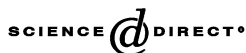




ELSEVIER

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

Journal of Number Theory 107 (2004) 161–167

**JOURNAL OF  
Number  
Theory**<http://www.elsevier.com/locate/jnt>

# LLL & ABC

Tim Dokchitser

*Department of Mathematical Sciences, University of Durham, UK*

Received 4 August 2003; revised 12 December 2003

Communicated by D. Zagier

---

## Abstract

This note is an observation that the LLL algorithm applied to prime powers can be used to find “good” examples for the ABC and Szpiro conjectures.

© 2004 Elsevier Inc. All rights reserved.

*MSC:* Primary: 11D04; Secondary: 11D41, 11D99

*Keywords:* ABC-conjecture; Szpiro conjecture; LLL algorithm

---

Given non-zero integers  $A$ ,  $B$  and  $C$ , define the *radical*  $\text{rad}(A, B, C)$  to be the product of primes dividing  $ABC$ , the *size* to be  $\max(|A|, |B|, |C|)$  and the *power* of the triple to be

$$P = P(A, B, C) = \frac{\log \max(|A|, |B|, |C|)}{\log \text{rad}(A, B, C)}.$$

The ABC conjecture of Masser-Oesterlé [4,7] states that for any real  $\eta > 1$ , there are only finitely many triples with  $A, B, C$  relatively prime and  $P(A, B, C) \geq \eta$  which satisfy the ABC-equation

$$A + B = C.$$

In particular, some work has been done to look for examples of such solutions, called ABC-triples, of as large power as possible (e.g. [2,5,8]; see also the ABC page [6] for an extensive list of references). Similarly, one also looks for solutions with

---

*E-mail address:* [tim.dokchitser@durham.ac.uk](mailto:tim.dokchitser@durham.ac.uk).

large Szpiro quotient

$$\rho = \rho(A, B, C) = \frac{\log |ABC|}{\log \text{rad}(A, B, C)}.$$

These relate via Frey curves to Szpiro’s conjecture on the conductor and the discriminant of elliptic curves. One can also formulate the ABC conjecture over an arbitrary number field  $K/\mathbb{Q}$  in terms of the generalized power [1],

$$P(A, B, C) = \left( \log \prod_{\sigma} \max(|A|_{\sigma}, |B|_{\sigma}, |C|_{\sigma}) \right) / \log \left| A_{K/\mathbb{Q}} \prod_{p|ABC} N_{K/\mathbb{Q}}(p) \right|.$$

The product in the numerator is taken over all embeddings of  $K$  into  $\mathbb{C}$  and the denominator involves the discriminant of  $K$  and the absolute norms of the prime ideals dividing  $A, B$  and  $C$ .

The best examples known to date are: the ABC-triple found by Reysat,

$$A = 2, \quad B = 3^{10} \cdot 109, \quad C = 23^5 \quad \text{with } P = 1.629\dots,$$

and the Szpiro triple found by Nitaj,

$$A = 13 \cdot 19^6, \quad B = 2^{30}5, \quad C = 3^{13}11^231 \quad \text{with } \rho = 4.419\dots$$

The best algebraic ABC example (by de Weger) involves the roots  $r_i$  of  $x^3 - 2x^2 + 4x - 4 = 0$ ,

$$(r_3 - r_2)r_1^{52} + (r_1 - r_3)r_2^{52} + (r_2 - r_1)r_3^{52} = 0, \quad P = 1.920\dots$$

Following terminology of [6], we call a triple with  $P > 1.4$  a good ABC triple and one with  $\rho > 4$  a good Szpiro triple.

Our observation is that a simple method to look for such examples is as follows.

