$A + B = C$ and big Ш's

By BENJAMIN M. M. DE WEGER*

[Received February 11, 1997]

Abstract—Assuming standard conjectures we show that there exist elliptic curves with Tate-Shafarevich group of order essentially as large as the square root of the conductor. We present some concrete examples of such elliptic curves, related to good examples for the ABC-Conjecture.

1. Introduction

RECENTLY Goldfeld and Szpiro [**10**] posed the following conjecture.

CONJECTURE 1 (Goldfeld-Szpiro) *For elliptic curves over* $\mathbb{Q}$ *with Tate-Shafarevich group* Ш *and conductor* N *one has*

$$|\text{Ш}| \ll N^{1/2+\varepsilon}. \tag{1}$$

Goldfeld and Lieman [**9**] proved some results in the direction of this conjecture.

For modular elliptic curves that satisfy the Birch-Swinnerton-Dyer Conjecture, Goldfeld and Szpiro [**10**] show that the bound (1) is equivalent to the Szpiro Conjecture $|\Delta| \ll N^{6+\varepsilon}$, where Δ denotes the minimal discriminant of the elliptic curve. It is known that the Szpiro Conjecture implies a variant of the ABC-Conjecture. This latter implication is proved by considering for an example of coprime $A, B, C \in \mathbb{N}$ with $A + B = C$ the corresponding Frey-Hellegouarch curve

$$y^2 = x(x - A)(x + B), \tag{2}$$

see e.g. Osterlé [**22**] and Vojta [**28**]. Indeed, if $N(A, B, C)$ is the product of the primes dividing ABC, then the conductor N of the Frey-Hellegouarch curve (2) equals $N(A, B, C)$ up to a bounded power of 2, and its minimal discriminant Δ equals $(ABC)^2$ up to a bounded power of 2. In this paper we reserve the word *Frey-Hellegouarch curve* for a curve (2) with coprime $A, B \in \mathbb{N}$. Note that such curves are semi-stable at all odd primes, so that they are modular indeed, by the celebrated results of Wiles [**30**] and Diamond [**7**].

For an example of $A + B = C$ which is 'good' for the ABC-Conjecture, i.e. with $N(A, B, C)$ small compared to C, the Frey-Hellegouarch curve

* This research was supported by the Netherlands Mathematical Research Foundation SWON with financial aid from the Netherlands Organization for Scientific Research NWO.

(2) has relatively small conductor. One might hope that its Tate-Shafarevich group Ш is normally sized, whatever that may mean, and thus is large compared to the (square root of the) conductor. In this note we will show, assuming some standard conjectures, that that is indeed true for certain quadratic twists of this Frey-Hellegouarch curve. We can formulate the following conjecture, which is complementary to the Goldfeld-Szpiro Conjecture 1, in the sense that it asserts that the bound (1) is best possible, apart from ε's.

CONJECTURE 2 *For every* $\varepsilon > 0$ *there exist infinitely many elliptic curves over* $\mathbb{Q}$ *with* $|Ш| \gg N^{1/2-\varepsilon}$.

In fact, as we shall see below, the curves that we are dealing with have rank zero, all their 2-torsion rational, and are 'almost semistable'.

The implicit constant in the inequality in Conjecture 2 depends a priori on ε, but this can be removed. Let $\varepsilon > 0$ and $c > 0$ be given. Conjecture 2 implies the existence of a constant $c' > 0$, depending on ε, such that there are infinitely many curves with $|Ш| > c'N^{1/2-\varepsilon/2}$. Note that since there are only finitely many curves with given conductor, infinitely many of these curves have $N > (c/c')^{2/\varepsilon}$, and thus $|Ш| > cN^{1/2-\varepsilon}$. Thus Conjecture 2 implies the following.

CONJECTURE 3 *For every* $\varepsilon > 0$ *and every* $c > 0$ *there exist infinitely many elliptic curves over* $\mathbb{Q}$ *with* $|Ш| > cN^{1/2-\varepsilon}$.

We also formulate a similar conjecture in terms of the minimal discriminant instead of the conductor.

CONJECTURE 4 *For every* $\varepsilon > 0$ *there exist infinitely many elliptic curves over* $\mathbb{Q}$ *with* $|Ш| \gg \Delta^{1/12-\varepsilon}$.

We will show that these conjectures follow from a few standard conjectures. The situation is the best in the case of Conjecture 4, which depends only on the Birch-Swinnerton-Dyer Conjecture in the rank zero case. This latter has been 'almost proved' by Kolyvagin **[14]**, **[15]**.

The idea behind our proofs is more or less constructive, so that we can actually try to compute curves with big Tate-Shafarevich groups. We present some concrete examples, coming from good examples for the ABC-Conjecture. In searching for concrete examples one should take into account not only twists of Frey-Hellegouarch curves, but also all curves in the isogeny classes of these twists. Notice that a Frey-Hellegouarch curve has all its 2-torsion rational, and the same is true for its quadratic twists, but not necessarily for the other curves in its isogeny class. Conversely, any curve that has all its 2-torsion rational is a (quadratic twist of a) Frey-Hellegouarch curve.

The best example (in the sense that it has the largest $|Ш|$, and also in the sense that it has the largest value of $|\mathrm{III}|/\sqrt{N}$) that we found is the curve

$$y^2+xy+y=x^3+x^2$$
$$-16272564754316406252451x-798973042220714620227331980906826.$$

The curve has conductor $N=51636585$, and the order of III is (conjecturally) $50176=224^2$. So the ratio $|\mathrm{III}|/\sqrt{N}$ is large indeed, namely about 6.893. We found a number of other curves with $|\mathrm{III}|>\sqrt{N}$. Such curves were already known from the tables of Cremona, **[6]**. His best example (again with largest $|\mathrm{III}|$ and largest $|\mathrm{III}|/\sqrt{N}$) is the curve coded $546F_2$, with $|\mathrm{III}|=49$, $N=546$, hence $|\mathrm{III}|/\sqrt{N}\approx 2.097$. Brumer and McGuinness **[3]** mention a curve with $|\mathrm{III}|=289$, but they do not give the conductor, only that it is prime and at most 10^8, so all we know is that $|\mathrm{III}|/\sqrt{N}>0.0289$.

On the theoretical side it has been known for a long time that $|\mathrm{III}|$ is unbounded. Cassels **[4]** was the first to show this, and see also Bölling **[1]**, Kramer **[16]**, and Mai and Murty **[20]**. Cassels, Bölling and Kramer did not consider the conductors. Cassels and Bölling obtain their results by looking at quadratic twists by more and more primes. Each time a prime is added, they win a constant factor in $|\mathrm{III}|$, but the conductor goes up by the square of the prime. Thus it seems that at best their method gives elliptic curves with $|\mathrm{III}|\gg N^{c/\log\log N}$ for some constant $c>0$, by the Prime Number Theorem. Kramer has a somewhat different strategy, and finds semistable curves with discriminant $m(16m+1)$ and $|\mathrm{III}|\geqslant 2^{2k-2}$, where k is the number of prime factors of $16m+1$. Again it seems that at best this yields $|\mathrm{III}|\gg N^{c/\log\log N}$ for some constant $c>0$. Hence our Conjecture 2 gives a better lower bound than Cassels, Bölling and Kramer, but it relies on unproved assumptions, whereas the results of Cassels, Bölling and Kramer are unconditional. Mai and Murty **[20]** have shown, assuming only the Birch-Swinnerton-Dyer Conjecture, that there exist infinitely many elliptic curves with $|\mathrm{III}|\gg N^{1/4-\varepsilon}$. They too consider quadratic twists, and show that twisting by q causes the mean of $q^{-1/2}|\mathrm{III}_q|$ for $q<Q$ to be $\gg Q^{-\varepsilon}$ and $\ll Q^{\varepsilon}$, whereas the conductor is essentially q^2. In particular this means that their conductors are 'almost square'. In contrast, the curves we find below are 'almost semistable', i.e. the conductors are 'almost squarefree'.

