

CHEBYSHEV POLYNOMIALS AND PELL EQUATIONS
OVER FINITE FIELDS

BOAZ COHEN, Tel-Aviv Yaffo

Received October 10, 2019. Published online December 9, 2020.

Abstract. We shall describe how to construct a fundamental solution for the Pell equation $x^2 - my^2 = 1$ over finite fields of characteristic $p \neq 2$. Especially, a complete description of the structure of these fundamental solutions will be given using Chebyshev polynomials. Furthermore, we shall describe the structure of the solutions of the general Pell equation $x^2 - my^2 = n$.

Keywords: finite field; Chebyshev polynomial; Pell equation

MSC 2020: 12E20, 11D09, 12E10, 11D79, 11T99

1. INTRODUCTION

The classical Pell equation is the Diophantine equation $x^2 - my^2 = 1$, where m is an arbitrary integer. Given that m is a square-free positive integer, it is known that Pell equation has infinitely many solutions, which arise from a special “fundamental solution”. If the solutions of the classical Pell equation are ordered by magnitude, then the n th solution (x_n, y_n) with $x_n > 0$ and $y_n > 0$ can be expressed in terms of the first one (x_1, y_1) by $x_n + y_n\sqrt{m} = (x_1 + y_1\sqrt{m})^n$. Accordingly, the first solution (x_1, y_1) , or equivalently, the number $x_1 + y_1\sqrt{m}$, is called the *fundamental solution*. Therefore, solving the Pell equation reduces to finding a fundamental solution. This problem is extensively discussed in the literature. See, for instance, [3], pages 137–158.

In this paper we shall show that there exists a similar “fundamental solution” for Pell equations in the framework of *finite* fields of characteristic $p \neq 2$. Our main results are Theorems 4.5, 5.3 and 5.5. In Theorem 4.5 we describe how to construct a fundamental solution for the Pell equation $x^2 - my^2 = 1$ for non-square m . Under the same settings, in Theorem 5.3 we describe all the solutions of the general Pell

equation $x^2 - my^2 = n$. Finally, in Theorem 5.5 we solve a similar problem for square m .

The following notation will be used throughout this paper. If $a \neq 0$ is an integer and p a prime, $p^r \parallel a$ will mean p^r is the highest power of p dividing a . A finite field will be denoted by \mathbb{F} . Given such a field, it has a prime power $q = p^d$ elements. If the number $q = p^d$ of elements in \mathbb{F} is to be emphasized, \mathbb{F} will be denoted by \mathbb{F}_q . The prime number p is called the *characteristic* of \mathbb{F} and is denoted by $\text{char}(\mathbb{F})$. Throughout this paper we assume that $p > 2$, because for $p = 2$ the discussion of the Pell equation is a triviality. When $d = 1$, \mathbb{F}_p may be identified with the field $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p - 1\}$ of the residue classes of $\mathbb{Z} \bmod p$. If an element m of \mathbb{F} is a non-square in \mathbb{F} , the polynomial $f(x) = x^2 - m$ is irreducible over \mathbb{F} . We will denote the quadratic field extension $\mathbb{F}[x]/(f(x))$ of \mathbb{F} by $\mathbb{F}(\sqrt{m})$. Its elements may be regarded as $a + b\sqrt{m}$ with a, b in \mathbb{F} . The set \mathbb{F}_q^* of nonzero elements of a finite field \mathbb{F}_q is a cyclic group under multiplication of order $q - 1$. An element of \mathbb{F}_q^* is a generator of this group if and only if its order is coprime to $q - 1$. The *conjugate* of an element $\sigma = a + b\sqrt{m}$ of $\mathbb{F}(\sqrt{m})$ is the element $\bar{\sigma} := a - b\sqrt{m}$ of $\mathbb{F}(\sqrt{m})$. The *norm* $N(\sigma)$ of σ is defined by $N(\sigma) := \sigma\bar{\sigma} = a^2 - mb^2$. The norm is *multiplicative*, i.e., $N(\sigma\tau) = N(\sigma)N(\tau)$. Clearly, the set of solutions to our Pell equation $x^2 - my^2 = 1$ is the kernel, $\ker(N) = \{\sigma \in \mathbb{F}(\sqrt{m}) : N(\sigma) = 1\}$ of the norm $N: \mathbb{F}(\sqrt{m})^* \rightarrow \mathbb{F}^*$, which is a cyclic subgroup of $\mathbb{F}(\sqrt{m})^*$. Our aim in this paper is to describe a generator of $\ker(N)$.

2. PRELIMINARIES – CHEBYSHEV POLYNOMIALS OVER GENERAL FIELDS

The Chebyshev polynomials are well known sequences of polynomials. These polynomials have many interesting properties and appear in various branches of mathematics, especially in real and complex analysis. In this section we shall explore several of these properties, but in the framework of general fields.

Let \mathbb{F} be a field. The *Chebyshev polynomials of the first kind* (above \mathbb{F}) are defined by the following recurrence relation:

$$\begin{cases} T_0(x) = 1, \\ T_1(x) = x, \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \quad \text{if } n \geq 2, \end{cases}$$

and the *Chebyshev polynomials of the second kind* (above \mathbb{F}) are defined by

$$\begin{cases} S_0(x) = 1, \\ S_1(x) = 2x, \\ S_n(x) = 2xS_{n-1}(x) - S_{n-2}(x) \quad \text{if } n \geq 2. \end{cases}$$

We remark that in this context, we identify every integer $k \in \mathbb{Z}$ with the element $k1_{\mathbb{F}}$ of \mathbb{F} . The first ten Chebyshev polynomials of the first kind are

$$\begin{aligned} T_0(x) &= 1, \\ T_1(x) &= x, \\ T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1, \\ T_5(x) &= 16x^5 - 20x^3 + 5x, \\ T_6(x) &= 32x^6 - 48x^4 + 18x^2 - 1, \\ T_7(x) &= 64x^7 - 112x^5 + 56x^3 - 7x, \\ T_8(x) &= 128x^8 - 256x^6 + 160x^4 - 32x^2 + 1, \\ T_9(x) &= 256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x, \end{aligned}$$

and the first ten Chebyshev polynomials of the second kind are

$$\begin{aligned} S_0(x) &= 1, \\ S_1(x) &= 2x, \\ S_2(x) &= 4x^2 - 1, \\ S_3(x) &= 8x^3 - 4x, \\ S_4(x) &= 16x^4 - 12x^2 + 1, \\ S_5(x) &= 32x^5 - 32x^3 + 6x, \\ S_6(x) &= 64x^6 - 80x^4 + 24x^2 - 1, \\ S_7(x) &= 128x^7 - 192x^5 + 80x^3 - 8x, \\ S_8(x) &= 256x^8 - 448x^6 + 240x^4 - 40x^2 + 1, \\ S_9(x) &= 512x^9 - 1024x^7 + 672x^5 - 160x^3 + 10x. \end{aligned}$$

Observe that the recurrence relations defining the Chebyshev polynomials indeed produce polynomials in the ring $\mathbb{F}[x]$. Note that by the identification of every $k \in \mathbb{Z}$ with $k1_{\mathbb{F}} \in \mathbb{F}$, it follows that if $f(x) = g(x)$ over $\mathbb{Z}[x]$, then also $f(x) = g(x)$ over $\mathbb{F}[x]$. This observation can be applied in order to derive identities involving Chebyshev polynomials since, as one can verify directly from the recurrence relation, all the coefficients of Chebyshev polynomials are integers.

Another important point is related to the solutions of the recurrence relations defining the Chebyshev polynomials. The characteristic polynomial of the relation defining the Chebyshev polynomials of the first kind is $p(t) = t^2 - 2xt + 1$.

