Generalization of Manin's Conditional Algorithm

by Horst G. Zimmer

Fachbereich 9 Mathematik
Universität des Saarlandes
D-6600 Saarbrücken, Fed. Rep. Germany

1. Introduction and Manin's theorem

In a lecture [16] delivered at the conference on "Utilisation des calculateurs en mathématiques pures" in France, we developed some ideas regarding the implementation of Manin's conditional algorithm [7] for computing the rank and a basis of the group of rational points on an elliptic curve C over the rationals $\mathbb{Q}$. The aim of the present paper is to discuss to which extent this algorithm can be generalized to elliptic curves C defined over an arbitrary finite-algebraic number field K. Furthermore, certain problems concerning the implementation of the generalized algorithm will be treated. Some results obtained in this connection seem to be also per se of interest. In an appendix we shall give complete proofs of the assertions made in sections 1,4, and 6.

Let C denote an elliptic curve in Weierstrass normal form

$$Y^2 = X^3 + aX + b$$

with coefficients a,b in an algebraic number field K of finite degree $n=[K:\mathbb{Q}]$ over $\mathbb{Q}$. The nonzero discriminant of C is $\Delta = 4a^3+27b^2$. Without loss of generality, the coefficients a,b and thus the discriminant Δ may be assumed to be integers in K. By the Mordell-Weil theorem, the additive abelian group C_K of rational points of C over K is finitely generated. Hence this group can be written as a direct sum

$$C_K = \tilde{C}_K \oplus \hat{C}_K$$

of the finite subgroup $\tilde{C}_K$ of all torsion points (points of finite order) in C_K and a maximal free subgroup $\hat{C}_K$ of C_K of finite rank. The number r of basis elements of $\hat{C}_K$ is called the rank of the elliptic curve C over K. Manin's conditional algorithm consists in determining first the torsion subgroup $\tilde{C}_K$ of C_K and second a maximal free subgroup

$$\hat{C}_K \cong C_K/\tilde{C}_K \text{ of } C_K$$

in terms of a basis. Of course, this yields at the same time the rank r of C over K. The conditions on which the algorithm depends are the truth of the conjecture of Birch and Swinnerton-Dyer [7,1o] and the feasibility of estimating the L-series L(C,s) of C over K and its derivatives $L^{(i)}(C,s)$ at s=1, where i ranges from 1 through a certain positive integer r' (see [7] and Manin's theorem below). The latter condition is satisfied in the case K=$\mathbb{Q}$ provided that the Weil conjecture is true (see [7,11]).

Before stating Manin's theorem on which the algorithm is based we have to introduce some notation and recall certain facts.

Let us begin with defining the Néron-Tate height $\hat{h}$ on C_K which is an important tool in the algorithm. To this end we shall use an auxiliary function d on

C_K. The function d is the natural generalization of a corresponding function introduced in [16] for defining $\hat{h}$ in the special case $K=\mathbb{Q}$. For a point $P=(\xi,\eta)$ in C_K, the (affine) coordinates $\xi,\eta \in K$ can be written in the shape

$$\xi = \frac{x}{z^2} \text{ and } \eta = \frac{y}{z^3} ,$$

where x,y, and z are some integers in K. If ξ and η are both nonzero the integers x,y, and z are all nonzero and can moreover be chosen in such a way that the g.c.d.'s of x,z^2 and y,z^3 (as divisors of K) are

$$(x,z^2)=c^2 \text{ and } (y,z^3)=c^3$$

with an integral divisor c of K belonging to a fixed system V of representatives of the (finitely many) divisor classes of K. The divisors c will in fact be chosen in such a way that their norms are bounded by the Minkowski bound B (see [4,12,13] and appendix for details).

In what follows log will always denote the logarithm to a fixed base.

We now define the function d on C_K by setting

$$d(P)=\frac{3}{2n} \log \prod_{\nu=1}^{n} \max \{ \sqrt[2]{|a^{(\nu)}|}\, |z^{(\nu)}|^2 ,$$

$$\sqrt[3]{|b^{(\nu)}|}\, |z^{(\nu)}|^2, |x^{(\nu)}| \} \text{ for } P \in C_K ,$$

where $a^{(\nu)}$, $b^{(\nu)}$, $x^{(\nu)}$, and $z^{(\nu)}$ designate the images of a,b,x, and z under the $n = [K:\mathbb{Q}]$ distinct embeddings

$$K \xrightarrow{\cong} K^{(\nu)} \subseteq \mathbb{C} \quad (\nu=1,2,\ldots,n)$$

of the field K into the complex numbers $\mathbb{C}$ and $|\ldots|$ denotes ordinary absolute value on $\mathbb{C}$. This definition can also be used if $\xi=0$ by simply choosing x=0, z=1. If $P=0=(\infty,\infty)$ is the neutral element of the addition in C_K, we set d(P)=0. Notice that the function d arises from the usual Weil height h on C_K by only a slight modification [3,8,14]. We call d therefore the <u>modified Weil height</u> on C_K. The <u>Néron-Tate height</u> $\hat{h}$ on C_K is now defined by putting

$$\hat{h}(P) = \lim_{m\to\infty} \frac{d(2^m P)}{2^{2m}} \text{ for } P \in C_K .$$

The function $\hat{h}$ gives rise to a symmetric bilinear form g on $C_K \times C_K$ via [8]

$$g(P,Q)=\frac{1}{2} \{\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)\} \text{ for } (P,Q) \in C_K \times C_K .$$

By means of the bilinear form g we define the <u>determinant</u> of the elliptic curve C over K as the quantity

$$H=|\det(g(P_i,P_j))|_{i,j=1,\ldots,r} ,$$

where the points $P_1,\ldots P_r$ are a basis of a maximal free subgroup $\hat{C}_K$ of C_K. The determinant H clearly does not depend on the choice of the group $\hat{C}_K$ and the points $P_1,\ldots,P_r$ in $\hat{C}_K$ since any other choice just amounts to applying a unimodular transformation of determinant ± 1 to the points $P_1,\ldots,P_r$ originally chosen.

We need furthermore a lower bound h' for the values of the Néron-Tate height $\hat{h}$ on the set $C_K \setminus \tilde{C}_K$ (the complementary set to $\tilde{C}_K$ in C_K), that is, a real number h' such that

$$0<h' \le \min \{\hat{h}(P);\ P \in C_K \setminus \tilde{C}_K\} .$$

Finally, the deviation of the modified Weil height d from the Néron-Tate height $\hat{h}$ on C_K plays a significant role in Manin's theorem.

Let δ denote an upper bound for this deviation such that we have

$$|d(P)-\hat{h}(P)| \le \delta \quad \text{for } P \in C_K .$$

It is for the sake of keeping the bound δ as small as possible and making the function $\hat{h}$ easily computable that we have chosen the above modified Weil height d instead of the usual Weil height h for defining the Néron-Tate height $\hat{h}$ on C_K.

Manin's theorem assumes exactly the same shape as in the special case $K=\mathbb{Q}$ (see [7,16]), though the constants involved become somewhat more complicated.

Theorem (Manin [7,16]).

Suppose that $r' \in \mathbb{Z}$ and $H' \in \mathbb{R}$ are upper bounds for the rank r and the determinant H of the elliptic curve C over the number field K. Then, the set of points $P \in C_K \setminus \tilde{C}_K$ satisfying the inequality

$$d(P) \leq \delta + \frac{2^{2r'}}{c_{r'}^2} H'^2 \max\{1, h'^{2(1-r')}\},$$

where $c_{r'}$ stands for the volume ot the r'-dimensional unit ball in Euclidean space, generates a subgroup of index $\rho \leq r'!$ in a certain maximal free subgroup $\hat{C}_K \cong C_K/\tilde{C}_K$ of C_K.

