NNTDM Vol. 16 (2010), 2, 16-23

Infinitely many insolvable Diophantine equations II

Yasutsugu Fujita
Department of Mathematics, College of Industrial Technology
Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
Email: fujita.yasutsugu@cit.nihon-u.ac.jp
and
Noriaki Kimura
Department of Mathematics, College of Industrial Technology
Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
Email: nrkmr@kb4.so-net.ne.jp

Abstract

Let $f(X_1, \ldots, X_m)$ be a quadratic form in m variables $X_1, \ldots, X_m$ with integer coefficients. Then it is well-known that the Diophantine equation $f(X_1, \ldots, X_m) = 0$ has a nontrivial solution in integers if and only if the equation has a nontrivial solution in real numbers and the congruence $f(X_1, \ldots, X_m) \equiv 0 \pmod{N}$ has a nontrivial solution for every integer $N > 1$. Such a principle is called the Hasse principle. In this paper, we explicitly give several types of families of the Diophantine equations of degree two, not homogeneous, for which the Hasse principle fails.

2000 *Mathematics Subject Classification*: 11D09, 11A07

Key words: Hasse principle, Diophantine equations, congruences

1 Introduction

Let $f(X_1, \ldots, X_m)$ be a quadratic form in m variables $X_1, \ldots, X_m$ with integer coefficients. For an integer $N > 1$, the congruence $f(X_1, \ldots, X_m) \equiv 0 \pmod{N}$ is said to have a nontrivial solution, or simply, to be solvable if $f(X_1, \ldots, X_m) \equiv 0 \pmod{p^k}$ has a solution $(x_1, \ldots, x_m)$ with at least one of x_i's indivisible by p for each prime divisor p of N, where k is the positive integer such that p^k is the largest power of p dividing N. The Hasse-Minkowski theorem ([1, p. 61]) asserts that the Diophantine equation $f(X_1, \ldots, X_m) = 0$ has a solution in integers, not all zero, if and only if the equation has a solution in real numbers, not all zero, and the congruence $f(X_1, \ldots, X_m) \equiv 0 \pmod{N}$ has a nontrivial solution for every integer $N > 1$. Such a principle is called the Hasse principle.

If $f(X_1, \ldots, X_m)$ is not homogeneous, the Hasse principle does not hold in general for the equation $f(X_1, \ldots, X_m) = 0$. For example, the Hasse principle fails for the equation

$2X^2-219Y^2=-1$, which can be found in the book of Sierpiński ([7, p. 195]). Motivated by this example, Williams and the second author ([4]) found a certain type of families of the Diophantine equations of degree two for each of which the Hasse principle fails. Just after [4] appeared, Mollin ([6]) generalized their result in terms of (Extended) Richaud-Degert type (see [5, Section 3.2]). However, he does not give any explicit forms of families of such equations.

Our purpose in this paper is to give various types of families of such equations. More precisely, we slightly generalize the result in [4] (Theorem 3.3 (i)) and give several types of the families with polynomial coefficients of one variable (Theorems 3.5, 3.9 and 3.13). Furthermore, we give several families, not of polynomial type, including those families containing the above-mentioned example of Sierpiński for each of which the Hasse principle fails (Examples 3.8, 3.12 and 3.15).

We here consider the Diophantine equation of degree two

$$AX^2-BY^2=C, \tag{1.1}$$

where $(A,C)\in\{(2,\pm1),(1,\pm2)\}$ and B is a positive integer. The local solvability of (1.1) can be examined by a similar way to [4] (Propositions 3.1 and 4.1). Note that clearly (1.1) has a nontrivial solution in real numbers. In order to examine the global solvability (i.e., the solvability in integers) of (1.1), we consider the case where AB is of Richaud-Degert type (see Lemma 2.3), as Mollin did. However, unlike Mollin, we appeal to a result of Grelak and Grytczuk (Lemma 2.1; see also [2, 3]), which translates the solvability into the conditions for the fundamental solution of the Pell equation $U^2-ABV^2=1$.

Acknowledgement The first author is most grateful to Professor Alexander Grytczuk for kindly sending him a reprint of the manuscript [2]. He is also pleased to thank Professor Nobuhiro Terai for valuable suggestions.

2 Preliminary lemmas

The following lemma gives a criterion for the solvability of the Diophantine equation (1.1) with $C\in\{1,2\}$.

