Notes for the Oberwolfach meeting, “Explicit Methods in Number Theory”

William A. Stein

July 2001

```
Disclaimer: These are my notes, and as such they are my biased
personal opinions about what I saw during the lectures.  Text wrapped
in "[ ]"'s represents my remarks on the lecture.  For the most part
these notes are not in LaTeX.  They're in my own "pseudo-TeX", which I
use, e.g., when writing emails.  If you would like to suggest any
corrections to these notes, please write to me at was@math.harvard.edu.
```

TABLE OF CONTENTS

21. D. BYEON (16.00-16.30): Indivisibility of class numbers of real quadratic fields
22. X. ROBLOT (16.45-17.15): Stark-Chinburg's conjecture on icosahedral representations
23. B. ALLOMBERT (17.30-18.00): Computing automorphisms of Galois number fields with supersolvable Galois group

7-8:30 talk with E. Kowalski

24. M. JACOBSON (20.15-20.45): Fundamental unit computation in practice
25. M. GIRARD (20.50-21.20): Explicit computation of the group generated by the Weierstrass points of some plane quartics
26. H. GANGL (21.30-22.00): Calculations of the homology of GL(n,Z)

Day 5: Friday

27. D. BERNSTEIN (9.15-9.50): Finding polynomial values of small height
28. J.-F. MESTRE (10.15-11.00): Lifting of Galois extensions from k to k(t)
29. J. KLUENERS (11.15-12.00): Counting Galois extensions of number fields

30. M. STOLL (14.00-14.30): Reduction of binary forms -- a progress report
31. D. KOHEL (14.35-15.05): Computational aspects of Shimura curves
32. N. ELKIES (15.15-16.00): Progress report on genus 2

TALK: 1. MESTRE

SATOH. Canonical lift to count points on E/F, with F of small characteristic. Every month, somebody has an idea to turn this into an algorithm.

Idea of Legendre, Gauss: AGM = arithmetical geometrical mean. (1780)

I.

1. Facts about the AGM

$a, b > 0$;
$a_0 = a$, $b_0 = b$,
$[a_n, b_n] = [(a_{n-1} + b_{n-1})/2, \sqrt{a_{n-1}b_{n-1}}]$
$\longrightarrow M(a,b)$ = AGM of a and b,
convergence is quadratic: $|a_{n+1}-b_{n+1}| < c\, |a_n - b_n|^2$.

[Let's code this in MAGMA and play:

```
function agm(a,b, n)
   for i in [1..n] do
      sum := a+b;
      prod := a*b;
      a := sum/2;
      b := Sqrt(prod);
      [a,b];
   end for;
   return [a,b];
end function;
```

]

For fun, when Gauss was 13, he computed M(1,sqrt(2)) up to 60 digits.

Int_{0}^{\pi/2} dTheta / sqrt(cos^2(theta) + 2*sin^2(theta))

= pi / (2*M(1,Sqrt(2))).

Then he generalized:

Int_{0}^{\pi/2} dTheta / sqrt(a^2 cos^2 + b^2 sin^2)

= pi / (2*M(a,b)).

Proof --

theta = phi(theta')

Int_{0}^{pi/2} dTheta / Sqrt(a^2 cos^2 + b^2 sin^2)

= Int_{0}^{pi/2} dTheta' / Sqrt(a_1^2 cos^2 + b_1^2 sin^2)
= ... = 1/M(a,b) Int_{0}^{pi/2} dTheta/1.

2. a, b in C.

Which choice for sqrt?
If, after some steps, where you take any square root,
you should always take the "good one", (sqrt with real part > 0)
it converges.
AUDIENCE: what if real part = 0!!?
(no useful response)

The inverse of the limits is a lattice Z*alpha+Z*beta.

ZAGIER: Bzzzt. They're all in the right half plane. You should
instead take the sqrt that is closer to the usual mean.

ELKIES: That's what I thought! [Indeed, he had suggested that
immediately, but wasn't as insistent as Zagier.]

3. |q| < 1
Theta_0(q) = sum_{n in Z} q^{n^2}.
Theta_1(q) = sum_{n in Z} (-1)^n q^{n^2}.

(Theta_0(q)^2 + Theta_1(q)^2)/2 = Theta_0^2(q^2),

Somehow he claims that

M(Theta^2_0(q) ,Theta^2_1(q)) = 1.

Given a,b > 0 there exists alpha and q with |q|<1 such that
a = alpha Theta_0^2(q), b = alpha Theta_1^2(q).
Then M(a,b) = alpha*M(Theta_0^2(q), Theta_1^2(q)) = alpha.

Link with elliptic curves:

Int_{0}^{pi/2} dTheta / Sqrt(a^2 cos^2(theta) + b^2 sin^2(theta))

= Int_{0}^{infinity} dX / sqrt(x(x+a^2)(x+b^2) = omega.

E_{a_i, b_i}: y_i^2 = x_i(x_i+a_i^2)(x_i+b_i^2)

E_{a_1,b_1} --phi--> E_{a_0, b_0} is a 2-isogeny

phi^*(omega_1) = omega_0, where omega_i = dx_i/y_i

E_{a_i, b_i} has same omega.

E_{a_inf, b_inf}: y^2 = x(x+M^2(a,b))^2,
which is singular, so integral is very easy.

II. p-adic Case

K local field, pi uniformizer.

(1) Henniart - M.

a, b in K^*
b/a = 1 (mod 8pi).

Then the limit exists and the process is quadratically convergent.

Sqrt(ab) = a*sqrt(b/a),

and we choose sqrt( ) = 1 (mod 4*pi).

Suppose y^2 = x(x+a^2)(x+b^2) is a Tate curve.

Tate j = 1/q + ... can be computed quickly.

(2) K/Q_2 unramified of degree d.

Let E/K be an ordinary elliptic curve. Let P_0 be "the" point of
order 2 which corresponds to mu_2. Take this point as origin:

y^2 = x(x - a^2)(x-b^2)

(0,0) |---> P_0.

b/a = 1 (mod 8).

Sqrt(ab) = a Sqrt(b/a)

Sqrt(1+8( )) = 1+4( ).

```
                                phi_n
E_{a,b} <-- E_{a_1, b_1} <-- ... <----- E_{a_n, b_n}
```

phi_n^*(omega_n) = omega_{n-1}.

```
Thm: j(E_{nd}) ----> j(E), where E is the canonical lifting
               n->oo
```

of \tilde{E}.

More precisely, b_{nd}/a_{nd} converges.
This convergence is not quadratic. It is *linear*.

Suppose now that the initial curve is the canonical lift E.
Then E is isomorphic to E_d.

Lemma: k of characteristic 0.
E/k: f: E ---> E
Tr(f) = f + f^ = f^(omega)/omega + deg(f) omega/f^*(omega) in Z.

f^*(omega) = mu*omega, where mu in k.

Algorithm:

(1) Compute a_n, b_n until n = [d/2] .
(2) a_m, b_m --> (a_{m+d}, b_{m+d})

Then

Etilde(F_{p^d}) = p^d + 1 - (a_m/a_{m+d} + p^d a_{m+d}/a_m),

where p = 2.

Gudry and Hanley implemented this nicely.

TALK: 2. O'NEIL: Descent

Descent:
Part 1. Image of E(K) in Selmer.
Part 2. models for elements of Sel.

* If E has full n-torsion,

H^1(G_K, E[n]) isom K^*/(K^*)^m x K^*/(K^*)^m,

once we choose basis <S, T> of E[n] with e_n(S,T) = zeta.

* n = 3: E_{lambda}: x^3 + y^3 + z^3 + lambda xyz = 0.
O_{E_lambda} = (1,-1,0). (origin of group law)

Two maps: M_S = diag(1,zeta, zeta^2),
M_T = [[0,1,0], [0,0,1], [1,0,0]].

Elements of Sel_3(E_lambda) are given as a pair (a,b).

Part 1. P |---> (a,b) = (f_S(P), f_T(P)),

div(f_S) = 3(S) - 3(O)
div(H_O) = 3(O), H_S (gives f_S, up to scalar)
also there exists g_S, f_So[3] = g_S^3.

```
        div(g_S) = sum_{3u = s} (u),   where 3u=s
                 * So u = -2u+s.
                 * Look for fixed points of x |--> -2x+s.
                 * Get a cubic curve in P^2, that is
                   defined by a "generalized Henssian".

        Used Maple to find scalar.

Part 2. (a,b) |---> model in P^2.

         in

        H^1(G_K, E[3])

Thm: (a,b) in H^1(G_K,E[n]) has index | n <==> (a,b)_{Hilb,n} = 1.

     (a,b) in Sel_3 ===> (a,b)_{Hilb} = 1.
                    i.e., let alpha^3 = a, there exists beta in K(alpha)
                                            N_{K(alpha)/K}(beta) = b.

Write beta = beta_0 + beta_1*alpha + beta_2*alpha^2
find C = C_{(a,b)} = C_{(alpha,beta)}

  C ----------> P^2
  |              | <--- M_S, M_T
 \|/            \|/
  C ----------> P^2

The cubic F_{(alpha,beta)} defining C in P^2 is fixed by M_S, M_T,
so it's well defined (??)

THEOREM:

  F = explicit formula in terms of a, lamba, alpha, beta...

Remarks:
  -- set up extends to n=5 (or any prime)
  -- M_S, M_T act on V <-- space of dim 5 of quadrics


--------------------------------------------------------------
TALK 3. ZAGIER:

On Binary Cubic Forms

 * cubic forms & their class numbers
 * zeta functions (Shintani)
 * cubic forms <---> cubic rings
 * cubic forms <---> quadratic forms

Reminder: Binary quadratic forms

[A, B, C]    q(x,y) = Ax^2 + Bxy + Cy^2
            D(q) = B^2 - 4AC
```

```
 Let Q = {[A, B, C] : A, B, C in Z }   ----- D ----> Z  (D = B^2-4AC)
                                                    /|\
                                                     | -4
                                                     |
    Q^*= {[A, 2B, C] : A, B, C in Z }  ----- D^* --> Z  (D^* = AC-B^2
```

Q_D = {[A,B,C] | B^2-4AC=D}.
G = SL_2(Z).

Questions:

* class numbers
* analytic questions
* algebraic interpretation

h(D) = #(C_D^0 / G), where C_D^0 is the set of primitive forms.
H(D) = sum_{q in Q_D/Gamma} 1/ |Gamma_q|. (only D < 0 is interesting)

The only descent question is "what are the H(D) with D<0."
The generating function for H(D) is a weight 3/2's modular form, essentially.

Also C_D^0/G isom Cl_D (class group!)

```
|D| | 7   8   11    23   41   71
---------------------------------
    | 1   1    1     3    5    7

--------------------------------
```

C = {[a,b,c,d], a,b,c,d in Z }

F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3
Delta(F) = 18abcd - 4ac^3 + 4b^3d + b^2c^2 - 27a^2d^2.

C^* = {[a,3b,3c,d], a,b,c,d in Z }
F(x+x',y+y') = F(x,y) + F(x',y') mod 3.

D(F) = a^2d^2 - 3b^2c^2 + 4ac^3 + 4b^3d-6abcd = -1/27 Delta(F).

Class Numbers:

H(D)   = sum_{F in C_D/Gamma} 1/#Gamma_F   (always finite)

H^*(D) = sum_{F in C_D^*/Gamma} 1/#Gamma_F

H_3(\pm N), H_3^*(\pm N) (GL(2) acts on C(\C).... orbits, etc. the group has the same dimension as the space.)

The numbers H_3(\pm N), H_3^*(\pm N) all exist, and they are all interesting!

On the analytitic side, Shintani made four Dirichlet series:

Z_{\pm} (s) = \sum_{1}^{oo} H(+-N)/?...

```
     Z_{\pm}^* (s)
                jointly have mereomorphic continuation.
```

For some reason, nobody bothered to compute H^*(D), until five years ago. An actual table was made by Ohno (grad student in Japan then), shows:

There are really TWO SERIES of numbers. Two are the same, and 3 times one is another.

H_3(D) = H_3^*(D)*(up to factor of 3)

There is a proof in Nakagawa (Inv. 98).

How to map cubic forms to quadratic forms.

```
  C_D^* ------------> Q_D

  C_D^*/Gamma --> Q_D / Gamma.
```

The map

```
  F = [a,3b,3c,d] |----> q_F = [b^2-ac, bc-ad, c^2-bd] = [A, B, C]
```

is Gamma equivariant.

```
Proofs: (1) direct computations
        (2) check for sign change, interchange, and translation,
            and these three generate SL_2(Z).
        (3) q_F = -1/6[F_{xx}, F_{xy}; F_{yx}, F_{yy}]
                  = -[ax+by, bx+cy; bx+cy, cx+dy]
        (4) Invariant theory: S^3(ZxZ) ---> S^3 tensor S^3
                         --> S^0 + S^2 + S^4 + S^6 --> S^2
```

Eisenstein (1844): Let D be fundamental.

```
   C_D^*/Gamma --> Q_D/Gamma = Cl_D
       a\         \/
         \ Cl_D[3]
```

a is 3-1 if D positive and iso when D negative.
In Eisenstein's paper, he gave a proof in a special case.
He used the syzygy [the word "syzygy" mean "linear relation"]:

```
   4 q_F(x,y)^3 = G_F(x,y)^2 - D(F) F(x,y)^2

     G_F = 1/3 * det ...
```

Let

```
   tau_F = trilinear form associated to F.
```

```
q_F(xsi) q_F(eta) q_F(zeta) = (tau_{G_F}(xsi,eta,zeta)^2 -
                  D tau_F(xsi, eta, zeta)^2) / 4.
```

Now we come to the things that are "new":

C_D^* ---> Q_D = disjoint union over n in Z_{>0}, n^2 | D of
                 n * Q^0_{D/n^2}.