Of course, the set of points $P \in C_K \setminus \tilde{C}_K$ mentioned in the theorem is finite since there are only finitely many points in C_K having bounded Weil height [8,14].

The proof of the theorem (see [7]) is based on the method of successive minima from geometry of numbers applied to the lattice generated by the $\mathbb{Z}$-module C_K in the r-dimensional real space $C_K \otimes_{\mathbb{Z}} \mathbb{R}$. The Néron-Tate height $\hat{h}$ is a positive definite quadratic form [7,8,14] on $C_K \otimes_{\mathbb{Z}} \mathbb{R}$ and thus defines a Euclidean norm on this space. Since the kernel of the canoncical $\mathbb{Z}$-module homomorphism $C_K \to C_K \otimes_{\mathbb{Z}} \mathbb{R}$ is precisely the torsion subgroup $\tilde{C}_K$ of C_K, we get an injective embedding of any maximal free subgroup $\hat{C}_K \cong C_K/\tilde{C}_K \hookrightarrow C_K \otimes_{\mathbb{Z}} \mathbb{R}$ and may therefore identify $\hat{C}_K$ with the lattice generated by C_K in the space $C_K \otimes_{\mathbb{Z}} \mathbb{R}$.

Manin's algorithm now consists mainly in finding, by trial and error, all points satisfying the inequality of the theorem and then deriving from this set of points a maximal free subgroup $\hat{C}_K$ of C_K in terms of a basis. This is achieved by repeated "divisions by two" and the "infinite descent" procedure known from the proof of the Mordell-Weil theorem [8]. So far the algorithm was restricted to the case $K=\mathbb{Q}$. As pointed out at the beginning, we wish to discuss here the possibilities of extending it to the general case of an arbitrary finite-algebraic number field K as ground field for the curve C. The intended discussion concerns the determination of the torsion subgroup $\tilde{C}_K$ of C_K and the computation of the constants appearing in Manin's theorem.

2. The torsion subgroup

Manin (see [9]) has shown that, for any fixed prime p, the order of the p-component of the torsion subgroup $\tilde{C}_K$ of the rational point group C_K of any elliptic curve C over K is bounded by a constant depending only on K and p. On the basis of a similar result Dem'janenko [1] established the boundedness of the order of the group $\tilde{C}_K$ itself, the bound depending only on the field K (though the effectiveness of Dem'janenko's arguments does not seem to be quite clear). Thus, in some sense, there are not too many torsion points in C_K. The actual determination of the group $\tilde{C}_K$ can be accomplished by applying the height functions d and $\hat{h}$ on C_K in combination with a generalization of the classical theorem of Nagell and Lutz. This theorem holds originally only in the special case $K=\mathbb{Q}$ but it can be generalized to an arbitrary finite-algebraic number field K as was shown in [15], theorem 2. Similarly, the strengthened version of the theorem of Nagell and Lutz used in [16] for computing $\tilde{C}_K$ if $K=\mathbb{Q}$ carries over to the general case of an arbitrary finite-algebraic number field K (see theorem 1 in [15]). Other methods have been recently developed in [2].

We shall state the generalized strengthened version of the Nagell-Lutz theorem in a form which is most appropriate for computational purposes. To this end we introduce the (formal) coefficient divisor [15]

$$m = \prod_{\mathfrak{p}} \mathfrak{p}^{\bar{\mu}_{\mathfrak{p}}}$$

of the Weierstrass equation for C by

defining, for each prime divisor (finite place) $\mathfrak{p}$ of K, a rational exponent

$$\bar{\mu}_{\mathfrak{p}} = \min \{\tfrac{1}{2} w_{\mathfrak{p}}(a), \tfrac{1}{3} w_{\mathfrak{p}}(b)\} ,$$

where $w_{\mathfrak{p}}$ denotes the normalized valuation on K belonging to $\mathfrak{p}$ such that $w_{\mathfrak{p}}(K^*)=\mathbb{Z}$. A divisibility relation $\mathfrak{m}|\gamma$ between the (formal) divisor $\mathfrak{m}$ of K and a nonzero element $\gamma \in K$ is to be understood in the usual sense that $\bar{\mu}_{\mathfrak{p}} \le w_{\mathfrak{p}}(\gamma)$ for all prime divisors $\mathfrak{p}$ of K.

Theorem.

Let $P=(\xi,\eta)$ be a point of order m in $\tilde{C}_K$. Then, the following divisibility relations hold:

$$m|\xi \ , \ m^3|\eta^2$$

if m is not an odd prime power, and

$$m p^{-\frac{2}{p-1}} |\xi \ , \ m^3 p^{-\frac{6}{p-1}} |\eta^2$$

if $m=p^{\nu}(\nu \ge 1)$ is an odd prime power, and furthermore,

$$\eta^2 | \Delta m^{-3}$$

if m is neither 2 nor twice an odd prime power, and

$$\eta=0 \quad \text{or} \quad \eta^2 | \Delta m^{-3} p^{\frac{2}{p-1}}$$

if $m=2$ or $m=2p^{\nu}(\nu \ge 1)$ is twice an odd prime power.

The proof of this theorem is to be found in [15].

The theorem, giving only a necessary condition for a point $P=(\xi,\eta)$ in C_K to be a torsion point, can be applied in combination with the height functions d and $\hat{h}$ on C_K in order to determine the finite group $\tilde{C}_K$ as follows. A point P in C_K belongs to $\tilde{C}_K$ if and only if $\hat{h}(P)=0$ (see [14]). Therefore, we conclude from section 1 that $\tilde{C}_K$ is contained in the finite set $\mathfrak{S}_K$ of all points P in C_K satisfying

$$d(P) \le \delta$$

with the real bound δ which will be explicitly given in section 4. The set $\mathfrak{S}_K$ is known from Manin's theorem. Now we determine the subset $\mathfrak{T}_K \subseteq \mathfrak{S}_K$ consisting of the zero point O and all points $P=(\xi,\eta)$ in $\mathfrak{S}_K$ which fulfill the necessary condition of the above theorem. Then we get rid of those points in $\mathfrak{T}_K$ having infinite order by checking repeatedly if $2P \in \mathfrak{T}_K$ whenever $P \in \mathfrak{T}_K$. In case $2P \notin \mathfrak{T}_K$ for some $P \in \mathfrak{T}_K$ we discard the point P from the set $\mathfrak{T}_K$. After a finite number of steps we end up with the searched group $\tilde{C}_K$.

3. Bounds for the rank

Up to now it is not known if the rank r of any elliptic curve C over a number field K is bounded by a constant depending only on K or if r can become arbitrarily large as C ranges say over a suitably chosen infinite set of elliptic curves C over K. However, for a fixed elliptic curve C over K upper bounds for r, depending on C and K, can be given.

Whereas in the special case $K=\mathbb{Q}$ treated in [16] we used a method of Tate for estimating the rank r of C over K, we shall here refer to a bound for r which was recently given by Heuss [5] in the general case of a finite-algebraic number field K as ground field for C. Instead of the assumption, made in [16], that the group $C_{\mathbb{Q}}$ contains a point of order 2, we shall here require the group C_K to contain all points of order l of the curve C for a fixed prime number l. These so-called l-division points of C are known to form a subgroup of isomorphism type $\mathbb{Z}/l \times \mathbb{Z}/l$ in the torsion group $\tilde{C}_{\bar{K}}$ of the curve C over the algebraic closure $\bar{K}$ of K. The requirement imposed on the rational point group C_K amounts to a rather severe restriction of generality. Of course, one can always shift from K to

the finite extension T of K obtained by adjoining to K the coordinates of the l-division points of C and thus shift from C_K to the rational point group C_T of C considered as an elliptic curve over T. But then one encounters the open problem as to how the rank of the curve C behaves under the shift from K to the l-division field T over K as the new ground field for C.