Lemma 2.1. ([2, Theorem 2]; *see also* [3, Criteria 1, 2]) *Let* $C\in\{1,2\}$ *and let* A,B *be positive integers with* $AC>1$. *Assume that* $D=AB$ *is not a perfect square and* $gcd(C,D)=1$. *Denote by* (u_0,v_0) *the least positive integer solution of the Pell equation* $U^2-DV^2=1$, *which we call the fundamental solution of the Pell equation. Then equation* (1.1) *is solvable if and only if the numbers*

$$x_0=\sqrt{\frac{(u_0+1)C}{2A}}\ \ \textit{and}\ \ y_0=\sqrt{\frac{(u_0-1)C}{2B}}$$

are integers.

Remark 2.2. In case $C=1$, one may put the condition for the solvability of (1.1) into "$2A|u_0+1$ and $2B|u_0-1$" ([3, Criterion 1]). However, in case $C=2$, the condition "$A|u_0+1$ and $B|u_0-1$" ([2, Criterion 2]) is not sufficient for the solvability, as can be seen from the equation $5x^2-y^2=2$.

We consider the equation (1.1) with $D = AB$ satisfying the conditions in the following lemma.

Lemma 2.3. (cf. [5, Section 3.2], [8, Lemma 2]) *Let n be a positive integer and r an integer with $-n < r \leq n$, $r \notin \{0, -1, \pm 4\}$ and $2n \equiv 0 \pmod{r}$. Put $D = n^2 + r$. Then the fundamental solution (u_0, v_0) of the Pell equation $U^2 - DV^2 = 1$ is given by*

$$(u_0, v_0) = \left(\frac{2n^2 + r}{|r|}, \frac{2n}{|r|} \right).$$

3 Solvability of the equation $2X^2 - BY^2 = \pm 1$

In this section, we examine the solvability of equations

$$2X^2 - BY^2 = -1, \tag{3.1}$$

$$2X^2 - BY^2 = 1, \tag{3.2}$$

and congruences

$$2X^2 - BY^2 \equiv -1 \pmod{N}, \tag{3.3}$$

$$2X^2 - BY^2 \equiv 1 \pmod{N}. \tag{3.4}$$

We first give criteria for the solvability of congruences (3.3) and (3.4).

Proposition 3.1. (i) *If any prime divisor p of B satisfies $p \equiv 1$ or $3 \pmod 8$, then congruence (3.3) is solvable for every integer $N > 1$.*

(ii) *If any prime divisor p of B satisfies $p \equiv 1$ or $7 \pmod 8$, then congruence (3.4) is solvable for every integer $N > 1$.*

Proof. One can prove this proposition along the same lines as the proof of [4, Theorem] or [6, Theorem 4]. □

The following lemma is the key to find all types of families in this section.

Lemma 3.2. *Let n and a be integers with $n \geq 1$ and $a \notin \{0, -1, \pm 4\}$. Let $B = (n^2a^2 + a)/2$ be an integer with $B > 1$.*

(i) *Suppose that $a \neq 2$. If any prime divisor p of B satisfies $p \equiv 1$ or $3 \pmod 8$, then the Hasse principle fails for equation (3.1).*

(ii) *Suppose that $a \neq -2$. If any prime divisor p of B satisfies $p \equiv 1$ or $7 \pmod 8$, then the Hasse principle fails for equation (3.2).*

Proof. In view of Proposition 3.1, it suffices to show that (3.1) and (3.2) are unsolvable. By Lemma 2.3 the fundamental solution of $U^2 - 2BV^2 = 1$ is $(u_0, v_0) = ((2n^2a^2 + a)/|a|, 2n)$.

(i) Suppose that $u_0 + 1 \equiv 0 \pmod{(2B)}$. Then we see from the assumption $a \neq 2$ that $a = 1$, and that n must be odd, since $B = (n^2 + 1)/2$ is an integer. Thus, $u_0 - 1 \not\equiv 0 \pmod 4$. It follows from Lemma 2.1 that (3.1) is unsolvable.

(ii) One can prove this in the same way as (i). □

As the first application of Lemma 3.2, we give a slight generalization of [4, Theorem] and its analogue.

Theorem 3.3. *Let n be a positive integer.*

(i) *Let $a \geq 3$ be an integer such that any prime divisor p of a satisfies $p \equiv 1$ or $3 \pmod 8$. If $B = 2n^2a^4 + a^2$, then the Hasse principle fails for equation* (3.1).

(ii) *Let $a \geq 7$ be an integer such that any prime divisor p of a satisfies $p \equiv 1$ or $7 \pmod 8$. If $B = 2n^2a^4 - a^2$, then the Hasse principle fails for equation* (3.2).

