MÉMOIRES DE LA S. M. F.

HORST G. ZIMMER

# On Manin's conditional algorithm

*Mémoires de la S. M. F.*, tome 49-50 (1977), p. 211-224

<http://www.numdam.org/item?id=MSMF_1977__49-50__211_0>

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math. France.
Mémoire 49-50, 1977, p. 211-224



# On Manin's conditional algorithm

Horst G. Zimmer

Manin's conditional algorithm [2] was divised for computing the rank and a basis of the group $C_{\mathbb{Q}}$ of rational points of an elliptic curve C defined over the rationals $\mathbb{Q}$. According to the Mordell-Weil theorem (see [8]), the group $C_{\mathbb{Q}}$ is finitely generated. However, up to now the problem of determining the rank and a basis of $C_{\mathbb{Q}}$ in the general case of an arbitrary elliptic curve C over $\mathbb{Q}$ must be considered a very hard one (compare, e.g.[7]). Manin's algorithm solves both problems under the condition that two famous conjectures, the Weil conjecture and the Birch and Swinnerton-Dyer conjecture, are true. In this lecture, some ideas will be outlined regarding the implementation of the algorithm.

Let the elliptic curve C be given in Weierstrass normal form

$$Y^2 = X^3 + aX + b \qquad (a,b\in\mathbb{Q})$$

with discriminant $\Delta := 4a^3+27b^2 (\neq 0)$. On applying a birational transformation over $\mathbb{Q}$ of type

$$X \to \rho^2 X,\ Y \to \rho^3 Y \qquad (\rho\in\mathbb{Q},\rho\neq 0)$$

to the Weierstrass equation for C, if need be, we may assume the coefficients a,b of the equation to be integers. Moreover, it is convenient to set up the birational transformation in such a way that the new coefficients $a,b\in\mathbb{Z}$ have minimal p-values under all p-adic exponential valuations $v_p$ on $\mathbb{Q}$.

By the Mordell-Weil theorem, the additive abelian group $C_{\mathbb{Q}}$ is a direct sum

$$C_{\mathbb{Q}} = \tilde{C}_{\mathbb{Q}} \oplus \hat{C}_{\mathbb{Q}}$$

of its finite torsion subgroup $\tilde{C}_{\mathbb{Q}}$ and a maximal free subgroup $\hat{C}_{\mathbb{Q}}$ of finite rank r. We call r the <u>rank</u> of the elliptic curve C over $\mathbb{Q}$. In Manin's conditional algorithm first the rank r of C over $\mathbb{Q}$ is determined and then a basis of the group

$$\hat{C}_{\mathbb{Q}} \cong C_{\mathbb{Q}}/\tilde{C}_{\mathbb{Q}}$$

is found. The torsion subgroup $\tilde{C}_{\mathbb{Q}}$ ought to be computed in advance.

As in the proof of the Mordell-Weil theorem, the Néron-Tate height $\hat{h}$ on $C_{\mathbb{Q}}$ plays a crucial role in Manin's algorithm too. We define $\hat{h}$ on $C_{\mathbb{Q}}$ by means of an auxiliary function d on $C_{\mathbb{Q}}$ which is used in place of the Weil height h on $C_{\mathbb{Q}}$ (see [2], [11]). For each point $P=(\xi,\eta)\in C_{\mathbb{Q}}$, we put $\xi=\frac{x}{z}$ with $x,z\in\mathbb{Z}$ relatively prime and define

$$d(P) := \tfrac{3}{2}\max(\tfrac{1}{2}\log|a|_\infty+\log|z|_\infty,\ \tfrac{1}{3}\log|b|_\infty+\log|z|_\infty,\ \log|x|_\infty)$$

disregarding those of the rational numbers a,b,x or z which are equal to zero, where $|\ |_\infty$ denotes the ordinary absolute value on $\mathbb{Q}$. The neutral element $0=(\infty,\infty)$ of the addition in $C_{\mathbb{Q}}$ is included in the definition of d, viz.

$$d(0) = 0.$$

The Néron-Tate height $\hat{h}$ on $C_{\mathbb{Q}}$ can then be defined via

$$\hat{h}(P) := \lim_{n\to\infty} \frac{d(2^n P)}{2^{2n}} \quad \text{for each } P\in C_{\mathbb{Q}}.$$

We are now in a position to state the fundamental theorem on which Manin's algorithm is based. In our version of the theorem, the Weil height h on $C_{\mathbb{Q}}$ will be replaced by the function d on $C_{\mathbb{Q}}$.

