Arithmetic Invariant Theory + Hyperelliptic Curves

Evan Dummit – April 16, 2013

1 Goals

- This is a prep talk for Jerry Wang's talk.
- I aim to discuss extremely roughly the following topics:
  - (i) Some things about hyperelliptic curves (cf. Farkas and Kra's book)
  - (ii) A slapdash discussion of the 2-Selmer group (cf. Silverman 1)
  - (ii) "Arithmetic Invariant Theory" as it applies to hyperelliptic curves (cf. Bhargava and Gross's papers)

2 Hyperelliptic Curves

- This is adapted from Farkas/Kra's "Riemann Surfaces", so I might accidentally say "Riemann surface" instead of "algebraic curve" (though it shouldn't really matter anywhere).
- As we all know, if D is a divisor on C, then Riemann-Roch says $l(D) = \deg(D) - g + 1 + l(K - D)$, where K is the canonical divisor.
  - The rhetorical question we usually ask when talking about elliptic curves is: is there a meromorphic function with a pole at only one point? (Yes: $\wp$, and it has a double pole, because it's not possible to have only a single pole.)
  - The general version asks something like: given C of genus ≥ 2, what can we say about the points P such that there exists a meromorphic function of degree $\leq g$ with a pole only at P?
- Theorem (Weierstrass Gap): If C is a curve of genus $g \geq 2$ and P is any point of C, then there are precisely g integers $1 = n_1 < n_2 < \cdots < n_g < 2g$ such that there does not exist a function holomorphic on $M \backslash \{P\}$ with a pole of exact order n_j at P.
  - These numbers $n_1, \cdots, n_g$ are called the "gaps" at P; the other positive integers are called "non-gaps". The gaps and non-gaps obey a bunch of properties, which I won't list. (The non-gaps rather obviously form a semigroup.)
  - The theorem follows immediately by using Riemann-Roch on the sequence $l(0)$, $l(P)$, $l(2P)$, $l(3P)$, ... ; we are looking for entries that repeat. By Riemann-Roch we know that $l(kP) = k - g + 1$ for $k \geq 2g - 1$, so after $l((2g-1)P)$ there are no duplicates, and since $l(0) = 1$ and $l((2g-1)P) = g$, there are exactly g duplicate entries: hence there are g gaps, all in the set $\{1, \cdots, 2g - 1\}$, and 1 is always a gap.
- Definition: A point P on a curve of genus ≥ 2 is a Weierstrass point if at least one of the integers $2, \cdots, g$ is not a "gap", or equivalently, if the gaps are $1, g + 1, g + 2, \cdots, 2g - 1$.
  - There are finitely many Weierstrass points on a curve of genus ≥ 2; more precisely, there are between $2g + 2$ and $g^3 - g$ of them. (Both bounds are in fact attainable.)
- Definition: A hyperelliptic curve C is a ramified double cover of $\mathbb{P}^1$. If it has a point over k, then C has an affine integral model of the form $y^2 = f(x)$ where $f \in k[x]$ is a polynomial of degree $2g + 1$ with no repeated roots (for smoothness).

  - Degree 3 would give an elliptic curve. We'll allow this, except when we won't.
  - By a change of variables, we can assume that f has odd degree.

- Here are some things that are true about a hyperelliptic curve C of genus g over $\mathbb{Q}$ (with a given identity point, which we put at ∞):

  - Every curve of genus 2 is hyperelliptic, but this is not true of higher genus.
  - There is a function y of degree 2 on C, which is unique up to Mobius transformations.
  - There are exactly $2g+2$ Weierstrass points on C, and the gap sequence at each point is $1, 3, 5, \cdots, 2g-1$.
  - The Weierstrass points are in fact the branch points of y – or equivalently: they are ∞ along with the $2g+1$ roots of $f(x)$.
  - As such, the set of Weierstrass points provides a moduli space for the space of hyperelliptic curves: $2g+2$ distinct points in $\mathbb{P}^1$, up to Mobius transformations – thus, by dimension arguments, the space of hyperelliptic curves is something like $2g-1$-dimensional. (The space of genus-g curves I think has dimension $3g-3$ for $g > 1$, so feel free to compare the sizes.)