Acknowledgements

The author is grateful to several participants of the ICMS workshop on Curves and Computations in Edinburgh, 25–29 March 1996 (where the idea for this paper emerged), especially to Bryan Birch, John Cremona, Noam Elkies, Dorian Goldfeld, Joe Silverman, Nigel Smart and Jaap

Top. He is also grateful to Jean-Marc Deshouillers for pointing out the key idea to the proof of Lemma 1.

2 Conjectures

For an elliptic curve E defined over $\mathbb{Q}$ we adopt the following notations (for precise definitions see the standard textbooks such as those by Knapp **[12]** and Silverman **[23]**, **[24]**:

III = the Tate-Shafarevich group,
N = the conductor,
Δ = the minimal discriminant,
ω = the real period,
$\Omega = \omega$ or 2ω, according to $E(\mathbb{R})$ being connected or not,
T = the order of the torsion subgroup,
r = the rank,
R = the regulator,
$L(s)$ = the L-series,
c = the Tamagawa number, also called *fudge factor.*

The following conjectures are generally believed to be true but hopeless to prove.

Conjecture 5 (Birch-Swinnerton-Dyer)

$$\lim_{s\to 1}(s-1)^{-r}L(s)=\frac{c\Omega R\,|\text{III}|}{T^2}. \tag{3}$$

Conjecture 6 (Szpiro) $\Delta \ll N^{6+\varepsilon}$.

Furthermore we will need the following conjecture (cf. Goldfeld and Szpiro **[10]**.

Conjecture 7 (Riemann-hypothesis). *The Riemann-hypothesis for the Rankin-Selberg zeta-function associated to the weight $\frac{3}{2}$ modular form associated to E by the Shintani-Shimura lift is true.*

For the sake of completeness we mention the ABC-Conjecture. For A, B, $C \in \mathbb{N}$ we define

$$N(A,B,C)=\prod_{\text{primes } p \mid ABC} p.$$

Conjecture 8 (ABC-Conjecture, Masser-Oesterlé) *For coprime A, B, $C \in \mathbb{N}$ with $A+B=C$ one has*

$$C \ll N(A,B,C)^{1+\varepsilon}.$$

Note that for coprime A, B, C, the conductor N of the Frey-Hellegouarch curve (2) equals $N(A, B, C)$ times an absolutely bounded power of 2.

Various relations between the above mentioned conjectures are known. Assuming the Birch-Swinnerton-Dyer Conjecture, the Szpiro Conjecture 6 is equivalent to the Goldfeld-Szpiro Conjecture 1 (see **[10]**). The Szpiro Conjecture 6 is equivalent to a somewhat weaker form of the ABC-Conjecture 8 (the ABC-Conjecture 8 itself is equivalent to the so-called Generalized Szpiro Conjecture $\max\{|\Delta|, |g_2^3|\} \ll N^{6+\varepsilon}$), see Oesterlé **[22]** and Vojta **[28]**. At first sight this is true only for the cases where $16 \mid ABC$, but as Noam Elkies explained[1], this covers all cases for the ABC-Conjecture, by considering $A^4 + (C^4 - A^4) = C^4$ if $16 \nmid ABC$ (where, without loss of generality, B is assumed to be odd).

We will need the Birch-Swinnerton-Dyer formula (3) only in the case of rank $r = 0$. In this case major steps towards its proof have been made by Kolyvagin **[14]**, **[15]**. However, we need almost the full strength of the exact formula (3), which still is not shown to be true in the rank zero case.

The main results of this note can now be stated as follows.

THEOREM 1 *Assuming Conjecture* 5 (*in the rank zero case*) *and Conjectures* 6 *and* 7, *Conjecture* 2 *follows.*

THEOREM 2 *Assuming Conjecture* 5 (*in the rank zero case*), *Conjecture* 4 *follows.*

3 Sketch of the proofs

In this section we sketch the proof of Theorem 1, postponing the details and the proof of Theorem 2 to Section 5. Our starting point is the Birch-Swinnerton-Dyer formula (3) for a Frey-Hellegouarch curve (2) associated to an example of $A + B = C$ with, say, $C > N$. Such examples exist, as can easily be shown (simply take $A = 1$, $B = 3^{2^k} - 1$, or be more intelligent and see Stewart and Tijdeman **[26]**, who prove the existence of infinitely many examples with

$$C > N(A, B, C) \exp\left((4-\delta)\frac{\sqrt{\log N(A, B, C)}}{\log\log N(A, B, C)}\right)$$

for every $\delta > 0$).

We want to estimate $|\text{III}|$ by estimating all the other quantities occurring in the Birch-Swinnerton-Dyer formula (3). The order T of the torsion group is at least 1, and so does not bother us at all. The period Ω,

[1] Private communication.

which in the case of Frey-Hellegouarch curves always equals 2ω, is an elliptic integral, which can be estimated by

$$\omega \ll \frac{1}{\sqrt{C}} \log C.$$

Hence $\Omega \ll N^{-1/2+\varepsilon}$. Even if $A + B = C$ is not a 'good' example, we still have $C > (ABC)^{\frac{1}{3}} \geqslant N(A, B, C)^{\frac{1}{3}}$, hence $\Omega \ll N^{-1/6+\varepsilon}$. In a sense it is these small periods, occurring for all Frey-Hellegouarch curves, that make their Tate-Shafarevich groups big.

Upper bounds for the regulator and lower bounds for the value at $s = 1$ of the rth derivative of the L-series are not known (but see **[18]** for conjectures, which seem to be of no use to us). However, both problems can be solved at once by changing from the Frey-Hellegouarch curve (2) itself to an appropriate quadratic twist. By the curve twisted by a (squarefree) $q \in \mathbb{N}$ we mean the elliptic curve

$$qy^2 = x(x - A)(x + B). \tag{4}$$

We denote the L-series of this twist by $L_q(s)$. Following Kohnen and Zagier **[13]** (see **[8]** and **[10]**) it can be shown that

$$\sum_{q \leqslant N^2} L_q(1) \gg N^2, \tag{5}$$

and if one assumes Conjecture 7, then this can be improved to

$$\sum_{q \leqslant N^\varepsilon} L_q(1) \gg N^\varepsilon.$$

Here the sums are taken over the q's for which the quadratic Dirichlet character has a prescribed value at -1, depending only on A, B, C. Anyway, there is a quadratic twist by a small q for which

$$L_q(1) \gg 1. \tag{6}$$

It follows that $L_q(1) \neq 0$, so that according to the Birch-Swinnerton-Dyer Conjecture 5 the rank r of the twisted curve must be zero. Now we can kill two birds with one stone, since in the first place we have with (6) a lower bound for the left hand side in the Birch-Swinnerton-Dyer formula (3), and in the second place the regulator is trivial, namely $R = 1$. (In fact, we almost killed a third bird, by Kolyvagin's work **[14]**, **[15]**.) The twisting will change the period ω by a factor of about $\sqrt{q}$ (but only to our advantage), and the conductor N by a factor at most q^2 (to our disadvantage). This is the price that we pay for killing the birds. But if we also pay the price of assuming Conjecture 7, the conductor changes at worst by a factor of order N^ε.

It remains to estimate the Tamagawa number c. We cannot use trivial estimates here, because we have to deal with the possibility that the reduction at all the bad primes is split multiplicative, causing for each bad prime p a (possibly large) contribution of $\mathrm{ord}_p(\Delta)$ to the Tamagawa number. It seems to be folklore that c cannot be too large for arbitrary elliptic curves, but no proof was found in the literature. Moreover, when asked, experts seemed to guess a much better bound (e.g. $c \ll \log \Delta$) than we can prove. Therefore we spend the next section in analytic number theory to show that $c < \Delta^{\kappa/\log\log\Delta}$ for some absolute constant $\kappa > 0$. This is worse than any fixed large power of $\log \Delta$, but better than any fixed small positive power of Δ. With the Szpiro Conjecture 6 this thus implies $c \ll N^{\varepsilon}$, which is enough for our purposes.

