicity $\Rightarrow$ $\pi = q_0$ on ab. var., hence mult. q_0 is even $(= 2\dim A)$.

③ <u>Symplectic proof</u>
Take $V_\ell(A) =$ dual of H^1 (vect. sp/$\mathbb{Q}_\ell$).
& $\exists$ non-deg <u>alt</u>. form B on H^1 (def. by a polariz./$\mathbb{F}_q$)
π viewed as endom. of V is a similitude, i.e.,

$$B(\pi x, \pi y) = q\, B(x,y).$$

Now the eigenvalues of any symplectic similitude can be paired as λ_i, λ_i', $\ell - \ell$, λ_q, λ_q' s.t. $\lambda_i \lambda_i' = q$.

$\boxed{\checkmark}$

The same proof ③ shows our claim is still true for any cohomology in <u>odd</u> dimension.

<u>Example</u> in even dimension:

2-dim'l quadric over $\mathbb{F}_q$ coh is $H^0 \oplus H^2 \oplus H^4$

H^2 is 2-dim'l (basis corresps. to lines of the two rulings of the quadric)

• split quadric ($\overset{\text{say}}{x_1x_2 + x_3x_4 = 0}$), lines are def / $\mathbb{F}_q$ say e_1, e_2.

Then $\pi^* e_1 = q e_1$, $\pi^* e_2 = q e_2$, and the claim holds.

• non-split quadric: then $\pi^* e_1 = q e_2$ $\pi^* e_2 = q e_1$

eigenvectors are $e_1 + e_2$, $e_1 - e_2$ w/ eigenval $q, -q$

so claim is false.

Problem: why not $(\sqrt{q}, -\sqrt{q})$? So proof #2 is wrong.

So pair the π_i as given above. Set $a_i = \pi_i + \bar{\pi}_i$ $i = 1, \dots, g$.

So a_i real, family still $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable, since $a_i = \pi_i + \frac{q}{\pi_i}$.

And $|a_i| \le 2\sqrt{q}$.

Then $N(X) - (1-q) = -\sum_{i=1}^{2g} \pi_i = -(a_1 + \dots + a_g)$.

For an ab. variety dim g, want: $\underset{\substack{\| \\ |\sum_{i=1}^{g} a_i|}}{|T_1(\pi)|} \le g\lfloor 2q^{1/2} \rfloor$

Let $m = [2q^{1/2}]$. $|a_i| < m+1$

If we take $x_i = m + 1 + a_i$, then $x_i > 0$.

The x_i are $\left\{\begin{array}{l}\text{stable under Galois w/ multiplicities.}\\ \text{alg integers (since } \pi_i \text{ are).}\end{array}\right.$

Then $x_i > 0$, so:

$$\frac{x_1 + \cdots + x_g}{g} \geq (x_1 \cdots x_g)^{1/g}$$ with equality only if all x_i are equal.

so

$$m + 1 + \frac{\sum a_i}{g} \geq 1$$

so

$$\sum a_i \geq -mg$$ with equality only if $a_1 = \cdots = a_g$.

For the other ineq., apply same pf to $-$Frob.

So get $|\sum a_i| \leq mg$

If we have equality $\sum a_i = \pm mg$, a_i all equal, hence $a_i = \pm m$ each i.

So we have

$$-gm \leq Tr(\pi) \leq gm$$

and if $Tr(\pi) = gm$, then $a_1 = \cdots = a_g = m$

if $Tr(\pi) = -gm$, then $a_1 = \cdots = a_g = -m$.

Thm!

[This is general: can replace Deligne's $B \cdot q^{1/2}$ by $B/2$ $[2q^{1/2}]$,

Betti number

A ab var $/\mathbb{F}_q$, π Frob. endom.

<u>Thm 2</u>: (1) If $T_r(\pi) = gm - 1$ ("down by 1"), then

$$(a_1, \text{—}, a_g) = \begin{cases} (\underbrace{m, m, \dots, m}_{g-1}, m-1) & (g \geq 1) \\ (\underbrace{m, m, \dots, m}_{g-2}, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}) & (g \geq 2) \end{cases}$$

(2) If $T_r(\pi) = gm - 2$ ("down by 2"), then one of the ~~five~~ seven following possib. occurs:

$$(a_1, \text{—}, a_g) = \begin{cases} (m, m, \dots, m, m-2) & g \geq 1 \\ (m, \text{—}, m, m-1, m-1) & g \geq 2 \\ (m, \text{—}, m, m+\sqrt{2}-1, m-\sqrt{2}-1) & \\ (\text{same w/ } \sqrt{3} \quad) & \\ (m, \text{—}, m, m-1, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}) & \\ (m, \text{—}, m, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2}) & \\ (m, \text{—}, m, m+1-4\cos^2\frac{\pi}{7}, m+1-4\cos^2\frac{2\pi}{7}, m+1-4\cos^2\frac{3\pi}{7}) & \end{cases}$$

Smith has done computations which wd allow us to extend this, in principle. Cont. next Tues.

10/1 · defect 0 : $m, \dots, m$ $\quad g \geq 0$

— 1 : $\begin{cases} m, \dots, m, \; m-1 & g \geq 1 \\ m, \dots, m, \; m + \frac{-1+\sqrt{5}}{2}, \; m + \frac{-1-\sqrt{5}}{2} & g \geq 2 \end{cases}$

— 2 : $\begin{cases} m, \text{—}, m, \; m-2 & g \geq 1 \\ m, \text{—}, m, \; m-1, \; m-1 & g \geq 2 \\ m, \text{—}, m, \; m+\sqrt{2}-1, \; m-\sqrt{2}-1 & g \geq 2 \\ \quad '' \quad , \; m+\sqrt{3}-1, \; m-\sqrt{3}-1 & g \geq 2 \\ \quad '' \quad , \; m-1, \; m+\frac{-1+\sqrt{5}}{2}, \; m+\frac{-1-\sqrt{5}}{2} & g \geq 3 \\ \quad '' \quad , \; \underbrace{m+\frac{-1+\sqrt{5}}{2}, \; m+\frac{-1-\sqrt{5}}{2}}_{\text{twice}} & g \geq 4 \\ m, \text{—}, m, \; m+1-4\cos^2\frac{\pi}{7}, \; \dots & g \geq 3 \end{cases}$

A ab variety $/\mathbb{F}_q$, $\dim A = g$

$\pi : A \longrightarrow A$ Frobenius endom.

$\pi_\alpha, \bar{\pi}_\alpha$ eigenvalues $\qquad x_\alpha = \pi_\alpha + \bar{\pi}_\alpha$

$$\mathrm{Tr}(\pi) = \sum_{\alpha=1}^{g} (\pi_\alpha + \bar{\pi}_\alpha) \qquad , \quad m = [2\sqrt{q}].$$

Recall: $\mathrm{Tr}(\pi) \leq gm$ $\quad$ [for ab. vars, can twist to $\pi \longrightarrow -\pi$ so need not study the other ineq. $-gm \leq \mathrm{Tr}$

If $\mathrm{Tr}(\pi) = gm$, $\quad (x_1, \text{—}, x_g) = (m, \text{–} \text{–}, m)$ $\qquad$ ("defect 0")

"Defect 1" $\quad \mathrm{Tr}(\pi) = gm - 1$ $\quad \Big\rangle$ possibilities for $(x_1, \text{—}, x_g)$ are as above.
"Defect 2" $\quad \mathrm{Tr}(\pi) \; gm - 2$

For $k=2$, $d(\alpha) < 4$ so $d(\alpha) = 1, 2$ or 3

$d(\alpha) = 1 \rightsquigarrow \alpha = 3$

$d(\alpha) = 2 \rightsquigarrow \alpha$ satisfies $X^2 - 4X + q = 0$

roots real, hence $16 - 4q > 0$

so $q < 4$, so $q = 1, 2$ or 3

$X^2 - 4X + 1 = 0 \rightsquigarrow 2 \pm \sqrt{3}$

$X^2 - 4X + 2 = 0 \rightsquigarrow 2 \pm \sqrt{2}$

$X^2 - 4X + 3 = 0$ not deg 2

$\quad \shortparallel$

$(X-1)(X-3)$

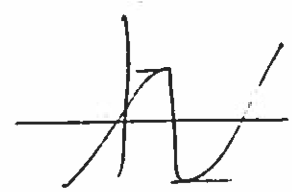
$d(\alpha) = 3 \longrightarrow P(X) = X^3 - 5X^2 + pX - q = 0$

three real positive roots

$\therefore$

$3X^2 - 10X + p = 0$

has 2 real roots



so $\frac{\Delta}{4} = 25 - 3p > 0$

So $p = 1, 2, \dots, 8$.

Fix p: find roots of P': $x = \frac{5 - \sqrt{25-3p}}{3}$

$y = \frac{5 + \sqrt{25-3p}}{3}$

Compute values of P at x, y, say f, g

We are interested in alg. integers α, tot >0, of deg. $d(\alpha)$ with "small" trace (w.r. to d).

<u>Thm</u> (Siegel, M.A. vol III, first paper) If α is as above and $\alpha \neq 1, \frac{3\pm\sqrt{5}}{2}$, then $Tr(\alpha) > \frac{3}{2} d(\alpha)$.

(If $\alpha = 1$, $Tr(\alpha) = d(\alpha)$, $\alpha = \frac{3\pm\sqrt{5}}{2}$, $Tr(\alpha) = 3 = \frac{3}{2} d(\alpha)$.)

[Best constant: instead of $\frac{3}{2}$, $\frac{5}{3}$].

Assume <u>Siegel's thm</u>: Separate out exceptional cases.

If k is a given integer ≥ 0, the number of tot >0 α's with $Tr(\alpha) = d(\alpha) + k$ is finite for each k, and these α's can be found effectively.

<u>Pf</u>: By Siegel, $d(\alpha) + k > \frac{3}{2} d(\alpha)$

so $d(\alpha) < 2k$ is <u>bounded</u>.

But α satisfies

$$X^d - (d+k) X^{d-1} + \cdots\cdot .$$

Conjugates $\alpha_1, \ldots, \alpha_d$ are all <u>positive</u>, and all $< d(\alpha) + k$.

Hence coeffs are effectively bounded, and we can list the possible α's. $\boxed{/}$

For $k=0$, get $\alpha = 1$

For $k=1$, can take $\alpha = \begin{cases} \frac{3\pm\sqrt{5}}{2} \\ 2 \end{cases}$

and no others since $d(\alpha) < 2$

Find only one irred. polynomial of this form! $p=6$, $f=1$

$X^3 - 5X^2 + 6X - 1$

Roots are $4\cos^2\frac{\pi}{7} = 2 + \omega + \bar{\omega}$ $\qquad \omega = e^{2\pi i/7}$

and its three conjugates

So $k=2$ $\begin{cases} 3 \\ 2 \pm \sqrt{3} \\ 2 \pm \sqrt{2} \\ \text{conjs. of } \; 4\cos^2\frac{\pi}{7}. \end{cases}$

Smyth, Annals Inst. Fourier, 1984 : up to $k=6$

Note: $\exists$ ∞ many α with $\mathrm{Tr}(\alpha) < 2\deg(\alpha)$

Smyth: $\exists$ only finitely many ∞ with $\mathrm{Tr}(\alpha) < 1.7719 \deg(\alpha)$.

Open question: what is the correct constant.

Consider map $\alpha \longmapsto \dfrac{\mathrm{Tr}(\alpha)}{\deg \alpha}$. Question is equiv. to : what is first accum. pt. of $\mathrm{Im}(\alpha)$?

Can look for polynomials (not nec. irred.) $X^d - a_1 X^{d-1} + \cdots$,
s.t. coeffs $\in \mathbb{Z}$, all roots are real > 0.

Let F_k = set of all such pol. with $a_1 = d + k$.

Wanted: For a given degree d, list of polyn. in F_k.

Write $P = Q_1 \cdots Q_r$ $\qquad Q_i$ irred / $\mathbb{Q}$

Q_i's have same property, and also

$$a_1(P) - \deg(P) = \sum_i \underbrace{a_1(Q_i) - \deg(Q_i)}_{\geq 0}.$$

So suppose $k = 1$: $P = Q_1 \ldots Q_r$

one Q_i with defect 1, others defect 0.

So $\quad (X-1)\cdots(X-1)\cdot(X-2)$

or

$\quad (X-1)\cdots(X-1)\cdot(X^2-3X+1)$.

Now if π is s.t. $Tr(\pi) = mg - k$, $x_\alpha = \pi_\alpha + \bar{\pi}_\alpha$

take $\quad P = \prod (X - (m+1-\pi_\alpha - \bar{\pi}_\alpha))$.

This has tot. positive roots, defect k, hence is part of my list, etc..

Set $\quad x = [x] + \{x\}$

int part $\quad$ frac'l part.

$$2\sqrt{q} = m + \{2\sqrt{q}\}.$$

So claim: second defect 1 case is possible only if $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2} = 0.6$

Since $\quad m + \frac{-1+\sqrt{5}}{2} \leq 2\sqrt{q}$ by Weil

so $\quad \{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{}$

And similarly, all the defect 2 cases except the first case has an inequality of this kind attached:

defect 0 —

defect 1 $\left\{\begin{array}{l} — \\ \{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2} \end{array}\right.$

defect 2 $\left\{\begin{array}{l} — \\ — \\ \{2\sqrt{q}\} > \sqrt{2}-1 = 0.4\ldots \\ \{2\sqrt{q}\} > \sqrt{3}-1 = 0.7\ldots \\ \{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2} = 0.6\ldots \\ -\text{same}- \\ \{2\sqrt{q}\} > 1-4\cos^2\frac{3\pi}{7} = 0.8\ldots \end{array}\right.$

Ex: The last case is possible for $q=2$:

$$\{2\sqrt{2}\} = 0.828\ldots > 1-4\cos^2\frac{3\pi}{7}.$$

We will see: $\exists$ curve$/\mathbb{F}_2$, $g=3$, 7 pts, $m=2$

$1+2+6=9$, so down by 2,

and is of the last kind. ☒

The possibilities all occur (one thinks) for abelian varieties — not nec. for curves.

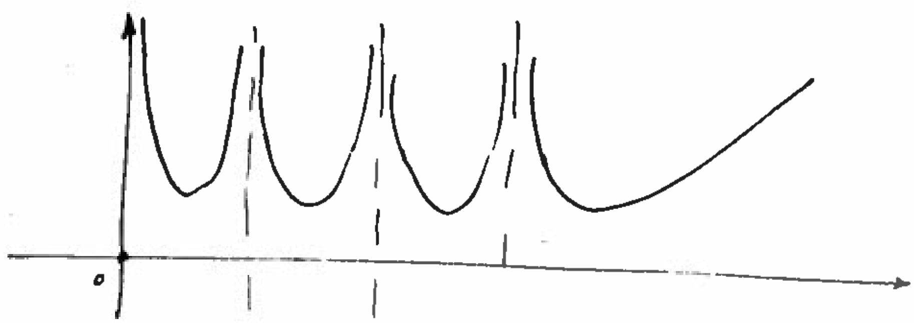
Smyth's proof of Siegel's thm:

Let $P_\lambda(X)$ be a finite family of polynomials which are monic, all roots real and positive $_{\geq 0}$, coeffs in $\mathbb{Z}$.
Let c_λ be ≥ 0 real numbers.

Let $$g(x) = x - \sum_\lambda c_\lambda \log |P_\lambda(x)| \qquad x > 0,\ x \neq \text{root of } P_\lambda.$$

and let $\min(g) =$ minimum of g on $[0, +\infty]$.

Graph is



, hence a min exists.

Let α be a totally positive alg integer $\neq$ roots of the P_λ.

Then $$\boxed{\frac{\mathrm{Tr}(\alpha)}{\deg(\alpha)} \geq \min g}.$$

Proof: Let $d = \deg(\alpha)$, $\overset{\alpha}{\alpha_1''}, \ldots, \alpha_d$ the conjugates, $\alpha_i > 0$.

$$|P_\lambda(\alpha_1) \cdot P_\lambda(\alpha_2) \ldots P_\lambda(\alpha_d)| \geq 1$$

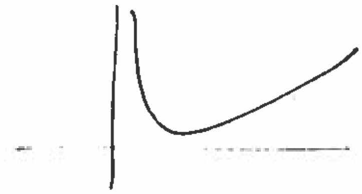
resultant of P_λ and irred polyn of α, so $\in \mathbb{Z}^*$

so $$\sum \log |P_\lambda(\alpha_i)| \geq 0.$$

$$\frac{\mathrm{Tr}(\alpha)}{\deg \alpha} = \frac{1}{d}\sum \alpha_i = \frac{1}{d}\sum g(\alpha_i) + \underbrace{\frac{1}{d}\sum_{i,\lambda} c_\lambda \log |P_\lambda(\alpha_i)|}_{\geq 0}$$

$$\geq \frac{1}{d}\sum g(\alpha_i) \geq \min g$$

Examples: • $g(x) = x - \log|x|$



$\min(g) = 1$

so get $Tr(\alpha) \geq \deg(\alpha)$

And get equality only for $\alpha = 1$.

• $g(x) = x - \frac{3}{4}\log|x| - \frac{3}{4}\log|x-1|$

optimal case will need equal minima

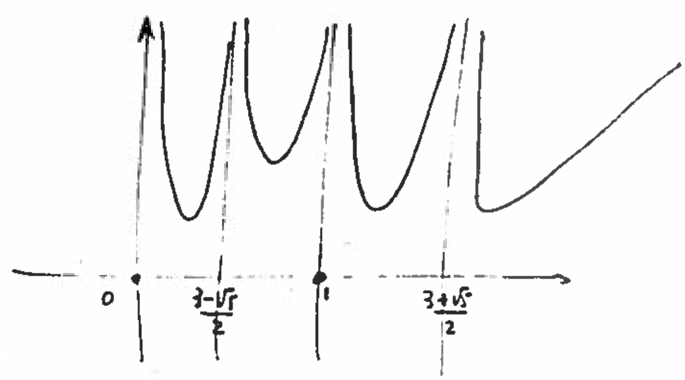
$g'(x) = 1 - \frac{3}{4x} - \frac{3}{4(x-1)}$

find zeros, etc.

Find: $\min g > 1.46$, hence get $\frac{Tr(\alpha)}{\deg(\alpha)} > 1.46$ for $\alpha \neq 1$.

• $g(x) = x - a\log|x| - b\log|x-1| - c\log|x^2 - 3x + 1|$

Taking
$a = 0.574$
$b = 0.879$
$c = 0.374$



one gets $\min g > 1.591$,

hence $\frac{Tr(\alpha)}{\deg(\alpha)} > 1.59$

$\alpha \neq 1$, $\alpha \neq \frac{3 \pm \sqrt{5}}{2}$ This improves Siegel.

• Smyth gets 1.7719

$x_\alpha = \pi_\alpha + \bar{\pi}_\alpha \qquad \alpha = 1, \ldots, g$

Theorem: Suppose $\{1, \ldots, g\}$ can be partitioned in two non-empty subsets I and J s.t.:

a) The x_α ($\alpha \in I$) are permuted by $Gal(\bar{Q}/Q)$ (Same for x_α ($\alpha \in J$)).

b) $x_\alpha - x_\beta \quad \alpha \in I, \beta \in J$ is a <u>unit</u> (any α, β).

Then the given abelian variety is not a jacobian.

(i.e., such a partition does not exist for the π_α's coming from a curve).

[Eg.: $m, m, \ldots, m, m-1$ is impossible for curves if $g \geq 2$]
second defect 1 case imp. " " " $g \geq 3$

defect 2
- —— ?
- ⟶ imp for curves if $g \geq 3$
- ⟶ " $g \geq 3$
- ⟶ ?
- ⟶ " $g \geq 3$ — $\underbrace{m, \ldots, m, m-1}, \underbrace{m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}}$
- ⟶ " $g \geq 5$
- ⟶ " $g \geq 4$

$\therefore$ For curves, many of the condns on g are <u>equalities</u>.

So table for curves is

defect 0	——	$g \geq 0$
defect 1	——	$g = 1$
	——	$g = 2$
defect 2	——	$g \geq 1$
	——	$g = 2$
	——	$g = 2$
	——	$g \geq 2$
	——	$g = 3$
	——	$g = 4$
	——	$g = 3$

Reformulate conditions:

$$P(X) = \prod_{\alpha=1}^{g} (X - x_\alpha) \qquad \text{monic, coeffs} \in \mathbb{Z}.$$

So (a) & (b) $\iff$ $P = P_1 \cdot P_2$ where $\deg(P_i) \geq 1$, P_i monic coeffs and $\operatorname{Res}(P_1, P_2) = \pm 1$.

$\iff$ P_1 & P_2 generate the unit ideal in $\mathbb{Z}[X]$.

Pf A ab. variety $/\mathbb{F}_q$, $\pi : A \longrightarrow A$, $\pi = F$ (Frobenius)

Have $V : A \longrightarrow A$ s.t. $FV = VF = q$.

(c. 1970, Waterhouse)

$x_\alpha = \pi_\alpha + \frac{q}{\pi_\alpha}$ F+V is ss on the $V_\ell(A)$.

So eigenvalues of F+V are the x_α (each twice).

Now $P(X) = \prod (X - x_\alpha)$, so $P(X)^2$ is char polyn of F+V.

This gives $P(F+V)^2 = 0$. In fact $P(F+V) = 0 \in \mathrm{End}(A)$.

So look at
$$\begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathrm{End}(A) \\ f & \longmapsto & f(F+V) \end{array}$$

get
$$\mathbb{Z}[X]/P \longrightarrow \mathrm{End}(A)$$

If $P = P_1 \cdot P_2$, P_1 & P_2 strongly rel. prime, so $1 = Q_1P_1 + Q_2P_2$,
get

$$\begin{array}{ccc} \mathbb{Z}[X]/P & \longrightarrow & \mathrm{End}\, A \\ \wr\wr & & \\ \mathbb{Z}[X]/P_1 \times \mathbb{Z}[X]/P_2 & & \end{array}$$

$\varepsilon_1 = Q_1P_1$ $\varepsilon_2 = Q_2P_2$

are orthogonal idempotents

So define $A_1 = \ker \varepsilon_2$, $A_2 = \ker \varepsilon_1$

Then one has $A_1 \times A_2 \hookrightarrow A$

And inverse is $A \xrightarrow[(\varepsilon_1, \varepsilon_2)]{} A_1 \times A_2$

So $A \cong A_1 \times A_2$ hence A_1, A_2 are ab. varieties

And eigenvalues of $F+V$ on A_1 give P_1.
on A_2 give P_2.

But $\mathrm{Hom}_{\mathbb{F}_q}(A_1, A_2) = 0$ (Since $\mathrm{Hom}_{\mathbb{F}_q}(\ ) \neq 0$ iff there is a common root of $F+V$.)

Polarization on ab. variety is a hom

$$\begin{array}{ccc} A & \longrightarrow & \hat{A} \\ \| & & \| \\ A_1 \times A_2 & \longrightarrow & \hat{A}_1 \times \hat{A}_2 \end{array}$$

Since $A_1 \sim \hat{A}_1$, $A_2 \sim \hat{A}_2$, must have $A_1 \longrightarrow \hat{A}_1$
$A_2 \longrightarrow \hat{A}_2$

So every polarization on A is decomposable.

So Θ divisor on A is $\Theta_1 \times A_2 + A_1 \times \Theta_2$

But: on a Jacobian, the Θ-divisor is irreducible. $\boxed{\text{\&}}$

10/8 **Theorem** (Beauville) If q $(=p^e, e \geq 1)$ is either of the form x^2+1 $(x \in \mathbb{Z})$ or x^2+x+1 $(x \in \mathbb{Z})$, then, if X is a curve of genus $g \geq 2$ on $\mathbb{F}_q$, $N(X) \neq q+1-gm$, $N(X) \neq q+1+gm$, where $m = [2q^{1/2}] = 2x$ or $2x+1$, resp.

Corollary: $|N(X) - (q+1)| < gm$

Take +70.

Special case (Stark): $q = 13 = 3^2+3+1$, $g=2$ so $m=7$.

So $|N - 14| < 14$

When $g=2,3$, $\exists$ different proof involving classes of Hermitian forms.

Note

1) If $q = x^2+1$, $4q = 4x^2+4 < (2x+1)^2$ (clear!)

so $4x^2 < 4q < (2x+1)^2$

So $[\sqrt{4q}] = 2x = m$.

If $q = x^2+x+1$ $4q = (2x+1)^2+3$ etc., so $m = 2x+1$.

so $m^2 - 4q = \begin{cases} -4 & \text{first case} \\ -3 & \text{second case} \end{cases}$.

2) If $q = p$ prime, it is open whether there are ∞ many such primes. One thinks there should be

In fact $\# \{p \leq P : p = x^2+1\} \sim c \dfrac{P}{(\log P)^2}$ is a conj

3) If $q = p^e$, e odd ≥ 3

Only sol'n: $7^3 = 18^2+18+1$

Point is $y^e = x^2 + 1$ no soln if e odd ≥ 3 (Lebesgue 1850

$y^e = x^2 + x + 1$ only one soln (non-trivial) e odd ≥ 3

Nagel, Ljundgren

Both cases: p-adic method of Skolem.

Proof: Consider the case $q = x^2+1$, so $m = 2x$; assume X is genus g and $N(X) = q+1-gm$.

Then I can arrange the eigenvalues of Frob π_α s.t.

$$\begin{cases} \pi_1 + \bar{\pi}_1 = m & \pi_1\bar{\pi}_1 = q = x^2+1 \\ \vdots & \\ \pi_g + \bar{\pi}_g = m & \pi_g\bar{\pi}_g = q \end{cases}$$

So $\begin{cases} \pi_1 = \cdots = \pi_g \\ \bar{\pi}_1 = \cdots = \bar{\pi}_g \end{cases}$

(If I assumed $N(X) = q+1+gm$, would get $\pi_1 = -x+i$;

If $q = x^2+x+1$, get $\mathbb{Z}[\omega]$, $\omega^3=1$

So $\pi_1 = x+i$, $\bar{\pi}_1 = x-i$

So $\mathbb{Z}[\pi_1] = \mathbb{Z}[i]$

Let F = Frob.; then eigenvalues are $x+i$ g times, $x-i$ g times.

Put $\sigma = F - x \in \mathrm{End}(\mathrm{Jac}(X))$

$\therefore$ eigenvalues of σ are i (g times), $-i$ (g times).

$\therefore \sigma^4 = 1$, $\sigma^2 = -1$.

Polariz are $\mathrm{Jac}(X) \xrightarrow{\sim} \mathrm{Jac}(X)^*$ (dual)
or equiv. classes of ample divisors

Recall:

Parenthesis on Torelli's theorem

X genus g (≥ 2) $\longrightarrow$ $\mathrm{Jac}(X)$, ab. variety dim g w/ a polarization given by image of X to power $g-1$ (which is ample divisor!).

: Weil, in 2 of coll. papers.

Thm: Let X, X' be two curves over a perfect field k.

Let $\varphi: \mathrm{Jac}(X) \xrightarrow{\cong} \mathrm{Jac}(X')$ be an isom. compatible with polarizations.

Then a) if X is hyperelliptic, there exists a unique isom. $f: X \xrightarrow{\cong} X'$ which gives φ.

b) if X is not hyperelliptic, there exists a unique isom $f: X \xrightarrow{\sim} X'$ and a unique $\varepsilon \in \{\pm 1\}$ s.t. f gives $\varepsilon\varphi$.

Corollary: If σ is an automorphism of $\mathrm{Jac}(X)$ preserving the polarization, then either σ or $-\sigma$ comes from an autom. of X.

Finit parentheses

Now we want to prove our σ is compatible with the polarization

Compatibility of σ w/ polarization

Can view polarization as giving an alternating form on V_ℓ.

V_ℓ = Tate-module attached to some ab. var.

Lauiz $\longleftrightarrow$ $E: V_\ell \times V_\ell \longrightarrow V_\ell(\mathbb{G}_m) \underset{\text{not can.}}{\simeq} \mathbb{Q}_\ell$ non-deg. alternating form.

and we have $E(Fx, Fy) = q\, E(x,y)$ F = Frob. is a similitude

(using V : $FV = q$, get $E(Fx, y) = E(x, Vy)$)

$\longrightarrow$ so adjoint of F w.r.t. E is V.

In our case F is like $x+i$, so V is like $x-i$ $\longrightarrow$

$\Longrightarrow$ in our case adj. on $\mathbb{Z}[i]$ = ring gen by F is cx conjugation.

i.e., for $\lambda \in \mathbb{Z}[F] \simeq \mathbb{Z}[i]$, $\operatorname{adj}(\lambda) = \bar\lambda$.

For our σ, get $E(\sigma x, y) = E(x, \bar\sigma y) = E(x, \sigma^{-1} y)$

$\therefore\ E(\sigma x, \sigma y) = E(x,y)$.

So σ preserves E $\therefore$ the polarization. $\blacksquare$

$\therefore$ σ or $-\sigma$ comes from an autom of X, so both are ($\sigma^3 = -\sigma$, el

(if $q = x^2+x+1$ get either σ or $\overset{\text{order } 3}{-\sigma}$) order 6

So σ comes from an autom. of X.

I claim: if $\omega_1, \dots, \omega_g$ are a basis of dfk's on X, then

$$\sigma^* \omega_i = \lambda \omega_i \quad , \lambda \text{ indep. of } i \text{ fixed.}$$

Pf: dfk's come from $\mathrm{Jac}(X)$, so we want to prove this on Tgt space to $\mathrm{Jac}(X)$. But $F = 0$ on tgt space, $\sigma = F - x$, hence σ acts by $-x$ on tgt space. So $\lambda = -x$ or x. $\boxed{}$

Canonical map: $\mathrm{can}: X \longrightarrow \mathbb{P}^{g-1}$

defined by taking $\omega_1, \dots, \omega_g$ as homog. coords.

Non-homogeneously: $Q \longmapsto \left(1, \frac{\omega_2}{\omega_1}(Q), \dots, \frac{\omega_g}{\omega_1}(Q)\right)$

for $g \geq 2$, if X is not hyperelliptic, can is an embedding

if X is hyperelliptic, image has genus zero & can has degree 2

(So gives $X \xrightarrow{\text{order } 2} \mathbb{P}^1$ covering)

Then σ acts trivially on image(can); in the first case, this implies $\sigma = 1$; in the second case, this implies σ is of order 2, $\sigma = \pm 1$ $\Rightarrow$. $\boxed{}$

[Original proof (w/o can) used "Woods Hole fixed pt formula".]

Review of $g = 1$:

Elliptic Curves

a determine curve up to $\mathbb{F}_q$-iso

$\pi, \bar{\pi}$ eigenvalues of F, $\pi\bar{\pi} = q$, $a = \pi + \bar{\pi}$ trace.

$|a| \le 2q^{1/2}$. $q = p^e$ $e \ge 1$, p prime

For a given q, what are the possibilities for a?

Answer is implicit in Deuring (~1942); Waterhouse (Ann. ENS, 1969):

Answer is: Suppose $a \in \mathbb{Z}$, $|a| \le 2q^{1/2}$

Theorem (i) if a is prime to p, a is OK (i.e., is $\mathrm{tr}\, F$ for some elliptic curve $/\mathbb{F}_q$) ("ordinary case").

(ii) if $p | a$, then a is OK if and only if either:

$$q = p^e,\ e \text{ even},\quad a = \pm 2p^{e/2}$$

$$q = p^e,\ e \text{ even},\quad a = \pm p^{e/2},\quad p \not\equiv 1 \pmod 3$$

$$q = p^e,\ e \text{ even},\quad a = 0 \qquad p \not\equiv 1 \pmod 4$$

$$q = p^e,\ e \text{ odd} \begin{cases} a = 0 \\ a = \pm p^{\frac{e+1}{2}} \qquad p = 2 \text{ or } 3 \end{cases}$$

[Note: $p^{\frac{e+1}{2}} \le 2p^{e/2} \Rightarrow p^{1/2} \le 2 \Rightarrow p \le 4$]

Proof (i) Start in char $= 0$ and reduce.

$\pi^2 - a\pi + q = 0 \implies \pi$ generates a ring $R \subset$ imag. q. field.

can prove $\implies \exists$ curve$/\mathbb{C}$ with $\mathrm{End} \cong R$.

Write it over $\bar{\mathbb{Q}}$, then some number field K.

Prove: good redn at p for K large enough, so reduce at p.

Get an "ordinary" curve because $p \nmid a$. So $\mathrm{End} \subset$ imag. quad. field.

Prove: this is def over some $\mathbb{F}_{q^N}$, and the Frob π' is π^N.

Now use descent. This gives the desired curve. ☒

(ii) supersingular curves

End = max'l order in the quat. algebra $H_{p,\infty}$ ramified at p and ∞ (and not elsewhere).

$\pi = \mathrm{Frob} \in \mathrm{End}$ has a power F^f $(f \geq 1)$ which is a scalar (i.e., $\in$ center$(H_{p,\infty})$).

So look for $\pi \in H_{p,\infty}$, π integer, $\pi\bar{\pi} = q$ s.t. some power of π is an element of $\mathbb{Q} \subset H_{p,\infty}$.

Such a π gives an ell. curve (take max'l order containing it, get ell curve, descend.)

(Know $\displaystyle\sum_{E \text{ s.s.}} \frac{1}{\# \mathrm{Aut}(E)} = \frac{p-1}{24}$ $\longrightarrow$ this shows that some ss curve exists.)

Suppose $q = p^e$, e even.

Look at $x = \frac{\pi}{p^{e/2}}$; this is still an integer (look at val'ns

So have $x\bar{x} = 1$, x integer $x \in$ quad. field

So $a = \pm 2p^{e/2} \longleftrightarrow$ roots of 1 : ± 1

$a = \pm p^{e/2} \longleftrightarrow$ roots of order 3, 6 or 4

(then $\mathbb{Q}(\sqrt{i}) \subset \mathbb{H}_{p,\infty}$, say, then p cannot be split).

etc.

Suppose $q = p^e$, e odd; let $x = \frac{\pi}{p^{e-1/2}}$

then $x^2 - \lambda x + p = 0$ and λ is div. by p (since $\lambda = x +$ look at valn

But $\lambda \leq 2p^{1/2}$.

So either $\lambda = 0$ or $p = 2$ $\lambda = \pm 2$, $p = 3$, $\lambda = \pm 3$.

This gives the result. ▨

Let $N_q(1)$ = max'l number of pts on ell. curve/$\mathbb{F}_q$, $m = [2q^{1/2}]$.

Theorem: $N_q(1) = q + 1 + m$, except when $q = p^e$, e odd, $e \geq 5$ and $m \equiv 0 \pmod{p}$, in which case $N_q(1) = q + m$.

smallest exceptional case: $q = 128 = 2^7$

Proof : When can we have $a = -m$?

a) OK when $p \nmid m$

b) OK when q is a square, since $a = -2q^{1/2}$ is allow

Remains : $q = p^e$, e odd, $p | m$.

If $e = 1$, OK : $p | a \Rightarrow \begin{cases} a = 0 \text{ if } p \geq 5 \\ a = \pm p \text{ if } p = 2, 3. \end{cases}$ But $m \neq 0$, cannot have $p|m$

If $e = 3$, have $4p^3 = m^2 + \varepsilon$ $\quad 1 \leq \varepsilon \leq 2m < 2^{3/2} p^{3/2}$

Now suppose $m = p\mu$: $4p^3 = p^2\mu^2 + \varepsilon \Rightarrow p^2 | \varepsilon$

so $p^2 < 2^{7/2} p^{3/2}$

$\Rightarrow p^{1/2} < 2^{3/2} \Rightarrow p < 8$

$\Rightarrow p = 2, 3, 5, 7$ and check these. $\longrightarrow$ cannot have $p|m$.

Finally, to get $N_q(1)$ for q exceptional, note $p|m \Rightarrow p \nmid (m-1)$.

Exceptional : $q = 2^7$, $q = 7^5$

Take $q = 2^*$. When is this exceptional?

$q = 2^7$: $\quad 2\sqrt{q} = 2 \cdot 2^{7/2} = 2^4 \cdot \sqrt{2}$

$\sqrt{2} = 1.01101010000001\ldots$ in binary

$2^4 \cdot \sqrt{2} = 10110.10\ldots$

$m = [2^4\sqrt{2}] = 10110 \quad \therefore \; p \mid m$

even!

Therefore 2^7 is exceptional, because $\sqrt{2} = 1.01101010000001\ldots$

$2^7 \quad 2^{11} \quad 2^{15} \quad 2^{17}$

$\therefore \; \exists$ infinitely many exceptional 2^*.

3^7 exceptional

$2\sqrt{3} = 3.110112022\ldots$ (3-adic)

$2\sqrt{7} = 5.20166\ldots$ (7-adic)

7^5 exceptional.

So cannot know how many exceptional p^e's for $p > 2$.

10/15

last time : $\underline{g=1}$

There $N_q(1)$ = max nbr of points of a curve of genus 1 over $\mathbb{F}_q$

[Get : $N_q(1) = 1 + q + m$, $m = [2\sqrt{q}]$,

except, when $q = p^e$, e odd ≥ 3, and $p | m$, in which case

$N_q(1) = q + m$]

To find exceptional q, look at p-adic expansion of $2\sqrt{q}$.

Problem: Ell. curve over $\mathbb{Q}$, reduce mod p. For what p's does it have maximal (or minimal) number of points?

Should find an infinite number, and should have to distinguish CM and non-CM. (Very hard to handle).

Still $g=1$

ref. Weil $= q + 1 + [2\sqrt{q}]$

So have $|\text{ref. Weil} - N_q(1)| \leq 1$ for all q.

(Will see : in $g=2$

$|\text{ref. Weil} - N_q(2)| \leq 3$.)

For $g=3$:

$$|\text{ref. Weil} - N_q(3)| \leq \ ?$$

Conjecture: For $g = 3, 4, 5$ and not many more,

$$|\text{ref. Weil} - N_q(g)| \leq C(g),$$

$C(g)$ depending only on g.

For $g=1,2$ (more generally, for hyperelliptic curves), have curve C, Frob. $\pi \in End(J(C))$.

C hyperelliptic $\Rightarrow \exists\, \sigma$ autom. of order 2 of C which acts by -1 on $Jac(X)$

$$\begin{array}{c} k' \\ {\scriptstyle 2}\big| \\ k \end{array} \text{ quad. twist; } \begin{array}{c} \mathbb{F}_{q^2} \\ \big| \\ \mathbb{F}_q \end{array} \quad \text{then Frob of } C_{\text{twisted}} = -\text{Frob of } C$$

And if $N(C) = q+1-a$, $N(C_{\text{twisted}}) = q+1+a$.

So $N(C)$ max $\Rightarrow N(C_{\text{twisted}})$ minimum (etc.).

If char $\neq 2$, C is $y^2 = f(x)$

C_{twist} is $y^2 = u f(x)$ $\quad u \in \mathbb{F}_q$ not a square.

char $= 2$ $\quad C$ is $y^2 + y = \varphi(x)$

C_{twist} is $y^2 + y = \varphi(x) + a$, $\quad a \in \mathbb{F}_q$, a not of

i.e., Tr

For $g=3$, not hyperelliptic, the "min" and "max" problems will separate. But for large g and fixed q, "min" will be sec

---

Results of Tate and Honda

(Tate, Inventiones 2 (1966), 134-144
Tate, Sem. Bourb., exp 352
Milne & Waterhouse, Symp Pure Math AMS, ___)

"Weil number" /q is an alg. integer π s.t. all conj. of π have (arch.) abs. value $q^{1/2}$.

one-one corresp:

$$\left(\begin{array}{l} A \text{ abelian variety } /\mathbb{F}_q \\ \text{simple } /\mathbb{F}_q \end{array}\right) \Big/ (\text{isogenies}) \longleftrightarrow (\text{Weil numbers}) \Big/ (\text{conjugation})$$

$$A \longmapsto \text{roots of Frobenius on } A$$

A s.t. eigenvalues of Frob are $\pi_1, \dots, \pi_d$ repeated a certain number of times $\longleftrightarrow$ $\pi_1, \dots \pi_d$, $d = \deg \pi$

Tate's theorem

π Weil number, A the corresp. simple abelian variety /$\mathbb{F}_q$. Let $\Lambda = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$.

Then we know:

(1) Λ is a division algebra.

(2) $\Lambda \supset \mathbb{Q}(\pi)$, $\mathbb{Q}(\pi)$ = center of Λ.

The local invariant of Λ as element of $Br(\mathbb{Q}(\pi))$ is (i_v), v place of $\mathbb{Q}(\pi)$, $i_v \in \mathbb{Q}/\mathbb{Z}$, $\sum i_v = 0$.

(3) If v is a real place, $i_v = \frac{1}{2}$

——— complex ——, $i_v = 0$

——— ℓ-adic place, $\ell \neq p$, $i_v = 0$

If v has residue char p, $i_v = \dfrac{v(\pi)}{v(q)} \left[\mathbb{Q}(\pi)_v : \mathbb{Q}_p\right]$.

(4) Call r the smallest common denominator of the i_v (i.e., the order of Λ in $Br(\mathbb{Q}(\pi))$).

Then $[\Lambda : \mathbb{Q}(\pi)] = r^2$

(5) $\dim A = \frac{r}{2}[\mathbb{Q}(\pi) : \mathbb{Q}] = d_\pi$

Corollary: The multiplicity of π as eigenvalue of Frob. in any ab. variety over $\mathbb{F}_q$ is a multiple of r.

(Since it occurs for A w/ multiplicity $r = 2d_\pi/\text{no. of conj's}$)

$q = p^2$, $\pi = p$

So $\mathbb{Q}(\pi) = \mathbb{Q}$ so $\begin{cases} i_\infty = 1/2 \\ i_\ell = 0 \\ i_p = \frac{1}{2}[\mathbb{Q}:\mathbb{Q}] = \frac{1}{2} \end{cases}$

So $\Lambda = H_{p,\infty}$ quat alg. ramified at p, ∞.
So $r = 2$, $\dim A = \frac{r}{2}[\mathbb{Q}:\mathbb{Q}] = 1$, so A is ell. curve.

$\pi = \sqrt{p}$, $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{p})$

($q = p$ = prime) two real places $i_{\infty_1} = \frac{1}{2}$, $i_{\infty_2} = \frac{1}{2}$

one p-adic place $i_p = 0$ (mod $\mathbb{Z}$).

(Since sum is zero mod $\mathbb{Z}$).

So get quat field in $\mathbb{Q}(\sqrt{p})$ ramif. at ∞, $= H_{p,\infty} \otimes \mathbb{Q}(\sqrt{p})$.
$r = 2$, $[\mathbb{Q}(\sqrt{p})_p : \mathbb{Q}] = 2$ so $\dim A = 2$.

$\therefore$ multiplicity of $\sqrt{p}$ as eigenvalue of Frob occurs always with even multiplicity (as desired way back when).

Ord. Ell. Curves: $\pi\bar{\pi} = p$, $\pi + \bar{\pi} = a$ $p \nmid a$
(over $\mathbb{F}_p$)
$[\mathbb{Q}(\pi):\mathbb{Q}] = 2$, p splits
(look at Newton polygon)
v_1, v_2 div p so $v_1(\pi) = 0$ $v_2(\pi) = 1$
So $i_{v_1} = 0$, $i_{v_2} = 1 \cdot 1 = 0 \in \mathbb{Q}/\mathbb{Z}$.
$\to$ no real places.

So $\Lambda = \mathbb{Q}(\pi)$.

Recall: $\exists$ quadratic π's "forbidden" for ell. curves

In particular:

$m = [2q^{1/2}]$ is not trace Frob if $q = p^e$ e odd ≥ 3 and $p \mid m$.

If $\pi = \dfrac{m + \sqrt{m^2 - 4q}}{2}$, π cannot be Frob on ell. curve.

In fact: In that case the "r" attached to π is odd ≥ 5.

[In particular, a curve of genus 2, 3, 4 over $\mathbb{F}_q$ cannot have $q+1 \pm gm$ points.

For that we need $\pi_1, \bar{\pi}_1, \dots \pi_g, \bar{\pi}_g$

with $\begin{cases} \pi_1 + \bar{\pi}_1 = -m \\ \vdots \\ \pi_g + \bar{\pi}_g = -m \end{cases}$ $\Longrightarrow$ $(\pi, \bar{\pi})$ repeated g times.

But Claim $\Rightarrow$ repeated at least $r \geq 5$ times.

$\therefore g \geq 5$. ///

Proof: Set $q = p^{2f+1}$, $f \geq 1$ (in fact $f \geq 2$).

Claim: p^{f+1} does not divide m

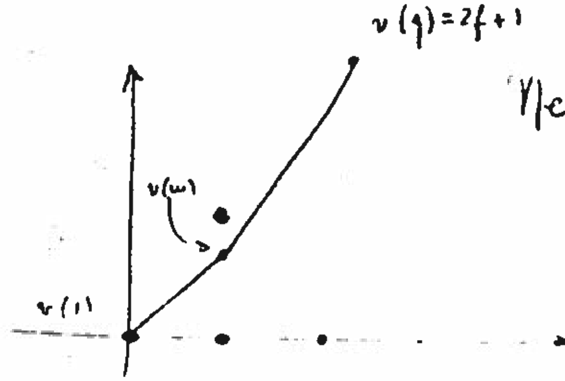
In fact $4q = m^2 + k$ $\qquad 1 \leq k \leq 2m$

$p^{f+1} \mid m \Rightarrow p^{2f+1} \mid 4q$ and $\mid m^2 \Rightarrow p^{2f+1} \mid k$

So $p^{f+\frac{1}{2}} \le 4 \underset{(f \ge 2)}{\Longrightarrow} p^{5/2} \le 4 \Rightarrow p^5 \le 16 \; \lightning$

Hence $v_p(m) \le f$.

π satisfies $\pi^2 - m\pi + q = 0$



Newton polygon

I've proved $v(m)$ is below the line.

Hence p splits in $\mathbb{Q}(\pi)$ and the val of π at the primes dividing p, are the slopes: $v(m)$, $2f+1-v(m)$.

i_v of Tate's theorem

At $\{\infty, \ell\} \longrightarrow 0$

At v_1 : $i_{v_1} = \dfrac{v(m)}{2f+1} = \alpha$ Know: $0 < \alpha < \frac{1}{2}$

At v_2 : $i_{v_2} = \dfrac{2f+1-v(m)}{2f+1}$

Denominator?

$r = \dfrac{2f+1}{\gcd(2f+1, v(m))}$ so r is odd, ≥ 3

So we need to show $r \neq 3$ $(\therefore r \geq 5)$.

<u>Assume $r = 3$</u>, so $\alpha = \frac{1}{3}$, $v(m) = \frac{1}{3}(2f+1)$ so $f = 1 + 3F$

So $q = p^{6F+3}$, $m = p^{2F+1} \cdot M$, $p \nmid M$

Write $4q = m^2 + k$ $\quad 1 \leq k \leq 2m \leq 4q^{1/2}$

So $4p^{6F+3} = p^{4F+2} M^2 + k$

So $p^{4F+2} \mid k \implies p^{4F+2} \leq 4p^{3F+3/2}$

$\implies p^{F+\frac{1}{2}} \leq 4$

$$\implies \begin{cases} p \leq 16 & \text{if } F = 0 \\ p^3 \leq 16 & \text{if } F = 1 \implies p = 2 \end{cases}$$

And check the possible cases. $\boxtimes$

For realizing the Weil bound, need $\pi = \dfrac{-m \pm \sqrt{m^2 - 4q}}{2}$, $p \nmid m$.
So have ell. curve E_π.

Want C s.t. $\text{Jac} \sim E_\pi \times \cdots \times E_\pi$

To go down by 2, find E' w/ $\text{Tr} = -(m-2)$, and look for $\text{Jac} \sim E_\pi \times \cdots \times E_\pi \times E'$.

Problem

FIND: Curves with Jacobian $\left\{ \begin{matrix} \text{isogenous} \\ \text{or} \\ \text{isomorphic} \end{matrix} \right\}$ to a product of ell. curves

"Reduction of abelian integrals to elliptic integrals"
diff^n forms

$$C \xrightarrow{1} \mathrm{Jac} \xrightarrow{\sim} E_1 \times \cdots \times E_g$$

find a basis of diff'l forms of first kind on C by taking $C \to E_i$ and pulling back the diff. first kind on E_i.

~ 1830, Legendre + Jacobi

α, β numbers

Take C genus 2 ramif. at $0, 1, \alpha, \beta, \alpha\beta, \infty$, so assume
$\alpha \neq 0, 1$
$\beta \neq 0, 1, \alpha, \alpha^{-1}$
i.e., all distinct.

Consider $y^2 = x(x-1)(x-\alpha)(x-\beta)(x-\alpha\beta)$

Basis of dfk : $\left\{ \dfrac{dx}{y}, \ \dfrac{x\,dx}{y} \right\}$

Define $\omega_1 = \dfrac{x + \sqrt{\alpha\beta}}{y}\, dx$

$\omega_2 = \dfrac{x - \sqrt{\alpha\beta}}{y}\, dx$

Change variables $(x,y) \longrightarrow (X, Y_1)$

$$X = x + \frac{\alpha\beta}{x}$$

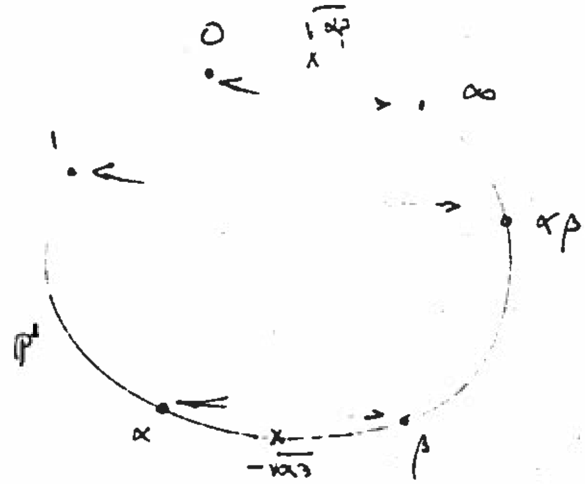
$$Y_1 = y\,\frac{x - \sqrt{\alpha\beta}}{x^2}$$

$$Y_1^{\,2} = (X - 2\sqrt{\alpha\beta})(X - (\alpha+\beta))(X - (1+\alpha\beta))$$

and pullback of $\frac{dX}{Y_1}$ is ω_1 : $\omega_1 = \frac{dX}{Y_1}$

Same for Y_2 w/ change of sign, $\omega_2 = \frac{dX}{Y_2}$.

Geometrically

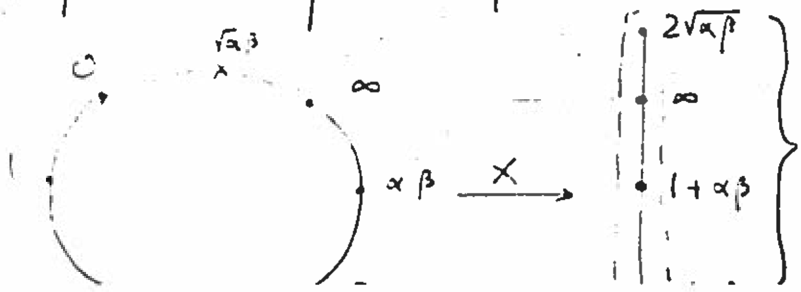


$$x \overset{\sigma}{\longmapsto} \frac{\alpha\beta}{x}$$

involution

fixed points: $x = \frac{\alpha\beta}{x} \Longrightarrow x = \sqrt{\alpha\beta}$, $x = -\sqrt{\alpha\beta}$

mod out by σ : X = quotient by $\sigma = x + \sigma(x)$



make the ell. curve ramified here

$$\begin{tikzcd} C \arrow[rr, dashed, "\text{check ramification}"] \arrow[d, "y"'] & & E_1 \arrow[d, "Y_1"] \\ x\text{ line} \arrow[rr] & & X\text{-line} \end{tikzcd}$$

Y_1 ramif at those four pts

And the map $C \longrightarrow E_1$ is as given above.

Or:

$$\begin{tikzcd} & C \arrow[dl] \arrow[d] \arrow[dr] & \\ E_1 \arrow[dr, "2"'] & \mathbb{P}_{1,x} \arrow[d, "2"] & E_2 \arrow[dl, "2"] \\ & \mathbb{P}_{1,X} & \end{tikzcd}$$

Program: "glue" elliptic curves to get C of genus 2

10/22: <u>Last time</u>: reduction of abelian integrals to elliptic ones.

<u>Legendre-Jacobi</u>: $g = 2$, example

<u>Kuhn</u>: information on general question: curves of genus g with Jacobian isogenous (or even isomorphic) to a product of elliptic curves.

Thesis

Does that exist for any g?

an infinite seq. of g's? | char $\neq$

(in char p, $x^{p^a+1} + y^{p^a+1} + z^{p^a+1} = 0$ has jac. which splits into s.s. elliptic curves).

Say, $g = 4$. Is it "likely" to get such curves?

$g = 4 \longrightarrow$ 4 parameters (to split into ell. curve
1 eqn $\to$ OK

$g = 10 \longrightarrow$ 10 parameters
$\frac{10.11}{2} - 21 \gg 0$ rather surprisi[ng] that examples exist.

