[M] A. A. Matveev, *A lower bound for linear forms in logarithms*, in *Transcendental Number Theory and its Applications*, Proc. Conf. Moscow Univ., Feb. 2–4, 1983 (Izd. Mosk. Univ. 1983).

[PW] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, 1988, pp. 280–312.

[W] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. 37 (1980), 257–283.

DEPARTMENT OF MATHEMATICS AND STATISTICS
BOWLING GREEN STATE UNIVERSITY
Bowling Green, Ohio 43403-0221 U.S.A.

Received on 30.7.1987
and in revised form on 30.5.1988 (1739)

ACTA ARITHMETICA
LV (1990)

Constants for lower bounds for linear forms in the logarithms of algebraic numbers II
The homogeneous rational case

by

JOSEF BLASS*, A. M. W. GLASS*, DAVID K. MANSKI**, DAVID B. MERONK** and RAY P. STEINER* (Bowling Green, Ohio)

1. Introduction. In this note we compute the constant for the lower bound of a homogeneous linear form in logarithms of non-zero algebraic numbers with rational coefficients. The constant we obtain improves that in [Wa]. Actually, we will derive the result from the special case when the rational coefficients are integers and a certain strong independence holds. In this paper, unlike the previous one, we only address the strongly independent case; although reduction to the strongly independent case can be done as in the previous paper (see Corollary 2 below), there may be cases when a reduction to strong independence is possible without increasing the bounds quite so much (see, e.g., [BS]). We will again follow [Wa] but with the modification given in [LMPW]; the reader will need to consult both papers since we will only give those steps in the proof which are different from those of [Wa] and [LMPW] (for more details, see [BGMMS1]). We will not bother to determine the constants of [PW, §5] since they are far greater ($c_5 \geqslant 2^n(n+1)^{n+2}n!$; since $c_0 \geqslant 1$,

$$c_0 c_1 c_2^n c_3 c_4 n^n/n! \geqslant 2^{n^2+2n}(n+1)^{n^2+5n+4}(n!)^{n+1}.$$

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers, $K = \boldsymbol{Q}(\alpha_1, \ldots, \alpha_n)$ and $D = [K:\boldsymbol{Q}]$. Let

$$V_1 = \max\{h(\alpha_1), |\log\alpha_1|/D, 1/D\}$$

and

$$V_{j+1} = \max\{h(\alpha_{j+1}), |\log\alpha_{j+1}|/D, V_j\} \quad (1 \leqslant j \leqslant n-1),$$

* Research supported in part by Bowling Green State University Faculty Research grants and a Challenge Grant from the Ohio Board of Regents.

** Research supported in part by a grant from the Bowling Green State University Graduate College.

We all wish to acknowledge, with thanks, the warm encouragement and assistance given by Michel Waldschmidt for this work; without it, this paper would not have been possible.

where again $h(\alpha)$ is the absolute logarithmic height of α. Let

$$a_j = DV_j/|\log\alpha_j| \geqslant 1 \quad (1 \leqslant j \leqslant n) \quad \text{and} \quad \frac{1}{a} = \frac{1}{n}\sum_{j=1}^{n}\frac{1}{a_j};$$

let $V_0^+ = 1$ and $V_j^+ = \max\{1, V_j\}$ $(1 \leqslant j \leqslant n)$. Let $b_1, \ldots, b_n$ be rational integers, $B_n \geqslant |b_n|$ and $B \geqslant \max\{|b_j|: 1 \leqslant j \leqslant n-1\}$. Let $E_2 = \min\{e^{2DV_1}, 4Da\}$ and $W \geqslant \log(B_n/V_1 + B/V_n + 1)$. Assume further that

$$W \geqslant \max\{\log E_2, (2/nD)\log E_2, n\log(2^7 nDV_n^+)\}$$

and that $\alpha_1, \ldots, \alpha_n$ are strongly independent (i.e., $[K(\alpha_1^{1/2}, \ldots, \alpha_n^{1/2}):K] = 2^n$). Let $M = 2(2^8 nDV_{n-1}^+ E_2)^n$ and $\Lambda = b_1\log\alpha_1 + \ldots + b_n\log\alpha_n$.

