Circles in $\mathbb{F}_q^2$

Jacob Haddock, Wesley Perkins, and John Pope
Faculty Adviser: Dr. Jeremy Chapman

Abstract. In Euclid's *The Elements*, a unique circle in $\mathbb{R}^2$ is determined by three noncollinear points. This is proven geometrically by constructing a triangle from the three points and showing that the intersection of the perpendicular bisectors of two sides of the triangle gives a point that is equidistant from all three vertices of the triangle [1]. This point is said to define the center of a circle which circumscribes the triangle formed by the points. In our research, we demonstrate that circles can be similarly determined in $\mathbb{F}_q^2$, the two-dimensional vector space over the finite field $\mathbb{F}_q$. However, the properties of $\mathbb{F}_q^2$ cause some interesting cases to arise. Among these is the possibility for two distinct points to have zero distance. Nevertheless, we were able to show that three distinct noncollinear points which have nonzero distance from each other determine a unique circle of nonzero radius.

1. Introduction

In our project, work was done specifically in $\mathbb{F}_q^2$. For completeness, we define the following:

Definition 1.1. The set G defines a **group** with respect to the binary operation $*$ if the following are satisfied:

(1) G is closed under $*$.
(2) $*$ is associative.
(3) G has an identity element, e.
(4) G contains inverses.

Note that if $*$ on G is commutative, then G is called an **abelian group**

Definition 1.2. The set R defines a **ring** with respect to addition and multiplication if the following are satisfied:

(1) R forms an abelian group with respect to addition.
(2) R is closed with respect to an associative multiplication.
(3) The following two distributive laws hold: $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$.

Note that if multiplication in R is commutative, then R is called a **commutative ring**.

Definition 1.3. The set F defines a **field** if the following are satisfied:

(1) F is a commutative ring.
(2) F has a unity $1 \neq 0$ such that $1 \cdot x = x \cdot 1 = x \ \forall \ x \in F$.
(3) Every nonzero element of F has a multiplicative inverse.

Every field is an **integral domain**, meaning that there are no zero divisors.[2] Zero divisors are nonzero elements of the integral domain, say $a \neq 0$, which can be multiplied by another nonzero element, say $b \neq 0$, to yield zero: $ab = 0$.

REMARK 1.4. Throughout this paper, we will use the following notation:

(1) $\frac{a}{b}$ will represent $(a)(b^{-1})$, where b^{-1} is the multiplicative inverse of b.
(2) $a - b$ will represent $a + (-b)$, where $-b$ is the additive inverse of b.

DEFINITION 1.5. The norm, or distance, between two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ where $P_1, P_2 \in F_q^2$, denoted $||P_2 - P_1||$, is $(x_2 - x_1)^2 + (y_2 - y_1)^2$.

Note that, because we are working in $\mathbb{F}_q^2$, it is possible for two distinct points to possess zero distance.

EXAMPLE 1.6. Consider $\mathbb{Z}_5^2$, the two-dimensional vector space over the finite field $\mathbb{Z}_5$. In this particular field, modular arithmetic allows us to demonstrate zero distance between the points $(\overline{2}, \overline{1})$ and $(\overline{0}, \overline{0})$. Substituting these points into the norm equation, we get $||P_2 - P_1|| = (\overline{2} - \overline{0})^2 + (\overline{1} - \overline{0})^2 = \overline{4} + \overline{1} = \overline{5} = \overline{0}$, since $5 \equiv 0 \pmod 5$.

Later, we will utilize more interesting consequences of the 0 norm problem.

DEFINITION 1.7. The perpendicular bisector of the line segment $\overline{P_1P_2}$, denoted $bisector(P_1, P_2)$, is given by:

$$bisector(P_1, P_2) = \left\{P \in \mathbb{F}_q^2 \mid ||P_1 - P|| = ||P_2 - P||\right\}$$

Note that the perpendicular bisector is a line and the slope is still the negative reciprocal of the line it bisects. This will be demonstrated in Section 3.1.

