Describing the Circle as a Degenerate Edwards Curve over $\mathbb{F}_p$

J.P. Olszewski and J.T. Pruim

April 12, 2023

Introduction

In this paper we study the circle as a degenerate Edwards curve ($d = 0$) over a prime field $\mathbb{F}_p$. For this, there are two possible cases to consider, $p \equiv 1 \mod (4)$ and $p \equiv 3 \mod (4)$. Thus we begin by defining the Edwards curve:

Definition 0.1. ***Edwards curve over*** $\mathbb{F}_p$
the set :

$$E = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p | x^2 + y^2 = 1 + dx^2y^2 \in \mathbb{F}_p | d \in \mathbb{F}_p\} \tag{1}$$

with the operation $+ : E \times E \to E$ *such that* $(x_1, y_1) + (x_2.y_2) = (\frac{x_1x_2 - y_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2})$ *is an abelian group. This group is defined to be the Edwards Curve over* $\mathbb{F}_p$

Our aim is to study the particular case:

$$E = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p | x^2 + y^2 = 1\} \tag{2}$$

where the group operation simplifies to

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \tag{3}$$

Edward's form elliptic curves are widely used in cryptography as they are secure (also to backdoor attacks) and relatively simple to work with. The degenerate case studied here has little cryptography use (to the knowledge of the authors at the time of writing), nonetheless, is an interesting problem to consider while investigating these curves.

We approach the problem by considering Homomorphisms between the Edwards curve and the groups related to $\mathbb{F}_p$. Since we take the Edwards curves over a finite field, $\mathbb{F}_p$, it is immediately clear that it also must be a finite group. Thus the majority of the paper is dedicated to computing the number of elements of the Edwards curve. In some cases

this proved to be constructive and allows us to conclude more on the structure of the Edwards group.

The paper is divided into five sections, of which section 2 and section 3 provide the main results. In these we begin by deriving results about the field $\mathbb{F}_p$, and the groups we associate with it, before arriving at the results about the Edwards Curve. The remaining sections provide examples.

To clarify notation, all dummy variables of polynomial rings are denoted with a capital letters, and all elements in $\mathbb{F}_p$ are denoted with lower case letters (unless stated otherwise), for example the element $x + yX + zX^5$ is an element of $\mathbb{F}_p[X]$ where $x, y, z \in \mathbb{F}_p$. Since we only study the degenerate case, the Edwards group defined in 2 is hereafter referred to only as E.

1. The simplest example

For the sake of completion we first consider E over $\mathbb{F}_2$, since 2 is the only prime which does not fit into the cases mentioned in the Introduction. This case my be quickly computed. Note that $\mathbb{F}_2 = \{0, 1\}$, thus $\mathbb{F}_2 \times \mathbb{F}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$. We can easily check the definition for all of these points and conclude that, for $p = 2$:

$$E = \{(1,0), (0,1)\}$$

Which is generated by $(0, 1)$, hence cyclic of order 2.

2. The case $p \equiv 1 \mod (4)$

2.1 Preliminaries 1

One thing to immediately note from the definition of an Edwards curve, is that the element $(0, 1)$ always has order 4 (except in the degenerate case $p = 2$, where it has order 2). This hints at the importance of finding elements of order 4 in $\mathbb{F}_p^*$.

Proposition 2.1. *Given a prime $p \equiv 1 \mod 4$, $\exists i \in \mathbb{F}_p^*$ such that $ord(i) = 4$.*

Proof. Fix the integer k such that $p = 1 + 4k$. Since p is prime, there exists an element $g \in \mathbb{F}_p^*$ which generates the group and hence has order $p - 1$. This implies:

$$\left(g^k\right)^4 = g^{4k} = g^{p-1} \equiv 1 \mod p$$

Since $k < p - 1$ we have that $i := g^k$ is non-trivial and has order 4. □

Remark 2.2. *Given the existence of such an element, consider the decomposition:*

$$(x + iy)(x - iy) = x^2 - i^2y^2 \tag{4}$$

note that $(i^2)^2 = 1$ therefore i^2 has order 2 but since p is a prime, $\mathbb{F}_p^*$ has only two elements of order 2. That is 1 and -1, and $i \neq 1$ by construction. Therefore $i^2 = -1$ and the decomposition below follows.