The roots of $p(t)$ are $\alpha(x) = x + \sqrt{x^2 - 1}$ and $\beta(x) = x - \sqrt{x^2 - 1}$. Note that these roots are elements of the field $\mathbb{F}(x, \Delta)$, where $\Delta(x) := \sqrt{x^2 - 1}$ is an element such that $\Delta^2(x) = x^2 - 1$. Therefore, the solution of this recurrence is of the form

$$T_n(x) = A(x)\alpha(x)^n + B(x)\beta(x)^n,$$

where $A(x), B(x) \in \mathbb{F}(x, \Delta)$. Since $T_0(x) = 1$ and $T_1(x) = x$, it follows that $A(x) + B(x) = 1$ and $A(x)\alpha(x) + B(x)\beta(x) = x$. Solving this system over $\mathbb{F}(x, \Delta)$ gives $A(x) = B(x) = \frac{1}{2}$. Therefore

$$T_n(x) = \frac{1}{2}(\alpha^n(x) + \beta^n(x)).$$

We remark that although the solution is expressed using the non-polynomial element Δ , the T_n 's are still polynomials over the ring $\mathbb{F}[x]$.

Similarly, as one can verify, the solution of the recurrence relation which defines the Chebyshev polynomials of the second kind is

$$S_n(x) = \frac{1}{2\Delta(x)}(\alpha^n(x) - \beta^n(x)).$$

Using these ideas we turn to prove a list of identities gathered in Proposition 2.1 below. We remark that in this section, for the purpose of clarity, we shall use T_n and S_n instead of $T_n(x)$ and $S_n(x)$, respectively.

Proposition 2.1. *Let \mathbb{F} be a field with $\text{char}(\mathbb{F}) \neq 2$ and let n be a positive integer. Then:*

- (1) $\deg T_n = n$,
- (2) $S_{n+1} - S_{n-1} = 2T_{n+1}$,
- (3) $S_{m+n} = S_m S_n - S_{m-1} S_{n-1}$ for all integers $m, n \geq 1$,
- (4) $2T_n T_m = T_{n+m} + T_{|n-m|}$ for all integers $m, n \geq 0$,
- (5) $S_n^2 = S_{n+1} S_{n-1} + 1$,
- (6) $S_{2n} = S_n^2 - S_{n-1}^2$ and $S_{2n+1} = 2S_n T_{n+1}$,
- (7) $S_n + S_{n-1} = 2(T_1 + T_2 + \dots + T_n) + 1$,
- (8) $T_{2n} - 1 = 2S_{n-1}^2(x^2 - 1)$,
- (9) $T_{2n+1} - 1 = (S_{n-1} + S_n)^2(x - 1)$.

Proof. We shall prove identities (5)–(9). By the above discussion, it follows that in order to prove the rest of the identities, it suffices to prove them over $\mathbb{Z}[x]$. The proof of (1)–(4) can be found in [1].

(5) The proof is by induction on n . For $n = 1$ indeed

$$S_2 S_0 + 1 = (4x^2 - 1)1 + 1 = (2x)^2 = S_1^2.$$

Let $n \geq 2$. By the definition of S_n and the inductive hypothesis we obtain

$$\begin{aligned} S_{n+1}S_{n-1} + 1 &= (2xS_n - S_{n-1})S_{n-1} + 1 = 2xS_nS_{n-1} - S_{n-1}^2 + 1 \\ &= 2xS_nS_{n-1} - (S_nS_{n-2} + 1) + 1 = S_n(2xS_{n-1} - S_{n-2}) = S_n^2. \end{aligned}$$

(6) By part (3) with $m = n$ we obtain

$$S_{2n} = S_n^2 - S_{n-1}^2.$$

In addition, by part (3) with $m = n + 1$ and part (2) we obtain

$$S_{2n+1} = S_{n+1}S_n - S_nS_{n-1} = S_n(S_{n+1} - S_{n-1}) = 2S_nT_{n+1}.$$

(7) The proof is by induction on n . For $n = 1$, indeed

$$S_1 + S_0 = 2x + 1 = 2T_1 + 1.$$

Let $n \geq 2$. By part (2) and the inductive hypothesis we obtain

$$\begin{aligned} S_n + S_{n-1} &= (S_n - S_{n-2}) + (S_{n-1} + S_{n-2}) = 2T_n + 2(T_1 + T_2 + \dots + T_{n-1}) + 1 \\ &= 2(T_1 + T_2 + \dots + T_n) + 1. \end{aligned}$$

(8) We shall use the explicit solutions of the recurrence relation of T_n and S_n developed previously. Note that

$$2S_{n-1}^2(x^2 - 1) = 2\left(\frac{1}{2\Delta}(\alpha^n - \beta^n)\right)^2(x^2 - 1) = \frac{2(x^2 - 1)}{4\Delta^2}(\alpha^{2n} - 2(\alpha\beta)^n + \beta^{2n}).$$

Since $\alpha\beta = 1$ and $\Delta^2 = x^2 - 1$, we obtain that

$$2S_{n-1}^2(x^2 - 1) = \frac{1}{2}(\alpha^{2n} - 2 + \beta^{2n}) = T_{2n}(x) - 1,$$

as required.

(9) The proof is by induction on n . For $n = 1$ indeed

$$T_3 - 1 = 4x^3 - 3x - 1 = (1 + 2x)^2(x - 1) = (S_0 + S_1)^2(x - 1).$$

Let $n \geq 2$. By the definition of T_n and S_n , parts (8) and (5), and by the inductive hypothesis we obtain

$$\begin{aligned}
 T_{2n+1} - 1 &= 2xT_{2n} - T_{2n-1} - 1 \\
 &= 2x(1 + 2(x^2 - 1)S_{n-1}^2) - (1 + (x - 1)(S_{n-2} + S_{n-1})^2) - 1 \\
 &= 2(x - 1) + 4x(x - 1)(x + 1)S_{n-1}^2 - (x - 1)(S_{n-2} + S_{n-1})^2 \\
 &= (x - 1)(2 + (2xS_{n-1})^2 + 2S_{n-1}(2xS_{n-1}) - (S_{n-2} + S_{n-1})^2) \\
 &= (x - 1)(2 + (S_n + S_{n-2})^2 + 2S_{n-1}(S_n + S_{n-2}) - (S_{n-2} + S_{n-1})^2) \\
 &= (x - 1)(2(1 + S_n S_{n-2}) + S_n^2 + 2S_{n-1}S_n - S_{n-1}^2) \\
 &= (x - 1)(2S_{n-1}^2 + S_n^2 + 2S_{n-1}S_n - S_{n-1}^2) \\
 &= (x - 1)(S_{n-1} + S_n)^2.
 \end{aligned}$$

□

Another two sequences of polynomials which will be important in the sequel are the conjugate Chebyshev polynomials. The *conjugate Chebyshev polynomials of the first kind* (above \mathbb{F}) are defined by the following recurrence relation:

$$\begin{cases}
 T_0^*(x) = 1, \\
 T_1^*(x) = x, \\
 T_n^*(x) = 2xT_{n-1}^*(x) + T_{n-2}^*(x) & \text{if } n \geq 2,
 \end{cases}$$

and the *conjugate Chebyshev polynomials of the second kind* (above \mathbb{F}) are defined by

$$\begin{cases}
 S_0^*(x) = 1, \\
 S_1^*(x) = 2x, \\
 S_n^*(x) = 2xS_{n-1}^*(x) + S_{n-2}^*(x) & \text{if } n \geq 2.
 \end{cases}$$

The first few conjugate Chebyshev polynomials are

$$\begin{array}{ll}
 T_0^*(x) = 1, & S_0^*(x) = 1, \\
 T_1^*(x) = x, & S_1^*(x) = 2x, \\
 T_2^*(x) = 2x^2 + 1, & S_2^*(x) = 4x^2 + 1, \\
 T_3^*(x) = 4x^3 + 3x, & S_3^*(x) = 8x^2 + 4x, \\
 T_4^*(x) = 8x^4 + 8x^2 + 1, & S_4^*(x) = 16x^4 + 12x^2 + 1, \\
 T_5^*(x) = 16x^5 + 20x^3 + 5x, & S_5^*(x) = 32x^5 + 32x^3 + 6x.
 \end{array}$$

The polynomials T_n^* and S_n^* can be expressed in terms of the polynomials T_n and S_n . In order to do so, we need to consider these polynomials over the field extension $\mathbb{F}(i)$, where i is an element such that $i^2 + 1 = 0$.