DEFINITION 1.8. A circle is defined as the set of all points equidistant from an arbitrary center. In particular, a circle centered at C of radius r is given by:

$$S_r(C) = \left\{P \in \mathbb{F}_q^2 \mid ||C - P|| = r\right\}$$

THEOREM 1.9. *Let $P_1, P_2, P_3 \in \mathbb{F}_q^2$ ($q = p^l$, $p > 2$ is a prime, and $l \in \mathbb{N}$) be three distinct, noncollinear points that are nonzero norm from each other. Then, these points determine a unique circle of nonzero radius in $\mathbb{F}_q^2$.*

In order to prove Theorem 1.9, we must first prove several lemmas which allow us to justify the nonzero claims of the theorem. The first lemma demonstrates that, when $||P_2 - P_1|| = 0$, the perpendicular bisector of $\overline{P_1P_2}$ is the line containing points $P_1, P_2 \in \mathbb{F}_q^2$. The second lemma uses the first to demonstrate that an arbitrary point $P \in \mathbb{F}_q^2$ is zero norm from P_1 and P_2 if it lies on the perpendicular bisector of $\overline{P_1P_2}$ and $||P_2 - P_1|| = 0$. The third lemma demonstrates that if the square root of an element of $\mathbb{F}_q$ exists, then there are exactly two square roots that exist so long as the element is not zero. The fourth lemma uses the third to demonstrate that if an arbitrary point $P \in \mathbb{F}_q^2$ lies on a zero line (see Definition 2.4), then it has exactly two zero lines that pass through it. The fifth lemma uses the second and fourth to demonstrate that if P_1, P_2, and P_3 are nonzero norm from one another and are noncollinear, then their perpendicular bisectors do not intersect at a point that is zero norm from P_1, P_2, and P_3, thus ruling out circles of radius zero. Figure 1 displays a circle of radius zero over $\mathbb{Z}_5^2$ to give an example of what such a circle would look like.

We exclude circles of zero radius on the basis that the unique properties of $\mathbb{F}_q^2$ are expected to alter the behavior of circles to such a degree warranting a separate in-depth investigation. Our proof of Theorem 1.9 is a direct proof which uses Definition 1.7 to algebraically derive expressions

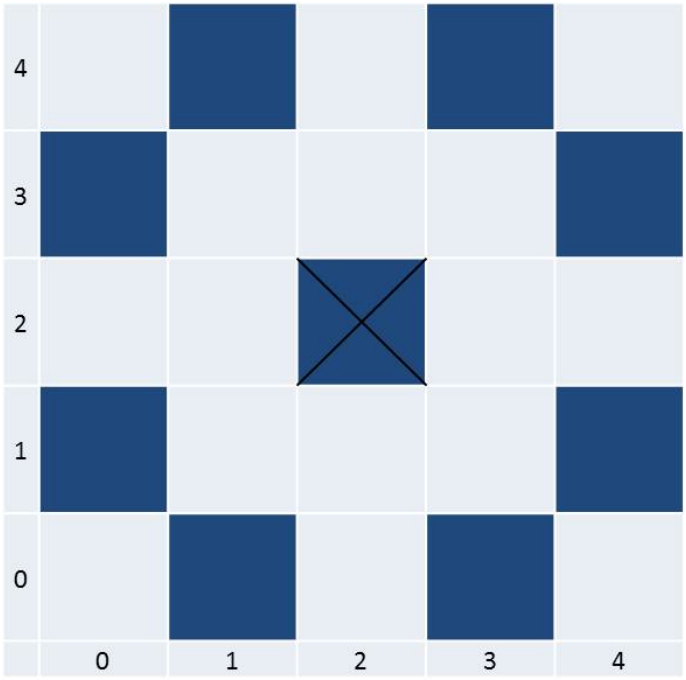

FIGURE 1. A circle of radius 0 centered at $(2, 2)$ over $\mathbb{Z}_5^2$. It is worth noting that in the case of a zero radius circle, the center of the circle is actually included as part of the circle.

for the center of the circle defined by three distinct, noncollinear points, the existence of which is verified by satisfying Definition 1.8. This proof also requires us to verify that the center exists and is unique, and validate any division operations required to reach our conclusion. Figure 3 demonstrates a circle of nonzero radius over $\mathbb{Z}_7^2$.

2. Proof of Lemmas

REMARK 2.1. Throughout the presented proofs involving zero lines, we multiply by $(x_2-x_1)^{-1}$ and $(y_2 - y_1)^{-1}$. This multiplication is valid as long as $(x_2 - x_1)^{-1}$ and $(y_2 - y_1)^{-1}$ exist, or in other words, as long as $x_1 \neq x_2$ and $y_1 \neq y_2$. We can verify that this is the case by considering the following:

If $x_2 - x_1 = 0$ and $y_2 - y_1 = 0$, i.e. $x_1 = x_2$ and $y_1 = y_2$, then we have only one point, $P_1 = P_2$, a violation of the initial conditions of our proofs.