Now we shall state the theorem giving a bound for the rank r of the elliptic curve C over K provided that C_K contains the l-division points of C for a fixed prime number l. Let S denote the set of prime divisors $\mathfrak{p}$ of K such that either $\mathfrak{p}$ divides the prime number l or the function field F_C/K of the curve C over K has bad reduction modulo $\mathfrak{p}$. Observe that S is a finite set.

Theorem (Heuss [5].

Let C be an elliptic curve over a finite-algebraic number field K whose rational point group C_K contains the l-division points of C for a fixed prime number l. Denote by S the set defined above. Then, the rank r of C over K satisfies the inequality

$$r \leq 2\{rk_l \mathfrak{C}_S(K) + rk\ u(K) + |S|\} + 1,$$

where $rk_l \mathfrak{C}_S(K)$ and rk u(K) stand for the usual rank of the l-component of the S-class group $\mathfrak{C}_S(K)$ of K and the usual rank of the unit group u(K) of K, respectively, and |S| designates the cardinality of the set S.

Remark. Section 2 yields right away the decision as to whether or not the condition of the theorem regarding the l-division points of C is satisfied for the given elliptic curve C over the algebraic number field K. As G. Frey pointed out to the author, a similar estimate for r can be derived from the theorem of Bashmakov and Tate (see [7]) even without the restriction made in the above theorem.

It is the bound of this theorem which we propose as the choice of the number r' occurring in Manin's theorem. This bound proves to be sharper than a similar bound exhibited by Honda (see [5,6]).

4. Calculations involving the Néron-Tate height

Let us first estimate the deviation of the function d defined in section 1 from the Néron-Tate height $\hat{h}$ on the rational point group C_K. Recall that K is a finite-algebraic number field of degree $n=[K:\mathbb{Q}]$. We have $n=r_1+2r_2$, where r_1 is the number of real and $2r_2$ the number of complex embeddings of the field K into the complex numbers $\mathbb{C}$. Designate by D the discriminant of the field K. Then we have for $P \in C_K$

$$-2 \log 2 \leq d(P)-\hat{h}(P) \leq 5 \log 2+\frac{9}{2n}\mu_\infty+\frac{3}{n}\log B,$$

where the quantity μ_∞ is defined by (compare section 1 and appendix)

$$\mu_\infty = \log \prod_{\nu=1}^{n} \max\{\sqrt[2]{|a^{(\nu)}|}, \sqrt[3]{|b^{(\nu)}|}\}$$

and B denotes the Minkowski bound of K (see [4,12,13]), that is,

$$B = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|D|}\ .$$

The above estimate for the difference $d(P)-\hat{h}(P)$, where $P \in C_K$, coincides precisely with the one indicated in [16] in the special case $K=\mathbb{Q}$ because we have then n=1 and the term involving the Minkowski bound disappears. Accordingly, we choose the constant δ of Manin's theorem as

$$\delta = 5 \log 2+ \frac{9}{2n}\mu_\infty + \frac{3}{n}\log B$$

which is the adaquate generalization of the choice of δ made in [16].

The determination of a lower bound h' for the Néron-Tate height $\hat{h}$ on $C_K \setminus \tilde{C}_K$ is achieved as in [7,16]. Since

$$d(P)-\hat{h}(P) \leq \delta \quad \text{for } P \in C_K\ ,$$

it suffices to choose

$$h' = \min \{\delta, \hat{h}(P);\ P \in C_K \setminus \tilde{C}_K \text{ such that } d(P) < 2\delta\}$$

because there holds $\hat{h}(P) \geq \delta$ for all $P \in C_K$ such that $d(P) \geq 2\delta$. As pointed out in section 2, we have $\hat{h}(P) = 0$ if and only if $P \in \tilde{C}_K$. Thus

$$0 < h' \leq \min \{\hat{h}(P);\ P \in C_K \setminus \tilde{C}_K\}$$

as desired, the positivity of h' being a consequence of the facts that $\hat{h}$ is positive definite on $C_K \setminus \tilde{C}_K$ and that there are only finitely many points P in C_K satisfying $d(P) < 2\delta$ (see [8,14]).

For actually determining h', one has to approximately calculate $\hat{h}(P)$ for a finite number of points $P \in C_K \setminus \tilde{C}_K$. These points are found by trial and error as in the application of Manin's theorem. In order to approximately compute $\hat{h}(P)$ for a given point $P \in C_K \setminus \tilde{C}_K$, one can utilize the relation [14]

$$\hat{h}(P) = d(P) + \sum_{i=1}^{\infty} \frac{d(2^{i-1}P, 2^{i-1}P)}{2^{2i}}$$

in which the expressions

$$d(2^{i-1}P,\ 2^{i-1}P) = d(2^i P) - 4d(2^{i-1}P)$$

satisfy the inequalities (see appendix)

$$-15\left(\log 2 + \frac{\mu_\infty}{n}\right) - \frac{12}{n} \log B \leq d(2^{i-1}P, 2^{i-1}P)$$
$$\leq 6\left(\log 2 + \frac{\mu_\infty}{4n}\right) + \frac{3}{n} \log B.$$

Hence, the degree of accuracy in the calculation of $\hat{h}(P)$ is evident from the estimate (see appendix)

$$-\frac{5}{2^{2m}}\left(\log 2 + \frac{\mu_\infty}{n}\right) - \frac{4}{n 2^{2m}} \log B$$
$$\leq \hat{h}(P) - d(P) - \sum_{i=1}^{m} \frac{d(2^{i-1}P, 2^{i-1}P)}{2^{2i}}$$
$$\leq \frac{2}{2^{2m}}\left(\log 2 + \frac{\mu_\infty}{4n}\right) + \frac{1}{n 2^{2m}} \log B\ .$$

An approximate calculation of $\hat{h}(P)$ for all $P \in C_K \setminus \tilde{C}_K$ such that $d(P) < 2\delta$ in accordance with the above explanations leads to the corresponding approximation of the searched value h', and this approximation can be carried through to a sufficient degree of accuracy.

5. Estimation of the determinant

In this section the most critical point of the attempted generalization of Manin's algorithm is reached. Estimating the determinant H of the elliptic curve C over K means a difficult problem because H is defined by virtue of a basis of the rational point group C_K (see section 1), whereas such a basis is just to be determined by the algorithm using H. Manin [7] solved this problem in the case $K = \mathbb{Q}$ under the condition that the Weil conjecture and the Birch and Swinnerton-Dyer conjecture are true. The determinant H is closely connected with the behavior of the L-series $L(C,s)$ of C over K near $s=1$ via the conjecture of Birch and Swinnerton-Dyer (see below). But for $K = \mathbb{Q}$ the function $L(C,s)$ and its derivatives $L^{(i)}(C,s)$ for $i = 1,\ldots,r'$ can be approximately evaluated at $s=1$ via the Weil conjecture. In this way the desired estimation of H is then accomplished.

Turning to the general case of an arbitrary finite-algebraic number field K over which the curve C is defined we still can utilize the relation, supplied by the conjecture of Birch and Swinnerton-Dyer, between the determinant H of C over K and the behavior of the L-series of C over K near $s=1$. But since an analogue of the Weil conjecture is lacking (see [11]), there seems to be no comparable tool for approximately evaluating $L(C,s)$ and $L^{(i)}(C,s)$ for $i = 1,\ldots,r'$ at $s=1$ in the general case.

Let us discuss the general situation in detail.

