Werk

Titel: Lower Bounds for Heights on Elliptic Curves.

Autor: Anderson, M.; Masser, David W.

Jahr: 1980

PURL: https://resolver.sub.uni-goettingen.de/purl?266833020_0174|log9

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Math. Z. 174, 23–34 (1980)

Mathematische Zeitschrift
© by Springer-Verlag 1980

Lower Bounds for Heights on Elliptic Curves

M. Anderson and David W. Masser

Department of Mathematics, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom

1. Introduction

Let α be an algebraic number of degree $d \geqq 1$, let $\alpha_1, \ldots, \alpha_d$ be its conjugates, and write temporarily

$$M(\alpha) = \prod_{i=1}^{d} \max(1, |\alpha_i|). \tag{1}$$

It is well-known that when α is an algebraic integer but not a root of unity, we have $M(\alpha) > 1$. It then becomes of interest to obtain estimates of the form

$$M(\alpha) \geqq 1 + f(d), \tag{2}$$

where $f(d)$ is a positive function of d. Such inequalities are useful in transcendence theory and related areas (see for example [13] and [15]). The first author in his thesis [2] recently proved a natural analogue of (2) for elliptic curves with complex multiplication. This too has applications in transcendence theory (see [1] and [4] as well as [2]), and it may also be useful in other problems on elliptic curves (see for example Manin's discussion of the Mordell-Weil group in [10]). Our purpose in this paper is to improve the result of [2] and generalize it to elliptic curves without complex multiplication.

Before we explain the elliptic analogue, it is helpful to reformulate the classical results for $M(\alpha)$. If F is an algebraic number field containing α we write

$$H_F(\alpha) = \prod_{v} \max(1, |\alpha|_v), \tag{3}$$

where v runs over all valuations of F normalized in the usual way to satisfy the product formula $\prod_v |\alpha|_v = 1$ for $\alpha \neq 0$. More precisely, for each embedding σ of F into the complex field $\mathbb{C}$ there is an archimedean valuation v defined by $|\alpha|_v = |\sigma(\alpha)|$, and for each prime ideal $\mathfrak{p}$ of F with absolute norm $N\mathfrak{p}$ there is a non-archimedean valuation v defined by $|\alpha|_v = (N\mathfrak{p})^{-m}$, where $\mathfrak{p}^m$ is the exact power of $\mathfrak{p}$ in the fractional principal ideal of F generated by α. If F is of degree

0025-5874/80/0174/0023/$02.40

N over the rational field $\mathbb{Q}$, the number

$$H(\alpha)=(H_F(\alpha))^{1/N} \tag{4}$$

is independent of F, and we shall call $H(\alpha)$ the absolute height of α. We also define the logarithmic absolute height $h(\alpha)$ by

$$h(\alpha)=\log H(\alpha). \tag{5}$$

Note that if α is an algebraic integer, then $|\alpha|_v \leqq 1$ for all non-archimedean v, and so $h(\alpha)=d^{-1}\log M(\alpha)$; otherwise $|\alpha|_v \geqq 2$ for some non-archimedean v, and thus $h(\alpha)\geqq d^{-1}\log 2$. Note also that if (2) holds, then by taking $\alpha=2^{1/d}$ we deduce $f(d)\leqq 1$. It follows easily that the validity of (2) for all algebraic integers α except roots of unity is equivalent to the inequality

$$h(\alpha)\geqq d^{-1}\log(1+f(d)) \tag{6}$$

for all algebraic numbers α except roots of unity. Henceforth we shall refer only to (6).

For convenience suppose $d\leqq D$ for some $D\geqq 3$. Until quite recently the best known version of (6) was of the form

$$h(\alpha)\geqq c_1 D^{-2}(\log D)^{-1} \tag{7}$$

for an absolute constant $c_1>0$; this was proved by Blanksby and Montgomery [5]. In [16] Stewart found a different proof of (7) using techniques associated with transcendence theory. Very recently Dobrowolski [6] has developed Stewart's method to prove that

$$h(\alpha)\geqq c_2 D^{-1}(\log D/\log\log D)^{-3} \tag{8}$$

for some absolute constant $c_2>0$. Lehmer's question [9] amounts in this context to asking whether $h(\alpha)\geqq c_3 D^{-1}$ for some absolute constant $c_3>0$; if this is true, it would be best possible, as the example $h(2^{1/D})=D^{-1}\log 2$ shows.

