

COURS DE JEAN-PIERRE SERRE

JEAN-PIERRE SERRE

FERNANDO Q. GOUVÊA (réd.)

Rational Points on Curves over Finite Fields

Cours de Jean-Pierre Serre, tome 6 (1985)

http://www.numdam.org/item?id=CJPS_1985__6_

© Bibliothèque de l'IHP, 2015, tous droits réservés.

L'accès aux archives de la collection « Cours de Jean-Pierre Serre » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Notes numérisées par l'IHP et diffusées par le programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

F

31 MAI 1999

Rational Points on Curves
over Finite Fields

Part I "q large"

N° Cote :	78 923 928
Institut Henri Poincaré BIBLIOTHÈQUE	
11, rue P.-et-M.-Curie 75231 PARIS CEDEX 05	
N° Inventaire :	028327

Harvard, 1985

Curves over Finite Fields

Jean-Pierre Serre

RATIONAL POINTS ON CURVES

OVER FINITE FIELDS

PART I: "q LARGE"

Jean-Pierre Serre

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

(b) Asymptotic result - due to Drinfeld-Vladimir:

for fixed q (and $x \rightarrow \infty$) $\limsup N_q(x)/x \leq \sqrt{q} + 1$,

with equality when q is a square (Mazur-Zink).

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

(d) Numerical results:

$x \backslash q$	2	3	4	5	7	8	9	11	13	16	17	19	23	25
1	3	7	9	10	13	14	16	18	21	25	26	28	31	34
2	6	8	10	12	16	18	20	24	27	32	34	38	41	44
3	7	10	12	14	18	20	22	26	29	36	38	42	46	49
4	8	12	14	16	20	22	24	28	31	40	42	46	50	54
5	9	13	15	17	21	23	25	30	33	42	44	48	52	56
6	10	14	16	18	22	24	26	32	35	44	46	50	54	58
7	11	15	17	19	23	25	27	34	37	46	48	52	56	60

Table of
values
of $N_q(x)$

Lectures given at Harvard
University, September to
December 1985.

Notes by Fernando Q. Gouvêa

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

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

For a given pair (q, g) , let $N_q(g) = \sup_C N(C)$. Weil's inequality implies :

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

I shall discuss several improvements of this bound. Namely :

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

(b) (Asymptotic result - due to Drinfeld-Vladuť) :

for fixed q (and $g \rightarrow \infty$) $\limsup. N_q(g)/g \leq \sqrt{q} - 1,$

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 $N_q(g)$

$g \backslash q$	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										66
5	9													
6	10													
7	10									65				

Contents - Part I

Introduction

Se 1

Weil bound
Connections to codes

Se 1
Se 1a

General Results

Se 3a

Refined Weil bound
Refinements using traces of algebraic integers
Smyth's proof of Siegel's Theorem
Indecomposability of jacobians and applications
Beauville's Theorem

Se 3a
Se 6
Se 10
Se 11
Se 13

The case $g=1$ (review)

Se 15a

The case $g=2$

Se 19

Results of Tate and Honda and applications
"Glueing" elliptic curves
Statement of Theorem
Remarks on "special" q
The elementary glueing
Proof for q a square
Intermezzo on polarizations
Conclusion of proof for q a square
Proof for q not a square, not special
Proof for q not a square, special
"Glueing" and Hermitian modules
Proof using hermitian modules
The Skolem method for diophantine equations

Se 19
Se 22
Se 24a
Se 25
Se 26a
Se 30a
Se 32a
Se 35a
Se 39
Se 42
Se 49a
Se 53a
Se 61

The case $g=3$

Se 64 a

Voloch's bound

Se 64 a

Constructing curves: some examples

Se 66

Conjectures

Se 71

One knows:

Well bound:

$$|N(x) - (g+1)| \leq 2g\sqrt{g}$$

if one wants $|N(x) - (g+1)| \leq 2g\sqrt{g}$ as a function of g , then one is optimal.

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

What: upper bound, no curves with "many" pts.

Def: $N(g) = \sup_x N(x)$ (given g).

So that is:
$$N(g) \leq 1 + g + 2g\sqrt{g}$$

Curves over $\mathbb{F}_q$

$$q = p^e, \quad p \text{ prime}, \quad e \geq 1$$

$X = \text{curve}$ (smooth, complete, abs. irreducible).

genus of $X = g$ is well-defined

$$\begin{aligned} N(X) &= \text{nbr of pts of } X \text{ rat'l / } \mathbb{F}_q \\ &= \# X(\mathbb{F}_q) \end{aligned}$$

One knows:

Weil bound:

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

If one wants $|\# X(\mathbb{F}_{q^n}) - (q^n+1)| \leq 2gq^{n/2}$

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: $N_g(q) = \sup_{X \text{ genus } g} N(X)$ (given g, q).

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

E.g., $g=2, q=50$; then Weil is $N \leq 1+2+100\sqrt{2} = 144 \dots$
 so $N \leq 144$ (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	] Tuesday Ab. Varichies
	$g=2$ known	
	$g=3$ known only for $q < 23$	

g large, q small
(Thursday)

(see Part II)

[asymptotic results]

analogy:

curves w/ many pts

rel. to

coding theory

$\longleftrightarrow$

fields w/
small
discriminant
rel. to
geom. of #s

$\longleftrightarrow$

Y. Ihara : some modular curves have lots of pts,
over $\mathbb{F}_p$.

Coding theory : Goppa : curves w/ many pts
 $\uparrow$ 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 $(x_1, \dots, x_n) \in \mathbb{F}_q^n$ 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 $001001111 \in V$

might be sent as 011001110

$\rightarrow H-d=2$

$\uparrow$ two errors.

So we want an error-correcting code.

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

Suppose $H-d \geq 5$ (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 :

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

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 $x = (x_1, \dots, x_n) \in V$ with $x_i \neq 0$.

Then consider the fct.

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

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

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

$$n = \# \text{ of fts}$$

What is $H-d$? Let $m = \max. \# \text{ of } P_i \text{ lying on}$
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.

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

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

And map

$$\begin{array}{ccc} V & \xrightarrow{\quad} & \mathbb{F}_q^n \\ & \searrow & \parallel \\ & & L_{P_1} \otimes \dots \otimes L_{P_n} \\ & \nearrow & \\ & & (s(P_1), \dots, s(P_n)) \end{array}$$

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

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

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

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

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

Pf: Weil comes from:

$N = \text{nb of fixed pts of } \text{Frob} = \pi : X \rightarrow X$
 $(x_0, -, x_d) = (x_0^p, -, x_d^p)$.

So shd have $N = \text{Trace } \pi \text{ on } H^0(X) \rightsquigarrow 1$

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

$+ \text{Trace } \pi \text{ on } H^2(X) \rightsquigarrow g$

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

Then he proved $\left\{ \begin{array}{l} |\pi_i| = g^{1/2} \quad (\text{R.H. for } X) \\ \pi_i \text{ is an alg. integer} \end{array} \right.$

family of π_i (mult. included) is stable under $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, 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
$$\# X(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{i=1}^{2g} \pi_i^n$$

And then this determines the π_i .

We know $\pi_i \bar{\pi}_i = q$ 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:

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

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

(Note: it's clear for all the ? Not for the other cases.)

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

② Can assume the ab. variety is simple over $\mathbb{F}_q$.

Suppose q_0 is eigenv. with mult ≥ 1 .

Then the endom. $\pi - q_0$ has a kernel and

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

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

③ Symplectic proof

Take $V(A) = \text{dual of } H'$ (vect. sp. / $\mathbb{Q}_\ell$).

$\star$ $\exists$ non-deg alt. form B on H' (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 $\lambda_i, \lambda_i', -1, \lambda_j, \lambda_j'$ s.t. $\lambda_i \lambda_i' = q$.

□

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

Example 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 corresponds to lines of the two rulings of the quadric)

- split quadric ($x_1 x_2 + x_3 x_4 = 0$), lines are def / $\mathbb{H}_g$ say e_1, e_2 .
Then $\pi^* e_1 = f e_1$, $\pi^* e_2 = g e_2$, and the claim holds.
- non-split quadric: then $\pi^* e_1 = g e_2$, $\pi^* e_2 = f e_1$,
eigenvectors are $e_1 + e_2, e_1 - e_2$ w/ eigenval $f, -g$
so claim is false.

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

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

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

And $|a_i| \leq 2\sqrt{g}$.

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

For an ab. variety dim g , want: $|T_i(\pi)| \leq g [2g^{1/2}]$
 $| \sum_{i=1}^g a_i |$

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

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

The x_i are } stable under Galois w/ multiplicities.
 } all integers (since π_i are).

$\therefore x_1, \dots, x_g \in \mathbb{Z}$ and is positive.

Then $x_i > 0$, so:

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

so

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

so

$$\sum a_i \geq -mg \quad \text{with equality only if } a_1 = \dots = a_g.$$

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

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

$$\left. \begin{array}{l} -gm \leq \text{Tr}(\sigma) \leq gm \\ \text{and } \left\{ \begin{array}{l} \text{if } \text{Tr}(\sigma) = gm, \text{ then } a_1 = \dots = a_g = m \\ \text{if } \text{Tr}(\sigma) = -gm, \text{ then } a_1 = \dots = a_g = -m. \end{array} \right. \end{array} \right\} \text{Then!}$$

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

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

Thm 2: (1) If $T_2(\pi) = qu - 1$ ("down by 1"), then

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

(2) If $T_2(\pi) = qu - 2$ ("down by 2"), then one of the ~~few~~ following forms occurs:

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

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

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

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

— 2 : $\begin{cases} m, -, m, m-2 \\ m, -, m, m-1, m-1 \\ m, -, m, m+\sqrt{2}-1, m-\sqrt{2}-1 \\ " , m+\sqrt{3}-1, m-\sqrt{3}-1 \\ " , m-1, m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2} \\ " , m+\frac{-1+\sqrt{5}}{2}, m+\frac{-1-\sqrt{5}}{2} \\ m, -, m, m+1-4\cos^2\frac{\pi}{7}, \dots \end{cases}$ $g \geq 1$ $g \geq 2$ $g \geq 2$ $g \geq 2$ $g \geq 3$ $g \geq 4$ $g \geq 3$

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

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

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

$T_r(\pi) = \sum_{\alpha=1}^g (\pi_\alpha + \bar{\pi}_\alpha)$, $m = \lfloor 2\sqrt{q} \rfloor$.

Recall: $T_r(\pi) \leq gm$ [for ab. var., can twist to $\pi \rightarrow -\pi$ so need not study the other ineq. $-gm \leq T_r(\pi)$]

iff $T_r(\pi) = gm$, $(x_1, \dots, x_g) = (m, \dots, m)$ ("defect 0")

"Defect 1" $T_r(\pi) = gm - 1$
 "Defect 2" $T_r(\pi) = gm - 2$ $\rangle$ possibilities for $(x_1, \dots, x_g)$ are as above.

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

Thm (Siegel, M.A. vol III, first paper) If α is as above and $\alpha \neq 1, \frac{3 \pm \sqrt{5}}{2}$, then $T_1(\alpha) > \frac{3}{2} d(\alpha)$.

(If $\alpha = 1$, $T_1(\alpha) = d(\alpha)$, $\alpha = \frac{3 \pm \sqrt{5}}{2}$, $T_1(\alpha) = 3 = \frac{3}{2} d(\alpha)$.)

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

Assume Siegel's thm: Separate out exceptional cases.

If k is a given integer ≥ 0 , the number of tot > 0 α 's with $T_1(\alpha) = d(\alpha) + k$ is finite for each k , and these α 's can be found effectively.

If: By Siegel, $d(\alpha) + k > \frac{3}{2} d(\alpha)$

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

But α satisfies

$$x^d - (d+k)x^{d-1} + \dots$$

Conjugates $\alpha_1, \dots, \alpha_d$ are all positive, and all $< d(\alpha) + k$.

Hence coeffs are effectively bounded, and we can list the possible α 's. $\square$

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 ¹⁶ $d(\alpha) < 2$.

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

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

$$d(\alpha) = 2 \quad \rightsquigarrow \quad \alpha \text{ satisfies } x^2 - 4x + q = 0$$

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

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

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

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

$$x^2 - 4x + 3 = 0$$

" not deg 2
(x-1)(x-3)

$$d(\alpha) = 3 \quad \longrightarrow \quad p(x) = x^3 - 5x^2 + px - q = 0$$

three real positive roots

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

has 2 real roots

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

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

Want max positive, min negative, etc., Get $g < q < f$.

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

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

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

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: $\exists \infty$ many α with $T_1(\alpha) < 2 \deg(\alpha)$

Smyth: $\exists$ only finitely many α with $T_2(\alpha) < 1.7719 \deg(\alpha)$.

Open question: what is the correct constant.

Consider map $\alpha \mapsto \frac{T_1(\alpha)}{\deg \alpha}$. Question is equiv. to : what is first accum. pt. of $\text{Inv}(\alpha)$?

Can look for polynomials (not nec. irred.) $X^d - a_1 X^{d-1} + \dots$,
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 $P = Q_1 \dots Q_k$ 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 $k=1$: $P = Q_1 = Q_2$

one Q_i with defect 1, others defect 0.

$$\text{So } (x-1) \dots (x-1) \cdot (x-2)$$

$$\text{or } (x-1) \dots (x-1) \cdot (x^2 - 3x + 1)$$

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

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

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

Set $x = [x] + \{x\}$
 int part 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 $m + \frac{-1+\sqrt{5}}{2} \leq 2\sqrt{q}$ by Weil

$$\text{so } \{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2} \quad 19$$

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

defect 0 —

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

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

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

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

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

$$1+2+6=9, \text{ so down by } 2,$$

and is of the last kind. $\square$

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

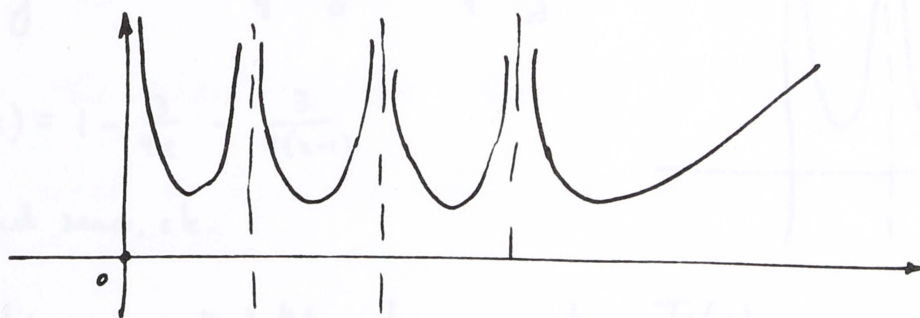
Smyth's proof of Siegel's thm :

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

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

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

Proof : let $d = \deg(\alpha)$, $\alpha_1, \dots, \alpha_d$ the conjugates, $\alpha_i > 0$.

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

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

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

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

$$\geq \frac{1}{d} \sum_{i=1}^d g(\alpha_i) \geq \min g$$



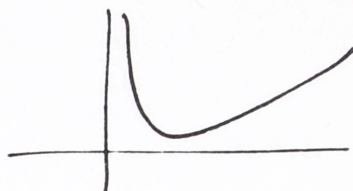
and conclude that all α are units

Examples: • $g(x) = x - \log|x|$

$$\min(g) = 1$$

so get $\text{Tr}(\alpha) \geq \deg(\alpha)$

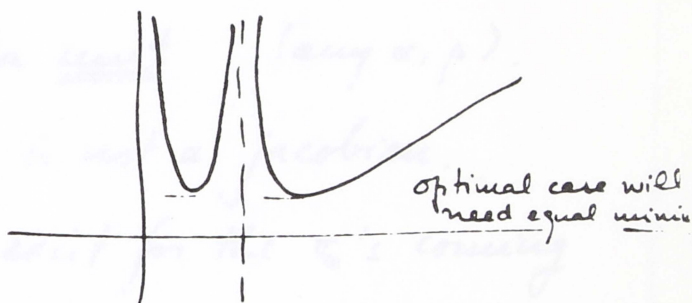
And get equality only for $\alpha = 1$.



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

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

find zero, etc.



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

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

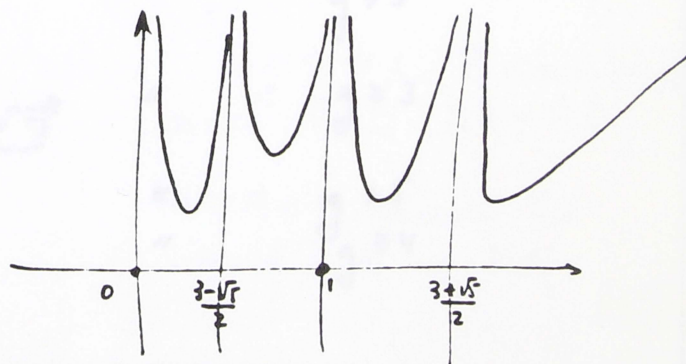
Taking $a = 0.574$
 $b = 0.879$
 $c = 0.374$

one gets $\min g > 1.591$,

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

$$\alpha \neq 1, \alpha \neq \frac{3 \pm \sqrt{5}}{2}$$

This improves Siegel.



• Smyth gets 1.7719

$$x_\alpha = \pi_\alpha + \bar{\pi}_\alpha \quad \alpha = 1, \dots, g$$

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

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

b) $x_\alpha - x_\beta$ $\alpha \in I, \beta \in J$ is a unit (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.: $m, m, \dots, m, m-1$ is impossible for curves if $g \geq 2$
second defect 1 case sup. " " " $g \geq 3$

defect 2 {
 $\longrightarrow$?
 $\longrightarrow$ imp for curves if $g \geq 3$
 $\longrightarrow$ " $g \geq 3$
 $\longrightarrow$?
 $\longrightarrow$ " $g \geq 3$
 $\underbrace{m, \dots, m, m-1, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}}_{\text{second defect 1 case sup.}} \quad \text{"} \quad g \geq 3$
 $\longrightarrow$ " $g \geq 5$
 $\longrightarrow$ " $g \geq 4$

$\therefore$ For curves, many of the condns on g are equalities.

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:

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

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

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

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

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

(c. 1970, Waterhouse)

$$x_a = \pi_a + \frac{q}{\pi_a}$$

$F+V$ is so on the $V_2(A)$.

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

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

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

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

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

If $P = P_1 \cdot P_2$, P_1, P_2 strongly rel. prime, so $1 = Q_1 P_1 + Q_2 P_2$,
get

$$\mathbb{Z}[x]/P \xrightarrow{\quad} \text{End } A$$

$$\mathbb{Z}[x]/P_1 \times \mathbb{Z}[x]/P_2$$

$$\varepsilon_1 = Q_1 P_1$$

$$\varepsilon_2 = Q_2 P_2$$

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 $A \cong A_1 \times A_2$, ²⁵ 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 $\text{Hom}_{\mathbb{F}_1}(A_1, A_2) = 0$ (Since $\text{Hom}_{\mathbb{F}_1}(\) \neq 0$ iff there is a common root of $F+V$.)

Polarization on ab. variety is a hom $A \longrightarrow \hat{A}$
" " " "
 $A_1 \times A_2 \longrightarrow \hat{A}_1 \times \hat{A}_2$

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. □

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 $m = [2g^{1/2}] = 2x$ 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 $g=2,3$, 3 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 $\#\{p \leq P : p = x^2 + 1\} \sim c \frac{P}{(\log P)^2}$ 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, Ljunggren

Both cases: p -adic method of Skolem.

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

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

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

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

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

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

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

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

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

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

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

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

Polarizations $Jac(X) \xrightarrow{\sim} Jac(X)^*(\text{dual})$ Se 14
 or equiv. classes of ample divisors

Recall:

Parenthesis on Torelli's theorem

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

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

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

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

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

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

Finite 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_k .

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

skew $\leftrightarrow E: V_\ell \times V_\ell \longrightarrow V_\ell(\mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$ non-deg. alternating form.

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

(using $V: FV = \varphi$, get $E(Fx, y) = E(x, Vy)$)
 $\rightarrow$ is adjoint of F w.r.t. E in V .

in our case F is like $x+i$, so V is like $x-i \implies$

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

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

For our σ , get $E(\sigma x, y) = E(x, \bar{\sigma} y) = E(x, \sigma' y)$
 $\therefore E(\sigma x, \sigma y) = E(x, y)$.

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

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

(if $\varphi = x^2 + x + 1$ get either σ or $-\sigma$ ^{order 3} _{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
 $\sigma^* \omega_i = \lambda \omega_i$, λ indep. of i fixed.

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

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

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

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

for $g \geq 2$, $\left\{ \begin{array}{l} \text{if } X \text{ is not hyperelliptic, } \text{can} \text{ is an embedding} \\ \text{if } X \text{ is hyperelliptic, image has genus zero \& can has degree 2} \end{array} \right.$

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

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

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

Review of $q=1$:

Elliptic Curves

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

$$|a| \leq 2q^{1/2}. \quad q = p^e \quad e \geq 1, p \text{ prime}$$

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

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

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

Theorem

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

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

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

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

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

$$q = p^e, e \text{ odd} \left\{ \begin{array}{l} a = 0 \\ a = \pm p^{\frac{e+1}{2}} \end{array} \right. \quad p = 2 \text{ or } 3$$

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

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

$$\pi^2 - a\pi + q = 0 \Rightarrow \pi \text{ generates a ring } R \subset \text{imag. q. field.}$$

can prove $\Rightarrow \exists \text{ curve}/\mathbb{Q}$ with $\text{End} \cong R$.

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 $\text{End} \subset \text{imag. quad. field.}$

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. $\square$

(ii) supersingular curves

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

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

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 $\sum_{E \text{ s.s.}} \frac{1}{\# \text{Aut}(E)} = \frac{p-1}{24}$ $\rightarrow$ 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's)

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

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

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

(then $\mathbb{Q}(\sqrt{1}) \subset \mathbb{H}_{p,\infty}$, say, then p cannot be split).

etc.

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

then $x^2 - \lambda x + p = 0$ and λ is div. by p (since $\lambda = x + \bar{x}$ look at values)

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. $\square$

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

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 allowed

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

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

df $e = 3$, have $4p^3 = m^2 + \epsilon$ $1 \leq \epsilon \leq 2m < 2^{3/2} p^{3/2}$

Now suppose $m = p\mu$: $4p^3 = p^2\mu^2 + \epsilon \Rightarrow p^2 \mid \epsilon$

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

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

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

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

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

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

$$\sqrt{2} = 1.0110101000001\dots \text{ in binary}$$

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

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

↑
even!

Therefore 2^7 is exceptional, because $\sqrt{2} = 1.0110101000001\dots$

↑ ↑ ↑ ↑
 2^7 2^{11} 2^{15} 2^{17}

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

$$2\sqrt{3} = 3.110112022\dots \quad (3\text{-adic})$$

↑ 3^7 exceptional

$$2\sqrt{7} = 5.20166\dots \quad (7\text{-adic})$$

↑ 7^5 exceptional

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

10/15

last time: $g=1$

Then $N_q(1) = \text{max nber of points of a curve of genus 1 over } \mathbb{F}_q$

Get: $N_q(1) = 1 + q + m$, $m = [2\sqrt{q}]$,
 except, where $q = p^e$, 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 $g=1$

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

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 $g=3$:

$$|\text{ref. Weil} - N_7(3)| \leq ?$$

Conjecture: For $g=3, 4, 5$ and not many more,
 $|\text{ref. Weil} - N_7(g)| \leq C(g),$

$C(g)$ depending only on g .

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

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

$\begin{matrix} k' \\ 2 \mid \\ k \end{matrix}$ quad. twist; $\begin{matrix} \mathbb{F}_q^2 \\ \mid \\ \mathbb{F}_q \end{matrix}$ 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 $N(C) \text{ max} \Rightarrow N(C_{\text{twisted}}) \text{ minimum (etc.)}$.

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

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

$\text{char} = 2$ C is $y^2 + y = \varphi(x)$

C_{twist} is $y^2 + y = \varphi(x) + a$, $a \in \mathbb{F}_q$, a not of the form $b^2 + b$.
 i.e., $\text{Tr}(a) = 1$

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

Results of Tate and Honda

(Tate, Inventiones 2 (1966), 134-144

Tate, Sem. Bourb., exp 352

Milne & Waterhouse, Symp Pure Math AMS, —)

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

one-one corresp:

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

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

A s.t. eigenvalues of Frob are $\pi_1, \dots, \pi_d$ repeated a certain number of times

$$\longleftarrow \pi_1, \dots, \pi_d, \quad d = \deg \pi$$

Tate's theorem

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

Then we know:

(1) Λ is a division algebra.

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

The local invariant of Λ as element of $\text{Br}(\mathbb{Q}(\pi))$ 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 , $i_v = \frac{v(\pi)}{v(q)} [\mathbb{Q}(\pi)_v : \mathbb{Q}_p]$.

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

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 $r = 2d_\pi / \text{no. of conj's}$)

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

$$\text{So } \mathbb{Q}(\pi) = \mathbb{Q}$$

$$\text{so } \begin{cases} i_\infty = \frac{1}{2} \\ i_p = 0 \\ i_f = \frac{1}{2} [\mathbb{Q} : \mathbb{Q}] = \frac{1}{2} \end{cases}$$

So $1 = H_{p,\infty}$ just alg. ramified at p, ∞ .

So $r=2$, $\dim A = \frac{2}{2} [\mathbb{Q}:\mathbb{Q}] = 1$, so A is ell. curve.

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

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

one p -adic place $i_p = 0 \pmod{\mathbb{Z}}$.

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

So get just field in $\mathbb{Q}(\sqrt{p})$ ramif. at ∞ , $= 1 +_{p,\infty} \otimes \mathbb{Q}(\sqrt{p})$.

$r=2$, $[\mathbb{Q}(\sqrt{p})/\mathbb{Q}] = 2$ 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: $\pi \bar{\pi} = p, \pi + \bar{\pi} = a \pmod{p}$

(over $\mathbb{F}_p$)

$$[\mathbb{Q}(\pi):\mathbb{Q}] = 2, \quad p \text{ splits}$$

(look at
Newton polygon)

$$v_1, v_2 \text{ div } p \text{ so } v_1(\pi) = 0, v_2(\pi) = 1$$

$$\text{So } i_{v_1} = 0, i_{v_2} = 1 \cdot 1 = 0 \in \mathbb{Q}/\mathbb{Z}.$$

$\rightarrow$ no real places.

So $1 = \mathbb{Q}(\pi)$.

Recall: 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 $p \nmid m$.

iff $\pi = \frac{m + \sqrt{m^2 - 4q}}{2}$, 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 $\pi_1, \bar{\pi}_1, \dots, \pi_g, \bar{\pi}_g$

$$\text{with } \begin{cases} \pi_1 + \bar{\pi}_1 = -m \\ \pi_g + \bar{\pi}_g = -m \end{cases}$$

$\Rightarrow (\pi_i, \bar{\pi}_i)$ repeated g times.

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

$\therefore g \geq 5$. $\square$

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

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

$$\text{In fact } 4q = m^2 + k \quad 1 \leq k \leq 2m$$

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

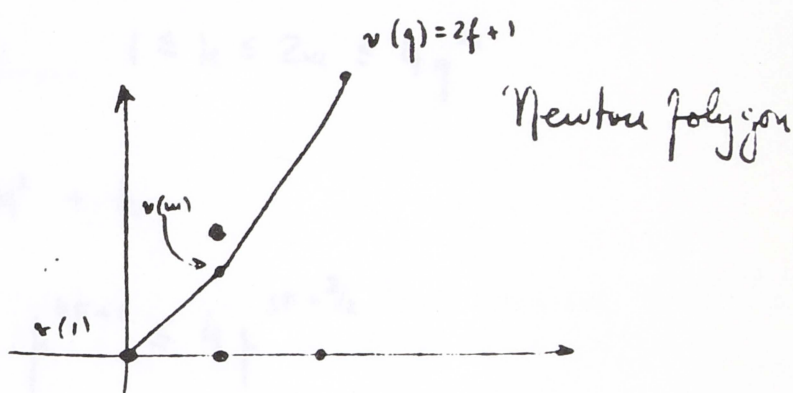
$$\text{But } 2m \leq 4q^{1/2}, \text{ so } p^{2f+1} \leq k \leq 2m \leq 4p^{f+1/2}$$

$$\text{So } p^{f+\frac{1}{2}} \leq 4 \Rightarrow p^{5/2} \leq 4 \Rightarrow p^5 \leq 16 \quad \swarrow \searrow$$

($f \geq 2$)

Hence $v_p(m) \leq f$.

