COLLOQUIUM MATHEMATICUM

VOL. 128 2012 NO. 1

CUBIC FORMS, POWERS OF PRIMES AND THE KRAUS METHOD

BY

ANDRZEJ DĄBROWSKI, TOMASZ JĘDRZEJAK and
KAROLINA KRAWCIÓW (Szczecin)

Abstract. We consider the Diophantine equation $(x+y)(x^2+Bxy+y^2)=Dz^p$, where B, D are integers ($B\neq\pm 2$, $D\neq 0$) and p is a prime >5. We give Kraus type criteria of nonsolvability for this equation (explicitly, for many B and D) in terms of Galois representations and modular forms. We apply these criteria to numerous equations (with $B=0,1,3,4,5,6$, specific D's, and $p\in(10,10^6)$). In the last section we discuss reductions of the above Diophantine equations to those of signature $(p,p,2)$.

1. Introduction. Fix nonzero integers A, B, and C. For given positive integers p, q, r satisfying $1/p+1/q+1/r<1$, the generalized Fermat equation

$$Ax^p+By^q=Cz^r \tag{1.1}$$

has only finitely many primitive integer solutions [10]. Modern techniques coming from Galois representations and modular forms (methods of Frey–Hellegouarch curves and variants of Ribet's level-lowering theorem [12], [17], [18], and of course, the modularity of elliptic curves over the rationals proved by Wiles et al. [20], [5]) allow one to give partial (sometimes complete) results concerning the set of solutions to (1.1), at least when (p,q,r) is of the type (p,p,p), $(p,p,2)$, $(p,p,3)$, $(4,4,p)$, $(3,3,p)$, $(5,5,p)$ or $(2,4,p)$. For the first four signatures, the results are mostly of the type: *no primitive integer solution in x, y, z if p is larger than some positive constant depending on A, B, and C* (see, for instance, [20], [14], [13], [11], [1], [9], [2], [8]).

Many classical equations are, however, still out of reach. Consider, for example, the Diophantine equation

$$x^3+y^3=z^p,\qquad p \text{ an odd prime.} \tag{1.2}$$

It is expected (and follows from a weak effective *abc* conjecture, see Remark 3.8) that there are no primitive solutions for any odd prime p. Kraus [15] used the modular approach to show that the above equation has no primitive solutions for $17\le p\le 10^4$. He introduced a very interesting criterion ([15, Théorème 3.1]) that often allows one to prove that (1.2) has no primitive

2010 *Mathematics Subject Classification*: 11D41, 11F80, 11G05.
Key words and phrases: Diophantine equations, modular forms, elliptic curves, Galois representations.

DOI: 10.4064/cm128-1-5

© Instytut Matematyczny PAN, 2012

solution for fixed p, and verified his criterion for primes in the above range. This range is easily extendable. Recently Chen and Siksek [7] have checked the criterion for primes $p \leq 10^9$; they have also shown that the set of exponents p for which (1.2) has primitive solutions, has density 0. They actually refine Kraus' criterion by using a combination of the modular approach together with an obstruction to solutions that is of the Brauer–Manin type. Such a refinement of Kraus' criterion is much faster in practice for large primes p.

Of course, we can replace the left hand side of (1.2) by a more general cubic form with integer coefficients, and try to find a variant of Kraus' method here. In this paper we present such a method for Diophantine equations of the shape

$$(x+y)(x^2+Bxy+y^2) = Dz^p. \tag{1.3}$$

Note that the case $B=-1$, $D=1$ reduces to the equation investigated by Kraus. Billerey [3] proved that (1.3) has no primitive solutions (x,y,z) with $z \neq \pm 1$ for $B=0$ and $D \in \{2,6,10,22\}$.

The results presented in Section 2 concern equation (1.3) with $B \in \{0,1,3,4,5,6\}$. For specific choices of B and D, and for primes p greater than an explicit positive constant $C_{B,D}$, we can prove that (1.3) has no primitive solutions (x,y,z) with $z \neq \pm 1$ (see, for instance, Theorems 2.4 and 2.5). Our main purpose is, however, to generalize Kraus' criterion to equations (1.3) with $B = 0,1,3,4,5$ or 6, and (more or less) arbitrary D. For each B as above, and specific values of D, we use these criteria to check, using Magma [4], nonsolubility of (1.3) for primes $7 \leq p < 10^6$.

We give detailed proofs of all stated results in the case $B=1$ (see Subsections 2.2 and 2.3). In Subsection 2.4 we state, without further explanations, results of our investigations for $B=0,3,4,5,6$.

In Section 3, we consider a special case of (1.3) with $B = q^n+2$ and $D=1$, where q is a prime. In this case, the solubility questions can be reduced to studying several Diophantine equations of signature $(p,p,2)$. We will also show, under the conjectures of Ivorra and Kraus [13], that (1.3) has no primitive solutions for infinitely many B (and $D=1$) and for all but finitely many primes p. Of course, such a statement also follows from Conjecture (A) in [3], and from the famous *abc* conjecture.

The calculations in Magma were carried out by the second and third authors. The corresponding algorithms were prepared by the third author; details of computations and further information are available on request.

2. Kraus type criteria. Let $p \geq 7$ be a prime, and let $B \neq \pm 2$ and $D \neq 0$ be integers. Suppose that there exist nonzero integers a, b, and c such that $(a+b)(a^2+Bab+b^2) = Dc^p$. We will call the triple (a,b,c) a *primitive* *solution* of equation (1.3) if $\gcd(a,b) = 1$ (equivalently, $\gcd(a,b,Dc) = 1$). Let us describe possible commmon divisors of $a+b$ and $a^2+Bab+b^2$ in this case.

