Journal of Number Theory 133 (2013) 963–969

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On an analogue of the Lutz–Nagell Theorem for hyperelliptic curves

David Grant

Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309-0395, USA

ARTICLE INFO

Article history:
Received 21 June 2011
Accepted 21 February 2012
Available online 29 May 2012
Communicated by David Goss

To the memory of David Hayes

MSC:
11G30
14G05

Keywords:
Arithmetic of hyperelliptic curves

ABSTRACT

We produce a version of the Lutz–Nagell Theorem for hyperelliptic curves of genus $g \geqslant 1$. We consider curves C defined by $y^2 = f(x)$, where f is a monic polynomial of degree $2g+1$ defined over the ring of integers of a number field F or its non-archimedean completions. If J is the Jacobian of C, and ϕ is the Abel–Jacobi map of C into J sending the point at ∞ of our model of C to the origin of J, we show that if $P = (a, b)$ is a rational point of C such that $\phi(P)$ is torsion in J, then a and b are integral if the order n of P is not a prime power, and bound the denominators of a and b if n is. When a and b are integral, we give criteria for when b^2 divides the discriminant $\Delta(f)$ of f. Finally we show for $f \in \mathbb{Z}[x]$, that if $P = (a, b) \in C(\mathbb{Q})$ and $\phi(P)$ is a torsion point of order $n \geqslant 2$, then we have $a, b \in \mathbb{Z}$, and either $b = 0$ or b^2 divides $\Delta(f)$.

0. Introduction

One of the central results in the arithmetic of elliptic curves is the Lutz–Nagell Theorem, which says that if

$$E: \quad y^2 = f(x) = x^3 + Ax + B, \quad A, B \in \mathbb{Z},$$

is an affine model of an elliptic curve over $\mathbb{Q}$, then for any nontrivial torsion point $P = (a, b) \in E(\mathbb{Q})$, that a and b are integers, and if $b \neq 0$ (that is, P is not of order 2), then b^2 divides $-(4A^3 + 27B^2)$, the discriminant of f [Lu,N]. The integrality and divisibility statements at odd primes p of good reduction for the model E and P of prime-to-p order are not surprising: they are only saying that such torsion points do not reduce to the origin or 2-torsion points modulo p. Indeed, the analogous statements

E-mail address: grant@boulder.colorado.edu.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.02.023

hold for hyperelliptic curves (see comments below). The depth of the Lutz–Nagell Theorem (and its generalization over number fields F and their non-archimedean completions $F_{\mathfrak{p}}$, due to Cassels [C]), comes from the study of torsion points in the formal group on the kernel of reduction modulo $\mathfrak{p}$ of a minimal model for E over the ring of integers of $F_{\mathfrak{p}}$. As such, the theorem is usually stated as a corollary to the study of torsion points in a 1-dimensional formal group over any complete discrete valuation ring [Si], which is the path we will emulate for the Jacobians of hyperelliptic curves.

The theorem one would like to prove to generalize the Lutz–Nagell Theorem is an integrality (and divisibility) statement for coordinates of torsion points on any abelian variety A over the rationals (or any number field F). This is related to the problem of finding analogues for abelian varieties of elliptic units, a problem where only small progress has been made [Ar,BB,FK,FKN,GL,G1,G2]. (The function field analogue of elliptic units is due to Hayes [H].) A conjecture of Tate and Voloch would say that for any effective divisor D on A, for any prime $\mathfrak{p}$ of F, there is a lower bound on the $\mathfrak{p}$-adic distance of all torsion points of A (not in D) to D [TV] (see also [B,Sc,V]). On the other hand, a conjecture of Ih ([BIR]: see also [GI]) would say that for such a D and fixed S, the torsion points in A which are S-integral with respect to D are not Zariski dense in A if the support of D does not consist of translates of abelian subvarieties of A by torsion points.

For Jacobians J of curves of genus 2 defined over number fields, akin to the Lutz–Nagell Theorem, one can effectively find all the rational torsion points by bounding their Weil height. Flynn and Smart did this by computing the difference between the absolute Weil height and the canonical height of points on J, and the result follows from the fact that torsion points have canonical height 0 [FS]. This approach will assuredly work for Jacobians of hyperelliptic curves of any genus, and perhaps enough is now known about explicit equations defining all Jacobians to successfully follow this approach in general [An].

