Canad. Math. Bull. Vol. **45** (2), 2002 pp. 247–256

On a Few Diophantine Equations Related to Fermat's Last Theorem

O. Kihel and C. Levesque

Abstract. We combine the deep methods of Frey, Ribet, Serre and Wiles with some results of Darmon, Merel and Poonen to solve certain explicit diophantine equations. In particular, we prove that the area of a primitive Pythagorean triangle is never a perfect power, and that each of the equations $X^4 - 4Y^4 = Z^p$, $X^4 + 4Y^p = Z^2$ has no non-trivial solution. Proofs are short and rest heavily on results whose proofs required Wiles' deep machinery.

1 Introduction

Very recently, A. Wiles [W] proved that *every semi-stable elliptic curve over $\mathbb{Q}$ is modular*, a result from which he deduced a proof of

Theorem 1.1 **(Fermat's Last Theorem)** *For $n \geq 3$, the diophantine equation*

$$X^n + Y^n = Z^n$$

has no solution with $XYZ \neq 0$.

The last theorem implies that for p an odd prime and $q = \frac{p-1}{2}$, the diophantine equation

$$(x + y + z)^p = G(x, y, z).$$

where

$$G(x, y, z) = 4(xyz) \sum_{j=0}^{q} \sum_{i=0}^{q-1-j} \binom{p}{2j+1} \binom{p-1-2j}{2i+1} x^{p-1-2j-2i} y^{2i} z^{2j},$$

has no non-trivial solution, because of the *Lamé identity*:

$$(x + y + z)^p - (-x + y + z)^p - (x - y + z)^p - (x + y - z)^p = G(x, y, z).$$

Theorem 1.1 allowed Cao [C2] to prove that the diophantine equation

$$X^4 - Y^4 = Z^p, \tag{1.1}$$

Received by the editors October 19, 2000; revised April 12, 2001.
AMS subject classification: 11D41.
Keywords: Diophantine equations.

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

with p prime ≥ 3, has no solution with $XYZ \neq 0$ and $\gcd(X, Y) = 1$. In fact, equation (1.1) was previously studied by B. Powell [P] and H. Darmon [D2]. Cao [C2] also considered the equation

$$X^4 - 1 = 2^m Z^p \tag{1.2}$$

with p prime ≥ 3, $m \in \mathbb{N} = \{0, 1, 2, \dots, \}$, and we will solve in Theorem 2.1 (i) the more general equation

$$X^4 - Y^4 = 2^m Z^p. \tag{1.3}$$

We will also solve in Theorem 2.1 (ii) the diophantine equation

$$X^4 - 4Y^4 = Z^p \quad (p \text{ prime}), \tag{1.4}$$

whose study was initiated by B. Powell [P] and Cao [C2].

Thanks to A. Wiles and some members (C. Breuil, B. Conrad, F. Diamond and R. L. Taylor) of his school, we know that the Shimura-Taniyama conjecture is true [B-C-D-T]: *Every elliptic curve over $\mathbb{Q}$ is modular.* As a result, some new challenging diophantine equations were completely solved by Darmon [D1], Ribet [Ribet], Serre [S], Darmon and Merel [D-M] and Poonen [P].

***Theorem 1.2* (Darmon)** *The diophantine equation*

$$X^n + 4Y^n = Z^2, \tag{1.5}$$

where n is a prime $\equiv 1 \pmod 4$, has no non-trivial solution with $\gcd(X, Y) = 1$.

***Theorem 1.3* (Serre)** *Let p be a prime ≥ 11, let q be a prime of*

$$\mathcal{S} = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$$

with $q \neq p$, and let $m \in \mathbb{N}$. Then there are no triples of non-zero integers (X, Y, Z) which satisfy

$$X^p + q^m Y^p + Z^p = 0. \tag{1.6}$$

***Theorem 1.4* (Ribet)** *Let p be a prime ≥ 3. Then for $a \geq 2$, the equation*

$$X^p + 2^a Y^p + Z^p = 0 \tag{1.7}$$

has no solution in non-zero integers with $\gcd(X, Z) = 1$.

