On the cubic Pell equation over finite fields

Simone Dutto*, Nadir Murru**
* Politecnico di Torino, Department of Mathematics
simone.dutto@polito.it
** Università degli Studi di Trento, Department of Mathematics
nadir.murru@unitn.it

Abstract

The classical Pell equation can be extended to the cubic case considering the elements of norm one in $\mathbb{Z}[\sqrt[3]{r}]$, which satisfy

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1.$$

The solution of the cubic Pell equation is harder than the classical case, indeed a method for solving it as Diophantine equation is still missing [3]. In this paper, we study the cubic Pell equation over finite fields, extending the results that hold for the classical one. In particular, we provide a novel method for counting the number of solutions in all possible cases depending on the value of r. Moreover, we are also able to provide a method for generating all the solutions.

1 Introduction

The Pell equation

$$x^2 - dy^2 = 1,$$

is an important and well studied Diophantine equation, for d a non–square positive integer. Finding its solutions is equivalent to finding the elements of $\mathbb{Z}[\sqrt{d}]$ of norm one. There are well known methods for solving this equation. They are mainly based on continued fractions that allow to find a fundamental solution, which is then used for generating all the other ones. Currently, there are still several important issues regarding the Pell equation. For instance, the study of the size of the fundamental solution is an interesting problem addressed in several papers, e.g., [8, 12, 23]. Recently, the solvability of simultaneous Pell equations and explicit formulas for their solutions have been also studied in [15, 9, 13]. Moreover, it is also interesting to study the Pell equation over finite fields, determining the number of solutions and their properties [19, 21, 20, 10]. For further information about the importance of the study of the Pell equation see, e.g., [17].

Thus, it is natural to consider generalizations of the Pell equation, starting from the cubic case. Considering the connection between the Pell equation and the elements of norm one in a quadratic field, the analogue of the Pell equation in the cubic case is given by the equation

$$x^3 + ry^3 + r^2z^3 - 3rxyz = 1,$$

where r is a cube–free integer, i.e., we are asking for the elements of norm one in $\mathbb{Z}[\sqrt[3]{r}]$. First studies of the cubic Pell equation can be found in [18] and [22]. In [11], the author proposed a method for solving the cubic Pell equation by means of a generalization of continued fractions due to Jacobi [16]. However, this method is not always useful for this purpose, since the periodicity of the Jacobi algorithm is still a fascinating open problem for all cubic irrationals. This question was also addressed, e.g., in [6] and [7]. The solutions of the cubic Pell equation were studied in [2] from the point of view of recurrent sequences, since Lucas sequences are solutions, up to constants, of the classical Pell equation. In general, the cubic Pell equation is very hard to solve for any cube–free r. In [3], the author exhibited an algorithm for finding the fundamental solutions of the cubic Pell equation that works only in some cases. Thus, the problem of solving the cubic Pell equation is still open. For more motivation and results about the cubic Pell equation see also [14].

In this paper, we address the problem of solving the cubic Pell equation over finite fields. In particular, in Section 2 we recall the classical Pell equation and its definition as the elements of norm one in a quadratic field. We also introduce a particular parameterization, which is useful for studying the Pell equation over finite fields and it is also handy for a generalization in the cubic case. Section 3 is devoted to the introduction of the cubic Pell equation. Here, we also introduce its parameterization that will allow to study its structure over finite fields, giving also methods for generating the solutions. Finally, in Section 4, we fully describe the behavior of the cubic Pell equation over finite fields.

2 The Pell equation

This section is devoted to the classical Pell equation. In particular, in Section 2.1, we provide a brief overview about the Pell equation and the known results about its group structure, with a particular focus on its behaviour over finite fields. Then, in Section 2.2, we introduce and study a specific parameterization for the Pell conic which is useful for obtaining in a different way some results about the Pell conic, with the possibility to be generalized to the cubic case. Moreover, the parameterization also allows to generate in a direct way all the solutions of the Pell equation.

2.1 Preliminaries

The classical Pell equation is the equation of the form

$$x^2 - dy^2 = 1,$$

where d is a positive square–free integer and solutions are sought for $(x, y) \in \mathbb{Z}^2$.

In this work we consider the Pell equation in general terms, considering any element d in a field $\mathbb{F}$ and taking the polynomial ring

$$\mathcal{R}_d := \mathbb{F}[t]/\langle t^2 - d\rangle,$$

whose elements are the classes of equivalence

$$[x + yt] := \{x + yt + k(t)(t^2 - d) \mid k(t) \in \mathbb{F}[t]\}, \quad \text{for any } x, y \in \mathbb{F}.$$

This quotient ring inherits from the polynomial product the operation

$$[x_1 + y_1 t] \cdot [x_2 + y_2 t] = [(x_1 x_2 + d y_1 y_2) + (x_1 y_2 + y_1 x_2) t]. \tag{2.1}$$

The conjugate of an element $[x + yt] \in \mathcal{R}_d$ is defined as $[x - yt]$. The product of an element with its conjugate defines the norm

$$N_d([x + yt]) := [x + yt] \cdot [x - yt] = x^2 - dy^2 \in \mathbb{F}.$$

The unitary elements of $\mathcal{R}_d$ with respect to the norm N_d is denoted by

$$\mathcal{U}(\mathcal{R}_d) := \{[x + yt] \in \mathcal{R}_d \mid N_d([x + yt]) = 1\},$$

and form a commutative group that is clearly isomorphic to the *Pell conic*

$$\mathcal{C}_d := \{(x, y) \in \mathbb{F}^2 \mid x^2 - dy^2 = 1\},$$

equipped with the classical Brahmagupta product

$$(x_1, y_1) \otimes_d (x_2, y_2) := (x_1 x_2 + d y_1 y_2, x_1 y_2 + y_1 x_2).$$

Due to this isomorphism, in the following we will use the norm N_d also for the points of the conic and the notation $\otimes_d$ also for denoting the product over $\mathcal{R}_d$. In general, we denote by $(x, y)^{\otimes_d k}$ the k-power of (x, y) with respect to $\otimes_d$.

The operation $\otimes_d$ over the Pell conic has an interesting geometric interpretation [5]: in order to obtain the point $(x_1, y_1) \otimes_d (x_2, y_2)$, consider the line through $(x_1, y_1), (x_2, y_2)$ and take its parallel line through $(1, 0)$; the latter intersects the conic in a second point that is actually $(x_1, y_1) \otimes_d (x_2, y_2)$. As observed in [5], this geometric interpretation is analogous to the classical operation on elliptic curves.

In [19], the authors fully described the group structure of the Pell equation over a finite field $\mathbb{F}_q$, with $q = p^k$ and p prime. We summarize these results in the following theorem.

Theorem 2.1.

1. If d is a non–square in $\mathbb{F}_q$, then $(\mathcal{C}_d, \otimes_d)$ is a cyclic group of order $q + 1$.
2. If d is a square in $\mathbb{F}_q$, then $(\mathcal{C}_d, \otimes_d)$ is a cyclic group of order $q - 1$, moreover there is the following isomorphism:

$$\begin{aligned} (\mathcal{C}_d, \otimes_d) \;&\cong\; \mathbb{F}_q^{\times}, \\ (x, y) &\longmapsto x - sy, \\ \left(\frac{1 + u^2}{2u}, \frac{1 - u^2}{2su} \right) &\longleftarrow u. \end{aligned}$$

Proof. See [19]. □

Unfortunately, it is not possible to generalize the techniques used in [19] for a full description of the cubic case. For this reason, in Section 2.2, we introduce and exploit a particular parameterization for the Pell conic that allows to recover the results of Theorem 2.1 and can be also generalized to the cubic case. Moreover, the use of the parameterization gives a method for generating in a simple and direct way all the solutions of the Pell equation. In this way, in Sections 3 and 4, we will be able to fully describe the group structure of the solutions of the cubic Pell equation over finite fields. This will also give a method for generating all the solutions.

2.2 A parameterization for the Pell conic

Here we define a parameterization for the Pell conic over any field $\mathbb{F}$ and describe its elements depending on d being or not a square. Then, we prove that it is actually isomorphic to the Pell conic, providing also the explicit group isomorphism. As we will observe in Section 3, this result is not adaptable to the cubic case. Thus, we also provide a specific result for the case d square in a finite field, that will allow us to obtain generalizations for some instances in the cubic case.

