Algorithms for Finding Good Examples for the abc and Szpiro Conjectures

Abderrahmane Nitaj

CONTENTS

The radical $\mathbf{rad}\, n$ of an integer $n \neq 0$ is the product of the primes dividing n. The abc-conjecture and the Szpiro conjecture imply that, for any positive relatively prime integers a, b, and c such that $a+b=c$, the expressions

$$\frac{\log c}{\log \operatorname{rad}(abc)} \quad \text{and} \quad \frac{\log abc}{\log \operatorname{rad}(abc)}$$

are bounded. We give an algorithm for finding triples (a,b,c) for which these ratios are high with respect to their conjectured asymptotic values. The algorithm is based on approximation methods for solving the equation $Ax^n - By^n = Cz$ in integers x, y, and z with small $|z|$.

Additionally, we employ these triples to obtain semistable elliptic curves over $\mathbf{Q}$ with high Szpiro ratio

$$\sigma = \frac{\log |\Delta|}{\log N},$$

where Δ is the discriminant and N is the conductor.

1. INTRODUCTION

An abc-example is a triple (a,b,c) of positive relatively prime integers such that $a+b=c$ and $a<b$. The abc-conjecture of Masser and Oesterlé [Oesterlé 1988] implies that the expression

$$\alpha = \alpha(a,b,c) = \frac{\log c}{\log \operatorname{rad}(abc)} \tag{1.1}$$

is bounded, where $\operatorname{rad}(abc)$ is the radical of abc (the product of all distinct primes dividing abc). The conjectured asymptotic value of $\alpha(a,b,c)$ is 1, so the more α exceeds 1, the more an abc-example is interesting from the point of view of the abc-conjecture.

1058-6458/96 $0.50 per page

Let E be a semistable elliptic curve over $\mathbf{Q}$ with minimal discriminant Δ and conductor N. The original Szpiro conjecture says that, for any $\varepsilon > 0$, there exists $c(\varepsilon)$ such that

$$|\Delta| \leq c(\varepsilon) N^{6+\varepsilon}.$$

This inequality implies that the *Szpiro ratio*

$$\sigma = \frac{\log |\Delta|}{\log N} \tag{1.2}$$

is bounded. Applied to the elliptic curve given by

$$y^2 + xy = x^3 + \frac{b-a-1}{4}x^2 - \frac{ab}{16}x,$$

where a and b are relatively prime integers with $a \equiv -1 \bmod 4$ and $b \equiv 0 \bmod 16$, the Szpiro conjecture implies that the ratio

$$\rho = \rho(a,b,c) = \frac{\log |abc|}{\log \operatorname{rad}(abc)} \tag{1.3}$$

is bounded [Oesterlé 1988], where $c = a + b$. The conjectured asymptotic value of $\rho(a,b,c)$ is 3; the more ρ exceeds 3, the more an abc-example is interesting from this point of view.

This paper gives an algorithm that yields many abc-examples with high α or ρ. Section 2 motivates the algorithm, Section 3 gives it in its simplest form, and Sections 4 and 5 indicate how to make it more efficient.

Section 6 describes our experiments, which consisted in running the algorithm for various settings of the bounds and collecting the resulting abc-examples with $\alpha \geq 1.4$ or $\rho \geq 3.8$. Note that, while the algorithm does not allow an exhaustive search for c in a given range, it can, with relative ease, find examples with c quite large. The largest one we have found is

$$109^3\, 2383^3 + 2^{50}\, 7^2\, 17\, 19\, 31 = 3^{17}\, 53^6\, 193,$$

with $\alpha = 1.37839$ and $\rho = 3.83622$, for which $c > 2^{69}$.

Section 7 is an application of the abc-examples to the construction of two families of elliptic curves with high Szpiro ratio.

2. ON A DIOPHANTINE EQUATION

Let $n \geq 2$ be an integer, and let A, B, C be relatively prime integers with $A, C > 0$ and $B \neq 0$. Our search for good abc-examples will be based on the study of the diophantine equation

$$Ax^n - By^n = Cz, \tag{2.1}$$

where we require that $\gcd(y, C) = 1$. (Note that this implies $x \neq 0$.) This equation has a solution satisfying this condition if and only if the congruence

$$At^n \equiv B \bmod C \tag{2.2}$$

can be solved for t. Indeed, saying that $At^n - B$ divides C is saying that $(x,y,z) = (t,1,z)$ is a solution of (2.1) for some integer z. Conversely, if $Ax^n \equiv By^n \bmod C$ and $\gcd(C,y) = 1$, any integer representative t of $xy^{-1} \bmod C$ satisfies (2.2). In this case we can also write $x = ty - Cu$, for some integer u.