Thus, for D<0, H(D) = sum_{n^2 | D} h^(D/n^2)/(something in 1,2,3)

Also, C_D^* is disjoint union over n^2 | D of
         C_{D,n}^* = {F | q_F = nQ for some n in Z, Q in Q^0_{D/n^2})

When |G_F| = 3, find that F = [alpha, beta, -3alpha-beta, alpha],
D = (beta^2 + 3*alpha*beta + 9*alpha^2)^2.

In any case,
 H_3^*(D) = sum_{n^2 | D} H_3^*(D,n)

So, taking only primitive things, get
  C_{D,1}^*/Gamma --===--> Cl_D[3]   (maybe up to something with 3's?)

Recall that
  Cl_D = { a = fractional proper O_D-ideals} / linear equivalence

  Cl_D[3] = {(a, theta) | a^3 = (theta) } /
                  (a,theta) equiv (lambda a, lambda^3)

           here a in I_D, theta in K^*, theta = a^3

 Theorem: C_{D,n}^* = {(a, theta) : a in I_D, theta in a^3, [a^3:(theta)]=n}
                          modulo stuff.
    and sum C_{D,n}^* n^{-s} = sum of things zeta_D(A^3,s)
                              = sum of things L_K(s,chi).

TALK: 4. LENSTRA: Zeta functions of curves over almost finite fields.

Let k be a finite field in kbar = union_{n >= 1} k_n, [k_n : k]=n.

Let X be a scheme of finite type over k.

X(kbar) = union_{n>=1} X(k_n)

Frobenius (raising coordinates to #k)
  phi: X(kbar) --> X(kbar)   (a bijection)

N_n = N_n(X) = #X(k_n) = #{x in X(kbar) : phi^n(x) = x}.

a_n = a_n(X) = #{x in X closed point : deg(x) = n}
    = #{n-cycles of phi on X(kbar)}

sum_{d|n} d*a_d = N_n.

Z(X)(T) = prod_{n\geq 1} (1 - T^n)^{-a_n} in Lambda(Z).
If R is a ring, then Lambda(R) = 1 + T*R[[T]].

TZ'/Z = sum_{n\geq 1} N_n T^n. (logarithmetic derivative)

Let ell be a prime number. It isn't really important whether ell equals char(k) or not. "But certainly it will be one or the other." [Trademark Lenstra humor!]

Consider

   (Z(X) mod ell) in Lambda(F_ell).

We have three sequences:

(1) (a_n(X))_{n=1}^{\infty}

(2) (N_n)_{n=1}^{infty}

(3) (coefficients of Z(X))_{n=1}^{infty}

Relations in the diagram (a triangle)

(1) |---> (2)
(2) |-.-.-> (1) (-.-. means "bad denominators")

(3) |---> (2)
(2) |-.-.-> (3)

(3) |-.-.-> (1)
(1) |-.-.-> (3)

Fact: It is equivalent to know the following:

  (a) Z(X) mod ell

  (b) sum_{i=0}^{oo} a_{n*ell^i}(X)*ell^i as an ell-adic integer
      for each n>=1, with ell\nmid n.

  (c) lim_{i-->oo} N_{n\ell^i}(X) as an element of Z_ell for
      each n>=1.

Union_{i>=0} k_{n\ell^i}

  (d) Z(X_K / K), where K = maximal ell-extension of k and
      X_K = X x_k K.

What is "knowledge"?

Let f and g be two functions on a set S. Then "knowing f(x) implies knowing g(x), for all x in S" means that there exists h such that h o f = g.

Proof of the fact:

prod_{n>=1, ell\nmid n} Z_ell ----======---> Lambda(F_ell)

The isomorphism sends
(b_n) to prod (1-T^n)^{-b_n}.

```
(Z(X) mod ell) = prod_{n=1}^{oo} (1-T^n)^{-sum_{i=0}^{oo} a_{n\ell^i}\cdot \ell^i}
               ell \nmid n
```

For (b) and (c) write
  N_{n\ell^i}(X) = \sum_{d | n} d \sum_{i=0}^{oo} ....

Exercise: If m >= 2, then knowing (Z(X) mod ell^m) [??] is equivalent
to knowing (Z(X) mod ell) and (a_n(X) mod ell^(m-1))_{n>=1}

Definition: A field K is "nearly finite" if it is algebraic over a
finite field and
   k' in K implies k' finite or [K:k'] < oo.

Let K be a nearly finite field, ell = char(K), postpone choice of k.

  G_K = Gal(Kbar/K) isom projlim_{all n with \ell \nmid n} Z/nZ

Y/K scheme of finite type
Each closed point y in Y has degree n for some n>=1, ell \nmid n.

Y/K/k. In fact, k can be chosen, so K is the maximal ell-extension
of k and Y = X_K, with X / k.

Then a_n(Y) =def= sum_{i>=0} a_{n*ell^i}*ell^i is an
ell-adic integer independent of the choice of the X.

Define Z(Y/K) = prod_{n>=1, \ell\nmid n}(1-T^n)^{-a_n(Y)} in /\(Z_ell).

TZ'/Z = \sum{n\geq 1} N_n T^n.

Remark: This well-defined zeta function can be written as a limit:

   Z(Y/K) = lim_{i--->oo} Z(X_{k_\ell^i})

[Which is how he *should* have defined it, no?]

Now to prove equivalence of (d) with others:

```
/\(Z_ell) -----rho--------> /\(F_ell)
   ||                          ||
   ||                          ||
prod_{n>=1} Z_ell ------> prod_{ell\nmid n} Z_ell.
```

Theorem: K, ell, Y as before. Then Z(Y/K) is a rational function
with all zeros and poles equal to roots of unity of order
coprime to ell.

1 The Definitions

Let $E/\mathbb{Q}$ be an elliptic curve that is an *optimal quotient* of $J_0(N_E)$, where $N = N_E$ is the conductor of E. Here $J_0(N)$ is the Jacobian of the algebraic curve $X_0(N)$ and a deep theorem implies that there is a surjective morphism $\pi : X_0(N) \to E$. The condition that E is optimal means that the induced map $\pi_* : J_0(N) \to E$ has (geometrically) connected kernel.

Definition 1.1. The *modular degree* of E is

$$m_E = \deg(\pi).$$

One reason that the modular degree is well worth thinking about is that an assertion about how m_E grows relative to N_E is equivalent to the ABC Conjecture.

Let $f = f_E = \sum a_n q^n \in S_2(\Gamma_0(N))$ be the newform attached to E.

Definition 1.2. The *congruence modulus* of E is

$$c_E = \#\left(\frac{S_2(\Gamma_0(N), \mathbb{Z})}{\mathbb{Z}f + (\mathbb{Z}f)^\perp}\right),$$

where $(\mathbb{Z}f)^\perp$ is the unique $\mathbb{T} = \mathbb{Z}[\ldots T_n \ldots]$-module complement of $\mathbb{Z}f$ in $S_2(\Gamma_0(N), \mathbb{Z})$. Equivalently,

$$c_E = \max\{c : f \equiv g \pmod{c} \text{ for some } g \in (\mathbb{Z}f)^\perp\ \}.$$

2 The History

- **<1984:** ??
- **1984:** Don Zagier wrote the often-cited paper *Modular parametrizations of elliptic curves* (1985), in which he gave an algorithm to compute m_E (sometimes?). The paper inclucced
  - A result of Ribet:

    Theorem 2.1 (Ribet). *If N_E is prime, then*

    $$m_E = c_E.$$
  - It also said
    $$c_E \mid m_E.$$
- **1998:** Frey and Müller published a wonderful survey: *Arithmetic of modular curves and applications.*
  - They ask: **Question 4.4**: Let E be an optimal quotient of any conductor. Does $m_E = c_E$?
  - They remark that $c_E \mid m_E$ and give two references [Ribet 83, Inventiones] and [Zagier 1985].
- **1995:** Cremona wrote a Math. Comp. paper, and computed m_E for every curve of conductor $\leq N$, where N is a few thousand.
- **2001:** Mark Watkins, who did a Ph.D. on the class number problem of Gauss, computed m_E for some curves with N_E **HUGE**, using an algorithm he created from a formula of M. Flach.

3 The Naive Algorithms

3.1 A way to compute m_E

Use the (not-exact!) sequence:

$$H_1(E,\mathbb{Z}) \to H_1(X_0(N),\mathbb{Z}) \to H_1(E,\mathbb{Z}).$$

The composition map from $H_1(E,\mathbb{Z}) \to H_1(E,\mathbb{Z})$ is multiplication by m_E, and $H_1(E,\mathbb{Z})$ can be computed because its image in $H_1(X_0(N),\mathbb{Z})$ is saturated, as E is optimal. This algorithm is described in detail in [Kohel-Stein, ANTS IV], and amounts to finding "left and right eigenvectors" and taking their dot product.

3.2 A way to compute c_E

Compute $S_2(\Gamma_0(N),\mathbb{Z}) \subset \mathbb{Z}[[q]]$ to precision $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]/6$ using, e.g., modular symbols, then use a Smith Normal Form algorithm.

4 The Examples

These examples were computed by myself and Amod Agashe.

- **54B**: Let E be the elliptic curve $y^2+xy+y = x^3-x^2+x-1$. Then $m_E = 2$ and $c_E = 6$. In fact, it's easy to see that $3 \mid c_E$ "by hand" by writing down the form f corresponding to **54B** and the form g corresponding to $X_0(27)$ and noting that $f(q) \equiv g(q) + g(q^2) \pmod 3$. (Because of the "Sturm Bound", it suffices to check this up to $O(q^{19})$.)

  Hey $c_E \neq m_E$!! In fact, $c_E \nmid m_E$!! When we first did this computation, Ribet had already mentioned to us that he had really proved that $m_E \mid c_E$, not vice-versa. We were, however, extremely surprised to find so quickly an example in which $c_{\mathcal{E}} \neq m_E$.

- **T-shirt**: My t-shirt has **243A** and **243B** on it. For **243A**, we have $m_E = 9$ and $c_E = 27$. For **243B**, we have $m_E = 6$ and $c_E = 54$. I designed the t-shirt many months before I knew that question 4.4 had a negative answer.

- **242B**: $N = 2 \cdot 11^2$.

  $$m_E = 2^4 \neq c_E = 2^4 \cdot 11$$

  The failure is probably not just a "small primes" phenomenon.

Moral: A little computation sometimes greatly cleans the air.

5 The Future

Based on computations, Amod and I conjectured and Ribet proved the following theorem.

Theorem 5.1 (Ribet, 2001). *Let E be an elliptic curve of conductor N. If $p^2 \nmid N$ then $\mathrm{ord}_p(m_E) = \mathrm{ord}_p(c_E)$.*

New Version of "**Question 4.4**. For all $N_E \leq 539$, we have

$$2 \cdot \mathrm{ord}_p(c_E/m_E) \leq \mathrm{ord}_p(N_E).$$

In particular, for $p \geq 5$, do we have

$$\mathrm{ord}_p(c_E/m_E) \leq 1?$$

Is this true in general?

- ideas from audience: hendrik, change to 2·!
- try to find a more refined exact formula for $p = 2, 3$. (Brumer)
- analogue of ques 4.4 for abelian varieties (Birch)
- elkies said something???

TALK 6: KOWALSKI: "Some analytic problems for elliptic curves"

Motivations:

* BSD conjecture for E/Q (what sort of local-to-global problems that have to do with elliptic curves have a positive solution.)

* sum_{P<=X} i(P).

* Classical problems related to primes in progressions to large moduli.

Invariant: p a prime of good reduction.

E_p(F_p) = Z/d_1Z oplus Z/(d_1 d_2)Z.

i(p) = d_1(p).

d_1(p) = largest d such that p is totally split in Q(E[d]).

sum_{p<=X} d_1(p) = sum_{d <= sqrt{x} + 1} phi(d) pi_E(X,d,1),
where pi_E is the number of p<=X st p is tot split in Q(E[d]).

Titch. division problem:

sum_{p<=X} d(p-1) = cX + d X/log(X) + O(X(log log X)/(log X)^2),

where c = zeta(2)zeta(3)/zeta(6).

Linnik, Fouvry, Bombieri, Friedlander-Iw.

Problem: Evaluate the sum, asymptotically.

Conjecture: If E has no CM, then

sum d_1(p) asymptotic to c_E X/log(X),

if E has CM, then

sum d_1(p) asymptotic to c_E X,

where c_E = sum_{d>=1} phi(d)/#G_d, (converges by Serre's "big image" theorem)

where G_d = Gal(Q(E[d])/Q).

Even on assuming GRH, I've not been able to prove this.

Asymptotic formula: pi_E(X,d,1)

```
                    =  1/#G_d li(X) + O(sqrt(X) log dX), d <= X^{1/8}.

Problem 2: Look for d_1(p) that are "abnormally large".

d_1(p) <= sqrt(p) + 1
Example: y^2 = x^3-6x+2.
p = 196561, d_1(p) = 140, #G_{d_1(p)} = 92897280.

Problem 3: Count, as X--> oo, the number of "bad" p<=X.

Example: p<=3*10^8.
   10 bad primes
   all are <= 1.46*10^8.

Approach, that might work, but won't, but leads to another interesting
problem.

Suppose p < q (two bad primes), with d_1(p) = d_1(q) "large"

   d_1^2 | p+1-a_p  \---------\  d_1^2 | p-q + (a_q - a_p).
   d_1^2 | q+1-a_q  /---------/
                                   (if nonzero, and if d_1 > 8q^{1/4}).
  ==> q >= p + (d_1^2 / 2)

Def: p and q are E-twins iff #E(F_p) = #E(F_q).

Problem: Evaluate

   J(X) =  # { p<=X | p has a twin }

    ( 1/sqrt(p) ) * ( sqrt(p) / log(p) ) = 1/log(p)

Probably is about the same as that a prime number has a twin.


Problem:

Show if E has no CM, then

        J(X) asymp to c'_E * X/(log X)^2.

I have no candidate value for c'_E.


In CM case, one can prove some things:

            #E(F_p) = #E(F_q)

  <====>  N(psi(p) - 1) = N(psi(q) - 1).

N((psi(p) - 1)/(psi(q)-1)) = 1

psi(p) = u(psi(q)-1)+1.
```

Conjecture:
Let k>=1 be an arbitrary integer.

     sum_{p<=X} m(p)^k asymp c_{E,k} X(log X)^{2^k-k-2}

This is the correct upper bound. Lower bound is harder (i.e., harder
than the twin primes conjecture.)