Take, for instance, large prime powers  $A_0 = p^a$ ,  $B_0 = q^b$  and  $C_0 = r^c$  of comparable size with small  $p, q$  and  $r$ . Using the LLL lattice reduction algorithm [3], one can find the smallest integral relation between them with respect to the  $l^2$ -norm,

$$\alpha A_0 + \beta B_0 + \gamma C_0 = 0. \tag{1}$$

Since the coefficients  $\alpha, \beta$  and  $\gamma$  are relatively small, the numbers  $\alpha p^a, \beta q^b$  and  $\gamma r^c$  with suitably chosen signs give a potential candidate for a high-powered ABC-triple. Instead of prime powers one may also take a product of two prime powers or, more generally, any large number with small radical. For example, the smallest relation of the form (1) between

$$A_0 = 71^8, \quad B_0 = 2^5 5^{18} 17^3 \quad \text{and} \quad C_0 = 3^{38}$$

has  $(\alpha, \beta, \gamma) = (12649337, 336633577, -149459713)$ . This gives a previously unknown good triple,

$$A = 71^8 233^3, \quad B = 2^5 5^{18} 7^3 17^3 981439, \quad C = 3^{38} 13^4 5233, \quad P = 1.414\dots$$

Incidentally, this is the largest (with respect to size as above) good ABC example known to the author.

To give an empirical analysis of this approach, take  $A_0 = p^a$ ,  $B_0 = q^b$  and  $C_0 = r^c$  as above, all three approximately of size  $N$ . Then in the worst case the smallest zero combination of the form (1) has coefficients  $\alpha$ ,  $\beta$  and  $\gamma$  roughly of size  $\sqrt{3N}$ . In fact, there are about  $(\sqrt{3N})^3$  combinations

$$iA_0 + jB_0 + kC_0, \quad 0 \leq i, j, k \leq \sqrt{3N}. \tag{2}$$

As they are all of size at most  $3 \times N\sqrt{3N} = (\sqrt{3N})^3$ , two of them must be equal by the box principle and their difference gives a required relation. Therefore, in the worst case the resulting triple has

$$P(A, B, C) \approx \frac{\log(N\sqrt{3N})}{3 \log \sqrt{3N} + \log p + \log q + \log r}.$$

For fixed  $p$ ,  $q$  and  $r$ , this expression tends to 1 as  $N$  goes to infinity, so the triples are “on the edge” of what is predicted by the ABC conjecture.

It is easy to implement the above method to actually search for some explicit new examples. To illustrate one practical consideration, take

$$A_0 = 1, \quad B_0 = 3^4, \quad C_0 = 5^4.$$

Here LLL reduction shows that the lattice of relations between these numbers is generated by

$$v_1 = (23, -8, 1) \quad \text{and} \quad v_2 = (12, 23, -3).$$

Then  $v_1$  gives a reasonable ABC-triple, but a few other small combinations of  $v_1$  and  $v_2$  yield even better ones,

$$\begin{aligned} v_1 &= (23, -8, 1) \Rightarrow (A, B, C) = (23, 5^4, 2^3 3^4), \quad P = 0.990\dots, \\ -v_1 + 2v_2 &= (1, 54, -7) \Rightarrow (A, B, C) = (1, 2 \cdot 3^7, 5^4 7), \quad P = 1.567\dots, \\ 4v_1 - v_2 &= (104, -9, 1) \Rightarrow (A, B, C) = (2^3 13, 5^4, 3^6), \quad P = 1.104\dots \end{aligned}$$

This suggests to run a search as follows. Take a list  $L$  of numbers to serve as  $A_0$ ,  $B_0$  and  $C_0$ . For example, choose bounds  $M$  and  $N$  and consider all numbers less than  $M$  whose prime factors are less than  $N$ . Then for all distinct  $A_0$ ,  $B_0$ , and  $C_0$  in  $L$  use LLL to determine the reduced set of generators for the lattice of relations between

them. Then take “small” combinations of these generators and check whether the resulting ABC-triple has a sufficiently high power.

This does raise a question of how to decide which combinations of the  $v_i$  one should try. A few experiments suggest that a sensible choice is to try those  $v = c_1 v_1 + c_2 v_2$  which simply make one of the elements of  $v$  small. This is a cheap way to keep the radical of the product of the elements of  $v$  to be as small as possible. To achieve this for an index  $i \in \{1, 2, 3\}$ , look at minus the  $i$ th entry of  $v_1$  divided by that of  $v_2$  and try several continued fraction approximations  $c_2/c_1$  of this quotient. (In the example above,  $-2/1$  is the first approximation to  $-23/12$  and it makes the first entry small.) Incidentally, this is essentially using a form of LLL again.