For each prime divisor $\mathfrak{p}$ of the number field K, we define the local L-series of the elliptic curve C over K as follows. Suppose first that C has good reduction modulo $\mathfrak{p}$ such that the reduced curve $C(\mathfrak{p})=C \bmod \mathfrak{p}$ is an elliptic curve defined over the residue field $K(\mathfrak{p})$ of K with respect to $\mathfrak{p}$. Recall that the norm $\mathfrak{N}\mathfrak{p}=p^{f_\mathfrak{p}}=q$ is just the cardinality of $K(\mathfrak{p})$ (see [4,12]), where $f_\mathfrak{p}=[K(\mathfrak{p}):\mathbb{F}_p]$ stands for the degree of $\mathfrak{p}$ over the prime p of $\mathbb{Q}$ such that $\mathfrak{p}|p$ ($\mathbb{F}_p$ being the prime field of characteristic p). The local L-series of the curve C over K at $\mathfrak{p}$ is now defined by

$$L_\mathfrak{p}(C,s) = \{(1-\alpha_\mathfrak{p} q^{-s})(1-\bar{\alpha}_\mathfrak{p} q^{-s})\}^{-1},$$

where the (complex) numbers $\alpha_\mathfrak{p}$ and $\bar{\alpha}_\mathfrak{p}$ are characterized by the relations

$$|\alpha_\mathfrak{p}|=|\bar{\alpha}_\mathfrak{p}|=\sqrt{q} \text{ and } N_\mathfrak{p}=1+q-\alpha_\mathfrak{p}-\bar{\alpha}_\mathfrak{p} ,$$

$N_\mathfrak{p}$ denoting the number of points of the reduced curve $C(\mathfrak{p})$ over the finite field $K(\mathfrak{p})$. Suppose next that C has bad reduction modulo $\mathfrak{p}$ such that $C(\mathfrak{p})=C \bmod \mathfrak{p}$ is a cubic defined over $K(\mathfrak{p})$ and having a singularity. Then we set

$$L_\mathfrak{p}(C,s)=(1-q^{-s})^{-1} , (1+q^{-s})^{-1}, \text{ or } 1 ,$$

according as the singularity of the reduced curve $C(\mathfrak{p})$ over $K(\mathfrak{p})$ is an ordinary double point with two (distinct) rational tangents, an ordinary double point with two irrational tangents, or a cusp, respectively. Again we call $L_\mathfrak{p}(C,s)$ the local L-series of the curve C over K at $\mathfrak{p}$.

Now the global L-series of the curve C over K is defined as the Euler product

$$L(C,s) = \prod_\mathfrak{p} L_\mathfrak{p}(C,s)$$

taken over all prime divisors (finite places) $\mathfrak{p}$ of K. The global L-series L(C,s) is known to converge in the complex halfplane Re $s>\frac{3}{2}$.

To state the conjecture of Birch and Swinnerton-Dyer, one has to presuppose that L(C,s) can be analytically continued over the whole complex plane or at least up to a neighbourhood of s=1. Furthermore, the Tate-Šafarevič group Ш of C over K must be assumed finite (see [7,1o, 11]).

Conjecture of Birch and Swinnerton-Dyer [7,1o,11]

The L-series of the elliptic curve C over K has the asymptotic expansion near s=1

$$L(C,s) \sim (s-1)^r \frac{|Ш|\,H}{|\tilde{C}_K|^2} \cdot \frac{2^{r_2}}{\sqrt{|D|}} \cdot M ,$$

where the bars signify cardinalities and M is the product of some local factors which correspond to a certain finite set of places of K including all the infinite places and those finite places $\mathfrak{p}$ at which C has bad reduction modulo $\mathfrak{p}$.

Taking the r-th derivatives on both sides, we derive from the Birch and Swinnerton-Dyer conjecture the asymptotic expansion near s=1

$$L^{(r)}(C,s) \sim r! \frac{|Ш|\,H}{|\tilde{C}_K|^2} \cdot \frac{2^{r_2}}{\sqrt{|D|}} \cdot M.$$

Now suppose we know an upper bound Λ for the r-th derivative of L(C,s) at s=1 and a lower bound λ for the factor M, more precisely, suppose that

$$\left|\frac{1}{r!} L^{(r)}(C,1)\right| \le \Lambda \text{ and } M \ge \lambda > 0.$$

Then it follows from the asymptotic expansion of $L^{(r)}(C,s)$ near s=1 that we have

$$H \le 2^{-r_2} \lambda^{-1} \Lambda \, |\tilde{C}_K|^2 \sqrt{|D|}.$$

Thus we can choose this upper bound for H as the constant H' in Manin's theorem. In the case $K=\mathbb{Q}$ this choice for H' is exactly the same as the one made in [7,16].

However, as pointed out at the beginning of this section, the feasibility of

estimating $L^{(r)}(C,1)$ is an open problem in the general case of an elliptic curve C over a finite-algebraic number field $K \neq \mathbb{Q}$.

6. "Division by two" and the "infinite descent"

As soon as the constants in Manin's theorem are known, the points $P \in C_K \setminus \tilde{C}_K$ satisfying the inequality for d(P) in that theorem can be determined by the method indicated in section 1. Suppose we have found these points by trial and error. Denote them by $P_1,\ldots,P_m$. According to Manin's theorem, the points $P_1,\ldots,P_m$ generate a certain subgroup

$$\hat{C}_K^{(o)} \cong C_K^{(o)}/\tilde{C}_K$$

of finite index $\rho \leq r'!$ in a maximal free subgroup $\hat{C}_K \cong C_K/\tilde{C}_K$ of rank $r \leq r'$ in the rational point group C_K. The group $\hat{C}_K$ is to be determined in terms of a basis.

Next we factor out the subgroup $2\hat{C}_K$ of $\hat{C}_K$ consisting of all points $P \in \hat{C}_K$ such that $P = 2Q$ for some $Q \in \hat{C}_K$. This yields

$$(\hat{C}_K^{(o)} + 2\hat{C}_K)/2\hat{C}_K \leq \hat{C}_K/2\hat{C}_K ,$$

where the factor group on the right has order 2^r. By a finite procedure of repeated "divisions by two" of the points in $\hat{C}_K^{(o)}$ we shall obtain a subgroup $\hat{C}_K^{(\varkappa)} \leq \hat{C}_K$ such that

$$\hat{C}_K^{(\varkappa)} + 2\hat{C}_K = \hat{C}_K \qquad (\varkappa \geq 0)$$

in the following manner.

We have $\hat{C}_K^{(o)} = \langle P_1,\ldots,P_m \rangle$. Apply the subsequent two steps executing the required divisions by two by means of the duplication formula for the point addition in C_K.

(1) Try to divide all points P_i by 2 $(i=1,\ldots,m)$. Suppose that $P_1,\ldots,P_\alpha$ are not divisible by 2, whereas $P_{\alpha+1},\ldots,P_m$ are divisible by 2. Then we have

$P_\nu = 2P_\nu'$ for some $P_\nu' \in C_K$ $(\nu=\alpha+1,\ldots,m)$.

(2) Try to divide all points P_i+P_j by 2 $(1 \leq i < j \leq \alpha)$.
Suppose that $P_1,\ldots,P_\beta$ are such that the P_i+P_j are not divisible by $2 (1 \leq i < j \leq \beta)$, whereas we have

$P_\nu = P_{j_\nu} + 2P_\nu'$ for some $P_\nu' \in C_K (\nu=\beta+1,\ldots,\alpha$; $1 \leq j_\nu \leq \beta)$.