Example:

E: p<=10^8,   M(n) <= 5.

F: y^2 = x^3 - x.

M(128180000) = 24
   ||
  2^4*5^3*13*17*29

Problem: M(n) << n^eps for non-CM curve.

TALK: 7. BEUKERS and EDWARDS: The super-Fermat equation; a complete
solution to x^2+y^3+z^5=0 (??)

The superfermat equation:
x^p + y^q = z^r in x,y,z in Z with gcd(x,y,z)=1,
p,q,r in Z_{>=2}.

1 + 2 = 3 (primitive)
gives:
2^14*3^6 + 2^15*3^6 = 2^14*3^7   boring!
(2^7*3^3)^2 + (2^5*3^2)^3 = (2^2*3)^7.

Case I. 1/p + 1/q + 1/r < 1

THEOREM (Darmon-Granville): #soln < oo.
Sketch of proof: Find a curve C and a Galois cover
    phi:C-->P^1 = {(X:Y:Z) : X+Y=Z} in P^2.
phi ramifies of order p above X=0
             of order q above Y=0
             of order r above Z=0

Let x^p + y^q = z^r be a solution.
Consider phi^{-1}(x^p:y^q:z^r).
There exists a number field K such that
phi^{-1}(x^p:y^q:z^r) in C(K) for ALL (x,y,z) with x^p+y^q=z^r.
1/p + 1/q + 1/r < 1 <==> genus(C)>=2 ===> #C(K) < oo.   [QED]

There is a list of 10 known solutions:
1^k + 2^3 = 3^2
13^2 + 7^3 = 2^9
...
which includes spectacular ones, such as
 9262^3 + 15312283^2 = 113^7.

Known results:

{p,q,r} = {2,3,8}, {2,4,5} don't occur.

N. Bruin solved for the exponents in this list of 10 using Chabauthy's method.
I.e., he showed that for these exponents, there are no other solutions.

2nd method: Galois representations
x^p + y^p = z^2   (no nontrivial solutions)
x^p + y^p = z^3   solved using the Wiles method.
x^2 + y^4 = z^p   (being worked on by Skinner and Ellenberg)

[Beukers says it's a conjecture that this list is complete.
ZAGIER: No! I don't think it should be a conjecture.   The heuristics
say there should be between 0 and 3 (?) more solutions.]

Case II. 1/p + 1/q + 1/r = 1.
{p,q,r} = {3,3,3}, {2,3,6}, {2,4,4}
All of these can be easily solved using rational points
on elliptic curves:
x^3 + y^3 = z^3; x^2+y^3 = +/-z^6, y^2+/-x^4 = z^4.

Case III. 1/p + 1/q + 1/r > 1 ===>

{p,q,r} = {2,2,k}, {2,3,3}, {2,3,4}, {2,3,5}.
k>=2.

Infinitely many solutions in each case. What are they?
For example:

* {2,2,2} gives x^2+y^2+z^2 = 1. (easy param)

* {2,3,3} Mordell: 5 parametrized solutions.

  x^3 + y^3 = z^2: x = -4p^3q+4q^4, y = p^4+8pq^3, z = ..., etc.

  Invariant theory of quartic forms were used to resolve this.

* {2,3,4} Zagier (no literature) 11 parametrized families.

* {2,3,5} Not done before...!

Now we talk about {2,3,5}. It was known that only a finite list was
needed, but a complete list wasn't given until now.

Reduction Theory
f(x,y) = prod_{i=1..k} (nu_i x - mu_i y)
[most of the rest of the talk involves slides, so I am too lazy to take
further notes.]

TALK: 8. TOP (11.00-11.45): Legendre elliptic curves over finite fields

Joint work with Roland Auer.

History:
2001, February: Netherlands thesis of V. Shabat: "Curves with many points".

Notation: C/F_q complete, geom. irred. curve of genus g.

max { #C(F_q) : all C of genus g} = N_q (g).

Hasse-Weil-Serre bound (HWS):

N_q(g) <= q+1+g*Floor(2*Sqrt(q))

Past work:
N_q(1): Duering, 1941
N_q(2): Serre, 1983 (written down in a 1985 Harvard course).
princ. polarized ==> is Jacobian (also true for dim 3 [??])
genus two are always hyperelliptic (not true for genus 3)

What about g=3?

Ibikiyama: q=p^{2n}
Theoretical max is q+1+6*p^n.
He shows that for half the even n's, this max is reached.
[And something about q+1-6*p^n.]
ELKIES: That doesn't work for q=4. Because, "the curve over F_{16}
would have -7 points."

C. Lauter proved: For every q, one can reach either

* a number a distance at most 3 from HWS

or

* a number at most 3 from the minimum.

In Serre's notes, he had a table:

g = 3

```
q       2   3   4   5   7   8   ... 23
--------------------------------------- ....
N_q(3)  .. .. ...           ..  ... ??
```

"It's always a pleasure to find a "?" in a paper of Serre,
because that's a challenge."

(a) We can easily list ALL hyperelliptic curves

(b) We can write down the general quartic and search over all possibilities.

Naive approach:
Uses some results that originate in MY thesis.

Consider the one-paramater family

C_lambda: x^4 + y^4 +z^4 = (lambda + 1)(x^2y^2 + y^2z^2 + z^2x^2)

Has an S_4 symmetry.

This family includes the Kleine curve and the Fermat curve
of degreee 4.

Fact: Jacobian(C_lambda) --- isogenous --> (E_{\lambda}^(3+y))^3.

Corollary: #C_lambda(\F_q) = q + 1 - 3*t_lambda(q)

Here,
E_{\lambda}^{(a)} is the elliptic curve ay^2 = x(x-1)(x-lambda).

If the a depends on lambda, then the Jacobian is a triple product.

t_lambda(q) = q+1 - #E_{\lambda}^{(\lambda+3)}(\F_q).

Problem: Maximize t_lambda(q).

Next, we ask an easier question abot elliptic curves. What are the possible
values of #E_{\lambda}(F_q).

Answers: "All values, except one in one case.".

Theorem: Let E/F_q be an elliptic curve.

* [F_q: F_p] odd: there exists lambda s.t. #E(F_q) = #E_lambda(F_q)
  <===> #E(F_q) = 0 (mod 4).

* [F_q: F_p] even: then q=r^2, r = 1(mod 4).
  there exists lambda st #E(F_q) = #E_Lambda(F_q)
  <===> #E(F_q) = 0 (mod 4) *and* #E(F_q) =/= (r+1)^2.

Proof:
Has an easy and hard direction.

Idea in <===:

Given a curve E: y^2 = x(x-alpha)(x-beta).

One has, at least, that E isom to E_{lambda}^{(alpha)}, where lambda=beta/alpha.

Using the group structure possibilities that one has in an isogeny class,
one finds E isog to E_lambda'.

9. BRUIN (16.00-16.30): Cyclic covers of hyperelliptic curves

joint work with victor flynn.
(BR. Supp. by PIMS.)
[I asked him what "BR." means but he wouldn't tell me, and I still don't know.]

Theorem [Faltings]: Let C be a curve of general type over a number field k (i.e., genus >= 2). Then C(k) is finite.

Problem: Determine C(k).

Technique (Chaubauty): k_p = completion of k at a finite prime p.

```
C(k) ------------------> A(k)
                          consider closure of A(k) in A(k_p).
C(k_p) ----------------> A(k_p)
```

C(k) is contained in (closure of A(k)) and C(k_p). The latter might
be finite.

A way out when rank A(k) is too big is to use covering collections.
The idea here is to construct a finite set of covers

```
              phi_delta: D_delta --> C
```

such that union of the phi_delta(D_delta(k)) === C(k).

A way to get such a covering collection is to take an
unramified abelian cover. It's a theorem that you get
all unram abelian covers using the following the construction.

```
         D ------->Jac_C
         |           |
         |           | N
        \|/         \|/
         C \-----> Jac_C
```

[What is D? Why is it irreducible? Is it? Is it [N]^{-1}(C) in
Jac_C? Is the map from D to Jac_C injective? What is the genus of
D? -- RH ==>]

Theorem: A finite number of twists D_delta of D form a covering
collection.

Hyperelliptic Curves
C: y^2 = F(x) with F square free.
Take N =2.

```
    D
    |
    |  mult-by-2 cover; group is Jac_C[2]
   \|/
    C
    |
    |  2
   \|/
   P^1
```

Gal(D/P^1) is Jac_C[2] x {+/- 1} = (Z/2)^r.
There are lots of subcovers F between D and P^1. People really
work with these subcovers instead of D, since g(D) is sometimes too large.

```
CYCLIC COVERS OF ODD ORDER N > 2.

Assume: there exists T in Jac_C[N](K)  [really only need <T> K-rational!]

 Jac_C --> Jac_C/<T> = A^
dualize
 A ------> Jac_C  (not injective; degree N)

Pullback and get D ---> C --deg 2-> P^1 with Gal(D/P^1) dihedral.

  tau_1, ..., tau_N involutions in Aut(D/P^1).
  F_i = D/<tau_i>.

genus(D) ===Riemann Hurwitz== N*(g(C)-1)+1.
genus(F_i) ================== (g(C)-1)*(N-1)/2.

"Two of the F_i is enough to give all information."

Conjecture:

   Jac_D is isogenous to Jac_C x Jac_{F_i} x Jac_{F_j}

EXAMPLE:
Now we will specialize to genus 2 and degree 3.
  C: y^2 = G(x)^2 + (constant)*H(x)^3,  where G,H in K[x],
     deg(G) = 3, deg(H) = 2.

Let alpha1, alpha2 but the roots of H.
Let T = [(alpha1, G(alpha1)) + (alpha2,G(alpha2)) - oo^+ - oo^-].
Also
   (Y-G(x)) = 3T.

D_{delta} is given by the equation
    2*delta* u^3*G(x) = delta^2*u^6 - (constant)*H(x)^3
    y = delta*u^3-G(x),   delta in K(3,???) subset K^*/(K^*)^3.

[More equations, which you should get from Nils's latest paper!]

He gives tau_i explicitly.

D_delta / <tau_i> = F_{delta, c_i} = F:  equations.  (genus one!)

E = Jac_F.  (elliptic curve)

Assume P0 in D_{delta}(K).

D_delta ---> Jac_{D_delta} --> E

[He gives these map explicitly, and notes that their sum is 0.]

... some remarks ...

C: y^2 = (x^3 + 2)^2 + (x^2 + x + 1)^3  ?

E : y^2 =. ...
```

[Maybe he's rushing at the end of his talk, because I can't read his handwriting with confidence.]

TALK: 10. GROENEWEGEN (16.45-17.15): Computing the tame kernel

O in F, a number field. discriminant Delta.

{a,b} in K_2(F) = (F^* tensor F^*) / <a tensor b : a + b = 1>

Ex. {a,-a} = 1.

If v : F ---> Z union {oo} is a finite prime, then there is a map

t_v : K_2 F ----> k_v^*
{a,b} |---> (-1)^{v(a)v(b)} a^{v(b)}/ b^{v(a)} "mod v".

v(u) = 0, {u,pi} |--------> u mod v
pi(v) = 1.

K_2 F -----------> sum_{all finite v} k_v^*.

The kernel of this map is called the tame kernel, denoted K_2 O, and it's finite. (Theorem of Garland)
[According to Brumer: Howard (I think) Garland is a differential geometer who proved finiteness of K2(O) in early 70's. He is at Yale or was after Columbia...]

Filtration of F^*:

Let S be a set of primes containing S_oo.

U_S = {x in F^* : v(x) = 0 for v not in S}.

S_m = S_oo union { all primes with norm N_v <= m }.

U_m = U_{S_m}.

K^{(m)} = (U_m tensor U_m) / <a tensor b : a + b = 1, a+b = 0>

Let K^m be the image of K^{(m)} in K_2(F).

Theorem:

(a)[H. Bass-Tate] There exists c_F such that if m > c_F, then

K^{(m)} / im K^{(m-1)} ---isom---> sum_{N_v = m} k_v^* .

(b) There exists c'_F : K^{(m)} ---isom---> K^m if m > c'_F

[Me] One can take c_F = 4*|Delta|^{3/2}.

Example:
F quadratic field with |Delta|>631. c_F = 0.2340*|Delta|^{3/2}.

Applications:
(a) if m > c_F then K_2(O_K) subset K^m, so we get
    generators for K_2(O_K)

(b) m > c'_F then K_2(O) subset K^m = K^{(m)} (completely explicit)

F. Kenne claims he can determine (K_2(O))_p (p-primary part).

Theorem: There is an algorithm to compute the tame kernel.

HENDRIK: Doesn't this mean there is an algorithm to compute c'_F after all!?

[Finally, it appears that the speaker uses the snake lemma to easily deduce that (b) follows from (a). He only briefly says (maybe!), orally, that he is proving "(a) ===> (b)" and then writes tons on the board about the proof. It would be vastly better if her were to at least write, with confidence, that he is going to prove (a) ==> (b). Then any question about what is being done is removed from the listener's mind, and also the listener can easily hop back into the lecture even if the proof is not understood.]

Questions?

STEIN (me): Any examples at all? [In fact, I know, from talking with Herbert Gangl earlier today that K_2(Z) is Z/2Z.]