Such a search has been implemented as a straightforward Pari script with a running time of one weekend distributed over 30 PCs. We found 145 out of 154 known good ABC-triples, 44 out of 47 known good Szpiro triples and many new examples, listed in Tables 1 and 2.

Let us conclude with a few remarks.

First, note that although the approach presented here is apparently new, LLL has been used in different ways in relation to the ABC conjecture; see e.g. [6].

Second, the method seems to work best when  $A_0$ ,  $B_0$  and  $C_0$  are of approximately equal size. In particular, one might expect it to be more suitable for finding new Szpiro examples rather than ABC examples. And, indeed, we have 48 new (47 known) good Szpiro triples but only 41 new (154 known) good ABC triples.

One can also perform a similar search in number fields and find several interesting algebraic examples. For instance, take the field  $K = \mathbb{Q}(\sqrt{13})$  and  $w = (3 + \sqrt{13})/2$ , the fundamental unit of  $K$ . Let

$$A = w^{-5}(w - 1) = 0.0058594420567\dots,$$

$$B = w^5(w - 2) = 511.9941405579432\dots,$$

$$C = 2^9 = 512.0000000000000\dots$$

Then  $A$  and  $B$  are conjugate and  $A + B = C$ . Moreover, 2 is prime in  $K$  and  $(w - 1)(w - 2) = 3$ . Hence the ABC-ratio is

$$P(A, B, C) = \frac{2 \log(512)}{\log 13 + \log 3 + \log 3 + \log 4} = 2.0292288501126\dots$$

So, this example is a new record for the algebraic ABC conjecture.

Finally, the same method can be also used to look for examples for the generalization of the ABC-conjecture to solutions of  $a_1 + \dots + a_n = 0$ , known as the  $n$ -conjecture, see Browkin–Brzezinski [2].

The author would like to thank N. Afanassieva for providing inspiration to work on this problem and V. Dokchitser for helpful discussions.

