BIRS 2012 – Nils Bruin: 3. Chabauty's Method and Mordell-Weil Sieving

June 16, 2012

3.1 : Geometric interpretation of Thue Equations

We have looked at Thue equations on one hand and rational points on projective curves on the other. As it turns out, Thue equations are closely related to *integral* points on curves. The notion of integral points is rather obvious on affine varieties. For instance, consider the affine curve

$$C' \colon x^2y - xy^2 + 3xy + 1 = 0.$$

The *(rational) integral points* on this curve are the points $(x_0, y_0) \in C'(\mathbb{Q})$ for which $x_0, y_0 \in \mathbb{Z}$.

We can consider the projective closure

$$C \colon X^2Y - XY^2 + 3XYZ + Z^3 = 0,$$

and we have the embedding

$$\begin{array}{ccc} C' & \to & C \\ (x, y) & \mapsto & (x : y : 1) \end{array}$$

Thus, we see that the *integral* points on C' map to points $(X_0 : Y_0 : Z_0)$ that can be represented by $X_0, Y_0, Z_0 \in \mathbb{Z}$ and $Z_0 = 1$ (or more generally, a unit). These are exactly the rational projective points on C that do no reduce to any of the 3 points $(1 : 0 : 0), (0 : 1 : 0), (1 : 1 : 0)$, which are the points where C intersects the *line at infinity* $Z = 0$.

The curve C is a genus 0 curve, as shown by the parametrization

$$\begin{array}{ccc} \mathbb{P}^1 & \to & C \\ (U : V) & \to & (U^3 : V^3 : UV(U - V)). \end{array}$$

Thus, we see that the integral points on C' correspond to solutions to

$$f(U, V) = UV(U - V) = \pm 1 \text{ with } U, V \in \mathbb{Z}.$$

Furthermore, since $C' = C \setminus \{Z = 0\}$, we find that

$$C' \simeq \mathbb{P}^1 \setminus \{UV(U - V) = 0\}.$$

This applies in general: Solving Thue equations is essentially the same as finding the integral points on projective lines minus points (if you do this over rings of integers with non-trivial class groups there are some complications)

3.2 : Embedding in a group variety

Let us consider a degree d Thue equation

$$f(x, y) = c$$

where $f(z, 1) \in \mathbb{Z}[z]$ is monic of degree d in z. Let $L = \mathbb{Q}[\theta] = \mathbb{Q}[z]/(f(z, 1))$ and consider the affine variety J obtained from

$$\mathbb{P}^{d-1} \text{ with coordinates } (z_0 : \cdots : z_{d-1})$$

by removing the hypersurface

$$N_{L/\mathbb{Q}}(z_0 + z_1\theta + \cdots + z_{d-1}\theta^{d-1}) = 0.$$

Then we can induce the structure of an abelian group on J by using the multiplication on $L^\times$, written out with respect to the basis $\{1, \theta, \ldots, \theta^{d-1}\}$ (it is clear you get a group structure on the affine cone over J in $\mathbb{A}^d$ and homogeneity shows that the group law descends to $J \subset \mathbb{P}^{d-1}$ too. We have $J(\mathbb{Q}) \simeq L^\times/\mathbb{Q}^\times$ and $J(\mathbb{Z}) \subset \mathcal{O}_L^\times/\mathbb{Z}^\times$. As we saw in a previous lecture, solving Thue-equations amounts to solving equations of the form

$$\frac{x-\theta y}{\gamma} \in \mathcal{O}_L^\times,$$

which corresponds to finding integral points on a curve $X \subset J$, where γ is an element of norm c.

3.3 Key Ingredient: Dirichlet Unit Theorem yields that $J(\mathbb{Z})$ is a finitely generated abelian group.

3.4 : Reduction and Sieving

As before let p be a prime of good reduction for J. We have the reduction homomorphism $\rho_p\colon J(\mathbb{Z}) \to J(\mathbb{F}_p)$ and write $\Lambda_p = \ker(\rho_p)$, which is a finite index subgroup. From

$$\begin{tikzcd}
X(\mathbb{Z}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Z}) \arrow[d, "\rho_S"] \\
\prod_{p\in S} X(\mathbb{F}_p) \arrow[r, "\iota_S"] & \prod_{p\in S} J(\mathbb{F}_p)
\end{tikzcd}$$

we can compute

$$V_S := \operatorname{im}\iota_S \cap \operatorname{im}\rho_S$$

which consists of a relatively small number of cosets of

$$\Lambda_S := \bigcap_{p\in S} \Lambda_p$$

in which $X(\mathbb{Z})$ must lie.