Now let $\mathbb{C}^\times$ denote the multiplicative group of all non-zero complex numbers. We regard h as a height function on the subgroup of algebraic points of $\mathbb{C}^\times$; that is, the group of all non-zero algebraic numbers. It reflects the group structure by the identity

$$h(\alpha^m)=mh(\alpha) \tag{9}$$

for any positive integer m. In fact (9) holds for all integers m by virtue of the product formula. Moreover, h vanishes exactly at the torsion points of $\mathbb{C}^\times$.

The elliptic analogue of all this comes about by replacing the multiplicative group $\mathbb{C}^\times$ by the additive group represented by an elliptic curve $\mathscr{E}$ defined over an algebraic number field. We take $\mathscr{E}$ as the set of solutions of the equation

$$y^2=4x^3-g_2x-g_3 \tag{10}$$

for fixed algebraic numbers g_2, g_3 with $g_2^3\neq 27g_3^2$, and we add the point at infinity O. An algebraic point P on $\mathscr{E}$ is either O or a point on (10) with

algebraic coordinates x, y. Since the work of Néron [14] and Tate, it is known that a more or less canonical height function $\hat{h}$ can be defined on the subgroup of algebraic points of $\mathscr{E}$. It satisfies

$$\hat{h}(mP) = m^2 \hat{h}(P) \tag{11}$$

for all integers m, and it vanishes exactly at the torsion points of $\mathscr{E}$. We construct $\hat{h}$ as follows. For an algebraic point P on (10) given by $x=\alpha$, $y=\beta$, and an algebraic number field F containing α and β, write

$$H_F(P) = \prod_v \max(1, |\alpha|_v, |\beta|_v), \tag{12}$$

where v runs over all normalized valuations of F. As before, if $N=[F:\mathbb{Q}]$, the number

$$H(P) = (H_F(P))^{1/N} \tag{13}$$

is independent of F, and we put

$$h(P) = \log H(P). \tag{14}$$

Define also $h(O)=0$. It can then be shown that the limit

$$\hat{h}(P) = \lim_{m\to\infty} m^{-2} h(mP)$$

exists and has the properties stated. Moreover, there is a constant κ, depending only on g_2 and g_3, such that

$$|\hat{h}(P) - h(P)| \leqq \kappa \tag{15}$$

for all algebraic points P. A thorough exposition can be found in Chapter IV of Lang's book [8].

For an algebraic point P on (10) given by $x=\alpha$, $y=\beta$, we define the degree $d(P)$ of P as the index

$$d(P) = [\mathbb{Q}(g_2, g_3, \alpha, \beta) : \mathbb{Q}(g_2, g_3)]. \tag{16}$$

The main results of this paper are as follows.

Theorem. *There is a constant $\gamma > 0$ depending only on g_2 and g_3 such that for any non-torsion algebraic point P on $\mathscr{E}$ with degree at most $D \geqq 3$ we have*

$$\hat{h}(P) \geqq \gamma D^{-10} (\log D)^{-6}.$$

If further $\mathscr{E}$ has complex multiplication we have

$$\hat{h}(P) \geqq \gamma D^{-3} (\log D)^{-2}.$$

It might now be asked, by analogy with Lehmer's question, whether the Theorem holds with $\hat{h}(P) \geqq \gamma D^{-1}$. Again this would be best possible, as the following argument shows. Let Q be a fixed non-torsion algebraic point of $\mathscr{E}$, and for $m \geqq 1$ let P_m be such that $mP_m = Q$. Then $d(P_m) \leqq c_4 m^2$ for some c_4 independent of m (see for example [11] Lemma 6.4). Hence for all sufficiently

large D there is an integer m with $d(P_m) \leqq D$ and $m \geqq c_5 D^{1/2}$ for $c_5 > 0$ independent of D. So by (11) we have $\hat{h}(P_m) \leqq c_6 D^{-1}$ for some c_6 independent of D.

In [2] the first author showed that $\hat{h}(P) \geqq \gamma D^{-4} (\log D)^{-3}$ in the case of complex multiplication. He used an elaboration of Stewart's method [16]. The proof of our Theorem runs on similar lines, but with some substantial simplifications in the argument which make it much closer to Stewart's original proof.

2. Preliminary Lemmas

The following simple result shows the superiority of the height function $H(\alpha)$ over more traditional heights used in transcendence theory.