Now, on putting all our estimates together with the Birch-Swinnerton-Dyer formula (3), Theorem 1 follows.

4 Bounding the Tamagawa number

For a positive integer n we define $c(n)$ to be the product of the exponents in the prime decomposition of n. We need a bound for $c(n)$, but could not find one in the literature.

LEMMA 1 *For any $n \in \mathbb{N}$ we have*

$$c(n) \ll N^{\frac{\log 3}{3}(1+\varepsilon)/\log\log n}.$$

P. Erdös, who in a letter to the present author dated September 3, 1996 conjectured this result, noted that the constant $\dfrac{\log 3}{3}$ cannot be improved, as the cubes of the products of the first r primes show. The proof below mimics a similar proof for the function $d(n)$ (the number of divisors of n), as given in Theorems 315–317 of **[11]**. This line of proof was pointed out to the author by Jean-Marc Deshouillers.

Proof. Let $\varepsilon > 0$ be given. Put $\delta = \dfrac{\log 3}{3}(1 + \frac{1}{2}\varepsilon)/\log\log n$. For the primes $p > 3^{1/(3\delta)}$ dividing n we use that for $n \in \mathbb{N}$ we have

$$\frac{n}{p^{\delta n}} \leqslant \frac{n}{3^{n/3}} \leqslant 1.$$

For the primes $p \leqslant 3^{1(3\delta)}$ dividing n, of which there are at most $3^{1/(3\delta)}$, we use

$$\frac{n}{p^{\delta n}} \leqslant \exp\left(\frac{1}{\delta \log 2}\right).$$

If the prime decomposition of n is given by $n = \prod_{i=1}^{r} p_i^{n_i}$, then we have $\frac{c(n)}{n^{\delta}} = \prod_{i=1}^{r} \frac{n_i}{p_i^{\delta n_i}}$, and thus

$$\log c(n) - \delta \log n \leqslant 3^{1/(3\delta)} \frac{1}{\delta \log 2}$$

$$= \frac{3(\log n)^{1/(1+\frac{1}{2}\varepsilon)} \log\log n}{(\log 2)(\log 3)(1+\frac{1}{2}\varepsilon)} < \frac{\log 3}{3}\left(\frac{1}{2}\varepsilon\right)\frac{\log n}{\log\log n}$$

for n large enough, and the result follows.

Now we are in a position to prove a bound for the Tamagawa number.

THEOREM 3 *For the Tamagawa number c of any elliptic curve defined over $\mathbb{Q}$ we have*

$$c < \Delta^{\kappa/(\log\log\Delta)}$$

for some absolute constant κ.

Proof. We have $c = \prod_p c_p$, where the product runs through the bad primes, i.e. the primes p that divide Δ, and c_p is given in Tate's algorithm (see [**27**] or [**24**]). From this algorithm it becomes clear that

$$c_p \leqslant \max\{4, \operatorname{ord}_p(\Delta)\}$$

(see also [**23**], Corollary C.15.2.1). Let $\Delta = \Delta_1\Delta_2$, where Δ_1 contains the factors from the prime decomposition of Δ with exponents at most 4. Let s be the number of those factors. Then it follows that

$$c \leqslant 4^s c(\Delta_2).$$

If $2 = p_1 < p_2 < \cdots < p_s$ are the first s primes, then certainly

$$\log \Delta_1 \geqslant \sum_{i=1}^{s} \log p_i \geqslant \sum_{i=1}^{s} \log(i+1)$$

$$> \int_1^{s+1} \log x\, dx = (s+1)\log(s+1) - s > \kappa_1 s \log s$$

for some constant $\kappa_1 > 0$. It follows that for some constant $\kappa_2 > 0$ we have

$$s < \kappa_2 \frac{\log \Delta_1}{\log\log\Delta_1},$$

so that for a constant $\kappa_3 > 0$

$$4^s < \Delta_1^{\kappa_3/\log\log\Delta_1} < \Delta^{\kappa_3/\log\log\Delta}.$$

Here in the last step we used $e^e < \Delta_1 \leqslant \Delta$. But if $\Delta_1 < e^e$ then $s \leqslant 2$, and the required inequality is trivial. Lemma 1 implies the existence of a constant $\kappa_4 > 0$ such that

$$c(\Delta_2) < \Delta_2^{\kappa_4/\log\log\Delta_2} < \Delta^{\kappa_4/\log\log\Delta},$$

where again we used that $e^e < \Delta_2 \leqslant \Delta$. But if $\Delta_2 < e^e$ then $c(\Delta_2) \leqslant 3$, and the required inequality is again trivial. The result now follows with $\kappa = \kappa_3 + \kappa_4$.

An immediate consequence of Theorem 3 is the following.

COROLLARY. *If the Szpiro Conjecture 6 is true, then the Tamagawa number of any elliptic curve defined over $\mathbb{Q}$ satisfies*

$$c \ll N^{\varepsilon}.$$

Proof. From Theorem 3 and the Szpiro Conjecture 6 we clearly even have

$$c \ll N^{(6\kappa + \varepsilon)/(\log\log N)}.$$

5 Details of the proof of Theorems 1 and 2

In the proof below, treating Theorems 1 and 2 at the same time, the small positive number ε will change its precise meaning almost every other line and sometimes within one line, but this should not cause difficulties. We use notations as given in Section 2. Always N will be assumed to approach ∞.

Proof. Let A,B,C be coprime positive integers such that $A + B = C$ and $C > N(A, B, C)$. Such triples exist with arbitrarily large $N(A, B, C)$, by the results of [**26**]. Let E be the Frey-Hellegouarch curve (2). Then N is squarefree apart from a possible power of 2, which is at most 2^8. Thus certainly $C \gg N$, because $N(A, B, C)$ is the squarefree part of N.

For the quadratic twist E_q of E by q, defined by (4), we denote all the parameters by the subscript q. By Conjecture 7 (see [**13**] and [**10**]) there exists a $q < N^{\varepsilon}$, that we may take squarefree, such that E_q has rank $r_q = 0$ and $L_q(1) \gg 1$. Hence $R_q = 1$, and also of course $T_q \geqslant 1$. By the Birch-Swinnerton-Dyer formula (3), the Szpiro Conjecture 6 and the Corollary to Theorem 3 we thus have

$$|\text{III}_q| = \frac{T_q^2 L_q(1)}{c_q \Omega_q} \gg N_q^{-\varepsilon} \Omega_q^{-1}. \tag{7}$$

Notice that the transformation of variables $(x, y) := (qx, q^2 y)$ in equation (4) shows that E_q can also be described by the equation

$$y^2 = x(x - qA)(x + qB), \tag{8}$$

thus equation (2) with A,B multiplied by q. It now follows that apart from the power of 2, the conductor N_q of the twisted curve is lcm (N, q^2), and the difference in the power of 2 is at most 2^8. Hence

$$N_q \leqslant 2^8 N q^2 \ll N^{1+\varepsilon}. \tag{9}$$

It remains to estimate $\Omega_q = 2\omega_q$. We have for the Frey-Hellegouarch curve (2) $\omega = \omega_1$, with

$$\omega_1 = \int_{-B}^{0} \frac{\mathrm{d}x}{\sqrt{x(x-A)(x+B)}}$$

By equation (8) we now have

$$\omega_q = u \int_{-qB}^{0} \frac{\mathrm{d}x}{\sqrt{x(x-qA)(x+qB)}} = \frac{u}{\sqrt{q}}\,\omega_1 \leqslant u\omega_1,$$

where $u \in \mathbb{N}$ is the scaling factor that is introduced in turning the model (8) into a minimal one. We first estimate ω_1, and then u.

