Algebra & Number Theory

Volume 2
2008
No. 8

Integral points on hyperelliptic curves

Yann Bugeaud, Maurice Mignotte, Samir Siksek,
Michael Stoll and Szabolcs Tengely

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 2:8(2008)

Integral points on hyperelliptic curves

Yann Bugeaud, Maurice Mignotte, Samir Siksek,
Michael Stoll and Szabolcs Tengely

Let $C : Y^2 = a_n X^n + \cdots + a_0$ be a hyperelliptic curve with the a_i rational integers, $n \geq 5$, and the polynomial on the right-hand side irreducible. Let J be its Jacobian. We give a completely explicit upper bound for the integral points on the model C, provided we know at least one rational point on C and a Mordell–Weil basis for $J(\mathbb{Q})$. We also explain a powerful refinement of the Mordell–Weil sieve which, combined with the upper bound, is capable of determining all the integral points. Our method is illustrated by determining the integral points on the genus 2 hyperelliptic models $Y^2 - Y = X^5 - X$ and $\binom{Y}{2} = \binom{X}{5}$.

1. Introduction

Consider the hyperelliptic curve with affine model

$$C : \ Y^2 = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \tag{1-1}$$

with $a_0, \ldots, a_n$ rational integers, $a_n \neq 0$, $n \geq 5$, and the polynomial on the right-hand side irreducible. Let $H = \max\{|a_0|, \ldots, |a_n|\}$. In one of the earliest applications of his theory of lower bounds for linear forms in logarithms, Baker [1969] showed that any integral point (X, Y) on this affine model satisfies

$$\max(|X|, |Y|) \leq \exp\exp\exp\big((n^{10n} H)^{n^2}\big).$$

Such bounds have been improved considerably by many authors, including Sprindžuk [1977], Brindza [1984], Schmidt [1992], Poulakis [1991], Bilu [1995], Bugeaud [1997] and Voutier [1995]. Despite the improvements, the bounds remain astronomical and often involve inexplicit constants.

In this paper we explain a new method for explicitly computing the integral points on affine models of hyperelliptic curves (1-1). The method falls into two distinct steps:

MSC2000: primary 11G30; secondary 11J86.

Keywords: curve, integral point, Jacobian, height, Mordell–Weil group, Baker's bound, Mordell–Weil sieve.

(i) We give a completely explicit upper bound for the size of integral solutions of (1-1). This upper bound combines many refinements found in the papers of Voutier, Bugeaud, and others, together with Matveev's bounds [2000] for linear forms in logarithms, and a method for bounding the regulators based on a theorem of Landau [1918].

(ii) The bounds obtained in (i), whilst substantially better than bounds given by earlier authors, are still astronomical. We explain a powerful variant of the Mordell–Weil sieve which, combined with the bound obtained in (i), is capable of showing that the known solutions to (1-1) are the only ones.

Step (i) requires two assumptions:

(a) We assume that we know at least one rational point P_0 on C.

(b) Let J be the Jacobian of C. We assume that a Mordell–Weil basis for $J(\mathbb{Q})$ is known.

For step (ii) we need assumptions (a), (b) and also:

(c) We assume that the canonical height $\hat{h} : J(\mathbb{Q}) \to \mathbb{R}$ is explicitly computable and that we have explicit bounds for the difference

$$\mu_1 \le h(D) - \hat{h}(D) \le \mu_1' \tag{1-2}$$

where h is an appropriately normalized logarithmic height on J that allows us to enumerate points P in $J(\mathbb{Q})$ with $h(P) \le B$ for a given bound B.

Assumptions (a)–(c) deserve a comment or two. For many families of curves of higher genus, practical descent strategies are available for estimating the rank of the Mordell–Weil group; see for example [Cassels and Flynn 1996; Poonen and Schaefer 1997; Schaefer 1995; Stoll 2001]. To provably determine the Mordell–Weil group one however needs bounds for the difference between the logarithmic and canonical heights. For Jacobians of curves of genus 2 such bounds have been determined by Stoll [1999; 2002], building on previous work of Flynn and Smart [1997]. At present, no such bounds have been determined for Jacobians of curves of genus ≥ 3, though work on this is in progress. The assumption about the knowledge of a rational point is a common sense assumption that brings some simplifications to our method, though the method can be modified to cope with the situation where no rational point is known. However, if a search on a curve of genus ≥ 2 reveals no rational points, it is probable that there are none, and the methods of Bruin and Stoll [2008a; 2008b; $\ge$ 2008] are likely to succeed in proving this.

We illustrate the practicality of our approach by proving:

Theorem 1.1. *The only integral solutions to the equation*

$$Y^2 - Y = X^5 - X \tag{1-3}$$

are

$$(X, Y) = (-1, 0),\ (-1, 1),\ (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, -5),\\ (2, 6),\ (3, -15),\ (3, 16),\ (30, -4929),\ (30, 4930).$$

Theorem 1.2. *The only integral solutions to the equation*

$$\binom{Y}{2} = \binom{X}{5} \tag{1-4}$$

are

$$(X, Y) = (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, 0),\ (2, 1),\ (3, 0),\\ (3, 1),\ (4, 0),\ (4, 1),\ (5, -1),\ (5, 2),\ (6, -3),\ (6, 4),\\ (7, -6),\ (7, 7),\ (15, -77),\ (15, 78),\ (19, -152),\ (19, 153).$$

Equations (1-3) and (1-4) are of historical interest and Section 2 gives a brief outline of their history. For now we merely mention that these two equations are the first two problems on a list of 22 unsolved Diophantine problems, compiled by Evertse and Tijdeman [2007] following a recent workshop on Diophantine equations at Leiden.

To appreciate why the innocent-looking (1-3) and (1-4) have resisted previous attempts, let us briefly survey the available methods which apply to hyperelliptic curves and then briefly explain why they fail in these cases. To determine the integral points on the affine model C given by (1-1) there are four available methods:

(I) The first is Chabauty's elegant method which in fact determines all rational points on C in many cases, provided the rank of the Mordell–Weil group of its Jacobian is strictly less than the genus g; see for example [Flynn 1997; Wetherell 1997]. Chabauty's method fails if the rank of the Mordell–Weil group exceeds the genus.

(II) The second method is to use coverings, often combined with a version of Chabauty called *Elliptic Curve Chabauty*. See [Bruin 1999; 2003; Flynn and Wetherell 1999; 2001]. This approach often requires computations of Mordell–Weil groups over number fields (and does fail if the rank of the Mordell–Weil groups is too large).

(III) The third method is to combine Baker's approach through S-units with the LLL algorithm to obtain all the solutions provided that certain relevant unit groups and class groups can be computed; for a modern treatment, see [Bilu and Hanrot 1998] or [Smart 1998, Section XIV.4]. This strategy often fails in practice as the number fields involved have very high degree.

(IV) The fourth approach is to apply Skolem's method to the S-unit equations (see [Smart 1998, Section III.2]). This needs the same expensive information as method (III).

The Jacobians of the curves given by (1-3) and (1-4) respectively have ranks 3 and 6 and so Chabauty's method fails. To employ Elliptic Curve Chabauty would require the computation of Mordell–Weil groups of elliptic curves without rational 2-torsion over number fields of degree 5 (which does not seem practical at present). To apply the S-unit approach (with either LLL or Skolem) requires the computations of the unit groups and class groups of several number fields of degree 40 — a computation that seems completely impractical at present.

Our paper is arranged as follows. Section 2 gives a brief history of (1-3) and (1-4). In Section 3 we show, after appropriate scaling, that an integral point (x, y) satisfies $x - \alpha = \kappa\xi^2$ where α is some fixed algebraic integer, $\xi \in \mathbb{Q}(\alpha)$, and κ is an algebraic integer belonging to a finite computable set. In Section 9 we give bounds for the size of solutions $x \in \mathbb{Z}$ to an equation of the form $x - \alpha = \kappa\xi^2$ where α and κ are fixed algebraic integers. Thus, in effect, we obtain bounds for the size of solutions of the integral points on our affine model (1-1). Sections 4–8 are preparation for Section 9: in particular Section 4 is concerned with heights; Section 5 explains how a theorem of Landau can be used to bound the regulators of number fields; Section 6 collects and refines various results on appropriate choices of systems of fundamental units; Section 7 is devoted to Matveev's bounds for linear forms in logarithms; in Section 8 we use Matveev's bounds and the results of previous sections to prove a bound on the size of solutions of unit equations; in Section 9 we deduce the bounds for x alluded to above from the bounds for solutions of unit equations. Despite our best efforts, the bounds obtained for x are still so large that no naive search up to those bounds is conceivable. Over Sections 10, 11 and 12 we explain how to sieve effectively up to these bounds using the Mordell–Weil group of the Jacobian. In particular, Section 11 gives a powerful refinement of the Mordell–Weil sieve (see [Bruin and Stoll 2008a; Bruin and Stoll $\geq$ 2008]) which we expect to have applications elsewhere. Finally, in Section 13 we apply the method of this paper to prove Theorems 1.1 and 1.2.

2. History of (1-3) and (1-4)

Equation (1-3) is a special case of the family of Diophantine equations

$$Y^p - Y = X^q - X, \qquad 2 \leq p < q. \tag{2-1}$$

This family has previously been studied by Fielder and Alford [1998] and by Mignotte and Pethő [1999]. The (genus 1) case $p = 2$, $q = 3$ was solved by

Mordell [1963] who showed that the only solutions in this case are

$$(X, Y) = (0, 0), (0, 1), (\pm 1, 0), (\pm 1, 1), (2, 3), (2, -2), (6, 15), (6, -14).$$

Fielder and Alford presented the following list of solutions with $X, Y > 1$:

$$(p, q, X, Y) = (2, 3, 2, 3), (2, 3, 6, 15), (2, 5, 2, 6), (2, 5, 3, 16),$$
$$(2, 5, 30, 4930), (2, 7, 5, 280), (2, 13, 2, 91), (3, 7, 3, 13).$$

Mignotte and Pethő proved that for given p and q with $2 \le p < q$, the Diophantine equation (2-1) has only a finite number of integral solutions. Assuming the abc-conjecture, they showed that (2-1) has only finitely many solutions with $X, Y > 1$.