THEOREM. *Under the above hypotheses $\Lambda = 0$ or*

$$|\Lambda| > \exp\left\{-(24e^2)^n\frac{n^{2n+1}}{n!}2^{21}D^{n+2}V_1\ldots V_n(\log M)W/(\log E_2)^{n+1}\right\}.$$

Now

$$(24e^2)^n\frac{n^{2n+1}}{n!}\frac{\log M}{(\log E_2)^{n+1}} \leqslant (24e^3)^n 2^{23} n^{n+2}\frac{\log(DV_{n-1}^+ E_2)}{(\log E_2)^{n+1}}.$$

This compares with $2^{9n+26}n^{n+4}\log(DV_{n-1}^+ E_1)/(\log E_1)^{n+1}$ of [Wa, Proposition 3.8]. Since $E_2 \geqslant E_1$, this gives an improvement in excess of $8n^2(1.06)^n$. In [M], the claim is $e^8 n^{n+4.5}(2e^3)^n\log(DV_{n-1}^+ E_2)$ in place of $(24e^2)^n\frac{n^{2n+1}}{n!}\frac{\log M}{(\log E_2)^{n+1}}$, an improvement of at most $\left(\frac{12}{\log E_2}\right)^n\frac{2^{11}}{n^{2.5}} \leqslant (8\frac{2}{3})^n 2^{11}/n^{2.5}$.

Finally, we observe that the allegation in [ACHP] concerning the constant in [LMPW] seems to be quite without foundation; indeed, [ACHP] needs to be reworked. The constant we give here is the best for which there is a valid proof in the literature.

If $b_1, \ldots, b_n$ are merely rational numbers we easily deduce that if the positive rational integer d is such that $db_1, \ldots, db_n$ are all rational integers, then the theorem holds if $W \geqslant \log(dB_n/V_1 + dB/V_n + 1) + \log d$ (still assuming that $\alpha_1, \ldots, \alpha_n$ are strongly independent). Hence

COROLLARY 1. *If $b_1, \ldots, b_n$ are rational, $\alpha_1, \ldots, \alpha_n$ are strongly independent and d is at least as large as the least common denominator of $b_1, \ldots, b_n$, then $\Lambda = 0$ or*

$$|\Lambda| > \exp\left\{-(24e^2)^n 2^{21}\frac{n^{2n+1}}{n!}D^{n+2}V_1\ldots V_n(\log M)(W + \log d)/(\log E_2)^{n+1}\right\}$$

if

$$W \geqslant \max\{\log(dB_n/V_1 + dB/V_n + 1), \log E_2, (2/nD)\log E_2, n\log(2^7 nDV_n^+)\}.$$

Note that we have only bothered with case that the prime is 2. If $[K(\alpha_1^{1/q}, \ldots, \alpha_n^{1/q}):K] = q^n$ for some prime q other than 2, the only modifications necessary are those of the previous paper; i.e., the Proposition of [BGMMS2] holds provided only that

$$W \geqslant \max\{\log(dB_n/V_1 + dB/V_n + 1), \log E_2, (q/nD)\log E_2, n\log(2^5 nq^2 DV_n^+)\},$$

where E_2 is defined as in [BGMMS2].

Let $\bar{B} = \max\{B_n, B\}$. If we remove the assumption that $\alpha_1, \ldots, \alpha_n$ are strongly independent, then we must replace each V_j by jV_j $(1 \leqslant j \leqslant n)$, W by W^* of the previous paper (where here $W \geqslant \log(nd\bar{B}/V_1 + d\bar{B}/V_n + 1)$ instead of $W \geqslant \{h(b_j): 1 \leqslant j \leqslant n\}$) and E_2 by $\bar{E}_2 = \min\{e^{2DV_1}, 4a\}$ (where $\frac{1}{a_j} = \frac{1}{j}\sum_{i=1}^{j}\frac{1}{a_i}$ and $\frac{1}{a} = \frac{1}{n}\sum_{j=1}^{n}\frac{1}{a_j}$). Hence

COROLLARY 2. *If $b_1, \ldots, b_n$ are rational numbers and $\alpha_1, \ldots, \alpha_n$ are non-zero algebraic numbers, then with the above notation and hypotheses, $\Lambda = 0$ or*

$$|\Lambda| > \exp\left\{\frac{-(24e^2)^n 2^{20}}{(\log\bar{E}_2)^{n+1}}D^{n+2}V_1\ldots V_n(\log\bar{M})(W^* + C(n, D))\right\}$$

where

$$C(n, D) = n(n+1)\log(D^3\bar{V}_n) + x_n^*/n + \log d, \quad \bar{V}_j = \max\{jV_j, 1\} \quad (1 \leqslant j \leqslant n)$$

x_n^* is defined in the previous paper, and $\bar{M} = M(\bar{V}_{n-1}/V_{n-1}^+)^n$.