π satisfies $\pi^2 - m\pi + q = 0$



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

Hence p splits in $\mathbb{Q}(\pi)$ and the val of π at v_1, v_2 dividing p are the slopes: $v(m)$, $2f+1 - v(m)$.

is of Tate's theorem

At $\{ \infty \} \rightarrow 0$

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

Know: $0 < \alpha < \frac{1}{2}$

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

Denominator?

$$n = \frac{2f+1}{\gcd(2f+1, v(m))}$$

so n is odd, ≥ 3

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

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

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

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

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

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

$$\Rightarrow p^{F+1/2} \leq 4$$

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

And check the possible cases. $\square$

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

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

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

Problem

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

"Reduction of abelian integrals to elliptic integrals"
diff forms

$$C \rightarrow Jac \simeq E_1 \times \dots \times E_g$$

find a basis of diff'l forms of first kind on C by taking $C \rightarrow E_i$ 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 $dfk : \left\{ \frac{dx}{y}, \frac{x dx}{y} \right\}$

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

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

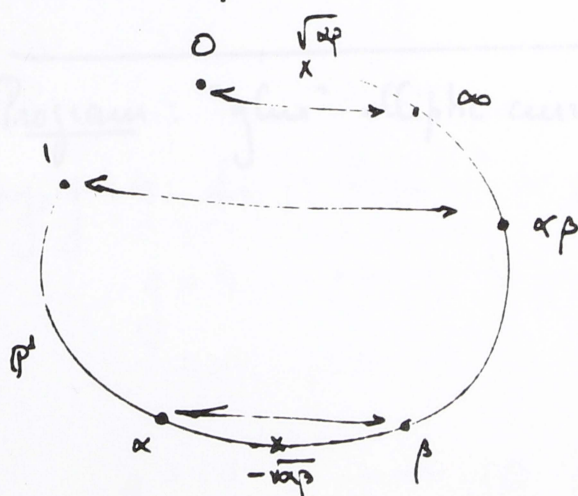
Change variables $(x, y) \longrightarrow (X, Y_1)$ $X = z + \frac{\alpha\beta}{z}$
 $Y_1 = y \frac{z - \sqrt{\alpha\beta}}{z^2}$

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

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

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

Geometrically

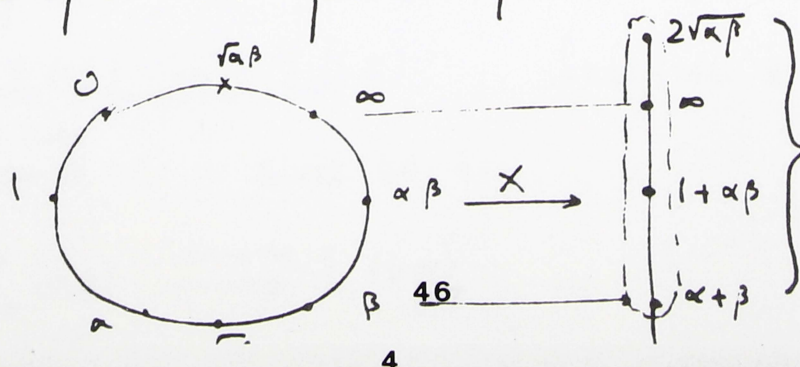


$$x \xrightarrow{\sigma} \frac{\alpha\beta}{x}$$

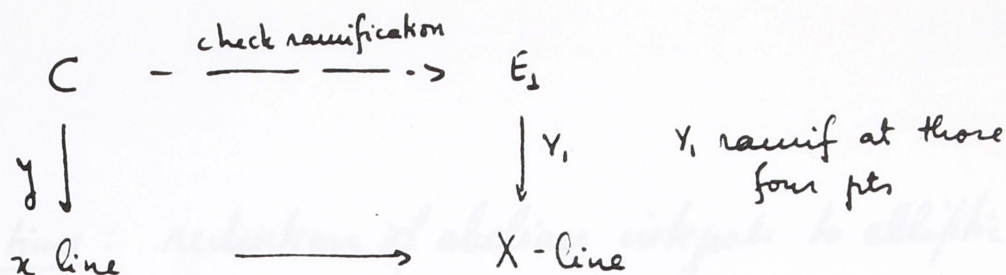
involution

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

mod out by $\sigma : X = \text{quotient by } \sigma = x + \sigma(x)$

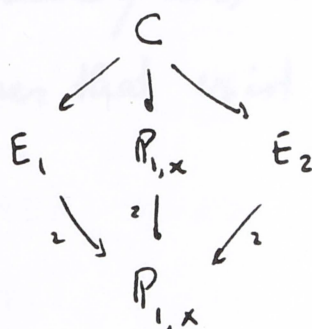


make the ell. curve ramified here



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

Or:



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

10/22:

Last time: reduction of abelian integrals to elliptic ones.

Legendre-Jacobi: $g=2$, example

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

Does that exist for any g ?

an infinite seq. of g 's? / char zero
(in char p , $x^{p^4} + y^{p^4} + z^{p^4} = 0$ 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. curves)
 1 eqn $\longrightarrow$ ok

$g=10 \longrightarrow 10$ parameters
 $\frac{10 \cdot 11}{2} - 27 \gg 0$ } rather surprising that examples exist.

Example: $g=7$, $X_0(60)$; let $J_0(60) = \text{Jac } X_0(60)$

$J_0(15) \implies J_0(60)$ (maps are $z \rightarrow z, z \rightarrow 2z, z \rightarrow 4z$).
ell. curve over $\mathbb{Q}$ Since $60 = 4 \times 15$

$J_0(20) \implies J_0(60)$
ell. curve over $\mathbb{Q}$ 48

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

$$J_0(60) \sim \text{product} \cdot J_0(15)^3 \times J_0(20)^2 \times J_0(30)$$

Antwort: $\left\{ \begin{array}{l} X_0(180) ; g=25, \text{ splits} \\ X_0(198), g=29, \text{ splits} \\ X_0(288), g=33, \text{ splits} \\ X_0(300), g=43, \text{ splits} \end{array} \right.$

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

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

Question: why so often?

Theorem for $g=2$: (Conjecture $N_2(2)$) Let $m = \lfloor 2g^{1/2} \rfloor$

(a) If g is a square, then:

- if $g \neq 4, 9$, then $N = 1 + g + 4g^{1/2} = 1 + g + 2m$
- if $g = 4$, $N = 10$ (Weil: 13) (down by 3)
- if $g = 9$, $N = \overset{49}{20}$ (Weil: 22) (down by 2)

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 $2\sqrt{p}$), for a given p .

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

Write:

$$2\sqrt{p} = a_1.a_2 \dots 101 \overbrace{}^{\{2\sqrt{p}\}}$$

↑
exceptional q

should be $<$ slightly more often than $>$. ($0.6 > 0.5$)

LIST OF $q = p^{2e+1}$ $e \geq 1$

There are only 14 :

$$q \leq 10^9 \text{ s.t. } p \mid m$$

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

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

Thus (Lebesgue, Nagell, Ljunggren)

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

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

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

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

The Theorem is about

$$y^n = x^2 + 1 \quad (x^2+x+1, x^2+x+2)$$

$$\text{e.g. } y^n = x^2 + 1, \quad n \geq 2, \quad x, y \in \mathbb{Z}$$

$x \neq 0$
has no solutions.

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

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

$$\{2\sqrt{7^3}\} = 0.01... \quad 4 \cdot 7^3 = 37^2_{51} 3$$

$$\text{So } 2\sqrt{7^3} \approx 37$$

Recall

$$\sqrt{2} = 1.0110101000001\dots$$

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 "QV5": using a thm. of Shimura.
- 4) Non-existence proofs $\rightarrow$ hermitian forms.

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

$$\text{we proved } \max \text{ of } \# \text{ pts} = \begin{cases} 1+g+w \\ g+w \end{cases}$$

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

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

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

Schoof: one can compute # of pts in $(\log q)^3$ steps.
(but 'implementable').

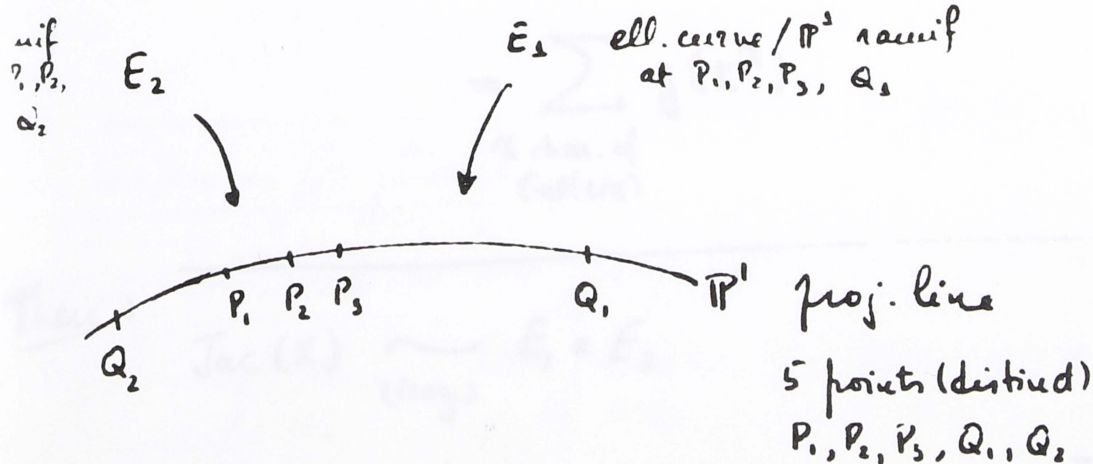
Can compute $E_{p-1}(c_4, c_6) \equiv a_p \pmod{p}$

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

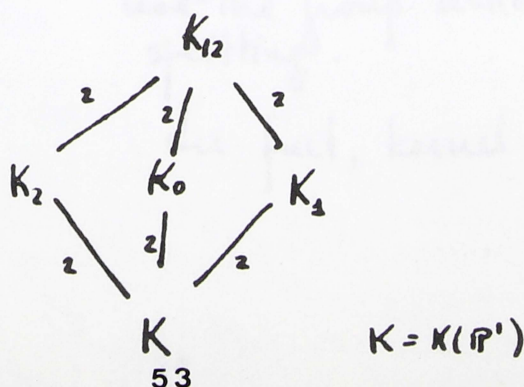
Our construction in 1) is effective if we know the eqn. for $g=1$.

Legendre construction

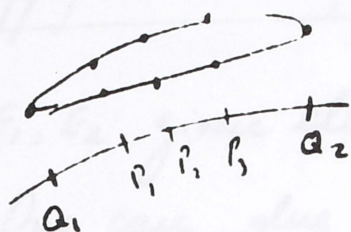
char $\neq 2$.



In terms of fields:



$K_0 \xrightarrow{2} E_0$ 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 $P_1', P_1'', P_2', P_2'', P_3', P_3''$
 $X_{12} = X \leftrightarrow K_{12}$ Have a group of type $(2,2)$ acting on X

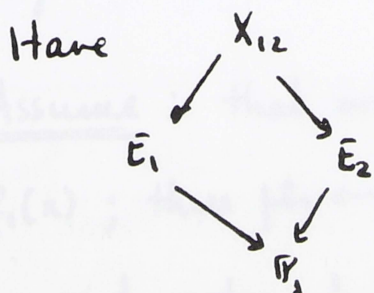
Exercise: In general, L/K $g(K) = 0$, $\text{Gal}(L/K)$ of type $(2,2, \dots, 2)$.
 Then

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

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

Then:

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



; these give a map $\text{Jac}(X) \rightarrow E_1 \times E_2$;
 use the group action to get the splitting.

du fait, 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" $\iff$ $\exists X$ of genus 2 (over $\mathbb{F}_q$)

$$\text{Jac } X \underset{\substack{\text{isog} \\ \text{over } \mathbb{F}_q}}{\sim} \bar{E}_1 \times \bar{E}_2$$

$\iff$ eigenv. of Frob. on $X = \{\text{those on } \bar{E}_1\} \cup \{\text{those of } \bar{E}_2\}$
 Tate-Honda

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

so
$$N(X) = N(\bar{E}_1) + N(\bar{E}_2) - q - 1.$$

Criterion for "gluing"

Let $(E_i)_2$ be the group of 2-div. pts of E_i (if type $(2, 4)$)



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 $\bar{E}_2$.

$(y^2 = f_i(x); \text{ three pts } \leftrightarrow \text{ zeros of } f_i(x))$
 and order 1, 2, 3 corresponds to

- $\uparrow$ all three pts are rat'l
- $\swarrow$ one ⁵⁵rat'l, other two conj.
- $\searrow$ zero pts rat'l.

Thm (char $\neq 2$) Under this assumption, one can glue E_1 to E_2 , except maybe if:

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

(So if $\text{Aut } E_1 = \text{Aut } E_2 = \{\pm 1\}$, these assumptions $\Rightarrow$ one can glue E_1 & E_2).

Example of non-gluing

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

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

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

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

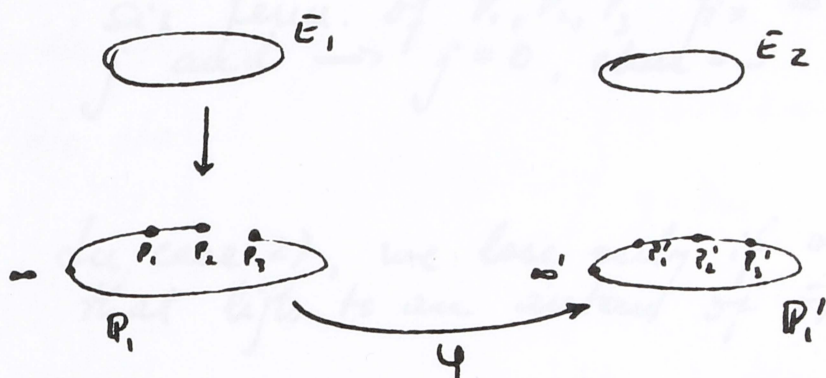
(If $\pi = -3$, $N(E_1) = 16$, so $N(X) = 22$ but X is a two-fold cover of $\mathbb{P}_q$ which has 10 pts, so $N(X) \leq 20$.)

Proof: 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.)

$n = \text{order of Frob}$

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. $\left\{ \begin{array}{l} \varphi \infty \neq \infty' \\ \varphi \{P_1, P_2, P_3\} = \{P_1', P_2', P_3'\} \\ \varphi \circ \text{Frob} = \text{Frob} \circ \varphi \end{array} \right.$

Claim: φ exists (unless we are in the 3 exceptional cases).

Choose an isom 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 $\left\{ \begin{array}{c} \times \times \circ \\ \times \times \circ \end{array} \right\}$
two possible φ (φ_1 and $\pi \circ \varphi_1$)

3) If order of Frob = 3, have cyclic order on Pts
three possible φ ($\varphi, \pi \varphi, \pi^2 \varphi$)

Solving this finds a φ satisfying 2nd & 3rd cond.; remain 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.!) $\square$

In case 2), we lose only if ∞ is fixed by $(P_1 P_2 P_3) \rightarrow (P_1 P_3 P_2)$ that lifts to an autom of E , of order 4, so $j=1/28$.

Similarly in case 3). $\square$

10/29

$\boxed{q=2}$, cont.

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

We stated:

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

$m = \lfloor 2q^{1/2} \rfloor$

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

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

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

Elementary gluing

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

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

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

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

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

(a) Suppose, first, $p \neq 2, 3$.

Choose a supersingular curve E over $\mathbb{F}_p$ with $\text{Frob} = p$. (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 $\text{Frob} = -q^{1/2}$).

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

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

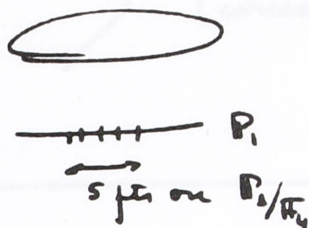
(b) $q=4$ or 9

$$q=4, \text{ Weil} = 1 + q + 2u = 1 + 4 + 24 = 13$$

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

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

This gives covering



3 simple poles $\Rightarrow$

$$\Rightarrow g = 2.$$

So to prove: every pt splits completely

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

$$x = p, p^2 \quad (p^3 = 1, p \neq 1)$$

$$\left\{ \begin{array}{ll} x = 0 & \rightarrow \text{RHS} = 0 \\ x = 1 & \rightarrow \text{RHS} = 1 \\ x = \infty & \rightarrow = 0 \\ x = p & \rightarrow = 1 \\ x = p^2 & \rightarrow = 1 \end{array} \right.$$

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

Over $\mathbb{F}_2$, $N_1 = 4$, $N_2 = 10$

write $a_1 = \pi_1 + \bar{\pi}_1$
 $a_2 = \pi_2 + \bar{\pi}_2$

then

$$\left\{ \begin{array}{l} 1 + 2\bar{a}_1 - a_2 = 4 \\ 1 + 4 - (a_1^2 - 4) - (a_2^2 - 4) = 10 \end{array} \right.$$

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

So

$$\left\{ \begin{array}{l} a_1 + a_2 = -1 \\ a_1^2 + a_2^2 = 3 \end{array} \right.$$

$$\text{So } a_1 = \frac{-1 \pm \sqrt{5}}{2}$$

$$a_2 = \frac{-1 - \sqrt{5}}{2}$$

ab var. of dim 2, irred.
(comes from $\mathbb{Q}(\sqrt{5})$).

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

$$\text{eqn: } y^2 = (x^3 - x)^2 - 1 = (x^3 - x + 1)(x^3 - x - 1)$$

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

$x = \infty$ — OK (look at coeff)

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

$x \in \mathbb{F}_9 - \mathbb{F}_3$, $x^3 - x$ is antisym. under $x \mapsto x^3$
so $(x^3 - x)^2$ is sym, 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 V is isog to product $E_1 \times E_2$.

(c) $q = 2^{2e}, e \geq 2$

To construct: curve with Weil bound

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

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

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

Over $\mathbb{F}_4$, $\pi = -2$, Frob = -2.

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

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

Consider

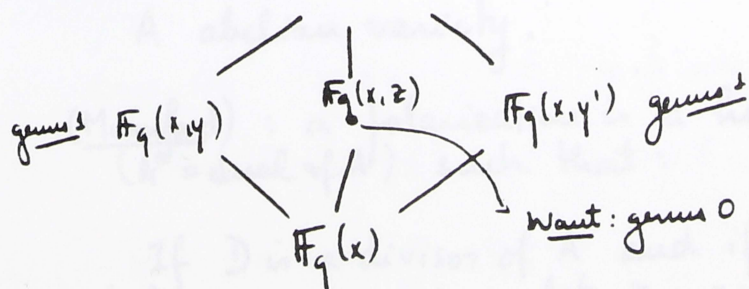
$$\begin{array}{ccc} \mathbb{F}_q(x, y) & & \mathbb{F}_q(x, y') \\ 2 \downarrow & \searrow 2 & \\ \mathbb{F}_q(x) & & \end{array}$$

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:



And don't want constant field extn.

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

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

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

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

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 $\text{Jac} \sim \text{product } E \times E$

This gives the ~~desired~~ desired construction. $\square$

④ For $q = 3^{2e}$, $e \geq 2$

We use a different method.

Intermezzo: On polarizations

A abelian variety.

(Mumford): a polarization is a homomorphism $\psi: A \rightarrow A^*$
(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 $\tau_a: x \mapsto x + a$, $D_a = \tau_a(D)$.

Then $D_a - D$ represents a point in $A^* = \text{Pic}^0(A)$.

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

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

$$\deg_{\text{pol}}(\varphi) = \sqrt{\deg \varphi} = \frac{D^2}{g!} = \chi(A, \mathcal{L}(D)) = \dim H^0(A, \mathcal{L}(D)).$$

(cf. Mumford, Ab. Varieties)

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

Criterion: $\varphi: A \rightarrow A^*$ comes from an element (ample or not) of $\text{NS}(A) \iff \varphi^* = \varphi$

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

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

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

$$A^* = E^* \times \dots \times E^* = E \times \dots \times E$$

$$\varphi: E \times \dots \times E \longrightarrow E \times \dots \times E$$

$$\text{End}(E) = \mathbb{Z}$$

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

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

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

φ polarization $\iff \varphi = {}^t\varphi$ (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 $E \times \underline{1} \times E$.

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 $C \rightarrow J$, then define

$$\Theta = \underbrace{C + \dots + C}_{g-1 \text{ times}} \underset{\text{binate}}{\cong} C^{(g-1)}$$

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

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

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

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

or 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 generated by $\text{Gal}(k'/k)$ 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]

Proof: principal polarization $\Rightarrow C \cdot C = C^2 = 2$
 $(\deg \varphi = \frac{C^g}{g!} \text{ and } g=2)$

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

$$\text{So } \sum m_i m_j C_i \cdot C_j = 2$$

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

So either we have $2 = 2$
 or $2 = 1 + 1$

so either $\left\{ \begin{array}{l} C \text{ is irred} \end{array} \right.$

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

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

If C irred, need still prove nonsing of genus 2.

Cannot be genus 0 or 1. Let $g_a = \text{arith. genus of } C = \dim H^1(C, \mathcal{O}_C)$.

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

Adjunction formula : $\boxed{2g_a - 2 = C \cdot C + C \cdot K}$
 $K = \text{can. divisor}$

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 $g=2$ and nonsingular.

(Proof of exercise : adj. formula $\Rightarrow C \cdot C \geq 0$ 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



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

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 $\epsilon \in \{\pm 1\}$ s.t. f gives ϵF by functoriality.

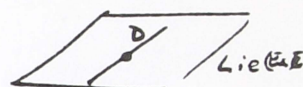
In particular, $\text{Aut}(C) \times \{\pm 1\} = \text{Aut}(J, \text{pol.})$

Fine de l'Inferno

Back to F_{g^e} , $e \geq 2$

Take E w/ $\text{Frob} = -g^{1/2}$

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



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

will choose D not rat'l over $\mathbb{F}_p^2$

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

Prop: this descends to J & becomes principal there, and J is indec., which gives a curve.

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

J

ab. scheme

P_1

corresponds to a surface

S

$\downarrow$

$\mathbb{P}_1$

s.t. generic fiber is curve of genus 2

$5p-5$ exceptional fibers all curves

For $\begin{cases} p=2, \\ p=3 \\ p \geq 5 \end{cases}$ $\begin{cases} 5p-5 = 5 \rightarrow \text{rat'l pts} / \mathbb{F}_4 \\ 5p-5 = 10 \rightarrow \text{pts left over!} / \mathbb{F}_5 \end{cases}$

$\rangle$ So this picks out the exceptional pts.

11/5 ($q=2$ cont.)

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

We have proved this except:

Missing case: $q = q^e$, $e \geq 2$.

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

For such E : Well-known: $\text{End}(E)$ 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 $\text{End } E \ni \alpha$ 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: $\psi: A \longrightarrow A^* = E \times E$

$$\psi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$a, b, c, d \in \text{End}(E)$$

φ is a polarization $\iff \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 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 $\varphi: A \rightarrow A^*$ as End , and asks which φ are polarizations.
So says, take $\text{End} \otimes \mathbb{R}$, and then φ polar. corresponds to positive definite symmetric matrices.

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

(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: $\text{Ker } \varphi$ has order p^2 (say, look at ℓ -adic representations.)

tgt space at E is 1-dim'l, so $\text{End } E \rightarrow \mathbb{F}_p$ (action on tgt space)
residue field at p .
 $\alpha \rightarrow 0$ ($\alpha \bar{\alpha} = p(p-1) \rightarrow 0$!)
 $p \rightarrow 0$

So ψ 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 $\text{Ker } \psi = t_A$ in our case.

Take $\mathbb{F}_q \supseteq \mathbb{F}_{p^2}$, 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 not in $\mathbb{F}_{p^2}$. [This means something since $A = E \times E$.]

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

"tangent space" $\longleftrightarrow t_A$

$D \longleftrightarrow [D] \subset t_A$ (subgroup scheme)

(stable under p -th power map)

(which is zero here) $\rightarrow$ 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. $A: y^2 = x^3 + ax + b$

$\text{Fr} \downarrow$

$A^{(p)}: y^2 = x^3 + a^p x + b^p$

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 polarisation descends to J :

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A^* \\ \pi \downarrow & & \uparrow \pi^* \\ J & \xrightarrow{\exists \varphi_J?} & J^* \end{array}$$

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

(de Murfod): if D has dim. 1, this nec. condn. is also sufficient.

[General fact is $\left\{ \begin{array}{l} \varphi: A \rightarrow A^* \text{ polariz.} \\ N \text{ finite subgp of } A \\ \text{Assume } N \subset \ker \varphi, |N| \text{ is prime.} \end{array} \right.$

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

$\deg \varphi_J = ?$ 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 $\Lambda: k \oplus kx \oplus \dots \oplus kx^{p-1}; x^p = 0$
 $k[x]/(x^p)$

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

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

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

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

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

Claim: $\text{tgt}(E)$ 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 $\text{Frob} = p$ (for any such E). Then $\text{tgt}(E)$ comes from the tgt space over $\mathbb{F}_{p^2}$.

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

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

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

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

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^2 (since H^1 is invariant under isogeny), so this realizes the Weil minimum.

So $q = \text{square}$ is done. $\square$

q non-square

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

Thm: If q is not special, then $N_q(2) = 1 + q + 2m$.

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

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

We use the "elementary gluing":

② $p \neq 2$

Lemma: 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 $\text{Tr}(\text{Frob}) = a$
and $j(E) \neq 0, 1728$.

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

If $\text{End}(E) \neq \mathbb{Z}[i]$ or $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, then $j(E) \neq 0, 1728$,
so ok.

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

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

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/ $\text{End} = \mathbb{Z}[\pi]$.]

[Instead:]

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

So $\pi \equiv x \pmod{l\text{End } E}$,

so π acts by homothety on l -div. pts

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

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

Then $\text{End}(E/D) = \{x + iy \mid l \nmid y\} + \mathbb{Z}[i]$, so choose E/D now.

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

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

(if $u^2 - 4q = -4 \Rightarrow 4q = 4 + u^2 \Rightarrow 2 \nmid u \Rightarrow q = 1 + (\frac{u}{2})^2$,
if $u^2 - 4q = -3$, similar)

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

① $p=2$ 2^e (e odd) is nonspecial iff $\begin{cases} 2 \nmid m \\ 2^e \text{ is not } x^2+x+2 \end{cases}$

~~Choose E_1 and E_2 with $T_2(\text{Frob}) = -u$ and which are not isom., even after quadratic field extension.~~

Choose E_1 and E_2 with $T_2(\text{Frob}) = -u$ 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 $x \sim -x$.

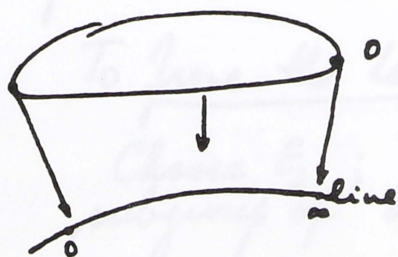
Other ramif pt is the pt of order 2, rat'l, so can map to zero.

So Artin-Schreier eqn is

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

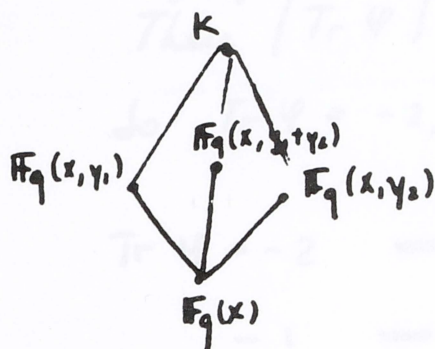
replace x by λx , so can write $y^2 + y = x + \frac{\mu}{x} + \nu$

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



So have $E_1 : \begin{cases} y_1^2 + y_1 = x + \frac{\mu_1}{x} + v_1 \\ y_2^2 + y_2 = x + \frac{\mu_2}{x} + v_2 \end{cases}$

$$\mu_1 \neq \mu_2$$



$$(y_1 + y_2)^2 - (y_1 + y_2) = \frac{\mu_1 + \mu_2}{x} + v_1 + v_2$$

genus zero

[if $\mu_1 = \mu_2$ ~~extr.~~ $\mu_1 + \mu_2 = 0$ so get const field

So K is the field of a curve of genus 2. This proves gluing $\square$

To prove the Lemma (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 $\exists \varphi: E_1 \rightarrow E_1$ with kernel N , hence of degree 2.

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

Then $|\text{Tr } \varphi| \leq 2\sqrt{2}$ (since $|\varphi| = \sqrt{2}$)

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

$\text{Tr } \varphi = -2$	$\Rightarrow$	$\varphi = -1 \pm i$	} impossible, since 2 splits in $\text{End } E$ by general facts.
-1	$\Rightarrow$	$\varphi = \frac{-1 \pm \sqrt{-7}}{2}$	
0	$\Rightarrow$	$\varphi = \pm \sqrt{-2}$	
1	$\Rightarrow$	$\varphi = 1 \pm i$	
2	$\Rightarrow$	$\varphi = \frac{1 \pm \sqrt{-7}}{2}$	

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

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

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

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

Again: claim that $y^2 \neq 1$

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

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

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

Need to show: if q is special:

- a) $q+1+2m$ is impossible
- b) $q+2m$ is possible iff $|2q| > \frac{q-1}{2}$
- c) if q is special and $|2q| = \frac{q-1}{2}$, then $q+2m-1$ is possible.

a) Proof: q is special means (a) q is represented by the quad. poly x^2+1/x^2+2 (special case of discriminant)

or (b) q is represented by x^2+2x+2 (so $q \equiv 2 \pmod{4}$, x odd). One finds $x = 1, 3, 5, 13, \dots$ (see this later)

or (c) plus

$$x^2 + 1/x^2 + 2$$

$$x^4 + (x+1)^2 + 7 = y^2 + 1$$

Ramanujan's equation

11/12

$$\boxed{q=2}$$

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

Need to show: if q is special:

- $$\left\{ \begin{array}{l} \text{a) } q+1+2u \text{ is impossible} \\ \text{b) } q+2u \text{ is possible iff } \{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2} \\ \text{c) if } q \text{ special and } \{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}, \text{ then } q+2u-1 \text{ is possible.} \end{array} \right.$$

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 $e=1, 3, 5, 13, \dots \rightarrow$ see this later

OR

a3) $p|m$

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

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

Ramanujan's equation

Case a2: We show that $q+1+2m$ is impossible.