In this paper our goal will be far more modest. We will consider affine models $y^2 = f(x)$ of hyperelliptic curves C of genus $g \geqslant 1$ over a number field F (and its non-archimedean completions $F_{\mathfrak{p}}$), where f is a monic polynomial of degree $2g+1$ over the ring of integers of F or $F_{\mathfrak{p}}$. Let ϕ be the Abel–Jacobi map embedding C into its Jacobian J using the point at infinity ∞ as basepoint. We will prove (see Theorem 3) that for $F = \mathbb{Q}$, if $P = (a, b) \in C(\mathbb{Q})$, then if $\phi(P)$ is torsion on J, then a and b are integers, and that if $b \neq 0$, then b^2 divides the discriminant $\Delta(f)$ of f (and we will discuss what is true over general number fields). As above, that something like this should be true is not surprising—it is easy to prove integrality at primes of good reduction for the model and for torsion points of order prime to the residue characteristic. The way we proceed in general to prove integrality is to find a smooth model $\mathcal{C}$ for C over a complete discrete valuation ring R, and then extend the Abel–Jacobi map to a morphism from $\mathcal{C}$ into a Néron model $\mathcal{J}$ for J. One then makes use of the formal group on the kernel of reduction of $\mathcal{J}$ to bound the denominators of a and b (see Theorem 1).

To get the divisibility of $\Delta(f)$ by b^2 by mimicking the standard proof from the elliptic curve case would require doubling P in J, and using that this is a nontrivial torsion point (see e.g., [Si,ST]). If $g > 1$ and P is not a Weierstrass point of C, then this doubled point is no longer on $\phi(C)$, so we will have to consider a different approach, making use of the Abel–Jacobi map from C into J when *any* of the $2g+2$ Weierstrass points of C is taken as basepoint (see Theorem 2). This provides a new approach to the Lutz–Nagell Theorem even in the case of elliptic curves.

The reason this result for $g > 1$ is so much more modest than when $g = 1$, is that unlike in the elliptic curve case, the Manin–Mumford Conjecture (first proved by Raynaud [R]: see Tzermias's survey article [T] for more) shows that there are only finitely-many torsion points of J which lie on $\phi(C)$. Yet despite its modest scope, there are interesting computational applications of our result. For example, for any prime $p \geqslant 2$, the family of genus 2 curves over $\mathbb{Q}$:

$$y^2 = f(x) = x^5 + \left(p^2x - 1\right)\left(Ax^3 + Bx^2 + Cx + D\right), \quad A, B, C, D \in \mathbb{Z},\ \Delta(f) \neq 0,$$

all have Jacobians with positive Mordell–Weil rank over $\mathbb{Q}$, because each curve in the family has the non-integral rational point $(x, y) = (1/p^2, 1/p^5)$.

1. Statements and proofs

Let $\lfloor c \rfloor$ denote the floor of (greatest integer less than or equal to) a real number c. Our main tool is:

Theorem 1. *Suppose that R is a complete discrete valuation domain, with fraction field K, maximal ideal $\mathfrak{p} = (\pi)$, and with perfect residue field k of characteristic p. Let v be the valuation on R normalized so that $v(\pi) = 1$. Let*

$$y^2 = f(x) = x^{2g+1} + b_1 x^{2g} + \cdots + b_{2g} x + b_{2g+1}, \quad b_i \in R,$$

define an affine piece C' of a projective non-singular curve C over K of genus $g \geqslant 1$, i.e., f has no multiple roots in an algebraic closure of K. Let $\infty \in C(K)$ denote the point at infinity of this model (i.e., $\infty = C - C'$). Let J be the Jacobian of C, and ϕ the Abel–Jacobi map that takes any $P \in C$ to the divisor class of $P - \infty$ in J. If (a, b) are the (x, y)-coordinates of a point P in $C'(K)$, and $\phi(P)$ is torsion of order n on J, then:

(i) *If n is not a power of p, then $a, b \in R$.*
(ii) *If $n = p^m$, then if $r = \lfloor v(p)/(p^m - p^{m-1}) \rfloor$, then*

$$v(a) \geqslant -2r, \qquad v(b) \geqslant -(2g+1)r.$$

Proof. The proof follows from the existence of the Néron model $\mathcal{J}$ of J over R, along with a computation involving formal groups.

