# ON DIOPHANTINE EQUATIONS $\mathbf{x^2 - dy^2 = AB}$

Yungchen Cheng

Southwest Missouri State University

**1. Introduction.** There are lots of examples like $13^2 - 94 \cdot 1^2 = 5^2 \cdot 3$, $223^2 - 94 \cdot 23^2 = 3$ and $44^2 - 67 \cdot 5^2 = 3^2 \cdot 29$, $573^2 - 67 \cdot 70^2 = 29$ which suggest that the Diophantine equation $x^2 - dy^2 = c$ is solvable whenever $x^2 - dy^2 = p^2c$ is solvable where $p$ is a prime. However, it will be shown in this paper that the equation $x^2 - 799y^2 = 89$ does not have an integer solution (see Proposition 4.1), even though we have $40^2 - 799 \cdot 1^2 = 3^2 \cdot 89$. This counterexample motivates the need to find conditions that would assure solvability of $x^2 - dy^2 = p^2c$.

It is well known that there is an intimate relationship between the solvability of general Diophantine equations $x^2 - dy^2 = c$ (when $|c| < \sqrt{d}$) and the continued fraction representation of $\sqrt{d}$ [5, p. 352]. But this result does not explain the correlation between the solvabilities of $x^2 - dy^2 = p^2c$ and $x^2 - dy^2 = c$.

Most of the work (since 1940) referenced in *Mathematical Reviews* [see [6], [7]) on general Diophantine equations $x^2 - dy^2 = c$ have focused on the following: (1) methods of finding solutions ([14], [19]); (2) the number of solution classes ([3], [9], [11], [16], [17], [18]); (3) special cases like $x^2 - dy^2 = \pm 4$ ([2], [3], [4], [11]), $x^2 - dy^2 = 4c$ ([11]), $x^2 - 2y^2 = c$ ([15]), or $x^2 - py^2 = 2c$ ([1]). T. Nagell has also done some work that dealt with the solutions of equations such as $Ax^2 \pm By^2 = \pm 1, \pm 2, \pm 4$ ([10]), $Ax^2 \pm By^2 = p$ or $2p$ ([12], [13]) when $D = AB$ is fixed.

This paper will differ from the work mentioned above by attempting to treat the more general case: $x^2 - dy^2 = AB$ vs. $x^2 - dy^2 = B$ for general $d$, $A$, and $B$. The main result is Theorem 2.1 in section 2. We then discuss the special cases $A = p$ and $A = p^2$ in section 3. The main results are Propositions 3.1 and 3.2. In section 4 we give an example to show that the condition required in Proposition 3.2 is necessary and therefore resolve the question raised at the beginning. The author would like to thank Liang-Cheng Zhang's valuable suggestions related to this paper.

For any integer $c$, the equation $x^2 - dy^2 = c$ is said to be *solvable* if there are integers $m$ and $n$ such that $m^2 - dn^2 = c$. The solution $x = m$, $y = n$ is called *primitive* if $m$ and $n$ are relatively prime. Technically speaking, we will allow both $m = 1$, $n = 0$ and $m = 0$, $n = 1$ to be considered primitive solutions.

**2. Main Theorem.** We start with the general case: $x^2 - dy^2 = AB$. The goal is to see how the solvability of $x^2 - dy^2 = B$ can be derived from the solvability of $x^2 - dy^2 = AB$. The following theorem provides an answer to this question. Note that $d$ is not necessarily assumed to be square-free.

Theorem 2.1. Let $d$, $A$, and $B$ be nonzero integers. Assume that the congruence $x^2 \equiv d \pmod{A}$ has at most two incongruent solutions.

(1) If both equations $x^2 - dy^2 = AB$ and $x^2 - dy^2 = A$ have primitive solutions, then the equation $x^2 - dy^2 = B$ is solvable.

(2) If we further assume in (1) that $A$ and $B$ are relatively prime, then the equation $x^2 - dy^2 = B$ has a primitive solution.