Definition 2.1. The *projectivization* of $\mathcal{R}_d$ is $\mathbb{P}_d := \mathcal{R}_d^{\otimes_d}/\mathbb{F}^\times$, where $\mathcal{R}_d^{\otimes_d}$ is the set of the invertible elements of $\mathcal{R}_d$ with respect to $\otimes_d$. We denote the elements of $\mathbb{P}_d$ by $[m:n]$. In particular, they are the classes of equivalence of the elements $[m+nt] \in \mathcal{R}_d^{\otimes_d}$ given by

$$[m:n] := \{\lambda[m+nt] \mid \lambda \in \mathbb{F}^\times\}.$$

If $n \in \mathbb{F}^\times$, then $[m+nt] \in \mathcal{R}_d^{\otimes_d}$ is equivalent to $[mn^{-1}+t] \in \mathcal{R}_d^{\otimes_d}$. Thus, when $n=0$ we choose as *canonical representative* in $\mathbb{P}_d$ $[1:0]$ while, in the other cases, we take $[mn^{-1}:1]$.
Since the Brahmagupta product $\otimes_d$ consists of homogeneous polynomials, it is well defined also on $\mathbb{P}_d$ and determines a commutative group with identity $[1:0]$ and inverse of $[m:1]$ given by $[-m:1]$.

The elements in $\mathbb{P}_d$ depends on the elements in $\mathcal{R}_d^{\otimes_d}$, in particular:

1. if d is a non–square element in $\mathbb{F}$, then $\mathcal{R}_d^{\otimes_d} = \mathcal{R}_d \smallsetminus \{[0]\}$ and

   $$\mathbb{P}_d = \{[m:1] \mid m \in \mathbb{F}\} \cup \{[1:0]\} \sim \mathbb{F} \cup \{\alpha\}, \tag{2.2}$$

   where α denotes an element not in $\mathbb{F}$ that can be seen as the point at infinity;

2. if d is a square in $\mathbb{F}$ and s is a fixed square root of d in $\mathbb{F}$, then there is the factorization $t^2 - d = (t+s)(t-s) \in \mathbb{F}[t]$ and, for any $y \in \mathbb{F}$, the classes $[y(s+t)]$ and $[y(-s+t)]$ are zero–divisors in $\mathcal{R}_d$, so that

   $$\mathcal{R}_d^{\otimes_d} = \mathcal{R}_d \smallsetminus \{[0], [sy+yt], [-sy+yt] \mid y \in \mathbb{F}\}.$$

   Thus,

   $$\mathbb{P}_d = \big\{[m:1] \mid m \in \mathbb{F}\smallsetminus\{\pm s\}\big\} \cup \big\{[1:0]\big\} \sim (\mathbb{F}\smallsetminus\{\pm s\}) \cup \{\alpha\}. \tag{2.3}$$

The following theorem provides an explicit group isomorphism between the projectivization $(\mathbb{P}_d, \otimes_d)$ and the Pell conic $(\mathcal{C}_d, \otimes_d)$. The result was introduced in [4], here we give a different formulation and a proof that can be adapted to the cubic case.

Theorem 2.2. Given $d \in \mathbb{F}$, the following map is a group isomorphism

$$\begin{aligned} \phi : \big(\mathbb{P}_d, \otimes_d\big) &\xrightarrow{\sim} \big(\mathcal{C}_d, \otimes_d\big), \\ [m:n] &\longmapsto \frac{(m,n)^{\otimes_d 2}}{N_d(m,n)} = \left(\frac{m^2+dn^2}{m^2-dn^2}, \frac{2mn}{m^2-dn^2}\right), \end{aligned}$$

and its inverse is

$$\begin{aligned}\phi^{-1} : \big(\mathcal{C}_d, \otimes_d\big) &\xrightarrow{\sim} \big(\mathbb{P}_d, \otimes_d\big),\\ (-1,0) &\longmapsto [0:1],\\ (x,y) &\longmapsto [x+1:y].\end{aligned}$$

Proof. In order for ϕ to be a group isomorphism, it must be:

- well defined: if $[m:n] = [m':n'] \in \mathbb{P}_d$, then there is $\lambda \in \mathbb{F}^\times$ such that $[m':n'] = [\lambda m : \lambda n]$, and

$$\frac{(\lambda m, \lambda n)^{\otimes_d 2}}{N_d(\lambda m, \lambda n)} = \frac{\lambda^2 (m,n)^{\otimes_d 2}}{\lambda^2 N_d(m,n)} = \frac{(m,n)^{\otimes_d 2}}{N_d(m,n)},$$

  therefore ϕ is well defined. In addition, $\phi(\mathbb{P}_d) \subseteq \mathcal{C}_d$ since

$$N_d\big(\phi([m:n])\big) = \frac{N_d(m,n)^2}{N_d(m,n)^2} = 1;$$

- a group homomorphism: for any $[m_1:n_1], [m_2:n_2] \in \mathbb{P}_d$ we have

$$[m_1:n_1] \otimes_d [m_2:n_2] = [m_1 m_2 + d n_1 n_2 : m_1 n_2 + n_1 m_2],$$

  so that

$$\begin{aligned}\phi([m_1:n_1] \otimes_d [m_2:n_2]) &= \frac{(m_1 m_2 + d n_1 n_2, m_1 n_2 + n_1 m_2)^{\otimes_d 2}}{N_d(m_1 m_2 + d n_1 n_2, m_1 n_2 + n_1 m_2)}\\ &= \frac{(m_1, n_1)^{\otimes_d 2} \otimes_d (m_2, n_2)^{\otimes_d 2}}{N_d(m_1,n_1) N_d(m_2,n_2)}\\ &= \phi([m_1:n_1]) \otimes_d \phi([m_2:n_2]);\end{aligned}$$

- injective: for any $[m:n] \in \mathbb{P}_d$,

$$\begin{aligned}\phi([m:n]) = (1,0) &\Leftrightarrow \begin{cases} m^2 - dn^2 = m^2 + dn^2,\\ 0 = 2mn \end{cases}\\ &\Leftrightarrow n = 0 \Leftrightarrow \ker(\phi) = \{[1:0]\};\end{aligned}$$

- surjective: if $(x,0) \in \mathcal{C}_d$, then $x^2 = 1$, that is $x = \pm 1$ and we have $\phi([1:0]) = (1,0)$ and $\phi([0:1]) = (-1,0)$. Now let $(x,y) \in \mathcal{C}_d$ with $y \neq 0$. We have $d = \frac{x^2-1}{y^2}$ and, since $d \neq 0$, $x \neq \pm 1$. In particular, we are looking for $[m:n] \in \mathbb{P}_d$ such that

$$\begin{cases} x = \frac{m^2y^2 + (x^2-1)n^2}{m^2y^2 - (x^2-1)n^2},\\ y = \frac{2mny^2}{m^2y^2-(x^2-1)n^2} \end{cases} \Leftrightarrow \begin{cases} m^2y^2 - 2mnxy + n^2(x^2-1) = 0,\\ m^2y^2 - 2mny - n^2(x^2-1) = 0. \end{cases}$$

  Subtracting the second equation to the first one, we obtain

$$2n^2(x^2-1) = 2mn(x-1).$$

  Since $x \neq 1$ and $n \neq 0$, we get $m = n\frac{x+1}{y}$. Therefore $\phi([x+1:y]) = (x,y)$ and this concludes the proof of the surjectivity.

In conclusion, ϕ is a group isomorphism with the wanted inverse. $\square$

Thus, the projectivization $\mathbb{P}_d$ is actually a parameterization of the Pell conic, which is useful for studying some of its properties over finite fields and will be naturally generalized also to the cubic case.

Remark 2.1. The group isomorphism ϕ gives also a direct method to generate all the solutions of the Pell equation $x^2 - dy^2 = 1 \in \mathbb{F}$ from the elements of $\mathbb{P}_d$, which require half the size to be stored when the notation introduced in Eqs. (2.2) and (2.3) is exploited, since

$$\begin{aligned}\phi(\alpha) &= \phi([1:0]) = (1,0),\\ \phi(0) &= \phi([0:1]) = (-1,0),\\ \phi(m) &= \phi([m:1]) = \left(\frac{m^2+d}{m^2-d}, \frac{2m}{m^2-d}\right), \quad \text{for } m \neq \alpha, 0.\end{aligned}$$

Theorem 2.2 gives also an idea on how to obtain a parameterization for the cubic Pell equation. However, the theorem can not be generalized to the cubic case over a generic field. In order to obtain a full characterization of the Pell cubic over finite fields, we will generalize the results in Theorem 2.1 but we also need the following theorem. The statement follows directly from Theorems 2.1 and 2.2, but we give an alternative proof without exploiting Theorem 2.2, so that it can be easily generalized to the cubic case.