We start by writing down a projective scheme over R whose generic fibre is isomorphic to C. Let $x_0, x_1, \ldots, x_{g+1}, z$ be coordinates in $\mathbb{P}^{g+2}_R$, and let $\mathcal{C}$ be the projective scheme over R defined by:

$$z^2 = x_{g+1}x_g + b_1 x_g^2 + \cdots + b_{2g} x_1 x_0 + b_{2g+1} x_0^2,$$
$$x_i x_j = x_k x_l, \quad 0 \leqslant i, j, k, l \leqslant g+1,\ i + j = k + l.$$

We will write $f : \mathcal{C} \to \operatorname{Spec}(R)$ for the structure map. Note that $\mathcal{C}$ is covered by the open R-subschemes $\mathcal{D}_{g+1} = \mathcal{C} \cap (x_{g+1} \neq 0)$ and $\mathcal{D}_0 = \mathcal{C} \cap (x_0 \neq 0)$, which are respectively isomorphic over R to the affine planar R-schemes defined by

$$t^2 = x_g + b_1 x_g^2 + \cdots + b_{2g+1} x_g^{2g+2}, \tag{1}$$

and

$$y^2 = x_1^{2g+1} + b_1 x_1^{2g} + \cdots + b_{2g+1}. \tag{2}$$

It follows standardly that the generic fibre of $\mathcal{C}$ is isomorphic to C. We will let C_r denote the special fibre of $\mathcal{C}$. It is easy to check that $\mathcal{D}_0$ and $\mathcal{D}_{g+1}$ are integral and that f restricted to $\mathcal{D}_0$ and $\mathcal{D}_{g+1}$ are of finite type and surjective, and since $\mathcal{D}_0$ and $\mathcal{D}_{g+1}$ are not disjoint, that $\mathcal{C}$ is integral and f is surjective and of finite type. Since R is a Dedekind domain, f is flat over R [Liu, p. 137, Cor. 3.10]. Hence a point $P \in \mathcal{C}$ is smooth over R if and only if it is smooth in the fibre $\mathcal{C}_{f(P)}$ over the residue field of $f(P)$ [Liu, p. 142, Def. 3.35].

Let $\infty = (0, 0, \ldots, 0, 1, 0) \in \mathbb{P}^{g+2}_R$, an R-point of $\mathcal{C}$, and $\overline{\infty} = \infty \cap C_r = (0, 0, \ldots, 0, 1, 0) \in \mathbb{P}^{g+2}_k$ be the reduction modulo $\mathfrak{p}$ of ∞ on C_r. The Jacobian criterion shows that C_r is smooth at $\overline{\infty}$. Hence $\overline{\infty}$ is a smooth point of $\mathcal{C}$ over R.

Since C is smooth over K, the only non-smooth points of $\mathcal{C}$ over R are on C_r. Let $\mathcal{C}^s$ be the smooth locus of $\mathcal{C}$, that is, the open subscheme of $\mathcal{C}$ consisting of the points smooth over R. The induced map

$\mathcal{C}^s \to \mathrm{Spec}(R)$ is surjective and of finite type, and we can identify the generic fibre of $\mathcal{C}^s$ with C. We denote its special fibre by C_r^s.