Proposition 2.2. *Let n be a positive integer. Then*

- (1) $T_n(ix) = i^n T_n^*(x)$ and $S_n(ix) = i^n S_n^*(x)$,
- (2) $T_{2n}^* = 2(T_n^*)^2 - (-1)^n$.

Proof. (1) The proof is by induction on n . For $n = 1$ and $n = 2$ indeed

$$\begin{aligned} T_1(ix) &= ix = i^1 T_1^*(x), \\ S_1(ix) &= 2ix = i(2x) = i^1 S_1^*(x), \\ T_2(ix) &= 2(ix)^2 - 1 = -(2x^2 + 1) = i^2 T_2^*(x), \\ S_2(ix) &= 4(ix)^2 - 1 = -(4x^2 + 1) = i^2 S_2^*(x). \end{aligned}$$

Let $n \geq 3$. By the definitions of both T_n^* and S_n^* and by the inductive hypothesis we obtain

$$\begin{aligned} T_n(ix) &= 2ixT_{n-1}(ix) - T_{n-2}(ix) = 2ixi^{n-1}T_{n-1}^*(x) - i^{n-2}T_{n-2}^*(x) \\ &= 2i^n x T_{n-1}^*(x) - i^n i^{-2} T_{n-2}^*(x) = i^n (2x T_{n-1}^*(x) + T_{n-2}^*(x)) = i^n T_n^*(x). \end{aligned}$$

Since S_n and S_n^* are defined by the same recursive relation as T_n and T_n^* , the above calculations will be also suitable for proving the identity for $S_n(ix)$.

(2) By part (1) and Proposition 2.1 (4) we obtain

$$\begin{aligned} T_{2n}^*(x) &= i^{-2n} T_{2n}(ix) = i^{-2n} T_{n+n}(ix) = (-1)^n (2T_n^2(ix) - 1) \\ &= (-1)^n (2(i^n T_n^*(x))^2 - 1) = (-1)^n (2(-1)^n (T_n^*)^2(x) - 1) \\ &= 2(T_n^*)^2(x) - (-1)^n. \end{aligned}$$

□

3. BASIC PROPERTIES OF THE EXTENSION FIELD $\mathbb{F}(\sqrt{m})$

The analysis of the solutions of Pell equations will be performed using the framework of the quadratic extension fields as recalled briefly in the introductory section.

Proposition 3.1. *Let \mathbb{F} be a finite field with q elements, $a \in \mathbb{F}$ and let n be a positive integer. Then the equation $x^n = a$ is solvable if and only if $a^{(q-1)/d} = 1$, where $d = \gcd(n, q - 1)$. Moreover, if there are solutions, then there are exactly d solutions.*

For a proof see [2], page 80. The following property of $\mathbb{F}(\sqrt{m})$ is of a particular importance for us:

Proposition 3.2. *Suppose that \mathbb{F} is a finite field with q elements and $m \in \mathbb{F}$ is a non-square element. Then $\sigma^q = \bar{\sigma}$ for every $\sigma \in \mathbb{F}(\sqrt{m})$.*

Proof. Set $a = m^{(q-1)/2}$. First we shall prove that $a = -1$. Note that since $\text{char}(\mathbb{F}) \neq 2$, it follows that q is odd, so $q - 1$ is even. Hence, a is well defined.

Since $|\mathbb{F}^*| = q - 1$ and $m \in \mathbb{F}^*$, it follows that $a^2 = m^{q-1} = 1$. Therefore, either $a = 1$ or $a = -1$. By the assumption, m is a non-square element, so the equation $x^2 = m$ is not solvable. Hence, by Proposition 3.1 it follows that $a \neq 1$. Therefore $a = -1$, as required.

In view of the fact that $(\alpha + \beta)^{p^s} = \alpha^{p^s} + \beta^{p^s}$ for every α, β in a field of characteristic p and for every positive integer s (see [2], page 81), it follows that for every $x, y \in \mathbb{F}$

$$(x + y\sqrt{m})^q = x^q + y^q(\sqrt{m})^q = x + \sqrt{m}(\sqrt{m})^{q-1}y.$$

Note that since $m^{(q-1)/2} = -1$, we obtain that

$$(\sqrt{m})^{q-1} = (\sqrt{m^2})^{(q-1)/2} = m^{(q-1)/2} = -1.$$

Therefore, $(x + y\sqrt{m})^q = x - y\sqrt{m} = \overline{x + y\sqrt{m}}$, as required. \square

As we shall see, there is a connection between the solutions of Pell equations and the set of n th roots of unity in $\mathbb{F}(\sqrt{m})$. In order to reveal this connection, we need the following result, which follows from Proposition 3.1:

Proposition 3.3. *Let \mathbb{F} be a finite field and let n be a positive integer. Then the set of n th-roots of unity in \mathbb{F} forms a cyclic subgroup of \mathbb{F}^* of order $\text{gcd}(n, |\mathbb{F}^*|)$.*

4. THE SOLUTION OF THE PELL EQUATION $x^2 - my^2 = 1$

In this section we shall describe the solutions of Pell equations $x^2 - my^2 = 1$ over finite fields \mathbb{F} . This will be done for *non-square* m 's. Note that in this case, there is a bijection between the elements of $\mathbb{F} \times \mathbb{F}$ and $\mathbb{F}(\sqrt{m})$. Therefore, it is convenient to refer to $x + y\sqrt{m}$ as (x, y) , as a solution of a Pell equation.

We begin with the following result, which follows from Propositions 3.2 and 3.3:

Proposition 4.1. *Suppose that \mathbb{F} is a finite field with q elements. If $m \in \mathbb{F}$ is a non-square element, then the set*

$$G = \ker(N) = \{\sigma \in \mathbb{F}(\sqrt{m}) : N(\sigma) = 1\}$$

is a cyclic subgroup of $\mathbb{F}(\sqrt{m})^$ of order $q + 1$.*

Proposition 4.2. Suppose $m \in \mathbb{F}$ is a non-square element, $a, b \in \mathbb{F}$ and n is a positive integer. Then

$$(a + b\sqrt{m})^n = T_n(a) + bS_{n-1}(a)\sqrt{m}$$

if $a^2 - mb^2 = 1$, and

$$(a + b\sqrt{m})^n = T_n^*(a) + bS_{n-1}^*(a)\sqrt{m}$$

if $a^2 - mb^2 = -1$.

Proof. Note that over the field $\mathbb{F}(x, \Delta)$ we have the following identity:

$$T_n + S_{n-1}\Delta = \frac{1}{2}(a^n + \beta^n) + \frac{1}{2\Delta}(a^n - \beta^n) \cdot \Delta = a^n,$$

that is

$$T_n(x) + S_{n-1}(x)\sqrt{x^2 - 1} = (x + \sqrt{x^2 - 1})^n.$$

Now, if $a^2 - mb^2 = 1$, then $mb^2 = a^2 - 1$, so without loss of generality we may deduce that $b\sqrt{m} = \sqrt{a^2 - 1}$. Therefore,

$$(a + b\sqrt{m})^n = (a + \sqrt{a^2 - 1})^n = T_n(a) + S_{n-1}(a)\sqrt{a^2 - 1} = T_n(a) + bS_{n-1}(a)\sqrt{m},$$

as required.