If $p = 2$, $q > 2$ and y is a prime power, then Mignotte and Pethő found all solutions of the equation and these are all in Fielder and Alford's list.

Equation (1-4) is a special case of the Diophantine equation

$$\binom{n}{k} = \binom{m}{l}, \tag{2-2}$$

in unknowns k, l, m, n. This is usually considered with the restrictions $2 \le k \le \frac{n}{2}$, and $2 \le l \le \frac{m}{2}$. The only known solutions (with these restrictions) are

$$\binom{16}{2} = \binom{10}{3}, \ \binom{56}{2} = \binom{22}{3}, \ \binom{120}{2} = \binom{36}{3}, \ \binom{21}{2} = \binom{10}{4},$$
$$\binom{153}{2} = \binom{19}{5}, \ \binom{78}{2} = \binom{15}{5} = \binom{14}{6}, \ \binom{221}{2} = \binom{17}{8},$$
$$\binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3} - 1}{F_{2i}F_{2i+3} + 1} \quad \text{for } i = 1, 2, \ldots,$$

where F_n is the n-th Fibonacci number. It is known that there are no other nontrivial solutions with $\binom{n}{k} \le 10^{30}$ or $n \le 1000$; see [de Weger 1997]. The infinite family of solutions was found by Lind [1968] and Singmaster [1975].

Equation (2-2) has been completely solved for pairs

$$(k, l) = (2, 3), \ (2, 4), \ (2, 6), \ (2, 8), \ (3, 4), \ (3, 6), \ (4, 6).$$

These are the cases when one can easily reduce the equation to the determination of solutions of a number of Thue equations or elliptic Diophantine equations. Avanesov [1966/1967] found all solutions of (2-2) with $(k, l) = (2, 3)$. De Weger [1996] and independently Pintér [1995] solved the equation with $(k, l) = (2, 4)$. The case $(k, l) = (3, 4)$ reduces to the equation

$$Y(Y + 1) = X(X + 1)(X + 2)$$

which was solved by Mordell [1963]. The remaining pairs

$$(2, 6), (2, 8), (3, 6), (4, 6)$$

were treated by Stroeker and de Weger [1999], using linear forms in elliptic logarithms.

There are also some general finiteness results related to (2-2). Kiss [1988] proved that if $k = 2$ and l is a given odd prime, then the equation has only finitely many positive integral solutions. Using Baker's method, Brindza [1991] showed that (2-2) with $k = 2$ and $l \geq 3$ has only finitely many positive integral solutions.

3. Descent

Consider the integral points on the affine model of the hyperelliptic curve (1-1). If the polynomial on the right-hand side is reducible then the obvious factorisation argument reduces the problem of determining the integral points for (1-1) to determining those on simpler hyperelliptic curves, or on genus 1 curves. The integral points on a genus 1 curve can be determined by highly successful algorithms (see for example [Smart 1998; Stroeker and Tzanakis 2003]) based on LLL and David's bound for linear forms in elliptic logarithms.

We therefore suppose henceforth that the polynomial on the right-hand side of (1-1) is irreducible; this is certainly the most difficult case. By appropriate scaling, one transforms the problem of integral points on (1-1) to integral points on a model of the form

$$ay^2 = x^n + b_{n-1}x^{n-1} + \cdots + b_0, \tag{3-1}$$

where a and b_i are integers, with $a \neq 0$. We shall work henceforth with this model of the hyperelliptic curve. Denote the polynomial on the right-hand side by f and let α be a root of f. Then a standard argument shows that

$$x - \alpha = \kappa\xi^2$$

where $\kappa, \xi \in K = \mathbb{Q}(\alpha)$ and κ is an *algebraic integer that comes from a finite computable set*. In this section we suppose that the Mordell–Weil group $J(\mathbb{Q})$ of the curve C is known, and we show how to compute such a set of κ using our knowledge of the Mordell–Weil group $J(\mathbb{Q})$. The method for doing this depends on whether the degree n is odd or even.

3A. ***The odd degree case.*** Each coset of $J(\mathbb{Q})/2J(\mathbb{Q})$ has a coset representative of the form $\sum_{i=1}^{m}(P_i - \infty)$ where the set $\{P_1, \ldots, P_m\}$ is stable under the action of Galois, and where all $y(P_i)$ are nonzero. Now write $x(P_i) = \gamma_i/d_i^2$ where γ_i is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$; moreover if P_i, P_j are conjugate then we may suppose that $d_i = d_j$ and so γ_i, γ_j are conjugate. To such a coset representative of

$J(\mathbb{Q})/2J(\mathbb{Q})$ we associate

$$\kappa = a^{(m \bmod 2)} \prod_{i=1}^{m} (\gamma_i - \alpha d_i^2).$$

Lemma 3.1. *Let $\mathcal{K}$ be a set of κ associated as above to a complete set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$. Then $\mathcal{K}$ is a finite subset of $\mathcal{O}_K$ and if (x, y) is an integral point on the model* (3-1) *then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.*

Proof. This follows trivially from the standard homomorphism

$$\theta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^*/K^{*2}$$

that is given by

$$\theta\left(\sum_{i=1}^{m} (P_i - \infty)\right) = a^m \prod_{i=1}^{m} (x(P_i) - \alpha) \pmod{K^{*2}}$$

for coset representatives $\sum(P_i - \infty)$ with $y(P_i) \neq 0$; see [Stoll 2001, Section 4]. □

3B. ***The even degree case.*** As mentioned in the introduction, we shall assume the existence of at least one rational point P_0. If P_0 is one of the two points at infinity, let $\epsilon_0 = 1$. Otherwise, as f is irreducible, $y(P_0) \neq 0$; write $x(P_0) = \gamma_0/d_0^2$ with $\gamma_0 \in \mathbb{Z}$ and $d_0 \in \mathbb{Z}_{\geq 1}$ and let $\epsilon_0 = \gamma_0 - \alpha d_0^2$.

Each coset of $J(\mathbb{Q})/2J(\mathbb{Q})$ has a coset representative of the form $\sum_{i=1}^{m}(P_i - P_0)$ where the set $\{P_1, \ldots, P_m\}$ is stable under the action of Galois, and where all $y(P_i)$ are nonzero for $i = 1, \ldots, m$. Write $x(P_i) = \gamma_i/d_i^2$ where γ_i is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$; moreover if P_i, P_j are conjugate then we may suppose that $d_i = d_j$ and so γ_i, γ_j are conjugate. To such a coset representative of $J(\mathbb{Q})/2J(\mathbb{Q})$ we associate

$$\epsilon = \epsilon_0^{(m \bmod 2)} \prod_{i=1}^{m} (\gamma_i - \alpha d_i^2).$$

Lemma 3.2. *Let $\mathcal{E}$ be a set of ϵ associated as above to a complete set of coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$. Let Δ be the discriminant of the polynomial f. For each $\epsilon \in \mathcal{E}$, let $\mathcal{B}_\epsilon$ be the set of square-free rational integers supported only by primes dividing $a\Delta \operatorname{Norm}_{K/\mathbb{Q}}(\epsilon)$. Let $\mathcal{K} = \{\epsilon b : \epsilon \in \mathcal{E},\ b \in \mathcal{B}_\epsilon\}$. Then $\mathcal{K}$ is a finite subset of $\mathcal{O}_K$ and if (x, y) is an integral point on the model* (3-1) *then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.*

Proof. In our even degree case, the homomorphism θ takes values in $K^*/\mathbb{Q}^*K^{*2}$. Thus if (x, y) is an integral point on the model (3-1), we have that $(x - \alpha) = \epsilon b\xi^2$

for some $\epsilon \in \mathscr{E}$ and b a square-free rational integer. A standard argument shows that $2 \mid \mathrm{ord}_{\wp}(x-\alpha)$ for all prime ideals $\wp \nmid a\Delta$. Hence, $2 \mid \mathrm{ord}_{\wp}(b)$ for all $\wp \nmid a\Delta\epsilon$. Let $\wp \mid p$ where p is a rational prime not dividing $a\Delta\,\mathrm{Norm}_{K/\mathbb{Q}}(\epsilon)$. Then p is unramified in $K/\mathbb{Q}$ and so $\mathrm{ord}_p(b) = \mathrm{ord}_{\wp}(b) \equiv 0 \pmod 2$. This shows that $b \in \mathscr{B}_\epsilon$ and proves the lemma. □

3C. ***Remarks.*** The following remarks are applicable to both odd and even degree cases.

(i) We point out that we can still obtain a suitable (though larger) set of κ that satisfies the conclusions of Lemmas 3.1 and 3.2, even if we do not know coset representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$, provided we are able to compute the class group and unit group of the number field K; for this see for example [Bruin 1999, Section 2.2].

(ii) We can use local information at small and bad primes to restrict the set $\mathscr{H}$ further, compare [Bruin and Stoll 2008a; 2008b], where this is applied to rational points. In our case, we can restrict the local computations to $x \in \mathbb{Z}_p$ instead of $\mathbb{Q}_p$.

4. Heights

We fix once and for all the following notation.

K	a number field,
$\mathbb{O}_K$	the ring of integers of K,
M_K	the set of all places of K,
M_K^0	the set of non-Archimedean places of K,
M_K^∞	the set of Archimedean places of K,
v	a place of K,
K_v	the completion of K at v,
d_v	the local degree $[K_v : \mathbb{Q}_v]$.

