S-unit equations and curves of genus 2 with good reduction away from 3

James Rowan

Mentor: Borys Kadets

Project suggested by: Andrew Sutherland

August 3, 2016

Abstract

The Shafarevich conjecture (now a theorem of Faltings) guarantees that for any genus $g \geq 1$, there are only finitely many isomorphism classes of curves over $\mathbb{Q}$ with good reduction outside any given finite set of primes. For hyperelliptic curves, an effective bound is known, but it is too large to enable an explicit enumeration even for single primes. N. P. Smart has produced an explicit list of all genus 2 curves with good reduction outside 2 by transforming the problem into the problem of solving S-unit equations over a specific set of number fields. We adapt these methods to the prime 3 and produce tighter bounds on the number of possible hyperelliptic curves of genus 2 with good reduction outside 3 in a number of cases, subject to the restriction that the curve must have a rational Weierstrass point. We also list a few such curves.

1 Introduction

By a *curve* over a number field K, we will mean a smooth, irreducible algebraic variety of dimension 1 A *hyperelliptic curve* is a double cover of $\mathbb{P}^1$. An elliptic curve is a hyperelliptic curve of genus 1 (and any genus 1 hyperelliptic curve with a rational point is an elliptic curve). All curves of genus 2 are hyperelliptic, but this is not true for higher genus. A genus 2 curve C has six distinguished points over $\overline{K}$, called *Weierstrass points*, corresponding to the ramification points of the double cover $\mathbb{P}^1 \to C$ (or, equivalently, the fixed points of the hyperelliptic involution exchanging sheets of the associated double cover).

The coordinates of the images in $\mathbb{P}^1$ of the Weierstrass points allow us to write down a *Weierstrass model* for a genus 2 curve C, a defining equation of the form

$$y^2 + h(x)y = f(x), \tag{1}$$

where f is a polynomial over K of degree 5 or 6 and h is a polynomial over K of degree at most 3. One can write down explicilty the condition for two Weierstrass models to correspond to isomorphic curves; see [1], Equation (2.1.2).

For a prime p of K, a hyperelliptic curve C is said to have *good reduction* at p if there exists a Weierstrass model for C such that reducing the coefficients of the Weierstrass model modulo p gives a smooth curve; a curve is said to have good reduction outside a finite set S of primes if it has good reduction at each $p \notin S$. A curve with a Weierstrass model whose discriminant is only divisible by rational primes in some set T has good reduction outside T, so showing that a curve has bad reduction at p requires finding a Weierstrass model that is *minimal* with respect to p but still has a factor of p in its discriminant (i.e. has the discriminant with the smallest exponent for p over all models, but still a positive exponent).

For example, the Weierstrass models $y^2 = x^6 - 6x^3 + 3$ has discriminant $2^7 3^{11}$, but the Weierstrass model $y^2 + (x^3 + 1)y = -x^6 - 2x^3$ has discriminant 3^{11}, despite defining an isomorphic curve. Since there is a Weierstrass model wtih discriminant a power of 3, this curve is an example of a genus 2 curve with good reduction outside $\{3\}$.

Lists of elliptic curves with good reduction outside given sets S of primes have been found (see, for example [14] for the case $S = \{2\}$), and in fact such lists can be computed for general S and general number fields [3].

The Shafarevich conjecture (now a theorem of Faltings) shows that for curves of any genus greater than or equal to 1, there are only finitely many isomorphism classes of curves over $\mathbb{Q}$ with good reduction outside a finite set of primes. An effective proof is known for hyperelliptic curves [22], so there are effective bounds on the number of curves of genus 2 with good reduction outside S. These bounds are too high to be useful, though. For curves over $\mathbb{Q}$ and $S = \{3\}$, the effective Shafarevich conjecture gives a bound on the logarithmic Weil height of the Weierstrass model for curves of genus 2 with a rational Weierstrass point of $2^{14400}3^{7380}5^{3600}$, which is completely impractical. The bound for curves without a rational Weierstrass point is even larger; see Section 3 of [22].

For curves with a rational Weierstrass point, Merriman and Smart [13] were able to list all genus 2 curves over $\mathbb{Q}$ with a rational Weierstrass point and good reduction outside 2 using fairly elementary Diophantine techniques. Smart[18] was able to extend this to a list of all genus 2 curves over $\mathbb{Q}$ and good reduction outside 2 by extending an effective finiteness result for binary forms of given discriminant due to Evertse and Győry [5] to give an algorithm for classifying binary forms with roots in given fields and degree at most 6.

An analogous computation was also done by Malmskog and Rasmussen [12] for curves of genus 3 with models of the form $y^3 = f(x)$ with $f(x)$ a quartic (such curves are called *Picard curves*) and good reduction outisde $\{3\}$.

In this paper, we recall the techniques used in the case $S = \{2\}$ and adapt them to study the problem of finding all isomorphism classes of curves of genus 2 over $\mathbb{Q}$ with good reduction outside $S = \{3\}$. Section 2 discusses the relationships between the Weierstrass models for a curve and the places it has bad reduction, transforming the problem into one of enumerating polynomials (or, equivalently, binary forms) with prescribed discriminant and roots over certain fields. Section 3 gives a method for enumerating some of the desired polynomials by transforming the problem into S-unit equations over number fields. Section 4 gives an outline of an algorithm for solving S-unit equations, which is the central step both in the method described in Section 3 and in the more general method of [18]. Finally, Section 5 gives a (very incomplete) table of non-isomorphic curves of genus 2 with good reduction outside 3.

