Bull. Aust. Math. Soc. **91** (2015), 11–18
doi:10.1017/S0004972714000719

ON EXPONENTIAL DIOPHANTINE EQUATIONS CONTAINING THE EULER QUOTIENT

NOBUHIRO TERAI

(Received 22 February 2014; accepted 24 August 2014; first published online 14 October 2014)

Abstract

Let a and m be relatively prime positive integers with $a > 1$ and $m > 2$. Let $\phi(m)$ be Euler's totient function. The quotient $E_m(a) = (a^{\phi(m)} - 1)/m$ is called the *Euler quotient* of m with base a. By Euler's theorem, $E_m(a)$ is an integer. In this paper, we consider the Diophantine equation $E_m(a) = x^l$ in integers $x > 1, l > 1$. We conjecture that this equation has exactly five solutions (a, m, x, l) except for $(l, m) = (2, 3), (2, 6)$, and show that if the equation has solutions, then $m = p^s$ or $m = 2p^s$ with p an odd prime and $s \geq 1$.

2010 *Mathematics subject classification*: primary 11D61.

Keywords and phrases: exponential Diophantine equations, Fermat quotient, Euler quotient, integer solutions.

1. Introduction

Let p be an odd prime and a a positive integer prime to p. The quotient

$$Q_p(a) = \frac{a^{p-1} - 1}{p}$$

is called the *Fermat quotient* of p with base a. By Fermat's little theorem, $Q_p(a)$ is an integer. Lucas [Lu] proved that $Q_p(2)$ is a square only for $p = 3$ and 7 (see also Dickson [D, Ch. IV, page 106]). To generalise Lucas' theorem, in the previous papers [OT, T], we studied the Diophantine equation

$$Q_p(a) = x^l \tag{1.1}$$

in integers $x > 1, l > 1$. In particular, we completely solved three cases of (1.1):

$$Q_p(a) = x^2, \quad Q_p(r) = x^r, \quad Q_p(2) = x^l,$$

where r is an odd prime. Le [Le] showed that if $p \equiv 1 \pmod 4$ and $p > 4 \cdot 10^{176}$, then equation (1.1) has no solutions with $l > 2$. Cao [Ca] improved Le's result by showing that if $p \equiv 1 \pmod 4$, then (1.1) has no solutions with $l > 2$. Moreover, Cao [Ca] proved that if $p \equiv 1 \pmod 4$, then the equation

$$Q_p(a) = 2^n x^l$$

has only the solution $(a, p, n, x, l) = (3, 5, 1, 2, 3)$ with $l > 2$ and $n \geq 1$. Kihel and Levesque [KL] also established similar results.

Let a and m be relatively prime positive integers with $a > 1$ and $m > 2$. Let $\phi(m)$ be Euler's totient function. The quotient

$$E_m(a) = \frac{a^{\phi(m)} - 1}{m}$$

is called the *Euler quotient* of m with base a. (See Agoh *et al.* [ADS] for more on Fermat quotients and Euler quotients.) By Euler's theorem, $E_m(a)$ is an integer. In the case where $m = p$ is an odd prime, we have $E_m(a) = Q_p(a)$.

In this paper, we consider the Diophantine equation

$$E_m(a) = x^l \tag{1.2}$$

in integers $x > 1, l > 1$. When $(l, m) = (2, 3)$ or $(2, 6)$, (1.2) becomes

$$a^2 - 3x^2 = 1 \quad \text{or} \quad a^2 - 6x^2 = 1,$$

respectively. Since the above equations are Pell equations, there are infinitely many positive integer solutions a, x in each case. From now on, the cases

$$(l, m) = (2, 3), (2, 6)$$

are eliminated as 'exceptional cases'. As an analogue to the results for (1.1) containing Fermat quotients, we propose the following conjecture.

Conjecture 1.1. After eliminating 'exceptional cases' with $(l, m) = (2, 3)$ and $(2, 6)$, (1.2) has only the solutions $(a, m, x, l) = (2, 7, 3, 2), (3, 5, 4, 2), (3, 10, 2, 3), (5, 3, 2, 3), (7, 6, 2, 3)$.