Theorem 2.3. If d is a square in $\mathbb{F}_q$, then the group isomorphism between $\mathcal{P}_d$ and $\mathbb{F}_q^\times$ is given by the following map

$$\begin{aligned}\left(\mathbb{P}_d, \otimes_d\right) &\cong \mathbb{F}_q^\times,\\ [m:n] &\longmapsto \frac{m - sn}{m + sn}\end{aligned}$$

whose inverse is

$$[s(1+u) : 1-u] \longleftarrow u.$$

Proof. Fix s square root of d in $\mathbb{F}_q$, $t^2 - d$ is reducible over $\mathbb{F}_q$ as

$$t^2 - d = (t-s)(t+s),$$

so that, using the Chinese remainder theorem, there is the ring isomorphism

$$\begin{aligned}\mathcal{R}_d = \mathbb{F}_q[t]/\langle t^2 - d\rangle &\xrightarrow{\sim} \mathbb{F}_q[t]/\langle t-s\rangle \times \mathbb{F}_q[t]/\langle t+s\rangle,\\ [x+yt] &\longmapsto ([x+sy],[x-sy]).\end{aligned}$$

In addition, $\mathbb{F}_q[t]/\langle t-s\rangle \cong \mathbb{F}_q[t]/\langle t+s\rangle \cong \mathbb{F}_q$. When passing to the quotients, we obtain that

$$\left(\mathbb{P}_d, \otimes_d\right) = \mathcal{R}_d^{\otimes_d}/\mathbb{F}_q^\times \cong (\mathbb{F}_q^\times \times \mathbb{F}_q^\times)/\mathbb{F}_q^\times \cong \mathbb{F}_q^\times,$$

through the map in the statement. This confirms that $\left(\mathbb{P}_d, \otimes_d\right)$ is a cyclic group of order $q-1$. $\square$

For completeness, we observe that if d is not a square in $\mathbb{F}_q$, then $\mathcal{R}_d \cong \mathbb{F}_{q^2}$ and we have that $\mathbb{P}_d$ is cyclic of order $q+1$ because

$$\left(\mathbb{P}_d, \otimes_d\right) = \mathcal{R}_d^{\otimes_d}/\mathbb{F}_q^\times \cong \mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times.$$

Now we are ready to study the cubic Pell equation by generalizing the described results for the Pell conic.

3 The cubic Pell equation

In this section, we introduce and study the cubic Pell equation introducing a parameterization similar to the one given in Definition 2.1 and studying its group structure. Then we approach the study of the Pell cubic equation over finite fields in the next section.

Given a field $\mathbb{F}$ and an element $r \in \mathbb{F}$, we consider the polynomial ring

$$\mathcal{R}_r := \mathbb{F}[t]/\langle t^3 - r \rangle,$$

whose elements are the classes of equivalence

$$[x + yt + zt^2] := \{x + yt + zt^2 + k(t)(t^3 - r) \mid k(t) \in \mathbb{F}[t]\}.$$

This quotient ring inherits from the polynomial product the operation

$$\begin{aligned}[x_1 + y_1 t + z_1 t^2] \cdot [x_2 + y_2 t + z_2 t^2] = [&x_1 x_2 + r(y_1 z_2 + z_1 y_2) \\ &+ (x_1 y_2 + y_1 x_2 + r z_1 z_2)t \\ &+ (x_1 z_2 + y_1 y_2 + z_1 x_2)t^2].\end{aligned}$$

Considering the cubic roots of unity $\{1, \omega, \omega^2\}$, an element $[x+yt+zt^2] \in \mathcal{R}_r$ has two conjugates

$$[x + y\omega t + z\omega^2 t^2], \quad [x + y\omega^2 t + z\omega t^2],$$

which we use analogously to the quadratic case to define the norm

$$\begin{aligned}N_r([x + yt + zt^2]) &:= [x + yt + zt^2] \cdot [x + y\omega t + z\omega^2 t^2] \cdot [x + y\omega^2 t + z\omega t^2] \\ &= x^3 - 3rxyz + ry^3 + r^2 z^3.\end{aligned}$$

As for the Pell conic, this allows to provide a trivial group isomorphism between the unitary elements of $\mathcal{R}_r$, denoted by

$$\mathcal{U}(\mathcal{R}_r) := \{[x + yt + zt^2] \in \mathcal{R}_r \mid N_r([x + yt + zt^2]) = 1\},$$

and the *Pell cubic*

$$\mathcal{C}_r := \{(x, y, z) \in \mathbb{F}^3 \mid x^3 - 3rxyz + ry^3 + r^2 z^3 = 1\}.$$

The Pell cubic, with the generalization of the Brahmagupta product

$$\begin{aligned}(x_1, y_1, z_1) \odot_r (x_2, y_2, z_2) := \big(&x_1 x_2 + r(y_1 z_2 + z_1 y_2), \\ &x_1 y_2 + y_1 x_2 + r z_1 z_2, \\ &x_1 z_2 + y_1 y_2 + z_1 x_2\big),\end{aligned}$$

is a commutative group with identity $(1, 0, 0)$ and inverse of an element (x, y, z) given by the product of its conjugates

$$(x, y\omega, z\omega^2) \odot_r (x, y\omega^2, z\omega t^2) = (x^2 - ryz, rz^2 - xy, y^2 - xz).$$

Due to this group isomorphism, in the following we will use the norm N_r also for the points of the cubic and the notation $\odot_r$ also for denoting the product over $\mathcal{R}_r$. In general, we denote by $(x, y, z)^{\odot_r k}$ the k-power of (x, y, z) with $\odot_r$.

Now, we introduce a parameterization for the Pell cubic, similar to the one described in Definition 2.1, then we study its group structure.

Definition 3.1. The *projectivization* of $\mathcal{R}_r$ is $\mathbb{P}_r := \mathcal{R}_r^{\odot_r}/\mathbb{F}^\times$, where $\mathcal{R}_r^{\odot_r}$ is the set of the invertible elements of $\mathcal{R}_r$ with respect to $\odot_r$. We denote the elements of $\mathbb{P}_r$ by $[l : m : n]$. In particular, they are the classes of equivalence of the elements $[l + mt + nt^2] \in \mathcal{R}_r^{\odot_r}$ given by

$$[l : m : n] := \{\lambda[l + mt + nt^2] \mid \lambda \in \mathbb{F}^\times\}.$$

If $n \in \mathbb{F}^\times$, then $[l+mt+nt^2]$ is equivalent to $[ln^{-1}+mn^{-1}t+t^2]$ and we choose $[ln^{-1} : mn^{-1} : 1]$ as *canonical representative* in $\mathbb{P}_r$. Otherwise, if $n = 0$ and $m \in \mathbb{F}^\times$, then we take as canonical representative $[lm^{-1} : 1 : 0]$ and finally, when $m = n = 0$, the canonical representative is $[1 : 0 : 0]$.
Since the product $\odot_r$ consists of homogeneous polynomials, it is well defined also on $\mathbb{P}_r$ and determines a commutative group with identity $[1 : 0 : 0]$ and inverse of $[l : m : n]$ given by $[l^2 - rmn : rn^2 - lm : m^2 - ln]$, i.e.,

$$[l : m : 1] \odot_r [l^2 - rm : r - lm : m^2 - l] = [1 : 0 : 0],$$
$$[l : 1 : 0] \odot_r [l^2 : -l : 1] = [1 : 0 : 0].$$

Now, we study the elements of the projectivization depending on the parameter r since it is useful for giving a complete characterization of the Pell cubic over finite fields. Specifically, there are three possible cases:

1. if r is not a cube in $\mathbb{F}$, then $N_r([x + yt + zt^2]) \neq 0 \Leftrightarrow [x + yt + zt^2] \neq [0]$ and
$$\begin{aligned}\mathbb{P}_r &= \{[l : m : 1], [l : 1 : 0], [1 : 0 : 0] \mid l, m \in \mathbb{F}\} \\ &\sim (\mathbb{F} \times \mathbb{F}) \cup (\mathbb{F} \times \{\alpha\}) \cup \{(\alpha, \alpha)\},\end{aligned} \tag{3.1}$$
where α denotes an elements not in $\mathbb{F}$. Because of its special behaviour with respect to $\odot_r$, we isolate the point at infinity (α, α) from the line at infinity $\mathbb{F} \times \{\alpha\}$;