<u>Example</u>: $g = 7$, $X_0(60)$; let $J_0(60) = \mathrm{Jac}\, X_0(60)$

$J_0(15) \overset{\longrightarrow}{\underset{\longrightarrow}{\longrightarrow}} J_0(60)$ (maps are $z \to z$, $z \to 2z$, $z \to 4z$)
ell. curve over $\mathbb{Q}$

since $60 = 4 \times 15$

$J_0(20) \longrightarrow J_0(60)$

finally $\underset{\text{ell. curve}}{J_0(30)^{new}} \Longrightarrow J_0(60)$

$J_0(60) \sim$ product $J_0(15)^3 \times J_0(20)^2 \times J_0(3$

Antwerp: $\begin{cases} X_0(180); \ g = 25, \text{ splits} \\ X_0(198), \ g = 29, \text{ splits} \\ X_0(288), \ g = 33, \text{ splits} \\ X_0(300), \ g = 43, \text{ splits} \end{cases}$

Kuhn gets infinitely many examples w/ $g = 37$.

$J_0(300)$ includes 2 copies of $J_0(150)^{new}$, which splits into three elliptic curves. So have some "accidental" splitting.

Question: why so often?

Theorem for $g = 2$: (Computes $N_q(2)$) Set $m = [2q^{1/2}]$

(a) If q is a square, then:

- if $q \neq 4, 9$, then $N = 1 + q + 4q^{1/2} = 1 + q + 2m$
- if $q = 4$, $N = 10$ (Weil: 13) (down by 3)

(6) If q is not a square, define q to be special if either $p|m$ or q is represented by one of the quadratic polynomials x^2+1, x^2+x+1, x^2+x+2. Then:

- if q is not special, $N = 1+q+2m$ (Weil)
- if q is special, $N = \begin{cases} q+2m & \text{if } \{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2} = 0.618.. \\ q+2m-1 & \text{if not.} \end{cases}$

Remark on the special q's: $q = p^{2e+1}$, $e \geq 0$

If $e=0$, i.e., $q=p$, then p is special iff representable by x^2+1, x^2+x+1.

[$p|m$ only for $p=2,3$, and they are repres. by polyn.] [x^2+x+2 is even, so only for $2 = 1^2+1$.]

If $e \geq 1$, then $p|m$ should occur for infinitely many e (question is zeros in p-expansion of $2\sqrt{q}$), for a given p.

Both $\{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2}$ and $< \frac{\sqrt{5}-1}{2}$ should occur infinitely often

Write:

$2\sqrt{p} = x.a_1 a_2 \ldots 1 0 1 1 \longrightarrow$ $\{2\sqrt{q}\}$

exceptional q

should be < slightly more often than >. (0.6-

LIST OF $q = p^{2e+1}$ $e \geq 1$ $q \leq 10^9$ s.t. $p | m$

There are only 14 :
$$\left\{\begin{array}{l} 2^{7,11,15,17,19,21,23,27,29} \\ 3^{7,15} \\ 5^{9,11} \\ 7^{5} \end{array}\right. \qquad \leq 10^9$$

These are special by the first condition. What about second one ?

<u>Thm</u> (Lebesgue, Nagell, Ljunggren)

If $q = p^{2e+1}$, $e \geq 1$ is representable by x^2+1, x^2+x+1 or x^2+x+2, then

$$q = 2^3, 2^5, 2^{13} \quad (\text{rep. by } x^2+x+2)$$
$$q = 7^3 \quad (\text{rep. by } x^2+x+1)$$

$$\left\{\begin{array}{l} 2^3 = 2^2+2+2 \\ 2^5 = 5^2+5+2 \\ 2^{13} = 90^2+90+2 \\ \\ 7^3 = 18^2+18+1 \end{array}\right.$$

> The Theorem is about
> $y^n = x^2+1$ $(x^2+x+1, x^2+x+$
> E.g. $y^n = x^2+1$, $n \geq 2$, $x, y \in \mathbb{Z}$, $x \neq 0$
> has no solutions.

2^3 : $\{2\sqrt{8}\} = \{4\sqrt{2}\} = 0.65\ldots > \frac{\sqrt{5}-1}{2}$ so $q=8 \to$ down by 1

$2^5, 2^{13}, 7^3$ $\longrightarrow$ down by 2

$\{2\sqrt{7^3}\} = 0.01\ldots$ $\quad 4.\underline{7}^3 = 37^2+3$

Recall

$$\sqrt{2} = \underbrace{1.0110101}\underbrace{000001\ldots}_{\text{small}}$$

$$2\sqrt{2^{13}} = 181.\text{small}$$

Ideas for proof:

1) elementary construction of curves of genus 2 starting from ell. curves (Legendre)
2) using hermitian forms will give curves.

(In both of these, Jac $\sim E_1 \times E_2$)

1–3 gives existence proofs

3) Case "$\mathbb{Q}\sqrt{5}$" : using a thm. of Shimura.
4) Non-existence proofs $\longrightarrow$ hermitian forms.

In the genus 1 case, our proof wasn't effective in the following sense:

we proved max of pts $= \begin{cases} 1+q+m \\ \text{or} \\ q+m \end{cases}$.

But not how to construct the corresp. ell. curve.

Only idea: Take all ell. curves (about $2q$ of them), compute number of pts on each. Stop when get the desired no. of pts.

This takes $q^2(\log q)^\alpha$ steps by the stupidest method.

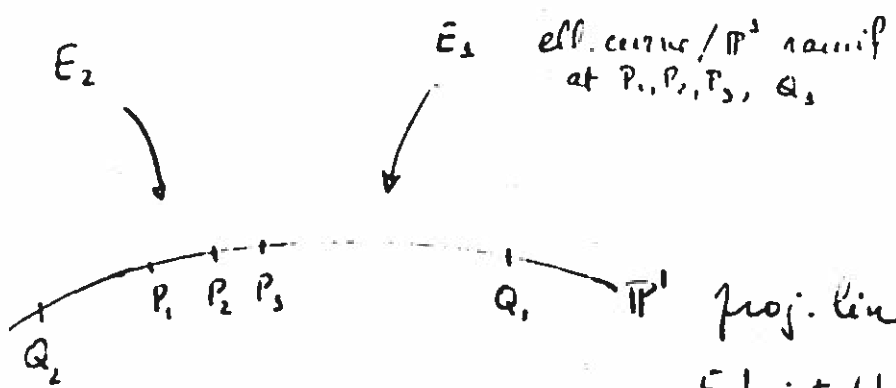
Schoof: one can compute # of pts in $(\log q)^\alpha$ steps

Can compute $E_{p-1}(c_4, c_6) \equiv a_p \pmod{p}$

So have to solve it in c_4, c_6. But can use it to count # of pts. No great gain.

Our construction in 1) is effective <u>if we know the eqn. for $g=1$</u>.

<u>Legendre construction</u> <u>char $\neq 2$</u>.



proj. line

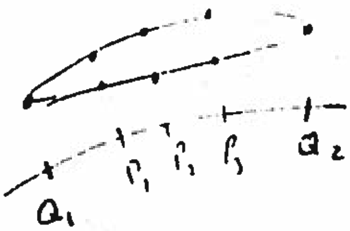
5 points (distinct) P_1, P_2, P_3, Q_1, Q_2

In terms of fields:

$$\begin{tikzcd} & K_{12} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\ K_2 \arrow[dr, dash, "2"'] & K_0 \arrow[d, dash, "2"] & K_1 \arrow[dl, dash, "2"] \\ & K & \end{tikzcd}$$

$K = K(\mathbb{P}^1)$

$K_0 \longleftrightarrow E_0$ ramif. only at Q_1, Q_2 $\therefore$ genus zero



$$g(K_0) = 0$$

P_i split into P_i', P_i''

$g(K_{12}) = 2$ ram. at the pts $P_1', P_1'', P_2'', P_2', P_3', P_3''$

$X_{12} = X \longleftrightarrow K_{12}$ Have a group of type $(2,2)$ acting on X

Exercise: In general, L/K, $g(K) = 0$, $Gal(L/K)$ of type $(2,2,\dots,2)$. Then

$$g(L) = \sum_{\substack{K' \subset L \\ [K':K]=2}} g(K') .$$

$$= \sum_{\substack{\chi \text{ char. of} \\ Gal(L/K)}} g(K^\chi)$$

Thm: $Jac(X) \underset{(\text{isog.})}{\sim} E_1 \times E_2$

Have
$$\begin{tikzcd} & X_{12} \arrow[dl] \arrow[dr] & \\ E_1 \arrow[dr] & & E_2 \arrow[dl] \\ & \mathbb{P}_1 & \end{tikzcd}$$
; these give a map $Jac(X) \to E_1 \times E_2$; use the group action to get the splitting.

In fact, kernel has type $(2,2)$.

We apply this over $\mathbb{F}_q$, char $\neq 2$:

E_1, E_2 given ell. curves.

" One can glue them " $\Longleftrightarrow$ $\exists X$ of genus 2 (over $\mathbb{F}_q$) s.t.

$$\mathrm{Jac}\, X \underset{\substack{\text{isog}\\ \text{over } \mathbb{F}_q}}{\sim} E_1 \times E_2$$

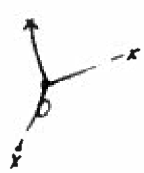
$\underset{\text{Tate-Honda}}{\Longleftrightarrow}$ eigenv. of Frob. on X = {those on E_1} $\cup$ {those of E_2}

$$\Rightarrow \text{Then} \quad N(X) = 1 + q - \underbrace{(\pi_1 + \bar{\pi}_1)}_{\text{eigenv. for } E_1} - \underbrace{(\pi_2 + \bar{\pi}_2)}_{\text{for } E_2}$$

so $$\boxed{N(X) = N(E_1) + N(E_2) - q - 1.}$$

Criterion for "gluing"

Let $(E_1)_2$ be the group of 2-div. pts of E_1 (of type $(2,2)$)



Frob acts on the three non-zero pts: perm. of order 1, 2, or 3.

[Ord]: Assume: that order is the same for E_1 and E_2.

($y^2 = f_1(x)$; three pts $\longleftrightarrow$ zeros of $f_1(x)$

and order 1, 2, 3 corresp to)

1 $\updownarrow$ all three

2 $\to$ one rat'l,

3 $\to$ zero pts rat'l.

<u>Thus</u> (char $\neq 2$) Under this assumption, one can glue E_1 to E_2, except maybe if:

$$\begin{cases} \text{order of Frob} = 1,\ p=3, & j(E_1)=j(E_2)=0 \\ \text{order of Frob} = 2,\ \text{any } p, & j(E_1)=j(E_2)=1728 \\ \text{———————} = 3,\ \text{any } p, & j(E_1)=j(E_2)=0 \end{cases}.$$

(So if $\mathrm{Aut}\,E_1 = \mathrm{Aut}\,E_2 = \{\pm 1\}$, then assumption $\Rightarrow$ one can glue E_1 & E_2).

<u>Example of non-gluing</u>

$$\left[\begin{array}{l} q = 9, \quad E_1 \text{ s. sing.}, \quad \pi = +3 \\ E_2 = E_1 \end{array} \right.$$

$3x = x$ since $2x = 0$ so [Ord] is true

If X exists, then $N(X) = N(E_1) + N(E_2) - q - 1$

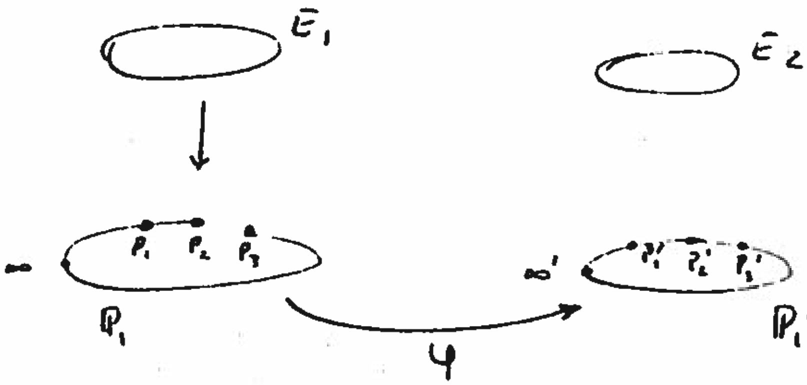
$$= \underbrace{9+1-6} + \underbrace{9+1-6} - 9 - 1 = -2$$

(If $\pi = -3$, $N(E_1) = 16$, so $N(X) = 22$ but X is a two-sheeted cover of $\mathbb{F}_9$ which has 10 pts, so $N(X) \leq 20$ ↯.)

<u>Proof</u>: Write E_1 as quad. covering of $\mathbb{P}^1$ ramif. at ∞ and at P_1, P_2, P_3 (corresp to the 2-div. pts!)

= order of Frob So n acts on P_1, P_2, P_3.

Write E_2 as quad extn of some other $\mathbb{P}_1'$ ramif at ∞' and $P_1' / P_2', P_3'$



Want: $\varphi : \mathbb{P}_1 \longrightarrow \mathbb{P}_1'$ s.t.
$$\begin{cases} \varphi\infty = \infty' \\ \varphi\{P_1, P_2, P_3\} = \{P_1', P_2', P_3'\} \\ \varphi \circ \mathrm{Frob} = \mathrm{Frob} \circ \varphi \end{cases}$$

<u>Claim</u>: φ exists (unless we are in the 3 exceptional cases).

Choose an <u>isom</u> of the set $\{P_1, P_2, P_3\}$, viewed as a set w/ Galois action, onto $\{P_1', P_2', P_3'\}$.

1) If order of Frob $= 1$, trivial action, 6 possible φ (up to an elem. of S_3)

2) If order of Frob $= 2$ $\quad \{\times\times \;\; \bullet\} \quad \{\times\times \;\; \bullet\}$

two possible φ (φ_1 and $\pi \circ \varphi_1$)

3) If order of Frob $= 3$, have cyclic order on Pts

three possible φ (φ, $\pi\varphi$, $\pi^2\varphi$).

Solving this finds a φ satisfying 2^{nd} & 3^{rd} cond.; remains to check if $\varphi\infty \neq \infty'$.

In case 1), we lose (no φ works) only if the six perm. of P_1, P_2, P_3 fix ∞, and this $\Rightarrow$ same j and $\Rightarrow$ $j = 0$, char $= 3$ (because a large gp of autom.!)

In case 2), we lose only if ∞ is fixed by $(P_1\, P_2\, P_3) \to (P_1\, P_3\, P_2)$ that lifts to an autom of E, of order 4, so $j = 1728$.

Similarly in case 3). $\boxtimes$

10/29 $\boxed{q=2}$, cont.

We are trying to compute $N_q(2)$.

We stated:

$$N_q(2) = \begin{cases} q+1+2m & \text{nonspecial} \\ q+2m & \\ q+2m-1 & \end{cases}\Bigg\} \text{special}$$

$m = [2q^{1/2}]$

in one case ($q=4$), 3 less: ~~q+1+2m~~ $q+2m-2$

q square : special $\Leftrightarrow q = 4$ or 9

q nonsquare : special $\Longleftrightarrow p \mid m$ or $q = x^2+1, x^2+x+1, x^2+x+2$

<u>Elementary glueing</u>

E, E' over $\mathbb{F}_q$

"can glue them" $\Longleftrightarrow$ there is a curve C of genus 2 over $\mathbb{F}_q$, $\mathrm{Jac}(C) \sim E \times E'$

$\xleftrightarrow{\text{Tate-Honda}}$ eigenv. of Frob. for C =
= (eigen. for E) $\cup$ (eigenv. for E')

We gave a construction which will give a glueing in many cases.

Let q be a square : $q = p^{2e}$

ⓐ Suppose, first, $p \neq 2, 3$.

Choose a supersingular curve E over $\mathbb{F}_{p^2}$ with Frob $= p$. (Known: such exist).

To be proved: one can glue E to E over $\mathbb{F}_{p^2}$, hence over $\mathbb{F}_q$!

Assume that; then we get C of genus 2, w/ eigenv. of Frob over $\mathbb{F}_q$ all equal to p^e.
So $N = 1 + q - 4p^e$.!

Making a quad. twist changes it to a curve with maximum no. of points, $N = 1 + q + 4p^e$.

(alternatively start w/ s.s. $E/\mathbb{F}_q$ with Frob $= -q^{1/2}$).

To prove glueing: look at the 2-division pts and action of Frob. on these pts.

Here Frob $= 1$ (identity) on 2-division pts, since Frob $(x) = \pm q^{1/2} x = x$ iff $2x = 0$! $\overset{(q \text{ odd})}{\Longrightarrow}$ no trouble (except if $p = 3$, $j = 0$, which is not the case).

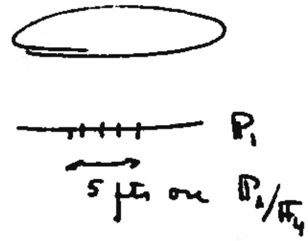
ⓑ $q = 4$ or 9

$q = 4$, Weil $= 1 + q + 2m = 1 + 4 + 24 = 13$

and covering argument $\to N \leq 2(q+1) = 10$

10 is the exact bound: eqn is $y^2 + y = \dfrac{x}{x^3 + x + 1}$ over $\mathbb{F}_4$.

This gives covering



3 simple poles $\Rightarrow$
$\Rightarrow g = 2$.

So to prove: every pt splits completely

So : $\quad x = 0, 1, \infty \qquad (\in \mathbb{F}_2)$

$\qquad x = \rho, \rho^2 \qquad (\rho^3 = 1, \rho \neq 1)$

$$\begin{cases} x = 0 \longrightarrow \text{RHS} = 0 \\ x = 1 \longrightarrow \text{RHS} = 1 \\ x = \infty \longrightarrow \quad = 0 \\ x = \rho \longrightarrow \quad = 1 \\ x = \rho^2 \longrightarrow \quad = 1 \end{cases}$$

LHS is a trace so splits completely $\Leftrightarrow$ RHS is 0 or 1.

Over $\mathbb{F}_2$, $N_1 = 4$, $N_2 = 10$ $\qquad$ write $a_1 = \pi_1 + \bar{\pi}_1$
$a_2 = \pi_2 + \bar{\pi}_2$

then
$$\begin{cases} 1 + 2 - a_1 - a_2 = 4 \\ 1 + 4 - (a_1^2 - 4) - (a_2^2 - 4) = 10 \end{cases}$$

$\pi \longrightarrow \pi^2 \quad a_1 \longrightarrow a_1^2 - 2\pi_1\bar{\pi}_1$
$= a_1^2 - 4$

So
$$\begin{cases} a_1 + a_2 = -1 \\ a_1^2 + a_2^2 = 3 \end{cases}$$

So $a_1 = \dfrac{-1 \pm \sqrt{5}}{2}$, $a_2 = \dfrac{-1-\sqrt{5}}{2}$ — ab. var. of dim 2, irred. (comes from $\mathbb{Q}(\sqrt{5})$).

For $\mathbb{F}_9$: $N \le 20$

eqn: $y^2 = (x^3 - x)^2 - 1 = (x^3-x+1)(x^3-x-1)$

Clearly $g=2$, to show: can be solved in $\mathbb{F}_9$ for every value of x.

$x = \infty$ — OK (look at coeff.)

$x \in \mathbb{F}_3$, $x^3 - x = 0 \longrightarrow y^2 = -1$ (but -1 is a square in $\mathbb{F}_9$)

$x \in \mathbb{F}_9 - \mathbb{F}_3$, $x^3 - x$ is antisymm. under $x \mapsto x^3$ so $(x^3-x)^2$ is symm., hence $\in \mathbb{F}_3^\times$, in fact $= -1$, so works.

$$y^2 = (x^3-x)^2 - 1$$
$$= x^6 + x^4 + x^2 - 1$$

and map to $y^2 = x^3 + x^2 + x - 1$

so Jac V is isog to product $E_1 \times E_2$.

ⓒ $q = 2^{2e}$, $e \geq 2$

To construct: curve with Weil bound

[ⓓ For $q = 3^{2e}$, $e \geq 2$ $\longrightarrow$ assigned to Bob Kuhn !?]

Start w/ $y^2 + y = x^3$ $/\mathbb{F}_2$, s.s.

This has 3 points, so $\pi = \sqrt{-2}$, since $1 + 2 - (\pi + \bar{\pi}) = 3$

<u>Over</u> $\mathbb{F}_4$, $\pi = -2$, Frob $= -2$.

Over $\mathbb{F}_q$, $q = 4^e$, Frob $= (-2)^e$

<u>To be proved</u>: E can be glued to itself over $\mathbb{F}_{4^e}$, $e \geq 2$.

Consider

$$\begin{tikzcd} \mathbb{F}_q(x,y) \arrow[d, dash, "2"'] & \mathbb{F}_q(x,y') \\ \mathbb{F}_q(x) \arrow[ur, dash, "2"'] & \end{tikzcd}$$

Where $(y')^2 + y' = (x+c)^3$, $c \in \mathbb{F}_q - \mathbb{F}_4$.

(Clearly isom. over $\overline{\mathbb{F}_q}$)

Want to make composition:

$$\begin{tikzcd} & \cdot \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \text{genus } 1 \ \mathbb{F}_q(x,y) \arrow[dr, dash] & \mathbb{F}_q(x,z) \arrow[d, dash] & \mathbb{F}_q(x,y') \ \text{genus } 1 \arrow[dl, dash] \\ & \mathbb{F}_q(x) & \end{tikzcd}$$

<u>Want</u>: genus 0

And don't want constant field extn.

Middle field is $\mathbb{F}_q(x,z)$, $z = y + y'$ (Artin-Schreier extn).

$$z^2 + z = x^3 + x^3 + cx^2 + c^2x + c^3$$
$$= \underbrace{(c^{1/2}x)^2 + c^{1/2}x} + (c^2 + c^{1/2})x + c^3$$

$t = z + c^{1/2}x$

$$t^2 + t = (c^2 + c^{1/2})x + c^3$$

Artin-Schreier, pole of order 1 (odd) at ∞

$c^2 + c^{1/2} \neq 0$, because $c^4 \neq c$ (since $c \notin \mathbb{F}_4$).

This is a conic, hence genus zero.

So composite has genus 2, and Jac $\sim$ product $E \times E$

This gives the desired construction. $\boxtimes$

(d) For $q = 3^{2e}$, $e \geq 2$

We use a different method.

Intermezzo: On polarizations

A abelian variety.

(Mumford): a polarization is a homomorphism $\varphi : A \longrightarrow A^*$
(A^* = dual of A) such that:

If D is a divisor of A and if $a \in A$, let D_a = translate of D by a, i.e., let $\tau_a : x \longmapsto x + a$, $D_a = \tau_a(D)$.

Then $D_a - D$ represents a point in $A^* = \mathrm{Pic}^\circ(A)$.

This map $a \longmapsto D_a - D \in A^*$ is a homomorphism $\varphi_D : A \longrightarrow A^*$.

Then a *polarization* is $\varphi : A \longrightarrow A^*$ s.t. there exists (over some extn of $\mathbb{F}_q$) an *ample* divisor D s.t. $\varphi_D = \varphi$.
This defines Class$(D) \in NS(A)$ uniquely.
(φ is an isogeny, hence has a degree / deg φ.)

$$\deg_{pol}(\varphi) = \sqrt{\deg \varphi} = \frac{D^g}{g!} = \chi(A, \mathcal{L}(D)) = \dim H^0(A, \mathcal{L}(D))$$

(cf. Mumford, Ab. Varieties)

$$D^g = \underbrace{D \cdot D \cdot \ldots \cdot D}_{\text{intersection multiplicity}}$$

Criterion: $\varphi : A \longrightarrow A^*$ comes from an element (ample or not) of $NS(A) \Longleftrightarrow \varphi^* = \varphi$

[$\varphi^* : A^{**} = A \longrightarrow A^*$, so this makes sense] $\leftarrow$ cf. Mumford.

Example: Let E be an elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

Consider $A = E \times \cdots \times E$ n times.

$$A^* = E^* \times \text{—} \times E^* = E \times \text{—} \times E$$

$$\varphi : E \times \text{—} \times E \longrightarrow E \times \text{—} \times E \qquad \mathrm{End}(E) = \mathbb{Z}$$

So $\varphi = \begin{pmatrix} a_{11} & a_{1n} \\ \cdot & \\ a_{n1} & a_{nn} \end{pmatrix}$ $\quad a_{ij} \in \mathbb{Z}$.

$\varphi = \varphi_0$, $D \in NS(A) \Longleftrightarrow \varphi = \varphi^*$.

So comes from $NS(A) \longleftrightarrow \varphi = {}^t\varphi$

φ polarization $\Longleftrightarrow \varphi = {}^t\varphi$ (φ symm) and φ is the matrix of a pos. definite quad. form.

E.g., use the E_8 quad form, to put an interesting polarization of deg 1 on $E \times \underset{8}{\underline{\quad}} \times E$.

Loojenga, Inventiones ~1974/75 (careful: don't believe the statements).

---

polarization of degree 1 = principal polarization.

If C is a curve of genus g, its jacobian J has a natural polarization of degree 1 whose D is "Θ".

Have a map $C \longrightarrow J$, then define

$$\Theta = \underbrace{C + \cdots + C}_{g-1 \text{ times}} \underset{\text{birat'l}}{\simeq} C^{(g-1)}$$

So this gives $\varphi : J \xrightarrow{\sim} J^*$.

principal $\Rightarrow \deg_{\text{pol}} \varphi = 1 \Rightarrow \dim H^0(A, \underline{\mathcal{L}}(D)) = 1 \Longrightarrow$ the divisor class (for lin. equiv.) contains a unique positive divisor

So up to translation, can speak of the divisor of φ.

<u>Theorem</u>: Let A be an ab. variety of dim 2 with principal polarization and let C be its theta divisor. Then <u>either</u> C is nonsingular irred of genus 2 and
$A = Jac(C)$

<u>or</u> C is $E_1 \cup E_2$ intersecting at 1 pt and
$A = E_1 \times E_2$ (as polarized variety).

If everything is over k and k perfect, then, in the indecomposable case everything is over k; in the decomposable case the ell. curves might be permuted by $Gal(k'/k)$ for some quad. extn. k'/k, and then A will be indec. over k and dec. over k'.

[A similar theorem is true in dim 3, but that is harder]

<u>Proof</u>: principal polarization $\Longrightarrow$ $C \cdot C = C^2 = 2$

$$\left(\deg \varphi = \frac{C^g}{g!} \text{ and } g = 2\right)$$

Write $C = \sum m_i C_i$, C_i irreducible.

So $\sum m_i m_j C_i \cdot C_j = 2$

(on ab. variety, $C_i \cdot C_j \geq 0$ and even > 0 except when $C_i = C_j =$ ell. curve
$\to$ use translation on A $\to$ find argument).

So either we have $2 = 2$

or

$2 = 1 + 1$

so either $\left\{ \begin{array}{l} C \text{ is irred} \\ \text{or} \quad C = E_1 + E_2 \quad \text{2 ell. curves w/ } E_1 \cdot E_2 = 1 \end{array} \right.$

$$C^2 = \underbrace{E_1^2 + E_2^2}_{=0} + 2E_1E_2$$

If C irred, need still prove nonsing of genus 2.
Cannot be genus 0 or 1. Let g_a = arith. genus of C =
$= \dim H^1(C, \mathcal{O}_C)$.

Then $g_a = g + \sum$ local contrib. at sing. pts.

<u>Adjunction formula</u> : $\boxed{2g_a - 2 = C \cdot C + C \cdot K}$

K = can. divisor

Here ab. variety so $K = 0$, and $C \cdot C = 2$,
hence $2g_a = 4$ so $\boxed{g_a = 2}$.

Since $g = 0$ is impossible (can't embed in ab. var.)
If $g = 1$, map is homom., so can't be.
So <u>$g = 2$ and nonsingular</u>.

(Proof of exercise : <u>adj. formula</u> $\Rightarrow$ $C \cdot C \geq 0$ and $C \cdot C = 0$ only if $g_a = 1$.)

Dictionary for $g=2$ Over a perfect field k

Abelian varieties$/k$ w/ principal polariz. which are indecomposable over any quad. extn of k $\Longleftrightarrow$ curves of genus 2 $/k$ (up to isom.)

Statement of Torelli's theorem in general (over a perfect field k)

Assume $g \geq 2$.

Let C and C' be curves of genus g over k, J, J' their jacobians as polarized abelian varieties.

(*) If J and J' are isomorphic$/k$ then C and C' are isom.$/k$.

More precisely:

i) if C is hyperelliptic and $F: J \longrightarrow J'$ is an isom. of polarized ab. varieties, then $\exists! f : C \xrightarrow{\cong} C'$ giving F by functoriality.
In particular, $\mathrm{Aut}(C) \xrightarrow{\sim} \mathrm{Aut}(J, \text{pol.})$

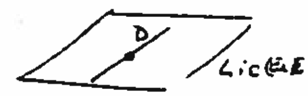
ii) if C is not hyperelliptic, for every $F: J \xrightarrow{\cong} J'$, there exists a unique isom. $f: C \xrightarrow{\cong} C'$ and a unique $\varepsilon \in \{\pm 1\}$ s.t. f gives εF by functoriality.

In particular. $\mathrm{Aut}(C) \times \{\pm 1\} = \mathrm{Aut}(J, \text{pol})$

Fine de l'Intermezzo

Back to $\mathbb{F}_{q^e}$, $e \geq 2$

Take E w/ Frob $= -q^{1/2}$

Will consider $E \times E \xrightarrow[\text{insep. isogeny}]{} J \longleftrightarrow$ classified by 

J = same pts, but only fcts whose deriv. along the given line $= 0$

will choose D <u>not</u> rat'l over $\mathbb{F}_{p^2}$

Put a polarization on $E \times E$ by $\begin{pmatrix} p & \alpha \\ \bar{\alpha} & p \end{pmatrix}$, $\alpha\bar{\alpha} = p(p-1)$,

<u>Prove</u>: this descends to J & becomes principal there, and J is indec., which gives a curve!

<u>Moret-Bailly</u> $\rightarrow$ this kind of construction w/ varying D. Find

$$\begin{array}{c} J \\ \big\downarrow \text{ab. scheme} \\ \mathbb{P}_1 \end{array}$$

corresp to a surface $\begin{array}{c} S \\ \big\downarrow \\ \mathbb{P}_1 \end{array}$

s.t. generic fiber is curve of genus 2

$5p-5$ exceptional fibers  ell curves

For $p=2$, $5p-5 = 5 \rightarrow$ rat'l pts $/ \mathbb{F}_4$
$p=3$, $5p-5 = 10 \rightarrow$ ——— $/ \mathbb{F}_9$
$p \geq 5$ pts left over!

So this picks out the exceptional pts.

11/V ($g=2$ cont.)

q square $\Longrightarrow$ Weil bound is attained except for $q = 4, 9$

We have proved this except:
Missing case : $q = 9^e$, $e \geq 2$.

Start with E ell. curve, supersingular, over $\mathbb{F}_{p^2}$, s.t. Frob on $E = p$.

For such E: Well-known : $\mathrm{End}(E)$ is a max'l order in the quaternion algebra $H_{p,\infty}$
(and this max'l order can be imposed on E).

Choose E such that $\mathrm{End}\,E \ni \alpha$ with $\alpha\bar{\alpha} = p(p-1)$

This is possible: Consider $\mathbb{Q}(\sqrt{-p(p-1)})$; this is imag. quad., ramif. at p, so splits $H_{p,\infty}$.
So $\alpha = \sqrt{-p(p-1)}$ is an integer of this field, and can be included in $H_{p,\infty}$.
So choose a max'l order containing the image of α.

Now let $A = E \times E$

polarization : $\varphi : A \longrightarrow A^* = E \times E$

$$\varphi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad a, b, c, d \in \mathrm{End}(E)$$

φ is a polarization $\Longleftrightarrow$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ hermitian $\gg 0$

("between the lines" in Mumford, Ab. Vars., toward the end.)

[Mumford starts w/ $E \times E$, say, w/ a given polarization, say the obvious one.
Identify $\varphi : A \longrightarrow A^*$ as End, and asks which φ are polarizations.
So says, take End $\otimes \mathbb{R}$, and then φ polar. corresp to positive definite symmetric matrices.

φ is of degree 1 $\Longleftrightarrow$ "det" $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$

(Note : hermitian $\Rightarrow$ $a, d \in \mathbb{Z}$
$b = \bar{c}$ so we have only
$ad - b\bar{b} = 1$).

Choose $\varphi = \begin{pmatrix} p & \alpha \\ \bar{\alpha} & p \end{pmatrix}$

$$\det \varphi = p^2 - \alpha\bar{\alpha} = p^2 - p(p-1) = p .$$

We find : Ker φ has order p^2 (say, look at ℓ-adic representations.)

tgt space at E is 1-dim'l, so $\operatorname{End} E \longrightarrow \mathbb{F}_{p^2}$ (action on tgt space)

residue field at p.

$\alpha \longrightarrow 0$ $\quad$ ($\alpha\bar{\alpha} = p(p-1) \longrightarrow 0$!)

$p \longrightarrow 0$

So φ is 0 on the tgt space of A.

A ab variety in char p., dim. g, there is a subgroup of A t_A: "kernel of Fr"; this is one point with nilpotents. If $x_1, \dots, x_g$ are local coords around 0 and k is the ground field, the group

t_A is def. by $x_i^p = 0$

the order of t_A (as gp scheme) is p^g, $g = \dim A$.

(the algebra is $k[x_1, \dots, x_g]/(x_i^p)$).

So counting orders gives $\operatorname{Ker} \varphi = t_A$ in our case.

Take $\mathbb{F}_q \supsetneq \mathbb{F}_{p^2}$, so $q = p^{2e}$, $e \geq 2$, and now view E and A over $\mathbb{F}_q$.

Choose a line $D \subset$ tgt space of A whose slope is <u>not</u> in $\mathbb{F}_{p^2}$. [This means something since $A = E \times E$.]

It makes sense to "divide" A by D; this means

$$\begin{array}{ccc} \text{"tangent space"} & \longleftrightarrow & t_A \\ \cup & & \\ D & \longleftrightarrow & [D] \subset t_A \end{array}$$ (subgroup scheme)

(stable under p-th power map)

(which is zero here) $\to$ curve is s.s.!

So "dividing A by D" is just taking $A/[D]$.

Direct def'n of $A/[D]$:

- same pts as A
- less rat'l functions : those having derivative by D equal to 0.

(So, e.g., $A/t_A = A^{(p)}$).

E.g.
$$\begin{array}{ll} A : & y^2 = x^3 + ax + b \\ \Big\downarrow \mathrm{Fr} & \\ A^{(p)} & Y^2 = X^3 + a^p X + b^p \end{array}$$

Fr is $Y = y^p$, $X = x^p$

take $t = \frac{x}{y}$ param. near zero ; so kernel is given by $t^p = 0$.

So set $J = A/[D]$.

So ask whether the polarization descends to J :
$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\pi"'] & A^* \\ J \arrow[r, dashed, "\exists \varphi_J ?"'] & J^* \arrow[u, "\pi^*"'] \end{tikzcd}$$

For this, a nec. condn is $\varphi([D]) = 0$; in our case, this holds, since $\ker \varphi = t_A$.

(du Mumford) : If D has dim. 1, this nec. condn. is also sufficient.

[<u>General fact</u> is

<u>If</u> $\left\{ \begin{array}{l} \varphi : A \longrightarrow A^* \quad \text{polariz.} \\ N \text{ finite subgp of } A \\ \text{Assume } N \subset \ker \varphi,\ |N| \text{ is prime.} \end{array} \right.$

Then φ descends to a polarization of A/N.]

$\operatorname{Deg} \varphi_J = ?$ Count degrees of various kernels $\Rightarrow \deg \varphi_J = 1$.

J has a polarization of deg. 1 (def. over $\mathbb{F}_q$).

[D as an alg. group $/k$

Affine algebra is $\Lambda : k \oplus kx \oplus \cdots \oplus kx^{p-1}$; $x^p = 0$

$$\Lambda = k[x]/(x^p)$$

Comultiplication is $x \longmapsto x \otimes 1 + 1 \otimes x$

$\operatorname{order}(D) = \dim_k \Lambda = p$

t_A is a group of order p^2 which, over $\overline{\mathbb{F}}_p$, has infinitely many subgroups of order p.]

<u>Claim</u>: J is not isomorphic over k (as abelian variety) to a product of two elliptic curve. (k any extn of $\mathbb{F}_q$).

If E is any ss elliptic curve $/ k \supset \mathbb{F}_{p^2}$, look at $\operatorname{tgt}(E)$.

<u>Claim</u>: $\operatorname{tgt}(E)$ has a natural "$\mathbb{F}_{p^2}$-structure" which is functorial.

This is so because E comes by scalar extn from a curve over $\mathbb{F}_{p^2}$ with Frob $= p$ (for any such E). Then tgt(E) comes from the tgt space over $\mathbb{F}_{p^2}$.

Suppose now $J = E_1 \times E_2$, E_i s.s.

Then $A = E \times E \longrightarrow J \xrightarrow{\sim} E_1 \times E_2$.

Look at tgt map to $E \times E \longrightarrow E_1 \times E_2$, which is $\mathbb{F}_{p^2}$-rational.

But $\ker = D$ has irrational slope, so contrad. ↯.

So J is not $E_1 \times E_2$.

$\therefore$ This J is the jacobian of a $C/\mathbb{F}_q$ of genus 2, and Frob will be p^e (since that is invariant under isogeny), so this realizes the Weil minimum.

So q = square is done. $\boxtimes$

---

q non-square

$$q \text{ special} \iff \begin{cases} p \mid m & m = [2q^{1/2}] \\ q = x^2 + 1 \\ \quad\; x^2 + x + 1 \\ \quad\; x^2 + x + 2 \end{cases}$$

<u>Thus</u>: If q is not special, then $N_q(2) = 1 + q + 2m$.

We will choose an ell. curve E with $\mathrm{Trace}(\mathrm{Frob}) = -m$.
This exists because q is not special (seen before!)

To be proved: E can be glued to itself, i.e., $\exists\, C$ s.t. $\mathrm{Jac}(C) \underset{\text{isogenous}}{\sim} E \times E$.

We use the "elementary glueing":

ⓐ <u>$p \neq 2$</u>

<u>Lemma</u>: *Let $a \in \mathbb{Z}$, $p \nmid a$ and $|a| \leq 2\sqrt{q}$, $a^2 - 4q \neq -3, -4$, q not a square.
Then there exists an elliptic curve $E/_{\mathbb{F}_q}$ with $Tr(\mathrm{Frob}) = a$ and $j(E) \neq 0, 1728$.*

<u>Proof</u>: An E exists with $Tr(\mathrm{Frob}) = a$, and this is an <u>ordinary</u> curve since $p \nmid a$.

If $\mathrm{End}(E) \not\cong \mathbb{Z}[i]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, then $j(E) \neq 0, 1728$, so ok.

Assume for instance that $\mathrm{End}\, E = \mathbb{Z}[i]$, and let $\pi = \mathrm{Frob}$, [redacted] $\pi = x + yi$,

and $\begin{cases} Tr\, \pi = a = 2x \\ x^2 + y^2 = \pi\bar{\pi} = q \end{cases}$

Claim: $y \neq \pm 1$

(if $y^2 = 1$, $q = x^2 + 1$ so $4q = 4x^2 + 4 = a^2 + 4$ and $a^2 - 4q = -4$ against hypothesis).

So $\mathbb{Z}[\pi] \subsetneq \mathbb{Z}[i]$

[Can use: $\exists$ another curve isog to E w/ $\mathrm{End} = \mathbb{Z}[\pi]$.]

[Instead:]

Choose ℓ prime, $\ell | y$; look at the action of π on ℓ-division points ($\ell \neq p$; otherwise $p | x$ so $p | a$)

So $\pi \equiv x \mod (\ell \,\mathrm{End}\, E)$,

so π acts by homothety on ℓ-div. pts

have $\ell + 1$ subgps of order ℓ, all stable by π, of these, at most 2 are stable by $\mathbb{Z}[i]$.

So choose a subgp D which is not stable by $\mathbb{Z}[i]$, and replace E by E/D.

Then $\mathrm{End}(E/D) = \{x + iy \mid \ell | y\} \neq \mathbb{Z}[i]$, so choose E/D now.

In the other case, proceed similarly. $\boxtimes$

Now choose E acc. to lemma for $a = m$, since $m^2 - 4q \neq -3, -4$

(if $m^2 - 4q = -4 \Rightarrow 4q = 4 + m^2 \Rightarrow 2 | m \Rightarrow q = 1 + (\frac{m}{2})^2$ $\mathcal{S}$)

$ = -3$ similar

Now E can be glued to itself (because exceptions had $j=0$ or 1728), and we are done. ☒

④ $\underline{p=2}$ $\quad 2^e$ (e odd) is nonspecial iff $\begin{cases} 2 \nmid m \\ 2^e \text{ is not } x^2+x+2 \end{cases}$

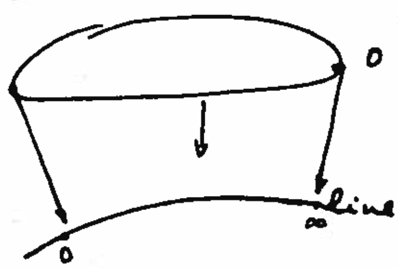
[redacted]

Choose E_1 and E_2 with $\mathrm{Tr}(\mathrm{Frob}) = -m$ and which are not isom., even after quadratic field extension.

(1) Lemma: This is possible — later.

(2) Then one can glue E_1 to E_2.

Proof of (2)



Write E as quad covering of $\mathbb{P}_1$ ram at ∞.

Covering is $E/\sim$ where $x \sim -x$.

Other ramif pt is the pt of order 2, rat'l, so can map to zero.

So Artin-Schreier eqn is

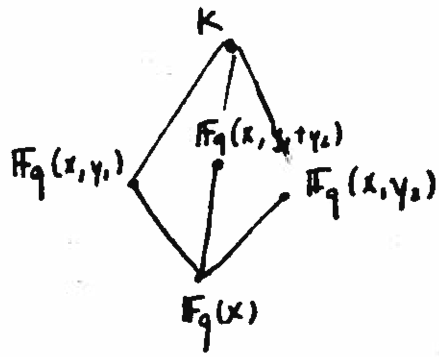
$$\boxed{y^2 + y = \lambda x + \mu/x + \nu} \quad \lambda, \mu \neq 0$$

replace x by λx, so can write $y^2+y = x + \dfrac{\mu}{x} + \nu$

(over $\overline{\mathbb{F}}_2$, write μ as x^2+x, and then ν can be taken $=0$)

So have $E_1 : \begin{cases} y_1^2 + y_1 = x + \cancel{\dfrac{\mu_1}{x}} + \nu_1 \\ y_2^2 + y_2 = x + \cancel{\dfrac{\mu_2}{x}} + \nu_2 \end{cases}$

$\cancel{\mu_1 + \mu_2}$



$$(y_1+y_2)^2 - (y_1+y_2) = \cancel{\frac{\mu_1+\mu_2}{x}} + \nu_1 + \nu_2$$

<u>genus zero</u>

[if $\mu_1 = \mu_2$, $\cancel{\mu_1+\mu_2} = 0$ so get const field extn.]

So K is the field of a curve of genus 2. This proves glueing $\boxtimes$

To <u>prove the Lemma</u> (1):

Choose E_1; E_1 ordinary $\Rightarrow$ E_1 has a unique subgroup of order 2, say N.

Put $E_2 = E_1/N$. Is $E_2 \cong E_1$?

If not, we are done.

If $E_1 \cong E_2$, then $\exists\, \varphi : E_1 \longrightarrow E_1$ with kernel N, hence of degree 2.

Now E_1 ordinary, so $\mathrm{End}(E_1)$ is an order in an imag. quad. field, and $\varphi \in \mathrm{End}(E_1)$, $\varphi\bar{\varphi} = 2$.

Then $|\mathrm{Tr}\,\varphi| \le 2\sqrt{2}$ (since $|\varphi| = \sqrt{2}$)

So $\mathrm{Tr}\,\varphi = -2, -1, 0, 1, 2$

$$
\left.\begin{array}{lll}
\mathrm{Tr}\,\varphi = -2 & \Longrightarrow & \varphi = \cancel{-1 \pm i} \\
-1 & \Longrightarrow & \varphi = \frac{-1 + \sqrt{-7}}{2} \\
0 & \Longrightarrow & \varphi = \pm\cancel{\sqrt{2}} \\
1 & \Longrightarrow & \cancel{1 \pm i}
\end{array}\right\}
$$

impossible, since 2 splits in End E by general facts.

$$2 \Longrightarrow \frac{1 \pm \sqrt{-7}}{2}$$

So $\varphi = \pm\frac{1 \pm \sqrt{-7}}{2}$, and $\mathrm{End}\,E_1 = \mathbb{Z}\left[\frac{1 \pm \sqrt{-7}}{2}\right]$

So remains to show that I can choose E_1 with $\mathrm{End}(E_1) \neq \mathbb{Z}\left[\frac{1 \pm \sqrt{-7}}{2}\right]$.

Assume $\mathrm{End}\,E_1 = \mathbb{Z}\left[\frac{1 + \sqrt{-7}}{2}\right]$

$$\mathrm{Frob} = \pi = x + \frac{1 + \sqrt{-7}}{2}\,y \qquad x, y \in \mathbb{Z}$$

Again: <u>claim that $y^2 \neq 1$</u>

$$\pi\bar{\pi} = q = (x + \tfrac{1}{2})^2 + 7\,\frac{y^2}{4}$$

if $y^2 = 1$, get $q = (x + \frac{1}{2})^2 + \frac{7}{4} = x^2 + x + 2$

Now $\mathbb{Z}[\pi] \subsetneqq \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, and by the argument above I can change E_1 s.t. $\mathrm{End}(E_1) = \mathbb{Z}[\pi]$, for instance (or choose l/y as before, etc.). $\boxtimes$

11/12

$\boxed{g=2}$

We were reduced to q not a square; q is non-special is done (we get $q+1+2m$, $m=[2\sqrt{q}]$.)

Need to show: if q is special:

a) $q+1+2m$ is impossible

b) $q+2m$ is possible iff $\{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2}$

c) if q special and $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$, then $q+2m-1$ is possible.

a) Proof: q is special $\iff$

a1) q is represented by the quad. polyn. x^2+1, x^2+x+1 (special case of Beauville)

OR

a2) q is represented by x^2+x+2 (so $q=2^e$, e odd) One finds $e=1,3,5,13$. $\longrightarrow$ $\longrightarrow$ see this later

OR

a3) $p \mid m$

$2^e = x^2+x+2$

$2^{e+2} = (2x+1)^2+7 = y^2+7$

Ramanujan's equation

<u>Case a2</u> : We show that $q+1+2m$ is impossible.

→ If $q=2$, $[2\sqrt{2}]=2$, so this is special also because $p|m$ (d3).

$$1+q+2m = 1+2+4 = 7 > 2(q+1)$$, so of course we are done.

→ If $q=2^3$, $[2\sqrt{8}] = [\sqrt{32}] = 5$, so $1+q+2m = 1+8+10 = 19 > 2(q+1)$, again impossible.

→ Recall that $1+q+2m$ is possible only if eigenvalues of Frob are $\pi, \bar{\pi}, \pi, \bar{\pi}$, $\pi+\bar{\pi} = -m$, $\pi\bar{\pi} = q$.

If $q = 2^5$, $m = [2\sqrt{32}] = [\sqrt{128}] = 11$, so

$$m^2 - 4q = 121 - 128 = -7$$

So $\boxed{\pi = \dfrac{-11+\sqrt{-7}}{2}}$.

We must show this is impossible.

in $\mathbb{Q}(\sqrt{-7})$, 2 splits as $(\alpha)(\bar{\alpha})$, $\alpha = \frac{1+\sqrt{-7}}{2}$, $\alpha\bar{\alpha} = 2$.

Since $\pi\bar{\pi} = 2^5$, so $(\pi) = (\alpha)^i(\bar{\alpha})^j$ $i+j=5$, but $2 \nmid \pi$, so must have $(\pi) = (\alpha)^5$ or $(\pi) = (\bar{\alpha})^5$

So $\pi = \pm\alpha^5$ or $\pm\bar{\alpha}^5$. In fact, $\pi = -\alpha^5 = (-\alpha)^5$

So Frob. over $\mathbb{F}_{2^5}$ is a fifth power.

Take $\mathrm{Jac}(C)/_{\mathbb{F}_{2^5}}$.

$\mathrm{End}(\mathrm{Jac}(C)) \supset \mathbb{Z}[\pi]$ (in fact $= M_2(\mathbb{Z}[\pi])$)

So $\quad \mathrm{End}(\mathrm{Jac}(C)) \supset \mathbb{Z}[\pi] = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$

define $\pi_1 = -\alpha \in \mathrm{End}(\mathrm{Jac}(C))$, and then $\pi_1^5 = \pi =$ Frobenius on $\mathrm{Jac}(C)$.

• So have ab. var. $A/\mathbb{F}_{p^e}$, $\pi = \mathrm{Frob}/\mathbb{F}_{p^e}$, and $\pi = \pi_1^e$ for some $\pi_1 \in \mathrm{End}(A)$. Would like to conclude: exists a structure $/\mathbb{F}_p$ for A with Frobenius π_1.

Need <u>more</u>: π_1 acts by 0 on the tangent space of A.

(Above $\alpha = \frac{1+\sqrt{-7}}{2}$, $\pi = \frac{-11+\sqrt{-7}}{2}$, so $\alpha = \pi + 6$, and both π and 6 act by 0 on tangent space, hence so do α and $\pi_1 = -\alpha$!)

Now define $\quad A^{(p)}$ as usual. Then we have

$$\begin{tikzcd} A \arrow[r, "F_p"] \arrow[dr, "\pi_1"'] & A^{(p)} \arrow[d, dashed] \\ & A \end{tikzcd}$$

(The map $\downarrow$ exists if and only if π_1 kills the tgt space, so OK.)

$A^{(p)} \xrightarrow{\cong} A$ is an isom. by degree computation!

So $A \xrightarrow{\pi_1} A$ gives an isom. of $A^{(p)}$ to A, so Galois descent is OK.

Hence we have an $\mathbb{F}_2$-structure on $\mathrm{Jac}(C)$ with Frobenius $-\alpha$ (π respects the

So we get (Torelli): there is an $\mathbb{F}_2$-structure on C with Frob $-\alpha$.

Now go to $\mathbb{F}_8 = \mathbb{F}_{2^3}$, and get Frobenius $= -\alpha^3 = \frac{5+\sqrt{-7}}{2}$

Now nber of pts$/\mathbb{F}_8$ $= 1 + 8 - 2\cdot 5 = -1$ $\lightning$. (Contrad).

$\rightarrow$ If $q = 2^{13}$, we find $m = 191$, and use

$$\left(\frac{1+\sqrt{-7}}{2}\right)^{13} = -\frac{181+\sqrt{-7}}{2}$$

$$\left(\frac{1+\sqrt{-7}}{2}\right)^{e} = \frac{a_e + b_e\sqrt{-7}}{2}$$

When is $b_e = \pm 1$?

e odd; $e = 3, 5, 13$

$\rightarrow$ analytic method!

we'll come back to this.

Case a3: $p | m$; I can assume $q = p^e$, e odd ≥ 3 (when $e=1$, $p|m \Rightarrow p = 2$ or 3 and these have been done already).

have $1+q+2m$ iff $\pi, \bar{\pi}, \pi, \bar{\pi}$, $\begin{cases} \pi + \bar{\pi} = -m \\ \pi\bar{\pi} = q \end{cases}$

Now, $p \mid m$, $q = p^e$ e odd ≥ 3.

By Tate's theorem, $\exists f_\pi$ (we saw f_π odd ≥ 5) s.t. the multiplicity of π as root of Frob. in any abelian variety is divisible by f_π.

So we cannot have $f_\pi \mid 2$! So the jacobian cannot exist in this case, done. $\boxed{/}$

b) $\begin{cases} \text{If } \{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}, \text{ then } q+2m \text{ is impossible} \\ \text{If } \{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2}, \text{ then } q+2m \text{ \underline{is} possible.} \end{cases}$

We've shown "down by one" (for a curve of genus 2) is possible <u>only</u> if

$$\text{Frob}: \quad \pi_1, \bar{\pi}_1, \bar{\pi}_2, \pi_2$$

where
$$\begin{cases} \pi_1 + \bar{\pi}_1 = -m + \dfrac{1+\sqrt{5}}{2} \\ \pi_2 + \bar{\pi}_2 = -m + \dfrac{1-\sqrt{5}}{2} \end{cases}$$

and this is possible only when $m + \frac{-1+\sqrt{5}}{2} \leq 2\sqrt{q}$, i.e, only when $\{2\sqrt{q}\} = 2\sqrt{q} - m \geq \frac{\sqrt{5}-1}{2}$

So first statement is OK.

Now assume $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$

First, make an ab. variety of dim. 2 with $\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2$ as required above, i.e.,

$$\begin{cases} \pi_1 + \bar{\pi}_1 = -m + \frac{1+\sqrt{5}}{2} \\ \\ \pi_2 + \bar{\pi}_2 = -m + \frac{1-\sqrt{5}}{2} \end{cases}$$

We want this ab. variety to be <u>ordinary</u>:

• $\pi_1 + \bar{\pi}_1$ and $\pi_2 + \bar{\pi}_2$ are prime to p

× if $p \mid m$, obvious, since $\frac{1 \pm \sqrt{5}}{2}$ is a unit

× if $p \nmid m$, q is repres. by x^2+1, x^2+x+1, x^2+x+2,
so

$$4q = 4x^2+4 \overset{= (2x)^2+4}{} \quad \text{so} \quad m = 2x$$

$$4q = 4x^2+4x+4 \overset{= (2x+1)^2+3}{} \quad \text{so} \quad m = 2x+1$$

$$4q = 4x^2+4x+8 = (2x+1)^2+7, \quad \text{so} \quad m = 2x+3.$$

so $\{2\sqrt{q}\}$ is small, usually $< \frac{\sqrt{5}-1}{2}$. (at least for $q > 8$)

Only exceptions are $q = 2, 8$ (2 is covered: $p \mid m$)

$$\{2\sqrt{8}\} = 0.656\ldots > \frac{\sqrt{5}-1}{2}$$

[For $q=2$, want $g=2$, 6 pts. Take
$$y^2+y = \frac{x^2+x}{x^3+x+1}$$]

Construction of a curve w/ 18 $(= 2(1+8))$ points over $\mathbb{F}_8$

Choose an irred cubic polyn $f(x)$ on $\mathbb{F}_8$, e.g. x^3+x+c for suitable c.

