Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Alfred J. Van der Poorten

The polynomial $x^3 + x^2 + x - 1$ and elliptic curves of conductor 11

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, n° 2 (1976-1977), exp. n° 17, p. 1-7

<http://www.numdam.org/item?id=SDPP_1976-1977__18_2_A1_0>

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1976-1977, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 17, 7 p.

28 février 1977

THE POLYNOMIAL $x^3 + x^2 + x - 1$ AND ELLIPTIC CURVES OF CONDUCTOR 11.

by Alfred J. VAN DER POORTEN

This is a summary of a more extensive report in preparation at present. For each positive integer N, let $\Gamma_0(N)$ be the group of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a, b, c, d are integers with $ad - bc = 1$ and c divisible by N. According to a conjecture of Taniyama-Weil (see [12]), all elliptic curves of conductor N, which are defined over the rational field $\underset{\sim}{Q}$, are parametrized by modular functions for $\Gamma_0(N)$. Until the present work, the first case, $N = 11$, has remained open.

Three curves of conductor 11 were known, namely

$$y^2 - y = x^3 - x^2 - 10x - 20 \tag{1}$$

$$y^2 - y = x^3 - x^2 \tag{2}$$

$$y^2 - y = x^3 - x^2 - 7820x - 263580 . \tag{3}$$

The first of these curves is a model for the compactification of the quotient $\mathcal{H}/\Gamma_0(11)$, $\mathcal{H}$ being the upper half plane. The second and third curves are isogenous to the first over $\underset{\sim}{Q}$. Hence all three curves are parametrised by modular functions for $\Gamma_0(11)$. Moreover, SERRE [7] has shown that, up to isomorphism, (2) and (3) are the only elliptic curves which are isogenous to (1) over $\underset{\sim}{Q}$. Thus the conjecture is true for $N = 11$ if, and only if, (1), (2) and (3) are the only elliptic curves of conductor 11 defined over $\underset{\sim}{Q}$, up to isomorphism. Below we describe a calculation which proves this to be the case.

1. Obtaining a Thue-Mahler equation.

Consider the field B of 2-division points of an elliptic curve E of conductor p. If E has no rational 2-division point then $B/\underset{\sim}{Q}$ has Galois group S_3; B is cubic cyclic over a field F with $F = \underset{\sim}{Q}[\sqrt{p}]$ or $\underset{\sim}{Q}(\sqrt{-p})$; and B/F is unramified except at 2 (see SETZER [8]). Let B be a field with the above properties (a "possible 2-division field for a prime p"). Denote by k a cubic extension obtained by adjoining the x-coordinate of one 2-division point to $\underset{\sim}{Q}$. Let O_k be the integers of k, and let $1, \omega_1, \omega_2$ be a basis of O_k as a $\underset{\sim}{Z}$-module. For any θ in O_k define M_θ to be the ring generated by θ; then M_θ is of finite index in O_k. Define $I(\theta)$ to be that index. Let D_θ be the discriminant of M_θ.

Let $\theta = u\omega_1 + v\omega_2$ with u, $v \in \underset{\sim}{Z}$. Then $\theta^2 = q_0 + q_1\,\omega_1 + q_2\,\omega_2$ where the q_i are quadratic forms in u, v, and $I(\theta) = |uq_2 - vq_1|$. Define the index form to be $f(u, v) = uq_2 - vq_1$. It is a homogeneous cubic with rational integer coefficients.

We note that $f(u, v)$ factors in k; indeed $|f(u, v)| = I(\omega_1)|N(u + \zeta v)|$ where $\zeta = (\omega_2' - \omega_2'')/(\omega_1' - \omega_1'')$ is in k (α, α', α'', are the conjugates of $\alpha \in k$).

We can find a model for the elliptic curve E of the shape

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6 \quad \text{with} \quad \Delta = \pm 2^{12} p^r$$

and such that $(\theta, 0)$ is a 2-division point on E, where $\theta = u\omega_1 + v\omega_2$ for some u, $v \in \underset{\sim}{Z}$. Then D_θ, the discriminant of $x^3 + a_2 x^2 + a_4 x + a_6$, is given by $\Delta/16 = \pm 2^8 p^r$. Let D be the field discriminant of k/Q. Then $D_\theta = I(\theta)^2 D$ so $f(u, v) = (D^{-1}(\pm 2^8 p^r))^{\frac{1}{2}}$. Now $D = \pm p$ or $\pm 4p$ so we have

$$f(u, v) = \pm 2^e p^s$$

where $r = 2s + 1$, s an integer, and $e = 3$ if 2 ramifies in k/Q, $e = 4$ if not; the sign of Δ is the same as that of D.