$$x^2 + y^2 = (x + iy)(x - iy) \tag{5}$$

This decomposition is an important result as it allows us to cinsider the elements of the form $x + iy \in \mathbb{F}_p^*$ rather then pairs of elements $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$. This restating of the problem makes it more approachable and much easier to work with. It follows that we would like to rewrite the elements in $\mathbb{F}_p^*$ in this form.

Remark 2.3. *Any element $x \in \mathbb{F}_p^*$ can be written in the form $x = a + ib$. Take, for example, an arbitrary $a \in \mathbb{F}_p$ and let $b = (i^3 x + ia)$. Note that this solution forces b to be non-zero.*

To satisfy equation 2, we construct these decompositions in such a way that their conjugates are their inverses.

Lemma 2.4. *Any element $z \in \mathbb{F}_p^*$ can be uniquely written in the form $z = x + iy$ such that $z^{-1} = x - iy$.*

Proof. $zz^{-1} = 1$, we can always re-write z^{-1} as $z^{-1} = z - i(2y)$ for some $y \in \mathbb{F}_p$. Let $x := z - iy$. Thus we have:

$$1 = zz^{-1} = (z - iy + iy)(z^{-1} - iy + iy) = (x + iy)(x - iy) = 1 \tag{6}$$

thus $(x+iy)^{-1} = (x-iy)$. As for uniqueness, let $z = (a+ib) = (c+id)$ be two arbitrary decompositions of z such that $z^{-1} = (a - ib) = (c - id)$. This implies that:

$$\begin{aligned} a + ib = c + id &\iff a - c = i(d - b) \\ a - ib = c - id &\iff a - c = i(b - d) \end{aligned}$$

subtracting the second equation from the first we get:

$$0 = 2i(d - b) \implies d - b = 0 \implies d = b$$

Since these fixes $d = b$, it implies that $a = c$ since $a + ib = c + ib$. □

Note that this lemma is more general then is necessary as we make no assumption about the element i itself. Namely such a unique decomposition still exists if we replace i with any other element of $\mathbb{F}_p^*$.

2.2 The main result, part 1

Having developed enough tools, we now tackle the main problem of computing the size of E in this case of p.

Theorem 2.5. *(Isomorphism)*
Given that $p \equiv 1 \mod (4)$, then $\mathbb{F}_p^* \cong E$

Proof. consider the map $\varphi : \mathbb{F}_p^* \to E$ such that $x = a + ib \mapsto (a, b)$ where $a, b \in \mathbb{F}_p$ are such that $x^{-1} = a - ib$. By Lemma 2.4 such a, b exist and are unique thus this map is

well defined. We first claim that φ is a homomorphism:

$$\begin{aligned}
&\varphi(x \cdot y) \\
&= \varphi((a+ib)\cdot(c+id)) = \varphi((ac-bd)+i(ac+bd)) \\
&= ((ac-bd),(ac+bd)) \\
&= (a,b)+(c,d) = \varphi(a+ib)+\varphi(c+id) \\
&= \varphi(x)+\varphi(y)
\end{aligned}$$

Now we want to show that it is also a bijection. Thus if we take $x \in \ker(\varphi)$, this implies $x = 1 + i(0) = 1$ and so the kernel is trivial (φ is injective). Now take an arbitrary $(x, y) \in E$, by definition this point satisfies $x^2 + y^2 = 1$ over $\mathbb{F}_p$, which is equivalent to $(x + iy)(x - iy) = 1$ (by remark 2.2), hence $(x + iy)^{-1} = (x - iy)$ and therefore is the image of $z = (x + iy) \in \mathbb{F}_p^*$ where x, y are uniquely determined. This means that φ is surjective. Hence φ is an isomorphism:

$$\mathbb{F}_p^* \cong E \tag{7}$$

□

Since we have show an isomorphism of E, we can fully describe the group structure.