2. if r is a cube and $\{1, \omega, \omega^2\} \subset \mathbb{F}$, then $\mathbb{F}$ contains also all the cubic roots of r that, when denoting one of them with s, are $\{s, s\omega, s\omega^2\}$. In this case, $t^3 - r = (t - s)(t - s\omega)(t - s\omega^2) \in \mathbb{F}[t]$ and the elements of norm zero in $\mathcal{R}_r$ must be multiples of the classes of the three zero–divisors. Looking at the projectivization, this means that
$$\mathbb{P}_r = \{[l : m : n] \mid l, m, n \in \mathbb{F}\} \setminus \langle [-s : 1 : 0], [-s\omega : 1 : 0], [-s\omega^2 : 1 : 0]\rangle.$$
Hence, in order to obtain an explicit form for $\mathbb{P}_r$ like in Eq. (3.1), we need to study the multiples of these three elements.
The multiples of $[-s : 1 : 0]$ are, for any $l \in \mathbb{F}$,
$$[-s : 1 : 0] \odot_r [l : 1 : 0] = [-ls : -s + l : 1],$$
and, for any $l', m' \in \mathbb{F}$,
$$\begin{aligned}[-s : 1 : 0] \odot_r [l' : m' : 1] &= [-l's + s^3 : -m's + l' : -s + m'] \\ &= \begin{cases} [-s(l' - s^2) : l' - s^2 : 0], & \text{if } m' = s, \\ \left[-\left(\frac{l'-s^2}{m'-s}\right) s : \left(\frac{l'-s^2}{m'-s}\right) - s : 1\right], & \text{otherwise} \end{cases} \\ &= \begin{cases} [-s : 1 : 0], & \text{if } m' = s, \\ [-ls : l - s : 1], & \text{with } l = \frac{l'-s^2}{m'-s} \text{ otherwise.} \end{cases}\end{aligned}$$

We obtain analogous results for the other multiples, specifically

$$\begin{aligned}\big\langle[-s:1:0]\big\rangle &= \{[-s:1:0],[-ls:l-s:1]\,|\,l\in\mathbb{F}\},\\ \big\langle[-s\omega:1:0]\big\rangle &= \{[-s\omega:1:0],[-ls\omega:l-s\omega:1]\,|\,l\in\mathbb{F}\},\\ \big\langle[-s\omega^2:1:0]\big\rangle &= \{[-s\omega^2:1:0],[-ls\omega^2:l-s\omega^2:1]\,|\,l\in\mathbb{F}\}.\end{aligned}\tag{3.2}$$

In order to list precisely the elements of $\mathbb{P}_r$, we still need to study the intersections between the three obtained sets: if $0\le i<j\le 2$, then $[-ls\omega^i:l-s\omega^i:1]=[-l's\omega^j:l'-s\omega^j:1]$ if and only if

$$\begin{cases}-ls\omega^i=-l's\omega^j,\\ l-s\omega^i=l'-s\omega^j\end{cases}\Leftrightarrow\begin{cases}l=l'\omega^{j-i},\\ l'\omega^{j-i}-l'=s\omega^i-s\omega^j\end{cases}\Leftrightarrow\begin{cases}l=-s\omega^j,\\ l'=-s\omega^i.\end{cases}$$

This means that, for any $0\le i<j\le 2$,

$$\begin{aligned}\big\langle(-s\omega^i,1,0)\big\rangle\cap\big\langle(-s\omega^j,1,0)\big\rangle &= \big\{[s^2\omega^{i+j}:-s(\omega^i+\omega^j):1]\big\}\\ &= \big\{[s^2\omega^{i+j}:s\omega^k:1],\ k=3-i-j\big\}.\end{aligned}$$

Thus, when listing the elements of $\mathbb{P}_r$ by using the sets in Eq. (3.2), we have to consider that three elements are obtained twice. In particular, in $\langle[-s\omega^i:1:0]\rangle$, they are those with second coordinate $m=s\omega^k$ for $k\neq i$. For instance, one of the duplicates can be removed by the list by excluding for each $i\in\{0,1,2\}$ the element with $m=s\omega^{i-1}$, so that

$$\begin{aligned}\mathbb{P}_r=&\big\{[l:m:1],[l:1:0],[1:0:0]\,|\,l,m\in\mathbb{F}\big\}\\ &\smallsetminus\bigcup_{i\in\{0,1,2\}}\big\{[-s\omega^i:1:0],[-(m+s\omega^i)s\omega^i:m:1]\,|\,m\in\mathbb{F}\smallsetminus\{s\omega^{i-1}\}\big\};\end{aligned}\tag{3.3}$$

3. if r is a cube and $\mathbb{F}$ does not contain any non–trivial cubic root of unity, i.e., $\{\omega,\omega^2\}\not\subset\mathbb{F}$, then only one root s of r is in $\mathbb{F}$. In this case, we have $t^3-r=(t-s)(t^2+st+s^2)\in\mathbb{F}[t]$ and the elements of norm zero in $\mathcal{R}_r$ must be multiples of the classes of the two zero–divisors. Looking at the projectivization, this means that

   $$\mathbb{P}_r=\{[l:m:n]\,|\,l,m,n\in\mathbb{F}\}\smallsetminus\big\langle[-s:1:0],[s^2:s:1]\big\rangle.$$

   As in the previous case, the non–trivial multiples of $[-s:1:0]$ are the elements $[-(m+s)s:m:1]$ for $m\in\mathbb{F}$.

   This list already contains all the non–trivial multiples of the second zero–divisor since for every $[l:m:n]$ non multiple of $[-s:1:0]$, we have

   $$\begin{aligned}[s^2:s:1]\odot_r[l:m:n]&=[s^2(l+ms+ns^2):s(l+ms+ns^2):l+ms+ns^2]\\ &=[s^2:s:1].\end{aligned}$$

   In conclusion, the elements in the projectivization are exactly

   $$\begin{aligned}\mathbb{P}_r=&\big\{[l:m:1],[l:1:0],[1:0:0]\,|\,l,m\in\mathbb{F}\big\}\\ &\smallsetminus\big\{[-s:1:0],[-(m+s)s:m:1],[s^2:s:1]\,|\,m\in\mathbb{F}\big\}.\end{aligned}\tag{3.4}$$

Differently from the quadratic case, the group isomorphism between $(\mathbb{P}_r,\odot_r)$ and $(\mathcal{C}_r,\odot_r)$ is not easy to find in the case of a general field $\mathbb{F}$. However, we can exploit $\mathbb{P}_r$ for fully describing the group structure of $\mathcal{C}_r$ over finite fields.

4 The Pell cubic over finite fields

In this section, we give a full description of the solutions of the cubic Pell equation over a finite field $\mathbb{F}_q$ with $q = p^k$ and p prime, by generalizing the results described in Section 2. This characterization depends on the parameter $r \in \mathbb{F}_q$ and there are three different scenarios due to the value of $\gcd(3, q-1)$ in the extended Euler criterion [1]:

$$r \in \mathbb{F}_q \text{ is a cube} \Leftrightarrow r^{(q-1)/\gcd(3,q-1)} = 1.$$

In particular, there are three cases that we fully describe in the following subsections. When $q \equiv 1 \pmod 3$, r can be a non–cube or a cube with three roots in $\mathbb{F}_q$, and we can determine the structure of $(\mathcal{C}_r, \odot_r)$ without exploiting $(\mathbb{P}_r, \odot_r)$. However, we also obtain the connection with the projectivization in order to have an easy method for generating all the solutions of the cubic Pell equation. For the case $q \not\equiv 1 \pmod 3$, any r is a cube with only one root in $\mathbb{F}_q$, and we can characterize the structure of $(\mathcal{C}_r, \odot_r)$ only by using $(\mathbb{P}_r, \odot_r)$.

4.1 r non–cube

We know from the extended Euler criterion that a finite field $\mathbb{F}_q$ contains a non–cube element r if and only if $\gcd(3, q-1) > 1$, i.e., $q \equiv 1 \pmod 3$, so that

$$\begin{cases} r^{(q-1)/3} \neq 1, \\ r^{q-1} = 1 \end{cases} \Leftrightarrow r^{\lfloor q/3 \rfloor} = \omega, \text{ primitive cubic root of unity.}$$

In addition, the polynomial $t^3 - r$ is irreducible over $\mathbb{F}_q$, so that

$$\mathcal{R}_r = \mathbb{F}_q[t]/\langle t^3 - r\rangle \cong \mathbb{F}_{q^3},$$

and we obtain the following characterization of the Pell cubic by generalizing the first result in Theorem 2.1.

Theorem 4.1. If r is a non–cube in $\mathbb{F}_q$, then $(\mathcal{C}_r, \odot_r)$ is cyclic of order q^2+q+1.