The following theorems are the main results of this paper.

Theorem 1.2. *Suppose that a is even. After eliminating 'exceptional cases' with $(l, m) = (2, 3)$ and $(2, 6)$, (1.2) has only the solution $(a, m, x, l) = (2, 7, 3, 2)$.*

Theorem 1.3. *After eliminating 'exceptional cases' with $m = 3$ and 6, the Diophantine equation*

$$E_m(a) = x^2 \tag{1.3}$$

has only the solutions $(a, m, x) = (2, 7, 3), (3, 5, 4)$.

Theorem 1.4. *Suppose that m has at least two odd prime divisors or $m \equiv 0 \pmod 4$. Then (1.2) has no solutions.*

The following corollary is an immediate consequence of Theorems 1.2–1.4.

Corollary 1.5. *If (1.2) has solutions, then $m = p^s$ or $m = 2p^s$ with p an odd prime and $s \geq 1$.*

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press

This paper is organised as follows. In Section 2 we state several lemmas concerning exponential Diophantine equations such as

$$x^m - y^n = 1, \quad x^l \pm 1 = 2y^2, \quad x^2 + 1 = 2y^l,$$

with $m > 1$, $n > 1$ and $l > 2$. In Sections 3–5 we give the proofs of Theorems 1.2–1.4, respectively. Our method is to reduce equation (1.2) to deep results concerning the above equations due to Mihailescu [M] and Benett and Skinner [BS], by comparing a certain factorisation of $a^{\phi(m)} - 1$ with relatively prime factors and the prime factorisation of m. In Section 6, using the results of Cao [Ca], we show that if m has no prime divisor p of the form $p \equiv 3 \pmod 4$ and $l > 2$, then (1.2) has only the solution $(a, m, x, l) = (3, 10, 2, 3)$.

2. Preliminaries

We use the following lemmas to prove our Theorems 1.2–6.1.

Lemma 2.1 (Cohn [Co]). *The Diophantine equation*

$$x^4 - Dy^2 = 1 \quad (D = 5, 10, 15, 30)$$

has only the positive integer solution $(x, y) = (3, 4)$ *if* $D = 5$, $(x, y) = (2, 1)$ *if* $D = 15$, *and no solutions if* $D = 10, 30$, *respectively.*

The following result is well known (cf. Nagell [N, Ch. VII, pages 229–230]).

Lemma 2.2 (Nagell [N]). *The Diophantine equation*

$$x^4 \pm 1 = 2y^2$$

has no positive integer solutions x, y *with* $xy > 1$.

In Lemma 2.3, the case $l > 4$ follows from [BVY, Theorem 1.5]. Note that the cases $l = 3, 4$ can be easily solved by Magma [BC].

Lemma 2.3 (Bennett *et al.* [BVY]). *Let* l *be a positive integer with* $l \geq 3$. *Then the Diophantine equation*

$$|x^l - 3y^l| = 2$$

has no integer solutions x, y *with* $|xy| > 1$.

The following result resolves Catalan's conjecture, which is one of the famous classical problems in number theory.

Lemma 2.4 (Mihailescu [M]). *Let* x, y, m, n *be positive integers with* $x, y, m, n > 1$. *Then the Diophantine equation*

$$x^m - y^n = 1$$

has only the positive integer solution $(x, y, m, n) = (3, 2, 2, 3)$.

Lemma 2.5 (Bennett and Skinner [BS]). *Let* l *be a positive integer with* $l \geq 3$.

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press

(i) *The Diophantine equation*

$$x^l + 1 = 2y^2$$

has only the positive integer solutions $(x, y, l) = (1, 1, l), (23, 78, 3)$.

(ii) *The Diophantine equation*

$$x^l - 1 = 2y^2$$

has only the positive integer solution $(x, y, l) = (3, 11, 5)$.

Lemma 2.6.

(i) (Störmer [S]) *The Diophantine equation*

$$x^2 + 1 = 2y^l$$

has no solutions in integers $x > 1$*,* $y \geq 1$ *and* l *odd* ≥ 3.

