8-DESCENT ON ELLIPTIC CURVES

TOM FISHER

Example 1. (Stoll 2002) The rank 1 elliptic curve $y^2 = x^3 + 7823$ has a 4-covering

$$C_4 = \left\{ \begin{array}{rcl} 2x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3^2 - 2x_4^2 & = & 0 \\ x_1^2 + x_1x_3 - x_1x_4 + 2x_2^2 - x_2x_3 + 2x_2x_4 - x_3^2 - x_3x_4 + x_4^2 & = & 0 \end{array} \right\} \subset \mathbb{P}^3.$$

Searching for rational points we find

$$(116 : 207 : 474 : -332) \in C_4(\mathbb{Q}).$$

This point maps to a generator $(r/t^2, s/t^3)$ for $E(\mathbb{Q})$, where

$$\begin{array}{rcl} t & = & 11981673410095561 \\ r & = & 22635821433214215021002092335177777 \\ s & = & 1863981525846233056248375514855967700281447766557 56. \end{array}$$

This is a point of canonical height $77.617\ldots$.

	$n=2$	$n=4$	$n=8$
Equations for C_n	Cassels	Siksek	Stamminger
Minimisation	Birch, Swinnerton-Dyer	Womack	
Reduction	Birch, Swinnerton-Dyer	Stoll	(This talk)
Point search	Elkies, Stahlke, Stoll	p-adic Elkies, Watkins	p-adic Elkies, Watkins

Suppose that $C_n \subset \mathbb{P}^{n-1}$ is a genus 1 normal curve. Let $E = \operatorname{Jac} C_n$. Then C_n is a torsor under E. The action of $E[n]$ on C_n extends to an action of $E[n]$ on $\mathbb{P}^{n-1}$. Over $\mathbb{C}$, we can choose coordinates such that generators of $E[n]$ act on $\mathbb{P}^{n-1}$ by the matrices

$$\begin{pmatrix} 1 & & & \\ & \zeta & & \\ & & \ddots & \\ & & & \zeta^{n-1} \end{pmatrix}, \quad \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix}$$

where $\zeta = e^{2\pi i/n}$.

Idea of reduction: Make a choice of coordinates such the action of n-torsion is given by matrices close to those above.

The Heisenberg group H_n is defined by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_n & \longrightarrow & H_n & \longrightarrow & E[n] & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \rho} & & \downarrow & & \\ 0 & \longrightarrow & \mu_n & \longrightarrow & \mathrm{SL}_n & \longrightarrow & \mathrm{PGL}_n & \longrightarrow & 0. \end{array}$$

Date: July 22, 2007.

Then $\rho\colon H_n \to \mathrm{GL}_n$ is an irreducible n-dimensional representation of H_n. By the Weyl unitary trick there is a unique H_n-invariant inner product $\langle\ ,\ \rangle$ on $\mathbb{C}^n$. This is the inner product we use for reduction.

Problem: Compute $\langle\ ,\ \rangle$.

Suppose we have locally soluble coverings $C_4 \to C_2 \to E$, where C_4 is $Q_1 = Q_2 = 0$ in $\mathbb{P}^3$, and C_2 is $y^2 = g(x)$ mapping to $\mathbb{P}^1$. Each Q_i corresponds to a symmetric 4×4 matrix A_i, and $g(x) = \det(xA_1 + A_2)$.

The map $C_4 \to \mathbb{P}^1$ is given by quadrics T_1, T_2. Let $F = \mathbb{Q}[x]/(g(x)) = \mathbb{Q}(\theta)$. (Assume for this talk that F is a field. The general case is similar.)

$$T_1 - \theta T_2 = \xi z^2 \pmod{I(C_4)}$$

where $\xi \in F^\times$ and $z \in F[x_1, \dots, x_4]$ is a linear form. The form z has conjugates $z_1, \dots, z_4 \in \mathbb{C}[x_1, \dots, x_4]$, and θ has conjugates $\theta_1, \dots, \theta_4$, and ξ has conjugates $\xi_1, \dots, \xi_4$. Then $\langle\ ,\ \rangle$ is determined by

$$|\xi_i|\langle z_i, z_j\rangle = \delta_{ij}|g'(\theta_i)|^{1/2}. \tag{1}$$

Eight-descent (Stamminger): Let $Q_\theta = \theta Q_1 + Q_2$. This is the equation of a (cone over a) conic. By an explicit form of the Hasse principle we can find an F-rational point on this conic. Let $L \in F[x_1, \dots, x_4]$ be a linear form defining the tangent to the cone at this point.

$$C_4(\mathbb{Q}) \to F^\times/F^{\times 2}\mathbb{Q}^\times$$
$$P \mapsto L(P)$$

Then $\operatorname{im} C_4(\mathbb{Q}) \subset S \subset F^\times/F^{\times 2}\mathbb{Q}^\times$, where S is a finite set computed by Stamminger.

Problem: Given $\xi \in F^\times$, representing an element of S, compute equations for a 2-covering of C_4.