Let us first introduce some notation.

If $P_1,\dots,P_r$ is a basis of $\hat{C}_{\mathbb{Q}}$, we put

$$H := \left|\det\left(\tfrac{1}{2}(\hat{h}(P_i+P_j)-\hat{h}(P_i)-\hat{h}(P_j))\right)_{i,j=1,\dots,r}\right|_\infty .$$

Clearly, the quantity H is independent of the choice of $P_1,\dots,P_r$ since any other basis of $\hat{C}_{\mathbb{Q}}$ is obtained from the given one by a unimodular transformation of determinant $\pm 1$. We call H the <u>determinant</u> of the elliptic curve C over $\mathbb{Q}$.

Furthermore, let $h'\in\mathbb{R}$ designate an estimate from below for the Néron-Tate height $\hat{h}$ on $C_{\mathbb{Q}}\setminus\tilde{C}_{\mathbb{Q}}$ such that we have

$$0 < h' \le \min\{\hat{h}(P)/P\in C_{\mathbb{Q}}\setminus\tilde{C}_{\mathbb{Q}}\}.$$

Finally, let there be given a measure $\delta\in\mathbb{R}$ for the deviation of

the function d on $C_Q$ from the Néron-Tate height $\hat{h}$ on $C_Q$, namely,

$d(P)-\hat{h}(P) \leq \delta$ for each $P \in C_Q$.

Theorem (Manin). Suppose that upper bounds $r' \in \mathbb{Z}$ and $H' \in \mathbb{R}$ are known for the rank r and the determinant H respectively of the elliptic curve C over Q. Then, the set of points $P \in C_Q$ 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 of the r'-dimensional unit ball in Euclidean space, generates a subgroup of $\hat{C}_Q \cong C_Q/\tilde{C}_Q$ of index $\leq r'!$

We remark that the set of points $P \in C_Q$ mentioned in the theorem is finite since there are only finitely many points in $C_Q$ having bounded Weil height (see [8], [11]).

The proof of the theorem relies on the method of successive minima with respect to the lattice generated by $C_Q$ in the r-dimensional real space $C_Q \otimes \mathbb{R}$ on which the Néron-Tate height $\hat{h}$ is a positive definite quadratic form (cf.[2],[11]). Since the kernel of the canonical $\mathbb{Z}$-module homomorphism $C_Q \to C_Q \otimes \mathbb{R}$ is precisely the torsion subgroup $\tilde{C}_Q$ of $C_Q$, we get an embedding of the free subgroup $\hat{C}_Q \cong C_Q/\tilde{C}_Q \hookrightarrow C_Q \otimes \mathbb{R}$ and may therefore identify $\hat{C}_Q$ with the lattice generated by $C_Q$ in the space $C_Q \otimes \mathbb{R}$.

Starting off then with the set of generators of the subgroup of finite index in $\hat{C}_Q$ found in accordance with the theorem, one can exhibit a basis of $\hat{C}_Q$ by the "infinite" descent procedure that is used in the proof of the Mordell-Weil theorem. In the present lecture we wish to discuss some devices and methods by which the torsion subgroup $\tilde{C}_Q$ and the constants occurring in the upper bound for d(P) can be computed or at least be estimated.

1. Determination of the torsion subgroup. Manin [2] recommends to apply purely local methods for determining the torsion subgroup $\tilde{C}_Q$ of $C_Q$. Instead, we propose here to use a strengthened version of the classical theorem of Nagell and

Lutz giving a necessary condition for a point $P \in C_{\mathbb{Q}}$ to be of finite order.