We will be primarily interested in finding solutions of (2.1) such that $|z| = 1$. We distinguish two cases, depending on the values of B and n.

Theorem 2.1. *Suppose $B < 0$ and n even. If $(x,y,1)$ is a solution of (2.1) with $y > 0$ and $\gcd(C,y) = 1$, there exists a solution t of (2.2) with $0 \leq t < C$ and such that u/y is a convergent of t/C, where u is defined by $x = ty - Cu$.*

Proof. The only thing we have not shown is that u/y is a convergent of t/C (recall that this means that no other integer fraction with denominator $\leq y$ is closer to t/C). Since $A > 0$ and $B < 0$, we have

$$2\,|x|\,y < x^2 + y^2 \leq x^n + y^n \leq Ax^n - By^n = c.$$

This implies that

$$pt\left|\frac{t}{C} - \frac{u}{y}\right| = \frac{|x|}{Cy} < \frac{1}{2y^2},$$

from which the desired result follows easily (see, for example, [Niven et al. 1991]). $\square$

To treat the complementary case, we set

$$\delta = \Big(\frac{B}{A}\Big)^{1/n},$$
$$y_0 = \Big(\frac{2^n}{An\delta^{n-1}}\Big)^{1/(n-2)} \quad \text{if } n \geq 3.$$

Theorem 2.2. *Assume that $B > 0$ or that n is odd. Let (x, y, z) be a solution of (2.1) with $y > 0$ relatively prime to C and with $z = \pm 1$, and set*

$$\varepsilon = \begin{cases} 1 & \text{if } x\delta > 0, \\ \cos\Big(2\pi\dfrac{\lfloor (n-1)/2 \rfloor}{n}\Big) & \text{if } x\delta < 0. \end{cases}$$

If $n = 2$ and $AB \geq 4$, or if $n \geq 3$ and $y \geq y_0$, there exists a solution t of (2.2) with $0 \leq t < C$ and such that u/y is a convergent of the continued-fraction expansion of $(t - \varepsilon\delta)/C$ (assuming $t - \varepsilon\delta \neq 0$), where u is defined by $x = ty - Cu$.

Here the notation $\lfloor w \rfloor$ represents the greatest integer not exceeding w, so that ε, in the case $x\delta < 0$, is simply the real part of the n-th root of unity nearest -1.

Proof. Let $\theta_k = \delta e^{2k\pi i/n}$, for $0 \leq k < n$, and choose k_0 such that

$$\Big|\frac{x}{y} - \theta_{k_0}\Big| = \min_{0 \leq k < n}\Big|\frac{x}{y} - \theta_k\Big|;$$

then $\operatorname{Re}\theta_{k_0} = \varepsilon\delta$. We have

$$\prod_{k \neq k_0}\Big|\frac{x}{y} - \theta_k\Big| \geq \frac{1}{2^{n-1}}\prod_{k \neq k_0}\Big(\Big|\frac{x}{y} - \theta_{k_0}\Big| + \Big|\frac{x}{y} - \theta_k\Big|\Big)$$
$$\geq \frac{1}{2^{n-1}}\prod_{k \neq k_0}|\theta_{k_0} - \theta_k| = \frac{n\delta^{n-1}}{2^{n-1}}.$$

At the same time,

$$\prod_{k=0}^{n-1}\Big|\frac{x}{y} - \theta_k\Big| = \Big|\Big(\frac{x}{y}\Big)^n - \delta^n\Big| = \frac{C}{Ay^n}.$$

