Chabauty over Number Fields

Samir Siksek — University of Warwick

K number field

$d = [K : \mathbb{Q}]$

C/K curve of genus $g \geq 2$

J Jacobian of C

r rank of $J(K)$

$Q_0 \in C(K)$ fixed K-rational point

$$\begin{aligned} j : C &\hookrightarrow J \\ Q &\longmapsto [Q - Q_0] \end{aligned}$$ Abel-Jacobi map

<u>Faltings</u> $C(K)$ is finite.

<u>Chabauty's Method</u> Practical method for computing $C(K)$ provided $r \leq g-1$, (and we know $J(K)$).

Other practical methods for computing $C(K)$ are based on some variant of Chabauty, e.g. Elliptic Curve Chabauty (Bruin, Wetherell, Flynn, ...)

<u>Heuristic Idea</u> Assume $K = \mathbb{Q}$. Use J to identify $C \subset J$. Let p be a finite prime. Then

$$C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap J(\mathbb{Q})$$
$$\subseteq C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$$

p-adic closure

$C(\mathbb{Q}_p)$ 1-dim $\mathbb{Q}_p$-submanifold of $J(\mathbb{Q}_p)$

$\overline{J(\mathbb{Q})}$ $\mathbb{Q}_p$ sub-Lie group of dim $\leq r$

$J(\mathbb{Q}_p)$ g-dim $\mathbb{Q}_p$-Lie group

If $r+1 \leq g$ then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.

<u>Coleman 1985</u> Suppose $r \leq g-1$. Let $p > 2g$ rational prime, $\upsilon | p$ place of K of good reduction for C. Then

$$\# C(K) \leq \# C(k_\upsilon) + 2g - 2.$$

<u>In Practice</u> If $r \leq g-1$ then can compute $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ to any required accuracy.

Wetherell Talk at MSRI

11/12/2000 "Chabauty Techniques over Number Fields"

① Chabauty can be adapted so that it probably works if $r \leq d(g-1)$.

② Example $K = \mathbb{Q}(i)$

$$C: y^2 = (9i)x^6 - (24+43i)x^4 + (72+47i)x^2 - (48+5i)$$

$r = 2 \qquad g = 2$

Proves $C(\mathbb{Q}(i)) = \{(\pm 1, \pm(2+2i))\}$.