Examples:
  * K_2(Z) = <{-1,-1}> = Z/2*Z

  * K_2(disc -303) = Z/22*Z   (evidently, this is a really big one).

TALK: 11. MESTRE (17.30-18.00): Genus 2 curves and the AGM

I. GOAL:
Let Ctilde be a curve of genus 2 over F_{2^d}. The problem:

   How do we quickly compute #Ctilde(F_{2^d})?
   How do we quickly compute charpoly(Frob) = X^4 + ...?

Frobenius?

Let E_0 be an elliptic curve
dx_0/y_0 = omega_0

1) Obtain a sufficient approx of the canonical lifting.

2) E_{0} <-- E_{1} <-- ... <----- E_{d}

   lambda_i(omega_{i-1}) = omega_i

Now, we would like to do the same for curves of genus 2.

1) We want to obtain a sufficiently good approximation A_0 of
   the canonical lifting of Jac(Ctilde).

2) A_0 <---lambda_1-- A_1 <--.... <---lambda_d--- A_d
   with explicit basis B_n of Omega^0(A_n) such that
   the matrix of lambda_i^* relative to B_{i-1} and B_i is
   the identity.

Compute: Guadry and Harley implemented this (principally with MAGMA!):
    d = 1000;
    they compute Ctilde(F_{2^d}) in 3 hours.

II. Case of R = real numbers

```
 C/R: y^2 = (x-x_1)*(x-x_2)*......*(x-x_6), with x_i in R and x_i < x_{i+1}
          =      p_1(x)    * p_2(x) * p_3(x)
```

Humbert's method (approx 1890)
(by geometry)

C = C_0 <----> C_1 "2,2-correspondence" [what's a
2,2-correspondence??] [which direction? Both? which functoriality below?]
GUESS: J(C_1) --> J(C_0) is an isogeny with kernel Z/2 x Z/2 [maybe
that's what a 2-2 correspondence is! he's very unclear
The fact is, he's lost me with his "2,2-correspondence", and, for whatever
reason, I'm definitely not going to ask.]

[He draws a picture with a circle and a triangle and so on. People
giggle because, as usual with professional mathematicians, the
intersections are drawn unconvincingly and poorly.]

Next, we convert this diagram into algebraic formulas. The formulas
will be true in any field of char. 0, such as Q_2.

[p,q] = p'(x)q(x) - p(x)q'(x).

IF deg(p) <= 2 and deg (q) <= 2 then deg([p,q]) <= 2.

C: y^2 = p_1(x)p_2(x)p_3(x)

C_1: Delta*y^2 = P_1(x)P_2(x)P_3(x)

P_1 = [p_2, p_3],
P_2 = [p_1, p_3],
P_3 = [p_1, p_2],.

Delta = det of p_1, p_2, p_3 in the basis 1,x,x^2.

Basis_0 := {x dx/y, dx/y}

Basis_1 := {X dX/Y, dX/Y}

The correspondence lambda_1 induces the identity matrix on the differentials B, B_1.

C/K with ordinary reduction.

y^2 ==congruent== (x-x_1)^2*(x-x_2)^2*(x-x_3)^2

with x_i distinct modulo 2. [[How can three things be distinct mod 2??? -- maybe they really lie in a nontrivial extension of Q_2 and mod 2 means mod a prime over 2 of degree > 1. Perhaps this is one of his conditions on C, or it's part of the "ordinary reduction" hypothesis. Yes, it's the good reduction part of ordinary.
Armand Brumer suggests that three can be distinct modulo 2, because one could be infinity.]]

y^2 = (x-x_1)*(x-x'_1)*(x-x_2)*(x-x'_2)*(x-x_3)*(x-x'_3)

Set p_i = (x-x_i)*(x-x'_i)

2) C_{0} <-- C_{1} <-- ... <----- ...

Thm: 1) (C_{nd})_n ---> canonical lift of Ctilde

2) J(C_d) <--- J(C_{d+1}) <--- ... <--- J(C_{2d})

y^2 = g_d(x) Y^2 = g_{2d}(X)

An isomorphism between C_d and C_{2d} is given by

(x,y) |----> ((ax+b)/(cx+d), lambda y / (cx+d)^3)

let M = (ad-bc)/lambda * [a,b ; c, d]

Charpoly of Frobenius:

charpoly(M)(x) * charpoly(M)(2^d/x).

TOP: Is anything known about genus 3?

Answer: Theoretically, probably not... Paper of Livne and Donagi.

Brumer remarks that "Gaudry is one of the patenters of Mestre's new algorithms."

BOOKMARK
TALK: 12. STEVENHAGEN (20.15-20.45): Computing primitive root densities

Fix a prime p. F_p^* = <a mod p>
Fix a in Z, a not 0, 1, -1.

For how many primes is a in Z a primitive root?
Does the set of such p have a density, call it delta(a)?

Heuristics:
a mod p is primitive <===> there is no prime ell such that
ell | [F^*_p : <a>]
<===> no prime ell such that p splits completely
in the field Q(zeta_ell, a^{1/ell}) = F_ell.

Chebotarev: For one ell, the set of p splitting completely in
F_ell/Q has density [F_ell:Q]^{-1}.

Conjecture: delta(a) = prod_{ell prime} (1 - 1/[F_ell:Q])
if a is not a perfect power
= A = prod_{ell prime} (1 - 1/(ell(ell-1))) approx 0.37.

Lehmers: delta(5) > delta(2).

Artin responded; the fields F_ell are NOT independent.

a=5: F_2 = Q(sqrt(5)) subset F_5 = Q(zeta_5, 5^{1/5}).

delta(5) = 20/19 * A (leave out 5 from the product)

In general:

delta(a) = sum_{n=1}^{infty} mu(n) / [F_n : Q]

where F_n = Q(zeta_n, a^{1/n}).

Problems
* analytic: Need to deal with ALL primes ell,
so the Chebotarev theory does not really apply.
This only works under GRH.
(Hooley proved the density in 1967 ASSUMING GRH.)

* algebraic: possible dependencies between fields F_ell.

Gal(prod F_ell/Q) \-----> prod Gal(F_ell/Q)

Hooley delt with this algebraic problem. The only
dependency occurs if F_2 = Q(sqrt(a)) has odd
discriminant d. Assume a is a perfect hth power in Z.

Correction: 1 + mu(|d|)prod_{ell | d, ell | h}
1/(ell-2) prod_{ell | d, ell \nmid h} 1/(ell^2-ell-1).

Generalizations of Artin's problem:

(1) [F_p^* : <a>] = t, *fixed*
(2) F_p^* = <a> and p cong b (mod f).
(3) F_p^* = <a, b>
(4) number fields, function fields (of curves over finite fields)

The algebraic problem becomes the main problem.

A generalization of Artin's question:

```
Q \----> F_ell = Q(zeta_ell, a^{1/ell}) subset L_{ell}
                           subset Q(zeta_{ell^oo}, a^{1/ell^oo}).

  G_ell = Gal(L_ell / Q)

  S_ell subset of G_ell.
```

For how many p does Frob_p in G_ell lie in S_ell for all primes ell < p.

Require: for almost all ell: F_ell= L_ell, S_ell = G_ell - {id}.

Associated ARtin constant: A = prod_{\ell} #S_ell / #G_ell.

* A is the associated density if the fields L_ell are independent
  (under GRH, Hooley).

-- only possible dependency if L_2 in Q(zeta_{2^oo}, a^{1/2^oo}) contains
   a quadratic field K of odd discriminant d.

```
       K <------> chi_K = prod_{ell > 2} chi_ell,
                  chi_2 = chi_K.
```

[This makes absolutely no sense!]

Theorem (Moree, Lenstra, ---)

If K as above, then the correction factor is of the form

```
      1 + prod_{ell} E_ell
```

```
with E_ell = 1/#S_ell sum_{chi in S_ell} chi_ell}(x)
           = average value of chi_ell on S_ell.
```

E.g. Artin. ell | 2d. E_ell = -1/#S_ell = -1/([F_ell:Q] - 1).

TALK: 13. SIMON (20.50-21.20): Integrality results linked to
nonmonic polynomials

When studying discriminant, we often restrict to monic polys. My
question is "why?" Maybe they are better? My aim is to prove the
contrary.

* the discriminant is invariant under SL_2. But SL_2 doesn't preserve
monicness. However, if we require monicness, then the automorphisms
are only X |---> X + c. So allowing nonmonics gives a bigger
automorphism group.

I. The Invariant Ring

Let RR be an integral domain, and let R be a subring and Rbar the
integral closure of R in RR.
Example: RR = Qbar, Rbar = Zbar, R = Z.

```
Let P in R[X] be a poly:
    P = a_0*X^n + a_1*X^{n-1} + ... + a_n
Let theta in RR be a root, so P(theta) = 0.
Let P_i(X) = a_0*X^i + a_1*X^{i-1} + ... + a_i, i >= 1.
    P_0 = 1 (=/= a_0)

Prop:
   * P_i(theta) in Rbar.

   * R[theta] := R + R*P_1(theta) + ... + R*P_{n-1}(theta) is a ring.

   * disc((P_i(theta))_{i=0}^{n-1} = disc(P)
          ||
        det (tr (P_i(theta)*P_j(theta)) )     (he's implicitly
                                       assuming something about tr, no?)

   * R[theta] is unchanged when we apply SL_2(R) to P.

I call R[theta] the "invariant ring of P".

Example:
P = 2x^3 + x^2 - 5x - 2.
disc of the field this defines is 31^2.
Not monogenic.
But R[theta] is the full ring of integers in this case.

---

II. Factorization of the discriminant.

Slogan:
 "a_0 is the product of the denominators of the roots of P  ."

Lemma: Let P in R[X], write P = a_0*prod_{j=1}^n (X - theta_j), theta_j in R.

then for J in {1,..., n},

                a_0 * prod_{j in J} theta_j in Rbar.

We will prove better that a_0 * prod_{j in J} (X - theta_j) in Rbar[X].
Prove by induction.
Enough to prove this with J = {1,...,n-1}

   a_0 * prod_{j=1...n-1} (X - theta_j) = P/(X-theta_n).

X*P_i + a_{i+1} = P_{i+1},

 so
     P/(X-theta_n) = a_0 X^{n-1} + P_1(theta)*X^{n-2} + ... + P_{n-1}(theta).

[whatever.  this speaking is (&*%*$%.]

Theorem (M-N Gras, 1986): Let ell >= 5.

There is at most one cyclic extension K of degree ell of Q
```

such that O_K = Z[theta], and it is Q(zeta_p + zeta_p^{-1})
when p = 2*ell + 1 is prime.

Theorem (----): Let ell >= 5. N>= 1

There are only finitely many cyclic extension K of degree ell of Q
such that [O_K : Z[theta]] <= N.

TALK: 14. SMYTH (21.25-21.55): Explicit formulas for a
family of 3-variable Mahler measure.
No notes, because he used slides... He computes Mahler measure
of some 3-variable polys. Zagier says it's not surprise.

TALK: 15. STOLL (22.00-22.30): Extreme Chabauty

[[See ''Uniform Chabauty bounds for twists'', available from
http://www.math.uni-duesseldorf.de/~stoll .
-- MS]]

Problem: C/K curve over # field, J = Jacobian,
phi : C(K) \---> J(K) tensor Q

Question 1. Let V in Jbar(K) = J(K) tensor Q be a Q-subvector space.
How large is C(K) intersect phi^{-1}(V)?

Question 2. Let S subset C(K). How large is dim <phi(S)>?

Best Answer:
#(C(K) intersect phi^{-1}(V)) <= dim V. (ques 1)
dim < phi(S) > = #S. (ques 2)

Fact: the best answers are correct under a bunch of hypotheses
when we restrict to twists of a fixed curve.

Examples

(1) Quadratic twists of hyperelliptic curves:
C: y^2 = f(x) / Q,   genus g >= 2.
C_d: dy^2 = f(x)

Let S be a subset of C_d(Q) such that

* S intersect S' = empty set, where S' is the
image of S under the hyperelliptic involution, and

* #S <= g.

====> dim<phi(S)> = #S, unless maybe for d in a finite exceptional set.

[[No condition on the rank of Jac(C_d); the condition is only
on #S, i.e., on dim<phi(S)>.]]

(2) Thue Equations:

Let f in Z[x,y] be homogeneous of degree n, squarefree.
For all but finitely many nth pwoer free h in Z, the Thue equation
C : f(x,y) = h has at most r (rational) solutions, where
r = MW rank of Jac(C), IF r <= n-3.

(3) *Tentative* result:
Let ell be a prime with ell >= 5.
Let p be a prime with p ==/== 1 mod ell, and p >= 3*(ell+1)/2.
Then there are at most (ell-1)/2 rational solutions of x^ell+y^ell = p.

[[Comment by MS: This will probably remain tentative for a while --
the problem is to show that the rank is at most (ell-1)/2, and
the argument I applied first was flawed. But I hope to remedy this
some time.]]

(4) Catalan twists:

C_A: y^2 = x^5 + A
If rank J_A(Q) = 1, then #C_A(Q) <= 7.
If #C_A(Q) = 7 (and rank J_A(Q) = 1), then A = 18^2.
Otherwise, #C_A(Q) <= 5.

Theorem: * Fix a curve C/K with genus g>=2,
* Gamma subset Aut_Kbar(C) a K-defined subgroup,
* K-rational Gamma-invariant divisor class D of positive degree,
and use this to map P in C to [d*P] - D in Jacobian.

Assume: All points of C fixed by a nonidentity element of
Gamma map to 0 in Jbar.

Now consider Gamma-twists C_{xsi}, xsi in H^1(K,Gamma) (cohomology set).
IF xsi is ramified at some place v of K such that

* C has good reduction at v

* p > 2n + 1 + e_v*#Gamma, where v | p

and V subset Jbar_xsi(K) is a subspace of dimension n,

THEN
#(phi^(-1)(V) intersect (C_xsi(K) \ C_xsi^triv(K))) <= f_C(n),

where C_xsi^triv(K) = {P in C_xsi(K) | gamma(P) = P for some 1=/=gamma in G}.

