Finite Fields and Their Applications 68 (2020) 101756



Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa



Orchards in elliptic curves over finite fields



R. Padmanabhan [a], Alok Shukla [b,*]

[a] *Department of Mathematics, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada*
[b] *Mathematical and Physical Sciences division, School of Arts and Sciences, Ahmedabad University, Central Campus, Navrangpura, Ahmedabad 380009, India*

ARTICLE INFO

Article history:
Received 2 March 2020
Received in revised form 31 August 2020
Accepted 2 September 2020
Available online 29 September 2020
Communicated by Neal Koblitz

MSC:
52C30
14Q05

Keywords:
Point-line arrangements
Orchard problem
Elliptic curves
Group law
Application of finite fields

ABSTRACT

Consider a set of n points on a plane. A line containing exactly 3 out of the n points is called a 3-rich line. The classical orchard problem asks for a configuration of the n points on the plane that maximizes the number of 3-rich lines. In this note, using the group law in elliptic curves over finite fields, we exhibit several (infinitely many) group models for orchards wherein the number of 3-rich lines agrees with the expected number given by Green-Tao (or, Burr, Grünbaum and Sloane) formula for the maximum number of lines. We also show, using elliptic curves over finite fields, that there exist infinitely many point-line configurations with the number of 3-rich lines exceeding the expected number given by Green-Tao formula by two, and this is the only other optimal possibility besides the case when the number of 3-rich lines agrees with the Green-Tao formula.

© 2020 Elsevier Inc. All rights reserved.

* Corresponding author.
E-mail addresses: padman@cc.umanitoba.ca (R. Padmanabhan), Alok.Shukla@ahduni.edu.in (A. Shukla).
URLs: http://home.cc.umanitoba.ca/~padman (R. Padmanabhan), https://ahduni.edu.in/alok-shukla (A. Shukla).

https://doi.org/10.1016/j.ffa.2020.101756
1071-5797/© 2020 Elsevier Inc. All rights reserved.

1. Introduction

Orchard problem has a rich history going back to 1821. Jackson posed this problem in a poetic style in his book, aptly entitled, "Rational Amusement for Winter Evenings ..." [4]. This problem was also posed by Sylvester in 1868 [11]. *The orchard problem* is to plant n trees in an orchard maximizing the number of possible rows which contain exactly three trees. Of course, trees can be considered as points on a plane and rows as lines. We say that a line is 3-rich if it contains exactly three points out of the n specified points. A (n,t)-arrangement is a set of n points and t 3-rich lines in the real projective plane. The classical orchard problem is to find an arrangement in the real projective plane with greatest number of 3-rich lines t for each given value of n. We say that (n,t) is optimal and $\mathcal{O}r(n) = t$, if t is the solution of the orchard problem for n points. Clearly, for 3 (also, 4) points there is only one 3-rich line possible, so arrangement $(3,1)$ (also, $(4,1)$) is optimal, and $\mathcal{O}r(3) = \mathcal{O}r(4) = 1$. Fig. 1 shows optimal arrangements $(5,2), (6,4), (7,6)$ and $(8,7)$.

Sylvester proved that $\mathcal{O}r(n) \geq \lfloor \frac{1}{6}(n-1)(n-2) \rfloor$, where, as noted earlier, $\mathcal{O}r(n)$ is the maximum number of 3-rich lines for n points. (Here, and in what follows, $\lfloor x \rfloor$ denotes the integer part of x.) Burr, Grünbaum and Sloane [1], discussed this problem in a paper in 1973, and proved that

$$\mathcal{O}r(n) \geq \lfloor n(n-3)/6 \rfloor + 1. \tag{1.1}$$

More recently, in 2013 Green and Tao solved the orchard problem for all but finitely many cases. More precisely, they have solved the orchard problem for such cases wherein the number of points n is greater than some sufficiently large constant.

Theorem 1 *(Green-Tao, [3]). Suppose that P is a finite set of n points in the plane. Suppose that $n \geq n_0$ for some sufficiently large absolute constant n_0. Then there are no more than $\lfloor n(n-3)/6 \rfloor + 1$ lines that are* 3-rich*, that is they contain precisely* 3 *points of P.*

In conjunction with (1.1), Green-Tao theorem shows that for all $n \geq n_0$,

$$\mathcal{O}r(n) = \lfloor n(n-3)/6 \rfloor + 1. \tag{1.2}$$

For brevity, we will call the bound given by Eq. (1.2), "Green-Tao" bound in the sequel. Although, it should more appropriately be addressed as "Burr, Grünbaum, Sloane, Green, Tao" bound owing to the result of Burr, Grünbaum and Sloane given in Eq. (1.1).

