Int. J. Anal. Appl. (2025), 23:32

International Journal of Analysis and Applications

Arithmetic Relation Between Family of Elliptic Curves Over Finite Field

Haleemah Ghazwani*

Department of Mathematics, Science College, Jazan university, Saudi Arabia

**Corresponding author:* hqghazwani@jazanu.edu.sa

Abstract. Let $\mathbb{F}_q$ be a finite field, where q is an odd prime such that $q > 3$. Let $f(t) = t^3 - t \in \mathbb{F}_q[t]$ be a polynomial of degree 3. For $\lambda \neq 0$ in $\mathbb{F}_q$, consider families of elliptic curves $\{E_\lambda\}_{\lambda \in \mathbb{F}_q^*}$ and $\{H_\lambda\}_{\lambda \in \mathbb{F}_q^*}$ defined respectively by

$$v^2 = \lambda f(u) \text{ and } f(v) = \lambda f(u).$$

In this paper, I investigate the relation between the rational points over finite field on $\left\{E_\lambda\left(\mathbb{F}_q\right)\right\}_{\lambda \in \mathbb{F}_q^*}$ and $\left\{H_\lambda\left(\mathbb{F}_q\right)\right\}_{\lambda \in \mathbb{F}_q^*}$, and determine the number of rational points on both of these family of curves.

1. Introduction

The Legendre symbol [5] of a element $\alpha \in \mathbb{F}_q$ is given as:

$$\left(\frac{\alpha}{q}\right) \equiv \alpha^{\frac{q-1}{2}} mod q.$$

Definition 1.1. *[5] Let q be a prime number, an element $\alpha \in \mathbb{F}_q$ is called quadratic residue if there exists $\beta \in \mathbb{F}_q$ satisfies*

$$\beta^2 = \alpha.$$

If there is no such β, then α a quadratic non-residue.

The quadratic character of $\chi : \mathbb{F}_q \to \mathbb{C}$ for $\alpha \in \mathbb{F}_q$, is given as follows:

$$\chi(\alpha) = \begin{cases} 0, & \text{if } \alpha = 0, \\ +1, & \text{if } \left(\frac{\alpha}{q}\right) = 1, \\ -1, & \text{otherwise.} \end{cases}$$

Received: Nov. 28, 2024.

2020 *Mathematics Subject Classification.* 14H52, 14G05, 11L10.

Key words and phrases. elliptic curve; rational points; Jacobsthal sums.

https://doi.org/10.28924/2291-8639-23-2025-32

ISSN: 2291-8639

Corollary 1.1. *[1] Let α, β, γ be integers with an odd prime such that $q \nmid \alpha$, then*

$$\sum_{u=0}^{q-1}\left(\frac{\alpha u^2+\beta u+\gamma}{q}\right)=\begin{cases} -\left(\frac{\alpha}{q}\right) & \text{if } \beta^2-4\alpha c\equiv 0\ (modq),\\ (q-1)\left(\frac{\alpha}{q}\right), & \text{if } \beta^2-4\alpha c\not\equiv 0\ (modq).\end{cases}$$

Definition 1.2. *[1] If $\alpha \in \mathbb{F}_q$, the Jacobsthal sum $\phi_n(\alpha)$ is defined by*

$$\phi_n(\alpha)=\sum_{u\in\mathbb{F}_q}\chi(u)\,\chi(u^n+\alpha),$$

where n is a positive integer.

For a smooth projective curve C, the Riemann hypothesis over finite fields says

$$|N-(q+1)|\leq 2g\sqrt{q},$$

where N is the number of $\mathbb{F}_q$- rational points on C, and g is a genus of C.