→ df $q=2$, $[2\sqrt{2}] = 2$, so this is special also because $p|m$ (a3).

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

→ df $q=2^3$, $[2\sqrt{8}] = [\sqrt{32}] = 5$, 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 $\pi, \bar{\pi}, \pi, \bar{\pi}$, $\pi + \bar{\pi} = -m$, $\pi\bar{\pi} = q$.

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

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

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

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 $\mathbb{F}_2$ is a fifth power.

Take $\text{Jac}(C)/\mathbb{F}_2$.

$$\text{End}(\text{Jac}(C)) \supset \mathbb{Z}[\pi] \quad (\text{in fact } = M_2(\mathbb{Z}[5]))$$

$$\text{So } \text{End}(\text{Jac}(C)) = \mathbb{Z}[\pi] = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$$

define $\pi_1 = -\alpha \in \text{End}(\text{Jac}(C))$, and then $\pi_1^5 = \pi = \text{Frobenius on } \text{Jac}(C)$.

• So have ab. var. $A/\mathbb{F}_p$, $\pi = \text{Frob}/\mathbb{F}_p$, and $\pi = \pi_1^e$ for some $\pi_1 \in \text{End}(A)$. Would like to conclude: exists a structure $/\mathbb{F}_p$ for A with Frobenius π_1 .

Need more: 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 $A^{(p)}$ as usual. Then we have

$$\begin{array}{ccc} A & \xrightarrow{F_p} & A^{(p)} \\ & \searrow \pi_1 & \downarrow \\ & & A \end{array}$$

(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 $\text{Jac}(C)$ with Frobenius $-\alpha$. Polariz. is invariant by $-\alpha$ ($\alpha = \pi + 6$!) (π respects the polarisation)

So we get (Torelli): there is an $\mathbb{F}_2$ -structure on C with $\text{Frob} = -\alpha$.

Now go to $\mathbb{F}_8 = \mathbb{F}_{2^3}$, and get Frobenius $= -\alpha^3 = \frac{5+\sqrt{-7}}{2}$

Now $\text{nbr of pts}/\mathbb{F}_8 = 1 + 8 - 2 \cdot 5 = -1 \quad \swarrow \text{ (contrad.)}$

$\rightarrow$ If $f = 2^{13}$, 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: $p \nmid m$; I can assume $f = p^e$, e odd ≥ 3

(when $e=1$, $p \nmid m \Rightarrow p=2$ or 3 and these have been done already).

$$\text{have } 1+q+2m \text{ iff } \pi, \bar{\pi}, \pi, \bar{\pi} \quad , \quad \left\{ \begin{array}{l} \pi + \bar{\pi} = -m \\ \pi \bar{\pi} = f \end{array} \right.$$

Now, $p|m$, $q = p^e$ 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 $f_\pi \nmid 2$! So the jacobian cannot exist in this case, done. $\square$

b) If $\{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$, then $q+2m$ is impossible
 If $\{2\sqrt{q}\} > \frac{\sqrt{5}-1}{2}$, then $q+2m$ is possible.

We've shown "down by one" (for a curve) ^{of genus 2} is possible only if

$$\text{Frob: } \pi_1, \bar{\pi}_1, \bar{\pi}_2, \pi_2$$

$$\text{where } \begin{cases} \pi_1 + \bar{\pi}_1 = -m + \frac{1+\sqrt{5}}{2} \\ \pi_2 + \bar{\pi}_2 = -m + \frac{1-\sqrt{5}}{2} \end{cases}$$

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.,

$$\begin{cases} \pi_1 + \bar{\pi}_1 = -u + \frac{1+\sqrt{5}}{2} \\ \pi_2 + \bar{\pi}_2 = -u + \frac{1-\sqrt{5}}{2} \end{cases}$$

We want this ab. variety to be ordinary:

• $\pi_1 + \bar{\pi}_1$ and $\pi_2 + \bar{\pi}_2$ are prime to p

* if $p|u$, obvious, since $\frac{1 \pm \sqrt{5}}{2}$ is a unit

* if $p \nmid u$, q is repres. by x^2+1, x^2+x+1, x^2+x+2 ,

so $4q = 4x^2 + 4 = (2x)^2 + 4$ so $u = 2x$

$4q = 4x^2 + 4x + 4 = (2x+1)^2 + 3$ so $u = 2x+1$

$4q = 4x^2 + 4x + 8 = (2x+1)^2 + 7$, so $u = 2x+1$.

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: $p|u$)

$\{2\sqrt{8}\} = 0.656... > \frac{\sqrt{5}-1}{2}$

[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 ($= 2(1+p)$) points over $\mathbb{F}_8$

Choose an irreducible cubic poly $f(x)$ on $\mathbb{F}_8$, e.g.
 $x^3 + x + c$ for suitable c .

Write

$$y^2 + y = \frac{a + bx + cx^2}{x^3 + x + c} \quad a, b, c \in \mathbb{F}_8.$$

$$(i.e.) \quad y^2 + y = \frac{a + bx + cx^2}{f(x)} \quad a, b, c \in \mathbb{F}_8.$$

We want to choose a, b, c s.t.

$$\text{Tr}_{\mathbb{F}_8/\mathbb{F}_2} \left(\frac{a + bx + cx^2}{f(x)} \right) = 0 \quad \text{for all } x \in \mathbb{F}_8.$$

$a, b, c \in \mathbb{F}_8 = \mathbb{F}_2^3$ (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 $Q(\pi) > Q(\sqrt{5})$..

Have $\mathbb{Q}(\pi) \xleftarrow{\text{CM-field of deg. 4 w/ assoc. real field } \mathbb{Q}(\sqrt{5})} \mathbb{Q}(\sqrt{5})$
 $\downarrow_2$ imag. quad. extn.
 $\mathbb{Q}(\sqrt{5})$
 $\downarrow_2$
 $\mathbb{Q}$

So $\text{End}_{\pi}(A) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ (Tate).

We have A up to isogeny.

Next step: existence of such an A having a polar-ization of degree 1.

(Shimura: A in char 0, CM by $\begin{smallmatrix} K \\ 2 \\ K_0 \end{smallmatrix} \rightarrow \text{OK}$)

Shimura's Thm (char 0): 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., 34 (1977), p. 67, remark.]

Here OK, since $\mathbb{Q}(\sqrt{5})$ has class number 1. $\rightarrow$ no quadratic unramified extn.

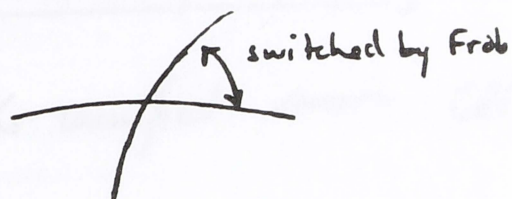
Claim: Sh's thm is OK in char p for ordinary abelian varieties

(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 $\text{End}_{\mathbb{F}_q}(A) = \mathbb{Q}(\pi)$ 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 $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$

so trace = 0.

But our trace is $-2m + 1 \neq 0$.

This proves that our curve exists. $\square$

Proof of Claim above

char 0 Shimura $\implies$ char p Shimura for ord ab. vars.

Use "canonical lifting": lift $A/\mathbb{F}_q$ into $\mathcal{A}/W(\mathbb{F}_q)$, and End does not change.

By Shimura, $\mathcal{A} \xrightarrow{\text{isog}} \mathcal{A}'$, on $\mathcal{A}'$ have a polariz. of degree 1. ker of $\mathcal{A} \rightarrow \mathcal{A}'$ is stable under max'l order

So $\mathcal{A} \rightarrow \mathcal{A}'$ exists over the field of fractions of $W(\mathbb{F}_q)$.

Polarization is $\mathcal{A}' \rightarrow (\mathcal{A}')^*$.

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 :

$$K/K_0 \text{ ramified} \iff \text{Cl}(K) \xrightarrow{\text{norm}} \text{Cl}^{\text{strict}}(K_0) \text{ is onto}$$

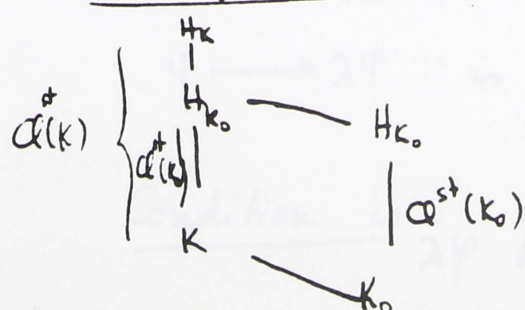
$$[\text{Cl}^{\text{strict}} : \sigma \sim 1 \text{ if } \sigma = (\alpha), \alpha \gg 0.]$$

For tot. imag. field, $\text{Cl}(K) = \text{Cl}^{\text{strict}}(K)$, and map is just $\sigma \mapsto \sigma \bar{\sigma}$.

Pf of $\Leftarrow$ CFT!

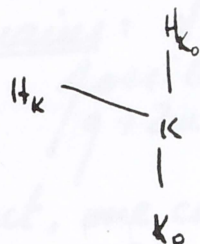
H_K = Hilbert class field
max. ab. unram. extn, except maybe at ∞

$$\text{Then } \text{Gal}(H_K/K_0) \cong \text{Cl}^{\text{strict}}(K_0)$$



and res: $\text{Gal}(H_K/K) \rightarrow \text{Gal}(H_{K_0}/K_0)$
is norm map.

if K/K_0 unram, we'd have,



and then coker $\mathcal{O}_K \rightarrow \mathcal{O}_K^{\text{st}}(K_0)$ has order 2. $\square$

Shimura's proof

Choose A s.t. $\text{End}(A)$ is a max'l order in K , and choose some polarization $\psi: A \rightarrow A^*$.

look at $\mathcal{O}$ ideal of $\mathcal{O}_K$ s.t. $\ker \psi \cong \mathcal{O}_K/\mathcal{O}$

Shimura-Taniyama: $\mathcal{O}$ "is" an ideal of $\mathcal{O}_{K_0}$.

Replacing ψ by $\lambda\psi$ gives a polarization if $\lambda \in \mathcal{O}_{K_0}^{\times}$, $\lambda \gg 0$.

May replace A by some $A/(\text{finite subgp stable by } \mathcal{O}_K)$ $\longleftrightarrow$ some ideal $\mathfrak{v} \subset \mathcal{O}_K$

Want $\lambda\psi$ to descend to $A/(\)$ w/ degree 1

$$\psi \mapsto \lambda\psi \quad \text{is} \quad \mathcal{O} \mapsto \lambda\mathcal{O}$$

Condition is: if $\lambda\mathcal{O} = \mathfrak{v}\overline{\mathcal{O}}$, then on $A/(\)$, $\lambda\psi$ has degree 1.

This is equiv to: the class of $\mathcal{O}$ in $\mathcal{O}_K^{\text{st}}(K_0)$ is an image of $\mathfrak{v} \in \mathcal{O}_K$. So OK if $\mathcal{O}_K \rightarrow \mathcal{O}_K^{\text{st}}(K_0)$ is onto.

This proves part (b). $\square$

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 ~~of type~~ 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) $p \nmid m$, 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 $\text{Trace}(F_{\text{rob}}) = -(m-1)$

$(m, m-2)$ possible: Can glue E_1, E_2 with $\text{Trace}(F_{\text{rob}}) = \begin{cases} -m \\ -(m-2) \end{cases}$

Case 1: $p|m$, hence $p|(m-1)$, so E_1 and E_2 exist (and are ordinary).

Also, $\mathbb{Z}[\tau]$ is an order in an imag. quad. field w/ disc. $-4q + \text{Tr}(\tau)^2 = -4q + (m-1)^2 = -(4q - (m-1)^2)$

$$4q = m^2 + k \quad 1 \leq k \leq 2m$$

$$4q - (m-1)^2 = m^2 + k - m^2 + 2m - 1 = k + 2m - 1 \geq 8$$

One can choose E_1, E_2 such that $\text{End}(E_i) = \mathbb{Z}[\tau]$.

So $\text{End} \not\cong \bigoplus_i \text{cube roots of } 1$

So $j \neq 0, 1, 2, 8$

so elementary glueing is OK.

$$k \equiv -m^2 \equiv 0 \text{ or } 3 \pmod{4}$$

$$\text{so } k \equiv 3 \pmod{4}$$

$$k = 3, 7, \dots$$

$$p|m, p \neq 2 \rightarrow 2m-1 \geq 5$$

$$\text{so } \geq 8.$$

Case 2: $\checkmark$ Choose E , End $E = \mathbb{Z}[x]$, and, ~~disc~~ $\text{disc} < -8$.

Now take $E, E' = E/E[2]$ (in char 2!)

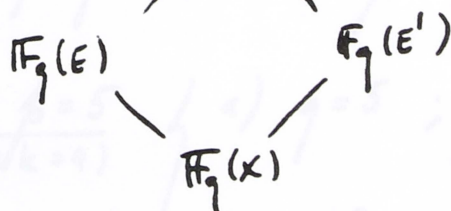
Not isomorphic (otherwise $\exists$ isogeny $E \rightarrow E$ deg 2 $\rightarrow \mathbb{Q}(\sqrt{-7})$).

Write them as $y^2 + y = x + \frac{a}{x} + b$

$$y^2 + y = x + \frac{a'}{x} + b'$$

$a \neq a'$

And we get the usual diagram
joining.



This does ②.

Case 3: $p \nmid m$, q special, $p \neq 2$:

Same proof, but problem is whether $p \mid m-1$.

$$q \text{ special}, p=2 \rightarrow 4q = m^2 + 3 \text{ or } 4q = m^2 + 4.$$

$$\text{So } 4q = m^2 + k, \quad k=3 \text{ or } 4$$

$$p \mid m-1 \Rightarrow m \equiv 1 \pmod{p} \Rightarrow k \equiv -1 \pmod{p}$$

$$\text{so } 4 \text{ or } 5 \equiv 0 \pmod{p}$$

$$\rightarrow p=5, \quad k=4, \quad m \text{ even}$$

• So if $p \neq 5$, same proof above works since $p \nmid (m-1)$.

• If $\frac{p=5}{(k=4)}$ $\left\{ \begin{array}{l} \text{a) } q=5; \text{ then } m = [2\sqrt{5}] = 4, \quad m-1 = 3 \\ \text{and } 5 \nmid 3. \text{ So OK.} \\ \text{b) } q=5^e, \quad e \text{ odd } \geq 3; \text{ would have } 5^e = \left(\frac{m}{2}\right)^2 + 1 \end{array} \right.$
 But the eqn: $y^e = x^2 + 1 \quad x \neq 0 \quad e \geq 2$ has
 no $\mathbb{Z}$ -solutions.
 [proof later].

So ⑥ is empty, and ③ is done.

Case 4: $q = 2^3, 2^5, 2^{13}$

Claim is: $(m, m-2)$ is possible.

$$p=2, 2|m \Rightarrow 2|m-2$$

So we find E_1, E_2 ord. elliptic curves with $\text{Tr}(\text{Frob}) = \begin{cases} -m \\ -(m-2) \end{cases}$
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
if $4q = m+7$ so $m=1 \Rightarrow q=2$. $\square$

Glueing and Hermitian Forms

Idea: $E, R = \text{End}_{\mathbb{F}_q}(E)$

We want to construct the jacobian of a curve

$$J = E \times E \quad \text{w/ a map } E \times E \xrightarrow{\varphi} E \times E$$

$$\text{given by } \Phi: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$$

$$\varphi \text{ polarization} \iff \Phi \text{ hermitian} \gg 0$$

$$\deg 1 \iff ad - bc = 1$$

If not decomposable, then $\exists!$ C of genus 2
with

$$\text{Jac}(C) = (E \times E, \varphi).$$

So E has been glued to E .

$$\underbrace{E \times \dots \times E}_{n \text{ times}} = "E \otimes_R L" \quad L \text{ free of rk } n \text{ over } R$$

So try for projective.

We want to develop this first, then.

Tensor Product (and Hom) in abelian categories

- $\left[\begin{array}{l} \mathcal{C} \text{ an abelian category} \\ R \text{ a ring w/ } 1. \\ \text{Let } E \in \mathcal{C} \text{ with a morphism } R \rightarrow \text{End}(E) \text{ given} \end{array} \right.$

To the pair $(M \text{ a right } R\text{-module, finitely presented}, E \text{ w/ } R\text{-action})$

I want to attach an object of $\mathcal{C}$ called " $M \otimes_R E$ "

Properties shd be : $\bullet R \otimes_R E = E$

$\bullet$ compatible w/ direct sum

$\bullet$ right exact.

Write $R^m \rightarrow R^n \rightarrow M \rightarrow 0$

Set $\begin{cases} R^m \otimes_R E = E^m \\ R^n \otimes_R E = E^n \end{cases}$

And define $M \otimes_R E = \text{Coker}(E^m \rightarrow E^n)$.

Indep. of resolution is easy, and also follows from alternate definition:

Want $\text{Hom}(M \otimes_R E, F) = \text{Hom}_R(M, \text{Hom}(E, F))$

(for $F \in \mathcal{C}$)

where $\text{Hom}(E, F)$ is a right R -module via the action on E .

So $M \otimes_R E$ represents the functor on the right.

Another construction is " $\text{Hom}_R(M, E)$ " where M is a finitely presented left R -module.

Do the same: choose a resolution

$$R^m \rightarrow R^n \rightarrow M \rightarrow 0$$

$$E^m \leftarrow E^n \leftarrow \text{Hom}_R(M, E) \leftarrow 0$$

transpose of
the matrix

define this as the kernel.

This represents a functor too:

$$\text{Hom}_R(F, \text{Hom}_R(M, E)) = \text{Hom}_R(M, \underbrace{\text{Hom}_R(F, E)})$$

viewed as a
left R -module

I'll apply this to: $\mathcal{C}$ category of ^{comm.} alg. groups / k
(or the subcat. of proper such).

And R will be Noeth., M finitely generated.

In this case, $\text{Hom}_R(M, E)$ can also be described by:

$$\begin{array}{c} s' \\ \swarrow \\ k = s \end{array} \quad (\text{Hom}_R(M, E))(s') = \text{Hom}_R(M, E(s'))$$

(This defines it as a functor on k -schemes, so determines it.)

Example: E ell. curve, $R = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$

$$\text{Then } \text{Hom}_{\mathbb{Z}}(M, E) = E[n]$$

$$\text{and the fla above says } E[n](s') = E(s')[n].$$

But $\odot$ is zero!

Now apply this to $\left\{ \begin{array}{l} E \text{ an elliptic curve} \\ R = \text{End}(E) \text{ , } M \text{ fin. generated.} \end{array} \right.$

Then $M \otimes_R E$ is an ab. variety of dimension $\text{rk}_R M (*)$
and $\text{Hom}_R(M, E)$ comm. group of dim = $\text{rk}_R M$.

(*) since it is $\text{Coker}(E^m \rightarrow E^n) !$

Note: can also define $\text{Tor}_n, \text{Ext}^n$ as before...

M projective :

Dual of $M \otimes_R E$ is $M^* \otimes_R E$, where M^* is the dual of M , $M^* = \text{Hom}(M, R)$ a left R -module in a natural way, but use the involution $r \mapsto \bar{r}$ of R corresp. to the polarization (= ex conj. or quat. conj.) and use this to make M^* a right R -module.

i.e., $\lambda \in M^*, r \in R$, define $(\lambda r)(m) = \lambda(m \bar{r})$.

(Note that M projective $\rightarrow$ have $M \xrightleftharpoons[\text{pr}]{\quad} R^n$)
So define $M \otimes_R E \rightleftharpoons E^n$ using the induced projector.)

(For an ab. variety $(M \otimes_R A)^* = M^* \otimes_R A^*$.)

[Can extend for M not projective?]

Claim: $\text{Hom}(M \otimes_R E, N \otimes_R E) = \text{Hom}_R(M, N)$

An arrow $\text{Hom}_R(M, N) \longrightarrow \text{Hom}(M \otimes_R E, N \otimes_R E)$ is obvious.

Since M is projective, it's enough to check for free modules, hence for $M = N = R$, and then

$$\text{Hom}(E, E) = \text{Hom}_R(R, R) = R$$

(by our assumption on R)

Claim: If $M \otimes_R E = B \oplus C$ B, C ab. varieties, then $M = M_B \oplus M_C$ as R -modules and $B = M_B \otimes E$, $C = M_C \otimes E$.

Pf: Corresponds to $p \in \text{End}(M \otimes_R E)$ s.t. $p^2 = p$; but this comes from a projector of M , which gives M_B & M_C . $\square$

E, R, M projective

Define $A = M \otimes_R E$. [Note that this is isg. to $\underbrace{E \times \dots \times E}_{\text{rk } M \text{ times}}$.]

What is a principal polarization on A ?

Claim: Corresp. to an R -hermitian $\gg 0$ form on M with discriminant 1.

Herm. form on M is $\Phi: M \times M \rightarrow R$ w/ the usual properties; can also view as $\varphi: M \rightarrow M^*$ have 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. $\rightarrow \Phi(m, m) > 0$ 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 $(R = \text{End } E!) \quad \{r \in R \mid \bar{r} = r\} = \mathbb{Z}$

So $\Phi(m, m) > 0$ makes sense.]

Now the equivalence

principal polariz on $\Lambda \iff R\text{-herm. form on } M, \left. \begin{array}{l} \text{pos. def. , disc 1.} \end{array} \right\} \begin{array}{l} \text{call} \\ \text{such} \\ \text{"hermitian"} \\ \text{modules"} \end{array}$

is clear, except maybe that pos. def $\iff \varphi$ polarization

If M is free, we have $E \times \xrightarrow{\varphi} E \times$ and then it's in Mumford.

Also

Indec of polariz. $\iff$ 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 $\text{Tr}(\text{Frob } E) \neq 0$, this is automatic. (saw this last time).

$$\text{Set } J = M \otimes_R E. \text{ Indec} \Rightarrow J = J(C)$$

Example

E CM by $\sqrt{-2}$

$$R = \mathbb{Z}[\sqrt{-2}]$$

$$M = R \times R$$

$$\Phi = \begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}, \quad \det = 4 - (1+2) = 1.$$

for def ✓

indec: values of Φ are even $\neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

So this gives a curve C

$$\tilde{S}_Y = \text{Aut}(M) = \text{Aut}(C)$$

$\tilde{S}_Y = 2\text{-sheeted cover of } S_Y$

$\text{genus}(C) = 2, \Rightarrow C$ unique up to quad. twist.

$$\text{eqn: } y^2 = x^5 - x$$

Will show: indec. hermitian M exist, except when R has disc. $-3, -4, -7$.

Also: under some conditions 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, $R = \text{End}_k(E)$; assume $\text{rk } R = 2$. (so $R = \text{order}$ in an imag. quad. field).

Choose an R -module P proj. of rank 2, with a Hermitian form $H: P \times P \rightarrow R$, positive definite (i.e., $H(x, x) > 0$ if $x \neq 0$), disc 1 (i.e., H define an isom. $P \rightarrow P^*$ (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 $\rightarrow A$ indec/ $k \Rightarrow A = \text{Jac}(C)$

for a well-defined C of genus 2.

[k field of defn]

indec. possibility is no problem because we assume $\text{End}_k(E) \neq \text{End}_k(E)$.

$$-d = \text{disc } R$$

$$\text{Write } R = R_{-d}, \text{ so } R_{-4} = \mathbb{Z}[i]$$

$$R_{-3} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

Theorem (Hayashida - Nishi)

Such an indecomposable binary form exists if and only if $d \neq 3, 4, 7$.

First: note: if $A = E \oplus P$, then $P = \text{Hom}_R(E, A)$

for $x \in P$, $H(x) = ?$

interpret x as $E \xrightarrow{x} A$

$H(x) = \text{degree of } x^* (\text{polarization})$

Proof that every P is trivial on R_{-3}, R_{-4}, R_{-7}

Here $P = R \oplus R$ since the class no. is 1.

$$\text{So } H = \begin{pmatrix} \lambda & \alpha \\ \bar{\alpha} & \mu \end{pmatrix}, \quad \lambda, \mu \in \mathbb{Z}, > 0$$

$$\lambda\mu - \alpha\bar{\alpha} = 1, \quad \alpha \in R$$

Want

$$H \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

s.e., ~~have~~ ^{have} e_1, e_2 basis of P s.t. $e_1 \cdot e_1 = 1$, etc.
 e_1 : any primitive vector (i.e., $e_1 \neq 0$, $\mathbb{R}e_1$ 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 $r \in \mathbb{R}$.

Claim: by suitable choice of r , I can make
 α to be such that $\alpha \bar{\alpha} < \frac{3}{4} \lambda^2$.

(Proof later)

$$\text{Then } \lambda \mu - \alpha \bar{\alpha} = 1 \Rightarrow \alpha \bar{\alpha} = \lambda \mu - 1 < \frac{3}{4} \lambda^2$$

$$\lambda \mu < \frac{3}{4} \lambda^2 + 1$$

$$\lambda \leq \mu \Rightarrow \lambda^2 < \frac{3}{4} \lambda^2 + 1 \Rightarrow \frac{1}{4} \lambda^2 < 1$$

$$\Rightarrow \boxed{\lambda = 1}.$$

Then take $r = -\alpha \Rightarrow \alpha$ can be made 0

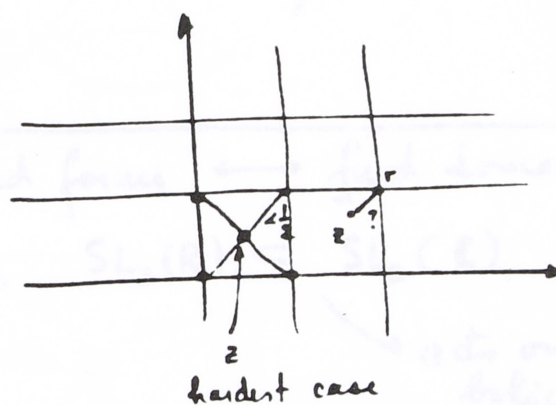
and $\lambda \mu - \alpha \bar{\alpha} = 1$ forces $\mu = 1$. $\square$

Proof of claim

I want to find z s.t. $\left| \frac{w}{\lambda} + z \right|^2 < \frac{3}{4}$.

Lemma: For every $z \in \mathbb{C}$, $\exists r \in \mathbb{R}$ s.t. $|z - r|^2 < \frac{3}{4}$.

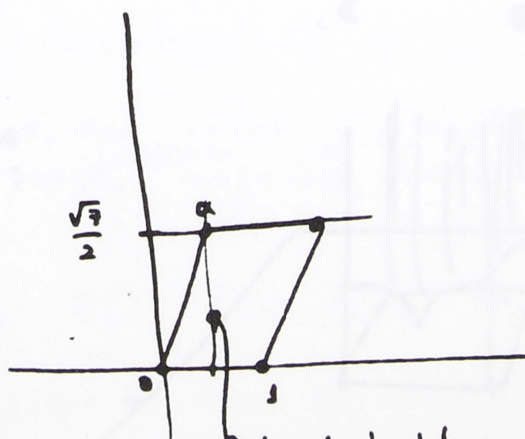
For $z[i]$:



so for $z[i]$ can get $|z - r| < \frac{1}{2}$

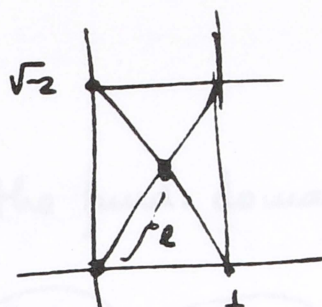
For $z[\frac{1+\sqrt{3}}{2}]$ find can get $|z - r| < \frac{1}{3}$

For R_1 :



hardest pt: center of circle through $0, 1, a$ — so check.

For R_2



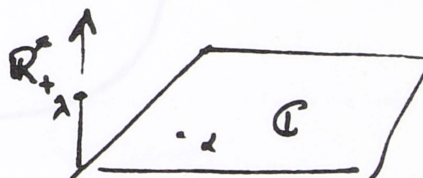
length = $\frac{3}{4}$
so can't work!

In fact, exists a unique unimod. form: $\begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix}$.