Since, every line cuts a cubic in three points, and four points on a cubic will never be collinear, cubic curves defined over real or complex numbers provide a natural tool to construct orchards. This has been done before, for example, by Burr, Grünbaum and Sloane [1] and Green-Tao [3] in obtaining their results described earlier.

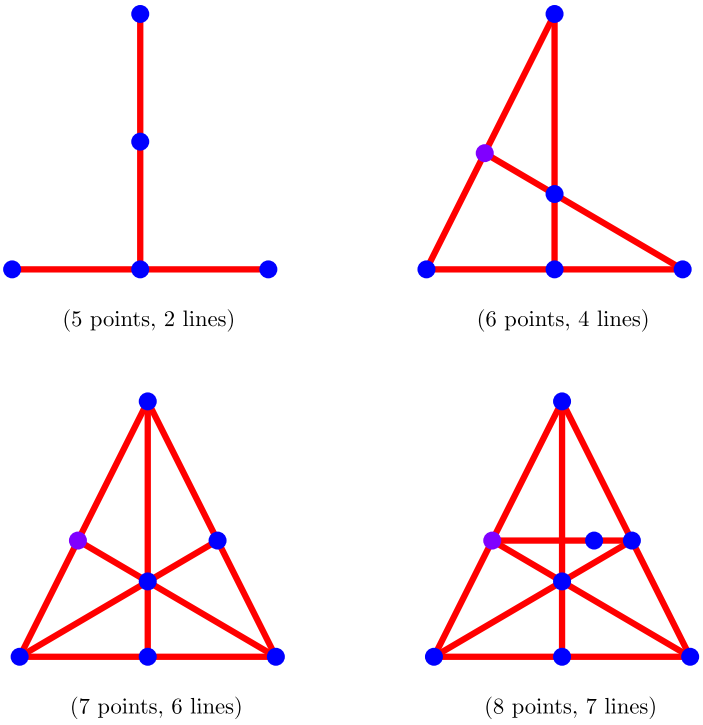


Fig. 1. Examples of optimal (p, t) arrangements for the orchard problem for $5 \leq p \leq 8$.

In this note, we give analogs of the classical orchard problem, by changing the 'ground plane' of orchards from a real projective plane to a projective plane defined over a finite field.

Orchard problem over finite fields: Consider a set of N points in a projective plane defined over a finite field. Find an optimal configuration of the given N points, such that the number of 3-rich lines is maximum.

Notation: In the sequel, by a slight abuse of notation, the number of 3-rich lines in an optimal configuration for the orchard problem over finite fields will also be denoted by $\mathcal{O}r(N)$. The finite field with q elements will be denoted by $\mathbb{F}_q$, where $q = p^n$ for some prime p and some positive integer n. For an elliptic curve E given by a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ defined over a field K, $E(K)$ will denote the set $\{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$.

Certain elliptic curves defined over finite fields will be used to obtain concrete group models for the orchards (N, t). In these group models, three points P, Q, R form a 3-rich line, if and only if, $P + Q + R = O$ in the underlying group structure. This enables one to count the number of lines and we give infinite families of examples using both ordinary and supersingular elliptic curves over finite fields wherein the Green-Tao bounds (see

(1.2)) are attained. Also, we show that there is just one other possibility, which also occurs infinitely many times, that the Green-Tao bounds are exceeded by two 3-rich lines.

Next we consider a numerical example to illustrate how the orchard problem can be treated on an elliptic curve over a finite field.

Example (6 points, 4 lines) Consider the elliptic curve E given by a minimal Weierstrass equation $y^2 = x^3 + 3$ over $\mathbb{F}_5$. It can be verified that $\#E(\mathbb{F}_5) = 6$ and $E(\mathbb{F}_5)$ contains the following points:

$$A = (1,2), \quad B = (1,8), \quad C = (2,1),$$
$$D = (2,4), \quad E = (3,0), \quad O = (0,1,0) \text{ (the point at infinity).}$$

The following four 3-rich lines could be formed using the points in $E(\mathbb{F}_5)$ (see Fig. 2):

$$\begin{aligned} l_1 &: \quad \text{containing} \quad \{O, A, B\}, \\ l_2 &: \quad \text{containing} \quad \{O, C, D\}, \\ l_3 &: \quad \text{containing} \quad \{A, C, E\}, \\ l_4 &: \quad \text{containing} \quad \{B, D, E\}. \end{aligned}$$

It can be verified that $E(\mathbb{F}_5) \cong \mathbb{Z}_6$ and $A = (1,2)$ is a generator of the group. It can be verified that all the points above lie on the elliptic curve $y^2 + 5xy - 15y = x^3 - 10x^2 + 35x - 42$, which is $y^2 = x^3 + 3 \mod 5$.