If we let one set of coordinates be equal, say $x_1 = x_2$, i.e. $x_2 - x_1 = 0$, and $||P_2 - P_1|| = (x_2 - x_1)^2 + (y_2 - y_1)^2 = 0$ (since we will be specifically investigaing 0 norms), then:

$$\begin{aligned} ||P_2 - P_1|| = (0)^2 + (y_2 - y_1)^2 &= 0 \\ \implies (y_2 - y_1)^2 &= 0 \\ \implies y_2 = y_1 \qquad & \text{Again, implying } P_1 = P_2 \end{aligned}$$

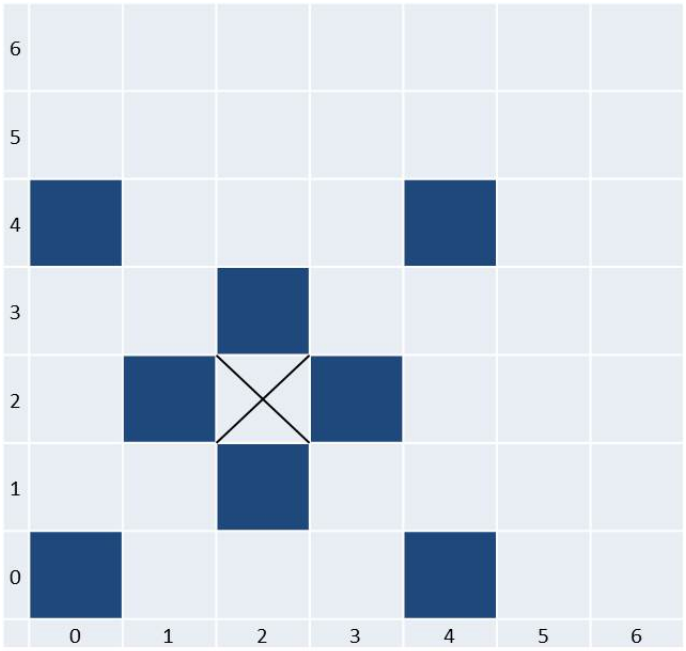

FIGURE 2. A circle of radius 1 centered at $(2, 2)$ over $\mathbb{Z}_7^2$

We get a similar result if we let $y_1 = y_2$. Note that, since fields are integral domains (see Definition 1.3), it follows that the square root of 0 is 0 in our case. From this set of justifications, we are also guaranteed that it is impossible to have a horizontal or vertical zero line (since $x_1 \neq x_2$ and $y_1 \neq y_2$ for any two arbitrary points on an arbitrary zero line).

LEMMA 2.2. *The perpendicular bisector of two distinct points zero norm apart is the line containing the two points.*

PROOF. Suppose $\exists\ P_1, P_2 \in \mathbb{F}_q^2$ such that $||P_2 - P_1|| = 0$. To show the perpendicular bisector and line $\overleftrightarrow{P_1P_2}$ are the same, it suffices to show both lines contain two points in common.
To begin, we make note of the fact that, as demonstrated in 3.1, we have that the perpendicular bisector of any two points $\in mathbbF_q^2$ is, in fact, a line.
Now we want to show that both the line $\overleftrightarrow{P_1P_2}$ and the perpendicular bisector of P_1 and P_2 contain two points in common. To do this, consider the definition of perpendicular bisector:

$$bisector(P_1, P_2) = \left\{P \in \mathbb{F}_q^2 \mid ||P_1 - P|| = ||P_2 - P||\right\}$$

If we pick point P_1, which is on $\overleftrightarrow{P_1P_2}$, it follows that P_1 also lies in $bisector(P_1, P_2)$, since $||P_1 - P_1|| = 0$ and $||P_2 - P_1|| = 0$, by assumption. This can also be shown for P_2. Since P_1 and P_2 both lie in the bisector, it follows that the bisector of P_1 and P_2 is the same line as $\overleftrightarrow{P_1P_2}$. □