Table 1  
New Szpiro examples with  $\rho(A, B, C) > 4$

A	B	C	$\log_{10} C$	$\rho(A, B, C)$
$19^8 43^4 149^2$	$2^{15} 5^{23} 101$	$3^{13} 13 \cdot 29^2 37^6 911$	22.6	4.23181492
$2^7 5^4 7^{22}$	$19^4 37 \cdot 47^4 53^6$	$3^{14} 11 \cdot 13^9 191 \cdot 7829$	23.9	4.21019250
$2^{17} 3^{19} 11 \cdot 25867$	$7^{12} 23^7$	$5 \cdot 37^{10} 53 \cdot 71$	20.0	4.14980287
$7^8 13 \cdot 89^3$	$3^{13} 5^3 11^4 1499$	$2 \cdot 19^{12}$	15.6	4.13636237
$11^3 31^5 101 \cdot 479$	$107^8$	$2^{31} 3^4 5^6 7$	16.3	4.13000150
$13^{10} 37^2$	$3^7 19^5 71^4 223$	$2^{26} 5^{12} 1873$	19.5	4.12465150
$2^{55} 23$	$3^{13} 7^9 13 \cdot 79^2$	$11^4 43^6 65353$	18.8	4.10906942
$11^8 13^9 53$	$2^4 5^{16} 17 \cdot 547 \cdot 6163$	$7^6 19^{12}$	20.4	4.10809327
$233^4 439$	$2^{15} 3^{19}$	$5^8 17^5 71$	13.6	4.10589886
$2^{13} 7^{12} 337^3$	$7^{13} 1117^2$	$3^{21} 13^3 73^2$	17.1	4.10470805
$5^7 23^7 1493$	$31^8 3907^2$	$2^{52} 3^2 331$	19.1	4.10115990
$2^{13} 5^{12} 13^4 29$	$7^{16} 19 \cdot 7451$	$3^{20} 11^4 353^2$	18.8	4.08362226
$11^{11} 73^2 991 \cdot 306083$	$2^2 3 \cdot 5^{11} 7^{15} 19^2$	$13^{15} 31^5$	24.2	4.08299029
$2 \cdot 5^9 11^4 41^2 53^3$	$3^9 7^{16} 37$	$23^{11} 40423$	19.6	4.08262163
$31 \cdot 59^6$	$2^{25} 3^{11}$	$5^3 11^7 13 \cdot 229$	12.9	4.07920132
$3^{13} 13 \cdot 23^3 97^2$	$2^{37} 157^2$	$5^5 31^7 67$	15.8	4.07456723
$3^2 73^{10}$	$5^{25} 17^2 23$	$2^2 7^{11} 827^2 373357$	21.3	4.07337395
$3^4 5^{18} 71 \cdot 419 \cdot 876581$	$2^{17} 13^2 19^{15}$	$7^6 11^{12} 977^3$	26.5	4.06888583
$2^{26} 11^4 7639$	$5^6 23^{11}$	$3^{18} 47^4 7879$	19.2	4.06704768
$5^{16} 19^2$	$3^8 7^3 89^4$	$2^{28} 11^2 6043$	14.3	4.06668234
$5^7 7^7 19^2 107$	$2^{14} 11^9 97$	$3^{10} 23^7 31$	15.8	4.06231271
$2^7 3 \cdot 821^5$	$13^{16}$	$5^{12} 101^2 324697$	17.9	4.06159736
$3^4 23^6 1013^2$	$2^{47} 5^3 19^2$	$7 \cdot 131^7 1373$	18.8	4.06076852
$3^5 5^{16} 19^3$	$7^5 23^2 233^4 1321$	$2^{48} 43^2 67$	19.5	4.06075266