Definition 1.3. *[7] For an odd prime, the number of solutions $(u,v)\in\mathbb{F}_q\times\mathbb{F}_q$ of quadratic polynomial $f(u)$ is given by*

$$\#\left\{(u,v)\in\mathbb{F}_q\times\mathbb{F}_q|v^2=f(u)\right\}=q+\sum_{u=0}^{q-1}\chi\left(f(u)\right).$$

Consider the projective curve $\mathcal{H}_\lambda$ defined by the equation homogeneous polynomial

$$F(u,v,z)=z^n f\left(\frac{v}{z}\right)-\lambda z^n f\left(\frac{u}{z}\right),\ \lambda^n\neq 1 \text{ and } \lambda\in\mathbb{F}_q^*.$$

Theorem 1.1. *[2] Let $\mathbb{F}_q$ be a finite field of characteristic q such that q does not divide n. The projective curve $\mathcal{H}_\lambda$ is non-singular at infinity.*

Definition 1.4. *[4] The genus of non-singular algebraic curve defined by a polynomial $F(u,v)$ of degree t is given by the formula*

$$g=\frac{1}{2}\left[(t-1)(t-2)\right].$$

2. Rational Points on a Family of Curves $v^2=\lambda f(u)$

Let $f(u)=u^3-u$ be a polynomial of degree 3 such that $u\in\mathbb{F}_q$, . Consider the elliptic curve E_λ which is defined by

$$F(u,v)=v^2-\lambda\left(u^3-u\right),\text{and },\lambda\in\mathbb{F}_q^*.$$

Let $E_\lambda\left(\mathbb{F}_q\right)$ denote the set of $\mathbb{F}_q-$rational points on the affine curve.

Theorem 2.1. *For $f(u)=u^3-u$, the number of rational points on the curve E_λ is given by*

$$\#E_\lambda\left(\mathbb{F}_q\right)=(q-3)+\chi(\lambda)\,\phi(-1)+3.$$

Proof. Let

$$S = \{(0,0), (\pm 1, 0)\},$$

be the set trivial rational points on a curve E_λ. Let $\#E_\lambda\left(\mathbb{F}_q\right)$ be the number of rational points $(u,v) \in \mathbb{F}_q \times \mathbb{F}_q$ of the congruence $v^2 = \lambda\left(u^3 - u\right) mod q$ and $u \neq 0, \pm 1$ which is given as follow,

$$\begin{aligned}
\#E_\lambda\left(\mathbb{F}_q\right) &= \sum_{u \in \mathbb{F}_q^*} \left(1 + \chi(\lambda)\chi\left(u^3 - u\right)\right) + \#S \\
&= \sum_{u \in \mathbb{F}_q^*} 1 + \sum_{u \in \mathbb{F}_q^*} \chi(\lambda)\chi\left(u^3 - u\right) + 3 \\
&= (q-3) + \chi(\lambda)\phi(-1) + 3.
\end{aligned}$$

□

Theorem 2.2. *Let $\{E_\lambda\}_{\lambda \in \mathbb{F}_q}$ be a family of elliptic curves, then $\#\left\{E_\lambda\left(\mathbb{F}_q\right)\right\}$ is given by*

$$\#\{E_\lambda\left(\mathbb{F}_q\right)\}_{\lambda \in \mathbb{F}_q^*} = (q-1)(q-3) + 3.$$

Proof. Consider the set

$$E_\lambda^*\left(\mathbb{F}_q\right) = \left\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q | v^2 = \lambda\left(u^3 - u\right), \lambda \in \mathbb{F}_q^*, v \neq 0\right\},$$

where $E_\lambda^*\left(\mathbb{F}_q\right) \cap E_\mu^*\left(\mathbb{F}_q\right) = \phi$ when $\lambda \neq \mu$. To prove this, assume $E_\lambda^*\left(\mathbb{F}_q\right) \cap E_\mu^*\left(\mathbb{F}_q\right) \neq \phi$ for $\lambda \neq \mu$, then there exists (α, β) that belongs to $E_\lambda\left(\mathbb{F}_q\right)$ and $E_\lambda\left(\mathbb{F}_q\right)$, so $\beta^2 = \lambda\left(\alpha^3 - \alpha\right)$ and $\beta^2 = \mu\left(\alpha^3 - \alpha\right)$, which implies either $\mu = \lambda$ or $\alpha = \pm 1$, a contradiction since $\lambda \neq \mu$ and $\beta \neq 0$.Let $QR\left(\mathbb{F}_q\right)$ be the collection of elements that are quadratic residues in $\mathbb{F}_q$, while $QNR\left(\mathbb{F}_q\right)$ is the the collection of elements that are quadratic non-residues in $\mathbb{F}_q$.