LEMMA 2.3. *An arbitrary point on the perpendicular bisector of two distinct points zero norm apart is zero norm from each of the two points.*

PROOF. Let $P_0 \in \mathbb{F}_q^2$ be an aribitrary point on $\overline{P_1P_2}$ (where $P_1, P_2 \in \mathbb{F}_q^2$) and $||P_2 - P_1|| = 0$. By Lemma 2.2 and Definition 1.7, it suffices to show $||P_0 - P_1|| = 0$.

$$
\begin{aligned}
& y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1 && \text{Equation for } \overline{P_1P_2} \\
& y_0 = \frac{y_2 - y_1}{x_2 - x_1}(x_0 - x_1) + y_1 && \text{Substituting } P_0 = (x_0, y_0) \\
\implies & ||P_0 - P_1|| = (x_0 - x_1)^2 + \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_0 - x_1) + y_1 - y_1\right]^2 && \text{Substituting } y_0 \text{ into } ||P_0 - P_1|| \\
\implies & ||P_0 - P_1|| = \frac{(x_0 - x_1)^2}{(x_2 - x_1)^2}\left[(x_2 - x_1)^2 + (y_2 - y_1)^2\right] && \text{Factoring out } (x_0 - x_1)^2(x_2 - x_1)^{-2} \\
\implies & ||P_0 - P_1|| = 0 && ||P_2 - P_1|| = 0 \text{ by assumption.}
\end{aligned}
$$

□

DEFINITION 2.4. We shall refer to the perpendicular bisector of (or the line through) two points that are zero norm from one another as a zero line. Note that by Lemma 2.3, each point on the zero line has a zero norm with each other point on the line.

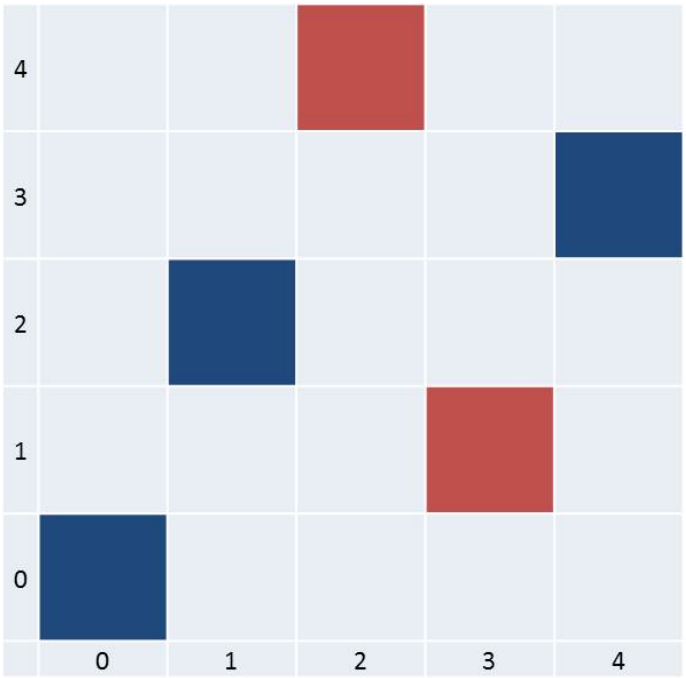

FIGURE 3. A zero line in $\mathbb{Z}_5^2$. Note that any two points chosen on the line will have a norm of zero.

LEMMA 2.5. *If $a \in \mathbb{F}_q$ has a square root, then the equation $x^2 = a$ has exactly two solutions as long as a is nonzero.*

PROOF. Suppose $a \neq 0$ has a square root, i.e $\exists\ b \in \mathbb{F}_q$ such that $b^2 = a$. Then,

$$\begin{aligned} & x^2 = a \\ \implies & x^2 = b^2 && \text{(by substituting } a \text{ with } b^2\text{)} \\ \implies & x^2 - b^2 = 0 \\ \implies & (x-b)(x+b) = 0 \\ \implies & x = \pm b \end{aligned}$$

Here we note that, since $b \neq 0$, x will only have one solution as long as $2 \neq 0$. Consequently, $x^2 = a$ has exactly two solutions as long as a has a square root and $2 \neq 0$.