Here, f_C is a function depending on the geometry of C.
For 0 <= n < g, n <= f_c(n) <= 2*n, for n >= g, f_C(n) = oo.

If C is a smooth plane curve of degree N, then f_C(n) = n for 0<=n<=N-3.

TALK: 16. STARK (9.15-10.00): Many digits of derivatives of p-adic L-functions at 0

Define zeta(s|f) = sum_{n=1}^{oo} (fn)^{-s},
zeta(s,x|f) = sum_{n=0}^{\infty}(nf+x)^{-s}.

```
r = res_{s=1} = 1/f,
k>=0: zeta(-k, x|f) = -1/(k+1)*b_{k+1}(x|f)  (Bournoulli poly)

  sum_{j=0}^{infty} b_g(x|f)/j! * t^j = te^{xt}/(e^{ft}-1),

  b_{k+1}(|f) = b_{k+1}(0|f) = f^k B_{k+1}

f=1: zeta'(0,x|1) ===essentially=== log(1/Gamma(x)) "and some sqrt(2pi)'s"

Omega = {m*omega_1 + n*omega_2 | m, n >= 0}
z(s | omega_1, omega_2)   = sum'_{w in Omega} omega^{-s},
z(s,w | omega_1, omega_2) =  sum_{w in Omega} (w + omega)^{-s},

res_{s=2} = R = 1/(omega_1*omega_2)
res_{s=1} z(s,w|) = ((omega_1+omega_2)/2 - w)R
k>=0:  z(-k,w) = 1/((k+2)(k+1)) C_{k+2}(w|,omega_1, omega_2)

ZAGIER: These formulas are, as far as I know, due to me, but he hasn't said anything.
No -- in fact, this is completely trivial by the standard methods.

C_j(w) = sum_{n=0}^j binom(j,n) c_n w^{j-m}
c_j = c_j(0)

sum_{j=0}^{\infty} c_j(w)/j t^j = t^2 e^{wt}/((e^{omega_1 t} - 1)(e^{omega_2 t} - 1)).

zeta(s,x) = sum_{j=0}^{k-1}binom(-s,j)zeta(s+j)x^j
+ x^{-s} sum_{n=1}^{\infty} ((nf+x)^{-s} - sum_{j=0}^{k+1} binom(-s,j) (nf)^{-s-j} x^j)
  \-------------------------------------------------------------------------------/
          this latter term is on the order of n^{-sigma-k-2}, analytic for sigma>-k-1.

Set s = -k: sum_{j=0^{k-1} binom(k,j) zeta(-(k-j)) x^j + x^k + 0.

f=1:
zeta(s,x) = zeta(s) - s*zeta(s+1)*x + x^{-s}
              + sum_{n=1}^{oo} [ (n+x)^{-s} - n^{-s} + s*n^{-s-1} x ]

The Gamma function pops up in zeta'(0,x):
zeta'(0,x) = zeta'(0) - gamma*x - log(x) - sum_{n=1}^{infty} [ log(n+x) - log(n) - x/n ]

Now that finishes the first part of the talk... which is good.

So, I want to p-adically continue these things.

p odd (out of laziness)
k --> oo,   (p-1)|k

The meaning of n^{-s}, p-adically:
n in Z^*_p and s in Z_p,
Then n^{-s} = exp(-s*log_p(n)),   log_p (n) = 1/{p-1} log(n^{p-1}).

x in Z_p, s in Z_p

 zeta_p(s,x) = lim_{N--p-adically-->-x, and N--->oo}  sum_{0<=n<N} (n+x)^{-s}
```

sum_{0<= n < N} (n+x)^k = zeta(-k,x) - zeta(-k,x+N) =
                          -1/(k+1)*(B_{k+1}(x) - B_{k+1}(x+N)).

as n --> -X, the RHS converges to B_{k+1}(x) - B_{k+1}(0)
                                 = B_{k+1}(x) (when k+1 is >1 and odd).

I can differentiate wrt s and substitute s=0.

1/Gamma_p(x) = lim_{as above} prod_{0 <= n < N} (n + x).

The Reason: There are lots of conjectures about these special values,
and I want to find more (in the imaginary quadratic case). The first
methods for computing

TALK: 17. SCZECH (10.15-11.00): Polylogarithms over real quadratic number fields.

F = real quadratic # field
L = lattice (fractional ideal), 1 not in L.
v(u) = sign(u), sign(u')

U = { eps in O_F^* | e >>0, e(1+L) = 1+L} is always o finite index in O_F^*

zeta(L+1,s) = sum_{u in L+1/U} v(u) |v(u)|^{-s}

xsi(L,s) = sum_{lambda in L} v(lambda) e(tr(lambda))/|N(lambd)|^s,
e(x) = exp(2*pi*i*x),

Functional equation ==> zeta(L+1, 1-m) =0 for m=1,2,3,4,...

zeta'(L+1,1-m) = Gamma(m)^2*|det L^*| / (2pi*i)^{2m-1} xsi(L^*,m).

Examples (jointly with Herbert Gangl).

1. F = Q(sqrt21)), e = (5+sqrt(21))/2, <e> = U, L=(e-1) = Z*alpha + Z*beta
alpha = (3 + sqrt(21))/2, beta = 3
zeta'(L+1,0) = log(eta), where eta = (e+sqrt(e-1))/(e-sqrt(e-1))
[The words "Stark unit" were just spoken.]
[It is hard for me to understand the speaker's accent, and Mestre
and other French folk are talking loudly behind me.]
Let E = F(sqrt{e'-1}) subset C.
The Bloch group B_2(E) can be represented by formal linear combinations
    xsi = sum_{i} n_i[x_i], where x_i in E and n_i in Z.
View xsi as an element of Z[E].
Subject the linear combinations to the condition that
    sum n_i(x_i /\ (1-x_i)) = 0 in /\^2 E^*.   (/\ = "wedge")
(Remark: (ab)/\c = a/\c + b/\c.)

Example: Take x = sqrt((3-sqrt{21})/2) in E.
Then xsi = -6[-1/2(x^2 - x - 1)] + 9[-1/2(x^2-x-3)] + [-1/2(x^3-3x^2+3x-2)]
         is an element of the Bloch group B_2(E).
Conjecture: It is a generator of B_2(E) modulo torsion.

ZAGIER: NONSENSE! Your B_2(E) has infinite rank!!! You have to
divide out by a subgroup of obvious things.

The speaker says: "OK. You have to maybe divide out by a subgroup...."

Recall Li_2(z) = sum_{n=1}^{oo} z^n / n^2, |z| < 1.
Bloch - Wigner dilograrithm:
D(z) = Im(Li_2(z) + log|z| log(1-z))
D(xsi) = sum_{i} n_i D(x_i) = 2.919705...

Conjecture: zeta'(L+1,-1) = 2/pi D(xsi).

2.
--

F = Q(sqrt(5)), L = (3Sqrt(5)) = conductor of E/F
the splitting field of
x^4 - (4+3sqrt(5))x^3 + 9*(3+sqrt(5))/2x^2 - (4+3sqrt(5))x + 1 = 0,
Gal(E/F) = Z/4Z.

Conjecture: exp(zeta'(L + k, 0)), k = 1, 2, 3, 4, are the roots
of the above polynomial.

At s = -1, H. Gangl has found two linearly indepedent elements
of the Bloch group xsi_1, xsi_2 in B(E) such that

  zeta'(L+-1, -1 = +- 1/pi*D(xsi_1)
  zeta'(L+-2, -1 = +- 1/pi*D(xsi_2)
  zeta'(L+-j, -2) = +- 30/pi^2\mathcal{L}_3(theta_j), theta_j in B_3(E), j = 1,2.

General Conjecture: zeta'(L+1, 1-m) = r*pi^{1-m} \mathcal{L}_m(xsi), where
                    xsi = xsi(L,m) in B_m(E).
                    E/F abelian [???] ext of F with conductor = L.

"Many of these results are only conjectures because they are results
of very very sophisticated experiments."

A group cocycle for Gamma=GL_2(Z).
Let x, sigma_1, sigma_2 in R^2 be nonzero vectors. R = real numbers

   f(sigma)(x) = det(sigma)/(<x,sigma_1><x,sigma_2>),   <x,y> = x_1 y_1 + x_2 y_2.

P in R[x,y],   f(sigma)(P,x) = P(-del_{x_1}, -del_{x_2}) f(sigma)(x)

is well defined outside the hyperplanes <x, sigma_j> =/= 0, j=1,2.

   A_1, A_2 in GL_2(), A_{ij} = jth column of A_i.

Then, for x=/=0, there is at least one column A_{ij} such that

       < x, A_{ij} > =/= 0.

Let A_{i,j_1} = the first column with that property.

Now I will define a rational cocycle.

Psi(A_1, A_2)(P,x) = f(A_{1,j_1}, A_{2,j_2}) (P,x)
is well defined for all x=/=0 in R^2.

Def: A in Gamma = GL_2(Z), u,v in R^2 \ {0}, P in R[x_1, x_2] homogeneous.

Psi(A)(P,u,v) = (2*pi*i)^(-1-deg(P) sum_{x in Z^2, x not 0} sign(xu) e(-xv) Psi(1,A)(P,x

conditionally convergent, but OK, but I won't talk about that since
it would take too much time.

Theorem 1: Psi is a 1-cocycle on Gamma, i.e.,
         Psi(AB) = Psi(A) + APsi(B),
where A Psi(B) (P,u,v) = Psi(B)(A^t(P), A^(-1)u, A^(-1)v).

Theorem 2: If u in Q^2\{0}, then the values of Psi can be expressed by a finite sum
of products of Bernoulli polynoials B_k(t), and the polylogarithmic functions

     lambda_k(t) = sum_{n in Z} e(nt)/n^k * sign(n),   where t in R.

Ex: A = [a,b; c,d], c=/=0, u=(1,0). Then

Psi(A)(1,u,v) = -2 sum_{all residues ell modulo c}
    Bbar_1((ell+v2)/|c|)log|1-e((al+av_2-cv_1)/c)|
                   - d/c 1/(2*pi*i) * lambda_2(a v_2 - c v_1).

Such a formula exists, in general; however, it is too complicated to
write down here on the board.

L^* = Z*alpha + Z*beta, u = (alpha, beta)^t, v = (tr(alpha), tr(beta))^t in Q^2.
P(x) = N(alpha x_1 + beta x_2).
U = <e>, e > 1
Then [e alpha, e beta]^t = [a,b; c,d]*[alpha,beta]^t.

Theorem 3: zeta'(L+1,1-m) = +-Psi(A)(P^{m-1},u,v).

So, basically, a cocycle is given by special values of a zeta function!!! WOW.
I've never seen anything like that before.

TALK: 18. COUVEIGNES (11.15-12.00): The Jacobi problem for graphs and
             related computational issues.

Jacobi Problem: K field, C_K curve, O in C_K(K)

(P_i)_{1<=i<=I} and D = sum_{i=1}^{I} e_i P_i = (sum e_i) O

Look for an effective divisor E of degree g such that D is
linearly equivalent to E - g O.
E = sum_{i=1}^g Q_i, where Q_i in C_K(Kbar)

K local field.
A complete dvr, v valuation
K = Fraction field of A
k = kbar residue field

C --> Spec(A) regular, finite type, C_K geo. inrr, complete, smooth
C_k nodal curve (reduced, ordinary double points)

G = intersection graph of C_k (points correspond to components of C_k, etc.)

Let L containing K ext of local fields
    B containing A corr ext of rings

C_B = BlowUpJustEnough(C tensor_A B)

xy = pi = (pi')^e <--- extension is no longer smooth, so must "make blowups".

Easy to determine G_e = G(C_B) from G=G(C). Chop each edge at two points,
into three pieces.

G_e = e-th division of G. (Same topological space as G, but with
a different cell-complex decomposition.)

Union_{e>=1} G_e^0 = G(Q) subset G.
This is the union of the vertices in G, where we view G as a topological
space.

Let P in C_K(K).

C ---> Spec(A)

P crosses C_k at a smooth point of it.

x(P) in G

P in C_K(Kbar)

x(P) in G(Q)

x: C(Kbar) --> G(Q)   [[huh?!?!!? I have no clue how he did that!?!]]

Knowing x(P_i) and e_i, can we guess x(Q_i)?

Answer < Raynaud - Neron models of Jacobians + some combinatorics

Integration in graph:
G, V, E
C_1(G,R) = R^E = vector space generated by edges
Bilinear form (,).   (e,e') = delta_{e,e'}.

Define a measure d mu on G.
If X subset G, for any edge e_0,

    sum_{e in E} mu(X intersect e_0) e = mu(X).

Example: (two loops touching at one point, and a certain X that is half of it.)

  mu(X) = 1/2*f + 1/2*e + 1/4*g in C_1(G,R).

Let gamma:[0,1] --> G be a path

Int_{gamma} d mu.

Fix a point O.

Universal covering:
U_O = {paths from O } / homotopy

pi_1(G,O) subset U_O   fundamental group, made from paths that are closed.

U_O -----> C_1(G,R) ---------------> H^1(G,R)

gamma|---> int_gamma dmu |---------> (int_gamma dmu, *)

phi(pi_1(G,sigma)) = tau   (the lattice of periods of the graph)

phi: G ---> H^1(G,R) / tau = T (The Jacobi map.)

H^1(G,Z) / tau   (finite group)

```
Cardinality = number of maximal trees in the graph
              (this is a very important classical result of Kirchov-Trent)
```

This is the Kirchov of "Kirchov's Law".

A maximal tree in a graph of genus g: remove g edges and what remains
is a tree. The number of maximal trees is the volume of the torus.

LENSTRA: Is that for only connected G.
Yes -- must be connected.

