Bull. Aust. Math. Soc. **98** (2018), 188–195
doi:10.1017/S0004972718000369

A NOTE ON THE DIOPHANTINE EQUATION $x^2 + (2c - 1)^m = c^n$

MOU-JIE DENG✉, JIN GUO and AI-JUAN XU

(Received 19 November 2017; accepted 7 April 2018; first published online 12 July 2018)

Abstract

Let $c \geq 2$ be a positive integer. Terai ['A note on the Diophantine equation $x^2 + q^m = c^n$', *Bull. Aust. Math. Soc.* **90** (2014), 20–27] conjectured that the exponential Diophantine equation $x^2 + (2c - 1)^m = c^n$ has only the positive integer solution $(x, m, n) = (c - 1, 1, 2)$. He proved his conjecture under various conditions on c and $2c - 1$. In this paper, we prove Terai's conjecture under a wider range of conditions on c and $2c - 1$. In particular, we show that the conjecture is true if $c \equiv 3 \pmod 4$ and $3 \leq c \leq 499$.

2010 *Mathematics subject classification*: primary 11D61.

Keywords and phrases: exponential Diophantine equation.

1. Introduction

Let $c \geq 2$ be a positive integer. Clearly, the Diophantine equation

$$x^2 + (2c - 1)^m = c^n \tag{1.1}$$

has the positive integer solution $(x, m, n) = (c - 1, 1, 2)$. In [6], Terai conjectured that (1.1) has no other solution and he proved this in five special cases determined by certain conditions on c and $2c - 1$ [6, Proposition 3.2]. When $2c - 1 = q$, where q is a prime, Terai obtained several results [6, Theorems 1.2–1.4] concerning the Diophantine equation

$$x^2 + q^m = c^n. \tag{1.2}$$

Using these results, together with results of Ljunggren [5], Zhu [7] and Arif–Abu Muriefah [1], Terai showed that, apart from $c = 12, 24$, his conjecture holds for $2 \leq c \leq 30$. The cases $c = 12, 24$ have been treated in [4]. In this paper, we show that Terai's conjecture is true under a wider range of conditions on c and $2c - 1$. The methods are elementary, but rely on results obtained by more advanced means. We prove the following theorems. Here $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

This research was supported by the National Natural Science Foundation of China (grant no. 11601108) and the Natural Science Foundation of Hainan Province (grant no. 20161002).

Theorem 1.1. *Suppose that $c \geq 2$ is a positive integer with $c \equiv 3 \pmod 4$. Let s be a positive integer and k, l, t be nonnegative integers. If one of the following conditions is satisfied, then Terai's conjecture is true:*

(i) $2c - 1$ *is a power of a prime;*
(ii) $2c - 1 = (8k+3)(8l+7)$ *with* $\gcd(8k+3, 8l+7) = 1$*;*
(iii) $2c - 1 = (8s+1)(8t+5)$ *with* $\gcd(8s+1, 87+5) = 1$ *and there is an odd prime q such that one of the following two alternatives holds:*

  (a) $q \mid (8(s+t)+6)$ *and* $q \nmid c$*;*
  (b) $q \equiv 3 \pmod 4$ *or* $q \equiv 5 \pmod 8$*, and* $8s + 1 \equiv 0 \pmod q$, $((8t+5)/q) = -1$*, or* $8t + 5 \equiv 0 \pmod q$, $((8s+1)/q) = -1$.

Theorem 1.2. *Suppose that p is an odd prime such that $p \equiv 3 \pmod 4$. Let s be a nonnegative integer. If $c = p^{2s+1}$, then Terai's conjecture is true.*

Theorem 1.3. *Let p be an odd prime and s and t be nonnegative integers. If one of the following conditions is satisfied, then Terai's conjecture is true:*

(i) $2c - 1 = 3^{2s+1}p^{2t+1}$*, where* $p \equiv 7 \pmod 8$ *or* $p \equiv 3 \pmod{16}$*;*
(ii) $2c - 1 = 3^{4s+1}p^{4t+1}$*, where* $p \equiv 5 \pmod{16}$ *or* $p \equiv 3 \pmod 5$*;*
(iii) $2c - 1 = 5^{2s+1}p^{2s+1}$*, where* $p \equiv 3 \pmod 8$ *and* $p + 5 \not\equiv 0 \pmod{32}$*;*
(iv) $2c - 1 = 9^{2^s}p^{2t+1}$*, where* $p \equiv 5 \pmod 8$*;*
(v) $c = 2^{s+1}$.