LEMMA 2.1. *For nonzero coprime integers a and b, we have*

$$\gcd(a+b, a^2+Bab+b^2) \mid B-2.$$

Proof. Let $d := \gcd(a+b, a^2+Bab+b^2)$. Then $d \mid a^2+Bab+b^2-(a+b)^2 = ab(B-2)$. By assumption $\gcd(d,ab) = 1$, hence the assertion follows. ∎

If (a,b,c) is a primitive solution of equation (1.3), then there exist integers D_1, D_2, c_1, c_2 such that $D = D_1D_2$, $\gcd(c_1,c_2) = 1$, and

$$\begin{cases} a+b = D_1c_1^p, \\ a^2+Bab+b^2 = D_2c_2^p. \end{cases} \tag{2.1}$$

One easily verifies the equality

$$(B+2)D_1^2c_1^{2p} - 4D_2c_2^p = (B-2)(a-b)^2, \tag{2.2}$$

hence $(c_1^2, c_2, a-b)$ solves the equation $(B+2)D_1^2u^p - 4D_2v^p = (B-2)w^2$.

2.1. Some elliptic curves. Let $p \geq 7$ be a prime, and let $B \neq \pm 2$ and $D \neq 0$ be integers. Suppose that there exists a primitive solution (a,b,c) of (1.3). Following Billerey [3], we associate to the triple (a,b,c) an elliptic curve E with the equation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{2.3}$$

where

$$\begin{cases} a_2 = (B+1)(a-b), \\ a_4 = (B+1)a^2 - (B^2+2B-2)ab + (B+1)b^2, \\ a_6 = a^3 - (B^2-1)a^2b + (B^2-1)ab^2 - b^3. \end{cases}$$

We have

$$\begin{cases} c_4 = 16(B-2)((B+2)(a+b)^2 - (a^2+Bab+b^2)), \\ c_6 = 32(b-a)(B-2)^2(2(B+2)(a+b)^2 + a^2+Bab+b^2), \\ \Delta = 16(B-2)^3(B+2)D^2c^{2p}. \end{cases}$$

Let Δ_E denote the minimal discriminant of E. The following lemma describes the reduction type of E at primes $l \nmid 2(B^2-4)D$.

LEMMA 2.2. *Let l be a prime number such that $l \nmid 2(B^2-4)D$. Equation* (2.3) *is minimal at l, the curve E has semistable reduction at l, and $v_l(\Delta_E) \equiv 0 \pmod{p}$.*

We attach to the curve E the mod p Galois representation

$$\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

which corresponds to the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $E[p]$ of E.

LEMMA 2.3. *Let $B \in \{0, 1, 3, 4, 5, 6\}$, and $c \neq \pm 1$. The representation $\overline{\rho}_{E,p}$ is irreducible for all primes $p \geq 7$.*

Proof. This follows from Lemme 2.5 of [3], since the elliptic curve E has a rational point $(b-a, 0)$ of order 2, and the j-invariant $j(E)$ is different from -15^3 and 255^3. ∎

2.2. The main theorems in the case $B = 1$. The theorems stated in this subsection (and proved in the next one) concern the Diophantine equation

$$(x+y)(x^2+xy+y^2) = Dz^p. \tag{2.4}$$

For certain choices of D, and primes p outside a finite set, equation (2.4) has no primitive solutions (x, y, z) with $z \neq \pm 1$. Theorems 2.4 and 2.5 below are results of this type.

THEOREM 2.4. *Let $p \geq 7$ be a prime, and let α, β and D be integers such that*

$$D = 2^\alpha \cdot 3^\beta, \qquad 0 \leq \alpha, \beta \leq p.$$

Then for all $\alpha \geq 4$, equation (2.4) *has no primitive solutions (x, y, z).*

Moreover, if there exists a primitive solution (x, y, z) of (2.4) *with $z \neq \pm 1$ for some $\alpha \leq 3$, then z is odd and $x \not\equiv y \pmod 3$.*

THEOREM 2.5. *Let p and r be primes, and let α, β, γ and D be integers such that*

$$D = 2^\alpha \cdot 3^\beta \cdot r^\gamma, \qquad r \neq p,\ 0 \leq \alpha, \beta \leq p,\ 1 \leq \gamma \leq p.$$

Suppose that p and D satisfy (*at least*) *one of the following conditions:*

(1) $p \geq 19$, $\alpha = 4$, $r \in \{29, 31, 41, 53, 59\,(p \neq 29), 79, 101, 103, 107\,(p \neq 53), 109\}$;
(2) $p \geq 23$, $\alpha = 4$, $\beta \neq 1$, $r \in \{17, 37, 61\,(p \neq 31), 67, 83, 89, 113\}$;
(3) $p \geq 11$, $\alpha \geq 5$, $\beta \neq 1$, $r \in \{31, 109\}$;
(4) $p \geq 19$, $\alpha \geq 2$, $\beta \neq 1$, $r \in \{79, 103\,(p \neq 31)\}$;
(5) $p \geq 23$, $\alpha \neq 1$, $\beta \neq 1$, $r \in \{53, 127\}$.

Then equation (2.4) *has no primitive solutions (x, y, z) with $z \neq \pm 1$.*

The next theorem is based on Kraus' method and it is stated for an arbitrary positive integer D. For this, we need some preparation.