Ordinary quad forms $\longleftrightarrow$ fund domain for $SL_2(\mathbb{Z})$

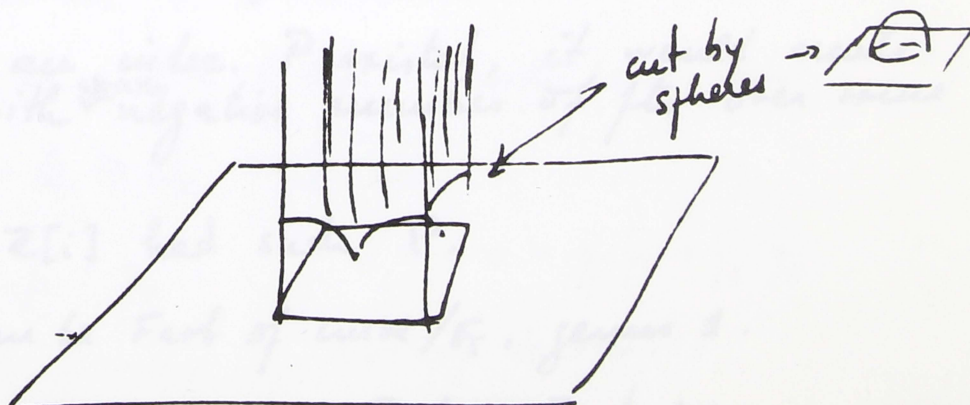
In our case, $SL_2(\mathbb{R}) \subset SL_2(\mathbb{C})$

acts on 3-dim'l hyperbolic space

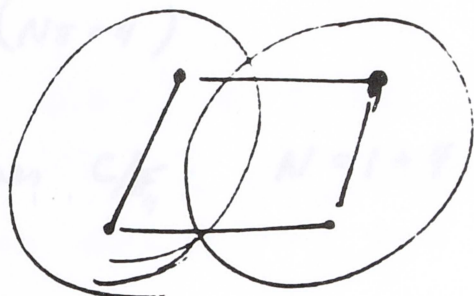


$$|z_1 + \underbrace{\alpha z_2}_{\in \mathbb{C}}|^2 + \underbrace{\lambda}_{\in \mathbb{R}} |z_2|^2$$

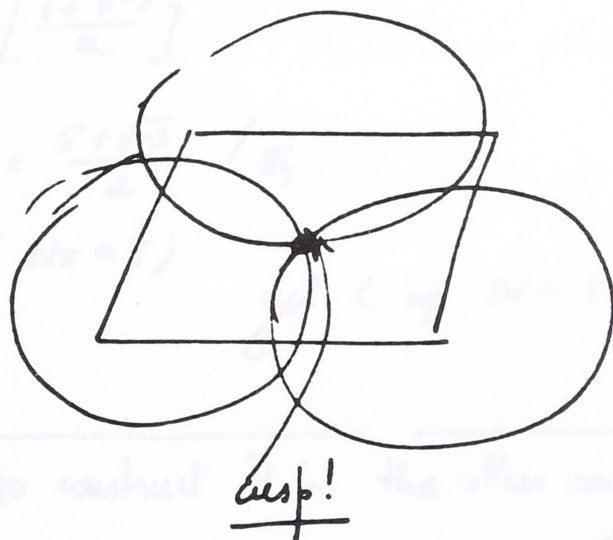
Fund. domain looks like:



So draw the fund. domain + the equators of the spheres



would have $d \neq 1$
(only cusp = ∞)



Biauchi has
such pictures
for low
discriminant.

2nd proof (of nonexistence if $d = -3, -4, -7$)

Idea: if such an $\text{isoc. } P$ 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.

$P \rightarrow \exists C/\mathbb{F}_5$ $g=2$, with Frob $\pi, \bar{\pi}$ twice.

So $N = 1 + 5 - 2(\pi + \bar{\pi}) = 6 - 8 = -2$ $\square$.

$$\cdot \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$$

$$\text{Take } \pi = \frac{3+\sqrt{-7}}{2} \quad / \mathbb{F}_4$$

$$(N\pi = 4)$$

$$P \text{ gives } C/\mathbb{F}_4 \quad N = 1 + 4 - 2(\pi + \bar{\pi}) = 5 - 6 = -1.$$

$$\cdot \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

$$\pi = \frac{5+\sqrt{-3}}{2} \quad / \mathbb{F}_7$$

$$(N\pi = 7)$$

$$\text{get } C \text{ w/ } N = 1 + 7 - 2(5) = -2.$$



Now to construct P in the other cases:

Lemma: Let P be such a ~~module~~ module: $P \in \mathcal{P}$.
Let $e \in P$, primitive and with $e \cdot e = 2$.

Then either P is indec.

or $P \cong R \oplus R$ with hermit. form $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Pf: Suppose $P = Q_1 \oplus Q_2$, Q_i rk 1.

$$\text{Then } e = q_1 + q_2$$

$$2 = e \cdot e = q_1 \cdot q_1 + q_2 \cdot q_2$$

(orthog. decomp!)

$\therefore$ either $q_1 \cdot q_1 = q_2 \cdot q_2 = 1$ and then q_1, q_2 give 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 $\text{disc } Q_1 = 2$ and $\text{disc } P = \text{disc } Q_1 \cdot \text{disc } Q_2 \neq 1$.

$e \cdot (\lambda e + \mu) = 2\lambda$ is also a contradiction. $\square$

Lemma 2: Let e, P be as in Lemma 1, and $f \in P$ such that

$$\begin{cases} \text{a) } e \cdot f \notin \mathbb{Z} \\ \text{b) } \text{[scribbled out]} f \cdot f = z_1 \bar{z}_1 + z_2 \bar{z}_2 \text{ with } z_1, z_2 \in \mathbb{C} \end{cases}$$

$$\Downarrow$$

$$z_1, z_2 \in \mathbb{Z}.$$

Then P is indecomposable.

Pf: P dec $\rightarrow P = R \oplus R$ 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 $f \cdot f = z_1 \bar{z}_1 + z_2 \bar{z}_2 \rightarrow z_1, z_2 \in \mathbb{Z}$ by (b).

But $e \cdot f = z_1 + z_2 \in \mathbb{Z}$ contradicting (a). $\square$

Now it remains to write down some matrices
 $\begin{pmatrix} 2 & a \\ \bar{2} & \mu \end{pmatrix}$ 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, (for def. disc. 1) on $R = \mathbb{Q}[i]$, 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 $\begin{cases} \sqrt{-d}/4 & \text{if } d \equiv 0 \pmod{4} \\ \frac{1+\sqrt{-d}}{2} & \text{if } d \equiv 3 \pmod{4} \end{cases}$

We want to prove: if $d \neq 3, 4, 7 \Rightarrow \exists$ indec. binary hermitian form

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) $\exists f, g \in P$, s.t. $e \cdot f \notin \mathbb{Z}$ and $f \cdot g = z_1 \bar{z}_1 + z_2 \bar{z}_2$, $z_i \in R_d \Rightarrow z_i, \bar{z}_i \in \mathbb{Z} \Rightarrow P$ indec.

Cases

① $d \equiv 0 \pmod{8}$, $P = R \oplus R$

$$\alpha = 1 + \sqrt{-d/4}$$

so $\alpha \bar{\alpha} = d/4 + 1 \equiv 1 \pmod{2}$

so $\mu = \frac{1 + \alpha \bar{\alpha}}{2} = 1 + \frac{d}{8}$.

In cases ① - ③,
 $P = R \oplus R$, matrix
 in $\begin{pmatrix} 2 & \alpha \\ \bar{\alpha} & \mu \end{pmatrix}$ $e = (1, 0)$
 $f = (0, 1)$
 $2\mu - \alpha \bar{\alpha} = 1$

Then $e \cdot e = 2$, primitive

$$e \cdot f = \alpha \notin \mathbb{Z}$$

$$f \cdot f = \mu = 1 + \frac{d}{8}$$

$$N(x + y\sqrt{-d/4}) = x^2 + \frac{d}{4}y^2 \geq \frac{d}{4} \text{ if } y \neq 0$$

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 .

$$(2) \quad d \equiv 4 \pmod{8}$$

take $\left\{ \begin{array}{l} \alpha = \sqrt{\frac{-d}{4}} \\ \mu = \frac{1+\alpha\bar{\alpha}}{2} = \frac{1}{2} + \frac{d}{8} \end{array} \right.$ and check as before.

$$(3) \quad d \equiv 3 \pmod{8}$$

take $\left\{ \begin{array}{l} \alpha = \frac{1+\sqrt{-d}}{2} \\ \mu = \frac{5+d}{8} \end{array} \right.$, so $\alpha\bar{\alpha} = \frac{1+d}{4}$,
again as before.

$$[d+7]$$

$$(4) \quad d \equiv 7 \pmod{8}$$

This implies $h(-d) > 1$: $\mathbb{Q}$ splits as $\mathfrak{p}\bar{\mathfrak{p}}$, i.e. :

$$R_{-d} \otimes \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \quad (*)$$

(*) : if $x = \frac{1+\sqrt{-d}}{2}$, x satisfies $x^2 - x + \frac{1+d}{4} = 0$.

$$\text{Mod } 2: \quad x^2 - x \equiv 0 \pmod{2}$$

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 ^{irr.} ideal $\mathfrak{a}$, not principal (e.g., $\mathfrak{p}$).

Now take $P = R + \sigma\tau$ (not free).

A hermitian form on P is given by a matrix

$$\begin{pmatrix} \lambda & \alpha \\ \bar{\alpha} & \mu \end{pmatrix} \quad \left[\begin{array}{l} \lambda \in \mathbb{Z} \quad , \quad \alpha \in \frac{1}{N\sigma\tau} \sigma\tau \quad , \quad (\bar{\alpha} \in \frac{1}{N\sigma\tau} \bar{\sigma}\tau) \\ \mu \in \frac{1}{N\sigma\tau} \mathbb{Z} \end{array} \right]$$

$$\left[\begin{array}{l} \text{herm form is } \lambda z_1 \bar{z}_1 + \alpha \underbrace{z_1 \bar{z}_2}_{\in \sigma\tau} + \bar{\alpha} \bar{z}_1 z_2 + \mu z_2 \bar{z}_2 \\ \text{with } z_1 \in R, z_2 \in \sigma\tau \end{array} \right]$$

So if $\alpha \in \frac{1}{N\sigma\tau} \sigma\tau$, OK!

To check: form is $R \oplus \sigma\tau \longrightarrow R \oplus \bar{\sigma}\tau$, so get conditions

"det = 1" means $(\lambda\mu - \alpha\bar{\alpha})N\sigma\tau = 1$

Take $\lambda=2$ to have a vector of length 2.

Claim: $\exists \alpha \in \frac{1}{N\sigma\tau} \sigma\tau$, $\exists \mu \in \frac{1}{N\sigma\tau} \mathbb{Z}$ s.t. $(2\mu - \alpha\bar{\alpha})N\sigma\tau = 1$

Write $\alpha = \frac{1}{N\sigma\tau} z$, $z \in \sigma\tau$, $\mu = \frac{m}{N\sigma\tau}$, and then we want

$$2m - \frac{z\bar{z}}{N\sigma\tau} = 1.$$

So we want: $\exists z \in \sigma\tau$ s.t. $\frac{z\bar{z}}{N\sigma\tau} \equiv 1 \pmod{2}$.

Choose z a local generator at $\mathfrak{z}$ (since locally principal!).

Then by Lemma 1, we are done, since P is not free. $\square$

[For ternary hermit. forms, ^{bad rings} should be $d = -3, -4, -8, -11$; still] can't prove those are all the bad rings.

E ell. curve, $R = \text{End}(E)$

* We associated $A = P \otimes_R E$.

Then form indec $\implies A$ indec, pol. deg 1

For $g=2 \implies \underline{\text{curve}}$.

* 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 $\tau = \frac{-7 \pm \sqrt{-23}}{2}$ twice,
which corresponds to E with $R = R_{-3}$.
Then $\text{Jac}(C) \cong P \otimes E$ for some P
polariz on $\text{Jac} \rightarrow$ hermit. form on P , indec.
contradiction!

by what
we'll prove!

Assume: E ordinary, $R = \text{End } E$, 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 gd. field to $\underbrace{E \times \bar{E} \times \dots \times \bar{E}}_g$.

Thus: Then $A \cong P \otimes_R E$, with $P = \text{Hom}_R(E, A)$,
and P is projective.

Pf: A is isogenous to $L \otimes E$ L free R -module.

$A \longrightarrow L \otimes E$ isogeny.

primes dividing order of kernel?

a) $l \neq \text{char.}$

$$\text{Use } V_l(A) = V_l(L \otimes E)$$

$$\begin{array}{ccc} \cup & & \cup \\ T_l A & \hookrightarrow & T_l(L \otimes E) \end{array}$$

and $l \mid \text{order of kernel} \rightarrow$ lattices are different

View $L \subset K?$

$L \subset P \subset K^3$ corresponds to: for finitely many i

$$L \otimes R_i \subset P \otimes R_i$$

Same for $P \subset L \subset K^3$.

So choose $P \subset L$ s.t. $P_i = P \otimes R_i = T_i A$

Then we'll have $T_i A = T_i(P \otimes E)$ so OK at L .

Since we have A ordinary, it has a $T_p A$, free of rank $2g$ over $\mathbb{Z}_p$.

$$T_p A = (\text{naïve } T_p) \oplus (\mathbb{Z}_p\text{-dual of } T_p^{\vee}) (\text{dual of } A)$$

$$T_p^{(1)}(A) \cong \underbrace{\varprojlim A[p^n]}_{\text{rk } g}$$

One proves that this $T_p A$ satisfies the same formalism as before.

[For general A , must add $\oplus$ piece coming from Witt-vectors cohomology]

Note: for ordinary E , $R_p = \mathbb{Z}_p \oplus \mathbb{Z}_p$

This gives a proof. $\square$

Skooleu Method

We needed to consider
$$\beta^n = \begin{cases} x^2 + 1 \\ x^2 + x + 1 \\ x^2 + x + 2 \end{cases}$$

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

$$\begin{cases} y^n = x^2 + 1 \\ y^n = x^2 + x + 1 \\ 2^n = x^2 + x + 2 \end{cases} \quad \begin{cases} y > 1 \\ n \text{ odd } \geq 3 \end{cases}$$

Claim: no other solutions than listed above.

- | | |
|--|---|
| ① $y^n = x^2 + 1$: Lebesgue | } Cf. Mordell, <u>Diophantine Equations</u> .
(Proofs for ① + ③, refs. for ②.) |
| ② $y^n = x^2 + x + 1$: Nagel + Ljunggren | |
| ③ $2^n = x^2 + x + 2$: Nagel ₁₂₁ | |

②: Nagel: $y^n = x^2 + x + 1 \Rightarrow n \equiv 0 \pmod{3}$ (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. Number Th.
18 (1984)

We give a proof for case ③: $2^n = x^2 + x + 2$.

$$\begin{aligned} \text{Note: } 4 \cdot 2^n &= 4x^2 + 4x + 1 + 7 \\ &= (2x+1)^2 + 7 \end{aligned}$$

$$\text{So work in } \mathbb{R}_{-7}, \text{ set } \omega = \frac{1+\sqrt{-7}}{2}, \text{ so } \begin{cases} \omega + \bar{\omega} = 1 \\ \omega \bar{\omega} = 2 \end{cases}$$

(So $\omega^2 - \omega + 2 = 0$).

$$\text{And our equation is } \boxed{\omega^n \bar{\omega}^n = (x+\omega)(x+\bar{\omega})}$$

Can replace x by $-1-x$, so choose x even.

Se 62

$$(\omega) = 8, \quad 2 = 8\bar{8}.$$

So we must have $x + \omega = 8^i \bar{8}^j \quad i+j=n$

And $2 \nmid x + \omega$. If $i, j \geq 1$, $x + \omega$ div by $8\bar{8} = 2$; no!

$$\text{So } x + \omega = \pm \omega^n \text{ or } \pm \bar{\omega}^n$$

x -even $\Rightarrow x + \omega = \pm \bar{\omega}^n$ is impossible.

$$\text{So } x + \omega = \pm \omega^n$$

$$\text{Now } \omega^n - \bar{\omega}^n = \pm (\omega - \bar{\omega})$$

sign is - :

$$\text{in } R/\omega^2 R = \mathbb{Z}/4\mathbb{Z}$$

$$\bar{\omega} \longrightarrow -1$$

$$\omega \longrightarrow 2$$

$$\omega^2 \longrightarrow 0$$

So image of eqn is

$$0 - (-1)^n = \pm (2 + 1)$$

$$n \text{ odd : } 1 = \pm (2 + 1)$$

so have - .

$$\text{So } \omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$$

$$\text{So } \boxed{\omega^n = -x - \omega}$$

$$\text{In } R = \mathbb{Z} + \mathbb{Z}\omega$$

$$\omega^n = a_n + b_n \omega$$

Question is: do we get $b_n = -1$?

We do for $n=3, 5, 13$. Claim: no others.

Skolem's method:

Look at $\omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$ as an eqn for n , and interpret p -adically.

[Works for $p=29, 37, 43, 71, 79, 109, 191, \dots$]

↳ We take $p=7$, but ↗

Take $K = \mathbb{Q}(\sqrt{-7})$, $\hat{K}$ = completion at the prime 7

$$v: \hat{K}^* \longrightarrow \mathbb{Z}$$

$$\pi = \sqrt{-7}, \quad v(\pi) = 1 \\ v(7) = 2, \quad \text{so } e = 2.$$

We want to think of the eqn. with $n \in \mathbb{Z}_7$, if possible.

$\omega \in U_{\hat{K}}$, but is not $\equiv 1 \pmod{\pi}$

Residue field is $\mathbb{F}_7^*$, and ω has order 6.

So we must work with $n \pmod{6}$.

Cases: $\begin{cases} n \equiv 1 \pmod{6} \\ n \equiv 3 \pmod{6} \\ n \equiv 5 \pmod{6} \end{cases}$

[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 $\omega^6 \equiv 1 \pmod{\pi}$

$$\omega = \frac{1+\pi}{2}, \text{ so } \alpha = \omega^6 = \frac{(1+\pi)^6}{2^6} = \frac{1+6\pi+\dots}{2^6}$$

$$\pmod{7}, \quad 2^6 \equiv 1, \quad 6 \equiv -1$$

$$\text{So get } \alpha \equiv 1 - \pi \pmod{\pi^2}$$

(note $7 \sim \pi^2$)

So our equation is $\boxed{\omega^{n_0} \alpha^t - \bar{\omega}^{n_0} \alpha^t = -(\omega - \bar{\omega})}$

Now take $t \in \mathbb{Z}_7$ $f(t)$ analytic.

We want to solve $f(t) = \text{const.}$

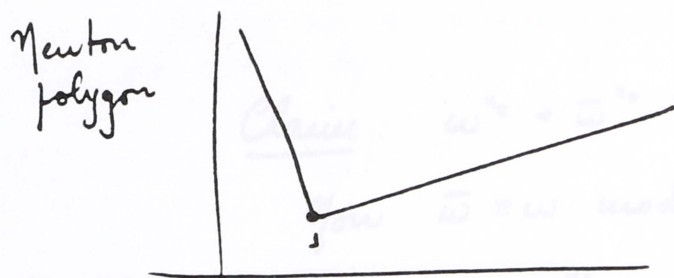
$\therefore$ only finitely many solutions.

So expand $f(t)$ in a power-series

$$f(t) = a_0 + a_1 t + a_2 t^2 + \dots \quad v(a_0) \geq 0$$

if we can show $v(a_1) = 1$, $v(a_n) \geq 2$ for $n \geq 2$

then we have at most one solution.



Or: know one solution, so choose u_0 s.t. $a_0 = 0$;
divide by t

$$f(t) = t \left(1 + \underbrace{\dots}_{v(\dots) \geq 0} \right)$$

$$\alpha^t = e^{t \log \alpha} \quad , \quad \text{so} \quad a_n = \omega^{n_0} \cdot \frac{(\log \alpha)^n}{n!} - \bar{\omega}^{n_0} \frac{(\log \bar{\alpha})^n}{n!}$$

$$\alpha = 1 - \pi \text{ mod } \pi^2$$

$$\therefore \log(\alpha) = -\pi \text{ mod } \pi^2 \quad \text{so} \quad v(\log \alpha) = v(\log \bar{\alpha}) = 1.$$

$$\text{So } v(a_1) \geq 1, \quad v(a_2) \geq 2, \dots, \quad v(a_6) \geq 6$$

For $n=7$ $v(a_7) \geq 7-2 = 5$, etc.

So $v(a_n) \geq 2$, $n \geq 2$

So only thing to check is $v(a_1) = 1$ (i.e., no cancellations).

$$\begin{aligned} a_1 &= \omega^{n_0}(-\pi) + \bar{\omega}^{n_0}(\bar{\pi}) \pmod{\pi^2} & \bar{\pi} &= -\pi \\ &= -\pi(\omega^{n_0} + \bar{\omega}^{n_0}) \pmod{\pi^2} \end{aligned}$$

Claim: $\omega^{n_0} + \bar{\omega}^{n_0} \not\equiv 0 \pmod{\pi}$

Now $\bar{\omega} \equiv \omega \pmod{\pi}$

So $\omega^{n_0} + \bar{\omega}^{n_0} \equiv 2\omega^{n_0} \pmod{\pi}$, done!

Remarks: * 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

$$\omega^n - \bar{\omega}^n = (\text{unit})^n (\omega - \bar{\omega})$$

and then we'd need more equations.

Other primes: take p , $(\frac{p}{7}) = 1$.

* We need, mod p , $\omega^n - \bar{\omega}^n = -(\omega - \bar{\omega})$ only for 3, 5, 13

* need $v(a_1) = 1$

(eg., 23 works for first *, not for second.)

12/5 $g=3$ — see table of (g, N) (p. Se 64b)

Voloch's bound (for $g=3$)

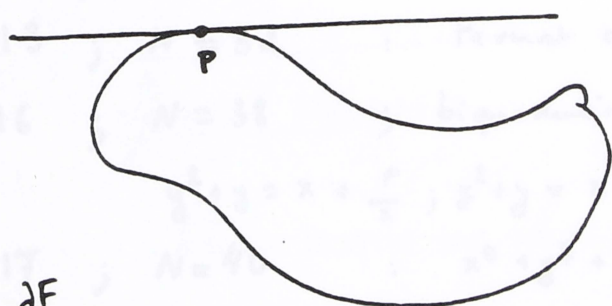
$$N \leq 2g + 6, \text{ except for "special cases"}$$

Assume not hyperelliptic (if hyperelliptic, $N \leq 2g+2$).

$\therefore$ curve is a nonsingular quartic in plane,
so given by

$$F(x, y) = 0$$

$$\text{or } F_4(x, y, z) = 0$$



$$F'_x = \frac{\partial F}{\partial x}$$

Write equation

"Frob of $P \in \text{tgt at } P$ "

in homog. coords:

$$G = x^9 F'_x + y^9 F'_y + z^9 F'_z = 0$$

"Special" if F divides G (i.e., $\text{Frob } P \in \text{tgt at } P$ 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 rational point, it clearly is in the intersection; moreover, the two curves are tangent at such a point, so each rat'l point counts at least twice.

$$\boxed{g=3}$$

Maximum number of points

$$\underline{2g+6}$$

$q=2$	$N=7$	: twisted Klein curve, $\Sigma x^4 + \Sigma x^2 y^2 + z^2 y z + x y^2 z = 0$	
$q=3$	$N=10$	: $y^3 - y = x^4 - x^2$	
$q=4$	$N=14$	: Klein curve $\Sigma x^4 + \Sigma x^2 y^2 + \Sigma x^2 y z = 0$	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	24
$q=9$	$N=28$	: Klein curve = Fermat curve $(x^4 + y^4 + z^4 = 0)$	28
$q=11$	$N=28$	: $x^4 + y^4 + z^4 + 2(3x^2 y^2 + 4y^2 z^2 + 4z^2 x^2) = 0$	32
$q=13$	$N=32$	: Fermat curve	38
$q=16$	$N=38$	: bi-quadratic extension of $\mathbb{F}_{16}(z)$ defined by $y^2 + y = x + \frac{p}{x}$; $y^2 + y = x + \frac{p^2}{1+x}$ where $p \in \mathbb{F}_4 - \mathbb{F}_2$	40
$q=17$	$N=40$	: $x^4 + y^4 + z^4 + 4y^2 z^2 = 0$	44
$q=19$	$N=44$		
$q=23$	$N=48$	: $x^4 + y^4 + z^4 - 5(x^2 y^2 + y^2 z^2 + z^2 x^2) = 0$	
$q=25$	$N=56$	: Klein curve	
$q=27$	$N=?$		
$q=29$	$N=?$		
?			
?			

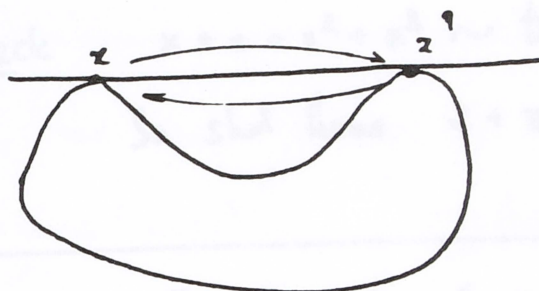
Voloch's bound.

(This list is not entirely guaranteed...)

J-P.S.

Therefore $N \leq 2(q+3) = 2q+6$.

Example:



x of deg 2
on a tangent
then $z \in \text{intersection}$

Similarly, could have a triangle.

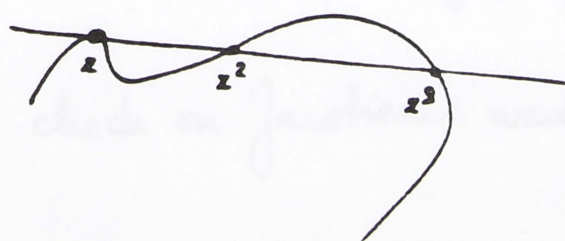
Special curves:

Klein curve in char. 2 / $\mathbb{F}_2$ or $\mathbb{F}_4$

$$Sx^4 + Sx^2y^2 + Sx^2yz = 0$$

$$\left\{ \begin{array}{l} Sx^4 = x^4 + y^4 + z^4, \\ \text{etc.} \end{array} \right.$$

Check:



for any x

Can write the polynomial as

(and then it's obvious that z, z^2, z^3
are collinear)

$$\frac{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^3 & y^3 & z^3 \end{vmatrix}}{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^4 & y^4 & z^4 \end{vmatrix}}$$

Eqn of tgt at ~~some~~ (x, y, z) is:

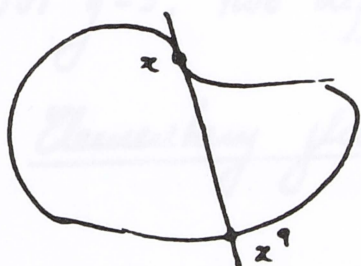
$$x \begin{vmatrix} y^2 & z^2 \\ y^8 & z^8 \end{vmatrix} + y \cdot \begin{vmatrix} x^2 & z^2 \\ x^8 & z^8 \end{vmatrix} + z \cdot \begin{vmatrix} x^2 & y^2 \\ x^8 & y^8 \end{vmatrix} = 0$$

Another check $x + x + x^2 + x^8 \sim$ trivial divisor

So shd have $2 + \pi + \pi^8 = 0$ on Jac.

Klein curve over $\mathbb{F}_3$ is special over $\mathbb{F}_9$.

Fermat $x^9 + y^9 = z^9$



Then: every tgt is inflection tangent, and other inflex is x^9 .

Write equations to check.

Tangent is $Xx^3 + Yy^3 + Zz^3 = 0$

at z^9 :

$$x^{12} + y^{12} + z^{12} \stackrel{?}{=} 0,$$

$$\text{yes since this is } (z^9 + y^9 + z^9)^3 = 0$$

(char 3!)

On check on Jacobian: want $3 + \pi_g = 0$

$$\pi_g = -3, \text{ which is true.}$$

This is why Voloch's bound fails at 8, 9.

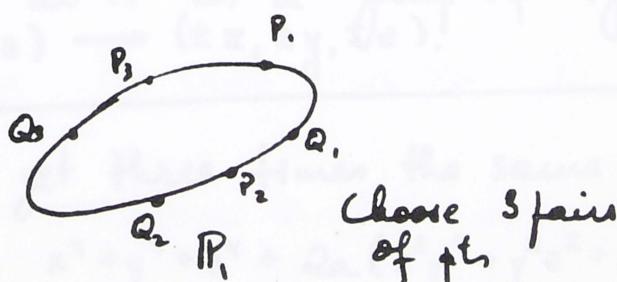
Can prove $\text{char} \geq 5 \Rightarrow$ non-special

Guess: these are the only special curves.

For $g=2$, we used gluing of elliptic curves, either
 { direct method "2-gluing"
 or
 hermitian forms

For $g=3$, two difficulties:

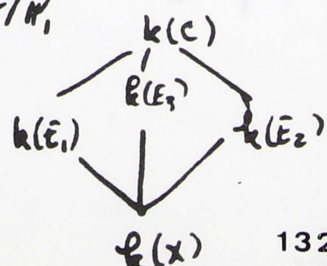
Elementary gluing



Make E_1/P_1 ramified at P_2, Q_2, P_3, Q_3

E_2/P_1 " " P_1, Q_1, P_3, Q_3

Get:



E_3 ramified only at P_1, Q_1, P_2, Q_2

So get C of genus 3, $\text{Jac}(C) \sim E_1 \times E_2 \times E_3$

Consider $\boxed{ax^4 + by^4 + cz^4 + dx^2y^2 + ey^2z^2 + fz^2x^2 = 0}$

Assume $\Delta \neq 0$

Set $z=1$: $ax^4 + by^4 + c + dx^2y^2 + ey^2 + fx^2 = 0$

Let $Y = y^2$

$ax^4 + bY^2 + c + dx^2Y + eY + fx^2 = 0$

$\downarrow$

$Y^2 = \lambda x^4 + \mu x^2 + \nu$

which is an elliptic curve.

doing w/ each variable, get 3 curves.