If $A > B$ then we put $\alpha = B/A$, and we have

$$\omega_1 = \frac{1}{\sqrt{A}} \int_{-\alpha}^{0} \frac{\mathrm{d}\xi}{\sqrt{\xi(\xi+\alpha)(\xi-1)}} < \frac{\pi\sqrt{2}}{\sqrt{C}} \ll N^{-\frac{1}{2}},$$

where we used the substitution $x = A\xi$, that $A > \frac{1}{2}C$, and that

$$2.622 < \int_{-\alpha}^{0} \frac{d\xi}{\sqrt{\xi(\xi+\alpha)(\xi-1)}} < \pi$$

for any $\alpha \in (0, 1)$.

If $A < B$ then we put $\alpha = A/B$, and we similarly have

$$\omega_1 = \frac{1}{\sqrt{B}} \int_{0}^{1} \frac{d\xi}{\sqrt{\xi(\xi+\alpha)(1-\xi)}} \ll \frac{1}{\sqrt{C}} \log C \ll N^{-1/2+\varepsilon},$$

because

$$\int_{0}^{1} \frac{\mathrm{d}\xi}{\sqrt{\xi(\xi+\alpha)(1-\xi)}} = \log\frac{1}{\alpha} + \mathrm{O}(1) \qquad \text{as} \quad \alpha \downarrow 0,$$

and $\dfrac{1}{\alpha} = \dfrac{B}{A} \leqslant B < C$.

So we obtain

$$\omega_1 \ll N^{-\frac{1}{2}+\varepsilon}. \tag{10}$$

To estimate the scaling factor u we study the algorithm for finding a minimal model of a curve, due to Tate. We use the version by Laska [**19**], as given by Cremona [**5**]. We denote the "c_6" and "Δ" of the models (4), (8) of the curves E, E_q by respectively $c_{6,1}$, $c_{6,q}$ and Δ_1, Δ_q. Then

$$\begin{aligned} c_{6,1} &= 32(A-B)(A+2B)(2A+B) \qquad & c_{6,q} &= q^3 c_{6,1}, \\ \Delta_1 &= 16A^2B^2(A+B)^2, & \Delta_q &= q^6\Delta_1. \end{aligned}$$

The odd primes p such that $p \nmid c_{6,q}$ or $p \nmid \Delta_q$ do not contribute to the scaling factor u. If p is an odd prime such that $p \mid c_{6,q}$ and $p \mid \Delta_q$, then the fact that A, B are coprime implies that $p \mid q$. But q is squarefree, so that $\mathrm{ord}_p(q) = 1$, and thus

$$\mathrm{ord}_p(c_{6,q}) = 3 + \mathrm{ord}_p(c_{6,1}), \qquad \mathrm{ord}_p(\Delta_q) = 6 + \mathrm{ord}_p(\Delta_1).$$

But, as noted above, if $p \mid \Delta_1$, then the coprimeness of A, B implies that $p \nmid c_{6,1}$. It follows that

$$\mathrm{ord}_p(\mathrm{gcd})c_{6,q}^2, \Delta_q)) \leqslant 6,$$

and by Laska's algorithm this means that p does not contribute to the scaling factor u. Finally we have to treat $p = 2$. Reasoning as above we see that if $4 \mid AB(A+B)$ then $\mathrm{ord}_2(c_{6,1}) = 6$, and by $4 \nmid q$ this means that

$$\mathrm{ord}_2(\mathrm{gcd}(c_{6,q}^2, \Delta_q)) \leqslant 6 + \mathrm{ord}_2(\mathrm{gcd}(c_{6,1}^2, \Delta_1)) \leqslant 18,$$

so that the contribution of the prime 2 to u is at most 2.

Our conclusion is that $u \leqslant 2$, and thus by (10) and (9) that

$$\Omega_q = 2\omega_q \leqslant 4\omega_1 \ll N^{-\frac{1}{2}+\varepsilon} \ll N_q^{-\frac{1}{2}+\varepsilon}.$$

With (7) this proves Theorem 1.

To prove Theorem 2, notice that if we allow q to be as large as N^2, then (5) guarantees that $L_q(1) \gg 1$, without assuming Conjecture 7. Similarly as above, using Theorem 3 (but not its corollary, so we also avoid Conjecture 6), we obtain

$$|\mathrm{III}_q| \gg \Delta_q^{-\varepsilon}\Omega_q^{-1} \gg \Delta_q^{-\varepsilon}\frac{\sqrt{C}}{\log C}.$$

By $N \ll \Delta$ we have $\Delta_q \leqslant q^6\Delta \ll N^{12}\Delta \ll \Delta^{13}$, and thus by $\Delta \leqslant (ABC)^2 < C^6$ we find

$$|\mathrm{III}_q| \gg \Delta^{\frac{1}{12}-\varepsilon},$$

as required. □

6 Examples

There are lists available of good examples of coprime $A, B, C \in \mathbb{N}$ such that $A + B = C$. Here, an example is called *good* if $\dfrac{\log C}{\log N(A, B, C)} > 1.4$, say. The first such list was published by the present author **[29]**, more recent ones in **[2]** and **[21]**. In July 1995 Browkin and Brzeziński distributed by e-mail an updated list with all known 115 examples of $\dfrac{\log C}{\log N(A, B, C)} > 1.4$.

Using software such as Cohen's Pari, Connell's Apecs and Cremona's Mwrank, we can try to compute (analytically) the value for the order of Ш for the curves in the isogeny classes of twists of the Frey-Hellegouarch curves (2) corresponding to these examples. We did so for a number of examples, with results as in the Table at the end of this paper. We found 11 curves with $|Ш| \gg \sqrt{N}$, which we list below. Here a_1, a_2, a_3, a_4, a_6 are the coefficients of a global minimal model $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. (*See Table opposite*).

Note that Cremona [**6**] also found several curves with $|Ш| > \sqrt{N}$, the best one being $y^2 + xy = x^3 - 3674496x - 2711401518$, coded $546F_2$, with $|Ш| = 49$, $N = 546$, hence $|Ш|/\sqrt{N} \approx 2.097$.

Further note that none of the curves in the table above are themselves Frey-Hellegouarch curves (2) or twists of Frey-Hellegouarch curves (4), although they are isogenous to such curves. The best example of a (twisted) Frey-Hellegouarch curve that we found comes from the best example of $A + B = C$, due to E. Reyssat, which is

$$A = 3^{10} \cdot 109, \qquad B = 2, \qquad C = 23^5,$$

with $N(A, B, C) = 15042$, so that $\dfrac{\log C}{\log N(A, B, C)} \approx 1.629911$. The corresponding Frey-Hellegouarch curve

$$y^2 = x(x - 6436341)(x + 2) = x^3 - 6436339x^2 - 12872682x$$

has rank zero, $N = 240672$, and $|Ш| = 361$, so $|Ш|/\sqrt{N} \approx 0.7358$.

In a Table at the end of this paper we present the results for some other isogeny classes of twists of Frey-Hellegouarch curves for good examples of $A + B = C$. The number refers to the list of Browkin and Brzeziński dated July 15, 1995, that was distributed via e-mail. We always take $A < B$, as the corresponding Frey-Hellegouarch curve with A and B interchanged is its twist by -1. Notice that all other permutations and sign changes of A, B, C lead to curves isomorphic to one of these two. For many examples of $A + B = C$ we considered for a few twisted Frey-Hellegouarch curves (4) the complete isogeny classes. The criteria for an isogeny class of curves to make the Table were:

- A, B, C appears in the list of Browkin and Brzeziński,
- $|q| \leqslant 3$,
- $N < 10^8$,
- the rank is zero,
- there is a curve in the class with $|Ш| > \max\{1, \sqrt{N}/100\}$,
- the computations could be done in a few minutes on a personal computer.

