What the Pell: Cryptanalysis of Degree-Two Pell Curves

Leonardo Errati[*]

Politecnico di Torino,
Corso Duca degli Abruzzi 24, Torino, 10129, Italy
leonardo.errati@polito.it

Abstract

Pell curves recently gained some degree of attention as algebraic groups for cryptographic security assumptions. We focus on Pell curves of degree two and prove they inherently expose overwhelming information on their group structure.
This ultimately nullifies any security and computational advantage over classical finite fields, and in particular the base field of the curve itself.

1 Introduction

The Pell equation $\mathcal{P}_d : x^2 - dy^2 = 1$ is a special case of Diophantine equation. This concept, better known for its number-theoretical applications, probably predates Alexander the Great. The $\mathbb{F}_q$-variety $\mathcal{P}_d(\mathbb{F}_q)$, adjoined to the Brahmagupta product $\otimes_d$, defines an algebraic group which gained some interest as an application for DLOG-like [2, 8] and RSA-like [17, 4] security assumptions. The general claim is that $(\mathcal{P}_d(\mathbb{F}_q), \otimes_d)$, much alike elliptic curves, provides an increased security level.

Menezes and Vanstone [15] first provided an analysis of their group structure via an isomorphism from $\mathcal{P}_d(\mathbb{F}_q)$ to a multiplicative subgroup of either $\mathbb{F}_q$ or $\mathbb{F}_q^2$, the exact extension depending on the quadratic character of the parameter d. Due to this isomorphism, they discouraged the use of degree-two Pell curves for security assumptions.
We base on their findings to adapt classical security problems to degree-two Pell curves: DLOG, RSA Inversion (RSAI), and Endomorphism Ring (EndRing). We then provide efficient, explicit forwards and backwards reductions. The reductions of DLOG and RSAI these reductions operate in at most probabilistic polynomial time (PPT), therefore they are equivalent to their finite field counterparts. As for EndRing, we prove its instantiation on such curves is trivial.
Further, we give the results of an asymptotic and empirical analysis of the efficiency of the degree-two Brahmagupta product $\otimes_d$ for varying field size q and parameter d. We discuss the impossibility of this operation to be faster than that on the isomorphic image of the curve.

Our results prove that degree-two Pell curves ultimately offer negligible security advantages over the finite fields on which they are defined, while also requiring operations that are not efficient enough to justify their adoption in cryptography. Constructively, this shows that protocols based on Pell curves can be further improved by adopting field arithmetic.
We conclude with a conjecture on the classification of degree-n Pell curves and its consequences on their cryptographic applications.

[*] L. Errati is a member of INDAM-GNSAGA and CrypTo, the research group of Cryptography and Number Theory of Politecnico di Torino.

2 Pell Curves of Degree Two

Unless otherwise specified, mentions of *Pell curves* in our work always refer to degree-two Pell curves. We cover degree-n Pell curves in Section A.

2.1 Structure

Definition 1. *For a fixed non-zero element d of the field $\mathbb{F}_q$, the* degree-two Pell curve over $\mathbb{F}_q$ of parameter d *is the $\mathbb{F}_q$-variety*

$$\mathcal{P}_d(\mathbb{F}_q) = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \,:\, x^2 - dy^2 = 1\right\}$$

We can define the operator $\otimes_d : \mathcal{P}_d(\mathbb{F}_q) \times \mathcal{P}_d(\mathbb{F}_q) \to \mathcal{P}_d(\mathbb{F}_q)$ over it, parametrised by the same d. This is named *Brahmagupta product* after its first known appearance in the work of the 7-th century mathematician Brahmagupta [5]. Given two points $\mathcal{A} = (x_\mathcal{A}, y_\mathcal{A})$ and $\mathcal{B} = (x_\mathcal{B}, y_\mathcal{B})$ lying in $\mathcal{P}_d(\mathbb{F}_q)$, their product $\mathcal{A} \otimes_d \mathcal{B}$ is

$$(x_\mathcal{A}, y_\mathcal{A}) \otimes_d (x_\mathcal{B}, y_\mathcal{B}) = (x_\mathcal{A} x_\mathcal{B} + d y_\mathcal{A} y_\mathcal{B}, x_\mathcal{A} y_\mathcal{B} + x_\mathcal{B} y_\mathcal{A}) \qquad (1)$$

This operation induces an abelian group structure $(\mathcal{P}_d(\mathbb{F}_q), \otimes_d)$ on the variety, which Menezes and Vanstone [15, Lemma 4] prove to be isomorphic to a cyclic group. The exact image of the isomorphism depends on the quadratic character of d, which is defined as

$$\chi(d) = \begin{cases} 0 & \text{if } d = 0 \\ +1 & \text{if } d \text{ is a quadratic residue} \\ -1 & \text{if } d \text{ is a quadratic non-residue} \end{cases}$$

Lemma 2 (Structure Lemma [15])**.** *Let U_{q+1} denote the unique subgroup of $(\mathbb{F}_{q^2}^*, \cdot)$ of order $q + 1$. Then $(\mathcal{P}_d(\mathbb{F}_q), \otimes_d)$ is isomorphic to a cyclic group of order $q - \chi(d)$, or more explicitly*

$$(\mathcal{P}_d(\mathbb{F}_q), \otimes_d) \simeq \begin{cases} (\mathbb{F}_q^*, \cdot) & \textit{if } \chi(d) = +1 \\ (U_{q+1}, \cdot) & \textit{if } \chi(d) = -1 \end{cases}$$

Since $\mathcal{P}_d(\mathbb{F}_q)$ is an algebraic variety, we adopt an additive notation and denote its elements with calligraphic letters. Menezes and Vanstone clearly remark on how this should discourage the use of Pell curves of any parameter d in any and all variations of the Discrete Logarithm Problem. This will be covered in Section 3.