On look at it as a group of type (2,2) acting by $(x,y,z) \rightarrow (\pm x, \pm y, \pm z)$.

E.g., to get three times the same curve E , we find $x^4 + y^4 + z^4 + 2a(x^2y^2 + y^2z^2 + z^2x^2) = 0$

So choose a to get the curve E .

E.g. for 11, 17 2 of one kind, 1 different
for 23 3 of the same

For $g=23$

Voloch bound doesn't work. (gives 52)

$$m = \lfloor 2\sqrt{23} \rfloor = \lfloor \sqrt{92} \rfloor = 9$$

$$m^2 - 4g = -11.$$

$$\text{Weil gives } N \leq 1 + g + 3m = 51$$

This is impossible:

$N=51$ only if $\text{Jac} \sim E \times \bar{E} \times E$ with $m=9$,
so Frob should be $\pi = \frac{-9 \pm \sqrt{-11}}{2}$.

$$\text{So } R = \text{End}(E) = \mathbb{Z}[\pi] = R_{-11}.$$

$\therefore \text{Jac} \cong E \times E \times E$ + polariz. $\longleftrightarrow$ indec. hermit. form as before, of rk 3.

Kneuer: No such form over R_{-11} .

$1+g+3m-1 \rightarrow$ down by 1 is impossible for $g=3$

$1+g+3m-2 = 49$ pts? down by 2, genus 3

only case is $m, m, m-2$

that would mean $\text{Jac} \sim E \times \bar{E} \times E'$

$$| E \sim | \pi = \frac{-9 \pm \sqrt{-11}}{2}$$

$$| E' \sim | \pi' = \frac{-7 \pm \sqrt{-43}}{2}$$

Claim: no such thing exists.

(Problem: Jac is only isogenous to $E \times E \times E'$).

$$\text{Let } \varphi = F + V = \pi + \bar{\pi}$$

$$J_9 = \text{conn comp of Ker}(\varphi + 9)$$

$$J_7 = \text{Ker}(\varphi + 7)$$

$$J_9 \cong E \times E \quad \text{isomorphic}$$

$$J_7 \cong E'$$

$$J_9 \cap J_7 \quad \text{killed by 2}$$

$$S_0 \quad J = J_9 \times J_7 / \Delta \quad \Delta \subset E'[2]$$

so Δ of type 1, (2) or (2, 2)

$$1 \rightarrow \text{Jac} = \text{product} \rightarrow \text{polariz. splits} \rightarrow \text{No.}$$

$$(2) \rightarrow \text{also can't be}$$

$$(2, 2)$$

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_9 .

J_9 has CM by R_{11} , so want

$$\begin{pmatrix} \lambda & \alpha \\ \bar{\alpha} & \mu \end{pmatrix} \left\{ \begin{array}{l} \lambda\mu - \alpha\bar{\alpha} = 2 \\ \lambda > 0 \\ \text{coeff} \in R_{11} \end{array} \right.$$

Theorem: only case is $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

But then J_9 splits: $J = E \times E \times E'/\Delta$, and the whole J splits, which is not possible. $\square$

9=19 Voloch bound gives 44.

$$\begin{cases} m = [2\sqrt{19}] = [\sqrt{76}] = 8 \\ m^2 - 4q = -12 \end{cases}$$

$$1 + 9 + 3 \cdot 8 = 44$$

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 $\sqrt[n]{R} = \mathbb{Z}[\sqrt[n]{3}] \subseteq \text{max.}$

Form is $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1+\sqrt{3} \\ 1 & 1-\sqrt{3} & 3 \end{pmatrix}$ on $R \oplus R \oplus R$.

To show indec., go to $\tilde{R} = \mathbb{Z}[\frac{1+\sqrt{3}}{2}]$. 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 $A = P \otimes_R E$.

Use:

Thm (Oort +):

A principally polarized 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. $\text{Jac } C \cong A/k$

2) If C not hyperelliptic, then $\exists C/k$ unique + a quad twist $\epsilon: \text{Gal}(E/k) \rightarrow \pm 1$ s.t. $\text{Jac } C \cong A(\text{twisted by } \epsilon)$.

over a finite field, Frob of C is either $\begin{cases} \text{Frob of } A \\ \text{or} \\ -\text{Frob of } A \end{cases}$

or put $\varphi = c \prod_{36} g$.
 Suppose $c=1$; then φ "is" the twist.

Reformulation:

the twist A_E (A twisted by E) can be written

$$A_E = P \otimes E_E$$

Start with P ; look at all E_E deduced from E by a quad. twist.

Then P determines a well-defined E_E among all those, the unique one s.t. $P \otimes E_E = \text{Jac}(C)$.

Example for Gross:

E w/ CM by $\frac{1+\sqrt{-7}}{2}$ ($j = -3^3 5^3$)

Look for P over this R :

$$P \text{ given by } \begin{pmatrix} 2 & \alpha & \bar{\alpha} \\ \bar{\alpha} & 2 & -1 \\ \alpha & -1 & 2 \end{pmatrix}, \quad \alpha = \frac{1+\sqrt{-7}}{2}$$

Automorphism = $\{\pm 1\} \times \widetilde{G_{168}}$ / $\mathbb{Q}(\sqrt{-7})$
simple of order 168

$$P \otimes E = \text{Jac}(\text{Klein})$$

So curve will have either 44 or $1+19-38 = -4$ points, so it has 44 pts.

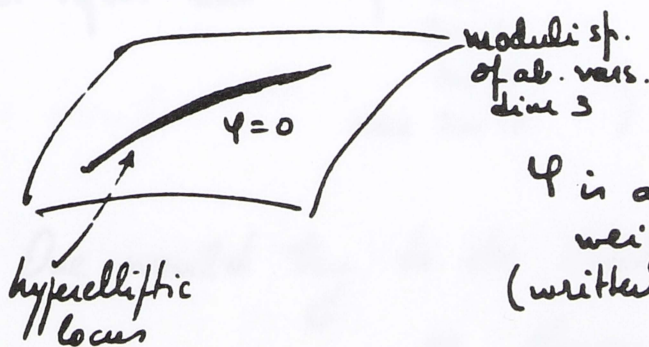
So E ell. curve, $R = \text{End}(E)$, take P hermitian module as usual.

Make $A = E \otimes_R P$

Cont + - = this is a jacobian.

① Is C hyperelliptic?

Given g_2, g_3 (P hermitian module) $\longrightarrow$ hyperelliptic?



ψ is a mod form on Siegel space weight 18 (written in Igusa on genus 3)

mod form on Siegel space (dim 3) $\Big|_{\text{CM} \otimes_R \text{hermitian modules}} = ?$

② If C not hyperelliptic ($\psi \neq 0$), find $E = \sqrt{\psi}$.

Igusa says: Klein noticed: take Δ of a plane quartic

Check $\frac{\Delta^2}{9} = c \cdot \frac{\psi}{18}$

$\psi = \frac{11}{36} \Delta$

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 $N_g(3) = \max$ nber of points for $g=3$ over $\mathbb{F}_q$.

Conjecture: $|N_g(3) - \text{Weil bound}|$ is bounded when
 q varies. (say $q \leq 6$)

(For $N_g(2)$ had
$$\begin{array}{c} 1+q+2m \\ 2m-1 \\ 2m-2 \\ \text{once } 2m-3 \end{array} \right).$$

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, $R = R_{-d}$.

$$d = 4q - (m-1)^2$$

$$4q \geq m^2 \quad \text{so} \quad d \geq 2m-1$$

So look at indec. herm. modules of rk 3 on R_{-d} .
 Number of such goes to ∞ like d^2 , d large.

$$d \gg g^{1/4}$$

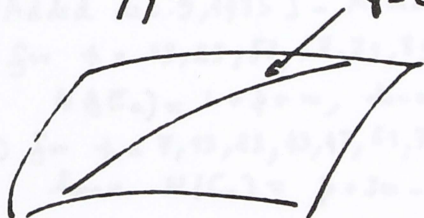
For each such hermit. module, should compute the sign.

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 $\frac{1}{g}$. But then quad twist, so chance is $\frac{1}{2g}$ of winning.

But number of P is large.

For very large q , say $q=100$, jacobians have too large a codimension.

So expect a breaking point between 3 + 10.

For $q=3$, using $x^4 + y^4 + z^4 + 2a(x^2y^2 + y^2z^2 + z^2x^2) = 0$. (C)

this has $\text{Jac} \sim E_x \times E_y \times E_z$, $E_x: y^2 = (a^2 - 1)x^2 + \dots$

Question: 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

$$N(E_a) = 1 + p + m, \text{ hence } N(C_a) = 1 + p + 3m : \text{optimal bound!}$$

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"

Harvard, 1985

Contents - Part II

General Results

RATIONAL POINTS ON CURVES OVER FINITE FIELDS

PART II : "g LARGE"

Jean-Pierre Serre

Class Field Towers

The Theorems of Galois and Shafarevich
Infinite class field towers
Constructions in characteristic $p \neq 2$
Constructions for $q = 2$
Something from Class Field Theory

Optimal bounds from the explicit formula

The optimisation problem and its
Ostrowski's Theorem

The case $q = 2$

Bounds
Construction of curves

Lectures given at Harvard
University, September to
December 1985

Notes by Fernando Q. Gouvêa

Contents - Part II

General Results

Se Th 1

The bound $g \leq \frac{1}{2}(q - q^{1/2})$
When is the Weil bound attained?
Explicit formula and applications
Asymptotic results as $g \rightarrow \infty$
Ihara's theorem on towers
Modular Curves and the case $q = p^2$

Se Th 1
Se Th 2
Se Th 3
Se Th 8a
Se Th 10
Se Th 11

Class Field Towers

Se Th 14

The Theorem of Golod and Šafarevič
Infinite class field towers
Constructions in characteristic $p \neq 2$
Constructions for $q = 2$
Something from Class Field Theory

Se Th 14
Se Th 17
Se Th 20a
Se Th 24a
Se Th 26c

Optimal bounds from the explicit formula

Se Th 29

The optimization problem and its dual
Oesterle's Theorem

Se Th 29
Se Th 32

The case $q = 2$

Se Th 38

Bounds
Construction of curves

Se Th 38
Se Th 40.

9/26 Thursday: g large.

Ihara: X genus g / $\mathbb{F}_q$, $g \geq 1$

Suppose $N(X) = q + 1 + 2gq^{1/2}$ (so q is a square).

Then: $g \leq \frac{1}{2}(q - q^{1/2})$

Proof: $N(X) = 1 + q - \sum_{\alpha=1}^{2g} \pi_\alpha$ $|\pi_\alpha| = q^{1/2}$

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 $1 + q^2 - 2gq \geq 1 + q + 2gq^{1/2}$

$$q^2 - q \geq 2g(q + q^{1/2})$$

$$\text{so } g \leq \frac{1}{2}(q - q^{1/2}) \quad \square$$

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 $N = q^{3/2} + 1 = q + 1 + 2gq^{1/2}$.

So the bound above is exact.

Proof of $N = q^{3/2} + 1$ for this curve.

Consider
$$\begin{array}{c} \mathbb{F}_q \\ 2 \mid \\ \mathbb{F}_{q^{1/2}} \end{array} \quad x \mapsto \bar{x} = x^{q^{1/2}}$$

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

$x\bar{x} = -(\underbrace{y\bar{y} + z\bar{z}}_{\in \mathbb{F}_{q^{1/2}}})$ has (in x) $\left\{ \begin{array}{l} 1 \text{ soln. } x=0 \text{ if } y\bar{y} + z\bar{z} = 0 \\ q_0 + 1 \text{ solns if not} \end{array} \right.$

$q_0 = q^{1/2}$

$$\begin{array}{ccc} \mathbb{F}_q & \xrightarrow{N} & \mathbb{F}_{q^{1/2}} \\ x & \mapsto & x\bar{x} \end{array}$$

$y\bar{y} + z\bar{z} = 0 \rightarrow \left\{ \begin{array}{l} y=0=z \\ \text{or} \\ z \neq 0, q_0 + 1 \text{ solns} \\ \text{(in } y \text{).} \end{array} \right.$

so $1 + (q_0^2 - 1)(q_0 + 1)$ solns

So solns in $\mathbb{F}_q^3$ is $1 + \underbrace{(q_0^2 - 1)(q_0 + 1) + (q_0 + 1)(q_0^4 - 1 - (q_0^2 - 1)(q_0 + 1))}_{\text{this}}$

so $N = \frac{(q_0^2 - 1)(q_0 + 1) + (q_0 + 1)(q_0^4 - 1 - (q_0^2 - 1)(q_0 + 1))}{(q_0^2 - 1)} = \frac{(q_0 + 1)(q_0^2 + 1 - q_0 + 1)}{(q_0^2 - 1)} = (q_0 + 1)(q_0^2 - q_0 + 1)$
 $\uparrow$
 in $\mathbb{P}^3$! $= q_0^3 + 1 \quad \square$

		group acts	
	$g=0$, $q+1$ pts, $\mathbb{P}^1$, $PG L_2$	(type A_1)	
	$g=\frac{1}{2}(q-q^{1/2})$, $q^{3/2}+1$, Fermat-type curve, PU_3	(type A_2^2) ($A_2^?$)	
can add	q^2+1	S_2	2B_2
	q^3+1	Rec	2G_2

When is the Weil bound attained?

g 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 $0 \leq g \leq \frac{1}{2}(q - q^{1/2})$?

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 $q^{1/2}=3$, set $x^4+y^4+z^4=0$, $g=3$.

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 $g=0 \rightarrow 10$ points, so $N \leq 20$.

(In fact, correct bd is 20).

$$3) g=16, g^{1/2}=4 \quad x^5+y^5+z^5=0.$$

$$\text{Weil bound is } 1+16+2g \cdot 4 = 17+8g$$

$$g=1 \rightarrow 25 \text{ OK}$$

$$g=2 \rightarrow 33 \text{ OK}$$

} see table

$$g=3 \rightarrow 41 \text{ not the bound (bound is 38).}$$

$$g=4, 5 ?$$

$$g=6 \rightarrow \text{yes, and the last one.}$$

Suppose X has Weil upper bound $= N(X)$ (or Weil lower bound).

And suppose

$$\begin{array}{c} X \\ \downarrow \text{non-const. morphism} \\ X' \end{array}$$

Then same holds for X' .

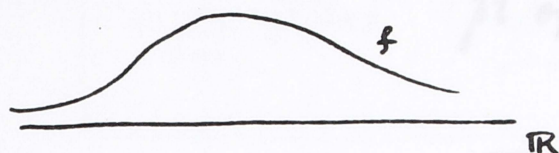
Think of Jac's. In X , every eigenvalue is $-g^{1/2}$ or $g^{1/2}$

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!

finite ker?

Explicit Formulas

Number Fields



and take $\sum f(\log p)$

And we want a formula: $\sum f(\log p) = - \sum_{\substack{\tau \text{ zero} \\ \text{of } \phi}} \phi(\tau) + \phi(0) + \phi(1)$

ϕ = Fourier Mellin transform of f

Stark: * includes $\log d$, and choose f, ϕ well

Get inequality for $d \rightarrow$ Stark, Odlyzko, Poitou.

Notations

X, q, q, π_α eigenvalues of Frob arranged as $\pi_1, \dots, \pi_g, \bar{\pi}_1, \dots, \bar{\pi}_g$

$$\pi_\alpha = q^{1/2} e^{i\varphi_\alpha}, \quad 0 \leq \varphi_\alpha \leq \pi$$

$$\begin{aligned} N_n &= \# X(\mathbb{F}_{q^n}) = 1 + q^n - \sum_{\alpha=1}^g (\pi_\alpha^n + \bar{\pi}_\alpha^n) \\ &= 1 + q^n - 2 \sum_{\alpha=1}^g q^{n/2} \cos n\varphi_\alpha \end{aligned}$$

$Z(T) =$ zeta-fct of X

$$= \exp \left\{ \sum_1^\infty \frac{N_n T^n}{n} \right\} = \frac{P(T)}{(1-T)(1-qT)}$$

where

$$P(T) = \prod_{\alpha=1}^g (1 - \pi_\alpha T)(1 - \bar{\pi}_\alpha T)$$

$$a_1 = N_1 = N$$

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 $X(\overline{\mathbb{F}_q})$.

$$\text{Have } N_n = \sum_{d|n} d a_d \quad (\text{clear!})$$

$$\text{And } Z(T) = \prod_{\substack{P \in X \\ \text{closed pt}}} \frac{1}{1 - T^{\deg P}}$$

$$= \prod_{d \geq 1} \frac{1}{(1 - T^d)^{a_d}}$$

Let $f(\theta)$ be a trigonometric polynomial of the form

$$f(\theta) = 1 + 2 \sum_{n \geq 1} c_n \cos n\theta \quad (\text{finite sum}).$$

$$= \sum_{n \in \mathbb{Z}} c_n e^{in\theta} \quad (c_0 = 1, c_{-n} = c_n).$$

To f I attach polynomials in t :

$$\psi_i(t) = \sum_{\substack{n \geq 1 \\ d|n}} c_n t^n$$

$$\psi(t) = \psi_i(t) = \sum_{n \geq 1} c_n t^n.$$

"Explicit formula"

$$\sum_{\alpha=1}^g f(\psi_\alpha) + \sum_{d \geq 1} da_d \psi_d(q^{-1/2}) = g + \psi(q^{-1/2}) + \psi(q^{1/2})$$

$$\sum_{\alpha=1}^g f(\psi_\alpha) = g + 2 \sum_{n, \alpha} c_n \cos n \psi_\alpha$$

$$= g + 2 \sum_n c_n \sum_\alpha \cos n \psi_\alpha$$

$$N_n = q^{n+1} - q^{n/2} \sum 2 \cos n \psi_\alpha$$

$$\text{so } \sum 2 \cos n \psi_\alpha = \frac{q^{n+1} - N_n}{q^{n/2}}$$

$$= g + \sum_{n \geq 1} c_n \underbrace{(q^{n/2} + q^{-n/2})}_{\psi(q^{1/2}) + \psi(q^{-1/2})} - q^{-n/2} N_n$$

Need only show that

$$\sum da_d \psi_d(q^{-1/2}) \stackrel{?}{=} \sum c_n q^{-n/2} N_n$$

$$\sum da_d \sum_{d|n} c_n q^{-n/2} \stackrel{?}{=} \sum c_n q^{-n/2} \sum_{d|n} da_d$$

no OK.



Examples:

i) $f=1$: $c_n=0$ $n \geq 1$, $\psi_d=0$

Get $g=g$.

ii) $f=1+\cos \theta$ $c_1=\frac{1}{2}$, $c_n=0$ $n \geq 2$.

$\psi_1=\psi=\frac{1}{2}t$

$\psi_n=0$ $n \geq 2$

Then:

$$g + \sum_{\alpha} \cos \psi_{\alpha} + N \frac{1}{2} g^{-1/2} = g + \frac{1}{2} g^{-1/2} + \frac{1}{2} g^{1/2}$$

$\times 2g^{1/2}$:

$$g^{1/2} \sum_{\alpha} 2 \cos \psi_{\alpha} + N = 1 + g$$

so $\boxed{N = g + 1 - g^{1/2} \sum_{\alpha} 2 \cos \psi_{\alpha}}$

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 $f \gg 0$,

$$\sum_{a \geq 0} f(\psi_a) + \sum_{d \geq 1} d a_d \underbrace{\psi_d}_{\geq 0}(\quad)$$

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 $N \psi(q^{-1/2}) \leq g + \psi(q^{-1/2}) + \psi(q^{1/2})$

$$\text{so } \boxed{N-1 \leq \frac{g + \psi(q^{1/2})}{\psi(q^{-1/2})}}$$

Now: we want to choose f so that this is optimal.

Also get

$$\boxed{g \geq (N-1) \psi(q^{-1/2}) - \psi(q^{1/2})}$$

One can then do:

- ① determine (for a given N, q), the "best" bound on g .
Solved by Deserle (at least for $q \geq 3$)

- ② Asymptotic results as $g \rightarrow \infty$, 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

$$N=q+1 \quad g=0$$

$$N=q^{3/2}+1 \quad g = \frac{1}{2}(g - q^{1/2}) \text{ } q \text{ a square}$$

For $N=q^2+1$

$$\text{Choose } f = 1 + \sqrt{2} \cos \theta + \frac{1}{2} \cos 2\theta$$

$$= \frac{1}{2} (1 + \sqrt{2} \cos \theta)^2$$

Then $f \gg 0$.

$$\text{Then } \begin{cases} \psi(t) = \frac{1}{2}(\sqrt{2}t + \frac{1}{2}t^2) \\ \psi_2(t) = \frac{1}{4}t^2 \end{cases}$$

$$N-1 = q^2$$

$$\text{Find } g \geq \left[q^2 \left(\sqrt{2} q^{-1/2} + \frac{1}{2} q^{-1} \right) - \left(\sqrt{2} q^{1/2} + \frac{1}{2} q \right) \right]^{1/2}$$

$$\text{so } \boxed{g \geq \frac{\sqrt{2}}{2} (q^{3/2} - q^{1/2})}$$

Is there such a curve?

$$q \stackrel{?}{=} \frac{\sqrt{2}}{2} (q^{3/2} - q^{1/2}) = (2q)^{1/2} (q - 1) \Rightarrow q = 2^{2f+1}$$

$\Rightarrow 2q = \text{square}$

$\leftrightarrow$ Suzuki groups?

Deligne-Lusztig varieties connected to semi-simple groups over $\mathbb{F}_q$ and their twisted forms.

$S_2 \leftrightarrow {}^2B_2$ - groups

Take, say, SL_n and Frobenius $x \mapsto x^{(q)}$

fixed pts give $SL_n(\mathbb{F}_q)$

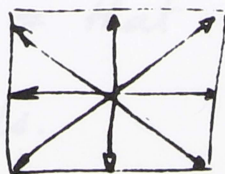
Now use $x \mapsto \sigma(x^{(q)})$

σ some outer autom. of the group.

If σ is $u \mapsto {}^t u$, get a different group.

char=2, B_2 has such a "bad" autom. (not algebraic)

Root system is



(See Tits in Sem. Bourbaki)

Suzuki grps are grps acting on q^2+1 elements, $q=2^{2f+1}$
 Simple if $f \geq 1$. Called $Sz(q)$.

$$Sz(2) = C_4 \cdot C_5$$

$Sz(3)$ 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

$$f = \cos^2 \varphi \left(1 + \frac{2}{\sqrt{3}} \cos \varphi\right)^2 \quad g \geq \frac{\sqrt{3}}{2} (q^{5/2} - q^{1/2}) + \frac{1}{2} (q^2 - 1)$$

g integer, = that $\Rightarrow f = 3^{2f+1}$

Have Ree groups.

We had:

10/3 X curve $/\mathbb{F}_q$, $\pi_\alpha = q^{1/2} e^{i\psi_\alpha}$

genus g

$$f(\theta) = 1 + \sum_{n \geq 1} 2c_n \cos n\theta \quad (\text{finite sum})$$

$$\Psi_d(t) = \sum_{\substack{n \geq 1 \\ n \equiv 0 \pmod{d}}} c_n t^n, \quad \Psi = \Psi_1$$

Then
$$\sum_{\alpha=1}^g f(\psi_\alpha) + \sum_{d \geq 1} d a_d \Psi_d(q^{-1/2}) = g + \Psi(q^{-1/2}) + \Psi(q^{1/2})$$

$a_d = \#$ closed pts. of degree d

$$N_n = \sum_{d|n} d a_d \quad N_1 = N = a_1$$

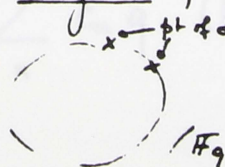
if $f \gg 0$ (i.e., $f(\theta) \geq 0$ for all θ and $c_n \geq 0$ for all n):

then
$$\sum d a_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{-1/2}) + \Psi(q^{1/2})$$

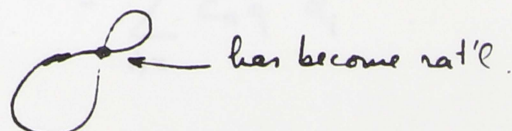
$$\Rightarrow (N-1) \Psi(q^{-1/2}) \leq g + \Psi(q^{1/2})$$

(Today: let $g \rightarrow \infty$)

Remark: We proved these inequalities for X projective nonsingular.
For X singular, the bound as stated doesn't work.



collapse:



So should replace g by sth which "sees" the topology.

X (singular) projective, abs. irred., let $B = 1^{\text{st}}$ Betti number (for ℓ -adic cohomology, for instance).

$$\text{Thm: } (N-1)\psi(q^{-1/2}) \leq B/2 + \psi(q^{1/2})$$

Define the "arithmetic genus" $p_a(X) = \dim H^1(X, \mathcal{O}_X)$

$$\text{Known: } B/2 \leq p_a(X).$$

$$\text{So we get } (N-1)\psi(q^{-1/2}) \leq p_a(X) + \psi(q^{1/2}).$$

Eg: $X \subset \mathbb{P}^2$ plane curve, abs. irred., of degree n .

$$\text{Then } p_a(X) = \frac{1}{2}(n-1)(n-2)$$

Pf (originally was given in terms of $N_n = \dots$)

$$\text{Claim: } N_n = 1 + q^n - \sum_{i=1}^B \alpha_i^n \quad |\alpha_i| = 1 \text{ or } q^{1/2}$$

Groth-Deligne: (Still the Lefschetz formula, except for the wrong size of eigenvalues)

Or: from Weil. $\square$

$$\text{Take } N_n - 1 = q^n - \sum_{i=1}^B \alpha_i^n \geq N - 1$$

$$\sum_n c_n q^{-n/2} (N_n - 1) = \sum_n c_n q^{n/2} - \sum_{i, n} c_n q^{-n/2} \alpha_i^n$$

$$\text{So } (N-1)\psi(q^{-1/2}) \leq \psi(q^{1/2}) - \sum_{i=1}^N c_n q^{-n/2} \alpha_i^n$$

$$\therefore \text{To be proved: } -\sum c_n q^{-n/2} \alpha_i^n \leq \frac{B}{2}$$

$$\text{or } \operatorname{Re}\left(-\sum c_n q^{-n/2} \alpha_i^n\right) \leq \frac{B}{2}$$

Since the LHS is real anyway

Consider $\frac{1}{2} + \psi(t) = F(t)$ polynomial in t

$$\text{If } t = e^{i\psi}, \operatorname{Re}(F(e^{i\psi})) = \operatorname{Re}\left(\frac{1}{2} + \sum c_n e^{in\psi}\right) = \frac{1}{2} f(\psi) \geq 0.$$

So: $\operatorname{Re}(F(t)) \geq 0$ for all t with $|t|=1$

$\Downarrow$ *cr analysis*

$$\operatorname{Re}(F(t)) \geq 0 \text{ for all } t \text{ with } |t| \leq 1.$$

(apply max. principle to $\exp(F(t))$.
Get
 $|\exp(-F(t))| \leq 1$
for $|t|=1$, hence
for $|t| \leq 1$.)

Now

$$\operatorname{Re}\left(-\sum c_n q^{-n/2} \alpha_i^n\right) = \sum_i \operatorname{Re}\left(\frac{1}{2} - F(q^{-1/2} \alpha_i)\right) \quad \text{and } |q^{-1/2} \alpha_i| \leq 1$$

$$\leq \sum_{i=1}^B \operatorname{Re}\left(\frac{1}{2}\right) = \frac{B}{2} \quad \text{so QED. } \square$$

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

$$\frac{B_3}{2} \geq N\psi(q^{-3/2}) - (\psi(q^{-3/2}) + \psi(q^{-1/2}) + \psi(q^{1/2}) + \psi(q^{3/2}))$$

(Exercise) (use Deligne — for large N this gives better bounds)

Now: q fixed, $g \rightarrow \infty$

we have:

let $k \geq 1$ be a fixed integer.

let X^λ be curves of genus $g_\lambda \rightarrow \infty$.

$$a_d(X^\lambda) =: a_d^\lambda$$

Theorem: $\limsup_{g_\lambda \rightarrow \infty} \frac{1}{g_\lambda} \sum_{d=1}^k \frac{d a_d^\lambda}{q^{d/2} - 1} \leq 1.$

Corollary: For $k=1$, $a_1^\lambda = N^\lambda = \# X^\lambda(\mathbb{F}_q)$, and we have

$$\limsup_{g_\lambda \rightarrow \infty} \frac{N^\lambda}{g_\lambda} \leq q^{1/2} - 1.$$

(Thm. of Drinfeld-Vladut).

Weil gives $N^2 \leq 1 + q + 2q^{\frac{1}{2}}$
 so $\frac{N^2}{q^{\frac{1}{2}}} \leq 2q^{\frac{1}{2}} + o(1)$

If $q=2$, Weil $2q^{\frac{1}{2}} = 2.828$, $[2q^{\frac{1}{2}}] = 2$, But $q^{\frac{1}{2}} - 1 = 0.414$.