Corollary 1.4. *If $c \equiv 3 \pmod 4$ and $3 \leq c \leq 499$, then Terai's conjecture is true.*

Theorem 1.3 extends Terai's results [6, Proposition 3.2(ii)–(v)] by allowing for multiple prime factors dividing $2c - 1$.

2. Lemmas

Lemma 2.1 [2, Theorem 1.1]. *If $n \geq 4$ is an integer and $C = 1, 2, 3, 5, 6, 10, 11, 13$ or 17, then the equation $x^n + y^n = Cz^2$ has no solutions in nonzero pairwise co-prime integers (x, y, z) with, say, $x > y$, unless $(n; C) = (4; 17)$ or $(n; C; x, y, z)$ is one of $(5; 2; 3, 1, \pm 11), (5; 11; 3, 2, \pm 5)$ or $(4; 2; 1, 1, \pm 1)$.*

Lemma 2.2 [3, Theorem XI]. *Let α, β be integers such that $3 \leq \alpha < \beta, 2 \nmid \alpha\beta$ and $\gcd(\alpha, \beta) = 1$. Suppose that p is an odd prime and $p^a \parallel \alpha + \beta$. Then $p^{a+1} \parallel \alpha^p + \beta^p$ and therefore $p \parallel (\alpha^p + \beta^p)/(\alpha + \beta)$.*

Lemma 2.3 [3, Theorem XXV]. *Let x, y be coprime positive integers with $x > y$ and let r be a positive integer. If $r > 2$, then $x^r + y^r$ has a prime divisor p such that $p \nmid x^k + y^k$ for $k = 1, 2, \ldots, r - 1$, except when $(x, y, r) = (2, 1, 3)$.*

Lemma 2.4. *Let x, y be positive integers such that $3 \leq x < y$ and $2 \nmid xy$. Then*

$$2(x + y) \leq xy + 1. \tag{2.1}$$

https://doi.org/10.1017/S0004972718000369 Published online by Cambridge University Press

Proof. Let $y = x + a$ and $f(x) = xy + 1 - 2(x + y) = x^2 + (a - 4)x - 2a + 1$. Clearly, a is even with $a \geq 2$. If $a = 2$, the only positive root of $f(x) = 0$ is $x = 3$, so (2.1) holds. Suppose that $a \geq 4$. Let the bigger root of $f(x) = 0$ be r. Since

$$2 < r = \frac{4 - a + \sqrt{a^2 + 12}}{2} < \frac{4 - a + a + 2}{2} = 3,$$

it follows that (2.1) still holds. □

Lemma 2.5. *Let $c > 1$ be a positive integer with $c \equiv 3 \pmod 4$ and suppose that (1.1) has a positive integer solution. Then:*

(i) *$m = 2m' + 1$ is odd and $n = 2N$ is even;*

(ii) *if $m = 3$ and $2c - 1 = PQ$ with $3 \leq P < Q$ and $\gcd(P, Q) = 1$, then $P^m + Q^m = 2c^N$ has no solution.*

Proof. (i) Taking (1.1) modulo c gives $m = 2m' + 1$. Since $2c - 1 \equiv 5 \pmod 8$, taking (1.1) modulo $2c - 1$ yields

$$1 = \left(\frac{x^2}{2c - 1}\right) = \left(\frac{c^n}{2c - 1}\right) = \left(\frac{2c - 1}{c}\right)^n = \left(\frac{-1}{c}\right)^n = (-1)^n$$

and hence $n = 2N$.