Proof. (i) Replacing a in Lemma 3.2 by $2a^2$ shows that (3.1) is unsolvable. On the other hand, for each prime divisor p of $2n^2a^2 + 1$ we have $(-2 \,|\, p) = 1$, where $(* \,|\, p)$ denotes the Legendre symbol modulo p, that is, $p \equiv 1$ or $3 \pmod 8$. Hence $B = a^2(2n^2a^2 + 1)$ is divisible only by primes congruent to 1 or 3. Therefore congruence (3.3) is solvable for every N by Lemma 3.2.

(ii) One can prove this in the same way as (i). □

Remark 3.4. (1) If $a = 1$ in the above theorem, then each of equations (3.1) and (3.2) has a trivial solution $(x, y) = (n, 1)$.

(2) As mentioned in [4], replacing a by a^m yields a parametric family for each of the a's satisfying the condition. The advantage is that our families are parametrized by two parameters m and n.

Since any odd prime dividing the sum of two coprime biquadrates is congruent to 1 modulo 8, Lemma 3.2 with $a = 1$ immediately implies the following

Theorem 3.5. *Let $n \geq 3$ be an odd integer and let $B = (n^4 + 1)/2$. Then the Hasse principle fails for equations* (3.1) *and* (3.2).

More generally, the following holds.

Proposition 3.6. *Let $n \geq 3$ be an odd integer and let $B = (n^2 + 1)/2$.*

(i) *If there exist positive integers α, β with $B = \alpha^2 - 2\beta^2$ and if any prime divisor p of $\gcd(\alpha, \beta)$ satisfies $p \equiv 1 \pmod 8$, then the Hasse principle fails for equation* (3.1).

(ii) *If there exist positive integers α, β with $B = \alpha^2 + 2\beta^2$ and if any prime divisor p of $\gcd(\alpha, \beta)$ satisfies $p \equiv 1 \pmod 8$, then the Hasse principle fails for equation* (3.2).

Proof. This proposition immediately follows from Lemma 3.2. □

Remark 3.7. Since

$$\begin{aligned} \frac{n^4+1}{2} &= (n^2+n+1)^2 - 2\left\{\frac{(n+1)^2}{2}\right\}^2 \\ &= n^2 + 2\left(\frac{n^2-1}{2}\right)^2, \end{aligned}$$

Theorem 3.5 can be regarded as a special case of Proposition 3.6.

Example 3.8. (i) The condition $(n^2+1)/2 = \alpha^2-2\beta^2$ is equivalent to $n^2-2\alpha^2 = -4\beta^2-1$. For example, let $\beta = 2$. Then $n^2 - 2\alpha^2 = -17$. Since α is odd, each positive solution of this equation gives the desired value of B. In fact, any solution of the equation has the form $n + \alpha\sqrt{2} = (\pm 1 + 3\sqrt{2})(3 + 2\sqrt{2})^m$, and we obtain

$$B = \frac{1}{8}\left\{(19 \pm 6\sqrt{2})(3+2\sqrt{2})^{2m} + (19 \mp 6\sqrt{2})(3-2\sqrt{2})^{2m} - 30\right\} \quad (m = 1, 2, \dots).$$

(ii) The condition $(n^2 + 1)/2 = \alpha^2 + 2\beta^2$ is equivalent to $n^2 - 2\alpha^2 = 4\beta^2 - 1$. For example, let $\beta = 4$. Then $n^2 - 2\alpha^2 = 63$, and $n + \alpha\sqrt{2} = (9 \pm 3\sqrt{2})(3 + 2\sqrt{2})^m$. Thus we obtain

$$B = \frac{1}{8}\left\{9(11 \pm 6\sqrt{2})(3+2\sqrt{2})^{2m} + 9(11 \mp 6\sqrt{2})(3-2\sqrt{2})^{2m} + 130\right\} \quad (m = 0, 1, 2, \dots).$$

Applying Lemma 3.2 with (i) $a = -2$ and (ii) $a = 2$, we obtain the following

Theorem 3.9. *Let n be a positive integer.*

(i) *If $B = n^4 + (n+1)^4$, then the Hasse principle fails for equation* (3.1).

(ii) *If $B = 16n^2(n \pm 1)^2 + (4n^2 - 1)^2$, where $n \not\equiv 2 \pmod 3$ in the plus sign case and $n \not\equiv 1 \pmod 3$ in the minus sign case, then the Hasse principle fails for equation* (3.2).

Proof. (i) Since $B = n^4 + (n+1)^4 = 2(n^2+n+1)^2 - 1$, the assertion immediately follows from Lemma 3.2 with $a = -2$.

(ii) Since $B = 16n^2(n\pm1)^2+(4n^2-1)^2 = 2\{2n(2n\pm1)\}^2+1$, the assertion immediately follows from Lemma 3.2 with $a = 2$. □

More generally, the following holds.