Consider the family of curves $\{E_\lambda\left(\mathbb{F}_q\right)\}_{\lambda \in \mathbb{F}_q^*}$, then

$$\begin{aligned}
\{E_\lambda\left(\mathbb{F}_q\right)\}_{\lambda \in \mathbb{F}_q^*} &= \bigcup_{\lambda \in \mathbb{F}_q^*} E_\lambda^*\left(\mathbb{F}_q\right) + S \\
\#\{E_\lambda\left(\mathbb{F}_q\right)\}_{\lambda \in \mathbb{F}_q^*} &= \sum_{\lambda \in \mathbb{F}_q^*} \#E_\lambda^*\left(\mathbb{F}_q\right) + \#S \\
&= \sum_{\lambda \in QR\left(\mathbb{F}_q\right)} \#E_\lambda^*\left(\mathbb{F}_q\right) + \sum_{\lambda \in QR\left(\mathbb{F}_q\right)} \#E_\lambda^*\left(\mathbb{F}_q\right) + \#S.
\end{aligned}$$

Moreover, by Theorem 2.1.

$$\begin{aligned}
&= \frac{q-1}{2}\left[(q-3) + \phi(-1)\right] + \frac{q-1}{2}\left[(q-3) - \phi(-1)\right] + 3 \\
&= \frac{q-1}{2}\left[(q-3) + \phi(-1) + (q-3) - \phi(-1)\right] + 3 \\
&= (q-1)(q-3) + 3.
\end{aligned}$$

□

3. Rational Points of the Curve $H_\lambda\left(\mathbb{F}_q\right)$

Consider the affine Holm curve [6] H_λ defined by $F(u,v) = f(v) - \lambda f(u)$

$$\begin{aligned} H_\lambda &: f(v) = \lambda f(u), \ \lambda \in \mathbb{F}_q^*, \\ H_\lambda &: v^3 - v = \lambda(u^3 - u), \ \lambda \in \mathbb{F}_q^*, \end{aligned}$$

and its projective model

$$\mathcal{H}_\lambda : v^3 - vz^2 = \lambda(u^3 - uz^2), \ \lambda \in \mathbb{F}_q^*,$$

By Theorem 1.1., $\mathcal{H}_\lambda$ has no singularity at infinity. In addition, by solving the system of equation $F_u = F_v = F_z = F = 0$, I obtain H_λ is non-singular curve, Moreover, by Definition 1.4., the genus of H_λ is one.

The following set

$$T = \{(0,0), (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)\},$$

of trivial points of cardinality 9 contained in the following set

$$H_\lambda\left(\mathbb{F}_q\right) = \left\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q : v^3 - v = \lambda\left(u^3 - u\right)\right\},$$

for each $\lambda \in \mathbb{F}_q^*$. Let $\#H_\lambda\left(\mathbb{F}_q\right)$ be the number of $\mathbb{F}_q$-rational points on the affine curve H_λ. Then by the Riemann Hypothesis over finite fields, I get

$$\left|\sum_{u=0}^{q-1} \chi\left(f(u)\right)\right| \leq 2\sqrt{q}.$$

Proposition 3.1. *For each $\lambda \in \mathbb{F}_q^*$,*

(1) $\#H_\lambda\left(\mathbb{F}_q\right) = \#H_\mu\left(\mathbb{F}_q\right)$, where λ is an additive inverse of λ.
(2) $\#H_\lambda\left(\mathbb{F}_q\right) = \#H_\mu\left(\mathbb{F}_q\right)$, where λ is an multiplicative inverse of λ.
(3) $\#H_1\left(\mathbb{F}_q\right) = \begin{cases} 2q+1 & q \equiv 1, 11 (mod 12), \\ 2q-1 & q \equiv 5, 7 (mod 12). \end{cases}$.

Proof. (1) Observe the map

$$G : H_\lambda\left(\mathbb{F}_q\right) \to H_\lambda\left(\mathbb{F}_q\right),$$

defined as $(\alpha, \beta) \to (-\alpha, \beta)$ is a bijective map. Hence, $\#H_\lambda\left(\mathbb{F}_q\right) = \#H_\mu\left(\mathbb{F}_q\right)$.

(2) Observe the map

$$G : H_\lambda\left(\mathbb{F}_q\right) \to H_\lambda\left(\mathbb{F}_q\right),$$

defined as $(\alpha, \beta) \to (\beta, \alpha)$ is a bijective map. Hence, $\#H_\lambda\left(\mathbb{F}_q\right) = \#H_\mu\left(\mathbb{F}_q\right)$.