(ii) Clearly, $N > 1$. Suppose that $N = 2$. From (1.1),

$$P^3Q^3 = (2c - 1)^3 = c^4 - x^2 = (c^2 - x)(c^2 + x) \quad \text{and} \quad \gcd(c^2 - x, c^2 + x) = 1,$$

so $c^2 - x = P^3, c^2 + x = Q^3$ and $P^3 + Q^3 = 2c^2$. Since $\gcd(P + Q, (P^3 + Q^3)/(P + Q)) = 1$ or 3, we have two cases to consider.

Case 1: $\gcd(P + Q, (P^3 + Q^3)/(P + Q)) = 1$. Write $c = c_1c_2$ with $\gcd(c_1, c_2) = 1$. From

$$P^3 + Q^3 = (P + Q)\left(\frac{P^3 + Q^3}{P + Q}\right) = 2c^2 = 2c_1^2 \cdot c_2^2,$$

we have $(P^3 + Q^3)/(P + Q) = c_2^2$, which leads to a contradiction because

$$\frac{P^3 + Q^3}{P + Q} = P^2 + Q^2 - PQ \equiv 2 - 5 \equiv 5 \not\equiv c_2^2 \equiv 1 \pmod 8.$$

Case 2: $\gcd(P + Q, (P^3 + Q^3)/(P + Q)) = 3$. By Lemma 2.2,

$$P + Q = 2 \cdot 3c_1^2, \quad \frac{P^3 + Q^3}{P + Q} = 3c_2^2,$$

where $c = 3c_1c_2$ with $\gcd(3c_1, c_2) = 1$. As in Case 1, we reach a contradiction because

$$\frac{P^3 + Q^3}{P + Q} = P^2 + Q^2 - PQ \equiv 2 - 5 \equiv 5 \not\equiv 3c_2^N \equiv 3 \pmod 8.$$

Finally, if $N \geq 3$, the equation $P^3 + Q^3 = 2c^N$ has no solution because, by Lemma 2.4,

$$P^3 + Q^3 < (P + Q)^3 \leq \left(\frac{PQ + 1}{2}\right)^3 = c^3 < 2c^3 \leq 2c^N.$$ □

https://doi.org/10.1017/S0004972718000369 Published online by Cambridge University Press

Lemma 2.6. *Suppose that $n = 2N$, where N is a positive integer. If one of the following conditions is satisfied, then Terai's conjecture is true:*

(i) $2c - 1 = p^s$, *where p is a prime;*

(ii) $P^m + Q^m = 2c^N$ *has no solution for $m > 1$, where $PQ = 2c-1, 3 \le P < Q$ and* $\gcd(P, Q) = 1$.

Proof. (i) As in part (ii) of the proof of Lemma 2.5, from $x^2 + (2c-1)^m = c^{2N}$, we have $c^N - x = 1$ and $c^N + x = (2c-1)^m$, which gives

$$(2c-1)^m + 1 = 2c^N. \tag{2.2}$$

If $m = 1$, (2.2) gives $N = 1$ and the solution $(x, m, n) = (c-1, 1, 2)$ to (2.2). If $m = 2$, then $2c^2 < (2c-1)^2 + 1 < 2c^3$ implies that (2.2) has no solution. If $m \ge 3$, then (2.2) has no solution by Lemma 2.3.

(ii) Suppose $x^2 + (2c-1)^m = c^{2N}$. As in (i), if $c^N - x = 1$ and $c^N + x = (2c-1)^m$, then $(2c-1)^m + 1 = 2c^N$ and, if $c^N - x = P^m, c^N + x = Q^m$, with $PQ = 2c-1$, $3 \le P < Q$ and $\gcd(P, Q) = 1$, then

$$P^m + Q^m = 2c^N. \tag{2.3}$$

As in (i), the equation $(2c-1)^m + 1 = 2c^N$ has no solution for $m > 1$. By assumption, (2.3) has no solution for $m > 1$. If $m = 1$, then $P + Q \le (PQ+1)/2 = c < 2c^N$ by Lemma 2.4, so again (2.3) has no solution. Hence, Terai's conjecture is true. □