Write

$$y^2+y = \frac{a+bx+cx^2}{x^3+x+c} \qquad a,b,c \in \mathbb{F}_8.$$

$$(\text{i.e.}) \quad y^2+y = \frac{a+bx+cx^2}{f(x)} \qquad a,b,c \in \mathbb{F}_8.$$

We want to choose a,b,c s.t.

$$\mathrm{Tr}_{/\mathbb{F}_2}\left(\frac{a+bx+cx^2}{f(x)}\right) = 0 \qquad \text{for all } x \in \mathbb{F}_8.$$

$a,b,c \in \mathbb{F}_8 = \mathbb{F}_2^{\,3}$ (as $\mathbb{F}_2$-vector space)

So $(a,b,c) \in \mathbb{F}_2^9$, and get 8 homog. eqns in 9 unknowns, so choose a solution which is not trivial!

Now Tate-Honda says such an ab. variety exists.

Note $\mathbb{Q}(\pi) \supset \mathbb{Q}(\sqrt{5})$..

Have

$$\begin{array}{l} \mathbb{Q}(\pi) \\ \big|\, 2 \quad \text{imag. quad. extn.} \\ \mathbb{Q}(\sqrt{5}) \\ \big|\, 2 \\ \mathbb{Q} \end{array}$$

$\mathbb{Q}(\pi) \longleftarrow$ CM-field of deg. 4 w/ assoc. real field $\mathbb{Q}(\sqrt{5})$.

So $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ (Tate).

We have A <u>up to isogeny</u>.

Next step: existence of such an A <u>having a polarization of degree 1</u>.

(<u>Shimura</u>: A in char 0, CM by $\begin{array}{c} K \\ 2\big| \\ K_0 \end{array} \longrightarrow$ OK)

<u>Shimura's Thm (char 0)</u>: If CM type is K/K_0 with K ramified over K_0, then $\exists$ A in the isogeny class having polariz. compatible w/ CM-type, of degree 1. [Proc. London Math. Soc., <u>34</u> (1977), p. 67, remark.]

Here OK, since $\mathbb{Q}(\sqrt{5})$ has class number 1. $\to$ no quadratic unramified extn.

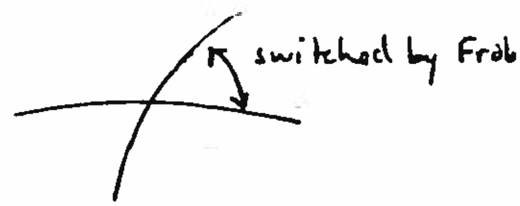
<u>Claim</u>: Sh's thm is OK in char p for ordinary abelian varieties

(proof later)

Then we get A w/ the right Frob + polarization of degree 1. It remains to check that this is indec. Over $\mathbb{F}_q$, it is indec. because $\mathrm{End}_{\mathbb{F}_q}(A) = \mathbb{Q}(\pi)$ is a field.

It could decompose over $\mathbb{F}_{q^2}$. This doesn't happen:

if indec over $\mathbb{F}_q$, dec over $\mathbb{F}_{q^2}$, it's



So on V_ℓ, matrix of Frob is $\left(\begin{array}{c|c} 0 & * \\ \hline * & 0 \end{array}\right)$

so trace $= 0$.

But our trace is $-2m + 1 \neq 0$.

This proves that our curve exists. ■

<u>Proof of Claim above</u>

char 0 Shimura $\Longrightarrow$ char p Shimura for <u>ord</u> ab. vars.

Use "canonical lifting": lift $A/\mathbb{F}_q$ into $\mathcal{A}/W(\mathbb{F}_q)$, and End does not change.

By Shimura, $\mathcal{A} \underset{\text{isog}}{\sim} \mathcal{A}'$, on $\mathcal{A}'$ have a polariz. of degree 1

ker of $\mathcal{A} \longrightarrow \mathcal{A}'$ is stable under max'l order

So $A \to A'$ exists over the field of fractions of $W(\bar{\mathbb{F}}_q)$.
Polarization is $A' \to (A')^*$.
So reduce everything mod p.

Another way: take Shimura's proof and show it works in char p.

Translation of K ramified over K_0:

K/K_0 ramified $\iff$ $Cl(K) \xrightarrow{\text{norm}} Cl^{\text{strict}}(K_0)$ is onto

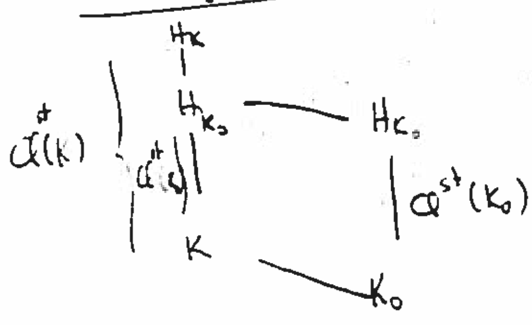
[Cl^{strict} : $\mathfrak{a} \sim 1$ if $\mathfrak{a} = (\alpha)$, $\alpha \gg 0$.
For tot. imag. field, $Cl(K) = Cl^{\text{strict}}(K)$, and map is just $\mathfrak{a} \longmapsto \mathfrak{a}\bar{\mathfrak{a}}$.]

Pf of $\iff$ CFT!

H_{K_0} = Hilbert class field = max. ab. unr extn, except maybe at ∞

$$\begin{array}{c} H_{K_0} \\ | \\ K_0 \end{array}$$

Then $Gal(H_{K_0}/K_0) \cong Cl^{\text{strict}}(K_0)$



and res: $Gal(H_K/K) \to Gal(H_{K_0}/K_0)$ is norm map.

If K/K_0 unr, we'd have,

$$\begin{array}{ccc} & & H_{K_0} \\ & & | \\ H_K & — & K \\ & & | \\ & & K_0 \end{array}$$

and then coker $Cl(K) \longrightarrow Cl^{st}(K_0)$ has order 2. $\boxed{\checkmark}$

<u>Shimura's proof</u>

Choose A s.t. $\mathrm{End}(A)$ is a max'l order in K, and choose some polarization φ. $\varphi : A \longrightarrow A^*$.

Look at $\mathfrak{a}$ ideal of $\mathcal{O}_K$ s.t. $\ker\varphi \cong \mathcal{O}_K/\mathfrak{a}$

<u>Shimura-Taniyama</u> : $\mathfrak{a}$ "is" an ideal of $\mathcal{O}_{K_0}$.

Replacing φ by $\lambda\varphi$ gives a polarization if $\lambda \in \mathcal{O}_{K_0}$, $\lambda \gg 0$

May replace A by some $A/\left(\begin{smallmatrix}\text{finite subgp}\\ \text{stable by } \mathcal{O}_K\end{smallmatrix}\right) \longleftrightarrow$ some ideal $\mathfrak{b} \subset \mathcal{O}_K$

Want $\lambda\varphi$ to descend to $A/(\quad)$ w/ degree 1

$\varphi \longmapsto \lambda\varphi$ in $\mathfrak{a} \longrightarrow \lambda\mathfrak{a}$

<u>Condition is</u> : if $\lambda\mathfrak{a} = \mathfrak{b}\bar{\mathfrak{b}}$, then on $A/(\;)$, $\lambda\varphi$ has degree 1.

... the class of $\mathfrak{a}$ in $Cl^{st}(K_0)$ is an

This proves part (b.) ☑

Remains to prove (c)

11/19: Remains: If q is not a square and "special", down by 2 is possible, i.e., there exists a curve with $q + 2m - 1$ points.

In fact, one can find a curve [redacted] of type $(m-1, m-1)$ or $(m, m-2)$.

For $q = 2, 3$ just write the equation.

more precisely, for $q = 2$, $(m, m-2)$ is possible, $(m-1, m-1)$ is not

for $q = 3$, both are possible

Assume $q \geq 5$.

Cases:
1) $p | m$ and $p \neq 2$ $\Rightarrow$ $(m-1, m-1)$ is possible
2) $p | m$ and $p = 2$ $\Rightarrow$ " " "
3) $p \nmid m$ and q special, $p \neq 2$ $\Rightarrow$ " " "
4) $p | m$, q special, $p = 2$ $\Rightarrow$ $(m, m-2)$ is possible

$\rightarrow$ only three cases: $q = 2^3, 2^5, 2^{13}$

This means

$(m-1, m-1)$ possible : Can glue E_1, E_2 with $\mathrm{Trace}(\mathrm{Frob}) = -(m-1)$

$(m, m-2)$ possible : Can glue E_1, E_2 with $\mathrm{Trace}(\mathrm{Frob}) = \begin{cases} -m \\ -(m-2) \end{cases}$

Case 1 : $p \mid m$, hence $p \nmid (m-1)$, so E_1 and E_2 exist (and are ordinary).

Also, $\mathbb{Z}[\pi]$ is an order in an imag. quad. field w/ disc. $-4q + \mathrm{Tr}(\pi)^2 = -4q + (m-1)^2 = -(4q - (m-1)^2)$

$$4q = m^2 + k \qquad 1 \le k \le 2m$$

$$4q - (m-1)^2 = m^2 + k - m^2 + 2m - 1 = k + 2m - 1 \geq 8$$

$k \equiv -m^2 \equiv 0$ or $3 \pmod 4$

so $k \equiv 3 \pmod 4$

$k = 3, 7, \dots$

$p \mid m$, $p \neq 2 \Rightarrow 2m - 1 \geq 5$

so ≥ 8.

One can choose E_1, E_2 such that $\mathrm{End}(E_i) = \mathbb{Z}[\pi]$.

So End $\not\ni$ {cube roots of 1 or i}

So $j \neq 0, 1728$

so elementary glueing is OK.

$\sqrt{p=2}$

<u>Case 2</u>: Choose E, $\operatorname{End} E = \mathbb{Z}[\pi]$, ord, disc < -8.

Now take E, $E' = E/_{E[2]}$ (in char 2!)

Not <u>isomorphic</u> (otherwise $\exists$ isogeny $E \to E$ deg 2 $\Longrightarrow \mathbb{Q}(\sqrt{-7}) \subseteq$).

Write these as $y^2 + y = x + \frac{a}{x} + b$

$$y^2 + y = x + \frac{a'}{x} + b'$$

$\underline{a \neq a'}$

And we get the usual diagram fusing.

$$\begin{tikzcd} & \text{fusing} \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{F}_q(E) \arrow[dr, dash] & & \mathbb{F}_q(E') \arrow[dl, dash] \\ & \mathbb{F}_q(X) & \end{tikzcd}$$

This does ②.

Case 3: $p \nmid m$, q special, $p \neq 2$:

Same proof, but problem is whether $p \mid m-1$.

q special, $p=2 \longrightarrow 4q = m^2+3$ or $4q = m^2+4$.

So $4q = m^2 + k$, $k = 3$ or 4

$p \mid m-1 \Rightarrow m \equiv 1 \pmod{p} \Rightarrow k \equiv -1 \bmod p$

so 4 or $5 \equiv 0 \bmod p$

$\longrightarrow p=5$, $k=4$, m even

- So if $p \neq 5$, same proof above works since $p \nmid (m-1)$.

- If $\underset{(\Rightarrow k=4)}{p=5}$ $\begin{cases} a) & q=5 \text{ ; then } m=[2\sqrt{5}]=4, \ m-1=3 \text{ and } 5\nmid 3. \text{ So OK.} \\ b) & q=5^e, \ e \text{ odd} \geq 3 \text{ ; would have } 5^e = \left(\frac{m}{2}\right)^2+1 \end{cases}$

But the eqn: $y^e = x^2+1$ $x \neq 0$ $e \geq 2$ has no $\mathbb{Z}$-solutions.
[proof later].

So (b) is empty, and (3) is done.

<u>Case 4</u>: $q = 2^3, 2^5, 2^{13}$

Claim is: $(m, m-2)$ is possible.

$p = 2,\ 2 \nmid m \implies 2 \nmid m-2$

So we find E_1, E_2 ord. elliptic curves with $Tr(Frob) = \begin{cases} -m \\ -(m- \end{cases}$

and we glue them as in 2 (and we know they are not geometrically isomorphic ~~because~~ $m \neq \pm(m-2)$. If $m = -m+2$, $m = 1$; bad case is $k = 7$, so $\sqrt{4q} = m + 7$ so $m = 1 \implies q = 2$.) $\blacksquare$

<u>Glueing and Hermitian Forms</u>

<u>Idea</u>: E, $R = End_{\mathbb{F}_q}(E)$

We want to construct the jacobian of a curve

$J = E \times E$ w/ a map $E \times E \xrightarrow{\varphi} E \times E$

given by $\Phi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$

φ polarization $\iff$ Φ hermitian $\gg 0$

deg 1 $\iff$ $ad - bc = 1$

If not decomposable, then $\exists! C$ of genus 2 with

$Jac(C) = (E \times E, \varphi)$.

So E has been glued to E.

$$\underbrace{E \times \cdots \times E}_{n \text{ times}} = \text{"} E \otimes_R L \text{"} \quad L \text{ free of rk } n \text{ over } R$$

So try for projective.

We want to develop this first, then.

Tensor Product (and Hom) in abelian categories

$\mathcal{C}$ an abelian category
R a ring w/ 1.
Let $E \in \mathcal{C}$ with a morphism $R \longrightarrow \mathrm{End}(E)$ give

To the pair (M a right R-module finitely presented, E w/ R-action)
I want to attach an object of $\mathcal{C}$ called "$M \otimes_R E$"

Properties shd be :
- $R \otimes_R E = E$
- compatible w/ direct sum
- right exact.

Write $R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$

Set $\begin{cases} R^m \otimes_R E = E^m \\ R^n \otimes_R E = E^n \end{cases}$

And define $M \otimes_R E = \operatorname{Coker}(E^m \longrightarrow E^n)$.

Indep. of resolution is easy, and also follows from alternate definition:

Want $\operatorname{Hom}(M \otimes_R E,\ F) = \operatorname{Hom}_R(M, \operatorname{Hom}(E,F))$

(for $F \in \mathcal{C}$) where $\operatorname{Hom}(E,F)$ is a right R-module via the action on E.

So $M \otimes_R E$ represents the functor on the right.

Another construction is "$\operatorname{Hom}_R(M,E)$" when M is a finitely presented left R-module.

Do the same: choose a resolution

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

$$E^m \longleftarrow E^n \longleftarrow \underbrace{\operatorname{Hom}_R(M,E)}_{\text{define this as the kernel.}} \longleftarrow 0$$

transpose of the matrix

This represents a functor too:

$$\mathrm{Hom}\,(F, \mathrm{Hom}_R(M,E)) = \mathrm{Hom}_R(M, \underbrace{\mathrm{Hom}(F,E)}_{\substack{\text{viewed as a} \\ \text{left } R\text{-module}}})$$

I'll apply this to: $\mathcal{C}$ category of $\overset{\text{comm.}}{\text{alg.}}$ groups $/k$
(or the subcat. of proper such).
And R will be Noeth., M finitely generated.

In this case, $\mathrm{Hom}_R(M,E)$ can also be described by:

$$\begin{array}{l} S' \\ \downarrow \\ k = S \end{array} \qquad (\mathrm{Hom}_R(M,E))(S') = \mathrm{Hom}_R(M, E(S'))$$

(This defines it as a functor on k-schemes, so determines it.)

Example: E ell. curve, $R = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$

Then $\mathrm{Hom}_{\mathbb{Z}}(M,E) = E[n]$

and the fla above says $E[n](S') = E(S')[n]$.

But "$\otimes$" is zero!

Now apply this to $\left\{ \begin{array}{l} E \text{ an elliptic curve} \\ R = \mathrm{End}(E)\ ,\ M \text{ fin. generated.} \end{array} \right.$

Then $M \otimes_R E$ is an ab. variety of dimension $rk_R M$ (*)
and $\mathrm{Hom}_R(M, E)$ comm. group of dim $= rk_R M$.

(*) since it is $\mathrm{Coker}(E^m \longrightarrow E^n)$!

Note: can also define Tor_n, Ext^n as before ...

<u>M projective</u> :

Dual of $M \otimes_R E$ is $M^* \otimes_R E$, where M^* is the dual of M, $M^* = \mathrm{Hom}(M, R)$ a <u>left</u> R-module in a natural way, but use the <u>involution</u> $r \mapsto \bar{r}$ of R corresp. to the polarization (= cx conj. or quat. conj.) and use this to make M^* a <u>right</u> R-module.

i.e., $\lambda \in M^*$, $r \in R$, define $\boxed{(\lambda r)(m) = \lambda(m\bar{r})}$.

(Note that M projective $\Longrightarrow$ have $M \underset{pr}{\rightleftarrows} R^n$
So define $M \otimes_R E \rightleftarrows E^n$ using the induced projector.)

(For an ab. variety $(M \otimes_R A)^* = M^* \otimes_R A^*$.)

[Can extend for M not projective ?]

<u>Claim</u>: $\mathrm{Hom}(M \otimes_R E, N \otimes_R E) = \mathrm{Hom}_R(M,N)$

An arrow $\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}(M \otimes_R E, N \otimes_R E)$ is obvious.

Since M is projective, it's enough to check for free modules, hence for $M=N=R$, and then

$$\mathrm{Hom}(E,E) = \mathrm{Hom}_R(R,R) = R$$

(by our assumption on R)

<u>Claim</u>: If $M \otimes_R E = B \oplus C$ B, C ab. varieties, then $M = M_B \oplus M_C$ as R-modules and $B = M_B \otimes E$, $C = M_C \otimes E$.

<u>Pf</u>: Corresponds to $p \in \mathrm{End}(M \otimes_R E)$ s.t. $p^2 = p$; but this comes from a projector of M, which gives M_B & M_C. $\boxtimes$

<u>E, R, M projective</u>

Define $A = M \otimes_R E$. [Note that this is isog. to $\underbrace{E \times \cdots \times E}_{\text{rk } M \text{ times}}$.]

What is a principal polarization on A?

<u>Claim</u>: Corresps. to an R-hermitian $\gg 0$ form on M with discriminant 1.

Herm. form on M is $\Phi\ M\times M \longrightarrow R$ w/ the usual properties; can also view as $\varphi: M \longrightarrow M^*$ hom s.t. $\varphi^* = \varphi$.

(via $\Phi(m_1, m_2) = \varphi(m_1)(m_2)$, antilinear in m_1, linear in m_2.)

Φ pos. def. $\longrightarrow$ $\Phi(m,m) > 0$ for all $m \neq 0$

disc 1 : φ is an isomorphism.

[Note $\phi(m,m) \in R$, $\overline{\phi(m,m)} = \phi(m,m)$

and $(R = \operatorname{End} E\,!)$ $\{r \in R \mid \bar{r} = r\} = \mathbb{Z}$

So $\phi(m,m) > 0$ makes sense.]

Now the equivalence

principal polariz on A $\longleftrightarrow$ R-herm. forms on M, pos. def., disc 1.] call such "hermitian modules"

is clear, except maybe that pos. def $\Longleftrightarrow$ φ polarization

If M is free, we have $E\times - \times E \xrightarrow{\varphi} E\times - - \times E$ and then it's in Mumford.

Also

Indec of polariz. $\longleftrightarrow$ Indec of the herm. module M.

(OK)

This gives a method for getting curves of genus 2 out of E and an indec. hermitian module of rk 2, but need to check indec. over quad. extn.

For instance, if $Tr(\text{Frob } E) \neq 0$, this is automatic. (saw this last time).

Set $J = M \otimes_R E$. Indec $\Rightarrow J = J(C)$

: *Example*

E CM by $\sqrt{-2}$

$R = \mathbb{Z}[\sqrt{-2}]$

$M = R \times R$

$\Phi = \begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}$, det $= 4 - (1+2) = 1$.

pos def ✓

indec: values of Φ are even $\not\cong \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

So this gives a curve C

$\tilde{S}_4 = \text{Aut}(M) = \text{Aut}(C)$

$\tilde{S}_4$ = 2-sheeted cover of S_4

genus$(C) = 2$, $\Longrightarrow$ C unique up to quad. twist.

eqn: $y^2 = x^5 - x$

Will show: indec. hermitian H exist, except when
R has disc. $-3, -4, -7$.

Also: under some condns on R, this gives every
ab. variety isog. to a product of E's.

11/26 $(g=2)$

We connected

curves $\longleftrightarrow$ "binary" hermitian forms,
pos. def. of disc. 1.

E ell. curve, $R = \mathrm{End}_k(E)$ [assume: $= \mathrm{End}_{\bar{k}}(E)$]; assume $\mathrm{rk}\, R = 2$. (so R = order in an imag. quad. field).

Choose an R-module P proj. of rank 2, with a Hermitian form $H: P \times P \longrightarrow R$, positive definite (i.e., $H(x,x) > 0$ if $x \neq 0$), disc 1, (i.e., H define an isom. $P \longrightarrow P^*$ (twisted dual)).

Then $E \otimes P = A$ is an ab. variety of dim 2 on which H gives a polariz. of deg 1.

H indec $\longrightarrow$ A indec$/_k$ $\Longrightarrow$ $A = \mathrm{Jac}(C)$

for a well-defined C of genus 2.

indecomposability is no problem because we assume $\mathrm{End}_k(E) = \mathrm{End}_{\bar{k}}(E)$.

[k field of defn]

$-d = \operatorname{disc} R$

Write $R = R_{-d}$, so $R_{-4} = \mathbb{Z}[i]$

$$R_{-3} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

Theorem (Hayashida - Nishi)

Such an indecomposable binary form exists if and only if $d \neq 3, 4, 7$.

First: note: if $A = E \otimes P$, then $P = \operatorname{Hom}_R(E, A)$

for $x \in P$, $H(x) = ?$

interpret x as $E \xrightarrow{x} A$

$H(x) =$ degree of x^* (polarization)

Proof that every P is trivial on R_{-3}, R_{-4}, R_{-7}

Here $P = R \oplus R$ since the class no. is 1.

So $H = \begin{pmatrix} \lambda & \alpha \\ \bar{\alpha} & \mu \end{pmatrix}$, $\lambda, \mu \in \mathbb{Z}, > 0$

$\lambda\mu - \alpha\bar{\alpha} = 1$, $\alpha \in R$

Want $H \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

i.e., have e_1, e_2 basis of P s.t. $e_1 \cdot e_1 = \lambda$, etc.

e_1 : any primitive vector (i.e., $e_1 \neq 0$, Re_1 direct factor).

Assume e_1 has been chosen with smallest $e_1 \cdot e_1$, i.e., λ is minimal.

So $\lambda \leq \mu$ (since $\mu \in \mathbb{Z}$ and $\mu = e_2 \cdot e_2$!)

and α can be changed into any $\alpha + \lambda r$ for $r \in R$.

Claim: by suitable choice of r, I can make α be such that $\alpha\bar{\alpha} < \frac{3}{4}\lambda^2$.

(Proof later)

Then $\quad \lambda\mu - \alpha\bar{\alpha} = 1 \implies \alpha\bar{\alpha} = \lambda\mu - 1 < \frac{3}{4}\lambda^2$

$$\lambda\mu < \frac{3}{4}\lambda^2 + 1$$

$$\lambda \leq \mu \implies \lambda^2 < \frac{3}{4}\lambda^2 + 1 \implies \frac{1}{4}\lambda^2 < 1$$

$$\implies \boxed{\lambda = 1}.$$

Then take $r = -\alpha \implies \alpha$ can be made 0

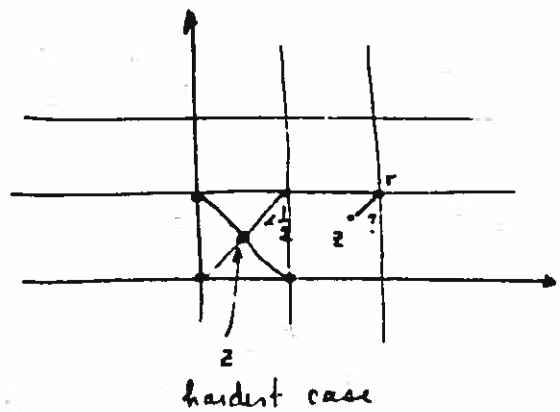
and $\lambda\mu - \alpha\bar{\alpha} = 1$ forces $\underline{\underline{\mu = 1}}$. ∎

<u>Proof of claim</u>

I want to find r s.t. $\left|\frac{\alpha}{\lambda} + r\right|^2 < \frac{3}{4}$.

<u>Lemma</u>: For every $z \in \mathbb{C}$, $\exists r \in R$ s.t. $|z - r|^2 < \frac{3}{4}$.

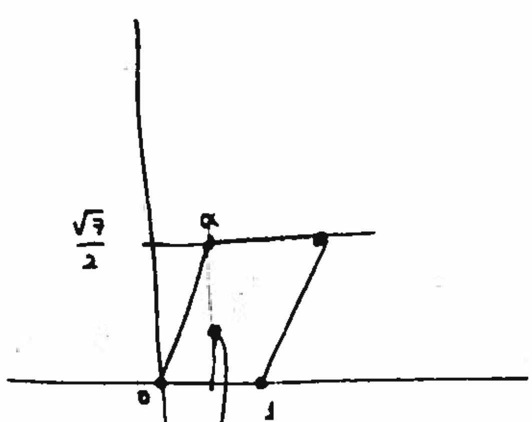
For $\mathbb{Z}[i]$:



so for $\mathbb{Z}[i]$ can get $|z - r| < \frac{1}{2}$

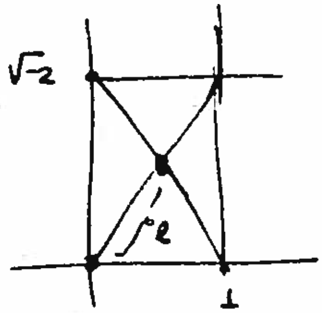
For $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ find can get $|z - r| < \frac{1}{3}$

For R_{-7}:



hardest pt: center of circle through $0, 1, \alpha$ — so check.

For R_{-8}



length $= \frac{3}{4}$

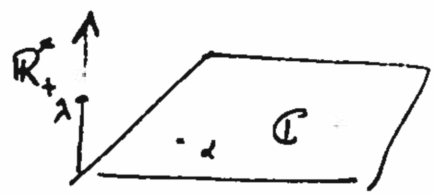
so can't work!

In fact, exists a unique indec. form: $\begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}$

Ordinary quad forms $\longleftrightarrow$ fund domain for $SL_2(\mathbb{Z})$

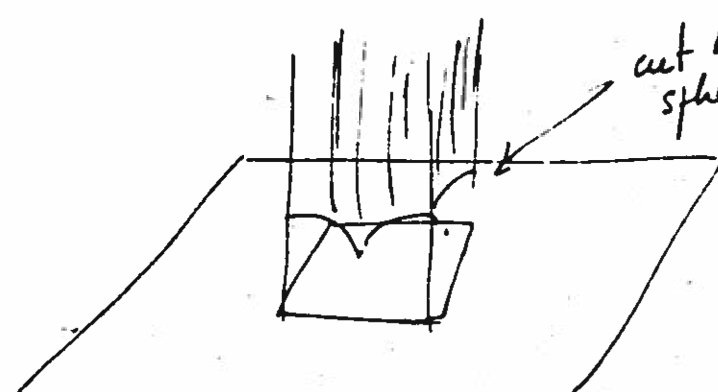
In our case, $SL_2(R) \subset SL_2(\mathbb{C})$

$\searrow$ acts on 3-dim'l hyperbolic space



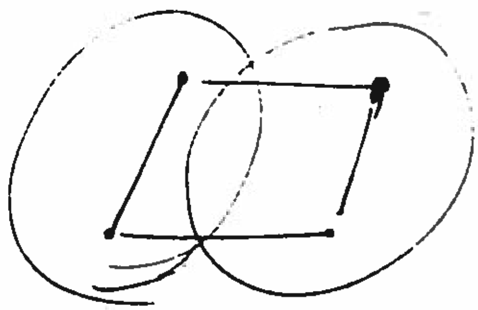
$$|z_1 + \underset{\mathbb{C}}{\underset{\cap}{\alpha}} z_2|^2 + \underset{\mathbb{R}}{\underset{\cap}{\lambda}} |z_2|^2$$

Fund. domain looks like:



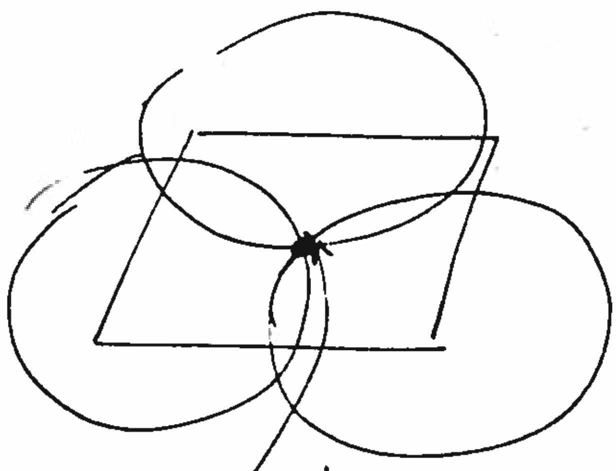
cut by spheres $\rightarrow$

So draw the fund. domain + the equators of the spheres



would have cl # = 1

(only cusp = ∞)



cusp!

Bianchi has such pictures for Clw discriminant.

2nd proof (of nonexistence if $d = -3, -4, -7$)

Idea: if such an indec. P existed, it would create a curve with strictly negative number of pts over some $\mathbb{F}_q$.

E.g., suppose $\mathbb{Z}[i]$ had such P.

$\pi = 2+i$ can be Frob of curve$/\mathbb{F}_5$, genus 1.

$P \longrightarrow \exists C/_{\mathbb{F}_5}$ $g = 2$, with Frob $\pi, \bar{\pi}$ twice.

$\therefore$ $N = 1 + 5 - 2(\pi + \bar{\pi}) = 6 - 8 = -2$ S

• $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$

Take $\pi = \frac{3+\sqrt{-7}}{2}$ $\quad /\mathbb{F}_4$

$(N\pi = 4)$

P gives $C/\mathbb{F}_4$ $\quad N = 1+4-2(\pi+\bar{\pi}) = 5-6 = -1$.

• $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

$\pi = \frac{5+\sqrt{-3}}{2}$ $\quad /\mathbb{F}_7$

$(N\pi = 7)$

get C w/ $N = 1+7-2(\cdot 5) = -2$. ∎

How to construct P in the other cases:

$\mathbf{P}$ = category of modules as above...

<u>Lemma</u>: Let P be such a [redacted] module: $P \in \mathbf{P}$. Let $e \in P$, primitive and with $e\cdot e = 2$. Then either P is indec.

or $P \cong R \oplus R$ with herm. form $\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

Pf: Suppose $P = Q_1 \oplus Q_2$, Q_i rk 1.

Then $e = q_1 + q_2$ $\qquad 2 = e\cdot e = q_1\cdot q_1 + q_2\cdot q_2$

(orthog. decomp!)

$\therefore$ either $q_1 \cdot q_1 = q_2 \cdot q_2 = 1$ and then q_1, q_2 gen Q_1, Q_2 and we have $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

or $e = q_1$ & $q_2 = 0$. This cannot occur, since

e is primitive, and would generate Q_1 so $\operatorname{disc} Q_1 = 2$ and $\operatorname{disc} P = \operatorname{disc} Q_1 \cdot \operatorname{disc} Q_2 \neq 1$.

$e \cdot (\lambda e + \mu) = 2\lambda$ is also a contradiction. ☒

<u>Lemma 2</u>: Let e, P be as in Lemma 1, and $f \in P$ such that

a) $e \cdot f \notin \mathbb{Z}$

b) [redacted] $f \cdot f = z_1 \bar{z}_1 + z_2 \bar{z}_2$ with $z_1, z_2 \in R$

$$\Downarrow$$

$$z_1, z_2 \in \mathbb{Z}.$$

Then P is indecomposable.

Pf: P dec $\longrightarrow P = R \oplus R$ with $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ by Lemma 1

and $e = (1, 1)$ (by the proof)

Say $f = (z_1, z_2)$.

Then $f \cdot f = z_1 \bar{z}_1 + z_2 \bar{z}_2 \longrightarrow z_1, z_2 \in \mathbb{Z}$ by (b).

But $e \cdot f = z_1 + z_2 \in \mathbb{Z}$ contradicting (a). ☒

Now it remains to write down some matrices $\begin{pmatrix} 2 & \alpha \\ \bar{\alpha} & \mu \end{pmatrix}$ under these conditions (μ will give the conditions on f, of course).

12/3 $g=2$ (the end)

We were looking at binary hermitian forms, (pos. def. disc. 1) on $R = R_{-d}$, order in an imag. quad. field.

(We know $d \equiv 0$ or $3 \pmod 4$, $d > 0$,

and R_{-d} has basis over $\mathbb{Z}$: 1 and either $\begin{cases} \sqrt{-d/4} & \text{if } d \equiv 0 \ (4) \\ \frac{1+\sqrt{-d}}{2} & \text{if } d \equiv 3 \ (4) \end{cases}$

We want to prove: if $d \neq 3, 4, 7 \Rightarrow \exists$ indec. binary herm. forms

Lemmas above: P proj hermitian module

1) $e \in P$, $e \cdot e = 2$, primitive

$\Rightarrow$ either P indec

or $P = R_{-d} \oplus R_{-d}$, $e \mapsto (1,1)$

2) $\exists f$, $f \in P$, s.t. $e \cdot f \notin \mathbb{Z}$ and $f \cdot f = z_1\bar{z}_1 + z_2\bar{z}_2$, $z_i \in R$, $\Rightarrow z_1, z_2 \in \mathbb{Z}$ $\Longrightarrow$ P indec.

Cases

① $d \equiv 0 \pmod 8$, $P = R \oplus R$

[In cases ① – ③, $P = R \oplus R$, matrix in
$$\begin{pmatrix} 2 & \alpha \\ \bar\alpha & \mu \end{pmatrix} \qquad e = (1,0) \quad f = (0,1)$$
$2\mu - \alpha\bar\alpha = 1$]

$$\alpha = 1 + \sqrt{-d/4}$$

so $\alpha\bar\alpha = d/4 + 1 \equiv 1 \mod 2$

so $\mu = \frac{1+\alpha\bar\alpha}{2} = 1 + \frac{d}{8}$.

Then $e \cdot e = 2$, primitive

$e \cdot f = \alpha \notin \mathbb{Z}$

$f \cdot f = \mu = 1 + \frac{d}{8}$

$$N\left(x + y\sqrt{\tfrac{-d}{4}}\right) = x^2 + \frac{d}{4}y^2 \geq \frac{d}{4} \text{ if } y \neq 0$$

But $\frac{d}{4} > 1 + \frac{d}{8}$ unless $d = 8$.

So if $d > 8$, P is indec.

If $d = 8$, $\begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}$

is indec, since $z \cdot z$ is even for any z.

② $d \equiv 4 \pmod 8$

take $\begin{cases} \alpha = \sqrt{\frac{-d}{4}} \\ \mu = \frac{1+\alpha\bar{\alpha}}{2} = \frac{1}{2} + \frac{d}{8} \end{cases}$ and check as before.

③ $d \equiv 3 \pmod 8$

take $\begin{cases} \alpha = \frac{1+\sqrt{-d}}{2} \\ \mu = \frac{5+d}{8} \end{cases}$, so $\alpha\bar{\alpha} = \frac{1+d}{4}$.

again as before.

$[d \neq 7]$

④ $d \equiv 7 \pmod 8$

This implies $h(-d) > 1$: 2 splits as $\mathfrak{p}\bar{\mathfrak{p}}$, i.e. :

$$R_{-d} \otimes \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad (*)$$

$(*)$: if $x = \frac{1+\sqrt{-d}}{2}$, x satisfies $x^2 - x + \frac{1+d}{4} = 0$.

Mod 2 : $x^2 - x \equiv 0 \pmod 2$

and this splits mod 2

And then one checks that $\mathfrak{p}$ is not principal.

If it were, $\exists \alpha \in R$ s.t. $\alpha\bar{\alpha} = 2$; but $d > 7$ so this can't be.

Choose an inv. ideal $\mathfrak{a}$, not principal (e.g., $\mathfrak{p}$).

Now take $P = R + \mathfrak{a}$ (not free).

A hermitian form on P is given by a matrix

$\begin{pmatrix} \lambda & \alpha \\ \bar\alpha & \mu \end{pmatrix}$ $\left[\begin{array}{l} \lambda \in \mathbb{Z} \quad , \alpha \in \frac{1}{N\mathfrak{a}}\mathfrak{a} \; , \; (\bar\alpha \in \frac{1}{N\mathfrak{a}}\bar{\mathfrak{a}}) \\ \mu \in \frac{1}{N\mathfrak{a}}\mathbb{Z} \end{array}\right.$

herm form is $\lambda z_1 \bar z_1 + \alpha \underbrace{z_1 \bar z_2}_{\in \bar{\mathfrak{a}}} + \bar\alpha \bar z_1 z_2 + \mu z_2 \bar z_2$

with $z_1 \in R$, $z_2 \in \mathfrak{a}$

$\bar{\mathfrak{a}}\mathfrak{a} = N\mathfrak{a}$.

So if $\alpha \in \frac{1}{N\mathfrak{a}}\mathfrak{a}$, ok!

To check: form is $R \oplus \mathfrak{a} \longrightarrow R \oplus \bar{\mathfrak{a}}$, so get conditions

"det = 1" means $(\lambda\mu - \alpha\bar\alpha) N\mathfrak{a} = 1$

Take $\lambda = 2$ to have a vector of length 2.

<u>Claim</u>: $\exists \alpha \in \frac{1}{N\mathfrak{a}}\mathfrak{a}$, $\exists \mu \in \frac{1}{N\mathfrak{a}}\mathbb{Z}$ s.t. $(2\mu - \alpha\bar\alpha)N\mathfrak{a} = 1$

Write $\alpha = \frac{1}{N\mathfrak{a}} z$, $z \in \mathfrak{a}$, $\mu = \frac{m}{N\mathfrak{a}}$, and then we want

$$2m - \frac{z\bar z}{N\mathfrak{a}} = 1 .$$

So we want: $\exists z \in \mathfrak{a}$ s.t. $\frac{z\bar z}{N\mathfrak{a}} \equiv 1 \pmod 2$.

Choose z a local generator at α (since locally principal!).

Then by Lemma 1, we are done, since P is <u>not</u> free. $\blacksquare$

[For ternary herm. forms, bad rings should be $d = -3, -4, -8, -11$; still can't prove those are all the bad rings.]

E ell. curve, $R = \mathrm{End}(E)$

* We associated $A = P \otimes_R E$.

Then

form indec $\Longrightarrow$ A indec, pol. deg 1

For $g = 2$ $\Longrightarrow$ <u>curve</u>.

* Which A's are of the form $P \otimes_R E$?

[Suppose we want to prove:
For $q = 13$, $g = 2$, $N \neq 28$.

If $N = 28$, should have $\pi = \dfrac{-7 \pm \sqrt{-3}}{2}$ twice,

which corresp to E with $R = R_{-3}$.

Then $\mathrm{Jac}(C) \cong P \otimes E$ for some P

polariz on Jac $\longrightarrow$ $\underbrace{\text{herm. form on } P, \text{ indec.}}_{\text{contradiction!}}$]

by what we'll prove!

__Assume__: E ordinary, $R = \mathrm{End}\, E$, R maximal order.

[if R not max. order, should use R is a __Gorenstein__ ring]

Let A be an abelian variety on which R acts, isogenous over fin. field to $\underbrace{E \times E \times \cdots \times E}_{g}$.

__Thm__: Then $A \cong P \otimes_R E$, with $P = \mathrm{Hom}_R(E, A)$,

and P is projective.

Pf: A is isogenous to $L \otimes E$ $\quad$ L free R-module.

$A \longrightarrow L \otimes E$ isogeny.

primes dividing order of kernel ?

a) $\ell \neq$ char.

Use
$$\begin{array}{ccc} V_\ell(A) & = & V_\ell(L \otimes E) \\ \cup & & \cup \\ T_\ell A & \hookrightarrow & T_\ell(L \otimes E) \end{array}$$

and $\ell \mid$ order of kernel $\Rightarrow$ lattices are different

View $L \subset K^g$

$L \subset P \subset K^g$ corresp to: for finitely many ℓ
$L \otimes R_\ell \subset P \otimes R_\ell$

Same for $P \subset L \subset K^g$.

So choose $P \subset L$ s.t. $P_\ell = P \otimes \mathbb{Z}_\ell = T_\ell A$

Then we'll have $T_\ell A = T_\ell(P \otimes E)$ so OK at ℓ.

Since we have A ordinary, it has a $T_p A$, free of rank $2g$ over $\mathbb{Z}_p$

$$T_pA = (\text{naïve } T_p) \oplus (\mathbb{Z}_p\text{-dual of } T_p^{(1)}(\text{dual of } A))$$

$$\underbrace{T_p^{(1)}(A) \text{''} \; \varprojlim \text{''} A[p^n]}_{\text{rk } g}$$

One proves that this T_pA satisfies the same formalism as before.

[For general A, must add $\oplus$ piece coming from Witt-vector cohomology]

Note: for ordinary E, $R_p = \mathbb{Z}_p \oplus \mathbb{Z}_p$

This gives a proof. $\boxtimes$

Skolem Method

We needed to consider $p^n = \begin{cases} x^2+1 \\ x^2+x+1 \\ x^2+x+2 \end{cases}$

n odd ≥ 3.

List: $\begin{cases} \text{none for } x^2+1 \\ 7^3 = 18^2+18+1 \\ 2^3 = 2^2+2+2 \\ 2^5 = 5^2+5+2 \\ 2^{13} = 90^2+90+2 \end{cases}$

So look at equations $\begin{cases} y^n = x^2+1 \\ y^n = x^2+x+1 \\ 2^n = x^2+x+2 \end{cases}$ $\begin{cases} y > 1 \\ n \text{ odd } \geq 3 \end{cases}$

Claim: no other solutions than listed above.

(1) $y^n = x^2+1$: Lebesgue
(2) $y^n = x^2+x+1$: Nagel + Ljunggren
(3) $2^n = x^2+x+2$: Nagel

Cf. Mordell, *Diophantine Equations* (Proofs for (1) + (3), refs.

②: Nagel: $y^n = x^2+x+1 \implies n \equiv 0 \pmod 3$ (easy; Nagel reduces to $y=13$. Then must show $13^n \neq x^2+x+1$ gives wrong argument, can be corrected.)

Once $3|n$, look at $y^3 = x^2+x+1$, and show integral points are $\begin{cases} y=1, & x=0 \text{ or } -1 \\ y=7, & x=90 \text{ or } -91 \end{cases}$ (Ljunggren)

Simpler proof: Tzanakis, J. Numb. Th 18 (1984)

We give a proof for case ③: $2^n = x^2+x+2$.

Note: $4\cdot 2^n = 4\cdot x^2 + 4\cdot x + 1 + 7$

$$= (2x+1)^2 + 7$$

So work in R_{-7}, set $\omega = \frac{1+\sqrt{-7}}{2}$, so $\begin{cases} \omega+\bar\omega = 1 \\ \omega\bar\omega = 2 \end{cases}$

(So $\omega^2 - \omega + 2 = 0$).

And our equation is $\boxed{\omega^n\bar\omega^n = (x+\omega)(x+\bar\omega)}$

Can replace x by $-1-x$, so choose x even. Se 62

$(\omega) = \gamma$, $2 = \gamma\bar{\gamma}$.

So we must have $x+\omega = \gamma^i \bar{\gamma}^j$ $i+j = n$

And $2 \nmid x+\omega$. If $i,j \geq 1$, $x+\omega$ div by $\gamma\bar{\gamma} = 2$, no!

So $x+\omega = \pm\omega^n$ or $\pm\bar{\omega}^n$

x even $\Longrightarrow$ $x+\omega = \pm\bar{\omega}^n$ is impossible.

So $x+\omega = \pm\omega^n$

Now $\omega^n - \bar{\omega}^n = \pm(\omega - \bar{\omega})$

sign is $-$: in $R/\omega^2 R = \mathbb{Z}/4\mathbb{Z}$

$\bar{\omega} \longrightarrow -1$

$\omega \longrightarrow 2$

$\omega^2 \longrightarrow 0$

So image of eqn is

$0 - (-1)^n = \pm(2+1)$

n odd : $1 = \pm(2+1)$

so have $-$.

So $\omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$

So $\boxed{\omega^n = -x - \omega}$

In $R = \mathbb{Z} + \mathbb{Z}\omega$

$\omega^n = a_n + b_n \omega$

Question is: do we get $b_n = -1$?

We do for $n = 3, 5, 13$. Claim: no others.

<u>Skolem's method</u>:

Look at $\omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$ as an eqn for n, and interpret p-adically.

[Works for $p = 29, 37, 43, 71, 79, 109, 191 \cdots$]

We take $p = 7$, but

Take $K = \mathbb{Q}(\sqrt{-7})$, $\hat{K}$ = completion at the prime $/7$

$v : \hat{K}^* \longrightarrow \mathbb{Z}$

$\pi = \sqrt{-7}$, $v(\pi) = 1$
$v(7) = 2$, so $e = 2$.

We want to think of the eqn. with $n \in \mathbb{Z}_7$, if possible.

$\omega \in U_{\hat{K}}$, but is not $\equiv 1 \mod \pi$

Residue field is $\mathbb{F}_7^*$, and ω has order 6.

So we must work with <u>$n \mod 6$</u>.

Cases: $\left\{ \begin{array}{l} n \equiv 1 \pmod 6 \\ n \equiv 3 \ (\ " \ ) \\ n \equiv 5 \ (\ " \ ) \end{array} \right.$

[our examples are 3, 5, 13 ; one in each case!]

To be proved: in each case, there exists at most **one** value n s.t.

$$\omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$$

Let n_0 = one solution, so $n = n_0 + 6t$

$$\omega^{n_0} \omega^{6t} - \bar{\omega}^{n_0} \bar{\omega}^{6t} = -(\omega - \bar{\omega})$$

Now $\omega^6 \equiv 1 \pmod \pi$

$$\omega = \frac{1+\pi}{2}, \text{ so } \alpha = \omega^6 = \frac{(1+\pi)^6}{2^6} = \frac{1+6\pi+\cdots}{2^6}$$

mod 7, $2^6 \equiv 1$, $6 \equiv -1$

So get $\alpha \equiv 1 - \pi \pmod{\pi^2}$ (note $7 \sim \pi^2$)

So our equation is $\boxed{\underbrace{\omega^{n_0} \alpha^t - \bar{\omega}^{n_0} \alpha^t}_{\|} = -(\omega - \bar{\omega})}$

Now take $t \in \mathbb{Z}_7$ $f(t)$ analytic

We want to solve $f(t) = \text{const.}$

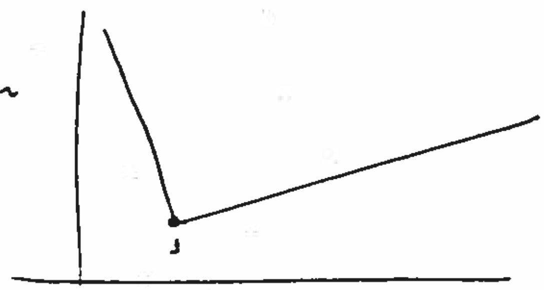
$\therefore$ only finitely many solutions.

So expand $f(t)$ in a power-series

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots \qquad v(a_0) \geq 0$$

if we can show $v(a_1) = 1$, $v(a_n) \geq 2$ for $n \geq 2$
then we have at most one solution.

Newton polygon



Or: know one solution, so choose n_0 s.t. $a_0 = 0$;
divide by t

$$f(t) = t(1 + \underbrace{- - -}_{v(\ ) \geq 0}) .$$

$$\alpha^t = e^{t \log \alpha} , \text{ so } \quad a_n = \omega^{n_0} \frac{(\log \alpha)^n}{n!} - \bar{\omega}^{n_0} \frac{(\log \bar{\alpha})^n}{n!}$$

$\alpha = 1 - \pi \mod \pi^2$

$\therefore \log(\alpha) \equiv -\pi \mod \pi^2$ so $v(\log \alpha) = v(\log \bar{\alpha}) = 1$.

So $v(a_1) \geq 1$, $v(a_2) \geq 2$, ..., $v(a_6) \geq 6$

For $n = 7$ $\quad v(a_7) \geq 7 - 2 = 5$, etc.

So $v(a_n) \geq 2$, $n \geq 2$

So only thing to check is $v(a_1) = 1$ (i.e., no cancellations).

$$a_1 = \omega^{n_0}(-\pi) + \bar{\omega}^{n_0}(\bar{\pi}) \mod \pi^2 \qquad \bar{\pi} = -\pi$$

$$= -\pi(\omega^{n_0} + \bar{\omega}^{n_0}) \mod \pi^2$$

<u>Claim</u>: $\omega^{n_0} + \bar{\omega}^{n_0} \not\equiv 0 \mod \pi$

Now $\bar{\omega} \equiv \omega \mod \pi$

So $\omega^{n_0} + \bar{\omega}^{n_0} \equiv 2\omega^{n_0} \pmod{\pi}$, done!

<u>Remarks</u>: * don't really need analytic fcts

* could use binomial expansion.

* we were helped by there being no unit in the field; if there were a unit, would get

$$\omega^n - \bar{\omega}^n = (\text{unit})^m (\omega - \bar{\omega})$$

and then we'd need more equations.

<u>Other primes</u> take p, $\left(\frac{p}{7}\right) = 1$.

* We need, mod p, $\omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$ only for 3, 5, 13

* need $v(a_1) = 1$.

12/5 <u>$g=3$</u> — see table of (q, N) (p. Se64b)

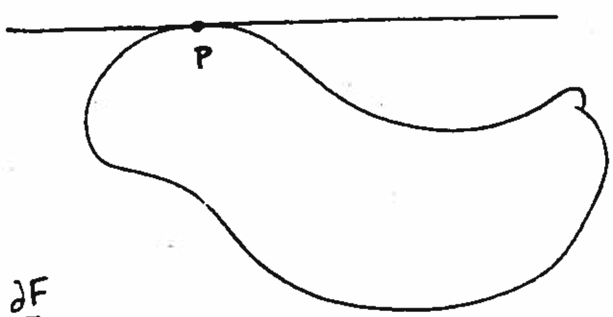
<u>Volock's bound</u> (for $g=3$)

$N \leq 2q + 6$, except for "special cases"

<u>Assume not hyperelliptic</u> (if hyperelliptic, $N \leq 2q+2$).

$\therefore$ curve is a nonsingular quartic in plane, so given by

$F(x,y) = 0$ or $F_4(x,y,z) = 0$



Write equation

"Frob of $P \in$ tgt at P"

in homog. coords:

$F'_x = \frac{\partial F}{\partial x}$

$$G = X^q F'_X + Y^q F'_Y + Z^q F'_Z = 0$$

"<u>Special" if F divides</u> G (i.e., Frob $P \in$ tgt at P for every P).

If not special, the number of inters. of $F=0$ & $G=0$ is $4(q+3)$.

If $P=(x,y,z)$ is a <u>rational</u> point, it clearly is in the intersection; moreover, the two curves are <u>tangent</u> at such a point, so each rat'l point counts at least twice.

$\boxed{g=3}$ **Maximum number of points** $2g+$

$q=2$; $N=7$: twisted Klein curve, $\Sigma x^4+\Sigma x^2y^2+x^2yz+xy^2z=0$

$q=3$; $N=10$: $y^3-y=x^4-x^2$

$q=4$; $N=14$: Klein curve $\Sigma x^4+\Sigma x^2y^2+\Sigma x^2yz=0$ 14

$q=5$; $N=16$: $x^4+y^4=2z^4$ 16

$q=7$; $N=20$: cubic covering $t^3=y-x^2+xy$ of the elliptic curve $y^2-y=x^3-x^2$ 20

$q=8$; $N=24$: Klein curve false 22

$q=9$; $N=28$: Klein curve = Fermat curve $(x^4+y^4+z^4=0)$ 24

$q=11$; $N=28$: $x^4+y^4+z^4+2(3x^2y^2+4y^2z^2+4z^2x^2)=0$ 28

$q=13$; $N=32$: Fermat curve 32

$q=16$; $N=38$; biquadratic extension of $\mathbb{F}_{16}(x)$ defined by 38

$y^2+y=x+\frac{\rho}{x}$; $y^2+y=x+\frac{\rho^2}{1+x}$ where $\rho\in\mathbb{F}_4-\mathbb{F}_2$

$q=17$; $N=40$: $x^4+y^4+z^4+4y^2z^2=0$ 40

$q=19$; $N=44$ 44

$q=23$; $N=48$: $x^4+y^4+z^4-5(x^2y^2+y^2z^2+z^2x^2)=0$

$q=25$; $N=56$: Klein curve

$q=27$; $N=$?

$q=29$; $N=$?

?

?