For $v \in M_K$, we let $|\cdot|_v$ be the usual normalized valuation corresponding to v; in particular if v is non-Archimedean and p is the rational prime below v then $|p|_v = p^{-1}$. Thus if L/K is a field extension, and ω a place of L above v then $|\alpha|_\omega = |\alpha|_v$, for all $\alpha \in K$.

Define

$$\|\alpha\|_v = |\alpha|_v^{d_v}.$$

Hence for $\alpha \in K^*$, the product formula states that

$$\prod_{v \in M_K} \|\alpha\|_v = 1.$$

In particular, if v is Archimedean, corresponding to a real or complex embedding σ of K, then

$$|\alpha|_v = |\sigma(\alpha)| \qquad \text{and} \qquad \|\alpha\|_v = \begin{cases} |\sigma(\alpha)| & \text{if } \sigma \text{ is real,} \\ |\sigma(\alpha)|^2 & \text{if } \sigma \text{ is complex.} \end{cases}$$

For $\alpha \in K$, the (absolute) logarithmic height $\mathrm{h}(\alpha)$ is given by

$$\mathrm{h}(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\} = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \max\{1, \|\alpha\|_v\}. \tag{4-1}$$

The absolute logarithmic height of α is independent of the field K containing α.

We shall need the following elementary properties of heights.

Lemma 4.1. *For any nonzero algebraic number α, we have $\mathrm{h}(\alpha^{-1}) = \mathrm{h}(\alpha)$. For algebraic numbers $\alpha_1, \ldots, \alpha_n$, we have*

$$\mathrm{h}(\alpha_1 \alpha_2 \cdots \alpha_n) \le \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n),$$
$$\mathrm{h}(\alpha_1 + \cdots + \alpha_n) \le \log n + \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n).$$

Proof. The lemma is [Silverman 1986, Exercise 8.8]. We do not know of a reference for the proof and so we will indicate briefly the proof of the second (more difficult) inequality. For $v \in M_K$, choose i_v in $\{1, \ldots, n\}$ to satisfy

$$\max\{|\alpha_1|_v, \ldots, |\alpha_n|_v\} = |\alpha_{i_v}|_v.$$

Note that

$$|\alpha_1 + \cdots + \alpha_n|_v \le \epsilon_v |\alpha_{i_v}|_v,$$

where $\epsilon_v = n$ if v is Archimedean or $\epsilon_v = 1$ otherwise. Thus

$$\begin{aligned} \log \max\{1, |\alpha_1 + \cdots + \alpha_n|_v\} &\le \log \epsilon_v + \log \max\{1, |\alpha_{i_v}|_v\} \\ &\le \log \epsilon_v + \sum_{i=1}^{n} \log \max\{1, |\alpha_i|_v\}. \end{aligned}$$

Observe that

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \epsilon_v = \frac{\log n}{[K:\mathbb{Q}]} \sum_{v \in M_K^\infty} d_v = \log n.$$

The desired inequality follows from the definition of logarithmic height (4-1). □

4A. ***Height lower bound.*** We need the following result of Voutier [1996] concerning Lehmer's problem.

Lemma 4.2. *Let K be a number field of degree d. Let*

$$\partial_K = \begin{cases} \frac{\log 2}{d} & \text{if } d = 1, 2, \\ \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3 & \text{if } d \geq 3. \end{cases}$$

Then, for every nonzero algebraic number α in K, which is not a root of unity,

$$\deg(\alpha)\,\mathrm{h}(\alpha) \geq \partial_K.$$

Throughout, by the logarithm of a complex number, we mean the principal determination of the logarithm. In other words, if $x \in \mathbb{C}^*$ we express $x = re^{i\theta}$ where $r > 0$ and $-\pi < \theta \leq \pi$; we then let $\log x = \log r + i\theta$.

Lemma 4.3. *Let K be a number field and let*

$$\partial'_K = \left(1 + \frac{\pi^2}{\partial_K^2}\right)^{1/2}.$$

For any nonzero $\alpha \in K$ and any place $v \in M_K$,

$$\log|\alpha|_v \leq \deg(\alpha)\,\mathrm{h}(\alpha), \qquad \log\|\alpha\|_v \leq [K:\mathbb{Q}]\,\mathrm{h}(\alpha).$$

Moreover, if α is not a root of unity and σ is a real or complex embedding of K then

$$|\log\sigma(\alpha)| \leq \partial'_K \deg(\alpha)\,\mathrm{h}(\alpha).$$

Proof. The first two inequalities are an immediate consequence of the definition of absolute logarithmic height. For the last, write $\sigma(\alpha) = e^{a+ib}$, with $a = \log|\sigma(\alpha)|$ and $|b| \leq \pi$, and let $d = \deg(\alpha)$. Then we have

$$|\log\sigma(\alpha)| = (a^2 + b^2)^{1/2} \leq (\log^2|\sigma(\alpha)| + \pi^2)^{1/2} \leq \left((d\,\mathrm{h}(\alpha))^2 + \pi^2\right)^{1/2}.$$

By Lemma 4.2 we have $d\,\mathrm{h}(\alpha) \geq \partial_K$, so

$$|\log\sigma(\alpha)| \leq d\,\mathrm{h}(\alpha)\left(1 + \frac{\pi^2}{\partial_K^2}\right)^{1/2},$$

as required. □

5. Bounds for regulators

Later on we need to give upper bounds for the regulators of complicated number fields of high degree. The following lemma, based on bounds of Landau [1918], is an easy way to obtain reasonable bounds.

Lemma 5.1. *Let K be a number field with degree $d = u + 2v$ where u and v are respectively the numbers of real and complex embeddings. Denote the absolute*

discriminant by D_K and the regulator by R_K, and the number of roots of unity in K by w. Suppose, moreover, that L is a real number such that $D_K \le L$. Let

$$a = 2^{-v}\pi^{-d/2}\sqrt{L}.$$

Define the function $f_K(L,s)$ by

$$f_K(L,s) = 2^{-u} w a^s \left(\Gamma\left(\frac{s}{2}\right)\right)^u (\Gamma(s))^v s^{d+1}(s-1)^{1-d},$$

and let $B_K(L) = \min\{f_K(L, 2-t/1000) : t = 0, 1, \ldots, 999\}$. Then $R_K < B_K(L)$.

Proof. Landau [1918, proof of Hilfssatz 1] established the inequality

$$R_K < f_K(D_K, s)$$

for all $s > 1$. It is thus clear that $R_K < B_K(L)$. □

Remark 5.2. For a complicated number field of high degree it is difficult to calculate the discriminant D_K exactly, though it is easy to give an upper bound L for its size. It is also difficult to minimise the function $f_K(L,s)$ analytically, but we have found that the above gives an accurate enough result, which is easy to calculate on a computer.

6. Fundamental units

For the number fields we are concerned with, we shall need to work with a certain system of fundamental units.

Lemma 6.1 [Bugeaud and Győry 1996, Lemma 1]. *Let K be a number field of degree d and let $r = r_K$ be its unit rank and R_K its regulator. Define the constants*

$$c_1 = c_1(K) = \frac{(r!)^2}{2^{r-1}d^r}, \quad c_2 = c_2(K) = c_1\left(\frac{d}{\partial_K}\right)^{r-1}, \quad c_3 = c_3(K) = c_1\frac{d^r}{\partial_K}.$$

Then K admits a system $\{\varepsilon_1, \ldots, \varepsilon_r\}$ of fundamental units such that:

(i) $\prod_{i=1}^r \mathrm{h}(\varepsilon_i) \le c_1 R_K$.

(ii) $\mathrm{h}(\varepsilon_i) \le c_2 R_K$, $1 \le i \le r$.

(iii) *Write $\mathcal{M}$ for the $r \times r$-matrix $(\log \|\varepsilon_i\|_v)$, where v runs over r of the Archimedean places of K and $1 \le i \le r$. Then the absolute values of the entries of $\mathcal{M}^{-1}$ are bounded above by c_3.*

Lemma 6.2. *Let K be a number field of degree d, and let $\{\varepsilon_1, \ldots, \varepsilon_r\}$ be a system of fundamental units as in Lemma 6.1. Define the constant $c_4 = c_4(K) = rdc_3$. Suppose $\varepsilon = \zeta\varepsilon_1^{b_1}\ldots\varepsilon_r^{b_r}$, where ζ is a root of unity in K. Then*

$$\max\{|b_1|, \ldots, |b_r|\} \le c_4\,\mathrm{h}(\varepsilon).$$

Proof. Note that for any Archimedean place v of K,

$$\log \|\varepsilon\|_v = \sum b_i \log \|\varepsilon_i\|_v.$$

The lemma now follows from part (iii) of Lemma 6.1, plus the fact that $\log \|\varepsilon\|_v \leq d\,\mathrm{h}(\varepsilon)$ for all v given by Lemma 4.3. □

The following result is a special case of [Bugeaud and Győry 1996, Lemma 2].