Lemma 1. *Let $P(x_1, \ldots, x_m)$ be a polynomial of degree at most $L_k \geqq 1$ in x_k $(1 \leqq k \leqq m)$, whose coefficients are rational integers of absolute values at most $U \geqq 1$. Let $\alpha_1, \ldots, \alpha_m$ be algebraic numbers with α_k of absolute height at most $H_k \geqq 1$ $(1 \leqq k \leqq m)$. Then the absolute height of $P(\alpha_1, \ldots, \alpha_m)$ is at most*

$$U \prod_{k=1}^{m} (L_k + 1) H_k^{L_k}.$$

Proof. Let F be an algebraic number field of degree N containing $\alpha_1, \ldots, \alpha_m$. For each valuation v of F we have

$$\max(1, |P(\alpha_1, \ldots, \alpha_m)|_v) \leqq C_v \prod_{k=1}^{m} (\max(1, |\alpha_k|_v))^{L_k}, \tag{17}$$

where

$$C_v = U \prod_{k=1}^{m} (L_k + 1)$$

if v is archimedean and $C_v = 1$ otherwise. Now Lemma 1 follows on multiplying together all the Eqs. (17) and taking the Nth root.

The next result is a version of Siegel's form of the Box Principle for solving linear equations. It is a straightforward extension of Lemma 4 of [13]. In order not to spend too much time on preliminaries we shall deduce it from a more general Proposition which we state and prove in an Appendix.

Lemma 2. *Let F be an algebraic number field of degree N, and let R, S be positive integers with $S \geqq 2NR$. For $1 \leqq s \leqq S$ let $P_s(x_1, \ldots, x_m)$ be polynomials of degree at most $L_k \geqq 1$ in x_k $(1 \leqq k \leqq m)$ whose coefficients are rational integers of absolute values at most $U \geqq 1$. For $1 \leqq r \leqq R$ let $\alpha_1^{(r)}, \ldots, \alpha_m^{(r)}$ be elements of F with $\alpha_k^{(r)}$ of absolute height at most $H_k \geqq 1$ $(1 \leqq k \leqq m)$. Then there exist rational integers $x_1, \ldots, x_S$, not all zero, with absolute values at most*

$$SU \prod_{k=1}^{m} (L_k + 1) H_k^{L_k},$$

such that

$$\sum_{s=1}^{S} P_s(\alpha_1^{(r)}, \ldots, \alpha_m^{(r)}) x_s = 0 \qquad (1 \leqq r \leqq R).$$

Proof. We only have to estimate the projective absolute heights (see Appendix) of the forms occurring in the lemma. As in (17), we have

$$|P_s(\alpha_1^{(r)}, \ldots, \alpha_m^{(r)})|_v \leqq C_v \prod_{k=1}^{m} (\max(1, |\alpha_k^{(r)}|_v)^{L_k} \quad (1 \leqq r \leqq R,\ 1 \leqq s \leqq S)$$

for any valuation v of F, where C_v is exactly as before. It follows as in the proof of Lemma 1 that the absolute projective heights are all at most

$$U \prod_{k=1}^{m} (L_k+1) H_k^{L_k},$$

and Lemma 2 follows at once from the Proposition.

For the main proof we shall use the Weierstrass elliptic function $\wp(z)$ determined by the differential equation

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2 \wp(z) - g_3. \tag{18}$$

Let $\sigma(z)$ denote the associated Weierstrass sigma function. For the remaining two lemmas of this section we do not need to suppose that g_2 and g_3 are algebraic numbers.

Lemma 3. *Suppose w is a complex number, not a pole of $\wp(z)$, such that $|w| \leqq W$ and $|\wp(w)| \leqq X$ for some $W \geqq 1$ and $X \geqq 1$. Then*

$$|\sigma(w)|^2 \geqq X^{-1} c^{-W^2}$$

for some constant $c > 1$ depending only on g_2 and g_3.