2.2 Alternative Construction

We will make use of an equivalent construction for Pell curves. More details can be found for example in the book by Clark [6, Chapter 7] and the article by Lenstra [14].
Consider the polynomial ring $\mathcal{R}_d = \mathbb{F}_q[W]/\langle W^2 - d\rangle$. Its ring automorphisms with respect to $\mathbb{F}_q$ are uniquely defined by the image of W; they are the identity $(W \mapsto W)$ and conjugation $(W \mapsto -W)$ automorphisms. The norm N_d of an element $f = x + yW \in \mathcal{R}_d$ is then

$$N_d(x + yW) = (x + yW)(x - yW) = x^2 - dy^2$$

Expressing the norm of f in terms of its conjugates $f, \overline{f}$ will be crucial for the description of explicit isomorphisms.

Lemma 3. *There is a correspondence between the algebraic variety of degree-*2 *Pell curves and the set of elements f in $\mathcal{R}_d$ of unitary norm. More explicitly,*

$$\mathcal{P}_d(\mathbb{F}_q) \simeq \mathcal{U}(\mathcal{R}_d) = \{x + yW \in \mathcal{R}_d \mid N_d(x + yW) = 1\}$$

The operation on $\mathcal{U}(\mathcal{R}_d)$ is induced by polynomial multiplication modulo $W^2 - d$, which becomes the Brahmagupta product. Consider $f_\mathcal{A} = x_\mathcal{A} + y_\mathcal{A}W$ and $f_\mathcal{B} = x_\mathcal{B} + y_\mathcal{B}W$ of unitary norm, their product is

$$\begin{aligned}(x_\mathcal{A} + y_\mathcal{A}W)(x_\mathcal{B} + y_\mathcal{B}W) &= x_\mathcal{A}x_\mathcal{B} + x_\mathcal{A}y_\mathcal{B}W + x_\mathcal{B}y_\mathcal{A}W + y_\mathcal{A}y_\mathcal{B}W^2\\ &= x_\mathcal{A}x_\mathcal{B} + dy_\mathcal{A}y_\mathcal{B} + (x_\mathcal{A}y_\mathcal{B} + x_\mathcal{B}y_\mathcal{A})W\end{aligned}$$

Under the correspondence, these are exactly the curve points $\mathcal{A} = (x_\mathcal{A}, y_\mathcal{A})$ and $\mathcal{B} = (x_\mathcal{B}, y_\mathcal{B})$, and the product is analogous to $\mathcal{A} \otimes_d \mathcal{B}$. Further, as a corollary of Dirichlet's Unit Theorem, this Subsection proves that $\mathcal{P}_d(\mathbb{F}_q)$ is a finite cyclic group. As a notable consequence, the solution (x_1, y_1) of least Euclidean norm generates the m-th solution (x_m, y_m) as $x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m$. This is called *fundamental solution.*

The construction via ideals was exploited in much of the subsequent work [4, 16, 2, 8, 9, 10]. Partly for the so-called *Pell curve parametrisation*, better detailed in Section B.
Another use is the algebraic construction of degree-three Pell curves from the group of units of $\mathbb{F}_q[W]/\langle W^3 - r\rangle$, on which we expand in Section A. Since Dutto and Murru [10] provide an analogue of the degree-two Structure Lemma (Theorem 2), our results likely adapt to degree three. If we denote by $\mathcal{Q}_r(\mathbb{F}_q)$ the degree-three Pell curve

$$\mathcal{Q}_r(\mathbb{F}_q) = \left\{(x, y, z) \in \mathbb{F}_q^3 \mid x^3 - 3rxyz + ry^3 + r^2z^3 = 1\right\}$$

and by $\odot_r$ the degree-three Brahmagupta product, then the following holds.

Lemma 4 ([10])**.** *Let U_{q^2+q+1} denote the unique subgroup of $(\mathbb{F}_{q^3}^*, \cdot)$ of order $q^2 + q + 1$. Then $(\mathcal{Q}_r(\mathbb{F}_q), \odot_r)$ is isomorphic to a cyclic group*

$$(\mathcal{Q}_r(\mathbb{F}_q), \odot_r) \simeq \begin{cases}(U_{q^2+q+1}, \cdot) & \textit{if } r \textit{ is non-cube}\\ (\mathbb{F}_q^* \times \mathbb{F}_q^*, \cdot) & \textit{if } r \textit{ is cube with three roots in } \mathbb{F}_q\\ (\mathbb{F}_{q^2}^*, \cdot) & \textit{if } r \textit{ is cube with one root in } \mathbb{F}_q\end{cases} \tag{2}$$

of orders $q^2 + q + 1$, $(q - 1)^2$, and $q^2 - 1$ respectively.

2.3 Efficient Isomorphisms

The isomorphisms from the Structure Lemma (Theorem 2) can be made explicit using the quotient construction of Section 2.2. Although the first case is trivial, we exhibit both for completeness.