***Theorem 1.5* (Darmon-Merel)** *Let $n \geq 3$. Then the diophantine equation*

$$X^n + Y^n = 2Z^n \tag{1.8}$$

has no primitive solution with $|XYZ| > 1$.

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

Theorem 1.6 **(Darmon-Merel-Poonen)**

(i) *For $n \geq 4$, the diophantine equation*

$$X^n + Y^n = Z^2 \tag{1.9}$$

has no solution with $XYZ \neq 0$ and $\gcd(X, Y) = 1$.

(ii) *For $n \geq 3$, the diophantine equation*

$$X^n + Y^n = Z^3 \tag{1.10}$$

has no solution with $XYZ \neq 0$ and $\gcd(X, Y) = 1$.

In fact, in Theorem 1.6, Poonen [P] took care of the equations

$$X^9 + Y^9 = Z^2, \quad X^5 + Y^5 = Z^2, \quad X^5 + Y^5 = Z^3.$$

In the following sections, we will solve some diophantine equations and solutions will rely on Theorems 1.1 to 1.6: see Theorems 2.1, 3.1, 3.2, 4.1 and 4.2. In some cases, we generalize some particular cases considered by previous authors. Though most of the times, proofs are short, they rest heavily on some deep results whose proofs required Wiles' machinery. A striking corollary of Theorem 3.1 is the following result.

Theorem 1.7 *The area of a primitive Pythagorean triangle is never a perfect power.*

This generalizes the previous result of Fermat that the area of a primitive Pythagorean triangle is never a perfect square (a fact which by the way is equivalent to the statement that 1 is not a congruent number).

2 Some Diophantine Equations

In this section, we will prove Theorem 2.1, sometimes using the equality

$$(x + y)^2 - (x - y)^2 = 2(x^2 + y^2). \tag{2.1}$$

Theorem 2.1 *Let p be an odd prime and let $m \in \mathbb{N}$. In cases (vii) to (x), if $m \neq 0$, then $p \geq 11$, and q is a prime of $\mathcal{S} = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$ with $q \neq p$. Then each of the following diophantine equations has no solution with $XYZ \neq 0$ and $\gcd(X, Y) = \gcd(X, Z) = \gcd(Y, Z) = 1$:*

(i) $X^4 - Y^4 = 2^m Z^p$;
(ii) $X^4 - 4Y^4 = Z^p$;
(iii) $X^{2p} + 2^m Y^p = Z^2$;
(iv) $X^4 + 4Y^p = Z^2$;
(v) $4X^4 + Y^p = Z^2$;
(vi) $X^6 + 4Y^p = Z^2$;
(vii) $X^4 - Y^4 = 8q^m Z^p$;
(viii) $2^{2p-2} q^{2m} X^{2p} - Y^2 = Z^p$;
(ix) $X^{2p} + 4q^m Y^p = Z^2$;

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

(x) $X^2 + 4Y^p = q^{2m}Z^{2p}$.

Proof (i) If $m = 0$, this is Cao's result [C2]. Let $m \geq 1$. The integers X, Y are odd since $\gcd(X, Y) = 1$. Moreover $\gcd(X^2 + Y^2, X^2 - Y^2) = 2$. Without loss of generality, Z is also odd. Suppose first $m \geq 2$. Then

$$\begin{cases} X \pm Y = 2^{m-2}c^p \\ X \mp Y = 2d^p \\ X^2 + Y^2 = 2b^p, \end{cases} \tag{2.2}$$

with $Z = cdb$, $\gcd(c, d) = \gcd(c, b) = \gcd(d, b) = 1$ and with c even if $m = 2$. Using (2.1), we obtain

$$2^{2m-6}c^{2p} + d^{2p} = b^p. \tag{2.3}$$

For $m = 3$, this contradicts Fermat's last theorem; for $m \geq 4$ and for $m = 2$, this is a contradiction to Theorem 1.4.