(ii) (Ljunggren [Lj]) *The Diophantine equation*

$$x^2 + 1 = 2y^4$$

has only the positive integer solution $(x, y) = (1, 1), (239, 13)$.

3. Proof of Theorem 1.2

Let (x, y, z) be a solution of (1.2). Suppose that a is even.

When $m = 3$, (1.2) becomes

$$a^2 - 1 = 3x^l.$$

Since a is even, we have the following two cases:

$$\begin{cases} a + 1 = x_1^l \\ a - 1 = 3x_2^l \end{cases} \quad \text{or} \quad \begin{cases} a + 1 = 3x_1^l \\ a - 1 = x_2^l, \end{cases}$$

where x_1 and x_2 are positive integers with $x = x_1x_2$. Subtracting the two equations in each pair yields

$$|X^l - 3Y^l| = 2,$$

where $X = x_1, Y = x_2$ or $X = x_2, Y = x_1$. It follows from Lemma 2.3 that the above equation has no positive integer solutions with $|XY| > 1$. We may thus suppose that $m > 3$.

Write the factorisation of an odd m as

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where the p_k for $1 \leq k \leq r$ are distinct odd primes such that $3 \leq p_i < p_j$ with $1 \leq i < j \leq r$ and the e_k for $1 \leq k \leq r$ are positive integers. Then

$$\phi(m) = p_1^{e_1-1} p_2^{e_2-1} \cdots p_r^{e_r-1}(p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press

Note that $\phi(m) \equiv 0 \pmod{2^r}$, and

$$\phi(m)/2^r > 1 \iff m > 3.$$

Now (1.2) can be written as

$$(A^{2^{r-1}} + 1)(A^{2^{r-2}} + 1) \cdots (A^2 + 1)(A + 1)(A - 1) = mx^l, \tag{3.1}$$

where A is a power of the form

$$A = a^{\phi(m)/2^r}.$$

Since a is even, the factors of the left-hand side of (3.1) are pairwise relatively prime. Furthermore, the number of distinct prime divisors of m is r, while the number of (relatively prime) factors of the left-hand side of (3.1) is $r + 1$. We therefore conclude that

$$A^{2^k} + 1 = x_0^l \tag{3.2}$$

or

$$A - 1 = x_0^l \tag{3.3}$$

for some integer k with $0 \leq k \leq r - 1$ and $x_0|x$. It follows from Lemma 2.4 that (3.2) has only the solution $(A, k, x_0, l) = (2^3, 0, 3, 2)$ and (3.3) has no solutions. Consequently we obtain $(a, m, x, l) = (2, 7, 3, 2)$. □

4. Proof of Theorem 1.3

Let (x, y, z) be a solution of (1.3). If a is even, then it follows from Theorem 1.2 that (1.3) has only the solution $(a, m, x) = (2, 7, 3)$. We may thus suppose that a is odd.

We now follow the notation and the line of proof of Theorem 1.2. Since a is odd, either m or x is even. Write the factorisation of m as

$$m = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where the p_k for $1 \leq k \leq r$ are distinct odd primes and e_0 is a nonnegative integer. Note that

$$\phi(m)/2^r > 2 \iff m \neq 3, 5, 6, 10, 15, 30.$$

If $m = 5, 10, 15, 30$, then it follows from Lemma 2.1 that (1.3) has only the solution $(a, m, x) = (3, 5, 4)$. Since $l = 2$, the cases $m = 3, 6$ can be eliminated by our assumption. We may thus suppose that $m \neq 3, 5, 6, 10, 15, 30$. Now (1.3) can be written as

$$(A^{2^{r-1}} + 1)(A^{2^{r-2}} + 1) \cdots (A^2 + 1)(A + 1)(A - 1) = 2^s p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} x_1^2, \tag{4.1}$$

where A is a power of the form $A = a^{\phi(m)/2^r}$ with $\phi(m)/2^r > 2$ and s is a positive integer. (Define x_1 by $x = 2x_1$ if m is odd, and $x = x_1$ if m is even.) Since a is odd, the greatest common divisor of the factors of the left-hand side of (4.1) is equal to 2. As in the proof of Theorem 1.2, we therefore conclude that

$$A^{2^k} + 1 = 2^{s_0} x_0^2 \tag{4.2}$$

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press

or

$$A - 1 = 2^{s_0} x_0^2 \tag{4.3}$$

for some integer k with $0 \le k \le r - 1$, $s_0 = 1, 2$ and $x_0 | 2x_1$. It follows from Lemmas 2.2, 2.4, 2.5 that (4.2) has only the solution $(A, k, s_0, x_0) = (23^3, 0, 1, 78)$, and (4.3) has only the solution $(A, s_0, x_0) = (3^5, 1, 11)$. But these yield no solutions of (1.3). □