Voloch bound

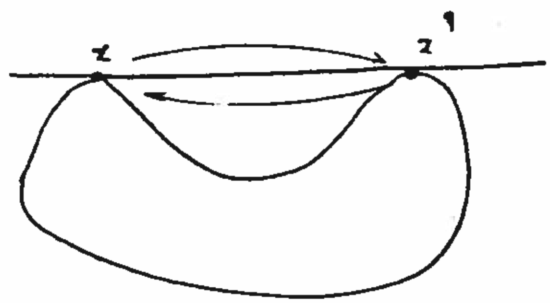
(This list is not entirely garanteed.)

J-P.S.

Harvard, dec. 85

Therefore $N \le 2(q+3) = 2q+6$.

<u>Example</u>:



x of deg 2 on a bitangent then $x \in$ intersection

Similarly, could have a triangle.

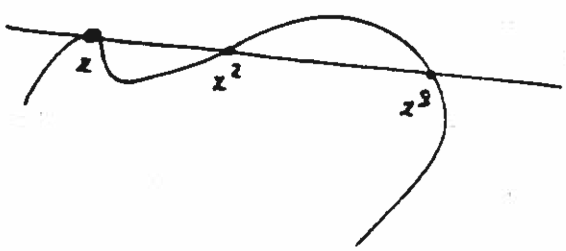
<u>Special curves</u>:

Klein curve in char. 2 / $\mathbb{F}_2$ or / $\mathbb{F}_8$

$$Sx^4 + Sx^2y^2 + Sx^2yz = 0$$

($Sx^4 = x^4+y^4+z^4$, etc.)

Check:



for any x

Can write the polynomial as
$$\frac{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^8 & y^8 & z^8 \end{vmatrix}}{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^4 & y^4 & z^4 \end{vmatrix}}$$

(and then it's obvious that x, x^2, x^8

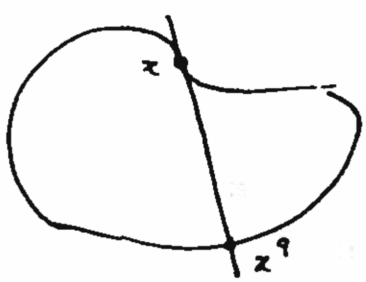
Eqn of tgt at [redacted] (x,y,z) is:

$$X \begin{vmatrix} y^2 & z^2 \\ y^8 & z^8 \end{vmatrix} + Y \cdot \begin{vmatrix} & \\ & \end{vmatrix} + Z \cdot \begin{vmatrix} & \\ & \end{vmatrix} = 0$$

<u>Another check</u> $x + x + x^2 + x^8 \sim$ trivial divisor

So shd have $2 + \pi + \pi^8 = 0$ on Jac.

Klein curve over $\mathbb{F}_3$ is special over $\mathbb{F}_9$.
$\shortparallel$
Fermat $x^4 + y^4 = z^4$



Then: every tgt is inflection tangent, and other inters. is x^9.

Write equations to check.

Tangent is $Xx^3 + Yy^3 + Zz^3 = 0$

at x^9: $x^{12} + y^{12} + z^{12} \overset{?}{=} 0$,
yes since this is
$(x^4 + y^4 + z^4)^3 = 0$

(char 3 !)

Or check on Jacobian: want $3 + \pi_9 = 0$

$\pi_9 = -3$, which is true.

This is why Voloch's bound fails at 8, 9.

Can prove char $\geq 5 \Rightarrow$ non-special

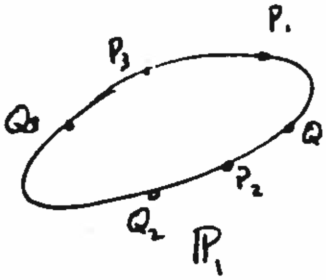
Guess: these are the <u>only</u> special curves.

For $g=2$, we used glueing of elliptic curves, either

$\left\{\begin{array}{l}\text{direct method} \quad \text{"2-glueing"} \\ \text{or} \\ \text{hermitian forms}\end{array}\right.$

For $g=3$, two difficulties:

<u>Elementary glueing</u>



Choose 3 pairs of pts

Make $E_1/\mathbb{P}_1$ ramified at $P_2\,Q_2\,P_3\,Q_3$

$E_2/\mathbb{P}_1$ " " $P_1\,Q_1\,P_3\,Q_3$

Get:
$$\begin{tikzcd}[column sep=small] & k(C) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ k(E_1) \arrow[dr, dash] & k(E_3) \arrow[d, dash] & k(E_2) \arrow[dl, dash] \\ & {} & \end{tikzcd}$$

E_3 ramified only at $P_1\,Q_1\,P_2\,Q_2$

So get C of genus 3, $\mathrm{Jac}(C) \sim E_1 \times E_2 \times E_3$

Consider $\boxed{a x^4 + b y^4 + c z^4 + d x^2 y^2 + e y^2 z^2 + f z^2 x^2 = 0}$

Assume $\Delta \neq 0$

Set $z = 1$: $\quad a x^4 + b y^4 + c + d x^2 y^2 + e y^2 + f x^2 = 0$

Set $Y = y^2$

$$a x^4 + b Y^2 + c + d x^2 Y + e Y + f x^2 = 0$$

$$\Downarrow$$

$$Y^2 = \lambda X^4 + \mu X^2 + \nu$$ which is an elliptic curve.

doing w/ each variable, get 3 curves.

Or look at it as a group of type $(2,2)$ acting by $(x, y, z) \longrightarrow (\pm x, \pm y, \pm z)$.

E.g., to get three times the same curve E, we find

$$x^4 + y^4 + z^4 + 2a(x^2 y^2 + y^2 z^2 + z^2 x^2) = 0$$

So choose a to get the curve E.

E.g. for 11, 17 $\quad$ 2 of one kind, 1 different
for 23 $\quad$ 3 of the same

For $q = 23$

Voloch bound doesn't work. (gives 52)

$m = [2\sqrt{23}] = [\sqrt{92}] = 9$

$m^2 - 4q = -11.$

Weil gives $N \leq 1 + q + 3m = 51$

This is impossible:

$N = 51$ only if Jac $\sim E \times E \times E$ with $m = 9$,
so Frob should be $\pi = \dfrac{-9 \pm \sqrt{-11}}{2}$.

So $R = \mathrm{End}(E) = \mathbb{Z}[\pi] = R_{-11}$.

$\therefore$ Jac $\cong E \times E \times E$ + polariz. $\longleftrightarrow$ indec. herm. forms as before, of rk 3.

Kneser: No such form over R_{-11}.

$1 + q + 3m - 1 \longrightarrow$ down by 1 is impossible for $g = 3$

$1 + q + 3m - 2 = 49$ pts? $\underbrace{\text{down by 2, genus 3}}$

only case is $m, m, m-2$

that would mean Jac $\sim E \times \bar{E} \times E'$

E w/ $\pi = \dfrac{-9 \pm \sqrt{-11}}{2}$

$-7 \pm \sqrt{-4}$[illegible]

<u>Claim</u>: no such thing exits.
(Problem: Jac is only <u>isogenous</u> to $E \times E \times E'$).

Let $\varphi = F + V = \pi + \bar{\pi}$

J_9 = conn comp of $\mathrm{Ker}(\varphi + 9)$

J_7 = ——— $\mathrm{Ker}(\varphi + 7)$

$J_9 \cong E \times E$ is<u>omorphic</u>

$J_7 \cong E'$

$J_9 \cap J_7$ <u>killed</u> by 2

So $J = J_9 \times J_7 / \Delta$ $\Delta \subset E'[2]$

so Δ of type $1, (2)$ or $(2,2)$

$1 \to$ Jac = product $\to$ polariz. splits $\to$ no.

$(2) \to$ also can't be

$(2,2)$

polariz of deg 1 on J gives a polariz on $J_9 \times J_7$, of degree 4.

Again, this splits; only interesting case is deg 2 on J_9, deg 2 on J_7.

So need polariz of deg 2 on J_q.
J_q has CM by R_{11}, so want

$$\begin{pmatrix} \lambda & \alpha \\ \bar{\alpha} & \mu \end{pmatrix} \qquad \begin{cases} \lambda\mu - \alpha\bar{\alpha} = 2 \\ \lambda > 0 \\ \text{coeff} \in R_{-11} \end{cases}$$

Theorem: only case is $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

But then J_q splits: $J = E \times E \times E'/\Delta$, and the whole J splits, which is not possible. $\boxed{V}$

$\underline{q=19}$ Voloch bound gives 44.

$$\left[\begin{array}{l} m = [2\sqrt{19}] = [\sqrt{76}] = 8 \\ m^2 - 4q = -12 \end{array}\right.$$

$1 + 9 + 3 \cdot 8 = 44$

So I want to prove m, m, m is possible.
So take E w/ $\pi = -4 \pm \sqrt{-3}$
Want Jac $\sim E \times E \times E$.

Look for a hermitian module for $\overset{R=}{\mathbb{Z}[\pi]} = \mathbb{Z}[\sqrt{-3}] \subsetneq$ max.

Form is
$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1+\sqrt{-3} \\ 1 & 1-\sqrt{-3} & 3 \end{pmatrix} \quad \text{on} \quad R \oplus R \oplus R.$$

To show indec., go to $\tilde{R} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. There it is decomposable, so look at the lattice in $\tilde{R} \times \tilde{R} \times \tilde{R}$, and check: there is no vector of length 1.

Take $A = P \underset{R}{\otimes} E$.

Use:

Thm (Oort + ______):

A principally polarised ab. variety of dim 3, indec., is a jacobian over a quad. extension.

1) If C hyperelliptic, then C can be chosen $/k$ s.t. $\mathrm{Jac}\, C \cong A/k$

2) If C not hyperelliptic, then $\exists\ C/k$ unique + a quad twist $\varepsilon : \mathrm{Gal}(E/k) \longrightarrow \pm 1$ s.t. $\mathrm{Jac}\, C \cong A$ (twisted by ε).

---

over a finite field, Frob of C is either $\begin{cases} \text{Frob of } A \\ \text{or} \\ -\text{Frob of } A \end{cases}$

So curve will have either 44 or $1+19-38=-4$ points, so it has 44 pts.

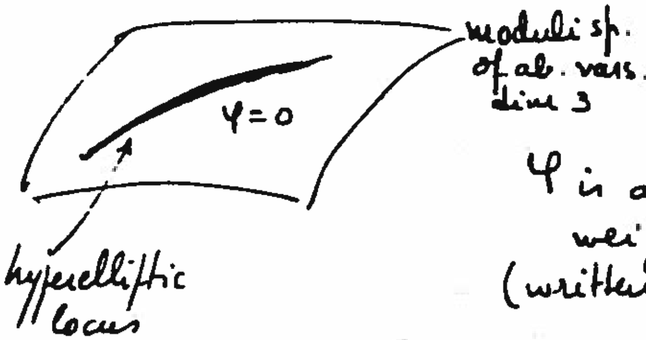
So E ell. curve, $R = \mathrm{End}(E)$, take P herm. module as usual.

Make $A = E \otimes_R P$

Cont + — = this is a jacobian.

① Is C hyperelliptic?

Given g_2, g_3 (P herm. module) $\longrightarrow$ hyperelliptic?



ψ is a mod form on Siegel space, weight 18
(written in Igusa on genus 3)

$$\text{mod form on Siegel space (dim 3)}\Big|_{CM \otimes_R \text{hermitian modules}} = ?$$

② If C not hyperelliptic ($\psi \neq 0$), find $\varepsilon = "\sqrt{\psi}"$.

Igusa says: Klein noticed:
take Δ of a plane quartic

$$\psi = \prod_{36} \vartheta.$$

or put $\varphi = c\prod_{36} \vartheta$.

Suppose $c = 1$; then φ "is" the twist.

Reformulation:

the twist A_ε (A twisted by ε) can be written
$$A_\varepsilon = P \otimes E_\varepsilon$$

Start with P; look at all E_ε deduced from E by a quad. twist.

Then P determines a well-defined E_ε among all those, the unique one s.t. $P \otimes E_\varepsilon = \mathrm{Jac}(C)$.

Example for Gross:

E w/ CM by $\frac{1+\sqrt{-7}}{2}$ $\quad (j = -3^3 5^3)$

Look for P over this R:

P given by $\begin{pmatrix} 2 & \alpha & \bar{\alpha} \\ \bar{\alpha} & 2 & -1 \\ \alpha & -1 & 2 \end{pmatrix}$, $\alpha = \frac{1+\sqrt{-7}}{2}$

Automorphism $= \{\pm 1\} \times \underbrace{G_{168}}_{\text{simple of order 168}}$ $\quad / \mathbb{Q}(\sqrt{-7})$

$P \otimes E = \mathrm{Jac}$ (Klein)

So P selects the E w/ good reduction outside 7.

Klein has potentially good redn. everywhere, but ~~over~~ in char 7, Klein becomes hyperelliptic.

In general, have no way to determine the sign when C is not hyperelliptic.

Define $N_q(3)$ = max nber of points for $g=3$ over $\mathbb{F}_q$.

<u>Conjecture</u>: $|N_q(3) - \text{Weil bound}|$ is bounded when q varies. (say ≤ 6)

(For $N_q(2)$ had $1+q+2m$
$2m-1$
$2m-2$
once $2m-3$).

One would try to do down by 3, $m-1, m-1, m-1$
or down by 6, $m-2, m-2, m-2$.

Take E w/ one of those, $R = R_{-d}$.

$d = 4q - (m-1)^2$

$4q \geq m^2$ so $d \geq 2m-1$

$d >> q^{1/4}$

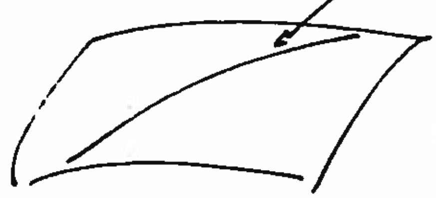
For each such hecu. module, should compute the sign.

Getting + gives curves w/ many pts.

For $g = 4$, would still make same conjecture (in fact for 5, 6, 7, or 8 too)

$A_p = P \otimes E$ pp.

$\Psi = 0$ hypersurface of jacobians



So want $\Psi(A_p) = 0$

So chance is $\frac{1}{q}$. But then quad twist, so chance is $\frac{1}{2q}$ of winning.

But number of P is large.

For very large g, say $g = 100$, jacobians have too large a codimension.

So expect a breaking point between 3 + 10.

For $g=3$, using $x^4 + y^4 + z^4 + 2a(x^2y^2 + y^2z^2 + z^2x^2) = 0$. (C_a)

this has $\mathrm{Jac} \sim E_a \times E_a \times E_a$, E_a: $y^2 = (a^2-1)x^4 + \cdots$

<u>Question</u>: can I choose E for $m-1$, say? I.e., how many pts can this have?

[Added dec. 9, 1985] – A machine computation, made by M. Nitzberg, shows that:

1) for $p = 19, 29, 53, 67, 71, 89$, one may choose a ($a = 3, 13, 0, 14, 36, 20$) such that $N(E_a) = 1 + p + m$, hence $N(C_a) = 1 + p + 3m$: optimal bound!

2) for $p = 7, 13, 23, 43, 47, 61, 79, 97$, one may choose a such that $N(E_a) = 1 + p + (m-1)$, hence $N(C_a) = p + 3m - 2$, which is optimal at least for $p = 7, 13, 23$

Rational Points on Curves over Finite Fields

Part II : "g large"

Jean-Pierre Serre

Lectures given at Harvard University, September to December 1985

Notes by Fernando Q. Gouvêa

Contents - Part II

9/26 Thursday: g large.

Ihara: X genus g / $\mathbb{F}_q$, $g \geq 1$

Suppose $N(X) = q + 1 + 2g q^{1/2}$ (so q is a square).

Then: $g \leq \frac{1}{2}(q - q^{1/2})$

Proof: $N(X) = 1 + q - \sum_{\alpha=1}^{2g} \pi_\alpha$ $\quad |\pi_\alpha| = q^{1/2}$

So we must have all $\pi_\alpha = -q^{1/2}$

So $\pi_\alpha^2 = q$, and if $N_2 = N_2(X) = \#(\mathbb{F}_{q^2})$,

$$N_2 = 1 + q^2 - \sum_{\alpha=1}^{2g} \pi_\alpha^2 = 1 + q^2 - 2gq$$

But $N_2 \geq N_1$, so $1 + q^2 - 2gq \geq 1 + q + 2gq^{1/2}$

$$q^2 - q \geq 2g(q + q^{1/2})$$

so $g \leq \frac{1}{2}(q - q^{1/2})$. $\boxed{\checkmark}$

B. Segre: Curve in $\mathbb{P}_3$ given by $x^{q^{1/2}+1} + y^{q^{1/2}+1} + z^{q^{1/2}+1} = 0$

has genus $g = \frac{1}{2}(q^{1/2})(q^{1/2} - 1) = \frac{1}{2}(q - q^{1/2})$.

and has $N = q^{3/2} + 1 = q + 1 + 2g q^{1/2}$.

So the bound above is exact.

Proof of $N = q^{3/2}+1$ for this curve.

Consider

$$\begin{array}{c} \mathbb{F}_q \\ 2 \Big| \\ \mathbb{F}_{q^{1/2}} \end{array} \qquad x \longmapsto \bar{x} = x^{q^{1/2}}$$

Then the eqn is $x\bar{x} + y\bar{y} + z\bar{z} = 0 \quad x,y,z \in \mathbb{F}_q$.

Hermitian form! Want: how many isotropic vectors?

E.g.: given $y, z \in \mathbb{F}_q$, want to solve

$q_0 = q^{1/2}$

$$x\bar{x} = -\underbrace{(y\bar{y} + z\bar{z})}_{\in \mathbb{F}_{q^{1/2}}} \quad \text{has (in } x\text{)} \begin{cases} 1 \text{ soln. } x = 0 \text{ if } y\bar{y}+z\bar{z}=0 \\ q_0+1 \text{ solns if not} \end{cases}$$

$$\mathbb{F}_q^{\times} \xrightarrow{N} \mathbb{F}_{q^{1/2}}^{\times}$$
$$x \longmapsto x\bar{x}$$

$$y\bar{y} + z\bar{z} = 0 \longrightarrow \begin{cases} y = 0 = z \\ \text{or} \\ z \neq 0 \text{ , } q_0+1 \text{ solns} \\ \binom{q-1}{\text{poss.}} \quad \text{in } y. \end{cases}$$

so $1 + (q_0^2-1)(q_0+1)$ solns

So solns in $\mathbb{F}_q^3$ is $\underbrace{1 + (q_0^2-1)(q_0+1) + (q_0+1)(q_0^4 - 1 - (q_0^2-1)(q_0+1))}_{\text{this}}$

so $N = (\text{this}) - 1 \Big/ (q^2-1) = (q_0+1)(1+q_0^2+1-q_0+1) = (q_0+1)(q_0^2-q_0+1)$

group acts

$g=0$, $q+1$ pts, $\mathbb{P}_1$, PGL_2 (type A_1)

$g=\frac{1}{2}(q-q^{1/2})$, $q^{3/2}+1$, Fermat-type curve, PU_3 (type A_2^2) ($^2A_2$

all odd { q^2+1 Sz $^2B_2$

q^3+1 Ree $^2G_2$

When is the Weil bound attained?

q square.

Then $N = q+1+2gq^{1/2} \implies g = ?$

$g = \frac{1}{2}(q - q^{1/2})$ is a possibility, and is the maximum.

For $0 \leq g \leq \frac{1}{2}(q - q^{1/2})$?

Examples: 1) $q=4$, so $q^{1/2}=2$

The Fermat curve is $x^3+y^3+z^3=0$, so $g=1$, has 9 points

2) $q=9$, so $q^{1/2}=3$, get $x^4+y^4+z^4=0$, $g=3$.

Have curves for $g=1$, $q=9$.

For $g=2$, no such curve!

Would give $N = 1+9+4\cdot 3 = 22$;

but $g=2$ is 2-sheeted cov. of $\mathbb{P}_1$, and $\mathbb{P}_1$ has
$q=9$ $\longrightarrow$ 10 points, so $N \leq 20$.

(In fact, correct bd is 20).

---

3) $q=16$, $q^{1/2}=4$ $\quad x^5+y^5+z^5=0$.

Weil bound is $1+16+2g\cdot 4 = 17+8g$

$g=1 \longrightarrow 25$ OK
$g=2 \longrightarrow 33$ OK
} see table

$g=3 \longrightarrow 41$ not the bound (bound is 38).

$g=4,5$?

$g=6 \longrightarrow$ yes, and the last one.

Suppose X has Weil upper bound $= N(X)$ (or Weil lower bound).

And suppose

$$\begin{array}{c} X \\ \big\downarrow \text{ non-const. morphism.} \\ X' \end{array}$$

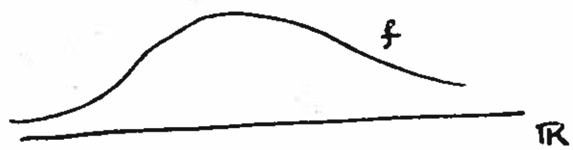
Then same holds for X'.

Trick of Jac's. In X, every eigenvalue is $-q^{1/2}$ or $q^{1/2}$

and $J(X') \hookrightarrow J(X)$ so eigenvalues on $J(X')$ must be a subset of those on $J(X)$, but those are all equal!

Explicit Formulae

Number Fields



and take $\sum f(\log p)$

And we want a fla: $*+\sum f(\log p) = -\sum_{\substack{\tau \text{ zero} \\ \text{of zeta}}} \Phi(\tau) + \Phi(0) + \Phi(1)$

Φ = Fourier / Mellin transform of f

Stark: $*$ includes $\log d$, and choose f, Φ well

Get inequality for d $\longrightarrow$ Stark, Odlyzko, Poitou

---

Notations

X, g, q, π_α eigenvalues of Frob arranged as $\pi_1, \dots, \pi_g, \bar{\pi}$

$$\pi_\alpha = q^{1/2} e^{i\varphi_\alpha}, \quad 0 \le \varphi_\alpha \le \pi$$

$$N_n = \# X(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{\alpha=1}^{g} (\pi_\alpha^n + \bar{\pi}_\alpha^n)$$

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

$Z(T)$ = zeta-fct of X

$$= \exp\left\{ \sum_{1}^{\infty} \frac{N_n T^n}{n} \right\} = \frac{P(T)}{(1-T)(1-qT)}$$

where

$P(T) = \prod^{g} (1-$

$$a_1 = N_1 = N$$

Also if a_d = number of "pts of degree d" of the scheme X.

pt of degree d = orbit of Frob of order d in $X(\overline{\mathbb{F}}_q)$.

Have $N_n = \sum_{d|n} d a_d$ (clear!)

And $Z(T) = \prod_{\substack{p \in X \\ \text{closed pt}}} \frac{1}{1 - T^{\deg p}}$

$$= \prod_{d \geq 1} \frac{1}{(1 - T^d)^{a_d}}$$

Let $f(\theta)$ be a trigonometric polynomial of the form

$$f(\theta) = 1 + 2 \sum_{n \geq 1} c_n \cos n\theta \qquad \text{(finite sum)}.$$

$$= \sum_{n \in \mathbb{Z}} c_n e^{in\theta} \qquad (c_0 = 1,\ c_{-n} = c_n).$$

To f I attach polynomials in t:

$$\Psi_d(t) = \sum_{\substack{n \geq 1 \\ d|n}} c_n t^n$$

"Explicit formula"

$$\boxed{\sum_{\alpha=1}^{g} f(\varphi_\alpha) + \sum_{d\geq 1} d a_d \Psi_d(q^{-1/2}) = g + \Psi(q^{-1/2}) + \Psi(q^{1/2})}$$

$$\sum_{\alpha=1}^{g} f(\varphi_\alpha) = g + 2\sum_{n,\alpha} c_n \cos n\varphi_\alpha$$

$$= g + 2\sum_n c_n \sum_\alpha \cos n\varphi_\alpha$$

$N_n = q^n + 1 - q^{n/2}\sum 2$

so $\sum 2\cos n\varphi_\alpha = \frac{q^n+1}{q}$

$$= \underbrace{g}_{\checkmark} + \sum_{n\geq 1} c_n(\underbrace{q^{n/2}}_{\Psi(q^{1/2})} + \underbrace{q^{-n/2}}_{\Psi(q^{-1/2})} - q^{-n/2}N_n).$$

Need only show that

$$\sum d a_d \Psi_d(q^{-1/2}) \stackrel{?}{=} \sum c_n q^{-n/2} N_n$$

$$\stackrel{?}{=} \sum c_n q^{-n/2} \sum_{d|n} d a_d$$

$$\sum d a_d \sum_{d|n} c_n q^{-n/2}$$

so OK. ▨

<u>Examples</u>:

i) $f = 1$: $c_n = 0 \quad n \geq 1$, $\psi_d = 0$

Get $g = g$.

ii) $f = 1 + \cos\theta$ $\qquad c_1 = \frac{1}{2}$, $c_n = 0 \quad n \geq 2$.

$\psi_1 = \psi = \frac{1}{2} t$

$\psi_n = 0 \qquad n \geq 2$

Then:

$$g + \sum_\alpha \cos\varphi_\alpha + N \tfrac{1}{2} q^{-1/2} = g + \tfrac{1}{2} q^{-1/2} + \tfrac{1}{2} q^{1/2}$$

$\times 2q^{1/2}$:

$$q^{1/2} \sum_\alpha 2\cos\varphi_\alpha + N = 1 + q$$

so $\boxed{N = q + 1 - q^{1/2} \sum_\alpha 2\cos\varphi_\alpha}$ is Weil's formula.

<u>Assumptions</u> : (1) $f(\theta) \geq 0$ for all θ

(2) $c_n \geq 0$ for all n

Abbreviate: "f is doubly positive", $f \gg 0$.

Examples: $f = 1$, $f = 1 + \cos\theta$

Now if $f \gg 0$,

$$\underbrace{\sum f(\varphi_a)}_{\geq 0} + \sum_{d \geq 1} d \underbrace{a_d}_{\geq 0} \underbrace{\Psi_d(\ )}_{\geq 0}$$

So in that case one gets

$$\sum_{d \geq 1} d a_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{-1/2}) + \Psi_1(q^{1/2})$$

Taking only $d=1$ $(a_1 = N)$, get $N\Psi_1(q^{-1/2}) \leq g + \Psi(q^{-1/2}) + \Psi_1(q^{1/2})$

so $$\boxed{N-1 \leq \frac{g + \Psi(q^{1/2})}{\Psi(q^{-1/2})}}$$

Now: we want to choose f so that this is optimal.

Also get $$\boxed{g \geq (N-1)\Psi_1(q^{-1/2}) - \Psi(q^{1/2})}$$

One can then do:

① determine (for a given N, q), the "best" bound on g

Solved by Oesterlé (at least for $q \geq 3$)

② Assymptotic results as $g \to \infty$, q fixed.

③ Nice special cases (Suzuki & Ree curves)

④ Numerical bounds, say, for $g=2$.

For $N = q+1$, $N = q^{3/2}+1$ we know

$N = q+1$ $\quad g = 0$

$N = q^{3/2}+1$ $\quad g = \frac{1}{2}(q - q^{1/2})$ $\quad q$ a square

---

For $N = q^2+1$

Choose $f = 1 + \sqrt{2}\cos\theta + \frac{1}{2}\cos 2\theta$

$= \frac{1}{2}(1+\sqrt{2}\cos\theta)^2$ $\quad$ Then $f >> 0$.

Then $\begin{cases} \psi(t) = \frac{1}{2}(\sqrt{2}t + \frac{1}{2}t^2) \\ \psi_2(t) = \frac{1}{4}t^2 \end{cases}$ $\quad N-1 = q^2$

Find $g \geq q^2(\sqrt{2}q^{-1/2} + \frac{1}{2}q^{-1}) - (\sqrt{2}q^{1/2} + \frac{1}{2}q)$

so $\boxed{g \geq \frac{\sqrt{2}}{2}(q^{3/2} - q^{1/2})}$

Is there such a curve?

$$g \overset{?}{=} \frac{\sqrt{2}}{2}\left(q^{3/2} - q^{1/2}\right) = \left(\frac{2q}{2}\right)^{1/2}(q-1) \Rightarrow q = 2^{2f+1}$$

$\Rightarrow$ $2q$ = square

$\leftrightarrow$ Suzuki groups?

<u>Deligne-Lusztig varieties</u> connected to semi-simple groups over $\mathbb{F}_q$ and their <u>twisted</u> forms.

$Sz \leftrightarrow$ " $^2B_2$ " - groups

Take, say, SL_n and Frobenius $x \longmapsto x^{(q)}$

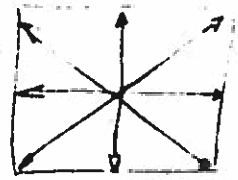
fixed pts give $SL_n(\mathbb{F}_q)$

Now use $x \longmapsto \sigma(x^{(q)})$ σ some outer autom. of the group.

If σ is $u \longmapsto {}^t u^{-1}$, get a different group.

char = 2, B_2 has such a "bad" autom. (not algebraic)

Root system is



(See Tits in Sem. Bourbaki)

Suzuki gps are gps acting on q^2+1 elements, $q = 2^{2f+1}$
Simple if $f \geq 1$. Called [redacted] $Sz(q)$.

$Sz(2) = C_4 \cdot C_5$

$Sz(3)$ is simple.

Deligne & Lusztig

Affine curve with no rat'l pt w/ action of $Sz(q)$.

Pts at ∞ are q^2+1 and give the original representation of $Sz(q)$

Lusztig in Inventiones: genus as given, etc.

Next case: q^3+1

$f = \cos^2\varphi\,(1 + \frac{2}{\sqrt{3}}\cos\varphi)^2 \qquad g \geq \frac{\sqrt{3}}{2}(q^{5/2} - q^{1/2}) + \frac{1}{2}(q^2 - q)$

g integer, $=$ that $\Rightarrow q = 3^{2f+1}$

Have Ree groups.

<u>We had</u>:

<u>10/3</u> X curve $/\mathbb{F}_q$, $\pi_\alpha = q^{1/2} e^{i\varphi_\alpha}$

genus g

$f(\theta) = 1 + \sum_{n \geq 1} 2 c_n \cos n\theta$ (finite sum)

$\Psi_d(t) = \sum_{\substack{n \geq 1 \\ n \equiv 0 \,(\mathrm{mod}\, d)}} c_n t^n$, $\Psi = \Psi_1$

Then $$\sum_{\alpha=1}^{g} f(\varphi_\alpha) + \sum_{d \geq 1} d a_d \Psi_d(q^{-1/2}) = g + \Psi(q^{-1/2}) + \Psi(q^{1/2})$$

a_d = # closed pts. of degree d

$N_n = \sum_{d \mid n} d a_d$ $\qquad N_1 = N = a_1$

If $f >> 0$ (i.e., $f(\theta) \geq 0$ for all θ and $c_n \geq 0$ for all n):

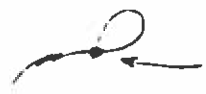
then $$\boxed{\sum d a_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{-1/2}) + \Psi(q^{1/2})}$$

$$\Rightarrow \boxed{(N-1)\Psi(q^{-1/2}) \leq g + \Psi(q^{1/2})}$$

(<u>Today</u>: let $g \to \infty$)

<u>Remark</u>: We proved these inequalities for X projective nonsingular.
For X <u>singular</u>, the bound as stated doesn't work.

x — pt. of deg 2 collapse:



has become rat'l

So should replace q by sth which "sees" the topology.

X (singular) projective, abs. irred., let $B = 1^{st}$ Betti number (for ℓ-adic cohomology, for instance).

Thm: $(N-1)\Psi(q^{-1/2}) \leq B/2 + \Psi(q^{1/2})$

Define the "arithmetic genus" $p_a(X) = \dim H^1(X, \mathcal{O}_X)$

Known: $B/2 \leq p_a(X)$.

So we get $(N-1)\Psi(q^{-1/2}) \leq p_a(X) + \Psi(q^{1/2})$.

Eg: $X \subset \mathbb{P}^2$ plane curve, abs. irred, of degree n.

Then $p_a(X) = \frac{1}{2}(n-1)(n-2)$

Pf (originally was given in terms of $N_n = \cdots$)

Claim: $N_n = 1 + q^n - \sum_{i=1}^{B} \alpha_i^n \qquad |\alpha_i| = 1$ or $q^{1/2}$

h.-Deligne: (Still the Lefschetz formula, except for the wrong size of eigenvalues)

Or: from Weil. $\boxed{A}$

Take $N_n - 1 = q^n - \sum_{i=1}^{B} \alpha_i^n \geq N - 1$

$$\sum_n c_n q^{-n/2}(N_n - 1) = \sum_n c_n q^{n/2} - \sum_{i,n} c_n q^{-n/2}\alpha_i^n$$

So $$(N-1)\Psi(q^{-1/2}) \leq \Psi(q^{1/2}) + \sum_{i,n} c_n q^{-n/2} \alpha_i^n$$

$\therefore$ To be proved : $$-\sum c_n q^{-n/2} \alpha_i^n \leq \frac{B}{2}.$$

or $$\mathrm{Re}\left(-\sum c_n q^{-n/2} \alpha_i^n\right) \leq \frac{B}{2}$$ Since the LHS is real anyway

Consider $\frac{1}{2} + \Psi(t) = F(t)$ polynomial in t

If $t = e^{i\varphi}$, $\mathrm{Re}(F(e^{i\varphi})) = \mathrm{Re}\left(\frac{1}{2} + \sum c_n e^{in\varphi}\right) = \frac{1}{2} f(\varphi) \geq 0.$

So : $\mathrm{Re}(F(t)) \geq 0$ for all t with $|t| = 1$

$\Downarrow$ cx analysis

$\mathrm{Re}(F(t)) \geq 0$ for all t with $|t| \leq 1$.

(apply max princip to $\exp(-F(t))$. Get $|\exp(-F(t))| \leq 1$ for $|t| = 1$, hence for $|t| \leq 1$.)

Now

$$\mathrm{Re}\left(-\sum c_n q^{-n/2} \alpha_i^n\right) = \sum_i \mathrm{Re}\left(\frac{1}{2} - F(q^{-1/2}\alpha_i)\right)$$ and $|q^{-1/2}\alpha_i| \leq 1$

$$\leq \sum_{i=1}^{B} \mathrm{Re}\left(\frac{1}{2}\right) = \frac{B}{2}$$ so QED. $\square$

One can do similar things for higher-dim'l varieties, in odd dimension.

Example: X proj non-sing variety, dim 3, abs. irred.
Assume: $B_1 = 0$, $B_2 = 1$, B_3 "large"
(E.g., any complete intersection)

If X has N points, one can prove

$$\frac{B_3}{2} \geq N\psi(q^{-3/2}) - \left(\psi(q^{-3/2}) + \psi(q^{-1/2}) + \psi(q^{1/2}) + \psi(q^{3/2})\right)$$

(Exercise) (use Deligne — for large N this gives better bounds)

Now: q fixed, $g \to \infty$
we have:

Let $k \geq 1$ be a fixed integer.

Let X^λ be curves of genus $g_\lambda \to \infty$.

$a_d(X^\lambda) =: a_d^\lambda$

Theorem: $\displaystyle \limsup_{g_\lambda \to \infty} \frac{1}{g_\lambda} \sum_{d=1}^{k} \frac{d\, a_d^\lambda}{q^{d/2} - 1} \leq 1.$

Corollary: For $k=1$, $a_1^\lambda = N^\lambda = \# X^\lambda(\mathbb{F}_q)$, and we have

$$\limsup_{g_\lambda \to \infty} \frac{N^\lambda}{g_\lambda} \leq q^{1/2} - 1.$$

(Thm. of Drinfeld-Vladut).

Weil gives $N^\lambda \le 1 + q + 2g^\lambda q^{1/2}$

so $\frac{N^\lambda}{g^\lambda} \le 2q^{1/2} + o(1)$

If $q = 2$, Weil $2q^{1/2} = 2.828$, $[2q^{1/2}] = 2$, But $q^{1/2} - 1 = 0.414$.

Proof of Thm:

We have $\sum_{d=1}^{k} d a_d^\lambda \Psi_d(q^{-1/2}) \le g^\lambda + \Psi(q^{1/2}) + \Psi(q^{-1/2})$

$$\frac{1}{g^\lambda} \sum_{d=1}^{k} d a_d^\lambda \Psi_d(q^{-1/2}) \le 1 + \frac{1}{g^\lambda}(\qquad)$$

$g_\lambda \to \infty$: $\left[\limsup \frac{1}{g^\lambda} \sum_{d=1}^{k} d a_d^\lambda \Psi_d(q^{-1/2}) \le 1.\right]$

true for every Ψ_d coming from an $f >\!\!> 0$.

Lemma: ① If $f >\!\!> 0$, $f = 1 + \sum 2c_n \cos n\theta$, then $c_n \le 1$.

② For any P, any $\varepsilon > 0$, $\exists f$ s.t. $c_n \ge 1 - \varepsilon$ for all $n = 1, 2, \dots, P$.

(So can get f like $1 + 2\cos\theta + 2\cos 2\theta + \cdots =$ "$\sum_{n\in\mathbb{Z}} e^{in\theta}$" = Dirac measure at 0 on the circle

If $c_n = 1$ for all n, then OK, because $\Psi(t) = t + t^2 + \cdots$

$\Psi_d(t) = t^d + t^{2d} + \cdots = \frac{t^d}{t^d - 1} = \frac{1}{t^{-d} - 1}$

and $\Psi_1(q^{-1/2}) = \frac{1}{\quad}$, which gives the theorem.

Then we need only do a convergence argument using the Lemma. $\boxed{//}$

Pf of Lemma :

① $\begin{cases} c_n = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} f(\theta)\cos n\theta \, d\theta \\ \text{and} \\ 1 = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} f(\theta) d\theta \end{cases}$

and since $|\cos n\theta| \leq 1$ we get

$$c_n = \left| \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\cos n\theta \, d\theta \right| \leq \frac{1}{2\pi}\int_0^{2\pi} \{f(\theta)\, |\cos n\theta| \, d\theta \leq 1 .$$

② Given P, ε

P integer ≥ 1, let $t = e^{i\theta}$

Write $$f_P = \frac{1}{2P+1}\left(t^{-P} + t^{-P+1} + \dots + 1 + \dots + t^{P} \right)^2$$

$$f_P(\theta) = \frac{1}{2P+1}\left(1 + 2\cos\theta + \dots + 2\cos P\theta\right)^2 .$$

$$f_P = \frac{1}{2P+1}\left(t^{-2P} + 2t^{-2P+1} + \dots + (2P+1)\cdot 1 + 2P t + \dots + t^{2P} \right)$$

So $$c_n(f_P) = \frac{2P-n+1}{2P+1}$$

for fixed n, $P \to \infty$, $c_n \to 1$. $\boxed{///}$

Ihara's tower theorem

X as usual $/\mathbb{F}_q$, g

S = finite non-empty set of closed points of X

<u>Assumption</u>: There exists a sequence $X^\lambda \to X$ of unramified finite covering of X in which every element of S splits completely and $\deg(X^\lambda \to X) \to \infty$.

Then: $$\boxed{\sum_{P\in S} \frac{\deg P}{q^{\deg(P)/2} - 1} \leq g - 1}.$$

<u>Special case</u>: If all points in S are rat'l ($\deg = 1$) we get

$$|S| \leq (g-1)(q^{1/2} - 1)$$

If $X = \mathbb{P}_1$, $S = \emptyset$, $X^\lambda = X/_{\mathbb{F}_{q^\lambda}}$ constant field extn.

then $\Sigma = 0 \leq 0 - 1$ is false.

So $S \neq \emptyset$ is necessary.

<u>Proof</u>: 1st <u>case</u>: the field of constants of the X^λ is just $\mathbb{F}_q$.

If $n^\lambda = [X^\lambda : X]$ = degree of covering, then $g^\lambda - 1 = n^\lambda(g-1)$
(Cover is unramified!)

$$a_d^\lambda \geq n^\lambda a_d(S) \qquad a_d(S) = \#\text{ of } P\in S \text{ of degree } d.$$

So get $$\limsup_{n^\lambda \to \infty} \frac{1}{1+n^\lambda(g-1)} \sum \frac{d\, n^\lambda a_d(S)}{q^{d/2}-1} \leq 1$$

$n^\lambda \to \infty$

Now $$\frac{n^\lambda}{1+n^\lambda(g-1)} \longrightarrow \frac{1}{g-1},$$

so $$\limsup_{n_\lambda \to \infty} \underbrace{\frac{1}{g-1} \sum \frac{d\, a_d(S)}{q^{d/2}-1}}_{\text{constant!}} \leq 1$$

So we get the inequality we want. $\boxed{/\!/}$

2^{nd} case: general case.

Note: degree of a const. field extn. has a bound:

Indeed, if $P \in S$ has degree d, the degree of the constant field extn divides d.

Now (take a subsequence) we can assume that the constant field extn is $\mathbb{F}_{q^d}$ (for some d) for all λ.

Then
$$\left.\begin{array}{c} X^\lambda \\ \downarrow \\ X/\mathbb{F}_{q^d} \end{array}\right\} \text{; apply case 1 to the top layer}$$
$$\begin{array}{c} \downarrow \\ X/\mathbb{F}_q \end{array}$$

Every $P \in S$ gives d points in $X/\mathbb{F}_{q^d}$ of degree $\deg(P)/d$,

and the new "q" is q^d.

Get $\displaystyle d \sum_{P \in S} \frac{\deg(P)/d}{(q^d)^{\frac{\deg(P)}{2d}} - 1} \le g - 1$ which is the 1 fla we want. ▨

Ihara, Journ. Math Soc. Japan?

Let $\displaystyle A(q) =: \limsup_{g \to \infty} \frac{N_q(g)}{g}$

Drinfeld-Vladut Thm $\Longrightarrow$ $\boxed{A(q) \le q^{1/2} - 1}$

Theorem (Ihara, Zink)

If q is a square, then $A(q) \geq q^{1/2} - 1$.

Corollary: If q is a square, $A(q) = q^{1/2} - 1$.

$A(q)$ is not known for other q.

Known: $A(q) > 0$; $A(q) > c \log q$ (some $c > 0$) [Use Golod-Shafarevich → next

For $q=2$:

$$\begin{cases} A(2) \le 0.414\ldots & (= \sqrt{2} - 1) \quad (D\text{-}V) \\ A(2) \geq 0.205. & (= \frac{8}{39}) \end{cases}$$

Proof when $q = p^2$: Use modular curves $X_0(N)$, etc.

(For $q = p^{2e}$, $e \geq 2$, use Shimura curves)

$\Gamma_0(N)$, $X_0(N)$ mod. curve

Choose $N = \ell$ prime. $\ell \equiv -1 \pmod{12}$ $\ell \neq p$.

Let $X = X_0(\ell)$, genus $g = \frac{\ell+1}{12}$.

Supersingular points are rat'l $/\mathbb{F}_{p^2}$, and their number N^{s} is given by

$$\boxed{N^{ss} = \frac{p-1}{12}(\ell+1)}$$

$$\begin{array}{c} X_0(\ell) \\ \big\downarrow \\ \mathbb{P}^1 \quad (\text{param. by } j) \end{array}$$

ss. j's

so $$\frac{N}{g} \geq \frac{N^{ss}}{g} = p - 1 = q^{1/2} - 1$$

Now take $\ell \to \infty$, and the bound is obtained. ☒

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

Have seen: 1) $A(q) \leq q^{1/2} - 1$ (Drinfeld - Vladut)

Now 2) If q is a square, $A(q) = q^{1/2} - 1$.

For $q = p^2$, modular curves $\longrightarrow$ enough s.s. points.

$\{1\} \subset G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$, ℓ prime, $\ell \geq 3$
subgp

Then the modular curve w.r.t. G, affine, but add pts at ∞. Corresps to moduli problem:

E ell. curve + "G-structure on its ℓ-div. pts"

G-structure: a family of $E_\ell \xrightarrow[\varphi]{\sim} \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$

s.t. 1) $\varphi, \varphi' \in$ family $\Rightarrow$ $\varphi' = s\varphi$ for some $s \in$

2) $\varphi' \in$ family, $s \in G$ $\Rightarrow$ $s\varphi' \in$ family.

X_G is the moduli space (completed).

Can view in terms of X_ℓ = mod. curve of level ℓ (corr to $G = \{\pm 1\}$)

X_ℓ
$|$

$$GL_2/\{\pm 1\} \xrightarrow{\det} \mathbb{F}_\ell^\times$$

gives an extension

$$\begin{tikzcd}
X_\ell \arrow[d, dash] & \text{abs. irred. here} \\
\mathbb{Q} \arrow[r, dashed, dash] & \mathbb{Q}(\zeta_\ell)
\end{tikzcd}$$

then: $X_G = X_\ell / G$

If $G \twoheadrightarrow \mathbb{F}_\ell^\times$, then X_G is defined over $\mathbb{Q}$.

Assume $G \supset \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{F}_\ell^\times$

so $\det G = \begin{cases} \mathbb{F}_\ell^\times \\ \text{or} \\ (\mathbb{F}_\ell^\times)^2 \end{cases}$

So ground field is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{\pm \ell})$, $\pm\ell \equiv 1\ (4)$.

Can do this over any k, char $k \neq \ell$ (for char $= \ell$, Katz–Mazur).

In char p, $p \neq \ell$, X_G is defined over either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

<u>Theorem</u>: Every s.s. point $((E, \varphi), E \text{ s.s.})$ is rational over $\mathbb{F}_{p^2}$ (on X_G).

Pf: E s.s. can be written on $\mathbb{F}_{p^2}$, its Frob. being $-p$. So $-p \in G$ by our assumption, and Frob. stabilizes (E, φ). ▣

a) $\Gamma_0(\ell)$-curve : $G = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ gives our result above.

b) interesting case: $G = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{F}_\ell^\times \right\}$ $\qquad X_G = X(\ell)$

genus of $X(\ell)$: $\quad 2g - 2 = \frac{1}{12}(\ell^2 - 1)(\ell - 6)$

s.s. points : $/\mathbb{F}_{p^2}$ $\quad N^{ss} = \dfrac{(p-1)(g-1)}{1 - \frac{6}{\ell}}$.

<u>For low values</u> :

$\ell = 7$ $\quad$ Klein curve $\qquad$ $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on $X(\ell)$

$|PSL_2(\mathbb{Z}/7\mathbb{Z})| = 168$ $\qquad$ ($PGL_2(\ )$ acts on curve over $\mathbb{Q}$, PSL_2 on curve over $\mathbb{Q}(\sqrt{-7})$)

$g = 3$, $\quad N^{ss} = 14(p-1)$

<u>Example</u> :

- $p = 2$, so $N^{ss} = 14$ (over $\mathbb{F}_4$)
- $p = 3$, $\quad N^{ss} = 28$ $\quad /\mathbb{F}_9$
- $p = 5$ $\quad N^{ss} = 56$ $\quad /\mathbb{F}_{25}$

Weil bound is $\quad 1 + p^2 + 6p \quad$ = resp, 17, 28, 56

$(2g\sqrt{p^2} = 6p.)$

[illegible]

$\Rightarrow$ for $p = 3, 5$, no rat'l cusps, etc.

Case prove: best for $p = 2$ also.

$\therefore$ Klein curve gives us the best for $q = 4, 9, 25$ (also 8, need: cusps are rational

---

alternate approach

$\mathrm{Jac}(X(7)) = E \times E \times E$ E has CM by $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$

unique such def $/\mathbb{Q}$, good red. outside 7, grossencharacter

for p inert: $\left(\frac{p}{7}\right) = -1 \Rightarrow$ eigenv. of $F_r / \mathbb{F}_p$ in E is $\pm\sqrt{-p}$

$\Rightarrow / \mathbb{F}_{p^2}$ it is $-p$ (twice).

So on $\mathrm{Jac}(X(7))$, get $-p$ (six times), so get the Weil bound for p inert.

$\ell = 11$, $g = 26$, $N^{ss} = 55(p-1)$

$p = 2$: $/\mathbb{F}_4$, $N^{ss} = 55$ which is best possible (exp. fi

$p = 3$: $/\mathbb{F}_9$, $N^{ss} = 110$ (?) (exp. flu gives ≤ 111).

$\quad = \# X(11)(\mathbb{F}_9)$

Use $Jac(X(11))$ is isogenous to the product of 11 times E_1, 10 times E_2, 5 times E_3, E_i ell curves

		Ant. IV
E_1	ell. curve cond 11	11
E_2	" " cond 11^2, no CM	121_F
E_3	" " cond 11^2, CM	121_D

Studied by Ligozat (Mod. Fcts V or VI)

So can check that the $N^{ss} = N$ (Ant. IV gives eigenvalues of Frob. on these curves).

Theorem (Golod-Šafarevič)

Thm on Artin local rings:

- R ring, I two-sided ideal, $R/I = k$ comm. field.
- Every $r \in R$, $r \notin I$ is invertible (i.e., R is local w/ max ideal I).
- R is "Artin" $\iff$ $\begin{cases} I^n = 0 \text{ for large } n \\ \text{and} \\ I^m/I^{m+1} \text{ is a finite dim'l } k\text{-vector sp} \\ \quad (\text{for } m = 0, 1, \dots) \end{cases}$

(Example: G finite ℓ-group, $R = \mathbb{F}_\ell[G]$, $I = \Delta(G)$, $k = \mathbb{F}_\ell$.)

Take M = f.g. R-module (left).

Then M/IM is a k-vector space of finite dim.

$d(M) = \dim (M/IM)$ = min no of generators of M

(If $x_1, -, x_d \in M$ give a basis for M/IM, NAK $\Rightarrow$ they generate

$$M \qquad\qquad d = d_0(M)$$

Choose $x_1, -, x_d \in M$ generating M. This gives

$$0 \longrightarrow M_1 \longrightarrow R^d \longrightarrow M \longrightarrow 0$$

M_1 = kernel = module of relations between the x_i

$$M_1 \subset IR^d$$

Up to isom., M_1 depends only on M. Define

$d_1(M) := d_0(M_1) =$ "nber of relations between x_i"

Also: exact seq. gives: $\otimes k$

$$0 = \mathrm{Tor}_1(R^d, k) \longrightarrow \mathrm{Tor}_1(M,k) \longrightarrow M_1/IM_1 \longrightarrow R^d/IR_d \underset{\cong}{\longrightarrow} M/IM \longrightarrow 0$$

So find $\mathrm{Tor}_1(M,k) \cong M_1/IM_1$,

so $d_1(M) = \dim_k \mathrm{Tor}_1(M,k)$

$d_i(M) = d_0(M_i)$ $\quad M_i = i^{\text{th}}$ term of a minimal resolution.

$= \dim_k \mathrm{Tor}_i(M,k)$.

Take $M = k$: $d_0(k) = 1$

$$0 \to I \longrightarrow R \longrightarrow k \to 0$$

So $M_1 = I$; $d_1(k) = \dim_k (I/I^2) = d$

$d_2(k) = r$ by defn.

<u>Theorem</u> (Golod-Šafarevič, refined by Vinberg and Gaschütz)

Assume $d \geq 1$, i.e., that $I \neq 0$, i.e., that R is not a field. Then

$$r > \frac{d^2}{4}.$$

[One has examples of $r \sim \frac{d^2}{3}$ or $\frac{3d^2}{8}$; $\frac{d^2}{2}$ is easy ; Best is unknown

[<u>Example</u>: if $R = \mathbb{Z}/\ell^2\mathbb{Z}$, $k = \mathbb{Z}/\ell\mathbb{Z}$, get $M_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, so all d_i :

<u>Pf</u>: Have $0 \to J \to R^d \longrightarrow I \longrightarrow 0$

$$R^r \longrightarrow J \to 0$$

So get $R^r \xrightarrow{\varepsilon} R^d \longrightarrow I \longrightarrow 0$ $\qquad \varepsilon(R^r) \subset IR^d$

Tensor w/ R/I^nR : $\qquad$ since $R^d/IR^d \xrightarrow{\sim} I/I^2$

$$\begin{tikzcd} R^r/I^nR^r \arrow[r] \arrow[dr] & R^d/I^nR^d \arrow[r] & I/I^{n+1} \arrow[r] & 0 \\ & R^r/I^{n-1}R^r \arrow[ur] & & \end{tikzcd}$$

$\therefore\ \varepsilon(I^{n-1}R^r) \subset I^nR^d$

so factors

So $\frac{R^r}{I^{n-1}R^r} \longrightarrow \frac{R^d}{I^n R^d} \longrightarrow \frac{I}{I^{n+1}} \longrightarrow 0$ $(n \geq 1)$

define $a(n) = \ell(R/I^n R) = \sum_{i=0}^{n-1} \dim_k (I^i/I^{i+1})$

$a(0) = 0$

$a(1) = 1$

$a(2) = 1 + d$ $R/I^2 : R/I, \; I/I^2$
$\quad 1 \quad d$

⋮

$a(n)$ ultimately constant.

Now exact seq. above gives:

$$d\,a(n) \leq r\,a(n-1) + \underbrace{a(n+1) - 1}_{\ell(I/I^{n+1})} \qquad n \geq 1$$

Claim: this implies $r > \frac{d^2}{4}$.