Let D be a positive integer. Fix positive integers D_1 and D_2 such that:

(i) $D = D_1 D_2$;
(ii) $\gcd(D_1, D_2) = 1$;

(iii) if $l \mid D_2$ for a prime l, then either $l \equiv 1 \pmod 3$, or $l = 3$ and $v_3(D_2) = 1$.

Let us denote by $\mathscr{F}_1(D)$ the set of all pairs (D_1, D_2) satisfying (i)–(iii).

We define the integers:

$$N_{D_1,D_2} := 2^{\epsilon_2} 3^{\epsilon_3} \prod_{l \mid D,\, l>3} l, \qquad N'_{D_1,D_2} := 2^4 3^{\epsilon_3} \prod_{l \mid D,\, l>3} l, \tag{2.5}$$

where

$$\epsilon_2 := \begin{cases} 5 & \text{if } v_2(D_1) = 1, \\ 4 & \text{if } v_2(D_1) \neq 1, \end{cases} \qquad \epsilon_3 := \begin{cases} 1 & \text{if } v_3(D_2) = 0, \\ 2 & \text{if } v_3(D_2) = 1. \end{cases}$$

Let $p \geq 7$ be a prime. Suppose that for every $(D_1, D_2) \in \mathscr{F}_1(D)$, and every newform $f = q + \sum_{n \geq 2} c_n q^n$ of weight 2 and level N_{D_1,D_2} or N'_{D_1,D_2} with the field of coefficients $K_f \neq \mathbb{Q}$, there exists a prime index $l \nmid pN$ such that

$$p \nmid \mathrm{Norm}_{K_f/\mathbb{Q}}(c_l - r) \quad \text{ for all } r \in \{x \in 2\mathbb{Z} : |x| < 2\sqrt{l}\} \cup \{-l-1, l+1\}.$$

We define $\mathscr{P}_1(D)$ as the set of those primes $p \nmid D$ which satisfy the claims above.

Let $q \geq 17$ be a prime number coprime to D, and let $n > 0$ be an integer factor of $q - 1$. Let $\mu_n(\mathbb{F}_q)$ denote the group of nth roots of unity in $\mathbb{F}_q^\times$. Write $\overline{D}_1$ and $\overline{D}_2$ for the reductions modulo q of D_1 and D_2, respectively. Set

$$A_{\overline{D}_1,\overline{D}_2}(n,q) = \{\xi \in \mu_n(\mathbb{F}_q) : -3\overline{D}_1^2 + 4\overline{D}_2\xi \text{ is a square in } \mathbb{F}_q\}.$$

For each $\xi \in A_{\overline{D}_1,\overline{D}_2}(n,q)$, we denote by δ_ξ the least nonnegative integer such that

$$\delta_\xi^2 \bmod q = -3\overline{D}_1^2 + 4\overline{D}_2\xi.$$

We associate with each $\xi \in A_{\overline{D}_1,\overline{D}_2}(n,q)$ the following equation:

$$Y^2 = X^3 + 2\delta_\xi X^2 + (-3\overline{D}_1^2 + 5\overline{D}_2\xi)X + \overline{D}_2\delta_\xi\xi. \tag{2.6}$$

Its discriminant equals $2^4 3(\overline{D}_1\overline{D}_2\xi)^2$, so it defines an elliptic curve E_ξ over $\mathbb{F}_q$. We put $a_q(\xi) := q + 1 - \#E_\xi(\mathbb{F}_q)$.

THEOREM 2.6. *Let $D \neq 0$ be an integer, and let $p \in \mathscr{P}_1(D)$. Suppose that for every $(D_1, D_2) \in \mathscr{F}_1(D)$, and every elliptic curve F over $\mathbb{Q}$ with conductor N_{D_1,D_2} (respectively N'_{D_1,D_2}), there exists a positive integer n such that the following conditions are satisfied:*

(1) *$q = pn + 1$ is a prime, and $q \nmid D$;*
(2) *$a_q(F)^2 \not\equiv 4 \pmod p$;*
(3) *$a_q(F)^2 \not\equiv a_q(\xi)^2 \pmod p$ for all $\xi \in A_{\overline{D}_1,\overline{D}_2}(n,q)$.*

Then equation (2.4) *has no primitive solutions (x, y, z) with odd* (*resp. even*) *$z \neq \pm 1$.*

COROLLARY 2.7. *Let $5 \le r \le 23$ be an odd prime, and let $0 \le \alpha \le 5$, $1 \le \beta \le 10$ be integers. Then equation* (2.4) *has no primitive solutions for*

$$D = 2^{\alpha} \cdot r^{\beta} \quad \text{and} \quad 37 \le p < 10^6,$$

unless $D \in \{7,\ 7^3,\ 2\cdot 7,\ 8\cdot 7^2,\ 16\cdot 7^4,\ 13,\ 4\cdot 13,\ 8\cdot 13^2,\ 2\cdot 19,\ 16\cdot 19^2\}$, or p and D are as follows:

p	D
37	$2\cdot 7^{10}$, $4\cdot 7^6$, $32\cdot 11^9$, $4\cdot 13^2$, $8\cdot 13^7$, $32\cdot 13$, $4\cdot 19^4$, $2\cdot 23^9$

p	D
41	11^{10}, $4\cdot 11^6$, $8\cdot 13^5$, $2\cdot 19^4$, $2\cdot 23^{10}$, $8\cdot 23^7$,
43	$16\cdot 7$, $4\cdot 17^6$, $2\cdot 23^3$

p	D
47	13^6
59	13^3
67	7^2

Proof. We have computed, using Magma, the appropriate values of n for all integers D and primes p in the range given in Corollary 2.7. ∎

REMARK 2.8. For each $(D_1, D_2) \in \mathscr{F}_1(D)$, the set $\mathscr{P}_1(D)$ contains all but finitely many primes. It is well known (see [14]) that

$$p \notin \mathscr{P}_1(D) \ \Rightarrow\ p \le (1 + \sqrt{\mu(N)/6})^{2g_0^+(N)},$$

where $\mu(N) := N\prod_{q|N}(1 + 1/q)$ and $g_0^+(N) := \dim_{\mathbb{C}} \mathcal{S}_2^{\mathrm{new}}(N)$.