Actually, $(24e^2)^n 2^{21}$ is not optimal. A computer search shows that for $n = 4$ and $D = 8$ $(D = 20)$, 2^{39} (2^{38}) suffices. Thus, for example, the constant obtained for the constant for the logarithms associated with the real quartic extension of the field of rational numbers having least discriminant is improved by a factor of 2^{30} over [Wa]. A table for the constant for small values of n and D (obtained by computer search) is included for the sake of completion.

We also provide at the end of Section 2 a modified version of the theorem and its corollaries which though more complicated to state, actually gives better constants in many practical cases.

2. Proof of the Theorem. As in our previous paper, we let $M = 2(2^8 nDV_{n-1}^+ E_2)^n$ and obtain

$$(3.7^0) \qquad \log M \leqslant 2\bar{B}n^2 DV_{n-1}^+ + n\log E_2 \leqslant 2\bar{A}n^2 DV_{n-1}^+\log E_2$$

where

$$\bar{A} = \begin{cases} 0.84 & \text{if } n, D \geqslant 2, \\ 2.79 & \text{if } n = D = 1, \\ 1.54 & \text{otherwise}; \end{cases} \qquad \bar{B} = \begin{cases} 0.98 & \text{if } n, D \geqslant 2, \\ 3.17 & \text{if } n = D = 1, \\ 1.78 & \text{otherwise}. \end{cases}$$

Let

$$U = c_0 c_1 c_2^n c_3 c_4 \frac{n^{2n+1}}{n!} 2^{3n} D^{n+2} V_1 \ldots V_n (\log M)\, W/(\log E_2)^{n+1}$$

and assume that

$$c_0 \geqslant 2, \quad c_0' = (c_0 + 2^{-9}) e^{1/256}, \quad c_0'' = (c_0 + 2^{-8}) e^{1/256}, \quad c_0'' c_4 \leqslant 2^{14},$$
$$c_0'' c_4 c_3 \leqslant 2^{22}, \quad c_4 \geqslant 2^4,$$

(3.2⁰) $$2^3 \leqslant c_3 \leqslant 2^{12}, \quad 2,\ 2^4/n \leqslant c_2 \leqslant 2^7/e, \quad c_1 = 2.5.$$

Let

$$\upsilon = \begin{cases} 2 & \text{if } n = D = 1 \text{ and } q \in \{2, 3\}, \\ 1 & \text{if } n = 1 \text{ and } qD \in \{4, 5, 6\}, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$2^{22+\upsilon} n^2 2^{n+1} D^2 \max\{W, V_n^+, WV_n^+/\log E_2\} \leqslant U$$

provided that

(3.3⁰) $$c_0 c_1 c_2^n c_3 c_4 \geqslant 2^{23+\upsilon}/(2n)^n.$$

We will assume (3.3⁰) from now on. (For example if $n \geqslant 3$, this holds if $c_0 = 2^2$, $c_2 = 2^5$ and $c_3 = c_4 = 2^9$.)

As in [Wa], we let

$$S = 2[c_3 nDW/\log E_2], \quad T = [U/c_1 c_3 2^n DW],$$
$$L_{-1} = [W/(\log E_2)^{n+1}], \quad L_0 = [U/c_1 c_4 2^n D (L_{-1}+1) \log M]$$

and

$$L_j = [U/c_1 c_2 n 2^{n+1} DSV_j] \quad (1 \leqslant j \leqslant n).$$

Note that our conditions imply $L_1 \geqslant \ldots \geqslant L_n \geqslant 1$.

It is easy to establish from these definitions that

(3.9⁰) $$T \leqslant e^{(1+2/n)W},$$

(3.10⁰) $$4E_2 L_n \leqslant M^{1+1/n},$$

(3.12⁰) $$(L_{-1}+1) \log M \leqslant (U/2^{22} 2^n D)\left(\bar{B} + \frac{1}{2nD}\right)\left(\frac{1}{(\log 4)^n} + 1\right),$$

(3.13⁰) $$L_1 + L_n \leqslant 2L_1 \leqslant e^{(1+1/n)W},$$

(3.14⁰) $$12(2^n L_n E_2 S) \leqslant (L_{-1}+1) M^{1+2/n},$$

using (3.7⁰), (3.2⁰) and $\log E_1 \leqslant E_1/e$.