Case 1: negative quadratic character. In the first case, the polynomial $W^2 - d$ is irreducible, therefore $\mathcal{R}_d$ is a field. We say that *the curve does not split.* The isomorphism, whose image is restricted to the unique subgroup of order $q + 1$ in $\mathbb{F}_{q^2}^*$, acts as

$$(x, y) \mapsto x + yW \tag{3}$$

$$x + Wy \mapsto (x, y) \tag{4}$$

Example 5. *The parameters $q = 5$ and $d = 3$ define the Pell curve*

$$\mathcal{P}_3(\mathbb{F}_5) = \{(1,0),(2,1),(2,4),(3,1),(3,4),(4,0)\}$$

of cardinality $5 - \chi(3) = 5$. Under the map of Equation (5), its algebraic group is isomorphic to the subgroup $U_6 \leq \mathbb{F}_{25}^*$ generated by $3 + W$.

Case 2: positive quadratic character. In the second case, the quotient polynomial is reducible, therefore the ring $\mathcal{R}_d$ contains a quadratic residual a such that $W^2 - d = (W - a)(W + a)$. We say that *the curve splits*, meaning that the polynomial does. The forward isomorphism acts as

$$(x, y) \mapsto x - ay \tag{5}$$

Finding its inverse is not straightforward. Some approaches are flawed: for instance, inverting some $t = x - ay$ in $\mathbb{F}_q$ via Euclidean division by $-a$ may not return the correct result, but the (x', y') of minimal Euclidean norm, not necessarily lying in $\mathcal{P}_d(\mathbb{F}_q)$.

Example 6. *The parameters $q = 5$ and $d = 4$ define the Pell curve*

$$\mathcal{P}_4(\mathbb{F}_5) = \{(0,1),(0,4),(1,0),(4,0)\}$$

of cardinality $5 - \chi(4) = 4$. Select $a = 2$ as root of d. The isomorphic image of $\mathcal{T} = (4,0)$ is $t = 4$, but Euclidean division of t by $-a$ returns $(0,3)$, which does not lie in the curve. However, this $(0,3)$ has smaller Euclidean norm than the correct $\mathcal{T}$.

We suggest a different approach.

Lemma 7. *If $\chi(d) = +1$, the evaluation of the inverse of φ in t is the curve point given by*

$$x = \frac{1+t^2}{2t} \quad \text{and} \quad y = \frac{1-t^2}{2at} \tag{6}$$

where a is one of the square roots of d.

Proof. If t in $\mathbb{F}_q^*$ lies in the image of φ, then $t = x - ay$ for some x and y such that $\mathcal{T} = (x, y)$ is a point of $\mathcal{P}_d(\mathbb{F}_q)$. Imposing this condition,

$$\begin{aligned} 1 &= N_d(t) && \text{alternative construction of } \mathcal{P}_d(\mathbb{F}_q) \\ &= (x - ay)(x + ay) && \text{definition of } N_d \end{aligned}$$

Since $x - ay = t$, this imposes $x + ay = 1/t$. Finally,

$$2x = t + \frac{1}{t} \quad \text{and} \quad 2ay = t - \frac{1}{t} \qquad \square$$

There are two different choices for the square root of d, one "positive" and one "negative". If we denote as $a_+ := a$ the one of least absolute value, the other is $a_- := -a$. They yield two different inverse isomorphisms:

$$\begin{aligned} \varphi_{a_+}^{-1} &: t \mapsto \left(\frac{1+t^2}{2t}, \frac{1-t^2}{2at}\right) =: (x, y) \\ \varphi_{a_-}^{-1} &: t \mapsto \left(\frac{1+t^2}{2t}, \frac{1-t^2}{2(-a)t}\right) = \left(\frac{1+t^2}{2t}, -\frac{1-t^2}{2at}\right) = (x, -y) \end{aligned}$$

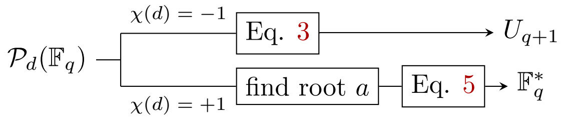

Figure 1: Isomorphism from the curve to an extension of the base field.

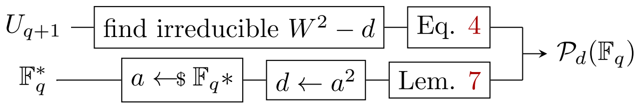
U_{q+1}
find irreducible $W^2 - d$
Eq. 4
$\mathbb{F}_q^*$
$a \leftarrow\$ \mathbb{F}_q*$
$d \leftarrow a^2$
Lem. 7
$\mathcal{P}_d(\mathbb{F}_q)$

Figure 2: Isomorphism from an extension of the base field to the curve.

We consider the first to be a canonical choice, as the composition $\varphi_{a_+}^{-1} \circ \varphi$ is the identity Id. The second returns $(x, -y)$, which lies in the same curve, but is undesirable since $\varphi_{a_-}^{-1} \circ \varphi = -\mathrm{Id}$. This is inconsequential in the efficiency of the inverse isomorphism; once a square root a_* of d is found, compute $-a_*$ and take a as the one of least representative.