Dividing by the previous inequality we get

$$\Big|\frac{x}{y} - \theta_{k_0}\Big| \leq \frac{2^{n-1}C}{An\delta^{n-1}y^n},$$

and therefore

$$\Big|\frac{t - \varepsilon\delta}{C} - \frac{u}{y}\Big| = \frac{1}{C}\Big|\frac{x}{y} - \varepsilon\delta\Big| \leq \frac{1}{C}\Big|\frac{x}{y} - \theta_{k_0}\Big|$$
$$\leq \frac{2^{n-1}}{an\delta^{n-1}y^n} \leq \frac{1}{2y^2},$$

where the last inequality depends on the fact that $AB \geq 4$ if $n = 2$ or $y \geq y_0$ if $n \geq 3$. As in the proof of the preceding theorem, this implies that u/y is a convergent of $(t - \varepsilon\delta)/C$. □

3. THE BASIC ALGORITHM

We now apply these ideas to create an algorithm that tends to give good *abc*-examples. The basic idea is to use for a, b, c the three terms of (2.1), with A and $|B|$ small and C a small multiple of a prime power, and hope to solve the equation with $|z| = 1$. The fact that all three terms are small multiples of a power then causes $\operatorname{rad}(ABC)$ to be much smaller than $|ABC|$, and this tends to increase the ratios α and ρ.

For simplicity, take first the case n even, $B < 0$. By Theorem 2.1, a solution of (2.1) with $z = 1$ leads to a convergent of t/C, where t is a solution of (2.2). Thus, by taking all the solutions t of (2.2) and examining the convergents of t/C, we will find the solutions of (2.1) with $z = 1$ (if any exist).

Formally, we have the following algorithm:

Algorithm 3.1. Given an even integer $n \geq 2$ and relatively prime integers $A > 0$, $B < 0$, $C > 0$:

- find all solutions of $At^n \equiv B \bmod C$ with $0 \leq t < C$; for each solution t:
  - compute the convergents u/y of t/C; for each such convergent:
    - set $a_0 = A(ty - Cu)^n$, $b_0 = -By^n$, $c_0 = a_0 + b_0$;
    - divide a_0, b_0 and c_0 by their gcd;
    - set $a = \min(|a_0|, |b_0|, |c_0|)$, $c = \max(|a_0|, |b_0|, |c_0|)$, and $b = c - a$;
    - compute the ratios α and ρ using (1.1) and (1.3); record (a, b, c) if either ratio exceeds the desired cutoff.

The procedure for n odd or $B > 0$ is similar, but is complicated by our not knowing in advance the value of ε in Theorem 2.2. Thus we have to loop over its two possible values:

Algorithm 3.2. Given an integer $n \geq 2$ and relatively prime integers $A > 0$, B, and $C > 0$, with n odd or $B > 0$:
- set $\delta = (B/A)^{1/n}$;
- find all solutions of $At^n \equiv B \bmod C$ with $0 \leq t < C$; for each solution t:
  - for $\varepsilon = 1$ and $\varepsilon = \cos\Bigl(2\pi \dfrac{\lfloor (n-1)/2 \rfloor}{n}\Bigr)$:
    - unless $t - \varepsilon\delta = 0$:
      - compute the convergents u/y of $(t-\varepsilon\delta)/C$, for y up to some fixed bound; for each such convergent, proceed as in the inner loop of Algorithm 3.1.

The dominant step in these algorithms is the computation of the radical of abc, which involves the factorization of large numbers.

Note that there is no guarantee that a given abc-example will appear only once. It is of course desirable to minimize such redundancies. In the next two sections, we prove two results that decrease the amount of redundancy when n is even (Section 4) or when c has a special form (Section 5).

4. SHORTCUT FOR n EVEN

For $n \geq 2$ even, if t is a solution of (2.2), so is $C - t$. We now show that, for the purposes of Algorithms 3.1 and 3.2, we only need to examine one of the two values. In other words, the outer loop of the algorithms needs to be executed only for $0 \leq t \leq \frac{1}{2}C$ when n is even.

Let t be a solution of (2.2) with $0 \leq t \leq \frac{1}{2}C$. If $B < 0$ let $\xi = t/C$ (case of Algorithm 3.1), and if $B > 0$ set $\xi = (t+\varepsilon\delta)/C = (t \pm (B/A)^{1/n})/C$ (case of Algorithm 3.2). Moreover, let $\nu = \xi - [\xi]$.