Since $\overline{\infty} \in \mathcal{C}^s$, the K-points C_0 of the generic fibre of $\mathcal{C}^s$ which reduce modulo $\mathfrak{p}$ to $\overline{\infty}$ can be identified with the K-points of the generic fibre of $\mathcal{C}$ which reduce modulo $\mathfrak{p}$ to $\overline{\infty}$. This latter set can be identified with the R-points of $\mathcal{C}$ whose x_{g+1} coordinate has unique minimal valuation, so are $\mathfrak{p}$-points on $\mathcal{D}_{g+1}$, which we identify with the $\mathfrak{p}$-points on (1). Since R is complete, the $\mathfrak{p}$-points of (1) are just those where $t \in \mathfrak{p}$. In terms of the coordinates on C', in (1) we have $x_g = 1/x$, $t = y/x^{g+1}$. So C_0 consists of the K-points of C where $t = y/x^{g+1} \in \mathfrak{p}$, which are the same as the points $P = (a, b) \in C'(K)$ where a and b are not integral. Indeed, it follows from (1) that if $v(t(P)) = r > 0$, then $v(a) = -2r$, hence from the definition of C', $v(b) = -(2g+1)r$. Furthermore, one can check that t considered in the local ring $\mathcal{O}_{C_r,\overline{\infty}}$ of C_r at $\overline{\infty}$ generates the maximal ideal. Identifying $\mathcal{O}_{C_r^s,\overline{\infty}}$ with $\mathcal{O}_{C_r,\overline{\infty}}$, since $\overline{\infty}$ is a smooth point of $\mathcal{C}^s$ over R, the completed local ring of $\mathcal{C}^s$ at $\overline{\infty}$, $\hat{\mathcal{O}}_{\mathcal{C}^s,\overline{\infty}}$, is $R[\![t]\!]$ [Liu, p. 469 Prop. 1.40 and p. 481, Exer. 1.14(c)].

Let $\mathcal{J}$ be the Néron model of J over R, which is a smooth R-scheme of finite type. Since $\mathcal{C}^s$ is smooth, the morphism ϕ on generic fibres extends to an R-morphism Φ from $\mathcal{C}^s$ to $\mathcal{J}$. We let J_r denote the special fibre of $\mathcal{J}$.

Let J_0 denote the K-points of J in the kernel of reduction of $\mathcal{J}$ modulo $\mathfrak{p}$. Since $\phi(\infty) = O$ on J, $\Phi(\overline{\infty})$ is the reduction of O modulo $\mathfrak{p}$, the origin $\overline{O}$ on J_r. Now [Liu, p. 481, Exer. 1.15(a)] gives that $\Phi(C_0) \subseteq J_0$.

Note that Φ, being a morphism of schemes over R, gives rise to an induced R-algebra homomorphism $\Phi_\sharp$ from the completed local ring $\hat{O}_{\mathcal{J},\overline{O}}$ of $\mathcal{J}$ at $\overline{O}$ to $\hat{O}_{\mathcal{C}^s,\overline{\infty}}$. Since $\mathcal{J}$ is smooth at $\overline{O}$, as above, its completed local ring at the point is isomorphic to $R[\![t_1, \ldots, t_g]\!]$ for any set of parameters $t_1, \ldots, t_g$ which vanish at O and generate the maximal ideal in $\mathcal{O}_{J_r,\overline{O}}$.

Therefore, for each $1 \leqslant i \leqslant g$, $\Phi_\sharp(t_i)$ is a power series f_i in t over R with no constant term. And by the completeness of R, for any point $P \in C_0$, $t_i(\phi(P)) = f_i(t(P))$. Therefore we have that

$$v\big(t(P)\big) \leqslant \min_{1 \leqslant i \leqslant g} v\big(f_i\big(t(P)\big)\big) = \min_{1 \leqslant i \leqslant g} v\big(t_i\big(\phi(P)\big)\big),$$

so it suffices to bound this last quantity. Since $\mathcal{J}$ is a group scheme of finite type over R, it is well known ([Liu, p. 482, Exer. 1.15(c)], or [HS, p. 271, Lemma C.2.4]), that the points of J_0 are the $\mathfrak{p}$-points of a g-dimensional commutative formal group $\mathcal{F}$ over R (whose group law is induced from that of $\mathcal{J}$, and whose parameters can be taken to be $t_1, \ldots, t_g$). Since $\mathcal{F}$ contains no torsion points of order not a power of p, this immediately gives that for $P \in C'(K)$, $\phi(P)$ torsion on J, $\phi(P)$ can only be in J_0 if it is p-power torsion. To finish the proof of (ii), we need a lemma on the valuation of p-power torsion points in formal groups over R. The following is assuredly well known, but lacking a suitable reference ($g = 1$ is in [Si]), we provide a proof.

