On the generalized Ramanujan-Nagell equation $x^2 + D = p^z$

Clemens Heuberger Maohua Le*

October 12, 1998

Abstract

Let $p \in \{3, 23\}$ and $D \in \mathbb{N}$ such that $p \nmid D$ and $D > p$. We prove in this paper that the diophantine equation

$$x^2 + D = p^z, \qquad x, z \in \mathbb{N}$$

has at most one solution (x, z). Moreover, we give an explicit upper bound for z.

1 Introduction

For $D \in \mathbb{N}$ and p an odd prime with $p \nmid D$ we denote the number of solutions of the generalized Ramanujan-Nagell equation

$$x^2 + D = p^z, \qquad x, n \in \mathbb{N} \tag{1}$$

by $N(D, p)$.

In 1960, Apéry [1] showed that for squarefree D, the number of solutions is bounded by $N(D, p) \leq 2$. This bound is sharp: If

$$D = 3s^2 \pm 1, \qquad p = 4s^2 \pm 1, \qquad s \in \mathbb{N},$$

— in which case (D, p) is called exceptional —, (1) has the two solutions $(x, z) = (s, 1)$ and $(8s^3 \pm 3s, 3)$, hence $N(D, p) = 2$.

No examples of non-exceptional (D, p) are known such that $N(D, p) \geq 2$, so we might conjecture that for all non-exceptional (D, p), we have $N(D, p) = 1$. The second author proved [5, 6] this conjecture for $\max(D, p) > 10^{10^{192}}$.

In this paper we shall verify the conjecture for $p = 3$ and $p = 23$:

Theorem 1.1. *Let $D \in \mathbb{N}$ and $p \in \{3, 23\}$ with $p \nmid D$ and $2 \neq D$ if $p = 3$ and $D \neq 7, 14, 19, 22$ if $p = 23$. Then the equation (1) has at most one solution (x, z). Moreover, this solution satisfies*

$$z < \frac{4}{\pi}\sqrt{D}\log(2e\sqrt{D}). \tag{2}$$

Besides a result of Tzanakis and Wolfskill [11], we shall use a series of papers of the second author. Since some formulations in these papers are ambiguous and misleading, we prefer to reformulate and reprove these results in a version suitable for our purposes. In order to make the exposition clear, we try to be rather explicit.

*Supported by the National Natural Science Foundation of China and Guangdong Provincial Natural Science Foundation

2 Binary quadratic forms

Let $a, b, c \in \mathbb{Z}$ and $D := b^2 - ac$. Then the form $F \in \mathbb{Z}[X, Y] = \mathbb{Z}[\mathbf{X}]$

$$F = aX^2 + 2bXY + cY^2 = \mathbf{X}^t \begin{pmatrix} a & b \\ b & c \end{pmatrix} \mathbf{X}$$

is called *binary quadratic form* with *discriminant* $4D$. For short, we write $F = \{a, 2b, c\}$. F is called *primitive*, if $\gcd(a, 2b, c) = 1$.

In the literature, binary quadratic forms are often introduced as $F = aX^2 + bXY + cY^2$ with $a, b, c \in \mathbb{Z}$, where the discriminant is defined as $b^2 - 4ac$, so yielding the same as in our notation, which restricts us to the case of an even discriminant. However, this notation will be enough for us.

Two binary quadratic forms $F = \mathbf{X}^t\mathbf{A}\mathbf{X}$ and $G = \mathbf{X}^t\mathbf{B}\mathbf{X}$ are called *equivalent*, written $F \sim G$, if there exists a Matrix $\mathbf{T} \in \mathrm{SL}(2, \mathbb{Z})$, i. e. a matrix $\mathbf{T}$ with $\det \mathbf{T}=1$, such that

$$\mathbf{A} = \mathbf{T}^t\mathbf{B}\mathbf{T}.$$

It is clear that this relation is an equivalence relation. Equivalent forms have the same discriminant, they are both primitive or not.

Theorem 2.1. *Let $\sim$ be the equivalence relation introduced above. Then the set of binary quadratic forms of discriminant $4D$ is partitioned into a finite number of equivalence classes. The number of classes of primitive binary quadratic forms of discriminant $4D$ is denoted by $h(4D)$.*

Proof. See for example Hua [4], Theorem 12.2.2. □

Proposition 2.2. *Let $D \leq -1$. Then the number of classes of primitive binary quadratic forms of discriminant $4D$ can be bounded by*

$$h(4D) \leq \frac{4\sqrt{|D|}}{\pi} \log(2e\sqrt{|D|}).$$

Proof. Combine Hua [4], Theorems 12.10.1, 12.14.3, and 11.4.3. For $D = -1$, see for example Exercise 2 at the end of 12.2 of [4]. □

3 Representations and characteristic numbers

Let F be a binary quadratic form. If $K, x, y \in \mathbb{Z}$ and

$$K = F(x, y) \qquad \gcd(x, y) = 1, \tag{3}$$

then (3) is called a *representation of K*.

In this section, we describe some properties of such representations. We follow Le [7].

Lemma 3.1. *Let $K = F(x, y)$ be a representation. Then there exists a unique $L \in \mathbb{Z}$ such that there are $\alpha, \beta \in \mathbb{Z}$ satisfying*

$$\beta x - \alpha y = 1$$
$$L = \alpha(ax + by) + \beta(bx + cy), \quad L^2 \equiv D \pmod{K}, \quad 0 \leq L < |K|\,.$$

It is called the characteristic number of the representation, we denote it by $L(F, x, y)$.