Lemma 6.3. *Let K be a number field of unit rank r and regulator K. Let α be a nonzero algebraic integer belonging to K. Then there exists a unit ε of K such that*

$$\mathrm{h}(\alpha\varepsilon) \leq c_5 R_K + \frac{\log|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|}{[K:\mathbb{Q}]}$$

where

$$c_5 = c_5(K) = \frac{r^{r+1}}{2\partial_K^{r-1}}.$$

Lemma 6.4. *Let K be a number field, $\beta, \varepsilon \in K^*$ with ε being a unit. Let σ be the real or complex embedding that makes $|\sigma(\beta\varepsilon)|$ minimal. Then*

$$\mathrm{h}(\beta\varepsilon) \leq \mathrm{h}(\beta) - \log|\sigma(\beta\varepsilon)|.$$

Proof. As usual, write $d = [K:\mathbb{Q}]$ and $d_v = [K_v:\mathbb{Q}_v]$. Then

$$\begin{aligned}
\mathrm{h}(\beta\varepsilon) &= \mathrm{h}\Big(\frac{1}{\beta\varepsilon}\Big) \\
&= \frac{1}{d}\sum_{v\in M_K^\infty} d_v \max\{0, \log(|\beta\varepsilon|_v^{-1})\} + \frac{1}{d}\sum_{v\in M_K^0} d_v \max\{0, \log(|\beta\varepsilon|_v^{-1})\} \\
&\leq \log(|\sigma(\beta\varepsilon)|^{-1}) + \frac{1}{d}\sum_{v\in M_K^0} d_v \max\{0, \log(|\beta|_v^{-1})\} \\
&\leq -\log|\sigma(\beta\varepsilon)| + \frac{1}{d}\sum_{v\in M_K} d_v \max\{0, \log(|\beta|_v^{-1})\} \\
&\leq -\log|\sigma(\beta\varepsilon)| + \mathrm{h}(\beta).
\end{aligned}$$

□

7. Matveev's lower bound for linear forms in logarithms

Let L be a number field and let σ be a real or complex embedding. For $\alpha \in L^*$ we define the *modified logarithmic height of α with respect to σ* to be

$$\mathrm{h}_{L,\sigma}(\alpha) := \max\{[L:\mathbb{Q}]\,\mathrm{h}(\alpha),\ |\log\sigma(\alpha)|,\ 0.16\}.$$

The modified height is clearly dependent on the number field; we shall need the following Lemma which gives a relation between the modified and absolute height.

Lemma 7.1. *Let $K \subseteq L$ be number fields and write*

$$\partial_{L/K} = \max\left\{[L:\mathbb{Q}],\ [K:\mathbb{Q}]\partial'_K,\ \frac{0.16[K:\mathbb{Q}]}{\partial_K}\right\}.$$

Then for any $\alpha \in K$ which is neither zero nor a root of unity, and any real or complex embedding σ of L,

$$\mathrm{h}_{L,\sigma}(\alpha) \le \partial_{L/K}\,\mathrm{h}(\alpha).$$

Proof. By Lemma 4.3 we have

$$[K:\mathbb{Q}]\partial'_K\,\mathrm{h}(\alpha) \ge \partial'_K \deg(\alpha)\,\mathrm{h}(\alpha) \ge |\log\sigma(\alpha)|.$$

Moreover, by Lemma 4.2,

$$\frac{0.16[K:\mathbb{Q}]\,\mathrm{h}(\alpha)}{\partial_K} \ge \frac{0.16\deg(\alpha)\,\mathrm{h}(\alpha)}{\partial_K} \ge 0.16.$$

The lemma follows. □

We shall apply lower bounds on linear forms, more precisely a version of Matveev's estimates [2000]. We recall that log denotes the principal determination of the logarithm.

Lemma 7.2. *Let L be a number field of degree d, with $\alpha_1, \dots, \alpha_n \in L^*$. Define a constant*

$$C(L,n) := 3\cdot 30^{n+4}\cdot(n+1)^{5.5}\,d^2\,(1+\log d).$$

Consider the "linear form"

$$\Lambda := \alpha_1^{b_1}\cdots\alpha_n^{b_n} - 1,$$

where $b_1, \dots, b_n$ are rational integers and let $B := \max\{|b_1|, \dots, |b_n|\}$. If $\Lambda \neq 0$, and σ is any real or complex embedding of L then

$$\log|\sigma(\Lambda)| > -C(L,n)(1+\log(nB))\prod_{j=1}^{n}\mathrm{h}_{L,\sigma}(\alpha_j).$$

Proof. This straightforward corollary of Matveev's estimates is [Bugeaud et al. 2006, Theorem 9.4]. □

8. Bounds for unit equations

Now we are ready to prove an explicit version of [Bugeaud 1997, Lemma 4]. The proposition below allows us to replace in the final estimate the regulator of the larger field by the product of the regulators of two of its subfields. This often results in a significant improvement of the upper bound for the height. This idea is due to Voutier [1995].

Proposition 8.1. *Let L be a number field of degree d, which contains K_1 and K_2 as subfields. Let R_{K_i} (respectively r_i) be the regulator (respectively the unit rank) of K_i. Suppose further that ν_1, ν_2 and ν_3 are nonzero elements of L with height $\le H$ (with $H \ge 1$) and consider the unit equation*

$$\nu_1\varepsilon_1 + \nu_2\varepsilon_2 + \nu_3\varepsilon_3 = 0 \tag{8-1}$$

where ε_1 is a unit of K_1, ε_2 a unit of K_2 and ε_3 a unit of L. Then, for $i = 1$ and 2,

$$\mathrm{h}\Big(\frac{\nu_i\varepsilon_i}{\nu_3\varepsilon_3}\Big) \le A_2 + A_1 \log(H + \max\{\mathrm{h}(\nu_1\varepsilon_1), \mathrm{h}(\nu_2\varepsilon_2)\}),$$

where

$$A_1 = 2H \cdot C(L, r_1 + r_2 + 1) \cdot c_1(K_1)c_1(K_2)\partial_{L/L} \cdot (\partial_{L/K_1})^{r_1} \cdot (\partial_{L/K_2})^{r_2} \cdot R_{K_1}R_{K_2},$$
$$A_2 = 2H + A_1 + A_1 \log\big((r_1 + r_2 + 1) \cdot \max\{c_4(K_1), c_4(K_2), 1\}\big).$$

Proof. Let $\{\mu_1, \dots, \mu_{r_1}\}$ and $\{\rho_1, \dots, \rho_{r_2}\}$ be respectively systems of fundamental units for K_1 and K_2 as in Lemma 6.1; in particular we know that

$$\prod_{j=1}^{r_1} \mathrm{h}(\mu_j) \le c_1(K_1)R_{K_1}, \qquad \prod_{j=1}^{r_2} \mathrm{h}(\rho_j) \le c_1(K_2)R_{K_2}. \tag{8-2}$$

We can write

$$\varepsilon_1 = \zeta_1\mu_1^{b_1} \cdots \mu_{r_1}^{b_{r_1}}, \quad \varepsilon_2 = \zeta_2\rho_1^{f_1} \cdots \rho_{r_2}^{f_{r_2}},$$

where ζ_1 and ζ_2 are roots of unity and $b_1, \dots, b_{r_1}$, and $f_1, \dots, f_{r_2}$ are rational integers. Set

$$B_1 = \max\{|b_1|, \dots, |b_{r_1}|\}, \quad B_2 = \max\{|f_1|, \dots, |f_{r_2}|\}, \quad B = \max\{B_1, B_2, 1\}.$$

Set $\alpha_0 = -\frac{\zeta_2\nu_2}{\zeta_1\nu_1}$ and $b_0 = 1$. By (8-1),

$$\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1} = \alpha_0^{b_0}\mu_1^{-b_1} \cdots \mu_{r_1}^{-b_{r_1}}\rho_1^{f_1} \cdots \rho_{r_2}^{f_{r_2}} - 1.$$

Now choose the real or complex embedding σ of L such that $|\sigma(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1})|$ is minimal. We apply Matveev's estimate (Lemma 7.2) to this "linear form", obtaining

$$\log\Big|\sigma\Big(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\Big)\Big| > -C(L, n)(1 + \log(nB))\,\mathrm{h}_{L,\sigma}(\alpha_0)\prod_{j=1}^{r_1}\mathrm{h}_{L,\sigma}(\mu_j)\prod_{j=1}^{r_2}\mathrm{h}_{L,\sigma}(\rho_j),$$

where $n = r_1 + r_2 + 1$. Using Lemma 7.1 and (8-2) we obtain

$$\prod_{j=1}^{r_1}\mathrm{h}_{L,\sigma}(\mu_j) \le (\partial_{L/K_1})^{r_1}\prod_{j=1}^{r_1}\mathrm{h}(\mu_j) \le c_1(K_1)(\partial_{L/K_1})^{r_1}R_{K_1},$$

and a similar estimate for $\prod_{j=1}^{r_2} \mathrm{h}_{L,\sigma}(\rho_j)$. Moreover, again by Lemma 7.1 and Lemma 4.1, $\mathrm{h}_{L,\sigma}(\alpha_0) \le 2H\partial_{L/L}$. Thus

$$\log\left|\sigma\left(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right)\right| > -A_1(1+\log(nB)).$$

Now applying Lemma 6.4, we obtain that

$$\mathrm{h}\left(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right) \le \mathrm{h}\left(\frac{\nu_3}{\nu_1}\right) + A_1(1+\log(nB)) \le 2H + A_1(1+\log(nB)).$$

The proof is complete on observing, from Lemma 6.2, that

$$B \le \max\{c_4(K_1), c_4(K_2), 1\} \cdot \max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\},$$

and from Lemma 4.1,

$$\mathrm{h}(\nu_i\varepsilon_i) \le \mathrm{h}(\varepsilon_i) + \mathrm{h}(\nu_i) \le \mathrm{h}(\varepsilon) + H. \qquad \square$$

9. Upper bounds for the size of integral points on hyperelliptic curves

We shall need the following standard sort of lemma.