$83^2 107^6$	$3^{17} 5^{10} 23$	$2 \cdot 7^2 13^9 17^2 131$	16.6	4.05751107
$2^6 23^{11} 53 \cdot 121523$	$7 \cdot 11^{17} 13^3 89$	$3^6 17 \cdot 311^8$	24.0	4.05572551
$5^9 2141^2$	$2^{17} 11 \cdot 53^4$	$3^2 7 \cdot 19^9$	13.3	4.05435143
$2^9 3^{12} 17^9 1049$	$5^{19} 23 \cdot 83 \cdot 491^2 761$	$7^{12} 13^4 19^8$	24.8	4.05071167
$13^3 17^2 131^5$	$2^{24} 7^4 11 \cdot 29^3 103$	$3^3 5^{19} 47^2$	18.1	4.04634190
$5^{26} 11^2 19^2$	$2^{11} 139 \cdot 401^6 463$	$3^{28} 7^2 37^2 67^2 89$	23.8	4.04303710
$2^{47} 3^7 13^2$	$19^{11} 23 \cdot 67^2 227$	$5 \cdot 11 \cdot 257^6 419^2$	21.4	4.04183984
$2^4 5^3 17^6 19^2 151$	$7^{11} 257^3$	$31^9 37^2$	16.6	4.04112782
$3^9 17^7 67$	$5^7 7^9 19 \cdot 439$	$2^4 13^{10} 23^3$	16.4	4.04071176
$5^2 17^6 61^2 269$	$2^{12} 11^{12}$	$3^{19} 7^5 13 \cdot 53$	16.1	4.03689092
$5^{20} 4021$	$2^{40} 13 \cdot 17^3 6763$	$3^6 7^7 11^3 29^6$	20.7	4.03545668
$2^{23} 5^2 17^8$	$3^2 67 \cdot 743^6$	$13^9 23^4 34679$	20.0	4.03484329
$23^5 43^5 397$	$3^{33} 5^3$	$2^{27} 7 \cdot 29 \cdot 73^3 101$	18.0	4.03482389
$3^7 7^5 17^2 239441$	$2^9 5^{13} 11^4$	$61^9$	16.1	4.03406000
$31^7 113 \cdot 491^2$	$5^{13} 11 \cdot 13 \cdot 19^8$	$2 \cdot 3^6 7^{18} 1249$	21.5	4.03083567
$2^2 5 \cdot 11^3 23^4 29^7$	$13^9 71^4 113^2$	$3^{34} 214033$	21.6	4.02756838
$2^7 7 \cdot 139^5$	$11 \cdot 41 \cdot 131^6$	$3^{27} 5 \cdot 61$	15.4	4.02755513
$2^{28} 101 \cdot 197^4$	$37^{11} 653$	$5^{14} 7^2 11^2 2083^2$	20.2	4.02174827
$5^2 13 \cdot 37^6 13789$	$2^9 7^8 47^4$	$3^{21} 19^3$	16.4	4.02095059
$3 \cdot 5 \cdot 67^9$	$11^8 13^3 47^3 73$	$2^{14} 7^3 41^6 149$	18.6	4.01929332
$2^{27} 3 \cdot 13^2 19^5$	$5^6 31^6 263^2$	$37^9 8677$	18.1	4.00826664
$71^8 233^3$	$2^5 5^{18} 7^3 17^3 981439$	$3^{38} 13^4 5233$	26.3	4.00747592
$5^{15} 13^6 23^2$	$2^{31} 61 \cdot 271^2 19157$	$3^{26} 7^3 67^3$	20.4	4.00512378
$11^7 41^4$	$5^2 7^7 13^4 211$	$2^{15} 3^{16} 127$	14.3	4.00133657