Proof. See Hua [4], Theorem 4.1. □

Lemma 3.2. *Let F be a binary quadratic form of discriminant $4D$, $K = F(x, y)$ a representation and $L = L(F, x, y)$ its characteristic number. Put $K' = (L^2 - D)/K$. Then the form F is equivalent to the form $\{K, 2L, K'\}$.*

Proof. Use the transformation matrix $T = \begin{pmatrix} x & \alpha \\ y & \beta \end{pmatrix}$. □

Lemma 3.3. *Let $K, L, D \in \mathbb{Z}$. Then the following two assertions are equivalent:*

1. *There is a primitive binary quadratic form F with discriminant $4D$ and there are $x, y \in \mathbb{Z}$ such that $F(x, y)$ is a representation of K and its characteristic number is L.*
2. *We have*

$$L^2 \equiv D \pmod{K}, \qquad 0 \le L < |K|, \qquad \gcd\left(K, 2L, \frac{L^2 - D}{K}\right) = 1.$$

Proof.$1 \Rightarrow 2$ The first two relations follow from Lemma 3.1. The last condition is satisfied because the form $\{K, 2L, \frac{L^2-D}{K}\}$ is equivalent to the primitive form F by Lemma 3.2.

$2 \Rightarrow 1$ Put $K' = (L^2 - D)/K$. It is an integer by the congruence condition. $F = \{K, 2L, K'\}$ is a binary quadratic form, it is primitive by the last condition of 2. Clearly, $F(1, 0)$ is a representation of K, taking $\alpha = 0$ and $\beta = 1$, we see that its characteristic number is L. □

Lemma 3.4. *Let F, F' be binary quadratic forms of discriminant $4D$. Furthermore, let x, y, x', $y' \in \mathbb{Z}$ such that $F(x, y) = K = F'(x', y')$ are representations and $L(F, x, y) = L = L(F', x', y')$. Then we have $F \sim F'$.*

Proof. This is clear, since both forms are equivalent to the form $\{K, 2L, K'\}$ by Lemma 3.2. □

Lemma 3.5. *Let $F = \{a, 2b, c\}$ be a binary quadratic form, $K, x, y \in \mathbb{Z}$ such that $K = F(x, y)$ is a representation of K and $L = L(F, x, y)$. Then we have*

$$ax + by \equiv -Ly \pmod{K}.$$

Proof. This is (7) in the proof of Theorem 11.4.2 in Hua [4]. □

Lemma 3.6. *Let $F = \{a, 2b, c\}$ be a primitive binary quadratic form of discriminant $4D$ and $K, x, y, x', y' \in \mathbb{Z}$ such that $F(x, y) = K$ is a representation. Moreover assume that D is not a square and $aK \neq 0$. Then the following two conditions are equivalent*

1. *We have the representation $K = F(x', y')$ and $L(F, x, y) = L(F, x', y')$.*
2. *There exist $u, v \in \mathbb{Z}$ such that*

$$u^2 - Dv^2 = 1$$

and

$$ax' + by' + y'\sqrt{D} = (ax + by + y\sqrt{D})(u + v\sqrt{D}).$$

Proof. See Hua [4], Theorem 11.4.2. □

4 Composition of forms

We describe a group law on the set of equivalence classes of binary quadratic forms following Cassels [3].

Lemma 4.1. *Let $\mathcal{C}_1$, $\mathcal{C}_2$ be two equivalence classes of primitive forms of discriminant $4D$. Then there exist two forms $F_j = \{a_j, 2b, c_j\} \in \mathcal{C}_j$ for $j = 1, 2$ such that the middle coefficient is the same and $\gcd(a_1, a_2) = 1$.*

Proof. This is Lemma 2.3 of chapter 14 in Cassels [3]. □

Let $F_j \in \mathcal{C}_j$ be two forms as described in the above lemma. We define the composition of these two forms to be the form $F = \{a_1a_2, 2b, (b^2 - D)/(a_1a_2)\}$. This composition of forms gives a unique composition of form classes:

Lemma 4.2. *Let $0 \neq D \in \mathbb{Z}$. Let $\mathcal{C}_1, \mathcal{C}_2$ be two classes of primitive forms of discriminant $4D$. Then there is a class $\mathcal{C}$ such that the composition of $f_j \in \mathcal{C}_j$, $j = 1, 2$, always lies in $\mathcal{C}$. In this case, we write $\mathcal{C} = \mathcal{C}_1\mathcal{C}_2$.*

Proof. This is Lemma 2.4 of chapter 14 in Cassels [3]. □

Theorem 4.3. *The composition of classes defined in the above lemma gives the set of primitive classes of binary quadratic forms of discriminant $4D$ the structure of a finite abelian group. The neutral element of the group is the class containing all forms representing 1, denoted by $\mathcal{E}$.*

Proof. Theorem 2.1 of chapter 14 in Cassels [3]. □

5 Representations of k^n

In this section we shall derive some properties of representations of k^n. Throughout this section, D and k will be fixed integers with $\gcd(D, k) = 1$ and $2 \nmid k$. We will follow Le [7].

Lemma 5.1. *Let F be a binary quadratic form of discriminant $4D$ and $x, y, z \in \mathbb{Z}$ such that there is a representation $k^z = F(x, y)$. Let $L = L(F, x, y)$. Then there exists a unique $l \in \mathbb{Z}$ such that*

$$\begin{gathered} L \equiv \pm l \pmod{k} \\ l^2 \equiv D \pmod{k}, \qquad 0 < l < \frac{|k|}{2}, \qquad \gcd\left(k, 2l, \frac{l^2 - D}{k}\right) = 1 \end{gathered} \tag{4}$$

We denote this unique l by $l(F, x, y)$.