Solution 1: Write $L = \xi z^2$ as

$$L(x_1, \dots, x_4) = (\xi_0 + \xi_1\theta + \xi_2\theta^2 + \xi_3\theta^3)(z_0 + z_1\theta + z_2\theta^2 + z_3\theta^3)^2,$$

expand to get four equations, each of which equates a linear form in the x_i with a quadratic form in z_0, z_1, z_2, z_3. Linear algebra expresses each x_i as a quadratic form in z_0, z_1, z_2, z_3. Substitute into Q_1 and Q_2 to get two quartics in z_0, z_1, z_2, z_3. These define the union of two 8-coverings in $\mathbb{P}^3$, say $C_8^+ \cup C_8^- \subset \mathbb{P}^3$. But we would like equations defining these 8-coverings individually. Here the norm conditions come in. Let $L_1, \dots, L_4$ be the conjugates of L. Then $\prod_{i=1}^4 L_i = cQ_3^2 \pmod{I(C_4)}$ for some $c \in \mathbb{Q}^\times$ and $Q_3 \in \mathbb{Q}[x_1, \dots, x_4]$ quadratic. From $L = \xi z^2$, we have $N(\xi)N(z)^2 = \prod_{i=1}^4 L_i = cQ_3^2$. Since $\xi \in S$, without loss of generality $N(\xi) = c$. We get $N(z) = \pm Q_3$. This gives a third quartic.

But a genus one normal curve $C_8 \subset \mathbb{P}^7$ of degree 8 is defined by 20 quadrics in 8 variables.

Solution 2: Parametrise the conic! $Q_\theta = \mathrm{const}(LL' - M^2)$ where L, L', M are linear forms. Write $L = \xi z^2$ and $L' = \xi(z')^2$ and $M = \xi z z'$. Get 12 equations equating a linear form in $x_1, \dots, x_4$ with a quadratic form in $z_1, \dots, z_4$; this leads to 8 quadrics in $z_0, \dots, z_3, z_0', \dots, z_3'$. It turns out that using the norm condition we can get a further 12 quadrics.

We have found a formula analogous to (1) defining the reduction inner product on the 8-covering, relative to the basis $z_0, \dots, z_3, z_0', \dots, z_3'$.

Using these methods, we found a 2-covering of the curve C_4 in Example 1. On this 8-covering of E we found the rational point

$$(0:0:0:0:0:0:0:1).$$

Example 2. (from the Stein-Watkins database) Let E be the rank 2 elliptic curve

$$y^2 + xy + y = x^3 - 3961560x - 3035251137$$

of prime conductor $N_E = 3801444643$. We find $E(\mathbb{Q}) = \langle P_1, P_2 \rangle$ where

$$P_1 = (-10343/9, 15502/27)$$

has canonical height $2.946\ldots$. To find the second generator we first compute the everywhere locally soluble 4-coverings of E. One of these is

$$C_4 = \left\{ \begin{array}{rcl} x_1x_2 + x_1x_4 + x_2^2 + 3x_2x_3 - 7x_2x_4 + x_3^2 - 2x_3x_4 + x_4^2 & = & 0 \\ 6x_1^2 - x_1x_2 + 2x_1x_3 + 4x_1x_4 - 6x_2x_3 + 4x_3^2 + 15x_3x_4 + 9x_4^2 & = & 0 \end{array} \right\} \subset \mathbb{P}^3.$$

We then computed a 2-covering $C_8 \to C_4$, given by equations $q_1, \ldots q_{20}$ where *e.g.*

$$\begin{array}{rcl} q_1 & = & -x_1^2 - x_1x_4 + 2x_1x_5 - x_1x_6 + x_1x_7 - x_1x_8 - x_2x_4 - x_2x_7 + x_2x_8 + x_3x_7 - x_4x_5 \\ & & +x_4x_6 + x_4x_7 - 2x_4x_8 - x_5^2 + x_5x_6 - x_5x_7 - x_5x_8 - x_6x_7 - x_7x_8 - x_8^2. \end{array}$$

Magma's `PointSearch` function finds a point on C_8:

$$(1271949 : 796042 : 358611 : -1843491 : 513534 : 2531537 : -2330994 : -1142028)$$

which then maps down to a point on C_4:

$$(6208516310474059 : -59514597662857514 : -9255924243407388 : -11423017679615138).$$

This in turn maps down to a point $(r/t^2, s/t^3)$ on E where

$$\begin{array}{rcl} t & = & 57204436729631275386786939121147787660092078210368817\backslash \\ & & 6713689179795703 \\ r & = & 10919607812201754697433435297074399487856433325041687\backslash \\ & & 77513308874330935296419878516832700736490562061911804\backslash \\ & & 1367649330569338668462349885915896 17 \\ s & = & -27377971829284059683039474561467462839030905785481 58\backslash \\ & & 61014680910657479930315094343194702609558488223853230\backslash \\ & & 08062298231051955202642360966377771000745512359951954\backslash \\ & & 68495932769359879847797588744588934431428635199899 7810. \end{array}$$

This is a point of canonical height 325.048, and is independent of P_1. (We earlier found this second generator using 12-descent, but using 8-descent is much quicker.)