Proof of (1). Let $m$, $n$, $h$, $k$ be integers such that $(m, n) = 1 = (h, k)$ and

$$m^2 - dn^2 = AB, \quad h^2 - dk^2 = A.$$

Without loss of generality we may assume that both $n$ and $k$ are nonzero because, otherwise, $m = 1$ and/or $h = 1$ reduce both (1) and (2) to trivial cases. We then have $m^2 \equiv dn^2$, $h^2 \equiv dk^2 \pmod{A}$. If an integer $q$ divides $n$ and $A$, then $q$ divides $m$. Hence, $n$ and $A$ must be relatively prime. This implies that there exists an integer $M$ such that

$$0 \leq M < |A| \text{ and } m \equiv Mn \pmod{A} \text{ (i.e. } M \equiv n^{-1}m).$$

From this we have $dn^2 \equiv m^2 \equiv M^2n^2$, $d \equiv M^2 \pmod{A}$. Similarly, there exists an integer $L$ such that

$$0 \leq L < |A|, \quad h \equiv Lk, \quad d \equiv L^2 \pmod{A}.$$

Since there are at most two incongruent solutions for the equation $x^2 \equiv d \pmod{A}$, we must have $M \equiv L \pmod{A}$ or $M \equiv -L \pmod{A}$. If $M \equiv -L \pmod{A}$, then $h \equiv M(-k)$ and $x = h$, $y = -k$ is still a solution of $x^2 - dy^2 = A$. Without loss of generality we may therefore assume that $M \equiv L \pmod{A}$.

Let $z = (m + n\sqrt{d})/(h + k\sqrt{d})$ in $\mathbb{Q}[\sqrt{d}]$ and apply the norm function $N(a + b\sqrt{d}) = a^2 - db^2$ in $\mathbb{Q}[\sqrt{d}]$ to $z$, we see that

$$N(z) = N(m + n\sqrt{d})/N(h + k\sqrt{d}) = AB/A = B$$

and

$$\begin{aligned} z &= [(mh - nkd) + (nh - mk)\sqrt{d}]/(h^2 - dk^2) \\ &= [(mh - nkd) + (nh - mk)\sqrt{d}]/A. \end{aligned}$$

However,

$$mh \equiv M^2 nk \equiv nkd, \quad \text{and} \quad mk \equiv Mnk \equiv nh \pmod{A}.$$

Therefore, $z \in \mathbb{Z}[\sqrt{d}]$ and $x = (mh - nkd)/A$ and $y = (nh - mk)/A$ is an integer solution of the equation $x^2 - dy^2 = B$.

Proof of (2). In (1), if a prime $q$ divides both $(mh - nkd)/A$ and $(nh - mk)/A$ then $q$ divides $mh - nkd$, $nh - mk$, and $B$. Furthermore, $q$ will divide $mh^2 - nhkd$, $nhkd - mk^2d$, $mhk - nk^2d$, and $nh^2 - mhk$, which implies that both $m(h^2 - dk^2) = mA$ and $n(h^2 - dk^2) = nA$ are divisible by $q$. Since $A$ and $B$ are relatively prime, $q$ must divide both $m$ and $n$, a contradiction. Therefore, $(mh - nkd)/A$ and $(nh - mk)/A$ are relatively prime, giving a primitive solution $x = (mh - nkd)/A$, $y = (nh - mk)/A$ to the equation $x^2 - dy^2 = B$.

**3. Special Cases.** First, we consider the case when $A = p$ is a prime.

Proposition 3.1. Let $d$ and $B$ be nonzero integers and $p$ be a prime integer. Assume that the equation $x^2 - dy^2 = p$ is solvable.

(1) If $B$ is not divisible by $p$ and the equation $x^2 - dy^2 = pB$ is solvable, so is the equation $x^2 - dy^2 = B$.

(2) If the equation $x^2 - dy^2 = pB$ has a primitive solution, then the equation $x^2 - dy^2 = B$ is solvable.

(3) If the equation $x^2 - dy^2 = pB$ has and primitive solution and $B$ is not divisible by $p$, then the equation $x^2 - dy^2 = B$ has a primitive solution.