Lemma 9.1. *Let a, b, c, y be positive numbers and suppose that*

$$y \le a + b\log(c+y).$$

Then

$$y \le 2b\log b + 2a + c.$$

Proof. Let $z = c + y$, so that

$$z \le (a+c) + b\log z.$$

Now we apply the case $h = 1$ of [Pethö and de Weger 1986, Lemma 2.2]; this gives

$$z \le 2(b\log b + a + c). \qquad \square$$

Theorem 9.2. *Let α be an algebraic integer of degree at least 3, and let κ be an integer belonging to K. Let $\alpha_1, \alpha_2, \alpha_3$ be distinct conjugates of α and $\kappa_1, \kappa_2, \kappa_3$ be the corresponding conjugates of κ. Let*

$$K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \sqrt{\kappa_1\kappa_2}), \quad K_2 = \mathbb{Q}(\alpha_1, \alpha_3, \sqrt{\kappa_1\kappa_3}), \quad K_3 = \mathbb{Q}(\alpha_2, \alpha_3, \sqrt{\kappa_2\kappa_3}),$$

and

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1\kappa_2}, \sqrt{\kappa_1\kappa_3}).$$

Let R be an upper bound for the regulators of K_1, K_2 and K_3. Let r be the maximum of the unit ranks of K_1, K_2, K_3. Let

$$\begin{aligned}
c_j^* &= \max_{1\le i\le 3} c_j(K_i),\\
N &= \max_{1\le i,j\le 3} \left|\mathrm{Norm}_{\mathbb{Q}(\alpha_i,\alpha_j)/\mathbb{Q}}(\kappa_i(\alpha_i-\alpha_j))\right|^2,\\
H^* &= c_5^* R + \frac{\log N}{\min_{1\le i\le 3}[K_i:\mathbb{Q}]} + \mathrm{h}(\kappa),\\
A_1^* &= 2H^*\cdot C(L,2r+1)\cdot (c_1^*)^2\partial_{L/L}\cdot\Big(\max_{1\le i\le 3}\partial_{L/K_i}\Big)^{2r}\cdot R^2,\\
A_2^* &= 2H^* + A_1^* + A_1^*\log((2r+1)\cdot\max\{c_4^*,1\}).
\end{aligned}$$

If $x\in\mathbb{Z}\backslash\{0\}$ satisfies $x-\alpha=\kappa\xi^2$ for some $\xi\in K$ then

$$\log|x| \le 8A_1^*\log(4A_1^*) + 8A_2^* + H^* + 20\log 2 + 13\,\mathrm{h}(\kappa) + 19\,\mathrm{h}(\alpha).$$

Proof. Conjugating the relation $x-\alpha=\kappa\xi^2$ appropriately and taking differences we obtain

$$\alpha_1-\alpha_2=\kappa_2\xi_2^2-\kappa_1\xi_1^2,\quad \alpha_3-\alpha_1=\kappa_1\xi_1^2-\kappa_3\xi_3^2,\quad \alpha_2-\alpha_3=\kappa_3\xi_3^2-\kappa_2\xi_2^2.$$

Let

$$\tau_1=\kappa_1\xi_1,\qquad \tau_2=\sqrt{\kappa_1\kappa_2}\xi_2,\qquad \tau_3=\sqrt{\kappa_1\kappa_3}\xi_3.$$

Observe that

$$\kappa_1(\alpha_1-\alpha_2)=\tau_2^2-\tau_1^2,\quad \kappa_1(\alpha_3-\alpha_1)=\tau_1^2-\tau_3^2,\quad \kappa_1(\alpha_2-\alpha_3)=\tau_3^2-\tau_2^2,$$

and

$$\tau_2\pm\tau_1\in K_1,\quad \tau_1\pm\tau_3\in K_2,\quad \tau_3\pm\tau_2\in\sqrt{\frac{\kappa_1}{\kappa_2}}K_3.$$

We claim that each $\tau_i\pm\tau_j$ can be written in the form $\nu\varepsilon$ where ε is a unit in one of the K_i and $\nu\in L$ is an integer satisfying $\mathrm{h}(\nu)\le H^*$. Let us show this for $\tau_2-\tau_3$; the other cases are either similar or easier. Note that $\tau_2-\tau_3=\sqrt{\frac{\kappa_1}{\kappa_2}}\nu''$ where ν'' is an integer belonging to K_3. Moreover, ν'' divides

$$\sqrt{\frac{\kappa_2}{\kappa_1}}(\tau_3-\tau_2)\cdot\sqrt{\frac{\kappa_2}{\kappa_1}}(\tau_3+\tau_2)=\kappa_2(\alpha_2-\alpha_3).$$

Hence $|\mathrm{Norm}_{K_3/\mathbb{Q}}(\nu'')|\le N$. By Lemma 6.3, we can write $\nu''=\nu'\varepsilon$ where $\varepsilon\in K_3$ and

$$\mathrm{h}(\nu')\le c_5(K_3)R+\frac{\log N}{[K_3:\mathbb{Q}]}.$$

Now let $\nu=\sqrt{\frac{\kappa_1}{\kappa_2}}\nu'$. Thus $\tau_2-\tau_3=\nu\varepsilon$ where $\mathrm{h}(\nu)\le\mathrm{h}(\nu')+\mathrm{h}(\kappa)\le H^*$ proving our claim.

We apply Proposition 8.1 to the unit equation

$$(\tau_1 - \tau_2) + (\tau_3 - \tau_1) + (\tau_2 - \tau_3) = 0,$$

which is indeed of the form $\nu_1\varepsilon_1 + \nu_2\varepsilon_2 + \nu_3\varepsilon_3 = 0$ where the ν_i and ε_i satisfy the conditions of that proposition with H replaced by H^*. We obtain

$$\mathrm{h}\Big(\frac{\tau_1 - \tau_2}{\tau_1 - \tau_3}\Big) \le A_2^* + A_1^* \log(H^* + \max\{\mathrm{h}(\tau_2 - \tau_3), \mathrm{h}(\tau_1 - \tau_2)\}).$$

Observe that

$$\begin{aligned}\mathrm{h}(\tau_i \pm \tau_j) &\le \log 2 + \mathrm{h}(\tau_i) + \mathrm{h}(\tau_j) \le \log 2 + 2\,\mathrm{h}(\kappa) + 2\,\mathrm{h}(\xi)\\ &\le \log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(x - \alpha) \le 2\log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(\alpha) + \log|x|,\end{aligned}$$

where we have made repeated use of Lemma 4.1. Thus

$$\mathrm{h}\Big(\frac{\tau_1 - \tau_2}{\tau_1 - \tau_3}\Big) \le A_2^* + A_1^* \log(A_3^* + \log|x|),$$

where $A_3^* = H^* + 2\log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(\alpha)$.

We also apply Proposition 8.1 to the unit equation

$$(\tau_1 + \tau_2) + (\tau_3 - \tau_1) - (\tau_2 + \tau_3) = 0,$$

to obtain precisely the same bound for $\mathrm{h}(\frac{\tau_1+\tau_2}{\tau_1-\tau_3})$. Using the identity

$$\Big(\frac{\tau_1 - \tau_2}{\tau_1 - \tau_3}\Big) \cdot \Big(\frac{\tau_1 + \tau_2}{\tau_1 - \tau_3}\Big) = \frac{\kappa_1(\alpha_2 - \alpha_1)}{(\tau_1 - \tau_3)^2},$$

we obtain that

$$\mathrm{h}(\tau_1 - \tau_3) \le \frac{\log 2 + \mathrm{h}(\kappa)}{2} + \mathrm{h}(\alpha) + A_2^* + A_1^* \log(A_3^* + \log|x|).$$

Now

$$\begin{aligned}\log|x| &\le \log 2 + \mathrm{h}(\alpha) + \mathrm{h}(x - \alpha_1)\\ &\le \log 2 + \mathrm{h}(\alpha) + \mathrm{h}(\kappa) + 2\,\mathrm{h}(\tau_1) \qquad (\text{using } x - \alpha_1 = \tfrac{\tau_1^2}{\kappa_1})\\ &\le 5\log 2 + \mathrm{h}(\alpha) + \mathrm{h}(\kappa) + 2\,\mathrm{h}(\tau_1 + \tau_3) + 2\,\mathrm{h}(\tau_1 - \tau_3)\\ &\le 5\log 2 + \mathrm{h}(\alpha) + \mathrm{h}(\kappa) + 2\,\mathrm{h}\Big(\frac{\kappa_1(\alpha_3 - \alpha_1)}{\tau_1 - \tau_3}\Big) + 2\,\mathrm{h}(\tau_1 - \tau_3)\\ &\le 7\log 2 + 5\,\mathrm{h}(\alpha) + 3\,\mathrm{h}(\kappa) + 4\,\mathrm{h}(\tau_1 - \tau_3)\\ &\le 9\log 2 + 9\,\mathrm{h}(\alpha) + 5\,\mathrm{h}(\kappa) + 4A_2^* + 4A_1^* \log(A_3^* + \log|x|).\end{aligned}$$

The theorem follows from Lemma 9.1. □

10. The Mordell–Weil sieve I

The Mordell–Weil sieve is a technique that can be used to show the nonexistence of rational points on a curve (for example [Bruin and Stoll 2008a; ≥ 2008]), or to help determine the set of rational points in conjunction with the method of Chabauty (for example [Bruin and Elkies 2002]); for connections to the Brauer–Manin obstruction see, for example, [Flynn 2004; Poonen 2006; Stoll 2007]. In this section and the next we explain how the Mordell–Weil sieve can be used to show that any rational point on a curve of genus ≥ 2 is either a known rational point or a very large rational point.

In this section we let $C/\mathbb{Q}$ be a smooth projective curve (not necessarily hyperelliptic) of genus $g \geq 2$ and we let J be its Jacobian. As indicated in the introduction, we assume the knowledge of some rational points on C; henceforth let D be a fixed rational point on C (or even a fixed rational divisor of degree 1) and let $\jmath$ be the corresponding Abel–Jacobi map:

$$\jmath : C \to J, \qquad P \mapsto [P - D].$$

Let W be the image in J of the known rational points on C. The Mordell–Weil sieve is a strategy for obtaining a very large and "smooth" positive integer B such that

$$\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q}).$$

Recall that a positive integer B is called *A-smooth* if all its prime factors are $\leq A$. By saying that B is smooth, we loosely mean that it is A-smooth with A much smaller than B.

