A REMARK ON A PAPER OF LUCA AND WALSH[1]

Zhao-Jun Li
Department of Mathematics, Anhui Normal University, Wuhu, China

Min Tang[2]
Department of Mathematics, Anhui Normal University, Wuhu, China
tmzzz2000@163.com

Received: 7/5/10, Revised: 3/27/11, Accepted: 5/12/11, Published: 6/8/11

Abstract

In 2002, F. Luca and P. G. Walsh studied the diophantine equations of the form $(a^k-1)(b^k-1)=x^2$, for all (a,b) in the range $2 \le b < a \le 100$ with sixty-nine exceptions. In this paper, we solve two of the exceptions. In fact, we consider the equations of the form $(a^k-1)(b^k-1)=x^2$, with $(a,b)=(13,4),(28,13)$.

1. Introduction

In 2000, Szalay [5] determined that the diophantine equation $(2^n-1)(3^n-1)=x^2$ has no solutions in positive integers n and x, $(2^n-1)(5^n-1)=x^2$ has only one solution $n=1, x=2$, and $(2^n-1)((2^k)^n-1)=x^2$ has only one solution $k=2, n=3, x=21$. In 2000, Hajdu and Szalay [1] proved that the equation $(2^n-1)(6^n-1)=x^2$ has no solutions in positive integers (n,x), while the only solutions to the equation $(a^n-1)(a^{kn}-1)=x^2$, with $a>1, k>1, kn>2$ are $(a,n,k,x)=(2,3,2,21),(3,1,5,22),\ (7,1,4,120)$.

In 2002, F. Luca and P. G. Walsh [4] proved that the Diophantine equation $(a^k-1)(b^k-1)=x^n$ has a finite number of solutions (k,x,n) in positive integers, with $n>1$. Moreover, they showed how one can determine all integer solutions $(k,x,2)$ of the above equation with $k>1$, for almost all pairs (a,b) with $2 \le b < a \le 100$. The sixty-nine exceptional pairs were concisely described:

Theorem A ([4] Theorem 3.1) *Let $2 \le b < a \le 100$ be integers, and assume that (a,b) is not in one of the following three sets:*

[1]This work was supported by the National Natural Science Foundation of China, Grant No 10901002 and the foundation for reserved candidates of 2010 Anhui Province academic and technical leaders

[2]Corresponding author.

1. $\{(22,2);(22,4)\}$;
2. $\{(a,b);(a-1)(b-1)$ *is a square*, $a\equiv b \pmod 2$, *and* $(a,b)\neq(9,3),(64,8)\}$;
3. $\{(a,b);(a-1)(b-1)$ *is a square*, $a+b\equiv 1 \pmod 2$, *and* $ab\equiv 0 \pmod 4\}$.

If $(a^k-1)(b^k-1)=x^2$, *then* $k=2$, *except only for the pair* $(a,b)=(4,2)$, *in which case the only solution to the equation occurs at* $k=3$.

For the other related problems, see [2], [3], [6] and [7].

In this paper, we consider two of the exceptions: $(a,b)=(13,4),(28,13)$ and obtain the following results:

Theorem 1. *The equation*

$$(4^n-1)(13^n-1)=x^2 \tag{1}$$

has only one solution $n=1, x=6$ *in positive integers* n *and* x.

Theorem 2. *The equation*

$$(13^n-1)(28^n-1)=x^2 \tag{2}$$

has only one solution $n=1, x=18$ *in positive integers* n *and* x.

For two relatively prime positive integers a and m, the least positive integer x with $a^x\equiv 1 \pmod m$ is called *the order of* a *modulo* m. We denote the order of a modulo m by $\mathrm{ord}_m(a)$. For an odd prime p and an integer a, let $(\frac{a}{p})$ denote the Legendre symbol.

2. Proofs

Proof of Theorem 1. It is easy to verify that if $n\le 3$ then Eq. (1) has only one solution $n=1, x=6$. Suppose that a pair (n,x) with $n\ge 4$ is a solution of Eq. (1), we consider the following 10 cases.