Theorem 4.1. *Let the notation be as above.*

(i) *If $\xi \neq 0$ and $\nu \leq \frac{1}{2}$, every abc-example arising from a convergent of ξ also arises from a convergent of $1 - \xi$.*

(ii) *If $\xi \neq 0$ and $\nu > \frac{1}{2}$, every abc-example arising from a convergent of $1 - \xi$ also arises from a convergent of ξ.*

Proof. Assume that $\xi \neq 0$, and let $[a_0, a_1, \dots]$ be the continued-fraction expansion of ξ. We have $a_0 = \lfloor \xi \rfloor$ and $a_1 = \lfloor 1/\nu \rfloor$. To show (i), assume that $\nu \leq \frac{1}{2}$. Then $a_1 \geq 2$ and

$$1 - \xi = [-a_0, 1, a_1 - 1, a_2, a_3, \dots].$$

Let u_i/y_i and u'_i/y'_i, for $i = -2, -1, \dots$, be the convergents of the continued fraction expansion of ξ and $1 - \xi$ respectively. Then, for all $i \geq 1$, $u'_i = y_{i-1} - u_{i-1}$ and $y'_i = y_{i-1}$. Let $y = y_{i-1}$ and $x = ty_{i-1} - Cu_{i-1}$. Since n is even, we have

$$\begin{aligned} Ax^n - By^n &= A(ty_{i-1} - Cu_{i-1})^n - By_{i-1}^n \\ &= A((C-t)y_{i-1} - C(y_{i-1} - u_{i-1}))^n - By_{i-1}^n \\ &= A((C-t)y'_i - Cu'_i)^n - By'^n_i. \end{aligned}$$

Hence, for $i \geq 1$, every convergent u_{i-1}/y_{i-1} of ξ gives the same abc-example as the convergent u'_i/y'_i of $1 - \xi$. This completes the proof of (i).

Part (ii) follows by replacing ξ with $1 - \xi$ and applying (i). □

5. SHORTCUT FOR SPECIAL VALUES OF c

As remarked in the beginning of Section 3, it is reasonable to run the algorithm with C a prime power, because this makes $\operatorname{rad} C$ small compared with C. In fact, it is even more efficient to consider in sequence values of C of the form p^e, for successive values of e, for two reasons, the first being that if the congruence $At^n \equiv B$ has already been solved mod p^e, it is very easy to solve it mod p^{e+1}. The second reason is given by Theorem 5.1 below: some convergents can be ignored.

For the sake of generality, the theorem will in fact be stated for $C = p^e C_0$, were C_0 may be greater than one (and p is prime, $\gcd(C_0, p) = 1$, and $e > 0$.) We fix $A > 0$, $B \neq 0$, and $n \geq 2$, and vary only C.

Theorem 5.1. *Let the notation be as above, and consider an abc-example obtained by an application of*

Algorithm 3.1 *or* 3.2 *with* $C = p^e C_0$. *If the convergent* u/y *from which it arises satisfies* $y \equiv 0 \bmod p$, *the same example can be obtained by an application of the algorithm with* $C = p^j C_0$ *for some* $j < e$.

In other words, if we have already run the algorithm for $C = p^j C_0$, with $j < e$, we can ignore convergents whose denominators divide p when running it for $C = p^e C_0$.

Proof. Set $C_j = p^j C_0$ for $0 < j < e$, so $C = C_e$. Suppose for concreteness that we are in the situation of Algorithm 3.2 (the reasoning would in any case apply without changes to Algorithm 3.1 if we set $\delta = \varepsilon = 0$).

By the theorem's assumptions, we have a solution t of $At^n \equiv B \bmod C_e$, a convergent u/y of $(t-\varepsilon\delta)/C_e$, and integers $x = ty - Cu \neq 0$ and z such that

$$Ax^n - By^n = zC_e.$$

Let $q = (At^n - B)/C_e$, and write $y = p^{e'} y'$ with $e' > 0$ and $\gcd(p, y') = 1$. Then

$$A(tp^{e'}y' - p^e C_0 u)^n - B(p^{e'}y')^n = p^e C_0 z, \quad (5.1)$$

so that

$$z = qp^{ne'}y'^n + Au \sum_{i=1}^{n} (-1)^i \binom{n}{i} p^{(n-i)e'+(i-1)e}(ty')^{n-i}(uC_0)^{i-1}.$$