(3) The curve $H_1\left(\mathbb{F}_q\right)$ is defined by the equation

$$\begin{aligned} v^3 - v - \left(u^3 - u\right) &= 0, \\ (v-u)\left(v^2 + uv + u^2\right) - (v-u) &= 0, \\ (v-u)(v^2 + uv + u^2 - 1) &= 0, \end{aligned}$$

if $(v-u)=0$, then $\#\{(u,v):u=v\}=q$. Otherwise, if $v^2+uv+u^2-1=0$, this leaves two cases:

Case 1: Let $u=v$, then $3u^2=1$, if $\chi(3)=+1$ this implies $\left(\frac{-1}{\sqrt{3}},\frac{-1}{\sqrt{3}}\right)$ and $\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right)$ belong to

$$\{(u,v):u=v\};$$

moreover, $\chi(3)=+1$ when $q\equiv 1,11(mod 12)$. Therefore,

$$\#\left\{(u,v);v^2+uv+u^2=1,u=v\right\}=\begin{cases}2 & q\equiv 1,11(mod 12),\\ 0 & q\equiv 5,7(mod 12).\end{cases}$$

Case 2: Let $v\neq u$. Dividing by v and putting $\beta=\frac{1}{v}$ and $\alpha=\frac{u}{v}$,

$$\{(\alpha,\beta)\in\mathbb{F}_q\times\mathbb{F}_q:\beta^2=\alpha^2+\alpha+1\},$$

then by Corollary 1.1.

$$\#\{(\alpha,\beta)\in\mathbb{F}_q\times\mathbb{F}_q:\beta^2=\alpha^2+\alpha+1\}=q-1.$$

Now, If $q\equiv 1,11(mod 12)$, then $\{(u,v):u=v\}\cap\left\{(u,v);v^2+uv+u^2=1\right\}=2$, therefore

$$\left\{(u,v);v^2+uv+u^2=1\right\}=\begin{cases}q-3 & q\equiv 1,11(mod 12),\\ q-1 & q\equiv 5,7(cmod 12).\end{cases}$$

Therefore, I conclude

$$\#H_1\left(\mathbb{F}_q\right)=\begin{cases}2q-3 & q\equiv 1,11(mod 12),\\ 2q-1 & q\equiv 5,7(mod 12).\end{cases}$$

□

4. Arithmetic Relation between $\{E_\lambda\}_{\lambda\in\mathbb{F}_q^*}$ and $\{H_\lambda\}_{\lambda\in\mathbb{F}_q^*}$

Throughout this section, I study the arithmetic relation between elliptic curves $\{E_\lambda\}_{\lambda\in\mathbb{F}_q^*}$ and $\{H_\lambda\}_{\lambda\in\mathbb{F}_q^*}$. Consider

$$\begin{aligned}E_\lambda\left(\mathbb{F}_q\right) &: \left\{(u,v)\in\mathbb{F}_q\times\mathbb{F}_q,v^2=\lambda f(u),\lambda\in\mathbb{F}_q^*\right\},\\ E_\lambda^*\left(\mathbb{F}_q\right) &: \left\{(u,v)\in\mathbb{F}_q\times\mathbb{F}_q,v^2=\lambda f(u),f(u)\neq 0,\lambda\in\mathbb{F}_q^*\right\}.\end{aligned}$$

And consider the sets

$$\begin{aligned}\Pi &= \left\{(q_1,q_2)\in E_\lambda^*\times E_\mu^*:q_1=(u_1,v_1),q_2=(u_2,v_2),v_1^2=v_2^2,\lambda\neq\mu\right\},\\ H_\lambda^*\left(\mathbb{F}_q\right) &= \left\{(u,v)\in\mathbb{F}_q\times\mathbb{F}_q:f(v)=\lambda f(u),f(v)\neq 0,f(u)\neq 0,\lambda\in\mathbb{F}_q^*\right\}.\end{aligned}$$