Suppose now $m = 1$. Then $X^4 - Y^4 = (X^2 + Y^2)(X^2 - Y^2) = 2Z^p$. Hence $X^2 + Y^2 = 2b^p$ and $X^2 - Y^2 = 2^p a^p$, $X \pm Y = 2a_1^p$, $X \mp Y = 2^{p-1}a_2^p$; from (2.1), we deduce $a_1^{2p} + 2^{2p-4}a_2^{2p} = b^p$, a contradiction to Theorem 1.4.

(ii) We have $(X^2 - 2Y^2)(X^2 + 2Y^2) = Z^p$ with $\gcd(X^2 - 2Y^2, X^2 + 2Y^2) = 1$. Hence

$$\begin{cases} X^2 - 2Y^2 = a^p \\ X^2 + 2Y^2 = b^p, \end{cases} \tag{2.4}$$

with $Z = ab$ and $\gcd(a, b) = 1$, whereupon $(2Y)^2 = a^p + b^p$, a contradiction to Theorem 1.5 (ii).

(iii) Theorem 1.6 takes care of $m = 0$. Let $m \geq 1$. Then $(Z-X^p)(Z+X^p) = 2^mY^p$ leads to

$$\begin{cases} Z \pm X^p = 2a^p \\ Z \mp X^p = 2^{m-1}b^p, \end{cases} \tag{2.5}$$

with $Y = ab$, $\gcd(a, b) = 1$, and with b even if $m = 1$. Hence $\pm X^p = a^p - 2^{m-2}b^p$, a contradiction to Theorems 1.1 and 1.4.

(iv) Here $(Z + X^2)(Z - X^2) = 4Y^p$ with $\gcd(Z + X^2, Z - X^2) = 2$, so

$$\begin{cases} Z + X^2 = 2Y_1^p \\ Z - X^2 = 2Y_2^p, \end{cases} \tag{2.6}$$

whereupon $X^2 = Y_1^p - Y_2^p$, a contradiction to Theorem 1.6.

(v) From $(Z + 2X^2)(Z - 2X^2) = Y^p$ and $\gcd(Z + 2X^2, Z - 2X^2) = 1$, we deduce

$$\begin{cases} Z + 2X^2 = Y_1^p \\ Z - 2X^2 = Y_2^p, \end{cases} \tag{2.7}$$

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

whereupon $(2X)^2 = Y_1^p - Y_2^p$, another contradiction to Theorem 1.6.

(vi) We have $(Z + X^3)(Z - X^3) = 4Y^p$ with $\gcd(Z + X^3, Z - X^3) = 2$. Hence

$$\begin{cases} Z + X^3 = 2Y_1^p \\ Z - X^3 = 2Y_2^p, \end{cases} \tag{2.8}$$

whereupon $X^3 = Y_1^p - Y_2^p$, a contradiction to Theorem 1.6.

(vii) Again X and Y have to be odd. Since $(X^2+Y^2)(X^2-Y^2) = 8q^m Z^p$, we obtain

$$\begin{cases} X^2 + Y^2 = 2q^m a^p \\ X^2 - Y^2 = 4b^p \end{cases} \quad \text{or} \quad \begin{cases} X^2 + Y^2 = 2a^p \\ X^2 - Y^2 = 4q^m b^p, \end{cases}$$

with $Z = ab$ and $\gcd(a, b) = 1$. Therefore we have

$$\begin{cases} X^2 + Y^2 = 2q^m a^p \\ X \pm Y = 2c^p \\ X \mp Y = 2d^p \end{cases} \quad \text{or} \quad \begin{cases} X^2 + Y^2 = 2a^p \\ X \pm Y = 2q^m c^p \\ X \mp Y = 2d^p, \end{cases}$$

with $b = cd$ and $\gcd(a, c) = \gcd(a, d) = \gcd(c, d) = 1$. Using (2.1), we obtain

$$c^{2p} + d^{2p} = q^m a^p \quad \text{or} \quad q^{2m} c^{2p} + d^{2p} = a^p,$$

which are contradictions to Theorems 1.1 and 1.4.