Let $j = e - \min(e, e')$ and $k = e' - \min(e, e')$. Dividing (5.1) by $p^{\min(ne, ne')}$, we get

$$A(tp^k y' - p^j C_0 u)^n - B(p^k y')^n \equiv 0 \bmod p^j C_0. \quad (5.2)$$

Write t as $t = p^j C_0 r + t'$, with $0 < t' < p^j C_0$. Since $At^n \equiv B \bmod p^e C_0$, the same congruence holds mod $p^j C_0$. Rewrite (5.2) as

$$A(t'p^k y' - p^j C_0(u - rp^k y'))^n - Bp^k y'^n \equiv 0 \bmod p^j C_0.$$

Since u/y is a convergent of $\dfrac{t-\varepsilon\delta}{p^e C_0}$, we have

$$\left|\frac{t-\varepsilon\delta}{p^e C_0} - \frac{u}{y}\right| < \frac{1}{y^2},$$

that is,

$$\left|\frac{p^j C_0 r + t' - \varepsilon\delta}{p^e C_0} - \frac{u}{p^{e'}y'}\right| < \frac{1}{(p^{e'}y')^2}.$$

Then

$$\left|\frac{t'-\varepsilon\delta}{p^j C_0} - \frac{u - rp^k y'}{p^k y'}\right| < \frac{1}{p^{e'+k}y'^2} \leq \frac{1}{2y'^2},$$

which implies that $(u - rp^k y')/(p^k y')$ is a convergent of $(t' - \varepsilon\delta)/(p^j C_0)$, concluding the proof. □

6. THE EXPERIMENTS

We have applied the algorithm in the following cases.

(i) $n = 2$, $1 \leq a \leq |b| \leq 300$ with $b < 0$, and $c = p^e$, where p is a prime ≤ 31 and e is such that $p^e \leq 2^{60}$ [Nitaj 1992].
(ii) $n = 2$, $1 \leq a \leq b \leq 300$, and $c = p^e$, where p is a prime ≤ 31 and e is such that $p^e \leq 2^{40}$ [Nitaj 1992].
(iii) $n = 3, 5$, $1 \leq a \leq b \leq 200$, and $c = p^e$, where p is a prime ≤ 31 and e is such that $p^e \leq 2^{40}$.

We have found 103 examples with $\rho \geq 3.8$ and 86 examples with $\alpha \geq 1.4$. The left half of Table 1 lists the examples that we believe were previously unknown and that have the largest α. The right half is similar, and lists the examples with largest ρ.

We remark that in these runs we recovered all the triples found by N. Elkies and J. Kanapka in their recent tabulation of all *abc*-examples with $c < 2^{32}$ and $\alpha \geq 1.2$ [Elkies and Kanapka].

See also the section on software availability at the end of this article.

7. APPLICATION TO THE SZPIRO RATIO

Our goal in this section is to find examples of elliptic curves for which the Szpiro ratio (1.2) exceeds significantly the conjectural asymptotic value 6. To do this, we define two families of elliptic curves.