Let S be a finite set of primes, which for now we assume to be primes of good reduction for the curve C. The basic idea is to consider the following commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\jmath} & J(\mathbb{Q})/BJ(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \displaystyle\prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\jmath} & \displaystyle\prod_{p\in S} J(\mathbb{F}_p)/BJ(\mathbb{F}_p). \end{array}$$

The image of $C(\mathbb{Q})$ in $J(\mathbb{Q})/BJ(\mathbb{Q})$ must then be contained in the subset of $J(\mathbb{Q})/BJ(\mathbb{Q})$ of elements that map under α into the image of the lower horizontal map. If we find that this subset equals the image of W in $J(\mathbb{Q})/BJ(\mathbb{Q})$, then we have shown that

$$\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})$$

as desired. Note that, at least in principle, the required computation is finite: each set $C(\mathbb{F}_p)$ is finite and can be enumerated, hence $\jmath(C(\mathbb{F}_p))$ can be determined, and

we assume that we know explicit generators of $J(\mathbb{Q})$, which allows us to construct the finite set $J(\mathbb{Q})/BJ(\mathbb{Q})$. In practice, and in particular for the application we have in mind here, we will need a very large value of B, so this naive approach is much too inefficient. In [Bruin and Stoll 2008a; $\geq$ 2008], the authors describe how one can perform this computation in a more efficient way.

One obvious improvement is to replace the lower horizontal map in the diagram above by a product of maps

$$C(\mathbb{Q}_p) \xrightarrow{J} G_p/BG_p$$

with suitable finite quotients G_p of $J(\mathbb{Q}_p)$. We have used this to incorporate information modulo higher powers of p for small primes p. This kind of information is often called "deep" information, as opposed to the "flat" information obtained from reduction modulo good primes.

We can always force B to be divisible by any given (not too big) number. In our application we will want B to kill the rational torsion subgroup of J.

11. The Mordell–Weil sieve II

We continue with the notation of Section 10. Let W be the image in $J(\mathbb{Q})$ of all the known rational points on C. We assume that the strategy of Section 10 is successful in yielding a large "smooth" integer B such that any point $P \in C(\mathbb{Q})$ satisfies $_J(P) - w \in BJ(\mathbb{Q})$ for some $w \in W$, and moreover, that B kills all the torsion of $J(\mathbb{Q})$.

Let $D_1, \ldots, D_r$ be a basis of the free part of $J(\mathbb{Q})$ and let

$$\phi : \mathbb{Z}^r \to J(\mathbb{Q}), \qquad \phi(a_1, \ldots, a_r) = \sum a_i D_i,$$

so that the image of ϕ is simply the free part of $J(\mathbb{Q})$. Our assumption now is that

$$_J(C(\mathbb{Q})) \subset W + \phi(B\mathbb{Z}^r).$$

Set $L_0 = B\mathbb{Z}^r$. We explain a method of obtaining a (very long) decreasing sequence of lattices in $\mathbb{Z}^r$:

$$B\mathbb{Z}^r = L_0 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots \supsetneq L_k \tag{11-1}$$

such that

$$_J(C(\mathbb{Q})) \subset W + \phi(L_j)$$

for $j = 1, \ldots, k$.

If q is a prime of good reduction for J we denote by

$$\phi_q : \mathbb{Z}^r \to J(\mathbb{F}_q), \qquad \phi_q(a_1, \ldots, a_r) = \sum a_i \tilde{D}_i,$$

and so $\phi_q(\mathbf{l}) = \widetilde{\phi(\mathbf{l})}$.

Lemma 11.1. *Let W be a finite subset of $J(\mathbb{Q})$, and let L be a subgroup of $\mathbb{Z}^r$. Suppose that $\jmath(C(\mathbb{Q})) \subset W + \phi(L)$. Let q be a prime of good reduction for C and J. Let L' be the kernel of the restriction $\phi_q|_L$. Let $\mathbf{l}_1, \ldots, \mathbf{l}_m$ be representatives of the* nonzero *cosets of L/L' and suppose that $\tilde{w} + \phi_q(\mathbf{l}_i) \notin \jmath C(\mathbb{F}_q)$ for all $w \in W$ and $i = 1, \ldots, m$. Then $\jmath(C(\mathbb{Q})) \subset W + \phi(L')$.*

Proof. Suppose $P \in C(\mathbb{Q})$. Since $\jmath(C(\mathbb{Q})) \subset W + \phi(L)$, we may write $\jmath(P) = w + \phi(\mathbf{l})$ for some $\mathbf{l} \in L$. Now let $\mathbf{l}_0 = \mathbf{0}$, so that $\mathbf{l}_0, \ldots, \mathbf{l}_m$ represent *all* cosets of L/L'. Then $\mathbf{l} = \mathbf{l}_i + \mathbf{l}'$ for some $\mathbf{l}' \in L'$ and $i = 0, \ldots, m$. However, $\phi_q(\mathbf{l}') = 0$, or in other words, $\widetilde{\phi(\mathbf{l}')} = 0$. Hence

$$\jmath(\tilde{P}) = \widetilde{\jmath(P)} = \tilde{w} + \phi_q(\mathbf{l}) = \tilde{w} + \phi_q(\mathbf{l}_i) + \phi_q(\mathbf{l}') = \tilde{w} + \phi_q(\mathbf{l}_i).$$

By hypothesis, $\tilde{w} + \phi_q(\mathbf{l}_i) \notin \jmath C(\mathbb{F}_q)$ for $i = 1, \ldots, m$, so $i = 0$ and so $\mathbf{l}_i = 0$. Hence $\jmath(P) = w + \mathbf{l}' \in W + L'$ as required. □

We obtain a very long strictly decreasing sequence of lattices as in (11-1) by repeated application of Lemma 11.1. However, the conditions of Lemma 11.1 are unlikely to be satisfied for a prime q chosen at random. Here we give criteria that we have employed in practice to choose the primes q:

(I) $\gcd(B, \#J(\mathbb{F}_q)) > (\#J(\mathbb{F}_q))^{0.6}$.

(II) $L' \neq L$.

(III) $\#W \cdot (\#L/L' - 1) < 2q$.

(IV) $\tilde{w} + \phi_q(\mathbf{l}_i) \notin \jmath C(\mathbb{F}_q)$ for all $w \in W$ and $i = 1, \ldots, m$.

The criteria (I)–(IV) are listed in the order in which we check them in practice. Criterion (IV) is just the criterion of the lemma. Criterion (II) ensures that L' is strictly smaller than L, otherwise we gain no new information. Although we would like L' to be strictly smaller than L, we do not want the index L/L' to be too large and this is reflected in Criteria (I) and (III). Note that the number of checks required by Criterion (IV) (or the lemma) is $\#W \cdot (\#L/L' - 1)$. If this number is large then Criterion (IV) is likely to fail. Let us look at this in probabilistic terms. Assume that the genus of C is 2. Then the probability that a random element of $J(\mathbb{F}_q)$ lies in the image of $C(\mathbb{F}_q)$ is about $\frac{1}{q}$. If $N = \#W \cdot (\#L/L' - 1)$ then the probability that Criterion (IV) is satisfied is about $(1 - q^{-1})^N$. Since $(1 - q^{-1})^q \sim e^{-1}$, we do not want N to be too large in comparison to q, and this explains the choice of $2q$ in Criterion (III).

We still have not justified Criterion (I). The computation involved in obtaining L' is a little expensive. Since we need to do this with many primes, we would like a way of picking only primes where this computation is not wasted, and in particular $\#L/L'$ is not too large. Now at every stage of our computations, L will be some element of our decreasing sequence (11-1) and so contained in $B\mathbb{Z}^r$. Criterion (I)

ensures that a "large chunk" of L will be in the kernel of $\phi_q : \mathbb{Z}^r \to J(\mathbb{F}_q)$ and so that $\#L/L'$ is not too large. The exponent 0.6 in Criterion (I) is chosen on the basis of computational experience.

12. Lower bounds for the size of rational points

In this section, we suppose that the strategy of Sections 10 and 11 succeeded in showing that $\jmath(C(\mathbb{Q})) \subset W + \phi(L)$ for some lattice L of huge index in $\mathbb{Z}^r$, where W is the image in J of the set of known rational points in C. In this section we provide a lower bound for the size of rational points not belonging to the set of known rational points.

Lemma 12.1. *Let W be a finite subset of $J(\mathbb{Q})$, and let L be a sublattice of $\mathbb{Z}^r$. Suppose that $\jmath(C(\mathbb{Q})) \subset W + \phi(L)$. Let μ_1 be a lower bound for $h - \hat{h}$ as in* (1-2). *Let*

$$\mu_2 = \max\left\{\sqrt{\hat{h}(w)} : w \in W\right\}.$$

Let M be the height-pairing matrix for the Mordell–Weil basis $D_1, \ldots, D_r$ and let $\lambda_1, \ldots, \lambda_r$ be its eigenvalues. Let

$$\mu_3 = \min\{\sqrt{\lambda_j} : j = 1, \ldots, r\}.$$

Let $m(L)$ be the Euclidean norm of the shortest nonzero vector of L, and suppose that $\mu_3 m(L) \geq \mu_2$. Then, for any $P \in C(\mathbb{Q})$, either $\jmath(P) \in W$ or

$$h(\jmath(P)) \geq (\mu_3 m(L) - \mu_2)^2 + \mu_1.$$

Note that $m(L)$ is called the *minimum of L* and can be computed using an algorithm of Fincke and Pohst [1985].

Proof. Suppose that $\jmath(P) \notin W$. Then $\jmath(P) = w + \phi(\mathbf{l})$ for some nonzero element $\mathbf{l} \in L$. In particular, if $\|\cdot\|$ denotes Euclidean norm then $\|\mathbf{l}\| \geq m(L)$.

