Astérisque

D. W. MASSER

Note on a conjecture of Szpiro

Astérisque, tome 183 (1990), p. 19-23
<http://www.numdam.org/item?id=AST_1990__183__19_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) 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/

Société Mathématique de France
Astérisque 183 (1990)

NOTE ON A CONJECTURE OF SZPIRO

D. W. MASSER

1. Elliptic Curves.

L. Szpiro has put forward the

Conjecture. For each $\varepsilon > 0$ there is a constant $C(\varepsilon)$ with the following property. Let E be any elliptic curve defined over the rationals with minimal discriminant D and conductor N. Then $|D| \leq C(\varepsilon)N^{6+\varepsilon}$.

This has a number of remarkable consequences (see for example [V] and [HS]), and so a proof would be of considerable interest. Perhaps also a disproof would have some significance. In the present note we show at least that the inequality of the conjecture cannot be much improved; in particular, it would be false in the form $|D| \leq CN^6(\log N)^k$ for any absolute constants C and k. This research was supported in part by the National Science Foundation.

Theorem. For any $\delta > 0$ and N_0 there is an elliptic curve E defined over the rationals whose minimal discriminant D and conductor $N \geq N_0$ satisfy

$$|D| \geq N^6 \exp\{(24-\delta)(\log N)^{1/2}(\log\log N)^{-1}\} .$$

The proof of this result will be reduced to number theory using the following observation. First for a non-zero rational integer n we write $S(n)$ for the square-free kernel of n; that is, the product of all distinct positive primes dividing n.

Lemma 1. Suppose a,b,c are coprime rational integers with

$$a+b+c = 0, \quad a \equiv 1 \pmod 4, \quad c \equiv 0 \pmod{32} .$$

Then the equation

$$y^2 = x(x-a)(x+b) \tag{1}$$

defines an elliptic curve E whose minimal discriminant D and conductor N satisfy

$$|D| = 2^{-8}(abc)^2, \quad N = S(abc) .$$

Proof. In the standard notation ([S] p. 46) the equation (1) gives

$$c_4 = 16(a^2+ab+b^2), \quad \Delta = 16(abc)^2 .$$

Let p be an odd prime. It is easy to verify that if p divides Δ then p cannot divide c_4. It follows (see [S] p. 172) that the equation (1) is minimal for all $p \neq 2$.

This is not so for $p = 2$. Indeed, the change of variables

$$x = 4x' + a \;, \; y = 8y' + 4x'$$

leads to the equation

$$y'^2 + x'y' = x'^3 + (\alpha + 8\beta)x'^2 + 2a\beta x' \;, \tag{2}$$

where the integers α and β are defined by

$$a = 4\alpha + 1 \;, \; c = -32\beta \;.$$

For this new equation we have

$$c_4' = a^2 + ab + b^2 \;, \quad \Delta' = 2^{-8}(abc)^2 \;;$$

and since c_4' is odd, we see now that (2) is minimal for $p = 2$.

The formula for D follows at once. The formula for N follows from the definition ([S] p. 361). For if p does not divide abc (in particular $p \neq 2$) then E has good reduction at p. If p divides abc and $p \neq 2$ then (1) is minimal and p does not divide c_4, so E has multiplicative reduction ([S] p. 180). Finally if $p = 2$ then (2) is minimal, c_4' is odd, and again E has multiplicative reduction. This completes the proof of Lemma 1.

It is clear that our Theorem is a consequence of Lemma 1 together with the following

Proposition. For any $\delta > 0$ and S_0 there are coprime rational integers a,b,c with

$$a + b + c = 0 \;, \quad a \equiv 1 \pmod 4 \;, \; c \equiv 0 \pmod{32}$$

and $S = S(abc) \geq S_0$ satisfying

$$|abc| \geq S^3 \exp\{(12-\delta)(\log S)^{1/2}(\log\log S)^{-1}\} \;. \tag{3}$$

A similar result with the weaker inequality

$$\max(|a|,|b|,|c|) \geq S \exp\{(4-\delta)(\log S)^{1/2}(\log\log S)^{-1}\}$$

was established recently by C. Stewart and R. Tijdeman [ST]. In the next section we shall prove our Proposition by means of a small modification in their proof.

2. Number Theory.

We require a preliminary lemma. For $y \geq 0$ write $\theta(y) = \sum_{p \leq y} \log p$ as usual, and for $x \geq 0$ let $\Psi_o(x,y)$ be the number of positive odd integers not exceeding x that are divisible only by primes not exceeding y.

Lemma 2. For any $\delta > 0$ and all sufficiently large x we have

$$e^{-\theta(y)}\Psi_o(x,y) \geq \exp\{(4-\delta)(\log x)^{1/2}(\log\log x)^{-1}\},$$

where $y = (\log x)^{1/2}$.