Now suppose $f(u, v) = au^3 + bu^2 v + cuv^2 + dv^3$ and $f(u_0, v_0) = \pm 2^e p^s$ where the discriminant of f is $\pm 2^{8-2e} p$. Let $k = \underset{\sim}{Q}(\omega_1)$ where ω_1 is a zero of $X^3 + bX^2 + acX + a^2 d$, and define ω_2 by $\omega_2^2 = -ac - b\omega_1 + a\omega_2$. Then ω_2 is a zero of $X^3 - cX^2 + bdX - ad^2$. Then 1, ω_1, ω_2 is a basis for O_k and f is the form giving $I(\theta)$ for $\theta = u\omega_1 + v\omega_2$. Let $X^3 + a_2 X^2 + a_4 X + a_6$ be the minimal polynomial for $u_0\,\omega_1 + v_0\,\omega_2$. Then for

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6, \tag{4}$$

we have $\Delta = \pm 2^{12} p^{2s+1}$. After checking (4) for reduction at 2 and p one may obtain, from solutions of $f(u, v) = \pm 2^e p^s$, an elliptic curve of conductor p given by (4).

Let $p = 11$. Then E has no rational 2-division point and the only possible 2-division field is the field generated by the zeros of $X^3 + X^2 + X - 1$, which has discriminant -44 (see [4]). Thus to find all elliptic curves over $\underset{\sim}{Q}$ with conductor 11, it suffices to consider integer solutions u, v with $(u, v, 11) = 1$ on the Thue-Mahler equation

$$u^3 - u^2 v + uv^2 + v^3 = 2^3 \cdot 11^s .$$

Plainly, for any solution, $2/u$, $2/v$.

The above argument is taken from SETZER [8]. A different, and extremely involved, argument of AGRAWAL and COATES [1] also leads to the conclusion reached above.

2. Obtaining linear forms in logarithms.

Let $\varepsilon \in \underset{\sim}{R}$, δ and $\overline{\delta}$ be the zero of $p(x) = x^3 + x^2 + x - 1$. Then in $\underset{\sim}{K=Q}(\varepsilon)$,

we have $11 = (1 + 2\varepsilon)(2 + \varepsilon^2)^2$, and

$$f(u , v) = (u + \varepsilon v)(u + \delta v)(u + \overline{\delta} v) = 11^s$$

implies

(5) $$u + v = \pm \varepsilon^{b_0} (1 + 2\varepsilon)^{b_1} (2 + \varepsilon^2)^{b_2} , \quad b_i \in \underset{\sim}{Z} ; \quad b_1 + b_2 = s ; \quad b_1 , b_2 \geqslant 0 ,$$

where we note that ε is a fundamental unit of $\underset{\sim}{K}$.

By the identity

$$(\delta - \overline{\delta})(u + \varepsilon v) + (\overline{\delta} - \varepsilon)(u + \delta v) + (\varepsilon - \delta)(u + \overline{\delta} v) = 0 ,$$

we have

(6) $$1 - \frac{\varepsilon - \delta}{\varepsilon - \overline{\delta}} \frac{u + \overline{\delta} v}{u + \delta v} = \frac{\delta - \overline{\delta}}{\varepsilon - \overline{\delta}} \frac{u + \varepsilon v}{u + \delta v} ,$$

which by (5) and its conjugates is

(7) $$1 - \frac{\varepsilon - \delta}{\varepsilon - \overline{\delta}} \left(\frac{\delta}{\overline{\delta}}\right)^{b_0} \left(\frac{2 + \delta^2}{2 + \overline{\delta}^2}\right)^{b_2 - 2b_1} = \frac{\delta - \overline{\delta}}{\varepsilon - \overline{\delta}} \left(\frac{\varepsilon}{\overline{\delta}}\right)^{b_0} \left(\frac{2 + \varepsilon^2}{2 + \overline{\delta}^2}\right)^{b_2 - 2b_1} .$$

Write $h_0 = b_0$, $h_1 = 2b_1 - b_2$ and $H = \max(|h_0| , |h_1|)$. AGRAWAL and COATES [1] verified by hand that for $H \leqslant 17$ the equation [7] gives rise to 7 solutions of $f(u , v) = 11^s$, 3 of which, namely $u = 0$, $v = 1$, $s = 0$ $(h_0 = 1 , b_1 = b_2 = 0)$; $u = 4$, $v = -3$, $s = 2$ $(h_0 = 1 , b_1 = 2 , b_2 = 0)$ and respectively $u = 56$, $v = -103$, $s = 0$ $(h_0 = 17 , b_1 = b_2 = 0)$ give rise to elliptic curves of conductor 11, namely the curves (1), (2) and respectively (3) mentioned above.