We can write $M = N\Lambda N^t$ where N is orthogonal and Λ is the diagonal matrix with diagonal entries λ_i. Let $\mathbf{x} = \mathbf{l}N$ and write $\mathbf{x} = (x_1, \ldots, x_r)$. Then

$$\hat{h}(\phi(\mathbf{l})) = \mathbf{l}M\mathbf{l}^t = \mathbf{x}\Lambda\mathbf{x}^t \geq \mu_3^2\|\mathbf{x}\|^2 = \mu_3^2\|\mathbf{l}\|^2 \geq \mu_3^2 m(L)^2.$$

Now recall that $D \mapsto \sqrt{\hat{h}(D)}$ defines a norm on $J(\mathbb{Q}) \otimes \mathbb{R}$ and so by the triangle inequality

$$\sqrt{\hat{h}(\jmath(P))} \geq \sqrt{\hat{h}(\phi(\mathbf{l}))} - \sqrt{\hat{h}(w)} \geq \mu_3 m(L) - \mu_2.$$

The lemma now follows from (1-2). □

Remark 12.2. We can replace $\mu_3 m(L)$ with the minimum of L with respect to the height pairing matrix. This is should lead to a very slight improvement. Since in practice our lattice L has very large index, computing the minimum of L with

Table 1

coset of $J(\mathbb{Q})/2J(\mathbb{Q})$	κ	unit rank of K_i	bound R for regulator of K_i	bound for $\log x$
0	1	12	1.8×10^{26}	1.0×10^{263}
D_1	-2α	21	6.2×10^{53}	7.6×10^{492}
D_2	$4-2\alpha$	25	1.3×10^{54}	2.3×10^{560}
D_3	$-4-2\alpha$	21	3.7×10^{55}	1.6×10^{498}
D_1+D_2	$-2\alpha+\alpha^2$	21	1.0×10^{52}	3.2×10^{487}
D_1+D_3	$2\alpha+\alpha^2$	25	7.9×10^{55}	5.1×10^{565}
D_2+D_3	$-4+\alpha^2$	21	3.7×10^{55}	1.6×10^{498}
$D_1+D_2+D_3$	$8\alpha-2\alpha^3$	25	7.9×10^{55}	5.1×10^{565}

respect to the height pairing matrix may require the computation of the height pairing matrix to very great accuracy, and such a computation is inconvenient. We therefore prefer to work with the Euclidean norm on $\mathbb{Z}^r$.

13. Proofs of Theorems 1.1 and 1.2

The equation $Y^2 - Y = X^5 - X$ is transformed into

$$C: \quad 2y^2 = x^5 - 16x + 8, \tag{13-1}$$

via the change of variables $y = 4Y - 2$ and $x = 2X$ which preserves integrality. We shall work with the model (13-1). Let C be the smooth projective genus 2 curve with affine model given by (13-1), and let J be its Jacobian. Using `MAGMA` [Bosma et al. 1997] we know that $J(\mathbb{Q})$ is free of rank 3 with Mordell–Weil basis given by

$$D_1 = (0, 2) - \infty, \qquad D_2 = (2, 2) - \infty, \qquad D_3 = (-2, 2) - \infty.$$

The `MAGMA` programs used for this step are based on Stoll's papers [1999; 2001; 2002].

Let $f = x^5 - 16x + 8$. Let α be a root of f. We shall choose for coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$ the linear combinations $\sum_{i=1}^{3} n_i D_i$ with $n_i \in \{0, 1\}$. Then

$$x - \alpha = \kappa \xi^2,$$

where $\kappa \in \mathcal{K}$ and $\mathcal{K}$ is constructed as in Lemma 3.1. We tabulate the κ corresponding to the $\sum_{i=1}^{3} n_i D_i$ in Table 1.

Next we compute the bounds for $\log x$ given by Theorem 9.2 for each value of κ. We implemented our bounds in `MAGMA`. Here the Galois group of f is S_5 which implies that the fields K_1, K_2, K_3 corresponding to a particular κ are isomorphic. The unit ranks of K_i, the bounds for their regulators as given by Lemma 5.1, and the corresponding bounds for $\log x$ are tabulated also in Table 1.

A quick search reveals 17 rational points on C:

$$\infty,\ (-2,\pm 2),\ (0,\pm 2),\ (2,\pm 2),\ (4,\pm 22),\ (6,\pm 62),$$
$$(1/2,\pm 1/8),\ (-15/8,\pm 697/256),\ (60,\pm 9859).$$

Let W denote the image of this set in $J(\mathbb{Q})$. Applying the implementation of the Mordell–Weil sieve due to Bruin and Stoll which is explained in Section 10 we obtain that $\jmath(C(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})$ where

$$\begin{aligned} B &= 44493297806147482064729726861799406525157544832743067965682140480 00 \\ &= 2^8 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31^2 \cdot \prod_{\substack{37 \le p \le 149 \\ p \ne 107}} p. \end{aligned}$$

For this computation, we used "deep" information modulo 2^9, 3^6, 5^4, 7^3, 11^3, 13^2, 17^2, 19^2, and "flat" information from all primes $p < 50000$ such that $\#J(\mathbb{F}_p)$ is 500-smooth (but keeping only information coming from the maximal 150-smooth quotient group of $J(\mathbb{F}_p)$). Recall that an integer is called *A-smooth* if all its prime divisors are $\le A$. This computation took about 7 hours on a 2 GHz Intel Core 2 CPU.

We now apply the new extension of the Mordell–Weil sieve which is explained in Section 11. We start with $L_0 = B\mathbb{Z}^3$ where B is as above. We successively apply Lemma 11.1 using all primes $q < 10^6$ which are primes of good reduction and satisfy criteria (I)–(IV) of Section 11. There are 78,498 primes less than 10^6. Of these, we discard 2, 139, 449 as they are primes of bad reduction for C. This leaves us with 78,495 primes. Of these, Criterion (I) fails for 77,073 of them, Criterion (II) fails for 220 of the remaining, Criterion (III) fails for 43 primes that survive Criteria (I) and (II), and Criterion (IV) fails for 237 primes that survive Criteria (I)–(III). Altogether, only 922 primes $q < 10^6$ satisfy Criteria (I)–(IV) and increase the index of L.

The index of the final L in $\mathbb{Z}^3$ is approximately 3.32×10^{3240}. This part of the computation lasted about 37 hours on a 2.8 GHZ Dual-Core AMD Opteron.

Let μ_1, μ_2, μ_3 be as in the notation of Lemma 12.1. Using `MAGMA` we find $\mu_1 = 2.677$, $\mu_2 = 2.612$ and $\mu_3 = 0.378$ (to 3 decimal places). The shortest vector of the final lattice L is of Euclidean length approximately 1.156×10^{1080} (it should be no surprise that this is roughly the cube root of the index of L in $\mathbb{Z}^3$). By Lemma 12.1 if $P \in C(\mathbb{Q})$ is not one of the 17 known rational points then

$$h(\jmath(P)) \ge 1.9 \times 10^{2159}.$$

If P is an integral point, then $h(\jmath(P)) = \log 2 + 2\log x(P)$. Thus

$$\log x(P) \geq 0.95 \times 10^{2159}.$$

This contradicts the bounds for $\log x$ in Table 1 and shows that the integral point P must be one of the 17 known rational points. This completes the proof of Theorem 1.1. The proof of Theorem 1.2 is similar and we omit the details.

The reader can find the `MAGMA` programs for verifying the above computations at: `http://www.warwick.ac.uk/staff/S.Siksek/progs/intpoint/`.

Acknowledgments

We are grateful to the referee and editors for many useful comments, and to Mr. Homero Gallegos–Ruiz for spotting many misprints.

References

[Avanesov 1966/1967] È. T. Avanesov, "Lösung eines Problems der figurierten Zahlen", *Acta Arith.* **12** (1966/1967), 409–420. In Russian. MR 35 #6619 Zbl 0153.06403

[Baker 1969] A. Baker, "Bounds for the solutions of the hyperelliptic equation", *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444. MR 38 #3226 Zbl 0174.33803

[Bilu 1995] Y. Bilu, "Effective analysis of integral points on algebraic curves", *Israel J. Math.* **90**:1-3 (1995), 235–252. MR 96e:11082 Zbl 0840.11028

[Bilu and Hanrot 1998] Y. F. Bilu and G. Hanrot, "Solving superelliptic Diophantine equations by Baker's method", *Compositio Math.* **112**:3 (1998), 273–312. MR 99d:11028 Zbl 0915.11065

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Brindza 1984] B. Brindza, "On S-integral solutions of the equation $y^m = f(x)$", *Acta Math. Hungar.* **44**:1-2 (1984), 133–139. MR 85m:11017 Zbl 0552.10009

[Brindza 1991] B. Brindza, "On a special superelliptic equation", *Publ. Math. Debrecen* **39**:1-2 (1991), 159–162. MR 92j:11029 Zbl 0749.11024

[Bruin 1999] N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, PhD Thesis, University of Leiden, Leiden, 1999.

[Bruin 2003] N. Bruin, "Chabauty methods using elliptic curves", *J. Reine Angew. Math.* **562** (2003), 27–49. MR 2004j:11051 Zbl 1135.11320

[Bruin and Elkies 2002] N. Bruin and N. D. Elkies, "Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order 168 and $8 \cdot 168$", pp. 172–188 in *Algorithmic number theory* (Sydney, 2002), edited by F. Claus and K. D. R., Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002. MR 2005d:11094 Zbl 1058.11044

[Bruin and Stoll 2008a] N. Bruin and M. Stoll, "Deciding existence of rational points on curves: an experiment", *Experiment. Math.* **17** (2008), 181–189. arXiv math/0604524

[Bruin and Stoll 2008b] N. Bruin and M. Stoll, "Two-cover descent on hyperelliptic curves", preprint, 2008. arXiv 0803.2052

[Bruin and Stoll ≥ 2008] N. Bruin and M. Stoll, "The Mordell–Weil sieve: proving the non-existence of rational points on curves". In preparation.