(viii) Here $2^{p-1} q^m X^p + Y = a^p$ and $2^{p-1} q^m X^p - Y = b^p$ with $Z = ab$, whereupon $q^m (2X)^p = a^p + b^p$, a contradiction to Theorem 1.4.

(ix) There exist a, b such that $Y = ab$ and

$$\begin{cases} Z \pm X^p = 2q^m a^p \\ Z \mp X^p = 2b^p. \end{cases}$$

Hence $\pm X^p = q^m a^p - b^p$, a contradiction to Theorems 1.1 and 1.4.

(x) From $(q^m Z^p + X)(q^m Z^p - X) = 4Y^p$, with $\gcd(q^m Z^p + X, q^m Z^p - X) = 1$, we obtain

$$\begin{cases} q^m Z^p + X = 2a^p \\ q^m Z^p - X = 2b^p, \end{cases}$$

with $Y = ab$, from which (after adding) we deduce $q^m Z^p = a^p + b^p$, a contradiction to Theorem 1.3. ■

3 Other Diophantine Equations

Let us recall that the primitive solutions of $X^2+Y^2 = Z^2$ are given by the Pythagorean triples

$$X = a^2 - b^2, \quad Y = 2ab, \quad Z = a^2 - b^2, \tag{3.1}$$

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

with $a, b \in \mathbb{N}$, $\gcd(a, b) = 1$ and $2|ab$. By definition, a *Pythagorean triangle* is a right triangle with integral sides.

Fermat proved that *the area of a primitive Pythagorean triangle cannot be a square.* In fact, we will prove a stronger result.

Theorem 3.1 *Let p be an odd prime and let $m \in \mathbb{N}$. If $m \neq 0$, then $p \geq 11$, and q is a prime of $\mathcal{S} = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$ with $q \neq p$. Then there is no integral solution to*

$$X^2 + Y^2 = Z^2 \quad \textit{with} \quad XY = 2q^m T^p, \tag{3.2}$$

where $XYZ \neq 0$ and $\gcd(X, Y) = 1$.

Proof From (3.1), we have $X = a^2 - b^2$, $Y = 2ab$, $Z = a^2 + b^2$, subject to $a, b \in \mathbb{N}$, $\gcd(a, b) = 1$ and $2|ab$. Hence $XY = 2ab(a^2 - b^2) = 2q^m T^p$ with $(a, b) = 1$. Then we have three possibilities

a	$q^m r^p$	r^p	r^p
b	s^p	$q^m s^p$	s^p
$a^2 - b^2$	t^p	t^p	$q^m t^p$

leading respectively to

$$q^{2m} r^{2p} - s^{2p} = t^p, \quad r^{2p} - q^{2m} s^{2p} = t^p, \quad r^{2p} - s^{2p} = q^m t^p,$$

three contradictions to Theorem 1.3. ■

As a corollary, we have Theorem 1.7 given in the introduction. By the way, the hypothesis that the Pythagorean triangle be primitive is a crucial one as can be seen with $A = 3 \cdot 6^s$, $B = 4 \cdot 6^s$, $C = 5 \cdot 6^s$ $(s \geq 1)$, where $A^2 + B^2 = C^2$ and $\frac{1}{2}AB = 6^{2s+1}$.

Theorem 3.2 *Let $q \in \{3, 7, 11, 19, 23, 59\}$ and let p be a prime ≥ 11 with $q \neq p$. Then the diophantine equation*

$$X^2 + qY^2 = Z^2 \quad \textit{with} \quad XY = 2D^p \tag{3.3}$$

has no solution with $XYZ \neq 0$ and $\gcd(X, Y) = 1$. Moreover, the only positive integral solution of

$$X^2 + 2Y^2 = Z^2 \quad \textit{with} \quad XY = 2D^p \geq 2, \tag{3.4}$$

where $XYZ \neq 0$ and $\gcd(X, Y) = 1$, is $X = 1$, $Y = 2$, $Z = 3$.