Suppose now that $a^2 - mb^2 = -1$. Note that over the field $\mathbb{F}(i)$ this can be written as $(ia)^2 - m(ib)^2 = 1$. Using the first part of the proof and Proposition 2.2(1) we obtain

$$\begin{aligned} (ia + ib\sqrt{m})^n &= T_n(ia) + ibS_{n-1}(ia)\sqrt{m} = i^n T_n^*(a) + ibi^{n-1} S_{n-1}^*(a)\sqrt{m} \\ &= i^n (T_n^*(a) + bS_{n-1}^*(a)\sqrt{m}). \end{aligned}$$

Hence $(a + b\sqrt{m})^n = T_n^*(a) + bS_{n-1}^*(a)\sqrt{m}$, as required. \square

The following two theorems are the building blocks of our main result. We begin with the case of primes $p > 2$.

Theorem 4.3. Suppose that \mathbb{F} is a finite field with q elements. Suppose also that p is an odd prime such that $p \mid q + 1$, c is the positive integer such that $p^c \parallel q + 1$ and r is a positive integer satisfying $1 \leq r \leq c$. In addition, given a non-square element $m \in \mathbb{F}$, consider the group

$$G = \{\sigma \in \mathbb{F}(\sqrt{m}) : N(\sigma) = 1\}.$$

Let $\sigma = a + b\sqrt{m} \in G$ and $k_r = \frac{1}{2}(p^r - 1)$. Then:

- (a) If $\sigma \neq 1$, then $\text{ord}(\sigma) \mid p^r$ if and only if $S_{k_r}(a) + S_{k_r-1}(a) = 0$.
(b) $\text{ord}(\sigma) = p^r$ if and only if $L_{p^r}(a) = 0$, where L_{p^r} denotes the polynomial

$$L_{p^r}(x) := 2 \sum_{j=1}^{(p-1)/2} T_{jp^{r-1}}(x) + 1.$$

Proof. In this proof, for the purpose of clarity, we shall use T_k and S_k instead of $T_k(a)$ and $S_k(a)$.

- (a) Set $n = k_r$. By Propositions 4.2 and 2.1 (6), (9) we obtain

$$\begin{aligned} (a + b\sqrt{m})^{p^r} &= (a + b\sqrt{m})^{2n+1} = T_{2n+1} + bS_{2n}\sqrt{m} \\ &= 1 + (S_n + S_{n-1})^2(a-1) + b(S_n^2 - S_{n-1}^2)\sqrt{m} \\ &= 1 + (S_n + S_{n-1})((a-1)(S_n + S_{n-1}) + b(S_n - S_{n-1})\sqrt{m}). \end{aligned}$$

Hence, if $S_n(a) + S_{n-1}(a) = 0$, then $\sigma^{p^r} = 1$, so $\text{ord}(\sigma) \mid p^r$, as required.

Conversely, if $\text{ord}(\sigma) \mid p^r$, then $\sigma^{p^r} = 1$. Hence either $S_n + S_{n-1} = 0$ or

$$(*) \quad (a-1)(S_n + S_{n-1}) + b(S_n - S_{n-1})\sqrt{m} = 0.$$

We claim that $S_n + S_{n-1} = 0$. Suppose otherwise that $S_n + S_{n-1} \neq 0$. Since $\sigma \neq 1$ and $N(\sigma) = a^2 - mb^2 = 1$, it follows that $a \neq 1$, so $(a-1)(S_n + S_{n-1}) \neq 0$, which contradicts (*). Therefore $S_n + S_{n-1} = 0$, as claimed.

- (b) Consider the sets

$$\begin{aligned} A &= \{a + b\sqrt{m} \in G : a, b \in \mathbb{F}, \text{ord}(a + b\sqrt{m}) = p^r\}, \\ B &= \{a + b\sqrt{m} \in G : a, b \in \mathbb{F}, L_{p^r}(a) = 0\}. \end{aligned}$$

It suffices to prove that $A = B$. First we shall prove using induction on r that

$$L_p L_{p^2} \dots L_{p^r} = S_{k_r} + S_{k_r-1}.$$

If $r = 1$, then it follows by Proposition 2.1 (7) that

$$L_p = 2 \sum_{j=1}^{(p-1)/2} T_j + 1 = 2 \sum_{j=1}^{k_1} T_j + 1 = S_{k_1} + S_{k_1-1}.$$

Suppose that $r \geq 2$. By the inductive hypothesis, Proposition 2.1 (4) (7) and the definition of L_{p^r} we obtain

$$\begin{aligned}
L_p \dots L_{p^{r-1}} L_{p^r} &= (S_{k_{r-1}} + S_{k_{r-1}-1}) L_{p^r} \\
&= \left(2 \sum_{i=1}^{k_{r-1}} T_i + 1 \right) \left(2 \sum_{j=1}^{(p-1)/2} T_{jp^{r-1}} + 1 \right) \\
&= 2 \sum_{i=1}^{k_{r-1}} \sum_{j=1}^{(p-1)/2} 2T_i T_{jp^{r-1}} + 2 \sum_{i=1}^{k_{r-1}} T_i + 2 \sum_{j=1}^{(p-1)/2} T_{jp^{r-1}} + 1 \\
&= 2 \sum_{i=1}^{k_{r-1}} T_i + 2 \sum_{j=1}^{(p-1)/2} \sum_{i=1}^{k_{r-1}} (T_{jp^{r-1}+i} + T_{jp^{r-1}-i}) + 2 \sum_{j=1}^{(p-1)/2} T_{jp^{r-1}} + 1 \\
&= 2 \left(\sum_{l=1}^{k_{r-1}} T_l + \sum_{j=1}^{(p-1)/2} \sum_{l=jp^{r-1}-k_{r-1}}^{jp^{r-1}+k_{r-1}} T_l \right) + 1.
\end{aligned}$$

Note that for every $0 \leq j \leq \frac{1}{2}(p-1) - 1$ we have

$$((j+1)p^{r-1} - k_{r-1}) - (jp^{r-1} + k_{r-1}) = p^{r-1} - 2k_{r-1} = 1.$$

Therefore

$$L_p L_{p^2} \dots L_{p^r} = 2 \sum_{l=1}^{(p-1)p^{r-1}/2 + k_{r-1}} T_l + 1 = 2 \sum_{l=1}^{(p^r-1)/2} T_l + 1 = S_{k_r} + S_{k_{r-1}},$$

as claimed.

Returning to our central claim, first we shall prove that $A \subseteq B$. So suppose that $\sigma = a + b\sqrt{m}$ has order p^r . Hence $S_{k_r}(a) + S_{k_{r-1}}(a) = 0$ by part (a). Since $L_p L_{p^2} \dots L_{p^r} = S_{k_r} + S_{k_{r-1}}$, it follows that $L_p(a) L_{p^2}(a) \dots L_{p^r}(a) = 0$. If $r = 1$, then $L_p(a) = 0$ and we are done. Suppose that $r \geq 2$ but $L_{p^r}(a) \neq 0$. Then $L_p(a) \dots L_{p^{r-1}}(a) = 0$, and since $L_p \dots L_{p^{r-1}} = S_{k_{r-1}} + S_{k_{r-1}-1}$, it follows that $S_{k_{r-1}}(a) + S_{k_{r-1}-1}(a) = 0$. By part (a) we deduce that $\text{ord}(\sigma) \mid p^{r-1}$, which contradicts the fact that the order of σ is p^r .