Proof. By Lemma 3.3 we have

$$L^2 \equiv D \pmod{k}, \qquad 0 < L < |k^z|, \qquad \gcd\left(k^z, 2L, \frac{L^2 - D}{k^z}\right) = 1.$$

There is a unique $l' \in \mathbb{Z}$ such that $L \equiv l' \pmod{k}$ and $0 < l' < |k|$, hence we have $l'^2 \equiv D \pmod{k}$. Since we assumed $\gcd(D, k) = 1$, we have $\gcd(k, 2l') = 1$, hence $\gcd(k, 2l', (l'^2 - D)/k) = 1$. We define

$$l = \begin{cases} l' & \text{if } l' < |k|/2 \\ |k| - l' & \text{otherwise} \end{cases}$$

This unique l satisfies all assertions of the lemma. □

The following lemma shows that it is enough to know the characteristic number of a representation of k^n modulo k.

Lemma 5.2. *Let F_1, F_2 be two binary quadratic forms of discriminant $4D$, $n \in \mathbb{N}$. For $i = 1, 2$ let $x_i, y_i \in \mathbb{Z}$ such that $F_1(x_1, y_1) = k^n = F_2(x_2, y_2)$ and $l(F_1, x_1, y_1) = l = l(F_2, x_2, y_2)$. Then we have*

$$L(F_2, x_2, y_2) \in \{L(F_1, x_1, y_1), |k|^n - L(F_1, x_1, y_1)\}.$$

Proof. For $i = 1, 2$ write $L_i = L(F_i, x_i, y_i)$. By definition of l we have $L_1 \equiv uL_2 \pmod{k}$, where $u = \pm 1$. We claim that

$$L_1 \equiv uL_2 \pmod{k^n}.$$

Let $k = \prod p_j^{\alpha_j}$ be the prime factor decomposition of k. By Lemma 3.1 we have

$$L_i^2 \equiv D \pmod{p_j^{n\alpha_j}}, \qquad i = 1, 2.$$

By HUA [4], Theorem 2.9.3, the equations

$$X^2 \equiv D \pmod{p_j^{n\alpha_j}} \tag{5}$$

$$X^2 \equiv D \pmod{p_j} \tag{6}$$

have the same number of solutions, since $X^2 - D \equiv 0 \pmod{p_j}$ and $2X \equiv 0 \pmod{p_j}$ has no common solution since $2 \nmid k$ and $\gcd(D, k) = 1$. Since (6) has exactly 2 solutions (namely $\pm L_1$), the same is true for (5). Since $L_1 \equiv uL_2 \pmod{p_j}$, the same congruence holds $\mod p_j^{n\alpha_j}$, which yields the assertion. □

Lemma 5.3. *Assume that D is a quadratic residue modulo k. Denote the number of distinct prime factors of k by $\omega(k)$. Then there are exactly $2^{\omega(k)-1}$ integers l satisfying* (4) .

Proof. All solutions of (4) satisfy

$$l^2 \equiv D \pmod{k}, \qquad 0 < l < |k| .$$

This congruence has $2^{\omega(k)}$ solutions by HUA [4], Theorem 2.8.1, and Lemma 5.2, since it has one solution by assumption. Since $2 \nmid k$, the assertion of the lemma follows. □

Lemma 5.4. *1. Let F be a binary quadratic form and $x, y \in \mathbb{Z}$ such that we have a representation $F(x, y) = k$, $\mathcal{C}_r$ the class of F and $n \in \mathbb{N}$. Then there are a form F' and integers x', y' such that we have a representation $k^n = F'(x', y')$ satisfying $L(F, x, y) \equiv L(F', x', y') \pmod{k}$ and $\mathcal{C}_s = \mathcal{C}_r^n$, where $\mathcal{C}_s$ denotes the class of F'.*

2. Conversely, if there are a form F' and integers x', y' such that k^n has a representation $k^n = F'(x', y')$, then there exist a form F and integers x, y such that we have a representation $k = F(x, y)$ satisfying $L(F, x, y) \equiv L(F', x', y') \pmod{k}$, and $\mathcal{C}_s = \mathcal{C}_r^n$, where $\mathcal{C}_s$ and $\mathcal{C}_r$ denote the classes of F' and F respectively.

Proof. 1. We proceed by induction on n. For $n = 1$, there is nothing to prove. For $n > 1$, we suppose that there exist F'', x'', y'' such that $k^{n-1} = F''(x'', y'')$ with characteristic number $L'' = L(F'', x'', y'')$ satisfying $L'' \equiv L \pmod{k}$, where $L := L(F, x, y)$ and $F'' \in \mathcal{C}_r^{n-1}$. By Lemma 3.2, F and F'' are equivalent to the forms $\{k, 2L, *\}$ and $\{k^{n-1}, 2L'', *\}$ respectively, where $*$ denotes some integer which is of no importance for us. By HUA [4], Theorem 2.9.3, — cf. the proof of Lemma 5.2 — there is a L' satisfying $L'^2 \equiv D \pmod{k^n}$ and $L' \equiv L'' \pmod{k^{n-1}}$ and $L' \equiv L \equiv L'' \pmod{k}$. Hence we have q, r such that $L' = L'' + rk^{n-1} = L + qk$, hence transforming the above forms by $\left(\begin{smallmatrix} 1 & q \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$ respectively, we see that $F \sim \{k, 2L', *\}$ and $F'' \sim \{k^{n-1}, 2L', *\}$. The composition of these two forms is a form $F' = \{k^n, 2L', \frac{L'^2 - D}{k^n}\}$, which is therefore in the class $\mathcal{C}_r^n$, represents $k^n = F(1, 0)$, and fulfills $L' \equiv L \pmod{k}$ by construction.