Proof. Let $\mathscr{R}$ be a fixed compact set containing a complete period parallelogram of $\wp(z)$. There exists w_0 in $\mathscr{R}$ congruent to w modulo the period lattice, and we have $|\sigma(w_0)| \geqq c_1^{-W^2} |\sigma(w)|$ by well-known estimates (e.g. [11], p. 78), where $c_1 > 0$ depends only on g_2 and g_3. The functions $g(z) = (\sigma(z))^2$, $f(z) = (\sigma(z))^2 \wp(z)$ are analytic on $\mathscr{R}$ and have no common zeroes; hence the continuous function $\mu(z) = \max(|f(z)|, |g(z)|)$ satisfies $\mu(z) \geqq c_2$ on $\mathscr{R}$ for some $c_2 > 0$ depending only on g_2 and g_3. Thus $\mu(w_0) \geqq c_2$, and since $\wp(w_0) = \wp(w)$, the estimate of Lemma 3 follows at once.

Lemma 4. *Suppose $P(z, x)$ is a non-zero polynomial of degree at most $L \geqq 1$ in z and of degree at most $M \geqq 1$ in x. Then for any $Z \geqq 0$ the function $P(z, \wp(z))$ cannot have more than $c(LM + MZ^2)$ zeroes in the disc $|z| \leqq Z$, where c depends only on g_2 and g_3.*

Proof. This result is a special case of the zero-estimates proved as Lemmas 8 and 9 of [12]; see in particular p. 72 of [12]. We take $n = 1$, $f_1(z) = \wp(z)$, and $\theta(z) = (\sigma(z))^2$. Note that for $n = 1$ the proofs can be made quite elementary by careful use of the Lagrange interpolation formula (cf. Lemma 3 of [1]).

3. Proof of the Theorem

Let $\mathscr{E}$ be the elliptic curve defined by (10), and for an integer $D \geqq 3$ let P be a non-torsion algebraic point on $\mathscr{E}$ with $d(P) \leqq D$. We assume that $\hat{h}(P)$ has its

minimum value η, where η satisfies

$$\eta^{-1} \geqq C^{30} D^{10} (\log D)^6. \tag{19}$$

for some positive constant C depending only on g_2 and g_3. We shall prove the first part of the Theorem by deducing a contradiction from (19) if C is sufficiently large. At the end of this section we shall briefly indicate how the argument is modified in the case of complex multiplication.

Let $\wp(z)$ be the Weierstrass function satisfying (18), and let u be any complex number such that P has coordinates $x=\wp(u)$, $y=\wp'(u)$ on (10). For the rest of this section we write $c, c_1, c_2, \ldots$ for positive constants depending only on g_2 and g_3, and we assume $C \leqq c$ is sufficiently large for the validity of the subsequent estimates. Let

$$B = C^{10} D^3 (\log D)^2. \tag{20}$$

Lemma 5. *There exists an integer b with $1 \leqq b \leqq B$, and a period ω of $\wp(z)$, such that $v = bu - \omega$ satisfies*

$$0 < |v| \leqq c_1 B^{-1/2}. \tag{21}$$

Proof. This is a straightforward application of the Box Principle, provided we note that since P is not a torsion point, we have $bu \neq \omega$ for any integer $b \neq 0$ and any period ω of $\wp(z)$.

Next, let $F = \mathbb{Q}(g_2, g_3, \wp(u))$, and suppose $[F:\mathbb{Q}] = N$. Then by (16) we have $N \leqq c_2 D$. We can construct a basis of F over $\mathbb{Q}$ consisting of monomials $g_2^i g_3^j (\wp(u))^k$ for non-negative integers i, j, k not exceeding N. Denote the elements of such a basis by $\alpha_1, \ldots, \alpha_N$. Define

$$L = [C^2 D], \qquad M = [C^2 D \log D], \qquad R = [C^3 D^2 \log D]. \tag{22}$$

Lemma 6. *There exist rational integers $p(l, m, n)$, not all zero, with absolute values at most $\exp(c_3 C^2 D \log D)$, such that the function*

$$\Phi(z) = \sum_{l=0}^{L} \sum_{m=0}^{M} \sum_{n=1}^{N} p(l, m, n) \alpha_n z^l (\wp(vz))^m$$

satisfies $\Phi(r) = 0$ for all integers r with $1 \leqq r \leqq R$.