2.3. Proofs of the main theorems in the case $B = 1$. Let $D > 0$ be an integer, and let $p \ge 7$ be a prime such that $p \nmid D$. Suppose that equation (2.4) has a primitive solution (a, b, c). Let D_1, D_2, c_1, and c_2 be nonzero integers satisfying the conditions (2.1) for this solution. It follows from Lemma 2.1 that $\gcd(D_1c_1, D_2c_2) = 1$. Hence we may assume that $D_1D_2 = D$. Simple calculation shows that prime divisors l of D such that $l \equiv 2 \pmod 3$ fail to divide D_2. Moreover, for all coprime integers a and b we have $v_3(D_2) = v_3(a^2 + ab + b^2) \le 1$. These properties of D_1 and D_2 completely describe the set $\mathscr{F}_1(D)$ defined in Subsection 2.2.

If (a, b, c) with $c \ne \pm 1$ is a primitive solution of (2.4), then the elliptic curve E with equation

$$E: \quad y^2 = x^3 + 2(a-b)x^2 + (2a^2 - ab + 2b^2)x + a^3 - b^3$$

is the Frey type curve associated to (a, b, c). We have

$$c_4 = -16(2a^2+5ab+2b^2),\ \ c_6 = -32(a-b)(7a^2+13ab+7b^2),\ \ \Delta = -48D^2c^{2p}.$$

If $a \equiv 1 \pmod 4$ and $v_2(Dc) \ge 4$, then the discriminant Δ is not minimal at 2. Hence, $\Delta_E = 2^{-12}\Delta$ in this case, and $\Delta_E = \Delta$ otherwise.

We may assume that if ab is even, then a is odd. Let $\nu := \pm 1$ satisfy the congruence $\nu \equiv a \pmod 4$. Obviously, we do not need to check both cases $a \equiv 1 \pmod 4$ and $a \equiv -1 \pmod 4$, since both (a, b, c) and $(-a, -b, -c)$ are solutions of (2.4).

The curve E has conductor

$$N_E = 2^{f_2} \cdot 3^{f_3} \cdot \prod_{l \mid Dc,\, l>3} l,$$

where f_2 and f_3 are defined as follows:

$$f_3 := \begin{cases} 2 & \text{if } v_3(a^2+ab+b^2) = 1, \\ 1 & \text{if } v_3(a^2+ab+b^2) \neq 1, \end{cases}$$

$$f_2 := \begin{cases} 5 & \text{if } v_2(a+b) = 1, \\ 1 & \text{if } \nu = 1 \text{ and } v_2(a+b) > 4, \\ 0 & \text{if } \nu = 1 \text{ and } v_2(a+b) = 4, \\ 3 & \text{if } \nu = 1 \text{ and either } v_2(a+b) \in \{2,3\} \text{ or } v_2(b) \geq 2, \\ 2 & \text{if } \nu = 1 \text{ and } v_2(b) = 1, \\ 4 & \text{if } \nu = -1 \text{ and } v_2(a+b) \neq 1. \end{cases} \tag{2.7}$$

Our computations of this and other conductors are based on [19] and [16].

The modulo p Galois representation $\overline{\rho}_{E,p}$ attached to E has conductor

$$N = 2^{f_2'} \cdot 3^{f_3'} \cdot \prod_{l \mid D,\, l>3} l \quad \text{with} \quad f_3' := f_3 \quad \text{and} \quad f_2' := \begin{cases} 0 & \text{if } v_2(D_1) = 4, \\ f_2 & \text{otherwise.} \end{cases}$$

From the Modularity Theorem and Ribet's level-lowering it follows that there exists a newform

$$f = q + \sum_{n=2}^{\infty} c_n q^n \qquad (q := e^{2\pi i \tau})$$

of weight 2 and level N such that $\overline{\rho}_{E,p}$ arises from f (i.e. the corresponding Galois representation $\overline{\rho}_{f,p}$ is equivalent to $\overline{\rho}_{E,p}$). Let K_f denote the number field generated by the Fourier coefficients of f. Recall the following well known result (see for example Prop. 4.3 in [1]).

Proposition 2.9. *Suppose that $f \in \mathcal{S}_2^{\mathrm{new}}(N)$ gives rise to $\overline{\rho}_{E,p}$. If l is a prime coprime to pN, then one of the following conditions is satisfied:*

(1) $p \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(c_l \pm (l+1))$ *and* $l \mid N_E$;
(2) $p \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(c_l \pm 2r)$ *for some integer* $0 \leq r \leq \sqrt{l}$ *and* $l \nmid N_E$.

Proofs of Theorems 2.4 and 2.5. We use Proposition 2.9 and nonexistence of newforms of given levels (here we use Magma). Here we assume that $\nu = 1$ in the definition of f_2. It can be checked by elementary considerations that the Thue–Mahler equation $(x+y)(x^2+xy+y^2) = 2^\alpha 3^\beta$ has only one solution (x, y, α, β) with $\gcd(x, y) = 1$ and $\alpha, \beta \geq 0$, namely $(1, 1, 1, 1)$. Therefore, we omit the condition $z \neq \pm 1$ in the first part of Theorem 2.4.