Raynaud, e.g., proved that this group H^1(G,Z)/tau is also the component
group of the Jacobian of the curve.

Theorem (Raynaud, see also BLR):

```
sum_i e_i phi(x(P_i)) = sum_{i=1}^g phi(x(Q_i)) in T.
\-------------------/
         known
```

phi: G --> T

phi^g: G^g ---> T

Assume genus of curve is genus of the graph (true if, e.g., C is a
"Mumford curve" [whatever that is!?!]).

phi^g (g_1,...,g_g) = phi(g_1) + phi(g_2) + ... + phi(g_g)

This is analogous to the map from C^g to Jac(C).

```
Surjective.

v : Sym^g(G) ----> T
{x_1,...,x_g} |---> sum phi(x_i)

----------------------------------------------------------
THEOREM:
  * surjective
  * the set of rigged points in T is dense
  * there exists a unique continuous section to v.
----------------------------------------------------------

Recall that G is a Hausdorff compact topological space CW complex blah blah

There is a section sigma : T -----> Sym^g(G), which gives a generic
answer to the Jacobi problem.

Let B be the set of staBle points in G^g.
(x_1,...,x_g) stable <====> there exists (e_1, ..., e_g) such that x_i
                            in e_i and g - union e_i is a tree.

      B subset G^g

Sym_g acts on B


     Can form the quotient B/Sym_g = K  subset Sym^g(G)

     K is a CW-complex, called the Kirchov complex.

     K is a torus and v|K is a homomorphism.

The equivalent to the Jacobian of the graph is a subspace of the
symmetric product.
```

20. D. ZAGIER & K. BELABAS (10.30-11.45): Cubic forms, fields and orders

```
Binary Cubic Forms :
  - binary quadratic forms
  - cubic fields
  - cubic rings

C   = {F = [a,b,c,d] in Z^4 },     F(x,y) = ax^3 + ...
C^+ = {[a, 3b, 3c, d]}, up to Gamma, SL_2(Z), GL_2(Z).

M = rank 2 Z-module
S^n(M) = (M tensor ... tensor M) / (a_1 tensor ... tensor a_n - a_{pi(1)}
                                       tensor ... tensor a_{pi(n)})
S_n(M) = (M tensor ... tensor M)^{Sigma_n}

F : M ---> Z cubic,   Gamma_F : S_3(M) ---> Z (linear)
T : S^3(M) ---> Z   T(x,y,z)
C^{+}(M) subset C(M) = { cubic forms } = Hom(S_3(M), Z)
T^* subset T(M) = trilinear
```

```
T --isom--> C^* \----> C --isom--> T^*

comp is multiplication by 3.

C_D^* = {F : D(F) = D}

C_{D,n}^* = {F : q_F = nQ, Q in Q_D^0}

D integer, O_D = Z + Z(D+Sqrt(D))/2
           I_D = {fractional O_D-ideals}
           Cl_D = I_D/K^* = {a} / (a equiv lambda*a) = Q_D / Gamma

Prop 1 (Nakagawa):
  C_{D,n}^*/Gamma =isom= {(a,theta) : a in I_D, theta in a^3,
                            Norm(theta)/Norm(a)^3 = n}/K^* ---> Cl_D

lambda in K^*:   lambda*(a,theta) = (lambda*a, lambda^3*theta)

Example: C_{D,1}^*/Gamma --isom--> Cl_D[3]

         H_3^*(D,1) = [O_D^* : (O_D^*)^3] * #Cl_D[3],   D =/= -3, Square

-----------------------------

Start with \a <---> Q = prim qf [A,B,C]
Find F st q_F = n*Q???

F.q_F = 0 where the inner product is

  C^* tensor Q ---> Z^2

[a, 3b, 3c, d] * [A, B, C]
  = (Ac-Bb+Ca, Ad-Bc+Cb]

Answer: L_Q = {F : F . Q = 0}   rank 2 lattice
F <---> theta in \a^3.

(theta) in \a^3, with index n

\a ---F---> Z
 x |----> Tr(n*x^3/(theta*Sqrt(D)))

\a = Z*A + Z*(B+Sqrt(D))/2

F = [a,3b,3c,d] in L_Q <==> a, b, c = (Bb-Ca)/A, d = (Bc-Cb)/A in Z

theta = b*A - a*(B+Sqrt(D))/2 in \a

...

I've showed that L_Q = \a^3.  Explicit construction of \a^3 as the set
of quadratic forms with the property that they are orthogonal to Q.
[He described it, but in an incomprehensible manner.]
```

K = Q(sqrt(D))
theta in \a^3,   N(theta) = n*N(\a)^3 = n*A^3
N(n*theta) = n^3*A^3
alpha = (n*theta)^(1/3), alpha' = (n*theta')^(1/3), alpha*alpha' = nA

```
            N = K(alpha, sqrt(-3))
            |                      \                      beta
            |                       \                      ||
            L = K(alpha)            Ltilde = Q((alpha-alpha')/sqrt(-3))
           / \                          |
        2 /   \ 3                       |  degree-3 cyclic abelian extension
         /     \                        |
  C=Q(al+al')   K=Q(sqrt(D))        Ktilde = Q(sqrt(-3D)).
        \       /
       3 \     / 2
          \   /
            Q
```

Cubic Ring R   comm. associ. ring with 1, R = Z^3 as group

Prop 2 (Delone - Faddeev):
{cubic rings} / equiv <-------- 1:1 bijection ------> (cubic forms)/GL_2(Z) == C

[notes stop]
============
K. Belabas:

\C^{irr} = { (a,b,c,d) in \C, irreducible over Q[x,y] }.

\R   = {\O cubic rings subset Qbar, [Fr(O) : Q] = 3}

I. Maximal Orders

{\O in \R, disc(\O) = D} / tilde ------------> {F in \C^{irr}, disc F} / Gamma = GL_2(Z)

Definition
[no more!]
----

23. B. ALLOMBERT (17.30-18.00): Computing automorphisms of Galois
    number fields with supersolvable Galois group

T in k[X], T is monic irreducible
K = Q[X]/(T)
I assume K/Q is Galois.   [or -- see as a test of whether or not Galois]
What is Gal(K/Q)?

sigma(X) = S(X) (mod T)
sigma(P(X)) = P o S(X) mod T.

II. Factorization over number field

i) Algorithm of Roublot, Pohst, etc.
ii) LLL algorithm directly
iii) KLUENERS (combinatorics)

Now for my algorithm, which is like Kluners's, but with better
combinatorial optimization.

p a prime number that does not divide disc(T)
p O_K = prod_{i=1}^g \p_i.
f = deg \p_i
F_{\p_i} = O_K / \p_i =isom=F_{p^f}

```
Gamma:  Gal(K/Q) --> Aut(O_K / p O_K)
          sigma|----> (x mod p O_K ---> sigma(x) mod p O_K)
```

Gamma is injective, he claims.

Aut(O_K / p O_K) = a semidirect product of (Z/fZ)^g and something he calls S_g.
#Aut(O_K / p O_K) = f^g*g!

Prop:
There exists an efficient algorithm that given s in Aut(O_K / p O_K)
determines whether or not s in Im(Gamma). If yes, finds explicitly
an element sigma in G such that Gamma(sigma) = s.

Definition:
We say that an automorphism sigma is diagonal (wrt to p) if it
does not permute the idea above p.

Prop:
There exists a diagonal element sigma in G with sigma =/= 1 if and only if
there exists d | f , d =/= f, so that <phi_1^d> is normal in G, [where
phi_1 "is Frobenius"].

In addition, there is a map

* psi: {1,2,..., g} ---> (Z/(f/d)Z)^*
  such that for i in {1,...,g}, sigma=phi_i^{d psi(i)}.

* Im(psi) is a subgroup of (Z/(f/d)Z)^*.

H = Im(psi), h = #H

QUOTE from Kluners: "I can understand this, because I know this
algorithm already. If you don't already know it, you have no chance!"

Definition (Supersolvable group):
[Maybe the definition is that the successive quotients in the
descending series are cyclic.]

Of groups of order < 100, 975 are supersolvable out of 1048 groups.
[I can hardly read his writing!]

Theorem. Let G be a SS group of order n = prod_{i=1}^r p_i,
with p_1 >= p_2 >= ... >= p_r.
[Some symbols but no logical connectives, and I can't understand what
he says, so I don't know what the theorem is.]

[I give up on trying to take notes for this talk.]

25. M. GIRARD (20.50-21.20): Explicit computation of the group generated by
the Weierstrass points of some plane quartics

C a curve of genus g>=2.
P is a Weierstrass point <==> there exists a regular differential
0=/=omega in H^0(C,Omega_C) with ord_P(omega) >= g.
weight.
W = { Weierstrass points }

```
Fix oo in W:  j : C \-----> Jac(C) = Pic^0(C)
                  P |-----> [P - oo]
```

WW = < j(W) > is independent of the choice of j.

g(g^2 - 1) Weierstrass points.

```
Hyperelliptic curves:  W = { ramification points wrt to the map to P^1 },
                       W = (Z/2Z)^(2g).
```

```
Non-hyperelliptic curves of genus 3: plane quartics
W = { flexes }         24 = r + 2s
T_p(C).C = 3P+Q            r   weight 1
T_p(C).C = 4P hyperflexes  s   weight 2
```

If oo is a hyperflex: sum w(P) j(P) = 0.
Naive bound on the rank: rank W <= 24-2s-1 if s =/= r.

[Now slides with LOTS of examples and theorems!!!]

```
Some groups:
W = (Z/2Z) x (Z/7Z)^3   (Klein quartic)
W = (Z/4Z)^5 x (Z/2)  Fermat quartic
W = Z^4 x (Z/3Z)^5    a quartic with a a parameter
etc.
```

Main tools to get such cool results:

```
C
|
|  family of smooth projective curves of genus g
|
S  W_eta group generated by the Weierstrass points in the generic fiber
   W_s   group generated by the Weierstrass points in the special fiber.

   (algebraic: Laksov-Thorup, analytic Hubbard)
```

* W_eta -->> W_s   (group quotient map)
* specialization is injective on the torsion part.   [for all but finitely many fibers????]

For a particular curve:
----

* Jacobian is isogenous to E_1 x E_2 x E_3, and reduce WP's modulo various primes

* descent via an isogeny.

For a family of curves:

-- Geometric arguments to reduce the number of generators

W_0 --------> W

-- For a suitable choice of the parameter, W_{C_0} = W_0

-- since W_eta = W_0

-- specialization theorem of Silverman:
When S is a smooth projective curve and Jac(C) --> S is a (flat)
family of abelian varieties, then the set {s in s(Kbar) | sigma_s is
non-injective} is of bounded height.

Stratification of M_g depending on the number of hyperflexes (Vermeulen):

M_g^{0} = { [C] in M_g, C non-hyperelliptic}

M_g   = { [C] in M_g, C possesses at least 5 hyperflexes }

M_1, M_2 are irreducible (of dimensions 5 and 4)
M_3 has 2 irreducible comonents X_2, X_5, dim X_ = 3
M_4 has 5 irreducible comonents ..

[Now she puts a frightening slide! Here's a line from the slide:]

s = 0, W_{\eta} = Z^r with 11<=r<=23.
(s is the number of hyperflexes)

26. H. GANGL (21.30-22.00): Calculations of the homology of GL(n,Z)

This talk represents joint work with Elbaz-Vincent and Soul\'e.

Motivation: Ever since Quillen defined higher algebraic K-theory, for
rings, fundamental problem has been:

determine K_*(Z)

History of "knowledge":

K_0(Z) = Z

```
K_1(Z) = Z/2Z
K_2(Z) = Z/2Z
K_3(Z) = Z/48Z    (Lee-Szczarba, 76)
K_4(Z) = 0

K_4: Rognes 2000, Soule '79 but written up in 2000, Rognes-Weibel AMS
2000, Voevodsky's work on Milnor conjecture (new version of his proof
on the web).

K_5(Z) = Z x (3 group)
K_6(Z) = expected to be 0

Lee-Szczarba:  H_*(GL_N(Z), Steinberg or Z or Z[1/p's])  |--info--> K_*(Z)

Explicit way to determine homology:

Voronoi's reduction theory for quadratic forms
---------------------------------------------

C_N = space of real symmetric NxN-matrices that are positive definite

Action of scalars R_*^+

Let X_N = C_N / R_*^+

Add "rational" cells:

C_N^* = space of real symmetric NxN-matrices, semi-positive definite,
        and the kernel of the matrix lies in subspace of Q^N.

X_N^* = C_N^* / R_*^+.

action of g in GL_N(Z) on C_N^*:

   A * g = g^t * A * G

preserves C_N, boundary(C_N^*) = C_N* - C_N  [huh???]

y_N^* = X_N^* / GL_N(Z)

Perfect forms:  (characterized by its innermost qualities)

A in C_N^*,

on C_N^*:  mu(A) = min { b^t A b | b in Z^N \ {0}}

on X_N^*:  m(A) = {b in Z^N : b^t A b = mu(A)}

A perfect form is characterized by the following property:

  if B in X_N^* satisfies m(B) = m(A) then B = A.

Geometrically interpret:

  Each b in Z^N defines a point b*b^t in C_N^*
```

Associate to A its convex hull of m(A). This gives
a cell decomposition of C_N^*, GL_N(Z)-equivariant,
which induces a cell decomposition on Y_N^*.

Voronoi (Fundamental theorem)

This gives a finite CW complex in terms of perfect forms.

perfect forms = # cells

```
N         2  3   4    5         6        7               8
---------------------------------------------------------------
# cells   1  1   2    3         7       33              >10000
         \-------------/
Voronoi, Korkhine-Zolotareff Barnes   Stacey         "Martinet group"
                             Stacey   Jaquet (1990)    in Bordeaux
                             Watson                  "This is not a
                                                      mathematical group..."  [laughs]
```

Jaquet gave all data necessary for computaiton of full CW complex.
I.e., all perfect forms and neighbours. Further tools (Bernd Souvignier)
  * algorithm for determining GL_N - isomorphism between two quadratic forms
  * algorithm to compute automorphism group of quadratic forms.