Example 8. *Consider the Pell curve from Theorem 6. The two roots of $d = 4$ are the positive $a_+ = 2$ and the negative $a_- = 3$. If we pick again $\mathcal{T} = (4, 0)$, with isomorphic image $t = 4$, then the positive inverse correctly returns $\mathcal{T}$. In this case the two isomorphisms coincide.*

The overall operations described in this Section are in Figures 1 and 2.

3 Security assumptions

3.1 Discrete Logarithm problem

Problem 9 (DLOG)**.** *Consider a finite cyclic group $\mathbb{G} = \langle g \rangle$ of order n.*
Parameters: a description $(\mathbb{G}, g)$ of $\mathbb{G}$.
Instance: an element $h \in G$.
Task: find the unique $x \in \mathbb{Z}_n$ such that $g^x = h$.

We shall discuss of two different formulations. One on the multiplicative group of a field, which is either $\mathbb{F}_q^*$ or $U_{q+1} \leq \mathbb{F}_{q^2}^*$, and one on a Pell curve $\mathcal{P}_d(\mathbb{F}_q)$. They will be denoted as DLOG-$\mathbb{F}$ and DLOG-$\mathcal{P}$, respectively. The nature of said $\mathbb{F}$ will be clear from the context, and specified when necessary.

Lemma 10 (Menezes and Vanstone [15])**.** *If $\chi(d) = -1$, then DLOG-$\mathcal{P}$ is reducible in constant time to DLOG-U_{q+1}. If $\chi(d) = +1$, then DLOG-$\mathcal{P}$ is reducible in probabilistic polynomial time to DLOG-$\mathbb{F}_q^*$.*

Example 11. *Consider the Pell curve from Theorem 6,*

$$\mathcal{P}_4(\mathbb{F}_5) = \{(0, 1), (0, 4), (1, 0), (4, 0)\}$$

The generator of its algebraic group is $\mathcal{G} = (0, 1)$. Since d has positive characteristic, the group of points of $\mathcal{P}_4(\mathbb{F}_5)$ is isomorphic to the multiplicative group $\mathbb{F}_5^* = \{1, 2, 3, 4\} = \langle 3 \rangle$.
Consider an instance $\mathcal{H} = (0, 4)$ of DLOG-$\mathcal{P}$. Its isomorphic image is $h = 2$, a DLOG-$\mathbb{F}$

instance itself. Its solution $x = 3$ uniquely characterises the solution of $\mathcal{H} = (0, 4)$, since

$$\begin{aligned} h = g^x = \varphi(\mathcal{G})^x = \varphi(x\mathcal{G}) && \textit{isomorphism of Theorem 2} \\ = \varphi(\mathcal{H}) && \textit{construction of } h \end{aligned}$$

therefore $x = 3$ is also the solution for the original instance.

The probabilistic computation of $a = \sqrt{d}$ in the case $\chi(d) = +1$ is the main bottleneck. However, since we operate in $\mathbb{F}_q^*$, we know of algorithms such as Tonelli-Shanks, Cipolla, or Peralta that are quite efficient. See Adiguzel-Goktas and Ozdemir [1, Section 2] for technical details and an efficiency comparisons. Mind that we implicitly require a to be the positive root with the nomenclature of Section 2.

Theorem 12. *DLOG-$\mathcal{P}$ is PPT-equivalent to DLOG-$\mathbb{F}$.*

Proof. We already know that DLOG-$\mathcal{P}$ can be reduced in PPT to DLOG-$\mathbb{F}$.

To reduce DLOG-$\mathbb{F}$, we operate as shown in Figure 2.

(U_{q+1}) Search for a non-square d in $\mathbb{F}_q^*$, then $W^2 - d$ is irreducible and defines a non-splitting quotient $\mathcal{R}_d$. The isomorphism of Equation (4) then maps to a DLOG-$\mathcal{P}$ instance $\mathcal{H} = \varphi(h)$. This Las Vegas algorithm operates in PPT: half of the elements are non-residuals, and residuosity can be tested in worst case via Euler's criterion, with $\mathcal{O}(\log^3 q)$ operations. Once solved, the instance can be mapped back via Equation (3) in constant time.

($\mathbb{F}_q^*$) Pick an $a \in \mathbb{F}_q$ and set $d = a^2$; this constructs a splitting quotient $\mathcal{R}_d$, and the formulas in Theorem 7 map to a DLOG-$\mathcal{P}$ instance $\mathcal{H} = \varphi(h)$. Once solved it can be traced back via Equation (5), keeping the same a. These steps are far easier and clearly PPT.

Since φ is a group isomorphism, the above reductions are correct. □

3.2 RSA Inversion problem

Problem 13 (RSA Inversion)**.** *Consider a finite cyclic group $\mathbb{G} = \langle g \rangle$ of order N .*
Parameters: a description $(\mathbb{G}, g)$ of $\mathbb{G}$, an e in $\mathbb{Z}_N$ such that $\gcd(e, N) = 1$.
Instance: an element $x \in \mathbb{G}$.
Task: find the unique $y \in \mathbb{G}$ such that $y^e = x$.

With the same notation of the previous Subsection, RSAI-$\mathbb{F}$ will denote the formulation in the multiplicative group of a field, RSAI-$\mathcal{P}$ that in the algebraic group of a Pell curve.