Having carried out steps (1) and (2) we proceed as follows. For $\nu=1,\ldots,\beta$,we write $P_\nu' = P_\nu$. For $\nu=\beta+1,\ldots,\alpha,\ldots,m$, we replace P_ν by P_ν' whenever $P_\nu' \neq P_i'$ for $i=1,\ldots,\nu-1$, and we drop P_ν and P_ν' otherwise. After a suitable renumbering of the points P_ν' for $\nu=\beta+1,\ldots,\alpha,\ldots,m$, if need be, we obtain a subgroup $\hat{C}_K' = \langle P_1',\ldots,P_\beta',\ldots,P_{m'}' \rangle$ of index ρ' in $\hat{C}_K$ such that $\hat{C}_K^{(o)} \leq \hat{C}_K' \leq \hat{C}_K$, $\rho' | \rho$, and $m' \leq m$. Then we repeat steps (1) and (2) for the points $P_{\beta+1}',\ldots,P_{m'}'$ of the new group $\hat{C}_K'$ in place of $\hat{C}_K^{(o)}$, keeping in mind that the points $P_1',\ldots,P_\beta'$ have been treated already. Going on this way we end up, after a finite number of steps, with a certain subgroup $C_K^{(\varkappa)} = \langle P_1^{(\varkappa)},\ldots,P_{m^{(\varkappa)}}^{(\varkappa)} \rangle$ of $\hat{C}_K$ such that neither the $P_i^{(\varkappa)}$ $(i=1,\ldots,m^{(\varkappa)})$ nor the $P_i^{(\varkappa)}+P_j^{(\varkappa)}$ $(1 \leq i < j \leq m^{(\varkappa)})$ are divisible by 2, where $m^{(\varkappa)} \leq m$. Then, we conclude that $\hat{C}_K^{(\varkappa)}$ has odd index $\rho^{(\varkappa)}$ in $\hat{C}_K$, where $\rho^{(\varkappa)} | \rho$. Hence, we see that

$\hat{C}_K^{(\varkappa)} + 2\hat{C}_K = \hat{C}_K$ and, a fortiori,

$$(\hat{C}_K^{(\varkappa)} + 2\hat{C}_K)/2\hat{C}_K = \hat{C}_K/2\hat{C}_K$$

as desired. From the set of all points of the form $P_{i_1}^{(\varkappa)} + \ldots + P_{i_\nu}^{(\varkappa)} (1 \leq i_1 < \ldots < i_\nu \leq m^{(\varkappa)})$ in $\hat{C}_K^{(\varkappa)}$ we can therefore select a complete set of representatives in $\hat{C}_K$ of the 2^r cosets in the factor group $\hat{C}_K/2\hat{C}_K$. As a by-product of this process, we obtain the rank r of the curve C over K.

Let $\{Q_1,\ldots,Q_{2^r}\}$ be such a set of

representatives in $\hat{C}_K$ for $\hat{C}_K/2\hat{C}_K$. There is a point $Q_\nu (1\le\nu\le 2^r)$ such that

$$\hat{h}(Q_\nu) = \max_{i=1,\dots,2^r} \{\hat{h}(Q_i)\}.$$

We shall briefly write $Q=Q_\nu$. The "infinite descent" procedure now shows that the group $\hat{C}_K$ is generated by the set $\{Q_1,\dots,Q_{2^r}\}$ and the set $\{R_1,\dots,R_t\}$ of all points $R_j\in\hat{C}_K$ such that

$$\hat{h}(R_j) \le 1+\hat{h}(Q)$$

(see appendix), where the fact that $t<\infty$ was already noted in section 1. For actually finding all points $R_j\in\hat{C}_K$ satisfying this condition it suffices to determine the (possibly a little larger) finite set of all points $R_j\in\hat{C}_K$ such that

$$d(R_j) \le 1+2\log 2 + \delta + d(Q)$$
$$= 1+7\log 2+\frac{9}{2n}\mu_\infty+\frac{3}{n}\log B + d(Q).$$

This is clear from the estimate of the difference $d(P) - \hat{h}(P)$ given in section 4. The points $R_j\in\hat{C}_K$ fulfilling this latter condition are obtained by employing once more the trial-and-error method. In doing so, one can utilize earlier calculations in connection with Manin's theorem (section 1) and the theorem on the torsion subgroup $\tilde{C}_K$ (section 2).

Finally, we get a basis of the group $\hat{C}_K$ by applying the elementary divisor theorem to the set $\{Q_1,\dots,Q_{2^r},R_1,\dots R_t\}$ of generators of $\hat{C}_K$. Since the torsion subgroup $\tilde{C}_K$ of the rational point group C_K is known from section 2, one can exhibit a basis of the whole group $C_K=\tilde{C}_K\oplus\hat{C}_K$ itself.

7. Concluding remarks

The above exposition of a generalization of Manin's conditional algorithm is to be considered a modest first step towards the implementation of a procedure for determining the rank and a basis of the group C_K of rational points on an elliptic curve C over a finite-algebraic number field K. The amount of calculation involved will surely require the use of an electronic high speed computer. The algorithm is "conditional" insofar as its feasibility depends essentially on the truth of the conjecture of Birch and Swinnerton-Dyer which has to be taken for granted. The term "conditional" is moreover referring to the (open) problem of estimating the r-th derivative of the L-series L(C,s) of C over K at s=1. In the special case $K=\mathbb{Q}$, this problem can be solved by assuming the truth of the Weil conjecture as was shown by Manin [7]. The Weil conjecture guarantees in particular also that L(C,s) can be analytically continued over the whole complex plane, a property needed for stating the conjecture of Birch and Swinnerton-Dyer.

Next we remind of the condition, appearing in the theorem of section 3, according to which the l-division points of C over K have to belong to K for some prime number l. (But compare the remark at the end of section 3.)

Beyond the above-mentioned conditions, the feasibility of the generalized algorithm depends also on a rather good knowledge of the arithmetic of the number field K over which the elliptic curve C is defined.

For example, a complete system of integral divisors of K, representing the finitely many divisor classes of K, is used for writing the coordinates of the points $P\in C_K$ as quotients of integers in a suitable manner as required in the definition of d(P) (see section 1). Such a system can be obtained, e.g., by the method described in [13]. The same method yields also the class number and the structure of the class group $\mathfrak{C}(K)$ of the field K and, more generally, the S-class number and the structure of the S-class

group $\mathfrak{C}_S(K)$ of K for any finite set S of prime divisors of K. Then, the rank $rk_l\mathfrak{C}_S(K)$ of the l-Sylow subgroup of $\mathfrak{C}_S(K)$ can be computed for any prime number l. Of course, the quantity $rk_l\mathfrak{C}_S(K)$, appearing in the bound for the rank r of C over K in the theorem of section 3, does not exceed the l-rank $rk_l\mathfrak{C}(K)$ of the ordinary class group $\mathfrak{C}(K)$ (see [12]).

The definition of $d(P)$ is furthermore based on the $n=r_1+2r_2$ distinct embeddings of the field K into the complex numbers $\mathbb{C}$ (see section 1). With these embeddings of K, we know the rank $rk\,u(K)=r_1+r_2$ of the unit group $u(K)$ of K which also appears in the bound for the rank r of C over K given in the theorem of section 3.

For determining the torsion subgroup $\tilde{C}_K$ of C_K by virtue of the theorem of section 2, an explicit knowledge of the decomposition law [4,12], according to which the primes p of $\mathbb{Q}$ split in K, is helpful (compare [15]). The decomposition law is also useful as a tool in the calculation of the local L-series $L_p(C,s)$ of C over K. Specifically, the discriminant D of the field K must be computed. We have seen that D occurs in the Minkowski bound of K and thus in the bound measuring the deviation of the modified Weil height d from the Néron-Tate height $\hat{h}$ on C_K.

In passing, we direct attention to the remarkable fact that Manin's conditional algorithm is the first procedure devised for determining a basis of the rational point group C_K of the curve C over the number field K.

Appendix

We shall prove here those assertions which were left without proof in the above exposition, thus verifying also the corresponding unproved assertions in [16].

To section 1

Let us begin with establishing the representation required in section 1 for the coordinates of the rational points $P=(\xi,\eta)$ in C_K such that $\xi\neq 0$, $\eta\neq 0$. We follow closely [5].