Remark 2.7. In the case $2c - 1 = p^s$, to prove Terai's conjecture, we need only prove that $n = 2N$ by Lemma 2.6(i). In the case $2c - 1 \neq p^s$, from the proof of Lemma 2.6(ii), we see that (2.3) has no solution for $m = 1$ and $(2c-1)^m + 1 = 2c^N$ has only one solution. Therefore, in the case $2c - 1 \neq p^s$, to prove Terai's conjecture, we need only prove that $n = 2N$ and that (2.3) has no solution for $m > 1$. Under some circumstances, we can prove that (2.3) has no solution without assuming that $m > 1$ (see the proof of Theorem 1.1(iii) and the proofs of Theorem 1.3(i), (ii) and (iv)).

3. Proof of the main results

Proof of Theorem 1.1. By Lemma 2.5(i), m is odd and $n = 2N$ is even.

For part (i), the result follows from Lemma 2.6(i).

For part (ii), by Remark 2.7, we only need to prove that

$$P^m + Q^m = 2c^N, \quad P = 8k + 3, Q = 8l + 7 \tag{3.1}$$

has no solution for $m > 1$, where $PQ = 2c - 1, P \ge 3, Q \ge 3$ and $\gcd(P, Q) = 1$. By interchanging P and Q, if necessary, we can suppose that $P < Q$. By taking (3.1) modulo 8, we see that N is even. By Lemma 2.1, we get $m \le 3$. But $m > 1$, so this gives $m = 3$ and (3.1) has no solution by Lemma 2.5(ii). Therefore, (3.1) has no solution for $m > 1$.

For part (iii), we will prove that

$$P^m + Q^m = 2c^N, \quad P = 8k + 1, Q = 8l + 5 \tag{3.2}$$

https://doi.org/10.1017/S0004972718000369 Published online by Cambridge University Press

has no solution, where $PQ = 2c - 1, P \geq 3, Q \geq 3$ and $\gcd(P, Q) = 1$. We consider three cases.

Case 1. If there is an odd prime q such that $q \mid (P + Q)$ and $q \nmid c$, then (3.2) clearly has no solution.

Case 2. By assumption,

$$PQ = 2c - 1 = (8k + 1)(8l + 5) \tag{3.3}$$

and there is a prime q with $q \equiv 3 \pmod 4$ or $q \equiv 5 \pmod 8$ such that

$$8k + 1 \equiv 0 \pmod q \quad \text{and} \quad \left(\frac{8l + 5}{q}\right) = -1. \tag{3.4}$$

If $q \equiv 3$ or $5 \pmod 8$, from (3.3),

$$\left(\frac{2c}{q}\right) = \left(\frac{2}{q}\right) \cdot \left(\frac{c}{q}\right) = -\left(\frac{c}{q}\right) = \left(\frac{1}{q}\right) = 1 \quad \Longrightarrow \quad \left(\frac{c}{q}\right) = -1.$$

Taking (3.2) modulo q and using (3.4),

$$-1 = \left(\frac{8l + 5}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{c}{q}\right)^N = (-1)^{N+1}.$$

Therefore, N is even. Taking (3.2) modulo 8 gives the contradiction

$$P^m + Q^m \equiv 6 \not\equiv 2c^N \equiv 2 \pmod 8,$$

so (3.2) has no solution.

If $q \equiv 7 \pmod 8$, from (3.3),

$$\left(\frac{2c}{q}\right) = \left(\frac{2}{q}\right) \cdot \left(\frac{c}{q}\right) = \left(\frac{1}{q}\right) = 1 \quad \Longrightarrow \quad \left(\frac{c}{q}\right) = -1.$$

Taking (3.2) modulo q and using (3.4),

$$\left(\frac{P^m + Q^m}{q}\right) = \left(\frac{8l + 5}{q}\right) = -1 = \left(\frac{2c^N}{q}\right) = 1$$

which is impossible.