`Case 1.` $n\equiv 0 \pmod 4$. Then n can uniquely be written in the form $n=4\cdot 5^k l$, where $5\nmid l, k\ge 0$. By induction on k, we have

$$4^{4\cdot 5^k l}\equiv 1+5^{k+1}l \pmod{5^{k+2}}, \tag{3}$$

$$13^{4\cdot 5^k l}\equiv 1+2\cdot 5^{k+1}l \pmod{5^{k+2}}. \tag{4}$$

By the assumption and (3), (4) we have

$$\frac{x^2}{5^{2k+2}}\equiv 2l^2 \pmod 5,$$

thus 2 is a quadratic residue modulo 5, a contradiction.

`Case 2.` $n \equiv 2, 3 \pmod 4$. By $\mathrm{ord}_{16}(13) = 4$, we have $x^2 \equiv (-1)(13^2-1), (-1)(13^3-1) \equiv 8, 12 \pmod{16}$. These are impossible.
`Case 3.` $n \equiv 5 \pmod{12}$. Then $x^2 \equiv (4^5-1)(6^5-1) \equiv 5 \pmod 7$, a contradiction.
`Case 4.` $n \equiv 9 \pmod{12}$. Then $x^2 \equiv (4^9-1)(-1) \equiv 2 \pmod{13}$, a contradiction.
`Case 5.` $n \equiv 1 \pmod{24}$. By $\mathrm{ord}_{32}(13) = 8$, we have $x^2 \equiv (-1)(13-1) \equiv 20 \pmod{32}$. Hence $4|x^2$. Let $x = 2x_1$ with $x_1 \in \mathbb{Z}$. Then $x_1^2 \equiv 5 \pmod 8$. This is impossible.
`Case 6.` $n \equiv 13, 109 \pmod{120}$. Then $n \equiv 3, 9 \pmod{10}$ and $n \equiv 13, 29 \pmod{40}$. By $\mathrm{ord}_{41}(4) = 10$ and $\mathrm{ord}_{41}(13) = 40$, we have $x^2 \equiv (4^3-1)(13^{13}-1), (4^9-1)(13^{29}-1) \equiv 15, 6 \pmod{41}$. These contradict the fact that $\left(\frac{15}{41}\right) = \left(\frac{6}{41}\right) = -1$.
`Case 7.` $n \equiv 37 \pmod{120}$. Then $n \equiv 7 \pmod{30}$ and $n \equiv 1 \pmod 3$. By $\mathrm{ord}_{61}(4) = 30$ and $\mathrm{ord}_{61}(13) = 3$, we have $x^2 \equiv (4^7-1)(13-1) \equiv 54 \pmod{61}$. This contradicts the fact that $\left(\frac{54}{61}\right) = -1$.
`Case 8.` $n \equiv 301, 325, 541, 565, 661, 685, 781 \pmod{840}$. Then $n \equiv 21, 10, 16, 5, 31, 20, 11 \pmod{35}$ and $n \equiv 21, 45, 51, 5, 31, 55, 11 \pmod{70}$. By $\mathrm{ord}_{71}(4) = 35$ and $\mathrm{ord}_{71}(13) = 70$, we have $x^2 \equiv (4^{21}-1)(13^{21}-1)$, $(4^{10}-1)(13^{45}-1)$, $(4^{16}-1)(13^{51}-1)$, $(4^5-1)(13^5-1)$, $(4^{31}-1)(13^{31}-1)$, $(4^{20}-1)(13^{55}-1)$, $(4^{11}-1)(13^{11}-1) \equiv 44, 7, 59, 34, 47, 65, 53 \pmod{71}$. These contradict the fact that $\left(\frac{44}{71}\right) = \left(\frac{59}{71}\right) = \left(\frac{47}{71}\right) = \left(\frac{53}{71}\right) = \left(\frac{7}{71}\right) = \left(\frac{34}{71}\right) = \left(\frac{65}{71}\right) = -1$.
`Case 9.` $n \equiv 61, 85, 181, 421, 805 \pmod{840}$. Then $n \equiv 5, 1, 13, 7 \pmod{14}$ and $n \equiv 5, 29, 13, 21 \pmod{56}$. By $\mathrm{ord}_{113}(4) = 14$ and $\mathrm{ord}_{113}(13) = 56$, we have $x^2 \equiv (4^5-1)(13^5-1), (4-1)(13^{29}-1), (4^{13}-1)(13^{13}-1), (4^7-1)(13^{21}-1) \equiv 70, 71, 39, 79 \pmod{113}$. These contradict the fact that $\left(\frac{70}{113}\right) = \left(\frac{39}{113}\right) = \left(\frac{71}{113}\right) = \left(\frac{79}{113}\right) = -1$.