Proof. We must solve the equations

$$\sum_{l=0}^{L} \sum_{m=0}^{M} \sum_{n=1}^{N} p(l, m, n) \alpha_n r^l \beta_r^m = 0 \qquad (1 \leqq r \leqq R) \tag{23}$$

for the unknowns $p(l, m, n)$, where

$$\beta_r = \wp(rv) = \wp(rbu). \tag{24}$$

By the multiplication formula for $\wp(z)$ (see for example [8], p. 38) these equations have coefficients in F. There are

$$R \leqq C^3 D^2 \log D$$

equations, and

$$S=(L+1)(M+1)N \geqq C^4 N D^2 \log D$$

unknowns; thus we can use Lemma 2. For $1 \leqq r \leqq R$ the coefficients of the unknowns in the rth equation (23) are monomials in the five numbers $g_2, g_3, \wp(u), r$ and β_r, of degree at most N in the first three and of degrees at most L and M in the fourth and fifth respectively. We proceed to estimate the heights of these five numbers.

Firstly we note that $H(g_2)$ and $H(g_3)$ are independent of D, and $H(r)=r$. Secondly, for any positive integer m we have from (11), (12) and (15)

$$H(\wp(mu)) \leqq \exp(h(mP)) \leqq \exp(\hat{h}(mP)+\kappa) = \exp(m^2\eta+\kappa). \tag{25}$$

If $m \leqq C^{15} D^5 (\log D)^3$ this is at most c_4; we deduce in particular that $H(\wp(u)) \leqq c_4$, and, since $BR \leqq C^{13} D^5 (\log D)^3$, we get from (24)

$$H(\beta_r) \leqq c_4 \qquad (1 \leqq r \leqq C^2 R). \tag{26}$$

It follows incidentally that

$$H(\alpha_n) \leqq c_5^D \qquad (1 \leqq n \leqq N). \tag{27}$$

Thus from Lemma 2 we can choose the $p(l, m, n)$ as rational integers, not all zero, of absolute values at most

$$S(N+1)^3 (L+1)(M+1) c_6^{N+M} R^L \leqq \exp(c_3 C^2 D \log D).$$

This completes the proof of Lemma 6.

Lemma 7. *There exists an integer r with $1 \leqq r \leqq C^2 R$ such that*

$$\xi = \Phi(r) \neq 0.$$

Proof. We observe that the function $\Phi(z/v)$ is of the type considered in Lemma 4, and the corresponding polynomial P is non-zero since $\alpha_1, \ldots, \alpha_N$ are linearly independent over $\mathbb{Q}$. Hence the number of zeroes of $\Phi(z/v)$ in the disc $|z| \leqq C^2 R |v|$ is at most

$$c_7(LM + C^4 M R^2 |v|^2).$$

Since

$$M R^2 B^{-1} \leqq C^{-2} D^2 \log D, \tag{28}$$

this number does not exceed

$$c_8 C^4 D^2 \log D \leqq \tfrac{1}{2} C^2 R.$$

Therefore $\Phi(z/v)$ cannot vanish at the points $z=rv$ for all integers r with $1 \leqq r \leqq C^2 R$, and this implies the lemma.

Lemma 8. *We have the estimate*

$$|(\sigma(rv))^{2M} \xi| \leqq 3^{-R}.$$

Proof. Let $g(z)=(\sigma(z))^2$ and $f(z)=(\sigma(z))^2\,\wp(z)$; then the function

$$\begin{aligned} F(z)&=(\sigma(vz))^{2M}\,\Phi(z)\\ &=\sum_{l=0}^{L}\sum_{m=0}^{M}\sum_{n=1}^{N} p(l,m,n)\,\alpha_n z^l\,(g(vz))^{M-m}\,(f(vz))^m \end{aligned} \tag{29}$$

is entire. Moreover, if

$$W(z)=\prod_{r=1}^{R}(z-r),$$

then by Lemma 6 the quotient $F(z)/W(z)$ is also entire. Now comparison of the maximum moduli on the circles $|z|=C^2R$ and $|z|=9\,C^2R$ gives in the usual way

$$|F(r)|\leqq 4^{-R}\,Y, \tag{30}$$

where Y is the maximum modulus of $F(z)$ on the latter circle. We have

$$|g(z)|\leqq c_9^{|z|^2+1},\qquad |f(z)|\leqq c_9^{|z|^2+1},$$

and therefore (29) and the estimates of Lemma 6 give

$$Y\leqq A(9\,C^2R)^L\exp(c_{10}\,C^2\,D\log D)\exp(c_{10}\,C^4MR^2\,|v|^2), \tag{31}$$

where A is an upper bound for the $|\alpha_n|$ $(1\leqq n\leqq N)$. But recalling (27) we get

$$|\alpha_n|\leqq H_F(\alpha_n)=(H(\alpha_n))^N\leqq c_{11}^{D^2}\qquad (1\leqq n\leqq N).$$

Thus from (28) we find easily that

$$Y\leqq\exp(c_{12}\,C^2\,D^2\log D),$$

and now (30) gives the required estimate for $F(r)=(\sigma(rv))^{2M}\,\xi$.