Proof. Note that all solutions $x^2 - dy^2 = p$ are primitive. If $a^2 \equiv d \equiv b^2 \pmod{p}$, then $a \equiv b$ or $a \equiv -b$. This means that $x^2 \equiv d$ has at most two incongruent solutions modulo $p$. So (2) and (3) hold by Theorem 2.1.

As for (1), if $B$ is not divisible by $p$, then the solvability of $x^2 - dy^2 = pB$ guarantees a primitive solution for the equation $x^2 - dy^2 = p(B/C^2)$ for some integer $C$. Therefore, $x^2 - dy^2 = (B/C^2)$ is solvable by (2), so is $x^2 - dy^2 = B$.

Next, we consider the case $A = p^2$, where $p$ is a prime. By observing the example:

$$9^2 - 18 \cdot 2^2 = 3^2 \quad \text{where} \quad 0^2 \equiv 3^2 \equiv 6^2 \equiv 18 \pmod{3^2},$$

we know it is possible for $x^2 - dy^2 = p^2$ to have a primitive solution and, at the same time, there are more than two incongruent solutions to $x^2 \equiv d \pmod{p^2}$. This of course has something to do with the fact that $p^2|d$. However, it is easy to see that, whenever the equation $x^2 - dy^2 = p^2$ has a primitive solution, then $p^2|d$ if and only if $p|d$. We therefore require the additional condition that $p \nmid d$ in the following proposition.

Proposition 3.2. Let $d$ and $B$ be nonzero integers, and $p$ a prime integer that does not divide $d$ when $p$ is odd.

(1) If the equation $x^2 - dy^2 = p^2B$ is solvable and the equation $x^2 - dy^2 = p^2$ has a primitive solution, then the equation $x^2 - dy^2 = B$ is solvable.

(2) If we further assume in (1) that $B$ is not divisible by $p$ and the solution of $x^2 - dy^2 = p^2B$ is primitive, then the equation $x^2 - dy^2 = B$ has a primitive solution.

Proof. Obviously, $x^2 \equiv d \pmod{2^2}$ has at most two incongruent solutions for any $d$. We may therefore only consider odd primes $p$. If $d \equiv x^2 \equiv y^2 \pmod{p^2}$, then $p^2|(x-y)(x+y)$. If $p|(x-y)$ and $p|(x+y)$, then $p|2x$ and hence, $p|x$. This implies that $d$ is divisible by $p$, a contradiction. So, $p^2|(x-y)$ or $p^2|(x+y)$. That is, $x \equiv -y$ or $x \equiv y \pmod{p^2}$, and the congruence equation $x^2 \equiv d \pmod{p^2}$ has at most two incongruent solutions modulo $p^2$.

If we know that $m^2 - dn^2 = p^2B$ with some prime $q$ dividing both $m$ and $n$, then $q^2|p^2B$. One possibility is $q = p$, which makes

$$\left(\frac{m}{p}\right)^2 - d\left(\frac{n}{p}\right)^2 = B$$

and we are done. The other possibility is $q^2|B$, which implies

$$\left(\frac{m}{q}\right)^2 - d\left(\frac{n}{q}\right)^2 = p^2(B/q^2).$$

Repeating this process if necessary, we may eventually obtain an integer $C$ such that $C^2|B$ and either $x^2 - dy^2 = B/C^2$ is solvable or $x^2 - dy^2 = p^2(B/C^2)$ has a primitive solution. The first case makes $x^2 - dy^2 = B$ solvable automatically, while applying Theorem 2.1 to the second case allows $x^2 - dy^2 = B/C^2$ to be solvable, which in turn shows that, again $x^2 - dy^2 = B$ is solvable. This proves (1). As for (2), it is an immediate result of Theorem 2.1.