We next determine f_1–f_7. As in our previous paper we obtain

$$f_1 = \frac{1+\frac{2}{n}}{c_1 c_3} + \frac{1+\frac{2}{n}}{c_1 c_4} + \frac{\left(1+\frac{2}{n}\right)}{2^{22}}\left(\frac{1}{(\log 4)^n} + 1\right)\left(\bar{B} + \frac{1}{2nD}\right)$$

and

$$f_2 = \frac{\log 3}{c_1 c_3}\left(\frac{1}{(\log 4)^{n+1}} + \frac{1}{9n \log 2}\right) + \frac{2\left(1+\frac{1}{n}\right)}{c_1 c_4} + \frac{2\left(1+\frac{1}{n}\right)}{2^{22}}\left(\frac{1}{(\log 4)^n} + 1\right)\left(\bar{B} + \frac{1}{2nD}\right).$$

As shown in [LMPW],

$$\log\left(\prod_{r=1}^{n-1} |\Delta(b_n \lambda_r - b_r \lambda_n; \tau_r)|\right) \leqslant T \log 2e\left(1 + \frac{(n-1)(BL_n + b_n L_1 + 1)}{T}\right).$$

Since $\log x \leqslant (x \log 2e)/2e$ if $x \geqslant 2e$, we obtain

$$T\left(1 + \frac{(n-1)(BL_n + b_n L_1 + 1)}{T}\right) \log(2e)$$

as an upper bound for the latter and hence,

$$\log\left(\prod_{r=1}^{n-1} |\Delta(b_n \lambda_r - b_r \lambda_n; \tau_r)|\right) \leqslant \frac{U}{2^n D} \frac{1}{c_1 c_3}.$$

Thus we obtain

$$f_3 = \frac{1}{c_0 - 1}\left\{f_1 + f_2 + \frac{1}{2c_1 c_2} + \frac{1}{c_1 c_3} + \frac{2 + 1/(2n)}{2^{22}}\right\} + \frac{1}{2^{24} n}$$

and

$$f_3' = f_3 + \frac{2D}{2^{23} n^2}.$$

Consequently we may take

$$f_4 = \frac{1}{2c_1 c_2} + \frac{1}{2^n D}\left(f_1 + f_3' + \frac{1}{c_1 c_3} + \frac{2}{2^{22}}\right).$$

That $f_4 \leqslant 1/2$ will follow immediately from (3.1⁰). As in our previous paper, we next deduce that

$$f_5 = f_6 = f_1 + f_2 + f_3 + \frac{1}{2c_1 c_2} + \frac{1}{c_1 c_3} + \frac{2 + n^{-1}}{2^{22}}$$

and

$$f_7 = \frac{1}{4c_1} - \left\{\frac{f_1}{2D} + \frac{f_3'}{2D} + \frac{(D/4)+1}{2Dc_1 c_3} + \frac{4}{c_1 c_4} + \frac{1}{2^{23} D}\left(2 + \frac{2D}{n} + \frac{c_3}{n^2}\right)\right\}.$$

As before, to obtain the desired contradiction we require that

$$f_7 \geqslant f_6 + \frac{1}{2^{24} n}.$$

This is equivalent to

$$(3.1^0) \quad 1 \geqslant \frac{18}{c_2} + \frac{1}{c_3}\left(8.5 + \frac{4}{D} + \frac{8}{n} + \frac{4}{nD} + 4\log 3\left(\frac{1}{(\log 4)^{n+1}} + \frac{1}{9n\log 2}\right)\right)$$
$$+\frac{1}{c_4}\left(12 + \frac{16}{n} + \frac{2}{D} + \frac{4}{nD}\right)$$
$$+\frac{c_1}{2^{22}}\left\{8 + \frac{12}{n} + \frac{2}{n^2} + \frac{1}{D}\left(4 + \frac{2}{n} + \frac{c_3}{n^2}\right)\right.$$
$$+\left(\frac{1}{(\log 4)^n} + 1\right)\left(\bar{B} + \frac{1}{2nD}\right)\left(12 + \frac{16}{n} + \frac{2}{D}\left(1 + \frac{2}{n}\right)\right)\Bigg\}$$
$$+\left(4 + \frac{2}{D}\right)\frac{1}{(c_0 - 1)}\left\{\frac{1}{2c_2} + \frac{1}{c_3}\left(2 + \frac{2}{n} + \frac{\log 3}{(\log 4)^{n+1}} + \frac{\log 3}{9n\log 2}\right)\right.$$
$$\left.+\frac{3 + (4/n)}{c_4} + \frac{c_1}{2^{22}}\left(2 + \frac{1}{n} + \left(\bar{B} + \frac{1}{2nD}\right)\left(3 + \frac{4}{n}\right)\left(\frac{1}{(\log 4)^n} + 1\right)\right)\right\}.$$