Finally we show that Lemma 7 and Lemma 8 contradict each other. We start by estimating $\sigma(rv)$. By (26) we have

$$|\wp(rv)|\leqq H_F(\beta_r)=(H(\beta_r))^N\leqq c_{13}^{D}.$$

It follows from Lemma 3 that

$$|\sigma(rv)|^2\geqq c_{14}^{-D}\exp(-c_{14}\,C^4R^2\,|v|^2).$$

Hence by (28) and Lemma 8 we get

$$|\xi|\leqq 2^{-R}. \tag{32}$$

On the other hand, the height of

$$\xi=\sum_{l=0}^{L}\sum_{m=0}^{M}\sum_{n=1}^{N} p(l,m,n)\,\alpha_n r^l\,\beta_r^m$$

can easily be estimated by Lemma 1 using (26) and the monomial expressions for $\alpha_1, \ldots, \alpha_N$; we find that

$$H(\xi) \leqq c_{15}^{N+M} (C^2 R)^L \exp(c_{15} C^2 D \log D),$$

which is at most $\exp(c_{16} C^2 D \log D)$. Since $\xi \neq 0$, the property (9) of heights shows that

$$|\xi^{-1}| \leqq H_F(\xi^{-1}) = H_F(\xi) = (H(\xi))^N.$$

Therefore

$$|\xi| \geqq \exp(-c_{17} C^2 D^2 \log D).$$

This contradicts (32), and thereby establishes the first part of the Theorem.

For the second part of the Theorem, in the case of complex multiplication, the arguments are very similar, except that we work with the full endomorphism ring E rather than the ring of rational integers. In Lemma 5 we put $B = C^4 (D \log D)^{1/2}$, and we choose an endomorphism β and a period ω such that $0 < |\beta| \leqq B$ and $v = \beta u - \omega$ satisfies $|v| \leqq c_1 B^{-1}$. In Lemma 6 we take $R = CD(\log D)^{1/2}$, and, with the same choice of L and M, we construct $\Phi(z)$ so that $\Phi(\rho) = 0$ for all endomorphisms ρ with $0 < |\rho| \leqq R$. By Lemma 4, there is an endomorphism ρ with $0 < |\rho| \leqq C^2 R$ such that $\Phi(\rho) \neq 0$. All this gives a contradiction provided we have $\eta^{-1} \geqq C^{14} D^3 (\log D)^2$ in place of (19). We leave the details of the proof to the reader.

It should perhaps be noted that both these proofs can be modified so as to avoid the appeal to Lemma 4. For the general case we can extend the range of zeroes arbitrarily far by introducing division values $\Phi(r/q)$ as in Baker's paper [3]. Note that these then lie in a field whose degree is of order Dq^2. When there is complex multiplication a similar procedure can be carried out without even using division values.

We also remark that there is no difficulty in principle in estimating the constants γ of the Theorem explicitly in terms of g_2 and g_3. The very precise inequalities for the constant κ in (15) obtained by Zimmer in [17] would be useful in this context.

In addition the methods of this paper extend to simple abelian varieties. The extension is relatively straightforward when there are many complex multiplications as in [12], but otherwise we have to use some zero-estimates of a new type. This will be the subject of a later paper.

Finally there remains the interesting problem of adapting Dobrowolski's argument [6] to prove analogues of the sharper result (8) for elliptic curves and abelian varieties.

Appendix: Solving Linear Equations

Let

$$L = L(x_1, \ldots, x_S) = \alpha_1 x_1 + \ldots + \alpha_S x_S$$

be a linear form with algebraic coefficients $\alpha_1, \ldots, \alpha_S$. For an algebraic number field F of degree N containing $\alpha_1, \ldots, \alpha_S$, and a valuation v of F we put

$$|L|_v = \max(|\alpha_1|_v, \ldots, |\alpha_S|_v).$$

We define

$$H_F(L)=\prod_v |L|_v$$

and

$$H(L)=(H_F(L))^{1/N};$$

then $H(L)$ is independent of F and we call it the projective absolute height of L. Note that if $\alpha_s \neq 0$ for some s with $1 \leqq s \leqq S$, then

$$H_F(L) \geqq \prod_v |\alpha_s|_v = 1.$$

Hence if $L \neq 0$, we have $H(L) \geqq 1$. The following result generalizes and sharpens several earlier results of the same type (but see especially the Lemma of Stewart's paper [16]).