Moreover, since $f(u)\neq 0,u^3-u\neq 0$, then $u\neq 0,\pm 1$, which leads to $v\neq 0,\pm 1$. Now consider

$$\Pi^*=\Pi-\left\{(q_1,q_2)\in E_\lambda^*\times E_\mu^*:q_1=(u_1,\pm 1),q_2=(u_2,\pm 1)\right\}.$$

Theorem 4.1. *The arithmetic relation between two family of elliptic curves $\{H_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}_q^*}$ and $\{E_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\lambda\in\mathbb{F}_q^*}$ is given as follows*

$$\underset{(q_1,q_2)\mapsto(u_1,u_2)}{G:\Pi^*\to H_\lambda\left(\mathbb{F}_q\right).}$$

Proof. Let $(q_1, q_2) \in \Pi^*$, such that $q_1 = (\alpha_1, \beta_1) \in E^*_\lambda$, $q_2 = (\alpha_2, \beta_2) \in E^*_\mu$ where $\lambda \neq \mu$, I have proved that when $\lambda \neq \mu$, $E^*_\lambda \cap E^*_\mu = \phi$, then

$$\beta_1^2 = \lambda\left(\alpha_1^3 - \alpha_1\right), \beta_2^2 = \mu\left(\alpha_2^3 - \alpha_2\right), \text{ and } \beta_1^2 = \beta_1^2,$$

then the rational point (α_1, α_2) would be lying on the following curve

$$\left(\alpha_1^3 - \alpha_1\right) = \rho\left(\alpha_2^3 - \alpha_2\right), \text{ where } \rho = \frac{\mu}{\lambda}.$$

Conversely: suppose that $(\alpha_1, \alpha_2) \in H_\lambda\left(\mathbb{F}_q\right)$, *then*

$$\left(\alpha_1^3 - \alpha_1\right) = \lambda\left(\alpha_2^3 - \alpha_2\right),$$

this leaves two cases:

Case 1: If the curve $\left(\alpha_1^3 - \alpha_1\right) = \lambda\left(\alpha_2^3 - \alpha_2\right)$ is a quadratic equation, then there exists $\beta \in \mathbb{F}_q^*$ such that

$$\left(\alpha_1^3 - \alpha_1\right) = \lambda\left(\alpha_2^3 - \alpha_2\right) = \beta^2,$$

then, $(\alpha_1, \pm\beta) \in E^*_1\left(\mathbb{F}_q\right)$,and $(\alpha_2, \pm\beta) \in E^*_\mu\left(\mathbb{F}_q\right)$.

Case 2: If the curve $\left(\alpha_1^3 - \alpha_1\right) = \lambda\left(\alpha_2^3 - \alpha_2\right)$ is not a quadratic equation, then there exists $\rho \in \mathbb{F}_q^*\left(\mathbb{F}_q\right)$ such that

$$\rho\left(\alpha_1^3 - \alpha_1\right) = \rho\lambda\left(\alpha_2^3 - \alpha_2\right) = \beta^2.$$

Let $\rho\lambda = \mu$ then, $(\alpha_1, \pm\beta) \in E^*_\rho\left(\mathbb{F}_q\right)$ and $(\alpha_2, \pm\beta) \in E^*_\mu\left(\mathbb{F}_q\right)$. □

Theorem 4.2. *Let $\{H_\lambda\}_{\lambda\in\mathbb{F}_q^*}$ be a family of elliptic curves, then $\#\{H_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}_q^*}$ is given as follows*

$$\#\{H_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}_q^*} = (q-3)^2 + 9.$$

Proof. Consider the set

$$\begin{aligned} H_\lambda\left(\mathbb{F}_q\right) &= \left\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q : v^3 - v = \lambda\left(u^3 - u\right), \lambda \in \mathbb{F}_q^*\right\}, \\ H^*_\lambda\left(\mathbb{F}_q\right) &= \left\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q : v^3 - v = \lambda\left(u^3 - u\right), \lambda \in \mathbb{F}_q^*\right\} - T, \end{aligned}$$

where $H^*_\lambda\left(\mathbb{F}_q\right) \cap H^*_\lambda\left(\mathbb{F}_q\right) = \phi$ when $\lambda \neq \mu$. since $f(v) \neq 0$ and $f(u) \neq 0$, which implies $v \neq \pm 1$

$$\begin{aligned} \{H^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}_q} &= \bigcup_{\lambda\in\mathbb{F}_q} H^*_\lambda\left(\mathbb{F}_q\right) \\ \#\{H^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}_q} &= \sum_{\lambda\in\mathbb{F}_q} \#H^*_\lambda\left(\mathbb{F}_q\right) \\ &= \#\pi^* - \#\left\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q | v^2 = \lambda f(u), v = \pm 1\right\}. \end{aligned}$$