For this introduce $\sum_{n=0}^{\infty} a(n) t^n = t + (1+d)t^2 + \cdots = t f(t)$

so $\underline{f(t) = \sum_{n=0}^{\infty} a(n+1) t^n}$

multiply ineq by t^n and add:

$$\sum_{n\geq 1} d\,a(n)t^n < r\sum_{n\geq 1} a(n-1)t^n + \sum_{n\geq 1} a(n+1)t^n - \sum_{n\geq 1} t^n$$

$$d f(t)t < r t^2 f(t) + f(t) - 1 - \sum_{n\geq 1} t^n$$

so $$d f(t) t < r t^2 f(t) + f(t) - \frac{1}{1-t}$$

so $$f(t)(rt^2 - dt + 1) > \frac{1}{1-t}$$

Assume $r \leq \frac{d^2}{4}$; then $rt^2 - dt + 1 = (1-\lambda t)(1-\mu t)$ $\lambda\mu \geq$

Now, $\frac{1}{1-\lambda t}$ has pos. coeffs.

λ & μ can't both be zero, since $d \neq 0$.

Multiply!

$$f(t) > \frac{1}{(1-t)(1-\lambda t)(1-\mu t)}$$

and either λ or μ is ≥ 1: $\lambda + \mu = d \geq 1$, $\lambda\mu = r$

But the coeffs of $f(t)$ are bounded, since the $a(n)$ are.

So it's enough to show the coeffs of RHS are not bded.

$$\text{RHS} > \frac{1}{(1-t)^2}$$ coeffs not bded. ▨

G finite ℓ-group, $R = \mathbb{F}_\ell[G]$, $I = \Delta(G)$

Why is I = radical of G? Up to isom., an ℓ-group has only one irred. repres. in $\operatorname{char} \ell$, namely the trivial repres.
(any non-triv. repres. has a fixed vector)
then radical $= \bigcap \ker(\text{repres}) = I$.

$d = \dim \operatorname{Tor}_1^R(k,k) = \dim H_1(G, \mathbb{Z}/\ell\mathbb{Z})$

$r = \dim \operatorname{Tor}_2^R(k,k) = \dim H_2(G, \mathbb{Z}/\ell\mathbb{Z})$

dual of $H_i = H^i$

so $\begin{cases} d = \dim H^1(G, \mathbb{Z}/\ell\mathbb{Z}) \\ r = \dim H^2(G, \mathbb{Z}/\ell\mathbb{Z}) \end{cases}$

And: d = min. no. of generators of G
assume $x_1, \dots, x_d \in G$ generate G;
then r = min. nber of rels between x's which define G as an ℓ-group. (or pro-ℓ-group)

Theorem (Golod-Šaf.) If G is a finite non-triv. ℓ-group then d and r as above satisfy $r > d^2/4$.

$d = 1$, $r > \frac{1}{4}$ i.e., $r \geq 1$; x gen, $x^\ell = 1$ cyclic order ℓ (sh

$d = 2$, $r > \frac{4}{4}$ i.e., $r \geq 2$; x, y gen., $yxy^{-1} = x^{1+\ell}$, $xyx^{-1} = y^{1+\ell}$
(order is ℓ^3)

Define $z = xyx^{-1}y^{-1} = y^\ell = x^{-\ell}$, so $z \in Z(G)$

$x^\ell y^{-1} = x^{\ell+\ell^2}$ so $x^{\ell^2} = 1$ so $z^\ell = 1$. So order ℓ^3.

$\|$ since $x^\ell = y^{-\ell}$]

$d=3$, $r > \frac{9}{4}$ i.e., $r \geq 3$ (ℓ odd): 3 gen. z, y, x

$$\begin{cases} y x y^{-1} = x^{1+\ell} \\ z y z^{-1} = y^{1+\ell} \\ x z x^{-1} = z^{1+\ell} \end{cases}$$

Mennicke → finite group. $d=$

$d=4$, $r > \frac{16}{4}$ i.e., $r \geq 5$ → is $d=4, r=5$ possible!

(think: $d=4, r=6$ is.)

$x_1, \ldots, x_d$ with $(x_i, x_j) = 1$, $x_i^\ell = 1$ give $\frac{d(d-1)}{2} + d$ rel

10/17 Class Field Towers

C curve, genus g, over $\mathbb{F}_q$, p = char.

K its function field.

ℓ a prime number ($\ell = p$ is ok)

S finite non-empty set of "primes" of K i.e., of closed points of C.

Look at K_1 = max. abelian ℓ-extension of K, (whose Galois group is an...) unramified (everywhere) in which the elements of S split completely

$$\begin{array}{c} K_1 \\ | \\ K \end{array}$$

Cond. on S makes it finite (otherwise if $S=\emptyset$, have the const field extn.)

If ℓ divides the $\deg(P)$ for every $P \in S$, then K_1 conta[ins] $\mathbb{F}_{q^\ell} \cdot K$. If not, it does not.

$$\begin{array}{ccc} K_1 & & C_1 \\ | & \rightsquigarrow & \downarrow \\ K & & C \end{array}$$

Define $K_2 = (K_1)_1$ with respect to S_1 = inverse image of S.

So have $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty = \bigcup_n K_n$

K_∞ = max. Galois extension of K where S splits completely, whose Galois group is pro-ℓ, and unramified.

<u>Question</u>: Is K_∞ / K finite?

Let $G_S = Gal(K_\infty/K) = \varprojlim Gal(K_n/K)$

Assume G_S is finite; it is an ℓ-group. Then we have

$d = \dim H_1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ (min. nber of generators)

$r = \dim H_2(G_S, \mathbb{Z}/\ell\mathbb{Z})$ (min. nber of "relations" (as ℓ-group).)

<u>Theorem</u>: Assume G_S is finite (i.e., the tower stops). Then

$$r - d \le \begin{cases} |S| - 1 & \text{if } \ell \nmid q-1 \\ |S| & \text{if } \ell \mid q-1 . \end{cases}$$

(We know: $r > \frac{d^2}{4}$ if $d \ge 1$ Golod-Šaf., which will give a contradiction for suitable S.)

Proof (Same as Iwasawa's in the field case):

First: Using class field theory to find $Gal(K_1/K)$:

C_K = idèle class group

Have

$$1 \longrightarrow E_S \longrightarrow \prod_{p \in S} K_p^* \times \prod_{v \notin S} U_v \longrightarrow C_K \longrightarrow \underset{\text{(quotient)}}{Ab_S} \longrightarrow 1$$

E_S = S-units (= unit outside S)

Then $Gal(K_1/K) = (Ab_S)_\ell$ (ℓ-part)

Next: Now: K_∞/K finite, so $(K_\infty)_1 = K_\infty$

Write s.e.s. for K_∞:

$$1 \longrightarrow \underset{\substack{\| \\ S_\infty\text{-units of } K_\infty}}{E_{S_\infty}} \longrightarrow \prod_{\tilde{p} \in S_\infty} K_{\infty,\tilde{p}}^* \times \prod_{\tilde{v} \notin S_\infty} U_{\tilde{v}} \longrightarrow C_{K_\infty} \longrightarrow Ab_\infty \longrightarrow$$

$(K_\infty)_1 = K_\infty \iff (Ab_\infty)_\ell = \{1\}$

Let $G = G_S$; G acts on everything.

- Ab_∞ has trivial cohomology (order prime to ℓ, G ℓ-

Also · For the product

K_p^*-part : $\tilde{p}$ ⟲ G permutes $\qquad \prod_{\tilde{p}\to p} K^*_{\infty,\tilde{p}}$ is <u>induced</u> (trivial coh.)

$$\tilde{p} \downarrow p \in S$$

U_v-part : $\tilde{v}$ $\qquad G_{\tilde{v}}$ -- stab $\tilde{v}$

$$\tilde{v} \downarrow v$$

Shapiro's lemma :

coh $= H^q(G_{\tilde{v}}, U_{\tilde{v}})$ = trivial (because everything is unramified).

So LES of coh gives a map

$$\hat{H}^q(G, C_{K_\infty}) \xrightarrow[\cong]{\delta} \hat{H}^{q+1}(G, E_{S_\infty}) \qquad \text{for each } q \in \mathbb{Z}$$

δ is an isom. for all q because middle term has trivial cohom.

$\boxed{\hat{H}^q \text{ is Tate cohomology}}$

Know: $\quad \hat{H}^q(G, C_{K_\infty}) \xleftarrow[\smile u_{K_\infty}]{\cong} \hat{H}^{q-2}(G, \mathbb{Z})$

$$u_{K_\infty} \in H^2(G, C_{K_\infty})$$

Choose $q+1=0$ so $q=-1$: Get $\hat{H}^{-3}(G,\mathbb{Z}) \cong \hat{H}^0(G, E_{S_\infty}) =$ $\_\, E_S/$

Know $E_S \cong \mathbb{Z}^{|S|-1} \times \mathbb{F}_q^{\times}$.

We want a quotient of E_S/Norms which is an ℓ-group

So

$$rk_\ell(\hat{H}^{-3}(G,\mathbb{Z})) \leq \begin{cases} |S|-1 & \text{if } \ell \nmid (q-1) \\ |S| & \text{if } \ell \mid (q-1) \end{cases}$$

<u>It remains to show</u>: $rk_\ell(\hat{H}^{-3}(G,\mathbb{Z})) = r-d$.

$$\hat{H}^{-3}(G,\mathbb{Z}) = H_2(G,\mathbb{Z})$$

[Group of coeffs A, trivial action :

$$H_q(G,A) = H_q(G,\mathbb{Z}) \otimes A \oplus \mathrm{Tor}_1(H_{q-1}(G,\mathbb{Z}),A)$$

$q=2$, $A=\mathbb{Z}/\ell\mathbb{Z}$:

$$H_2(G,\mathbb{Z}/\ell\mathbb{Z}) = H_2(G,\mathbb{Z}) \otimes \mathbb{Z}/\ell\mathbb{Z} \oplus \mathrm{Tor}_1(H_1(G,\mathbb{Z}),A)$$

$$= H_2(G,\mathbb{Z})/\ell H_2(G,\mathbb{Z}) \oplus \ell\text{-part of } H_1(G,\mathbb{Z})$$

So take ranks: $r = rk_\ell(H_2(G,\mathbb{Z})) + d$.

Since: $H_1(G,\mathbb{Z}/\ell\mathbb{Z}) = H_1(G,\mathbb{Z})/\ell H_1(G,\mathbb{Z})$ since H_0 is free

So $rk_\ell\, \hat{H}^{-3}(G,\mathbb{Z}) = r-d$.]

Or: Look at

$$0 \to \mathbb{Z} \xrightarrow{\ell} \mathbb{Z} \longrightarrow \mathbb{Z}/\ell\mathbb{Z} \to 0$$

$$H_2(G,\mathbb{Z}) \xrightarrow{\ell} H_2(G,\mathbb{Z}) \longrightarrow H_2(G, \mathbb{Z}/\ell\mathbb{Z}) \longrightarrow H_1(\ ) \xrightarrow{\ell} H_1(\ )$$

So $$0 \to H_2(G,\mathbb{Z})/\ell H_2(G,\mathbb{Z}) \longrightarrow H_2(G, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{Ker}(\ell \text{ in } H_1(G,\mathbb{Z}))$$

So dimensions add. So QED! $\boxtimes$

<u>Theorem</u>: The $(S-\ell)$ class field tower of K is infinite if $|S| \lneq \frac{d^2}{4} - d + \begin{cases} 1 & \text{if } \ell \mid (q-1) \\ 0 & \text{if not} \end{cases}$, and $d \geq 2$.

Pf: Otherwise

$$r - d \leq \begin{cases} |S| - 1 \\ |S| \end{cases}$$

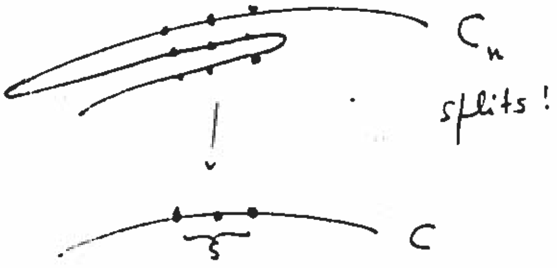
$$r > \frac{d^2}{4} \qquad \text{if } d \geq 1$$

And of course $d=1$ doesn't work (get $|S| \leq \frac{1}{4}$) $\boxtimes$

Suppose that all elements in S have degree 1, i.e., S is made up of rational points, and assume that the corresp. class field tower is infinite.

Then $A(q) \geq \dfrac{|S|}{g_c - 1}$, where $A(q) = \limsup\limits_{g\to\infty} \dfrac{N_q(g)}{g}$

g_c = genus of C.



So nber of rat'l pts of $C_n \geq [C_n : C]$

genus of $C_n = g_{C_n}$; $g_{C_n} - 1 = [C_n : C]$

Notice that $g_c \geq 2$ (For $g_c = 0$, no unr. coverings; for $g_c = 1$, covering would have $g_{C_n} = 1$ and nber pts $\to \infty$!)

So $$\frac{N_q(g_n)}{g_n} \geq |S| \frac{[C_n : C]}{1 + [C_n : C](g_c - 1)}$$

$$\geq |S| \frac{1}{\frac{1}{[C_n : C]} + g_c - 1}$$

$n \to \infty$ so $$\boxed{A(q) \geq \frac{|S|}{g_c - 1}}.$$

Corollary: If (S, C) satisfy $|S| \leq \frac{d^2}{4} - d + \{^1_0\}$, $d \geq 2$, then

$$A(q) \geq \frac{|S|}{g_c - 1}$$

(and in particular $A(q) > 0$).

• For every q, we want to find K, S, ℓ satisfying

$$(*) : \quad |S| \le \frac{d^2}{4} - d + \begin{cases} 1 & \text{if } \ell \mid q-1, \\ 0 & \text{if not.} \end{cases} \qquad d \ge 2.$$

We'll want to take $|S| = 1$, $d \ge 5$.
We'll choose $\ell = 2$ (So for q odd, enough to find $d \ge 4$).

<u>Construction</u> (char $= p \ne 2$)

Choose $\ell = 2$; K will be some quadratic extension of $K_0 = \mathbb{F}_q(T)$ corresp. to curve $/C_{-1}$ of genus 0.

Want

$$\begin{tikzcd} C_0 \arrow[dr, dash] & C_1 \arrow[d, dash] & \cdots & C_d \arrow[dll, dash] \\ & C_{-1} & & \end{tikzcd}$$

point at ∞ should split completely.

Let $\Phi_0, \dots, \Phi_d$ be irred. monic polyn. of even degree disti[nct]

Then define C_i by $y_i^2 = \Phi_i(T)$.

$$y_i^2 = T^{\text{even}} + \cdots \Rightarrow \infty \text{ is split in } C_i$$

So set $K = \mathbb{F}_q(T, \sqrt{\Phi_0 \cdots \Phi_d})$

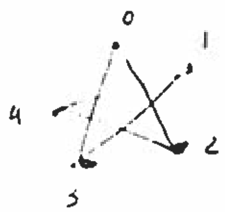
Over K, I have d indep. quadratic extens, unramified, ∞ splits completely.

Choose $d = 5$, for instance, and the "d" in the theorem is then at least 5, so done. ☒

For char $=2$, do the same with Artin-Schreier extensions

Now want: In $\mathbb{F}_q$, $A, B \subset \mathbb{F}_q$ as large as possible s.t. every $a-b$, for $a \in A$, $b \in B$, is a non-square.

E.g. $q=5$

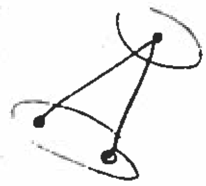


$\mathbb{F}_5$

join pts whose difference is not a square

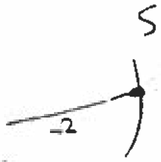
Want: a maximal complete bipartite graph embedded in this graph

Call this a B-subgraph

E.g.  in our case.

<u>Graph theorem</u>

Let R, S be two finite sets, $\Omega \subset R \times S$.



Let $m \geq 1$ be such that every $s \in S$ is Ω-related to at least m points of R.

Let a, b be integers ≥ 1 such that $b \binom{|R|}{a} \leq |S| \binom{m}{a}$.

Then $\exists\, A \subset R$ and $B \subset S$ with $\begin{cases} |A| = a, \ |B| = b \\ A \times B \subset \Omega. \end{cases}$

Let X = set of pairs (A, s) with $|A| = a$, $s \in S$ and $A \times \{s\} \subset \Omega$.

Then $|X| = ?$

Project $X \xrightarrow{\varphi} S$
$(A,s) \longmapsto s$

Let $R(s)$ be the subset of R made of the elements r s.t. $(r,s) \in \Omega$.

So $|\varphi^{-1}(s)|$ = nber subsets of $R(s)$ w/ a elements

$$= \binom{R(s)}{a} \geq \binom{m}{a} \qquad \text{since } R(s) \geq m$$

Then $|X| \geq |S| \binom{m}{a}$

Then $X \xrightarrow{\psi}$ Set of subsets of R with a elements $\leftarrow$ has $\binom{|R|}{a}$ element.
$(A, s) \longmapsto A$

Hence some fiber of ψ has at least $|X| / \binom{|R|}{a}$ element.

But $$\frac{|X|}{\binom{|R|}{a}} \geq \frac{|S|\binom{m}{a}}{\binom{|R|}{a}} \geq b.$$

So choose A whose fiber has $\geq b$ elements, and choose B in the fiber with $|B| = b$. Done! $\boxtimes$

10/23 Class Field Towers (cont.)

We showed: If $\begin{cases} \Omega \subset R \times S \\ \text{every } s \in S \text{ is } \Omega\text{-related to at least } m \text{ elements of } R \end{cases}$

then $\exists A \subset R$, $B \subset S$, $|A| = a$, $|B| = b$ given, s.t. $A \times B \subset \Omega$

provided that $b\binom{|R|}{a} \leq |S| \binom{m}{a}$.

For $\mathbb{F}_q$, $q = p^e$, $p \neq 2$:

Take $R = S = \mathbb{F}_q$, $\Omega = \{(r,s) \mid r - s$ is a nonzero square in $\mathbb{F}_q\}$, so $m = \frac{q-1}{2}$.

Let $q \longmapsto a(q), b(q)$ be two functions of a variable q, with integral values ≥ 1 for $q = p^e$, p prime $\neq 2$, with

$$\begin{cases} a(q) \leq c_1 \log q \\ b(q) \leq q^{c_2} \end{cases}$$

where $c_2 + c_1 \log 2 < 1$.

Claim: Then, for q large enough, there exists $A, B \subset \mathbb{F}_q$ with $|A| = a(q)$, $|B| = b(q)$, and $A \times B \subset \Omega$.

[This is approx. what the naive approach would give

$b_1 \quad b_2 \quad \cdots\cdots \quad b_n$ $\qquad q\left(\frac{1}{2}\right)^{\alpha}$?

$\alpha \sim \log q \implies \left(\frac{1}{2}\right)^{\alpha} = \frac{1}{q^{\varepsilon}}$

which suggests $a(q) \leq c_1 \log q$ is reasonable]

If q is a square,

$$\begin{array}{c} \mathbb{F}_q \\ | \\ \mathbb{F}_{q^{1/2}} \end{array} \qquad \underbrace{|\!-\!-\!-\!|}_{\frac{1}{2}q^{1/2}}\ \underbrace{|\!-\!-\!-\!-\!|}_{\frac{1}{2}q^{1/2}}$$

every difference $\in \mathbb{F}_{q^{1/2}} \subset (\mathbb{F}_q^{\times})^2$

So $a(q) \leq q^{1/2}$, $b(q) \leq q^{1/2}$. Much larger!

Proof of Claim

To be checked: for q large enough,

$$b(q)\binom{q}{a(q)} \overset{?}{\leq} q\binom{\frac{q-1}{2}}{a(q)}$$

i.e.,
$$b(q)\frac{q!}{(q-a(q))!} \overset{?}{\leq} q\,\frac{\left(\frac{q-1}{2}\right)!}{\left(\frac{q-1}{2}-a(q)\right)!}$$

Stirling: $\log(x!) = (x+\frac{1}{2})\log x - x + O(1)$

Suppose $1 \le y \le x^{1/2}$. Then

$$\log\left(\frac{x!}{(x-y)!}\right) = (x+\tfrac{1}{2})\log x - x - (x-y+\tfrac{1}{2})\left(\log x + \log(1-\tfrac{y}{x})\right) + x - y + O(1)$$

$$= y\log x + O(1)$$

[Since $-y - (x-y+\tfrac{1}{2})\log(1-\tfrac{y}{x}) =$

$$= \cancel{-y} - (x - \cancel{y} + \tfrac{1}{2})\left(-\tfrac{y}{x} + O\left(\tfrac{y^2}{x^2}\right)\right)$$

$y^2 \le 1$

$= O(1)$]

So check that

$$\log b(q) + a(q)\log q + O(1) \overset{?}{\le} \log q + a(q)\log\frac{q-1}{2}$$

$\left.\begin{matrix} a(q) \le c_1 \log q \\ b(q) \le q^{c_2} \end{matrix}\right]$ $\log b(q) \le c_2 \log q$.

So $\log q - \log b(q) \overset{?}{\ge} a(q)\left(\log q - \log\frac{q-1}{2}\right) + O(1)$

$\log\frac{q-1}{2} = \log(q-1) - \log 2 = \log q + \log(1-\frac{1}{q})$ -

So $a(q)\left(\log q - \log \frac{q-1}{2}\right) + O(1) \leq c_1 \log q \ (\log 2 + o(1))$

$\log q - \log b(q) \geq (\log q)(1-c_2)$

So want $\boxed{1 - c_2 > c_1 \log 2}$, which is our condition. ∎

Starting from such $A, B \subset \mathbb{F}_q$, we make a 2-class field tower starting from $\mathbb{P}_1$ and making quadratic extensio

Assume $a = \text{even} = 2\alpha$

Write $\{a_1, a_1', \ldots, a_\alpha, a_\alpha'\} = A$.

If t is the variable in $\mathbb{P}_1$, take the quad. extn. given by $\sqrt{(t-a_i)(t-a_i')}$ $i = 1, \ldots, \alpha$.

(So Fct. field is $\mathbb{F}_q(t, \sqrt{(t-a_i)(t-a_i')}))$)

In that ext., the points of B split completely (by our choice of ≤ 2).

Now go to $C \longleftrightarrow \mathbb{F}_q(t, \sqrt{\prod (t-a_i)(t-a_i')})$

Elements of B give B_C = subset of C coming from B

$|B_C| = 2|B| = 2b(q)$

and C has $\alpha - 1$ independent quadratic extns which are unramified and where B_C splits completely.

(Namely, given by $\sqrt{(t-a_i)(t-a_i')}$ $i = 1, \ldots, \alpha - 1$.

The 2-class field tower is infinite if $|B_c| \leq \frac{(\alpha-1)^2}{4} - (\alpha-1)$

So choose $\alpha \sim c \log q$

$$|B_c| \sim c'(\log q)^2$$

if $c' < \frac{c}{4}$, the condn. is satisfied.

Hence, infinite class field tower, so

$$A(q) \geqslant \frac{|B_c|}{g_c - 1} \asymp \frac{(\log q)^2}{\log q} \asymp \log q.$$

C is hyperelliptic, ramified at $2\alpha = a(q)$ pts, and so $g_C = \alpha - 1 \asymp \log q$.

So $\boxed{A(q) \geqslant c \log q}$ for some c. (For q odd

When q is a square, we can take $|B_c| \asymp q^{1/2}$, $g_c \asymp q^{1/4}$
so get $A(q) \geqslant c q^{1/4}$.

(But modular tower gives $q^{1/2}$).

For $q = 2^e$, can use Artin-Schreier extns
or
a 3-tower

Construction for $g=2$ Claim: $A(2) \geq \frac{2}{9} = 0.222\ldots$

First: Simple construction for $A(2) \geq \frac{1}{5} = 0.2$.

Take
$$\begin{array}{ccl} C & & y^2+y = t^3+t+\sum\limits_{\substack{\text{irred polyn } \varphi(t) \\ \text{of deg } 2,3,4}} \frac{t^2+t}{\varphi(t)} \\ \big\downarrow{\scriptstyle 2} & & \\ \mathbb{P}_1 & t & \end{array}$$

so: sum is over
$$\left\{\begin{array}{l} \deg 2 \longrightarrow \\ \deg 3 \longrightarrow \\ \deg 4 \longrightarrow \end{array}\right\} \begin{array}{l} t^2+t+1 \\ t^3+t+1,\ t^3+t^2+1 \\ t^4+t+1,\ t^4+t^3+1,\ t^4+t^3+t^2+t+1. \end{array}$$

We'll see $g_C = 21$.

Take $\{0,1\} \subset \mathbb{P}_1$; these split completely in C to give a set S of 4 pts.

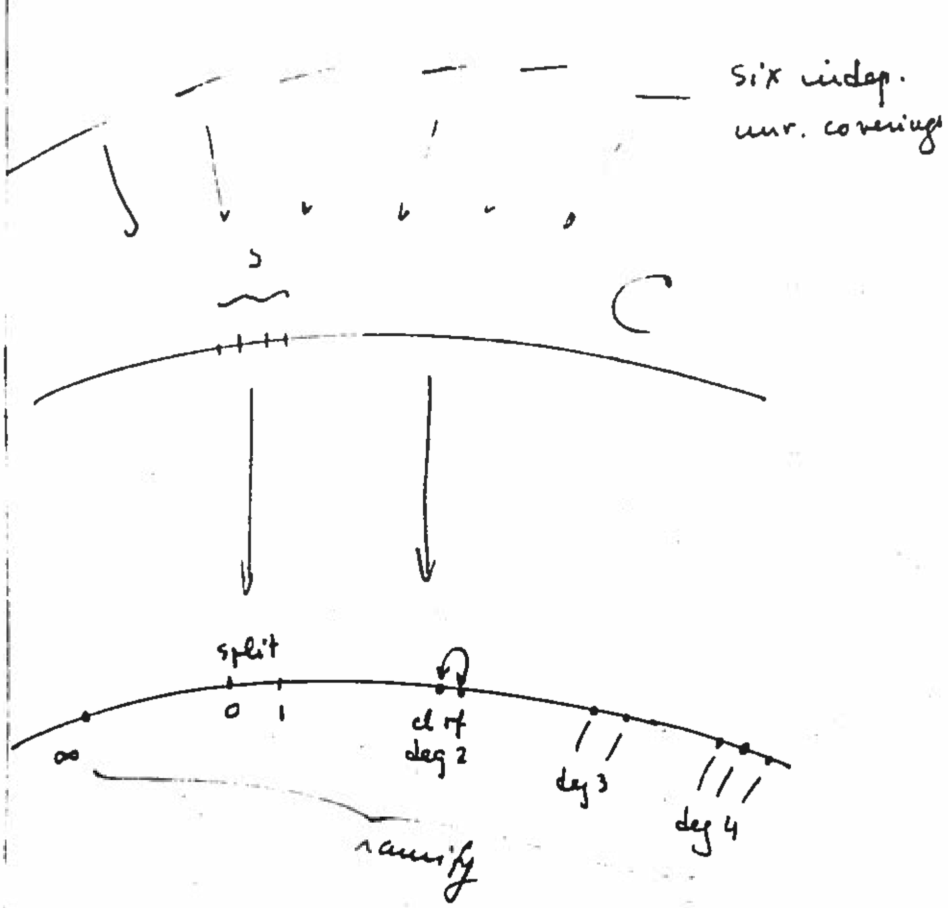
$$\begin{array}{cc} S & C \\ \big\downarrow & \big\downarrow{\scriptstyle 2} \\ \{0,1\} & \mathbb{P}_1 \end{array}$$

Have 6 indep. unramified quad. extns, given by
$$y^2+y = \frac{t^2+t}{\varphi(t)} \quad \text{for the six } \varphi(t) \text{ above}$$

and $\{0,1\}$ split completely. (Same argument as before.

C is ramif at roots of $\varphi(t)$ and at ∞.

Picture $\longrightarrow$



<u>Assume</u>: $g_C = 21$, class field tower is infinite.

Then $A(2) \geq \dfrac{|S|}{g_C - 1} = \dfrac{4}{21-1} = \dfrac{4}{20} = \dfrac{1}{5}$.

<u>Class Field Tower</u>: condition is $|S| \leq \dfrac{d^2}{4} - d + 1$

$|S| = 4$, $d \geq 6$, so $\dfrac{d^2}{4} - d + 1 \geq \dfrac{36}{4} - 6 + 1 \geq 4$.

So class field tower is infinite.

<u>Genus</u>: Know: $g_C - 1 = n(g_{C_0} - 1) + \sum$ contrib. of ramification.
?

$$\begin{array}{c} C \\ n \big\downarrow \\ P \in C_0 \end{array}$$

Go to alg. closure: take a local param. t at
Look at dt. Lift it to C.
Ramif $\Rightarrow$ dt will have zeros on the fiber

and

To see this, take ω diff'l form $\neq 0$ on C_0, w/o zero or pole at the ramif. pts.

Lift to ω_c. Now $2g_c - 2 = \deg(\omega_c) = n\deg(\omega)$ + extra ze

$= n\deg(\omega) + \sum$ deg of ... on f...

Now divide by 2 to get the formula.

Now suppose $p=2$, Artin-Schreier extn $\quad y^2 + y = \psi(t)$

local computation, so work in field of power-series,

$$\psi(t) = \frac{c_0}{t^n} + \cdots \qquad n \text{ odd} \geq 1.$$

[If ψ is hol., no ramif.; if $\frac{1}{t^2} + \cdots$, remove $\psi - \left(\frac{1}{t^2} + \frac{1}{t}\right)$ until we get n odd].

Claim: Local contrib at that place is $\frac{1}{2}(n+1)$,

i.e., "deg of dt in extension" $= n+1 \quad$ (even)

$$\begin{array}{l} K \\ \Big|\,2 \\ K_0 \quad t \end{array} \qquad v_K(y) = \tfrac{1}{2} v_K\left(\tfrac{1}{t^n}\right) = -n \quad \text{since } v(t) = 2 \text{ (ramification}$$

$$dy = \frac{c_0}{t^{n+1}}\,dt + \cdots \qquad \text{(char 2)}$$

If θ local parameter of K, $\qquad y = \theta^{-n} \cdot \text{unit},$

so $\quad dy = \dfrac{d\theta}{\theta^{n+1}} + \cdots$

so $\quad v_K(dy) = -(n+1)$

So $\quad v_K(dy) = -2(n+1) + v_K(dt) \implies v_K(dt) = n+1.$

In our case, $y^2 + y = \underbrace{t^3 + t}_{} + \sum_{\deg 2,3,4} \dfrac{t^2+t}{\varphi(t)}$ ---

pole of order $3 = n$ at ∞
$\frac{1}{2}(n+1) = 2$

simple poles at these
$\deg \varphi = 2 \longrightarrow$ two simple poles
$\longrightarrow \frac{1}{2}(2) + \frac{1}{2}(2) = 2$
Same for $\deg \varphi = 3$ or 4

So $\quad g_C - 1 = 2(g_0 - 1) + \sum$ local contrib
$\quad = -2 + 2 + \sum \deg \varphi$
$\quad = -2 + 2 + 20$

So $\boxed{g_C = 21}$. ▨

Lemma Let C be a curve over $\mathbb{F}_2$; let S be a set of closed points of C, let $\underline{m}$ be a positive divisor of C disjoint from S. Assume that $\deg(\underline{m}) \geq 151$. Then there is a quadratic extension of C which is unramified outside $\underline{m}$, where S splits completely and where the contribution of ramification is at most $\deg \underline{m}$.

Proof – later (done by CFT)

Assuming the Lemma, we can improve the result above:

Choose C = an elliptic curve with 2 rational points (and no more).

$$N_1 = \# C(\mathbb{F}_2) = 2$$

Now $N_n = \# C(\mathbb{F}_n) = 1 + 2^n - \underbrace{(\pi^n + \bar{\pi}^n)}_{t_n}$

and $t_n = t_{n-1} t_1 - q t_{n-2}$ since $\pi\bar{\pi} = q$!

Here $t_0 = 2$, $t_1 = 1$, $q = 2$ $(N_1 = 2 = 1 + 2 - t_1$

So $t_n = t_{n-1} - 2t_{n-2}$

So $t_2 = -3$, $t_3 = -5$, $t_4 = 1$

$\therefore$ $N_1 = 2$, $N_2 = 8$, $N_3 = 14$, $N_4 = 16$

If a_i = nber of closed pts of $C/\mathbb{F}_2$ of degree i (so $N_n = \sum_{i|n} i$

So $\underbrace{a_2 = 3, \; a_3 = 4}_{\text{lots of these}}$, $a_4 = 2$.

Make 7 quadratic extensions of C s.t. two rat'l pts split comp ramified each at a different closed pt of degree 2 or 3; contrib. to ramificat will be just 2, 2, 2, 3, 3, 3, 3.

ith same instruction before} $d = 6$ as before, and $g - 1 = 2(1-1) + \sum$ contrib

$$g - 1 = 18 \implies g = 19$$

10/31 Something from CFT

X curve $/\mathbb{F}_q$, genus g, K fct. field.

(modulus) $\underline{m} = \sum_{P \in S} n_P P$ be a positive divisor, S finite, $n_P \geq 1$, P closed.

$$Cl_{\underline{m}}(X) = \{\text{divisors of } X \text{ prime to } S\} \big/ \{(f)\}$$

where $f \in K^\times$, and $f \equiv 1 \mod^\times \underline{m}$

(this means that $f \in 1 + \max_P^{n_P}$ locally at each $P \in S$, or equiv., $v_P(f-1) \geq n_P$ $\forall P \in S$.

If $\underline{m} = 0$, $Cl_{\underline{0}}(X) = Pic(X)$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad \| $
$\quad\quad\quad\quad\quad\quad\quad\quad\quad Cl(X)$

Recall $\boxed{0 \longrightarrow J(\mathbb{F}_q) \longrightarrow Cl(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0}$ exact

and

$$0 \to \text{kernel} \to Cl_{\underline{m}}(X) \longrightarrow Cl(X) \to 0$$

obvious almost obvious.

assume $\underline{m} \neq 0$; [redacted] if U_P = local units at P, $U_P^{(n_P)} = \{u \in U_P \mid v(u-1$

We have $0 \longrightarrow \mathbb{F}_q^\times \longrightarrow \prod_{P \in S} U_P / U_P^{(n_P)} \to Cl_{\underline{m}}(X) \longrightarrow Cl(X) \to 0$

CFT:

Let G be a finite group and let

$$\alpha : Cl_{m}(X) \longrightarrow G \quad \text{be onto.}$$

Then CFT constructs an abelian extension K_α/K with Galois group G s.t.

1) K_α/K unramified outside S

2) If $P \notin S$, the Frob of P in G is the image by α of "P", viewed as a divisor.

3) If $P \in S$, the map

$$\begin{tikzcd} U_P \arrow[r] \arrow[rr, bend right] & Cl_{m}(X) \arrow[r, "\alpha"] & G \end{tikzcd}$$

is the one attached by local class field theory, and the image is the inertia group.

I also have $K_P^\times \longrightarrow G$, image is decomp. group.

Let $P_1, \ldots, P_s$ be closed points disjoint from S. If I want extns in which these split completely, I have:

To have P_i split in K_α/K it is nec. & suff. that $\alpha((P_i)) = 0$, $(P_i) \in Cl_m(X)$.

Let ℓ be a prime number, let d_P = ℓ-rank of $U_P/U_P^{n_P}$ (this is a group of order $(q^{\deg(P)} - 1)q^{(n_P-1)\deg(P)}$)

Let ε = ℓ-rank of $\mathbb{F}_q^\times$ $\left(\begin{matrix} 0 \text{ if } \ell \nmid q-1 \\ 1 \text{ if } \ell \mid q-1 \end{matrix}\right)$

<u>Claim</u> $\left\{\begin{array}{l} \text{Assume that } s \leq \sum d_P - \varepsilon. \\ \text{Then: } \exists \text{ a cyclic extension of deg } \ell \text{ obtained} \\ \text{through an } \alpha, \text{ where the } P_i\text{'s } \underline{\text{split}} \text{ } \underline{\text{completely}}. \end{array}\right.$

Have $0 \to \text{Local} \to Cl_m \to J(\mathbb{F}_q) \times \mathbb{Z} \to 0$,

so $Cl_m \cong \mathbb{Z} \times \Phi$ $\Phi \supset \text{Local}$, <u>finite</u>.

So ℓ-rank of $Cl_m/\ell Cl_m$ is $\geq 1 + \sum d_P - \varepsilon$.

There is a <u>hyperplane</u> $Cl_m/\ell Cl_m$ (as $\mathbb{F}_\ell$-vector sp.) containing all the P_i; this gives the desired extension.

Given K_α/K, assuming no constant-field extn. corresps to the condn:

$$\begin{array}{ccc} Cl_m & \xrightarrow{\deg} & \mathbb{Z} \\ & \searrow^{\alpha} & \\ & & G \end{array}$$

$\deg : \operatorname{Ker}\alpha \to \mathbb{Z}$ is surjective.

In this case, I want the genus of K_α.

Look at characters $\chi : G \to \mathbb{C}^\times$. This gives maps

$$U_P \to Cl_{m} \to G \xrightarrow{\chi} \mathbb{C}^\times .$$

So exp. of cond. of χ at $P = f_P(\chi) = \begin{cases} 0 & \text{if } U_P \to \mathbb{C}^\times \text{ is trivial} \\ \text{smallest } e \text{ s.t. } U_P \to \mathbb{C}^\times \text{ is trivial on } U_P^{(e)} \end{cases}$.

So Formula for the genus g_α of K_α:

$$2g_\alpha - 2 = [K_\alpha : K](2g-2) + \deg(\text{discriminant ideal})$$

and $\quad \text{disc} = \sum_{P,\chi} f_P(\chi)\cdot P$,

so we get

$$\boxed{2g_\alpha - 2 = |G|(2g-2) + \sum f_P(\chi)\deg P}$$

In our situation: $g = 2$, $\ell = 2$, $|G| = 2$

At each P we get one number f_P (only one character!).

On the other hand, we've noted that writing

$$y^2 + y = \frac{a_0}{t^m} + \dots = \varphi \quad m \text{ odd} \geq 1,$$

the local contrib was measured by:

Have: $\boxed{f_p = m+1}$

"Proof": I get $\quad U_p \longrightarrow \{\pm 1\} = \mathbb{Z}/2\mathbb{Z}$

explicitly: $\quad u \in U_p$ can be viewed as $u(t) \in \mathbb{F}_{2^e}[[t]]$; then the map is

$$u(t) \longmapsto \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}\left(\mathrm{Res}\left[\varphi(t)\frac{du(t)}{u(t)}\right]\right)$$

(For an Artin-Schreier extn as above!)

Then, if $\quad u \equiv 1 \mod t^{m+1}$

$$\frac{du}{u} = c\,t^m\,dt + \dots$$

$$\varphi\,\frac{du}{u} \text{ hol., so } \mathrm{Res} = 0$$

But if $\; u \equiv 1 \mod t^m$, not $\mod t^{m+1}$, will get simple pole, hence $\mathrm{Res} \neq 0$.

2-rank of $U_p/U_p^{(n_p)}$ $\qquad$ n_p even ≥ 2

res field $\mathbb{F}_{2^e}$

$U_p/U_p^{(n_p)} = \{ \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} \mod t^n \}$ $\qquad$ $\alpha_0 \neq 0 \Rightarrow \alpha_0 \in \mathbb{F}_{2^e}^*$, $\alpha_i \in \mathbb{F}_{2^e}$

for 2-rank, think only

$1 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1}$ $\qquad$ $\alpha_i \in \mathbb{F}_q = \mathbb{F}_{2^e}$, so

order $= q^{n-1}$

squares : $\underbrace{1 + \alpha_1^2 t^2 + \cdots}$ = those where $\alpha_1 = \alpha_3 = \cdots = 0$)

there are $\frac{n}{2}$ odd indices, so order $= q^{n/2 - 1}$

So : $|G/G^2| = q^{n/2}$, so 2-rank $= e \cdot \frac{n}{2}$.

This proves the statement made last time about constructing extensions where certain points split. (Just check that #points < $\sum d_p - \epsilon$)

Optimal functions for number of points

$\mathbb{F}_q$, genus g, N points

(*) If $c_n \geq 0$, and $f = 1 + \sum 2c_n \cos n\theta \geq 0$ for all θ
$= 1 + \sum c_n (t^n + t^{-n})$, $t \in S^1$ unit circle.

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

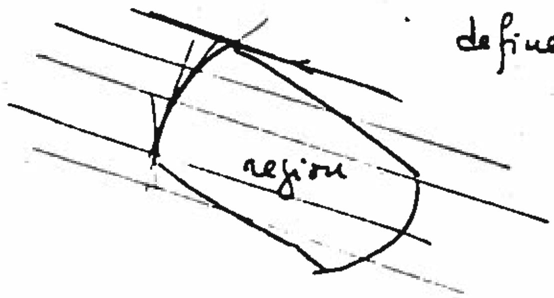
Problem: Knowing N and q, what is (if any) the best choice of (c_n)? (I.e., the one that maximizes the expression.)

If $(c_n) \in (*)$, what is the max of $\sum c_n \left((N-1) q^{-n/2} - q^{n/2} \right)$?

Call the max $g(N, q)$ $-\sum c_n$

This is a linear programming question:

given variables, linear inequalities on them
$\underbrace{\hphantom{linear inequalities on them}}$ defines some convex region



given linear form $\longleftrightarrow$ cut region by lines

look for max. value.

In linear programming, every problem has a dual problem. So let's introduce the dual problem, but in a more natural way.

Suppose we want $\geq N$ pts, $g \to$ genus?

We must have then $N_n \geq N$, $\forall n$. $\left(N_n = \# X(\mathbb{F}_{q^n}) \right)$

If $\varphi_1, \ldots, \varphi_g$ are the angles of Frob.

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

So $$q^n + 1 - q^{n/2} \sum_{\alpha=1}^{g} 2\cos n\varphi_\alpha \geq N$$

Introduce the measure on S^1 $\mu = \sum \left(\delta_{e^{i\varphi_\alpha}} + \delta_{e^{-i\varphi_\alpha}} \right)$ δ = Dirac measure.

$\mu \geq 0$, $\mu(S^1) = 2g$.

Then $$\sum_{\alpha=1}^{g} 2\cos n\varphi_\alpha = \int t^n \mu(t) \quad \left[= \int \tfrac{1}{2}(t^n + t^{-n}) \mu(t) \right.$$

So I'm looking for $\mu \geq 0$ on S^1 with

$$\int t^n \mu(t) \leq \underbrace{q^{n/2} - (N-1) q^{-n/2}}_{\gamma_n} \qquad n = 1, 2, \ldots$$

So look at all

$$\boxed{\mu \geq 0, \quad \underbrace{\int t^n \mu(t) \leq \gamma_n}_{(**)_n} \quad n = 1, 2, \dots} \qquad (**),$$

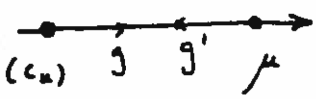
and ask what is the lower bound of $\frac{1}{2}\int 1\,\mu(t)$?

Call it $g'(N, q)$

This is the dual problem.

Lemma 1: If $\mu \in (**)$, $(c_n) \in (*)$, then

$$-\sum c_n \gamma_n \leq \int \tfrac{1}{2}\mu(t).$$



In particular, $g(N,q) \leq g'(N,q)$

Lemma 2: We have equality above iff μ has support contained in the set of zeros of the fct $1 + \sum c_n (t^n + t^{-n})$ on S^1 and $(**)_n$ is an equality for every n s.t. $c_n = 0$.

Theorem: Let μ and (c_n) be such as in Lemma 2. Then $g(N, q) = \frac{1}{2}\int \mu(t) = -\sum c_n \gamma_n$.

<u>Proof</u>: Let $f = 1 + \sum c_n (t^n + t^{-n}) \geq 0$

So $\mu(f) = \int f\mu = \mu(1) + 2\sum c_n \mu(t^n) \geq 0$

But $\mu(t^n) = \int t^n d\mu \leq \gamma_n$, so

$$\mu(\tfrac{1}{2}) \geq -\sum c_n \mu(t^n) \geq -\sum c_n \gamma_n$$

QED, Lemma 1.

<u>Proof</u> (2): Want $\mu(f) = 0$ above, hence since $f \geq 0$ μ must be concentrated on the zeros.

I also want $\mu(t^n) = \gamma_n$ unless $c_n = 0$,

QED (2). ☑

<u>Example</u>: Take $q + 1 \leq N \leq q^{3/2} + 1$

<u>Claim</u>: in this range Weil is optimal.

Weil $\longleftrightarrow$ $1 + \cos\theta$, so $\underline{c_1 = \frac{1}{2},\ c_n = 0,\ n \geq 2}$

<u>Claim</u>: this choice is optimal.

It is enough to exhibit a μ with equality!

We want $g = -\frac{1}{2}\gamma_1 = -\frac{1}{2}\left(q^{1/2} - (N-1)q^{-1/2}\right)$

$$= \frac{1}{2}\left((N-1)q^{-1/2} - q^{1/2}\right) \geq 0$$

And take μ = Dirac at $t=-1$ (angle $\theta = \pi$) with weight $2q$, where q is given by this last eqn.

To check: $\begin{cases} 1+\cos\theta \geq 0 \quad \text{OK}, \quad c_n \geq 0 \quad \text{OK} \\ \text{so } (*) \text{ OK.} \end{cases}$

$\begin{cases} \text{clearly } \mu \text{ is concentrated at the zero of } 1+\cos\theta \\ \text{to check: } \begin{cases} \mu(t^n) \leq \gamma_n \quad \text{for } n \geq 1 \\ \mu(t) = \gamma_1 \end{cases} \end{cases}$

$\mu(t) = 2q(-1) = -2q$

to check $-2q = \gamma_1$ OK by construction

$\mu(t^2) = 2q(-1)^2 = -\gamma_1 \overset{?}{\leq} \gamma_2$

$$-\gamma_1 = -q^{1/2} + (N-1)q^{-1/2} \overset{?}{\leq} q - (N-1)q^{-1} = \gamma_2$$

$$(N-1)(q^{-1/2} + q^{-1}) \overset{?}{\leq} q + q^{1/2}$$

$$(N-1)(1+q^{1/2}) \overset{?}{\leq} q^{3/2}(1+q^{1/2})$$

$$(N-1) \overset{?}{\leq} q^{3/2} \qquad \underline{\text{OK}} \text{ by } \underline{\text{condition on}}$$

$$\mu(t^3) = -2g = \gamma_1 \overset{?}{\leq} \gamma_3 \qquad \gamma_3 \geq 0,\ -2g < 0 \ \text{ ok}.$$

$$\mu(t^4) = 2g = -\gamma_1 \leq \underbrace{\gamma_2 \leq \gamma_4}$$

γ_n increases for n large.

and larger n are similarly ok. ▨

Theorem on Linear Inequalities on $\mathbb{R}^n$:

Let f_α be finitely many additive functions $(\sum \alpha_i x_i + \beta)$ on $\mathbb{R}^n$. Then the following are equiv.:

(i) The equations $f_\alpha \geq 0$ have no common solution.

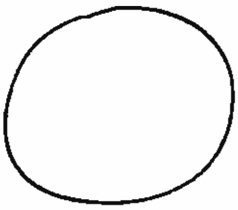
(ii) $\exists\, c_\alpha \geq 0$ s.t. $1 + \sum c_\alpha f_\alpha = 0$ identically in $\mathbb{R}^n$.

11/7 Oesterlé's "Optimal" computation of lower bound for g (given N, q)

On Machine: $\left\{\begin{array}{ll} \text{ON} & \\ \text{RUN 2000} & \\ \text{NOMBRE DE POINTS?} & 65 \text{ enter} \\ \text{Q ?} & 8 \quad " \\ \text{GENRE} >= 14 & \end{array}\right.$

<u>Recall</u>: Last time we defined a "dual" problem to what we wanted, and saw that

$$\left.\begin{array}{c}\text{admissible } \mu \text{ measure} \\ + \\ \text{admissible } (c_n)\end{array}\right\} \text{match} \longrightarrow \text{optimal solution.}$$



$S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

admissible μ $\left[\begin{array}{l} \mu \text{ will be a positive measure on } S^1 \text{ s.t.} \\ \bullet \text{ symmetric w.r.t } z \mapsto \bar{z} = z^{-1} \\ \bullet \int t^n \mu(t) = \langle t^n, \mu \rangle \geq q^{n/2} - (N-1) q^{-n/2} \\ \qquad \text{for } n \geq 1 \end{array}\right.$

(Where N, q are given).

admissible (c_n) $\left[\begin{array}{l} c_n \geq 0 \\ 1 + \sum_{n \geq 1} c_n (t^n + t^{-n}) \geq 0 \text{ on } S^1 \end{array}\right.$

We attach

$$\begin{cases} \mu \longmapsto \frac{1}{2}\int \mu(t) = \langle \frac{1}{2}, \mu \rangle \\ (c_n) \longmapsto \sum c_n \left((N-1) q^{-n/2} - q^{n/2} \right) \end{cases} \geq$$

We say μ and (c_n) match if $\frac{1}{2}\int \mu(t) = \sum c_n(\quad)$; if this happens, the common value is the best $g(N,q)$ that the explicit formula can give.

(Usually not even rational, of course...)

Oesterlé found an explicit choice of (c_n) (working for every (q,N)), an explicit choice of μ (working for $q \geq 3$ and sometimes for $q=2$), and they match.

Hence, this gives $g(N,q)$, at least for $q \geq 3$.

• Let $\lambda = N-1$, $\alpha = q^{1/2}$

So condn. on μ is $\int t^n \mu(t) \geq \alpha^n - \lambda\alpha^{-n}$, $n \geq 1$

We showed $\begin{cases} \lambda \leq \alpha^3 \longrightarrow \text{Weil estimate is best} \\ \quad \text{(i.e., optimal is given by } 1+\frac{1}{2}(t+t^{-1}) = 1+\cos\varphi \text{)} \\ \lambda = \alpha^4 \longrightarrow \text{Suzuki (char = 2)} \\ \lambda = \alpha^6 \longrightarrow \text{Ree} \end{cases}$

Method:

Define m by $\boxed{\alpha^m < \lambda \leq \alpha^{m+1}}$. $\left(m = \left[\frac{\log \lambda}{\log \alpha}\right]\right)$

I will assume $m \geq 2$. (if not, $g = 0$ is OK ...)

Put $u = \dfrac{\alpha^{m+1} - \lambda}{\lambda\alpha - \alpha^m}$; by the assumptions, $0 \leq u < 1$.

Consider the equation:

$$\cos \frac{m+1}{2}\varphi + u \cos \frac{m-1}{2}\varphi = 0$$

There is exactly one solution φ_0 in the range $\frac{\pi}{m+1} \leq \varphi_0 < \frac{\pi}{m}$.

Then the optimal g (for $q \geq 3$, at least) is

$$\boxed{g = \frac{(\lambda-1)\alpha \cos \varphi_0 + \alpha^2 - \lambda}{\alpha^2 - 2\alpha \cos \varphi_0 + 1}}$$

(When $q = 2$, this is the value given by a choice of (ε_n).)

We try to find μ of the following shape:

concentrated on a symmetric set $T \subset S^1$, with $|T| = m-1$, with

(7) $$\int t^n \mu(t) = \alpha^n - \lambda\alpha^{-n} \quad \text{for } n = 1, \ldots, m-1,$$

and the mass ν_t of $t \in T$ being strictly positive. We also need $\nu_t = \nu_{\bar t}$, of course.

On the other hand, look for (c_n) s.t.

$$f(t) = 1 + \sum_{n=1}^{m-1} c_n (t^n + t^{-n}) \quad \text{is } \underline{\text{zero}} \text{ on } T$$

$(c_n \geq 0,\ f(t) \geq 0$ on $S^1)$.

If we can do this, we have a match (as seen before).

__Lemma__ If T satisfies the condition (T), then T is __contained__ in the set of solutions of

$$t^{m+1} + 1 + u(t^m + t) = 0 \qquad (1)$$

(This has $m+1$ solutions on S^1, which are symmetric, so to get T we need to discard one pair).

Rewrite as $t = e^{i\varphi}$, get the equation for u given above.

So we throw out the solutions $t = e^{\pm i\varphi_0}$:

T = solutions of (1) which are different from $e^{\pm i\varphi_0}$.

Proof of Lemma: Suppose T is given.

T has $m-1$ elements in S^1.

$\mu = \sum \nu_t \delta_t$ so the integral is $\sum_{t\in T} \nu_t t^n = \alpha^n - \lambda\alpha^{-n}$ $n=1,\dots,m-1$

The system $\boxed{\sum_{t\in T} \nu_t t^n = \alpha^n - \lambda\alpha^{-n} \qquad n=1,\dots,m-1}$ (*)

has $(m-1)$ linear eqns, $(m-1)$ unknowns, determinant is Van der Monde t $(t\in T)$, so $\neq 0$.

So it has a unique solution $\nu_t = $ ——

Now force $\nu_t = \bar{\nu}_t$ for every $t \in T$. This will imply equation (1).