Let us first recall some special results on torsion points in $C_{\mathbb{Q}}$. It is known (see [3],[5]) that there are elliptic curves $C$ over $\mathbb{Q}$ having rational points of orders

1,2,3,4,5,6,7,8,9,10,12

and that there are no elliptic curves $C$ over $\mathbb{Q}$ having rational points of orders

11,13,14,15,16,17,20,24.

Dem'janenko [1] has shown that if the group $C_{\mathbb{Q}}$ contains a point of order $2p$ or $p$, $p$ denoting a prime of $\mathbb{Q}$, then $p \leq 509$ or $p < 6144$ respectively. On the other hand, Dem'janenko has also proved that the order of the torsion subgroup $\tilde{C}_{\mathbb{Q}}$ of $C_{\mathbb{Q}}$ is bounded by a constant not depending on the curve $C$.

On this background we can cope with the task of computing the torsion subgroup $\tilde{C}_{\mathbb{Q}}$ of $C_{\mathbb{Q}}$ by virtue of the following strong form of the well-known theorem of Nagell and Lutz (compare [10],[12]).

Let $\mathbb{P}$ denote the set of (finite) primes $p$ of $\mathbb{Q}$. Writing $v_p$ for the $p$-adic exponential valuation on $\mathbb{Q}$, we put for each $p \in \mathbb{P}$

$\mu_p := \min(\frac{1}{2} v_p(a), \frac{1}{3} v_p(b))$. In this section we designate by $\{\gamma\}$ and $[\gamma]$ respectively the least integer not smaller than $\gamma \in \mathbb{R}$ and the greatest integer smaller than or equal to $\gamma \in \mathbb{R}$. We then use the following symbolic notation.

$$\{m\} := \prod_{p \in \mathbb{P}} p^{\{\mu_p\}}, \quad \{m^{\frac{3}{2}}\} := \prod_{p \in \mathbb{P}} p^{\{\frac{3}{2}\mu_p\}},$$

$$\{m_p\} := p^{\{\mu_p - \frac{2}{p-1}\}} \prod_{p \neq q \in \mathbb{P}} q^{\{\mu_q\}}, \{m_p^{\frac{3}{2}}\} := p^{\{\frac{3}{2}\mu_p - \frac{3}{p-1}\}} \prod_{p \neq q \in \mathbb{P}} q^{\{\frac{3}{2}\mu_q\}}$$

if $p \neq 3$ and

$$\{m_3\} := 3^{\{\mu_3 - \frac{1}{4}\}} \prod_{3 \neq q \in \mathbb{P}} q^{\{\mu_q\}}, \quad \{m_3^{\frac{3}{2}}\} := 3^{\{\frac{3}{2}\mu_3 - \frac{3}{8}\}} \prod_{3 \neq q \in \mathbb{P}} q^{\{\frac{3}{2}\mu_q\}},$$

$$\{\Delta^{\frac{1}{2}} m^{-3}\} := \prod_{p \in \mathbb{P}} p^{\{\frac{1}{2}v_p(\Delta) - 3\mu_p\}},$$

$$[m^{\frac{3}{2}}] := \prod_{p \in \mathbb{P}} p^{[\frac{3}{2}\mu_p]}, \quad [m_p^{\frac{3}{2}}] := p^{[\frac{3}{2}\mu_p + \frac{1}{p-1}]} \prod_{p \neq q \in \mathbb{P}} q^{[\frac{3}{2}\mu_q]}$$

Theorem: Let $P=(x,y)\in\tilde{C}_{\mathbb{Q}}$ be a point of order n.
Then, the following divisibility relations hold:
$\{m\}|x$ or $\{m_p\}|x$
according as $n\neq p^\nu$ or $n=p^\nu(\nu\in\mathbb{N})$ each for $p=5$ or 7,
$\{m^{\frac{3}{2}}\}|y$ or $\{m_p^{\frac{3}{2}}\}|y$

according as $n\neq p^\nu$ or $n=p^\nu(\nu\in\mathbb{N})$ each for $p=3,5$ or 7,
and
$y=0$ or $y|[m^{\frac{3}{2}}]\{\Delta^{\frac{1}{2}}m^{-3}\}$ or $y|[m_p^{\frac{3}{2}}]\{\Delta^{\frac{1}{2}}m^{-3}\}$
according as $n=2$ or $n\neq 2\cdot p^\nu$ or $n=2\cdot p^\nu(\nu\in\mathbb{N})$ each for $p=5$.