a_1	a_2	a_3	a_4 a_6	N	$\lvert III \rvert$	$\lvert III \rvert/\sqrt{N}$	$L(1)$	Ω	T	c
1	1	1	−16272564754316406252451 −798973042220714620227331980906826	51636585	50176	6.893	0.67070507	0.000013367049	2	4
0	0	0	−4358303498643228291 −3502065934280224627838744290	6758136	11664	4.487	1.2187586	0.00010448891	2	4
1	−1	0	−18833678425803718656 −31459429289115474813631365120	10270602	8464	2.641	0.30669834	0.000072471252	2	2
0	−1	0	−3002051866725984577 −2002045804153515476030738975	69736128	18496	2.215	4.2428035	0.00011469516	2	8
0	−1	0	−48032787133026543937 −128131170909298191596538712607	69736128	18496	2.215	4.2428035	0.000057347582	2	16
1	1	1	−1017035320827560464021 −12483953174541050415482339358682	51636585	12544	1.746	0.67070507	0.000026734099	2	8
1	−1	0	−128663470800000 −17763600445139557105664	334170	784	1.356	2.4998376	0.00079714209	2	16
0	−1	0	−33482094979206610944 −74570499055681125484163235840	2738872	6084	1.163	2.2910621	0.000062761946	2	24
0	0	0	−272393982224918931 −54719774502855128687059954	6758136	2916	1.122	1.2187586	0.00020897781	2	8
1	0	0	−119300 −16229850	210	16	1.104	2.0518660	0.12824163	2	4
1	0	0	−1920800 −1024800150	210	16	1.104	2.0518660	0.12824163	2	4

One effect of these criteria is that the asymptotics cannot be properly illustrated, as for physical reasons we cannot do computations for very large conductor. Another effect is that we seem to have biased for small Tamagawa numbers. We found a number of curves with a large Tamagawa number, causing a small $|\text{III}|$, that thus did not make the Table. Indeed, we feel that for rank zero curves with small conductor, say $N < 10^{12}$ or so, the Tamagawa number might be the main factor determining $|\text{III}|$. Finally, we omitted the isogeny classes we found with all curves having $|\text{III}| = 1$ and $N < 10^4$, although they do have $|\text{III}| > \sqrt{N}/1000$. Notice that *all* the curves in Cremona's tables [**5**] satisfy $|\text{III}| > \sqrt{N}/100$.

For each curve we tried to compute the conductor N, the rank r, the order of the Tate-Shafarevich group III, the period $\Omega = 2\omega$, the value $L(1)$, the order T of the torsion group, and the Tamagawa number c. We give these numbers for the twisted Frey-Hellegouarch curve (4), and for the curve in the isogeny class with maximal $|\text{III}|$. If there are more curves in the isogeny class having maximal $|\text{III}|$ then we give data for the curve with minimal Tamagawa number. In no case do we claim to have proved that the entries for $|\text{III}|$ in our Table are correct, only that they are probably true under the Birch-Swinnerton-Dyer Conjecture (but notice that our numerical results do not depend on other conjectures than the Birch-Swinnerton-Dyer Conjecture in the rank zero case). All our results are numerical in the sense that they have been obtained by analytic techniques using approximations of L-series.

Note that isogenous curves do have the same L-series, but may have different torsion groups, periods, Tamagawa numbers and III's. This phenomenon had been noted before, and is not rare at all (see e.g. Cremona [**6**]), as it seems to be in the more or less comparable situation of non-isomorphic number fields with the same zeta-functions but with different class groups, of which the first examples were found only recently, cf. [**25**].

Finally we note that, although usually in an isogeny class there is only one curve of the form (2), there are a few cases in which there are two isogenous Frey-Hellegouarch curves of this form, thus linking two examples of $A + B = C$ that at first sight seem to be unrelated. A curve defined by an equation of type (2) has all its 2-torsion rational, and conversely, any curve with only rational 2-torsion is defined by an equation (2) (with A, B not necessarily coprime), hence is a (twisted) Frey-Hellegouarch curve of some example of $A + B = C$. Kubert [**17**] has parametrized occurrences of isogenous pairs with rational 2-torsion. Studying these parametrizations revealed the following results for isogenies of degree 2 and 3. We give the results in terms of examples for $A + B = C$. A pair $A + B = C$, $A' + B' = C'$ with isogenous Frey-Hellegouarch curves can be called an *isogenous pair* of examples of $A + B = C$.

Isogenies of degree 2 correspond to

$$A = x^2, \qquad B = (y-x)(y+x), \qquad C = y^2,$$

with coprime $x, y \in \mathbb{N}$. Then the isogenous example is

$$A' = \left(\frac{y-x}{d}\right)^2, \qquad B' = \frac{4xy}{d^2}, \qquad C' = \left(\frac{y+x}{d}\right)^2,$$

with $d = 2$ if both x and y are odd, and $d = 1$ otherwise. In the list of Browkin and Brzeziński this happens at the numbers 20, 26, 46, 76, 86 and 87 (maybe with A and B interchanged). The numbers 86 and 87 are isogenous, and the $A' + B' = C'$ for the other examples have $\dfrac{\log C'}{\log N(A', B', C')} < 1.4$, so do not appear in their list. The number 26 is a special example, because here also B' happens to be square. So interchanging A' and B' yields a third isogenous example.

Isogenies of degree 3 correspond to

$$A = x\left(\frac{x-2y}{d}\right)^3, \qquad B = y\left(\frac{2x-y}{d}\right)^3, \qquad C = (x-y)\left(\frac{x+y}{d}\right)^3,$$

with coprime $x, y \in \mathbb{N}$, and $d = 3$ if $3 \mid x+y$, and $d = 1$ otherwise. Then the isogenous example is

$$A' = x^3 \frac{x-2y}{d}, \qquad B' = y^3 \frac{2x-y}{d}, \qquad C' = (x-y)^3 \frac{x+y}{d}.$$

In the list of Browkin and Brzeziński this happens at number 31. The isogenous example $A' + B' = C'$ has $\dfrac{\log C'}{\log N(A', B', C')} < 1.4$, so does not appear in their list.

In the following table we present the isogenous paris of examples for $A + B = C$ that we found. Notice that by definition $N(A, B, C) = N(A', B', C')$, and that if $\dfrac{\log C}{\log N(A, B, C)}$ is large, then so is $\dfrac{\log C'}{\log N(A, B, C)}$.

no.	A	B	C	$\frac{\log C}{\log N(A,B,C)}$	A'	B'	C'	$\frac{\log C'}{\log N(A',B',C')}$	deg
20	7^2	$2^{10} \cdot 11 \cdot 53^2$	$3^4 \cdot 5^8$	1.4741	53^4	$3^2 \cdot 5^4 \cdot 7$	$2^{16} \cdot 11^2$	1.3560	2
26	1	$2^5 \cdot 3 \cdot 5^2$	7^4	1.4557	$2^6 \cdot 3^2$	7^2	5^4	1.2039	2
	7^2	$2^6 \cdot 3^2$	5^4	1.2039	3^4	$5^2 \cdot 7$	2^8	1.0370	2
31	$3^5 \cdot 7^3$	$2^{13} \cdot 23^3 \cdot 59$	$5^3 \cdot 19^6$	1.4509	$3^{15} \cdot 7$	$2^7 \cdot 23 \cdot 59^3$	$5^9 \cdot 19^2$	1.3140	3
46	1	$2^4 \cdot 367 \cdot 547$	$5^8 \cdot 7^2$	1.4391	3^{14}	$5^4 \cdot 7$	$2^6 \cdot 547^2$	1.3201	2
76	7^2	$2^{17} \cdot 181^2$	$3^8 \cdot 809^2$	1.4189	181^4	$3^4 \cdot 7 \cdot 809$	2^{30}	1.3302	2
86	3^{14}	$2^6 \cdot 5 \cdot 137$.	13^6	1.4137	5^2	$3^7 \cdot 13^3$	$2^8 \cdot 137^2$	1.4133	2
87	5^2	$3^7 \cdot 13^3$	$2^8 \cdot 137^2$	1.4133	3^{14}	$2^6 \cdot 5 \cdot 137$	13^6	1.4137	2