[Bugeaud 1997] Y. Bugeaud, "Bounds for the solutions of superelliptic equations", *Compositio Math.* **107**:2 (1997), 187–219. MR 98c:11025 Zbl 0886.11016

[Bugeaud and Győry 1996] Y. Bugeaud and K. Győry, "Bounds for the solutions of unit equations", *Acta Arith.* **74**:1 (1996), 67–80. MR 97b:11045 Zbl 0861.11023

[Bugeaud et al. 2006] Y. Bugeaud, M. Mignotte, and S. Siksek, "Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers", *Ann. of Math.* (2) **163**:3 (2006), 969–1018. MR 2007f:11031 Zbl 1113.11021

[Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series **230**, Cambridge University Press, Cambridge, 1996. MR 97i:11071 Zbl 0857.14018

[Evertse and Tijdeman 2007] J.-H. Evertse and R. Tijdeman, "Some open problems about Diophantine equations", 2007, available at http://www.math.leidenuniv.nl/ evertse/07-workshop-problems.pdf.

[Fielder and Alford 1998] D. C. Fielder and C. O. Alford, "Observations from computer experiments on an integer equation", pp. 93–103 in *Applications of Fibonacci numbers* (Graz, 1996), vol. 7, edited by G. E. Bergum et al., Kluwer Acad. Publ., Dordrecht, 1998. MR 1638435 Zbl 0913.11014

[Fincke and Pohst 1985] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis", *Math. Comp.* **44**:170 (1985), 463–471. MR 86e:11050 Zbl 0556.10022

[Flynn 1997] E. V. Flynn, "A flexible method for applying Chabauty's theorem", *Compositio Math.* **105**:1 (1997), 79–94. MR 97m:11083 Zbl 0882.14009

[Flynn 2004] E. V. Flynn, "The Hasse principle and the Brauer–Manin obstruction for curves", *Manuscripta Math.* **115**:4 (2004), 437–466. MR 2005j:11047 Zbl 1069.11023

[Flynn and Smart 1997] E. V. Flynn and N. P. Smart, "Canonical heights on the Jacobians of curves of genus 2 and the infinite descent", *Acta Arith.* **79**:4 (1997), 333–352. MR 98f:11066 Zbl 0895.11026

[Flynn and Wetherell 1999] E. V. Flynn and J. L. Wetherell, "Finding rational points on bielliptic genus 2 curves", *Manuscripta Math.* **100**:4 (1999), 519–533. MR 2001g:11098 Zbl 1029.11024

[Flynn and Wetherell 2001] E. V. Flynn and J. L. Wetherell, "Covering collections and a challenge problem of Serre", *Acta Arith.* **98**:2 (2001), 197–205. MR 2002b:11088 Zbl 1049.11066

[Kiss 1988] P. Kiss, "On the number of solutions of the Diophantine equation $\binom{x}{p} = \binom{y}{2}$", *Fibonacci Quart.* **26**:2 (1988), 127–130. MR 89f:11050 Zbl 0641.10016

[Landau 1918] E. Landau, "Verallgemeinerung eines *Pólya*schen Satzes auf algebraische Zahlkörper.", *Gött. Nachr.* (1918), 478–488. JFM 46.0267.01

[Lind 1968] D. A. Lind, "The quadratic field $Q(\sqrt{5})$ and a certain Diophantine equation", *Fibonacci Quart.* **6**:3 (1968), 86–93. MR 38 #112 Zbl 0174.33801

[Matveev 2000] E. M. Matveev, "An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II", *Izv. Ross. Akad. Nauk Ser. Mat.* **64**:6 (2000), 125–180. English translation in *Izv. Math.* **64** *(2000), no. 6, 1217–1269.* MR 2002e:11091 Zbl 1013.11043

[Mignotte and Pethő 1999] M. Mignotte and A. Pethő, "On the Diophantine equation $x^p - x = y^q - y$", *Publ. Mat.* **43**:1 (1999), 207–216. MR 2000d:11044 Zbl 0949.11022

[Mordell 1963] L. J. Mordell, "On the integer solutions of $y(y+1) = x(x+1)(x+2)$", *Pacific J. Math.* **13** (1963), 1347–1351. MR 27 #3590 Zbl 0124.27402

[Pethö and de Weger 1986] A. Pethö and B. M. M. de Weger, "Products of prime powers in binary recurrence sequences. I. The hyperbolic case, with an application to the generalized Ramanujan–Nagell equation", *Math. Comp.* **47**:176 (1986), 713–727. MR 87m:11027a Zbl 0623.10011

[Pintér 1995] Á. Pintér, "A note on the Diophantine equation $\binom{x}{4} = \binom{y}{2}$", *Publ. Math. Debrecen* **47**:3-4 (1995), 411–415. MR 96i:11027 Zbl 0856.11019

[Poonen 2006] B. Poonen, "Heuristics for the Brauer–Manin obstruction for curves", *Experiment. Math.* **15**:4 (2006), 415–420. MR 2008d:11062 Zbl 05196200

[Poonen and Schaefer 1997] B. Poonen and E. F. Schaefer, "Explicit descent for Jacobians of cyclic covers of the projective line", *J. Reine Angew. Math.* **488** (1997), 141–188. MR 98k:11087 Zbl 0888.11023

[Poulakis 1991] D. Poulakis, "Solutions entières de l'équation $Y^m = f(X)$", *Sém. Théor. Nombres Bordeaux* (2) **3**:1 (1991), 187–199. MR 93a:11025 Zbl 0733.11009

[Schaefer 1995] E. F. Schaefer, "2-descent on the Jacobians of hyperelliptic curves", *J. Number Theory* **51**:2 (1995), 219–232. MR 96c:11066 Zbl 0832.14016

[Schmidt 1992] W. M. Schmidt, "Integer points on curves of genus 1", *Compositio Math.* **81**:1 (1992), 33–59. MR 93e:11076 Zbl 0747.11026

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 95m:11054 Zbl 0585.14026

[Singmaster 1975] D. Singmaster, "Repeated binomial coefficients and Fibonacci numbers", *Fibonacci Quart.* **13**:4 (1975), 295–298. MR 54 #224 Zbl 0324.05007

[Smart 1998] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts **41**, Cambridge University Press, Cambridge, 1998. MR 2000c:11208 Zbl 0907.11001

[Sprindžuk 1977] V. G. Sprindžuk, "The arithmetic structure of integer polynomials and class numbers", *Trudy Mat. Inst. Steklov.* **143** (1977), 152–174, 210. MR 58 #589

[Stoll 1999] M. Stoll, "On the height constant for curves of genus two", *Acta Arith.* **90**:2 (1999), 183–201. MR 2000h:11069 Zbl 0932.11043

[Stoll 2001] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98**:3 (2001), 245–277. MR 2002b:11089 Zbl 0972.11058

[Stoll 2002] M. Stoll, "On the height constant for curves of genus two. II", *Acta Arith.* **104**:2 (2002), 165–182. MR 2003f:11093 Zbl 1139.11318

[Stoll 2007] M. Stoll, "Finite descent obstructions and rational points on curves", *Algebra Number Theory* **1**:4 (2007), 349–391. MR 2008i:11086

[Stroeker and de Weger 1999] R. J. Stroeker and B. M. M. de Weger, "Elliptic binomial Diophantine equations", *Math. Comp.* **68**:227 (1999), 1257–1281. MR 99i:11122 Zbl 0920.11014

[Stroeker and Tzanakis 2003] R. J. Stroeker and N. Tzanakis, "Computing all integer solutions of a genus 1 equation", *Math. Comp.* **72**:244 (2003), 1917–1933. MR 2004b:11037 Zbl 1089.11019

[Voutier 1995] P. M. Voutier, "An upper bound for the size of integral solutions to $Y^m = f(X)$", *J. Number Theory* **53**:2 (1995), 247–271. MR 96f:11049 Zbl 0842.11008

[Voutier 1996] P. Voutier, "An effective lower bound for the height of algebraic numbers", *Acta Arith.* **74**:1 (1996), 81–95. MR 96j:11098 Zbl 0838.11065

[de Weger 1996] B. M. M. de Weger, "A binomial Diophantine equation", *Quart. J. Math. Oxford Ser.* (2) **47**:186 (1996), 221–231. MR 97c:11041 Zbl 0863.11022

[de Weger 1997] B. M. M. de Weger, "Equal binomial coefficients: some elementary considerations", *J. Number Theory* **63**:2 (1997), 373–386. MR 98b:11027 Zbl 0873.11023

[Wetherell 1997] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD Thesis, University of California, Berkeley, 1997.

Communicated by Bjorn Poonen
Received 2008-01-28 Revised 2008-09-02 Accepted 2008-09-12

bugeaud@math.u-strasbg.fr *Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France*
http://www-irma.u-strasbg.fr/~bugeaud/

mignotte@math.u-strasbg.fr *Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France*

s.siksek@warwick.ac.uk *Institute of Mathematics, University of Warwick, Coventry CV4 7AL, United Kingdom*
http://www.warwick.ac.uk/~maseap/

Michael.Stoll@uni-bayreuth.de *Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany*
http://www.mathe2.uni-bayreuth.de/stoll/

tengely@math.klte.hu *Institute of Mathematics, University of Debrecen, Number Theory Research Group, Hungarian Academy of Sciences, P.O.Box 12, 4010 Debrecen, Hungary*
http://www.math.klte.hu/~tengely/