Remark: This theorem is strong enough to facilitate the complete determination of the torsion subgroup $\tilde{C}_{\mathbb{Q}}$ of the group $C_{\mathbb{Q}}$ for large classes of elliptic curves C over $\mathbb{Q}$. For those classes of curves C, the group $\tilde{C}_{\mathbb{Q}}$ is generated by points of orders $2^\nu$, $3^\nu, 5^\nu, 2\cdot 5^\nu$ and $7^\nu$ with bounded $\nu\in\mathbb{N}$. One might be tempted to ask the question if a result of this type holds for arbitrary elliptic curves C over $\mathbb{Q}$.
The proof of the theorem proceeds along the lines of [10] and is given in [12].
Example (see Nagell [4]).

$$C: Y^2=X^3+2^4\cdot 3^3\cdot 5X+2^4\cdot 3^3\cdot 5\cdot 79$$

with discriminant $\Delta=2^8\cdot 3^{17}\cdot 5^2$. The non-zero points $P=(x,y)$ of order $p=5$ in $\tilde{C}_{\mathbb{Q}}$ are

$$(-2^3\cdot 3, \pm 2^2\cdot 3^4),\ (2^2\cdot 3\cdot 7, \pm 2^2\cdot 3^5).$$

We have

$\mu_2=\frac{4}{3}$, $\mu_3=1$, $\mu_5=\frac{1}{3}$, and $\mu_q=0$ for $q\in\mathbb{P}$, $q\neq 2,3,5$, hence

$\frac{3}{2}\mu_2=2$, $\frac{3}{2}\mu_3=\frac{3}{2}$, $\frac{3}{2}\mu_5=\frac{1}{2}$, and $\frac{3}{2}\mu_q=0$ for $q\in\mathbb{P}$, $q\neq 2,3,5$.

Therefore,

$\{m_5\}=2^2\cdot 3|x=-2^3\cdot 3,\ 2^2\cdot 3\cdot 7$, whereas $\{m\}=2^2\cdot 3\cdot 5\nmid x=2^3\cdot 3, 2^2\cdot 3\cdot 7$;

$\{m_5^{\frac{3}{2}}\}=2^2\cdot 3^2|\pm y=\pm 2^2\cdot 3^4, \pm 2^2\cdot 3^5$, whereas $\{m^{\frac{3}{2}}\}=2^2\cdot 3^2\cdot 5\nmid\pm y=\pm 2^2\cdot 3^4, \pm 2^2\cdot 3^5$;

$$\pm y=\pm 2^2\cdot 3^4\pm 2^2\cdot 3^5|[m^{\frac{3}{2}}]\cdot\{\Delta^{\frac{1}{2}}m^{-3}\}=[2^2\cdot 3]\cdot 3^6=2^2\cdot 3^7.$$

In particular, there are only 6 possibilities for $|y|_\infty \neq 0$ of a torsion point $P=(x,y)$ in $\tilde{C}_Q$. An easy calculation (using a pocket calculator) reveals by means of the theorem that there are no other torsion points in $\tilde{C}_Q$ besides those already found.

2. An estimate for the rank. Very little is known about the rank r of an elliptic curve C over Q. Néron proved that there exist curves C over Q with rank r=10 but gave no examples. Penney and Pomerance [6] exhibited curves C over Q having a rank $r\geq 6$. However, one does not know if there are elliptic curves C over Q of arbitrarilylarge rank or if the rank is bounded. Following Tate [8] we give here an upper bound r' for the rank of $\hat{C}_Q$ under the assumption that the elliptic curve C over Q has a rational point $P_o=(x_o,y_o)$ of order 2 or, what amounts to the same, that the equation $X^3+aX+b=0$ has a solution $x_o\in\mathbb{Z}$.