Theorem 14. *RSA-$\mathcal{P}$ is PPT-equivalent to RSA-$\mathbb{F}$.*

Proof. This follows the same steps of the proof of Theorem 12.
An instance of RSAI-$\mathcal{P}$ for a non-splitting curve is equivalent to RSAI-U_{q+1}. An instance of RSAI-$\mathcal{P}$ for a splitting curve is equivalent to RSAI-$\mathbb{F}_q$.
These reductions are correct due to the properties of φ: instances on one side are mapped to instances on the other side, parametrised by a different group but with same e. □

Example 15. *Consider again the Pell curve from Theorem 6. Given the parameters $e = 3$ and $N = |\mathbb{G}| = 4$, the instance $\mathcal{X} = (4, 0)$ has isomorphic image $x = 4$. This is an RSA Inversion instance in $\mathbb{F}_5^*$ of same parameter e, whose solution is $y = 3$. The inverse isomorphisms correctly returns $\mathcal{Y} = (4, 0)$, which satisfies $3\mathcal{Y} = \mathcal{X}$.*

3.3 Endomorphism ring problem

We now focus on the *endomorphisms* of curves as algebraic groups.

Problem 16 (EndRing)**.** *Consider the algebraic variety of a curve $\mathcal{C}$ over a field $\mathbb{F}_q$.*
Parameters: the field size q.
Instance: a curve $\mathcal{C}$ with an algebraic group structure over $\mathbb{F}_q$.
Task: find a basis of the endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_q}(\mathcal{C})$ as a $\mathbb{Z}$-module.

Theorem 17. *Denoting the Frobenius endomorphism by π, then*

$$\mathrm{End}_{\overline{\mathbb{F}}_q}(\mathcal{P}_d(\mathbb{F}_q)) \simeq \langle 1, \pi \rangle_{\mathbb{Z}}$$

Proof. Endomorphisms of the curve are exactly those of its isomorphic image; therefore, we are left only with the field endomorphisms. □

Instantiations of EndRing with Pell curves are not suitable as security assumptions, as their only endomorphism are the field ones.

4 Efficiency Analysis

We proved computational problems on Pell curves offer no significant security gain over classical structures. However, their adoption could be justified by some computational advantage.
This Section includes a comparison of theoretical and empirical costs. Test results can be found in Section 4.

Bit-length	**Brahmagupta Product Ratio**		**Square & Multiply Ratio**
(n)	splitting $(\mathbb{F}_q)$	non-splitting $(\mathbb{F}_{q^2})$	
256	3.30431	1.00153	2.81250
1024	3.82800	0.99473	2.78440
2048	4.01572	0.99999	2.83910
4096	3.96329	1.00052	2.82560

Table 1: Results of the experiments detailed in this Section. Each entry represents the mean timing ratio of our tests.

4.1 Point Addition and Isomorphisms

Consider operations on the base field $\mathbb{F}_q$, which are addition $(T_+(\mathbb{F}_q))$ and multiplication $(T_\times(\mathbb{F}_q))$ of two field elements. In terms of these, the Brahmagupta product (Equation (1)) of two curve points requires

$$T_{\otimes_d}(\mathcal{P}) = 5T_\times(\mathbb{F}_q) + 2T_+(\mathbb{F}_q)$$

operations in the worst case. Let $n = \lceil \log_2(q) \rceil$ denote the bit-size of q, the worst case complexity of the Brahmagupta product is $\mathcal{O}(n^2) + \mathcal{O}(n) = \mathcal{O}(n^2)$. The dominating cost is that of field multiplication, which can be improved considering modern algorithms such as Karatsuba $(\mathcal{O}(n^{\log_2 3}))$ or Schonage-Strassen $(\mathcal{O}(n \cdot \log n \cdot \log\log n))$.

One could adopt the isomorphisms of Section 2.3, whose operations are detailed in Figures 1 and 2.
If d has positive character, the cost of the isomorphisms is dominated by that of finding a positive square root a of d. The backwards isomorphism is given by the same a and d.
If d has negative character, the cost is dominated by usual field operations, as the irreducible $W^2 - d$ is already given and doesn't need to be searched for.
However, this is (strictly) lower bounded by the cost of multiplication in the isomorphic image, which is either $\mathbb{F}_q^2$ or $\mathbb{F}_q$. Further optimisations would unlikely result in this being more efficient than the product on the base field.

The empirical analysis was designed as follows. Consider the bit-lengths n of the benchmarks in [2]. Pick q of length n and a random parameter d. From a theoretical standpoint the actual choice of d matters little, as curves of the same character are isomorphic. However, larger values result in a slightly heavier computation, thus we select a uniformly random d in $[1, q-1]$.
Compare the cost of the Brahmagupta product of two random curve, $\mathcal{A} \otimes_d \mathcal{B}$, to that of the multiplication of their isomorphic images, $\varphi(\mathcal{A}) \cdot \varphi(\mathcal{B})$. This was repeated 100 times on the *Caronte* cluster at DISMA, Politecnico di Torino[1]. Results can be found in Figure 3. Even if the isomorphisms were to have null cost, we would not gain a computational advantage over the isomorphic image of the curve.