- Now let us take a hyperelliptic curve C with equation $y^2 = f(x) = x^{2g+1} + c_2 x^{2g-1} + \cdots + c_{2g+1}$.

  - The ring of rational functions regular away from ∞ is $\mathbb{Q}[x, y] = \mathbb{Q}[x, \sqrt{f(x)}]$.
  - C has a unique affine integral equation $y^2 = x^{2g+1} + c_2 x^{2g-1} + \cdots + c_{2g+1}$, if we clear denominators, and further assume that it is not the case that there is a prime p such that p^k divides c_k for all k – in such a case we say the coefficients are <u>indivisible</u> [with liberty and justice for all].
  - The discriminant of $f(x)$ is nonzero and has homogeneous degree $2g(2g+1)$ in the coefficients c_m (where c_m has degree m).
  - <u>Definition</u>: The discriminant Δ of the curve C is $\Delta(C) = 4^{2n} D$. As usual, if p doesn't divide Δ then the curve has good reduction at p.
  - <u>Definition</u>: The naive height H of the curve is $H(C) = \max \left\{ |c_k|^{2g(2g+1)/k} \right\}_{2 \le k \le 2g+1}$.
  - The discriminant and height extend those for elliptic curves. The height is useful because it gives a way to order the hyperelliptic curves, since there are only finitely many curves with $H(C) < X$ for any X.

3 The 2-Selmer Group

- <u>Definition</u>: The 2-Selmer group $S_2(J)$ of the Jacobian $\mathrm{Jac}(C)$ is a finite subgroup of $H^1(\mathbb{Q}, J[2])$, and is the necessary piece in the exact sequence $0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to S_2(J) \to Ш_J[2] \to 0$.

  - This definition is rather opaque, even if you've seen it before. (Plus, I haven't defined the Tate-Shafarevich group.) I will try to unpack it a little bit.
  - $S_2(J)$ is a finite subgroup of the Galois cohomology group $H^1(\mathbb{Q}, J[2])$, and measures in some sense the failure of the Hasse principle in this setting.
  - In the land of elliptic curves (i.e., the context with which the author is actually familiar), the 2-Selmer group arises in a reasonably natural way. For the general version one needs only replace "elliptic curve" with "Jacobian of an abelian variety" everywhere... probably!

- So say that E is an elliptic curve over K, and suppose that we want to talk about $E(K)/2E(K)$ – say, in order to compute the weak Mordell-Weil group.

  - Also adopt the usual shorthand: fix an algebraic closure $\bar{K}$ of K and let $G(\bar{K}/K)$ be the Galois group $\mathrm{Gal}(\bar{K}/K)$.

- If we let $\phi : E \to E$ be the multiplication-by-2 map, we have an exact sequence of $G(\bar{K}/K)$-modules $0 \to E[2] \to E \overset{\cdot 2}{\to} E \to 0$, so taking Galois cohomology gives the long exact sequence $0 \to E/K[2] \to E(K) \overset{\cdot 2}{\to} E(K) \to H^1(G(\bar{K}/K), E[2]) \to H^1(G(\bar{K}/K), E) \to H^1(G(\bar{K}/K), E) \to \cdots$.