Proof of Theorem 2.6. Suppose that (a, b, c) is a primitive solution of equation (2.4). Let E be the corresponding Frey curve.

Let p be an element of $\mathscr{P}_1(D)$. Proposition 2.9 implies that the representation $\overline{\rho}_{E,p}$ arises from a newform $f \in \mathcal{S}_2^{\mathrm{new}}(N)$ with rational coefficients. The theory of Eichler and Shimura ensures that there exists an elliptic curve F over $\mathbb{Q}$ with conductor N such that $\overline{\rho}_{E,p} \cong \overline{\rho}_{F,p}$.

Suppose that for every curve F over $\mathbb{Q}$ with conductor N there exists an integer n such that conditions (1)–(3) of Theorem 2.6 are satisfied.

LEMMA 2.10. *The curve E has good reduction at the prime $q = np + 1$.*

Proof. Suppose that E has bad reduction at q. Since q does not divide $6D$, it follows that q divides c.

Let F be an elliptic curve over $\mathbb{Q}$ with conductor N such that $\rho_{E,p} \cong \rho_{F,p}$. The curve F has good reduction at q. From Proposition 2.9, we have

$$a_q(F) \equiv \pm(q+1) \pmod{p}.$$

Hence we obtain

$$a_q(F)^2 \equiv 4 \pmod{p},$$

and this contradicts condition (2) of Theorem 2.6. ∎

From Lemma 2.10, it follows that the prime q does not divide c, so since $pn = q - 1$, we deduce that $c_1^p \bmod q$ and $c_2^p \bmod q$ are nth roots of unity in $\mathbb{F}_q^\times$. Let $\overline{a}$, $\overline{b}$, $\overline{D}_1$ and $\overline{D}_2$ denote the reductions of a, b, D_1 and D_2 modulo q. It follows from (2.1) that there exist $u, v \in \mu_n(\mathbb{F}_q)$ such that

$$\begin{cases} \overline{a} + \overline{b} = \overline{D}_1 u, \\ \overline{a}^2 + \overline{a}\overline{b} + \overline{b}^2 = \overline{D}_2 v. \end{cases}$$

The substitutions

$$\overline{a}' = \overline{a}/u, \qquad \overline{b}' = \overline{b}/u, \qquad \xi = v/u^2$$

lead to the equality

$$\overline{b}'^2 - \overline{D}_1\overline{b}' + \overline{D}_1^2 - \overline{D}_2\xi = 0.$$

It follows that $\xi \in A_{\overline{D}_1,\overline{D}_2}$, and either

$$(\overline{a}', \overline{b}') = \left(\frac{\overline{D}_1 + \delta_\xi}{2}, \frac{\overline{D}_1 - \delta_\xi}{2}\right) \quad \text{or} \quad (\overline{a}', \overline{b}') = \left(\frac{\overline{D}_1 - \delta_\xi}{2}, \frac{\overline{D}_1 + \delta_\xi}{2}\right).$$

Easy verification shows that the curve E_ξ with equation (2.6) is a quadratic twist by $\sqrt{\pm u}$ of the elliptic curve $\overline{E}_q$ over $\mathbb{F}_q$ obtained from E by reduction modulo q. Since $\overline{\rho}_{E,p} \cong \overline{\rho}_{F,p}$ for some curve F, we obtain

$$a_q(\xi)^2 \equiv a_q(F)^2 \pmod{p}.$$

This contradicts condition (3) of Theorem 2.6. Hence there exist no primitive solution (a, b, c) of equation (2.4) satisfying (2.1).

2.4. Further examples of Kraus type criteria. We have worked out a few Kraus type criteria for further special cases of equation (1.3), with $B = 0, 3, 4, 5, 6$ and specific choices of D. We omit the formulations and proofs, as they are similar to (the proof of) Theorem 2.6. We only state the results of our numerical investigations based on these criteria.

Case $B = 0$. The equation

$$(x + y)(x^2 + y^2) = Dz^p \tag{2.8}$$

was considered by Billerey in [3]. He proved that there exists no primitive solution of (2.8) if $p > 5$ and $D \in \{2, 6, 10, 22\}$. In the case $D = 1$ he deduced that the integer z must be odd ([3, Thm. 3.1]). Another proof of this fact was given by Dąbrowski in [9].

Result 2.11. *Let* $D = 2^\alpha r^\beta$, *where* $0 \leq \alpha \leq 3$ *and* $0 \leq \beta \leq 10$ *are integers, and* $r \in \{1, 3, 5, 7, 11, 13, 17, 19, 23\}$. *Let* p *be a prime such that* $37 < p < 10^6$. *Then equation* (2.8) *has no primitive solutions* (x, y, z) *with* $z \neq \pm 1$, *unless* $D \in \{1, 5, 5^2, 13, 13^4\}$.

Case $B = 3$. Consider the equation

$$(x + y)(x^2 + 3xy + y^2) = Dz^p, \tag{2.9}$$

where p is a prime number and D a positive integer.

Result 2.12. *Let* $D = 2^\alpha r^\beta$, *where* $0 \leq \alpha \leq 3$ *and* $0 < \beta \leq 10$ *are integers, and* $r \in \{3, 5, 7, 11, 13, 17, 19\}$. *Let* p *be a prime such that* $37 < p < 10^6$. *Then equation* (2.9) *has no primitive solutions* (x, y, z) *with* $z \neq \pm 1$.