Lemma. *Let $\overline{R}$ be the ring of integers in an algebraic closure of K, and extend v to a valuation on $\overline{R}$. Suppose $\mathcal{F}$ is a g-dimensional commutative formal group over R, given by a formal group law in parameters $t_1, \ldots, t_g$. Suppose Q is a point of order p^n in $\mathcal{F}(\overline{R})$, and $\mu_n = \min_{1 \leqslant i \leqslant g} v(t_i(Q))$. Then*

$$\mu_n \leqslant \frac{v(p)}{p^n - p^{n-1}}.$$

Proof. We prove this by induction. The base case $n = 1$ is in [Se, LG 4.26, Thm. 4]. It is shown in [Se, LG 4.19] that the multiplication-by-p map $[p]_{\mathcal{F}}$ of $\mathcal{F}$ consists of g power series, for $1 \leqslant i \leqslant g$, of the form

$$pt_i + p\big(d^\circ \geqslant 2\big) + \big(d^\circ \geqslant p\big),$$

where $(d^\circ \geqslant m)$ denotes a power series in $t_1, \ldots, t_g$ with coefficients in R, all of whose terms have total degree at least m. If $n > 1$, then $[p]_{\mathcal{F}} Q \neq O$, so has some coordinate t_i at which it has minimal valuation μ_{n-1}. The valuation of the term on the left hand side of

$$t_i\big([p]_{\mathcal{F}} Q\big) = p t_i(Q) + p\big(d^\circ \geqslant 2\big)(Q) + \big(d^\circ \geqslant p\big)(Q),$$

cannot be less than the valuation of every term on the right hand side. Hence assuming the result for $n-1$ gives $\mu_{n-1} \leqslant v(p)$, so we must have

$$\mu_{n-1} \geqslant p\mu_n,$$

which establishes the inductive step of the proof of the lemma. □

Noting that the valuation of $t(P)$ is an integer finishes the proof of part (ii) of Theorem 1. □

We can now use this result to get a bound the powers of the primes that divide b^2.

Theorem 2. *Let R, K, v, p, C', f, ϕ and J be as in Theorem 1, and let $e = v(p)$. Suppose that $e < \max(p-1, 2)$. If (a, b) are the (x, y)-coordinates of a point P in $C'(K)$, and $\phi(P)$ is torsion on J, then*:

(i) *a, b are in R, and*
(ii) *either $b = 0$ or $b^2 | \Delta(f)$.*

Proof. If $\phi(a, b)$ is 2-torsion, $b = 0$ and a is integral over R, hence in R. Now suppose $\phi(a, b)$ is n-torsion for some $n > 2$. Then Theorem 1 gives us that a and b are in R if n is not a p-power. But even if $n = p^m > 2$, the hypothesis that $e < p-1$ for p odd gives us that $\lfloor v(p)/(p^m - p^{m-1}) \rfloor$ is 0, and that if $p = 2$, $e = 1$ and $m \geqslant 2$, so $\lfloor v(p)/(p^m - p^{m-1}) \rfloor$ is also 0. So (i) holds in any case.

To prove (ii), let L be the splitting field of f, and suppose f factors into a product of monic irreducibles $\prod f_i$ over K. Let ρ be a root of f_i in L for some i. It suffices to prove that for any such ρ,

$$a - \rho | f'(\rho), \tag{3}$$

since taking the product of (3) over all ρ gives $b^2 | \Delta(f)$. We note that (3) is trivial if the degree d of f_i is greater than 1. Indeed, then there is an element s in the Galois group of L over K such that $s(\rho) \neq \rho$. Suppose then that $v(a - \rho) = \ell$ for some $\ell > 0$. Then $v(a - s(\rho)) = \ell$ too, so subtracting we get $v(\rho - s(\rho)) \geqslant \ell$. Since $\rho - s(\rho)$ is a factor of $f_i'(\rho)$, we have that $a - \rho | f_i'(\rho) | f'(\rho)$ (since $f'(\rho) = f_i'(\rho) \prod_{j \neq i} f_j(\rho)$) as claimed.