Proof. Let $\Psi(x,y)$ denote the usual number of positive integers not exceeding x that are divisible only by primes not exceeding y. Good estimates when $y = (\log x)^{1/2}$ were obtained by V. Ennola [E]; we use the version

$$\Psi(x,y) = \exp\{\pi(y)\log\log x - y + O(y(\log y)^{-2})\}$$

given by K.K. Norton ([N] p. 25). Here

$$\pi(y) = y(\log y)^{-1} + y(\log y)^{-2} + O(y(\log y)^{-3})$$

is the usual prime counting function, and we deduce that

$$\Psi(x,y) = \exp\{y + 2y(\log y)^{-1} + O(y(\log y)^{-2})\}. \tag{4}$$

Clearly also

$$\Psi(x,y) = \sum_{h=o}^{\infty} \Psi_o(2^{-h}x,y) = \sum_{h=o}^{H} \Psi_o(2^{-h}x,y) \leq (H+1)\Psi_o(x,y) \tag{5}$$

for $H = [(\log x)/(\log 2)]$. Finally

$$\theta(y) = y + O(y(\log y)^{-2}), \tag{6}$$

and this together with (4) and (5) leads to the inequality of Lemma 2.

Proof of Proposition. Select x large, put $y = (\log x)^{1/2}$, and let p be the least prime greater than y. Write $T = \Psi_o(x,y)$ and define the positive integer t by

$$x \leq 2^t < 2x .$$

From Lemma 2 we see that $T/pt \to \infty$ as $x \to \infty$. Define the positive integer n by

$$\tfrac{1}{2}T \leq 2^n pt < T ,$$

and assume x is so large that $n \geq 5$. Since $T > 2^n pt$, a simple application of the Box Principle enables us to find $t+1$ odd integers $x_o,\ldots,x_t$, divisible only by primes not exceeding y, satisfying

$$1 \leq x_o < x_1 < \ldots < x_t \leq x ,$$

and in the same residue class modulo $2^n p$. Since $2^t \geq x$, we can find i with $1 \leq i \leq t$ and

$$x_i \leq 2x_{i-1} . \tag{7}$$

Let d be the highest common factor of x_i and x_{i-1}, and write

$$a = \pm x_i/d , \quad b = \mp x_{i-1}/d , \quad c = \mp(x_i - x_{i-1})/d ,$$

where the sign is chosen such that $a \equiv 1 \pmod 4$. Since d is odd and $n \geq 5$, we also have $c \equiv 0 \pmod{32}$; and clearly $a+b+c = 0$. Further $p > y$ and so p does not divide x_i; thus p does not divide d. Because p divides $x_i - x_{i-1}$, it must divide c, so that

$$S = S(abc) \geq p .$$

Therefore by assuming x sufficiently large we may suppose $S \geq S_o$ as required.

It remains to check (3). Now clearly $S(ab) \leq \frac{1}{2}e^{\theta(y)}$, and since 2^n divides c we have $S(c) \leq 2^{-(n-1)}|c|$. Thus

$$S \leq S(ab)S(c) \leq 2^{-n}e^{\theta(y)}|c| . \tag{8}$$

Also $|a| \geq |c|$, and (7) gives $|b| \geq \frac{1}{2}|a| \geq \frac{1}{2}|c|$, so that

$$|abc| \geq \tfrac{1}{2}|c|^3 \geq \tfrac{1}{2}S^3(2^n e^{-\theta(y)})^3 .$$

Further $p \leq 2y$ and so

$$2^n \geq T/(2pt) \geq T/(4yt) \geq (1/8)T(\log x)^{-3/2} .$$

Therefore

$$|abc| \geq 2^{-10}S^3(\log x)^{-9/2}(e^{-\theta(y)}T)^3 .$$

Hence by Lemma 2, if x is sufficiently large we have

$$|abc| \geq S^3\exp\{(12-\delta)(\log x)^{1/2}(\log\log x)^{-1}\} .$$

The Proposition follows on noting from (6) and (8) that if x is sufficiently large then

$$S \leq e^{\theta(y)}|c| \leq e^{2y}x \leq x^{1+\delta} .$$

References

[E] V. Ennola, On numbers with small prime divisors, Ann. Acad. Sci. Fenn. (Series AI) 440 (1969), 1-16.

[HS] M. Hindry and J.H. Silverman, The canonical height and integral points on elliptic curves, Invent. Math. 93 (1988), 419-450.

[N] K.K. Norton, Numbers with small prime factors, and the least k-th power non-residue, Memoirs A.M.S. Vol. 106 (1971).

[S] J.H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Math. Vol. 106, Springer-Verlag, New York - Berlin - Heidelberg - Tokyo 1985.

[ST] C.L. Stewart and R. Tijdeman, On the Oesterlé-Masser conjecture, Monats. Math. 102 (1986), 251-257.

[V] P. Vojta, Dicphantine approximations and value distribution theory, Lectures Notes in Math. Vol. 1239, Springer-Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo 1987.

D.W.MASSER
University of Michigan
Ann Arbor, USA