We should remark that, for $s = 0$, the solutions are already reported by DELONE and FADEEV [4].

Thus it suffices for us to show that (7) has no solutions with $H > 17$ (or, if there be solutions, that these do not give rise to curves of conductor 11). It is easily seen (see below) that not both b_1 , b_2 are positive, and in any event $b_2 \leqslant 1$.

We write $\gamma_0 = \delta/\overline{\delta}$, $\gamma_1 = (2 + \overline{\delta}^2)/(2 + \delta^2)$, $\gamma_2 = (\varepsilon - \overline{\delta})/(\varepsilon - \delta)$. Then we have

(8) $$|1 - \gamma_0^{h_0} \gamma_1^{h_1} \gamma_2^{-1}| < (0{,}20582 \times 2\pi) e^{-\Delta' H} ,$$

where $\Delta' = 0{,}8665$, provided that $h_0 \geqslant |h_1|$.

Further, writing $\gamma_0 = \exp(2\pi i \psi_0)$, $\gamma_1 = \exp(2\pi i \psi_1)$, $\gamma_2 = \exp(2\pi i \psi_2)$, we obtain

(9) $$\|h_0 \psi_0 + h_1 \psi_1 - \psi_2\| < e^{-\Delta H} , \quad \Delta = 3/4 , \quad H > 17 \text{ say}$$

(where, as usual, $\|x\|$ denotes the distance of the real number x from the nearest integer).

We now turn to the 11-adic situation. The polynomial $p(x)$ splits over $\underset{\sim}{Q}_{11}(\sqrt{-11})$ (we shall write $\theta = \sqrt{-11}$ in the 11-adic case) with zeros

$\varepsilon = 5 + 7.11 + 2.11^2 + 7.11^3 + 2.11^4 + \ldots$; $\delta = 8 + 5\theta + 1.11 + 2.11\theta + 4.11^2 + \ldots$,

and $\overline{\delta}$. With the same notation for the 11-adic numbers as for the complex numbers defined above, we obtain the 11-adic analogue of (8), namely

$$\text{ord}_\theta(1 - \gamma_0^{h_0}\,\gamma_1^{h_1}\,\gamma_2^{-1}) = 1 + h_1 \ . \tag{10}$$

We note that from the 11-adic estimates given above we can read off that $\theta \| \delta - \overline{\delta}$, $\theta^2 \| 1 + 2\varepsilon$, $\theta \| 2 + \delta^2$ whilst ε , δ , $2 + \varepsilon^2$, $1 + 2\delta$ are relatively prime to θ . Moreover from (5) and its conjugates we see that $\theta^{2b_1} \| u + \varepsilon v$, $\theta^{b_2} \| u + \delta v$, since $\theta(\varepsilon - \delta)$ and $(u , v , 11) = 1$, it follows that not both b_1 and b_2 are positive, and since $\theta \| (\delta - \overline{\delta})$ in any event $b_2 \leqslant 1$.

Since each γ_i in (10) satisfies $\theta \| (\gamma_i - 1)$ the 11-adic logarithms $\log \gamma_i$ exist. In particular, $\text{ord}_\theta \log \gamma_2 = \text{ord}_\theta(\gamma_2 - 1) = 1$ and on writing

$$\psi_0 = \log \gamma_0 / \log \gamma_2 \quad \text{and} \quad \psi_1 = \log \gamma_1 / \log \gamma_2 \ ,$$

(10) becomes

$$\text{ord}_{11}(h_0\,\psi_0 + h_1\,\psi_1 - 1) = \tfrac{1}{2} H \ , \tag{11}$$

provided that $h_1 \geqslant |h_0|$ (note that h_1 is not negative).

We are apparently left with the possibility that $|h_0| > h_1$ but $h_0 < 0$. But already when $h_0 \leqslant -2$ and $|h_0| \geqslant h_1$ the right hand side of (7) has absolute value > 2 whilst the left hand side plainly has absolute value at most 2 (being 1 minus a number on the unit circle). Here we use

$$\varepsilon = 0{,}543689013\ldots \ , \quad \delta = -0{,}771844507\ldots \pm i \times 1{,}115142508\ldots$$

in making the above estimates.