Proof (i) If X is even, then Y and Z are odd and the congruence $X^2 + qY^2 \equiv Z^2$ is impossible modulo 4, because $q \equiv 3 \pmod 4$. Since $XY = 2D^p$, we have $X = a^p$, $Y = 2b^p$ with $D = ab$. From $(Z+X)(Z-X) = 4qb^{2p}$ with $\gcd(Z+X, Z-X) = 1$, we get

$$\begin{cases} Z \pm X = 2qb_1^{2p} \\ Z \mp X = 2b_2^{2p}, \end{cases}$$

whereupon upon subtraction, we deduce

$$\pm a^p = \pm X = qb_1^{2p} - b_2^{2p},$$

a contradiction to Theorem 1.3.

(ii) We have $X = a^p$, $Y = 2b^p$, $(Z+X)(Z-X) = 8b^{2p}$, so

$$\begin{cases} Z \pm X = 2b_1^{2p} \\ Z \mp X = 4b_2^{2p}, \end{cases}$$

with $b = b_1 b_2$. Hence $\pm a^p = \pm X = b_1^{2p} - 2b_2^{2p}$, whereupon by Theorem 1.6, we have $|ab_1b_2| \leq 1$, *i.e.*, $X = 1$, $Y = 2$, $Z = 3$. ■

4 Equations Involving Fermat Quotients

For an odd prime p, the *Fermat quotient* $Q_p(X)$ of an integer X coprime to p is defined by

$$Q_p(X) = \frac{X^{p-1} - 1}{p}. \tag{4.1}$$

Lucas already knew that $Q_p(2)$ is a square only for $p = 3, 7$. Cao and Pan proved that $Q_p(X)$ is a square only for $(p, X) = (5, 3), (7, 2)$, and that $Q_p(X)$ is never the double of a square (see [C-P] or [C2]). Osada and Terai [O-T] proved that the diophantine equation

$$Q_p(X) = Z^q \quad (q \text{ odd prime}) \tag{4.2}$$

has no solution for $p \geq 5$ and Z odd and that for $p = 3$ the only solution is $X = 2$. Cao [C2] proved that if $p \equiv 1 \pmod 4$, then (4.2) has no solution, improving upon a previous result of Le [L]. Moreover, Le [L] proved that for $p \equiv 1 \pmod 4$, the only solution of $Q_p(X) = 2^m Z^q$ is $(p, q, m, X, Z) = (5, 3, 1, 3, 2)$. The next theorem covers other cases.

Theorem 4.1 *Let p be an odd prime $\equiv 1 \pmod 3$, let q be an odd prime, let $m \in \mathbb{N}$, and let $\zeta_3 = \exp(\frac{2\pi i}{3})$ be a third root of unity. Let $\mathcal{T}$ be the set of primes of $\mathbb{N}$ which do not split in $\mathbb{Q}(\zeta_3)$ (i.e., which are inert or which ramify in $\mathbb{Q}(\zeta_3)$). Let P be a finite product of elements of $\mathcal{T}$ (repetitions are allowed and an empty product is 1). Then the only solution with $X > 1$ of the diophantine equation*

$$Q_p(X) = p^m P Z^q \tag{4.3}$$

corresponds to $P = 3 \cdot 3$ and is given by $X = 2$, $p = 7$, $m = 0$, $Z = 1$.

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

Proof Note that $r \in \mathcal{T}$ if and only if $r = 3$ or $r \equiv 2 \pmod 3$ (see [E-M]). Here $p = 6k + 1$ for some $k \in \mathbb{N}$. Since $(X^{3k} + 1)(X^{3k} - 1) = p^{m+1}PZ^q$, we have three possibilities to investigate

$X^{3k} \pm 1$	$p^{m+1}P_1a^q$	$2p^{m+1}P_1a^q$	$2P_1a^q$
$X^{3k} \mp 1$	P_2b^q	$2^{q-1}P_2b^q$	$2^{q-1}p^{m+1}P_2b^q$

where $P = P_1P_2$ and $Z = ab$ with $\gcd(P_1, P_2) = 1$ and $\gcd(a, b) = 1$.