Proof. We clearly have that $\mathcal{R}_r^{\odot_r} \cong \mathbb{F}_{q^3}^\times$ has $q^3 - 1$ elements. If $G \subset \mathbb{F}_{q^3}^\times$ denotes the multiplicative subgroup of order $q^2 + q + 1$, then $x + yt + zt^2 \in G$ if and only if $(x + yt + zt^2)^{q^2+q+1} = 1$ and

$$\begin{aligned}(x + yt + zt^2)^{q^2+q+1} &= (x + yt + zt^2)^{q^2}(x + yt + zt^2)^q(x + yt + zt^2) \\ &= (x + yt^q + zt^{2q})^q(x + yt^q + zt^{2q})(x + yt + zt^2),\end{aligned}$$

where

$$t^q = (t^3)^{(q-1)/3}t = r^{\lfloor q/3 \rfloor}t = \omega t, \quad \omega^q = (\omega^3)^{(q-1)/3}\omega = \omega,$$

so that

$$\begin{aligned}(x + yt + zt^2)^{q^2+q+1} &= (x + y\omega t + z\omega^2t^2)^q(x + y\omega t + z\omega^2t^2)(x + yt + zt^2) \\ &= (x + y\omega^q t^q + z\omega^{2q}t^{2q})(x + y\omega t + z\omega^2t^2)(x + yt + zt^2) \\ &= (x + y\omega^2 t + z\omega t^q)(x + y\omega t + z\omega^2t^2)(x + yt + zt^2) \\ &= x^3 - 3rxyz + ry^3 + r^2z^3.\end{aligned}$$

Thus, $x+yt+zt^2 \in G \Leftrightarrow (x, y, z) \in \mathcal{C}_r$. This association is a group isomorphism between G and $(\mathcal{C}_r, \odot_r)$, hence the Pell cubic is cyclic with order $q^2 + q + 1$. □

When looking at the projectivization, we have that $\#\mathbb{P}_r = q^2+q+1$ from Eq. (3.1) and, in addition, $(\mathbb{P}_r, \odot_r)$ is cyclic because quotient of cyclic groups

$$\big(\mathbb{P}_r, \odot_r\big) = \mathcal{R}_r^{\odot_r}/\mathbb{F}_q^\times \cong \mathbb{F}_{q^3}^\times/\mathbb{F}_q^\times.$$

Thus, we are sure that $(\mathbb{P}_r, \odot_r)$ is isomorphic to $(\mathcal{C}_r, \odot_r)$. In the following result, we obtain the explicit group isomorphism, which represents a useful method to generate all the solutions of the cubic Pell equation over $\mathbb{F}_q$.

Theorem 4.2. If $q \equiv 1 \pmod 3$ and $r \in \mathbb{F}_q^\times$ is a non–cube, then there is the group isomorphism

$$\begin{aligned}\psi_1 : \big(\mathbb{P}_r, \odot_r\big) &\xrightarrow{\sim} \big(\mathcal{C}_r, \odot_r\big),\\ [l:m:n] &\longmapsto N_r(l,m,n)^{\lfloor q/3\rfloor -1}(l,m,n)^{\odot_r 3}.\end{aligned}$$

Proof. In order for ψ_1 to be a group isomorphism, it must be:

- well defined: if $[l:m:n] = [l':m':n'] \in \mathbb{P}_r$, then there is $\lambda \in \mathbb{F}^\times$ such that $[l':m':n'] = [\lambda l : \lambda m : \lambda n]$, and since $\lfloor q/3\rfloor - 1 = (q-4)/3$

  $$\begin{aligned}N_r(\lambda l, \lambda m, \lambda n)^{\frac{q-4}{3}}(\lambda l, \lambda m, \lambda n)^{\odot_r 3} &= \big(\lambda^3 N_r(l,m,n)\big)^{\frac{q-4}{3}}\lambda^3(l,m,n)^{\odot_r 3}\\ &= \lambda^{q-1}N_r(l,m,n)^{\frac{q-4}{3}}(l,m,n)^{\odot_r 3},\end{aligned}$$

  therefore ψ_1 is well defined. In addition, $\psi_1\big(\mathbb{P}_r\big) \subseteq \mathcal{C}_r$ because

  $$\begin{aligned}N_r\big(\psi_1([l:m:n])\big) &= N_r(l,m,n)^{q-4}N_r(l,m,n)^3\\ &= N_r(l,m,n)^{q-1} = 1;\end{aligned}$$

- a group homomorphism: given $[l_1 : m_1 : n_1], [l_2 : m_2 : n_2] \in \mathbb{P}_r$, by denoting $[l:m:n] = [l_1 : m_1 : n_1] \odot_r [l_2 : m_2 : n_2]$, we have

  $$\begin{aligned}\psi_1([l:m:n]) &= N_r(l,m,n)^{\lfloor q/3\rfloor -1}(l,m,n)^{\odot_r 3}\\ &= N_r(l_1,m_1,n_1)^{\lfloor q/3\rfloor -1}N_r(l_2,m_2,n_2)^{\lfloor q/3\rfloor -1}\\ &\qquad (l_1,m_1,n_1)^{\odot_r 3} \odot_r (l_2,m_2,n_2)^{\odot_r 3}\\ &= \psi_1([l_1:m_1:n_1]) \odot_r \psi_1([l_2:m_2:n_2]);\end{aligned}$$

- injective: for any $[l:m:n] \in \mathbb{P}_r$, $\psi_1([l:m:n]) = (1,0,0)$ if and only if

  $$\begin{cases} N_r(l,m,n)^{\lfloor q/3\rfloor -1}(l^3+6rlmn+rm^3+r^2n^3) = 1,\\ N_r(l,m,n)^{\lfloor q/3\rfloor -1}(l^2m+rln^2+rm^2n) = 0,\\ N_r(l,m,n)^{\lfloor q/3\rfloor -1}(l^2n+lm^2+rmn^2) = 0,\end{cases}$$

  with $N_r(l,m,n) \neq 0$, so that:

  - if $m, n \neq 0$, then

    $$\begin{cases} l^2mn + rln^3 + rm^2n^2 = 0,\\ l^2mn + lm^3 + rm^2n^2 = 0\end{cases} \quad \Leftrightarrow \quad l(rn^3 - m^3) = 0.$$

    Since r is not a cube, the only solution is $l = 0$. However, this implies that $rm^2n^2 = 0$, which is satisfied only if $m = 0$ or $n = 0$. Therefore, there are no solutions such that $m, n \neq 0$;

– if $m \neq n = 0$, then from the third equation $lm^2 = 0$, i.e., $l = 0$, so that $[l : m : n] = [0 : 1 : 0]$ and the first equation becomes $r^{\lfloor q/3 \rfloor} = 1$. This is in contradiction with $r^{(q-1)/3} = \omega$ deduced from our assumption at the beginning of the subsection. Therefore, there are no solutions such that $m \neq n = 0$;
– if $n \neq m = 0$, then from the second equation $rln^2 = 0$, i.e., $l = 0$, so that $[l : m : n] = [0 : 0 : 1]$ and the first equation becomes $r^{2\lfloor q/3 \rfloor} = 1$, i.e., $r^{(q-1)/3} = \pm 1$. The case $r^{(q-1)/3} = 1$ is again in contradiction with $r^{(q-1)/3} = \omega$ obtained from the extended Euler criterion. On the other hand, $r^{(q-1)/3} = -1$ implies $r^{q-1} = -1$, which does not respect the field order. Therefore, there are no solutions such that $n \neq m = 0$;
– $m = n = 0$ implies $[l : m : n] = [1 : 0 : 0]$ which is a solution.

We have finally proved that $\ker(\psi_1) = \{[1 : 0 : 0]\}$;

- the surjectivity follows from the fact that we have an injective map between two finite groups of same cardinality $q^2 + q + 1$.

In conclusion, ψ_1 is a group isomorphism. □

The group isomorphism ψ_1 allows to find all the solutions of the cubic Pell equation over $\mathbb{F}_q$. Indeed, it is sufficient to evaluate ψ_1 over all the elements of $\mathbb{P}_r = \{[l : m : 1], [l : 1 : 0], [1 : 0 : 0] \,|\, l, m \in \mathbb{F}\}$, as obtained in Eq. (3.1). However, since the explicit inverse is missing, it is difficult to describe each point of the Pell cubic as a point of the projectivization.