□

LEMMA 2.6. *If an arbitrary point P_0 lies on a zero line, there are exactly two zero lines passing through P_0.*

PROOF. Assume that $P_0 = (x_0, y_0) \in \mathbb{F}_q^2$ lies on a zero line. This implies that there exists an $(a, b) \in \mathbb{F}_q^2$ such that $(x_0 - a)^2 + (y_0 - b)^2 = 0$. Consequently, $(y_0 - b)^2 = -(x_0 - a)^2$. In other words, $-(x_0 - a)^2$ has a square root. Then, the equation $(y_0 - y)^2 = -(x_0 - a)^2$ has solutions $y_0 - y = \pm(y_0 - b) \implies y = b, 2y_0 - b$, by Lemma 2.5. These values for y are distinct because these two values can only be equal when $y_0 = b$, which can not happen since a zero line can not be horizontal by Remark **??**. Thus, there are two vaules for y that are zero distance from (x_0, y_0), and since (a, b) and $(a, 2y_0 - b)$ are nonzero norm from each other, they must lie on separate zero lines by Lemma 2.3. □

LEMMA 2.7. *If three distinct points are chosen such that P_1, P_2, and P_3 are nonzero norm from one another and they are noncollinear, their perpendicular bisectors can not intersect at a point C such that $||P_1 - C|| = ||P_2 - C|| = ||P_3 - C|| = 0$*

PROOF. Let P_1, P_2, $P_3 \in \mathbb{F}_q^2$. Let C be the unique intersection of $bisector(P_1, P_2)$ and $bisector(P_2, P_3)$. Furthermore, $||P_1 - P_2|| \neq 0$, $||P_1 - P_3|| \neq 0$, and $||P_2 - P_3|| \neq 0$. For a contradiction, consider the possibility that $||P_1 - C|| = ||P_2 - C|| = ||P_3 - C|| = 0$. Then C shares a zero line with P_1, P_2, and P_3. Since, by Lemma 2.6, C has only two zero lines passing through it, at least one pair of the points P_1, P_2, and P_3 must lie on the same zero line. Since all points on a zero line are zero norm from one another, this would imply that either $||P_1 - P_2|| = 0$, $||P_1 - P_3|| = 0$, or $||P_2 - P_3|| = 0$, all of which are contradictions to the hypothesis that none of the points are zero norm from one another. □

As a result of these lemmas, it follows that zero norm between any two of the three points implies a zero radius circle, thereby allowing us to specify a circle of nonzero radius by maintaining that the three points defining it are all nonzero norm from each other (See Theorem 1.9).

3. Proof of Theorem 1.9

To prove Theorem 1.9, we consider the following:

(1) Three noncollinear points, $P_1, P_2, P_3 \in \mathbb{F}_q^2$, all nonzero norm from each other.

(2) The perpendicular bisectors of $\overline{P_1P_2}$ and $\overline{P_2P_3}$.
(3) Some arbitrary point $C = (x, y)$ which is said to lay on each of the perpendicular bisectors at their intersection.

We want to show C exists and is a unique solution for the intersection of the bisectors. This resulting solution will define the center of the circle containing P_1, P_2, P_3.

3.1. Derivation of Perpendicular Bisectors.

To obtain the bisector of $\overline{P_1P_2}$, let:

$$||P_1 - C|| = ||P_2 - C|| \qquad \text{By Definition 1.7}$$
$$\implies (x_1 - x)^2 + (y_1 - y)^2 = (x_2 - x)^2 + (y_2 - y)^2 \qquad \text{By Definition 1.5}$$
$$\implies x_1^2 - 2x_1x + x^2 + y_1^2 - 2y_1y + y^2 = x_2^2 - 2x_2x + x^2 + y_2^2 - 2y_2y + y^2$$
$$\implies x_1^2 - 2x_1x + y_1^2 - 2y_1y = x_2^2 - 2x_2x + y_2^2 - 2y_2y$$
$$\implies 2y(y_1 - y_2) + 2x(x_1 - x_2) = x_1^2 - x_2^2 + y_1^2 - y_2^2$$
$$\implies y = -\left(\frac{x_1 - x_2}{y_1 - y_2}\right)x + \frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2(y_1 - y_2)} \qquad bisector(P_1, P_2)$$