In case this assumption is not satisfied for the curve C, one obtains an upper bound r' for r in a similar manner by adjoining to Q a solution $x_o$ of that equation and working over the number field $K=Q(x_o)$ instead of Q. Now we introduce the following numbers of primes.

$$s:=|\{p\in\mathbb{P}\,/\,p|(3x_o^2+a)\}|,\ t:=|\{p\in\mathbb{P}\,/\,p|(3x_o^2+4a)\}|.$$

Then, the number

$$r' := \begin{cases} s+t+1 & \text{if } -(3x_o^2+4a) \text{ is not a square} \\ s+t & \text{if } -(3x_o^2+4a) \text{ is a square} \end{cases}$$

is the desired upper bound for the rank r, that is, $r \leq r'$.

3. Deviation of d from the Néron-Tate height and a lower bound for the Néron-Tate height. The deviation of the function d on $C_Q$ from the Néron-Tate height $\hat{h}$ on $C_Q$ is bounded according to the inequalities (compare [11])

$$-2\log 2 \leq d(P)-\hat{h}(P)\leq\frac{9}{5}\max\left(\tfrac{1}{2}\log|a|_\infty,\ \tfrac{1}{3}\log|b|_\infty\right)+5\log 2.$$

Hence, the quantity

$$\delta := \frac{9}{2}\max\left(\frac{1}{2}\log|a|_\infty, \frac{1}{3}\log|b|_\infty\right) + 5\log 2$$

can be taken as the first summand of the bound for $d(P)$ in Manin's theorem.

Next we wish to determine a lower bound $h'$ for the Néron-Tate height $\hat{h}$ on $C_Q \setminus \tilde{C}_Q$. Note that $\hat{h}(P)=0$ if and only if $P \in \tilde{C}_Q$ (compare [11]). According to Manin [2] it suffices to choose

$$h' := \min\{\delta, \hat{h}(P) \mid P \in C_Q \setminus \tilde{C}_Q, d(P) < 2\delta\}$$

because for all $P \in C_Q$ such that $d(P) \geq 2\delta$, we have $\hat{h}(P) \geq \delta$. Then, clearly

$$\min\{\hat{h}(P) \mid P \in C_Q \setminus \tilde{C}_Q\} \geq h'.$$

Moreover, since $\hat{h}$ is positive definite on $C_Q \setminus \tilde{C}_Q$ and since there are only finitely many points $P$ in $C_Q$ satisfying $d(P)<2\delta$, it follows that

$$h' > 0.$$

Hence, the real number $h'$ is the desired lower bound for the Néron-Tate height $\hat{h}$ on $C_Q \setminus \tilde{C}_Q$.

For actually determining $h'$, one has to compute $\hat{h}(P)$ for a finite number of points $P \in C_Q$. The points themselves are found by the same successive minima method from geometry of numbers which is used in the proof of Manin's theorem. In order to compute $\hat{h}(P)$ for a given point $P \in C_Q$, one can take the relation (cf. [11])

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

in which the expressions

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

satisfy the inequalities (compare [11])

$$-15\left(\max\left(\frac{1}{2}\log|a|_\infty, \frac{1}{3}\log|b|_\infty\right) + \log 2\right) \leq d(2^{i-1}P, 2^{i-1}P)$$

$$\leq 6\left(\frac{1}{4}\min\left(\frac{1}{2}\log|a|_\infty, \frac{1}{3}\log|b|_\infty\right) + \log 2\right)$$

for each $i\in\mathbb{N}$. Hence, the degree of accuracy in the calculation of $\hat{h}(P)$ is evident from

$$-\frac{5}{2^{2n}}\ (\max(\tfrac{1}{2}\log|a|_\infty,\ \tfrac{1}{3}\log|b|_\infty)+\ \log 2)$$
$$\le \hat{h}(P)-d(P)-\sum_{i=1}^{n}\frac{d(2^{i-1}P,\ 2^{i-1}P)}{2^{2i}}$$
$$\le \frac{2}{2^{2n}}(\tfrac{1}{4}\min(\tfrac{1}{2}\log|a|_\infty,\ \tfrac{1}{3}\log|b|_\infty)+\ \log 2).$$