Proposition 3.10. *Let α, β be positive integers such that any prime divisor of $\gcd(\alpha, \beta)$ satisfies $p \equiv 1 \pmod 8$. Let $B = 4\alpha^2 + \beta^2$.*

(i) *If there exists a positive integer n with $B = 2n^2 - 1$, then the Hasse principle fails for equation* (3.1).

(ii) *If there exists a positive integer n with $B = 2n^2 + 1$, then the Hasse principle fails for equation* (3.2).

Proof. This proposition is an easy corollary of Lemma 3.2. □

Remark 3.11. The minimal B's such that the Hasse principle fails for equations (3.1) and (3.2) are $B = 17 (= 4 \cdot 2^2 + 1^2 = 2 \cdot 3^2 - 1)$ and $B = 41 (= (3^4 + 1)/2)$, respectively.

Example 3.12. (i) The condition $2n^2-1 = 4\alpha^2+\beta^2$ is equivalent to $n^2-2\alpha^2 = (\beta^2+1)/2$. For example, let $\beta = 1$. Then $n^2 - 2\alpha^2 = 1$, and hence we obtain

$$B = \frac{1}{2}\left\{(3+2\sqrt{2})^{2m} + (3-2\sqrt{2})^{2m}\right\} \quad (m = 1, 2, \dots).$$

(ii) The condition $2n^2 + 1 = 4\alpha^2 + \beta^2$ is equivalent to $n^2 - 2\alpha^2 = (\beta^2 - 1)/2$. For example, let $\beta = 3$. Then $n^2 - 2\alpha^2 = 4$, and hence we obtain

$$B = 2(3+2\sqrt{2})^{2m} + 2(3-2\sqrt{2})^{2m} + 5 \quad (m = 1, 2, \dots).$$

We give one more application of Lemma 3.2 for the families of polynomial type.

Theorem 3.13. *Let n be a positive* (*even*) *integer.*

(i) *If* $2B = (n^4+2)^2(n^2+1)^2 - (n^4+2)$*, then the Hasse principle fails for equation* (3.1)*.*

(ii) *If* $2B = (n^4+2)^2(n^2-1)^2 - (n^4+2)$*, then the Hasse principle fails for equation* (3.2)*.*

Proof. This theorem follows from Lemma 3.2 together with the identities

$$(n^4+2)^2(n^2\pm 1)^2 - (n^4+2) = (n^4+2)\left\{(n^4\pm n^2+1)^2 \pm 2n^2\right\}.$$

□

Using the following proposition, we can construct infinitely many desired families.

Proposition 3.14. *Let k be a positive integer.*

(i) *Let $n = 2k^2+1$. Suppose that there exist positive integers α, β such that any prime divisor p of* $\gcd(k,\beta)$ *satisfies* $p \equiv 1$ *or* $3 \pmod 8$*. If*

$$2B = (n\alpha)^2 - n = n\{(n\beta)^2 + n - 1\}, \tag{3.5}$$

then the Hasse principle fails for equation (3.1)*.*

(ii) *Let $n = 2k^2-1$. Suppose that there exist positive integers α, β such that any prime divisor p of* $\gcd(k,\beta)$ *satisfies* $p \equiv 1$ *or* $7 \pmod 8$*. If*

$$2B = (n\alpha)^2 - n = n\{(n\beta)^2 - n - 1\}, \tag{3.6}$$

then the Hasse principle fails for equation (3.2)*.*

Proof. This proposition is an easy corollary of Lemma 3.2. □

Example 3.15. (i) The latter equation of (3.5) is equivalent to

$$\alpha^2 - n\beta^2 = 1.$$

Hence for each non-square n with $n = 2k^2+1$ one can easily express B satisfying (3.5) as a parametric family. For example, in case $n = 3$, an odd α satisfies $\alpha + \beta\sqrt{3} = (2+\sqrt{3})^{2m}$, which yields

$$B = \frac{3}{8}\left[3\left\{(2+\sqrt{3})^{4m} + (2-\sqrt{3})^{4m}\right\} + 2\right] \quad (m = 1, 2, \dots).$$

This family contains the example $B = 219$ of Sierpiński with $m = 1$ ($\alpha = 7$, $\beta = 4$).