Similarly, the bisector of $\overline{P_2P_3}$ can be obtained:

$$||P_2 - C|| = ||P_3 - C|| \qquad \text{By Definition 1.7}$$
$$\implies (x_2 - x)^2 + (y_2 - y)^2 = (x_3 - x)^2 + (y_3 - y)^2 \qquad \text{By Definition 1.5}$$
$$\implies y = -\left(\frac{x_2 - x_3}{y_2 - y_3}\right)x + \frac{x_2^2 - x_3^2 + y_2^2 - y_3^2}{2(y_2 - y_3)} \qquad bisector(P_2, P_3)$$

Note that if either $\overline{P_1P_2}$ or $\overline{P_2P_3}$ are horizontal, then either $y_1 - y_2$ or $y_2 - y_3$ are zero. We must then solve for x instead of y to avoid dividing by zero (it is easily verified that, in such a case, the perpendicular bisector of 2 points, say (x_1, y_1) and (x_2, y_2) horizontal to one another is the vertical line $x = \frac{x_1+x_2}{2}$).

Because, by Definition 1.7, we know that $||P_1 - C|| = ||P_2 - C||$ and $||P_2 - C|| = ||P_3 - C||$, it follows that $||P_1 - C|| = ||P_3 - C||$ and C is the point equidistant from points P_1, P_2, and P_3; namely, the center of the circle defined by these points (see Definition 1.8). Then, using the two perpendicular bisectors we derived, we can obtain a generalized solution for the center $C = (x, y)$.

3.2. Solving for the Center.

To obtain the, x-coordinate of C, let:

$bisector(P_1, P_2) = bisector(P_2, P_3)$

$$\implies -\left(\frac{x_1 - x_2}{y_1 - y_2}\right)x + \frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2(y_1 - y_2)} = -\left(\frac{x_2 - x_3}{y_2 - y_3}\right)x + \frac{x_2^2 - x_3^2 + y_2^2 - y_3^2}{2(y_2 - y_3)}$$

$$\implies x\left(-\frac{x_1 - x_2}{y_1 - y_2} + \frac{x_2 - x_3}{y_2 - y_3}\right) = \frac{x_2^2 - x_3^2 + y_2^2 - y_3^2}{2(y_2 - y_3)} - \frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2(y_1 - y_2)}$$

$$\implies x\left(\frac{(y_1 - y_2)(x_2 - x_3) - (y_2 - y_3)(x_1 - x_2)}{(y_1 - y_2)(y_2 - y_3)}\right) = \frac{(y_1 - y_2)(x_2^2 - x_3^2 + y_2^2 - y_3^2) - (y_2 - y_3)(x_1^2 - x_2^2 + y_1^2 - y_2^2)}{2(y_1 - y_2)(y_2 - y_3)}$$

$$\implies x = \frac{(y_1 - y_2)(x_2^2 - x_3^2 + y_2^2 - y_3^2) - (y_2 - y_3)(x_1^2 - x_2^2 + y_1^2 - y_2^2)}{2[(y_1 - y_2)(x_2 - x_3) - (y_2 - y_3)(x_1 - x_2)]}$$

To obtain the y-coordinate of C:

Substitute the solution for x into either $bisector(P_1, P_2)$ or $bisector(P_2, P_3)$

$$\implies y = \left(-\frac{x_1 - x_2}{y_1 - y_2}\right)\left[\frac{(y_1 - y_2)(x_2^2 - x_3^2 + y_2^2 - y_3^2) - (y_2 - y_3)(x_1^2 - x_2^2 + y_1^2 - y_2^2)}{2[(y_1 - y_2)(x_2 - x_3) - (y_2 - y_3)(x_1 - x_2)}\right] + \frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2(y_1 - y_2)}$$

$$\implies y = \frac{(x_1 - x_2)(x_2^2 - x_3^2 + y_2^2 - y_3^2) - (x_2 - x_3)(x_1^2 - x_2^2 + y_1^2 - y_2^2)}{2[(x_1 - x_2)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_2)]}$$

It remains to be verified that this solution exists and is unique.

3.3. Justifications.

REMARK 3.1. We know our solution for C exists if the denomintors for both x and y are nonzero; namely, if $2[(y_1-y_2)(x_2-x_3)-(y_2-y_3)(x_1-x_2)] \neq 0$ and $2[(x_1-x_2)(y_2-y_3)-(x_2-x_3)(y_1-y_2)] \neq 0$.