Rewrite (*) as follows:

(*) $\Longleftrightarrow$ for every polynomial Φ of degree $\le m-1$, with constant term 0,

$$\boxed{\sum \nu_t \Phi(t) = \Phi(\alpha) - \lambda\Phi(\alpha^{-1})}. \qquad (**)$$

Let
$$P(x) = \prod_{t\in T}(x-t)$$

T symmetric $\Rightarrow$ $P(x^{-1}) = P(x)\,x^{1-m}$

$$-\frac{1}{x^2}P'(x^{-1}) = P'(x)\,x^{1-m} + (1-m)P(x)x^{-m}$$

So if $t \in T$, $-\frac{1}{t^2} = \bar{t}^2$:

$$\boxed{-\bar{t}^2 P'(\bar{t}) = P'(t)\, t^{1-m}}$$

Let $t \in T$; define $Q_t(x) = x \prod_{\substack{t' \in T \\ t' \neq t}} (x - t') = \dfrac{x P(x)}{x - t}$

Now $\begin{cases} Q_t(t') = 0 & \text{for } t' \in T,\ t' \neq t. \\ Q_t(t) = t P'(t) \end{cases}$

Apply (**) to $\Phi = Q_t$:

get $\quad \nu_t Q_t(t) = Q_t(\alpha) - \lambda Q_t(\alpha^{-1})$

so $\quad \boxed{\nu_t = \dfrac{Q_t(\alpha) - \lambda Q_t(\alpha^{-1})}{t P'(t)}}$

rewrite :

$$t P'(t) \nu_t = \frac{\alpha P(\alpha)}{\alpha - t} - \lambda \frac{\alpha^{-1} P(\alpha^{-1})}{\alpha^{-1} - t}$$

we have $\quad P(\alpha^{-1}) = P(\alpha)\, \alpha^{1-m}$

so $\quad t P'(t) \nu_t = P(\alpha) \left\{ \dfrac{\alpha}{\alpha - t} - \lambda \dfrac{\alpha^{-m}}{\alpha^{-1} - t} \right\}$

$$t P'(t)\, \nu_t = P(\alpha) \frac{1-\alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1-\alpha t - \alpha^{-1}t + t^2}$$

Now $\nu_t = \nu_{\bar t} \longrightarrow \frac{1}{tP'(t)} \cdot \frac{1-\alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1-\alpha t - \alpha^{-1}t + t^2} = \frac{1}{\bar t P'(\bar t)} \frac{1-\alpha\bar t - \lambda\alpha^{1-m} + \bar t\lambda\alpha^{-m}}{1-\alpha\bar t - \alpha^{-1}\bar t + \bar t^2}$

Also $-P'(\bar t) = P'(t) \cdot t^{3-m}$, so

$$\frac{1}{t} \cdot \{\text{———}\} = \frac{-1}{t^{2-m}} \cdot \{\text{———}\}$$

so $-t^{1-m} \cdot \{\text{———}\} = \{\text{———}\}$

$$-t^2 (1 - \alpha\bar t - \alpha^{-1}\bar t + \bar t^2) = 1 - \alpha t - \alpha^{-1} t + t^2$$

So end up with

$$-t^{m+1} (1 - \alpha\bar t - \lambda\alpha^{1-m} + \lambda\alpha^{-m}\bar t) = (1 - \alpha t - \lambda\alpha^{1-m} + \lambda\alpha^{-m} t)$$

$$t^{m+1}(1-\lambda\alpha^{1-m}) + t^m(\lambda\alpha^{-m} - \alpha) - t(\alpha - \lambda\alpha^{-m}) + (1-\lambda\alpha^{1-m}) =$$

$$u = \frac{\alpha^{m+1} - \lambda}{\lambda\alpha - \alpha^m} = \frac{\alpha - \lambda\alpha^{-m}}{\lambda\alpha^{1-m} - 1}$$

So

$$t^{m+1} + 1 + u(t^m + t) = 0. \quad \blacksquare$$

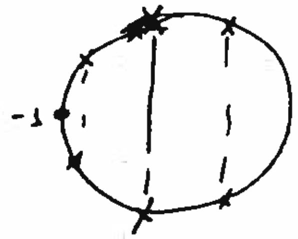
Note this works for any m ; our choice of m is equiv to $u \in [0,1)$.

Now, study the equation $\cos\frac{m+1}{2}\varphi + u\cos\frac{m-1}{2}\varphi = 0$, where $0 \le u < 1$.

$$F(\varphi) = \frac{\cos\frac{m+1}{2}\varphi}{\cos\frac{m-1}{2}\varphi}$$

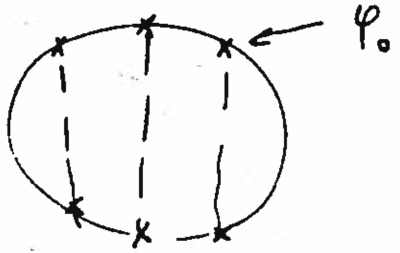
(We want to show $t^{m+1}+1+u(t^m+t)=0$ has $m+1$ distinct solutions on S^1, and "locate" them.)

if m is even : -1 is a solution



$(m = 6)$

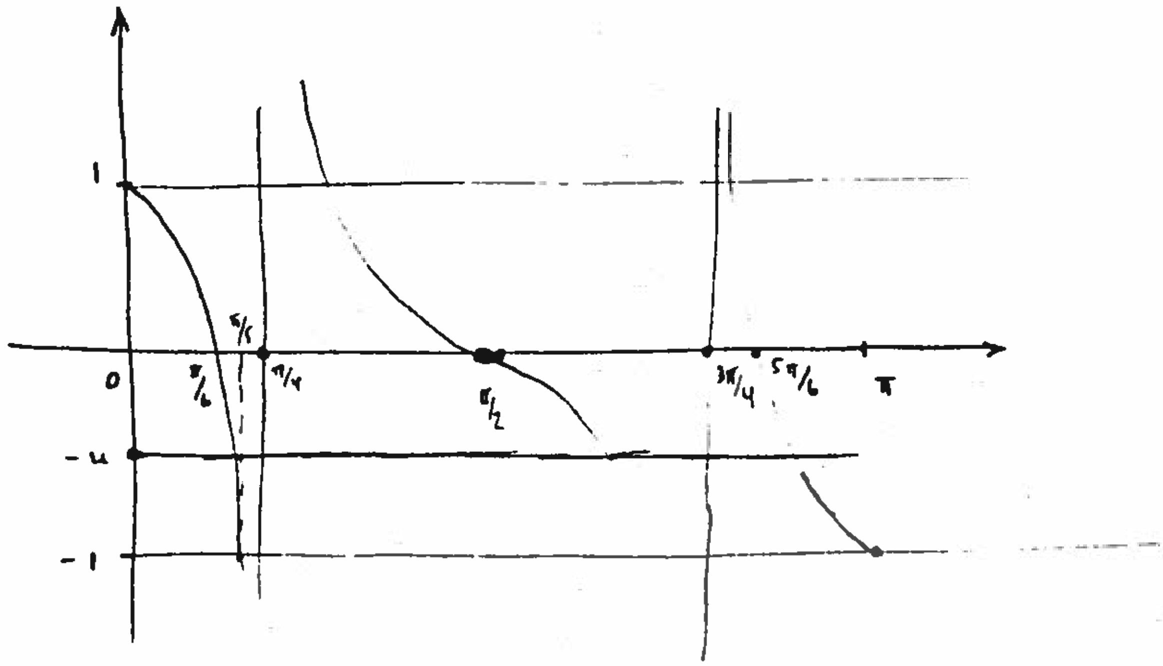
if m is odd : -1 is not a solution



$m = 5$

Take $n = 5$, for instance.

Graph on $0 \le \varphi \le \pi$ of $F(\varphi) = \dfrac{\cos 3\varphi}{\cos 2\varphi}$



$\cos 2\varphi = 0 \iff 2\varphi = \frac{\pi}{2}, \frac{3\pi}{2} \Rightarrow \varphi = \frac{\pi}{4}$ or $\frac{3\pi}{4}$

$F(\pi/5) = \dfrac{\cos 3\pi/5}{\cos 2\pi/5} = -1$ (since $3\pi/5 + 2\pi/5 = \pi$)

Given $u \in [0,1)$, I want $F(\varphi) = -u$ 3 times

We know: the first soln. is φ_0, $\frac{\pi}{6} \le \varphi_0 < \frac{\pi}{5}$

and that is the only soln in that interval.

(And the same happens from any n).

So we know:

the eqn. $t^{m+1} + 1 + u(t^m + t) = 0$ has exactly $m+1$ solns. on S^1, and exactly one of the form $e^{i\varphi_0}$, $\frac{\pi}{m+1} \leq \varphi_0 < \frac{\pi}{m}$.

Define T as the complement of $e^{i\varphi_0}$, $e^{-i\varphi_0}$ in the set of roots of the equation.

Define ν_t by solving the system of equations
$$\sum \nu_t t^n = \alpha^n - \lambda\alpha^{-n}, \quad n = 1, \ldots, m-1$$
(we even have an explicit formula).

We prove: $\nu_t > 0$ all t (computations).

Admissibility means $\sum \nu_t t^n \leq \alpha^n - \lambda\alpha^{-n}$ for $n = m, m+1$,

This is a long computation; it shows: OK if $\alpha \geq \sqrt{3}$, i.e. $g \geq 3$.

Also OK if $\alpha = \sqrt{2}$ and $n = m, m+1$ (but not always of $\alpha = \sqrt{2}$, $n = m+2$, $n \geq m+3$, OK again!)

Up to $\lambda =$ [redacted] $\sqrt{}^{130}$, bad N's are
51, 52, 53
70, 71, ..., 77
98, 99, .. 110
137, ...

Guess: bad if: $\frac{\log\lambda}{\log\alpha} \simeq$ integer $\times$ 0.4

$N = 50$, $g \geq 65$; $N = 54$, $g \geq 72$

(For bad N's, Oesterlé's result is not optimal.)

Now to give $f = 1 + \sum c_n (x^n + x^{-n})$ which will match.

Take $P(x) = \prod_{t \in T} (x - t)$; write

$$P(x)P(x^{-1}) = \sum_{-(m-1)}^{m-1} a_n x^n \quad , \; a_n > 0$$

Defn: $f(x) = \frac{1}{a_0} P(x)P(x^{-1})$

$$\therefore \quad c_n = \frac{a_n}{a_0}$$

To compute a_n

$$\begin{cases} a_n = (m-n)\cos n\varphi_0 \sin\varphi_0 + \sin(m-n)\varphi_0 \\ a_0 = m\sin\varphi_0 + \sin(m\varphi_0) \end{cases}$$

Finally

$$\frac{1}{2}\sum y_t = g = \sum c_n (\lambda\alpha^{-n} - \alpha^n)$$ (by the formulas!)

and we end up with $g = \dfrac{(\lambda - 1)\alpha\cos\varphi_0 + \alpha^2 - \lambda}{\alpha^2 - 2\alpha\cos\varphi_0 + 1}$.

[Recall : the zeta fct of a curve is

$$\frac{\prod_{\alpha=1}^{2g} (1 - q^{1/2} e^{i\varphi_\alpha} T)}{(1-T)(1-qT)}$$

ν_t is connected to $\quad \prod (1 - q^{1/2} t T)^{\nu_t}$

So numberfield analog: replace the zeros of ζ by a measure.]

<u>Remark</u> : If λ <u>large</u> w.r.t. α $(= q^{1/2})$

Then $\varphi \approx 0$, so get $g \approx \dfrac{\lambda\alpha - \lambda}{(\alpha-1)^2} = \dfrac{\lambda}{\alpha - 1}$

So we expect $g \approx \dfrac{N}{\sqrt{q} - 1}$.

A better approx comes from $\varphi \simeq \dfrac{\pi}{m}$, $m \sim \dfrac{\log \lambda}{\log \alpha}$.

Then : for large λ,

$$g \geq \frac{\lambda}{\alpha - 1} - \frac{\pi^2}{2} \frac{\alpha(\alpha+1)}{(\alpha-1)^3} \frac{\lambda}{(\log \lambda)^2} + O\left(\frac{\lambda}{(\log \lambda)^3}\right)$$

11/21 We look at $q = 2$ with varying g

① Upper bounds for N

Use the explicit formula

given $f(\theta) = 1 + \sum c_n 2\cos n\theta$, $c_n \geq 0$, $f(\theta) \geq 0$,

we have
$$g \geq (N-1)\sum c_n q^{-n/2} - \sum c_n q^{n/2} .$$

Start with the example
$$f(\theta) = \frac{1}{c}\sum (1 + 2x_1 \cos\theta + \cdots + 2x_m \cos m\theta)^2$$
$$x_i \geq 0 \quad , \; c = 1 + 2x_1^2 + \cdots + 2x_m^2 .$$

1st choice : $x_1 = 1$, $x_2 = 0.7$, $x_3 = 0.2$

gives $N \leq 0.83\, g + 5.35$

$g = 1 \rightarrow$ not good $N \leq 6$ ($N = 5$ is best)

$g = 2, 3, \ldots, 11 \implies$ bound given (except for $g = 7$, $N \leq 11$, and $N = 10$ is best).

e.g., $g = 5 \implies N \leq 4.15 + 5.35 \leq 9.50 \longrightarrow N \leq 9$ and we'll construct curves ~~[illegible]~~ later.

2nd choice: $x_1 = 1.05$, $x_2 = 0.8$, $x_3 = 0.4$

$$N \leq 0.766g + 5.97$$

for $g = 13, \dots, 20$ gives same as Oesterlé

3rd choice: 1, 0.8, 0.6, 0.4, 0.1

$$N \leq 0.6272g + 9.562$$

for $g = 50$, $N \leq 31.36 + 9.562 = 40.9\dots$

so $N \leq 40$.

This justifies all the upper bounds on the table except for $g = 7$. tables: see pp. Se Th 38b, 38c

$g = 7$: bound given by explicit fla is 11

Theorem: A curve with $N = 11$ does not exist.

Proof: Let C be such a curve.

What is its zeta function?

Eigenvalues of Frob are $\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2, \text{—}, \pi_7, \bar{\pi}_7$.

We'll know ζ if we know N over $\mathbb{F}_2, \dots, \mathbb{F}_{2^7}$; if a_d = # closed pt's of deg d.

Need: $a_1, a_2, \text{—}, a_7$.

Know: $a_1 = 11$

Maximal number of points of a curve of genus g over the field $\mathbb{F}_2$

g	Max. nber
0	3
1	5
2	6
3	7
4	8
5	9
6	10
7	10
8	11
9	12

g	Max. nber
10	12 or 13
11	13 or 14
12	14 or 15
13	14 or 15
14	15 or 16
15	17
16	16, 17 or 18
17	17 or 18
18	18 or 19
19	20

g	Max. nber
20	19, 20 or 21
21	21
...	
39	33
...	
50	40

Bounds for N = Max. Nber

$$N \leq 0.83\,g + 5.35$$

$$N \leq 0.766\,g + 5.97$$

$$N \leq 0.6272\,g + 9.562$$

Se Th 38c

Upper bound for the number of points of a curve of genus g over the field F_2

This upper bound is the one obtained by the " explicit formula " using Oesterlé's trigonometrical polynomial.

g :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
N ≤	5	6	7	8	9	10	11	11	12	13	14	15	15	16	17	18
g :	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
N ≤	18	19	20	21	21	22	23	23	24	25	25	26	27	27	28	29
g :	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
N ≤	29	30	31	31	32	33	33	34	35	35	36	37	37	38	38	39
g :	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
N ≤	40	40	41	42	42	43	43	44	45	45	46	47	47	48	48	49
g :	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
N ≤	50	50	51	51	52	53	53	54	54	55	56	56	57	57	58	59
g :	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
N ≤	59	60	60	61	62	62	63	63	64	65	65	66	66	67	68	68
g :	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
N ≤	69	69	70	70	71	72	72	73	73	74	75	75	76	76	77	77
g :	113	114	115	116	117	118	119	120								
N ≤	78	79	79	80	80	81	82	82								

Let $f = \frac{25}{109}(1+\cos\theta)(1+\frac{6}{5}\cos\theta+\frac{6}{5}\cos 2\theta)^2$

$$= 1 + \sum 2c_n \cos n\theta$$

$$c_1 = \frac{98}{109}, \ldots, \quad c_5 = \frac{9}{218}$$

We have

$$\sum_{d=2}^{5} d a_d \sum_{n \equiv 0 (d)} c_n q^{-n/2} \leq g + \sum c_n q^{-n/2} - (N-1)\sum c_n q^{n/2}$$

$$0.743 a_2 + 0.408 a_3 + 0.165 a_4 + 0.036 a_5 \leq 7 + 4.577 -$$
$$- 11.506$$
$$\leq 0.069$$

This implies $\boxed{a_2 = a_3 = a_4 = 0, \quad a_5 \leq 1.}$

Have a_6 and a_7 to consider, still:

Let $a_5 = \alpha$, $a_6 = \beta$, $a_7 = \gamma$ (so $\alpha = 0$ or 1).

Have $\pi_1, \text{—}, \pi_7$, $\quad u_i = \pi_i + \bar{\pi}_i$

Define $f(T) = \prod_{i=1}^{7} (T - u_i) \in \mathbb{Z}[T]$.

this has real roots in the interval $[-2\sqrt{2}, 2\sqrt{2}]$.

Writing $f(T)$ in terms of α, β, γ :

$$f(T) = T^7 + 8T^6 + 21T^5 + 14T^4 - 19T^3 + (\alpha - 20)T^2 +$$
$$+ (8\alpha + \beta - 5)T + 31\alpha + 8\beta + \gamma - 106 .$$

Theorem: Such a polynomial $f_{\alpha\beta\gamma}$ with $\alpha, \beta, \gamma \in \mathbb{Z}$, $\alpha = 0$ or 1, has all its ~~roots~~ roots real and in $[-2\sqrt{2}, 2\sqrt{2}]$ if and only if $(\alpha, \beta, \gamma) = (0, 11, 22)$.

[Sturm $\to$ condition for $f_{\alpha\beta\gamma}$ to have roots in some interval]

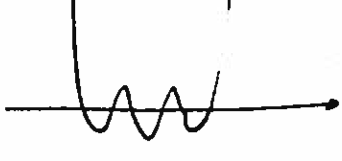
$f_{\alpha\beta\gamma}$ all roots real $\longrightarrow$ derivative also has real roots

So first check that $f'''(T)$ does have four real roots.

Have $\alpha = 0$ or $\alpha = 1$.

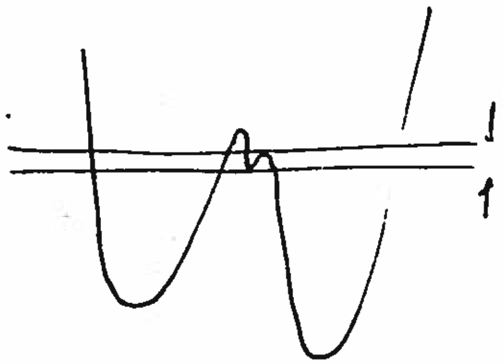
$\alpha = 0$ take $f''(T)$ is ok.

know $f'(T)$ up to translation



to adjust the constant, look at highest min, lowest max

E.g.



constant must make x-axis lie here

This gives : $\begin{cases} \text{if } \alpha = 1, & 5 \le \beta \le 10 \\ \text{if } \alpha = 0 & 9 \le \beta \le 13 \end{cases}$

This gives only eleven cases : look one-by-one at $f(T)$ in the same way.

Find $\alpha = 1$ not possible.

$\alpha = 0, \beta = 11, \gamma = 22$ works (by a hair). $\boxtimes$

(Conditions are $\gamma \le 22$, $\gamma \ge 22$, $\gamma \le 22$, $\gamma \ge 22$, $\gamma \le 25$, $\gamma \ge 18$, $\gamma \ge -9650$).

We find
$$f = T^7 + 8T^6 + 21T^5 + 14T^4 - 19T^3 - 20T^2 + 6T + 4$$
$$= \underbrace{(T+2)(T^2+2T-2)}_{}\underbrace{(T^2+T-1)(T^2+3T+1)}_{}$$
$$= \quad g(T) \quad \cdot \quad h(T)$$

then g, h generate $\mathbb{Z}[T]$

So if u_1, u_2, u_3 roots of g, u_4, u_5, u_6, u_7 roots of h, then every $u_1 - u_4, \ldots, u_1 - u_7, u_2 - u_4, \ldots, u_3 - u_7$ is a unit

$g = 0$ is no fun

$g = 1$ we've seen, $g = 2$ too

Formulae: $g = 1: \quad y^2 + y = x^3 + x$

$g = 2: \quad y^2 + y = \dfrac{x^2 + x}{x^3 + x + 1}$

$\underline{g = 3}$ if hyperelliptic, at most 6 pts (in general, th hyperelliptic curves have too few pts).

if not, it is a plane quartic in $\mathbb{P}^2$, which itself has 7 points!

So take $[x, y, z]$ homog. coords, find a polyn which passes through all pts:

get $x^3y + y^3z + z^3x + x^2y^2 + y^2z^2 + z^2x^2 + x^2yz + y^2zx$

need to prove: $\underline{\text{nonsingular}}$ (hence $g = 3$) and goes through all pts.

(since $x, y, z \in \mathbb{F}_2 \Rightarrow x^2 = x$, etc., so just

$\cancel{xy} + \cancel{yz} + \cancel{zx} + \cancel{xy} + \cancel{yz} + \cancel{zx} + \cancel{xyz} + \cancel{xyz} = 0$!)

To check it's nonsingular, need only check irreducibility. For that: exists an automorphism of $\mathbb{P}_2$ of order 7 fixing the curve.

This implies irreducibility.

e.g., $u_2 = -1 + \sqrt{3}$ $\quad u_4 = \frac{-1+\sqrt{5}}{2}$

$$u_2 - u_4 = -\tfrac{1}{2} + \sqrt{3} - \tfrac{\sqrt{5}}{2}$$

multiply be this w/ $-\sqrt{3}$ $\longrightarrow \left(-\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^2 - 3 = \frac{3\sqrt{5}}{2} - 3$

$= \frac{-3+\sqrt{5}}{2}$ unit.

etc.

So $f = g \cdot h$, g & h generate $\mathbb{Z}[T]$, and this is impossible for a Jacobian, so the curve C does not exist. ✓ ▨

Next unknown case is $g = 10$: analogous method on a computer gave 100 or 200 polynomials...

Construction of Examples

We want to construct curves

g	0	1	2	3	4	5	6	7	8	9	10	...
N	3	5	6	7	8	9	10	10	11	12	12 or 13	

bd = 13
have curve = 12

Exercise: Prove that minimum no. of points is 3 when $g = 0$, 1 when $g = 1$, 0 when $g \geq 2$.

$g=0$ is no fun

$g=1$ we've seen, $g=2$ too

Formulas : $g=1$: $y^2+y=x^3+x$

$g=2$: $y^2+y=\frac{x^2+x}{x^3+x+1}$

$g=3$ if hyperelliptic, at most 6 pts (in general, th hyperelliptic curves have too few pts).

if not, it is a plane quartic in $\mathbb{P}^2$, which itself has 7 points!

So take $[x,y,z]$ homog. coords, find a polyn which passes through all pts:

get $x^3y+y^3z+z^3x+x^2y^2+y^2z^2+z^2x^2+x^2yz+y^2zx$

need to prove: nonsingular (hence $g=3$) and goes through all pts.

(since $x,y,z\in\mathbb{F}_2 \Rightarrow x^2=x$, etc., so just

$\cancel{xy}+\cancel{yz}+\cancel{zx}+\cancel{xy}+\cancel{yz}+\cancel{zx}+\cancel{xyz}+\cancel{xyz}=0$!)

To check it's nonsingular, need only check irreducibility. For that: exists an automorphism of $\mathbb{P}_2$ of order 7 fixing the curve.

This implies irreducibility.

This is a <u>twist</u> of the Klein curve

$G = SL_3(\mathbb{F}_2) = GL_3(\mathbb{F}_2)$ order 168

G acts on $\mathbb{P}_2$; to find inv. polynomials

do:

$$Q_4(x,y,z) = \frac{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^8 & y^8 & z^8 \end{vmatrix}}{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^4 & y^4 & z^4 \end{vmatrix}}$$ has degree 4

= product of all the linear forms

this gives the Klein curve

This has no rat'l point.

If we twist it by a $C_7 \subset G$, we get the curve above. (i.e., wrt $\begin{array}{c}\mathbb{F}_{2^7} \\ | \, C_7 \\ \mathbb{F}_2\end{array}$

For $\underline{g=4}$: if not hyperelliptic, can. embedding in $\mathbb{P}_3$
then curve = inters. of surfaces

curve = (quadric $\underbrace{\text{surface}) \cap (}$cubic surface)

transversal inters, but surfaces can have singularities.

if quadric = $\mathbb{P}_1 \times \mathbb{P}_1$, 9 pts — so not obvious once we can get

In $\mathbb{P}_1 \times \mathbb{P}_1$, the curve we want has affine eqn:

$$x^2y^3 + x^3y^2 + xy^3 + x^3y + x^2y^2 + x^2 + y^2 + 1 = 0.$$

After $g=4$, explicit construction is not practical. Use CFT instead.

Start from C_1, known.

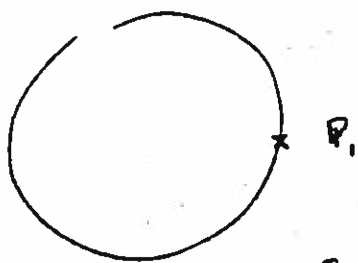
Try to find
$$\begin{array}{c} C_2 \\ \Big\downarrow \text{abelian extn.} \\ C_1 \end{array}$$

With "little" ramification ($g(C_2)$ small)

and s.t. "many" rational points split.

<u>1st case</u>: $C_1 = \mathbb{P}_1$, $g = 0$

Choose $Q \in \mathbb{P}_1$ with $\deg Q = 3$, so res. field $= \mathbb{F}_8$.



$\mathbb{F}_8^\times$ = cyclic order 7.

Take $m = Q$, look at Cl_m.

$$0 \longrightarrow \mathbb{F}_8^\times \longrightarrow Cl_m \xrightarrow[\deg]{} \mathbb{Z} \longrightarrow 0$$

CFT: finite quotients of Cl_m describe the ab. extns w/ cond. $\leq Q$.

Choose a rat'l point $R \in \mathbb{P}_1(\mathbb{F}_2)$.

$R \longmapsto Cl_m$, $\deg R = 1$

So let $G =$ quotient of Cl_m by $\langle R \rangle \cong \mathbb{F}_8^{\times}$.

So corresps to

$$\begin{array}{c} C \\ \Big\downarrow \text{⑦} \\ \mathbb{P}_1 \end{array}$$

Frob R is killed $\Rightarrow$ R splits completely giving 7 pts
(and $\Rightarrow$ no const. field extn.)

$$2g(C) - 2 = 7(-2) + \underbrace{6 \cdot 3}_{\text{sum of Artin conductors}}$$

$$2g = 2 - 14 + 18 = 6$$

So $\boxed{g = 3}$, $N = 7$

Now play the same game as follows:

take R_1, R_2 rat'l points on $\mathbb{P}_1$

$m = 4.R_2$, construct G as before, $G = Cl_m / \langle R_1 \rangle$

$\cong$ local group mod 4.

Se Th 43

get: $G \cong$ local gp mod $4R_2$

$= \{1+\alpha_1 t + \cdots + \alpha_3 t^3\} / 1+t^4$

$\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

So find $C \xrightarrow{G} \mathbb{P}_1$ s.t. : $\begin{cases} R_1 \text{ splits completely into 8 pts (rat'l)} \\ R_2 \text{ is completely ramified} \to 1 \text{ pt which is rat'l.} \end{cases}$

$$2g-2 = 8(-2) + \sum f_\chi$$

Characters on G

$\chi = 1$: $f=0$

χ trivial on t^3 : $f=2$

χ trivial on t^2 : $f=3$ twice

———— : $f=4$ four times

So $2g-2 = -16+2+6+16 = 8 \implies \boxed{g=5}$.

So this gives the curve we need for $g=5$. ☒

11/26 ($q=2$, cont.) See table, pp. SeTh 43b, 43c

Construction

Start from sth you know, say $g=0$, 3 pts, C_0

$$\begin{array}{c} C \\ \big\downarrow \text{abelian} \\ C_0 \end{array}$$

give: conductor, group G, n pts in C_0 splitting completely.

$\underline{g=50}$ $N=40$? $40=8\times 5$

So want C_0 w/ $g_0=1$, ell curve $y^2+y=x^3+x$ w/ 5 rat'l pts.

Want a covering of degree 8 in which all five pts split completely.

G = of type $(2,2,2) = (2)\times(2)\times(2)$.

First make a $(2,\dots,2)$ extension of rank 8; then $P_1,\dots,P_5$ give Frob. elements.

$(2,\dots,2) = \mathbb{F}_2^8$ has a quotient of dim 3 ($(2,2,2)$) in which $P_1,\dots,P_5 \to 0$ $\Longrightarrow$ pts split completely.

Choose a pt P_7, of degree 7 $(=8-1)$

(# pts over $\mathbb{F}_{2^7}$ is $\geq 2^7+1-2\cdot 2^{7/2} > 129-32 > 5$)

Choose conductor $\underline{m} = 2P_7$

Se Th 43b

TABLE

of curves of low genus over $\underset{\sim}{F}_2$ having many points

Each curve C is obtained as an abelian covering $C \to C_o$ of a curve C_o of lower genus, occuring earlier in the table (or of genus 0).

The table gives :

the genus g of C;

the number N of rational points of C (I underline N if it maximal for the corresponding genus);

the genus g_o of C_o;

the conductor $\underline{m}$ of $C \to C_o$ (I write $\underline{m}$ as $aP_1 + a'P_1' + bP$ where P_1, P_1', P_2 ... are distinct closed points of C_o of degree $1,1,2,\ldots$);

the Galois group G of the covering $C \to C_o$ (a cyclic group order m is denoted by (m));

the number n of rational points of C_o which split complete

the number r of rational points of C_o which are totally ra in C.

For all the cases considered in the table, we have $N = r + |G|$

g	N	g_o	$\underline{m}$	G	n	r
1	<u>5</u>	0	$4P_1$	(2)	2	1
2	<u>6</u>	0	$2P_3$	(2)	3	0
3	<u>7</u>	0	P_3	(7)	1	0
4	<u>8</u>	1	$2P_1 + 4P_1'$	(2)	3	2
5	<u>9</u>	0	$4P_1$	(2)×(4)	1	1
6	<u>10</u>	1	$2P_5$	(2)	5	0
7	<u>10</u>	1	$2P_6$	(2)	5	0
8	<u>11</u>	2	$2P_1 + 2P_4$	(2)	5	1
9	<u>12</u>	2	$2P_6$	(2)	6	0

Se Th 43c

Table (continued)

g	N	g_0	$\underline{m}$	G	n	r
10	12	2	$2P_7$	(2)	6	0
11	13	3	$12P_1$	(2)	6	1
12	14	0	$P_3 + P'_3$	(7)	2	0
13	14	3	$2P_3 + 2P_5$	(2)	7	0
14	15	0	P_4	(3)×(5)	1	0
15	$\underline{17}$	1	$10P_1$	(2)×(2)	4	1
16	16	4	$2P_9$	(2)	8	0
17	17	0	$5P_1$	(2)×(8)	1	1
18	18	5	$2P_9$	(2)	9	0
19	$\underline{20}$	1	$2P_6$	(2)×(2)	5	0
20	19	2	0	(19)	1	0
21	$\underline{21}$	0	$P_2 + P_3$	(3)×(7)	1	0
39	$\underline{33}$	1	$12P_1$	(2)×(2)×(2)	4	1
50	$\underline{40}$	1	$2P_7$	(2)×(2)×(2)	5	0

Harvard, November 1985

J-P Serre

look at $Cl_{\underline{m}}$:

$$0 \longrightarrow L_{\underline{m}} \longrightarrow Cl_{\underline{m}} \longrightarrow Cl_0 = \mathbb{Z}/(5) \times \mathbb{Z} \longrightarrow 0$$

$$L_{\underline{m}} = \mathbb{F}_{2^7}[[x]]^{\times} / \{1 + (x^2)\} = \mathbb{F}_{2^7}^{*} \times \mathbb{F}_{2^7}$$

$$Cl_{\underline{m}} / 2 Cl_{\underline{m}} = \mathbb{F}_{2^7} \times \mathbb{Z}/2 \quad \text{of type } (2, \ldots, 2), \text{ rank } 8.$$

$$\begin{tikzcd} & \tilde{C} \arrow[dl] \arrow[dd] \\ C \arrow[dr, "{(2,2,2)}"'] & \\ & C_0 \end{tikzcd}$$

: max'l $(2,2,\ldots,2)$ extension w/ cond $\le 2P_7$.

(this includes a const. field extn.)

where the 5 pts split. (I.e., choose a quotient of type $(2,2,2)$ such that pts split)

$$2g - 2 = 2^3 (2g_0 - 2) + \sum_{\chi \neq 1} \deg f_\chi$$

χ = char of order 2 so cond $= 2P_7$ or but can't be zero so $f_\chi = 1$

$$2g - 2 = 8 \times 0 + (8-1) \times 14$$

$$g = 1 + 7 \times 7 = 50.$$

With $2P_6$, would get $\overset{\text{extn }(2,2)\text{ w/}}{\sqrt{\ }}$ $4 \cdot 5 = \overset{20}{\ }$ pts and

$$2g - 2 = 0 + (4-1) \times 12$$

so $\boxed{g = 19}$.

---

with $2P_5$, get extn. of deg 2, w/

$$2g - 2 = 0 + 10 \longrightarrow \boxed{g = 6,\ N = 10}$$

$\boxed{g = 13}$ $N = 14$, $g_0 = 3$, $|G| = 2$
w/ 7 pts

$$2g - 2 = 2(6-2) + \deg f$$

$$24 = 8 + \deg f$$

So $\deg f = 16$. Must take $\underline{m} = 2P_8$ (contra table!)

table: $\underline{m}$: $2P_3 + 2P_5$ must check there is a pt of deg 3 (and one of deg 5)

take $L_{\underline{m}}$, $\mathbb{Z}$

so $rk = 1 + \deg \underline{m}$
$= 9$

so mod out as before.

• Recall construction: $\begin{array}{c} C_3 \\ 7 \downarrow \\ C_0 \cong \mathbb{P}_1 \end{array}$

res field $= \mathbb{F}_8$ ramif at a $P_3 \in C_0$

so C_3 has a pt of deg 3

$g = 20 \quad N = 19$, $g_0 = 2$, $h = 19$

$Cl_0 = \mathbb{Z} \times \mathbb{Z}/(19)$

P_1

Split so that $P_1 \to$ generator. Get an extn. by the quotient

Then $2g - 2 = 19(22 - 2) \to g = 1 + 19 = 20$.

For very large g (say $g \sim 10^{10}$) we only get N of about the same order (say $0.2 \cdot 10^{10}$) using the class field towers, as before.

For $10 \leq g \leq 20$, one might be able to fill some of the gaps.

Rational Points on Curves over Finite Fields

Part II : "g large"

Jean-Pierre Serre

Lectures given at Harvard University, September to December 1985

Notes by Fernando Q. Gouvêa

Contents - Part II

9/26 Thursday: g large.

Ihara: X genus g / $\mathbb{F}_q$, $g \geq 1$

Suppose $N(X) = q + 1 + 2g q^{1/2}$ (so q is a square).

Then: $g \leq \frac{1}{2}(q - q^{1/2})$

Proof: $N(X) = 1 + q - \sum_{\alpha=1}^{2g} \pi_\alpha$ $\qquad |\pi_\alpha| = q^{1/2}$

So we must have all $\pi_\alpha = -q^{1/2}$

So $\pi_\alpha^2 = q$, and if $N_2 = N_2(X) = \#(\mathbb{F}_{q^2})$,

$$N_2 = 1 + q^2 - \sum_{\alpha=1}^{2g} \pi_\alpha^2 = 1 + q^2 - 2gq$$

But $N_2 \geq N_1$, so $1 + q^2 - 2gq \geq 1 + q + 2gq^{1/2}$

$$q^2 - q \geq 2g(q + q^{1/2})$$

so $g \leq \frac{1}{2}(q - q^{1/2})$. $\boxed{}$

B. Segre: Curve in $\mathbb{P}_3$ given by $x^{q^{1/2}+1} + y^{q^{1/2}+1} + z^{q^{1/2}+1} = 0$

has genus $g = \frac{1}{2}(q^{1/2})(q^{1/2}-1) = \frac{1}{2}(q - q^{1/2})$.

and has $N = q^{3/2} + 1 = q + 1 + 2g q^{1/2}$.

So the bound above is exact.

Proof of $N = q^{3/2}+1$ for this curve.

Consider

$$\begin{array}{c} \mathbb{F}_q \\ 2 \Big| \\ \mathbb{F}_{q^{1/2}} \end{array} \qquad x \longmapsto \bar{x} = x^{q^{1/2}}$$

Then the eqn is $x\bar{x} + y\bar{y} + z\bar{z} = 0 \quad x, y, z \in \mathbb{F}_q$.

Hermitian form! Want: how many isotropic vectors?

E.g.: given $y, z \in \mathbb{F}_q$, want to solve

$$x\bar{x} = -(\underbrace{y\bar{y}+z\bar{z}}_{\in \mathbb{F}_{q^{1/2}}}) \text{ has (in } x) \begin{cases} 1 \text{ soln. } x=0 \text{ if } y\bar{y}+z\bar{z}=0 \\ q_0+1 \text{ solns if not} \end{cases}$$

$q_0 = q^{1/2}$

$\mathbb{F}_q^{\times} \xrightarrow{N} \mathbb{F}_{q^{1/2}}^{\times}$

$x \longmapsto x\bar{x}$

$$y\bar{y}+z\bar{z} = 0 \longrightarrow \begin{cases} y = 0 = z \\ \text{or} \\ z \neq 0 \text{ , } q_0+1 \text{ solns in } y. \\ (q-1 \text{ poss.}) \end{cases}$$

so $1 + (q_0^2-1)(q_0+1)$ solns

So solns in $\mathbb{F}_q^3$ is $\underbrace{1 + (q_0^2-1)(q_0+1) + (q_0+1)(q_0^4-1-(q_0^2-1)(q_0+1))}_{\text{this}}$

so $N = (\text{this}) - 1 \Big/ (q^2-1) = (q_0+1)(1+q_0^2+1-q_0+1) = (q_0+1)(q_0^2-q_0+1)$

group acts

$g=0$, $q+1$ pts, $\mathbb{P}_1$, PGL_2 (type A_1)

$g=\frac{1}{2}(q-q^{1/2})$, $q^{3/2}+1$, Fermat-type curve, PU_3 (type A_2^2) ($^2A_2$

all odd
q^2+1 Sz $^2B_2$

q^3+1 Rec $^2G_2$

When is the Weil bound attained?

q square.

Then $N=q+1+2gq^{1/2} \Rightarrow g=?$

$g=\frac{1}{2}(q-q^{1/2})$ is a possibility, and is the maximum

For $0 \le g \le \frac{1}{2}(q-q^{1/2})$?

Examples: 1) $q=4$, so $q^{1/2}=2$

The Fermat curve is $x^3+y^3+z^3=0$, so $g=1$, has 9 points

2) $q=9$, so $q^{1/2}=3$, get $x^4+y^4+z^4=0$, $g=3$.

Have curves for $g=1$, $q=9$.

For $g=2$, no such curve!

Would give $N=1+9+4\cdot3=22$;

but $g=2$ is 2-sheeted cov. of $\mathbb{P}_1$, and $\mathbb{P}_1$ has
$q=9 \to 10$ points, so $N \le 20$.

(In fact, correct bd is 20).

---

3) $q=16$, $q^{1/2}=4$ $\quad x^5+y^5+z^5=0$.

Weil bound is $1+16+2g\cdot 4 = 17+8g$

$g=1 \longrightarrow 25$ OK
$g=2 \longrightarrow 33$ OK
$\Big\}$ see table

$g=3 \longrightarrow 41$ not the bound (bound is 38).

$g=4,5$?

$g=6 \to$ yes, and the last one.

Suppose X has Weil upper bound $= N(X)$ (or Weil lower bound).

And suppose $\begin{array}{c} X \\ \Big\downarrow \text{non-const. morphism.} \\ X' \end{array}$

Then same holds for X'.

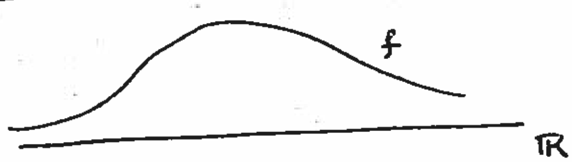
Trick of Jac's. In X, every eigenvalue is $-q^{1/2}$ or $q^{1/2}$

and $J(X') \longrightarrow J(X)$ so eigenvalues on $J(X')$ must be a subset of those on $J(X)$,

but these are all ...

Explicit Formulae

Number Fields



and take $\sum f(\log p)$

And we want a fla : $* + \sum f(\log p) = -\sum_{\substack{\tau \text{ zero} \\ \text{of zeta}}} \Phi(\tau) + \Phi(0) + \Phi(1)$

Φ = Fourier / Mellin transform of f

Stark: $*$ includes $\log d$, and choose f, Φ well

Get inequality for d $\longrightarrow$ Stark, Odlyzko, Poitou

---

Notations

X, g, q, π_α eigenvalues of Frob arranged as $\pi_1, \ldots, \pi_g, \bar{\pi}$

$$\pi_\alpha = q^{1/2} e^{i\varphi_\alpha} \quad , \quad 0 \le \varphi_\alpha \le \pi$$

$$N_n = \# X(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{\alpha=1}^{g} (\pi_\alpha^n + \bar{\pi}_\alpha^n)$$

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

$Z(T)$ = zeta-fct of X

$= \exp\{\sum^\infty N_n T^n / n\} = \frac{P(T)}{(1-T)(1-qT)}$ where $P(T) = \prod^{g} (1 - \pi$

$$a_1 = N_1 = N$$

Also if a_d = number of "pts of degree d" of the scheme X.

pt of degree d = orbit of Frob of order d in $X(\overline{\mathbb{F}_q})$.

Have $N_n = \sum_{d|n} d a_d$ (clear!)

And $Z(T) = \prod_{\substack{p \in X \\ \text{closed pt}}} \frac{1}{1 - T^{\deg p}}$

$$= \prod_{d \geq 1} \frac{1}{(1-T^d)^{a_d}}$$

Let $f(\theta)$ be a trigonometric polynomial of the form

$$f(\theta) = 1 + 2 \sum_{n \geq 1} c_n \cos n\theta \qquad \text{(finite sum)}.$$

$$= \sum_{n \in \mathbb{Z}} c_n e^{in\theta} \qquad (c_0 = 1,\ c_{-n} = c_n).$$

To f I attach polynomials in t:

$$\psi_d(t) = \sum_{\substack{n \geq 1 \\ d|n}} c_n t^n$$

"Explicit formula"

$$\boxed{\sum_{\alpha=1}^{g} f(\varphi_\alpha) + \sum_{d\geq 1} d a_d \Psi_d(q^{-1/2}) = g + \Psi(q^{-1/2}) + \Psi(q^{1/2})}$$

$$\sum_{\alpha=1}^{g} f(\varphi_\alpha) = g + 2\sum_{n,\alpha} c_n \cos n\varphi_\alpha$$

$$= g + 2\sum_{n} c_n \sum_{\alpha} \cos n\varphi_\alpha$$

$N_n = q^n + 1 - q^{n/2}\sum 2c$

so $\sum 2\cos n\varphi_\alpha = \frac{q^n+1}{q}$

$$= \underbrace{g}_{\checkmark} + \sum_{n\geq 1} c_n(q^{n/2} + q^{-n/2} - q^{-n/2}N_n).$$

$$\Psi(q^{1/2}) \quad \Psi(q^{-1/2})$$

Need only show that

$$\sum d a_d \Psi_d(q^{-1/2}) \stackrel{?}{=} \sum c_n q^{-n/2} N_n$$

$$\stackrel{?}{=} \sum c_n q^{-n/2} \sum_{d|n} d a_d$$

$$\sum d a_d \sum_{d|n} c_n q^{-n/2}$$

so OK.

Examples:

i) $f=1$: $c_n = 0 \quad n \geq 1$, $\psi_d = 0$

Get $g = g$.

ii) $f = 1 + \cos\theta$ $\quad c_1 = \frac{1}{2}$, $c_n = 0 \quad n \geq 2$.

$$\psi_1 = \psi = \tfrac{1}{2} t$$

$$\psi_n = 0 \qquad n \geq 2$$

Then:

$$g + \sum_\alpha \cos\varphi_\alpha + N \tfrac{1}{2} q^{-1/2} = g + \tfrac{1}{2} q^{-1/2} + \tfrac{1}{2} q^{1/2}$$

$\times 2q^{1/2}$:

$$q^{1/2} \sum_\alpha 2\cos\varphi_\alpha + N = 1 + q$$

so $$\boxed{N = q + 1 - q^{1/2} \sum_\alpha 2\cos\varphi_\alpha}$$ is Weil's formula.

Assumptions: (1) $f(\theta) \geq 0$ for all θ

(2) $c_n \geq 0$ for all n

Abbreviate: "f is doubly positive", $f \gg 0$.

Examples: $f = 1$, $f = 1 + \cos\theta$

Now if $f \gg 0$,

$$\underbrace{\sum f(\varphi_a)}_{\geq 0} + \sum_{d \geq 1} \underbrace{d a_d}_{\geq 0} \underbrace{\Psi_d(\ )}_{\geq 0}$$

So in that case one gets

$$\sum_{d \geq 1} d a_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{-1/2}) + \Psi(q^{1/2})$$

Taking only $d=1$ $(a_1 = N)$, get $N \Psi_1(q^{-1/2}) \leq g + \Psi_1(q^{-1/2}) + \Psi_1(q^{1/2})$

so $\boxed{N - 1 \leq \dfrac{g + \Psi(q^{1/2})}{\Psi(q^{-1/2})}}$

Now: we want to choose f so that this is optimal.

Also get $\boxed{g \geq (N-1)\Psi_1(q^{-1/2}) - \Psi(q^{1/2})}$

One can then do:

① determine (for a given N, q), the "best" bound on g.
Solved by Oesterlé (at least for $q \geq 3$)

(2) Assymptotic results as $g \to \infty$, q fixed.

(3) Nice special cases (Suzuki & Ree curves)

(4) Numerical bounds, say, for $g = 2$.

For $N = q+1$, $N = q^{3/2}+1$ we know

$N = q+1$ $\qquad g = 0$

$N = q^{3/2}+1$ $\qquad g = \frac{1}{2}(q - q^{1/2})$ $\quad q$ a square

---

For $N = q^2+1$

Choose $f = 1 + \sqrt{2}\cos\theta + \frac{1}{2}\cos 2\theta$

$= \frac{1}{2}(1+\sqrt{2}\cos\theta)^2$ $\qquad$ Then $f >> 0$.

Then $\begin{cases} \psi(t) = \frac{1}{2}(\sqrt{2}t + \frac{1}{2}t^2) \\ \psi_2(t) = \frac{1}{4}t^2 \end{cases}$ $\qquad N-1 = q^2$

Find $g \geq \left[q^2\left(\sqrt{2}q^{-1/2} + \frac{1}{2}q^{-1}\right) - \left(\sqrt{2}q^{1/2} + \frac{1}{2}q\right)\right]\frac{1}{2}$

so $\boxed{g \geq \frac{\sqrt{2}}{2}(q^{3/2} - q^{1/2})}$

Is there such a curve?

$$g \overset{?}{=} \frac{\sqrt{2}}{2}\left(q^{3/2} - q^{1/2}\right) = \left(\frac{2q}{2}\right)^{1/2}(q-1) \Rightarrow q = 2^{2f+1}$$

$\Rightarrow$ 2q = square

$\leftrightarrow$ Suzuki groups ?

<u>Deligne - Lusztig varieties</u> connected to semi-simple groups over $\mathbb{F}_q$ and their <u>twisted</u> forms.

$Sz \longleftrightarrow$ " $^2B_2$ " - groups

Take, say, SL_n and Frobenius $x \longmapsto x^{(q)}$

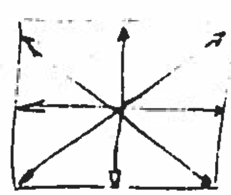
fixed pts give $SL_n(\mathbb{F}_q)$

Now use $x \longmapsto \sigma(x^{(q)})$ $\quad$ σ some outer autom. of the group.

If σ is $u \longmapsto {}^t u^{-1}$, get a different group.

char = 2, B_2 has such a "out" autom. (not algebraic)

Root system is



(See Tits in Sem. Bourbaki)

Suzuki gps are gps acting on q^2+1 elements, $q = 2^{2f+1}$
Simple if $f \geq 1$. Called [redacted] $Sz(q)$.

$Sz(2) = C_4 \cdot C_5$

$Sz(3)$ is simple.

Deligne & Lusztig

Affine curve with no rat'l pt w/ action of $Sz(q)$.

Pts at ∞ are q^2+1 and give the original representation of $Sz(q)$

Lusztig in Inventiones: genus as given, etc.

Next case: q^3+1

$f = \cos^2\varphi \left(1 + \frac{2}{\sqrt{3}} \cos\varphi\right)^2 \qquad g \geq \frac{\sqrt{3}}{2}\left(q^{5/2} - q^{1/2}\right) + \frac{1}{2}\left(q^2 - q\right)$

g integer, = that $\Rightarrow q = 3^{2f+1}$

Have Ree groups.

<u>We had</u>:

10/3 X curve $/\mathbb{F}_q$, $\pi_\alpha = q^{1/2} e^{i\varphi_\alpha}$

genus g

$f(\theta) = 1 + \sum_{n \geq 1} 2 c_n \cos n\theta$ (finite sum)

$\Psi_d(t) = \sum_{\substack{n \geq 1 \\ n \equiv 0 \,(\mathrm{mod}\, d)}} c_n t^n$, $\Psi = \Psi_1$

Then
$$\sum_{\alpha=1}^{g} f(\varphi_\alpha) + \sum_{d \geq 1} d a_d \Psi_d(q^{-1/2}) = g + \Psi(q^{-1/2}) + \Psi(q^{1/2})$$

$a_d = \#$ closed pts. of degree d

$N_n = \sum_{d \mid n} d a_d$ $\qquad N_1 = N = a_1$

If $f >> 0$ (i.e., $f(\theta) \geq 0$ for all θ and $c_n \geq 0$ for all n):

then
$$\boxed{\sum d a_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{-1/2}) + \Psi(q^{1/2})}$$

$$\Rightarrow \boxed{(N-1)\,\Psi(q^{-1/2}) \leq g + \Psi(q^{1/2})}$$

(Today: let $g \longrightarrow \infty$)

<u>Remark</u>: We proved these inequalities for X projective nonsingular.
For X <u>singular</u>, the bound as stated doesn't work.

x — pt of deg 2

collapse:

line becomes rat'l

So should replace g by sth which "sees" the topology.

X (singular) projective, abs. irred., let $B = 1^{st}$ Betti number (for ℓ-adic cohomology, for instance).

Thm: $(N-1)\psi(q^{-1/2}) \leq B/2 + \psi(q^{1/2})$

Define the "arithmetic genus" $p_a(X) = \dim H^1(X, \mathcal{O}_X)$

Known: $B/2 \leq p_a(X)$.

So we get $(N-1)\psi(q^{-1/2}) \leq p_a(X) + \psi(q^{1/2})$.

Eg: $X \subset \mathbb{P}^2$ plane curve, abs. irred, of degree n.

Then $p_a(X) = \frac{1}{2}(n-1)(n-2)$

Pf (originally was given in terms of $N_n = \ldots$)

Claim: $N_n = 1 + q^n - \sum_{i=1}^{B} \alpha_i^n \qquad |\alpha_i| = 1$ or $q^{1/2}$

k.-Deligne: (Still the Lefschetz formula, except for the wrong size of eigenvalues)

Or: from Weil. $\boxed{A}$

Take $N_n - 1 = q^n - \sum_{i=1}^{B} \alpha_i^n \geq N - 1$

$$\sum_n c_n q^{-n/2}(N_n - 1) = \sum_n c_n q^{n/2} - \sum_{i,n} c_n q^{-n/2}\alpha_i^n$$

So $$(N-1)\Psi(q^{-1/2}) \leq \Psi(q^{1/2}) - \sum_{i,n} c_n q^{-n/2}\alpha_i^n$$

$\therefore$ To be proved : $$-\sum c_n q^{-n/2}\alpha_i^n \leq \frac{B}{2}.$$

or $$\mathrm{Re}\left(-\sum c_n q^{-n/2}\alpha_i^n\right) \leq \frac{B}{2}$$ Since the LHS is real anyway

Consider $\frac{1}{2} + \Psi(t) = F(t)$ polynomial in t

If $t = e^{i\varphi}$, $\mathrm{Re}(F(e^{i\varphi})) = \mathrm{Re}\left(\frac{1}{2} + \sum c_n e^{in\varphi}\right) = \frac{1}{2} f(\varphi) \geq 0.$

So : $\mathrm{Re}(F(t)) \geq 0$ for all t with $|t| = 1$

$\Downarrow$ cx analysis

$\mathrm{Re}(F(t)) \geq 0$ for all t with $|t| \leq 1$.

(apply max. princip to $\exp(-F(t))$. Get $|\exp(-F(t))| \leq 1$ for $|t| = 1$, hence for $|t| \leq 1$.)

Now

$$\mathrm{Re}\left(-\sum c_n q^{-n/2}\alpha_i^n\right) = \sum_i \mathrm{Re}\left(\frac{1}{2} - F(q^{-1/2}\alpha_i)\right)$$ and $|q^{-1/2}\alpha_i| \leq 1$

$$\leq \sum_{i=1}^{B} \mathrm{Re}\left(\frac{1}{2}\right) = \frac{B}{2}$$ so QED. $\boxtimes$

One can do similar things for higher-dim'l varieties, in <u>odd</u> dimension.