5. Proof of Theorem 1.4

Let (x, y, z) be a solution of (1.2). By Theorems 1.2 and 1.3, we may suppose that a is odd and $l \ge 3$. We now follow the notation and the line of the proof of Theorem 1.2.

First consider the case where m has at least two odd prime divisors. Since a is odd, either m or x is even. Write the factorisation of m as

$$m = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where the p_k for $1 \le k \le r$ are distinct odd primes and e_0 is a nonnegative integer. Now (1.2) can be written as

$$(A^{2^{r-1}} + 1)(A^{2^{r-2}} + 1) \cdots (A^2 + 1)(A + 1)(A - 1) = 2^s p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} x_1^l,$$

where $A = a^{\phi(m)/2^r}$ and s is a positive integer. (Define x_1 by $x = 2x_1$ if m is odd, and $x = x_1$ if m is even.) Note that for $k \ge 1$ and two odd primes p, q with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, we have

$$A^{2^k} + 1 \not\equiv 0 \pmod 4, \quad A^{2^k} + 1 \not\equiv 0 \pmod q, \quad p - 1 \equiv 0 \pmod 4.$$

Using these properties, we conclude that

$$A^{2^k} + 1 = 2x_0^l \tag{5.1}$$

for some integer k with $1 \le k \le r - 1$ and $x_0 | x_1$. It follows from Lemma 2.6 that (5.1) has no solutions.

Next consider the case where $m \equiv 0 \pmod 4$. When $m = 4$, (1.2) becomes

$$a^2 - 1 = 4x^l.$$

This implies that $a + 1 = 2x_1^l$ and $a - 1 = 2x_2^l$, and hence $1 = x_1^l - x_2^l$, which is impossible. Thus, $m = 2^s$ with $s \ge 3$ or $m = 4m_0$ with m_0 odd > 1. Then, as above, (1.2) can be reduced to solving (5.1). Therefore, (1.2) has no solutions. □

6. The case where $m = p^s$ or $m = 2p^s$

It follows from Corollary 1.5 that if (1.2) has solutions, then $m = p^s$ or $m = 2p^s$ with p an odd prime and $s \ge 1$.

Suppose that $m = p^s$. Then (1.2) becomes

$$(A^{p^{s-2}} - 1) \cdot \frac{A^{p^{s-1}} - 1}{A^{p^{s-2}} - 1} = p^s x^l$$

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press

with $A = a^{p-1}$. Recall that $\gcd(c-1, (c^p-1)/(c-1)) = p$ and $(c^p-1)/(c-1) \equiv p \pmod{p^2}$, for an odd prime p and a positive integer c with $c - 1 \equiv 0 \pmod{p}$. Since $A - 1 = a^{p-1} - 1 \equiv 0 \pmod{p}$ from Fermat's little theorem, we obtain

$$A^{p^{s-2}} - 1 = p^{s-1}x_1^l, \qquad \frac{A^{p^{s-1}} - 1}{A^{p^{s-2}} - 1} = px_2^l,$$

with $x_1x_2 = x$. Repeating this, (1.2) with $m = p^s$ can be reduced to solving

$$a^{p-1} - 1 = pu^l \tag{6.1}$$

with $x \equiv 0 \pmod{u}$. Similarly, the case $m = 2p^s$ also yields the equation

$$a^{p-1} - 1 = 2pu^l, \tag{6.2}$$

since $(A^{p^j} - 1)/(A^{p^{j-1}} - 1)$ is odd. By the results of Cao [Ca], we see that if $p \equiv 1 \pmod{4}$ and $l > 2$, then (6.1) has no solutions, and (6.2) has only the solution $(a, p, u, l) = (3, 5, 2, 3)$. To sum up, we have shown the following result.