2 Geometric preliminaries

We will consider only Weierstrass models all of whose coefficients are in $\mathbb{Q}$; such a model exists for any curve defined over $\mathbb{Q}$. To enumerate isomorphism classes of curves, we will enumerate equivalence classes of Weierstrass models. We now lay out the restrictions placed on Weierstrass models of curves with prescribed reduction.

Proposition 1. *Let S be a finite set of rational primes, and let C be a curve of genus 2 over $\mathbb{Q}$ having good reduction outside S. The field extension $K_{wei}/\mathbb{Q}$ containing all the Weierstrass points of C is an algebraic extension of degree at most 6! which is unramified away from $S \cup \{2\}$.*

Proof. See [15], Proposition 2. □

The Weierstrass points are permuted by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so any individual Weierstrass point lies in a (not necessarily Galois) algebraic extension of $\mathbb{Q}$ of degree at most 6; the field K_{wei} may be isomorphic as a field extension of $\mathbb{Q}$ to a series of extensions whose total degree is greater at most 6!. For example, the curve with Weierstrsas model $y^2 = (x^2 - 5)(x^2 - 3)(x^2 - 2)$ has all of its Weierstrass points over one of the three quadratic extensions $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{2})$, its corresponding field $K_{wei} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is of degree 8 over $\mathbb{Q}$.

There are several hundred fields of degree at most 6 unramified away from $\{2, 3\}$, so as a proof of concept we consider only those curves of genus 2 whose

Weierstrass points lie over fields in the family $\mathcal{F}$ of fields where 3 is the only rational prime that ramifies. The main impediment to finding all curves of genus 2 with good reduction away from 3 is practical—the lack of an implementation of an S-unit equation solver for general number fields—and not theoretical.

Corollary 1. *If C is a genus 2 curve over $\mathbb{Q}$ with good reduction outside $S = \{3\}$ whose Weierstrass points lie over fields in the family $\mathcal{F}$ where 3 is the only prime that ramifies, all of the Weierstrass points of C lie over either $\mathbb{Q}$ or one of the algebraic extensions of $\mathbb{Q}$ given by adjoining a root of one of the following polynomials:*

$$x^2 - x + 1, \quad x^3 - 3, \quad x^3 - 3x - 1, \quad x^6 - x^3 + 1, \quad x^6 + 3, \quad x^6 - 3x^3 + 3. \tag{2}$$

Proof. Proposition 1 states that the field K_{wei} containing the Weierstrass points of C is an extension of $\mathbb{Q}$ of degree at most 6 and unramified away from $\{2, 3\}$. Restricting our attention to just the fields in $\mathcal{F}$, a database of number fields ramified only at prescribed primes is given by [9]; their database is proven correct for the cases we need to check. Testing fields with all the possible degrees, we find that the desired fieds are precisely the fields with minimal polynomials given in Equation 2. □

We now convert the problem of finding curves of good reduction outside 3 into a "diophantine" problem by considering polynomial models for curves of genus 2. The following result, a rephrasing of [13], Theorem 4, provides this link:

Proposition 2. *Let C be a curve of genus 2 defined over $\mathbb{Q}$, and let K_{wei} be the extension of $\mathbb{Q}$ over which the Weierstrass points of C are defined. Let S be a finite set of primes lying above the all the rational primes at which C does not have good reduction, all the primes of K_{wei} lying above the rational prime 2, and such that the ring of S-integers, $\mathcal{O}_S$, is a principal ideal domain.*

Then there exist S-integers a_1, a_2, a_3, a_4, a_5, and a_6 such that C has a Weierstrass model.

$$f(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2 + a_5x + a_6 \tag{3}$$

and such that $\mathrm{disc}(f)$*, the discriminant of f, is an S-unit.*

Suppose that C has a rational Weierstrass point P. Then there exist S-integers a_1, a_2, a_3, a_4, and a_5 such that C has a plane model

$$f(x) = x^5 + a_1x^4 + a - 2x^3 + a_3x^2 + a_4x + a_5 \tag{4}$$

and such that $\mathrm{disc}(f)$ *is an S-unit. The Weierstrass point P corresponds to the unique point at infinity on this model.*

Further, suppose that the curve has another rational Weierstrass point, Q, distinct from P. Then the equation 4 for the model can be chosen so that $a_5 = 0$ and such that the Weierstrass point Q has coordinates $(0, 0)$. In this case the coefficient a_4 is also an S-unit.

Finding all curves of genus 2 defined over $\mathbb{Q}$ with good reduction outside $\{3\}$, Weierstrass points in a given K_{wei}, and at least one rational Weierstrass point amounts to finding all monic quintic polynomials with roots in K_{wei} whose coefficients are in $\mathbb{Z}[1/2, 1/3]$ with discriminant of the form $\pm 2^a 3^b$ for nonnegative integers a and b. Similarly, finding all curves of genus 2 defined over $\mathbb{Q}$ with good reduction outside $\{3\}$ and Weierstrass points in a given K_{wei} without a rational Weierstrass point amounts to finding all monic sextic polynomials with roots in K_{wei} whose coefficients are in $\mathbb{Z}[1/2, 1/3]$ with discriminant of the form $\pm 2^a 3^b$ for nonnegative integers a and b.

We cannot require that the curves have discriminant which is purely of the form $\pm 3^b$ because the process of completeting the square used to transform a general Weierstrass model into the form 3 cannot be done in characteristic 2. The Weierstrass models we will find of the form 3 are minimal for primes outside $\{2, 3\}$ in the sense that their discriminants have minimal valuations for (i.e. 0) for those primes, but Proposition 2 does not minimize the valuation at 2. An example of such a model that is not minimal at $p = 2$ was given in the introduction.