In view of the fact that $A \subseteq B$, in order to prove that $A = B$, it suffices to prove that $|A| \geq |B|$. Since $\text{char}(\mathbb{F}) \neq 2$, Proposition 2.1 (1) implies that

$$\deg L_{p^r} = \deg \left(2 \sum_{j=1}^{(p-1)/2} T_{jp^{r-1}} + 1 \right) = \deg(T_{(p-1)p^{r-1}/2}) = \frac{(p-1)p^{r-1}}{2} = \frac{\varphi(p^r)}{2},$$

where φ denotes Euler's totient function. It follows that L_{p^r} has at most $\frac{1}{2}\varphi(p^r)$ roots in \mathbb{F} . Now, given an element $a \in \mathbb{F}$ such that $L_{p^r}(a) = 0$, there are at most

two elements $b \in \mathbb{F}$ such that $a^2 - mb^2 = 1$ (namely b and $(-b)$). Hence $|B| \leq \frac{1}{2}\varphi(p^r) \cdot 2 = \varphi(p^r)$.

Regarding $|A|$, since $\text{ord}(a + b\sqrt{m}) = p^r$, it follows that $p^r \mid |G|$. But by Proposition 4.1 the group G is cyclic, so the number of elements in G of order p^r is exactly $\varphi(p^r)$. Thus $|A| = \varphi(p^r)$, so $|B| \leq |A|$, as required. \square

Next we prove the complementary theorem for the case $p = 2$.

Theorem 4.4. *Suppose that \mathbb{F} is a finite field with q elements. Suppose also that c is the positive integer such that $2^c \parallel q + 1$ and r is a positive integer satisfying $1 \leq r \leq c$. In addition, given a non-square element $m \in \mathbb{F}$, consider the group*

$$G = \{\sigma \in \mathbb{F}(\sqrt{m}) : N(\sigma) = 1\}.$$

Let $\sigma = a + b\sqrt{m} \in G$. Then:

- (a) If $\sigma \neq \pm 1$, then $\text{ord}(\sigma) \mid 2^r$ if and only if $S_{2^{r-1}-1}(a) = 0$.
- (b) If $r \geq 2$, then $\text{ord}(\sigma) = 2^r$ if and only if $T_{2^{r-2}}(a) = 0$.

Proof. In this proof, for the purpose of clarity, we shall use T_k and S_k instead of $T_k(a)$ and $S_k(a)$.

(a) Set $n = 2^{r-1}$. By Propositions 4.2 and 2.1 (6), (8) we obtain

$$\begin{aligned} (a + b\sqrt{m})^{2^r} &= (a + b\sqrt{m})^{2n} = T_{2n} + bS_{2n-1}\sqrt{m} \\ &= 1 + 2S_{n-1}^2(a^2 - 1) + 2bS_{n-1}T_n\sqrt{m} \\ &= 1 + 2S_{n-1}((a^2 - 1)S_{n-1} + bT_n\sqrt{m}). \end{aligned}$$

Hence, if $S_{n-1}(a) = 0$, then $\sigma^{2^r} = 1$, so $\text{ord}(\sigma) \mid 2^r$, as required.

Conversely, if $\text{ord}(\sigma) \mid 2^r$, then $\sigma^{2^r} = 1$. Hence either $S_{n-1} = 0$ or

$$(*) \quad (a^2 - 1)S_{n-1} + bT_n\sqrt{m} = 0.$$

We claim that $S_{n-1} = 0$. Suppose otherwise that $S_{n-1} \neq 0$. Since $a + b\sqrt{m} \neq \pm 1$ and $a^2 - mb^2 = 1$ it follows that $a \neq \pm 1$, so $(a^2 - 1)S_{n-1} \neq 0$, which contradicts (*). Therefore $S_{n-1}(a) = 0$, as required.

(b) Consider the sets

$$\begin{aligned} A &= \{a + b\sqrt{m} \in G : a, b \in \mathbb{F}, \text{ord}(a + b\sqrt{m}) = 2^r\}, \\ B &= \{a + b\sqrt{m} \in G : a, b \in \mathbb{F}, T_{2^{r-2}}(a) = 0\}. \end{aligned}$$

It suffices to prove that $A = B$. We begin by proving that

$$S_{2^r-1} = 2^r T_{2^0} T_{2^1} T_{2^2} \dots T_{2^{r-1}}$$

for every $r \geq 1$. The proof is by induction on r . If $r = 1$, then indeed $S_{2^1-1} = S_1 = 2x = 2T_1 = 2^1T_{2^0}$. Suppose now that $r \geq 2$. By Proposition 2.1 (6) and the inductive hypothesis it follows that

$$S_{2^r-1} = 2S_{2^{r-1}-1}T_{2^r-1} = 2(2^{r-1}T_{2^0}T_{2^1} \dots T_{2^{r-2}})T_{2^r-1} = 2^rT_{2^0}T_{2^1} \dots T_{2^{r-1}},$$

as claimed.

Returning to our central claim, we shall prove that $A \subseteq B$. So suppose that $a + b\sqrt{m}$ has order 2^r and $r \geq 2$. By part (a) it follows that $S_{2^{r-1}-1}(a) = 0$. Since

$$S_{2^{r-1}-1} = 2^{r-1}T_{2^0}T_{2^1} \dots T_{2^{r-2}}$$

and $\text{char}(\mathbb{F}) \neq 2$ it follows that

$$T_{2^0}(a)T_{2^1}(a) \dots T_{2^{r-2}}(a) = 0.$$

If $r = 2$, then $T_{2^0}(a) = 0$ and we are done. Assume that $r \geq 3$ but $T_{2^{r-2}}(a) \neq 0$. Then $T_{2^0}(a)T_{2^1}(a) \dots T_{2^{r-3}}(a) = 0$, and since $2^{r-2}T_{2^0}T_{2^1} \dots T_{2^{r-3}} = S_{2^{r-2}-1}$, it follows that $S_{2^{r-2}-1}(a) = 0$. But then, by part (a) we deduce that $\text{ord}(a + b\sqrt{m}) \mid 2^{r-1}$, which contradicts the fact that the order of $a + b\sqrt{m}$ is 2^r .

In view of the fact that $A \subseteq B$, in order to prove that $A = B$, it suffices to prove that $|A| \geq |B|$. Since $\text{char}(\mathbb{F}) \neq 2$, Proposition 2.1 (1) implies that $\deg(T_{2^{r-2}}) = 2^{r-2} = \frac{1}{2}\varphi(2^r)$. It follows that $T_{2^{r-2}}$ has at most $\frac{1}{2}\varphi(2^r)$ roots in \mathbb{F} . Given an element $a \in \mathbb{F}$ such that $T_{2^{r-2}}(a) = 0$, there are at most two elements $b \in \mathbb{F}$ such that $a^2 - mb^2 = 1$ (namely b and $(-b)$). Hence, $|B| \leq \frac{1}{2}\varphi(2^r) \cdot 2 = \varphi(2^r)$.

Regarding $|A|$, since $\text{ord}(a + b\sqrt{m}) = 2^r$, it follows that $2^r \mid |G|$. But by Proposition 4.1 the group G is cyclic, so the number of elements in G of order 2^r is exactly $\varphi(2^r)$. Thus $|A| = \varphi(2^r)$, so $|B| \leq |A|$, as required. \square

Now we can prove the main result of this section.

Theorem 4.5. *Suppose that \mathbb{F} is a finite field with q elements and let $m \in \mathbb{F}$. Consider the equation*

$$(*) \quad x^2 - my^2 = 1.$$

If m is a non-square element, then () has exactly $q + 1$ solutions (x, y) over \mathbb{F} . Moreover, these solutions are given by*

$$x + y\sqrt{m} = \omega_{q+1}^k, \quad k \in \{0, 1, \dots, q\},$$

where $\omega_{q+1} = \prod \omega_{p^r}$, in which the product extends over all prime powers $p^r \parallel q+1$, and the ω_{p^r} 's are chosen as follows:

- (a) If $p > 2$, then $\omega_{p^r} = a + b\sqrt{m}$ is any solution of (*) such that $L_{p^r}(a) = 0$, where L_{p^r} is the polynomial

$$L_{p^r}(x) := 2 \sum_{j=1}^{(p-1)/2} T_{jp^{r-1}}(x) + 1,$$

and T_k denotes the k th Chebyshev polynomial.