③ Tries to prove an analogue of Coleman's bound for

$$C: y^2 = ax^6 + bx^4 + cx^2 + d$$

provided $r \leq d(g-1)$

Heuristic $V = \mathrm{Res}_{K/\mathbb{Q}}\, C \qquad \dim V = d$

$A = \mathrm{Res}_{K/\mathbb{Q}}\, J \qquad \dim A = dg$

$C(K) \cong V(\mathbb{Q}) \qquad J(K) \cong A(\mathbb{Q})$

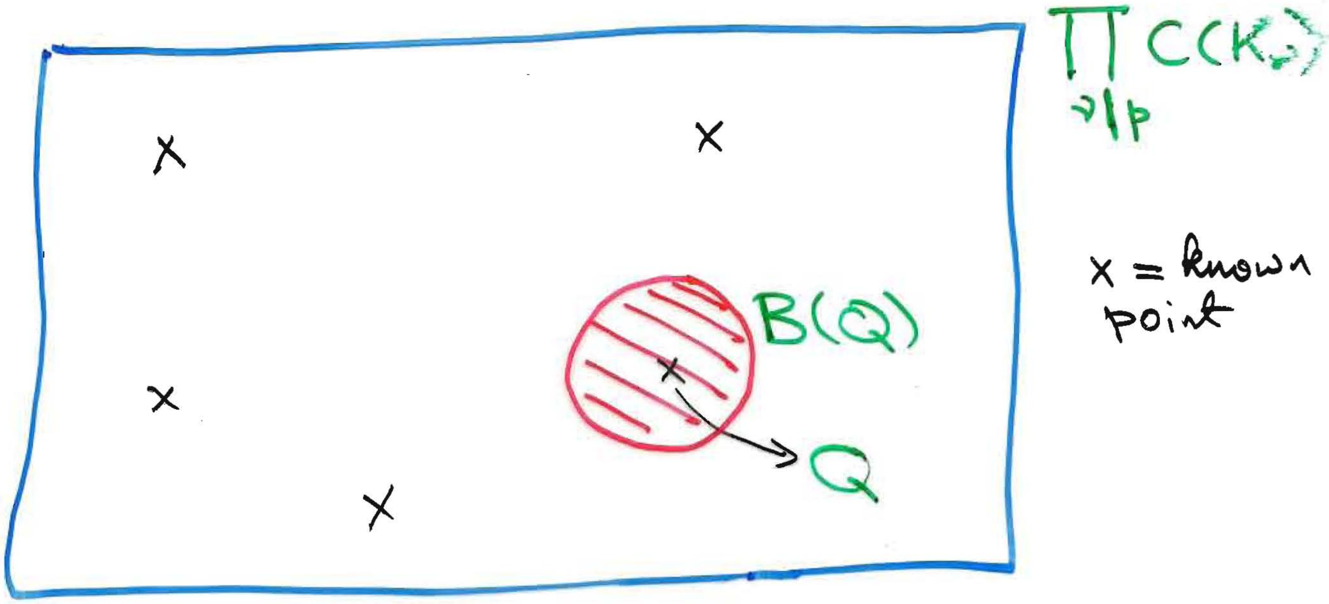
$$C(K) \cong V(\mathbb{Q}) \subseteq \underbrace{V(\mathbb{Q}_p)}_{\dim = d} \cap \underbrace{\overline{A(\mathbb{Q})}}_{\dim \leq r}$$

If $r + d \leq dg$ "expect" then intersection is finite.

Challenge $\mathcal{L} \subseteq C(K)$
← known points

Prove that $C(K) = \mathcal{L}$.

p finite rational prime ≥ 3
unramified in K
C has good reduction at all $v \mid p$.



$$B(Q) = \left\{ (Q_v)_v : \widetilde{Q}_v \equiv \widetilde{Q} \bmod v \ \ \forall v \mid p \right\}$$

To show $C(K) = \mathcal{L}$ it is enough to show (i) $B(Q) \cap C(K) = \{Q\} \quad \forall\, Q \in \mathcal{L}$

(ii) "Empty space" outside the $B(Q)$ is really empty.

Integration

global 1-forms

$$\Omega_{C/K_v} \times J(K_v) \longrightarrow K_v$$

$$(\omega, [\Sigma P_i - Q_i]) \longmapsto \sum \int_{Q_i}^{P_i} \omega$$

(i) K_v - linear on left

(ii) $\mathbb{Z}$ - linear on right

(iii) kernel on right $= J(K_v)_{tor}$

Let $Q \in \mathcal{L}$ $\qquad Q' \in B(Q) \cap C(K)$

Objective Show that $Q' = Q$.

Let $D_1, \text{—}, D_r$ basis for $J(K)/_{\text{torsion}}$

Then

$$[Q' - Q] = \sum_{i=1}^{r} n_i D_i \quad (\text{mod torsion})$$

$n_i \in \mathbb{Z}$.

Fix $v \mid p$

π uniformizer for v

$\omega \in \Omega_{\mathcal{C}_v/\mathcal{O}_v}$

$$\int_Q^{Q'} \omega = \sum_{i=1}^{r} n_i \tau_i \qquad \tau_i = \int_{D_i} \omega \qquad n_i \in \mathbb{Z}$$

Can choose $t \in K_v(C)$ such that:

(a) $t(Q) = 0$

(b) $t(\tilde{Q}) \equiv 0 \mod \pi$

(c) $t : \{ R \in C(K_v) : \tilde{R} \equiv \tilde{Q} \mod \pi \} \xrightarrow{\text{bijection}} \pi \mathcal{O}_v$

(d) $R = Q \iff t(R) = 0.$

Let $s = t(Q')$. Then $s \in \pi \mathcal{O}_v$

Enough to show that $s = 0$.