Remark. It is a fact that the equation $x^2 \equiv d \pmod{q^n}$ can have more than two incongruent solutions if $q|d$ and $n > 1$. By using the Chinese Remainder Theorem we can show that the condition $x^2 \equiv d \pmod{A}$ has at most two incongruent solutions, is satisfied when $A = 2^e p^k q_1 \cdots q_t$ (where $e = 0, 1, k \geq 0, p$ and $q_i$ are distinct odd primes such that $p \nmid d$ and $q_i|d$) or $A = 4q_1 \cdots q_t$ (where $q_i$ are distinct odd primes that $q_i|d$). Analogous results to Proposition 3.1 and 3.2 can be obtained similarly.

The following is a direct result of Theorem 2.1 and has an "if and only if" situation.

Corollary 3.3. Let $d$ be a nonzero integer and $A$, $B$ be relatively prime (nonzero) integers. If each of the congruences $x^2 \equiv d \pmod{A}$ and $x^2 \equiv d \pmod{B}$ has at most two incongruent solutions and the equation $x^2 - dy^2 = AB$ has a primitive solution, then the equation $x^2 - dy^2 = A$ has a primitive solution if and only if the equation $x^2 - dy^2 = B$ has a primitive solution.

If we concentrate on the cases of only two distinct primes $p$ and $q$, we have the following.

Corollary 3.4. Let $d$ be a nonzero integer and let $p$, $q$ be distinct prime integers. Let $e = 1$ or $2$ and $f = 1$ or $2$. Assume that the equation $x^2 - dy^2 = p^e q^f$ has a primitive solution. Then the equation $x^2 - dy^2 = p^e$, with $p|d$ when $e = 2$, has a primitive solution if and only if the equation $x^2 - dy^2 = q^f$, with $q|d$ when $f = 2$, has a primitive solution.

**4. An Example.**

Proposition 4.1. $x^2 - 799y^2 = 89$ is not solvable. However, $x^2 - 799y^2 = 3^2 \cdot 89$ is solvable, since $40^2 - 799 \cdot 1^2 = 3^2 \cdot 89$.

Proof. By Proposition 3.2 we only have to show that

(1) $x^2 - 799y^2 = 3^2$ does not have primitive solutions. Because $32^2 - 799 \cdot 1^2 = 3^2 \cdot 5^2$, this is equivalent, by Corollary 3.4, to showing

(2) $x^2 - 799y^2 = 5^2$ does not have primitive solutions. In order to verify (2), we will use the following two special observations.

(3) Each of $x^2 - 799y^2 = \pm 10$ and $x^2 - 799y^2 = \pm 5$ is not solvable.

(4) Each of $47x^2 - 17y^2 = \pm 10$ and $47x^2 - 17y^2 = \pm 5$ is not solvable.

It is easy to see that (3) is true because the only squares modulo 17 are $0, 1, 4, 9, 16, 8, 2, 15$, and 13, and none of these is congruent to $\pm 10$ and $\pm 5 \pmod{17}$. A similar argument can be used for (4).

Now, let us verify (2). Let $m^2 - 799n^2 = 5^2$. It suffices to assume that both $m$ and $n$ are positive. Then $m^2 \equiv 8 \pmod{17}$ implies that $m \equiv \pm 5 \pmod{17}$, and so $m = \pm 5 + 17k$ for some integer $k > 1$. Therefore,

$$\begin{aligned} 25 \pm 170k + 17^2k^2 - 799n^2 &= 25 \\ \pm 10k + 17k^2 - 47n^2 &= 0 \\ k(17k \pm 10) &= 47n^2. \end{aligned}$$

If $47|k$, say $k = 47t$ for some $t \in \mathbb{N}$, then

$$\begin{aligned} t(799t \pm 10) &= n^2 \\ n^2 - 799t^2 &= \pm 10. \end{aligned}$$

This contradicts the fact that the equation $x^2 - 799y^2 = \pm 10$ is not solvable. Thus, $k$ is not divisible by 47.