- (b) If $p = 2$ and $r = 1$, then $\omega_2 = -1$.
(c) If $p = 2$ and $r \geq 2$, then $\omega_{2^r} = a + b\sqrt{m}$ is any solution of (*) such that $T_{2^{r-2}}(a) = 0$.

P r o o f. Set $G = \{(x, y) : x, y \in \mathbb{F}, x^2 - my^2 = 1\}$. By Proposition 4.1, G is a cyclic group of order $q+1$. Let ω_{q+1} be a generator of G . By the fundamental theorem of cyclic groups, we have that

$$\omega_{q+1} = \prod_{p^r \parallel q+1} \omega_{p^r},$$

where the product extends over all prime powers $p^r \parallel q+1$, and $\omega_{p^r} \in G$ is of order p^r .

If $p > 2$, then by Theorem 4.3 (b), the element ω_{p^r} is of the form $\omega_{p^r} = a + b\sqrt{m}$, where $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 - mb^2 = 1$ and $L_{p^r}(a) = 0$, as required.

Suppose that $p = 2$. If $r = 1$, then we may choose $\omega_2 = -1$, since clearly $-1 \in G$ and $\text{ord}(-1) = 2$. If $r \geq 2$, then by Theorem 4.4 (b), ω_{2^r} is of the form $\omega_{2^r} = a + b\sqrt{m}$, where $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 - mb^2 = 1$ and $T_{2^{r-2}}(a) = 0$, as required. The proof is therefore complete. \square

We conclude this section with several examples illustrating Theorem 4.5.

Example 4.6. Let us solve the Pell equation $x^2 - 3y^2 = 1$ over the field \mathbb{F}_{149} . Here, using the notation of Theorem 4.5, $\mathbb{F} = \mathbb{F}_{149}$, $q = 149$ and $m = 3$. Hence $q+1 = 2 \cdot 3 \cdot 5^2$. Note that since

$$\left(\frac{3}{149}\right) = \left(\frac{149}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

it follows that $m = 3$ is a non-square element in \mathbb{F} . By Theorem 4.5, we deduce that $x^2 - 3y^2 = 1$ has $q+1 = 150$ solutions and a fundamental solution for this equation is $\omega_{150} = \omega_2\omega_3\omega_{25}$.

First we find ω_2 . In this case $r = 1$, so by Theorem 4.5 (b) we obtain that $\omega_2 = -1$. Next we find ω_3 . In this case $p = 3$ and $r = 1$. By Theorem 4.5 (a) we obtain that

$\omega_3 = a + b\sqrt{3}$, where $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 - 3b^2 = 1$ and $L_3(a) = 0$. Here

$$L_3(x) = 2T_1(x) + 1 = 2x + 1.$$

Since $a = 74$ and $b = 22$ satisfy both $a^2 - 3b^2 = 1$ and $L_3(a) = 0$, we may choose $\omega_3 = 74 + 22\sqrt{3}$.

Finally we find ω_{25} . By Theorem 4.5 (a) we obtain that $\omega_{25} = a + b\sqrt{3}$, where $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 - 3b^2 = 1$ and $L_{25}(a) = 0$. Here

$$\begin{aligned} L_{25}(x) &= 2(T_5(x) + T_{10}(x)) + 1 \\ &= 130x^{10} - 27x^8 + 5x^6 + 32x^5 - 55x^4 - 40x^3 - 49x^2 + 10x - 1. \end{aligned}$$

Since $a = 10$ and $b = 35$ satisfy both $a^2 - 3b^2 = 1$ and $L_{25}(a) = 0$, we may choose $\omega_{25} = 10 + 35\sqrt{3}$.

Once we found the ω_2 , ω_3 and ω_{25} , the fundamental solution of $x^2 - 3y^2 = 1$ is

$$\omega_2\omega_3\omega_{25} = (-1)(74 + 22\sqrt{3})(10 + 35\sqrt{3}) = 79 + 21\sqrt{3}.$$

Therefore, the solutions (x, y) of the Pell equation $x^2 - 3y^2 = 1$ over \mathbb{F}_{149} are given by $x + y\sqrt{3} = (79 + 21\sqrt{3})^k$, where $k \in \{0, 1, 2, \dots, 149\}$.

Example 4.7. Let us solve the Pell equation $x^2 + y^2 = 1$ over the field $\mathbb{F} = \mathbb{F}_{167}$. Here $q = 167$, $m = -1$. Hence $q + 1 = 2^3 \cdot 3 \cdot 7$. Note that

$$\left(\frac{-1}{167}\right) = -1$$

since $167 \equiv -1 \pmod{4}$, so $m = -1$ is a non-square element in \mathbb{F} . By Theorem 4.5, we deduce that $x^2 + y^2 = 1$ has $q + 1 = 168$ solutions and a fundamental solution for this equation is $\omega_{168} = \omega_8\omega_3\omega_7$.

First we find ω_8 . In this case $r = 3$, so by Theorem 4.5 (c) $\omega_8 = a + bi$, where $i := \sqrt{-1}$ and $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 + b^2 = 1$ and $T_2(a) = 0$. Here $T_2(x) = 2x^2 - 1$. Since $a = 77$ and $b = 77$ satisfy both $a^2 + b^2 = 1$ and $T_2(a) = 0$, we may choose $\omega_8 = 77 + 77i$.

Next we find ω_3 . By Theorem 4.5 (a) $\omega_3 = a + bi$, where $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 + b^2 = 1$ and $L_3(a) = 0$. Here $L_3(x) = 2T_1(x) + 1 = 2x + 1$. Since $a = 83$ and $b = 31$ satisfy both $a^2 + b^2 = 1$ and $L_3(a) = 0$, we may choose $\omega_3 = 83 + 31i$.

Finally we find ω_7 . By Theorem 4.5 (a) $\omega_7 = a + bi$, where $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 + b^2 = 1$ and $L_7(a) = 0$. Here

$$L_7(x) = 2(T_1(x) + T_2(x) + T_3(x)) + 1 = 8x^3 + 4x^2 - 4x - 1.$$

Since $a = 61$ and $b = 11$ satisfy both $a^2 + b^2 = 1$ and $L_7(a) = 0$, we may choose $\omega_7 = 61 + 11i$. Once we found the ω_8 , ω_3 and ω_7 , the fundamental solution of $x^2 + y^2 = 1$ is

$$\omega_8\omega_3\omega_7 = (77 + 77i)(83 + 31i)(61 + 11i) = 58 + 12i.$$

Therefore, the solutions (x, y) of the Pell equation $x^2 + y^2 = 1$ over \mathbb{F}_{167} are given by $x + yi = (58 + 12i)^k$, where $k \in \{0, 1, 2, \dots, 167\}$.

5. THE SOLUTION OF THE GENERAL PELL EQUATION $x^2 - my^2 = n$

In this section we shall solve the general Pell equation $x^2 - my^2 = n$ for any $m, n \in \mathbb{F}$. As we shall see, in order to solve the general Pell equation, it suffices to find a fundamental solution for $x^2 - my^2 = 1$ and a particular solution for $x^2 - my^2 = n$. We begin by proving the existence and form of a solution for the *negative* Pell equation $x^2 - my^2 = -1$.