7 The Table

no.	A	B	q	N	$\lvert\mathrm{III}\rvert$	$\lvert\mathrm{III}\rvert/\sqrt{N}$	$L(1)$	Ω	T	c
1	2	$3^{10}\cdot 109$	-1	240672	361	0.7359	0.8941	0.002477	4	16
				isog.:	361, 361, 361	0.7359	0.8941	0.0002477	2	4
2	11^2	$3^2\cdot 5^6\cdot 7^3$	1	53130	1	0.004338	3.682	0.009024	4	6528
				isog.:	1, 1, 4	0.01735	3.682	0.009024	2	408
			-1	425040	9	0.01380	4.690	0.0009047	4	9216
				isog.:	9, 36, 36	0.05522	4.690	0.0009047	2	576
			2	1700160	25	0.01917	2.552	0.003191	4	512
				isog.:	25, 25, 25	0.01917	2.552	0.003191	2	128
4	283	$5^{11}\cdot 13^2$	-3	45030960	49	0.007302	2.066	0.00003993	4	16896
				isog.:	49, 49, 196	0.02921	2.066	0.000001997	2	2112
5	1	$2\cdot 3^7$	1	3360	1	0.01725	1.349	0.3373	4	64
				isog.:	1, 1, 4	0.06901	1.349	0.3373	2	4
			-1	3360	1	0.01725	2.660	0.09500	4	448
				isog.:	1, 1, 4	0.06901	2.660	0.04750	2	56
			-2	6720	9	0.1098	1.209	0.06717	4	32
				isog.:	9, 9, 36	0.4392	1.209	0.3359	2	9
6	7^3	3^{10}	1	9744	4	0.4052	1.563	0.06512	4	96
				isog.:	1, 4, 16	0.1621	1.563	0.03256	2	12
			-1	1218	1	0.02865	3.615	0.05164	4	1120
				isog.:	1, 1, 4	0.1146	3.615	0.02582	2	140
			3	3654	1	0.01654	0.1504	0.07520	4	32
				isog.:	1, 1, 4	0.06617	0.1504	0.03760	2	4
			-3	29232	9	0.05264	1.610	0.01491	4	192
				isog.:	9, 9, 9	0.05264	1.610	0.01491	2	48
9	$13\cdot 19^6$	$2^{30}\cdot 5$	1	20214480	16	0.003559	2.652	0.0001328	4	19968
				isog.:	16, 64, 64	0.01423	2.652	0.00006640	2	2496
			-3	60643440	529	0.06793	9.788	0.00004818	4	6144
				isog.:	529, 2116, 2116	0.2717	9.788	0.00002409	2	768

11	239	$5 \cdot 17^3$	−1	1503310	49	0.03996	4.048	0.0002869	4	4608
				isog.:	49, 49, 196	0.1599	4.048	0.0001434	2	576
16	11^2	$3^9 \cdot 13$	1	4290	1	0.01527	3.463	0.08246	4	672
				isog.:	1, 1, 4	0.06107	3.463	0.08246	2	42
			−1	34320	1	0.005398	2.683	0.01242	4	3456
				isog.:	1, 1, 4	0.02159	2.683	0.006210	2	432
			−2	137280	25	0.06747	0.8782	0.008782	4	64
				isog.:	25, 25, 100	0.2699	0.8782	0.004391	2	8
			−3	12870	16	0.1410	1.836	0.01434	4	128
				isog.:	16, 16, 64	0.5641	1.836	0.007171	2	16
17	37	2^{15}	2	35520	25	0.1326	3.733	0.07466	4	32
				isog.:	25, 25, 25	0.1326	3.733	0.07466	2	8
			−3	26640	49	0.3002	3.927	0.02003	4	64
				isog.:	49, 49, 49	0.3002	3.927	0.04007	2	8
19	1	$3^{16} \cdot 7$	−1	4505424	9	0.004240	1.251	0.0003620	4	6144
				isog.:	9, 36, 144	0.06784	1.251	0.0001810	2	192
			−2	18021696	100	0.02356	0.2048	0.0002559	4	128
				isog.:	25, 100, 1600	0.3769	0.2048	0.0001279	2	4
			−3	6758136	729	0.2804	1.219	0.0002090	4	128
				isog.:	729, 2916, 11664	4.487	1.219	0.0001045	2	4
20	7^2	$2^{10} \cdot 11 \cdot 53^2$	1	979440	4	0.004042	5.880	0.005742	8	16384
				isog.:	4, 4, 16, 16, 16	0.01617	5.880	0.005742	2	256
			2	3917760	36	0.01819	2.339	0.004061	4	256
				isog.:	9, 9, 36, 144, 144	0.07275	2.339	0.002030	2	32
			−2	3917760	25	0.01263	0.6319	0.0007898	4	512
				isog.:	25, 25, 25, 25, 100	0.05052	0.6319	0.0003949	2	64
			3	367290	49	0.08085	2.599	0.006631	4	128
				isog.:	49, 49, 49, 49, 49	0.08085	2.599	0.006631	2	32
23	$2^7 \cdot 5^2$	$7^6 \cdot 41$	1	37310	16	0.08283	3.528	0.01838	4	192
				isog.:	4, 16, 64	0.3313	3.528	0.009188	2	24
			3	335790	25	0.1725	0.6606	0.003303	4	128
				isog.:	25, 25, 100	0.1725	0.6606	0.001651	2	16

7 The Table—(continued)

no.	A	B	q	N	$\|III\|$	$\|III\|/\sqrt{N}$	$L(1)$	Ω	T	c
26	1	$2^5 \cdot 3 \cdot 5^2$	1	1680	1	0.02440	1.724	0.4309	8	256
				isog.:	1, 1, 1, 1, 1, 4, 4	0.09759	1.724	0.4309	2	8
			−1	210	4	0.2760	2.052	0.2565	4	32
				isog.:	1, 1, 1, 1, 1, 16. 16	1.104	2.052	0.1282	2	4
			2	6720	1	0.01220	2.438	0.3047	4	128
				isog.:	1, 1, 1, 1, 1, 1, 4	0.04880	2.438	0.1523	2	16
			−3	5040	1	0.01409	1.185	0.07404	4	256
				isog.:	1, 1, 1, 1, 1, 1, 4	0.05634	1.185	0.07404	2	16
29	$2^{19} \cdot 13 \cdot 103$	7^{11}	1	24744720	196	0.03940	1.035	0.0001650	4	512
				isog.:	196, 784, 3136	0.6304	1.035	0.00008251	2	16
30	$3^5 \cdot 7$	$5^6 \cdot 67$	1	14070	1	0.008430	2.156	0.03594	4	960
				isog.:	1, 1, 4	0.03372	2.156	0.03594	2	60
			−1	112560	16	0.04769	2.357	0.006138	4	384
				isog.:	16, 64, 64	0.1908	2.357	0.006138	2	24
			3	337680	25	0.04302	2.075	0.01037	4	128
				isog.:	25, 25, 25	0.04302	2.075	0.01037	2	32
31	$3^5 \cdot 7^3$	$2^{13} \cdot 23^3 \cdot 59$	3	16243290	9	0.002233	3.264	0.004197	12	124416
				isog.:	9, 36, 36, 81, 81, 324, 324	0.08039	3.264	0.0004197	2	96
32	1	$3^3 \cdot 5^3 \cdot 7^7 \cdot 23$	1	28318290	1	0.0001879	0.7559	0.0004375	4	27648
				isog.:	1, 4, 64	0.01203	0.7559	0.0004375	2	108
33	1	$3 \cdot 5^2 \cdot 47^2$	1	11390	1	0.0002996	2.414	0.01724	4	2240
				isog.:	1, 1, 4	0.01198	2.414	0.01724	2	140
			−3	334170	196	0.3391	2.500	0.001594	4	128
				isog.:	49, 196, 784	1.356	2.500	0.0007971	2	16