Example 4.1. Let us consider $q = 7$ and $r = 2$, which is not a cube in $\mathbb{F}_7$. Thanks to the previous results we know that the cubic Pell equation

$$x^3 + 2y^3 + 4z^3 - 6xyz \equiv 1 \pmod 7,$$

admits $q^2 + q + 1 = 57$ solutions and we are able to find all of them evaluating

$$\begin{gathered}\psi_1([l : m : 1]), \quad \forall\, l, m \in \mathbb{F}_7, \\ \psi_1([l : 1 : 0]), \quad \forall\, l \in \mathbb{F}_7, \\ \psi_1([1 : 0 : 0]) = (1, 0, 0).\end{gathered}$$

For instance, for finding a random solution of the cubic Pell equation, we can take two random elements $l, m \in \mathbb{F}_7$, e.g., $l = 3$ and $m = 5$ and evaluate

$$\psi_1([3 : 5 : 1]) = (5, 4, 4).$$

One can check that

$$5^3 + 2 \cdot 4^3 + 4 \cdot 4^3 - 6 \cdot 5 \cdot 4 \cdot 4 \equiv 1 \pmod 7.$$

Similarly, we can take $l = 4$ and $[4 : 1 : 0] \in \mathbb{P}_2$, so that

$$\psi_1([4 : 1 : 0]) = (2, 4, 1),$$

is another solution of the cubic Pell equation.

Note that this method for finding all the solutions of the cubic Pell equation has complexity $O(q^2)$, so that it is not efficient for large values of q, even if it is surely better than an exhaustive search that has complexity $O(q^3)$.

However, for large values of q, it is really interesting to use the above method for generating random solutions of the cubic Pell equation since, exploiting ψ_1 as in the previous example, we are always able to generate different solutions.

4.2 r cube with three roots in $\mathbb{F}_q$

If $q \equiv 1 \pmod 3$, given ω primitive cubic root of unity, then $\{1, \omega, \omega^2\} \subset \mathbb{F}_q$. In addition, if r is a cube and $s \in \mathbb{F}_q^\times$ is a fixed cubic root of r, then the other two cubic roots are $\omega s, \omega^2 s$ and $\{s, \omega s, \omega^2 s\} \subseteq \mathbb{F}_q^\times$.

In this case, we characterize the structure of the Pell cubic through the following theorem, obtained by generalizing the second result in Theorem 2.1.

Theorem 4.3. If $q \equiv 1 \pmod 3$ and $r \in \mathbb{F}_q^\times$ is a cube, then $(\mathcal{C}_r, \odot_r)$ is isomorphic to $\mathbb{F}_q^\times \times \mathbb{F}_q^\times$ through

$$\begin{gathered}
\big(\mathcal{C}_r, \odot_r\big) \ \cong \ \mathbb{F}_q^\times \times \mathbb{F}_q^\times \\
(x, y, z) \longmapsto (x + \omega s y + \omega^2 s^2 z, x + \omega^2 s y + \omega s^2 z), \\
\left(\frac{1 + uv^2 + u^2 v}{3uv}, \frac{1 + \omega u v^2 + \omega^2 u^2 v}{3suv}, \frac{1 + \omega^2 u v^2 + \omega u^2 v}{3s^2 uv}, \right) \longleftarrow (u, v).
\end{gathered}$$

Proof. Fix a cubic root $s \in \mathbb{F}_q^\times$ of r, the norm of a point $(x, y, z) \in \mathcal{C}_r$ can be written as

$$\begin{aligned}
1 &= x^3 - 3rxyz + ry^3 + r^2 z^3 \\
&= (x + \omega s y + \omega^2 s^2 z)(x + \omega^2 s y + \omega s^2 z)(x + sy + s^2 z) = uvw,
\end{aligned}$$

so that

$$x = \frac{w + v + u}{3}, \quad y = \frac{w + \omega v + \omega^2 u}{3s}, \quad z = \frac{w + \omega^2 v + \omega u}{3s^2},$$

is a bijective correspondence between the points $(x, y, z) \in \mathcal{C}_r$ and $(u, v, w) \in \mathbb{F}_q^3$ such that $uvw = 1$. The equation $uvw = 1$ has exactly $(q-1)^2$ solutions in $\mathbb{F}_q^3$ and, in particular, a unique solution for each $(u, v) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times$. Thus, the map in the statement is bijective and also a group homomorphism. $\square$

When considering the projectivization, $\#\mathbb{P}_r = q^2 + q + 1 - 3q = (q-1)^2$ from Eq. (3.3). This is the same size of the Pell cubic, and we actually find an explicit group isomorphism through the combination of the previous theorem with the following result, that is obtained as a generalization of Theorem 2.3.

Theorem 4.4. If $q \equiv 1 \pmod 3$ and $r \in \mathbb{F}_q^\times$ is a cube, then $(\mathbb{P}_r, \odot_r)$ is isomorphic to $\mathbb{F}_q^\times \times \mathbb{F}_q^\times$ through

$$\begin{aligned}
\big(\mathbb{P}_r, \odot_r\big) \ &\cong \ \mathbb{F}_q^\times \times \mathbb{F}_q^\times, \\
[l : m : n] &\mapsto \left(\frac{l + \omega s m + \omega^2 s^2 n}{l + sm + s^2 n}, \frac{l + \omega^2 s m + \omega s^2 n}{l + sm + s^2 n}\right),
\end{aligned}$$

$$[s^2(1+v+u) : s(1+\omega v+\omega^2 u) : 1+\omega^2 v+\omega u] \leftarrow (u, v).$$

Proof. Fix s cubic root of r in $\mathbb{F}_q$, $t^3 - r$ is reducible over $\mathbb{F}_q$ as

$$t^3 - r = (t - s)(t - \omega s)(t - \omega^2 s),$$

so that, using the Chinese remainder theorem, there is the ring isomorphism

$$\begin{aligned} \mathcal{R}_r = \mathbb{F}_q[t]/\langle t^3 - r\rangle &\xrightarrow{\sim} \mathbb{F}_q[t]/\langle t - s\rangle \times \mathbb{F}_q[t]/\langle t - \omega s\rangle \times \mathbb{F}_q[t]/\langle t - \omega^2 s\rangle, \\ x + yt + zt^2 &\longmapsto (x + sy + s^2 z, x + \omega sy + \omega^2 s^2 z, x + \omega^2 sy + \omega s^2 z). \end{aligned}$$

In addition, $\mathbb{F}_q[t]/\langle t-s\rangle \cong \mathbb{F}_q[t]/\langle t-\omega s\rangle \cong \mathbb{F}_q[t]/\langle t-\omega^2 s\rangle \cong \mathbb{F}_q$. When passing to the quotients, we obtain that

$$\left(\mathbb{P}_r, \odot_r\right) = \mathcal{R}_r^{\odot_r}/\mathbb{F}_q^\times \cong (\mathbb{F}_q^\times \times \mathbb{F}_q^\times \times \mathbb{F}_q^\times)/\mathbb{F}_q^\times \cong \mathbb{F}_q^\times \times \mathbb{F}_q^\times,$$

through the map in the statement. □

Combining the obtained results gives the explicit group isomorphism

$$\begin{aligned} \psi_2 : \left(\mathbb{P}_r, \odot_r\right) &\xrightarrow{\sim} \left(\mathcal{C}_r, \odot_r\right), \\ [l : m : n] &\mapsto \Bigg(\frac{l^3 + 2s^2 l(m^2 + smn + s^2 n^2) + s^4 mn(m + sn)}{N_r(l, m, n)}, \\ &\qquad \frac{s^2 m^3 + 2m(l^2 + s^2 ln + s^4 n^2) + sln(l + s^2 n)}{N_r(l, m, n)}, \\ &\qquad \frac{s^5 n^3 + 2sn(l^2 + slm + s^2 m^2) + lm(l + sm)}{sN_r(l, m, n)} \Bigg), \end{aligned}$$

where the sum of the numerators is $(l + sm + s^2 n)^3$. The inverse is given by

$$\begin{aligned} \psi_2^{-1} : \left(\mathcal{C}_r, \odot_r\right) &\xrightarrow{\sim} \left(\mathbb{P}_r, \odot_r\right), \\ (x, y, z) &\mapsto \left[s^2(1+2x-sy-s^2 z) : s(1-x+2sy-s^2 z) : 1-x-sy+2s^2 z\right]. \end{aligned}$$

The group isomorphism ψ_2 allows to find all the solutions of the cubic Pell equation: it is sufficient to evaluate ψ_2 over all the elements of $\mathbb{P}_r$ described explicitly in Eq. (3.3). In addition, differently from the previous case, the explicit inverse of the group isomorphism can be used to describe each point of the Pell cubic with two thirds of the size with respect to the classical notation for the points in $\mathbb{F}_q^3$.