Case $B = 4$. Consider the equation

$$(x + y)(x^2 + 4xy + y^2) = r^k z^p, \tag{2.10}$$

where $r > 3$ is a prime or $r = 1$, and $0 < k < p$.

Result 2.13. *Equation* (2.10) *has no primitive solutions with* $z \neq \pm 1$ *for*

(i) $1 \leq k \leq 10$, $r \in \{5, 7, 13\}$, *and* $31 < p < 10^6$, *or*
(ii) $2 \leq k \leq 10$, $r = 11$, *and* $53 < p < 10^6$.

Moreover, this equation has no primitive solutions with even z *for*

(iii) $r = 1$, *and* $13 < p < 10^6$, *or*
(iv) $k = 1$, $r = 11$, *and* $31 < p < 10^6$.

Case $B = 5$. Consider the equation

$$(x + y)(x^2 + 5xy + y^2) = r^k z^p, \tag{2.11}$$

where $r > 3, r \neq 7$ is a prime or $r = 1$, and $0 < k < p$.

Result 2.14. *Equation* (2.11) *has no primitive solutions with* $z \neq \pm 1$ *for*

(i) $1 \le k \le 10$, $r \in \{11, 13\}$, *and* $41 < p < 10^6$.

Equation (2.11) *has no primitive solutions with* z *divisible by* 3 *or* $v_2(y) \neq 1$ *for*

(ii) $1 \le k \le 10$, $r = 5$, *and* $67 < p < 10^6$, *or*
(iii) $1 \le k \le 10$, $r = 17$, *and* $37 < p < 10^6$.

Equation (2.11) *has no primitive solutions with* $z \neq \pm 1$ *not divisible by* 3 *and* $v_2(y) = 1$ *for*

(iv) $k = 2$ *or* $4 \le k \le 10$, $r = 5$, *and* $31 < p < 10^6$, *or*
(v) $2 \le k \le 10$, $r = 17$, *and* $47 < p < 10^6$.

Moreover this equation has no primitive solutions with z *divisible by* 3 *or* xy *not divisible by* 4 *for*

(vi) $r = 1$ *and* $19 < p < 10^6$.

Case $B = 6$. Consider the equation

$$(x + y)(x^2 + 6xy + y^2) = r^k z^p, \tag{2.12}$$

where $r > 3$ is a prime or $r = 1$, and $0 < k < p$.

RESULT 2.15. *Equation* (2.12) *has no primitive solutions with odd* $z \neq \pm 1$ *for*

(i) $r = 17$, *all* $k > 0$ *and all primes* $p > 7$, *or*
(ii) $r = 1$ *and* $7 < p < 10^6$, *or*
(iii) $2 \le k \le 10$, $r \in \{5, 7\}$, *and* $23 < p < 10^6$, *or*
(iv) $1 \le k \le 10$, $r = 11$, *and* $7 < p < 10^6$.

Moreover this equation has no primitive solutions with even z *for*

(v) $1 \le k \le 10$, $r \in \{5, 7, 11, 17\}$, *and* $47 < p < 10^6$.

RESULT 2.16. *Equation* (2.12) *has no primitive solutions with* $z \neq \pm 1$ *for* $r \in \{191, 251, 317, 479, 541, 607, 631, 647, 719, 757, 769, 853, 887, 911, 937, 971\}$, *all positive integers* k, *and all but finitely many primes* p.

3. Reductions to a class of Diophantine equations of signature $(p, p, 2)$. Conjecture (A) in [3] says, in particular, that the Diophantine equation (1.3) has no primitive solutions for primes p greater than a positive constant $C_{B,D}$. In this section we show that for an (infinite) subfamily of equations (1.3), the analogous statement follows from two conjectures formulated by Ivorra and Kraus (see [13]) concerning Diophantine equations of signature $(p, p, 2)$. It is well known that Conjecture (A) as well as the conjectures of Ivorra and Kraus follow from the *abc* conjecture.

This section was partially suggested by Sections 4 and 5 in [9]. Consider the following special case of (1.3):

$$(x+y)(x^2+(q^n+2)xy+y^2)=z^p, \tag{3.1}$$

where q is a prime, and n is a positive integer. In this case, the solubility questions for (1.3) can be reduced to studying equations of the type $(p,p,2)$.

The following lemma will be helpful.

LEMMA 3.1. *Suppose that $p>5$ is a prime. If $\alpha \geq 2$, then the equation $x^p+2^\alpha y^p=z^2$ has no primitive solution (x,y,z) with $xy \neq 1$.*

Proof. This is a special case of Theorem 1.2 in [1]. ∎

First, let us consider the simplest case $q=n=2$ (hence $B=6$).

PROPOSITION 3.2. *For any prime $p>5$ the equation $(x+y)(x^2+6xy+y^2) = z^p$ has no primitive solution (x,y,z) with even z.*

Proof. Suppose that such a solution exists. By Lemma 2.1 we get

$$d:=\gcd(x+y,\ x^2+6xy+y^2)=2 \text{ or } 4$$

(note that x,y must be odd). From the equality $x^2+6xy+y^2=(x-y)^2+8xy$ we conclude that $x^2+6xy+y^2 \equiv 8$ or $12 \pmod{16}$. Since $p>5$, it follows that $d=4$. Hence, there exist coprime integers z_1 and z_2 such that

$$\begin{cases} x+y=2^{p-2}z_1^p, \\ x^2+6xy+y^2=4z_2^p. \end{cases}$$

By substituting $y=2^{p-2}z_1^p-x$ in the second equation, we find that x and y are roots of the quadratic polynomial $P(X)=X^2-2^{p-2}z_1^pX-2^{2p-6}z_1^{2p}+z_2^p$. Since $P(X)$ has integer roots, its discriminant $\Delta=4(2^{p-5}(2z_1^2)^p-z_2^p)$ must be a square in $\mathbb{Z}$. But this contradicts Lemma 3.1. ∎