Plug this algorithm into PARI up to N=6.

V_N = Finite cell complex --- relative homology H_*(O_N^*, boundary(Y_N^*), Z[-])

Theorem: For N = 5, 6, we have

n<=14

```
                          /---   Lambda_5,  n = 9 or 14
   H_n(V_5, Lambda_5) = --
                          \---   0          otherwise
```

Lambda_5 = Z[1/2,1/3,1/5]

n<=20

```
                          /---   Lambda_6,  n = 10, 11, 14
   H_n(V_6, Lambda_6) = --
                          \---   0          otherwise
```

Lambda_6 = Z[1/2,1/3,1/5,1/7].

[Do you have a conjecture for H_n(V_i, Lambda_i).] Answer: NO!!

Link to K-theory:

* vanishing of homology groups

* stabilizers of cells involved ---> homology

* equivariant spectral sequence

*

*

Theorem: (joint with Soule and Elbaz-Vincent)

     K_5(Z) = Z

Theorem: K_6(Z) has only p-torsion for p<=7 and no torsion-free.

* ranks of all K-groups of rings of integers are known and the formula is easy

```
   rank K_n(O_F) = {r1 + r2     or r2    or 0
    n>1             1 od 4      3 mod 4     n even
```

----

28. J.-F. MESTRE (10.15-11.00): Lifting of Galois extensions from k to k(t)

Inverse Galois problem
G finite group
a) Does it arise as the galois group of an extension of K of Q

b) Galois group of regular extension of Q(T)

Problem: Suppose given K/Q with group G.
Does it exist M/Q(T) regular, with group G.
s.t. T = 0 we recover the original K/Q.
REGULAR == M intersect Qbar = Q.

We will see some generalizations of Poncelet's theorem on conics and so.

Theorem: True for G = PSL_2(F_7) ==isom== PGL_3(F_2).

What it means?

More precisely, there exists H in Z[a_0,...,a_6],
H =/= 0, s.t., if P in k[X], deg(P) = 7,
P = X^7 + a_6*X^6 + ... + a_0, with H(a_0,...,a_6)=/=0
"Have to don't verify."
with Gal_k(P) \subset PSL_2(F_7)
there exists Q in k[X], deg(Q) <= 6
such that Gal_{k(T)} (P - TQ) = PSL_2(F_7).

HENDRIK: Does the Theorem follow from the "More precisely"?
MESTRE: Uh-- no. If you prefer, the theorem is false. It is not proved.
HENDRIK: I made my point.

"The theorem is more general... no!... it is different."

Theorem: Let x_1,...,x_7 be indeterminates in K = k(x_1,...,x_7);
P(X) = prod_{i=1}^7 (X - x_i)
then there exists Q with deg(Q) = 6, Q in K[X],
Gal_{K(T)}(P-T*Q) = PSL_2(F_7).

The coefficients of Q are invariant by PSL_2(F_7) subset S_7.

Trinck: P = X^7 - 7X + 3 --> G isom PSL_2(F_7)

Q = (X-1)^2*(X+1)*(2*X^2+X+2)

===> Gal_{Q(T)}(P-T*Q) = PSL_2(F_7).

La Macchia found families of polynomials with group
PSL_2(F_7):
  P_n(X) - T*Q_n(X)

Matzat & M[??] found families of polynomials with group
PSL_2(F_7):
  P_{a,b}(X) - T*Q_{a,b}(X)

f : (X,T) ----> T   (degree 7)
    P(X) - T*Q(X) = 0

This covering is ramified in 6 points with type (2,2).
fiber = 2 simple points and 2 points of order 2

From point of view of coverings, it's a covering from P^1 ---> P^1
with ramification type (2,2).

II. Correspondences of type PGL_3(F_2):

P^2(F_2) ------------> incidence relations between points and lines

Fano plane: a triangle with vertices labeled 1,2,3. [He draws
a familiar diagram.]
He now lists the lines:
  (1') = (2,3,4)
  (2') = (1,3,5)
  (3') = (1,2,6)
  (4') = (1,4,7)
  (5') = (2,5,7)
  (6') = (3,6,7)
  (7') = (4,5,6)

Definition: Let F be an element of k[X,Y]
of bidegree (3,3). Let
    A = (x_1,...,x_7) in k^7,
    B = (y_1,...,y_7) in k^7
F is PGL_2 configuration for A and B   [ZAGIER says: call it a "PGL_3 configuration"!]

      if f(x_i, y_j) = 0 <===> i in j, and P_i in D_j.

roots of F(x_1,y) are y_1, y_3, y_k

[HELP!!!]

Now he draws a big horizontal tree-like thing that uses a confusing
notation, but somehow encodes the correspondence defined by F.

Recall construction of Poncelet:
...

Theorem: Let x_1,...,x_7 be indeterminates.
There exists y_1,...,y_7 in K = k(x_1,...,x_7)
such that
  i) there exists F in K[X,Y] of bidegree (7,7) [???]
     of GL_3(F_2) configuration for (x_1,...,x_7), (y_1,...,y_7)
 ii) there exists G in K[X,Y] of bidegree (4,4) such that
       G(x_i, y_j) = 0 <===> i=/=j.

F(X,Y) G(X,Y) = V(Y) X^7 + ... = V(Y)P(X) - U(Y)Q(X),
                        = det ([P,Q; U, V])

where

    P = prod (X-x_i)
    U = prod (Y-y_i)   i=1,2,...,7.

If T is an indeterminate,
    P_T(X) = P(X) - T*Q(X)
    U_T(Y) = U(Y) - T*V(Y)

det ([P,Q; U, V]) ==also== P_T(X)*V(Y) - U_T(Y)*Q(X).

Theorem: If a 3-3 correspondence of P^1 x P^1 has one PGL_2(F_2)
configuration, then from any point x in P^1, we obtain a
PGL_3(2)-configuration.

Fact: Gal_{k(T)}(P-T*Q) = PGL_3(F_2).

To prove.
 a) Gal_{k(T)}(P-T*Q) subset PGL_3(F_2)
 b) In fact, equality.

 29. J. KLUENERS (11.15-12.00): Counting Galois extensions of number fields
(joint with Gunter Malle)

1 =/= G subgroup S_n (transitive)
Inverse Galois Problem:
Given a number field K, does there exist K/k such that Gal(K/k) = G?

G solvable group: YES.

```
k = Q, G=M_{23}, there is no known one.  (only sporadic one not known to occur)

If 1 =/= sigma in G, let

          ind(sigma) = n - #cycles(sigma).   [id has n cycles, (1...n) has 1 cycle.]

   i(G) := min_{1=/= sigma in G} (ind(sigma)),

   a(G) := 1/i(G)

S subset P(k) finite

--> Z(k,G,S; x) := #{K/k | Gal(K/k) = G, |N(d_{K/k})| <= x,  K/k is unramified in S}.

Any extension of fields K/k:   Gal(K/k) has group G if normal closure Khat
of K/k has group G and K = Khat^{G_1}.   (G_1 is some sort of "point stabilizer".)

    Z(k,G,x) = Z(k,G,empty_set, x)

Conjecture 1 (Malle):  for all eps > 0, there exists c_1(k,G,S) > 0 and a constant
c_2(k,G,eps) such that

          c_1*x^{a(G)} <= Z(k,G,S; x) <= c_2*x^{a(G)+eps} for x >> 0.

The point of the conejcture is that a(G) is as defined; the point is
that it only depends on G, not the ground field.

Conjecture 2 (see H. Cohen's MSRI proceedings article):
             There exists a constant c=c(k,G)>0 and b=b(k,G)>=0 such that
             Z(k,G; x) asymptotically c*X^{a(G)}*(log(X)^{b})

D. Wright (1989): Conjecture 2 is true for Abelian groups, so Conjecture 1 is also.

Other results: Conjecture 2 is true for G = S_3.

Remarks:
(1) 1/(n-1) <= a(G) <= 1,  a(G) =1  <==> G contains a transposition

(2) G regular (#G = n),  ell the smallest prime dividing n.
    Then i(G) = n - n/ell = n(ell-1)/ell ======> a(G) = ell/n*(ell-1).

Main Theorem (K - M):
---------------------    [what does "in regular representation" mean???]
                       /-------------------------\
Suppose G is nilpotent in regular representation, then conjecture 1 is true.

Other results:

(i) Suppose G is an ell-group, which is not necessarily
regular [what is regular???], then the upper bound of conjecture 1
holds.

(ii) Lower bound of conjecture 1 holds for G = (C_2 wreath product H),
if there exists K/k with group H.
```

So, if 2|n then there exists a group G not S_n such that Z(k,G,x) grows
at least linearly.

Proof: G nilpotent, ell the smallest prime dividing #G = n.

(*) 1 --> C_ell --> G --> H --> 1 central extension.

```
        Ltilde = Ktilde(u^{1/ell})
       /  |
      /   |
  /--L    |
 /   |  2/Ktilde
/    | /  |
G    K    |
 \   |  /-ktilde
  \  | /
   \-k
```

The embedding problem for Ktilde/ktilde is a Brauer embedding problem.
... All solutions are of the form

Ltilde_b = Ktilde((b*alpha)^{1/ell}), b in ktilde^*/(ktilde^*)^ell.

Question: For which b do we have Gal(Ltilde_b/k) = C_2 x G. In this
case, L_b denoes the subfield of Ltilde_b such that Gal(Lb/k) = G.

Question <==> Gal(Ltilde_b/K) isom C_ell x C_2 ,==> Gal(Ltilde_b / K) is abelian.

Shafarevich: sigma(b*alpha)/(b*alpha)^q in Ktilde^{ell},
------------   sigma(zeta_ell) = zeta_ell^q.

Assumption: Ltilde_1 = Ltilde, Gal(Ltilde/k) = G x C_z ---->
sigma(alpha)/alpha^4 in Ktilde^{ell}

<==> sigma(b)/b^q in Ktilde^{ell}

[The "<==>", as he uses them, are horrid notation.]

Special case: H = 1 ---> b has above property --> k_b / k is cyclic of order ell.

Lemma: k_b |---> L_b has finite fibers (globally bounded)

(So, IN SOME SENSE, I've reduced my problem to counting cyclic extensions of
the ground field, which is much easier to do.)

d_{L_b} = d_K^{\ell} N(d_{L_b/K... [I can't read that side of the board,
but you get the idea.]

Motivation for conjecture:

Suppose p | d_K and that K is tamely ramified at p. Let sigma in
inertia group (maybe inertia group is cyclic and sigma is a
generator), then p^{ind(sigma)} || d_K This is some philosophy about

why this conjecture could be true.

COHEN's question: By working a little harder, what can you say about the eps?
   Do you know if it is a power of log?

----

30. M. STOLL (14.00-14.30): Reduction of binary forms -- a progress report

http://www.math.uni-duesseldorf.de/~stoll

[[Edited by M. Stoll]]

Problem: F = a_0 X^n + a_1 X^(n-1)*Y + ... + a_n Y^n in Z[X,Y]_n,
         squarefree, n>=3.
Find gamma = [a,b; c,d] in SL_2(Z) such that
F*gamma = F(ax+bY, cX+dY) (right action) is "small",
and some bound on the size of such an F*gamma.

||F|| = sum_{i=0}^n |a_i|^2 (not really a norm!)
      = int_{0}^{1} |F(e^{2\pi i phi}, 1)|^2 d phi

Motivation: * x^2 + y^3 = z^5 (BEUKERS & EDWARDS)
              * cubic fields   (ZAGIER & BELABAS)
              * hyperelliptic curves   y^2 = F(x,z),   deg F = 2g+2

Generalization: F in C[X,Z]_n,   Gamma subset SL_2(C)

1. The story so far (very brief):
----
  * 1848   Hermite ("Her-meet" is the correct pronunciation)
           (10 pages, Crelle, v.36) over R and degree n = 3, 4

  * 1917   G. Julia (300 pages) redoes what Hermite did and extends it to C.
           n=3,4.

  * (1999) Cremona & Stoll: n >= 5.

  * April 2000: Hendrik made a remark right after my talk last year in
           Leiden. It was an innocent remark... he was looking for a
           coordinate-free formulation. But the remark led me to rethink.

2. The story revisited (a fake prehistory of Hermite's idea):

Consider \h = upper half space = C x R_{>0}
    z = t+u*j in \h,
    t in C, u in R_{>0}, j = (0,1).

There is a correspondence. Let Q = a(|X-tY|^2 + u^2|Y|^2) be a positive
definite Hermitian form, where a>0 and t and u are above.

Then Q corresponds to t+u*j:

    Q = a(|X-tY|^2 + u^2|Y|^2) |-------> t + u*j in \h.

Call this correspondence z. Define the discriminant of Q to be

    disc(Q) = a^2*u^2.

This corresponds to the discriminant of Gauss for quadratic forms.

                          \/------------- the "prime" means "square-free forms"
IDEA: Set up a map z : C[X,Y]'_n ----> \h, equivariant with respect to SL_2(C)

This idea already "fixes things" for n=3, 4 because of symmetry considerations.

Look at the extreme case: Gamma = SL_2(C).
Let \F = {j} be a "fundamental domain" for the action of Gamma on \h.

ZAGIER: That's not arbitrary at all. You've already chosen
coordinates and j is the point of smallest height.

Want: ||F|| small when z(F) = j.

Define thetatilde(F) = min_{gamma in SL_2(C)} ||F*gamma||.