2. Write $L' = L(F', x', y')$. Then there is a unique $L \equiv L' \pmod{k}$, which satisfies $L^2 \equiv D \pmod{k}$, $0 < L < |k|$ and $\gcd(k, 2L, (L^2 - D)/k) = 1$ — see the proof of Lemma 5.1. By Lemma 3.3 we see that there are a form F and integers x, y such that there is a representation $k = F(x, y)$ with $L = L(F, x, y)$. We still have to prove the assertion about the classes. By the first part of the lemma, there are a form F'' and integers x'', y'' such that we have a representation $k^n = F''(x'', y'')$ with an $L'' = L(F'', x'', y'')$ satisfying $L'' \equiv L' \pmod{k}$. By the proof of Lemma 5.2 this yields $L'' = L'$, hence by Lemma 3.4 $F'' \sim F'$. Hence the class $\mathcal{C}_s$ is that of F'', which is $\mathcal{C}_r^n$ by the first part of the lemma.

□

6 The diophantine equation $D_1X^2 - D_2Y^2 = k^Z$

Let $D_1, D_2, k \in \mathbb{Z}$, $D := D_1D_2$, $\gcd(D_1, D_2) = 1$, $\gcd(D, k) = 1$, $2 \nmid k$, and D non square. We are interested in the diophantine equation

$$D_1X^2 - D_2Y^2 = k^Z, \qquad \gcd(X, Y) = 1, \qquad Z > 0 \tag{7}$$

We will follow Le [7].

Clearly, $F^* := D_1X^2 - D_2Y^2$ is a primitive form of discriminant $4D$. Each solution (x, y, z) of (7) is a representation

$$k^z = F^*(x, y). \tag{8}$$

By Lemma 5.1 we have a unique number $l = l(F^*, x, y)$ associated to each solution. We define

$$S_l := \{(x, y, z) \text{ solution of } (7) : l = l(F^*, x, y)\}.$$

We will prove the following two theorems:

Theorem 6.1. *Let the notations be as described above. Let l be such that $S_l \neq \emptyset$.*

Then there is a positive solution $(x_l, y_l, z_l) \in S_l$ such that $z_l \leq z$ for all $(x, y, z) \in S_l$. If there are integer solutions (u, v) to the equation

$$D_1u^2 - D_2v^2 = 1, \tag{9}$$

then we have $z_l \mid h(4D)$, otherwise, we have $2z_l \mid h(4D)$, where $h(4D)$ denotes the number of classes of primitive binary quadratic forms of discriminant $4D$.

Theorem 6.2. *Let the notations be as described above. Additionally, let $D_1 = 1$. Assume that (7) has a solution. Then all solutions of (7) can be put in exactly $2^{\omega(k)-1}$ classes S_l, where $\omega(k)$ denotes the number of distinct prime factors of k. For each solution class S_l, let (x_l, y_l, z_l) be a solution as described in Theorem 6.1. Then all solutions $(x, y, z) \in S_l$ can be described as*

$$z = z_lt, \qquad x + y\sqrt{D} = (x_l \pm y_l\sqrt{D})^t(u + v\sqrt{D}), \tag{10}$$

where $t \in \mathbb{N}$ and (u, v) is a solution of

$$u^2 - Dv^2 = 1. \tag{11}$$

We denote the class of F^* by $\mathcal{C}^*$. Furthermore, we define

$$S_l^+ = \{(x, y, z) \in S_l : D_1x \equiv -ly \pmod{k}\}$$
$$S_l^- = \{(x, y, z) \in S_l : D_1x \equiv +ly \pmod{k}\}.$$

Lemma 3.5 and Lemma 5.1 show that $S_l^+ \cup S_l^- = S_l$. Lemma 5.2 shows that all representations $k^z = F^*(x, y)$ from S_l^+ with z fixed have the same characteristic number $L(F^*, x, y)$.

Lemma 6.3. *We have*

$$|\mathcal{C}^*| = \begin{cases} 1, & \text{if (9) has solutions} \\ 2, & \text{otherwise.} \end{cases}$$

Proof. The form F^* is equivalent to the form $\overline{F}^* = \{-D_2, 0, D_1\}$ via the transformation matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. The composition of F^* and $\overline{F}^*$ is $\{-D, 0, 1\}$, so $\mathcal{C}^{*2} = \mathcal{E}$ by Theorem 4.3, hence $|\mathcal{C}^*| \in \{1, 2\}$.

If (9) has a solution (u, v), then we have $\gcd(u, v) = 1$, hence there are $r, s \in \mathbb{Z}$ such that we have $us - vr = 1$, then we have

$$\begin{pmatrix} u & v \\ r & s \end{pmatrix} \begin{pmatrix} D_1 & 0 \\ 0 & -D_2 \end{pmatrix} \begin{pmatrix} u & r \\ v & s \end{pmatrix} = \begin{pmatrix} u^2D_1 - v^2D_2 & ruD_1 - svD_2 \\ ruD_1 - svD_2 & r^2D_1 - s^2D_2 \end{pmatrix},$$

hence $\mathcal{C}^* = \mathcal{E}$ is the unit class. Conversely, if $\mathcal{C}^*$ is the unit class, then 1 can be represented by F^*, hence we find a solution to (9) by the above calculation. □

Lemma 6.4. *Let l be a number satisfying (4) such that $F_0 = \{k, 2l, *\}$ is a primitive binary form of discriminant $4D$. Let $z \in \mathbb{N}$ and $\mathcal{C}_0$ be the class of F_0. Then the following two assertions are equivalent:*

1. *There are x, y such that $(x, y, z) \in S_l^+$.*

2. *We have $\mathcal{C}_0^z = \mathcal{C}^*$.*

Proof. $1 \Rightarrow 2$ Let $(x, y, z) \in S_l^+$. Then we have a representation $k^z = F^*(x, y)$. Write $L = L(F^*, x, y)$. By Lemma 5.4, there are a form F_1 and integers x_1, y_1 such that $k = F_1(x_1, y_1)$. Writing $L_1 = L(F_1, x_1, y_1)$, we have $L_1 \equiv L \equiv l \pmod{k}$, since $(x, y, z) \in S_l^+$. This yields $L_1 = l$. Hence $F_1 \in \mathcal{C}_0$ by Lemma 3.4, and we have $\mathcal{C}_0^z = \mathcal{C}^*$ by Lemma 5.4.