`Case 10.` $n \equiv 205, 445, 1045, 1285 \pmod{1680}$. Then $n \equiv 1 \pmod{12}$ and $n \equiv 85, 205 \pmod{240}$. By $\mathrm{ord}_{241}(4) = 12$ and $\mathrm{ord}_{241}(13) = 240$, we have $x^2 \equiv (4-1)(13^{85}-1), (4-1)(13^{205}-1) \equiv 124, 111 \pmod{241}$. These contradict the fact that $\left(\frac{111}{241}\right) = \left(\frac{124}{241}\right) = -1$.

The above ten cases are exhaustive, thereby completing the proof. $\square$

Proof of Theorem 2. It is easy to verify that if $n \le 3$ then Eq. (2) has only one solution: $n = 1, x = 18$. Suppose that a pair (n, x) with $n \ge 4$ is the solution of Eq. (2), we consider the following 16 cases.
`Case 1.` $n \equiv 0 \pmod 4$. Then n can uniquely be written in the form $n = 4 \cdot 5^k l$, where $k \ge 0, 5 \nmid l$. By induction on k, we have

$$13^{4\cdot 5^k l} \equiv 1 + 2 \cdot 5^{k+1} l \pmod{5^{k+2}}, \tag{5}$$

$$28^{4\cdot 5^k l} \equiv 1 + 5^{k+1} l \pmod{5^{k+2}}. \tag{6}$$

By the assumption and (5), (6) we have

$$\frac{x^2}{5^{2k+2}} \equiv 2l^2 \pmod 5;$$

thus, 2 is a quadratic residue modulo 5, a contradiction.

Case 2. $n \equiv 2, 3 \pmod 4$. By $\mathrm{ord}_{16}(13) = 4$, we have $x^2 \equiv (13^2 - 1)(-1), (13^3 - 1)(-1) \equiv 8, 12 \pmod{16}$. These are impossible.

Case 3. $n \equiv 1 \pmod 8$. By $\mathrm{ord}_{32}(13) = 8$, we have $x^2 \equiv (13 - 1)(-1) \equiv 20 \pmod{32}$. Hence $4|x^2$. Let $x = 2x_1$ with $x_1 \in \mathbb{Z}$. Then $x_1^2 \equiv 5 \pmod 8$. This is impossible.

Case 4. $n \equiv 5, 21, 29, 61 \pmod{72}$. Then $n \equiv 5, 21, 29, 25 \pmod{36}$ and $n \equiv 5, 3, 11, 7 \pmod{18}$. By $\mathrm{ord}_{37}(13) = 36$ and $\mathrm{ord}_{37}(28) = 18$, we have $x^2 \equiv (13^5 - 1)(28^5 - 1), (13^{21} - 1)(28^3 - 1), (13^{29} - 1)(28^{11} - 1), (13^{25} - 1)(28^7 - 1) \equiv 31, 35, 17, 6 \pmod{37}$. These contradict the fact that $\left(\frac{31}{37}\right) = \left(\frac{35}{37}\right) = \left(\frac{17}{37}\right) = \left(\frac{6}{37}\right) = -1$.

Case 5. $n \equiv 53, 69 \pmod{72}$. By $\mathrm{ord}_{73}(13) = \mathrm{ord}_{73}(28) = 72$, we have $x^2 \equiv (13^{53} - 1)(28^{53} - 1), (13^{69} - 1)(28^{69} - 1) \equiv 40, 59 \pmod{73}$. These contradict the fact that $\left(\frac{40}{73}\right) = \left(\frac{59}{73}\right) = -1$.

Case 6. $n \equiv 13, 253, 333, 109, 189, 229 \pmod{360}$. Then $n \equiv 13, 29 \pmod{40}$. By $\mathrm{ord}_{41}(13) = \mathrm{ord}_{41}(28) = 40$, we have $x^2 \equiv (13^{13} - 1)(28^{13} - 1), (13^{29} - 1)(28^{29} - 1) \equiv 3, 34 \pmod{41}$. These contradict the fact that $\left(\frac{3}{41}\right) = \left(\frac{34}{41}\right) = -1$.