Consider the case that the denominator is 0:

$2[(y_1 - y_2)(x_2 - x_3) - (y_2 - y_3)(x_1 - x_2)] = 0$

$\implies (y_1 - y_2)(x_2 - x_3) - (y_2 - y_3)(x_1 - x_2) = 0$ Dividing by 2

$\implies (y_1 - y_2)(x_2 - x_3) = (y_2 - y_3)(x_1 - x_2)$

$\implies \frac{(y_1 - y_2)}{(x_1 - x_2)} = \frac{(y_2 - y_3)}{(x_2 - x_3)}$ Slopes of $\overline{P_1P_2}$ and $\overline{P_2P_3}$ are equal

Similarly,

$2[(x_1 - x_2)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_2)] = 0$

$\implies (x_1 - x_2)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_2) = 0$ Dividing by 2

$\implies \frac{(y_2 - y_3)}{(x_2 - x_3)} = \frac{(y_1 - y_2)}{(x_1 - x_2)}$ Slopes of $\overline{P_1P_2}$ and $\overline{P_2P_3}$ are equal

We have shown that when the denominators of both expressions are zero, the slopes of $\overline{P_1P_2}$ and $\overline{P_2P_3}$ are equal. Since both segments contain a common point P_2, this shows that in order for x and y to have invalid solutions, P_1, P_2, and P_3 must be collinear, a contradiction of the assumptions of Theorem 1.9.

It is important to note that for both of these cases we divide by (x_1-x_2) and (x_2-x_3). However, either of these quantities can be 0. Consequently, we must justify that when this happens the denominator is still nonzero. Note that if $x_1-x_2=0$, then $(y_1-y_2)(x_2-x_3)=(y_2-y_3)(x_1-x_2) \implies (y_1-y_2)(x_2-x_3)=0$. In order for this to be true, then either $y_1-y_2=0$ or $x_2-x_3=0$. If $y_1-y_2=0$, then $y_1=y_2$, which means that $P_1=P_2$, a contradiction. If $x_2-x_3=0$, then $x_1=x_2=x_3$, which means that the points are collinear, a contradiction. A similar situation occurs when $x_2-x_3=0$.

REMARK 3.2. The following verifies the uniqueness of our solution for C:

The point of intersection of two non parallel lines, defined by an arbitrary point (x,y), exists and is unique. Suppose $\exists$ two lines $y=m_1x+b_1$ and $y=m_2x+b_2$, where $m_1 \neq m_2$. We want to find the intersection of these two lines. Well, $m_1x+b_1=m_2x+b_2 \implies (m_1-m_2)x=b_2-b_1$. This gives a solution as long as the lines in question are not parallel to one another. $x=\dfrac{b_2-b_1}{m_1-m_2}$. By inserting this solution back into the equations for x, a solution for y can be obtained: $y=m_1\left(\dfrac{b_2-b_1}{m_1-m_2}\right)+b_1$ and $y=m_2\left(\dfrac{b_2-b_1}{m_1-m_2}\right)+b_2$. Rewriting these expressions gives $y=\dfrac{m_1b_2-m_1b_1+m_1b_1-m_2b_1}{m_1-m_2}$ and $y=\dfrac{m_2b_2-m_2b_1+m_1b_2-m_2b_2}{m_1-m_2}$ which reduce to the solution $y=\dfrac{m_1b_2-m_2b_1}{m_1-m_2}$. Thus, the intersection exists and is unique between two nonparallel lines.

4. Conclusion

We have proved directly that three noncolinear points, all of which are nonzero distance from each other, determine a unique circle of nonzero radius in $\mathbb{F}_q^2$ ($q=p^l$, $p>2$ is a prime, and $l \in \mathbb{N}$). Given three points which satisfy these conditions, it is possible to find the center of the circle they determine by finding the intersection of the perpendicular bisectors of two sets of the points. Using the definition of perpendicular bisector, it follows that this intersection is equidistant from all three points, showing that the intersection determines the center of a circle containing the three points. By the definition of a circle, deriving this center, showing it exists, and showing it is unique sufficiently demonstrates the existence of the circle containing the three points.

References

[1] Euclid. *The Elements Book IV*. Trans. Sir Thomas L. Heath. NewYork: Dover, 1956. Print. 1

[2] Gilbert, Jimmie, and Linda Gilbert. *Elements of Modern Algebra*. 6th ed. Belmont: Thomson Books/Cole, 2005. Print. 2