A complete characterization of possible curves of genus 2 with good reduction at 2 is available [21]; the computer algebra system MAGMA [2] has a function for p-minimal Weierstrass models that correctly handles the case of $p = 2$. Since the above technique finds all curves with good reduction outside $\{2, 3\}$ which might have good reduction at 2, this enables us to filter our list of polynomials with discriminant $\pm 2^a 3^b$ to find the curves with good reduction at 3 alone.

We now fix some notation, following that of [18]. Let α denote a root of $x^2 - x + 1$, β a root of $x^3 - 3$, and γ a root of $x^3 - 3x - 1$. Let θ_1, θ_2, and θ_3 denote roots of the irreducible sextics $x^6 - x^3 + 1$, $x^6 + 3$, and $x^6 - 3x^3 + 3$, respectively.

Let $K_1 = \mathbb{Q}(\alpha)$, $K_2 = \mathbb{Q}(\beta)$, and $K_3 = \mathbb{Q}(\beta)$, and let L_1, L_2, and L_3 denote $\mathbb{Q}(\theta_1)$, $\mathbb{Q}(\theta_2)$, and $\mathbb{Q}(\theta_3)$, respectively.

For a binary form $F(X, Z)$ over $\mathbb{Q}$ which factors into irreducible polynomials as

$$F(X, Z) = F_1(X, Z) \cdots F_m(X, Z),$$

define its *field system* $(M_1, \ldots, M_m)$ to be the sequence of fields $M_i = \mathbb{Q}(\alpha_i)$ for which $F(\alpha_i, 1) = 0$ (when $F_j = Z$, set $M_j = \mathbb{Q}$). For example, the field system of

$$F(X, Z) = X(X^2 - 3XZ + 3Z^2)(X^3 - 3X^2Z + 3XZ^2 - 4Z^3)$$

is $(\mathbb{Q}, K_1, K_2)$. For a polynomial $f(x)$ (or a curve with model $y^2 = f(x)$) which factors into irreducible factors as

$$f(x) = f_1(x) \cdots f_m(x)$$

over $\mathbb{Q}[x]$, define the field system of f analogously.

We can thus Corollary 1 and Proposition 2 as follows:

Proposition 3. *If C is a genus 2 curve over $\mathbb{Q}$ with good reduction outside $S = \{3\}$ and $K_{wei} \in \mathcal{F}$, then it has a Weierstrass model of the form $y^2 = f(x)$,*

where $\mathrm{disc}(f) = \pm 2^a, 3^b$ *for nonnegative integers* a *and* b *and* f *has one of the field systems in the following table:*

Number of rational Weierstrass points	Field system
6	$(\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q})$
4	$(\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_1)$
3	$(\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_2)$
3	$(\mathbb{Q}, \mathbb{Q}, \mathbb{Q}, K_3)$
2	$(\mathbb{Q}, \mathbb{Q}, K_1, K_1)$
1	$(\mathbb{Q}, K_1, K_2)$
1	$(\mathbb{Q}, K_1, K_3)$
0	(K_1, K_1, K_1)
0	(K_2, K_2)
0	(K_3, K_3)
0	(K_2, K_3)
0	(L_1)
0	(L_2)
0	(L_3)

3 Triangularly-connected decomposable form equations

We seek to find all polynomials of degree 5 or 6 with discriminant of the form $\pm 2^a 3^b$ and field system one of those given in Proposition 3.

The field system $(\mathbb{Q}, K_1, K_3)$ was handled by N. P. Smart in [17]. By testing the 40 possible polynomials from the final table of that paper for good reduction at 2, we find no examples of curves with good reduction outside 3.

We will focus in the following on the case of the field system $(\mathbb{Q}, K_1, K_2)$, following the plan of [17], Section 9. This example illustrates the general technique for any field system of the form $(\mathbb{Q}, \mathbb{Q}(\rho_1), \mathbb{Q}(\rho_2))$ where $\mathbb{Q}(\rho_1)$ is a quadratic extension of $\mathbb{Q}$, $\mathbb{Q}(\rho_2)$ is a cubic extension of $\mathbb{Q}$, and $\mathbb{Q}(\rho_1, \rho_2)$ is Galois. Computations were done using the Sage computer algebra system [4].

Fix $S = \{2, 3\}$. We will work over the field $K = L_2 = \mathbb{Q}(\theta_2)$, where $\theta_2^6 + 3 = 0$. The minimal elements α and β of K_1 and K_2 are in L_2 with $\alpha = \theta_2^3$ and $\beta = \theta_2^2$. This field is a Galois extension of $\mathbb{Q}$, with Galois group G isomorphic to S_3. Let $\beta = \beta^{(1)}$, $\beta^{(2)}$, and $\beta^{(3)}$ denote the conjugates of β.

The S-unit group of K is isomorphic to $C_6 \times \mathbb{Z}^6$, with root of unity $\zeta = \frac{1}{2}\theta_1^3 + \frac{1}{2}$, fundamental units $\eta_1 = \frac{1}{2}\theta_2^3 - \theta_2^2 + \theta_2 - \frac{1}{2}$ and $\eta_2 = \frac{1}{2}\theta_2^5 + \frac{1}{2}\theta_2^4 + \frac{1}{2}\theta_2^3 + \frac{1}{2}\theta_2^2 - \frac{1}{2}\theta_2 - \frac{1}{2}$, three primes $\pi_1 = -\frac{1}{2}\theta_2^3 - \theta_2 + \frac{1}{2}$, $\pi_2 = \frac{1}{2}\theta_2^5 + \frac{1}{2}\theta_2^3 + \frac{1}{2}\theta_2^2 + \frac{1}{2}$, and $\pi_3 = \frac{1}{2}\theta_2^3 + \theta_2 + \frac{1}{2}$ lying above 2, and a prime $\pi_4 = -\theta_2$ of ramification index 6 lying above 3.