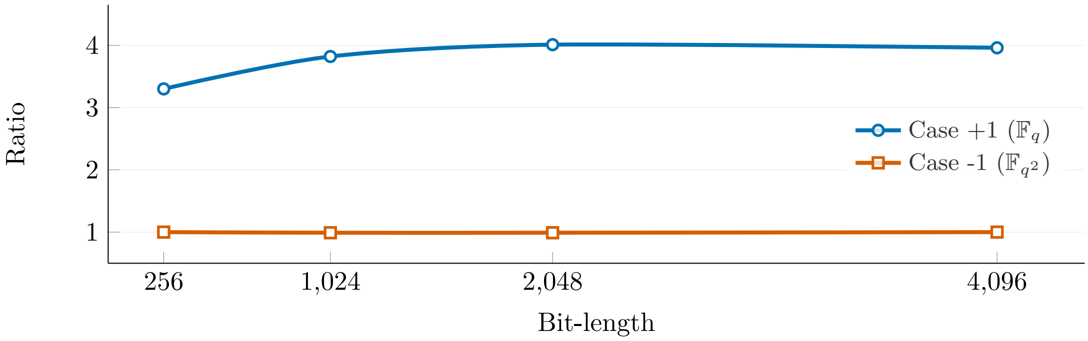

Figure 3: Empirical ratio between $T_{\otimes_d}(\mathcal{P})$ and $T_\times(\mathbb{F}_q)$ if the curve splits (blue), $T_\times(\mathbb{F}_{q^2})$ if the curve does not split (red). The cost of curve computations is comparable to the isomorphic field when the curve is non-splitting, worse when it splits.

4.2 Square and Multiply

Alecci, Dutto and Murru [2] provided a square-and-multiply variant, detailed in Figure 5 . From a cryptographic perspective, this is perhaps the most interesting algorithm.

The empirical analysis was designed as follows. Consider the bit-lengths n of the benchmarks in [2]. Pick q of length n, a random parameter d, and a k of length close to n. Compare the cost of multiplying a random point $\mathcal{A}$ by k to that of exponentiating its isomorphic image $\varphi(\mathcal{A})$ by the same k. This was repeated 100 times.
Results can be found in Figure 5.Were we to adopt the isomorphisms, their cost and the need to perform further (identical) operations would still make the curve variant far slower.

[1] OS Linux 5.14, Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz, 125Gi RAM (16 cores).

```
PellSquareMultiply($\mathcal{A} = (x_{\mathcal{A}}, y_{\mathcal{A}}), e, d, q$)
$(x, y) \leftarrow (1, 0)$
for $b$ in binary($e$) do
    $x = x^2 + dy^2 \pmod q$
    $y = 2xy \pmod q$
    if $b = 1$ do
        $x = x \cdot x_{\mathcal{A}} + d \cdot y \cdot y_{\mathcal{A}} \pmod q$
        $y = x \cdot y_{\mathcal{A}} + y \cdot x_{\mathcal{A}} \pmod q$
return $(x, y)$
```

```
FieldSquareMultiply($x, e, q$)
$r \leftarrow 1$
for $b$ in binary($e$) do
    $r = r^2 \pmod q$
    if $b = 1$ do
        $r = r \cdot x \pmod q$
return $r$
```

Figure 4: On the left, the square-and-multiply variant for the computation of $e\mathcal{A}$ on $\mathcal{P}_d(\mathbb{F}_q)$. On the right, classical square-and-multiply for the computation of x^e in $\mathbb{F}_q$.

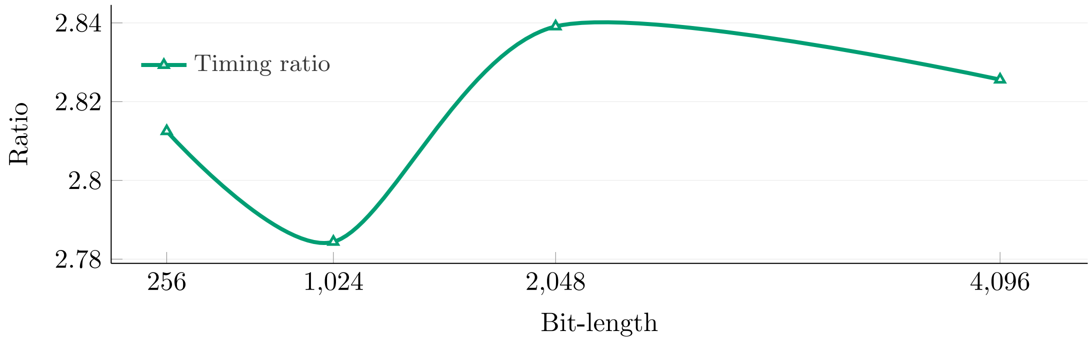

Figure 5: Empirical ratio between $T_{\mathsf{PellSquareMultiply}}$ and $T_{\mathsf{FieldSquareMultiply}}$.

5 Conclusions

We presented the Pell curve variants of famous security assumptions and studied the efficiency of their group operation. If d has positive quadratic character, DLOG and RSAI are PPT-equivalent to their counterparts in $\mathbb{F}_q^2$, with a base operation costing at least as multiplication in $\mathbb{F}_q^2$. If d has negative quadratic character, they are PPT-equivalent to their counterparts in $\mathbb{F}_q$ instead, with a base operation costing at least as multiplication in $\mathbb{F}_q$. EndRing, on the other hand, is trivial and should be ignored.
This is far from surprising: Theorem 10 already proved that Pell curves are the multiplicative group of a field in disguise.