3. Computational methods.

By virtue of refined versions of Baker's inequality for linear forms in logarithms with rational coefficients (prepared by the author with the present problem in mind), it may be concluded that (9) has no solution with $H \geqslant 10^{15}$ say, and that (11) has no solution with $H \geqslant 10^{15}$ say (by virtue of an 11-adic version of the cited inequality).

David C. HUNT and the author have shown that the inequalities (9) and (11) have no solution in the range $17 < H < 10^{15}$. D. C. HUNT used the DC program (infinite precision desk calculator) available as part of the UNIX operating system (Bell laboratories) on the University of New South Wales School of Mathematics PDP-11/40 (Digital Equipment Corporation). DC provides, automatically, infinite integer precision and 99 decimal places ; it also has n-ary arithmetic for $n < 16$ (this was convenient, with $n = 11$). We firstly did all calculations (of course to quite limited accuracy) on the HP-67 (Hewlett-Packard) pocket programmable calculator ; all numerical data reported here is from that source. It proved easy to check the calculations of AGRAWAL and COATES in this way. It is perhaps amusing to remark that the solution $h_0 = 17$, $h_1 = 0$ of (7) , that is, the solution $u = 56$, $v = -103$,

$s = 0$ of $f(u , v) = 11^s$ arises from $\varepsilon^{17} = 56 - 103\varepsilon$ and implies

$$|\varepsilon - 56/103| < (103)^{-3,235} .$$

4. An idea of DAVENPORT-ELLISON.

Our techniques borrow heavily from suggestions of ELLISON [5] which generalise an idea of DAVENPORT (see [3]).

In (9), we simultaneously approximate ψ_0 , ψ_1 obtaining

$$|\psi_i - p_i/q| < 10^{-60} , \text{ with } |p_0| , |p_1| , q < 10^{40} .$$

If $\|q\psi_2\| > 3.10^{-5}$ and $r_i = q\psi_i - p_i$ then

$$\|(h_0 r_0 + h_1 r_1) - q\psi_2 + (h_0 p_0 + h_1 p_1)\| < 10^{40} e^{-3H/4} \tag{12}$$

is a contradiction whenever $45 \log 10 < 3H/4$, that is if $H \geqslant 139$. This argument rapidly brings H down to reasonable size (the next step showed that (9) has no solution with $H \geqslant 28$) and the remaining cases were then checked by hand.

We employed an efficient simultaneous approximation algorithm due to G. SZEKERES [9]. The principle of this algorithm is sequential "Farey bisection" of simplexes of "maximal" size ; in practise, it appears to provide plenty of good simultaneous approximations at reasonable speed (some 600 steps were required above).

In the 11-adic case, we notice that each γ_i is of the shape

$$\gamma = (a + b\theta)/(a - b\theta) \text{ with } a , b \text{ units in } \mathbb{Q}_{11} .$$

Writing $b/a = c$, we have, conveniently,

$$\log \gamma = \log(1 + c\theta)/(1 - c\theta) = 2\theta(c - \frac{11c^3}{3} + \frac{11^2 c^5}{5} - \frac{11^3 c^7}{7} + \ldots) .$$

Even using the 11-ary facility of DC , the calculation presents some difficulty because of the need to separately express the $1/(2n + 1)$ as 11-adic expansions ; the divisions by which we obtain ψ_0 , ψ_1 were also a lengthy task.

As in the complex case, we now simultaneously approximate ψ_0 , ψ_1 obtaining, say,

$$\operatorname{ord}_{11}(\psi_i - p/q) \geqslant 60 \text{ with } |p_0| , |p_1| , q < \tfrac{1}{3}.11^{45} . \tag{13}$$

Writing $11^{60} r_i = q\psi_i - p_i$, we obtain

$$\operatorname{ord}_{11}(11^{60}(h_0 r_0 + h_1 r_1) + (h_0 p_0 + h_1 p_1 - q)) = \tfrac{1}{2} H , \tag{14}$$

But $|h_0 p_0 + h_1 p_1 - q| < 11^{60}$, so if $H \geqslant 120$, we see that

$$h_0 p_0 + h_1 p_1 - q = 0 . \tag{15}$$

In fact, the Szekeres algorithm automatically yields 2 further solutions $(p_0^{(1)} , p_1^{(1)} , q^{(1)})$ and $(p_0^{(2)} , p_1^{(2)} , q^{(2)})$ to (13) so that the determinant of the 3 solutions is ± 1 . Then the results (15) are inconsistent, and we can conclude that $H < 120$. A repetition of the argument yields $H < 24$ and remaining

cases are checked by hand.