Proof of Thm:

We have $\sum_{d=1}^k da_d^2 \psi_d(q^{-\frac{1}{2}}) \leq q^{\frac{1}{2}} + \psi(q^{\frac{1}{2}}) + \psi(q^{-\frac{1}{2}})$

$$\frac{1}{q^{\frac{1}{2}}} \sum_{d=1}^k da_d^2 \psi_d(q^{-\frac{1}{2}}) \leq 1 + \frac{1}{q^{\frac{1}{2}}} (\quad)$$

$q^{\frac{1}{2}} \rightarrow \infty$: $\boxed{\limsup \frac{1}{q^{\frac{1}{2}}} \sum_{d=1}^k da_d^2 \psi_d(q^{-\frac{1}{2}}) \leq 1.}$

true for every ψ_d coming from an $f \gg 0$.

Lemma: ① If $f \gg 0$, $f = 1 + \sum 2c_n \cos n\theta$, then $c_n \leq 1$.
 ② For any P , any $\epsilon > 0$, $\exists f$ s.t. $c_n \geq 1 - \epsilon$ for all $n=1, \dots, P$.
 (So can get f like $1 + 2\cos \theta + 2\cos 2\theta + \dots = \sum_{n \in \mathbb{Z}} e^{in\theta} =$ Dirac measure at 0 on the circle)

If $c_n = 1$ for all n , then OK, because $\psi(t) = t + t^2 + \dots$,
 $\psi_d(t) = t^d + t^{2d} + \dots = \frac{t^d}{t^d - 1} = \frac{1}{t^{-d} - 1}$

and $\psi_d(q^{-\frac{1}{2}}) = \frac{1}{q^{\frac{d}{2}} - 1}$, which gives the theorem.

Then we need only do a convergence argument using the Lemma. $\square$

Pf of Lemma :

$$\textcircled{1} \quad \begin{cases} c_n = \frac{1}{2\pi} \int_0^{2\pi} f(\theta) \cos n\theta \, d\theta \\ \text{and} \\ 1 = \frac{1}{2\pi} \int_0^{2\pi} f(\theta) \, d\theta \end{cases}$$

and since $|\cos n\theta| \leq 1$ 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 $f_P = \frac{1}{2P+1} (t^{-P} + t^{-P+1} + \dots + 1 + \dots + t^P)^2$

$$f_P(\theta) = \frac{1}{2P+1} (1 + 2\cos\theta + \dots + 2\cos P\theta)^2.$$

$$f_P = \frac{1}{2P+1} (t^{-2P} + 2t^{-2P+1} + \dots + (2P+1) \cdot 1 + 2Pt + \dots + t^{2P})$$

$$\text{So } c_n(f_P) = \frac{2P - n + 1}{2P + 1}$$

for fixed n , $P \rightarrow \infty$, $c_n \rightarrow 1$. $\square$

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 $X^\lambda \rightarrow X$ of ^{unramified} finite coverings of X in which every element of S splits completely and $\deg(X^\lambda \rightarrow X) \rightarrow \infty$.

Then:
$$\sum_{P \in S} \frac{\deg P}{q^{\deg(P)/2} - 1} \leq g - 1.$$

Special case: If all points in S are rat'l ($\deg = 1$) we get

$$|S| \leq (g-1)(q^{1/2}-1)$$

If $X = \mathbb{P}^1$, $S = \emptyset$, $X^\lambda = X/\mathbb{F}_{q^2}$ constant field extn.

then $\Sigma = 0 \leq 0-1$ is false.

So $S \neq \emptyset$ is necessary.

Proof: 1st 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!)

$$a_d^\lambda \geq n^\lambda a_d(S)$$

$$a_d(S) = \# \text{ of } P \in S \text{ of degree } d.$$

So get $\limsup_{n^2 \rightarrow \infty} \frac{1}{1+n^2(g-1)} \sum \frac{d n^2 a_d(s)}{q^{d/2} - 1} \leq 1$

$n^2 \rightarrow \infty$

Now $\frac{n^2}{1+n^2(g-1)} \rightarrow \frac{1}{g-1}$,

so $\limsup_{n^2 \rightarrow \infty} \underbrace{\frac{1}{g-1} \sum \frac{d a_d(s)}{q^{d/2} - 1}}_{\text{constant!}} \leq 1$

So we get the inequality we want. $\square$

2nd 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 $X^\lambda \downarrow X/\mathbb{F}_{q^d} \downarrow X/\mathbb{F}_q$; apply case 1 to the top layer

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 .

So this gives exactly the same formula! $\square$

Get
$$d \sum_{P \in S} \frac{\deg(P)/d}{(q^d)^{\frac{\deg(P)}{2d}} - 1} \leq g^{-1}$$
 which is the fla we want. $\square$

Ihara, Journ. Math. Soc. Japan?

Let
$$A(q) = \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}$$

Drinfeld-Vladut Thm $\implies \boxed{A(q) \leq q^{1/2} - 1}$

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!] $\rightarrow$ next time

For $q=2$:

$$\begin{cases} A(2) \leq 0.414... & (= \sqrt{2} - 1) & (D-V) \\ A(2) \geq 0.205... & (= \frac{8}{39}) \end{cases}$$

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

Choose $N = \ell$ prime, $\ell \equiv -1 \pmod{12}$, $\ell \neq p$.

Let $X = X_0(\ell)$, genus $g = \frac{\ell+1}{12}$.

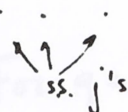
Supersingular points are rat'l / $\mathbb{F}_p^2$, and their number N^{ss} is given by

$$N^{ss} = \frac{p-1}{12} (\ell+1)$$

$X_0(\ell)$



$\mathbb{P}^1$ (param. by j)



$$\text{so } \frac{N}{g} \geq \frac{N^{ss}}{g} = p-1 = q^{1/2} - 1$$

You take $\ell \rightarrow \infty$, and the bound is obtained. $\square$

$$A(q) = \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}$$

Have seen: 1) $A(q) \leq q^{1/2} - 1$ (Drinfeld - Vladut)

Now 2) $\forall q$ is a square, $A(q) = q^{1/2} - 1$.

For $q = p^2$, modular curves $\rightarrow$ enough s.s. points.

$\{ \pm 1 \} \subset G \subset GL_2(\mathbb{Z}/\ell\mathbb{Z})$, ℓ prime, $\ell \geq 3$
 subgp

Then the modular curve w.r. to G , affine, but add pts at ∞ . Corresponds to moduli problem:

E ell. curve + " G -structure on its ℓ -div. pts"

G -structure: a family $E_c \xrightarrow[\varphi]{\sim} \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
 of

s.t. 1) $\varphi, \varphi' \in \text{family} \Rightarrow \varphi' = s\varphi$ for some $s \in G$

2) $\varphi' \in \text{family}, u \in G \Rightarrow s\varphi' \in \text{family}$.

X_G is the moduli space (completed).

Can view in terms of $X_\ell = \text{mod. curve of level } \ell \text{ (corresponds to } G = \{ \pm 1 \})$

X_ℓ
 $\downarrow$
 $\mathbb{Q}$

$$GL_2/\{\pm 1\} \xrightarrow{\det} \mathbb{F}_\ell^\times$$

gives an extension

$$\begin{array}{c} x_\ell \text{ (abs. inv. here)} \\ | \\ \mathbb{Q} \text{ --- } \mathbb{Q}(x_\ell) \end{array}$$

then: $X_G = x_\ell / G$

If $G \rightarrow \mathbb{F}_\ell^\times$, then X_G is defined over $\mathbb{Q}$.

Assume $G = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, $\lambda \in \mathbb{F}_\ell^\times$

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 $\mathbb{Q}(\sqrt{\ell})$, $\ell \equiv 1 \pmod{4}$

Can do this over any k , char $k \neq \ell$ (for char = ℓ , Katz + Mazur).

In char p , $p \neq \ell$, X_G is defined ^{over} either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

Theorem: Every ss. point $((E, \varphi), E \text{ s.s.})$ is rational over $\mathbb{F}_{p^2}$ (or 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. stabilizes (E, φ) . $\square$

a) $\Gamma_0(\ell)$ -curve: $G = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ gives our result above.

b) interesting case: $G = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{F}_\ell^\times \right\}$ $X_G = X(\ell)$

$$\begin{cases} \text{genus of } X(\ell): & 2g - 2 = \frac{1}{12} (\ell^2 - 1)(\ell - 6) \\ \# \text{ s.s. points: } / \mathbb{F}_{p^2} & N^{ss} = \frac{(p-1)(g-1)}{1 - \frac{6}{\ell}} \end{cases}$$

For low values:

$\ell = 7$ Klein curve

$PSL_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on $X(\ell)$

$$|PSL_2(\mathbb{Z}/7\mathbb{Z})| = 168$$

$$g = 3, \quad N^{ss} = 14(p-1)$$

($PGL_2(\)$ acts on curve over $\mathbb{Q}$, PSL_2 on curve over $\mathbb{Q}(\sqrt{-7})$)

Example:

$$\begin{cases} \beta = 2, & N^{ss} = 14 & (\text{over } \mathbb{F}_4) \\ \beta = 3, & N^{ss} = 28 & / \mathbb{F}_9 \\ \beta = 5 & N^{ss} = 56 & / \mathbb{F}_{25} \end{cases}$$

Weil bound is $1 + p^2 + 6p = \text{resp. } 17, 28, 56$

$$(2g\sqrt{p^2} = 6p.)$$

$\hookrightarrow$ for $\ell=3$ we have curves with max. no. of pts

The $\text{Jac}(X(11))$ 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

Aut. IV
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 $N^{ss} = N$ (Aut. IV gives eigenvalues of Frob. on these curves).

Theorem (Golod-Šafarevič)

Then 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" $\iff \begin{cases} I^n = 0 \text{ for large } n \\ \text{and} \\ I^m/I^{m+1} \text{ is a finite dim'd } k\text{-vector space} \\ \text{(for } m=0,1,\dots) \end{cases}$

(Example: G finite l-group, $R = \mathbb{F}_\ell[G]$, $I = \Delta(G)$, $k = \mathbb{F}_\ell$.)

Take $M = \text{f.g. } R\text{-module (left)}.$

Then $M/I^m M$ is a k -vector space of finite dim.

$$d_0(M) = \dim_k (M/I^m M) = \text{min. no. of generators of } M.$$

(If $x_1, \dots, x_d \in M$ give a basis for M/IM , NAK $\Rightarrow$ they generate M)

$$M \quad d = d_0(M)$$

Choose $x_1, \dots, x_d \in M$ generating M . This gives

$$0 \rightarrow M_1 \rightarrow R^d \rightarrow M \rightarrow 0$$

kernel = module of relations between the x_i
 $M_1 \subset IR^d$

Up to isom., M_1 depends only on M . Define

$$d_1(M) := d_0(M_1) = \text{"number of relations between } x_i \text{"}$$

Also: exact seq. gives:

$$0 = \text{Tor}_1(R^d, k) \rightarrow \text{Tor}_1(M_1, k) \rightarrow M_1/IM_1 \rightarrow R/IR_d \xrightarrow{\cong} M/IM \rightarrow 0$$

$$\text{So find } \text{Tor}_1(M, k) \cong M_1/IM_1,$$

$$\text{so } d_1(M) = \dim_k \text{Tor}_1(M, k)$$

$$d_i(M) = d_0(M_i) \quad M_i = i^{\text{th}} \text{ term of a minimal resolution of } M \\ \text{" } \dim_k \text{Tor}_i(M, k) \text{"}$$

Take $M=k$: $d_0(k)=1$

$$0 \rightarrow I \rightarrow R \rightarrow k \rightarrow 0$$

So $M_1 = I$; $d_1(k) = \dim_k (I/I^2) = \textcircled{d}$

$d_2(k) = \textcircled{r}$ by defn.

Theorem (Gold-Safarevič, refined by Vinberg and Gorchütz)

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.

[Example: if $R = \mathbb{Z}/2\mathbb{Z}$, $k = \mathbb{Z}/2\mathbb{Z}$, yet $M_1 \cong \mathbb{Z}/2\mathbb{Z}$, so all $d_i = 1$.

Pf: Have $0 \rightarrow J \rightarrow R^d \rightarrow I \rightarrow 0$

$$R^2 \rightarrow J \rightarrow 0$$

So get $R^2 \xrightarrow{\epsilon} R^d \rightarrow I \rightarrow 0$

$$\epsilon(R^2) \subset IR^d$$

Tensor w/ $R/I^n R$:

since $R^d/IR^d \xrightarrow{\sim} I/I^2$

$$\begin{array}{ccccc} R^2/I^n R^2 & \rightarrow & R^d/I^n R^d & \rightarrow & I/I^{n+1} \rightarrow 0 \\ & \searrow & \nearrow & & \\ & R^2/I^{n+1} R^2 & & & \end{array}$$

$\therefore \epsilon(I^{n+1} R^2) \subset I^n R^d$
no factors

$$\text{So } \frac{R^2}{I^{n-1}R^2} \rightarrow \frac{R^d}{I^n R^d} \rightarrow \frac{I}{I^{n+1}} \rightarrow 0 \quad (n \geq 1)$$

$$\text{Define } a(n) = \ell\left(\frac{R}{I^n R}\right) = \sum_{i=0}^{n-1} \dim_k \left(\frac{I^i}{I^{i+1}} \right)$$

$$a(0) = 0$$

$$a(1) = 1$$

$$a(2) = 1 + d$$

$$\frac{R}{I^2} : \begin{array}{cc} \frac{R}{I} & \frac{I^2}{I} \\ \vdots & \vdots \\ 1 & 1 \end{array}$$

⋮

$a(n)$ ultimately constant.

Now exact seq. above gives:

$$da(n) \leq ra(n-1) + \underbrace{a(n+1) - 1}_{\ell(I/I^2)} \quad n \geq 1$$

Claim: this implies $r > \frac{d^2}{4}$.

For this introduce $\sum_{n=0}^{\infty} a(n)t^n = t + (1+d)t^2 + \dots = tf(t)$

$$\text{so } \underline{f(t) = \sum_{n=0}^{\infty} a(n+1)t^n}$$

Write $f > 0$ for : all ¹⁷³ coeffs of f are ≥ 0 .

multiply ineq by t^n and add:

$$\sum_{n \geq 1} d a(n) t^n < r \sum_{n \geq 1} a(n-1) t^n + \sum_{n \geq 1} a(n+1) t^n - \sum_{n \geq 1} t^n$$

$$d f(t) t < r t^2 f(t) + f(t) - 1 - \sum_{n \geq 1} t^n$$

$$\text{so } d f(t) t < r t^2 f(t) + f(t) - \frac{1}{1-t}$$

$$\text{so } f(t) (r t^2 - d t + 1) > \frac{1}{1-t}$$

Assume $r \leq \frac{d^2}{4}$; then $r t^2 - d t + 1 = (1 - \lambda t)(1 - \mu t)$ $\lambda, \mu \geq 0$

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.

$$\text{RHS} > \frac{1}{(1-t)^2} \text{ coeffs not bded. } \square$$

$d=3, r > \frac{1}{4}$ i.e., $r \geq 3$ (l odd): 3 gen. z, y, x

$$\begin{cases} yxy^{-1} = x^{1+l} \\ zyz^{-1} = y^{1+l} \\ xzx^{-1} = z^{1+l} \end{cases}$$

Mennicke $\rightarrow$ finite group. $d=3, r=$

$d=4, r > \frac{16}{4}$ i.e., $r \geq 5 \rightarrow$ is $d=4, r=5$ possible?

(think: $d=4, r=6$ is.)

$x_1, \dots, x_d$ with $(x_i, x_j) = 1, x_i^2 = 1$ give $\frac{d(d-1)}{2} + d$ rels.

10/17

Class Field Towers

C curve, genus g , over $\mathbb{F}_q$, $p = \text{char.}$

K its function field.

l a prime number ($l=p$ is ok)

S finite non-empty set of "primes" of K i.e., of closed points of C .

look at $K_1 = \text{max. abelian } l\text{-extension of } K, \text{ (whose Galois group is an } l\text{-group)}$
 $\quad \quad \quad \mid$
 $\quad \quad \quad K$
 unramified (everywhere) in which the elements of S split completely.

K_1/K is a finite extension of K

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 $\mathbb{F}_q \cdot K$. If not, it does not.



Define $K_2 = (K_1)_S$ with respect to $S_1 = \text{inverse image of } S$.

So have $K \subset K_1 \subset K_2 \subset \dots \subset K_\infty = \bigcup_n K_n$

$K_\infty = \max.$ ^{Galois} extension of K where S splits completely, whose Galois group is pro- ℓ , and unramified.

Question: Is K_∞/K finite?

Let $G_S = \text{Gal}(K_\infty/K) = \varprojlim \text{Gal}(K_n/K)$

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).)

Theorem: Assume G_S is finite (i.e., the tower stops). Then

$$r - d \leq \begin{cases} |S| - 1 & \text{if } \ell \nmid q-1 \\ |S| & \text{if } \ell \mid q-1. \end{cases}$$

(We know: $r > \frac{d^2}{4}$ if $d \geq 1$ Golod-Shaf., which will give a contradiction for suitable S .)

Proof (Same as Iwasawa's in No. field case):

First: Using class field theory to find $\text{Gal}(K_1/K)$:

$C_K = \text{idèle class group}$

Have

$$1 \rightarrow E_S \rightarrow \prod_{p \in S} K_p^* \times \prod_{v \notin S} U_v \rightarrow C_K \xrightarrow{\text{quotient}} Ab_S \rightarrow 1$$

$E_S = S\text{-units} (= \text{unit outside } S)$

Then $\text{Gal}(K_1/K) = (Ab_S)_\ell$ (ℓ -part)

Next:

Now: K_∞/K finite, so $(K_\infty)_S = K_\infty$

Write seq. for K_∞ :

$$1 \rightarrow E_{S_\infty} \rightarrow \prod_{\hat{p} \in S_\infty} K_{\infty, \hat{p}}^* \times \prod_{\tilde{v} \notin S_\infty} U_{\tilde{v}} \rightarrow C_{K_\infty} \rightarrow Ab_\infty \rightarrow 1$$

"
 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 -group).

Also. For the product

$$K_p^* \text{-fact} : \begin{array}{c} \tilde{P} \hookrightarrow G \text{ permutes} \\ \downarrow \\ P \in S \end{array} \quad \prod_{\tilde{P} \rightarrow P} K_{\infty, P}^* \text{ is induced (trivial coh.)}$$

$$U_v \text{-fact} : \begin{array}{c} \tilde{v} \\ \downarrow \\ v \end{array} \quad G_v \text{-stab } \tilde{v}$$

Shapiro's lemma :

$$\text{coh} = H^q(G_{\tilde{v}}, U_{\tilde{v}}) = \text{trivial (because everything is unramified)}$$

So LES of coh gives a map

$$\hat{H}^q(G, C_{K_\infty}) \xrightarrow[\cong]{\delta} \hat{H}^{q+1}(G, E_{S_\infty}) \quad \text{for each } q \in \mathbb{Z}.$$

δ is an isom. for all q because middle term has trivial coh.

$\hat{H}^q$ is Tate cohomology

$$\text{Know: } \hat{H}^q(G, C_{K_\infty}) \xleftarrow[\cong]{\sim} \hat{H}^{q-2}(G, \mathbb{Z})$$

$$u_{K_\infty} \in H^2(G, C_{K_\infty})$$

$$\text{Choose } q+1=0 \text{ so } q=-1 : \text{Get } \hat{H}^{-3}(G, \mathbb{Z}) \cong \hat{H}^0(G, E_{S_\infty}) = \frac{E_S}{\text{Norm}(E_{S_\infty})}$$

know $E_S \cong \mathbb{Z}^{|S|-1} \times \mathbb{F}_q^*$.

We want a quotient of E_S / Norms which is an ℓ -group.

So

$$\text{rk}_\ell(\hat{H}^{-3}(G, \mathbb{Z})) \leq \begin{cases} |S|-1 & \text{if } \ell \nmid (q-1) \\ |S| & \text{if } \ell \mid (q-1). \end{cases}$$

It remains to show: $\text{rk}_\ell(\hat{H}^{-3}(G, \mathbb{Z})) = 2 - d$.

$$\hat{H}^{-3}(G, \mathbb{Z}) = H_2(G, \mathbb{Z})$$

[Group of coeffs A , trivial action]

$$H_q(G, A) = H_q(G, \mathbb{Z}) \otimes A \oplus \text{Tor}_1(H_{q-1}(G, \mathbb{Z}), A)$$

$$q=2, A = \mathbb{Z}/\ell\mathbb{Z} :$$

$$H_2(G, \mathbb{Z}/\ell\mathbb{Z}) = H_2(G, \mathbb{Z}) \otimes \mathbb{Z}/\ell\mathbb{Z} \oplus \text{Tor}_1(H_1(G, \mathbb{Z}), \mathbb{Z}/\ell\mathbb{Z})$$

$$= H_2(G, \mathbb{Z}) / \ell H_2(G, \mathbb{Z}) \oplus \ell\text{-part of } H_1(G, \mathbb{Z})$$

So take ranks: $r = \text{rk}_\ell(H_2(G, \mathbb{Z})) + d$.

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 $\text{rk}_\ell \hat{H}^{-3}(G, \mathbb{Z}) = 2 - d$.

On: look at

$$0 \rightarrow \mathbb{Z} \xrightarrow{\ell} \mathbb{Z} \rightarrow \mathbb{Z}/\ell\mathbb{Z} \rightarrow 0$$

$$a \quad H_2(G, \mathbb{Z}) \xrightarrow{\ell} H_2(G, \mathbb{Z}) \rightarrow H_2(G, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H_1(\quad) \xrightarrow{\ell} H_1(\quad)$$

$$\text{So } 0 \rightarrow \frac{H_2(G, \mathbb{Z})}{\ell H_2(G, \mathbb{Z})} \rightarrow H_2(G, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow \text{Ker}(\ell \text{ in } H_1(G, \mathbb{Z})) \rightarrow 0$$

So dimensions add. So QED! $\square$

Theorem: The $(S-\ell)$ class field tower of K is infinite if $|S| \geq \frac{d^2}{4} - d + \begin{cases} 1 & \text{if } \ell \mid (g-1) \\ 0 & \text{if not} \end{cases}$, and $d \geq 2$.

Pf: Otherwise

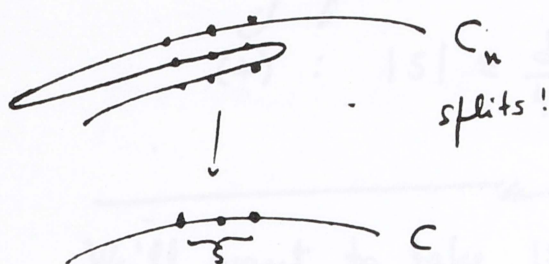
$$r - d \leq \begin{cases} |S| - 1 \\ |S| \end{cases}$$

$$r > \frac{d^2}{4} \quad \text{if } d \geq 1$$

And of course $d=1$ doesn't work (get $|S| \leq \frac{1}{4}$) $\square$

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 $A(g) \geq \frac{|S|}{g-1}$, where $A(g) = \limsup_{g \rightarrow \infty} \frac{N_g(g)}{g}$
(and in particular $A(g) > 0$)
 $g_c = \text{genus of } C$.



So nber of rat'l pts of $C_n \geq [C_n:C] \cdot 15$
 genus of $C_n = g_{C_n}$; $g_{C_n} - 1 = [C_n:C](g-1)$

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 $\rightarrow \infty$!)

$$\text{So } \frac{N_q(g_n)}{g_n} \geq |S| \frac{[C_n:C]}{1 + [C_n:C](g-1)}$$

$$\geq |S| \frac{1}{\frac{1}{[C_n:C]} + g - 1}$$

$n \rightarrow \infty$ so

$$\boxed{A(q) \geq \frac{|S|}{g_c - 1}}$$

Corollary: If (S, ℓ) satisfy $|S| \leq \frac{d^2}{4} - d + \{0\}^1$, $d \geq 2$,
 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

$$(*) : |S| \leq \frac{d^2}{4} - d + \begin{cases} 1 & \text{if } \ell \mid q-1 \\ 0 & \text{if not} \end{cases}, \quad d \geq 2.$$

We'll want to take $|S|=1$, $d \geq 5$.

We'll choose $\ell=2$ (So for q odd, enough to find $d \geq 4$).

Construction ($\text{char} = p \neq 2$)

Choose $\ell=2$; K will be some quadratic extension of $K_0 = \mathbb{F}_q(T)$ corresp. to curve C_0 of genus 0.

Want $C_0 \searrow \begin{matrix} C_1 \\ \vdots \\ C_d \end{matrix} \nearrow C_d$ point at ∞ should split completely.

Let $\phi_0, \dots, \phi_d$ be indep. monic polyn. of even degree distinct

Then define C_i by $y_i^2 = \phi_i(T)$.

$$y_i^2 = T^{\text{even}} + \dots \Rightarrow \infty \text{ is split in each } C_i$$

$$\text{So set } K = \mathbb{F}_q(T, \sqrt{\phi_0 \dots \phi_d})$$

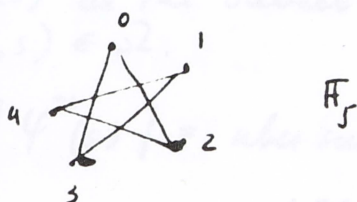
Over K , I have d indep. quadratic extens, unramified, ∞ splits completely.

Choose $d=5$, for instance, and the " d " in the theorem is then at least 5, so done. $\square$

For $\text{char} = 2$, do the same with Artin-Schreier extensions.

You 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. $q = 5$



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 $X = \text{set of pairs } (A, s) \text{ with } |A| = a, s \in S$
and $A \times \{s\} \subset \Omega$.

Then $|X| = ?$

Project $X \xrightarrow{\psi} S$
 $(A, s) \mapsto s$

Let $R(s)$ be the subset of R made of the elements r
s.t. $(r, s) \in \Omega$.

$$\begin{aligned} \text{So } |\psi^{-1}(s)| &= \text{nbr subsets of } R(s) \text{ w/ } a \text{ elements} \\ &= \binom{|R(s)|}{a} \geq \binom{m}{a} \quad \text{since } |R(s)| \geq m \end{aligned}$$

$$\text{Then } |X| \geq |S| \binom{m}{a}$$

Then $X \xrightarrow{\psi} \text{Set of subsets of } R \text{ with } a \text{ elements}$ $\leftarrow$ has $\binom{|R|}{a}$ elements
 $(A, s) \mapsto A$

Hence some fiber of ψ has at least $|X| / \binom{|R|}{a}$ elements

$$\text{But } \frac{|X|}{\binom{|R|}{a}} \geq \frac{|S| \binom{m}{a}}{\binom{|R|}{a}} \geq b.$$

So choose A whose fiber has $\geq b$ elements, and
choose B in the fiber with $|B| = b$. Done! $\square$

10/23 Class Field Towers (cont.)

We showed: $\perp\Omega \subset R \times S$

If $\left\{ \begin{array}{l} \text{every } s \in S \text{ is } \Omega\text{-related to at least } m \text{ elements} \\ \text{of } R \end{array} \right.$

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 $R = S = \mathbb{F}_q$, $\Omega = \{(r, s) \mid r - s \text{ is a nonzero square in } \mathbb{F}_q\}$,
so $m = \frac{q-1}{2}$.

Let $g \mapsto a(g), b(g)$ be two functions of a variable g , with integral values ≥ 1 for $g = p^e$, 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: There, for g large enough, there exists $A, B \subset \mathbb{H}_g^+$ with $|A| = a(g)$, $|B| = b(g)$, and $A \times B \subset \Omega$.

[This is approx. what the naïve approach would give

$$186 \cdot \left(\frac{1}{2}\right)^2$$

$$b_1, b_2, \dots, b_n$$

$$q \left(\frac{1}{2}\right)^\alpha ?$$

$$\alpha \sim \log q \Rightarrow \left(\frac{1}{2}\right)^\alpha = \frac{1}{q^\epsilon}$$

which suggests $a(q) \leq c_1 \log q$ is
reasonable]

If q is a square,

$$\begin{array}{c} \mathbb{F}_q \\ | \\ \mathbb{F}_{q^{1/2}} \end{array} \quad \begin{array}{c} \text{---} \text{---} \text{---} \\ \frac{1}{2} q^{1/2} \quad \frac{1}{2} q^{1/2} \end{array}$$

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,

$$b(q) \binom{q}{a(q)} \stackrel{?}{\leq} q \binom{\frac{q-1}{2}}{a(q)}$$

i.e.,
$$b(q) \frac{q!}{(q-a(q))!} \stackrel{?}{\leq} q \frac{\left(\frac{q-1}{2}\right)!}{\left(\frac{q-1}{2}-a(q)\right)!}$$

Stirling: $\log(x!) = (x + \frac{1}{2}) \log x - x + O(1)$

Suppose $1 \leq y \leq x^{1/2}$. Then

$$\log \left(\frac{x!}{(x-y)!} \right) = (x + \frac{1}{2}) \log x - x - (x-y + \frac{1}{2}) (\log x + \log(1 - \frac{y}{x})) + x - y + O(1)$$

$$= y \log x + O(1)$$

$$\left[\begin{aligned} \text{Since } -y - (x-y + \frac{1}{2}) \log(1 - \frac{y}{x}) &= \\ &= -y - \underbrace{(x-y + \frac{1}{2}) \left(-\frac{y}{x} + O\left(\frac{y^2}{x^2}\right) \right)}_{\frac{y^2}{x} \leq 1} \\ &= O(1) \end{aligned} \right]$$

So check that

$$\log b(q) + a(q) \log q + O(1) \stackrel{?}{\leq} \log q + a(q) \log \frac{q-1}{2}$$

$$\left[\begin{aligned} a(q) &\leq c_1 \log q \\ b(q) &\leq q^{c_2} \end{aligned} \right] \log b(q) \leq c_2 \log q.$$

$$\text{So } \log q - \log b(q) \stackrel{?}{\geq} a(q) (\log q - \log \frac{q-1}{2}) + O(1)$$

$$\log \frac{q-1}{2} = \log(q-1) - \log 2 = \log q + \log(1 - \frac{1}{q}) - \log 2$$

$$\text{So } a(q) (\log q - \log \frac{q-1}{2}) + O(1) \leq c_1 \log q (\log 2 + o(1))$$

$$\log q - \log b(q) \geq (\log q) (1 - c_2)$$

So want $\boxed{1 - c_2 > c_1 \log 2}$, which is our condition. $\square$

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 $\{a_1, a_1', \dots, a_\alpha, a_\alpha'\} = A$.