These equations are satisfied by $c_0 = 2$, $c_2 = 2^6$, $c_3 = 171$ and $c_4 = 2^8$ if $n = 1$; by $c_0 = 3$, $c_2 = 2^5$, $c_3 = 131$ and $c_4 = 2^8$ if $n = 2$ or 3; $c_0 = 5$, $c_2 = 3e^2$, $c_3 = 369$ and $c_4 = 2^8$ if $n \geqslant 4$. This completes the proof of the first part of the theorem.

As before the rest of the theorem is proved by first noting, as in the previous paper, that (3.9^0) and (3.13^0) may be modified to

$$T \leqslant e^{W^*/(n+1)}$$

and

$$2L_1 \leqslant e^{W^*/(n+1)}$$

respectively if $n \geqslant 3$ and W^* is sufficiently large. Hence we obtain

$$1 \geqslant \frac{18}{c_2} + \frac{1}{c_3}\left(4.5 + \frac{2}{D} + \frac{4}{n+1} + \frac{2}{(n+1)D} + 4\log 3\left(\frac{1}{(\log 4)^{n+1}} + \frac{1}{5n(n+1)}\right)\right)$$
$$+\frac{1}{c_4}\left(12 + \frac{16}{n} + \frac{2}{D} + \frac{4}{nD}\right) + \frac{c_1}{2^{22}}\left(8 + \frac{4}{D} + \frac{12}{n} + \frac{2}{nD} + \frac{2}{n^2} + \frac{c_3}{n^2 D}\right.$$
$$+\left(\bar{B} + \frac{1}{2nD}\right)\left(12 + \frac{16}{n} + \frac{2}{D} + \frac{4}{nD}\right)\left(1 + \frac{1}{(\log 4)^n}\right)\Bigg)$$

$$+\frac{(4 + (2/D))}{c_0 - 1}\left\{\frac{1}{2c_2} + \frac{1}{c_3}\left(1 + \frac{1}{n+1} + \log 3\left(\frac{1}{(\log 4)^{n+1}} + \frac{1}{5n(n+1)}\right)\right)\right.$$
$$\left.+\frac{3 + (4/n)}{c_4} + \frac{c_1}{2^{22}}\left(\left(3 + \frac{4}{n}\right)\left(\bar{B} + \frac{1}{2nD}\right)\left(1 + \frac{1}{(\log 4)^n} + 1 + \frac{1}{n}\right)\right)\right\}.$$

If $n = 3$, this is satisfied by $c_0 = 5$, $c_2 = 2^5$, $c_3 = 56$ and $c_4 = 2^7$; if $n \geqslant 4$, this is satisfied by $c_0 = 5$, $c_2 = 3e^2$, $c_3 = 191$ and $c_4 = 2^8$. This establishes Theorem A. ∎

As in the previous paper, if $n \geqslant 25$, then setting $c_0 = 4$, $c_3 = 2^{10}$ and $c_4 = 2^{11}$, by (3.1^0) we may take c_2 to be 21.6 (and $c_2 \to 21.51$ approximately as $n \to \infty$). So the constant $2^{6n+22} n^{n+1}/e^n$ can be replaced by $(21.6)^n 2^{25} n^{n+1}$ if $n \geqslant 25$.

The computer gave minimum values for $c = c_0'' c_1 c_2'' c_3 c_4$ of the same order of magnitude as in the previous paper. Indeed, c can be taken to be 7/8 of the previous computer values if $2 \leqslant n \leqslant 10$ and $2 \leqslant D \leqslant 9$, .8 of the previous computer values if $2 \leqslant n \leqslant 10$ for all other values of D, and the previous computer values if $n = 1$.