$2 \Rightarrow 1$ Clearly, we have a representation $k = F_0(1, 0)$ with $L(F_0, 1, 0) = l$. By Lemma 5.4 there are a form F_1, integers x_1, y_1 and a representation $k^z = F_1(x_1, y_1)$ with $L_1 := L(F_1, x_1, y_1) \equiv l \pmod{k}$. By Lemma 5.4, $F_1 \in \mathcal{C}_0^z = \mathcal{C}^*$, i. e. $F_1 \sim F^*$, hence we can write

$$F_1 = \mathbf{X}^t \mathbf{T}^t \begin{pmatrix} D_1 & 0 \\ 0 & -D_2 \end{pmatrix} \mathbf{T} \mathbf{X}$$

with some $\mathbf{T} \in \mathrm{SL}(2, \mathbb{Z})$. Putting $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \mathbf{T} \left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right)$, we have a representation $F^*(x, y) = k^z$. Let $\alpha_1, \beta_1 \in \mathbb{Z}$ such that $\beta_1 x_1 - \alpha_1 y_1 = 1$ and $L_1 = \left(\begin{smallmatrix} \alpha_1 & \beta_1 \end{smallmatrix}\right) \mathbf{T}^t \left(\begin{smallmatrix} D_1 & 0 \\ 0 & -D_2 \end{smallmatrix}\right) \mathbf{T} \left(\begin{smallmatrix} x_1 \\ y_1 \end{smallmatrix}\right)$. Put $\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right) := T \left(\begin{smallmatrix} \alpha_1 \\ \beta_1 \end{smallmatrix}\right)$. Then we have

$$\begin{pmatrix} x & \alpha \\ y & \beta \end{pmatrix} = \mathbf{T} \begin{pmatrix} x_1 & \alpha_1 \\ y_1 & \beta_1 \end{pmatrix},$$

hence $\beta x - \alpha y = 1$ and

$$\begin{pmatrix} \alpha & \beta \end{pmatrix} \begin{pmatrix} D_1 & 0 \\ 0 & -D_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = L_1,$$

hence $L_1 = L(F^*, x, y)$ and $(x, y, z) \in S_l^+$.

□

Proof of Theorem 6.1. There exists a $(x_l^+, y_l^+, z_l^+) \in S_l^+$ such that $z_l^+ \le z$ for all $(x, y, z) \in S_l^+$. Since $(x, y, z) \in S_l^+$ implies $(x, -y, z) \in S_l^-$, we have $z_l^+ \le z$ for all $(x, y, z) \in S_l$. Since $(x, y, z) \in S_l^+$ is equivalent to $(-x, y, z) \in S_l^-$, we can choose a positive solution $(x_l, y_l, z_l) \in S_l$ with $z_l = z_l^+$.

By Lemma 6.4 we see that z_l is the minimal z such that $\mathcal{C}_0^z = \mathcal{C}^*$. If (9) has solutions, then $\mathcal{C}^*$ is the unit class by Lemma 6.3, hence $z_l = |\mathcal{C}_0| \mid h(4D)$. Otherwise, $2z_l = |\mathcal{C}_0| \mid h(4D)$. □

Proof of Theorem 6.2. Since there exists one solution to (4), there are $2^{\omega(k)-1}$ solutions to (4) by Lemma 5.3. Fix one such solution l. Since (9) has obviously the solution $(1, 0)$, we have $|\mathcal{C}^*| = 1$ by Lemma 6.3. So by Lemma 6.4, there is a solution $(x_l, y_l, z_l) \in S_l$ such that $z_l = |\mathcal{C}_0|$. Still by Lemma 6.4 there is a solution $k^z = F^*(x, y)$ if and only if there is a $t \in \mathbb{N}$ such that $z = z_l t$. Without restriction, we assume that $(x_l, y_l, z_l) \in S_l^+$.

We consider now

$$z_t = z_l t, \qquad x_t + y_t \sqrt{D} = (x_l + y_l \sqrt{D})^t.$$

Since D is not a square, this yields

$$x_t = \sum_{i=0}^{\lfloor t/2 \rfloor} \binom{t}{2i} D^i x_l^{t-2i} y_l^{2i}, \qquad y_t = \sum_{i=0}^{\lfloor (t-1)/2 \rfloor} \binom{t}{2i+1} D^i x_l^{t-2i-1} y_l^{2i+1}$$

and

$$x_t \equiv 2^{t-1} x_l^t \pmod{k}, \qquad y_t \equiv 2^{t-1} x_l^{t-1} y_l \pmod{k}.$$

For clearly $x_t^2 - D y_t^2 = k^{z_l t} = k^{z_t}$. Hence any prime q dividing $\gcd(x_t, y_t)$ divides k, hence $2^{t-1} x_l^t$. Since $2 \nmid k$, we have $q \mid x_l$, $q \mid D y_l^2$, hence $q \mid y_l$ since $\gcd(D, k) = 1$. This is a contradiction to $\gcd(x_l, y_l) = 1$. Moreover, $\gcd(k, y_t) = 1$. Since $x_t \equiv -l y_t \pmod{k}$, we see that $(x_t, y_t, z_t) \in S_l^+$.

By Lemma 5.2 and Lemma 3.6, we get the representation (10), since $(x_l, -y_l, z_l) \in S_l^-$.