If $k$ and $17k \pm 10$ are relatively prime, then $k$ is a square factor of $n^2$, say, $k = r^2$, and

$$r^2(17r^2 \pm 10) = 47r^2s^2 \quad \text{for some} \quad r, s \in \mathbb{N}.$$

This implies $47s^2 - 17r^2 = \pm 10$, a contradiction. Hence, there exists a prime factor $q$ of $n$ that divides both $k$ and $17k \pm 10$. This implies that $q|10$. Note that if $q = 5$, then both $m$ and $n$ are divisible by 5, and if $q = 2$, we have that

$$\frac{k}{2}\left(17 \cdot \frac{k}{2} \pm 5\right) = 47\left(\frac{n}{2}\right)^2.$$

If necessary, repeat the same process as above. Hence, we can find a prime factor $p$ of $n/2$ such that $p$ divides both $k/2$ and $17k/2 \pm 5$. This forces $p = 5$. Again, both $m$ and $n$ are divisible by 5. So, (2) is true.

## *References*


1. S. Chowla, "A Note Concerning a Problem Related to Hilbert's Tenth Problem," *Norske Vid. Selsk. Skr. (Trondheim)*, 5 (1970), 2.
2. H. Cohn, *Analytic Number Theory*, Lecture Notes in Mathematics, 899, Springer, Berlin, (1980), 221–230.
3. P. Heichelheim, "Some Remarks on Stolt's Theorems for Pellian Equations," *Ark. Mat.*, 12 (1974), 167–171.
4. L. Hua, "On the Least Solution of Pell's Equation," *Bull. Amer. Math. Soc.*, 48 (1942), 731–735.
5. I. Niven, H, Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley, New York, 1991.
6. *Reviews in Number Theory*, edited by W. LeVeque, vol. 2, American Mathematical Society, Providence, 1974.
7. *Reviews in Number Theory*, edited by R. Guy, vol. 2A, American Mathematical Society, Providence, 1984.
8. T. Nagell, "Über die Darstellung Ganzer Zahlen Durch eine Indefinite Binäre Quadratische Form," *Arch. Math.*, 2 (1950), 161–165.
9. T. Nagell, "Bemerkung über die Diophantische Gleichung $u^2 - Dv^2 = C$," *Arch. Math.*, 3 (1952), 8–9.
10. T. Nagell, "On a Special Class of Diophantine Equations of the Second Degree," *Ark. Mat.*, 3 (1954), 51–65.
11. T. Nagell, "Contribution to the Theory of a Category of Diophantine Equations of the Second Degree with Two Unknowns," *Nova Acta Soc. Sci. Upsal.*, 16 (1955), 38.
12. T. Nagell, "Über die Lösbarkeit Gewisser Diophantischer Gleichungen Zweiten Grades," *Arch. Math. (Basel)*, 21 (1970), 487–489.
13. T. Nagell, "Sur la Solubilité en Nombres Entiers des Équations du Second Degré à Deux Indéterminées," *Acta Arith.*, 18 (1971), 105–114.
14. W. Patz, "Über die Gleichung $X^2 - DY^2 - \pm c \cdot (2^{31} - 1)$, wo $c$ Möglichst Klein," S.-B. Math.-Nat. Kl. Bayer. Akad. Wiss., (1949), 21–30.
15. A. Schinzel and W. Sierpiński, "On the equation $x^2 - 2y^2 - k$, *Wiadom. Mat.*, 7 (1964), 229–232.
16. B. Stolt, "On the Diophantine Equation $u^2 - Dv^2 = \pm 4N$," *Ark. Mat.*, 2 (1952), 1–23.

17. B. Stolt, "On the Diophantine Equation $u^2 - Dv^2 = \pm 4N$ II," *Ark. Mat.*, 2 (1952), 251–268.

18. B. Stolt, "On the Diophantine Equation $u^2 - Dv^2 = \pm 4N$ III," *Ark. Mat.*, 3 (1955), 117–132.

19. O. Tino, "Sur la Réduction de L'équation Indéterminée du Second Degré $x^2 - \rho y^2 = l$ aux Équations $x^2 - \rho y^2 = \pm 1$ et $\alpha x^2 - \beta y^2 = \pm 1$," *Bull. Sci. École Polytech. Timisoara*, 10 (1941), 43–68.