Proposition 5.1. *Suppose that \mathbb{F} is a finite field with q elements and let $m \in \mathbb{F}$ be a non-square element. In addition, let c be the positive integer such that $2^c \parallel q + 1$. Then the polynomial $T_{2^{c-1}}^*$ has 2^{c-1} roots over \mathbb{F} . Furthermore, if $T_{2^{c-1}}^*(a) = 0$, then there exists $b \in \mathbb{F}$ such that $N(a + b\sqrt{m}) = -1$.*

Proof. Consider the sets

$$\begin{aligned} A &= \{a + b\sqrt{m} : a, b \in \mathbb{F}, \text{ord}(a + b\sqrt{m}) = 2^{c+1}\}, \\ B &= \{a + b\sqrt{m} : a, b \in \mathbb{F}, T_{2^{c-1}}^*(a) = 0, N(a + b\sqrt{m}) = -1\}. \end{aligned}$$

First we shall prove that $A = B$. We begin by proving that $A \subseteq B$. Suppose that $\sigma = a + b\sqrt{m}$ has order 2^{c+1} . We shall prove that $N(\sigma) = -1$ and $T_{2^{c-1}}^*(a) = 0$.

If $\text{ord}(\sigma) = 2^{c+1}$, then $\sigma^{2^c} \neq 1$. Since $\sigma^{2^{c+1}} = 1$ implies either $\sigma^{2^c} = 1$ or $\sigma^{2^c} = -1$, it follows that $\sigma^{2^c} = -1$. Therefore

$$(\sigma^{2^c})^{(q+1)/2^c} = (-1)^{(q+1)/2^c},$$

so $\sigma^{q+1} = -1$, since $(q + 1)/2^c$ is odd. By Proposition 3.2, $N(\sigma) = \sigma\bar{\sigma} = \sigma^{q+1}$, so $N(\sigma) = -1$, as required.

Next we prove that $T_{2^{c-1}}^*(a) = 0$. By our assumption, the order of σ is 2^{c+1} . Hence

$$(a + b\sqrt{m})^{2^c} = -1.$$

In addition, since $N(\sigma) = a^2 - mb^2 = -1$, we deduce by Proposition 4.2 that

$$T_{2^c}^*(a) + bS_{2^{c-1}}^*(a)\sqrt{m} = -1.$$

Therefore $T_{2^c}^*(a) = -1$. Since $T_{2^c}^* = 2(T_{2^{c-1}}^*)^2 - 1$ by Proposition 2.2 (2), it follows that $2(T_{2^{c-1}}^*)^2(a) = 0$, so $T_{2^{c-1}}^*(a) = 0$. Hence $A \subseteq B$, as required.

In view of the fact that $A \subseteq B$, it suffices to prove that $|A| \geq |B|$. Let r be the number of roots of $T_{2^{c-1}}^*$ over \mathbb{F} . Clearly, $|B| \leq 2r$. Since $|A| = \varphi(2^{c+1}) = 2^c$ and $A \subseteq B$, it follows that $2^c \leq |B|$. Thus $2^c \leq 2r$, that is, $2^{c-1} \leq r$. On the other hand, $r \leq \deg(T_{2^{c-1}}^*) = 2^{c-1}$, so $r = 2^{c-1}$. Therefore, $|B| \leq 2^c = |A|$, so $|A| = |B|$, as required.

Note that since $|B| = 2 \deg(T_{2^{c-1}}^*)$, it follows that for every root of $T_{2^{c-1}}^*$, there exists indeed at least one element $b \in \mathbb{F}$ such that $N(a + b\sqrt{m}) \neq -1$, as claimed. \square

Theorem 5.2. *Let $m \in \mathbb{F}$ be a non-square element. In addition, let c be the positive integer such that $2^c \parallel q + 1$. Then:*

- (a) *If $n \in \mathbb{F}$ is a square element, then $(\sqrt{n}, 0)$ is a solution of $x^2 - my^2 = n$, where \sqrt{n} denotes any pre-chosen root of n in \mathbb{F} .*
- (b) *If $n \in \mathbb{F}$ is a non-square element, then $(ny_0, nx_0/\sqrt{mn})$ is a solution of $x^2 - my^2 = n$, where \sqrt{mn} denotes any pre-chosen root of mn in \mathbb{F} and (x_0, y_0) is any solution of the negative Pell equation $x^2 - ny^2 = -1$ such that $T_{2^{c-1}}^*(x_0) = 0$, where T_k^* denotes the k th conjugate Chebyshev polynomial.*

Proof. Part (a) is clear, so we may proceed to part (b). As in the proof of Proposition 3.2, note that since m and n are both non-square, it follows by Proposition 3.1 that $m^{(q-1)/2} = -1$ and $n^{(q-1)/2} = -1$, so $(mn)^{(q-1)/2} = 1$. Therefore, mn is a square element, so \sqrt{mn} exists in \mathbb{F} . Now, since $x_0^2 - ny_0^2 = -1$, it follows that

$$(ny_0)^2 - m\left(\frac{nx_0}{\sqrt{mn}}\right)^2 = n^2y_0^2 - m \cdot \frac{n^2x_0^2}{mn} = n(ny_0^2 - x_0^2) = n.$$

Additionally, by Proposition 5.1 we may assume that x_0 satisfies $T_{2^{c-1}}^*(x_0) = 0$, as required. \square

Theorem 5.3. *Let $m, n \in \mathbb{F}$ such that m is a non-square. Then the equation $x^2 - my^2 = n$ has exactly $q + 1$ solutions over \mathbb{F} . Furthermore, these $q + 1$ solutions are given by*

$$x + y\sqrt{m} = \sigma\omega^k,$$

where $\sigma \in \mathbb{F}(\sqrt{m})$ is any particular solution of $x^2 - my^2 = n$, $\omega \in \mathbb{F}(\sqrt{m})$ is a fundamental solution of $x^2 - my^2 = 1$ and $k \in \{0, 1, 2, \dots, q\}$.

Proof. By Proposition 5.1 and Theorem 5.2 it follows that the general Pell equation $x^2 - my^2 = n$ is solvable. Let $\sigma \in \mathbb{F}(\sqrt{m})$ be a particular solution of $x^2 - my^2 = n$. Observe that it suffices to prove that

$$\{\tau \in \mathbb{F}(\sqrt{m}) : N(\tau) = n\} = \{\sigma\omega^k : 0 \leq k \leq q\}.$$

First, note that by our assumptions $N(\sigma) = n$ and $N(\omega) = 1$. Now, by the multiplicity of the norm, given $k \in \{0, 1, 2, \dots, q\}$, we obtain

$$N(\sigma\omega^k) = N(\sigma)N(\omega)^k = n \cdot 1^k = n,$$

so $\sigma\omega^k$ is a solution of $x^2 - my^2 = n$.

Conversely, suppose that $\tau \in \mathbb{F}(\sqrt{m})$ satisfies $N(\tau) = n$. Thus $N(\tau) = N(\sigma)$, so $N(\tau/\sigma) = N(\tau)/N(\sigma) = 1$. Therefore, τ/σ is a solution of $x^2 - my^2 = 1$ and hence, by Theorem 4.5 there exist a fundamental solution $\omega \in \mathbb{F}(\sqrt{m})$ and $k \in \{0, 1, \dots, q\}$ such that $\tau/\sigma = \omega^k$. Thus $\tau = \sigma\omega^k$, as required. \square

Example 5.4. Let us solve the equation $x^2 + y^2 + z^2 = 1$ over the field $\mathbb{F} = \mathbb{F}_7$. Clearly, this equation is equivalent to $x^2 + y^2 = 1 - z^2$, which by Theorem 5.3 is solvable for every $z \in \mathbb{F}$.

First, in order to solve this equation, we need to find a fundamental solution for $x^2 + y^2 = 1$. Here $m = -1$ and $q = 7$, so $q + 1 = 2^3$. Note that $(-1 \mid 7) = -1$ since $7 \equiv 3 \pmod{4}$, so $m = -1$ is a non-square element in \mathbb{F} . By Theorem 4.5, we deduce that $x^2 + y^2 = 1$ has $q + 1 = 8$ solutions and a fundamental solution for this equation is ω_8 . In this case $r = 3$, so by Theorem 4.5 (c) $\omega_8 = a + bi$, where $i := \sqrt{-1}$ and $a, b \in \mathbb{F}$ are any two elements that satisfy both of the equations $a^2 + b^2 = 1$ and $T_2(a) = 0$. Here $T_2(x) = 2x^2 - 1$. Since $a = 2$ and $b = 2$ satisfy both $a^2 + b^2 = 1$ and $T_2(a) = 0$, we may choose $\omega_8 = 2 + 2i$.