(i) Suppose $(X^k \mp 1)(X^{2k} \pm X^k + 1) = P_2b^q$. Let us recall that the prime decomposition in $\mathbb{Q}(\zeta_3)$ of a prime r is given by the decomposition modulo r of the minimal polynomial of ζ_3. Therefore a prime r different from 3 and dividing P_2 does not divide $X^{2k} \pm X^k + 1$, since it is inert in $\mathbb{Q}(\zeta_3)$. Hence

$$X^{2k} \pm X^k + 1 = b_1^q \quad \text{or} \quad X^{2k} \pm X^k + 1 = 3b_1^q. \tag{4.4}$$

According to Nagell (see p. 96 of [Riben]), the solutions (with $X > 1$) of the first equation of (4.4) correspond to $q = 3$, $\pm X^k = 18$ or -19, *i.e.*, $k = 1$, $X = 18$ or 19, and $p = 7$.

When $X = 18$, we have $18^6 - 1 = 7^{m+1}PZ^q$, *i.e.*, $m = 2$, $P = 17 \cdot 19 \cdot 307$, which leads to a contradiction, since in particular $19 \notin \mathcal{T}$. When $X = 19$, we have $19^6 - 1 = 2^3 3^3 5 \cdot 7^3 127 = 7^{m+1}PZ^q$. Since $q > 1$, we have $127 | P$, another contradiction since $127 \notin \mathcal{T}$.

As far as the equation $X^{2k} \pm X^k + 1 = 3b_1^q$ is concerned (see p. 105 of [Riben]), the solutions (with $X > 1$) are $\pm X^k = -2$, $q \neq 2$, *i.e.*, $k = 1$, $X = 2$. Hence $p = 7$, $2^6 - 1 = 3^2 7 = 7^{m+1}PZ^q$, *i.e.*, $P = 3^2$, $m = 0$, $Z = 1$.

(ii) Suppose $(X^k \mp 1)(X^{2k} \pm X^k + 1) = 2^{q-1}P_2b^q$. As in (i), we have

$$X^{2k} \pm X^k + 1 = c^q \quad \text{or} \quad X^{2k} \pm X^k + 1 = 3c^q, \tag{4.5}$$

which is dealt with as in (i).

(iii) Finally suppose $(X^k \mp 1)(X^{2k} \pm X^k + 1) = 2P_1a^q$. This case is again taken care of as before. ■

Last theorem takes care of $Q_p(X) = Z^q$ and of $Q_p(X) = 2^m Z^q$. Note also the infinite number of possibilities for the value of P.

For an odd prime p, we define the *generalized Fermat quotient* $Q_p(X, Y)$ of two integers X, Y coprime to p by

$$Q_p(X, Y) = \frac{X^{p-1} - Y^{p-1}}{p}. \tag{4.6}$$

Theorem 4.2 *Let p be an odd prime and let $m \in \mathbb{N}$.*

(i) *If $q = 2$ or 3, then the diophantine equation*

$$Q_p(X, Y) = p^m Z^q \tag{4.7}$$

has no non-zero solution with Z odd and $\gcd(X, Y) = 1$ *(i.e., with $2 | XY$).*

(ii) *If q is a prime dividing $p-1$, then the diophantine equation*

$$Q_p(X,Y) = 2^m Z^q. \tag{4.8}$$

has no non-zero solution with $\gcd(X,Y)=1$.

Proof (i) Write $p = 2k+1$. So we have

$$(X^k - Y^k)(X^k + Y^k) = p^{m+1} Z^q. \tag{4.9}$$

Since Z is odd, we obtain

$$X^k \pm Y^k = a^q, \quad X^k \mp Y^k = p^{m+1} b^q \tag{4.10}$$

with $Z = ab$ and $\gcd(a,b) = 1$. The first equation in (4.10) has no solution by Theorem 1.6.