Ivorra and Kraus (see [13]) considered the general Diophantine equation

$$Ax^p+By^p=Cz^2, \tag{3.2}$$

where p is a prime >3, and A, B, C are pairwise coprime positive integers. They showed that, in many cases, (3.2) has no primitive solutions (see also [1]) and formulated the following conjectures:

CONJECTURE 3.3. *Suppose that none of the three integers $A+B$, $A-B$, $B-A$ belong to $C\mathbb{Z}^2$. Then there exists a constant $f(A,B,C)$ such that for $p>f(A,B,C)$ equation (3.2) has no primitive solutions.*

CONJECTURE 3.4. *Suppose that some of the three integers $A+B$, $A-B$, $B-A$ belong to $C\mathbb{Z}^2$. Then there exists a constant $g(A,B,C)$ such that for $p>g(A,B,C)$ the only primitive solutions (a,b,c) of (3.2) are those satisfying $ab=\pm 1$.*

These conjectures follow from the *abc* conjecture.

PROPOSITION 3.5. *Assume that Conjecture* 3.4 *is true. Then*

(i) *for every $n \in \mathbb{N}$ there exists a constant $\alpha(n)$ such that for all primes $p > \alpha(n)$ the equation $(x+y)(x^2+(2^n+2)xy+y^2) = z^p$ has no primitive solutions (x, y, z) with $v_2(x+y) < n/2$;*

(ii) *for every prime $q > 2$ there exists a constant $\beta(q)$ such that for all primes $p > \beta(q)$ the equation $(x+y)(x^2+(q+2)xy+y^2) = z^p$ has no primitive solutions (x, y, z) with $v_q(x+y) = 0$.*

Proof. (i) Suppose the opposite is true, i.e. that there exists a primitive solution (x, y, z), satisfying $v_2(x+y) < n/2$. Put $m := v_2(x+y)$. By Lemma 2.1, we have

$$d := \gcd(x+y, x^2+(2^n+2)xy+y^2) = 2^m.$$

Note that $x^2+(2^n+2)xy+y^2 = (x+y)^2+2^n xy$. First, we assume that $d = 1$. Then we have $x+y = z_1^p$ and $x^2+(2^n+2)xy+y^2 = z_2^p$ for some coprime odd integers z_1 and z_2. As in the proof of Proposition 3.2, we obtain a quadratic equation with discriminant $\Delta = 2^{2n} z_1^{2p} + 2^{n+2}(z_1^{2p} - z_2^p)$. Suppose that $n = 1$ ($n > 1$ is odd, n is even, respectively). Then Δ is a square of an integer iff $3X^p + 2Y^p = Z^2$ ($(2^{n-2}+1)X^p + Y^p = 2Z^2$, $(2^{n-2}+1)X^p + Y^p = Z^2$, respectively) has an integer solution with $\gcd(X, Y) = 1$. But by the assumption these equations have no solutions for sufficiently large p, with the possible exception $XY = \pm 1$. Checking all possibilities we get only the trivial solutions $(x, y, z) = (0, \pm 1, \pm 1), (\pm 1, 0, \pm 1)$.

Now let $m > 0$. Note that $3m = v_2(z^p) = pv_2(z)$, so $m = pt$ for some $t \in \mathbb{N}$. Then there exist coprime odd integers z_1 and z_2 such that $x+y = 2^m z_1^p$ and $x^2+(2^n+2)xy+y^2 = 2^{2m} z_2^p$. We obtain the equation $-2^{n-2m}x^2 + 2^{n-m}xz_1^p + z_1^{2p} - z_2^p = 0$. For $n = 2$ (n odd, $n > 2$ even, respectively) its discriminant is a square iff $2X^p + Y^p = Z^2$ ($(2^{n-2}+1)X^p + Y^p = 2Z^2$, $(2^{n-2}+1)X^p + Y^p = Z^2$, respectively) has an integer solution with $\gcd(X, Y) = 1$. As before, these equations satisfy the assumptions of Conjecture 3.4. Hence, for p large enough, the only possible solutions satisfy $XY = \pm 1$. But this leads to the trivial solutions $(\pm 2^{pt}, 0, \pm 2^{3t}), (0, \pm 2^{pt}, \pm 2^{3t})$.

(ii) Suppose that the equation in (ii) has a primitive solution (x, y, z) with $v_q(x+y) = 0$. By the assumption and Lemma 2.1, we get $\gcd(x+y, x^2+(q+2)xy+y^2) = 1$.