Proposition. *Let F be an algebraic number field of degree N, and let R, S be positive integers with $\delta S \geqq (\delta+1)NR$ for some $\delta > 0$. Let $L_1(x_1, \ldots, x_S), \ldots, L_R(x_1, \ldots, x_S)$ be linear forms, with coefficients in F, whose projective absolute heights are at most $H \geqq 1$. Then there exist rational integers $x_1, \ldots, x_S$, not all zero, of absolute values at most $(SH)^\delta$, such that*

$$L_1(x_1, \ldots, x_S) = \ldots = L_R(x_1, \ldots, x_S) = 0.$$

The proof can be made rather concise once we have established the following lemma.

Lemma. *For each valuation v of F let μ_v be an element of F and let M_v be a non-negative real number such that $M_v = 1$ except for finitely many v. Put $M = \prod_v M_v$. Then there are at most $(2M^{1/N}+1)^N$ elements ξ of F such that*

$$|\xi - \mu_v|_v \leqq M_v \tag{A1}$$

for all v.

Proof of Lemma. This is suggested by some classical calculations in algebraic number theory; see for example [7], Chapter V. It is easily seen that we may assume without loss of generality that if $v, \bar{v}$ correspond to complex conjugate embeddings of F into $\mathbb{C}$, then $M_v = M_{\bar{v}}$. We may also suppose $M_v > 0$ for all v. For each archimedean v let F_v be $\mathbb{R}$ or $\mathbb{C}$ according to whether the associated embedding σ_v of F is real or complex. Choose a maximal subset V of the archimedean valuations containing no complex conjugate pairs, and let $\mathscr{F}$ be the direct product of the F_v for v in V, equipped with the product Lebesgue measure. For v in V let x_v denote the corresponding coordinate of a typical element of $\mathscr{F}$.

For each ξ in F consider the open set $\mathcal{O}(\xi)$ of $\mathscr{F}$ defined by

$$|x_v - \sigma_v(\xi)| < \tfrac{1}{2} M^{-1/N} M_v \tag{A2}$$

for all v in V. We first observe that if ξ_1, ξ_2 are elements of F satisfying (A1) and the sets $\mathcal{O}(\xi_1)$, $\mathcal{O}(\xi_2)$ overlap, then $\xi_1 = \xi_2$. For (A2) would lead to

$$|\xi_1 - \xi_2|_v = |\sigma_v(\xi_1) - \sigma_v(\xi_2)| < M^{-1/N} M_v \tag{A3}$$

for all v in V. This would then hold for all archimedean v. But also (A 1) would give

$$|\xi_1 - \xi_2|_v \leqq M_v \tag{A4}$$

for all non-archimedean v. It follows from (A 3) and (A 4) that

$$\prod_v |\xi_1 - \xi_2|_v < M^{-1} \prod_v M_v = 1.$$

Hence $\xi_1 = \xi_2$ by the product formula.

In other words, as ξ runs over all solutions of (A1) the sets $\mathcal{O}(\xi)$ are disjoint. By (A1) we have

$$|\sigma_v(\xi) - \sigma_v(\mu_v)| \leqq M_v$$

for v in V, and hence by (A2) these sets are contained in the region $\mathcal{U}$ of $\mathcal{F}$ defined by

$$|x_v - \sigma_v(\mu_v)| \leqq (1 + \tfrac{1}{2} M^{-1/N}) M_v \tag{A5}$$

for all v in V. We now compare measures. Clearly the $\mathcal{O}(\xi)$ are all translations of a set of measure $\gamma(\frac{1}{2}M^{-1/N})^N M'$, where γ depends only on F, and M' is the product of M_v taken over all archimedean v. Similarly the measure of $\mathcal{U}$ is $\gamma(1+\frac{1}{2}M^{-1/N})^N M'$. The ratio of these measures is $(2M^{1/N}+1)^N$, and this implies the lemma.

Actually it is not too hard to derive asymptotic estimates for the number of points in (A1) for large M; see Theorem 1 (p. 110) of [7]. These lead to asymptotic improvements of the Proposition.