If t is the variable in $\mathbb{P}_1$, take the quad. extn. given by

$$\sqrt{(t-a_i)(t-a_i')} \quad i=1, \dots, \alpha.$$

(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 Ω).

Now go to $C \longleftrightarrow \mathbb{F}_q(t, \sqrt{\prod (t-a_i)(t-a_i')})$

Elements of B give $B_C = \text{subset of } C \text{ coming from } B$,

$$|B_C| = 2|B| = 2b(q)$$

and C has $\alpha-1$ independent quadratic extns which are unramified and where B_C splits completely.

(Namely, given by $\sqrt{(t-a_i)(t-a_i')} \quad i=1, \dots, \alpha-1$.)

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

$$A(q) \geq \frac{|B_c|}{q-1} = \frac{(\log q)^2}{\log q} = \log q.$$

C is hyperelliptic, ramified at $2\alpha = a(q)$ pts, and so $g_c = \alpha - 1 = \log q$.

So $\boxed{A(q) \geq c \log q}$ for some c . (For q odd).

When q is a square, we can take $|B_c| \approx q^{1/2}$, $g_c = q^{1/4}$, so get $A(q) \geq c q^{1/4}$.

(But modular tower gives $q^{1/2}$).

For $q = 2^e$, can use } Artin-Schreier extns
 a
 a 3-tower

Construction for $g=2$ Claim: $A(2) \geq \frac{2}{9} = 0.222\dots$

First: Simple construction for $A(2) \geq \frac{1}{5} = 0.2$.

Take $\begin{array}{c} C \\ \downarrow \\ \mathbb{P}_1 \end{array} \quad t$ $y^2 + y = t^3 + t + \sum_{\substack{\text{irred poly } \varphi(t) \\ \text{of deg } 2, 3, 4}} \frac{t^2 + t}{\varphi(t)}$

So: sum is over $\left\{ \begin{array}{l} \text{deg } 2 \rightarrow \\ \text{deg } 3 \rightarrow \\ \text{deg } 4 \rightarrow \end{array} \right\} \left\{ \begin{array}{l} t^2 + t + 1 \\ t^3 + t + 1, \quad t^3 + t^2 + 1 \\ t^4 + t + 1, \quad t^4 + t^3 + 1, \quad t^4 + t^3 + t^2 + t + 1 \end{array} \right.$

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.

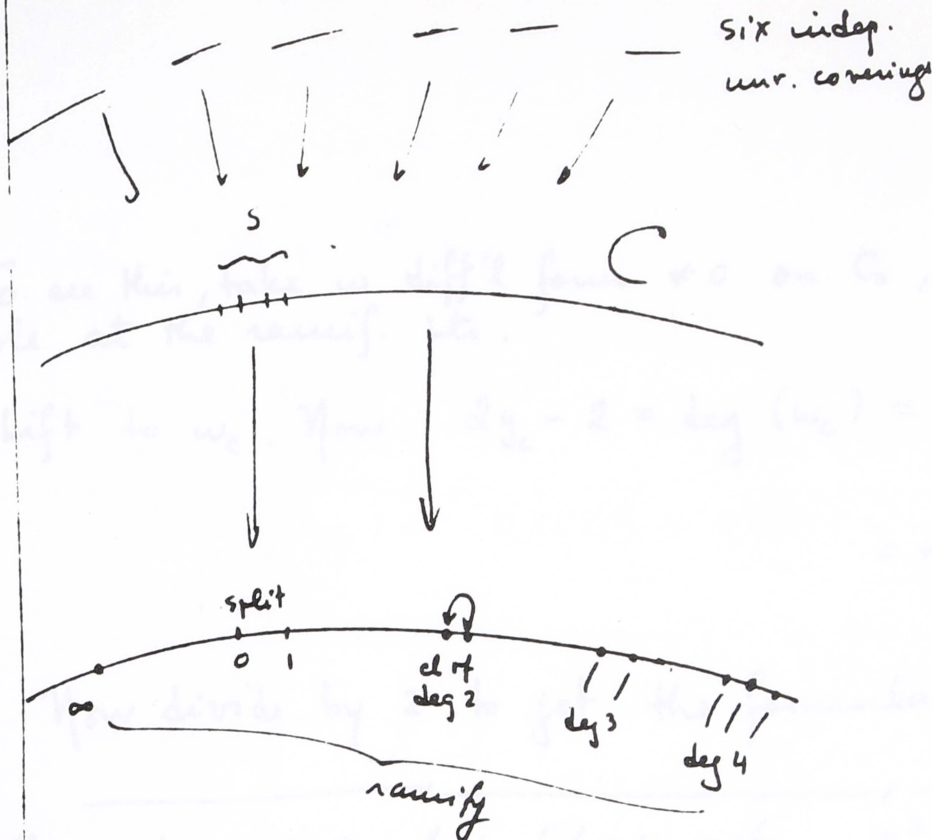
$\begin{array}{c} S \\ \downarrow \\ \{0, 1\} \end{array} \quad \begin{array}{c} C \\ \downarrow \\ \mathbb{P}_1 \end{array}$

Have 6 indep. unramified quad. exts, given by $y^2 + y = \frac{t^2 + t}{\varphi(t)}$ for the six $\varphi(t)$ above

and $\{0, 1\}$ split completely. (Same argument as before.)

C is ramif at roots of $\varphi(t)$ and at ∞ .

Picture $\rightarrow$



Assume: $g_c = 21$, class field tower is infinite.

Then $A(2) \geq \frac{|S|}{g-1} = \frac{4}{21-1} = \frac{4}{20} = \frac{1}{5}$.

Class Field Tower: condition is $|S| \leq \frac{d^2}{4} - d + 1$

$|S|=4$, $d \geq 6$, so $\frac{d^2}{4} - d + 1 \geq \frac{36}{4} - 6 + 1 \geq 4$.

So class field tower is infinite.

Genus: Know: $g_c - 1 = n(g_{C_0} - 1) + \sum \text{contrib. of ramification}$.

$$\begin{array}{c} C \\ n \downarrow \\ P \in C_0 \end{array}$$

Go to alg. closure: take a local param t at P , look at dt . lift it to C .

Ramify $\Rightarrow dt$ will have zero on the fiber

and

contrib of ramif = $\frac{1}{2}(\text{degree of } dt \text{ on the fiber})$

To see this, take w diff'l form $\neq 0$ on C_0 , w/o zero or pole at the ramif. pts.

$$\text{lift to } w_c. \text{ Now } 2g_c - 2 = \deg(w_c) = n \deg(w) + \text{extra zeros} \\ = n \deg(w) + \sum_{\text{on fibers}} \deg \text{ of } dt$$

Now divide by 2 to get the formula.

Now suppose $p=2$, Artin-Schreier extn $y^2 + y = \psi(t)$
local computation, no work in field of power-series
 $\psi(t) = \frac{c_0}{t^n} + \dots \quad n \text{ odd} \geq 1.$

[If ψ is hol., no ramif.; if $\frac{1}{t^2} + \dots$, remove $\psi - (\frac{1}{t^2} + \frac{1}{t})$ 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)

$$\begin{array}{c} K \\ | \\ K_0 \end{array} \quad \begin{array}{l} t \\ dy = \frac{c_0}{t^{n+1}} dt + \dots \end{array} \quad \begin{array}{l} v_K(y) = \frac{1}{2} v_K(\frac{1}{t^n}) = -n \quad \text{since } v(t) = 2 \text{ (ramification)} \\ \text{(char 2)} \end{array}$$

If θ local parameter of K ,

$$y = \theta^{-n} \cdot \text{unit},$$

so $dy = \frac{d\theta}{\theta^{n+1}} + \dots$

so $v_K(dy) = -(n+1)$

So $v_K(dy) = -2(n+1) + v_K(dt) \Rightarrow v_K(dt) = n+1.$

In our case, $y^2 + y = \underbrace{t^3 + t}_{\text{deg } 2, 1, 4} + \sum \frac{t^2 + t}{\varphi(t)}$

↙
pole of order 3 = n
at ∞
 $\frac{1}{2}(n+1) = 2$

↘ simple
poles at these
deg $\varphi = 2 \rightarrow$ two simple poles
 $\rightarrow \frac{1}{2}(2) + \frac{1}{2}(2) = 2$

So $g_C - 1 = 2(g_0 - 1) + \sum \text{local contrib}$ Same for deg $\varphi = 3$ or 4.

$= -2 + 2 + \sum \deg \varphi$

$= -2 + 2 + 20$

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 $\deg(\underline{m}) \geq 151$. 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 $\deg \underline{m}$. 194

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).

$$N_1 = \# C(\mathbb{F}_2) = 2$$

$$\text{Now } N_n = \# C(\mathbb{F}_n) = 1 + 2^n - \underbrace{(\pi^n + \bar{\pi}^n)}_{t_n}$$

$$\text{and } t_n = t_{n-1} t_1 - q t_{n-2} \quad \text{since } \pi \bar{\pi} = q !$$

$$\text{Here } t_0 = 2, t_1 = 1, q = 2 \quad (N_1 = 2 = 1 + 2 - t_1)$$

$$\text{So } t_n = t_{n-1} - 2 t_{n-2}$$

$$\text{So } t_2 = -3, t_3 = -5, t_4 = 1$$

$$\therefore N_1 = 2, N_2 = 8, N_3 = 14, N_4 = 16$$

If a_i = nber of closed pts of $C/\mathbb{F}_2$ of degree i (so $N_n = \sum_{i|n} i a_i$)

$$\text{So } a_2 = 3, a_3 = 4, a_4 = 2.$$

lots of these

s.t. two rat'l pts split completely

Make 7 quadratic extensions of C 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 as before

$$d = 6 \text{ as before, and } g - 1 = 2(1 - 1) + \sum \text{contrib}$$

$$g - 1 = 18 \quad \Rightarrow \quad g = 19$$

$$\text{So get } A(2) \geq \frac{4}{18} = \frac{2}{9}. \quad \square$$

0/31 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.

$$C_{\text{free}}(x) = \frac{\{\text{divisors of } x \text{ prime to } s\}}{\{f\}}$$

where $f \in K^*$, and $f \equiv 1 \pmod{m}$

(this means that $f \in 1 + \max_p^n$ locally at each $P \in S$, or. equiv., $v_P(f-1) \geq n_P \quad \forall P \in S$).

If $\underline{m} = 0$, $\mathcal{Q}_0(x) = \text{Pic}(x)$
 $\mathcal{Q}''(x)$

Recall $0 \rightarrow J(\mathbb{F}_q) \rightarrow \mathcal{O}(X) \xrightarrow{\deg} \mathbb{Z} \rightarrow 0$ exact

and

$$0 \rightarrow \text{kernel} \rightarrow \underline{Cl}_m(X) \xrightarrow{\text{obvious}} Cl(X) \xrightarrow{\text{almost obvious}} 0$$

assume $m \neq 0$; ~~if~~ if U_p = local units at P , $U_r = \{u \in U_p \mid v(u-1) \geq_{v_p} r\}$

We have $0 \rightarrow \mathbb{F}_q^* \rightarrow \prod_{p \in S} U_p / U_p^{(m_p)} \rightarrow \underline{cl}_m(X) \rightarrow cl(X) \rightarrow 0$

CFT:

Let G be a finite group and let
 $\alpha: \text{Cl}_K(X) \rightarrow G$ be onto.

Then CFT constructs an abelian extension K_2/K with Galois group G s.t.

1) K_2/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

$$U_P \xrightarrow{\quad} \text{Cl}_K(X) \xrightarrow{\alpha} G$$

is the one attached by local class field theory, and the image is the inertia group.

I also have $K_P^\times \rightarrow G$, image is decomp. group.

Let $P_1, \dots, P_s$ be closed points disjoint from S .
 If I want extras in which these split completely, I have:

To have P_i split in K_n/K it is nec. & suff.
that $\alpha((P_i)) = 0$, $(P_i) \in \text{Cl}_n(X)$.

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 $\epsilon = l$ -rank of $\mathbb{F}_q^x$ $\begin{pmatrix} 0 & \text{if } elq-1 \\ 1 & \text{if } elq-1 \end{pmatrix}$

Claim $\left\{ \begin{array}{l} \text{Assume that } s \leq \sum d_p - \epsilon. \\ \text{Then: } \exists \text{ a cyclic extension of deg } l \text{ obtained} \\ \text{through an } \alpha, \text{ where the } P_i \text{'s split completely.} \end{array} \right.$

Have $0 \rightarrow \text{Local} \rightarrow \text{Cl}_n \rightarrow J(\mathbb{F}_q) \times \mathbb{Z} \rightarrow 0$,
so $\text{Cl}_n \cong \mathbb{Z} \times \Phi$ $\Phi \supset \text{Local}$, finite.

So l -rank of $\text{Cl}_n/\ell\text{Cl}_n$ is $\geq 1 + \sum d_p - \epsilon$.

There is a hyperplane $\text{Cl}_n/\ell\text{Cl}_n$ (as $\mathbb{F}_\ell$ -vector sp.) contain-
ing all the P_i ; this gives the desired extension.

Given K_n/K , assuming no constant-field extn.
corresp to the
condn:

$\deg: \text{Ker } \alpha \rightarrow \mathbb{Z}$
is surjective.

$$\begin{array}{ccc} \text{Cl}_n & \xrightarrow{\deg} & \mathbb{Z} \\ & \searrow \alpha & \\ & & G \end{array}$$

In this case, I want the genus of K_α .

Look at characters $\chi: G \rightarrow \mathbb{C}^\times$. This gives maps

$$U_P \rightarrow \text{Cl}_\alpha \rightarrow G \xrightarrow{\chi} \mathbb{C}^\times.$$

$$\text{So exp. of cond. of } \chi \text{ at } P = f_P(\chi) = \begin{cases} 0 & \text{if } U_P \rightarrow \mathbb{C}^\times \text{ is trivial} \\ \text{smallest } e \text{ s.t.} \\ U_P \rightarrow \mathbb{C}^\times \text{ is trivial} \\ \text{on } U_P^{(e)} \end{cases}$$

So formula for the genus g_α of K_α :

$$2g_\alpha - 2 = [K_\alpha: K](2g - 2) + \deg(\text{discriminant ideal})$$

$$\text{and } \text{disc} = \sum_{P, \chi} f_P(\chi) \cdot P,$$

so we get

$$\boxed{2g_\alpha - 2 = 16(2g - 2) + \sum f_P(\chi) \deg P}$$

In our situation: $g=2, \ell=2, 16=2$

At each P we get one number f_P (only one character!).

On the other hand, we've noted that writing

$$y^2 + y = \frac{a_0}{t^m} + \dots = \varphi \text{ m odd } \geq 1,$$

the local contrib was measured by m.

Have: $\boxed{f_p = m+1}$

"Proof": I get $U_p \longrightarrow \{\pm 1\} = \mathbb{Z}/2\mathbb{Z}$

explicitly: $u \in U_p$ can be viewed as $u(t) \in \mathbb{F}_2[[t]]$; then the map is

$$u(t) \longmapsto \text{Tr}_{\mathbb{F}_2[[t]]/\mathbb{F}_2} \left(\text{Res} \left[\varphi(t) \frac{du(t)}{u(t)} \right] \right)$$

(For an Artin-Schreier extn as above!)

Then, if $u \equiv 1 \pmod{t^{m+1}}$

$$\frac{du}{u} = ct^m dt + \dots$$

$$\varphi \frac{du}{u} \text{ hol.}, \text{ so } \text{Res} = 0$$

But if $u \equiv 1 \pmod{t^m}$, not $\pmod{t^{m+1}}$, will get simple pole, hence $\text{Res} \neq 0$.

2-rank of $U_p/U_p^{(n_p)}$

n_p even ≥ 2

res field $\mathbb{F}_{2^e}$

$$U_p/U_p^{(n_p)} = \{ \alpha_0 + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1} \bmod t^n \} \quad \begin{matrix} \alpha_0 \neq 0 \Rightarrow \alpha_0 \in \mathbb{F}_{2^e} \\ \alpha_i \in \mathbb{F}_{2^e} \end{matrix}$$

for 2-rank, think only

$$1 + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1}$$

$\alpha_i \in \mathbb{F}_q = \mathbb{F}_{2^e}$, so

$$\text{order} = q^{n-1}$$

squares : $1 + \alpha_1^2 t^2 + \dots$ = those where $\alpha_1 = \alpha_3 = \dots = 0$)
 there are $\frac{n}{2}$ ^{odd} indices, so order = $q^{\frac{n}{2}-1}$

$\therefore \text{As } |G/G^2| = q^{n/2}, \text{ so } 2\text{-rank} = e \cdot \frac{n}{2}.$

This proves the statement made last time about constructing extensions where certain points split.
 (Just check that $\# \text{points} < \sum d_p - e$)

Optimal functions for number of points

F_g , 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 g , what is (if any) the best choice of (c_n) ? (I.e., the one that maximizes the expression.)

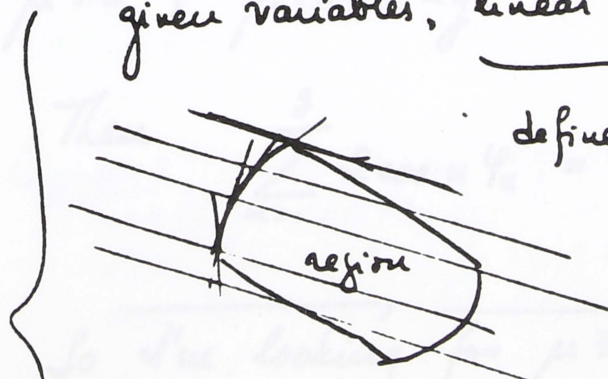
If $(c_n) \in (*)$, what is the max of $\sum c_n ((N-1)q^{-n/2} - q^{n/2})$

Call the max $g(N, q) = -\sum c_n \lambda_n$

This is a linear programming question:

given variables, linear inequalities on them

defines some ^{convex} region



given linear forms $\longleftrightarrow$ 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, $q \rightarrow$ genus?

We must have then $N_n \geq N, \forall n. (N_n = \# X(\mathbb{F}_{q^n}))$

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 $\mu = \sum (\delta_{e^{i\varphi_\alpha}} + \delta_{e^{-i\varphi_\alpha}})$ $\delta = \text{Dirac measure.}$
 $\mu \geq 0, \mu(S^1) = 2g.$

Then $\sum_{\alpha=1}^g 2 \cos n \varphi_\alpha = \int t^n \mu(t) = \int \frac{1}{2} (t^n + t^{-n}) \mu(t)$

So I'm looking for $\mu \geq 0$ on S^1 with

$$\int t^n \mu(t) \leq \underbrace{q^{n/2} - (N-1)q^{-n/2}}_{\gamma_n} \quad n=1, 2, \dots$$

(and μ symmetric with respect to $t \mapsto \bar{t}$)

So look at all

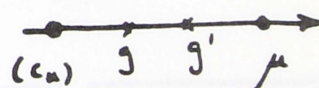
$$\mu \text{ symmetric} \quad \left[\mu \geq 0, \quad \int t^n \mu(t) \leq \gamma_n \quad n=1,2,\dots \right] \quad (**),$$

and ask what is the lower bound of $\frac{1}{2} \int \mu(t)$?
 Call it $g'(N, \gamma)$

This is the dual problem.

Lemma 1: If $\mu \in (**)$, $(c_n) \in (*)$, then

$$-\sum c_n \gamma_n \leq \int \frac{1}{2} \mu(t).$$



In particular, $g(N, \gamma) \leq g'(N, \gamma)$

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. $c_n \neq 0$.

Theorem: Let μ and (c_n) be such as in Lemma 2.
 Then $g(N, \gamma) = \frac{1}{2} \int \mu(t) = -\sum c_n \gamma_n$.

Proof: Let $f = 1 + \sum c_n(t^n + t^{-n}) \geq 0$

$$\text{So } \mu(f) = \int f d\mu = \mu(1) + 2 \sum c_n \mu(t^n) \geq 0$$

But $\mu(t^n) = \int t^n d\mu \leq \delta_n$, so

$$\mu\left(\frac{1}{2}\right) \geq - \sum c_n \mu(t^n) \geq - \sum c_n \delta_n$$

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 $\mu(t^n) = \delta_n$ unless $c_n = 0$,

QED (2). $\square$

Example: Take $q+1 \leq N \leq q^{3/2} + 1$

Claim: in this range Weil is optimal.

Weil $\longleftrightarrow 1 + \cos \theta$, so $c_1 = \frac{1}{2}$, $c_n = 0$, $n \geq 2$

Claim: this choice is optimal.

It is enough to exhibit a μ with equality!

$$\begin{aligned} \text{We want } q &= -\frac{1}{2} \delta_1 = -\frac{1}{2} (q^{1/2} - (N-1)q^{-1/2}) \\ &= \frac{1}{2} ((N-1)q^{-1/2} - q^{1/2}) \geq 0 \end{aligned}$$

Set 31

And take $\mu = \text{Dirac at } t = -1 \text{ (angle } \theta = \pi)$ with weight $2g$, where g is given by this last eqn.

To check: $\begin{cases} 1 + \cos \theta \geq 0 & \text{OK, } c_n \geq 0 & \text{OK} \\ \text{so (*) OK.} \end{cases}$

$\begin{cases} \text{clearly } \mu \text{ is concentrated at the zero of } 1 + \cos \theta \\ \text{to check: } \begin{cases} \mu(t^n) \leq \gamma_n & \text{for } n \geq 1 \\ \mu(t) = \gamma_1 \end{cases} \end{cases}$

$$\mu(t) = 2g(-1) = -2g$$

to check $-2g = \gamma_1$ OK by construction

$$\mu(t^2) = 2g(-1)^2 = -\gamma_1 \stackrel{?}{\leq} \gamma_2$$

$$-\gamma_1 = -q^{1/2} + (N-1)q^{-1/2} \stackrel{?}{\leq} q - (N-1)q^{-1} = \gamma_2$$

$$(N-1)(q^{-1/2} + q^{-1}) \stackrel{?}{\leq} q + q^{1/2}$$

$$(N-1)(1 + q^{1/2}) \stackrel{?}{\leq} q^{3/2}(1 + q^{1/2})$$

$$(N-1) \stackrel{?}{\leq} q^{3/2} \quad \text{OK by condition on } N.$$

$$\mu(t^3) = -2g = \delta_1 \leq \delta_3$$

$$\delta_3 \geq 0, -2g < 0 \text{ OK.}$$

$$\mu(t^4) = 2g = -\delta_1 \leq \delta_2 \leq \delta_4$$

δ_n increases for n large.

and larger n are similarly OK. $\square$

Theorem on Linear Inequalities on $\mathbb{R}^n$:

Let f_α be ^{finitely many} additive functions $(\sum \alpha_i x_i + \rho)$ 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 Aertse's "Optimal" computation of lower bound for g
(given N, q)

On Machine: $\left\{ \begin{array}{l} \text{ON} \\ \text{RUN 2000} \\ \text{NOMBRE DE POINTS?} \quad 65 \text{ enter} \\ Q? \quad 8 \text{ " } \\ \text{GENRE} \geq 14 \end{array} \right.$

Recall: Last time we defined a "dual" problem to what we wanted, and saw that

$\left. \begin{array}{l} \text{admissible } \mu \text{ measure} \\ + \\ \text{admissible } (c_n) \end{array} \right\} \text{ match} \rightarrow \text{optimal solution.}$



$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

admissible μ $\left[\begin{array}{l} \mu \text{ will be a positive measure on } S^1 \text{ s.t.} \\ \cdot \text{ symmetric w.r.t } z \mapsto \bar{z} = z^{-1} \\ \cdot \int t^n \mu(t) = \langle t^n, \mu \rangle \geq q^{n/2} - (N-1)q^{-n/2} \text{ for } n \geq 1 \end{array} \right.$

(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

$$\left\{ \begin{array}{l} \mu \mapsto \frac{1}{2} \int \mu(t) = \langle \frac{1}{2}, \mu \rangle \\ (c_n) \mapsto \sum c_n ((N-1)q^{-n/2} - q^{n/2}) \end{array} \right\}^N$$

We say μ and (c_n) match if $\frac{1}{2} \int \mu(t) = \sum c_n ()$; if this happens, the common value is the best $g(N, q)$ that the explicit formula can give.
(Usually not even rational, of course...)

Oesterle 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 $\left\{ \begin{array}{l} \lambda \leq \alpha^3 \rightarrow \text{Weil estimate is best} \\ \quad \quad \quad \text{(i.e., optimal is given by} \\ \quad \quad \quad 1 + \frac{1}{2}(t + t^{-1}) = 1 + \cos \varphi) \\ \lambda = \alpha^4 \rightarrow \text{Suzuki (char} = 2) \\ \lambda = \alpha^6 \rightarrow \text{Ree} \end{array} \right.$

Method:

Define m by $\boxed{\alpha^m < \lambda \leq \alpha^{m+1}}$. ($m = \lceil \frac{\log \lambda}{\log \alpha} \rceil$)

I will assume $m \geq 2$. (if not, $g = 0$ is ok ...)

Put $u = \frac{\alpha^{m+1} - \lambda}{\lambda \alpha - \alpha^m}$; 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 $g \geq 3$, at least) is

$$\boxed{g = \frac{(\lambda - 1) \alpha \cos \varphi_0 + \alpha^2 - \lambda}{\alpha^2 - 2\alpha \cos \varphi_0 + 1}}$$

(When $g = 2$, 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 $T \subset S^d$,
with $|T| = m - 1$, with

$$(T) \quad - \int t^u \mu(t) = \alpha^u - \lambda \alpha^{-u} \quad \text{for } u = 1, \dots, m-1,$$

and the mass ν_z of $t \in T$ being strictly positive.
We also need $\nu_z = \nu_{\bar{z}}$, of course.

On the other hand, look for (c_n) s.t.

$$f(t) = 1 + \sum_{n=1}^{m-1} c_n (t^n + \bar{t}^n) \text{ is zero on } T$$

($c_n \geq 0$, $f(t) \geq 0$ on S^1).

If we can do this, we have a match (as seen before).

Lemma If T satisfies the condition (T), then T is contained in the set of solutions of

$$t^{m+1} + 1 + u(t^m + \bar{t}) = 0 \quad (1)$$

(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 .

$\mu = \sum v_t \delta_t$ so the integral is $\sum_{t \in T} v_t t^\eta = \alpha^\eta - \lambda \alpha^{-\eta}$
 $\eta = 1, \dots, m-1$

The system $\left[\sum_{t \in T} v_t t^\eta = \alpha^\eta - \lambda \alpha^{-\eta} \quad \eta = 1, \dots, m-1 \right] \quad (*)$

has $(m-1)$ linear eqns, $(m-1)$ unknowns, determinant is Vander Monde t ($t \in T$), so $\neq 0$.

So it has a unique solution $v_t = \text{---}$

Now force $v_t = v_{\bar{t}}$ for every $t \in T$. This will imply equation (1).