- From this we get the short exact sequence $0 \to E(K)/2E(K) \to H^1(G(\bar{K}/K), E[2]) \to H^1(G(\bar{K}/K), E)[2] \to 0$.
- To try to understand this global picture better, let's look at the local one: if K_v is a completion, then we get a local sequence just like the one above. Then we can glue all of them into a nice commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & E(K)/2E(K) \arrow[r] \arrow[d] & H^1(G(\bar{K}/K), E[2]) \arrow[r] \arrow[d] & H^1(G(\bar{K}/K), E)[2] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v E(K_v)/2E(K_v) \arrow[r] & \prod_v H^1(G_v, E[2]) \arrow[r] & H^1(G_v, E)[2] \arrow[r] & 0
\end{tikzcd}$$

  where G_v is the decomposition group.
- We would like to find the image of $E(K)/2E(K)$ in $H^1(G(\bar{K}/K), E[2])$, which by exactness is equivalent to finding the kernel of $H^1(G(\bar{K}/K), E[2]) \to H^1(G(\bar{K}/K), E)[2]$. This in turn is equivalent to determining whether the appropriate principal homogeneous spaces are trivial – and this is hard, because we're asking whether a curve has a K-rational point, and Diophantine equations are hard to solve.
  - Remark: If E/K is an elliptic curve, a "principal homogeneous space" is a smooth curve C/K along with a simply transitive algebraic group action, defined over K, of E on C. It turns out that such a thing is secretly some twist of E/K, but one which may not actually have any K-rational points. The set of principal homogeneous spaces up to K-isomorphism forms the Weil-Chatelet group $WC(E/K)$ and is isomorphic to the Galois cohomology group $H^1(G(\bar{K}/K), E)$.
- However, if we look downstairs at all of the local questions, finding each local kernel (equivalently, finding whether some curve has a K_v-point) is reducible to a finite computation via Hensel's lemma.
- Thus it would be nice if, say, the global problem reduced to solving the local one. Unfortunately, this is not the case, and the failure of "locally trivial everywhere implies globally trivial" is measured by the 2-Selmer group, which is the kernel of the middle map $H^1(G(\bar{K}/K), E[2]) \to \prod_v H^1(G_v, E[2])$.
  - For completeness, the 2-part of the Tate-Shafarevich group Ш is the kernel of the map on the right.
  - Thus, to get the diagram which I originally drew to define the 2-Selmer group, merely take kernels of the vertical maps.
- So, in short: we care about the 2-Selmer group because it tells us things about the Mordell-Weil group.
- Exercise (for the reader): apply a homomorphism to the above discussion that replaces "elliptic curve" with "Jacobian of a hyperelliptic curve" in the appropriate locations.

4 Arithmetic Invariant Theory and Hyperelliptic Curves

- Let k be a field, G a reductive algebraic group over k, and V a linear representation of G.
  - Recall/Definition: A reductive algebraic group is one whose unipotent radical (i.e., the set of unipotent elements of the radical of G, the radical being the component containing 1 of its maximal normal solvable subgroup) is trivial. Semisimple groups like SL_n are reductive, as are tori and GL_n. The name comes from the fact that linear representations of such groups are completely reducible.
- The classical problem of invariant theory is to give some kind of description of the algebra of G-invariant polynomials with k-coefficients, and relate this to the G-orbits on V.
  - For example, if we take the 3-dimensional adjoint representation of SL_2 via conjugation on the trace-zero 2×2 matrices $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, then the determinant $-a^2 - bc$ is invariant under this action, and in fact this generates the ring of polynomial invariants in this case, if we are doing everything over $\mathbb{C}$. [Note that this is exactly the space of interest that I mentioned above!]
  - Things get more complicated – but also more interesting – in the non-algebraically-closed case. This is what we call "arithmetic invariant theory". There is a precise way of formulating this using nonabelian Galois cohomology, but we will not do this, because nonabelian Galois cohomology is terrifying (at least, for the novice).