3.5 Poonen's Heuristic: One expects that for any $B > 1$ one can carefully choose a set S such that $\Lambda_S \subset BJ(\mathbb{Z})$, we have that the image of V_S under $J(\mathbb{Z})/\Lambda_S \to J(\mathbb{Z})/BJ(\mathbb{Z})$ consists of cosets that actually contain a point from $X(\mathbb{Z})$.

The key ingredient here is that X is of dimension strictly less than the dimension of J and that $J(\mathbb{Z})$ is finitely generated, together with the assumptions that the group orders of $J(\mathbb{F}_p)$ and the images of ι_S behave sufficiently as if they were random.

3.6 Corollary: If $X(\mathbb{Z}) = \emptyset$, we expect to be able to prove this.

3.7 : Projective curves

Let us now consider a smooth projective curve X of genus $g \geq 2$. As we have seen, we naturally have an embedding $X \hookrightarrow \underline{\mathrm{Pic}}^1(X)$ and if we have a rational divisor class of degree 1, then the latter is isomorphic to $J = \underline{\mathrm{Pic}}^0(X)$, which is an Abelian variety of dimension g. This J is the *Jacobian* of X, which for curves is also the *Albanese variety* of X.

3.8 Degree 1 divisor classes: Note that if $X(\mathbb{Q}_p)$ is empty for some p then we can use that to prove that X has no rational points and hence determine $X(\mathbb{Q})$. If $X(\mathbb{Q}_p)$ is non-empty for all p then $\underline{\mathrm{Pic}}^1(X)$ has points everywhere locally, so $\underline{\mathrm{Pic}}^1(X)$ is an everywhere locally trivial J-torsor. That means $\underline{\mathrm{Pic}}^1(X)$ represents a class in $Ш(J)$. We will be needing $J(\mathbb{Q})$ soon anyway, and the main method we know to determine $J(\mathbb{Q})$ uses descent and can recognise whether $\underline{\mathrm{Pic}}^1(X)$ is a trivial torsor in the process.

Furthermore, if X has points everywhere locally, then any rational divisor class can actually be represented by a rational divisor. Therefore, from this point on, we assume that we have a degree 1 divisor on X, although not necessarily an effective one, so we are not assuming X has a rational point. This allows us to consider X as a subvariety of J.

3.9 Theorem (Mordell-Weil): $J(\mathbb{Q})$ is finitely generated.

Note that J is projective, so $J(\mathbb{Q}) = J(\mathbb{Z})$ and concepts like reduction work properly. Indeed, for primes of good reduction for X, we have $J(\mathbb{F}_p) = \mathrm{Pic}^0(X/\mathbb{F}_p)$. We write $\Lambda_p \subset J(\mathbb{Q})$ for the kernel of the natural reduction homomorphism $\rho_p\colon J(\mathbb{Z}) \to J(\mathbb{F}_p)$.

3.10 Mordell-Weil Sieving: We expect that for $B > 1$, we can exactly determine the cosets in $J(\mathbb{Q})/BJ(\mathbb{Q})$ that contain rational points from $X(\mathbb{Q})$.

3.11 Experiment: (B.-Stoll 2008) We've been able to decide for all genus 2 curves admitting models

$$y^2 = f_6x^6 + \cdots + f_0 \text{ with } f_0, \ldots, f_6 \in \{-3, \ldots, 3\}$$

if they have rational points using Mordell-Weil sieving.

3.12 : Chabauty's Method (general prime version)

Suppose we have a collection of rational points $\{P_1, \ldots, P_m\} \subset X(\mathbb{Q})$ and $B > 1$ and a prime $p > 2$ of good reduction of X such that

- $BJ(\mathbb{Q}) \subset \Lambda_p \subset J(\mathbb{Q})$
- The points $P_1, \ldots, P_m$ represent the cosets of $BJ(\mathbb{Q})$ that contain $X(\mathbb{Q})$.
- The points $P_1, \ldots, P_m$ have distinct reductions on $X(\mathbb{F}_p)$

(These properties can be relaxed considerably but not in a way that makes them considerably easier to meet and in their current form they remove some technical problems)

We are now interested in a method to prove that each P_i is the only rational point in its fibre of reduction modulo p. As it turns out, we can generalize the idea behind Skolem's method. General theory implies that $\Lambda_p \subset J(\mathbb{Q})$ is a free subgroup of finite index. We assume it is of rank $r < g$. This does not always apply, so this is where our method loses complete generality!

An important part in Skolem's method was the p-adic logarithm. Note that

$$\mathrm{Log}(1 + t_1) = \int_{t=0}^{t_1} \frac{1}{t} dt,$$

one of the key ingredients being that the differential $\frac{1}{t}dt$ has no poles outside $t = 0, \infty$.