Let $E_3 = 4$. Then (3.5) becomes $E_3 S \sum_{j=1}^{n} L_j |\log \alpha_j| \leqslant 2U/(c_1 c_2 q^n a)$. The proof of the Theorem goes through with the modifications that

(i) E_2 is replaced throughout by 4 and

(ii) the first summand on the right hand side of (3.1^0) is replaced by $(2 + (16/a))/c_2$. If, for example, $a = 16$ and $n \geqslant 4$, $(24e^2)^n 2^{21}$ is replaced by $5^n 2^{21}$. Hence we actually get an improvement of Matveev's claim (in this case) of at least $n^{2.5}/704$ which exceeds 1 if $n \geqslant 14$.

Similar considerations hold for the corollaries.

References

[ACHP] M. K. Agrawal, J. Coates, D. C. Hunt and A. J. van der Poorten, *Elliptic curves of conductor 11*, Math. Comp. 35 (1980), 991–1002.

[BS] A. Baker and C. L. Stewart, *On effective approximation to cubic irrationals*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, 1988, pp. 1–24.

[BGMMS1] J. Blass, A. M. W. Glass, D. Manski, D. B. Meronk and R. P. Steiner, *Constants for lower bounds for linear forms in logarithms: verifications*, Proc. Number Theory Sem. Université P. & M. Curie (ed. D. Bertrand), 88 (1988), II 1–31.

[BGMMS2] J. Blass, A. M. W. Glass, D. K. Manski, D. B. Meronk and R. P. Steiner, *Constants for lower bounds for linear forms in the logarithms of algebraic numbers I. The general case*, Acta Arith. 55 (1990), 1–13.

[LMPW] J. H. Loxton, M. Mignotte, A. J. van der Poorten and M. Waldschmidt, *A lower bound for linear forms in the logarithms of algebraic numbers*, C.R. Math. Rep. Acad. Sci. Math. XI (1987), 119–124.

[M] A. A. Matveev, *A lower bound for linear forms in logarithms*, in *Transcendental*

Number Theory and its Applications, Proc. Conf. Moscow Univ., Feb. 2–4, 1983 (Izd. Mosk. Univ. 1983).

[PW] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge Univ. Press, 1988, pp. 280–312.

[Wa] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arith. 37 (1980), 257–283.

DEPARTMENT OF MATHEMATICS AND STATISTICS
BOWLING GREEN STATE UNIVERSITY
Bowling Green, Ohio 43403-0221 U.S.A.

Received on 30.7.1987
and in revised form on 30.5.1988 (1740)

ACTA ARITHMETICA
LV (1990)

On the arithmetic of an elliptic curve over a Z_p-extension

by

FRANÇOIS RAMAROSON (Washington, D.C.)

1. Introduction. Let E/Q be an elliptic curve with conductor N. Assume that E admits a parametrization by modular functions and let φ be a Weil parametrization:

$$\varphi\colon X_0(N) \to E$$

where $X_0(N)$ is the Shimura canonical model for the Riemann surface $\mathscr{H}/\Gamma_0(N)$, quotient of the upper-half plane by the action by the group

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})\colon c \equiv 0 \pmod N\right\}.$$

For simplicity let us assume that N is prime and let K be an imaginary quadratic field in which N splits completely and with discriminant less than -4.

In [1], Gross developed the theory of Heegner points on $X_0(N)$. These points are rational over abelian extensions of K, and via the Weil parametrization mentioned above, they should contribute to the Mordell–Weil groups of the elliptic curve E over these abelian extensions.

Let now p be a prime which is ordinary for E, this means that E has good reduction at p and the trace of the Frobenius endomorphism of the reduced curve modulo p, is not divisible by p. For such a p, one can consider K_∞, the anticyclotomic Z_p-extension of K, which is contained in the union of all ring class fields corresponding to the orders of K of conductor p^n, $n = 0, 1, 2, \ldots$

The Heegner points are rational over these ring class fields and the Weil parametrization carries them over to E; taking norms gives points in the Mordell–Weil group of E rational over K_∞. The points so obtained in $E(K_\infty)$ fit together into an object called the Heegner module, which is a module over the relevant Iwasawa ring Λ.

In [6], Mazur made a precise conjecture concerning the structure of the Heegner module, namely, under a technical assumption, that it is a cyclic module of rank one, over the Iwasawa ring Λ.