If $f(x)$ is the right-hand side of a Weierstrass model for a genus 2 curve with

field system $(\mathbb{Q}, K_1, K_2)$, the five roots of f are given by

$$\gamma_1 = a + b\left(\frac{1+\alpha}{2}\right)$$
$$\gamma_2 = a + b\left(\frac{1-\alpha}{2}\right)$$
$$\gamma_{2+i} = c + d\Big(t\beta^{(i)} + v\big(\beta^{(i)}\big)^2\Big),$$

where $1 \leq i \leq 3$ and a, c, t, and v are integers with $(t, v) = 1$ and b and d of the form $\pm 2^\lambda 3^\mu$.

Since $\operatorname{disc}(f) = \pm 2^a 3^b$, we must have that each $\gamma_i - \gamma_j$ with $i \neq j$ must divide $\pm 2^a 3^b$. In particular, $2(\gamma_i - \gamma_{2+j})$ must divide $\pm 2^a 3^b$ for $1 \leq i \leq 2$, $1 \leq j \leq 3$. So for $j = 1, 2, 3$, we have that

$$L_{2j-1} = 2a + b - 2c + b\alpha - 2dt\beta^{(j)} - 2dv\big(\beta^{(j)}\big)^2$$
$$L_{2j} = 2a + b - 2c - b\alpha - 2dt\beta^{(j)} - 2dv\big(\beta^{(j)}\big)^2$$

are both S-units. To simplify notation, let $x_1 = 2a + b - 2c$, $x_2 = b$, $x_3 = -2dt$, and $x_4 = -2dv$. Let $L_7 = 2x_2\alpha$.

Consider the form

$$L(x_1, x_2, x_3, x_4) = \prod_{i=1}^{7} L_i(x_1, x_2, x_3, x_4) \tag{5}$$

For any i, j, k with $1 \leq i < j < k \leq 7$, we can find algebraic integers α_i, α_j, α_k such that

$$\alpha_i L_i + \alpha_j L_j + \alpha_k L_k = 0. \tag{6}$$

Since we can factor L into a product of linear forms all satisfying 6, it is called a *triangularly-connected decomposable form.*

The conditions that b and d are of the form $\pm 2^\lambda 3^\mu$, along with a restriction on the pair (t, v) that is only checked implicitly at the very end (when curves with bad reduction at some prime outside $\{2, 3\}$ are thrown out), ensure that $(\gamma_1 - \gamma_2)^2$ and $(\gamma_3 - \gamma_4)^2(\gamma_4 - \gamma_5)^2(\gamma_5 - \gamma_3)^2$ are S-units, so the equation $\operatorname{disc} f = \pm 2^a 3^b$ can be solved by considering the triangularly-connected decomposable form equation

$$L(x_1, x_2, x_3, x_4) = \pm 2^{e_1} 3^{3_2}, \tag{7}$$

where the x_i are not all 0 and the nonzero x_i are relatively prime. For more on triangularly-connected decomposable forms equations, see [20], Chapter 10.

To solve this equation, we consider the S-unit equation

$$\frac{L_1}{L_7} - \frac{L_2}{L_7} - 1 = 0. \tag{8}$$

Letting σ be the degree 3 generator of G and let τ be the degree 2 generator of G. We have

$$\sigma\left(\beta^{(1)}\right) = \beta^{(3)} \qquad \sigma(\alpha) = \alpha \qquad \tau\left(\beta^{(1)}\right) = \beta^{(1)} \qquad \tau(\alpha) = -\alpha. \tag{9}$$

This means that G acts transitively on $L_1, \ldots, L_6$. In particular, if we can solve the S-unit equation

$$\frac{L_1}{L_7} + \tau\sigma\left(\frac{L_1}{L_7}\right) = 1, \tag{10}$$

we can find the values of $\frac{L_i}{L_7}$ for all $1 \leq i \leq 6$ because a solution of 10 is of the form

$$\frac{L_1}{L_7} = \zeta^{a_0}\eta_1^{a_1}\eta_2^{a_2}\pi_1^{a_3}\pi_2^{a_4}\pi_3^{a_5}\pi_6^{a_7},$$

and the action of G on the generators of the S-unit group of K lets us write the other ratios $\frac{L_i}{L_7}$ explicitly. We can do solve 10 using the methods outlined in Section 4 below, noting that because it is an equation of the form $x+y=1$ where y is completely determined by x, we have half as many exponential variables to deal with.

We know x_2 is of the form $\pm 2^\lambda 3^\mu$, so we have that

$$L_7 = \zeta^{3v+3}(\pi_1\pi_2\pi_3)^{\lambda+1}\pi_4^{6\mu+3} \tag{11}$$

where either $v=0$ or $v=1$. From here, if we can find a bound on L_7, we can find the values of all the L_i that satisfy 7.

Consider the matrix

$$A = \begin{pmatrix} 1 & \alpha & \beta & \beta^2 \\ 1 & \sigma(\alpha) & \sigma(\beta) & \sigma\left(\beta^2\right) \\ 1 & \tau(\alpha) & \tau(\beta) & \tau\left(\beta^2\right) \\ 1 & \sigma\tau(\alpha) & \sigma\tau(\beta) & \sigma\tau\left(\beta^2\right) \end{pmatrix}.$$

By [17], Lemma 7, we have that $|\pm 2^{\lambda+1}3^\mu|^6 \leq N_{K/\mathbb{Q}}(\det(A))| \leq 54^6$. This means that $a' \leq 5$ and $a'' \leq 31$, where a' is the common exponent on π_1, π_2, and π_3 in L_7 and a'' is the exponent on π_4 in L_7.