Hence $x+y = z_1^p$ and $x^2+(q+2)xy+y^2 = z_2^p$, and we conclude that the equation $(q+4)X^p + 4Y^p = qZ^2$ has the solution $(z_1^2, -z_2, x-y)$ (see explanations after Lemma 2.1). Applying Conjecture 3.4 we get $z_1 z_2 = \pm 1$ (for p large enough). This leads to $(x, y, z) = (0, \pm 1, \pm 1)$ or $(\pm 1, 0, \pm 1)$, which is the desired result. ∎

PROPOSITION 3.6. *Assume that Conjectures* 3.3 *and* 3.4 *are true. Then for every prime $q > 2$ there exists a constant $\gamma(q)$ such that for $p > \gamma(q)$, the* *equation* $(x+y)(x^2+(q+2)xy+y^2)=z^p$ *has a primitive solution* (x,y,z) *with* $v_q(x+y)>0$ *if and only if* $q^{2p-3}(q+4)\pm 4$ *is a square of some integer. If* $q^{2p-3}(q+4)+4=u^2$*, then the solutions are*

$$(q^{p-1}\pm u)/2,(q^{p-1}\mp u)/2,-q),\ ((-q^{p-1}\pm u)/2,(-q^{p-1}\mp u)/2,q);$$

and if $q^{2p-3}(q+4)-4=v^2$*, then the solutions are*

$$((q^{p-1}\pm v)/2,(q^{p-1}\mp v)/2,q),\ ((-q^{p-1}\pm v)/2,(-q^{p-1}\mp v)/2,-q).$$

Proof. Assume (a,b,c) is such a solution. We have $v_q(a^2+(q+2)ab+b^2)=\min(2v_q(x+y),1)=1$. Hence, by Lemma 2.1 we get $x+y=q^{p-1}c_1^p$ and $a^2+(q+2)ab+b^2=qc_2^p$, where $\gcd(c_1,c_2)=1$ and $q\nmid c_2$. Then by a similar discussion we infer that $q^{2p-3}(q+4)X^p+4Y^p=Z^2$ has a solution with $\gcd(X,Y)=1$ and $q\nmid Y$. If $q^{2p-3}(q+4)\pm 4$ is not a square, then by Conjecture 3.3 this equation has no primitive solution for large p. If $q^{2p-3}(q+4)\pm 4$ is a square, then by Conjecture 3.4 the only solutions are those satisfying $XY=\pm 1$. The assertion follows. ∎

Corollary 3.7. *Assume that Conjectures* 3.3 *and* 3.4 *hold. Then for infinitely many* B *the equation* $(x+y)(x^2+Bxy+y^2)=z^p$ *has no primitive solutions for all but finitely many primes* p.

Proof. By Propositions 3.5 and 3.6, equation $(x+y)(x^2+(q+2)xy+y^2)=z^p$, where q is an odd prime, has the primitive solution for p large enough if and only if $q^{2p-3}(q+4)+4$ or $q^{2p-3}(q+4)-4$ is a square. Suppose that $q^{2p-3}(q+4)=x^2-4=(x-2)(x+2)$. Then x is odd and $\gcd(x-2,x+2)=1$. Hence, either q^{2p-3} divides $|x-2|$ or q^{2p-3} divides $|x+2|$, so for example, $|x+2|\geq q^{2p-3}$. Then we obtain $|x-2|\geq q^{2p-3}-4>q+4$, a contradiction. If $q^{2p-3}(q+4)=x^2+4=(x-2i)(x+2i)$, we assume that $q\equiv 3 \pmod 4$. Then q is a prime in $\mathbb{Z}[i]$, and as above we get a contradiction. ∎

Remark 3.8. Browkin [6] has formulated a weak effective version of the *abc* conjecture, and, assuming it, he described all solutions of some Diophantine equations. Assuming a variant of that conjecture (with $r=1.499$, say), one can easily prove that equation (1.2) has no primitive solutions for any odd prime p.

Problem: apply (a variant of) the above conjecture to (1.3) and deduce information about the number of solutions.

Acknowledgements. We would like to thank Nicolas Billerey for checking some of our computations, and for useful comments. We thank the referee for useful suggestions which allowed us to improve the final version of the article.

REFERENCES

[1] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. 56 (2004), 23–54.

[2] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compos. Math. 140 (2004), 1399–1416.
[3] N. Billerey, *Formes homogènes de degré 3 et puissances p-ièmes*, J. Number Theory 128 (2008), 1272–1294.
[4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, in: Computational Algebra and Number Theory (London, 1993), J. Symbolic Comput. 24 (1997), 235–265.
[5] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843–939.
[6] J. Browkin, *A weak effective abc-conjecture*, Funct. Approx. 39 (2008), 103–111.
[7] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra 322 (2009), 638–656.
[8] A. Dąbrowski, *On the integers represented by* $x^4 - y^4$, Bull. Austral. Math. Soc. 76 (2007), 133–136.
[9] A. Dąbrowski, *On a class of generalized Fermat equations*, Bull. Austral. Math. Soc. 82 (2010), 505–510.
[10] H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995), 513–543.
[11] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. 490 (1997), 81–100.
[12] G. Frey, *Links between solutions of* $A - B = C$ *and elliptic curves*, in: Number Theory (Ulm, 1987), Lecture Notes in Math. 1380, Springer, 1989, 31–62.
[13] W. Ivorra et A. Kraus, *Quelques résultats sur les équations* $ax^p + by^p = cz^2$, Canad. J. Math. 58 (2006), 115–153.
[14] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. 49 (1997), 1139–1161.
[15] A. Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experiment. Math. 7 (1998), 1–13.
[16] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3*, J. Number Theory 44 (1993), 119–152.
[17] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. 100 (1990), 431–476.
[18] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.
[19] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in: Modular Functions of One Variable, IV (Antwerp, 1972), Lecture Notes in Math. 476, Springer, 1975, 33–52.
[20] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443–551.

Andrzej Dąbrowski, Tomasz Jędrzejak, Karolina Krawciów
Institute of Mathematics
University of Szczecin
Wielkopolska 15
70-451 Szczecin, Poland
E-mail: dabrowsk@wmf.univ.szczecin.pl
tjedrzejak@gmail.com
karolina.krawciow@wmf.univ.szczecin.pl

Received 25 June 2012;
revised 10 July 2012 (5704)