Case 3. By assumption, (3.3) holds and there is a prime $q \equiv 3 \pmod 4$ or $q \equiv 5 \pmod 8$ such that

$$8l + 5 \equiv 0 \pmod q \quad \text{and} \quad \left(\frac{8k + 1}{q}\right) = -1.$$

Proceeding as in Case 2, we similarly prove that (3.2) has no solution.

This completes the proof of Theorem 1.1. □

https://doi.org/10.1017/S0004972718000369 Published online by Cambridge University Press

Proof of Theorem 1.2. By Lemma 2.5(i), m is odd and $n = 2N$ is even. By Remark 2.7, we consider

$$P^m + Q^m = 2c^N, \tag{3.5}$$

where $PQ = 2c - 1, 3 \le P < Q$ and $\gcd(P, Q) = 1$. Since $PQ = 2c - 1 \equiv 5 \pmod 8$, we see that $P + Q$ must have an odd prime factor; therefore, by Lemma 2.3, if $m > 1$, it follows that $P^m + Q^m$ has at least two different odd prime factors. Hence, (3.5) has no solution for $m > 1$. □

Proof of Theorem 1.3. We consider the five parts of the theorem in turn. In each case, by Remark 2.7, we need only consider (3.5), where $PQ = 2c - 1, P \ge 3, Q \ge 3$ and $\gcd(P, Q) = 1$.

(i) From $2c - 1 = 3^{2s+1}p^{2t+1}$, we get $c \equiv 2 \pmod 3$ and $1 \equiv x^2 \equiv c^n \pmod 3$, so $n = 2N$. We consider (3.5) with $P = 3^{2s+1}, Q = p^{2t+1}$.

If $p \equiv 7 \pmod 8$, then, from $PQ = 2c - 1 \equiv 5 \pmod 8$, we deduce that $c \equiv 3 \pmod 4$. By Theorem 1.1(ii), Terai's conjecture is true.

Now consider $p \equiv 3 \pmod{16}$. In this case, $c \equiv 5 \pmod 8$. Taking (3.5) modulo 16 gives $2 \cdot 3^m \equiv 2 \cdot 5^N \pmod{16}$, which means that $m \equiv N \equiv 0 \pmod 2$. But, taking (3.5) modulo 3 leads to the contradiction $1 \equiv P^m + Q^m = 2c^N \equiv 2 \pmod 3$. So, (3.5) has no solution.

(ii) Let $2c - 1 = PQ$, where $P = 3^{4s+1}, Q = p^{4t+1}$. If $p \equiv 5 \pmod{16}$, then $c \equiv 0 \pmod 8$, so $2c^N \equiv 0 \pmod{16}$. But $P^m + Q^m \equiv 2 \pmod 8$ if m is even, and $P^m + Q^m \equiv 8 \pmod{16}$ if m is odd. If $p \equiv 3 \pmod 5$, then $c \equiv 0 \pmod 5$ and, by taking (3.5) modulo 5, we get the contradiction $2 \cdot 3^m \equiv 2 \cdot c^N \equiv 0 \pmod 5$.

(iii) From $2c - 1 = 5^{2s+1}p^{2s+1}$ with $p \equiv 3 \pmod 8$, we deduce that $c \equiv 3 \pmod 5$ and $c \equiv 0 \pmod 4$. Taking (1.1) modulo 4 and 5 in turn gives $2 \nmid m$ and $2 \mid n$. Let $n = 2N$ and $P = 5^{2s+1}, Q = p^{2s+1}$. Since $(p + 5) \not\equiv 0 \pmod{32}, c \equiv 0 \pmod 4$ and $(5 + p) \mid (P^m + Q^m)$, we must have $N = 1$. If $m > 1$, then

$$P^m + Q^m \ge P^3 + Q^3 > 2PQ = 4c - 2 > 2c,$$

which is a contradiction. Thus, (3.5) with $P = 5^{2s+1}, Q = p^{2s+1}$ has no solution for $m > 1$.