Can write $\omega = (a_0 + a_1 t + a_2 t^2 + \cdots\cdots) \, dt$

$a_i \in \mathcal{O}_v$.

$$\int_Q^{Q'} \omega = \int_{t(Q)=0}^{t(Q')=s} (a_0 + a_1 t + \cdots\cdots) \, dt$$

$$= a_0 s + \frac{a_1}{2} s^2 + \cdots\cdots$$

$$(*) \quad \sum_{i=1}^{r} n_i \tau_i = a_0 s + \frac{a_1 s^2}{2} + \cdots \qquad n_i \in \mathbb{Z}, \quad s \in \pi \mathcal{O}_\nu$$

Let $d_\nu = [K_\nu : \mathbb{Q}_p] = [\mathcal{O}_\nu : \mathbb{Z}_p] = [k_\nu : \mathbb{F}_p]$

$\theta_1, \ldots, \theta_{d_\nu}$ basis for $\mathcal{O}_\nu / \mathbb{Z}_p$

$$s = \sum_{j=1}^{d_\nu} x_{j,\nu} \, \theta_j$$

Know $x_{j,\nu} \in p\mathbb{Z}_p$.
Want to show that $x_{j,\nu} = 0 \quad j = 1, -, d_\nu$

In $(*)$ write a_i, τ_i in terms of $\theta_1, -, \theta_{d_\nu}$ and expand.

Obtain $\underline{d_\nu \text{ equations}}$ of the form

$$(**) \quad \mu_1 n_1 + \cdots + \mu_r n_r = \alpha_1 x_{1,\nu} + \cdots + \alpha_{d_\nu} x_{d_\nu,\nu}$$
$$+ (\text{higher order terms})$$

We used only one $\omega \in \Omega_{\mathcal{C}_\nu/\mathcal{O}_\nu}$ to get d_ν equations. Take an $\mathcal{O}_\nu$-basis $\omega_1, -, \omega_g$, get $g d_\nu$ equations of the form $(**)$.

Vary $\nu | p$. Recall $d = [K:\mathbb{Q}] = \sum_{\nu | p} d_\nu$.

Get <u>$g \cdot d$ equations</u> of the form

$$\mu_1 n_1 + \cdots + \mu_r n_r = \alpha_1 x_1 + \cdots + \alpha_d x_d$$
$$+ \text{(higher order terms)}$$

$x_1, \ldots, x_d$ are $x_{1,\nu_1}, \ldots, x_{d_{\nu_1},\nu_1}, x_{2,\nu_2}, \ldots$

$$\boxed{\begin{array}{l}\text{Know } x_j \in p\mathbb{Z}_p. \\ \text{Want to show that } x_j = 0 \quad j = 1, \ldots, d.\end{array}}$$

Eliminate $n_1, \ldots, n_r$. Get $gd - r$ equations in $x_1, \ldots, x_d$:

$$A \begin{pmatrix} x_1 \\ | \\ x_d \end{pmatrix} = \text{higher order terms}$$

$(dg-r) \times d$ with entries in $\mathbb{Z}_p$

<u>Lemma</u> If $\tilde{A}$ has rank d then $Q' = Q$.

<u>Proof</u> Enough to show $x_j = 0$ $j = 1, \ldots, d$. Suppose otherwise. Let

$$1 \leq m = \min_{j=1,\ldots,d} \operatorname{ord}_p(x_j) < \infty.$$

Then $A\begin{pmatrix} x_1 \\ | \\ x_d \end{pmatrix} \equiv 0 \mod p^{2m}$.

Let $y_j = x_j / p^m \in \mathbb{Z}_p$. Then

$$A\begin{pmatrix} y_1 \\ | \\ y_d \end{pmatrix} \equiv 0 \mod p^m$$

If $\tilde{A}$ has rank d then $y_j \equiv 0 \mod p$

$\therefore$ $x_j \equiv 0 \mod p^{m+1}$. Contradiction. $\square$

Upshot Have a practical criterion for showing $B(Q) \cap C(K) = \{Q\}$.

Note A necessary condition for $\tilde{A}$ to have rank d is

$$dg - r \geq d$$

i.e. $r \leq d(g-1)$.

What to do about "empty space"?

Mordell-Weil sieve Bruin & Elkies, Scharaschkin, Stoll, ...