The Weierstrass equation of C applied to such a point P in C_K yields divisor representations of its coordinates in K of the form

$$\xi \cong \frac{\mathfrak{x}}{\mathfrak{z}^2} \quad \text{and} \quad \eta \cong \frac{\mathfrak{y}}{\mathfrak{z}^3}$$

with some integral divisors $\mathfrak{x},\mathfrak{y}$, and $\mathfrak{z}$ of K having the g.c.d.'s

$$(\mathfrak{x},\mathfrak{z}) = (\mathfrak{y},\mathfrak{z}) = 1.$$

Choose a fixed system V of representatives for the (finitely many) divisor classes of K such that V is made up of integral divisors $\mathfrak{c}$ of K whose norms do not exceed the Minkowski bound B of K (see [4,12,13]),

$$\mathfrak{N}\mathfrak{c}\leq B$$

Then, for the given divisor $\mathfrak{z}$ of K, there exists a divisor $\mathfrak{c}\in V$ such that $\mathfrak{z}\mathfrak{c}$ is a principal divisor of K,

$$\mathfrak{z}\mathfrak{c} \cong z \quad \text{for some nonzero } z\in K.$$

Hence we obtain the representations

$$\xi \cong \frac{\mathfrak{x}\mathfrak{c}^2}{\mathfrak{z}^2\mathfrak{c}^2} \cong \frac{x'}{z^2} \quad \text{and} \quad \eta \cong \frac{\mathfrak{y}\mathfrak{c}^3}{\mathfrak{z}^3\mathfrak{c}^3} \cong \frac{y'}{z^3} \quad \text{for some}$$

nonzero $x',y' \in K$.

On multiplying x' and y' by suitably chosen units of K, we end up with two nonzero elements x and y in K which furnish the desired representations

$$\xi = \frac{x}{z^2} \quad \text{and} \quad \eta = \frac{y}{z^3}$$

of the coordinates of $P\in C_K$ as quotients of integers x, z^2 and y, z^3 in K having the g.c.d.'s

$$(x,z^2) = \mathfrak{c}^2 \quad \text{and} \quad (y,z^3) = \mathfrak{c}^3.$$

To section 4

(a) We wish to derive the estimate claimed for the difference of the modified Weil height d and the Néron-Tate height $\hat{h}$ on the group C_K. In what follows we shall use the notation $\mathfrak{p}|\infty$ or $\mathfrak{p}\nmid\infty$ for the infinite or the finite places $\mathfrak{p}$ of K, writing in the latter case also $\mathfrak{p}|p$ instead of $\mathfrak{p}\nmid\infty$ in order to signify the prime p of $\mathbb{Q}$ over which $\mathfrak{p}$ lies. Let $v_{\mathfrak{p}}$, normalized as in [14], designate the absolute value on K corresponding to the (finite or infinite) place $\mathfrak{p}$ of K. Observe that this normalization of $v_{\mathfrak{p}}$ differs from the normalization of the valuation $w_{\mathfrak{p}}$ used in section 2 for the finite places $\mathfrak{p}$ of K. In fact, we have, for each nonzero $c\in K$, the relation

$$v_{\mathfrak{p}}(c)=\frac{1}{e_{\mathfrak{p}}}w_{\mathfrak{p}}(c)\log p \text{ whenever } \mathfrak{p}|p$$

(see [4]), where $e_{\mathfrak{p}}$ denotes the ramification index of $\mathfrak{p}$. As in [14] we now introduce the real numbers

$$\mu_{\mathfrak{p}}=\min\{\tfrac{1}{2}v_{\mathfrak{p}}(a),\ \tfrac{1}{3}v_{\mathfrak{p}}(b)\} \text{ for each place } \mathfrak{p} \text{ of } K.$$

Notice that the numbers $\mu_{\mathfrak{p}}$ differ, for each place $\mathfrak{p}$ of K such that $\mathfrak{p}|p$, only by a factor $\frac{1}{2e_{\mathfrak{p}}}\log p$ or $\frac{1}{3e_{\mathfrak{p}}}\log p$ from the numbers $\bar{\mu}_{\mathfrak{p}}$ introduced in section 2. For each place $\mathfrak{p}$ of K, let $n_{\mathfrak{p}}=[K_{\mathfrak{p}}:\mathbb{Q}_p]$ or $=[K_{\mathfrak{p}}:\mathbb{R}]$ denote the local degree of $\mathfrak{p}$ according as $\mathfrak{p}|p$ or $\mathfrak{p}|\infty$ respectively (see [4,12,14]). Then we put as in [14]

$$\mu=-\sum_{\mathfrak{p}} n_{\mathfrak{p}}\mu_{\mathfrak{p}},$$

the sum being taken over all (finite and infinite) places $\mathfrak{p}$ of K.

The function used in [14] for defining the Néron-Tate height $\hat{h}$ on C_K was

$$d_1(P)=\begin{cases}-\frac{3}{2n}\sum_{\mathfrak{p}} n_{\mathfrak{p}}\min\{\mu_{\mathfrak{p}},v_{\mathfrak{p}}(\xi)\} & \text{if } P=(\xi,\eta)\neq 0\\ \frac{3}{2n}\mu & \text{if } P=0\end{cases},$$

where $n=[K:\mathbb{Q}]$ is the field degree of K over $\mathbb{Q}$ as before. (Actually, we used in [14] the function nd_1 and called it d). The difference function $d_1-\hat{h}$ on C_K was shown in [14] to fulfill the estimate

$$-2\log 2\le d_1(P)-\hat{h}(P)\le 5\log 2+\frac{3}{n}\mu \text{ for } P\in C_K.$$

Starting off with this estimate we are left with the task of estimating the difference function $d-d_1$ on C_K. The modified Weil height d on C_K was introduced in section 1 as

$$d(P)=\frac{3}{2n}\log\prod_{\nu=1}^{n}\max\{\sqrt[2]{|a^{(\nu)}|}\,|z^{(\nu)}|^2,\ \sqrt[3]{|b^{(\nu)}|}\,|z^{(\nu)}|^2,\ |x^{(\nu)}|\}$$

with the coordinates of the point $P=(\xi,\eta)$ in C_K written in the shape

$$\xi=\frac{x}{z^2} \text{ and } \eta=\frac{y}{z^3} \quad (x,y,\text{and } z \text{ integers in } K)$$

as described in section 1 and at the beginning of this appendix. Hence, we obtain in the notation of [14] (making the convention that $\log 0=-\infty$)

$$\begin{aligned}d(P)&=\frac{3}{2n}\sum_{\nu=1}^{n}\max\{\tfrac{1}{2}\log|a^{(\nu)}|+2\log|z^{(\nu)}|,\\ &\tfrac{1}{3}\log|b^{(\nu)}|+2\log|z^{(\nu)}|,\log|x^{(\nu)}|\}\\ &=\frac{3}{2n}\sum_{\mathfrak{p}|\infty} n_{\mathfrak{p}}\max\{\tfrac{1}{2}\log|a|_{\mathfrak{p}}+2\log|z|_{\mathfrak{p}},\\ &\tfrac{1}{3}\log|b|_{\mathfrak{p}}+2\log|z|_{\mathfrak{p}},\log|x|_{\mathfrak{p}}\}\\ &=-\frac{3}{2n}\sum_{\mathfrak{p}|\infty} n_{\mathfrak{p}}\min\{\tfrac{1}{2}v_{\mathfrak{p}}(a)+2v_{\mathfrak{p}}(z),\tfrac{1}{3}v_{\mathfrak{p}}(b)+\\ &+2v_{\mathfrak{p}}(z),v_{\mathfrak{p}}(x)\}\\ &=-\frac{3}{2n}\sum_{\mathfrak{p}|\infty} n_{\mathfrak{p}}\min\{\mu_{\mathfrak{p}}+2v_{\mathfrak{p}}(z),v_{\mathfrak{p}}(x)\}.\end{aligned}$$