□

7 The diophantine equation $x^2 + D = p^z$

In this section, we will prove Theorem 1.1.

The crucial point of the of Tzanakis and Wolfskill [11], which is based on hypergeometric methods:

Proposition 7.1. *Let $q > 0$ be an integer, not a square. Assume*

$$x^2 + \Delta = a^2 w,$$

where w is an odd power of q, a is a positive integer and x, Δ any integers. Let r, s be positive integers such that

$$a^2 w \geq |\Delta|^{2+s/r} \cdot 4^{1+s/r}$$

and define ν by

$$w^\nu = 9a^2(81a^2 w/4)^{r/s}.$$

Let $N > w$ be an odd power of q and y any integer. Then

$$\left| \frac{y}{2\sqrt{N}} - 1 \right| > \frac{8}{2187 a^5 w^{3+\nu/2}} \left(\frac{81a^2 w}{4} \right)^{1/s} N^{-(1+\nu)/2}.$$

Proof. See Tzanakis and Wolfskill [11], Theorem I.2. □

Corollary 7.2. *Let m be any integer and $2 \nmid l$. Then we have*

$$\left| \frac{m}{3^{l/2}} - 1 \right| > 3^{-51.2 - 0.961 \cdot l} \tag{12a}$$

$$\left| \frac{m}{23^{l/2}} - 1 \right| > 23^{-17.2 - 0.968 \cdot l} \tag{12b}$$

Proof. Using the above proposition with

x	Δ	q	w	a	Equation	r	s	N	y	ν
3788	-37	3	3^{15}	1	$3788^2 - 37 = 3^{15}$	2	3	q^l	$2m$	.9217
2537	-26	23	23^5	1	$2537^2 - 26 = 23^5$	2	3	q^l	$2m$	.9347,

we get the assertions for $l > 15$ (resp. $l > 5$). The remaining cases can be verified by direct calculation. □

We will need the following properties of $p = 3, 23$ in the proof of our theorem:

1. $p \equiv 3 \pmod 4$ is a prime.
2. If $u_0 + \sqrt{p} v_0$ is the fundamental solution of Pell's equation

   $$u^2 - p v^2 = 1,$$

   then $p \nmid v_0$.

   For general p, this is an open question, see Mordell [10] and Beach, Williams, and Zarnke [2].
3. We have an estimate such as (12) with $\nu < 1$.

A computer search in the range $3 \leq p \leq 500$, $p < w < p^{500}$ found only two primes with these properties, namely 3 and 23.

We need the following special case of *Waring's Formula* (see [9, Theorem 1.76])

Lemma 7.3. *Let X, Y be indeterminates over a ring R and $t \in \mathbb{N}$. Then we have*

$$X^t + Y^t = \sum_{i=0}^{\lfloor t/2 \rfloor} (-1)^i \frac{(t-i-1)!t}{(t-2i)!i!}(X+Y)^{t-2i}(XY)^i,$$

where the coefficients $\frac{(t-i-1)!t}{(t-2i)!i!}$ are positive integers.

The following Lemma is a special case of Lemma 4 in Le [8]

Lemma 7.4. *Let p be an odd prime and $u_1 + v_1\sqrt{p}$ the fundamental solution of Pell's equation $u^2 - pv^2 = 1$ and (u, v) an arbitrary positive solution of the same equation. If $p \nmid v_1$ and $p^m \mid v$ for some $m \in \mathbb{N}$, then we have*

$$u + v\sqrt{p} = (u_1 + v_1\sqrt{p})^{p^m r}$$

for some $r \in \mathbb{N}$.

Proof. Since $u_1 + v_1\sqrt{p}$ is the fundamental solution of the equation, we have a representation

$$u + v\sqrt{p} = (u_1 + v_1\sqrt{p})^t$$

for some $t \in \mathbb{N}$. This yields

$$v = \sum_{0 \le 2l+1 \le t} \binom{t}{2l+1} u_1^{t-2l-1} v_1^{2l+1} p^l.$$

Let k be maximal such that $p^k \mid t$ and β_{2l+1} be maximal such that $p^{\beta_{2l+1}} \mid 2l+1$ for $0 \le 2l+1 \le t$. We have $\beta_{2l+1} \le \log(2l+1)/\log p$. If $p \ge 5$ and $l \ge 1$, we have $\beta_{2l+1} \le l-1$, since $\log(2l+1)/\log p \le \log(2l+1)/\log 5 \le l-1$ for $l \ge 2$ and $\beta_3 = 0$. If $p = 3$, we have similarly $\beta_{2l+1} \le l-1$ for $l \ge 2$.

Hence we have for $l \ge 1$ and $p \ne 3$

$$\binom{t}{2l+1} u_1^{t-2l-1} v_1^{2l+1} p^l = \frac{t}{2l+1}\binom{t-1}{2l} u_1^{t-2l-1} v_1^{2l+1} p^l \equiv 0 \pmod{p^{k-\beta_{2l+1}+l}}.$$

Since $k - \beta_{2l+1} + l \ge k+1$, we see that $v \equiv tu^{t-1}v_1 \pmod{p^{k+1}}$, which yields $p^m \mid t$.