(iv) From $2c - 1 = 9^{2^s}p^{2t+1}$, we obtain $3 \nmid c, p \nmid c$ and $2c - 1 \equiv 5 \pmod 8$; hence, $c \equiv 3 \pmod 4$. Taking (1.1) modulo c and 3 in turn gives $2 \nmid m$ and $2 \mid n$. Let $n = 2N$ and $P = 9^{2^s}, Q = p^{2t+1}$. We prove that (3.5) has no solution.

Since $\frac{1}{2}(P + Q) \equiv 3 \pmod 4$, there must be a prime q such that $q \equiv 3 \pmod 4$ and $P + Q \equiv 0 \pmod q$. Thus, $PQ \equiv -P^2 \pmod q$. On the other hand, $P + Q \equiv 0 \pmod q$, so $2c^N = P^m + Q^m = (P + Q)((P^m + Q^m)/(P + Q)) \equiv 0 \pmod q$ and $2c \equiv 0 \pmod q$. Hence,

$$2c = PQ + 1 \equiv -P^2 + 1 \equiv P^2 - 1 \equiv 0 \pmod q,$$

that is, $q \mid P^2 - 1$. Since

$$P^2 - 1 = (9^{2^s} - 1)(9^{2^s} + 1) = (9^2 - 1)(9^2 + 1) \cdots (9^{2^{s-1}} + 1)(9^{2^s} + 1)$$

https://doi.org/10.1017/S0004972718000369 Published online by Cambridge University Press

and $q \nmid (9-1)(9+1)$, there must be an integer i with $1 \le i \le s$ such that $q \mid (9^{2^i}+1)$. But this gives the contradiction

$$1 = \left(\frac{9^{2^i}}{q}\right) = \left(\frac{-1}{q}\right) = -1.$$

(v) By Terai's result in [6, Proposition 3.3], we can suppose that $s \ge 5$. Suppose first that $s = 2t$. Since $x^2 \equiv 1 \pmod 4$ and $2c - 1 \equiv 0 \pmod 3$, taking (1.1) modulo 4 and modulo 3 respectively gives $2 \nmid m$ and $n = 2N$. So, we have the equation

$$P^m + Q^m = 2c^N = 2 \cdot 2^{2tN}, \tag{3.6}$$

where $PQ = 2c - 1 = 2^{2t+1}, 3 \le P < Q$ and $\gcd(P, Q) = 1$.

If $2^{2t+1} - 1 = p^r$, Terai's conjecture is true by Lemma 2.6(i). If $2^{2t+1} - 1 \neq p^r$, we need to prove that (3.6) has no solution for $m > 1$. Since $m > 1$ and m, P and Q are odd, then, from Lemma 2.3, $P^m + Q^m$ has a prime factor $p \neq 2$. So, (3.6) has no solution for $m > 1$ and Terai's conjecture is true by Lemma 2.6(ii).

Now suppose that $s = 2t - 1$. Since $x^2 \equiv 1 \pmod 4$ and $2c - 1 \equiv 0 \pmod 3$, taking (1.1) modulo 4 gives $2 \nmid m$. Note that $2c - 1 = 2^{2t} - 1 \neq p^r$. So, similar to the proof in the case of $s = 2t$, we can show that Terai's conjecture is true.

This completes the proof of Theorem 1.3. □

Proof of Corollary 1.4. By the results obtained in [6] and [4], we may suppose that $31 \le c \le 499$ with $c \equiv 3 \pmod 4$.

For $c = p^{2s+1}$, where p is a prime, $p \equiv 3 \pmod 4$, $s \ge 0$ and $31 \le p^{2s+1} \le 499$, that is, $c \in \{31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199, 223, 227, 239, 243\,(= 3^5), 251, 263, 271, 283, 307, 311, 331, 343\,(= 7^3), 347, 359, 367, 379, 383, 419, 431, 439, 443, 463, 467, 479, 487, 491, 499\}$, we see that Terai's conjecture is true by Theorem 1.2.

For $c \in \{51, 55, 63, 75, 87, 91, 99, 115, 135, 147, 159, 175, 187, 195, 211, 231, 255, 279, 327, 339, 351, 355, 387, 399, 411, 415, 427, 471\}$, since $2c - 1$ is a power of a prime, the same conclusion follows from Theorem 1.1(i).