For each solution $(a_0, a_1, a_2, a_3, a_4, a_5, a_6)$ of 10 and all possible values of a' and a'', we can compute all the forms L_i. We can then symbolically solve the equation

$$\begin{pmatrix} 1 & \beta^{(1)} & \left(\beta^{(1)}\right)^2 \\ 1 & \beta^{(3)} & \left(\beta^{(3)}\right)^2 \\ 1 & \beta^{(2)} & \left(\beta^{(2)}\right)^2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} L_1 - x_2\alpha \\ \sigma\tau(L_1) - x_2\alpha \\ \sigma(L_1) - x_2\alpha \end{pmatrix} \tag{12}$$

and recover the values of x_1, x_3, and x_4 given a value of x_2.

In fact, we can take x_2 to be whatever we want without loss of generality, as multiplying x_2 scales L_1 by the same factor and thus scales x_1, x_3, and x_4 by the same factor as well. Since in the application to finding Weierstrass models of genus 2 curves, two solutions $\vec{x} = (x_1, x_2, x_3, x_4)$ and $\vec{y} = (y_1, y_2, y_3, y_4)$ with $\vec{x} = \lambda\vec{y}$ give isomorphic curves, we can fix x_2 to be some constant to make computations easier.

For each quadruple (x_1, x_2, x_3, x_4) so produced with x_3 and x_4 not both zero (since such curves correspond to curves which have no Weierstrass points in K_2)

and any integer c and $z = \pm 2^{e_1} e^{e_2}$, the curves with Weierstrass points given by

$$\begin{aligned}
\delta_1 &= z(x_1 + x_2\alpha)/2 + c \\
\delta_2 &= z(x_1 - x_2\alpha)/2 + c \\
\delta_3 &= z(-x_3\beta^{(1)} - x_4\beta^{(1)})/2 + c \\
\delta_4 &= z(-x_3\beta^{(2)} - x_4\beta^{(2)})/2 + c \\
\delta_5 &= z(-x_3\beta^{(3)} - x_4\beta^{(3)})/2 + c
\end{aligned}$$

and one Weierstrass point at infinity (corresponding to the rational Weierstrass point) will have have good reduction outside $\{2, 3\}$ and field system $(\mathbb{Q}, K_1, K_2)$. Making a change of variables $x \to x+c$, we can assume without loss of generality that the Weierstrass model is of the form

$$y^2 = \prod_{i=1}^{5} (x - \delta_i). \tag{13}$$

Moreover, a rescaling of the form $x \to 2^{2k}3^{2\ell}x$, $y \to 2^{5k}3^{5\ell}y$ means that all isomorphism classes of such curves can be represented by those with $z \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Applying this procedure to some "small" solutions to the S-unit equation 10 (defined as those where $-3 \leq a_i \leq 3$ for $1 \leq i \leq 6$), we find four curves of good reduction outside $\{2, 3\}$, none of which had good reduction at 2.

From a computational standpoint, the most intensive part of this process is computing the solutions to the S-unit equation 10. Between Sage and MAGMA, practical algorithms exist for all the computational tasks needed along the way (finding S-unit groups, symbolically determining the curves from the S-unit equation solutions, and checking the reduction type of the curves) except for the solution of the S-unit equations. Since there is a practical algorithm for S-unit equations over general number fields due to Wildanger [23] and Smart [19], the above technique should generalize to field systems of the form $(\mathbb{Q}, K, L)$, where $[K : \mathbb{Q}] = 2$ and $[L : Q] = 3$.

Building the triangularly-connected decomposable form 7 depended heavily on the degrees appearing in the field system. A more general approach to classifying binary forms (and hence Weierstrass models for genus 2 curves) by making use of the Galois group of the field extension containing all fields in a field system appears in [18], where the classification of binary forms with given field system is done by solving at most four S-unit equations involving certain cross-ratios.

4 Solution of S-unit equations

We give an outline of an algorithm for solving S-unit equations over number fields; the presentation closely follows that of [6].

Let K be a number field, and let Γ be the finitely-generated multiplicative subgroup of K containing the units of $\mathcal{O}_K$ and all primes of K lying above the

elements of a finite set S of rational primes. Let ζ denote the generator of the torsion subgroup of Γ and let $\xi_1, \ldots, \xi_r$ be the generators of the infinite part. We seek to solve the equation

$$\zeta^{b_{1,0}} \prod_{i=1}^{r} \xi_i^{b_{1,i}} + \zeta^{b_{2,0}} \prod_{i=1}^{r} \xi_i^{b_{2,i}} = 1. \tag{14}$$

Note that in general the two terms can be drawn from different multiplicative subgroups Γ_1 and Γ_2, and that the terms might have coefficients which are algebraic integers in K, but this setting is enough for our purposes.

The general approach is to first find a large effective bound B on the exponents $b_{i,j}$, reduce it using lattice basis reduction techniques, and enumerate the small solutions. The initial bounds can be larger than 10^{40} even for low-degree fields, and the reduced bounds can still be in the thousands, which for equations with four or more exponential variables give too large a search space for a brute-force search.

Let T denote the set of places (i.e. absolute values) of K consisting of all the finite places corresponding to the primes above the rational primes in S as well as all the infinite places (one corresponding to each real embedding $K \to \mathbb{R}$ and one corresponding to each pair of conjugate complex embeddings $K \to \mathbb{C}$). At each phase, we will need to consider each place separately. For the bounding phases, we always take the largest bound of any place in T.