On the basis of these inequalities, an approximate computation of $\hat{h}(P)$ is to be carried out for all $P=(\xi,\eta)\in C_Q\setminus\tilde{C}_Q$ such that $d(P)<2\delta$. that is, in view of $\xi=\frac{x}{z}$ for $x,z\in\mathbb{Z}$,

$$\tfrac{3}{2}\max(\tfrac{1}{2}\log|a|_\infty+\log|z|_\infty,\ \tfrac{1}{3}\log|b|_\infty+\log|z|_\infty,\ \log|x|_\infty)$$
$$< 9\max(\tfrac{1}{2}\log|a|_\infty,\ \tfrac{1}{3}\log|b|_\infty)+\ 10\log 2.$$

This procedure yields eventually the searched bound h'.

4. The "infinite" descent. Let us suppose that we have found by trial and error all points $P'\in C_Q\setminus\tilde{C}_Q$ satisfying the inequality for d(P') as it was given in Manin's theorem. Denote these points by $P'_1,\ldots,P'_{k'}$. According to the theorem, the points $P'_1,\ldots,P'_{k'}$ generate a certain subgroup $\hat{C}'_Q\cong C'_Q/\tilde{C}_Q$ of finite index in the maximal free subgroup $\hat{C}_Q\cong C_Q/\tilde{C}_Q$ of rank r in $C_Q$. Since there holds $|\hat{C}'_Q/2\hat{C}'_Q|=2^r$, it is at this point already possible to determine the rank r of C over Q by finding all relations modulo $2\hat{C}'_Q$ satisfied by $P'_1,\ldots,P'_{k'}$. Here one has to use the duplication formula.

To exhibit a basis for the group $\hat{C}_Q$ we first compute the classes of the points $P'_1,\ldots,P'_{k'}$ modulo the subgroup $2\hat{C}_Q$ of $\hat{C}_Q$ by trying to "divide by two" all differences $P'_i-P'_j\ (1\le i<j\le k')$. This is again accomplished by virtue of the duplication formula. Let $P'_{i_1},\ldots,P'_{i_k}$ be representatives of the distinct classes modulo $2\hat{C}_Q$ thus obtained. Then, one carries out the "division by two" as often as possible for each of the points $P'_{i_1},\ldots,P'_{i_k}$ and all their finite sums. In this way one ends up with certain maximal 2-powers $2^{l_{\nu_1\ldots\nu_\alpha}}$ such that

$$P'_{i_{\nu_1}}+\ldots+P'_{i_{\nu_\alpha}}=2^{l_{\nu_1\ldots\nu_\alpha}}P_{\nu_1\ldots\nu_\alpha}\quad(1\le\nu_1<\ldots<\nu_\alpha\le k)$$

for some points $P_{\nu_1 \dots \nu_\alpha} \in \hat{C}_Q$. This is true because the subgroup $\hat{C}_Q'$ has finite index in $\hat{C}_Q$. Observe also that the $P_{i_\rho}'$ $(\rho=1,\dots,k)$ have bounded d-value and hence bounded Néron-Tate height $\hat{h}$ by their construction in accordance with Manin's theorem. If need be, this process has to be repeated for the new points which result from the above "divisions by two".

After finitely many steps of this type we shall have constructed a set of generators for the whole group $\hat{C}_Q/2\hat{C}_Q$. Let $P_1,\dots,P_r$ be representatives in $\hat{C}_Q$ of a basis of the factor group $\hat{C}_Q/2\hat{C}_Q$. Then, by the "infinite" descent made in the proof of the Mordell-Weil theorem, these points together with certain other points $Q_1,\dots,Q_n$ in $\hat{C}_Q$ of bounded height $\hat{h}$ and hence of bounded d-value generate the whole group $\hat{C}_Q$ itself. It can in fact be shown that it suffices to choose $Q_1,\dots,Q_n$ as the entirety of all points $Q \in \hat{C}_Q \setminus \tilde{C}_Q$ fulfilling the condition

$$\hat{h}(Q) \leq 1+\max\{\hat{h}(P_{j_1}+\dots+P_{j_\rho})/1 \leq j_1 < \dots < j_\rho \leq r\}.$$