Try z(F) = gamma^-1*j for minimizing gamma --> problem: not unique

We want to find z(F) in \h, so we can look for Hermitian forms. Take

B(F) = {Q pos. def. Hermitian form | Q^n >= |F|^2 (pointwise)}

Then, if z(Q) = j, with Q = a(|x|^2 + |y|^2)
    ====> ||F|| = Int |F(e^{2\pi i phi, 1)|^2 d phi <= ... = 2^n (disc Q)^{n/2}.

So, define
 thetahat(F) = min_{Q in B(F)} 2^n (disc Q)^{n/2}.

and try z(F) = z(minimzing Q) --> problem: don't know B(F) well enough

Remedy this by restricting the set of Q's.

J(F) = {1/n*sum|F_i|^2 | F = F_1...F_n, F_i linear in C[x,y]} subset B(F)
by AGM inequality.
      (grew out of Hendrik's suggestion)
(lots of things in there, because of constants. F_1 |---> 1/2*F_1)

theta(F) = min_{Q in J(F)} 2^n (disc(Q))^{n/2},

z(F) = z(Q) for a minimizing Q.

This is what Hermite and Julia were doing, but formulated more nicely!

Theorem of Cremona and I: This is well defined; there is a unique such Q.

Also: Suppose F = a_0 \prod (X - alpha_i Y),

```
define R(F,t+u*j) = |a_0|^2\prod_{i=1}^n ((|alpha_i - t|^2 + u^2) / u)
for t+u*j \in \h

==> theta(F) = min_{z\in\h} R(F,z), and the minimum is attained only
at z = z(F).

[[ Comment by MS:
     This means that in order to find z(F) and theta(F), you only have
     to solve a minimization problem in three (or two, if we restrict
     to SL_2(R)) variables instead of n-1. This makes this approach
     practical. For Gamma = SL_2(Z) and forms in R[x,y], this is
     implemented in Magma. Check out the function Reduce. (There are
     a couple of bugs there, which will be removed soon. The computation
     of z(F) should work, though -- use Covariant, and the reduction
     of orms of degree >= 5 should also be OK.) ]]

3.  The story continued
------------------------

What have we lost?  Can we bound the loss?

Proposition:   2^{1-n} theta(F) <= thetatilde(F) <= thetahat(F) <= theta(F)
------------

So our theta(F) and z(F) are not far from the optimal one.

Theorem:   (i) 2^{1-n} <= ||F||/R(F,j) <= 2^{-n} binom(2n,n)
--------
          (ii) there exists eps(F) > 0 such that

           eps(F) cosh^{n-2} dist(z,z(F)) <= R(F,z)/theta(F)
                                          <= cosh^n dist(z,z(F)).

          dist(z,z(F)) is hyperbolic distance.

[[ Comment by MS:
     (1) tells you that R(F,j) is about as good as a
      measure of the size of F as ||F||.
      By Cremona-Stoll, R(F,z) is minimal at z=z(F), so we can get
      bounds on ||F|| by comparing R(F,j) with R(F,z(F)). This is
      done in (2). ]]

Well, this looks a bit technical, but you can use it to deduce a few
interesting facts.

Corollary:  Let \F be a fundamental domain for Gamma such that \F
            contains only points that are closest to j in their orbit.
            Then if z(F) in \F
---------
    (1) ||F|| <= binom(2n,n)*cosh^2 dist(z(F), j) / (2 eps(F)) || F*gamma ||
         for all gamma in Gamma.

    (2) ||F*gamma|| > ||F|| for all gamma in Gamma such that
          cosh ( dist(gamma^{-1}*z(F),j))
                               > (2^{n-1}/eps(F) * ||F|| / theta(F))^{1/(n-2)}
```

[[Comment by MS:
(1) says that the size of a reduced F (i.e. such that z(F) in \F) is fairly small, compared to other forms in the same orbit.
(2) provides a way to determine a finite set of gamma in Gamma such that ||F*gamma|| is minimal for one of these gamma's,if Gamma is a discrete subgroup like SL_2(Z). I.e., we have an algorithm that solves the problem stated at the beginning.]]

*31. D. KOHEL (14.35-15.05): Computational aspects of Shimura curves

Explicit approaches to X_0^D(m)

-- A progress report

A. Indefinite quaternion algebra \H/Q \-----> M_2(R)   (embedding exists because it's "indefinite").
O = Eichler order (intersection of two distinct maximal orders)
index m in a maximal order
D = disc(\H).
B. Matrix representation \H -----> \H \tensor_\Q K ---isom---> M_2(K) ---------> M_2(R)
K \--> H   real quadratic   given by a real embedding of K

Definition:

Gamma_0^D(m) = i(\U^1(\O)) (image of norm one units of the Eichler order)

Then Gamma_0^D(m) acts on \H

ZAGIER: This is very strange. Why *choose* the K? There's a natural map to H tensor R and the Shimura curve sits on the Hilbert modular surface. He's taking a projection. Why? It's unnatural. He's (H tensor R)_{N=1} isom SL_2(R) contains U_1. There's just no point in choosing this isomorphism.

(1) Supersingular points on X_0^D(m) / Fpbar

(2) Fundamental domains

Gamma_0^D(m) acts on \H

Gamma_0^D(m) \ \H = X_0^D(m)(C)

Elliptic points: gamma in Gamma_0^D(m) [with fixed points].

II. X_0^D(m)(C) moduli space of pairs

(Abelian surfaces A/C,   \O\--->End(A))   where \O is the Eichler order

BRUMER: Principally polarized!!!!!!
DAVID: I don't know...

N.B. \O \subset M_2(\Z) (discriminant 1 case)

Gamma_0(M) \subset \O , the Shiura curve is X_0(m).

A isogeneous to E x E.

B. Supersingular Points:
X_0^D(mp)/Fpbar contains SS(Fpbar)
(m,p), (D,p) = 1

free abelian group on supersingular points

Mestre-Oesterle: "Method of Graphs"   (D=1, E/Fpbar)
Pizer: Compute using quaternion algebras)

Applications:
(1) L-functions of simple factors of Jac(X_0^D(m))
-- modular symbols

(2) Monodromy pairing
Kohel - S. : Component groups

III. Fundamental domain.

Structure of Gamma_0^D(m) acting on \H.

```
H = Q<i, j>:   i^2 = a,  j^2 = b,  ij = -ji = k.
    \
     \
      -\ { [u, v; vbar*b, ubar] : u in Q(sqrt(a)) }.
```

eps in Q(sqrt(a))

[eps, 0; 0, epsbar-epsbar [what?]]:   z |---> eps^2 z.

Expands the upper half plane, he says.

"Now I'll describe a sketch of an algorithm [excuses...]"
Algorithm components:
We have a few, well, tools that are at our dispossal.

A. Problem: Gamma_0^D(1) may have no elliptic elements.
However, the normalizer, N(Gamma_0^D(1)), does have elliptic elements.

Gamma_0^D(1) subset SL_2(R) -----> SL_2(R) / SO_2(R) isom UpperHalfPlane

B. Searching for "small" generators.

C. Volume of a domain, known formulas for
Gamma_0^D(m) \backslash \H.

EXAMPLE:
Almost in the definitive reference: M-F. Vign\'{e}ras

X_0^{15}(1).

[David did not in any way say that much of the above is joint work with Helena Verrill. Maybe it isn't? That's weird.]

*32. N. ELKIES (15.15-16.00): Progress report on genus 2

Also the universal curves over them XX (N).

X_0, X_1, ... (N)

"Curve of general type" is a fancy way of saying a curve of genus at least two.

Steven Galbraith found a rational point on X_0(331)/w only a few years ago.

Next natural thing to study: curves of genus 2. Principally polarized abelian varieties of dimension 2.

Two generalizations of X_0 for genus 2.
X_0(N) (E, cyclic subroup order N) or (E, isogeny of degree N)
two generalizations of this for abelian varieties, since image of isogeny might not be principally polarized.
I will focus mostly on the Z/NZ subgroup interpretation.

Some rational moduli spaces of g=2 Jacobians

"\X_1(5):" {(C,P) | P in J_C[5] } rational: Z^2 + Z*A(x,y) = S(x,y)

o\'{u} A = L(Q-LL') - LQ, S=Q^2(Q-LL') for some linear L, L', quadratic Q.

P is represented by (Q = 0, Z = LQ); <w> : (L, L', Q) |---> (L', -L, Q-LL')]

This looks like X_1(5): Think of Q as the abscissa and L, L' as scalars!!

```
The cubic cover X_1(10) of X_1(5) is rational: (Q,Z) is 2-torsion
  <==> L'=(1-2t)(t/(t-1))^2*L,  Q=-t^4/(t-1)^2*L^2.  So to make x/y = 0, 1, oo
          \---f(t)--------/       \---g(t)---/
```

Weierstrass points on the \X_1(5) family: For any t_0, t_1, t_infty, solve for coefficints of L, L': L'/L(0) = f(t_0), L'/L(1) = f(t_1), etc.
Probably \X_1(N) has a rational parametrization like X_1(N) for all N such that g(X_1(N)) = 0, i.e., N=(1,) 2, 3, ..., 9, 10, 12. I have this for N=/= 9, 12, so far.

Some examples:

{C, (Z/4 x (Z/2)^3 \---> J } : is y^2 = X*\prod_{i=1}^4(X-x_i^2), It's P(B_4). cf. Sqrt(lambda) in Jaap Top's talk.

{C, (Weierstrass point) x (Z/3)^4 \---> J} : P(E_8^omega) The

Shephard-Todd #32; Shioda E_8/Q(mu_3)]

{C, (Z/2)^4\--- J, P, Q in C, D in Jac(C), P+Q = 2D} : P(D_6)
A Shioda-Usui "excellent family"

Conjecture[sic]: \X_0(N) of general type for all N>=N_0.

and eventually no rational Z/NZ subgroups or (N,N) isogeneis over Q
or any other given number field.

Harris said Kieran O'Grady tried hard to show this for sufficiently
divisible ones.

(2) Curves and Families with high-order torsion a la Leprevost

The curves below have simple Jacobians.
We know they are simple because: Lemma 3.1.2 (Leprevost)
If #Gal(Q(Frob_ell)/Q) = 8, for some ell then J is simple.

N=40: y^2 = (3x+4)(x^4+5x^3+8x^2+19/4*x+1), ((-2,1))-(oo) also X = 0,-1.

Howe Unpublished family with 30-torsion.

N=39: y^2 = x^6 + 4*x^4 + 10x^3 + 4x^2 -4x+1; (oo) - (oo') (also X=0,1,-1!!!)

Calculus nightmare:

```
 Int_(39x^2+9x-1)dx/y = 15*log|y+x^3+2x+5| + 3*log|y+5x^3+12x+10x+1|
                                + log|y+x^3+2x-1| + C
```

N=34: y^2=(9x^2+2x+1)(32x^3+81x^2-6x+1)...

N=32: a family over Q(t)

N=30

N=31, almost: A 31-element subbgroup of J generated by
points defined over (Q(mu_7))^+.
I know the equation.

J is simple, but has Z[sqrt(2)] multiplication (Poonen, Bending) and
is thus modular (Ellenberg) of conductor (245 = 5*7^2) (B. Poonen
using Q. Liu's program). Modular forms and mod-31 congruence with an
Eisenstein series, determined by W.A.Stein.

HENRI COHEN: I wrote "Q. Liu's program"!!! Liu's algorithm, but Cohen
implemented it!!!! [I didn't know that.]

A novel class of moduli problems.

Implicit in these constructions is the following class of problems:

```
Let \X be some arithmetic cover of \(1), so a generic point
of \X cooresponds to a genus 2 curve C with some torsion structure on J.
Suppose this structure includes a set S of ivisors of degree 1.
Let \X(S) = {c in X : all elements of S are effective} [i.e. "S subset C"]
Describe S.  Components?  Type of surface/genus of curve? ...?
Geometrically \X(S) is the intersection of |S| divisors coming from
Theta.  So one might expect a mechanical solutin, but
WARNINGS:
  * Typically, there exists boundary components:
          easy to put S in E_1 union E_2 subset E1 x E2

  * If D_1+D_2 = D_3 + D_4 nontrivially in S union i^*(S) must be on boundary.

  * \X(S) may have components of dim > 3-|S| due to Aut(C)
       (see B. Poonen - |S - (Weierstrass)| = 16)

  * Further accidents may occur.  e.g., S = {P_0, P_1, P_4} with
    P_0 Weierstrass, 4(P_1-P_0) sim P_4 - P_0, 17(P_1-P_0) sim 0
    ---> \X(S) = {s^2 + 3t^2 = 0}

Natrual Conjecture: Over C, if Aut(C) = {1,i}, then

  #{P in C | [P] - [i^* P] in J_{tors} - {0}} <= 3

with finitely many exceptions.  [===> #{ ... } = O(1)]

We've seen one exception (J[39]); any others?

---
A proof of a construction/computation:

y^2 = Q(x)        Weierstrass point oo
 P <------> x = 0
4P <------> x = -1

(4P) + iota^*(4P) - 5oo  = (y - A(x))

      4*(4P) - (P) - 5oo = (y - B(x))

y=A at P and iota(4P)
y=B at P and 4P
Q-A^2 = X(X^4+1)
Q-B^2 = (X^4+1)X
A^2-B^2 = (X+1)^4X- X^4(X+1)

etc.

[COMMENT OF NOAM:
One other thing I noticed: the previous work (which of course I should
have mentioned before starting on my N=40 etc. curves, not in the
middle as I did and as it thus wound up in your notes) is:

  Howe, Leprevost, Poonen: curves and families of curves whose Jacobians
  are isogenous with E*E' and have an N-torsion point for various N,
  the largest being 63
```

  Leprevost: curves and families with simple Jacobians and an N-torsion
  point for various N up to 29 (published) and 30 (an unpublished family
  reported to me by Howe)

I don't want to create another "Pell's equation" by misattributing
Leprevost's work to the intermediary who communicated it to me
(as Pell did x^2-Dy^2=1 from Fermat to Brouncker if memory serves)!
]

It's over!!!!