For ease of exposition, we explain each of the steps for the case of an infinite real place v only. Fuller accounts of this algorithm can also be found in [17], [18], [23], and [19].

4.1 Eliminating "large" solutions

While the finiteness of the number of solutions of 14 can be shown by Diophantine approximation techniques alone, Baker's theory of linear forms in logarithms enables us to write an effective bound for the exponents.

We can pick r places $v_1, \ldots, v_r$ of K such that the matrix

$$M = \begin{pmatrix} \log|\xi_{1,1}|_{v_1} & \cdots & \log|\xi_{1,r}|_{v_1} \\ \vdots & \ddots & \vdots \\ \log|\xi_{1,1}|_{v_r} & \cdots & \log|\xi_{1,r}|_{v_r} \end{pmatrix}$$

is invertible and thus that

$$M \begin{pmatrix} b_{1,1} \\ \vdots \\ b_{1,r} \end{pmatrix} = \begin{pmatrix} \log|x_1|_{v_1} \\ \vdots \\ \log|x_1|_{v_r} \end{pmatrix}.$$

This means that

$$B \leq c_1 |\log|x_1|_{v_k}|, \tag{15}$$

where c_1 is the row norm of M^{-1} (the maximal L_1-norm of a row of M^{-1}) and v_k is the place for which $|\log|x_1|_{v_k}| = \max_{v\in S}|\log|x_2|_{v_k}|$.

We note in passing that this constant c_1, which will appear again later, depends on the choice of basis for the group of S-units and the matrix M selected. A basis of S-units that is optimal with respect to c_1 can be computed which can reduce the computation time needed in the final step significantly [8].

We can show that for the place v_l where $|x_1|_{v_l}$ is minimal, $|x_1|_{v_l} \leq \exp(-c_2 B)$ for some positive real number $c_2 < \frac{1}{c_1(s-1)}$, where $s = |T|$. Let $\Lambda = 1 - x_2$. Then we have

$$|\Lambda|_{v_l} = |1 - x_2|_{v_l} = \left|1 - \zeta^{b_{2,0}} \prod_{i=1}^{r} \xi_i^{b_{2,i}}\right|_{v_l} \leq \exp(-c_2 B). \tag{16}$$

If $|1 - x_2| < 0.75$, then

$$\log|x_2| \leq 2|1 - x_2| \leq 2|\lambda|,$$

so that for

$$\Sigma = \log|\zeta^{b_{2,0}}| + \sum_{i=1}^{r} b_{2,i} \log\left|\xi_i^{b_{2,i}}\right|,$$

we have the upper bound

$$|\Sigma| \leq 2|\Lambda| \leq 2\exp(-c_2 B). \tag{17}$$

Since Σ is a linear form in logarithms, we can compute constants H, c_4, c_5, c_6 such that either

$$B \leq \frac{h}{c_4}$$

or

$$|\Sigma| > \exp\left(-c_5 H \log\left(\frac{c_6 B}{H}\right)\right).$$

Applying effective finiteness bounds for linear forms in logarithms as in [5], we are able to find a constant c_7 such that

$$B_0(v_l) = \max\left(\frac{H}{c_4}, c_7\right). \tag{18}$$

Applying these techniques (or their analogues for complex or finite places) to all the possible places v_l (since we don't know a priori which place will have the minimal absolute value for B_1), we get an initial bound B_0.

4.2 Eliminating "medium" solutions

We have inequalities of the form

$$|b_1\phi_1 + \cdots + b_t\phi_t| < c_1' \exp(-c_2' B) \tag{19}$$

for given positive constants c_1' and c_2' (arising from the first step), B at most the bound B_0 derived above, $\phi_1, \ldots, \phi_t$ logarithms of algebraic numbers, and $b_1, \ldots b_t$ rational integers bounded in absolute value by B. Our goal is to reduce the upper bound B_0.

Consider the lattice generated by the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ C\,\mathrm{Re}(\phi_1) & C\,\mathrm{Re}(\phi_2) & \cdots & C\,\mathrm{Re}(\phi_t) \\ C\,\mathrm{Im}(\phi_1) & C\,\mathrm{Im}(\phi_2) & \cdots & C\,\mathrm{Im}(\phi_t) \end{pmatrix} \tag{20}$$

for a large constant C (a good choice is to choose $C \approx B_0^t$).

Since the last two rows are much larger than the other rows of the lattice, by applying the LLL algorithm [11], we expect to be able to find a lattice basis with much smaller norms for the basis vectors. Let $\vec{a}_1$ denote the first vector of this LLL-reduced basis.

Lemma 1 (Gaál and Pohst)**.** *In the setting 19 and $\vec{a}_1$ defined as above, if*

$$||\vec{a}_1|| \geq \sqrt{(t+1)2^{2-1}} B_0,$$

then

$$B \leq \frac{\log C + \log c_1' - \log B_0}{c_2'}.$$

Proof. See [6], Lemma 5.2.1. □

For a relatively small cost in the extent to which B_0 can be reduced at each step, we can round the $C\,\mathrm{Re}(\phi_i)$ and $C\,\mathrm{Im}(\phi_i)$ entries of 20 to the nearest integer and use the integer version of the LLL reduction algorithm to ensure no floating point errors occur. A similar rounding-then-LLL procedure is done in [16], Theorem 2.

Since these bounds for the exponents are still large, we will give a more efficient algorithm for enumerating all solutions with maximal exponent less than our new reduced bound B_R.