On the other hand, the sum formula for the absolute values $v_{\mathfrak{p}}$ on K (see [14]) yields for the function d_1 on C_K

$$\begin{aligned}d_1(P)&=-\frac{3}{2n}\sum_{\mathfrak{p}} n_{\mathfrak{p}}\min\{\mu_{\mathfrak{p}},v_{\mathfrak{p}}(\tfrac{x}{z^2})\}\\ &=-\frac{3}{2n}\sum_{\mathfrak{p}} n_{\mathfrak{p}}\min\{\mu_{\mathfrak{p}}+2v_{\mathfrak{p}}(z),v_{\mathfrak{p}}(x)\}.\end{aligned}$$

A comparison of the last expressions for the functions d and d_1 on C_K shows at once that for $P \in C_K$

$$d_1(P) = d(P) - \frac{3}{2n} \sum_{p \nmid \infty} n_p \min\{\mu_p + 2v_p(z), v_p(x)\}.$$

Hence, taking into account that a,b,x, and z are integers in K, we obtain the inequality

$$d_1(P) \leq d(P) \text{ for } P \in C_K.$$

It remains to establish an inequality in the opposite direction between $d_1(P)$ and d(P) up to an additive constant not depending on the point P. We shall explicitly exhibit such a constant. Remembering the fact that $\mu_p \geq 0$ for each finite place p of K and keeping in mind the choice of the coordinate $\xi = \frac{x}{z^2}$ of P such that $(x,z^2) = c^2$ with $c \in V$, we derive from the above equation between $d_1(P)$ and d(P) the inequality

$$d_1(P) \geq d(P) - \frac{3}{2n} \sum_{p \nmid \infty} n_p \min\{\mu_p + 2v_p(z), \mu_p + v_p(x)\}$$

$$= d(P) - \frac{3}{2n} \sum_{p \nmid \infty} n_p \mu_p - \frac{3}{2n} \sum_{p \nmid \infty} n_p \min\{2v_p(z), v_p(x)\}$$

$$= d(P) - \frac{3}{2n} \sum_{p \nmid \infty} n_p \mu_p - \frac{3}{n} \sum_{p \nmid \infty} n_p v_p(c).$$

Consider the second and the third term of the last expression.

As regards the second term, we have in the notation of [14] and section 4

$$0 \geq -\frac{3}{2n} \sum_{p \nmid \infty} n_p \mu_p = \frac{3}{2n} \mu + \frac{3}{2n} \sum_{p \mid \infty} n_p \mu_p$$

$$= \frac{3}{2n} \mu + \frac{3}{2n} \sum_{p \mid \infty} n_p \min\{\tfrac{1}{2} v_p(a), \tfrac{1}{3} v_p(b)\}$$

$$= \frac{3}{2n} \mu - \frac{3}{2n} \sum_{p \mid \infty} n_p \max\{\tfrac{1}{2} \log|a|_p, \tfrac{1}{3} \log|b|_p\}$$

$$= \frac{3}{2n} \mu - \frac{3}{2n} \sum_{\nu=1}^{n} \max\{\tfrac{1}{2} \log|a^{(\nu)}|, \tfrac{1}{3} \log|b^{(\nu)}|\}$$

$$= \frac{3}{2n} \mu - \frac{3}{2n} \log \prod_{\nu=1}^{n} \max\{\sqrt[2]{|a^{(\nu)}|}, \sqrt[3]{|b^{(\nu)}|}\}$$

$$= \frac{3}{2n} \mu - \frac{3}{2n} \mu_\infty.$$

In particular, dropping the factor $\frac{3}{2n}$ and applying the sum formula for the absolute values v_p on K, we obtain

$$\mu_\infty \geq \mu = -\sum_p n_p \mu_p = -\sum_p n_p \min\{\tfrac{1}{2} v_p(a), \tfrac{1}{3} v_p(b)\}$$

$$\geq \begin{cases} -\frac{1}{2} \sum_p n_p v_p(a) & \text{if } a \neq 0 \\ -\frac{1}{3} \sum_p n_p v_p(b) & \text{if } b \neq 0 \end{cases} = 0.$$

Hence, the above second term under consideration satisfies the inequality

$$-\frac{3}{2n} \sum_{p \nmid \infty} n_p \mu_p \geq -\frac{3}{2n} \mu_\infty.$$

Now let us look at the third term $-\frac{3}{n} \sum_{p \nmid \infty} n_p v_p(c)$ of the above expression.

Since $c \in V$, the norm of c does not exceed the Minkowski bound B,

$$\mathfrak{N}c \leq B.$$

For the time being we shall denote, for each finite place p of K, by p_p the prime of $\mathbb{Q}$ such that $p \mid p_p$. Then, the norm inequality can be explicitly written as (see [4,12])

$$\mathfrak{N}c = \prod_{p \nmid \infty} p_p^{f_p w_p(c)} \leq B,$$

where f_p as usual stands for the degree of p over p_p (see section 5).

Taking logarithms on both sides, we get

$$\log \mathfrak{N}c = \sum_{p \nmid \infty} f_p w_p(c) \log p_p \leq \log B.$$

Hence, since $n_p = e_p f_p$ with the ramification index e_p of p, we have

$$\sum_{p \nmid \infty} n_p v_p(c) = \sum_{p \nmid \infty} \frac{1}{e_p} n_p w_p(c) \log p_p =$$

$$= \sum_{p \nmid \infty} f_p w_p(c) \log p_p \leq \log B.$$

The above third term under consideration thus satisfies the inequality

$$-\frac{3}{n} \sum_{p \nmid \infty} n_p v_p(c) \geq -\frac{3}{n} \log B.$$

In sum, we have established the estimate

$$d_1(P) \geq d(P) - \frac{3}{2n}\mu_\infty - \frac{3}{n}\log B \text{ for } P \in C_K.$$

Combining this estimate with the inequality $d_1(P) \leq d(P)$ derived before we obtain the desired estimate

$$0 \leq d(P) - d_1(P) \leq \frac{3}{2n}\mu_\infty + \frac{3}{n}\log B \text{ for } P \in C_K.$$

In combination with the above-quoted estimate for the difference $d_1 - \hat{h}$ on C_K, this result leads to the asserted inequalities

$$-2\log 2 \leq d(P) - \hat{h}(P) \leq 5\log 2 + \frac{3}{n}\mu + \frac{3}{2n}\mu_\infty + \frac{3}{n}\log B$$

$$\leq 5\log 2 + \frac{9}{2n}\mu_\infty + \frac{3}{n}\log B \text{ for } P \in C_K,$$

where in the last step we have again employed the relation $\mu \leq \mu_\infty$ which was shown above to be valid.