By virtue of the estimate indicated for the difference $d(P)-\hat{h}(P)$ in section 3, this condition can be converted into an inequality for the d-values, namely,

$$d(Q) \leq 1+\delta+2(2r-1)r \log 2+(2r-1)r \max_{i=1,\dots r}\{d(P_i)\}.$$

Here we have utilized the property of the Néron-Tate height $\hat{h}$ to be a positive definite quadratic form on $\hat{C}_Q$. The values $d(P_i)$ are bounded by an expression which depends in some way on the bound displayed in Manin's theorem. For example, if the process of "dividing by two" comes to an end already after the first step, one easily gets for $d(P_i)$ the crude bound

$$d(P_i) \leq \delta + \frac{(2k-1)k}{2^l}\left(2 \log 2+\delta + \frac{2^{2r}}{c_r^2} H'^2 \max(1,h'^{2(1-r)})\right), \text{ where}$$

$l:=\min\{l_{\nu_1 \dots \nu_\alpha}\}$ is taken from the relations by which the points $1 \leq \nu_1 < \dots < \nu_\alpha \leq k$

$P_i$ arise from the $P_i'$.

In any case the points $Q_1,\ldots,Q_n$ satisfying the above inequaltiy for $d(Q)$ are found by applying once more the successive minima method from geometry of numbers.

Finally, one gets a basis of the group $\hat{C}_Q$ by applying the elementary divisor theorem to the set of generators $P_1,\ldots,P_r$, $Q_1,\ldots,Q_n$ of $\hat{C}_Q$. Since the torsion subgroup $\tilde{C}_Q$ of the rational point group $C_Q$ is already known by section 1, we arrive at a basis of the whole group $C_Q=\tilde{C}_Q\oplus\hat{C}_Q$.

5. An estimate for the determinant. It is at this stage where the Weil conjecture and the Birch and Swinnerton-Dyer conjecture enter the picture and hence where things become hypothetic.
Let us briefly report on Manin's [2] ideas in this connection. For $N\in\mathbb{N}$ denote by $X_N$ the curve uniformizable by the group

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} A & B \\ C & D\end{smallmatrix}\right)\in PSL(2,\mathbb{Z}) \mid C \equiv 0 \bmod N\}$$

such that $X_N$ can be identified with the compactification of $H/\Gamma_0(N)$, H designating the complex upper half-plane. An elliptic curve C over $\mathbb{Q}$ of conductor N is said to be a Weil curve if it arises from $X_N$ by a morphism and if certain additional conditions are fulfilled (see [2]). Weil's conjecture now asserts that every elliptic curve C over $\mathbb{Q}$ is a Weil curve. Taking the Weil conjecture for granted, it can be shown that the canonical L-series of C over $\mathbb{Q}$ defined by the Euler product

$$L(C,s) = \prod_{p\in\mathbb{P}} L(C_p,s),$$

which is known to converge in the complex half-plane Re $s>\frac{3}{2}$, can be analytically continued over the whole complex plane. Here we have (cf.[7],[9])

$$L(C_p,s) := ((1-\alpha_p p^{-s})(1-\bar{\alpha}_p\, p^{-s}))^{-1}$$

for all primes $p\in\mathbb{P}$ at which C has good reduction such that $C_p:=C \bmod p$ is again an elliptic curve, this time defined over the prime field $\mathbb{F}_p$ of characteristic p. The quantities $\alpha_p$ and $\bar{\alpha}_p$ are characterized by the properties that

$|\alpha_p|_\infty = |\bar{\alpha}_p|_\infty = \sqrt{p}$ and $N_p = 1+p-\alpha_p-\bar{\alpha}_p$,

$N_p$ designating the number of points of $C_p$ over $\mathbb{F}_p$. For the primes $p \in \mathbb{P}$ at which C has bad reduction we have

$L(C_p,s) := (1-p^{-s})^{-1}$, $(1+p^{-s})^{-1}$, or 1

according as the reduced curve $C_p := C \bmod p$ has an ordinary double point with distinct rational tangents, an ordinary double point with irrational tangents or a cusp. (cf. [2]).