Corollary 2.6. *E is a cyclic group of order $p - 1$*

The following result is also a direct corollary of Theorem 2.5, however, in our investigation of the problem we proved this prior to Theorem 2.5. It is thus accompanied by a stand alone proof.

Corollary 2.7. *Given the Edwards circle, E, over $\mathbb{F}_p$, where $p \equiv 1 \mod 4$. E has exactly $p - 1$ elements.*

Proof. Note that $(x, y) \in E$ if and only if $x^2 + y^2 = 1$. By the remark above this is equivalent to the equation $(x + iy)(x - iy) = 1$. That is, the two factors are inverses of each other. Fixing one of the two to be an element in $\mathbb{F}_p^*$, say a, there must exist a $b \in \mathbb{F}_p$ such that $a^{-1} = a - 2ib$, **since** $2i$ **generates**[1] $\mathbb{F}_p$. Taking $x = a - bi$ and $y = b$ yields $(x + iy)(x - iy) = (a - bi + bi)(a - bi - bi) = (a)(a^{-1}) = 1$. Since there are exactly $p - 1$ such pairs to be found, E has at least $p - 1$ elements. Conversely, we can define a group morphism from E to $\mathbb{F}_p^*$:

$$\phi : (x, y) \mapsto x + iy$$

[1]NB: this is the additive group, not the multiplicative group!

because

$$\phi((x_1, y_1) + (x_2, y_2)) = \phi(x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$
$$= x_1x_2 - y_1y_2 + ix_1y_2 + ix_2y_1 = (x_1 + iy_1)(x_2 + iy_2)$$
$$= \phi((x_1, y_1)) + \phi((x_2, y_2))$$

Note that the kernel satisfies $x + iy = 1$, and $x - iy = 1^{-1} = 1$. Solving this system of linear equations yields the unique solution $(x, y) = (1, 0)$, hence the kernel is trivial and the morphism is injective, and by previous part hence has a well-defined inverse. This finishes the proof. □

3. The case $p \equiv 3 \mod (4)$

3.1 Preliminaries 2

Note that this case is somewhat the opposite of the first since now $p \equiv (-1) \mod (4)$. First, we show that such an element alike i does not exist.

Proposition 3.1. *Given that $p \equiv 3 \mod (4)$, There does not exist an element of order 4 in $\mathbb{F}_p^*$.*

Proof. Note that $\#\mathbb{F}_p^* = p - 1 = 2 + 4k$ for some $k \in \mathbb{Z}$.
Assume that $\exists i \in \mathbb{F}_p^*$ such that $ord(i) = 4$. This implies that $\langle i \rangle$ is a subgroup with precisely 4 elements which is a contradiction since $4 \nmid (2 + 4k)$ for all $k \in \mathbb{Z}$. □

The nonexistence of an element of order 4 is not unique to finite fields, as the most commonly known field $\mathbb{R}$ has the same problem. To help this, complex numbers were invented. The introduction of an "imaginary unit" to solve the equation $x^2 = -1$ is also used in this section.

Proposition 3.2. *Given $p \equiv 3 \mod (4)$, $X^2 + 1$ is irreducible over $\mathbb{F}_p^*$.*

Proof. Consider the following equation over $\mathbb{F}_p^*$.

$$X^2 + 1 = 0 \tag{8}$$

Assume that there exists a solution $i \in \mathbb{F}_p^*$. This implies that:

$$i^2 = -1 \implies (i^2)^2 = (-1)^2 = 1 \implies i^4 = 1$$

Which implies that i has order 4. This contradicts proposition 3.1. Therefore equation 8 can not be decomposed into linear factors with coefficients in $\mathbb{F}_p^*$ and thus is irreducible over this field. □

Remark 3.3. *From this result, it follows that $\mathbb{F}_p[X]/(X^2+1)$ forms a field. In particular, inverses exist for all non-zero elements.*

In this field, however, an element of order 4 does exist. Notice that, $X^2 \equiv -1 \mod (X^2 + 1)$, thus we define an element i such that we can also have the decomposition in 5.

$$i := X \mod (X^2 + 1) \tag{9}$$

Thus if we consider the equation of the circle over this extension we have:

$$x^2 + y^2 = (x + iy)(x - iy) = 1 \tag{10}$$

where $x, y \in \mathbb{F}_p$ and we can deduce that $(x-iy)$ is the inverse of $(x+iy)$ over $\mathbb{F}_p[X]/(X^2+1)$.
Describing the Edwards circle is now a problem of finding inverses to $a+ib$.