Now suppose that $d = 1$, and $f_i = x - \rho$ for some ρ in R.

Then we can rewrite C' as

$$y^2 = (x-\rho)^{2g+1} + \cdots + f'(\rho)(x-\rho),$$

and dividing by $(x-\rho)^{2g+2}$ and multiplying by $f'(\rho)^{2g}$, we get an affine model C'' for C of the form

$$w^2 = f'(\rho)^{2g-1} u + \cdots + u^{2g+1} \in R[u],$$

by taking $w = f'(\rho)^g y/(x-\rho)^{g+1}$, $u = f'(\rho)/x - \rho$. The Abel–Jacobi map ϕ_ρ for C'' that sends the point at infinity on $C - C''$ to the origin on J is the translate of ϕ by $\phi(\rho, 0)$, a 2-torsion point. Hence $\phi_\rho(a, b)$ is still a torsion point. Applying (i) to C'', we have $f'(\rho)/(a-\rho)$ in R, so (3) holds in this case as well. □

Remarks. (1) For general e and $(a,b) \in C'(K)$, if $\phi(a,b)$ is a torsion point and $a, b \in R$, the proof shows that $\Delta(f)/b^2$ can be expressed as an element in R times the product of $f'(\rho)/(a-\rho)$ over the roots ρ of f in K. If $\phi_\rho(a,b)$ is not p-power torsion, $f'(\rho)/(a-\rho)$ is in R. If $\phi_\rho(a,b)$ is p^n-torsion, then $f'(\rho)/(a-\rho)$ has valuation bounded below by $-2\lfloor v(p)/(p^n - p^{n-1})\rfloor$. Moreover, if $p \neq 2$, at most one such $\phi_\rho(a,b)$ can be p-power torsion, and if $\phi_\rho(a,b)$ is p^n-torsion, then $\phi(a,b)$ is not. So we can conclude that if $(a,b) \in C'(K)$ and $\phi(a,b)$ is a torsion point, then:

(i) If $a, b \in R$, and $\phi(a,b)$ is not of order twice a p-power, then b^2 divides $\Delta(f)$.
(ii) If $p \neq 2$, and $\phi(a,b)$ is of order $2p^n$, then $a, b \in R$, and the valuation of $\Delta(f)/b^2$ is bounded below by $-2\lfloor v(p)/(p^n - p^{n-1})\rfloor$.
(iii) If $\phi(a,b)$ is not p-power torsion, then $a, b \in R$, and if in addition $\phi(a,b)$ is not of order twice a p-power, then b^2 divides $\Delta(f)$.

(2) We apply Theorem 2 to curves over a number field F by applying it over all the non-archimedean completions $F_{\mathfrak{p}}$ of F. The hypotheses of Theorem 2 hold for all but finitely-many $\mathfrak{p}$. It would be interesting to see if a global result like Zimmer's [Z] holds in the case $g > 1$.

The following comes directly from Theorem 2 since $e = 1$ for every p in $\mathbb{Z}$.

Theorem 3. *Suppose that*

$$y^2 = f(x) = x^{2g+1} + b_1 x^{2g} + \cdots + b_{2g} x + b_{2g+1}, \quad b_i \in \mathbb{Z},$$

defines an affine piece C' of a projective non-singular curve C over $\mathbb{Q}$ of genus $g \geqslant 1$. Let $\infty \in C(\mathbb{Q})$ denote the point at infinity of this model (i.e., $\infty = C - C'$). Let J be the Jacobian of C, and ϕ the Abel–Jacobi map that takes any $P \in C$ to the divisor class of $P - \infty$ in J. If $P = (a,b)$ are the (x,y)-coordinates of a point in $C'(\mathbb{Q})$, and $\phi(P)$ is torsion in J, then $a, b \in \mathbb{Z}$, and either $b = 0$ or $b^2 | \Delta(f)$.

Acknowledgments

The author would like to thank Concordia University in Montreal and the University of Texas at Austin, whose hospitality he was enjoying while this paper was being written, and his colleague Sebastian Casalaina-Martin for several helpful comments.