Table 2  
New ABC examples with  $P(A, B, C) > 1.4$

$A$	$B$	$C$	$\log_{10} C$	$P(A, B, C)$
$13^{10} 37^2$	$3^7 19^5 71^4 223$	$2^{26} 5^{12} 1873$	19.5	1.50943262
$19^8 43^4 149^2$	$2^{15} 5^{23} 101$	$3^{13} 13 \cdot 29^2 37^6 911$	22.6	1.44280331
$3 \cdot 5^6 7^8 53$	$167^9$	$2 \cdot 11^6 193^4 20551$	20.0	1.43823826
$2^{26} 11^4 7639$	$5^6 23^{11}$	$3^{18} 47^4 7879$	19.2	1.43813867
$7^8 13 \cdot 89^3$	$3^{13} 5^3 11^4 1499$	$2 \cdot 19^{12}$	15.6	1.43785988
$17^4 19^6$	$41^{10} 1559$	$2^{12} 3^{15} 5 \cdot 29 \cdot 1567^2$	19.3	1.43654400
$3^4 7^2 41$	$2^{25} 227^7$	$5^9 11^8 2489197589$	24.0	1.43575084
$3^{17} 809$	$2^{27} 11^9$	$5 \cdot 7^4 13^5 59 \cdot 1097^2$	17.5	1.43485873
$11 \cdot 103^8$	$2^{45} 3^7 29 \cdot 37 \cdot 1997$	$5^{11} 7^{10} 79 \cdot 389^2$	23.2	1.43360120
$7^{11} 19$	$5^{12} 1019 \cdot 7151^2$	$2^{28} 3^{12} 11^3 67$	19.1	1.43309388
$2^{17} 13^3$	$7^3 11^7 43^2 5801$	$3^{17} 17^6 23$	16.9	1.43234742
$7^2 23^5$	$3^8 11^{12} 4703$	$2 \cdot 5^2 13^2 19^3 29^6 53^2$	20.0	1.42991591
$2^{20} 79 \cdot 97$	$5^3 7^6 11^{10}$	$3^4 13^7 8663^2$	17.6	1.42942802
$29^4$	$2^{14} 3^3 31 \cdot 47^2 199^3$	$7^{12} 4153^2$	17.4	1.42836105
$2^{27} 809$	$5^7 7^6 13^5$	$3^{23} 36251$	15.5	1.42460741
$2^{13} 3^{18} 2069$	$13^3 29^7 271^3$	$5^{14} 23^3 3187^2$	20.9	1.42340611
$31^7 113 \cdot 491^2$	$5^{13} 11 \cdot 13 \cdot 19^8$	$2 \cdot 3^6 7^{18} 1249$	21.5	1.42308625
$3^4 23^6 1013^2$	$2^{47} 5^3 19^2$	$7 \cdot 131^7 1373$	18.8	1.42201537
$3 \cdot 5 \cdot 13^6$	$2^7 7^5 53^6 2287$	$11^3 37^7 929^2$	20.0	1.42137859
$233^4 439$	$2^{15} 3^{19}$	$5^8 17^5 71$	13.6	1.42081322
$2^{13} 71^2 337^3$	$7^{13} 1117^2$	$3^{21} 13^3 73^2$	17.1	1.42075105
$17^2 47^5 73$	$2^{31} 5^9$	$3 \cdot 13^7 4723^2$	15.6	1.41627640
$2^7 5^4 7^{22}$	$19^4 37 \cdot 47^4 53^6$	$3^{14} 11 \cdot 13^9 191 \cdot 7829$	23.9	1.41582933
$5^{20} 4021$	$2^{40} 13 \cdot 17^3 6763$	$3^6 7^7 11^3 29^6$	20.7	1.41575870
$3^{22} 9787^2$	$5^{10} 11 \cdot 29^{10} 109$	$2^{37} 89^3 167^2 1823$	24.7	1.41570162
$71^8 233^3$	$2^5 5^{18} 7^3 17^3 981439$	$3^{38} 13^4 5233$	26.3	1.41457078
$29^4 2213^2$	$3 \cdot 13^2 23^{12} 89 \cdot 14717$	$2^9 5^{16} 11^9 79$	25.2	1.41234761
$5^4 17 \cdot 349^3$	$7^{17} 109$	$2^{35} 3^5 3037$	16.4	1.41227598
$3^{11} 7^2 37 \cdot 47$	$2^8 17^3 101^2 191^4$	$5^2 353^7$	19.2	1.41143590
$2^{29} 13$	$5^{11} 269^3$	$3^5 7^2 17^6 3307$	15.0	1.41090947
$5^4 53^2 59^4 101$	$2^4 11 \cdot 23^{15}$	$3^{14} 7^{12} 463 \cdot 1531$	22.7	1.41032306
$2^{11} 3^4 101^4 29221$	$13^{19}$	$5^{15} 17 \cdot 53093^2$	21.2	1.40944818
$7^4$	$3^{21} 11^2 13^4 138493$	$2^{26} 5^7 383 \cdot 1579^2$	21.7	1.40900897
$11^3 31^5 101 \cdot 479$	$107^8$	$2^{31} 3^4 5^6 7$	16.3	1.40714951
$3^5 5^{16} 19^3$	$7^5 23^2 233^4 1321$	$2^{48} 43^2 67$	19.5	1.40487025
$5^7 23^7 1493$	$31^8 3907^2$	$2^{52} 3^2 331$	19.1	1.40479669
$2^2 3^4 163^3 1006151$	$43^{13}$	$11^9 29^4 101^3$	21.2	1.40308397
$2^{11} 3^{17} 13^2 19^2$	$29 \cdot 41^2 83^8$	$5^4 47^2 53 \cdot 107^6$	20.0	1.40244119
$3^6 7^4 43 \cdot 16421$	$5^{12} 439^6$	$2^{59} 41 \cdot 73939$	24.2	1.40168452
$7^9 13^4$	$2^{10} 23^3 173^4$	$3^{12} 5 \cdot 11^6 2371$	16.0	1.40127027
$17^4$	$2 \cdot 7^{12} 29^3 743$	$3^9 5^6 13^5 23 \cdot 191$	17.7	1.40004159

## References

- [1] N. Broberg, Some examples related to the *abc*-conjecture for algebraic number fields, *Math. Comput.* 69 (232) (2000) 1707–1710.
- [2] J. Browkin, J. Brzezinski, Some remarks on the *abc*-conjecture, *Math. Comput.* 62 (206) (1994) 931–939.
- [3] A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (4) (1982) 515–534.
- [4] D. Masser, Open problems, in: W.W.L. Chen (Ed.), *Proceedings of the Symposium on Analytic Number Theory*, Imperial College, London, 1985.
- [5] A. Nitaj, Algorithms for finding good examples for the *abc* and Szpiro conjectures, *Exp. Math.* 2 (3) (1993) 223–230.
- [6] A. Nitaj, The ABC conjecture home page, [www.math.unicaen.fr/~nitaj/abc.html](http://www.math.unicaen.fr/~nitaj/abc.html).
- [7] J. Oesterlé, Nouvelle approches du théorème de Fermat, *Astérisque* 161–162 (1988) 165–186.
- [8] B.M.M. de Weger, Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Theory* 26 (1987) 326–367.