(ii) Since the latter equation of (3.6) is equivalent to

$$\alpha^2 - n\beta^2 = -1, \tag{3.7}$$

there exists infinitely many n's with $n = 2k^2-1$ such that (3.7) is solvable and k and β satisfy the conditions in (ii) of Proposition 3.14. Indeed, there exist infinitely many n's of the form $n = 2k^2 - 1 = (2l)^2 + 1$ for positive integers l, and then $(\alpha, \beta) = (2l, 1)$ is a solution of (3.7). The condition on the prime divisors of $\gcd(\beta, k)$ is clearly satisfied. For each of such n's, one can easily express B satisfying (3.6) as a parametric family. For example, in case $n = 17$, an odd α satisfies $\alpha + \beta\sqrt{17} = (4+\sqrt{17})^{2m}$, which yields

$$B = \frac{17}{8}\left[17\left\{(4+\sqrt{17})^{4m} + (4-\sqrt{17})^{4m}\right\} + 30\right] \quad (m = 1, 2, \dots).$$

4 Solvability of the equation $X^2 - BY^2 = \pm 2$

In this section, we examine the solvability of equations

$$X^2 - BY^2 = -2, \tag{4.1}$$

$$X^2 - BY^2 = 2, \tag{4.2}$$

and congruences

$$X^2 - BY^2 \equiv -2 \pmod{N}, \tag{4.3}$$

$$X^2 - BY^2 \equiv 2 \pmod{N}. \tag{4.4}$$

Proposition 4.1. (i) *If $B \equiv 3 \pmod 8$ and any prime divisor p of B satisfies $p \equiv 1$ or $3 \pmod 8$, then congruence (4.3) is solvable for every integer $N > 1$.*

(ii) *If $B \equiv 7 \pmod 8$ and any prime divisor p of B satisfies $p \equiv 1$ or $7 \pmod 8$, then congruence (4.4) is solvable for every integer $N > 1$.*

Proof. The only differences from Proposition 3.1 are the conditions $B \equiv 3 \pmod 8$ and $B \equiv 7 \pmod 8$. They are necessary for the proof of solvability of equations (4.3) and (4.4) with N a power of 2. The rest is similar to the proof of Proposition 3.1. □

If B is even, then x must be even, which leads to the equation $2X^2 - BY^2 = \pm 1$. Thus, we only consider the odd B case. This is why we could only obtain the analogue of Theorem 3.3.

Theorem 4.2. *Let n be a positive integer.*

(i) *Let $a \geq 3$ be an integer such that any prime divisor p of a satisfies $p \equiv 1$ or $3 \pmod 8$. If n is odd and $B = n^2a^4 + 2a^2$, then equation (4.1) is unsolvable and equation (4.3) is solvable for every integer $N > 1$.*

(ii) *Let $a \geq 7$ be an integer such that any prime divisor p of a satisfies $p \equiv 1$ or $7 \pmod 8$. If n is odd and $B = n^2a^4 - 2a^2$, then equation (4.2) is unsolvable and equation (4.4) is solvable for every integer $N > 1$.*

Proof. The assumptions immediately implies that $n^2a^4 + 2a^2 \equiv 3 \pmod 8$ and $n^2a^4 - 2a^2 \equiv 7 \pmod 8$. The rest is similar to the proof of Theorem 3.3 (see also the proof of Lemma 3.2).

□

Remark 4.3. (1) If $a = 1$ in the above theorem, then each of equations (4.1) and (4.2) has a trivial solution $(x, y) = (n, 1)$.

(2) The minimal odd B's such that the Hasse principle fails for equations (4.1) and (4.2) are $B = 99(= 1 \cdot 3^4 + 2 \cdot 3^2)$ and $B = 791(= 28^2 + 7 = 7 \cdot 113)$, respectively.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York and London, 1966.

[2] A. Grelak and A. Grytczuk, Some remarks on matrices and Diophantine equation $Ax^2 - By^2 = C$, Discuss. Math. 10 (1990), 13–27.

[3] A. Grelak and A. Grytczuk, On the Diophantine equation $ax^2 - by^2 = c$, Publ. Math. Debrecen 44 (1994), 1–9.

[4] N. Kimura and K. S. Williams, Infinitely many insolvable Diophantine equations, Amer. Math. Monthly (2004), 909–913.

[5] R. A. Mollin, *Quadratics*, CRC Press, 1996.

[6] R. A. Mollin, Infinitely many quadratic Diophantine equations solvable everywhere locally, but not solvable globally, JP J. Algebra Number Theory Appl. 4 (2004), 353–362.

[7] W. Sierpiński, *Elementary theory of numbers*, Monografic Matematyczne, Tom 42, Państwowe Wydawnictwo Naukowe, Warsaw, 1964.

[8] H. Yokoi, On real quadratic fields containing units with norm -1, Nagoya Math. J. 33 (1968), 139–152.