References

[An] G. Anderson, Abeliants and their application to an elementary construction of Jacobians, Adv. Math. 172 (2002) 169–205.
[Ar] J. Arledge, S-units attached to genus 3 hyperelliptic curves, J. Number Theory 63 (1997) 12–29.
[BIR] M. Baker, S. Ih, R. Rumely, A finiteness property of torsion points, Algebra Number Theory 2 (2008) 217–248.
[BB] J. Boxall, E. Bavencoffe, Quelques propriétés arithmétiques des points de 3-division de la jacobienne de $y^2 = x^5 - 1$, Sém. Théor. Nombres Bordeaux (2) 4 (1992) 113–128.
[B] A. Buium, An approximation property for Teichmüller points, Math. Res. Lett. 3 (1996) 453–457.
[C] J.W.S. Cassels, A note on the division values of $\wp(u)$, Math. Proc. Cambridge Philos. Soc. 45 (1949) 167–172.
[FS] E.V. Flynn, N. Smart, Canonical heights on the Jacobians of curves of genus 2 and the infinite descent, Acta Arith. 79 (1997) 333–352.
[FK] T. Fukuda, K. Komatsu, On a unit group generated by special values of Siegel modular functions, Math. Comp. 69 (2000) 1207–1212.
[FKN] T. Fukuda, N. Kanayama, K. Komatsu, Prime divisors of special values of theta functions in the ray class field of a certain quartic field modulo 2^n, Math. Proc. Cambridge Philos. Soc. 141 (2006) 1–13.
[GL] E.Z. Goren, K. Lauter, Class invariants for quartic CM fields, Ann. Inst. Fourier 57 (2007) 457–480.
[G1] D. Grant, Units from 3- and 4-torsion on Jacobians of curves of genus two, Compos. Math. 94 (1994) 311–320.
[G2] D. Grant, Units from 5-torsion on the Jacobian of $y^2 = x^5 + 1/4$ and the conjectures of Stark and Rubin, J. Number Theory 77 (1999) 227–251.
[GI] D. Grant, S. Ih, Integral division points on curves, preprint.
[H] D. Hayes, Elliptic units in function fields, in: Number Theory Related to Fermat's Last Theorem, Birkhäuser, Boston, 1982, pp. 321–340.

[HS] M. Hindry, J. Silverman, Diophantine Geometry. An Introduction, Grad. Texts in Math., vol. 201, Springer-Verlag, New York, 2000.
[Liu] Q. Liu, Algebraic Geometry and Arithmetic Curves, Oxford University Press, Oxford, 2002.
[Lu] E. Lutz, Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic, J. Reine Angew. Math. 177 (1937) 431–466.
[N] T. Nagell, Solution de quelque problémès dans la theorie arithmétique des cubiques planes du premier genre, Wid. Akad. Skrifter Oslo I (1) (1935).
[R] M. Raynaud, Courbes sur une variété abélienne et points de torsion, Invent. Math. 71 (1983) 207–233.
[Sc] T. Scanlon, The conjecture of Tate and Voloch on p-adic proximity to torsion, Int. Math. Res. Not. IMRN 17 (1999) 909–914.
[Se] J.-P. Serre, Lie Algebras and Lie Groups, Lecture Notes in Math., vol. 1500, Springer-Verlag, Berlin, 2006.
[Si] J. Silverman, The Arithmetic of Elliptic Curves, second ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009.
[ST] J. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York, 1992.
[TV] J. Tate, J.F. Voloch, Linear forms in p-adic roots of unity, Int. Math. Res. Not. IMRN 12 (1996) 589–601.
[T] P. Tzermias, The Manin–Mumford conjecture: A brief survey, Bull. Lond. Math. Soc. 32 (1999) 641–652.
[V] J.F. Voloch, Integrality of torsion points on abelian varieties over p-adic fields, Math. Res. Lett. 3 (1996) 787–791.
[Z] H. Zimmer, Points of finite order on elliptic curves over number fields, Arch. Math. (Basel) 27 (1976) 596–603.