a	b	c	α	a	b	c	ρ
283	$5^{11}\,13^2$	$2^8\,3^8\,17^3$	1.58076*	$13\,19^6$	$2^{30}\,5$	$3^{13}\,11^2\,31$	4.41901
$13\,19^6$	$2^{30}\,5$	$3^{13}\,11^2\,31$	1.52700	3^{21}	$7^2\,11^6\,199$	$2\,13^8\,17$	4.20094
239	$5^8\,17^3$	$2^{10}\,37^4$	1.50284*	$2^{16}\,41\,71$	$3^{15}\,7^2$	19^7	4.09655
$2^2\,11$	$3^2\,13^{10}\,17\,151\,4423$	$5^9\,139^6$	1.49243	$3^{12}\,5^6$	$7^9\,31^2$	$2^9\,11^5\,571$	4.09647
73	$2^{13}\,7^7\,941^2$	$3^{16}\,103^3\,127$	1.49159	$7^8\,19$	$2^{15}\,5^2\,37^2$	$3\,17^7$	4.09080
1	$3^{16}\,7$	$2^3\,11\,23\,53^3$	1.47445	$2^{24}\,3^5$	$5\,19^5\,59^2$	$7^{10}\,167$	4.07114
7^2	$2^{10}\,11\,53^2$	$3^4\,5^8$	1.47414*	$3^6\,157^3\,283$	23^{10}	$2^{30}\,5^2\,11^2\,13$	4.05990*
$3^4\,199$	11^8	$2^3\,5^7\,7^3$	1.47130*	$2^{13}\,3^{13}\,11^3$	$13\,29\,43^6\,673$	$5^{20}\,17$	4.04710
$3^2\,5^2$	$2^4\,17^3\,31^4$	$7^{10}\,257$	1.45707	$5^{13}\,13$	$2^{17}\,19^3\,23$	$3^{17}\,283$	4.04498
$3^5\,7$	$5^6\,67$	2^{20}	1.45134*	$3^2\,5^7\,79$	$2^{29}\,13$	$11^7\,19^2$	4.02943
1	$3^3\,5^3\,7^7\,23$	$2^{13}\,11^4\,13\,41$	1.45003	$2\,5^9$	3^{14}	$7^5\,11\,47$	4.01342
$11^2\,43$	$5^9\,7^2\,13^4\,97$	$2^3\,3\,73^7$	1.44798	$2^{10}\,19^{10}$	$5^6\,13^4\,29^5$	$3^{20}\,4425749$	4.00292
89	$7\,11^8$	$2^{20}\,3^3\,53$	1.44774	$5^3\,11^4\,31^2$	$3^{17}\,7^2$	$2^{25}\,241$	4.00087
$3^2\,5^7\,79$	$2^{29}\,13$	$11^7\,19^2$	1.44625	$2^8\,7^2\,19^6$	$5^9\,113^2\,193$	$3\,23^9$	3.99793
$2\,13^2$	5^8	$3\,19^4$	1.44506*	$7^7\,11^3$	$2^{18}\,3^4\,103$	$5^9\,41^2$	3.99129
$3^2\,19^3$	5^{11}	$2^{17}\,373$	1.44328*	19^8	31^7	$2^{11}\,7^4\,9049$	3.97796
31^3	$2\,17\,41^5$	$3\,5^7\,7^5$	1.44144	$2^{15}\,3\,19\,29^2$	$5^{10}\,7^4$	$13^2\,23^6$	3.97457
$3^4\,23^2$	31^5	$2^{15}\,5^3\,7$	1.44097*	$3^{10}\,7^4\,11^2$	$17^6\,31$	$2^{14}\,103^3$	3.96813
$2\,13^5$	$7^6\,173^2$	$3^{13}\,47^2$	1.43618	$2^{13}\,47^3$	$3^9\,17^3\,23$	$7^2\,13^7$	3.96555
$2^5\,3^{18}$	$5^6\,7^{10}\,23^2$	$11^9\,990203$	1.43346	$7^2\,17^4\,856897$	$2^{41}\,3^2$	13^{12}	3.96025
31^2	$3^5\,5^9$	$2^5\,23^4\,53$	1.43304*	$2^{25}\,3^4\,29\,10753$	$7^4\,151^2\,181^4$	5^{24}	3.95603
2^{21}	$7^6\,17\,8209^2$	$5^{12}\,743^2$	1.43290	61^4	$3^{13}\,53$	$2^{13}\,5\,7^4$	3.95432
$2^9\,19^2$	$59^6\,73$	$3^3\,5^7\,7^2\,31^3$	1.43109	$3^{13}\,19$	$7\,53^4$	$2^{10}\,17^4$	3.95368
193	$2\,5^6\,19^2\,1193^2$	$3^9\,13^8$	1.43042	$2^{19}\,367^3$	$5^{17}\,197\,281$	$13^2\,251^6$	3.94750
$3^9\,29$	$7^6\,43^2$	$2^{24}\,13$	1.42955	$2^{11}\,17^4$	$3^{14}\,7^3$	$5^6\,23\,71^2$	3.94732

TABLE 1. Previously unknown highest-α and highest-ρ examples obtained in the experiments described in Section 6. Those marked with an asterisk were found at the same time by Browkin and Brzezinski [1992]. The top example on the right has the highest ρ currently known.