Case 7. $n \equiv 37, 157 \pmod{360}$. Then $n \equiv 1 \pmod 3$ and $n \equiv 37 \pmod{60}$. By $\mathrm{ord}_{61}(13) = 3$ and $\mathrm{ord}_{61}(28) = 20$, we have $x^2 \equiv (13 - 1)(28^{37} - 1) \equiv 17 \pmod{61}$. This contradicts the fact that $\left(\frac{17}{61}\right) = -1$.

Case 8. $n \equiv 261, 301 \pmod{360}$. Then $n \equiv 36, 31 \pmod{45}$ and $n \equiv 81, 121 \pmod{180}$. By $\mathrm{ord}_{181}(13) = 45$ and $\mathrm{ord}_{181}(28) = 180$, we have $x^2 \equiv (13^{36} - 1)(28^{81} - 1), (13^{31} - 1)(28^{121} - 1) \equiv 86, 107 \pmod{181}$. These contradict the fact that $\left(\frac{86}{181}\right) = \left(\frac{107}{181}\right) = -1$.

Case 9. $n \equiv 85, 181, 1045, 445, 541, 1405, 477, 765 \pmod{1440}$. Then $n \equiv 85, 61, 93 \pmod{96}$ and $n \equiv 21, 29 \pmod{32}$. By $\mathrm{ord}_{97}(13) = 96$ and $\mathrm{ord}_{97}(28) = 32$, we have $x^2 \equiv (13^{85} - 1)(28^{21} - 1), (13^{61} - 1)(28^{29} - 1)\ (13^{93} - 1)(28^{29} - 1) \equiv 42, 26, 30 \pmod{97}$. These contradict the fact that $\left(\frac{42}{97}\right) = \left(\frac{26}{97}\right) = \left(\frac{30}{97}\right) = -1$.

Case 10. $n \equiv 325, 805, 685, 1165, 45, 117, 837 \pmod{1440}$. Then $n \equiv 85, 205, 45, 117 \pmod{240}$ and $n \equiv 5, 45, 37 \pmod{80}$. By $\mathrm{ord}_{241}(13) = 240$ and $\mathrm{ord}_{241}(28) = 80$, we have $x^2 \equiv (13^{85} - 1)(28^5 - 1), (13^{205} - 1)(28^{45} - 1), (13^{45} - 1)(28^{45} - 1), (13^{117} - 1)(28^{37} - 1) \equiv 208, 43, 139, 197 \pmod{241}$. These contradict the fact that $\left(\frac{208}{241}\right) = \left(\frac{43}{241}\right) = \left(\frac{139}{241}\right) = \left(\frac{197}{241}\right) = -1$.

`Case 11.` $n \equiv 1261, 4141, 405, 1845, 4005, 1197, 2637 \pmod{4320}$. Then $n \equiv 181, 37, 189, 117, 45 \pmod{216}$ and $n \equiv 397, 253, 405, 117, 333, 45 \pmod{432}$. By $\mathrm{ord}_{433}(13) = 216$ and $\mathrm{ord}_{433}(28) = 432$, we have $x^2 \equiv (13^{181} - 1)(28^{397} - 1)$, $(13^{37}-1)(28^{253}-1)$, $(13^{189}-1)(28^{405}-1)$, $(13^{117}-1)(28^{117}-1)$, $(13^{117}-1)(28^{333}-1)$, $(13^{45} - 1)(28^{45} - 1) \equiv 299, 393, 166, 201, 387, 279 \pmod{433}$. These contradict the fact that $\left(\frac{299}{433}\right) = \left(\frac{393}{433}\right) = \left(\frac{166}{433}\right) = \left(\frac{201}{433}\right) = \left(\frac{387}{433}\right) = \left(\frac{279}{433}\right) = -1$.

`Case 12.` $n \equiv 1125, 3285 \pmod{4320}$. Then $n \equiv 45 \pmod{540}$ and $n \equiv 18 \pmod{27}$. By $\mathrm{ord}_{541}(13) = 540$ and $\mathrm{ord}_{541}(28) = 27$, we have $x^2 \equiv (13^{45}-1)(28^{18} - 1) \equiv 295 \pmod{541}$. This contradicts the fact that $\left(\frac{295}{541}\right) = -1$.