For $c \in \{35, 39, 95, 119, 155, 171, 207, 219, 235, 259, 287, 291, 295, 299, 335, 375, 391, 395, 407, 435, 447, 459, 495\}$, since $2c - 1 = (8k + 3)(8l + 7)$, the conclusion follows from Theorem 1.1(ii).

For $c \in \{111, 123, 183, 203, 247, 267, 275, 303, 315, 319, 423, 451, 455, 475, 483\}$, since $2c - 1 = (8s + 1)(8t + 5)$, the conclusion follows from Theorem 1.1(iii). For example, take $c = 275$, so that $2c - 1 = 3^2 \cdot 61$. Set $P = 3^2, Q = 61$. Then Theorem 1.1(iii) applies because $(\frac{9}{61}) = (\frac{61}{3}) = 1$ and $7 \mid P + Q, 7 \nmid c$.

For $c \in \{143, 215, 323, 371, 403\}$, we have $2c - 1 = p_1 p_2 p_3$ and Terai's conjecture is true by Theorem 1.1(ii) and (iii). For example, $c = 143$ implies that $2c - 1 = 3 \cdot 5 \cdot 19$. If we take $P = 3, Q = 95$ or $P = 15, Q = 19$, then $2c - 1 = (8k + 3)(8l + 7)$ and Terai's conjecture follows by Theorem 1.1(ii). If we take $P = 5, Q = 57$, then $2c - 1 = (8s + 1)(8t + 5)$ and $(\frac{57}{5}) = -1$ and Terai's conjecture follows by Theorem 1.1(iii).

https://doi.org/10.1017/S0004972718000369 Published online by Cambridge University Press

Finally, suppose that $c = 3 \cdot 11^2 = 363$. Then $2c - 1 = 25 \cdot 29$, so, by Lemma 2.5(i), m is odd and $n = 2N$ is even. Consider the equation

$$25^m + 29^m = 2 \cdot 363^N = 2 \cdot 3^N \cdot 11^{2N}. \tag{3.7}$$

Taking (3.7) modulo 11 gives $m = 5(2s+1)$, so $(25^5 + 29^5) \mid (25^m + 29^m)$. But $50971 \mid (25^5 + 29^5)$, so (3.7) has no solution.

This completes the proof of Corollary 1.4. □

Acknowledgement

The authors sincerely thank the referees for their detailed comments.

References

[1] S. A. Arif and F. S. Abu Muriefah, 'On the Diophantine equation $x^2 + q^{2k+1} = y^n$', *J. Number Theory* **95** (2002), 95–100.

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

[3] R. D. Carmichael, 'On the numerical factor of the arithmetic forms $\alpha^n \pm \beta^n$', *Ann. Math.* **15** (1913), 30–70.

[4] M.-J. Deng, 'A note on the Diophantine equation $x^2 + q^m = c^{2n}$', *Proc. Japan Acad.* **91** (2015), 15–18.

[5] W. Ljunggren, 'Some theorems on indeterminate equations of the form $(x^n - 1/x - 1) = y^q$', *Norsk Mat. Tidsskr.* **25** (1943), 17–20; (in Norwegian).

[6] N. Terai, 'A note on the Diophantine equation $x^2 + q^m = c^n$', *Bull. Aust. Math. Soc.* **90** (2014), 20–27.

[7] H. L. Zhu, 'A note on the Diophantine equation $x^2 + q^m = y^3$', *Acta Arith.* **146** (2011), 195–202.

MOU-JIE DENG, Department of Applied Mathematics,
Hainan University, Haikou, Hainan 570228, PR China
e-mail: moujie_deng@163.com

JIN GUO, Department of Applied Mathematics,
Hainan University, Haikou, Hainan 570228, PR China
e-mail: guojinecho@163.com

AI-JUAN XU, Department of Applied Mathematics,
Hainan University, Haikou, Hainan 570228, PR China
e-mail: xaj1650404852@163.com