On a genus g curve X we can find a g-dimensional space of *regular* differentials on X, say $\langle \omega_1, \ldots, \omega_g \rangle$.

3.13 Example: On a genus 2 curve

$$y^2 = f_6x^6 + \cdots + f_0$$

the space of regular differentials is generated by

$$\omega_1 = \frac{1}{y}dx \text{ and } \omega_2 = \frac{x}{y}dx$$

3.14 Lemma: Let $D \in \Lambda_p$ and $P_0 \in X(\mathbb{Q}_p)$. Then D can be represented by a divisor of the form

$$Q_1 + \cdots + Q_g - gP_0.$$

3.15 Definition: Integration along degree 0 divisors. Let $D = Q_1 + \cdots + Q_g - gP_0$.

$$\int_D \omega_j = \sum_{i=1}^{g} \int_{P_0}^{Q_i} \omega_j$$

3.16 Definition: For P_0 and a good prime p we choose a *good uniformizer* in the following way. We take the reduction $\overline{P}_0 = P_0 \mod p$. We choose a uniformizer $\overline{t}$ at $\overline{P}_0$ (i.e., a function with a multiplicity 1 zero at $\overline{P}_0$). We lift this to a function t at P_0.

3.17 Lemma: If Q reduces to the same point as P_0 modulo p, then $t(Q) \in p\mathbb{Z}_p$. Furthermore, we can expand ω as $\omega = h(t)dt$, where $h(t) \in \mathbb{Q}_p[t]$, convergent on $p\mathbb{Z}_p$. Then

$$\int_{P_0}^{Q} \omega = \int_{t=0}^{t(Q)} h_\omega(t)dt$$

where the latter integral is the formal power series integral.

3.18 Proposition: We have a homomorphism of $\mathbb{Z}_p$-modules

$$\begin{array}{ccc} \Lambda_p \otimes \mathbb{Z}_p & \to & p\mathbb{Z}_p^g \\ D & \mapsto & (\int_D \omega_1, \ldots, \int_D \omega_g) \end{array}$$

3.19 Corollary: If $r < g$ then the image is a module of $\mathbb{Z}_p$-rank strictly smaller than g. Then there is a non-trivial $\mathbb{Z}_p$-linear combination ω of $\omega_1, \ldots, \omega_g$ such that $\int_D \omega = 0$ for all $D \in \Lambda_p$. We say that such a differential *annihilates the Mordell-Weil group*. Such a differential ω does not depend on the choice of base point P_0.

3.20 Proposition: Let $P_0 \in X(\mathbb{Q})$ and let ω be an annihilating differential. Let t be a good uniformizer. If there is a point $Q \in X(\mathbb{Q})$ with $Q \neq P$ but such that Q reduces to the same point modulo P then the power series

$$\int_0^{t_0} h_\omega(z)d(z) \in \mathbb{Q}_p[[t_0]]$$

must have a root $t_0 \in p\mathbb{Z}_p$ with $t_0 \neq 0$. In particular, $h_\omega(z)$ must be zero modulo p, so the reduction of ω modulo p has a zero at the reduction of P_0.

3.21 Corollary: Let ω be an annihilating p-adic differential. Then the only fibers of reduction of X modulo p that can contain more than one rational point are those where the reduction of ω has a zero.

3.22 : What if the Chabauty condition $r < g$ is not met?

Use a finite unramified cover $Y \to X$. The rational points of X are covered by the rational points on finitely many twists of Y, so we can reduce the question to trying to find the rational points on finitely many curves Y. Note that Y will usually be of far larger genus and there is no particular reason why the rank of its Jacobian should be far larger too, so there is a reasonable chance that Y is amenable to the method of Chabauty.

3.23 : Elliptic Chabauty

Determining $J(\mathbb{Q})$ is usually the stumbling block in these computations. One can sometimes get away with computing a smaller part. For instance, if X is a curve over $\mathbb{Q}$ that covers a genus 1 curve over an extension k:

$$\begin{tikzcd} & X \arrow[dl, "\text{defined over } k"'] \arrow[dd, "\text{defined over } \mathbb{Q}"] \\ E \arrow[dr, "\text{defined over } k"'] & \\ & \mathbb{P}^1 \end{tikzcd}$$

then we can map X into the $[k : \mathbb{Q}]$-dimensional abelian variety obtained by taking the Weil restriction of scalars of E with respect to $k/\mathbb{Q}$. The Mordell-Weil group of that variety is naturally isomorphic to $E(k)$, which is relatively easy to work with.

Alternatively, you can compute those points in $E(k)$ that map to $\mathbb{P}^1(\mathbb{Q})$. This is fully implemented in Magma.