Solving S-unit Equations in Sage

Beth Malmskog and Chris Rasmussen

June 16, 2014

Let k be a field of characteristic other than 2 or 3. A Picard curve C/k is a smooth, projective, absolutely irreducible cyclic trigonal curve of genus 3. The required degree 3 morphism $x\colon C \to \mathbb{P}^1$ is Galois, and one always may recover from this map a smooth affine model of the form

$$y^3 = F(x, 1),$$

where $F(X, Z) \in k[X, Z]$ is a binary quartic form. Picard curves are always non-hyperelliptic, and provide the simplest examples of curves of gonality 3. They have been studied for their unusual geometry (cite some other papers) and the remarkable efficiency of arithmetic on the associated Jacobian varieties over finite fields (cite some other papers). In recent work, we enumerated all $\mathbb{Q}$-isomorphism classes of Picard curves $C/\mathbb{Q}$ with good reduction away from 3. This was inspired by work of Nigel Smart. In [4], N. P. Smart enumerated all curves $C/\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, subject to the following constraints:

- C has genus 2,
- C has good reduction away from the prime 2.

As a necessary step in our investigation, we must solve an S-unit equation over a finite collection of fields. We use variations on methods of Smart [3], which employ Baker's theorem on linear forms in logarithms[1], the LLL algorithm for lattice reduction [2], and various sieving methods. Let K be a (fixed) number field, and let S be the set of primes dividing 3. By $\mathscr{O}_S$ we denote the ring of S-integers in K. Let $\boldsymbol{\mu}_K$ denote the set of roots of unity in K, and let $w = \#\boldsymbol{\mu}_K$. We fix a generator $\rho_0 \in \boldsymbol{\mu}_K$ for the roots of unity. The goal of this section is to find all unordered pairs (τ_0, τ_1) which solve the following equation (the so-called "S-unit equation"):

$$\tau_0 + \tau_1 = 1, \qquad \tau_i \in \mathscr{O}_S^\times. \tag{1}$$

The general strategy for solving such a problem is to first fix a basis $\{\rho_i\}_{i=1}^t$ for the torsion-free part of the $\mathbb{Z}$-module $\mathscr{O}_S^\times$. Then the set $\{\rho_i\}_{i=0}^t$ generates all of $\mathscr{O}_{K,S}$, and each solution may be described by the exponents $a_{j,i}$ such that

$$\tau_j = \prod_{i=0}^{t} \rho_i^{a_{j,i}}.$$

Thus, the tuple $(a_{j,0}, a_{j,1}, \ldots, a_{j,r}) \in \mathbb{Z}/w\mathbb{Z} \times \mathbb{Z}^r$ uniquely encodes the value τ_j. The number of solutions to (1) is known to be finite. To construct them explicitly, we proceed in roughly three steps:

1. Compute an explicit bound C_0, for which any solution must satisfy

$$|a_{j,i}| \leq C_0.$$

   As we will see, such a bound is usually much too large to be of any practical use.

2. Apply a LLL-type lattice argument to improve the bound by several orders of magnitude. Although this step is crucial, it alone is not enough to trivialize the problem; when the bound is C_1 and the rank of $\mathscr{O}_S^\times$ is r, the search space has size roughly $(2C_1)^{2r}$, and this is still too large to carry out a brute-force search in practice.

3. Use the arithmetic of potential solutions (such as symmetry arising from Galois action) and an assortment of sieving methods to search for possible solutions efficiently.

In our project, we wrote code to solve S-unit equations where $S_\mathbb{Q} = \{3, \infty\}$ and S is the set of primes lying above $S_\mathbb{Q}$ in a number field K which is unramified outside S and has $|K : Q| \leq 4$. The goal of this Sage Days project is to write general functions to compute the bound C_0 for more general number fields and sets S, reduce the bound using the LLL algorithm, and solve the given S-unit equation.

References

[1] A. Baker and G. Wüstholz. Logarithmic forms and group varieties. *J. Reine Angew. Math.*, 442:19–62, 1993.

[2] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[3] N. P. Smart. The solution of triangularly connected decomposable form equations. *Math. Comp.*, 64(210):819–840, 1995.

[4] N. P. Smart. S-unit equations, binary forms and curves of genus 2. *Proc. London Math. Soc. (3)*, 75(2):271–307, 1997.