Some protocols in published literature base their security or efficiency claims on Pell curves. Alecci, Dutto and Murru [2, 8] propose an ElGamal-like encryption scheme, whose setup algorithm samples curves of negative character. Due to Theorem 12, its security is equivalent to DLOG-$\mathbb{F}_q^2$ with an increased number of operations.
Padhye [17], and later Bellini and Murru [4], present various RSA-like schemes based on the RSA Inversion problem. Security-wise, As for efficiency, the claim is for faster decryption than standard RSA: however, the resulting message is encoded as a point in a curve, and decoding it nullifies the efficiency gain.

Degree-two Pell curves have been used to construct other primitives: time-lock puzzles [3], identity-based schemes [18], etc. This suggests that their use is overall avoidable, resulting in no security loss and increased efficiency with respect to the original Pell variant.

Degree three curves saw a further surge in interest [7, 8, 11, 13]; remarks in Section 2.3 and Section A indicate why cryptanalysis can be easily extended to degree three via the isomorphism of Theorem 4. Constructively, a direct translation on the base field would result in an efficiency gain. An example is the Pell Curve primality testing algorithm by Di Domenico and Murru [7], which would greatly benefit from this perspective.

What we discussed above likely holds for some cases of degree-n Pell curves. We are left with the following questions, which to the best of our knowledge remain open:

1. Consider generalised degree-2 Pell curves, defined as $\mathcal{P}_{d,k}(\mathbb{F}_q) : x^2 - dy^2 = k$. Is their algebraic variety isomorphic to a multiplicative subgroup of a field extension of $\mathbb{F}_q$?

2. Consider the definition of degree-n Pell curves in Section A. Is their algebraic variety isomorphic to a multiplicative subgroup of $\mathbb{F}^*_{q^n}$? We conjecture the answer to be as follows.

   Conjecture 18 (Pell curve classification conjecture)**.** *Consider the degree-n Pell curve over $\mathbb{F}_q$ of scale parameter d. If cyclic, its algebraic group is isomorphic to a subgroup of $(\mathbb{F}^*_{q^n}, \cdot)$. The exact subgroup is dictated by the properties of d.*

   However, this leaves a third open problem. See Section A for more details on acyclicity.

3. Consider the definition of degree-n Pell curves in Section A. In which cases is their algebraic group not cyclic?

References

[1] Ebru Adiguzel-Goktas and Enver Ozdemir. Square root computation in finite fields. *Designs, Codes and Cryptography*, 92(7):1947–1959, 2024.

[2] Gessica Alecci, Simone Dutto, and Nadir Murru. Pell hyperbolas in dlp–based cryptosystems. *Finite Fields and Their Applications*, 84:102112, 2022.

[3] Fadi Barbara, Enrico Guglielmino, Nadir Murru, and Claudio Schifanella. Btle: Atomic swaps with time-lock puzzles. *Journal of Mathematical Cryptology*, 19(1):20240044, 2025.

[4] Emanuele Bellini and Nadir Murru. An efficient and secure rsa-like cryptosystem exploiting rédei rational functions over conics. *Finite fields and their applications*, 39:179–194, 2016.

[5] Brahmagupta. *Brāhma-sphuṭa-siddhānta*. Government of Bengal, 628. English translation published in 1817 by Henry Thomas Colebrooke. Original Sanskrit verse, no symbolic notation.

[6] Pete L Clark. *Number theory: A contemporary introduction*. Dep. of Mathematics, University of Georgia, 2012.

[7] Luca Di Domenico and Nadir Murru. Novel performant primality test on a pell's cubic. *Mediterranean Journal of Mathematics*, 22(3):72, 2025.

[8] Simone Dutto. *Pell equation, Theory and applications to cryptography*. PhD thesis, 2022.

[9] Simone Dutto. Dlp-based cryptosystems with pell cubics. *Banach Center Publications*, 126:123–136, 2023.

[10] Simone Dutto and Nadir Murru. On the cubic pell equation over finite fields. *Quaestiones Mathematicae*, 46(10):2109–2128, 2023.

[11] Simone Dutto and Nadir Murru. On the cubic pell equation over finite fields. *Quaestiones Mathematicae*, 46(10):2109–2128, 2023.

[12] Simone Dutto and Nadir Murru. On the cubic pell equation over finite fields. *Quaestiones Mathematicae*, 46(10):2109–2128, 2023.

[13] R Elumalai and GSGN Anjaneyulu. An efficient practical alternative to ecc by pell curve cryptography with a new vision. *Cryptologia*, pages 1–41, 2024.

[14] Hendrik W Lenstra Jr. Solving the pell equation. *Notices of the AMS*, 49(2):182–192, 2002.

[15] Alfred J Menezes and Scott A Vanstone. A note on cyclic groups, finite fields, and the discrete logarithm problem. *Applicable Algebra in Engineering, communication and computing*, 3(1):67–74, 1992.

[16] Nadir Murru and Emanuele Bellini. A multi-factor rsa-like scheme with fast decryption based on rédei rational functions over the pell hyperbola. *Numerical Computations: Theory and Algorithms NUMTA 2019*, page 68, 2019.

[17] Sahadeo Padhye. A public key cryptosystem based on pell equation. *IACR Cryptology ePrint Archive*, 2006:191, 01 2006.

[18] Kondala Rao, PS Avadhani, D Lalitha Bhaskari, and KVSSRSS Sarma. An identity based encryption scheme based on pell's equation with jacobi symbol. *Int. J. Res. Eng. Sci*, 1:17–20, 2013.