MW-Sieve is a sieving strategy that yields a <u>very large & smooth</u> integer m such that:

$$\forall\, Q' \in C(K), \quad \exists\, Q \in \mathcal{L}$$

← known points

such that

$$[Q' - Q] \in m\, J(\mathbb{Q}).$$

<u>To finish</u> Choose p so that it satisfies all previous conditions, and

$$m \cdot J(k_\upsilon) = 0 \qquad \forall\, \upsilon \mid p$$

Then $\forall\, Q' \in C(K)$, $\exists\, Q \in \mathcal{L}$

such that

$$[\tilde{Q}' - \tilde{Q}] \in \{0\} \subseteq J(k_\upsilon)$$

$$\therefore\ \tilde{Q}' \equiv \tilde{Q} \bmod \upsilon \qquad \forall\, \upsilon \mid p$$

i.e. $Q' \in B(Q)$

$$\therefore\ Q' = Q.$$

$$\boxed{\text{Know} \quad C(K) = \mathcal{L}.}$$

Application Let $p, q, r \in \mathbb{Z}_{\geq 2}$

$$\underbrace{x^p + y^q = z^r}$$ x, y, z coprime

Fermat - Catalan eqn with signature (p, q, r)

Let $\chi = p^{-1} + q^{-1} + r^{-1}$

$\chi \geq 1$ {completely solved by Beukers, Zagier, Edwards.

$\chi < 1$ A handful of cases have been solved

Wiles & Taylor, Darmon & Merel, Kraus, Bennett, Ellenberg, Bruin, ...

$(2,3,7)$ Poonen, Schaefer & Stoll

$(2,3,8)$, $(2,3,9)$ } Nils Bruin

$x^2 + z^{10} = y^3$ { Sander Dahmen 2008
Using Galois representation and level-lowering

What about $x^2 + y^3 = z^{10}$?

$$(x-z^5)(x+z^5) = (-y)^3$$

One case $\quad x+z^5 = 2u^3 \quad$ u, v odd
$\quad x-z^5 = 4v^3 \quad$ coprime

$$\therefore \quad u^3 - 2v^3 = z^5$$

$\theta = \sqrt[3]{2} \qquad K = \mathbb{Q}(\theta) \qquad \varepsilon = 1-\theta.$ fund unit

$$(u - v\theta)(u^2+uv\theta+v^2\theta^2) = z^5$$

$u - v\theta = \varepsilon^s \alpha^5 \qquad -2 \leq s \leq 2$

$u^2+uv\theta+v^2\theta^2 = \varepsilon^{-s}\beta^5 \qquad \alpha, \beta \in \mathbb{Z}[\theta]$

Use identity:

$$(u-v\theta)^2 + 3(u+v\theta)^2 = 4(u^2+uv\theta+v^2\theta^2)$$

$$\Longrightarrow \quad \varepsilon^{2s}\alpha^{10} + 3(u+v\theta)^2 = 4\varepsilon^{-s}\beta^5$$

Let $\quad X = \dfrac{\beta}{\alpha^2} \qquad Y = \dfrac{3(u+v\theta)}{\alpha^5}$

$C_s : \; Y^2 = 3(4\varepsilon^{-s}X^5 - \varepsilon^{2s}) \qquad$ genus $= 2$
$d = 3$

Chabauty should work if

$$r \leq d(g-1) = 3.$$

Which it always is.

s	$\mathrm{rk}\, J(K)$	$C_s(K)$
-2	1	∞ $(\theta^2+\theta+1,\ \pm(\theta^2+2\theta+1))$
-1	3	∞ $\left(\frac{-\theta^2-2\theta-1}{3},\ \pm\frac{(\theta^2-\theta+1)}{3}\right)$ $(-\theta^2-\theta-1,\ \pm(11\theta^2+13\theta+17))$
0	2	∞ $\left(\frac{\theta^2+2\theta+1}{3},\ \pm\frac{(10\theta^2+8\theta+13)}{3}\right)$ $(1,\ \pm 3)$
1	3	∞ $(-\theta^2-\theta-1,\ \pm(40\theta^2+53\theta+67))$ $(-1,\ \pm(3\theta+3))$
2	0	∞

Theorem The only solution to $x^2+y^3=z^{10}$ in coprime integers x, y, z are $(\pm 3, -2, \pm 1)$, $(\pm 1, 0, \pm 1)$, $(\pm 1, -1, 0)$, $(0, 1, \pm 1)$.