(b) Now we shall prove the estimate indicated in section 4 for the expression $d(P,P) = d(2P) - 4d(P)$ as P ranges over the group C_K. To begin with we quote from [14] for the analog expression $d_1(P,P) = d_1(2P) - 4d_1(P)$ the estimate

$$-(15\log 2 + \frac{9}{n}\mu) \leq d_1(P,P) \leq 6\log 2 \text{ for } P \in C_K.$$

(Actually, we estimated in [14] the expression $nd_1(P,P)$ and denoted it by $d(P,P)$). On the other hand, it follows by definition of $d(P,P)$ and $d_1(P,P)$ from the estimate established in part (a) for the difference function $d - d_1$ on C_K, that we have

$$d_1(P,P) - \frac{6}{n}\mu_\infty - \frac{12}{n}\log B \leq d(P,P) \leq d_1(P,P) + \frac{3}{2n}\mu_\infty + \frac{3}{n}\log B \text{ for } P \in C_K.$$

On replacing $d_1(P,P)$ by its cited lower and upper bound from [14], respectively, and remembering that $\mu \leq \mu_\infty$, we get

$$-15(\log 2 + \frac{\mu_\infty}{n}) - \frac{12}{n}\log B \leq d(P,P) \leq 6(\log 2 + \frac{\mu_\infty}{4n}) + \frac{3}{n}\log B \text{ for } P \in C_K$$

as asserted in section 4.
In particular, this yields for the sum

$$\hat{h}(P) - d(P) - \sum_{i=1}^{m} \frac{d(2^{i-1}P, 2^{i-1}P)}{2^{2i}}$$

$$= \sum_{i=m+1}^{\infty} \frac{d(2^{i-1}P, 2^{i-1}P)}{2^{2i}} = \frac{1}{2^{2m}} \sum_{i=1}^{\infty} \frac{d(2^{m+i-1}P, 2^{m+i-1}P)}{2^{2i}}$$

the asserted estimate (compare [14])

$$-\frac{5}{2^{2m}}(\log 2 + \frac{\mu_\infty}{n}) - \frac{4}{n2^{2m}}\log B \leq \frac{1}{2^{2m}} \sum_{i=1}^{\infty} \frac{d(2^{m+i-1}P, 2^{m+i-1}P)}{2^{2i}} \leq \frac{2}{2^{2m}}(\log 2 + \frac{\mu_\infty}{4n}) + \frac{1}{n2^{2m}}\log B \text{ for } P \in C_K.$$

<u>To section 6</u> Let us show how to get a set of generators for the group $\hat{C}_K$ by applying the method of "infinite descent" (see [8]) to a given set $\{Q_1, \ldots, Q_{2^{r2^r}}\}$ of representatives in $\hat{C}_K$ of the 2^{r2^r} cosets in the factor group $\hat{C}_K / 2\hat{C}_K$.

We have

$$\hat{C}_K / 2\hat{C}_K = \{Q_1, \ldots, Q_{2^{r2^r}}\} / 2\hat{C}_K .$$

The "infinite descent" works as follows. Let $R \in \hat{C}_K$ be an arbitrary rational point. Put $R_o = R$. There is a rational point $R_1 \in \hat{C}_K$ such that

$$R_o = Q_{\nu_o} + 2R_1 \text{ for some index } \nu_o \text{ in } 1 \leq \nu_o \leq 2^{r2^r}.$$

Furthermore, there is a rational point $R_2 \in \hat{C}_K$ such that

$$R_1 = Q_{\nu_1} + 2R_2 \text{ for some index } \nu_1 \text{ in } 1 \leq \nu_1 \leq 2^{r2^r}.$$

Going on this way we obtain an infinite sequence $R_o, R_1, \ldots, R_{j-1}, R_j, \ldots$ of rational points in $\hat{C}_K$ sucht that

$R_{j-1}=Q_{\nu_{j-1}}+2R_j$ for some index ν_{j-1} in $1\le\nu_{j-1}\le 2^r$, where $j\ge 1$.

Fortunately, only a finite portion of this infinite sequence is needed for finding a basis of $\hat{C}_K$ as we shall see. By induction on j, it follows from the last relation that the given rational point $R\in\hat{C}_K$ admits a representation of the form

$$(*)\quad R=2^jR_j+2^{j-1}Q_{\nu_{j-1}}+\ldots+2Q_{\nu_1}+Q_{\nu_0}\quad (j\ge 1).$$

We wish to estimate the value of the Néron-Tate height $\hat{h}$ at the point R_j. To this end we utilize the property of $\hat{h}$ to be a positive definite quadratic form on the group $\hat{C}_K$ (see [8,14]). Applying the function $\hat{h}$ to the relation $2R_j=R_{j-1}-Q_{\nu_{j-1}}$ we obtain for $j\ge 1$

$$4\hat{h}(R_j)=2\hat{h}(R_{j-1})+2\hat{h}(Q_{\nu_{j-1}})-\hat{h}(R_{j-1}+Q_{\nu_{j-1}})$$
$$\le 2\hat{h}(R_{j-1})+2\hat{h}(Q_{\nu_{j-1}}).$$

In this inequality we may replace $Q_{\nu_{j-1}}$ by the point Q chosen in section 6 in order to gain

$$4\hat{h}(R_j)\le 2\hat{h}(R_{j-1})+2\hat{h}(Q)\quad (j\ge 1).$$

Now we use induction on j to infer from this the new inequality

$$\hat{h}(R_j)\le\hat{h}(Q)+\frac{1}{2^j}\{\hat{h}(R)-\hat{h}(Q)\}\quad (j\ge 1).$$

When we choose the index j sufficiently large, we arrive at a rational point $R_j\in\hat{C}_K$ such that

$$\hat{h}(R_j)\le 1+\hat{h}(Q)=1+\max_{i=1,\ldots,2^r}\{\hat{h}(Q_i)\}.$$

Thus the given point $R\in\hat{C}_K$ can be represented as a linear combination (*) of the points $Q_1,\ldots,Q_{2^r}$ and a point R_j satisfying the above inequality for its $\hat{h}$-value. By virtue of the estimate for the difference function $d-\hat{h}$ on $\hat{C}_K$, this last inequality turns into the corresponding inequality with the Néron-Tate height $\hat{h}$ replaced by the modified Weil height d.

References

1. V.A. Dem'janenko, Torsion of elliptic curves. Izv. Akad. Nauk SSSR, Ser. Mat. 35 (1971), 28o-3o7 = Math. USSR Izvestija 5 (1971), 289-318.
2. G. Frey, Some remarks concerning points of finite order on elliptic curves over global fields. To appear.
3. H. Hasse, Simultane Approximation algebraischer Zahlen durch algebraische Zahlen. Monatsh. Math. Phys. 48 (1939), 2o5-225.
4. H. Hasse, Zahlentheorie. Akademie-Verlag, Berlin 1969.
5. J. Heuss, Zum schwachen Endlichkeitssatz von Mordell. Diploma Thesis, Karlsruhe 1975.
6. T. Honda, Isogenies, rational points and section points of group varieties. Japanese J.Math. 3o (196o), 84-1o1.
7. Ju.I. Manin, Cyclotomic fields and modular curves. Uspehi Mat. Nauk 26 (1971) no. 6 (162), 7-71 = Russian Math. Surveys 26 (1971) no. 6, 7-78.
8. D. Mumford, Abelian Varieties. Oxford University Press, London 1974.
9. J.-P. Serre, p-Torsion des courbes elliptiques (d'après Ju.I. Manin). In: Sém. Bourbaki, 22e année, 1969/7o, no. 38o, 281-294.
1o. H.P.F.Swinnerton-Dyer, The conjectures of Birch and Swinnerton-Dyer, and of Tate. In: Proc. Conf. on Local Fields, 132-157, Springer-Verlag, Berlin-Göttingen-Heidelberg 1967.
11. H.P.F.Swinnerton-Dyer and B.J.Birch, Elliptic curves and modular functions.

In: Modular Functions of One Variable IV, Lecture Notes in Math., vol. 476, pp. 2-32, Springer-Verlag, Berlin-Heidelberg-New York 1975.

12. E. Weiss, Algebraic Number Theory, McGraw-Hill Book Company, New York 1963.

13. H.G. Zimmer, Some computational aspects of, and the use of computers in, algebraic number theory. Computing 8 (1971), 363-381.

14. H.G. Zimmer, On the difference of the Weil height and the Néron-Tate height. Math. Z. 147 (1976), 35-51.

15. H.G. Zimmer, Points of finite order on elliptic curves over number fields. To appear in Arch. d. Math.

16. H.G. Zimmer, On Manin's conditional algorithm. To appear in Proc.Conf. on "Utilisation des calculateurs en mathématiques pures", Limoges 1975.