(ii) Let $p-1 = 2lq$. Then we have $(X^{lq} + Y^{lq})(X^{lq} - Y^{lq}) = 2^m p Z^q$, so

$$(X^l)^q \pm (Y^l)^q = 2^s a^q, \quad (X^l)^q \mp (Y^l)^q = 2^t p b^q \tag{4.11}$$

with $Z = ab$, $\gcd(a,b) = 1$, and

$$s + t = \begin{cases} m & \text{if } m \geq 1, \\ 0 & \text{if } m = 0 \text{ and } Z \text{ is even}, \\ q & \text{if } m = 0 \text{ and } Z \text{ is odd}. \end{cases}$$

The first equation in (4.12) is impossible by Theorems 1.4, 1.5 and 1.1 according to whether $s \geq 2$, $s = 1$, $s = 0$ respectively. ■

Acknowledgements The second author benefitted from NSERC and FCAR grants and wishes to express his deepest gratitude to Professor N. H. J. Lacroix for his judicious remarks.

References

[B-C-D-T] C. Breuil, B. Conrad, P. Diamond and R. Taylor, *Result announcement.* Notices Amer. Math. Soc. (9) **46**(1999), 863.

[C1] Z. Cao, *The Diophantine equation $x^4 - Dy^2 = 1$.* (Chinese) J. Harbin Inst. Tech. (4) **13**(1981), 53–58; II. J. Harbin Inst. Tech. (3) **15**(1983), 133–138.

[C2] ———, *The Diophantine equations $x^4 - y^4 = z^p$ and $x^4 - 1 = dy^q$.* C. R. Math. Rep. Acad. Sci. Canada (1) **21**(1999), 23–27.

[C-P] Z. Cao and J. Pan, *The Diophantine equation $x^{2p} - Dy^2 = 1$ and the Fermat quotient $Q_p(m)$.* J. Harbin Inst. Tech. **25**(1993), 119–121.

[D1] H. Darmon, *The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$.* Intern. Math. Res. Notices (10) **1993**, 263–274.

[D2] ———, *The equation $x^4 - y^4 = z^p$.* C. R. Math. Rep. Acad. Sci. Canada **15**(1993), 286–290.

[D-M] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem.* J. Reine Angew. Math. **490**(1997), 81–100.

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press

[De] P. Dénes, *Uber die Diophantische Gleichung* $x^l + y^l = cz^l$. Acta Math. **88**(1952), 241–251.

[E-M] J. Esmonde and R. Murty, *Problems in Algebraic Number Theory.* Graduate Texts in Math. **190**, Springer-Verlag, 1999.

[L] M. Le, *A note on the Diophantine equation* $x^{p-1} - 1 = py^q$. C. R. Math. Rep. Acad. Sci. Canada. **15**(1993), 121–124.

[O-T] H. Osada and N. Terai, *Generalization of Lucas' theorem for Fermat quotient.* C. R. Math. Rep. Acad. Sci. Canada **11**(1989), 115–120.

[P] B. Powell, *Sur l'équation diophantienne* $x^4 \pm y^4 = z^p$. Bull. Sci. Math. **107**(1983), 219–223.

[Riben] P. Ribenboim, *Catalan's Conjecture.* Academic Press, 1994.

[Ribet] K. A. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$. Acta Arith. **79**(1997), 7–16.

[S] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* Gal$(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. **54**(1987), 179–230.

[T] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras.* Ann. of Math. **141**(1995), 553–572.

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. of Math. **141**(1995), 443–551.

Dept. of Math. and Comp. Sc.
University of Lethbridge
Lethbridge, Alberta
T1K 3M4

Dép. Mathématiques et CICMA
Université Laval
Québec
G1K 7P4

https://doi.org/10.4153/CMB-2002-028-1 Published online by Cambridge University Press