Rewrite (*) as follows:

(*) $\iff$ for every polynomial ϕ of degree $\leq m-1$, with constant term 0,

$$\left[\sum v_t \phi(t) = \phi(\alpha) - \lambda \phi(\alpha^{-1}) \right] \quad (**)$$

let

$$P(x) = \prod_{t \in T} (x - t)$$

$$\begin{aligned} T \text{ symmetric} &\implies P(x^{-1}) = P(x) x^{1-m} \\ &- \frac{1}{x^2} P'(x^{-1}) = P'(x) x^{1-m} + (1-m) P(x) x^{-m} \end{aligned}$$

So if $t \in T$, $-\frac{1}{t^2} = \bar{t}^2$:

$$\boxed{-\bar{t}^2 P'(\bar{t}) = P'(t) t^{1-\alpha}}$$

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 $Q_t(t') = 0$ for $t' \in T, t' \neq t$.

$$Q_t(t) = t P'(t)$$

Apply (**) to $\Phi = Q_t$:

get $v_t Q_t(t) = Q_t(\alpha) - \lambda Q_t(\alpha^{-1})$

so
$$\boxed{v_t = \frac{Q_t(\alpha) - \lambda Q_t(\alpha^{-1})}{t P'(t)}}$$

rewrite :

$$t P'(t) v_t = \frac{\alpha P(\alpha)}{\alpha - t} - \lambda \frac{\alpha^{-1} P(\alpha^{-1})}{\alpha^{-1} - t}$$

we have $P(\alpha^{-1}) = P(\alpha) \alpha^{1-\alpha}$

so
$$t P'(t) v_t = P(\alpha) \left\{ \frac{\alpha}{\alpha - t} - \lambda \frac{\alpha^{-\alpha}}{\alpha^{-1} - t} \right\}$$

LeTh35

$$tP'(t)v_t = P(\alpha) \frac{1 - \alpha t - \lambda \alpha^{1-m} + t \lambda \alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2}$$

$$\text{Now } v_t = v_{\bar{t}} \implies \frac{1}{tP'(t)} \cdot \frac{1 - \alpha t - \lambda \alpha^{1-m} + t \lambda \alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2} = \frac{1}{\bar{t}P'(\bar{t})} \frac{1 - \alpha \bar{t} - \lambda \alpha^{1-m} + \bar{t} \lambda \alpha^{-m}}{1 - \alpha \bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2}$$

$$\text{Also } -P'(\bar{t}) = P'(t) \cdot t^{3-m}, \text{ so}$$

$$\frac{1}{t} \cdot \left\{ \frac{1 - \alpha t - \lambda \alpha^{1-m} + t \lambda \alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2} \right\} = \frac{-1}{t^{2-m}} \cdot \left\{ \frac{1 - \alpha \bar{t} - \lambda \alpha^{1-m} + \bar{t} \lambda \alpha^{-m}}{1 - \alpha \bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2} \right\}$$

$$\text{so } -t^{1-m} \cdot \left\{ \frac{1 - \alpha t - \lambda \alpha^{1-m} + t \lambda \alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2} \right\} = \left\{ \frac{1 - \alpha \bar{t} - \lambda \alpha^{1-m} + \bar{t} \lambda \alpha^{-m}}{1 - \alpha \bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2} \right\}$$

$$-t^2 (1 - \alpha \bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2) = 1 - \alpha t - \alpha^{-1}t + t^2$$

So end up with

$$-t^{m+1} (1 - \alpha \bar{t} - \lambda \alpha^{1-m} + \lambda \alpha^{-m} \bar{t}) - (1 - \alpha \bar{t} - \lambda \alpha^{1-m} + \lambda \alpha^{-m} \bar{t})$$

$$t^{m+1} (1 - \lambda \alpha^{1-m}) + t^m (\lambda \alpha^{-m} - \alpha) - t (\alpha - \lambda \alpha^{-m}) + (1 - \lambda \alpha^{1-m}) = 0$$

$$u = \frac{\alpha^{m+1} - \lambda}{\lambda \alpha - \alpha^m} = \frac{\alpha - \lambda \alpha^{-m}}{\lambda \alpha^{1-m} - 1}$$

$$\text{So } t^{m+1} + 1 + u(t^m + t) = 0.$$



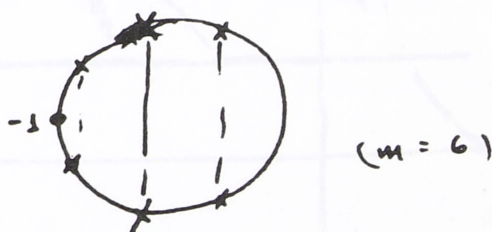
Note this works for any m ; our choice of m is equiv
to $u \in [0, 1)$.

Now, study the equation $\cos \frac{m+1}{2} \varphi + u \cos \frac{m-1}{2} \varphi = 0$,
where $0 \leq u < 1$.

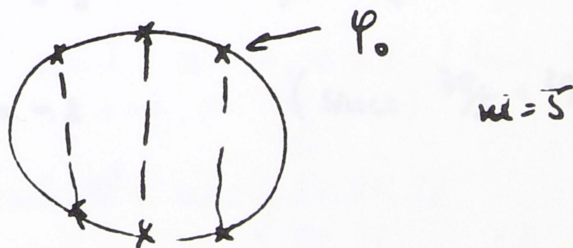
$$F(\varphi) = \frac{\cos \frac{m+1}{2} \varphi}{\cos \frac{m-1}{2} \varphi}$$

(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~~ even: -1 is a solution

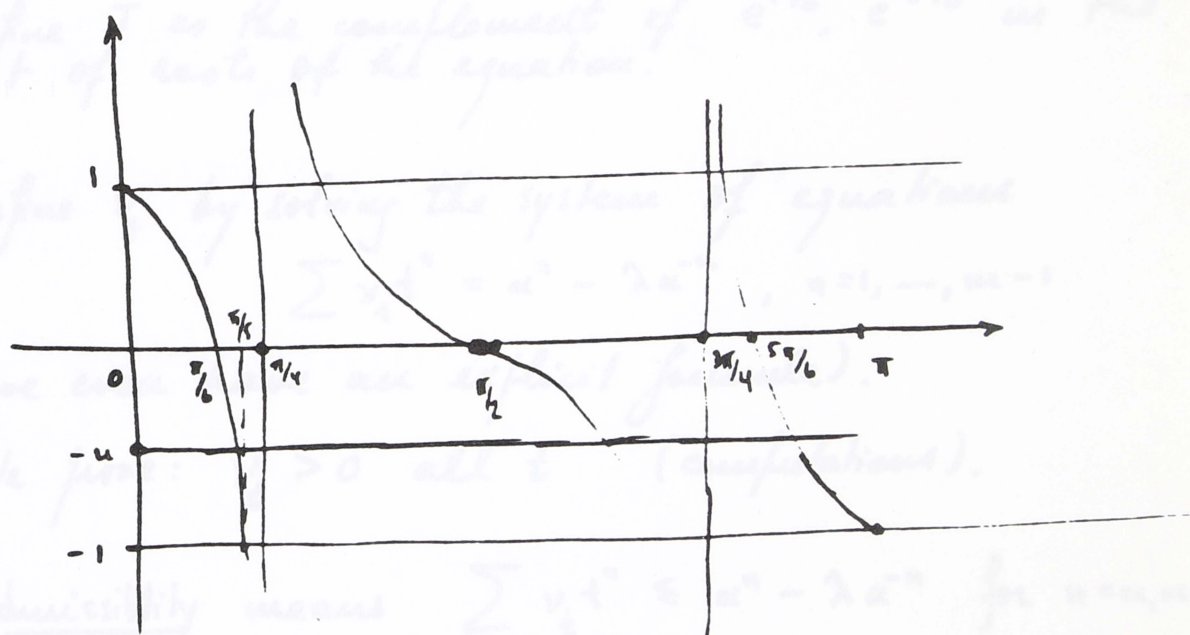


if m is odd: -1 is not a solution



Take $m=5$, for instance.

Graph on $0 \leq \varphi \leq \pi$ of $F(\varphi) = \frac{\cos 3\varphi}{\cos 2\varphi}$



$$\cos 2\varphi = 0 \iff 2\varphi = \frac{\pi}{2}, \frac{3\pi}{2} \Rightarrow \varphi = \frac{\pi}{4} \text{ or } \frac{3\pi}{4}$$

$$F\left(\frac{\pi}{5}\right) = \frac{\cos \frac{3\pi}{5}}{\cos \frac{2\pi}{5}} = -1 \quad (\text{since } \frac{3\pi}{5} + \frac{2\pi}{5} = \pi)$$

Given $u \in [0, 1)$, I want $F(\varphi) = -u$ 3 times

We know: the first soln. is φ_0 , $\frac{\pi}{6} \leq \varphi_0 < \frac{\pi}{5}$
and that is the only soln in that interval.

(And the same happens from any u).

So we know:

the eqn. $t^{m+1} + 1 + u(t^m + t) = 0$ has exactly $m+1$ solus. 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 v_t by solving the system of equations

$$\sum v_t t^n = \alpha^n - \lambda \alpha^{-n}, \quad n=1, \dots, m-1$$

(we even have an explicit formula).

We prove: $v_t > 0$ all t (computations).

Admissibility means $\sum v_t t^n \leq \alpha^n - \lambda \alpha^{-n}$ 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 $\lambda = \frac{130}{V}$, bad N 's are

$\left\{ \begin{array}{l} \text{up to } \lambda = \frac{130}{V} \text{, bad } N \text{'s are} \end{array} \right.$	51, 52, 53
	70, 71, ..., 77
	98, 99, ... 110
	137, ...

guess. $\frac{\log \lambda}{\log \alpha} \approx \text{integer} \approx 0.4$
bad if

$N=50, g \geq 65$; $N=54, g \geq 72$

(For bad N 's, Ostrovi's result is not optimal.)

Now to give $f = 1 + \sum c_n (z^n + z^{-n})$ which will match.

Take $P(x) = \prod_{t \in T} (x - t)$; write

$$P(x)P(x^{-1}) = \sum_{n=-(m-1)}^{m-1} a_n x^n, \quad a_n > 0$$

Defn : $f(x) = \frac{1}{a_0} P(x)P(x^{-1})$

$$\therefore c_n = \frac{a_n}{a_0}$$

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

$$\frac{1}{2} \sum \chi_i = g = \sum c_n (\lambda \alpha^{-n} - \alpha^n)$$

(by the formulas!)

and we end up with $g = \frac{(\lambda-1)\alpha \cos \varphi_0 + \alpha^2 - \lambda}{\alpha^2 - 2\alpha \cos \varphi_0 + 1}$.

[Recall: the zeta fct of a curve is

$$\frac{\prod_{a=1}^{2g} (1 - q^{1/2} e^{i\psi_a} T)}{(1-T)(1-qT)}$$

ν_t is connected to $\prod (1 - q^{1/2} e^{i\psi_a} T)^{\nu_t}$

So number field analog: replace the zeros of ζ by a measure.

Remark: If λ large w.r.t. $\alpha (= q^{1/2})$

Then $\psi \approx 0$, 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 $\psi \approx \frac{\pi}{m}$, $m \sim \frac{\log \lambda}{\log \alpha}$.

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

Start with the example

$$f(\theta) = \frac{1}{c} \sum (1 + 2x_1 \cos \theta + \dots + 2x_m \cos m\theta)^2$$

$$x_i \geq 0 , c = 1 + 2x_1^2 + \dots + 2x_m^2 .$$

1st choice : $x_1 = 1$, $x_2 = 0.7$, $x_3 = 0.2$

$$\text{gives } N \leq 0.83g + 5.35$$

$g=1 \rightarrow$ 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. , $g=5 \Rightarrow N \leq 4.15 + 5.35 \leq 9.50 \rightarrow N \leq 9$ and we'll construct $N=9$ curves ~~later~~ 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 Oort's

3rd choice: $1, 0.8, 0.6, 0.4, 0.1$

$$N \leq 0.6272g + 9.562$$

for $g = 50$, $N \leq 31.36 + 9.562 = 40.9\dots$

$$\text{so } \underline{N \leq 40}.$$

This justifies all the upper bounds on the table except for $g=7$. tables: see pp. SeTh 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 $\pi_1, \bar{\pi}_1, \pi_2, \bar{\pi}_2, \dots, \pi_7, \bar{\pi}_7$.

We'll know χ if we know N over $\mathbb{F}_2, \dots, \mathbb{F}_{2^d}$; if $a_d = \#$ closed pts of deg d .

Need: $a_1, a_2, \dots, a_7$.

Know: $a_1 = 11$

Maximal number of points of a curve of genus g
over the field $\mathbb{F}_2$

g	Max. nber	g	Max. nber	g	Max. nber
0	3	10	12 or 13	20	19, 20 or 21
1	5	11	13 or 14	21	21
2	6	12	14 or 15	...	
3	7	13	14 or 15	39	33
4	8	14	15 or 16	...	
5	9	15	17	50	40
6	10	16	16, 17 or 18		
7	10	17	17 or 18		
8	11	18	18 or 19		
9	12	19	20		

Bounds for $N = \text{Max. Nber}$

$$N \leq 0.83g + 5.35$$

$$N \leq 0.766g + 5.97$$

$$N \leq 0.6272g + 9.562$$

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
$N \leq$	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
$N \leq$	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
$N \leq$	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
$N \leq$	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
$N \leq$	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
$N \leq$	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
$N \leq$	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								
$N \leq$	78	79	79	80	80	81	82	82								

$$\begin{aligned} \text{Let } f &= \frac{25}{109} (1 + \cos \theta) \left(1 + \frac{6}{5} \cos \theta + \frac{6}{5} \cos 2\theta\right)^2 \\ &= 1 + \sum 2c_n \cos n\theta \\ c_1 &= \frac{98}{109}, \dots, c_5 = \frac{9}{218} \end{aligned}$$

We have

$$\sum_{d=2}^5 da_d \sum_{\substack{n \in \mathbb{N} \\ n \equiv 0 \pmod{d}}} c_n q^{-n/2} \leq g + \sum c_n q^{-n/2} - (N-1) \sum c_n q^{-n/2}$$

$$\begin{aligned} 0.743a_2 + 0.408a_3 + 0.165a_4 + 0.036a_5 &\leq 7 + 4.577 - \\ &\quad - 11.506 \\ &\leq 0.069 \end{aligned}$$

This implies

$$a_2 = a_3 = a_4 = 0, a_5 \leq 1.$$

Have a_6 and a_7 to consider, still:

$$\text{Let } a_5 = \alpha, a_6 = \beta, a_7 = \gamma \quad (\text{so } \alpha = 0 \text{ or } 1).$$

$$\text{Have } \pi_1, \dots, \pi_7, \quad u_i = \pi_i + \bar{\pi}_i$$

$$\text{Define } f(T) = \prod_{i=1}^7 (T - u_i) \in \mathbb{Z}[T].$$

this has real roots in the interval $[-2\sqrt{2}, 2\sqrt{2}]$.

Writing $f(T)$ in terms of α, β, δ :

$$f(T) = T^7 + 8T^6 + 21T^5 + 14T^4 - 19T^3 + (\alpha - 20)T^2 + (8\alpha + \beta - 5)T + 31\alpha + 8\beta + \delta - 106.$$

Theorem: Such a polynomial $f_{\alpha, \beta, \delta}$ with $\alpha, \beta, \delta \in \mathbb{Z}$, $\alpha = 0$ or 1 , has all its roots real and in $[-2\sqrt{2}, 2\sqrt{2}]$ if and only if $(\alpha, \beta, \delta) = (0, 11, 22)$.

[Sturm $\rightarrow$ condition for $f_{\alpha, \beta, \delta}$ to have roots in some interval]

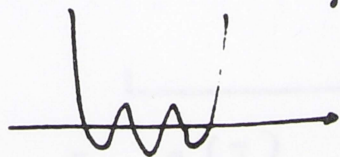
$f_{\alpha, \beta, \delta}$ all roots real $\rightarrow$ derivative also has real roots

So first check that $f''(T)$ does have four real roots.

Have $\alpha = 0$ or $\alpha = 1$.

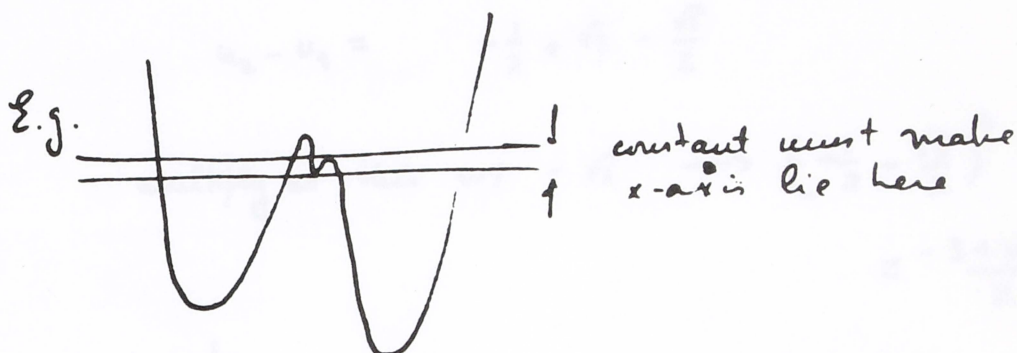
($\alpha = 0$) take $f''(T)$ is ok.

know $f'(T)$ up to translation



to adjust the constant, look at highest min, lowest max

Se Th 40



This gives : $\begin{cases} \text{if } \alpha=1, & 5 \leq \beta \leq 10 \\ \text{if } \alpha=0 & 9 \leq \beta \leq 13 \end{cases}$

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). $\square$

(Conditions are $\gamma \leq 22, \gamma \geq 22, \gamma \leq 22, \gamma \geq 22, \gamma \leq 25, \gamma \geq 18, \gamma \geq -9650$).

$$\begin{aligned} \text{We find } f &= T^7 + 8T^6 + 21T^5 + 14T^4 - 19T^3 - 20T^2 + 6T + 4 \\ &= (T+2)(T^2+2T-2)(T^2+T-1)(T^2+3T+1) \end{aligned}$$

$$= \overbrace{(T+2)(T^2+2T-2)}^{g(T)} \cdot \overbrace{(T^2+T-1)(T^2+3T+1)}^{h(T)}$$

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 unit.

e.g. , $u_2 = -1 + \sqrt{3}$ $u_4 = \frac{-1 + \sqrt{5}}{2}$

$$u_2 - u_4 = -\frac{1}{2} + \sqrt{3} - \frac{\sqrt{5}}{2}$$

multiply by this w/ $-\sqrt{3}$ $\rightarrow \left(-\frac{1}{2} - \frac{\sqrt{5}}{2}\right)^2 - 3 = \frac{3\sqrt{5}}{2} - 3$
 $= -\frac{3 + \sqrt{5}}{2}$ unit.

etc.

So $f = g \cdot h$
 this is impossible for a jacobian, so the curve C does not exist. $\square$

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	$\frac{12 \text{ or } 13}{13}$	

$bd = 13$

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, 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 poly which passes through all pts:

get $x^3y + y^3z + z^3x + x^2yz + y^2zx + z^2xy + x^2yz + y^2zx = 0$

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

$$xy + yz + zx + xy + yz + zx + xy + yz + zx = 0 \quad !)$$

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 twist of the Klein curve

$$G = SL_3(\mathbb{F}_2) = GL_2(\mathbb{F}_2) \text{ order } 168$$

G acts on $\mathbb{P}_2$; to find inv. polynomials

do:

$$Q_4(x, y, z) = \frac{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^3 & y^3 & z^3 \end{vmatrix}}{\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^4 & y^4 & z^4 \end{vmatrix}} \quad \text{has degree } 4$$

$$\begin{vmatrix} x & y & z \\ x^2 & y^2 & z^2 \\ x^4 & y^4 & z^4 \end{vmatrix}$$

= product of all the linear forms

→ this gives the Klein curve

This has no rat'l point.

If we twist it by a $G_7 \subset G$, (i.e., wrt $\begin{pmatrix} \mathbb{F}_2 \\ C_7 \\ \mathbb{F}_2 \end{pmatrix}$)
we get the curve above.

For $g=4$: if not hyperelliptic, can. embedding in $\mathbb{P}_3$
then curve = inters. of surfaces

$$\text{curve} = (\text{quadric surface}) \cap (\text{cubic surface})$$

transversal inters,
but surfaces can have
singularities.

if quadric = $\mathbb{P}_1 \times \mathbb{P}_1$, 1 pts — so not obvious at
once we can get 8.

On $\mathbb{P}_1 \times \mathbb{P}_1$, 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.

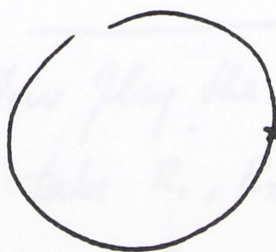
Try to find C_2
 $\downarrow$ abelian extn.
 C_1

With "little" ramification ($g(C_2)$ small)
 and s.t. "many" rational points split.

1st case: $C_1 = \mathbb{P}_1$, $g=0$

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 $\mathcal{C}_m$.

$$0 \rightarrow \mathbb{F}_8^\times \rightarrow \mathcal{C}_m \xrightarrow{\deg} \mathbb{Z} \rightarrow 0$$

CFT: finite quotients of $\mathcal{C}_m$ describe the ab.
 extns w/ cond. $\leq Q$.

Choose a rat'l point $R \in P_1(F_2)$.

$$R \mapsto Cl_m, \quad \deg R = 1$$

So let $G =$ quotient of Cl_m by $\langle R \rangle \cong F_8^*$.

So corresp to

$$\begin{array}{c} C \\ \downarrow \textcircled{7} \\ P_1 \end{array}$$

Frob R is killed $\Rightarrow R$ splits completely giving 7 pts.
(and $\Rightarrow$ no const. field extn.)

$$2g(C) - 2 = 7(-2) + \underbrace{6 \cdot 3}_{\text{sum of Artin conductors}}$$

$$2g = 2 - 14 + 18 = 6$$

$$\text{So } \boxed{g=3, N=7}$$

Now play the same game as follows:

take R_1, R_2 rat'l points on P_1

$m = 4 \cdot R_2$, construct G as before, $G = Cl_m / \langle R_1 \rangle$
 $\cong$ local group mod 4.

See Th 4.3

$$\begin{aligned} \text{get: } G &\cong \text{local gp mod } 4R_2 \\ &= \{1 + \alpha_1 t + \dots + \alpha_3 t^3\} / 1 + t^4 \\ &\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

So find $\begin{array}{c} C \\ \downarrow G \\ \mathbb{P}_1 \end{array}$ s.t. : $\begin{cases} R_1 \text{ splits completely into 8 pts} \\ R_2 \text{ is completely ramified} \end{cases}$ ^(rat'l)
 $\rightarrow 1 \text{ pt which is rat'l.}$

$$2g - 2 = 8(-2) + \sum f_x$$

Characters on G

$$\chi = 1 : f = 0$$

$$\chi \text{ trivial on } t^3 : f = 2$$

$$\chi \text{ trivial on } t^2 : f = 3 \text{ times}$$

$$\text{—————} : f = 4 \text{ four times}$$

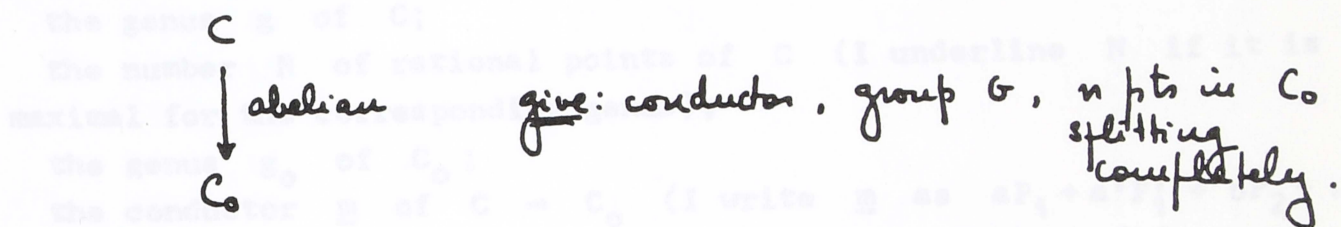
$$\text{So } 2g - 2 = -16 + 2 + 6 + 16 = 8 \Rightarrow \boxed{g = 5}$$

So this gives the curve we need for $g = 5$. $\square$

11/26 ($q=2$, cont.) See table, pp. ScTh 43b, 43c

Construction

Start from sth you know, say $g=0, 3$ pts, C_0



$g=50$ $N=40$? $40 = 8 \times 5$

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 $P_1, \dots, P_5 \rightarrow 0 \implies$ pts split completely.

Choose a pt P_1 , 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 $m = 2P_1$

TABLE
of curves of low genus over $\mathbb{F}_2$ having many points

Each curve C is obtained as an abelian covering $C \rightarrow C_0$ of a curve C_0 of lower genus, occurring 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_0 of C_0 ;

the conductor $\underline{m}$ of $C \rightarrow C_0$ (I write $\underline{m}$ as $aP_1 + a'P_1' + bP_2 + \dots$ where $P_1, P_1', P_2, \dots$ are distinct closed points of C_0 of degrees 1, 1, 2, ...);

the Galois group G of the covering $C \rightarrow C_0$ (a cyclic group of order m is denoted by (m));

the number n of rational points of C_0 which split completely in

the number r of rational points of C_0 which are totally ramified in C .

For all the cases considered in the table, we have $N = r + |G|n$.

g	N	g_0	$\underline{m}$	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	$4P_1$	$(2) \times (4)$	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

Table (continued)

g	N	g_0	$\underline{m}$	G	n	r
10	12	2	$2F_7$	(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	<u>17</u>	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	<u>20</u>	1	$2P_6$	(2)×(2)	5	0
20	19	2	0	(19)	1	0
21	<u>21</u>	0	$P_2 + P_3$	(3)×(7)	1	0
39	<u>33</u>	1	$12P_1$	(2)×(2)×(2)	4	1
50	<u>40</u>	1	$2P_7$	(2)×(2)×(2)	5	0

Harvard, November 1985

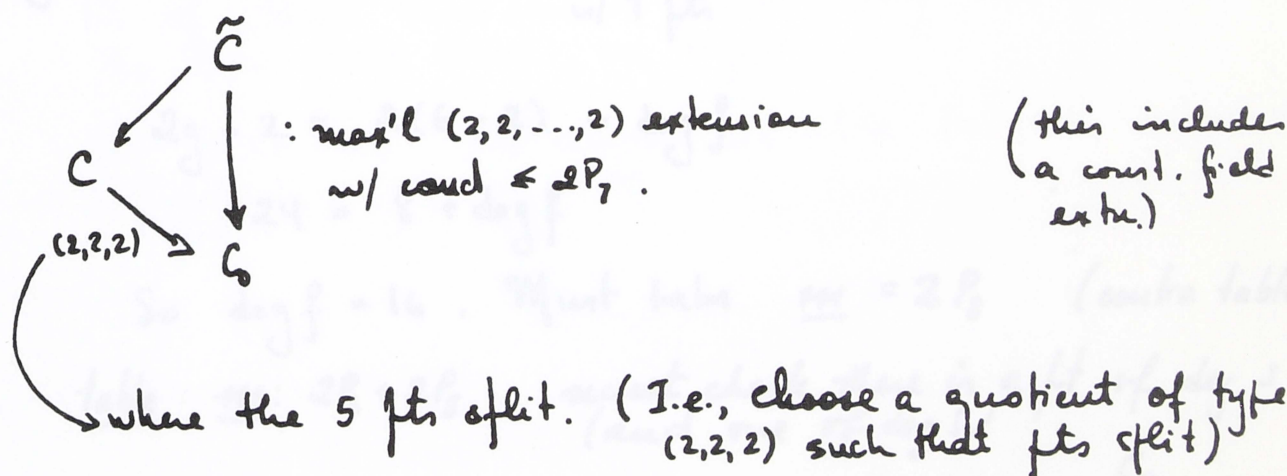
J. P. Saw.

look at $\mathcal{C}_m$:

$$0 \rightarrow L_m \rightarrow \mathcal{C}_m \rightarrow \mathcal{C}_0 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z} \rightarrow 0$$

$$L_m = \mathbb{F}_2[[x]]^x / \{1 + (x^2)\} = \mathbb{F}_2^* \times \mathbb{F}_2$$

$$\mathcal{C}_m / 2\mathcal{C}_m = \mathbb{F}_2^* \times \mathbb{Z}/2\mathbb{Z} \quad \text{of type } (2, \dots, 2), \text{ rank } 8.$$



$$2g - 2 = 2^3 (2g_0 - 2) + \sum_{\chi \neq 1} \deg f_\chi$$

$$2g - 2 = 8 \times 0 + (8-1) \times 14$$

$$g = 1 + 7 \times 7 = 50.$$

χ = char of order 2
 so cond = $2P_7$ or 0
 but can't be zero so $f_\chi = 14$.

With $2P_6$, would get $\overbrace{4.5}^{\text{extra (2,2) w/}} = \frac{20}{\cancel{4}} \text{pts}$ and

$$2g - 2 = 0 + (4-1) \times 12$$

$$\text{so } \boxed{g = 19}.$$

With $2P_5$, get extr. of deg 2, w/

$$2g - 2 = 0 + 10 \rightarrow \boxed{g = 6, N = 10}$$

$$\boxed{g = 13} \quad N = 14, \quad g_0 = 3 \wedge, \quad |G| = 2$$

w/ 7 pts

$$2g - 2 = 2(6 - 2) + \deg f$$

$$24 = 8 + \deg f$$

So $\deg f = 16$. Must take $\pi = 2P_6$ (contra table!)

table: $\pi: 2P_3 + 2P_5$

must check there is a pt of deg 3 (and one of deg 5)

take $L_\pi, \mathbb{Z}$

$$\text{so } rk = 1 + \deg \pi = 9$$

so used out as before.

Recall construction: $C_3 \rightarrow C_0 = P_3$

res field = $\mathbb{F}_3$ ramif at a $P_3 \in C_0$
so C_3 has a pt of deg 3

$$g = 20 \quad N = 19, \quad g_0 = 2, \quad h = 19$$

$$Cl_0 = \mathbb{Z} \times \mathbb{Z}/(19)$$

P_1

Split so that $P_1 \rightarrow$ generator. Get an extra. by the quotient.
Then $2g - 2 = 19(22 - 2) \rightarrow g = 1 + 19 = 20.$

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.