If $p = 3$, we have $v \equiv tu_1^{t-1}v_1 \pmod 3$, hence $t \equiv 0 \pmod 3$. By the argument of above, we see

$$v \equiv u_1^{t-3} t \left(u_1^2 + \frac{(t-1)(t-2)}{2} v_1^2 \right) \pmod{3^{k+1}}$$

Since $u_1^2 + (t-1)(t-2)/2v_1^2 \equiv 2 \pmod 3$ for $t \equiv 0 \pmod 3$, we again have $3^m \mid t$. □

Proof of Theorem 1.1. Assume that (1) has a solution (x_0, z_0). We consider the equation

$$X^2 + DY^2 = p^Z, \qquad \gcd(X, Y) = 1, \qquad Z > 0. \tag{13}$$

Obviously, it has the solution $(x_0, 1, z_0)$, hence by Theorem 6.2, it has one solution class and a solution (x_1, y_1, z_1) such that all solutions (x, y, z) of (13) can be described as

$$z = z_1 t, \qquad x + y\sqrt{-D} = \pm(x_1 \pm y_1\sqrt{-D})^t,$$

since $u^2 + Dv^2 = 1$ only has the solutions $(\pm 1, 0)$ for $D > 1$. If $D = 1$, then (13) has no solution, since $(\frac{-1}{p}) = -1$ for $p \equiv 3 \pmod 4$. This yields for the solution $(x_0, 1, z_0)$

$$\pm 1 = y_1 \left(\sum_{0 \le 2l+1 \le t} \binom{t}{2l+1} x_1^{t-2l-1} (\pm y_1)^{2l} (-D)^l \right),$$

hence $y_1 = 1$ and $(x_1, 1, z_1)$ is a solution of (1).

Assume now that we have at least two solutions (x, z) and (x_1, z_1) of (1). By the above discussion, we have

$$z = z_1 t, \qquad x + \sqrt{-D} = \lambda_1 (x_1 + \lambda_2 \sqrt{-D})^t, \qquad \lambda_1, \lambda_2 \in \{\pm 1\}.$$

Moreover $z_1 \geq 2$, since we excluded some values of D in the formulation of the theorem. Putting $\varepsilon = x_1 + \sqrt{-D}$ and $\overline{\varepsilon} = x_1 - \sqrt{-D}$, hence

$$\varepsilon + \overline{\varepsilon} = 2x_1, \qquad \varepsilon - \overline{\varepsilon} = 2\sqrt{-D}, \qquad \varepsilon\overline{\varepsilon} = p^{z_1} \tag{14}$$

we see that

$$\pm(\varepsilon^t - \overline{\varepsilon}^t) = \varepsilon - \overline{\varepsilon} = 2\sqrt{-D}. \tag{15}$$

Let τ be the minimal $t > 1$ such that (15) holds. Assume that τ is not a prime, $\tau = rs$, where $r, s > 1$. Then

$$2\sqrt{-D} = (\varepsilon^r - \overline{\varepsilon}^r)m = m2\sqrt{-D} \sum_{0 \leq 2l+1 \leq r} \binom{r}{2l+1} x_1^{r-2l-1} (-D)^l,$$

where m is the integer

$$m = \sum_{k=0}^{s-1} \varepsilon^{rk} \overline{\varepsilon}^{r(s-1-k)},$$

which implies that already $\pm(\varepsilon^r - \overline{\varepsilon}^r) = 2\sqrt{-D}$. Therefore, τ is a prime. Assume $\tau = 2$. Then we have

$$\pm 2\sqrt{-D} = (\varepsilon + \overline{\varepsilon})(\varepsilon - \overline{\varepsilon}) = 2x_1 2\sqrt{-D},$$

which is impossible. Therefore, τ is an odd prime.

For any $m \in \mathbb{N}$ we define $E(m) = (\varepsilon^m - \overline{\varepsilon}^m)/(\varepsilon - \overline{\varepsilon})$. By definition of τ, we have $E(\tau) = \pm 1$. Since by (14) and Lemma 7.3

$$E(m) = \sum_{i=0}^{m-1} \varepsilon^i \overline{\varepsilon}^{m-1-i} \equiv \varepsilon^{m-1} + \overline{\varepsilon}^{m-1} \equiv (\varepsilon + \overline{\varepsilon})^{m-1} \equiv (2x_1)^{m-1} \pmod{p},$$

and since $p \mid x_1$ implies $p \mid D$, we see that $E(m) \neq 0$. Clearly, $E(m) \in \mathbb{Z}$ for all integers m.

Since $E(\tau) = \pm 1$, we have

$$E(\tau) = \left(E\left(\frac{\tau+1}{2}\right)\right)^2 - p^{z_1}\left(E\left(\frac{\tau-1}{2}\right)\right)^2 = \pm 1.$$

Since $E(m) \neq 0$, the case $2 \mid z_1$ is impossible. A consideration mod4 shows that this implies

$$E(\tau) = \left(E\left(\frac{\tau+1}{2}\right)\right)^2 - p^{z_1}\left(E\left(\frac{\tau-1}{2}\right)\right)^2 = 1, \tag{16}$$

since $p \equiv 3 \pmod 4$. Hence

$$(u, v) := \left(\left|E\left(\frac{\tau+1}{2}\right)\right|, p^{(z_1-1)/2}\left|E\left(\frac{\tau-1}{2}\right)\right|\right)$$

is a solution of Pell's equation $u^2 - pv^2 = 1$. Let $u_0 + v_0\sqrt{p}$ be its fundamental solution. For the primes under investigation, we have $p \nmid v_0$. By Lemma 7.4, there is a $r \in \mathbb{N}$ such that

$$\left|E\left(\frac{\tau+1}{2}\right)\right| + p^{(z_1-1)/2}\left|E\left(\frac{\tau-1}{2}\right)\right|\sqrt{p} = (u_0 + v_0\sqrt{p})^{p^{(z_1-1)/2}r}. \tag{17}$$

Since for any positive integer m, we have

$$|E(m)| = \left| \sum_{i=0}^{m-1} \varepsilon^{m-1-i} \overline{\varepsilon}^{i} \right| \leq \sum_{i=0}^{m-1} |\varepsilon|^{m-1-i} \, |\overline{\varepsilon}|^{i} = m p^{z_1 \frac{m-1}{2}},$$

we see from (17) that

$$(u_0 + v_0\sqrt{p})^{p^{(z_1-1)/2}} \leq \tau p^{z_1(\tau-1)/4}.$$

Assume now $\tau \leq 2p^{(z_1-1)/2}/z_1$. Then we get

$$z_1 \left(v_0 + \frac{u_0}{\sqrt{p}} \right)^{p^{(z_1-1)/2}} \leq 2p^{\frac{z_1-2}{4}}.$$

Since $v_0 + u_0/\sqrt{p} \geq 2$, we get

$$\log z_1 + p^{(z_1-1)/2} \log 2 \leq \frac{z_1 - 2}{4} \log p + \log 2.$$

This is impossible for $z_1 \geq 3$.