Example 4.2. Let us consider $q = 13$ and $r = 5$, which is the cube of $\{7, 8, 11\}$ in $\mathbb{F}_{13}$. Thanks to the previous results we know that the cubic Pell equation

$$x^3 + 5y^3 - z^3 - 2xyz \equiv 1 \pmod{13},$$

admits $(q - 1)^2 = 144$ solutions and we are able to find all of them evaluating

$$\begin{gathered} \psi_2([l : m : 1]), \quad \forall\, m \in \mathbb{F}_{13},\, l \in \mathbb{F}_{13} \smallsetminus \{-7m + 3, -8m + 1, -11m + 9\}, \\ \psi_2([l : 1 : 0]), \quad \forall\, l \in \mathbb{F}_{13} \smallsetminus \{-7, -8, -11\}, \\ \psi_2([1 : 0 : 0]) = (1, 0, 0). \end{gathered}$$

For instance, for finding a random solution of the cubic Pell equation, we can take a random $m \in \mathbb{F}_{13}$, e.g., $m = 3$, and another element $l \in \mathbb{F}_{13} \smallsetminus \{8, 3, 2\}$, e.g., $l = 9$, and evaluate

$$\psi_2([9 : 3 : 1]) = (3, 4, 3).$$

One can check that

$$3^3 + 5 \cdot 4^3 - 3^3 - 2 \cdot 3 \cdot 4 \cdot 3 \equiv 1 \pmod{13}.$$

Similarly, we can take $l = 4 \notin \{6, 5, 2\}$ and $[4 : 1 : 0] \in \mathbb{P}_5$, so that

$$\psi_1([4 : 1 : 0]) = (10, 4, 9),$$

is another solution of the cubic Pell equation.

4.3 r cube with one root in $\mathbb{F}_q$

If $q \not\equiv 1 \pmod 3$, then $\mathbb{F}_q$ does not contain any non–trivial cubic root of unity. In addition, each $r \in \mathbb{F}_q^\times$ is a cube and has only one cubic root s in $\mathbb{F}_q$.

Differently from the previous cases, here we can characterize the structure of $(\mathcal{C}_r, \odot_r)$ only by using the projectivization. In particular, Eq. (3.4) holds and

$$\#\mathbb{P}_r = q^2 + q + 1 - (q + 2) = q^2 - 1,$$

unless there is a $m \in \mathbb{F}_q$ such that $[-(m + s)s : m : 1] = [s^2 : s : 1] \Leftrightarrow 3s^2 = 0$, which is satisfied only when $q = 3^k$, in which case $\#\mathbb{P}_r = q^2$. In the first case, we have the following result, obtained by generalizing Theorem 2.3.

Theorem 4.5. If $q \equiv 2 \pmod 3$ and $r \in \mathbb{F}_q^\times$, then there is the group isomorphism

$$\begin{aligned} \left(\mathbb{P}_r, \odot_r\right) \;&\cong\; \mathbb{F}_{q^2}^\times, \\ [l : m : n] = \{\lambda[l + mt + nt^2] \mid \lambda \neq 0\} &\longmapsto \left(\frac{l - s^2 n}{l + sm + s^2 n}, \frac{m - sn}{l + sm + s^2 n} \right), \\ [s^2(1-sv+2u) : s(1+2sv-u) : 1-sv-u] &\longleftarrow (u, v). \end{aligned}$$

Therefore, $(\mathbb{P}_r, \odot_r)$ is a cyclic group of order $q^2 - 1$.

Proof. Given s cubic root of r in $\mathbb{F}_q$, $t^3 - r$ is reducible over $\mathbb{F}_q$ as

$$t^3 - r = (t - s)(t^2 + st + s^2),$$

so that, using the Chinese remainder theorem, there is the ring isomorphism

$$\begin{aligned} \mathcal{R}_r = \mathbb{F}_q[t]/\langle t^3 - r\rangle &\xrightarrow{\sim} \mathbb{F}_q[t]/\langle t - s\rangle \times \mathbb{F}_q[t]/\langle t^2 + st + s^2\rangle, \\ x + yt + zt^2 &\longmapsto \big(x + sy + s^2 z, x - s^2 z + (y - sz)t\big). \end{aligned}$$

In addition, $\mathbb{F}_q[t]/\langle t - s\rangle \cong \mathbb{F}_q$ and $\mathbb{F}_q[t]/\langle t^2 + st + s^2\rangle \cong \mathbb{F}_{q^2}$. When passing to the quotients, we obtain that

$$\left(\mathbb{P}_r, \odot_r\right) = \mathcal{R}_r^{\odot_r}/\mathbb{F}_q^\times \;\cong\; (\mathbb{F}_q^\times \times \mathbb{F}_{q^2}^\times)/\mathbb{F}_q^\times \cong \mathbb{F}_{q^2}^\times,$$

through the map in the statement. This confirms that $(\mathbb{P}_r, \odot_r)$ is a cyclic group of order $q^2 - 1$. □

We prove that the Pell cubic has the same structure of the projectivization through the following result.

Theorem 4.6. If $q \equiv 2 \pmod 3$ and $r \in \mathbb{F}_q^\times$, then the following map is a group isomorphism

$$\begin{aligned} \psi_3 : \big(\mathbb{P}_r, \odot_r\big) &\xrightarrow{\sim} \big(\mathcal{C}_r, \odot_r\big), \\ [l : m : n] &\longmapsto N_r(l, m, n)^{\lfloor q/3 \rfloor}(l, m, n) \end{aligned}$$

and its inverse is

$$\begin{aligned} \psi_3^{-1} : \big(\mathcal{C}_r, \odot_r\big) &\xrightarrow{\sim} \big(\mathbb{P}_r, \odot_r\big), \\ (1, 0, 0) &\longmapsto [1 : 0 : 0], \\ (x, y, 0) &\longmapsto [x/y : 1 : 0], \\ (x, y, z) &\longmapsto [x/z : y/z : 1]. \end{aligned}$$

Proof. In order for ψ_3 to be a group isomorphism, it must be:

- well defined: if $[l : m : n] = [l' : m' : n'] \in \mathbb{P}_r$, then there is $\lambda \in \mathbb{F}^\times$ such that $[l' : m' : n'] = [\lambda l : \lambda m : \lambda n]$, and since $\lfloor q/3 \rfloor = (q-2)/3$

$$\begin{aligned} N_r(\lambda l, \lambda m, \lambda n)^{\frac{q-2}{3}}(\lambda l, \lambda m, \lambda n) &= \big(\lambda^3 N_r(l, m, n)\big)^{\frac{q-2}{3}} \lambda(l, m, n) \\ &= \lambda^{q-1} N_r(l, m, n)^{\frac{q-2}{3}}(l, m, n), \end{aligned}$$

  therefore ψ_3 is well defined. In addition, $\psi_3\big(\mathbb{P}_r\big) \subseteq \mathcal{C}_r$ because

$$\begin{aligned} N_r\big(\psi_3([l : m : n])\big) &= N_r(l, m, n)^{q-2} N_r(l, m, n) \\ &= N_r(l, m, n)^{q-1} = 1; \end{aligned}$$

- a group homomorphism: given $[l_1 : m_1 : n_1], [l_2 : m_2 : n_2] \in \mathbb{P}_r$, by denoting $[l : m : n] = [l_1 : m_1 : n_1] \odot_r [l_2 : m_2 : n_2]$, we have

$$\begin{aligned} \psi_3([l : m : n]) &= N_r(l, m, n)^{\lfloor q/3 \rfloor}(l, m, n) \\ &= N_r(l_1, m_1, n_1)^{\lfloor q/3 \rfloor} N_r(l_2, m_2, n_2)^{\lfloor q/3 \rfloor} \\ &\quad\ (l_1, m_1, n_1) \odot_r (l_2, m_2, n_2) \\ &= \psi_3([l_1 : m_1 : n_1]) \odot_r \psi_3([l_2 : m_2 : n_2]); \end{aligned}$$

- injective: for any $[l : m : n] \in \mathbb{P}_r$, $N_r(l, m, n) \neq 0$ and

$$\begin{aligned} \psi_3([l : m : n]) = (1, 0, 0) &\Leftrightarrow \begin{cases} N_r(l, m, n)^{\lfloor q/3 \rfloor} l = 1, \\ N_r(l, m, n)^{\lfloor q/3 \rfloor} m = 0, \\ N_r(l, m, n)^{\lfloor q/3 \rfloor} n = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} (l^3)^{(q-2)/3} l = 1, \\ m = 0, \\ n = 0, \end{cases} \\ &\Leftrightarrow [l : m : n] = [1 : 0 : 0]; \end{aligned}$$