- Here is the kind of thing one can prove with these techniques (for a sufficiently well-chosen definition of "one"):
- Theorem (Bhargava-Gross): When all hyperelliptic curves of fixed genus g over $\mathbb{Q}$ having a rational Weierstrass point are ordered by height, the average size of the 2-Selmer groups of their Jacobians is equal to 3.
    - If it is not already clear, a reason one might care about this is: the 2-rank of the 2-Selmer group bounds the rank of the Mordell-Weil group, so this gives us an "average upper bound" for the Mordell-Weil rank. This is extremely interesting.
    - The idea of the proof revolves around "arithmetic invariant theory", as it is so called by Bhargava and Gross (and probably others). The same techniques were used in Bhargava-Shankar to bound the average rank of elliptic curves. There, the idea was to convert the problem into one of studying the orbits of PGL_2 on Sym_4, the space of binary quartics.
    - Over $\mathbb{Q}$, PGL_2 is isomorphic to $SO(W)$ where W is the space of 2×2 matrices of trace zero (with quadratic form equal to the determinant), and the representation of PGL_2 on Sym_4 is essentially given by conjugation.
- The idea is to generalize this to looking at representations of $SO(W)$ for some other well-chosen W, which I will now attempt to talk about. [I will now use n in place of what was the genus g, because now I need g to be an element of a group.]
    - Let W be a bilinear space of rank $2n+1$ over $\mathbb{Q}$, where the matrix of the bilinear form $\langle w, u \rangle$ on $\mathbb{Q}^{2n+1}$ consists of the "anti-diagonal identity matrix" $A = \begin{bmatrix} 0 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 0 \end{bmatrix}$.
    - Let $SO(W)$ be the special orthogonal group of W over $\mathbb{Q}$: the subgroup of $GL(W)$ defined by $\langle gw, gu \rangle = \langle w, u \rangle$ and $\det(g) = +1$.
    - Let V be the representation of $SO(W)$ given by conjugation on the self-adjoint operators $T : W \to W$ of trace zero. With respect to the above basis, T is self-adjoint iff its matrix is symmetric about the "anti-diagonal".
    - The coefficients of the characteristic polynomial $f(x) = \det(xI - T) = x^{2n+1} + c_2 x^{2n-1} + \cdots + c_{2g+1}$ give $2g$ invariant polynomials c_k on V with c_k of degree k, and they generate the ring of $SO(W)$-invariants.
    - Note that this very similar to the thing I wrote down earlier describing hyperelliptic curves. The idea is: a class in the 2-Selmer group of the Jacobian of the hyperelliptic curve C with equation $y^2 = f(x)$ over $\mathbb{Q}$ corresponds to the orbit of $SO(W)(\mathbb{Q})$ on $V(\mathbb{Q})$ having those polynomial invariants.
        - The exact way this arises (which the author freely admits he does not understand at all) is by writing down the pencil of quadrics on $\mathbb{P}^{2n+1}$ generated by $Q(w,z) = \langle w, w \rangle$ and $Q'(w,z) = \langle w, Tw \rangle + z^2$, taking the discriminant locus $\text{disc}(xQ - x'Q')$, and then observing that the Fano variety of maximal linear isotropic subspaces of the base locus is smooth and forms a principal homogeneous space for the Jacobian $J(C)$.
        - Then by considering a natural involution $\tau(w,z) = (w, -z)$, one gets a principal homogeneous space P_T for the 2-torsion subgroup $J[2]$ of the Jacobian, and in fact the isomorphism class of this principal homogeneous space determines the orbit of T.
        - From here one gets an injection from the set of rational orbits of $SO(W)$ on V with characteristic polynomial $f(x)$ to the set of elements in $H^1(\mathbb{Q}, J[2])$.
- Theorem: For C given by $y^2 = f(x)$ where f is monic and separable as above, the the classes in the 2-Selmer group of the Jacobian $J(C)$ over $\mathbb{Q}$correspond bijectively to the orbits of $SO(W)(\mathbb{Q})$ on self-adjoing operators $T : W \to W$ with characteristic polynomial $f(x)$ such that the associated Fano variety F_T has points over $\mathbb{Q}_v$ for all places v.
    - Given this result (which is also hard), in order to get the main result, the problem is reduced to one of characterizing those orbits.
    - This counting is accomplished by constructing a fundamental domain for the action, and then counting the number of integral points in the domain with bounded height and applying some sieving arguments.
- To actually learn what this is all about, read the papers by Bhargava and Gross.