Proposition 3.4. *The set*

$$M := \{(a+ib) \in (\mathbb{F}_p[X]/(X^2+1))^* : (a+ib)^{-1} = (a-ib), a, b \in \mathbb{F}_p\} \tag{11}$$

forms a subgroup of $(\mathbb{F}_p[X]/(X^2+1))^*$ *with respect to multiplication.*

Proof. Note that $1 = 1 + 0i \in M$ and by definition every element also has an inverse in M. Furthermore, the set is closed under multiplication:

$$\begin{aligned}
(a+ib)(c+id) &= (ac-bd) + i(ad+bc) \\
&\text{and} \\
((a+ib)(c+id))^{-1} &= (a+ib)^{-1}(c+id)^{-1} \\
= (a-ib)(c-id) &= (ac-bd) + (a(-d) + (-b)c) \\
&= (ac-bd) - i(ad+bc) \\
\implies (ac-bd) + i(ad+bc) &\in M
\end{aligned}$$

Thus M is a subgroup. □

Note that multiplying two elements in M is analogous to performing the group operation two elements in E. In analogy to theorem 2.5 we can construct an isomorphism between M and E. This is exactly the same and thus we exclude the computation. Hence we only need to investigate the subgroup M. First note that $(\mathbb{F}_p[X]/(X^2+1))^*$ has p^2-1 elements, and so the order of M must divide this.

$$\begin{aligned}
&p^2 - 1 \\
&= (3+4k)^2 - 1 \\
&= 8 + 24k + 16k^2 \\
&= 2^3(1+k)(1+2k)
\end{aligned}$$

And since it is isomorphic to E it must also have an element of order 4. In fact, the subgroup has exactly $p+1$ elements.

Lemma 3.5. *Given* $p \equiv 3 \mod (4)$*, any element* $n \in \mathbb{F}_p$ *can be written as a sum of two squares in* $\mathbb{F}_p$*.*

Proof. [1] Consider the squaring map $x \mapsto x^2$, the image of $\mathbb{F}_p^*$ under this map has exactly $(p-1)/2$ elements, and adding 0 back in shows that $\frac{p+1}{2}$ elements in $\mathbb{F}_p$ are perfect squares.

Let S be the set of squares in $\mathbb{F}_p$, and let $k \in \mathbb{F}_p$ be an arbitrary element, then the set $T = k - S := \{k - y^2 | y^2 \in S\}$ also has exactly $(p+1)/2$ elements (because the addition of an integer only shifts the elements in $\mathbb{F}_p$). Note that these are both subsets of $\mathbb{F}_p$ which contains p elements, thus, by the Pigeonhole principal there exists an element $x^2 \in T \cap S$. This implies that $x^2 = k - y^2$ for some $y \in \mathbb{F}_p$ and hence $k = x^2 + y^2$. Since we took k to be arbitrary this implies that such a decomposition exists for all $k \in \mathbb{F}_p$. □

In particular, we see that any unit of $\mathbb{F}_p^*$ can be written as a sum of two squares.