Next, we shall solve $x^2 + y^2 = 1 - z^2$ for every $z \in \mathbb{F}$. For $z = 0$, the equation is $x^2 + y^2 = 1$ and we may take the particular solution $\sigma = 1$. For $z = \pm 1$, the equation is $x^2 + y^2 = 0$ and we may take the particular solution $\sigma = 0$. For $z = \pm 2$, the equation is $x^2 + y^2 = 4$ and we may take the particular solution $\sigma = 2$. Finally, for $z = \pm 3$, the equation is $x^2 + y^2 = 6$ and we may take the particular solution $\sigma = 3 + 2i$.

Therefore, the solutions of $x^2 + y^2 + z^2 = 1$ are the triples (x, y, z) such that

$$\begin{aligned} x + yi &= (2 + 2i)^k, & z &= 0, \\ x + yi &= 0, & z &= \pm 1, \\ x + yi &= 2(2 + 2i)^k, & z &= \pm 2, \\ x + yi &= (3 + 2i)(2 + 2i)^k, & z &= \pm 3, \end{aligned}$$

where $k \in \{0, 1, \dots, 7\}$. This gives us the following 42 solutions:

$$\begin{array}{ccccc}
 (1, 0, 0) & (2, 0, \pm 2) & (3, 2, \pm 3) & (0, 0, \pm 1) & (2, 2, 0) \\
 (4, 4, \pm 2) & (2, 3, \pm 3) & (0, 1, 0) & (0, 2, \pm 2) & (5, 3, \pm 3) \\
 (5, 2, 0) & (3, 4, \pm 2) & (4, 2, \pm 3) & (6, 0, 0) & (5, 0, \pm 2) \\
 (4, 5, \pm 3) & (5, 5, 0) & (3, 3, \pm 2) & (5, 4, \pm 3) & (0, 6, 0) \\
 (0, 5, \pm 2) & (2, 4, \pm 3) & (2, 5, 0) & (4, 3, \pm 2) & (3, 5, \pm 3)
 \end{array}$$

We conclude with a complete description of the solutions of the general Pell equation $x^2 - my^2 = n$ for a square element m .

Theorem 5.5. *Let $m, n \in \mathbb{F}$ such that $m \neq 0$ is a square element. Consider the equation*

$$(*) \quad x^2 - my^2 = n.$$

- (a) *If $n = 0$, then $(*)$ has exactly $2q - 1$ solutions (x, y) over \mathbb{F} . Moreover, these solutions are given by*

$$(x, y) = (\pm a\sqrt{m}, a),$$

where $a \in \mathbb{F}$ and \sqrt{m} denotes any pre-chosen root of m in \mathbb{F} .

- (b) *If $n \neq 0$, then $(*)$ has exactly $q - 1$ solutions (x, y) over \mathbb{F} . Moreover, these solutions are given by*

$$(x, y) = \left(\frac{a + n/a}{2}, \frac{a - n/a}{2\sqrt{m}} \right),$$

where $a \in \mathbb{F}^*$ and \sqrt{m} denotes any pre-chosen root of m in \mathbb{F} .

Proof. (a) If $a \in \mathbb{F}$, then $(x, y) = (\pm a\sqrt{m}, a)$ satisfies the equation $x^2 - my^2 = 0$. Indeed,

$$x^2 - my^2 = (\pm a\sqrt{m})^2 - ma^2 = a^2m - ma^2 = 0.$$

Conversely, if $x^2 - my^2 = 0$, then $(x - \sqrt{m}y)(x + \sqrt{m}y) = 0$, so either $x = \sqrt{m}y$ or $x = -\sqrt{m}y$. Therefore, there exists $a \in \mathbb{F}$ such that either $(x, y) = (a\sqrt{m}, a)$ or $(x, y) = (-a\sqrt{m}, a)$, as required.

Note that $(a\sqrt{m}, a) \neq (-a\sqrt{m}, a)$ if and only if $a \neq 0$, so when a extends over the nonzero elements of \mathbb{F} , the number of solutions is $2(q - 1)$. By adding to the count also the trivial solution $(0, 0)$, we obtain $2(q - 1) + 1 = 2q - 1$ solutions, as claimed.

- (b) If $a \in \mathbb{F}^*$, then

$$(x, y) = \left(\frac{a + 1/a}{2}, \frac{a - 1/a}{2\sqrt{m}} \right)$$

satisfies the equation $x^2 - my^2 = n$. Indeed,

$$x^2 - my^2 = \left(\frac{a + n/a}{2}\right)^2 - m\left(\frac{a - n/a}{2\sqrt{m}}\right)^2 = \frac{a^2 + n^2/a^2 + 2n}{4} - m \cdot \frac{a^2 + n^2/a^2 - 2n}{4m} = n.$$

Conversely, if $x^2 - my^2 = n$, then $(x - \sqrt{m}y)(x + \sqrt{m}y) = n$. Since $n \neq 0$, there exists $a \in \mathbb{F}^*$ such that

$$\begin{cases} x + \sqrt{m}y = a, \\ x - \sqrt{m}y = \frac{n}{a}. \end{cases}$$

Solving this system of linear equations gives

$$(x, y) = \left(\frac{a + n/a}{2}, \frac{a - n/a}{2\sqrt{m}}\right).$$

We note that since a extends over the nonzero elements of \mathbb{F} , the number of solutions is indeed $q - 1$. \square

Example 5.6. Let us solve the the general Pell equation $x^2 - 2y^2 = 5$ over the field $\mathbb{F} = \mathbb{F}_{17}$. Note that since $17 \equiv 1 \pmod{8}$, it follows that $(2 \mid 17) = 1$, so $m = 2$ is a square in \mathbb{F} . Indeed, in this case $2 = 6^2$, so we may choose $\sqrt{m} = 6$. By Theorem 5.5 (b), the solutions of $x^2 - 2y^2 = 5$ are

$$(x, y) = \left(\frac{a + 5/a}{2}, \frac{a - 5/a}{2\sqrt{m}}\right) = \left(\frac{a + 5/a}{2}, \frac{a - 5/a}{12}\right),$$

where $a \in \mathbb{F}_{17}^*$, which gives the following 16 solutions:

$$\begin{array}{cccccccc} (3,11) & (15,12) & (8,2) & (9,2) & (3,6) & (2,12) & (16,7) & (1,7) \\ (1,10) & (15,5) & (14,11) & (8,15) & (9,15) & (2,5) & (14,6) & (16,10) \end{array}$$

Acknowledgments. I wish to thank Prof. Marcel Herzog for his careful reading of the first draft of this paper. I also wish to thank the referee for his important remarks and suggestions.

References

- [1] *A. T. Benjamin, D. Walton*: Counting on Chebyshev polynomials. *Math. Mag.* 82 (2009), 117–126. [zbl](#) [MR](#) [doi](#)
- [2] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics 84. Springer, New York, 1990. [zbl](#) [MR](#) [doi](#)
- [3] *W. J. LeVeque*: Topics in Number Theory. Vol I. Dover Publications, Mineola, 2002. [zbl](#) [MR](#)

Author's address: Boaz Cohen, Department of Computer Science, The Academic College of Tel-Aviv, Rabenu Yeruham St., P.O.Box 8401 Tel-Aviv Yaffo, 6818211, Israel, e-mail: arctanx@gmail.com.