Therefore we have

$$z = z_1 \tau > 2p^{(z_1-1)/2}. \tag{18}$$

Furthermore, we have

$$\left| \frac{x}{p^{z/2}} - 1 \right| = \frac{D}{p^{z/2}(x + p^{z/2})} < \frac{D}{p^z}. \tag{19}$$

By Corollary 7.2 we have

$$p^{-\alpha_p - \beta_p z} < \left| \frac{x}{p^{z/2}} - 1 \right|,$$

where $\alpha_3 = 51.2, \beta_3 = 0.961, \alpha_{23} = 17.2, \beta_{23} = 0.968$. Together with (19) we have

$$p^{(1-\beta_p)z} < p^{\alpha_p} D.$$

Since $D + x_1^2 = p^{z_1}$, $D < p_1^z$ and we have

$$(1 - \beta_p)z < \alpha_p + z_1. \tag{20}$$

By (18)

$$(1 - \beta_p) 2p^{(z_1-1)/2} < \alpha_p + z_1.$$

This yields $z_1 \leq c_p$, where $c_3 = 13$ and $c_{23} = 3$.

By (16) and Lemma 7.3 we have

$$1 = E(\tau) = \sum_{i=0}^{(\tau-1)/2} \frac{(\tau - i - 1)! \tau}{(\tau - 2i)! i!} (-4D)^{(\tau-1)/2-i} p^{z_1 i}. \tag{21}$$

By (18) and (20) we have to check this equation for $3 \leq z_1 \leq c_p$, $D < p^{z_1}$ and τ an odd prime satisfying

$$\frac{2p^{(z_1-1)/2}}{z_1} < \tau < \frac{1}{1 - \beta_p} \left(1 + \frac{\alpha_p}{z_1} \right).$$

The only solution of (21) is $p = 3, z_1 = 3, D = 20, \tau = 3$, which yields no solution, since there is no x_1 such that $x_1^2 + 20 = 27$. This verification took 62 hours on a Alpha Workstation at 275 MHz. This is a contradiction to the assumption that there exist two solutions of (1).

By Theorem 6.1, $z_1 \mid h(-4D)$, by Proposition 2.2, $h(-4D) \leq 4\sqrt{D} \log(2e\sqrt{D})/\pi$. This completes the proof of the theorem. □

Remark that (2) enables us to find the only solution — if it exists — of (1) for a fixed D easily, even the constant is very reasonable. The following tables list all solutions (x, D, z) of (1) with $z \geq 2$, $1 \leq D \leq 100$ for $p = 3, 23$.

D	Equation
5	$2^2 + 5 = 3^2$
8	$1^2 + 8 = 3^2$
11	$4^2 + 11 = 3^3$
17	$8^2 + 17 = 3^4$
23	$2^2 + 23 = 3^3$
26	$1^2 + 26 = 3^3$
32	$7^2 + 32 = 3^4$
47	$14^2 + 47 = 3^5$
53	$26^2 + 53 = 3^6$
56	$5^2 + 56 = 3^4$
65	$4^2 + 65 = 3^4$
71	$46^2 + 71 = 3^7$
74	$13^2 + 74 = 3^5$
77	$2^2 + 77 = 3^4$
80	$1^2 + 80 = 3^4$
83	$140^2 + 83 = 3^9$

D	Equation
45	$22^2 + 45 = 23^2$
67	$110^2 + 67 = 23^3$
88	$21^2 + 88 = 23^2$

References

[1] R. Apéry, *Sur une équation diophantienne*, C. R. Acad. Sci Paris, Sér. A **251** (1960), 1451–1452.

[2] B. D. Beach and H. C. Williams and C. R. Zarnke, *Some computer results on units in quadratic and cubic fields.*, Proceedings of the 25th summer meeting of the Canadian Mathematical Congress, June 16-18, 1971. (W. R. Eames and R. G. Stanton and R. S. D. Thomas, ed.), Lakehead University, 1971, pp. 609–648.

[3] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, London-New York-San Francisco, 1978.

[4] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin-Heidelberg-New York, 1982.

[5] M.-H. Le, *On the generalized Ramanujan-Nagell equation II*, Chinese Sci. Bull. **30** (1985), 1698.

[6] ———, *On the number of solutions of the diophantine equation* $x^2 + D = p^n$, C. R. Acad. Sci. Paris, Série I **317** (1993), 135–138.

[7] ———, *Some Exponential Diophantine Equations. I. The Equation* $D_1x^2 - D_2y^2 = \lambda k^z$, J. Number Theory **55** (1995), 209–221.

[8] ———, *A note on the number of solutions of the generalized Ramanujan-Nagell equation* $x^2 - D = k^n$, Acta Arith. **78** (1996), 11–18.

[9] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, 1983.

[10] L. J. Mordell, *On a Pellian equation conjecture. II*, J. London Math. Soc. **36** (1961), 282–288.

[11] N. Tzanakis and J. Wolfskill, *On the Diophantine Equation* $y^2 = 4q^n + 4q + 1$, J. Number Theory **23** (1986), 219–237.