Deriving and reducing a bound on the exponents for the S-unit equation 10 over L_2 lets us bound the number of curves of genus 2 with a rational Weierstrass point, field system $(\mathbb{Q}, K_1, K_2)$, and good reduction outside 3 in a tighter way than the bound derived from [22]. Using Sage code by Koutsianas [10] implementing this method, we are able to reduce the bounds on the exponents to $|b_{i,j}| \leq 231345$, so that there are a total of $6 \cdot 231345^6 < 10^{33}$ possible solutions to the S-unit equation. The techniques of Section 3 tell us that each such solution can correspond to at most 8 curves of genus 2 with good reduction away from 3, so there are at most $8 \cdot 10^{33}$ curves of genus 2 with good reduction outside 3 and field system $(\mathbb{Q}, K_1, K_2)$.

By applying this method to the S-unit equations arising from the other allowed field systems and developing a systematic way to map S-unit equation solutions to polynomials, we could produce a bound for the number of curves of genus 2 with good reduction away from 3.

4.3 Enumerating "small" solutions

In cases like the S-unit equation 10 and more generally the S-unit equations arising from the method of [18], we have a linear relationship

$$L\vec{b}_1 = R\vec{b}_2, \tag{21}$$

where L and R are integer matrices and $\vec{b}_1 = (b_{1,0}, \ldots, b_{1,r})$ and $\vec{b}_2 = (b_{2,0}, \ldots, b_{2,r})$. This relationship enables the use of a sieving technique to find additional congruence relations on the exponents (until the search space is small enough to be searched with brute force).

A much faster method is to partition the reduced search space into nice subsets and then enumerate the solutions in those subsets using the Fincke-Pohst algorithm for finding lattice points in an ellipsoid [7].

Define

$$\langle\langle H, S\rangle\rangle = \left\{\alpha \in K | \frac{1}{H} \leq |\alpha|_v \leq H \text{ for all } v \in S\right\}. \tag{22}$$

Let $\mathscr{C}$ be the set of solutions to the S-unit equation, $\mathscr{C}_B$ the set of solutions with maximal exponent at most B, and $\mathscr{C}_B((H)$ the set of solutions with $x_1 \in \langle\langle H, S\rangle\rangle$.

Given our reduced bound B_R from the previous step, we can find a constant H_0 in terms of the $\xi_{1,i}$ such that $\mathscr{C} = \mathscr{C}_{B_R}(H_0)$.

Given an H_k we choose $H_{k+1} < H_k$. In practice, $H_{k+1} = H_k^{1/2}$ often works for large H_k.

Define the sets

$$\mathcal{T}_{1,v}(B_k, H_k, H_{k+1}) = \left\{(x_1, x_2) \in \mathscr{C}_{B_k}(H_k) \middle| |x_1 - 1|_v < \frac{1}{1 + H_{k+1}}\right\}$$

$$\mathcal{T}_{2,v}(B_k, H_k, H_{k+1}) = \left\{(x_1, x_2) \in \mathscr{C}_{B_k}(H_k) \middle| |\frac{1}{x_1} - 1|_v < \frac{1}{1 + H_{k+1}}\right\}$$

$$\mathcal{T}_{3,v}(B_k, H_k, H_{k+1}) = \left\{(x_1, x_2) \in \mathscr{C}_{B_k}(H_k) \middle| |x_2 - 1|_v < \frac{1}{H_{k+1}}, x_2 \in \langle\langle 1 + H_k, S\rangle\rangle\right\}$$

$$\mathcal{T}_{4,v}(B_k, H_k, H_{k+1}) = \left\{(x_1, x_2) \in \mathscr{C}_{B_k}(H_k) \middle| | - \frac{x_2}{x_1} - 1|_v < \frac{1}{H_{k+1}}\frac{x_2}{x_1} \in \langle\langle 1 + H_k, S\rangle\rangle\right\}$$

$$\mathcal{T}_i(B_k, H_k, H_{k+1}) = \bigcup_{v \in S} \mathcal{T}_{i,v}(B_k, H_k, H_{k+1}).$$

At each step of this final enumeration process, we can further reduce our bound B_k as long as we also enumerate the "remaining" solutions in the $\mathcal{T}_i(B_k, H_k, H_{k+1})$, as the following lemma shows.

Lemma 2. *Letting c_1 be the constant from 15 and $B_{k+1} = c_1 \log(H_{k+1} + 1)$, we have*

$$\mathscr{C}_{B_k}(H_k) = \mathscr{C}_{B_{k+1}}(H_{k+1}) \bigcup_{j=1}^{4} \mathcal{T}_j(B_k, H_k, H_{k+1}). \tag{23}$$

Proof. See [6], Lemma 5.3.1. □

In practice, especially for large B_k and H_k, these sets $\mathcal{T}_j(B_k, H_k, H_{k+1})$ are often empty. Since the sets $\mathcal{T}_{j,v}(B_k, H_k, H_{k+1})$ are balls of the form $|u-1|_v < \epsilon$ and where u is expressed as a product of powers of $\xi_{i,k}$, considering balls of the form

$$|\log |u|_v| \leq \log \frac{1}{1-\epsilon} \tag{24}$$

enables us to find the vectors of exponents $\vec{b_i}$. We also are guaranteed that there is some H with

$$\frac{1}{H} \leq |x|_{v_k} \leq H \tag{25}$$

for all places v_k. Considering the matrix M whose entries are $m_{i,k} = \log |\xi_k|_{v_i}$ for $1 \leq i \leq s$ and $v_i \neq v$ and $1 \leq k \leq r$, $m_{i,(r+1)} = 0$ for $1 \leq i \leq s$, $m_{i',k} = \frac{1}{\log 1/(1-\epsilon)} \log |\xi_k|_v$ for the row i' with $v_{i'} = v$, and $m_{s+1,k} = \frac{1}{\cos^{-1}(\sqrt{1-\epsilon})} \operatorname{Arg}(\xi_k)^{(i')}$, where the notation $\xi_k^{(i')}$ denotes the conjugate of ξ_k corresponding to v. Letting $N = \frac{1}{\log H} M$ and using the restrictions 24 and 25, we have that

$$||N\vec{b}|| \leq s + 1 \tag{26}$$

for an integer-valued vector $\vec{b}$ corresponding to a solution u.