THEOREM 6.1. *Suppose that m has no prime divisor p of the form $p \equiv 3 \pmod{4}$ and $l > 2$. Then (1.2) has only the solution $(a, m, x, l) = (3, 10, 2, 3)$.*

REMARK 6.2. In general, it is difficult to solve (6.1) and (6.2) when $p \equiv 3 \pmod{4}$ (cf. Cao [Ca] and Le [Le]). But for $(l, m) = (3, 3), (3, 6)$, (6.1) and (6.2) can be reduced to the following elliptic curves and so can be easily solved by Magma:

$$E_9 : Y^2 = X^3 + 9$$

with $X = 3u$ and $Y = 3a$, and $\operatorname{rank} E_9(\mathbb{Q}) = 1$ and all integer points on E_9 are $(X, Y) = (-2, \pm 1), (0, \pm 3), (3, \pm 6), (6, \pm 15), (40, \pm 253)$;

$$E_{36} : Y^2 = X^3 + 36$$

with $X = 6u$ and $Y = 6a$, and $\operatorname{rank} E_{36}(\mathbb{Q}) = 1$ and all integer points on E_{36} are $(X, Y) = (-3, \pm 3), (0, \pm 6), (4, \pm 10), (12, \pm 42)$. Consequently, (1.2) with $(l, m) = (3, 3)$, (3,6) has only the solutions $(a, m, x, l) = (5, 3, 2, 3)$, $(7, 6, 2, 3)$, respectively. These are fourth and fifth solutions listed in Conjecture 1.1.

References

[ADS] T. Agoh, K. Dilcher and L. Skula, 'Fermat quotients for composite moduli', *J. Number Theory* **66** (1997), 29–50.

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

[BVY] M. A. Bennett, V. Vatsal and S. Yazdani, 'Ternary Diophantine equations of signature $(p, p, 3)$', *Compositio Math.* **140** (2004), 1399–1416.

[BC] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, available online at http://magma.maths.usyd.edu.au/magma/.

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

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press

[Co] J.H.E. Cohn, 'The Diophantine equations $x^4 - Dy^2 = 1$, II', *Acta Arith.* **78** (1996/1997), 401–403.

[D] L.E. Dickson, *History of the Theory of Numbers,* Vol. I (Chelsea, New York, 1971).

[KL] O. Kihel and C. Levesque, 'On a few Diophantine equations related to Fermat's last theorem', *Canad. Math. Bull.* **45** (2002), 247–256.

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

[Lj] W. Ljunggren, 'Zur Theorie der Gleichung $x^2 + 1 = Dy^4$', *Avh. Norske Vid. Akad. Oslo* **5** (1942), 1–27.

[Lu] E. Lucas, *Théorie des nombres* (Gauthier-Villars, Paris, 1891), reprinted (A. Blanchard, Paris, 1961).

[M] P. Mihilescu, 'Primary cyclotomic units and a proof of Catalan's conjecture', *J. reine angew. Math.* **572** (2004), 167–195.

[N] T. Nagell, *Introduction to Number Theory*, 2nd edn (Chelsea, New York, 1964).

[OT] H. Osada and N. Terai, 'Generalization of Lucas' Theorem for Fermat's quotient', *C. R. Math. Rep. Acad. Sci. Can.* **11** (1989), 115–120.

[S] C. Störmer, 'L'équation $m \arctan 1/x + n \arctan 1/y = k\pi/4$', *Bull. Soc. Math. France* **27** (1899), 160–170.

[T] N. Terai, 'Generalization of Lucas' Theorem for Fermat's quotient II', *Tokyo J. Math.* **13** (1990), 277–287.

NOBUHIRO TERAI, Department of Computer Science
and Intelligent Systems, Faculty of Engineering,
Oita University, 700 Dannoharu, Oita 870-1192,
Japan
e-mail: terai-nobuhiro@oita-u.ac.jp

https://doi.org/10.1017/S0004972714000719 Published online by Cambridge University Press