35	89	$7 \cdot 11^8$	1	2179254	16	0.01084	2.053	0.002005	4	1024
				isog.:	4, 64, 64	0.04335	2.053	0.002005	2	64
			2	69736128	81	0.009700	11.02	0.0007087	4	3072
				isog.:	81, 81, 324	0.03880	11.02	0.0007087	2	192
			−2	69736128	4624	0.5537	4.243	0.0001147	4	128
				isog.:	4624, 18496, 18496	2.215	4.243	0.00005735	2	16
			3	52302096	49	0.006775	0.4537	0.0005787	4	256
				isog.:	49, 49, 196	0.02710	0.4537	0.0002893	2	32
36	$3^2 \cdot 5^7 \cdot 79$	$2^{29} \cdot 13$	−1	51514320	25	0.003483	5.885	0.00007506	4	50176
				isog.:	25, 100, 100	0.01393	5.885	0.0001501	2	1568
37	$2 \cdot 13^2$	5^8	−1	118560	25	0.07261	4.020	0.01005	4	256
				isog.:	25, 25, 100	0.2904	4.020	0.01005	2	16
			−3	355680	9	0.01509	3.342	0.005803	4	1024
				isog.:	9, 9, 36	0.06036	3.342	0.002901	2	128
40	1	$2^{12} \cdot 5^3$	1	72240	1	0.003721	5.339	0.04449	4	1920
				isog.:	1, 1, 4	0.01488	5.339	0.04449	2	120
41	$3^2 \cdot 19^3$	5^{11}	2	6803520	121	0.04639	1.850	0.001911	4	128
				isog.:	121, 121, 484	0.1856	1.850	0.0009556	2	16
			−3	5102640	529	0.2342	6.589	0.0005190	4	384
				isog.:	529, 529, 2116	0.9367	6.589	0.0005190	2	24
44	$3^4 \cdot 23^2$	31^5	1	149730	1	0.002584	7.322	0.006933	4	16896
				isog.:	1, 1, 16	0.04135	7.322	0.003466	2	528
			−1	1197840	4	0.003655	0.5634	0.001174	4	1920
				isog.;	1, 16, 16	0.01462	0.5634	0.0005869	2	240
46	1	$2^4 \cdot 3^7 \cdot 547$	1	918960	9	0.009388	1.286	0.008933	8	1024
				isog.:	9, 9, 9, 36, 36	0.03755	1.286	0.004466	2	32
			−1	57435	9	0.03755	1.448	0.002872	4	896
				isog.:	9, 9, 9, 9, 36	0.1502	1.448	0.001436	2	112
			−3	2756880	9	0.005420	0.1194	0.0008292	4	256
				isog.:	9, 9, 9, 9, 36	0.02168	0.1194	0.0004146	2	32
47	1	$19 \cdot 509^3$	−1	27388272	1521	0.2906	2.291	0.0001255	4	192
				isog.:	1521, 1521, 6084	1.163	2.291	0.00006276	2	24
			−3	10270602	529	0.1651	0.3067	0.0001449	4	64
				isog.:	529, 529, 8464	2.641	0.3067	0.00007247	2	2

7 The Table—(continued)

no.	A	B	q	N	$\lvert III \rvert$	$\lvert III \rvert / \sqrt{N}$	$L(1)$	Ω	T	c
49	$2^{10} \cdot 7$	5^7	1	2730	1	0.01914	1.166	0.07287	4	256
				isog.:	1, 1, 4	0.07655	1.166	0.03643	2	32
			−3	8190	1	0.01105	4.266	0.02539	4	2688
				isog.:	1, 1, 4	0.04420	4.266	0.01270	2	3368
53	31^2	$3^5 \cdot 5^9$	−1	9069360	9	0.002989	1.869	0.0002884	4	11520
				isog.:	9, 9, 36	0.01195	1.869	0.0001442	2	1440
			−3	3401010	289	0.1567	0.7700	0.0003330	4	128
				isog.:	289, 289, 1156	0.6268	0.7700	0.0001665	2	16
60	$3^9 \cdot 29$	$7^6 \cdot 43^2$	1	5446896	25	0.01071	12.76	0.001181	4	6912
				isog.:	25, 25, 100	0.04285	12.76	0.0005906	2	864
			−2	21785854	25	0.005356	0.5419	0.0003010	4	1152
				isog.:	25, 25, 100	0.02142	0.5419	0.0003010	2	72
			3	2042586	64	0.04478	1.397	0.001364	4	256
				isog.:	64, 64, 64	0.04478	1.397	0.001364	2	64
62	73^2	$2^{11} \cdot 11^4 \cdot 13^3$	−1	37267230	25	0.004095	8.225	0.00004896	4	107520
				isog.:	25, 25, 1600	0.2621	8.225	0.00002448	2	840
63	11	$7^3 \cdot 167^2$	3	3703392	25	0.01299	1.842	0.006141	4	192
				isog.:	25, 25, 25	0.01299	1.842	0.006141	2	48
			−3	3703392	196	0.1018	1.839	0.001173	4	128
				isog.:	49, 784, 784	0.4074	1.839	0.0005864	2	16
66	3^{10}	$7^8 \cdot 23$	−2	15734208	100	0.02521	1.235	0.0003858	4	512
				isog.:	25, 100, 400	0.1008	1.235	0.0001929	2	64
69	$5^2 \cdot 11$	$13^3 \cdot 1483^2$	3	19086210	25	0.005722	6.463	0.0006463	4	6400
				isog.:	25, 25, 100	0.02289	6.463	0.0003232	2	800

70	$2^4 \cdot 59$	$5^{12} \cdot 19$	−1	3144905	25	0.01410	3.321	0.0001845	4	11520
				isog.:	25, 25, 100	0.05639	3.321	0.0001845	2	720
			3	9433215	121	0.03940	1.193	0.0006165	4	256
				isog.:	121, 121, 484	0.1576	1.193	0.0003082	2	32
71	5^7	$11^5 \cdot 13^2$	−2	5445440	36	0.01543	0.9803	0.0008510	4	512
				isog.:	36, 36, 576	0.2468	0.9803	0.0004255	2	16
73	$7^8 \cdot 19$	$2^{15} \cdot 5^2 \cdot 37^2$	3	60233040	841	0.1084	4.664	0.0001733	4	512
				isog.:	841, 841, 841	0.1084	4.664	0.0001733	2	128
			−3	7529130	25	0.009111	7.449	0.0002116	4	22528
				isog.:	25, 25, 100	0.03644	7.449	0.0001058	2	2816
74	23^3	$3^9 \cdot 5^7 \cdot 31$	−1	33090330	289	0.05024	2.395	0.00005756	4	2304
				isog.:	289, 1156, 4624	0.8038	2.395	0.00002878	2	72
76	7^2	$2^{17} \cdot 181^2$	1	49200144	225	0.03208	9.256	0.0006428	8	4096
				isog.:	225, 225, 225, 900, 900	0.1283	9.256	0.0006428	2	64
			−1	6150018	121	0.04879	2.413	0.0001918	4	1664
				isog.:	121, 121, 121, 121, 484	0.1952	2.413	0.00009588	2	208
82	7^3	$5^{13} \cdot 181$	−1	51636585	3136	0.4364	0.6707	0.00002673	4	128
				isog.:	3136, 12544, 50176	6.893	0.6707	0.00001337	2	4
84	$3^{11} \cdot 5^4$	$7 \cdot 11^6 \cdot 43$	1	13508880	25	0.006802	6.454	0.0003667	4	11264
				isog.:	25, 25, 100	0.02721	6.454	0.0003667	2	704
			2	54035520	25	0.003401	0.6223	0.0002593	4	1536
				isog.:	25, 100, 100	0.01360	0.6223	0.0002593	2	96
86	$2^6 \cdot 5 \cdot 137$	3^{14}	−1	427440	16	0.02497	3.852	0.002866	8	5376
				isog.:	4, 4, 16, 16, 64	0.09789	3.852	0.001433	4	672
			3	1282320	9	0.007948	1.700	0.003935	4	768
				isog.:	9, 9, 9, 36, 36	0.03179	1.700	0.001967	2	96
87	5^2	$3^7 \cdot 13^3$	−1	427440	4	0.006118	3.852	0.002866	4	5376
				isog.:	4, 16, 16, 16, 64	0.09789	3.852	0.001433	4	672
			3	1282320	9	0.007948	1.700	0.007869	4	384
				isog.:	9, 9, 9, 36, 36	0.03179	1.700	0.001967	2	96
89	5	3^{11}	−1	41520	25	0.1227	0.7464	0.01493	4	32
				isog.:	25, 25, 100	0.4908	0.7464	0.007464	2	4