For a given $u_0 \in \mathbb{F}_q^*$ and $u_0 \neq \pm 1$, there are two points (u,v) on $E_\lambda\left(\mathbb{F}_q\right)$ with $u-$coordinate u_0; if $\lambda f(u_0)$ non-square in $\mathbb{F}_q$,

$$\begin{aligned} \#\{(u_0, v) \quad &: \quad (u_0, v) \in E_\lambda\left(\mathbb{F}_q\right)\} = 1 + \chi\left(\lambda f(u_0)\right) \\ &= 1 + \chi(\lambda)\, \phi(-1). \end{aligned}$$

The number of (u_0, v) on $\{E^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}^*_q}$

$$\begin{aligned}
\#\{(u_0, v) \quad : \quad (u_0, v) \in \{E^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}^*_q}\} &= \sum_{\lambda\in\mathbb{F}^*_q} 1 + \sum_{\lambda\in\mathbb{F}^*_q} \chi(\lambda)\,\phi(-1) \\
&= \sum_{\lambda\in\mathbb{F}^*_q} 1 + \phi(-1)\sum_{\lambda\in\mathbb{F}^*_q} \chi(\lambda) \\
&= (q-1) + \phi(-1)(0) \\
&= q-1.
\end{aligned}$$

So, there are $q-1$ of distinct rational points (u_0, v) for a given u_0. Now, for all over $u \in \mathbb{F}^*_q$ and $u \neq \pm 1$,

$$\#\pi^* = (q-3)(q-1).$$

Let C be the elliptic curve such that $v^2 = 1$, then $\lambda\left(u^3 - u\right) = 1$, so there are at most two points $(u, \pm 1) \in E^*_\lambda\left(\mathbb{F}_q\right)$ for each $\lambda \in \mathbb{F}^*_q$. By theorem 2.2 $\#\{E^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}^*_q} = (q-1)(q-3)$, then

$$\begin{aligned}
\#\left\{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q, \lambda\left(u^3 - u\right) = 1, \lambda \in \mathbb{F}^*_q\right\} &= 2\left[\frac{(q-1)(q-3)}{(q-1)}\right] \\
&= 2(q-3).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\#\{H^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}^*_q} &= \#\pi^* - \#\left\{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q | v^2 = \lambda f(u), v = \pm 1\right\} \\
\#\{H^*_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}^*_q} &= (q-3)(q-1) - 2(q-3) \\
&= (q-3)^2.
\end{aligned}$$

Moreover,

$$\#\{H_\lambda\left(\mathbb{F}_q\right)\}_{\lambda\in\mathbb{F}_q} = (q-3)^2 + 9.$$

□

5. Conclusion

In this paper, I have proved there is an arithmetic relation between families of elliptic curves $\{E_\lambda\}_{\lambda\in\mathbb{F}_q}$ and $\{H_\lambda\}_{\lambda\in\mathbb{F}_q}$ and calculated the number of rational points on each of $\{E_\lambda\}_{\lambda\in\mathbb{F}_q}$ and $\{H_\lambda\}_{\lambda\in\mathbb{F}_q}$.

Conflicts of Interest: The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley, New York, 1998.

[2] W. Fulton, R. Weiss, Algebraic Curves: An Introduction to Algebraic Geometry, Addison-Wesley Pub. Co., Redwood City, 2008.

[3] G.-M. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra: With Contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, Springer, 2008.

[4] H. Ghazwani, On the Genus of Holm's Curve over Finite Field, J. Algebra Appl. Math. 21 (2023), 1-16.

[5] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Cambridge University Press, 1996. https://doi.org/10.1017/CBO9780511525926.

[6] A. Rajan, F. Ramaroson, Ratios of Congruent Numbers, Acta Arith. 128 (2007), 101-106.

[7] L.C. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman and Hall/CRC, 2008. https://doi.org/10.1201/9781420071474.