RATIONAL POINTS ON CONICS AND GENERALIZATIONS

DENIS SIMON

1. Overview

There are several methods for finding a rational point on a conic over the rational numbers or a number field. All of them are located somewhere between the two extremes of looking at the equation of the conic either as a norm equation or as a quadratic equation in three variables. The following table summarizes various methods, their positions in this continuum and also their respective merits regarding description, speed and usability over general number fields.

norm equation $\to$ multipl. $\to$ arithm. of #fields	easy	bad	good
Legendre (improved by Cremona) (Fieker)			
Cochrane–Mitchell	to describe	speed	#fields
Ivanyos–Szanto and Simon			
quadratic equation $\to$ lattices and reduction	hard	good	bad

2. Norm equation

Let $q(X,Y,Z)=0$ be the equation of the conic. We diagonalize it to obtain an equation of the form

$$X^2 - a\,Y^2 = b\,Z^2\,.$$

Solving it is equivalent to solving $N_{K(\sqrt{a})/K}(*)=b$.

Consider b as an S-unit for a suitable finite set S of places of K.

Is b the norm of a S-unit? No in general, but Yes if the 2-part of the S-class group $\mathrm{Cl}_{2,S}(K(\sqrt{a}))$ is trivial.

Can we use genus theory to compute $\mathrm{Cl}_{2,S}(K(\sqrt{a}))$? Here: No.

3. Legendre

To solve the norm equation

$$X^2 - a\,Y^2 = b\,Z^2$$

with $a,b\in\mathbb{Z}$ squarefree, $|a|\le|b|$, we can do the following.

Notes by Sebastian Stamminger, edited by Michael Stoll.

(1) Find a square root x_0 of $a \bmod b$ (need to factor b); we can choose x_0 such that $|x_0| \le |b|/2$.
(2) We have $x_0^2 - a = bb'$ with $|b'| \le |b|/4 + 1 \le |b|$.
(3) We can reduce to $X^2 - aY^2 = b'Z^2$.
(4) Repeat until we get $X^2 \pm Y^2 = Z^2$.

Improvement:

Solve $X^2 \equiv a\,Y^2 \bmod b$, allowing $Y \neq 1$, with X, Y small.

Set $X = x_0 Y + bX'$ (with $x_0^2 \equiv a \bmod b$ as before), then

$$|(x_0 Y + bX')^2 - aY^2| \le (x_0 Y + bX')^2 + |a| Y^2 .$$

Reduction applied to the 2-dimensional lattice with norm given by the right-hand side leads to

$$X^2 - a\,Y^2 = b'\,Z^2$$

with $|b'| \le \sqrt{\frac{4}{3}}\sqrt{|a|}$.

Over a number field, we can reduce to $X^2 + \epsilon_1 Y^2 = \epsilon_2 Z^2$ for units (or at least fairly small elements) ϵ_1, ϵ_2.

4. Cochrane-Mitchell (Minimization and Reduction)

Let the equation be

$$a\,X^2 + b\,Y^2 + c\,Z^2 = 0$$

with $a, b, c \in \mathbb{Z}$ coprime in pairs and squarefree.

Fixing square roots of $-bc$ mod a etc. and stipulating that a solution gives rise to these square roots, we find that such a solution must belong to a sublattice $\mathcal{L}$ of $\mathbb{Z}^3$ of covolume $|abc|$ or $2|abc|$ (Minimization).

Reduce $|a|\,X^2 + |b|\,Y^2 + |c|\,Z^2$: a short vector gives a solution to the original equation.

But reduction is impossible over number fields.

5. Nondiagonal Equations

The equation can be minimized at all primes p dividing the determinant of q. This results in an equation with determinant 1. Now use LLL (for indefinite quadratic forms): a short vector is a solution

6. Dimension 4

Solve $q(W, X, Y, Z) = 0$, a quadratic equation in four variables.

First a remark on $\mathrm{Cl}_2(\mathbb{Q}\sqrt{D})$.

The elements of $\mathrm{Cl}(\mathbb{Q}\sqrt{D})[2]$ correspond to quadratic forms $aX^2 + bY^2$ where $-ab = D$ (ambiguous forms)

We need to take square roots in $\mathrm{Cl}_2(\mathbb{Q}(\sqrt{D}))$.

To find $\sqrt{aX^2 + bY^2}$, solve $aX^2 + bY^2 = Z^2$ and parametrize the solutions (optimally), leading to quadratic forms $X(s,t)$, $Y(s,t)$, $Z(s,t)$. $Z(s,t)$ is a quadratic form of det $= -D$; it is a square root of $aX^2 + bY^2$ in $\mathrm{Cl}(\mathbb{Q}\sqrt{D})$.

Back to the original question:

Given $q(W, X, Y, Z) = 0$ locally soluble, we know that with respect to a suitable basis, it is given by the matrix

$$Q = \left(\begin{array}{cc|c} 0 & 1 & \multirow{2}{*}{0} \\ 1 & 0 & \\ \hline \multicolumn{2}{c|}{0} & Q_2 \end{array}\right),$$

with Q_2 over $\mathbb{Z}$.

Compute the local invariants of Q_2 from those of $q \sim Q$ and build Q_2' having the same local invariants.

Consider $Q_6 = Q \oplus -Q_2'$. Q_6 can be minimized, leading to Q_6' with $\det Q_6' = -1$. Then $Q_6' = H \oplus H \oplus H$, and such a splitting can be found easily (use indefinite LLL again). From this we obtain a 3-dimensional isotropic subspace of Q_6, which intersects the subspace coming from Q nontrivially. The intersection gives a solution.