5. Rational approximation of p-adic numbers.

Since this is not obvious, we now remark on how one obtains good p-adic rational approximations (for some details, see MAHLER [6], p. 64). Above we "chop" the 11-adic expansion of the ψ_i at the 60-th term obtaining large integers $\psi_i' < 11^{60}$. (If $\psi = \sum_0^\infty a_i\, 11^i$ then $\psi' = a_0 + 11a_1 + 11^2 a_2 + \ldots + 11^{59} a_{59} \in \underset{\sim}{N}$.)

We now approximate (by the Szekeres algorithm) the two rational numbers $\psi_i'/11^{60}$, obtaining simultaneous approximants r_i/q with $q \lesssim 11^{40}$. Then

$$|\psi'/11^{60} - r/q| = |p/11^{60}\, q| < q^{-3/2} \quad \text{so} \quad |p| \lesssim 11^{40}$$

(here we have noticed that $\psi'/11^{60} - r/q$ is rational with denominator $11^{60}\, q$). Moreover $\psi' - p/q = 11^{60}\, r/q$ and this (usually) yields $\mathrm{ord}_{11}(\psi - p/q) \geqslant 60$ as required.

6. The "Baker inequalities".

In the manuscript on which the work described was based, namely that of AGRAWAL and COATES [1], the analogues of (8) and (10) are shown to have no solution with $H \geqslant 10^{700}$. We are now able to do much better. Firstly, the general techniques employed have very much improved ; for some details, see the papers of BAKER [2] and VAN DER POORTEN [10]. Secondly, I have learned from WALDSCHMIDT [11] a number of extra refinements that can be introduced. Principally, these involve a more efficient extrapolation, using the size rather than the height of the numbers involved, and noting whether the numbers involved are close to 1 relative to their size. Detailed results are in preparation.

7. Acknowledgement.

The work described was performed at the suggestion of John COATES who kindly provided us with the manuscript [1]. Although we have finally not had to appeal to the manuscript in any substantial way our work would have been impossible without the guidance provided by AGRAWAL and COATES through [1]. I obtained a copy of the thesis [8] from COATES, and was fortunate that WALDSCHMIDT sent me a copy of the draft paper [11].

All the substantive computations reported on were performed by David HUNT. The work was very much a joint effort and a final detailed report will appear inter alia under our joint authorship.

REFERENCES

[1] AGRAWAL (M.) and COATES (J.). - Elliptic curves of conductor 11 (unpublished manuscript, 1971).

[2] BAKER (A.). - The theory of linear forms in logarithms, "Transcendence theory : Advances and applications. Ed. A. Baker and D. Masser", Chap. 1, p. 1-27. - London, Academic Press, 1977.

[3] BAKER (A.) and DAVENPORT (H.). - The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Quart. J. Math., Oxford 2nd Series, t. 20, 1969, p. 129-137.

[4] DELONE (B. N.) and FADEEV (D. K.). - The theory of irrationalities of the third degree. - Providence, American mathematical Society, 1964.

[5] ELLISON (W. J.). - Recipes for solving diophantine problems by Baker's method, Publications mathématiques de Bordeaux, 1re année, 1972, fasc. 1.

[6] MAHLER (K.). - Lectures on diophantine approximations. - Ann Arbor, University of Notre-Dame, 1961.

[7] SERRE (J.-P.). - Représentations abéliennes modulo 1 et applications (à paraître).

[8] SETZER (C. B.). - Elliptic curves of prime conductor, Ph. D. Thesis, Harvard University, Cambridge, 1972.

[9] SZEKERES (G.). - Multidimensional continued fractions, Annales Univ. Sc. Budapest, Sectio Math., t. 13, 1970, p. 113-140.

[10] VAN DER POORTEN (A. J.). - Linear forms in logarithms in the p-adic case, "Transcendence theory : Advances and applications. Ed. A. Baker and D. Masser", chap. 2, p. 29-57. - London, Academic Press, 1977.

[11] WALDSCHMIDT (M.). - A lower bound for linear forms in logarithms (a preliminary draft).

[12] WEIL (A.). - Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Annalen, t. 168, 1967, p. 149-156.

(Texte reçu le 9 mai 1977)

Alfred J. VAN DER POORTEN
School of Mathematics
The University of New South Wales
KENSINGTON, Sydney, NSW 2031
(Australie)