7 The Table—(continued)

no.	A	B	q	N	$\lvert \text{III} \rvert$	$\lvert \text{III} \rvert / \sqrt{N}$	$L(1)$	Ω	T	c
90	79^3	$3^6 \cdot 7 \cdot 11 \cdot 13^5$	-1	20402382	4	0.0008856	3.510	0.00008704	4	161280
				isog.:	1, 16, 64	0.01417	3.510	0.00004352	2	5040
			3	61207146	100	0.01278	5.154	0.0002147	4	3840
				isog.:	25, 400, 400	0.05113	5.154	0.0002147	2	240
100	7^9	$3^2 \cdot 5^7 \cdot 13^3$	-1	3475290	49	0.02628	2.989	0.0003177	4	3072
				isog.:	49, 49, 784	0.4206	2.989	0.0001588	2	96
			3	10425870	25	0.007743	1.051	0.0003754	4	1792
				isog.:	25, 25, 100	0.03097	1.051	0.0003754	2	112
			-3	83406960	9	0.0009855	3.328	0.00009170	4	64512
				isog.:	9, 9, 144	0.01577	3.328	0.00004585	2	2016
102	$2^{16} \cdot 41 \cdot 71$	$3^{15} \cdot 7^2$	-1	2322978	81	0.05315	2.167	0.0004459	4	960
				isog.;	81, 81, 324	0.2126	2.167	0.0002230	2	120
			-3	55751472	361	0.04835	10.41	0.0001287	4	3584
				isog.:	361, 361, 5776	0.7736	10.41	0.00006436	4	448
104	$5 \cdot 7^2$	$13^2 \cdot 43^3$	3	2817360	49	0.02919	3.380	0.004311	4	256
				isog.:	49, 49, 49	0.02919	3.380	0.004311	2	64
105	13^3	$2^9 \cdot 37^2$	-3	346320	9	0.01529	2.182	0.004330	4	896
				isog.:	9, 9, 9	0.01529	2.182	0.008659	2	112
108	1	$3^9 \cdot 7^2 \cdot 197$	-1	6288240	9	0.003589	4.135	0.00045538	4	16128
				isog.:	9, 9, 144	0.05742	4.135	0.0002279	2	504
			-2	25152960	49	0.009770	0.2527	0.0003223	4	256
				isog.;	49, 49, 784	0.1583	0.2527	0.0001612	2	8
			3	18864720	49	0.01128	2.868	0.001829	4	512
				isog.:	49, 49, 784	0.1805	2.868	0.001829	2	8

REFERENCES

1. R. Bölling, 'Die Ordnung der Schafarewitsch–Tate Gruppe kann beliebig gross werden', *Math. Nachr.* **67** (1975), 157–179.

2. J. Browkin and J. Brzeziński, 'Some remarks on the *abc*-conjecture', *Math. Comp.* **62** (1994), 931–939.

3. A. Brumer and O. McGuinness, 'The behaviour of the Mordell–Weil group of elliptic curves', *Bull. Am. Math. Soc.* **23** (1990), 375–382.

4. J. W. S. Cassels, 'Arithmetic on curves of genus 1 (VI). The Tate–Safarevic group can be arbitrarily large', *J. reine angew. Math.* **214/215** (1964), 65–70.

5. J. E. Cremona, *Algorithms for Modular Elliptic Curves,* Cambridge University Press, Cambridge (1992).

6. J. E. Cremona, 'The analytic order of III for modular elliptic curves', *J. Th. Nombres Bordeaux* **5** (1993), 179–184.

7. F. Diamond, 'On deformation rings and Hecke rings', *Ann. Math.* (2) **144** (1996), 137–166.

8. D. Goldfeld, 'Modular elliptic curves and diophantine problems', in: R. A. Mollin (ed.), *Number Theory,* Proceedings C. N. T. A. Banff 1988, (1990), pp. 157–176.

9. D. Goldfeld and D. Lieman, 'Effective bounds on the size of the Tate–Shafarevich group', *Math. Res. Lett.* **3** (1996), 309–318.

10. D. Goldfeld and L. Szpiro, 'Bounds for the order of the Tate–Shafarevich group', *Comp. Math.* **97** (1995), 71–87.

11. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 5th edn, Oxford University Press, Oxford (1979).

12. A. W. Knapp, *Elliptic Curves,* Mathematical Notes Vol. 40, Princeton University Press, Princeton (1992).

13. W. Kohnen and D. B. Zagier, 'Values of L-series of modular forms at the centre of the critical strip', *Invent. Math.* **64** (1981), 175–198.

14. V. A. Kolyvagin, 'Finiteness of $E(\mathbb{Q})$ and $\text{III}(E, \mathbb{Q})$ for a subclass of Weil curves', *Math. USSR Izvestiya* **32** (1989), 523–541.

15. V. A. Kolyvagin, 'On the Mordell–Weil and Shafarevich–Tate groups for Weil elliptic curves', *Math. USSR Izvestiya* **33** (1989), 473–499.

16. K. Kramer, 'A family of semistable elliptic curves with large Tate–Shafarevich groups', *Proc. Am. Math. Soc.* **89** (1983), 379–386.

17. D. S. Kubert, 'Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (Third Series)* **33** (1976), 193–237.

18. S. Lang, 'Conjectured diophantine estimates on elliptic curves', in: *Arithmetic and Geometry Vol. I,* Progr. Math. Vol. 35, Birkhäuser, Boston, MA (1983), pp. 155–171.

19. M. Laska, 'An algorithm for finding a minimal Weierstrass equation for an elliptic curve', *Math. Comp.* **38** (1982), 257–260.

20. L. Mai and M. R. Murty, 'A note on quadratic twists of an elliptic curve', in: *Elliptic Curves and Related Topics,* CRM Proceedings and Lecture Notes Vol. 4, AMS (1994), pp. 121–124.

21. A. Nitaj, 'An algorithm for finding good *abc*-examples', *C. R. Acad. Sci. Paris Sér. I. Math.* **317** (1993), 811–815.

22. J. Oesterlé, 'Nouvelles approches du "Théorème" de Fermat', *Sém. Bourbaki,* Vol. 1987-1988, Exp. 694 (1988).

23. J. H. Silverman, *The Arithmetic of Elliptic Curves,* Springer Verlag, New York (1986).

24. J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* Springer Verlag, New York (1994).

25. B. de Smit and R. Perlis, 'Zeta functions do not determine class numbers', *Bull. Am. Math. Soc. (New Series)* **31** (1994), 213–215.

26. C. L. Stewart and R. Tijdeman, 'On the Oesterlé-Masser conjecture', *Monatsh. Math.* **102** (1986), 251–257.

27. J. Tate, 'Algorithm for determining the type of a singular fibre in an elliptic pencil', in: *Modular Functions of One Variable IV,* Lecture Notes in Math. **476**, B. J. Birch and W. Kuyk (eds), Springer Verlag, Berlin (1975), pp. 33–52.

28. P. Vojta, *Diophantine Approximations and Value Distribution Theory,* Lecture Notes in Math. **1239**, Springer Verlag, Berlin (1987).

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

30. A. Wiles, 'Modular elliptic curves and Fermat's last theorem', *Ann. Math.* (2) **141** (1995), 443–551.

Mathematical Institute
University of Leiden
and
Econometric Institute
Erasmus University Rotterdam
PO Box 1738
3000 *DR Rotterdam, The Netherlands*
E-Mail: *deweger@few.eur.nl*