- surjective: we observe that an entry of $\psi_3([l : m : n])$ is zero if and only if the corresponding entry of $[l : m : n]$ is null. Thus, given a point $(x, y, z) \in \mathcal{C}_r$, have three cases:

– if $y = z = 0$, then from the equation of the Pell cubic we have $x^3 = 1$, that admits only the solution $x = 1$. Therefore $(1, 0, 0)$ is the only point of $\mathcal{C}_r$ with $y = z = 0$, and it can be obtained through ψ_3 only from the identity $[1 : 0 : 0]$ of $\mathbb{P}_r$;
– if $z = 0$ but $y \neq 0$, then the preimage of $(x, y, 0)$ must have canonical representative $[l : 1 : 0]$ with

$$\begin{cases} x = (l^3 + r)^{\lfloor q/3 \rfloor} l, \\ y = (l^3 + r)^{\lfloor q/3 \rfloor} \end{cases} \Rightarrow l = \frac{x}{y};$$

– if $z \neq 0$, then the preimage of (x, y, z) must have canonical representative $[l : m : 1]$ with

$$\begin{cases} x = N_r(l, m, 1)^{\lfloor q/3 \rfloor} l, \\ y = N_r(l, m, 1)^{\lfloor q/3 \rfloor} m, \\ z = N_r(l, m, 1)^{\lfloor q/3 \rfloor} \end{cases} \Rightarrow \begin{cases} l = x/z, \\ m = y/z. \end{cases}$$

In conclusion, ψ_3 is a group isomorphism with the wanted inverse. □

For sake of completeness, when $q = p^k$ with $p = 3$, with an analogous proof, we obtain the group isomorphism

$$\begin{aligned} \psi_3' : \left(\mathbb{P}_r, \odot_r\right) &\xrightarrow{\sim} \left(\mathcal{C}_r, \odot_r\right), \\ [l : m : n] &\longmapsto N_r(l, m, n)^{q/3-1} (l, m, n)^{\odot_r 2}. \end{aligned}$$

Thanks to the group isomorphism ψ_3, the properties of $\left(\mathbb{P}_r, \odot_r\right)$ are inherited by $\left(\mathcal{C}_r, \odot_r\right)$, i.e, it is cyclic with $q^2 - 1$ elements. In addition, it allows to find all the solutions of the cubic Pell equation by simply evaluating ψ_3 over all the elements of $\mathbb{P}_r$, which are described explicitly in Eq. (3.4). As in the previous case, the explicit inverse can be used to describe each point of the Pell cubic with two thirds of the size of points in $\mathbb{F}_q^3$.

Example 4.3. Let us consider $q = 11$ and $r = 9$, which is the cube of 4 in $\mathbb{F}_{11}$. Thanks to the previous results we know that the cubic Pell equation

$$x^3 + 9y^3 + 4z^3 + 6xyz \equiv 1 \pmod{11},$$

admits $q^2 - 1 = 120$ solutions and we are able to find all of them evaluating

$$\begin{gathered} \psi_3([l : m : 1]), \quad \forall\, m \in \mathbb{F}_{11},\, l \in \mathbb{F}_{11} \smallsetminus \{-4m + 5\},\, (l, m) \neq (5, 4), \\ \psi_3([l : 1 : 0]), \quad \forall\, l \in \mathbb{F}_{11} \smallsetminus \{-4\}, \\ \psi_3([1 : 0 : 0]) = (1, 0, 0). \end{gathered}$$

For instance, for finding a random solution of the cubic Pell equation, we can take a random $m \in \mathbb{F}_{11}$, e.g., $m = 2$, and another element $l \in \mathbb{F}_{11} \smallsetminus \{8\}$, e.g., $l = 7$, and evaluate

$$\psi_3([7 : 2 : 1]) = (9, 1, 6).$$

One can check that $9^3 + 9 \cdot 1^3 + 4 \cdot 6^3 + 6 \cdot 9 \cdot 1 \cdot 6 \equiv 1 \pmod{11}$.

Similarly, we can take $l = 3 \neq 7$ and $[3 : 1 : 0] \in \mathbb{P}_9$, so that

$$\psi_1([3 : 1 : 0]) = (4, 5, 0),$$

is another solution of the cubic Pell equation.

References

[1] A. Aabrandt and V. L. Hansen. A Note on Powers in Finite Fields. *International Journal of Mathematical Education in Science and Technology*, 47(6):987–991, 2016.

[2] C. Ballot. Strong arithmetic properties of the integral solutions of $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$, where $D = M^3 \pm 1$, $M \in \mathbb{Z}^*$. *Acta Arithmetica*, 89:259–277, 1999.

[3] E. J. Barbeau. *Pell equation, Chapter 7: The Cubic Analogue of Pell Equation.* Springer, New York, 2003.

[4] S. Barbero, U. Cerruti, and N. Murru. Solving the Pell equation via Rédei rational functions. *Fibonacci Quarterly*, 48:348–357, 2010.

[5] E. Bellini, N. Murru, A. J. Di Scala, and M. Elia. Group law on affine conics and applications to cryptography. *Applied Mathematics and Computation*, 409, 2021.

[6] L. Bernstein. Fundamental units from the preperiod of a generalized Jacobi-Perron algorithm. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1974(268–269):391–409, 1974.

[7] L. Bernstein. Units and periodic Jacobi-Perron algorithms in real algebraic number fields of degree 3. *Transactions of the American Mathematical Society*, 212, 1975.

[8] J. Bourgain. A Remark on Solutions of the Pell Equation. *International Mathematics Research Notices*, 2015(10):2841–2855, 2015.

[9] M. Cipu. Explicit formula for the solution of simultaneous Pell equations $x^2 - (a^2-1)y^2 = 1$, $y^2 - bz^2 = v_1^2$. *Proceedings of the American Mathematical Society*, 146(3):983–992, 2018.

[10] B. Cohen. Chebyshev polynomials and Pell equations over finite fields. *Czechoslovak Mathematical Journal*, 71:491–510, 2021.

[11] P. H. Daus. Normal ternary continued fraction expansions for cubic irrationalities. *American Journal of Mathematics*, 51(1):67–98, 1929.

[12] E. Fouvry. On the size of the fundamental solution of the Pell equation. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2016(717):1–33, 2016.

[13] R. Fu and H. Yang. On the solvability of the simultaneous Pell equations $x^2 - ay^2 = 1$ and $y^2 - bz^2 = v_1^2$. *International Journal of Number Theory*, 17(9):1997–2008, 2021.

[14] S. A. Hambleton and H. C. Williams. *Cubic fields with geometry, Chapter 5: Cubic Pell Equation.* CMS Books in Mathematics. Springer Nature, New York, 2019.

[15] B. He, A. Pinter, and A. Togbé. On simultaneous Pell equations and related Thue equations. *Proceedings of the American Mathematical Society*, 143(11):4685–4693, 2015.

[16] C. G. J. Jacobi. *Gesammelte Werke*, volume VI. Reimer, Berlin, 1891.

[17] M. J. Jacobson and H. C. Williams. *Solving the Pell Equation.* CMS Books in Mathematics. Springer, New York, 2009.

[18] G. B. Mathews. On the arithmetic theory of the form $x^3 + ny^3 + n^2z^3 - 3nxyz$. *Proceedings of the London Mathematical Society*, S1-21(1):280–287, 1889.

[19] A. J. Menezes and S. A. Vanstone. A note on cyclic groups, finite fields, and the discrete logarithm problem. *Applicable Algebra in Engineering, Communication and Computing*, 3:67–74, 1992.

[20] A. Teckan. The number of solutions of Pell equations $x^2 - ky^2 = N$ and $x^2 + xy - ky^2 = N$ over $\mathbb{F}_p$. *Ars Combinatorica*, 102:225–236, 2011.

[21] A. Tekcan, A. Ozkoc, C. Kocapinar, and H. Alkan. The Pell equation $x^2 - Py^2 = Q$. *International Journal of Physical and Mathematical Sciences*, 4(7):795–798, 2010.

[22] C. L. E. Wolfe. On the indeterminate cubic equation $x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1$. *University of California Publications in Mathematics*, 1(16):359–369, 1923.

[23] P. Xi. Counting fundamental solutions to the Pell equation with prescribed size. *Compositio Mathematica*, 154:2379–2402, 2018.