`Case 13.` $n \equiv 2701 \pmod{8640}$. Then $n \equiv 13 \pmod{64}$ and $n \equiv 13 \pmod{48}$. By $\mathrm{ord}_{193}(13) = 64$ and $\mathrm{ord}_{193}(28) = 48$, we have $x^2 \equiv (13^{13} - 1)(28^{13} - 1) \equiv 71 \pmod{193}$. This contradicts the fact that $\left(\frac{71}{193}\right) = -1$.

`Case 14.` $n \equiv 2341, 5221, 8101, 2565, 6885 \pmod{8640}$. Then $n \equiv 37, 261, 549 \pmod{576}$. By $\mathrm{ord}_{577}(13) = \mathrm{ord}_{577}(28) = 576$, we have $x^2 \equiv (13^{37} - 1)(28^{37} - 1)$, $(13^{261} - 1)(28^{261} - 1)$, $(13^{549} - 1)(28^{549} - 1) \equiv 45, 222, 355 \pmod{577}$. These contradict the fact that $\left(\frac{45}{577}\right) = \left(\frac{222}{577}\right) = \left(\frac{355}{577}\right) - 1$.

`Case 15.` $n \equiv 3781, 7021, 4077, 8397 \pmod{8640}$. Then $n \equiv 1, 27 \pmod{135}$ and $n \equiv 1621, 541, 1917 \pmod{2160}$. By $\mathrm{ord}_{2161}(13) = 135$ and $\mathrm{ord}_{2161}(28) = 2160$, we have $x^2 \equiv (13 - 1)(28^{1621} - 1)$, $(13 - 1)(28^{541} - 1)$, $(13^{27} - 1)(28^{1917} - 1) \equiv 1838, 299, 2090 \pmod{2161}$. These contradict the fact that $\left(\frac{1838}{2161}\right) = \left(\frac{299}{2161}\right) = \left(\frac{2090}{2161}\right) = -1$.

`Case 16.` $n \equiv 901, 6661 \pmod{8640}$. Then $n \equiv 37, 613 \pmod{864}$. Since $\mathrm{ord}_{8641}(13) = 864$ and $\mathrm{ord}_{8641}(28) = 8640$, we have $x^2 \equiv (13^{37} - 1)(28^{901} - 1)$, $(13^{613} - 1)(28^{6661} - 1) \equiv 4110, 1277 \pmod{8641}$. These contradict the fact that $\left(\frac{4110}{8641}\right) = \left(\frac{1277}{8641}\right) = -1$.

The above sixteen cases are exhaustive, thereby completing the proof. □

Acknowledgement. We would like to thank the referee for his/her many helpful suggestions. We thank Professor Yong-Gao Chen and managing editor Bruce Landman for many helpful editing suggestions.

References

[1] L. Hajdu, L. Szalay, On the Diophantine equations $(2^n-1)(6^n-1)=x^2$ and $(a^n-1)(a^{kn}-1)=x^2$, *Period. Math. Hungar.* **40**(2000), 141-145.

[2] Li Lan and L. Szalay, On the exponential diophantine $(a^n-1)(b^n-1)=x^2$, *Publ. Math. Debrecen* **77**(2010), 1-6.

[3] M. H. Le, A note on the exponential Diophantine equation $(2^n-1)(b^n-1)=x^2$, *Publ. Math. Debrecen* **74**(2009), 401-403.

[4] F. Luca, P. G. Walsh, The product of like-indexed terms in binary recurrences, *J. Number Theory* **96**(2002), 152-173.

[5] L. Szalay, On the diophantine equations $(2^n-1)(3^n-1)=x^2$, *Publ. Math. Debrecen* **57**(2000), 1-9.

[6] Min Tang, *A note on the exponential diophantine equation* $(a^m-1)(b^n-1)=x^2$, J. Math. Research and Exposition, to appear.

[7] P. G. Walsh, On Diophantine equations of the form $(x^n-1)(y^m-1)=z^2$, *Tatra Mt. Math. Publ.* **20**(2000), 87-89.