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.

\mathcal{N} umdam

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

<u>Conjecture</u>. 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 $|D| < C(\varepsilon) N^{6+\varepsilon}$.

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 $N \ge N_0$ satisfy

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

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]. Suppose a,b,c are coprime rational integers with

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

Then the equation

$$y^2 = x(x-a)(x+b)$$
 (1)

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

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

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

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

D.W. MASSER

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

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

where the integers α and β are defined by

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

For this new equation we have

$$c'_4 = a^2 + ab + b^2$$
, $\Delta' = 2^{-8}(abc)^2$;

and since c'_{Δ} 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 there are coprime rational integers a,b,c with

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

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

 $|abc| \ge s^{3} \exp\{(12-\delta)(\log s)^{1/2}(\log \log s)^{-1}\}$. (3)

A similar result with the weaker inequality

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

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 $y \ge 0$ write

 $\theta(y) = \sum_{\substack{p \leq y \\ o}} \log p$ 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

$$e^{-\theta(y)} \Psi_{0}(x,y) \ge \exp\{(4-\delta)(\log x)^{1/2}(\log \log x)^{-1}\},$$

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

<u>Proof</u>. 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

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

Clearly also

$$\Psi(\mathbf{x},\mathbf{y}) = \sum_{h=0}^{\infty} \Psi_{\mathbf{0}}(2^{-h}\mathbf{x},\mathbf{y}) = \sum_{h=0}^{H} \Psi_{\mathbf{0}}(2^{-h}\mathbf{x},\mathbf{y}) \leq (H+1)\Psi_{\mathbf{0}}(\mathbf{x},\mathbf{y})$$
(5)

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

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

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

<u>Proof of Proposition</u>. 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 $\frac{1}{2}T \ \le 2^n pt \ \le T \ ,$

and assume x is so large that $n \ge 5$. Since $T > 2^n pt$, a simple application of the Box Principle enables us to find t+1 odd integers x_0, \ldots, x_t , divisible only by primes not exceeding y, satisfying

$$1 \leq x_0 < x_1 < \dots < x_t \leq x$$

and in the same residue class modulo 2^np . Since $2^t \ge x$, we can find i with $1 \le i \le t$ and

$$\mathbf{x}_{i} \leq 2\mathbf{x}_{i-1} \quad . \tag{7}$$

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

$$a = \frac{1}{2} x_{i}^{d} , \quad b = \frac{1}{2} x_{i-1}^{d} , \quad c = \frac{1}{2} (x_{i}^{d} - x_{i-1}^{d})^{d} ,$$

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

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

Therefore by assuming x sufficiently large we may suppose $S \ge S_0$ 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

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

Also $|\mathbf{a}| \ge |\mathbf{c}|$, and (7) gives $|\mathbf{b}| \ge \frac{1}{2}|\mathbf{a}| \ge \frac{1}{2}|\mathbf{c}|$, so that $|\mathbf{abc}| \ge \frac{1}{2}|\mathbf{c}|^3 \ge \frac{1}{2}\mathbf{s}^3(2^n e^{-\theta}(\mathbf{y}))^3$.