Using the Fincke-Pohst algorithm (making use of LLL reduction to speed up the computation), we can efficiently enumerate all the solutions to 26, and thus find the elements of $\mathcal{T}_{j,v}$.

For large triples (B_k, H_k, H_{k+1}), we might run into floating-point errors in employing the Fincke-Pohst algorithm. The techniques of [19], Section 3 enable us to rule out many of the sets $\mathcal{T}_{i,v}(B_k, H_k, H_{k+1})$ without needing to run the Fincke-Pohst algorithm.

On older hardware, Smart was able to solve S-unit equations over octic number fields in minutes using this algorithm, compared to hours and even machine-years using earlier sieving-based techniques. An implementation of this algorithm in a CAS like Sage or Magma would be a helpful direction for future work, as many classes of Diophantine problems can be stated in terms of S-unit equations (see [6], Chapters 9 and 10 for examples).

5 Some curves of genus 2 with good reduction outside $\{3\}$

In the following table, the curves are given by the coefficients of the polynomial $f(x) = a_0x^6 + a_1x^5 + a_2x^4 + a_3x^5 + a_4x^2 + a_5x + a_6$ in a Weierstrass model

$y^2 = f(x)$. Note that the second curve has Weierstrass points over a field not in $\mathcal{F}$.

a_0	a_1	a_2	a_3	a_4	a_5	a_6	Field System
0	-12	21	-22	15	-6	1	$(\mathbb{Q}, K_1, K_2)$
1	0	0	6	0	0	-3	$(\mathbb{Q}(\xi))$, $\xi^6 + 6\xi^3 - 3 = 0$
-3	0	0	6	0	0	9	$(\mathbb{Q}, K_1, K_2)$

Acknowledgments: The project was initially proposed by Andrew Sutherland. The author would like to thank his mentor Borys Kadets for providing useful readings and suggestions, as well as Dr. Slava Gerovitch, Prof. David Jerison and Prof. Ankur Moitra, for organizing the program and providing useful advice on carrying out and presenting mathematical research.

References

[1] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, and D. Yasaki, *A database of genus 2 curves over the rational numbers*, Algorithmic Number Theory 12th International Symposium (ANTS XII), LMS Journal of Computation and Mathematics (to appear), available at `1602.03715`.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).

[3] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312.

[4] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 6.10)*, 2015. `http://www.sagemath.org`.

[5] J.-H. Evertse and K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compositio Math. **79** (1991), no. 2, 169–204.

[6] Jan-Hendrik Evertse, Klmn Gyory, and Kalman Gyory, *Unit equations in diophantine number theory*, Cambridge studies in advanced mathematics, vol. 146, Cambridge University Press, 2015.

[7] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), no. 170, 463–471.

[8] Lajos Hajdu, *Optimal systems of fundamental S-units for LLL-reduction*, Period. Math. Hungar. **59** (2009), no. 1, 53–79.

[9] John W. Jones and David P. Roberts, *A database of number fields*, LMS J. Comput. Math. **17** (2014), no. 1, 595–618.

[10] A. Koutsianas, *Sage code for computing elliptic curves over number fields with good reduction outside s and solving s-unit equations*, Github repository, `https://github.com/akoutsianas/elliptic-curves-with-good-reduction-outside-S` (2016).

[11] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), no. 4, 515–534.

[12] B. Malmskog and C. Rasmussen, *Picard curves over Q with good reduction away from 3*, ArXiv e-prints (January 2016), available at `1407.7892`.

[13] J. R. Merriman and N. P. Smart, *Corrigenda: "Curves of genus* 2 *with good reduction away from* 2 *with a rational Weierstrass point" [Math. Proc. Cambridge Philos. Soc.* **114** *(1993), no. 2, 203–214; (94h:14031)]*, Math. Proc. Cambridge Philos. Soc. **118** (1995), no. 1, 189.

[14] A. P. Ogg, *Abelian curves of* 2*-power conductor*, Proc. Cambridge Philos. Soc. **62** (1966), 143–148.

[15] A. N. Paršin, *Minimal models of curves of genus* 2*, and homomorphisms of abelian varieties defined over a field of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 67–109.

[16] N. P. Smart, *A class of Diophantine equations*, Publ. Math. Debrecen **41** (1992), no. 3-4, 225–229.

[17] ———, *The solution of triangularly connected decomposable form equations*, Math. Comp. **64** (1995), no. 210, 819–840.

[18] ———, *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307.

[19] ———, *Determining the small solutions to S-unit equations*, Math. Comp. **68** (1999), no. 228, 1687–1699.

[20] Nigel P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998.

[21] Michael Stoll, *Readme for genus 2 curves data files*, 2013.

[22] Rafael von Känel, *An effective proof of the hyperelliptic Shafarevich conjecture*, J. Théor. Nombres Bordeaux **26** (2014), no. 2, 507–530.

[23] K. Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J. Number Theory **82** (2000), no. 2, 188–224.