The Birch and Swinnerton-Dyer conjecture is now the assertion that, near s=1, there holds the asymptotic expansion

$$L(C,s) \sim (s-1)^r \frac{|Ш|H}{|\tilde{C}_{\mathbb{Q}}|^2} M,$$

where Ш stands for the Tate-Shafarevich group and M is a well-defined factor due to the infinite prime of $\mathbb{Q}$ and to the primes $p \in \mathbb{P}$ at which C has bad reduction. Using this conjecture, an upper bound $\Lambda$ for the r-th derivative $\frac{1}{r!} L^{(r)}(C,s)$ of $L(C,s)$ at s=1 such that

$$|\tfrac{1}{r!} L^{(r)}(C,1)|_\infty \leq \Lambda,$$

and a lower bound $\lambda$ for the factor M such that

$$M \geq \lambda > 0,$$

Manin [2] derives the estimate

$$H \leq H' := |\tilde{C}_{\mathbb{Q}}|^2 \wedge \lambda^{-1}$$

for the determinant H of the elliptic curve C over $\mathbb{Q}$.
It is because of this portion of Manin's algorithm that it must be termed "conditional".

6. Concluding remarks. Although we have outlined here some handy methods and devices for the implementation of certain subroutines of Manin's algorithm, there remains still a lot of detailed work to be done. Moreover, our discussion is somewhat

theoretical and speculative. Manin quotes in [2] Shafarevich's opinion on the algorithm according to which the algorithm should be used to prove the algorithmic insolubility (!) of the problem of determining a basis of the group $C_{\mathbb{Q}}$ of rational points of an elliptic curve $C$ over $\mathbb{Q}$ and to refute (!) the Birch and Swinnerton-Dyer conjecture. Perhaps it would be a good possibility to start with a consideration of the elliptic curves treated by Stephens [7] and combine the methods of Manin with those of Stephens.

Hopefully this lecture will stimulate further research on Manin's algorithm with the ultimate aim of settling the above-mentioned problems one way or the other.

References

1. V.A.Dem'janenko, Bounded torsion of elliptic curves. Mat. Zametki 12(1972), 53-58 = Math. Notes 12(1972), 464-466.

2. 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.

3. B. Mazur and J. Tate, Points of order 13 on elliptic curves. Inventiones math. 22(1973), 41-49.

4. T. Nagell, Sur les propriétés arithmétiques des cubiques planes du premier genre. Acta Math. 52 (1929), 93-126.

5. A.P. Ogg, Rational points of finite order on elliptic curves. Inventiones math. 12 (1971), 105-111.

6. D.E. Penney and C. Pomerance, A search for elliptic curves with large rank. Math. Comp. 28,no. 127 (1974), 851-853.

7. N.M. Stephens, The diophantine equation $X^3+Y^3=DZ^3$ and the conjectures of Birch and Swinnerton-Dyer. J. reine angew. Math. 231 (1968), 121-162.

8. J. Tate, Rational points on elliptic curves. Philips Lectures, Haverford College 1961.

9. H.G. Zimmer, Computational Problems, Methods, and Results in Algebraic Number Theory. Lecture Notes in Math., Vol.262, Springer-Verlag, Berlin-Heidelberg-New York 1972.

10. H.G. Zimmer, Ein Analogon des Satzes von Nagell-Lutz über die Torsion einer elliptischen Kurve. J. reine angew. Math. 268|269 (1974), 360-378.

11. H.G. Zimmer, On the difference of the Weil height and the Néron-Tate height.
To appear in Math. Z.

12. H.G. Zimmer, Points of finite order on elliptic curves over number fields.
To appear.

Fachbereich 9 Mathematik
Universität des Saarlandes
D-66 Saarbrücken