Proof of Proposition. Let $X = [(SH)^\delta]$, and for each S-tuple $\mathbf{x} = (x_1, \ldots, x_S)$ of integers $x_1, \ldots, x_S$ with $0 \leqq x_s \leqq X$ $(1 \leqq s \leqq S)$ define an R-tuple $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_R)$ by $\lambda_r = L_r(x_1, \ldots, x_S)$ $(1 \leqq r \leqq R)$. The number of distinct vectors $\mathbf{x}$ is then $(X+1)^S$. To estimate the number of distinct vectors $\boldsymbol{\lambda}$, fix an integer r with $1 \leqq r \leqq R$, and put $\mu_v = L_r(\frac{1}{2}X, \ldots, \frac{1}{2}X)$ for v archimedean, and $\mu_v = 0$ otherwise. Then we have

$$|\lambda_r - \mu_v|_v \leqq C_v |L_r|_v,$$

where $C_v = \frac{1}{2}SX$ for v archimedean, and $C_v = 1$ otherwise. Hence by the Lemma, the number of possible values of λ_r is at most

$$(SXH(L_r)+1)^N \leqq (SH(X+1))^N.$$

It follows that the total number of possible distinct vectors $\boldsymbol{\lambda}$ is at most $(SH(X+1))^{NR}$. But we have $\delta(S-NR) \geqq NR$, and so

$$(X+1)^S = (X+1)^{S-NR}(X+1)^{NR} > (SH)^{NR}(X+1)^{NR}.$$

Hence some $\boldsymbol{\lambda}$ arises from two different values of $\mathbf{x}$, and their difference gives the required solution of the linear equations.

References

1. Anderson, M.: Inhomogeneous linear forms in algebraic points of an elliptic function. In: Transcendence theory: advances and applications (Eds. A. Baker and D.W. Masser). Proceedings of a Conference (Cambridge 1976), pp. 121–143. London-New York-San Francisco: Academic Press 1977
2. Anderson, M.: Ph. D. thesis. University of Nottingham 1978
3. Baker, A.: On the periods of the Weierstrass $\wp$-function. Symposia Mathematica **IV**, 155–174. London: Academic Press 1970
4. Bertrand, D.: Kummer theory on the product of an elliptic curve by the multiplicative group. Glasgow Math. J. (to appear)
5. Blanksby, P.E., Montgomery, H.L.: Algebraic integers near the unit circle. Acta Arith. **28**, 355–369 (1971)
6. Dobrowolski, E.: On a question of Lehmer and the number of irreducible factors of a polynomial. Acta Arith. **34**, 391–401 (1979)
7. Lang, S.: Algebraic number theory. Reading, Mass.: Addison-Wesley 1970
8. Lang, S.: Elliptic curves, diophantine analysis. Berlin-Heidelberg-New York: Springer 1978
9. Lehmer, D.H.: Factorization of certain cyclotomic functions. Ann. of Math. **34**, 461–479 (1933)
10. Manin, Ju.I.: Cyclotomic fields and modular curves. Uspehi Mat. Nauk **26**, 7–71 (1971) [Russ.]. Engl. Transl.: Russian Math. Surveys **26**, 7–78 (1971)
11. Masser, D.W.: Elliptic functions and transcendence. Lecture Notes in Mathematics **437**. Berlin-Heidelberg-New York: Springer 1975
12. Masser, D.W.: Diophantine approximation and lattices with complex multiplication. Invent. Math. **45**, 61–82 (1978)
13. Mignotte, M., Waldschmidt, M.: Linear forms in two logarithms and Schneider's method. Math. Ann. **231**, 241–267 (1978)
14. Néron, A.: Quasi-fonctions et hauteurs sur les variétés abéliennes. Ann. of Math. **82**, 249–331 (1965)
15. van der Poorten, A.J., Loxton, J.H.: Multiplicative relations in number fields. Bull. Austral. Math. Soc. **16**, 83–98 (1977); corrigendum and addendum, Bull. Austral. Math. Soc **17**, 151–155 (1977)
16. Stewart, C.L.: Algebraic integers whose conjugates lie near the unit circle. Bull. Soc. Math. France **106**, 169–176 (1978)
17. Zimmer, H.G.: On the difference of the Weil height and the Néron-Tate height. Math. Z. **147**, 35–51 (1976)

Received November 13, 1979