Let a and b be relatively prime integers. Define an elliptic curve E over $\mathbf{Q}$ by

$$y^2+(b^2+ab-a^2)xy+a^2b^3(b-a)y = x^3+a^2b(b-a)x^2, \tag{7.1}$$

The quantities c_4 and Δ [Silverman 1986] are

$$c_4 = (a^2-ab+b^2)\times (a^6-11a^5b+30a^4b^2-15a^3b^3-10a^2b^4+5ab^5+b^6),$$
$$\Delta = a^7b^7(a-b)^7(a^3-8a^2b+5ab^2+b^3).$$

Define also the isogenous elliptic curve E' over $\mathbf{Q}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{7.2}$$

where

$$a_1 = b^2 + ab - a^2,\quad a_2 = a^2b(b-a),\quad a_3 = a^2b^3(b-a),$$
$$a_4 = 5ab(b-a)(a^2-ab+b^2)(a^3+2a^2b-5ab^2+b^3),$$
$$a_6 = ab(b-a) \times (a^9+9a^8b-37a^7b^2+70a^6b^3-132a^5b^4 + 211a^4b^5-182a^3b^6+76a^2b^7-18ab^8+b^9).$$

The quantities c_4' and Δ' are

$$c_4' = (a^2-ab+b^2) \times (a^6+229a^5b+270a^4b^2 - 1695a^3b^3+1430a^2b^4-235ab^5+b^6),$$
$$\Delta' = ab(a-b)(a^3-8a^2b+5ab^2+b^3)^7.$$

a	b	σ
2^{15} 13	31^2 59	7.36246
2^6 7^2 47	3^5 83	7.10618
19^8	2^{11} 7^4 9049	6.80043
384079	3^2 5 37 79	6.76452
3^{13}	5 11 29 137	6.69128
149 1423	5^2 43 113	6.66500
11	3^2	6 61959

TABLE 2. Some curves E with equation (7.1) and high Szpiro ratio $\sigma > 6.6$.

a	b	σ
11	3^2	8.75732
487	2 3^5	7.44460
2^4 19	283	7.32780
5^4	2^5 17	7.20525
17^2 229	29^2	7.16913
2^{15} 13	31^2 59	7.13801
5 563	2^3 3^3 7	7.10156

TABLE 3. Some curves E' with equation (7.2) and high Szpiro ratio $\sigma > 7$.

The next result follows from [Silverman 1986], after some calculations:

Proposition 7.1. *Let a and b be relatively prime integers, and set $g = \gcd(\Delta, c_4)$. Then*

$$g = \gcd(a^2 - ab + b^2,\ a^3 - 8a^2b + 5ab^2 + b^3),$$

and, if g does not divide 7,

(i) *the equations* (7.1) *and* (7.2) *are minimal;*
(ii) *the elliptic curves E and E' are semistable;*
(iii) *the conductors of E and E' are the radicals of Δ and Δ'.*

We return to the Szpiro ratio (1.2). We see that the product $ab(a-b)$ appears in both Δ and Δ'. Hence, for every abc-example $X + Y = Z$, we can derive two elliptic curves E and E' by setting $a = Z$ and $b = X$ in (7.1) and (7.2), and another two by setting $a = Z$ and $b = Y$.

The examples so found for E with the highest Szpiro ratio are given in Table 2, and those for E' in Table 3.

ACKNOWLEDGMENTS

I wish to thank Professor Y. Hellegouarch for his encouragement and J. Browkin and J. Brzezinski for sending me their results.

SOFTWARE AVAILABILITY

The author will provide, upon request, a listing of the abc-examples known to him with $\alpha \geq 1.4$ or $\rho \geq 3.8$.

REFERENCES

[Browkin and Brzezinski 1992] J. Browkin and J. Brzezinski, "Some remarks on *abc*-conjecture", preprint 1992-30, Göteborg Univ.

[Elkies and Kanapka] N. Elkies and J. Kanapka, private communication. The results of this search are available upon request: contact the first author at elkies@math.harvard.edu.

[Nitaj 1992] A. Nitaj, "Algorithms for finding *abc*-examples", preprint **60**, Université de Caen (France), 1992.

[Niven et al. 1991] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, New York, 1991.

[Oesterlé 1988] J.Oesterlé, "Nouvelles approches du théorème de Fermat", Sém. Bourbaki 694, *Astérisque* **161–162** (1988), 165–186.

[Silverman 1986] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[de Weger 1987] B. M. M. de Weger, "Solving exponential diophantine equations using lattice basis reduction algorithms", *J. Number Theory* **26** (1987), 325–367.

Abderrahmane Nitaj, Département de Mathématiques, Université de Caen, 14032 Caen-Cedex, France (nitaj@univ-caen.fr)

Received March 12, 1993; accepted in revised form October 10