<u>Example</u>: X proj non-sing variety, dim 3, abs. irred.
Assume: $B_1 = 0$, $B_2 = 1$, B_3 "large"
(E.g., any <u>complete intersection</u>)

[If X has N points, one can prove

$$\frac{B_3}{2} \geq N\Psi(q^{-3/2}) - \left(\Psi(q^{-3/2}) + \Psi(q^{-1/2}) + \Psi(q^{1/2}) + \Psi(q^{3/2})\right)$$

(Exercise) (use Deligne – for large N this gives better bounds)

<u>Now</u>: q fixed, $g \to \infty$
we have:

Let $k \geq 1$ be a fixed integer.

Let X^λ be curves of genus $g_\lambda \to \infty$.

$a_d(X^\lambda) =: a_d^\lambda$

<u>Theorem</u>: $$\limsup_{g_\lambda \to \infty} \frac{1}{g_\lambda} \sum_{d=1}^{k} \frac{d\, a_d^\lambda}{q^{d/2} - 1} \leq 1.$$

<u>Corollary</u>: For $k=1$, $a_1^\lambda = N^\lambda = \# X^\lambda(\mathbb{F}_q)$, and we have

$$\limsup_{g_\lambda \to \infty} \frac{N^\lambda}{g_\lambda} \leq q^{1/2} - 1.$$

(Thm of Drinfeld–Vlad.t)

Weil gives $N^\lambda \le 1 + q + 2g^\lambda q^{1/2}$

so $\frac{N^\lambda}{g^\lambda} \le 2q^{1/2} + o(1)$

If $q = 2$, Weil $2q^{1/2} = 2.828$, $[2q^{1/2}] = 2$, But $q^{1/2} - 1 = 0.414$.

Proof of Thm:

We have $\sum_{d=1}^{k} d a_d^\lambda \psi_d(q^{-1/2}) \le g^\lambda + \Upsilon(q^{1/2}) + \Psi(q^{-1/2})$

$\frac{1}{g^\lambda} \sum_{d=1}^{k} d a_d^\lambda \psi_d(q^{-1/2}) \le 1 + \frac{1}{g^\lambda}(\qquad)$

$g_\lambda \to \infty$: $\left[\limsup \frac{1}{g^\lambda} \sum_{d=1}^{k} d a_d^\lambda \psi_d(q^{-1/2}) \le 1. \right]$

true for every ψ_d coming from an $f >> 0$.

Lemma: ① If $f >> 0$, $f = 1 + \sum 2c_n \cos n\theta$, then $c_n \le 1$.

② For any P, any $\varepsilon > 0$, $\exists f$ s.t. $c_n \ge 1 - \varepsilon$ for all $n = 1, \ldots, P$.

(So can get f like $1 + 2\cos\theta + 2\cos 2\theta + \cdots = $ "$\sum_{n\in\mathbb{Z}} e^{in\theta}$" $=$ Dirac measure at 0 on the circle

If $c_n = 1$ for all n, then OK, because $\Psi(t) = t + t^2 + \cdots$

$\Psi_d(t) = t^d + t^{2d} + \cdots = \frac{t^d}{1-t^d} = \frac{1}{t^{-d}-1}$

and $\Psi(q^{-1/2}) = \frac{1}{\quad}$ which ...

Then we need only do a convergence argument using the lemma. $\boxed{/\!/}$

Pf of Lemma :

① $$\begin{cases} c_n = \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\cos n\theta \, d\theta \\ \text{and} \\ 1 = \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\, d\theta \end{cases}$$

and since $|\cos n\theta| \le 1$ we get

$$c_n = \left| \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\cos n\theta \, d\theta \right| \le \frac{1}{2\pi}\int_0^{2\pi} f(\theta)\,|\cos n\theta|\, d\theta \le 1 .$$

② Given P, ε

P integer ≥ 1, let $t = e^{i\theta}$

Write $$f_P = \frac{1}{2P+1}\left(t^{-P} + t^{-P+1} + \dots + 1 + \dots + t^{P}\right)^2$$

$$f_P(\theta) = \frac{1}{2P+1}\left(1 + 2\cos\theta + \dots + 2\cos P\theta\right)^2 .$$

$$f_P = \frac{1}{2P+1}\left(t^{-2P} + 2t^{-2P+1} + \dots + (2P+1)\cdot 1 + 2Pt + \dots + t^{2P}\right)$$

So $$c_n(f_P) = \frac{2P-n+1}{2P+1}$$

for fixed n, $P \to \infty$, $c_n \to 1$ $\boxed{/\!/}$

Ihara's tower theorem

X as usual $/\mathbb{F}_q$, g

S = finite non-empty set of closed points of X

Assumption: There exists a sequence $X^\lambda \to X$ of unramified finite coverings of X in which every element of S splits completely and $\deg(X^\lambda \to X) \to \infty$.

Then:
$$\boxed{\sum_{P \in S} \frac{\deg P}{q^{\deg(P)/2} - 1} \leq g - 1}.$$

Special case: If all points in S are rat'l ($\deg = 1$) we get

$$|S| \leq (g-1)(q^{1/2} - 1)$$

If $X = \mathbb{P}_1$, $S = \emptyset$, $X^\lambda = X/\mathbb{F}_{q^\lambda}$ constant field extn.

then $\Sigma = 0 \leq 0 - 1$ is false.

So $S \neq \emptyset$ is necessary.

Proof: 1^{st} case: the field of constants of the X^λ is just $\mathbb{F}_q$.

If $n^\lambda = [X^\lambda : X]$ = degree of covering, then $g^\lambda - 1 = n^\lambda (g-1)$
(Cover is unramified!)

$a_1^\lambda \geq n^\lambda a_1(S)$ $\qquad$ $a_1(S) = \#$ of $P \in S$ of degree 1

So get $\limsup_{n^\lambda \to \infty} \frac{1}{1+n^\lambda(g-1)} \sum \frac{d\, n^\lambda a_d(S)}{q^{d/2}-1} \leq 1$

$n^\lambda \to \infty$

Now $\frac{n^\lambda}{1+n^\lambda(g-1)} \longrightarrow \frac{1}{g-1}$,

so $\limsup_{n_\lambda \to \infty} \underbrace{\frac{1}{g-1} \sum \frac{d\, a_d(S)}{q^{d/2}-1}}_{\text{constant!}} \leq 1$

So we get the inequality we want. $\boxed{/\!/}$

2^{nd} case: general case.

Note: degree of a const. field extn. has a bound:

Indeed, if $P \in S$ has degree d, the degree of the constant field extn divides d.

Now (take a subsequence) we can assume that the constant field extn is $\mathbb{F}_{q^d}$ (for some d) for all λ.

Then

$$\left.\begin{array}{c} X^\lambda \\ \downarrow \\ X/_{\mathbb{F}_{q^d}} \end{array}\right\} \text{; apply case 1 to the top layer}$$

$$\begin{array}{c} \downarrow \\ X/_{\mathbb{F}_q} \end{array}$$

Every $P \in S$ gives $\underline{d}$ points in $X/_{\mathbb{F}_{q^d}}$ of degree $\deg(P)/d$,

and the new "q" is q^d.

Get $\quad d \sum_{P \in S} \frac{\deg(P)/d}{(q^d)^{\frac{\deg(P)}{2d}} - 1} \leq g - 1$ which is the 1fla we want. ▨

Ihara, Journ. Math Soc. Japan ?

Let $A(q) =: \limsup_{g \to \infty} \frac{N_q(g)}{g}$

Drinfeld-Vladut Thm $\Longrightarrow \boxed{A(q) \leq q^{1/2} - 1}$

Theorem (Ihara, Zink)

If q is a square, then $A(q) \geq q^{1/2} - 1$.

Corollary: If q is a square, $A(q) = q^{1/2} - 1$.

$A(q)$ is not known for other q.

Known: $A(q) > 0$; $A(q) > c \log q$ (some $c > 0$) [Use Golod-Shafarevich!] → next time

For $q=2$:

$$\begin{cases} A(2) \leq 0.414\ldots & (= \sqrt{2} - 1) \quad \text{(D-V)} \\ A(2) \geq 0.205. & (= \frac{8}{39}) \end{cases}$$

Proof when $q = p^2$: Use modular curves $X_0(N)$, etc.

(For $q = p^{2e}$, $e \geq 2$, use Shimura curves)

$\Gamma_0(N)$, $X_0(N)$ mod. curve

Let $X = X_0(\ell)$, genus $g = \frac{\ell+1}{12}$.

Supersingular points are rat'l $/\mathbb{F}_{p^2}$, and their number N^{ss} is given by

$$\boxed{N^{ss} = \frac{p-1}{12}(\ell+1)}$$

$$\begin{array}{c} X_0(\ell) \\ \big\downarrow \\ \mathbb{P}^1 \end{array} \quad \text{(param. by } j\text{)}$$

ss. j's

so $$\frac{N}{g} \geq \frac{N^{ss}}{g} = p-1 = q^{1/2}-1$$

Now take $\ell \to \infty$, and the bound is obtained. $\blacksquare$

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

Have seen: 1) $A(q) \leq q^{1/2} - 1$ (Drinfeld - Vladut)

Now 2) If q is a square, $A(q) = q^{1/2} - 1$.

For $q = p^2$, modular curves $\longrightarrow$ enough s.s. points.

$\{1\} \subset G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$, ℓ prime, $\ell \geq 3$
subgp

Then the modular curve w.r.t. G, affine, but add pts at ∞. Corresp to moduli problem:

E ell. curve + "G-structure on its ℓ-div. pts"

G-structure: a family of $E_\ell \xrightarrow[\varphi]{\sim} \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$

s.t. 1) $\varphi, \varphi' \in$ family $\Rightarrow$ $\varphi' = s\varphi$ for some $s \in G$

2) $\varphi' \in$ family, $s \in G$ $\Rightarrow$ $s\varphi' \in$ family.

X_G is the moduli space (completed).

Can view in terms of X_ℓ = mod. curve of level ℓ (corresp to $G = \{\pm 1\}$)

X_ℓ
|

$$GL_2/\{\pm 1\} \xrightarrow{\det} \mathbb{F}_\ell^\times$$

gives an extension

$$\begin{tikzcd}[column sep=small]
X_\ell \arrow[d, dash] \arrow[dr, phantom, "\text{abs. irred. here}"] & \\
\mathbb{Q} \arrow[r, dash, dashed] & \mathbb{Q}(\zeta_\ell)
\end{tikzcd}$$

then: $X_G = X_\ell/G$

If $G \twoheadrightarrow \mathbb{F}_\ell^\times$, then X_G is defined over $\mathbb{Q}$.

Assume $G \supset \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{F}_\ell^\times$

so $\det G = \begin{cases} \mathbb{F}_\ell^\times \\ \text{or} \\ (\mathbb{F}_\ell^\times)^2 \end{cases}$

So ground field is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{\pm \ell})$, $\pm \ell \equiv 1 \ (4)$

Can do this over any k, char $k \neq \ell$ (for char $= \ell$, Katz + Mazur).

In char p, $p \neq \ell$, X_G is defined over either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

<u>Theorem</u>: Every s.s. point $((E, \varphi), E$ s.s.$)$ is rational over $\mathbb{F}_{p^2}$ (on X_G).

Pf: E ss. can be written on $\mathbb{F}_{p^2}$, its Frob. being $-p$. So $-p \in G$ by our assumption, and Frob. stabilises (E, φ)! ☒

a) $\Gamma_0(\ell)$-curve: $G = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ gives our result above.

b) interesting case: $G = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{F}_\ell^\times \right\}$ $\quad X_G = X(\ell)$

$$\begin{cases} \text{genus of } X(\ell): & 2g - 2 = \frac{1}{12}(\ell^2 - 1)(\ell - 6) \\ \#\text{ s.s. points}: /\mathbb{F}_{p^2} & N^{ss} = \text{[redacted]} \ \dfrac{(p-1)(g-1)}{1 - \frac{6}{\ell}}. \end{cases}$$

For low values:

$\ell = 7$ Klein curve $\quad PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on $X(\ell)$

$|PSL_2(\mathbb{Z}/7\mathbb{Z})| = 168$

$g = 3$, $N^{ss} = 14(p-1)$

($PGL_2(\ )$ acts on curve over $\mathbb{Q}$, PSL_2 on curve over $\mathbb{Q}(\sqrt{-7})$)

Example: $\begin{cases} p = 2, \text{ so } N^{ss} = 14 & (\text{over } \mathbb{F}_4) \\ p = 3, \quad N^{ss} = 28 & /\mathbb{F}_9 \\ p = 5 \quad N^{ss} = 56 & /\mathbb{F}_{25} \end{cases}$

Weil bound is $1 + p^2 + 6p$ = resp, 17, 28, 56

$(2g\sqrt{p^2} = 6p.)$

$\Rightarrow$ for $p = 3, 5$, no rat'l cusps, etc.

Can prove: best for $p = 2$ also.

$\therefore$ Klein curve gives us the best for $q = 4, 9, 25$ (also 8, but need: cusps are rational,

---

alternate approach

$\mathrm{Jac}(X(7)) = E \times E \times E$ $\qquad$ E has CM by $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$,
unique such def $/\mathbb{Q}$,
good red. outside 7,
grossencharacter

for p inert: $\left(\frac{p}{7}\right) = -1 \Longrightarrow$ eigenv. of $F_r / \mathbb{F}_p$ on E is $\pm\sqrt{-p}$
$\Longrightarrow / \mathbb{F}_{p^2}$ it is $-p$ (twice).

So on $\mathrm{Jac}(X(7))$, get $-p$ (six times), so get the Weil bound for p inert.

$\ell = 11$, $g = 26$, $N^{ss} = 55(p-1)$

$p = 2$: $/\mathbb{F}_4$, $N^{ss} = 55$ which is best possible (exp. fla.)

$p = 3$: $/\mathbb{F}_9$, $N^{ss} = 110$ (?) (exp. fla gives ≤ 111).
$= \# X(11)(\mathbb{F}_9)$

Use $Jac(X(11))$ is isogenous to the product of 11 times E_1, 10 times E_2, 5 times E_3, E_i ell curves

E_1 ell. curve cond 11		Ant. $\boxed{IV}$ $\overline{11}$
E_2 " " cond 11^2	, no CM	121_F
E_3 " " cond 11^2	, CM	121_D

Studied by Ligozat (Mod. Fcts V or VI)

So can check that the $N^{ss} = N$ (Ant. IV gives eigenvalues of Frob. on these curves).

Theorem (Golod-Šafarevič)

Thm on Artin local rings:

- R ring, I two-sided ideal, $R/I = k$ comm. field.
- Every $r \in R$, $r \notin I$ is invertible (i.e., R is local w/ max'l ideal I).
- R is "Artin" $\iff \begin{cases} I^n = 0 \text{ for large } n \\ \text{and} \\ I^m/I^{m+1} \text{ is a finite dim'l } k\text{-vector space} \\ \quad (\text{for } m = 0, 1, \dots) \end{cases}$

(Example: G finite ℓ-group, $R = \mathbb{F}_\ell[G]$, $I = \Delta(G)$, $k = \mathbb{F}_\ell$.)

Take M = f.g. R-module (left).

Then M/IM is a k-vector space of finite dim.

(If $x_1, -, x_d \in M$ give a basis for $M/_{IM}$, NAK => they generate M

$M \qquad\qquad d = d_0(M)$

Choose $x_1, -, x_d \in M$ generating M. This gives

$$0 \longrightarrow M_1 \longrightarrow R^d \longrightarrow M \longrightarrow 0$$

M_1 = kernel = module of relations between the x_i

$M_1 \subset IR^d$

Up to isom., M_1 depends only on M. Define

$d_1(M) := d_0(M_1)$ = "nber of relations between x_i"

Also: exact seq. gives: $\otimes k$

$$0 = \mathrm{Tor}_1(R^d, k) \longrightarrow \mathrm{Tor}_1(M,k) \longrightarrow M_1/_{IM_1} \longrightarrow R_d/_{IR_d} \xrightarrow[\cong]{} M/_{IM} \longrightarrow 0$$

So find $\mathrm{Tor}_1(M,k) \cong M_1/_{IM_1}$,

so $d_1(M) = \dim_k \mathrm{Tor}_1(M,k)$

$d_i(M) = d_0(M_i) \qquad M_i = i^{\text{th}}$ term of a minimal resolution of M

$= \dim_k \mathrm{Tor}_i(M,k)$.

Take $M = k$: $d_0(k) = 1$

$$0 \to I \to R \to k \to 0$$

So $M_1 = I$; $d_1(k) = \dim_k (I/I^2) = d$

$d_2(k) = r$ by defn.

<u>Theorem</u> (Golod-Šafarevič, refined by Vinberg and Gaschütz)

Assume $d \geq 1$, i.e., that $I \neq 0$, i.e., that R is not a field. Then

$$r > \frac{d^2}{4}.$$

[One has examples of $r \sim \frac{d^2}{3}$ or $\frac{3d^2}{8}$; $\frac{d^2}{2}$ is easy ; Best is unknown

[<u>Example</u>: if $R = \mathbb{Z}/\ell^2\mathbb{Z}$, $k = \mathbb{Z}/\ell\mathbb{Z}$, get $M_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, so all $d_i = 1$

<u>Pf</u>: Have $0 \to J \to R^d \to I \to 0$

$$R^r \to J \to 0$$

So get $R^r \xrightarrow{\varepsilon} R^d \to I \to 0$ $\qquad \varepsilon(R^r) \subset IR^d$

Tensor w/ R/I^nR : $\qquad$ since $R^d/IR^d \xrightarrow{\sim} I/I^2$

$$\begin{tikzcd}
R^r/I^nR^r \arrow[r] \arrow[dr] & R^d/I^nR^d \arrow[r] & I/I^{n+1} \arrow[r] & 0 \\
& R^r/I^{n-1}R^r \arrow[u] & &
\end{tikzcd}$$

$\therefore \varepsilon(I^{n-1}R^r) \subset I^nR^d$

So $\dfrac{R^r}{I^{n-1}R^r} \longrightarrow \dfrac{R^d}{I^n R^d} \longrightarrow \dfrac{I}{I^{n+1}} \longrightarrow 0$ $\quad (n \geq 1)$

define $a(n) = \ell\left(R/I^n R \right) = \sum_{i=0}^{n-1} \dim_k \left(I^i / I^{i+1} \right)$

$a(0) = 0$

$a(1) = 1$

$a(2) = 1 + d$ $\qquad R/I^2 : \; R/I, \; I^2/I$ (1, d)

$\vdots$

$a(n)$ ultimately constant.

Now exact seq. above gives:

$$d\,a(n) \leq r\,a(n-1) + \underbrace{a(n+1) - 1}_{\ell(I/I^{n+1})} \qquad n \geq 1$$

Claim: this implies $r > \frac{d^2}{4}$.

For this introduce $\sum_{n=0}^{\infty} a(n) t^n = t + (1+d)t^2 + \dots = t f(t)$

so $f(t) = \sum_{n=0}^{\infty} a(n+1) t^n$

multiply ineq by t^n and add:

$$\sum_{n\geq 1} d a(n) t^n \prec r \sum_{n\geq 1} a(n-1) t^n + \sum_{n\geq 1} a(n+1) t^n - \sum_{n\geq 1} t^n$$

$$d f(t) t \prec r t^2 f(t) + f(t) - 1 - \sum_{n\geq 1} t^n$$

so $$d f(t) t \prec r t^2 f(t) + f(t) - \frac{1}{1-t}$$

so $$f(t)(rt^2 - dt + 1) \succ \frac{1}{1-t}$$

Assume $r \leq \frac{d^2}{4}$; then $rt^2 - dt + 1 = (1-\lambda t)(1-\mu t)$ $\lambda\mu$ are ≥ 0

Now, $\frac{1}{1-\lambda t}$ has pos. coeffs.

λ & μ can't both be zero, since $d \neq 0$.

Multiply!

$$f(t) \succ \frac{1}{(1-t)(1-\lambda t)(1-\mu t)}$$

and either λ or μ is ≥ 1 : $\lambda + \mu = d \geq 1$, $\lambda\mu = r$

But the coeffs of $f(t)$ are bounded, since the $a(n)$ are.

So it's enough to show the coeffs of RHS are not bdded.

RHS $\succ \frac{1}{(1-t)^2}$ coeffs not bdded. ☒

G finite ℓ-group, $R = \mathbb{F}_\ell[G]$, $I = \Delta(G)$

Why is I = radical of G?

Up to isom., an ℓ-group has only one irred. repres. in dim ℓ, namely the trivial repres. (any non-triv. repres. has a fixed vector) then radical = $\bigcap \ker(\text{repres}) = I$.

$d = \dim \operatorname{Tor}_1^R(k, k) = \dim H_1(G, \mathbb{Z}/\ell\mathbb{Z})$

$r = \dim \operatorname{Tor}_2^R(k, k) = \dim H_2(G, \mathbb{Z}/\ell\mathbb{Z})$

dual of $H_i = H^i$

so $\begin{cases} d = \dim H^1(G, \mathbb{Z}/\ell\mathbb{Z}) \\ r = \dim H^2(G, \mathbb{Z}/\ell\mathbb{Z}) \end{cases}$

And: d = min. no. of generators of G
assume $x_1, \ldots, x_d \in G$ generate G;
then r = min. nber of rels between x's which define G as an ℓ-group. (or pro-ℓ-group)

Theorem (Golod-Šaf.) If G is a finite non-triv. ℓ-group then d and r as above satisfy $r > d^2/4$.

$d = 1$, $r > \frac{1}{4}$ i.e., $r \geq 1$; x gen, $x^\ell = 1$ cyclic order ℓ (sharp

$d = 2$, $r > \frac{4}{4}$ i.e., $r \geq 2$; x, y gen., $yxy^{-1} = x^{1+\ell}$, $xyx^{-1} = y^{1+\ell}$
(order is ℓ^3)

Define $z = xyx^{-1}y^{-1} = y^\ell = x^{-\ell}$, so $z \in Z(G)$

$x^\ell y^{-1} = x^{\ell+\ell^2}$ so $x^{\ell^2} = 1$ so $z^\ell = 1$. So order ℓ^3.

$\parallel$

since $\ell^{\ell} \ldots]$

$d=3$, $r > \frac{9}{4}$ i.e., $r \geq 3$ (ℓ odd) : 3 gen. z, y, x

$$\begin{cases} yxy^{-1} = x^{1+\ell} \\ zyz^{-1} = y^{1+\ell} \\ xzx^{-1} = z^{1+\ell} \end{cases}$$

Mennicke → finite group. $d=3$,

$d=4$, $r > \frac{16}{4}$ i.e., $r \geq 5$ → is $d=4$, $r=5$ possible?

(think: $d=4$, $r=6$ is.)

$x_1, \ldots, x_d$ with $(x_i, x_j) = 1$, $x_i^\ell = 1$ give $\frac{d(d-1)}{2} + d$ rels.

10/17 Class Field Towers

C curve, genus g, over $\mathbb{F}_q$, p = char.

K its function field.

ℓ a prime number ($\ell = p$ is ok)

S finite non-empty set of "primes" of K i.e., of closed points of C.

Look at K_1 = max. abelian ℓ-extension of K, (whose Gal group is an ℓ ...) unramified (everywhere) in which the elements of S split completely.

$$\begin{array}{c} K_1 \\ | \\ K \end{array}$$

Cond. on S makes it finite (otherwise if $S = \emptyset$, have the const. field extn.)

If ℓ divides the $\deg(P)$ for every $P \in S$, then K_1 contains $\mathbb{F}_{q^\ell} \cdot K$. If not, it does not.

$$\begin{tikzcd} K_1 \arrow[d, dash] & & C_1 \arrow[d] \\ K \arrow[rr, phantom, "\rightsquigarrow"] & & C \end{tikzcd}$$

Define $K_2 = (K_1)_S$ with respect to S_1 = inverse image of S.

So have $K \subset K_1 \subset K_2 \subset \cdots \subset K_\infty = \bigcup_n K_n$

K_∞ = max. Galois extension of K where S splits completely, whose Galois group is pro-ℓ, and unramified.

<u>Question</u>: Is K_∞ / K finite?

Let $G_S = Gal(K_\infty / K) = \varprojlim Gal(K_n / K)$

Assume G_S is finite; it is an ℓ-group. Then we have

$d = \dim H_1(G_S, \mathbb{Z}/\ell\mathbb{Z})$ (min. nber of generators)

$r = \dim H_2(G_S, \mathbb{Z}/\ell\mathbb{Z})$ (min. nber of "relations") (as ℓ-group).

<u>Theorem</u>: Assume G_S is finite (i.e., the tower stops). Then

$$r - d \le \begin{cases} |S| - 1 & \text{if } \ell \nmid q-1 \\ |S| & \text{if } \ell \mid q-1 . \end{cases}$$

(We know: $r > \frac{d^2}{4}$ if $d \geq 1$ Golod-Šaf., which will give a contradiction for suitable S.)

Proof (Same as Iwasawa's in the field case):

First: Using class field theory to find $Gal(K_1/K)$:

C_K = idèle class group

Have

$$1 \longrightarrow E_S \longrightarrow \prod_{p \in S} K_p^* \times \prod_{v \notin S} U_v \longrightarrow C_K \longrightarrow \underset{\text{(quotient)}}{Ab_S} \longrightarrow 1$$

E_S = S-units (= unit outside S)

Then $Gal(K_1/K) = (Ab_S)_\ell$ (ℓ-part)

Next: Now: K_∞/K finite, so $(K_\infty)_1 = K_\infty$

Write s.e.q. for K_∞:

$$1 \longrightarrow E_{S_\infty} \longrightarrow \prod_{\tilde{p} \in S_\infty} K^*_{\infty,\tilde{p}} \times \prod_{\tilde{v} \notin S_\infty} U_{\tilde{v}} \longrightarrow C_{K_\infty} \longrightarrow Ab_\infty \longrightarrow$$

E_{S_∞} = S_∞-units of K_∞

$(K_\infty)_1 = K_\infty \iff (Ab_\infty)_\ell = \{1\}$

Let $G = G_S$; G acts on everything.

- Ab_∞ has trivial cohomology (order prime to ℓ, G ℓ-gr

Also · For the product

K_p^*-part : $\tilde{P} \circlearrowleft G$ permutes $\prod_{\tilde{P} \to P} K^*_{\infty, P}$ is induced (trivial coh.)

$\tilde{P} \downarrow P \in S$

U_v-part : $\tilde{v} \downarrow v$ $G_{\tilde{v}}$ -- stab $\tilde{v}$

Shapiro's lemma :

coh $= H^q(G_{\tilde{v}}, U_{\tilde{v}}) =$ trivial (because everything is unramified).

So LES of coh gives a map

$$\hat{H}^q(G, C_{K_\infty}) \xrightarrow[\cong]{\delta} \hat{H}^{q+1}(G, E_{S_\infty}) \qquad \text{for each } q \in \mathbb{Z}.$$

δ is an isom. for all q because middle term has trivial cohom.

$\boxed{\hat{H}^q \text{ is Tate cohomology}}$

Know: $\hat{H}^q(G, C_{K_\infty}) \xleftarrow[\cap\, u_{K_\infty}]{\cong} \hat{H}^{q-2}(G, \mathbb{Z})$

$u_{K_\infty} \in H^2(G, C_{K_\infty})$

Choose $q+1=0$ so $q=-1$: Get $\hat{H}^{-3}(G, \mathbb{Z}) \cong \hat{H}^0(G, E_{S_\infty}) =$

$E_S /$

Know $E_S \cong \mathbb{Z}^{|S|-1} \times \mathbb{F}_q^{\times}$.

We want a quotient of E_S/Norms which is an ℓ-group.

So

$$rk_\ell(\hat{H}^{-3}(G,\mathbb{Z})) \leq \begin{cases} |S|-1 & \text{if } \ell \nmid (q-1) \\ |S| & \text{if } \ell \mid (q-1). \end{cases}$$

<u>It remains to show</u>: $rk_\ell(\hat{H}^{-3}(G,\mathbb{Z})) = r-d$.

$$\hat{H}^{-3}(G,\mathbb{Z}) = H_2(G,\mathbb{Z})$$

[Group of coeffs A, trivial action :

$H_q(G,A) = H_q(G,\mathbb{Z}) \otimes A \oplus \mathrm{Tor}_1(H_{q-1}(G,\mathbb{Z}), A)$

$q=2$, $A = \mathbb{Z}/\ell\mathbb{Z}$:

$$H_2(G,\mathbb{Z}/\ell\mathbb{Z}) = H_2(G,\mathbb{Z}) \otimes \mathbb{Z}/\ell\mathbb{Z} \quad \oplus \quad \mathrm{Tor}_1(H_1(G,\mathbb{Z}), A)$$

$$= H_2(G,\mathbb{Z})/\ell H_2(G,\mathbb{Z}) \quad \oplus \quad \ell\text{-part of } H_1(G,\mathbb{Z})$$

So take ranks: $\quad r = rk_\ell(H_2(G,\mathbb{Z})) + d.$

Since: $H_1(G,\mathbb{Z}/\ell\mathbb{Z}) = H_1(G,\mathbb{Z})/\ell H_1(G,\mathbb{Z})$ since H_0 is free

So $\quad rk_\ell\, \hat{H}^{-3}(G,\mathbb{Z}) = r-d.$ /

Or: Look at

$$0 \to \mathbb{Z} \xrightarrow{\ell} \mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \to 0$$

$$H_2(G,\mathbb{Z}) \xrightarrow{\ell} H_2(G,\mathbb{Z}) \to H_2(G, \mathbb{Z}/\ell\mathbb{Z}) \to H_1(\ ) \xrightarrow{\ell} H_1(\ )$$

So $$0 \to H_2(G,\mathbb{Z})/\ell H_2(G,\mathbb{Z}) \to H_2(G, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{Ker}(\ell \text{ in } H_1(G,\mathbb{Z})) \to$$

So dimensions add. So QED! $\boxed{}$

<u>Theorem</u>: The $(S-\ell)$ class field tower of K is infinite if $|S| \lneq \frac{d^2}{4} - d + \begin{cases} 1 & \text{if } \ell \mid (q-1) \\ 0 & \text{if not} \end{cases}$, and $d \geq 2$.

Pf: Otherwise

$$r - d \leq \begin{cases} |S| - 1 \\ |S| \end{cases}$$

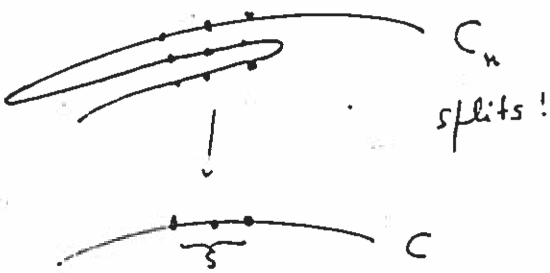
$$r > \frac{d^2}{4} \quad \text{if } d \geq 1$$

And of course $d=1$ doesn't work (get $|S| \leq \frac{1}{4}$) $\boxed{}$

Suppose that all elements in S have degree 1, i.e., S is made up of rational points, and assume that the corresp. class field tower is infinite.

Then $A(q) \geq \dfrac{|S|}{g_c - 1}$, where $A(q) = \limsup_{g \to \infty} \dfrac{N_q(g)}{g}$

g_c = genus of C.



So nber of rat'l pts of $C_n \geq [C_n : C] \cdot |S$

genus of $C_n = g_{C_n}$; $g_{C_n} - 1 = [C_n : C](g-$

Notice that $g_C \geq 2$ (For $g_C = 0$, no unr. coverings; for $g_C = 1$, covering would have $g_{C_n} = 1$ and nber pts $\to \infty$!)

So
$$\frac{N_q(g_n)}{g_n} \geq |S| \frac{[C_n : C]}{1 + [C_n : C](g_C - 1)}$$

$$\geq |S| \frac{1}{\frac{1}{[C_n : C]} + g_C - 1}$$

$n \to \infty$ so $\boxed{A(q) \geq \frac{|S|}{g_C - 1}}$.

Corollary: If (S, C) satisfy $|S| \leq \frac{d^2}{4} - d + \left\{ {}^{1}_{0} \right\}$, $d \geq 2$, then

$$A(q) \geq \frac{|S|}{g_C - 1}$$

(and in particular $A(q) > 0$).

• For every q, we want to find K, S, ℓ satisfying

$$(*) : \quad |S| \leq \frac{d^2}{4} - d + \begin{cases} 1 & \text{if } \ell | q-1 \\ 0 & \text{if not} \end{cases}, \quad d \geq 2.$$

We'll want to take $|S| = 1$, $d \geq 5$.
We'll choose $\ell = 2$ (So for q odd, enough to find $d \geq 4$).

<u>Construction</u> (char $= p \neq 2$)

Choose $\ell = 2$; K will be some quadratic extension of $K_0 = \mathbb{F}_q(T)$ corresp. to curve $/C_{-1}$ of genus 0.

Want

$$\begin{array}{ccccc} C_0 & C_1 & & & C_d \\ \backslash & | & \cdots & / & \\ & C_{-1} & & & \end{array}$$

point at ∞ should split completely.

Let $\Phi_0, \ldots, \Phi_d$ be irred. monic polyn. of even degree distinct

Then define C_i by $y_i^2 = \Phi_i(T)$.

$y_i^2 = T^{\text{even}} + \cdots \Rightarrow$ <u>∞ is split in each C_i</u>

So set $K = \mathbb{F}_q(T, \sqrt{\Phi_0 \cdots \Phi_d})$

Over K, I have d indep. quadratic extens, unramified, ∞ splits completely.

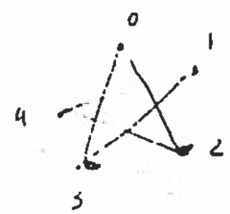
Choose $d = 5$, for instance, and the "d" in the theorem is then at least 5, so done $\boxtimes$

For char = 2, do the same with Artin-Schreier extensions

Now want: In $\mathbb{F}_q$, $A, B \subset \mathbb{F}_q$ as large as possible

s.t. every $a - b$, for $a \in A$, $b \in B$, is a non-square.

E.g. $q = 5$



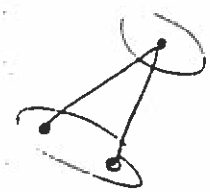
$\mathbb{F}_5$

join pts whose difference is not a square

Want: a maximal complete bipartite graph embedded in this graph

Call this a B-subgraph

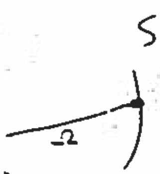
E.g.



in our case.

Graph theorem

Let R, S be two finite sets, $\Omega \subset R \times S$.



Let $m \geq 1$ be such that every $s \in S$ is Ω-related to at least m points of R.

Let a, b be integers ≥ 1 such that $b \binom{|R|}{a} \leq |S| \binom{m}{a}$. (*)

Then $\exists A \subset R$ and $B \subset S$ with $\begin{cases} |A| = a, \ |B| = b \\ A \times B \subset \Omega \end{cases}$

Let X = set of pairs (A, s) with $|A| = a$, $s \in S$ and $A \times \{s\} \subset \Omega$.

Then $|X| = ?$

Project $X \xrightarrow{\varphi} S$
$(A, s) \longmapsto s$

Let $R(s)$ be the subset of R made of the elements r s.t. $(r, s) \in \Omega$.

So $|\varphi^{-1}(s)|$ = nber subsets of $R(s)$ w/ a elements

$$= \binom{R(s)}{a} \geq \binom{m}{a} \qquad \text{since } R(s) \geq m$$

Then $|X| \geq |S| \binom{m}{a}$

Then $X \xrightarrow{\psi}$ Set of subsets of R with a elements $\longleftarrow$ has $\binom{|R|}{a}$ elements
$(A, s) \longmapsto A$

Hence some fiber of ψ has at least $|X| / \binom{|R|}{a}$ elements

But $$\frac{|X|}{\binom{|R|}{a}} \geq \frac{|S|\binom{m}{a}}{\binom{|R|}{a}} \geq b.$$

So choose A whose fiber has $\geq b$ elements, and choose B in the fiber with $|B| = b$. Done! $\boxed{/}$

10/23 Class Field Towers (cont.)

We showed: If $\begin{cases} \Omega \subset R \times S \\ \text{every } s \in S \text{ is } \Omega\text{-related to at least } m \text{ elements of } R \end{cases}$

then $\exists A \subset R$, $B \subset S$, $|A| = a$, $|B| = b$ given, s.t. $A \times B \subset \Omega$

provided that $b\binom{|R|}{a} \leq |S| \binom{m}{a}$.

For $\mathbb{F}_q$, $q = p^e$, $p \neq 2$:

Take $R = S = \mathbb{F}_q$, $\Omega = \{(r,s) \mid r - s$ is a nonzero square in $\mathbb{F}_q\}$
so $m = \frac{q-1}{2}$.

Let $q \longmapsto a(q), b(q)$ be two functions of a variable q, with integral values ≥ 1 for $q = p^e$, p prime $\neq 2$, with

$$\begin{cases} a(q) \leq c_1 \log q \\ b(q) \leq q^{c_2} \end{cases}$$

where $c_2 + c_1 \log 2 < 1$.

Claim: Then, for q large enough, there exists $A, B \subset \mathbb{F}_q$ with $|A| = a(q)$, $|B| = b(q)$, and $A \times B \subset \Omega$.

[This is approx. what the naive approach would give

$b_1 \quad b_2 \quad \cdots\cdots \quad b_m$ $\qquad q\left(\frac{1}{2}\right)^{\alpha}$?

$\alpha \sim \log q \Rightarrow \left(\frac{1}{2}\right)^{\alpha} = \frac{1}{q^{\varepsilon}}$

which suggests $a(q) \leq c_1 \log q$ is reasonable]

If q is a square,

$\mathbb{F}_q$

$\mathbb{F}_{q^{1/2}}$ $\quad \underbrace{\vdash\!\!\dashv}_{\frac{1}{2}q^{1/2}} \underbrace{\vdash\!\!\dashv}_{\frac{1}{2}q^{1/2}}$ $\qquad$ every difference $\in \mathbb{F}_{q^{1/2}} \subset (\mathbb{F}_q^{*})^2$

So $a(q) \leq q^{1/2}$, $b(q) \leq q^{1/2}$. Much larger!

Proof of Claim

To be checked: for q large enough,

$$b(q)\binom{q}{a(q)} \overset{?}{\leq} q\binom{\frac{q-1}{2}}{a(q)}$$

i.e.,
$$b(q)\frac{q!}{(q-a(q))!} \overset{?}{\leq} q\frac{\left(\frac{q-1}{2}\right)!}{\left(\frac{q-1}{2}-a(q)\right)!}$$

Stirling: $\log(x!) = (x+\frac{1}{2})\log x - x + O(1)$

Suppose $1 \le y \le x^{1/2}$. Then

$$\log\left(\frac{x!}{(x-y)!}\right) = (x+\tfrac{1}{2})\log x - x - (x-y+\tfrac{1}{2})\left(\log x + \log(1-\tfrac{y}{x})\right) + x - y + O(1)$$

$$= y\log x + O(1)$$

[Since $-y - (x-y+\tfrac{1}{2})\log(1-\tfrac{y}{x}) =$

$$= \cancel{-y} - (x - \cancel{y} + \tfrac{1}{2})\left(-\tfrac{y}{x} + O(\tfrac{y^2}{x^2})\right)$$

$y^2 \le x$

$$= O(1)$$]

So check that

$$\log b(q) + a(q)\log q + O(1) \overset{?}{\le} \log q + a(q)\log\frac{q-1}{2}$$

$a(q) \le c_1 \log q$
$b(q) \le q^{c_2}$] $\log b(q) \le c_2 \log q$.

So $\log q - \log b(q) \overset{?}{\ge} a(q)\left(\log q - \log\frac{q-1}{2}\right) + O(1)$

So $\quad a(q)\left(\log q - \log \frac{q-1}{2}\right) + O(1) \leq c_1 \log q \,(\log 2 + o(1))$

$$\log q - \log b(q) \geq (\log q)(1 - c_2)$$

So want $\boxed{1 - c_2 > c_1 \log 2}$, which is our condition. ☒

Starting from such $A, B \subset \mathbb{F}_q$, we make a 2-class field tower starting from $\mathbb{P}_1$ and making quadratic extensions.

Assume $a = \text{even} = 2\alpha$

Write $\{a_1, a_1', \ldots, a_\alpha, a_\alpha'\} = A$.

If t is the variable in $\mathbb{P}_1$, take the quad. extn. given by

$$\sqrt{(t-a_i)(t-a_i')} \quad i = 1, \ldots, \alpha.$$

(So Fct. field is $\mathbb{F}_q\left(t, \sqrt{(t-a_i)(t-a_i')}\right)$)

In that ext., the points of B split completely (by our choice of ≤ 2).

Now go to $C \longleftrightarrow \mathbb{F}_q\left(t, \sqrt{\prod (t-a_i)(t-a_i')}\right)$

Elements of B give B_C = subset of C coming from B,

$$|B_C| = 2|B| = 2b(q)$$

and C has $\alpha - 1$ independent quadratic extns which are unramified and where B_C splits completely.

(Namely given by

The 2-class field tower is infinite if $|B_c| \leq \frac{(\alpha-1)^2}{4} - (\alpha - 1)$

So choose $\alpha \sim c \log q$

$$|B_c| \sim c'(\log q)^2$$

if $c' < \frac{c}{4}$, the condn. is satisfied.

Hence, infinite class field tower, so

$$A(q) \geq \frac{|B_c|}{g_c - 1} \asymp \frac{(\log q)^2}{\log q} \asymp \log q.$$

C is hyperelliptic, ramified at $2\alpha = a(q)$ pts, and so $g_c = \alpha - 1 \asymp \log q$.

So $\boxed{A(q) \geq c \log q}$ for some c. (For q odd).

When q is a square, we can take $|B_c| \asymp q^{1/2}$, $g_c \doteq q^{1/4}$, so get $A(q) \geq c q^{1/4}$.

(But modular tower gives $q^{1/2}$).

For $q = 2^e$, can use $\left\{ \begin{array}{l} \text{Artin-Schreier extns} \\ \text{or} \\ \text{a 3-tower} \end{array} \right.$

<u>Construction for $g=2$</u> <u>Claim</u>: $A(2) \geq \frac{2}{9} = 0.222\ldots$

<u>First</u>: Simple construction for $A(2) \geq \frac{1}{5} = 0.2$.

Take

$$\begin{array}{c} C \\ {\scriptstyle 2}\big\downarrow \\ \mathbb{P}_1 \end{array} \quad y^2 + y = t^3 + t + \sum_{\substack{\text{irred polyn } \varphi(t) \\ \text{of deg } 2,3,4}} \frac{t^2+t}{\varphi(t)}$$

$\qquad\qquad t$

So: sum is over

$$\left\{\begin{array}{l} \deg 2 \longrightarrow \\ \deg 3 \longrightarrow \\ \deg 4 \longrightarrow \end{array}\right\} \begin{array}{l} t^2+t+1 \\ t^3+t+1,\ t^3+t^2+1 \\ t^4+t+1,\ t^4+t^3+1,\ t^4+t^3+t^2+t+1. \end{array}$$

We'll see $g_C = 21$.

Take $\{0,1\} \subset \mathbb{P}_1$; these split completely in C to give a set S of 4 pts.

$$\begin{array}{cc} S & C \\ \big\downarrow & \big\downarrow{\scriptstyle 2} \\ \{0,1\} & \mathbb{P}_1 \end{array}$$

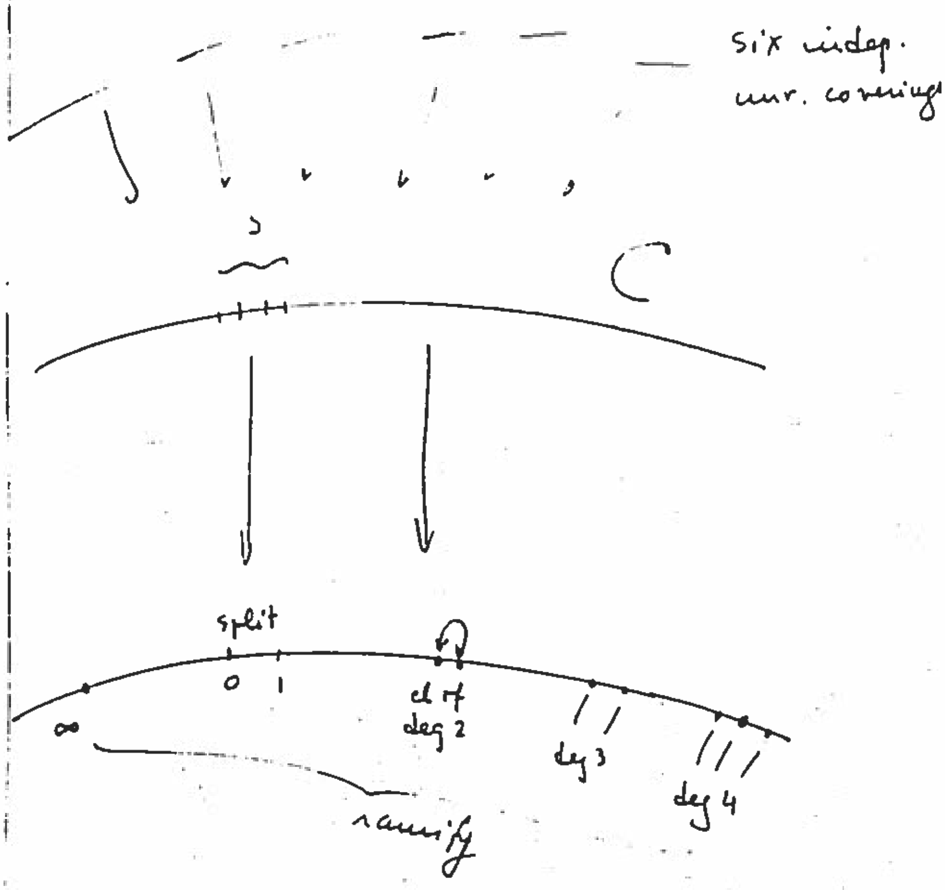
Have 6 indep. unramified quad. extns, given by

$$y^2 + y = \frac{t^2+t}{\varphi(t)} \quad \text{for the six } \varphi(t) \text{ above}$$

and $\{0,1\}$ split completely. (Same argument as before.)

C is ramif at roots of $\varphi(t)$ and at ∞.

Picture $\longrightarrow$



<u>Assume</u> : $g_c = 21$, class field tower is infinite.

Then $A(2) \geq \dfrac{|S|}{g_c - 1} = \dfrac{4}{21-1} = \dfrac{4}{20} = \dfrac{1}{5}$.

<u>Class Field Tower</u> : condition is $|S| \leq \dfrac{d^2}{4} - d + 1$

$|S| = 4$, $d \geq 6$, so $\dfrac{d^2}{4} - d + 1 \geq \dfrac{36}{4} - 6 + 1 \geq 4$.

So class field tower is infinite.

<u>Genus</u> : Know: $g_c - 1 = n(g_{c_0} - 1) + \sum$ contrib. of ramification.
?

$$C \xrightarrow{n} C_0 \ni P$$

Go to alg. closure: take a local param t at P,
Look at dt. Lift it to C.
Ramif $\Rightarrow$ dt will have zero on the fiber

and

To see this, take ω diff'l form $\neq 0$ on C_0, w/o zero or pole at the ramif. pts.

Lift to ω_c. Now $2g_c - 2 = \deg(\omega_c) = n\deg(\omega) + \text{extra zeros}$

$$= n\deg(\omega) + \sum \text{deg of } dt \text{ on fiber}$$

Now divide by 2 to get the formula.

Now suppose $p=2$, Artin-Schreier extn $y^2+y=\Psi(t)$
local computation, so work in field of power-series.

$$\Psi(t) = \frac{c_0}{t^n} + \cdots \qquad n \text{ odd} \geq 1.$$

[If Ψ is hol., no ramif.; if $\frac{1}{t^2}+\cdots$, remove $\Psi - \left(\frac{1}{t^2}+\frac{1}{t}\right)$ until we get n odd].

Claim: Local contrib at that place is $\frac{1}{2}(n+1)$,
i.e., "deg of dt in extension" $= n+1$ (even)

$$v_K(y) = \tfrac{1}{2} v_K\left(\frac{1}{t^n}\right) = -n \qquad \text{since } v(t)=2 \text{ (ramification)}$$

$$\begin{array}{c} K \\ {\scriptstyle 2}\,\Big| \\ K_0 \; t \end{array}$$

$$dy = \frac{c_0}{t^{n+1}}\,dt + \cdots \qquad (\text{char } 2)$$

If θ local parameter of K, $\qquad y = \theta^{-n}\cdot \text{unit},$

so $\quad dy = \frac{d\theta}{\theta^{n+1}} + \cdots$

so $\quad v_K(dy) = -(n+1)$

So $\quad v_K(dy) = -2(n+1) + v_K(dt) \implies v_K(dt) = n+1.$

In our case, $y^2+y = \underbrace{t^3+t}_{} + \underbrace{\sum_{\deg 2,3,4} \frac{t^2+t}{\varphi(t)}}_{}$

pole of order $3 = n$ at ∞

$\frac{1}{2}(n+1) = 2$

simple poles at these

$\deg \varphi = 2 \to$ two simple poles $\to \frac{1}{2}(2) + \frac{1}{2}(2) = 2$

Same for $\deg \varphi = 3$ or 4.

So $\quad g_C - 1 = 2(g_0 - 1) + \sum$ local contrib

$= -2 + 2 + \sum \deg \varphi$

$= -2 + 2 + 20$

So $\boxed{g_C = 21}$. ▨

Lemma Let C be a curve over $\mathbb{F}_2$; let S be a set of closed points of C, let $\underline{m}$ be a positive divisor of C disjoint from S. Assume that $\deg(\underline{m}) \geq |S|$. Then there is a quadratic extension of C which is unramified outside $\underline{m}$, where S splits completely and where the contribution of ramification is at most $\deg \underline{m}$.

Proof – later (done by CFT)

Assuming the lemma, we can improve the result above:

Choose C = an elliptic curve with 2 rational points (and no more).

$N_1' = \# C(\mathbb{F}_2) = 2$

Now $N_n = \# C(\mathbb{F}_n) = 1 + 2^n - \underbrace{(\pi^n + \bar{\pi}^n)}_{t_n}$

and $t_n = t_{n-1}\, t_1 - q\, t_{n-2}$ since $\pi\bar{\pi} = q$!

Here $t_0 = 2$, $t_1 = 1$, $q = 2$ $(N_1 = 2 = 1 + 2 - t_1$

So $t_n = t_{n-1} - 2 t_{n-2}$

So $t_2 = -3$, $t_3 = -5$, $t_4 = 1$

$\therefore N_1 = 2$, $N_2 = 8$, $N_3 = 14$, $N_4 = 16$

If a_i = nber of closed pts of $C/\mathbb{F}_2$ of degree i $(\text{so } N_n = \sum_{i|n} i a_i)$

So $\underbrace{a_2 = 3, \ a_3 = 4}_{\text{lots of these}}$, $a_4 = 2$.

Make 7 quadratic extensions of C s.t. two rat'l pts split completely ramified each at a different closed pt of degree 2 or 3; contrib. to ramification will be just 2, 2, 2, 3, 3, 3, 3.

with same construction before } $d = 6$ as before, and $g - 1 = 2(1-1) + \sum$ contrib

$g - 1 = 18 \implies g = 19$

10/31 **Something from CFT**

X curve $/\mathbb{F}_q$, genus g, K fct. field.

(modulus) $\quad \underline{m} = \sum_{P \in S} n_P P \quad$ be a positive divisor, S finite, $n_P \geq 1$, P closed.

$$Cl_{\underline{m}}(X) = \{\text{divisors of } X \text{ prime to } S\} \Big/ \{(f)\}$$

where $f \in K^{\times}$, and $f \equiv 1 \bmod^{\times} \underline{m}$

(this means that $f \in 1 + \mathfrak{max}_P^{\,n_P}$ locally at each $P \in S$, or equiv., $v_P(f-1) \geq n_P \quad \forall P \in S$).

If $\underline{m} = 0$, $\quad Cl_{\underline{0}}(X) = Pic(X)$
$\qquad\qquad\qquad\quad \overset{\shortparallel}{Cl(X)}$

Recall $\quad \boxed{0 \longrightarrow J(\mathbb{F}_q) \longrightarrow Cl(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0} \quad$ exact

and

$$0 \to \text{kernel} \to Cl_{\underline{m}}(X) \longrightarrow Cl(X) \longrightarrow 0$$

obvious $\qquad$ almost obvious.

assume $\underline{m} \neq 0$; [redacted] if U_P = local units at P, $U_P^{(n_P)} = \{u \in U_P \mid v(u-1) \geq n_P\}$

We have $\quad 0 \longrightarrow \mathbb{F}_q^{\times} \longrightarrow \prod U_P / U_P^{(n_P)} \longrightarrow Cl_{\underline{m}}(X) \longrightarrow Cl(X) \longrightarrow 0$

CFT:

Let G be a finite group and let
$$\alpha: Cl_m(X) \longrightarrow G \quad \text{be onto.}$$
Then CFT constructs an abelian extension K_α/K with Galois group G s.t.

1) K_α/K unramified outside S

2) If $P \notin S$, the Frob of P in G is the image by α of "P", viewed as a divisor.

3) If $P \in S$, the map
$$\begin{tikzcd} U_P \arrow[r] \arrow[rr, bend right] & Cl_m(X) \arrow[r, "\alpha"] & G \end{tikzcd}$$
is the one attached by local class field theory, and the image is the inertia group.

I also have $K_P^\times \longrightarrow G$, image is decomp. group.

Let $P_1, \ldots, P_s$ be closed points disjoint from S. If I want extns in which these split completely, I have:

To have P_i split in K_α/K it is nec. & suff. that $\alpha((P_i)) = 0$, $(P_i) \in Cl_m(X)$.