3.2 The main result, part 2

Theorem 3.6. *Given that $p \equiv 3 \mod (4)$, Then, E consists of $p+1$ points.*

Proof. Consider the homomorphism $\psi : (\mathbb{F}[X]/X^2 + 1)^* \to \mathbb{F}_p^*$ given by

$$\psi : x + iy \mapsto (x + iy)(x - iy) = x^2 + y^2$$

By definition, the kernel of this morphism is M, since the elements of M are precisely the elements that get mapped to 1 under ψ. Also, ψ is surjective, since any element in $\mathbb{F}_p^*$ can be written as the sum of two squares in $\mathbb{F}_p$ by lemma 3.5. By the first isomorphism theorem, we have that $\#M = \frac{\#(\mathbb{F}_p[X]/X^2+1)^*}{\#\mathbb{F}_p^*} = \frac{p^2-1}{p-1} = p + 1$. □

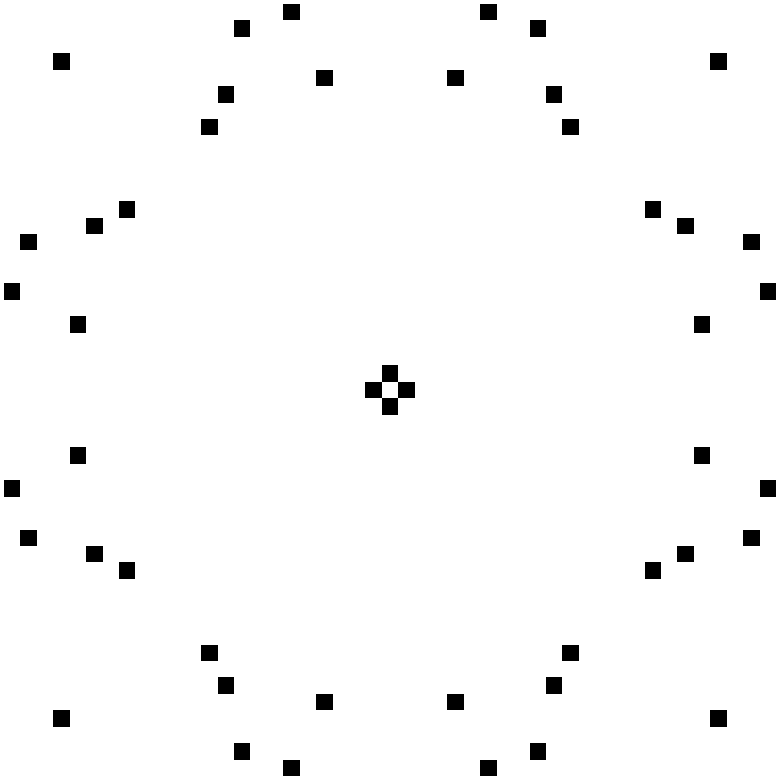
4. Examples

4.1 Plots

Plotting the points on the Edwards curve on a $p \times p$ grid with the origin at the centre, makes the 4-way symmetry of a circle very apparent. Here are the plots for $p = 17, 19, 47$:

(a) p=17

(b) p=19



(c) p=47

Figure 1: Edwards curves on a $p \times p$ grid with origin at the centre

4.2 Quadrants

The plots hint towards a four-way rotational symmetry, and as it turns out we can identify the points a "90-degree rotation" away by repeated multiplication of with the element of

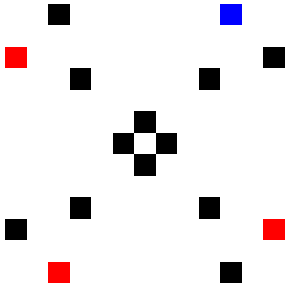


Figure 2

order 4. The subgroup $\langle i \rangle = \{i, i^2, i^3, i^4 = (1, 0)\} = \{(0, \pm 1), (\pm 1, 0)\}$ is normal because it is precisely the kernel of $p \mapsto p^4$. Quotienting this subgroup out of the Edwards curve $E/\langle i \rangle$ is analogous to only considering the first quadrant.

References

[1] PrimeRibeyeDeal (https://math.stackexchange.com/users/18159/primeribeyedeal). *Sum of two squares modulo p*. Mathematics Stack Exchange. URL:https://math.stackexchange.com (version: 2014-08-09). eprint: https://math.stackexchange.com/q/891996. URL: https://math.stackexchange.com/q/891996.