A Pell Curves of Degree n

The quotient construction of Section 2.2 can be adapted in order to construct degree-n Pell curves and their algebraic variety.
Consider the polynomial ring $\mathcal{R}_{n,d} = \mathbb{F}_q[W]/\langle W^n - d\rangle$ and its ring automorphisms $\psi_1, \ldots, \psi_n$. The norm N_d of an element $f = x_0 + x_1 W + \cdots + x_{n-1}W^{n-1} \in \mathcal{R}_{n,d}$ is then

$$N_d(f) = \psi_1(f) \cdots \psi_n(f)$$

There is a correspondence between the algebraic variety of degree-n Pell curves and the set of elements of unitary norm in the quotient ring $\mathcal{R}_{n,d}$. More explicitly,

$$\mathcal{U}(\mathcal{R}_{n,d}) = \{f \in \mathcal{R}_{n,d} \mid N_d(f) = 1\}$$

inherits the operation induced by polynomial multiplication modulo $W^n - d$. This correspondence defines the degree-n Pell Curve and the degree-n Brahmagupta product. Depending on the properties of d, the multiplicative group $(\mathcal{P}_{n,d}(\mathbb{F}_q), \otimes_{n,d})$ has different isomorphism classes. Some cases are studied using the following criterion.

Theorem 19 (Generalised Euler criterion)**.** *d in $\mathbb{F}_q$ is a n-th power residue if and only if $d^{(q-1)/\gcd(n,q-1)} \equiv 1 \pmod q$.*

The 3-dimensional case was studied by Dutto and Murru in [12], resulting in the classification theorem of Section 2.2. As stated in Section 5, their general classification is an open problem.

A.1 Degree-Three Pell Curves and the Non-cyclic Case

Consider the quotient ring $\mathcal{R}_{3,d}$ and its natural operation $\otimes_{3,d}$. We consider two criteria: the generalised Euler criterion for $n = 3$, and membership testing for a non-trivial cubic root of unity ω in $\mathbb{F}_q$ (i.e., $q \equiv 1 \mod 3$). This results in four main cases [12, Section 5]:

- d non-cube: the quotient $\mathcal{R}_{3,d}$ is a field and does not split.
- d cube and $q \equiv 1 \pmod 3$: d has three roots in $\mathbb{F}_q$, if one of them is a the others are $\omega a, \omega^2 a$ and $\mathcal{R}_{3,d}$ splits in three:

$$W^3 - d = (W - a)(W - \omega a)(W - \omega^2 a)$$

- d cube and $q \equiv 1 \pmod 3$: then d only has one cubic root a in $\mathbb{F}_q$ and splits in two:

$$W^3 - d = (W - a)(W^2 + aW + a^2)$$

- $q \equiv 0 \pmod 3$: the algebraic group of the resulting Pell curve is not cyclic.

B Projective Isomorphisms and Curve Parametrisations

We mentioned in Section 2.2 the existence of a bijection from the degree-two Pell curve to the projective quotient group defined as

$$\mathbb{P}_{d,q} := \mathcal{R}_d^*/\mathbb{F}_q^* = \begin{cases} \{[m+W] \mid m \in \mathbb{F}_q\} \cup \{[1_{\mathbb{F}_q}]\} & \text{if } d \text{ is not a square} \\ \{[m+W] \mid m \in \mathbb{F}_q, m \neq \pm\sqrt{d}\} \cup \{[1_{\mathbb{F}_q}]\} & \text{if } d \text{ is a square} \end{cases}$$

containing all equivalence classes $[x+yW] = [x/y+W] = \{\lambda(x+yW) \mid \lambda \in \mathbb{F}_q^*\}$. The naturally induced operation is

$$[m_1 + W] + [m_2 + W] = \begin{cases} \left[\frac{m_1 m_2 + d}{m_1 + m_2} + W\right] & \text{if } m_1 + m_2 \neq 0 \\ [1_{\mathbb{F}_q}] & \text{if } m_1 + m_2 = 0 \end{cases}$$

This is isomorphic to the algebraic variety of the degree-two pell curve over the same field $\mathbb{F}_q$ via the isomorphism

$$(x, y) \mapsto \begin{cases} [\frac{x+1}{y} + W] & \text{if } y \neq 0 \\ [W] & \text{if } x = -a, y = b \\ [1_{\mathbb{F}_q}] & \text{if } x = a, y = b \end{cases} \tag{7}$$

$$[m + W] \mapsto \begin{cases} (1, 0) & \text{if } [m+W] = [1_{\mathbb{F}_q}] \\ \left(\frac{m^2+d}{m^2-d}, \frac{2m}{m^2-d}\right) & \text{otherwise} \end{cases} \tag{8}$$

The isomorphisms are used by some authors [2, 8] to instantiate cryptographic schemes initially constructed for Pell curves (see, e.g., [2, Section 5]). Still, it suffers the same issues we saw in Section 4. The group operation alone requires a total of

$$T_+(\mathbb{P}) = 2T_\times(\mathbb{F}_q) + 2T_+(\mathbb{F}_q) + T_{1/x}(\mathbb{F}_q)$$

worst-case operations in the base field, where $T_{1/x}(\mathbb{F}_q)$ is the cost of inverting an element in $\mathbb{F}_q$. Similarly to what we concluded in Section 4, any optimisation would unlikely result in operations faster than multiplication in the isomorphic image of $\mathbb{P}_{d,q}$.