Let l be a prime number, let d_p = l-rank of $U_P/U_P^{(n_P)}$ (this is a group of order $(q^{\deg(P)} - 1)q^{(n_P-1)\deg(P)}$)

Let ε = l-rank of $\mathbb{F}_q^\times$ $\begin{pmatrix} 0 \text{ if } l \nmid q-1 \\ 1 \text{ if } l \mid q-1 \end{pmatrix}$

Claim $\left\{ \begin{array}{l} \text{Assume that } s \leq \sum d_p - \varepsilon. \\ \text{Then: } \exists \text{ a cyclic extension of deg } l \text{ obtained} \\ \text{through an } \alpha \text{, where the } P_i\text{'s } \underline{\text{split}} \ \underline{\text{completely}}. \end{array} \right.$

Have $\quad 0 \to \text{Local} \to Cl_m \longrightarrow J(\mathbb{F}_q) \times \mathbb{Z} \to 0,$

so

$$Cl_m \cong \mathbb{Z} \times \Phi \qquad \Phi \supset \text{Local}, \ \underline{\text{finite}}.$$

So l-rank of Cl_m/lCl_m is $\geq 1 + \sum d_p - \varepsilon$.

There is a $\underline{\text{hyperplane}}$ Cl_m/lCl_m (as $\mathbb{F}_l$-vector sp.) containing all the P_i; this gives the desired extension.

Given K_α/K, assuming no constant-field extn. corresp to the condn:

$$\begin{array}{ccc} Cl_m & \xrightarrow{\deg} & \mathbb{Z} \\ & \searrow^{\alpha} & \\ & & G \end{array}$$

$\deg: \operatorname{Ker}\alpha \to \mathbb{Z}$ is surjective.

In this case, I want the genus of K_α.

Look at characters $\chi : G \to \mathbb{C}^\times$. This gives maps

$$U_P \to Cl_m \to G \xrightarrow{\chi} \mathbb{C}^\times .$$

So exp. of cond. of χ at $P = f_P(\chi) = \begin{cases} 0 & \text{if } U_P \to \mathbb{C}^\times \text{ is trivial} \\ \text{smallest } e \text{ s.t. } U_P \to \mathbb{C}^\times \text{ is trivial on } U_P^{(e)} & \end{cases}$

So Formula for the genus g_α of K_α:

$$2g_\alpha - 2 = [K_\alpha : K](2g-2) + \deg(\text{discriminant ideal})$$

and $\quad \text{disc} = \sum_{P,\chi} f_P(\chi)\cdot P,$

so we get

$$\boxed{2g_\alpha - 2 = |G|(2g-2) + \sum f_P(\chi) \deg P}$$

In our situation: $g=2,\ \ell=2,\ |G|=2$

At each P we get <u>one</u> number f_P (only one character!).

On the other hand, we've noted that writing

$$y^2 + y = \frac{a_0}{t^m} + \dots = \varphi \quad m \text{ odd} \geq 1,$$

the local contrib was measured by m.

<u>Have</u>: $\boxed{f_p = m+1}$

"<u>Proof</u>": I get $\quad U_p \longrightarrow \{\pm 1\} = \mathbb{Z}/2\mathbb{Z}$

explicitly: $\quad u \in U_p$ can be viewed as $u(t) \in \mathbb{F}_{2^e}[[t]]$; then the map is

$$u(t) \longmapsto \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}\left(\mathrm{Res}\left[\varphi(t)\frac{du(t)}{u(t)}\right]\right)$$

(For an Artin-Schreier extn as above!)

Then, if $\quad u \equiv 1 \mod t^{m+1}$

$$\frac{du}{u} = c\,t^m\,dt + \dots$$

$$\varphi\frac{du}{u} \text{ hol.}, \text{ so } \mathrm{Res} = 0$$

But if $u \equiv 1 \mod t^m$, <u>not</u> mod t^{m+1}, will get simple pole, hence $\mathrm{Res} \neq 0$.

2-rank of $U_p/U_p^{(n_p)}$ $\qquad$ n_p even ≥ 2

res field $\mathbb{F}_{2^e}$

$$U_p/U_p^{(n_p)} = \{ \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} \mod t^n \} \quad \begin{matrix} \alpha_0 \neq 0 \Rightarrow \alpha_0 \in \mathbb{F}_{2^e}^* \\ \alpha_i \in \mathbb{F}_{2^e} \end{matrix}$$

for 2-rank, think only

$$1 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} \qquad \alpha_i \in \mathbb{F}_q = \mathbb{F}_{2^e} \text{, so}$$

order $= q^{n-1}$

squares : $\underbrace{1 + \alpha_1^2 t^2 + \cdots}$ = those where $\alpha_1 = \alpha_3 = \cdots = 0$)

there are $\frac{n}{2}$ odd indices, so order $= q^{n/2 - 1}$

$\therefore$ AB : $|G/G^2| = q^{n/2}$, so 2-rank $= e \cdot \frac{n}{2}$.

This proves the statement made last time about constructing extensions where certain points split.
(Just check that #points < $\sum d_p - e$!)

Se Th 29

Optimal functions for number of points

$\mathbb{F}_q$, genus g, N points

(*) If $c_n \geq 0$, and $f = 1 + \sum 2 c_n \cos n\theta \geq 0$ for all θ

$$= 1 + \sum c_n (t^n + t^{-n}) \quad , \; t \in S^1 \text{ unit circle.}$$

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

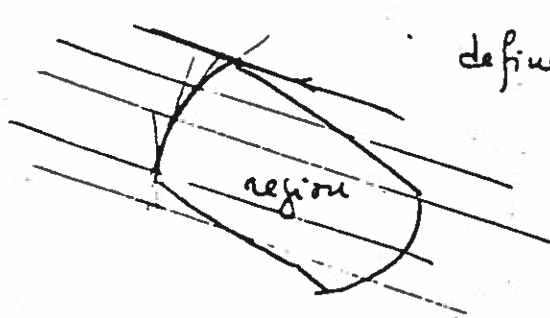
Problem: Knowing N and q, what is (if any) the best choice of (c_n)? (I.e., the one that maximizes the expression.)

If $(c_n) \in (*)$, what is the max of $\sum c_n \big(\underbrace{(N-1)q^{-n/2} - q^{n/2}}_{-\sum c_n \gamma_n}\big)$

Call the max $g(N,q)$.

This is a linear programming question:

given variables, $\underbrace{\text{linear inequalities on them}}_{\text{defines some convex region}}$



given linear form $\longleftrightarrow$ cut region by lines

In linear programming, every problem has a dual problem. So let's introduce the dual problem, but in a more natural way.

Suppose we want $\geq N$ pts, $g \to$ genus?
We must have then $N_n \geq N, \forall n$. $\left(N_n = \# X(\mathbb{F}_{q^n}) \right)$
If $\varphi_1, \dots, \varphi_g$ are the angles of Frob.

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

So $$q^n + 1 - q^{n/2} \sum_{\alpha=1}^{g} 2 \cos n\varphi_\alpha \geq N$$

Introduce the measure on S^1 $\mu = \sum \left(\delta_{e^{i\varphi_\alpha}} + \delta_{e^{-i\varphi_\alpha}} \right)$ $\quad \delta$ = Dirac measure.
$\mu \geq 0$, $\mu(S^1) = 2g$.

Then $$\sum_{\alpha=1}^{g} 2\cos n\varphi_\alpha = \int t^n \mu(t) \quad \left[= \int \tfrac{1}{2}(t^n + t^{-n}) \mu(t) \right.$$

So I'm looking for $\mu \geq 0$ on S^1 with

$$\int t^n \mu(t) \leq \underbrace{q^{n/2} - (N-1) q^{-n/2}}_{\gamma_n} \qquad n = 1, 2, \dots$$

So look at all

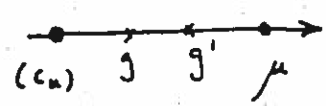
$$\boxed{\mu \geq 0, \quad \underbrace{\int t^n \mu(t) \leq \gamma_n}_{(**)_n} \quad n = 1, 2, \dots} \qquad (**),$$

and ask what is the <u>lower bound</u> of $\frac{1}{2}\int 1\,\mu(t)$?
Call it $g'(N, q)$

This is the dual problem.

<u>Lemma 1</u>: If $\mu \in (**)$, $(c_n) \in (*)$, then

$$-\sum c_n \gamma_n \leq \int \tfrac{1}{2}\mu(t).$$



In particular, $g(N, q) \leq g'(N, q)$.

<u>Lemma 2</u>: We have equality above iff μ has support contained in the set of zeros of the fct $1 + \sum c_n (t^n + t^{-n})$ on S^1 and $(**)_n$ is an equality for every n s.t. $c_n = 0$.

<u>Theorem</u>: Let μ and (c_n) be such as in Lemma 2.
Then $g(N, q) = \frac{1}{2}\int \mu(t) = -\sum c_n \gamma_n$.

Proof: Let $f = 1 + \sum c_n (t^n + t^{-n}) \geq 0$

So $\mu(f) = \int f \mu = \mu(1) + 2 \sum c_n \mu(t^n) \geq 0$

But $\mu(t^n) = \int t^n d\mu \leq \gamma_n$, so

$$\mu(\tfrac{1}{2}) \geq -\sum c_n \mu(t^n) \geq -\sum c_n \gamma_n$$

QED, Lemma 1.

Proof (2): Want $\mu(f) = 0$ above, hence since $f \geq 0$ μ must be concentrated on the zeros.

I also want $\mu(t^n) = \gamma_n$ unless $c_n = 0$,

QED (2). $\blacksquare$

Example: Take $q+1 \leq N \leq q^{3/2} + 1$

Claim: in this range Weil is optimal.

Weil $\longleftrightarrow$ $1 + \cos\theta$, so $\underbrace{c_1 = \tfrac{1}{2},\ c_n = 0,\ n \geq 2}$

Claim: this choice is optimal.

It is enough to exhibit a μ with equality!

We want $g = -\frac{1}{2}\gamma_1 = -\frac{1}{2}\left(q^{1/2} - (N-1)q^{-1/2}\right)$

$$= \frac{1}{2}\left((N-1)q^{-1/2} - q^{1/2}\right) \geq 0$$

And take μ = Dirac at $t=-1$ (angle $\overset{\theta=}{\pi}$) with weight $2g$, where g is given by this last eqn.

To check: $\begin{cases} 1+\cos\theta \geq 0 \quad \text{OK}, \quad c_n \geq 0 \quad \text{OK} \\ \text{so } (*) \text{ OK.} \end{cases}$

$\begin{cases} \text{clearly } \mu \text{ is concentrated at the zero of } 1+\cos\theta \\ \text{to check: } \begin{cases} \mu(t^n) \leq \gamma_n \quad \text{for } n \geq 1 \\ \mu(t) = \gamma_1 \end{cases} \end{cases}$

$$\mu(t) = 2g(-1) = -2g$$

to check $-2g = \gamma_1$ OK by construction

$$\mu(t^2) = 2g(-1)^2 = -\gamma_1 \overset{?}{\leq} \gamma_2$$

$$-\gamma_1 = -q^{1/2} + (N-1)q^{-1/2} \overset{?}{\leq} q - (N-1)q^{-1} = \gamma_2$$

$$(N-1)(q^{-1/2} + q^{-1}) \overset{?}{\leq} q + q^{1/2}$$

$$(N-1)(1+q^{1/2}) \overset{?}{\leq} q^{3/2}(1+q^{1/2})$$

$$(N-1) \overset{?}{\leq} q^{3/2}$$ OK by condition on N!

$$\mu(t^3) = -2g = \gamma_1 \overset{?}{\leq} \gamma_3 \qquad \gamma_3 \geq 0,\ -2g < 0 \ \text{ ok}.$$

$$\mu(t^4) = 2g = -\gamma_1 \leq \underbrace{\gamma_2 \leq \gamma_4}$$

γ_n increases for n large.

and larger n are similarly ok. $\blacksquare$

Theorem on Linear Inequalities on $\mathbb{R}^n$:

Let f_α be finitely many additive functions $(\sum \alpha_i x_i + \beta)$ on $\mathbb{R}^n$. Then the following are equiv.:

(i) The equations $f_\alpha \geq 0$ have no common solution.

(ii) $\exists\, c_\alpha \geq 0$ s.t. $1 + \sum c_\alpha f_\alpha = 0$ identically in $\mathbb{R}^n$.

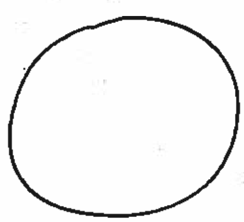
11/7

Oesterlé's "Optimal" computation of lower bound for g (given N, q)

On Machine:
$\left\{\begin{array}{ll} \text{ON} & \\ \text{RUN 2000} & \\ \text{NOMBRE DE POINTS?} & 65 \text{ enter} \\ \text{Q ?} & 8 \quad " \\ \text{GENRE} >= 14 & \end{array}\right.$

Recall: Last time we defined a "dual" problem to what we wanted, and saw that

$$\left.\begin{array}{l} \text{admissible } \mu \text{ measure} \\ + \\ \text{admissible } (c_n) \end{array}\right\} \text{match} \longrightarrow \text{optimal solution.}$$



$S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

admissible μ
$\left[\begin{array}{l} \mu \text{ will be a positive measure on } S^1 \text{ s.t.} \\ \bullet \text{ symmetric w.r.t. } z \mapsto \bar{z} = z^{-1} \\ \bullet \int t^n \mu(t) = \langle t^n, \mu \rangle \geq q^{n/2} - (N-1) q^{-n/2} \\ \qquad \text{for } n \geq 1 \end{array}\right.$

(Where N, q are given).

admissible (c_n)
$\left[\begin{array}{l} c_n \geq 0 \\ 1 + \sum_{n \geq 1} c_n (t^n + t^{-n}) \geq 0 \quad \text{on } S^1 \end{array}\right.$

We attach

$$\left\{\begin{array}{l} \mu \longmapsto \frac{1}{2}\int \mu(t) = \langle \tfrac{1}{2}, \mu \rangle \\ \\ (c_n) \longmapsto \sum c_n\left((N-1) q^{-n/2} - q^{n/2} \right) \end{array}\right) \geq$$

We say μ and (c_n) <u>match</u> if $\frac{1}{2}\int \mu(t) = \sum c_n(\quad)$; if this happens, the common value is the best $g(N,q)$ that the explicit formula can give.

(Usually not even rational, of course...)

Oesterlé found an explicit choice of (c_n) (working for every (q,N)), an explicit choice of μ (working for $q \geq 3$ and sometimes for $q = 2$), and they match.

Hence, this gives $g(N,q)$, at least for $q \geq 3$.

• <u>Let $\lambda = N-1$, $\alpha = q^{1/2}$</u>

So condn. on μ is $\int t^n \mu(t) \geq \alpha^n - \lambda\alpha^{-n}$, $n \geq 1$

We showed $\left\{\begin{array}{l} \lambda \leq \alpha^3 \longrightarrow \text{Weil estimate is best} \\ \qquad \text{(i.e., optimal is given by } 1 + \tfrac{1}{2}(t+t^{-1}) = 1 + \cos\varphi \text{)} \\ \\ \lambda = \alpha^4 \longrightarrow \text{Suzuki (char = 2)} \\ \\ \lambda = \alpha^6 \longrightarrow \text{Ree} \end{array}\right.$

Method:

Define m by $\boxed{\alpha^m < \lambda \leq \alpha^{m+1}}$. $\left(m = \left[\frac{\log\lambda}{\log\alpha}\right]\right)$

I will assume $m \geq 2$. (if not, $g = 0$ is OK ...)

Put $u = \dfrac{\alpha^{m+1} - \lambda}{\lambda\alpha - \alpha^m}$; by the assumptions, $0 \leq u < 1$.

Consider the equation:

$$\cos\frac{m+1}{2}\varphi + u\cos\frac{m-1}{2}\varphi = 0$$

There is exactly one solution φ_0 in the range $\frac{\pi}{m+1} \leq \varphi_0 < \frac{\pi}{m}$.

Then the optimal g (for $q \geq 3$, at least) is

$$\boxed{g = \frac{(\lambda-1)\alpha\cos\varphi_0 + \alpha^2 - \lambda}{\alpha^2 - 2\alpha\cos\varphi_0 + 1}}$$

(When $q=2$, this is the value given by a choice of (ε_n).)

We try to find μ of the following shape:

concentrated on a symmetric set $T \subset S^1$, with $|T| = m-1$, with

(T) $$\int t^n \mu(t) = \alpha^n - \lambda\alpha^{-n} \quad \text{for } n = 1, \dots, m-1,$$

and the mass ν_t of $t \in T$ being strictly positive. We also need $\nu_t = \nu_{\bar{t}}$, of course.

On the other hand, look for (c_n) s.t.

$$f(t) = 1 + \sum_{n=1}^{m-1} c_n (t^n + t^{-n}) \quad \text{is zero on } T$$

$(c_n \geq 0,\ f(t) \geq 0$ on $S^1)$.

If we can do this, we have a match (as seen before).

<u>Lemma</u> If T satisfies the condition (T), then T is <u>contained</u> in the set of solutions of)

$$t^{m+1} + 1 + u(t^m + t) = 0 \qquad (1)$$

(This has $m+1$ solutions on S^1, which are symmetric, so to get T we need to discard one pair).

Rewrite as $t = e^{i\varphi}$, get the equation for u given above.

So we throw out the solutions $t = e^{\pm i\varphi_0}$:

T = solutions of (1) which are different from $e^{\pm i\varphi_0}$.

<u>Proof of Lemma</u>: Suppose T is given.

T has $m-1$ elements in S^1.

$\mu = \sum \nu_t \delta_t$ so the integral is $\sum_{t \in T} \nu_t t^n = \alpha^n - \lambda \alpha^{-n}$ $n = 1, \ldots, m-1$

The system $\boxed{\sum_{t \in T} \nu_t t^n = \alpha^n - \lambda \alpha^{-n} \qquad n = 1, \ldots, m-1}$ $(*)$

has $(m-1)$ linear eqns, $(m-1)$ unknowns, determinant is Van der Monde t $(t \in T)$, so $\neq 0$.

So it has a unique solution $\nu_t = $ ——

Now force $\nu_t = \nu_{\bar{t}}$ for every $t \in T$. This will imply equation (1).

Rewrite $(*)$ as follows:

$(*) \longleftrightarrow$ for every polynomial Φ of degree $\leq m-1$, with constant term 0,

$$\boxed{\sum \nu_t \Phi(t) = \Phi(\alpha) - \lambda \Phi(\alpha^{-1})}. \qquad (**)$$

Let
$$P(X) = \prod_{t \in T} (X - t)$$

T symmetric $\Rightarrow$ $P(X^{-1}) = P(X) X^{1-m}$

$$-\frac{1}{X^2} P'(X^{-1}) = P'(X) X^{1-m} + (1-m) P(X) X^{-m}$$

So if $t \in T$, $-\frac{1}{t^2} = \bar{t}^2$:

$$\boxed{-\bar{t}^2 P'(\bar{t}) = P'(t)\, t^{1-m}}$$

Let $t \in T$; define $Q_t(x) = x \prod_{\substack{t' \in T \\ t' \neq t}} (x - t') = \frac{x\, P(x)}{x - t}$

Now $\left| \begin{array}{l} Q_t(t') = 0 \text{ for } t' \in T,\ t' \neq t. \\ Q_t(t) = t\, P'(t) \end{array} \right.$

Apply (**) to $\Phi = Q_t$:

get $\quad \nu_t\, Q_t(t) = Q_t(\alpha) - \lambda\, Q_t(\alpha^{-1})$

so $\quad \boxed{\nu_t = \frac{Q_t(\alpha) - \lambda\, Q_t(\alpha^{-1})}{t\, P'(t)}}$

rewrite :

$$t\, P'(t)\, \nu_t = \frac{\alpha P(\alpha)}{\alpha - t} - \lambda\, \frac{\alpha^{-1} P(\alpha^{-1})}{\alpha^{-1} - t}$$

we have $\quad P(\alpha^{-1}) = P(\alpha)\, \alpha^{1-m}$

so $\quad t\, P'(t)\, \nu_t = P(\alpha) \left\{ \frac{\alpha}{\alpha - t} - \lambda\, \frac{\alpha^{-m}}{\alpha^{-1} - t} \right\}$

$$t P'(t)\, \nu_t = P(\alpha) \frac{1-\alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1-\alpha t - \alpha^{-1} t + t^2}$$

Now $\nu_t = \nu_{\bar t} \longrightarrow \frac{1}{tP'(t)} \cdot \frac{1-\alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1-\alpha t - \alpha^{-1}t + t^2} = \frac{1}{\bar t P'(\bar t)} \frac{1-\alpha\bar t - \lambda\alpha^{1-m} + \bar t\lambda\alpha^{-m}}{1-\alpha\bar t - \alpha^{-1}\bar t + \bar t^2}$

Also $-P'(\bar t) = P'(t)\cdot t^{3-m}$, so

$$\frac{1}{t}\cdot\{\text{———}\} = \frac{-1}{t^{2-m}}\cdot\{\text{———}\}$$

so $-t^{1-m}\cdot\{\text{———}\} = \{\text{———}\}$

$$-t^2\left(1-\alpha\bar t - \alpha^{-1}\bar t + \bar t^2\right) = 1 - \alpha t - \alpha^{-1} t + t^2$$

So end up with

$$-t^{m+1}\left(1-\alpha\bar t - \lambda\alpha^{1-m} + \lambda\alpha^{-m}\bar t\right) = \left(1-\alpha t - \lambda\alpha^{1-m} + \lambda\alpha^{-m} t\right)$$

$$t^{m+1}(1-\lambda\alpha^{1-m}) + t^m(\lambda\alpha^{-m} - \alpha) - t(\alpha - \lambda\alpha^{-m}) + (1-\lambda\alpha^{1-m}) = 0$$

$$u = \frac{\alpha^{m+1} - \lambda}{\lambda\alpha - \alpha^m} = \frac{\alpha - \lambda\alpha^{-m}}{\lambda\alpha^{1-m} - 1}$$

So

$$t^{m+1} + 1 + u(t^m + t) = 0 .$$ ∎

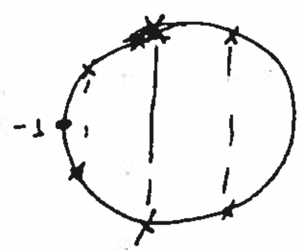
Note this works for any m ; our choice of m is equiv to $u \in [0,1)$.

Now, study the equation $\cos\frac{m+1}{2}\varphi + u\cos\frac{m-1}{2}\varphi = 0$, where $0 \le u < 1$.

$$F(\varphi) = \frac{\cos\frac{m+1}{2}\varphi}{\cos\frac{m-1}{2}\varphi}$$

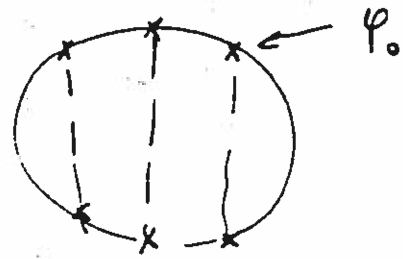
(We want to show $t^{m+1} + 1 + u(t^m + t) = 0$ has $m+1$ distinct solutions on S^1, and "locate" them.)

if m is even : -1 is a solution



($m = 6$)

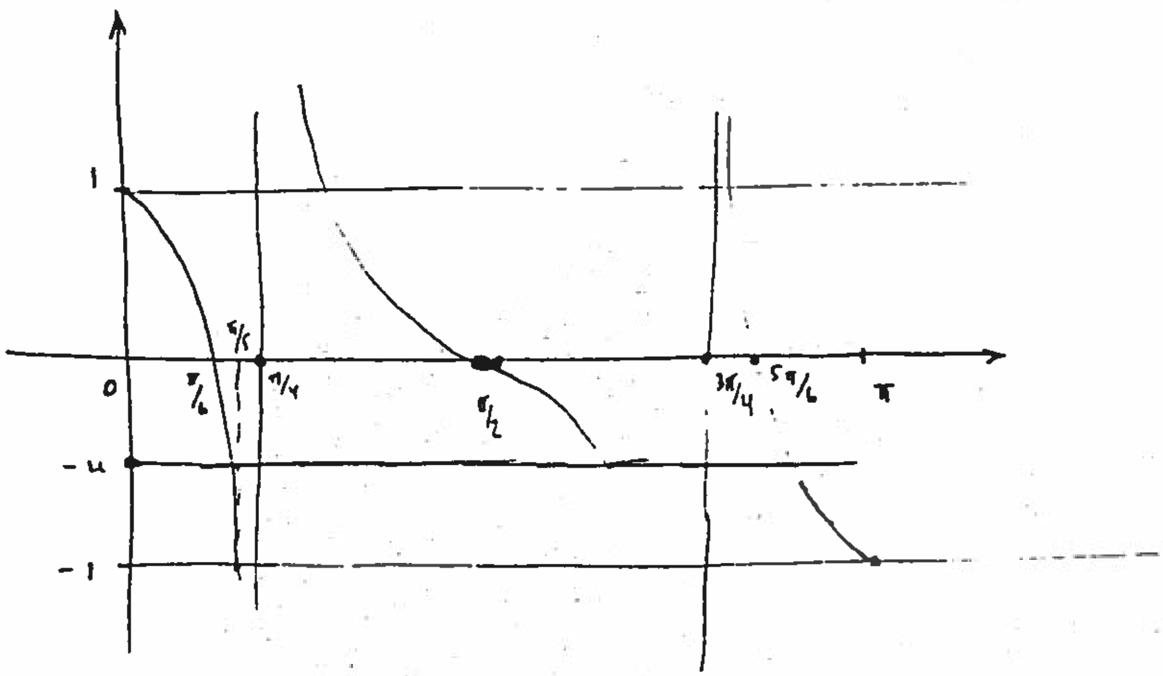
if m is odd : -1 is not a solution



$m = 5$

Take $m = 5$, for instance.

Graph on $0 \le \varphi \le \pi$ of $F(\varphi) = \dfrac{\cos 3\varphi}{\cos 2\varphi}$



$\cos 2\varphi = 0 \iff 2\varphi = \frac{\pi}{2}, \frac{3\pi}{2} \Rightarrow \varphi = \frac{\pi}{4}$ or $\frac{3\pi}{4}$

$F(\pi/5) = \dfrac{\cos 3\pi/5}{\cos 2\pi/5} = -1$ (since $3\pi/5 + 2\pi/5 = \pi$)

Given $u \in [0,1)$, I want $F(\varphi) = -u$ 3 times

We know: the first soln. is φ_0, $\frac{\pi}{6} \le \varphi_0 < \frac{\pi}{5}$ and that is the only soln in that interval.

(And the same happens from any m).

So we know:

the eqn. $t^{m+1} + 1 + u(t^m + t) = 0$ has exactly $m+1$ solns. on S^1, and exactly one of the form $e^{i\varphi_0}$, $\frac{\pi}{m+1} \le \varphi_0 < \frac{\pi}{m}$.

Define T as the complement of $e^{i\varphi_0}$, $e^{-i\varphi_0}$ in the set of roots of the equation.

Define ν_t by solving the system of equations

$$\sum \nu_t t^n = \alpha^n - \lambda \alpha^{-n} \quad , \; n = 1, \dots, m-1$$

(we even have an explicit formula).

We prove: $\nu_t > 0$ all t (computations).

Admissibility means $\sum \nu_t t^n \le \alpha^n - \lambda \alpha^{-n}$ for $n = m, m+1$,

This is a long computation; it shows: OK if $\alpha \geq \sqrt{3}$, i.e. $g \geq 3$.

Also OK if $\alpha = \sqrt{2}$ and $n = m, m+1$ (but not always if $\alpha = \sqrt{2}$, $n = m+2$, $n \geq m+3$, OK again!)

Up to $\lambda =$ [redacted] $\frac{130}{\sqrt{\ }}$, bad N's are
- 51, 52, 53
- 70, 71, ..., 77
- 98, 99, .. 110
- 137, ...

guess, bad if $\frac{\log \lambda}{\log \alpha} \simeq$ integer + 0.4

$N = 50$, $g \geq 65$; $N = 54$, $g \geq 72$

(For bad N's, Oesterlé's result is not optimal.)

Now to give $f = 1 + \sum c_n(X^n + X^{-n})$ which will match.

Take $P(X) = \prod_{t \in T} (x - t)$; write

$$P(x)P(x^{-1}) = \sum_{-(m-1)}^{m-1} a_n X^n \qquad , \; a_n > 0$$

Defn : $f(x) = \frac{1}{a_0} P(x)P(x^{-1})$

$$\therefore \; c_n = \frac{a_n}{a_0}$$

To compute a_n

$$\begin{cases} a_n = (m-n)\cos n\varphi_0 \sin\varphi_0 + \sin(m-n)\varphi_0 \\ a_0 = m\sin\varphi_0 + \sin(m\varphi_0) \end{cases}$$

Finally

(by the formulas!)

$$\frac{1}{2}\sum \gamma_t = g = \sum c_n(\lambda\alpha^{-n} - \alpha^n)$$

and we end up with $g = \dfrac{(\lambda-1)\alpha\cos\varphi_0 + \alpha^2 - \lambda}{\alpha^2 - 2\alpha\cos\varphi_0 + 1}$.

[Recall : the zeta fct of a curve is

$$\frac{\prod_{\alpha=1}^{2g}(1-q^{1/2}e^{i\varphi_\alpha}T)}{(1-T)(1-qT)}$$

ν_t is connected to $\prod(1-q^{1/2}tT)^{\nu_t}$

So number field analog: replace the zeros of ζ by a measure.]

<u>Remark</u> : If λ <u>large</u> w.r.t. α $(=q^{1/2})$

Then $\varphi\approx 0$, so get $g\approx\frac{\lambda\alpha-\lambda}{(\alpha-1)^2}=\frac{\lambda}{\alpha-1}$

So we expect $g\approx\frac{N}{\sqrt{q}-1}$.

A better approx comes from $\varphi\simeq\frac{\pi}{m}$, $m\sim\frac{\log\lambda}{\log\alpha}$.

Then : for large λ,

$$g\geq\frac{\lambda}{\alpha-1}-\frac{\pi^2}{2}\frac{\alpha(\alpha+1)}{(\alpha-1)^3}\frac{\lambda}{(\log\lambda)^2}+O\left(\frac{\lambda}{(\log\lambda)^3}\right)$$

11/21 We look at $q=2$ with varying g

① Upper bounds for N

Use the explicit formula

given $f(\theta) = 1 + \sum c_n 2\cos n\theta$, $c_n \geq 0$, $f(\theta) \geq 0$,

we have
$$g \geq (N-1)\sum c_n q^{-n/2} - \sum c_n q^{n/2}.$$

Start with the example
$$f(\theta) = \frac{1}{c}\sum(1+2x_1\cos\theta + \cdots + 2x_m\cos m\theta)^2$$
$$x_i \geq 0 \quad , \quad c = 1+2x_1^2+\cdots+2x_m^2.$$

1st choice : $x_1 = 1$, $x_2 = 0.7$, $x_3 = 0.2$

gives $N \leq 0.83\,g + 5.35$

$g=1 \to$ not good $N \leq 6$ ($N=5$ is best)

$g=2,3,\dots,11 \Rightarrow$ bound given (except for $g=7$, $N \leq 11$, and $N=10$ is best).

e.g., $g=5 \Rightarrow N \leq 4.15 + 5.35 \leq 9.50 \to N \leq 9$ and we'll construct $N=9$ curves ~~[illegible]~~ later.

$\underline{2^{nd}\text{ choice}}$: $x_1 = 1.05$, $x_2 = 0.8$, $x_3 = 0.4$

$$N \leq 0.766g + 5.97$$

for $g = 13, \dots, 20$ gives same as Oesterlé

$\underline{3^{rd}\text{ choice}}$: $1, 0.8, 0.6, 0.4, 0.1$

$$N \leq 0.6272g + 9.562$$

for $g = 50$, $N \leq 31.36 + 9.562 = 40.9\cdots$

so $\underline{N \leq 40}$.

This justifies all the upper bounds on the table except for $\underline{g=7}$. tables: see pp. Se Th 38b, 38c

$\underline{g=7}$ * bound given by explicit fla is 11

Theorem: A curve with $N = 11$ does not exist.

Proof: Let C be such a curve.

What is its zeta function?

Eigenvalues of Frob are $\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2, \text{—}, \pi_7, \bar{\pi}_7$.

We'll know ζ if we know N over $\mathbb{F}_2, \dots, \mathbb{F}_{2^7}$; if $a_d = \#$ closed pt's of deg d.

Need: $a_1, a_2, \text{—}, a_7$.

Know: $a_1 = 11$

Maximal number of points of a curve of genus g over the field $\mathbb{F}_2$

g	Max. nber
0	3
1	5
2	6
3	7
4	8
5	9
6	10
7	10
8	11
9	12

g	Max. nber
10	12 or 13
11	13 or 14
12	14 or 15
13	14 or 15
14	15 or 16
15	17
16	16, 17 or 18
17	17 or 18
18	18 or 19
19	20

g	Max. nber
20	19, 20 or 21
21	21
...	
39	33
...	
50	40

Bounds for N = Max. Nber

$$N \leq 0.83\, g + 5.35$$

$$N \leq 0.766\, g + 5.97$$

$$N \leq 0.6272\, g + 9.562$$

Se Th 38c

Upper bound for the number of points of a curve of genus g over the field F_2

This upper bound is the one obtained by the " <u>explicit formula</u> " using Oesterlé's trigonometrical polynomial.

g :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
N ≤	5	6	7	8	9	10	11	11	12	13	14	15	15	16	17	18
g :	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
N ≤	18	19	20	21	21	22	23	23	24	25	25	26	27	27	28	29
g :	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
N ≤	29	30	31	31	32	33	33	34	35	35	36	37	37	38	38	39
g :	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
N ≤	40	40	41	42	42	43	43	44	45	45	46	47	47	48	48	49
g :	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
N ≤	50	50	51	51	52	53	53	54	54	55	56	56	57	57	58	59
g :	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
N ≤	59	60	60	61	62	62	63	63	64	65	65	66	66	67	68	68
g :	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
N ≤	69	69	70	70	71	72	72	73	73	74	75	75	76	76	77	77
g :	113	114	115	116	117	118	119	120								
N ≤	78	79	79	80	80	81	82	82								

Let $f = \frac{25}{109}(1+\cos\theta)(1+\frac{6}{5}\cos\theta + \frac{6}{5}\cos 2\theta)^2$

$= 1 + \sum 2c_n \cos n\theta$

$c_1 = \frac{98}{109}, \ldots, c_5 = \frac{9}{218}$

We have

$$\sum_{d=2}^{5} d a_d \sum_{n \equiv 0 (d)} c_n q^{-n/2} \leq g + \sum c_n q^{-n/2} - (N-1)\sum c_n q^{n/2}$$

$$0.743 a_2 + 0.408 a_3 + 0.165 a_4 + 0.036 a_5 \leq 7 + 4.577 - 11.506 \leq 0.069$$

This implies $\boxed{a_2 = a_3 = a_4 = 0, \quad a_5 \leq 1.}$

Have a_6 and a_7 to consider, still:

Let $a_5 = \alpha$, $a_6 = \beta$, $a_7 = \gamma$ (so $\alpha = 0$ or 1).

Have $\pi_1, \text{—}, \pi_7$, $u_i = \pi_i + \bar{\pi}_i$

Define $f(T) = \prod_{i=1}^{7} (T - u_i) \in \mathbb{Z}[T]$.

this has real roots in the interval $[-2\sqrt{2}, 2\sqrt{2}]$.

Writing $f(T)$ in terms of α, β, γ :

$$f(T) = T^7 + 8T^6 + 21T^5 + 14T^4 - 19T^3 + (\alpha - 20)T^2 +$$
$$+ (8\alpha + \beta - 5)T + 31\alpha + 8\beta + \gamma - 106 .$$

Theorem: Such a polynomial $f_{\alpha,\beta,\gamma}$ with $\alpha, \beta, \gamma \in \mathbb{Z}$, $\alpha = 0$ or 1, has all its ~~roots~~ real and in $[-2\sqrt{2}, 2\sqrt{2}]$ if and only if $(\alpha, \beta, \gamma) = (0, 11, 22)$.

[Sturm → condition for $f_{\alpha\beta\gamma}$ to have roots in some interval]

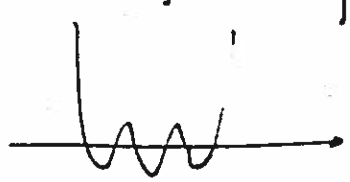
$f_{\alpha\beta\gamma}$ all roots real → derivative also has real roots

So first check that $f'''(T)$ does have four real roots.

Have $\alpha = 0$ or $\alpha = 1$.

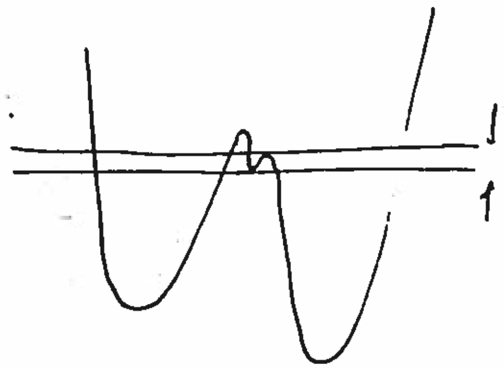
$\alpha = 0$ take $f''(T)$ is OK.

know $f'(T)$ up to translation



to adjust the constant, look at highest min, lowest max

E.g.



constant must make x-axis lie here

This gives : $\begin{cases} \text{if } \alpha = 1, & 5 \le \beta \le 10 \\ \text{if } \alpha = 0 & 9 \le \beta \le 13 \end{cases}$

This gives only eleven cases : look one-by-one at $f(T)$, in the same way.

Find $\alpha = 1$ not feasible.

$\alpha = 0, \beta = 11, \gamma = 22$ works (by a hair). $\boxtimes$

(Conditions are $\gamma \le 22$, $\gamma \ge 22$, $\gamma \le 22$, $\gamma \ge 22$, $\gamma \le 25$, $\gamma \ge 18$, $\gamma \ge -9650$).

We find
$$f = T^7 + 8T^6 + 21T^5 + 14T^4 - 19T^3 - 20T^2 + 6T + 4$$
$$= \underbrace{(T+2)(T^2+2T-2)}_{}\underbrace{(T^2+T-1)(T^2+3T+1)}_{}$$
$$= \quad g(T) \quad . \quad h(T)$$

then g, h generate $\mathbb{Z}[T]$

So if u_1, u_2, u_3 roots of g, u_4, u_5, u_6, u_7 roots of h, then every $u_1 - u_4, \dots, u_1 - u_7, u_2 - u_4, \dots, u_3 - u_7$ is a <u>unit</u>.

$g = 0$ is no fun

$g = 1$ we've seen, $g = 2$ too

Formulas: $g = 1$: $y^2 + y = x^3 + x$

$g = 2$: $y^2 + y = \dfrac{x^2 + x}{x^3 + x + 1}$

$\underline{g = 3}$ if hyperelliptic, at most 6 pts (in general, the hyperelliptic curves have too few pts).

if not, it is a plane quartic in $\mathbb{P}^2$, which itself has 7 points!

So take $[x, y, z]$ homog. coords, find a polyn which passes through all pts:

get $x^3y + y^3z + z^3x + x^2y^2 + y^2z^2 + z^2x^2 + x^2yz + y^2zx = 0$

need to prove: nonsingular (hence $g = 3$) and goes through all pts.

(since $x, y, z \in \mathbb{F}_2 \Rightarrow x^2 = x$, etc., so just

$\cancel{xy} + \cancel{yz} + \cancel{zx} + \cancel{xy} + yz + \cancel{zx} + \cancel{xyz} + xyz = 0$!)

To check it's nonsingular, need only check irreducibility. For that: exists an automorphism of $\mathbb{P}_2$ of order 7 fixing the curve.

This implies irreducibility.

e.g., $u_2 = -1 + \sqrt{3}$ $\quad u_4 = \frac{-1+\sqrt{5}}{2}$

$$u_2 - u_4 = \quad -\frac{1}{2} + \sqrt{3} - \frac{\sqrt{5}}{2}$$

multiply be this w/ $-\sqrt{3}$ $\longrightarrow \left(-\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^2 - 3 = \frac{3\sqrt{5}}{2} - 3$

$$= \frac{-3+\sqrt{5}}{2} \text{ unit.}$$

etc.

So $f = g \cdot h$, g & h generate $\mathbb{Z}[T]$, and this is impossible for a Jacobian, so the curve C does not exist. $\boxed{\text{///}}$

Next unknown case is $g = 10$: analogous method on a computer gave 100 or 200 polynomials...

Construction of Examples

We want to construct curves

g	0	1	2	3	4	5	6	7	8	9	10	...
N	3	5	6	7	8	9	10	10	11	12	12 or 13	

bd = 13

Have curve = 12

Exercise: Prove that minimum no. of points is 3 when $g = 0$, 1 when $g = 1$, 0 when $g \geq 2$.

$g=0$ is no fun

$g=1$ we've seen, $g=2$ too

Formulas: $g=1$: $y^2+y=x^3+x$

$g=2$: $y^2+y=\dfrac{x^2+x}{x^3+x+1}$

$g=3$ if hyperelliptic, at most 6 pts (in general, the hyperelliptic curves have too few pts).

if not, it is a plane quartic in $\mathbb{P}^2$, which itself has 7 points!

So take $[x,y,z]$ homog. coords, find a polyn which passes through all pts:

get $x^3y+y^3z+z^3x+x^2y^2+y^2z^2+z^2x^2+x^2yz+y^2zx=0$

need to prove: nonsingular (hence $g=3$) and goes through all pts.

(since $x,y,z\in\mathbb{F}_2^{\cdot}\Rightarrow x^2=x$, etc., so just

$\cancel{xy}+\cancel{yz}+\cancel{zx}+\cancel{xy}+\cancel{yz}+\cancel{zx}+\cancel{xyz}+\cancel{xyz}=0$!)

To check it's nonsingular, need only check irreducibility. For that: exists an automorphism of $\mathbb{P}_2$ of order 7 fixing the curve.

This implies irreducibility.

This is a <u>twist</u> of the Klein curve

$G = SL_3(\mathbb{F}_2) = GL_3(\mathbb{F}_2)$ order 168

G acts on $\mathbb{P}_2$; to find inv. polynomials

do:

$$Q_4(x,y,z) = \frac{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^8 & y^8 & z^8 \end{vmatrix}}{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^4 & y^4 & z^4 \end{vmatrix}}$$

has degree 4

= product of all the linear forms

this gives the Klein curve

This has no rat'l point.

If we twist it by a $C_7 \subset G$, we get the curve above. $\left(\text{i.e., wrt } \begin{matrix} \mathbb{F}_{2^7} \\ \mid C_7 \\ \mathbb{F}_2 \end{matrix}\right)$

For $g=4$: if not hyperelliptic, can. embedding in $\mathbb{P}_3$
then curve = inters. of surfaces

curve = (quadric surface) $\cap$ (cubic surface)

transversal inters, but surfaces can have singularities.

if quadric = $\mathbb{P}_1 \times \mathbb{P}_1$, 9 pts — so not obvious at once we can get 8.

In $\mathbb{P}_1 \times \mathbb{P}_1$, the curve we want has affine eqn:

$$x^2y^3 + x^3y^2 + xy^3 + x^3y + x^2y^2 + x^2 + y^2 + 1 = 0.$$

After $g = 4$, explicit construction is not practical. Use CFT instead.

Start from C_1, known.

Try to find

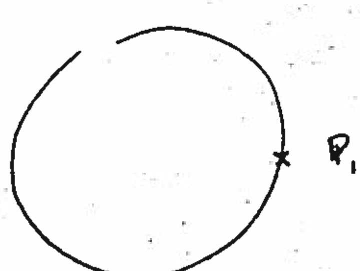
$$\begin{array}{c} C_2 \\ \big\downarrow \text{ abelian extn.} \\ C_1 \end{array}$$

With "little" ramification ($g(C_2)$ small)

and s.t. "many" rational points split.

<u>1st case</u>: $C_1 = \mathbb{P}_1$, $g = 0$

Choose $Q \in \mathbb{P}_1$ with $\deg Q = 3$, so res. field $= \mathbb{F}_8$.



$\mathbb{F}_8^\times$ = cyclic order 7.

Take $m = Q$, look at Cl_m.

$$0 \longrightarrow \mathbb{F}_8^\times \longrightarrow Cl_m \xrightarrow[\deg]{} \mathbb{Z} \longrightarrow 0$$

CFT: finite quotients of Cl_m describe the ab.

Choose a rat'l point $R \in \mathbb{P}_1(\mathbb{F}_2)$.

$R \longmapsto Cl_m$, $\deg R = 1$

So let G = quotient of Cl_m by $\langle R \rangle \cong \mathbb{F}_8^\times$.

So corresp to

$$\begin{array}{c} C \\ \Big\downarrow {\scriptstyle 7} \\ \mathbb{P}_1 \end{array}$$

Frob R is killed $\Rightarrow$ R splits completely giving 7 pts.
(and $\Rightarrow$ no const. field extn.)

$$2g(C) - 2 = 7(-2) + \underbrace{6 \cdot 3}_{\text{sum of Artin conductors}}$$

$$2g = 2 - 14 + 18 = 6$$

So $\boxed{g = 3 \,,\, N = 7}$

Now play the same game as follows:

take R_1, R_2 rat'l points on $\mathbb{P}_1$

$m = 4.R_2$, construct G as before, $G = Cl_m / \langle R_1 \rangle$

$\cong$ local group mod 4.

Se Th 43

get: $G \cong$ local gp mod $4R_2$

$$= \{1+\alpha_1 t + \cdots + \alpha_3 t^3\} \big/ {1+t^4}$$

$$\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

So find
$$\begin{tikzcd} C \arrow[d, "G"] \\ \mathbb{P}_1 \end{tikzcd}$$
s.t. : $\left\{ \begin{array}{l} R_1 \text{ splits completely into 8 pts (rat'l)} \\ R_2 \text{ is completely ramified} \to \\ \to 1 \text{ pt which is rat'l.} \end{array} \right.$

$$2g - 2 = 8(-2) + \sum f_\chi$$

Characters on G

$\chi = 1$: $f = 0$

χ trivial on t^3 : $f = 2$

χ trivial on t^2 : $f = 3$ twice

——— : $f = 4$ four times

So $2g - 2 = -16 + 2 + 6 + 16 = 8 \implies \boxed{g = 5}$.

So this gives the curve we need for $g = 5$.

11/26 ($q=2$, cont.) See table, pp. SeTh 43b, 43c

Construction

Start from sth you know, say $g=0$, 3 pts, C_0

$$\begin{array}{c} C \\ \Big\downarrow \text{abelian} \\ C_0 \end{array}$$

give: conductor, group G, n pts in C_0 splitting completely.

$g=50$ $N=40$? $40=8\times 5$

So want C_0 w/ $g_0=1$, ell curve $y^2+y=x^3+x$ w/ 5 rat'l pts.

Want a covering of degree 8 in which all five pts split completely.

G = of type $(2,2,2) = (2)\times(2)\times(2)$.

First make a $(2,\ldots,2)$ extension of rank 8; then $P_1,\ldots,P_5$ give Frob. elements.

$(2,\ldots,2) = \mathbb{F}_2^8$ has a quotient of dim 3 ($(2,2,2)$) in which $P_1, \ldots, P_5 \to 0$ $\Longrightarrow$ pts split completely.

Choose a pt P_7, of degree 7 ($=8-1$)

(# pts over $\mathbb{F}_{2^7}$ is $\geq 2^7+1-2\cdot 2^{7/2} > 129-32 > 5$)

Choose conductor $\underline{m} = 2P_7$

Se Th 43b

TABLE

of curves of low genus over F_2 having many points

Each curve C is obtained as an abelian covering $C \to C_o$ of a curve C_o of lower genus, occuring earlier in the table (or of genus 0).

The table gives :

the genus g of C;

the number N of rational points of C (I underline N if it is maximal for the corresponding genus);

the genus g_o of C_o;

the conductor $\underline{m}$ of $C \to C_o$ (I write $\underline{m}$ as $aP_1 + a'P_1' + bP_2 +$ ... where P_1, P_1', P_2 ... are distinct closed points of C_o of degrees 1,1,2,...);

the Galois group G of the covering $C \to C_o$ (a cyclic group of order m is denoted by (m));

the number n of rational points of C_o which split completely

the number r of rational points of C_o which are totally rami

in C.

For all the cases considered in the table, we have $N = r + |G|n$.

---

g	N	g_o	$\underline{m}$	G	n	r
1	**5**	0	$4P_1$	(2)	2	1
2	**6**	0	$2P_3$	(2)	3	0
3	**7**	0	P_3	(7)	1	0
4	**8**	1	$2P_1 + 4P_1'$	(2)	3	2
5	**9**	0	$4P_1$	(2)×(4)	1	1
6	**10**	1	$2P_5$	(2)	5	0
7	**10**	1	$2P_6$	(2)	5	0
8	**11**	2	$2P_1 + 2P_4$	(2)	5	1
9	**12**	2	$2P_6$	(2)	6	0

Se Th 43c

Table (continued)

g	N	g_o	$\underline{m}$	G	n	r
10	12	2	$2P_7$	(2)	6	0
11	13	3	$12P_1$	(2)	6	1
12	14	0	$P_3 + P'_3$	(7)	2	0
13	14	3	$2P_3 + 2P_5$	(2)	7	0
14	15	0	P_4	(3)×(5)	1	0
15	$\underline{17}$	1	$10P_1$	(2)×(2)	4	1
16	16	4	$2P_9$	(2)	8	0
17	17	0	$5P_1$	(2)×(8)	1	1
18	18	5	$2P_9$	(2)	9	0
19	$\underline{20}$	1	$2P_6$	(2)×(2)	5	0
20	19	2	0	(19)	1	0
21	$\underline{21}$	0	$P_2 + P_3$	(3)×(7)	1	0
39	$\underline{33}$	1	$12P_1$	(2)×(2)×(2)	4	1
50	$\underline{40}$	1	$2P_7$	(2)×(2)×(2)	5	0

Harvard, November 1985

J.-P. [illegible]

look at $Cl_{\underline{m}}$:

$$0 \longrightarrow L_{\underline{m}} \longrightarrow Cl_{\underline{m}} \longrightarrow Cl_0 = \mathbb{Z}/(5) \times \mathbb{Z} \longrightarrow 0$$

$$L_{\underline{m}} = \mathbb{F}_{2^7}[[x]]^\times \Big/ \{1 + (x^2)\} = \mathbb{F}_{2^7}^{*} \times \mathbb{F}_{2^7}$$

$$Cl_{\underline{m}} \big/ 2\,Cl_{\underline{m}} = \mathbb{F}_{2^7} \times \mathbb{Z}/2$$ of type $(2, \ldots, 2)$, rank 8.

$$\begin{tikzcd} & \tilde{C} \arrow[dl] \arrow[dd] \\ C \arrow[dr, "(2,2,2)"'] & \\ & C_0 \end{tikzcd}$$

: max'l $(2,2,\ldots,2)$ extension w/ cond $\leq 2P_7$.

(this includes a const. field extn.)

where the 5 pts split. (I.e., choose a quotient of type $(2,2,2)$ such that pts split)

$$2g - 2 = 2^3(2g_0 - 2) + \sum_{\chi \neq 1} \deg f_\chi$$

χ = char of order 2 so cond $= 2P_7$ or 0 but can't be zero so $f_\chi = 14$.

$$2g - 2 = 8 \times 0 + (8-1) \times 14$$

$$g = 1 + 7 \times 7 = 50.$$

With $2P_6$, would get $\overbrace{}^{\text{extn } (2,2) \text{ w/}}$ $4 \cdot 5 = 20$ r pts and

$$2g - 2 = 0 + (4-1) \times 12$$

so $\boxed{g = 19}$.

With $2P_5$, get extn. of deg 2, w/

$$2g - 2 = 0 + 10 \longrightarrow \boxed{g = 6,\ N = 10}$$

$\boxed{g = 13}$ $\quad N = 14$, $g_0 = 3$, $|G| = 2$
w/ 7 pts

$$2g - 2 = 2(6-2) + \deg f$$

$$24 = 8 + \deg f$$

So $\deg f = 16$. Must take $\underline{m} = 2P_8$ (contra table!)

$\underline{\text{table}}$: $\underline{m}$: $2P_3 + 2P_5$ must check there is a pt of deg 3 (and one of deg 5)

take $L_{\underline{m}}$, $\mathbb{Z}$

so $rk = 1 + \deg \underline{m}$
$= 9$

so mod out as before.

• Recall construction:

$$\begin{array}{c} C_3 \\ 7 \downarrow \\ C_0 \cong P_1 \end{array}$$

res field $= \mathbb{F}_8$ ramif at a $P_3 \in C_0$

so C_3 has a pt of deg 3

$g = \underline{20 \quad N = 19}$, $g_0 = 2$, $h = 19$

$Cl_0 = \mathbb{Z} \times \mathbb{Z}/(19)$

P_1

Split so that $P_1 \to$ generator. Get an extn. by the quotient.

Then $2g - 2 = 19(22-2) \longrightarrow g = 1 + 19 = 20$.

For very large g (say $g \sim 10^{10}$) we only get N of about the same order (say $0.2 \cdot 10^{10}$) using the class field towers, as before.

For $10 \leq g \leq 20$, one might be able to fill some of the gaps.