Now we give a brief organization of the paper. In the next section, i.e. Sect. 2, some important results on elliptic curves over finite fields will be reviewed. In Sect. 3 our main results are proved. Finally, in Sect. 4 we discuss some numerical examples and the question of realizability of our solutions on a real projective plane.

2. Elliptic curves over finite fields

The main purpose of this section is to collect some known structural results on elliptic curves over finite fields for later uses. Readers are referred to standard textbooks, such as [10] or [12], for details on the material related to this section.

An *elliptic curve* over a field K is a smooth cubic curve of genus one with a specified basepoint $O \in E(K)$. It is a consequence of Riemann-Roch theorem that every elliptic curve E/K can be given by an explicit Weierstrass equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with $a_i \in K$, and the extra point $[0,1,0]$ at infinity. If characteristic of K is not 2 or 3 one can always write equation of an elliptic curve in the following minimal Weierstrass form

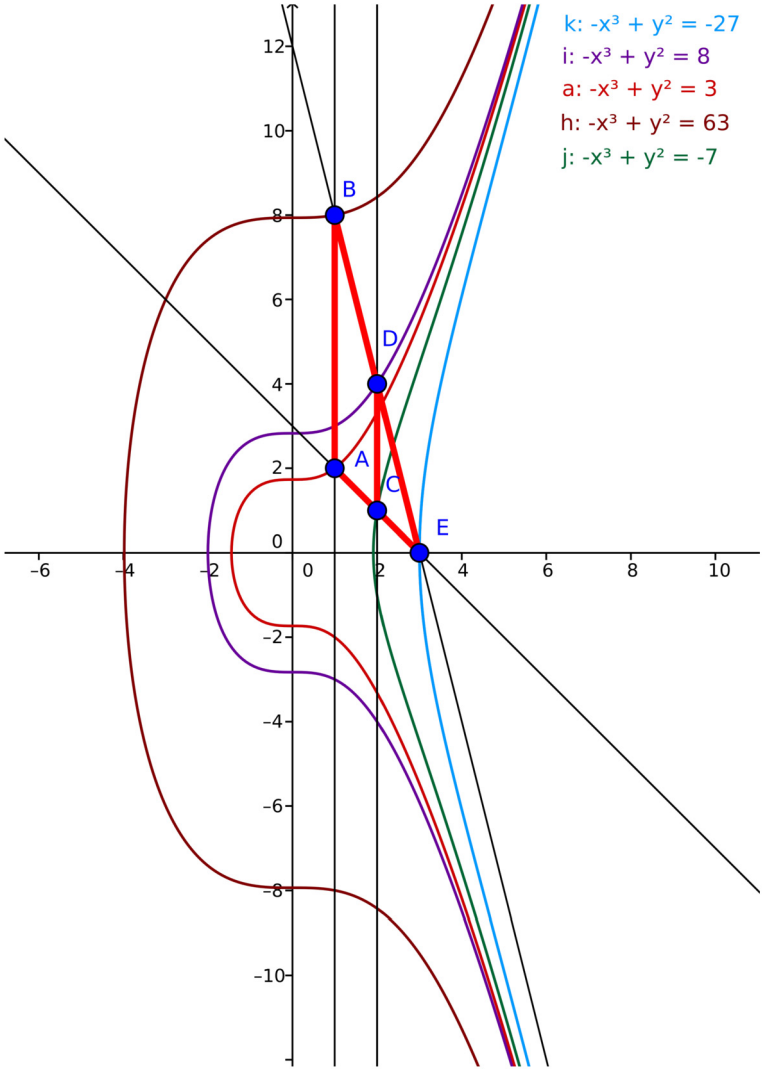


Fig. 2. Orchard configuration with (6 points, 4 lines) using elliptic curve given by a minimal Weierstrass equation $y^2 = x^3 + 3$ over $\mathbb{F}_5$. Note that all the five elliptic curves shown in the figure reduce to $y^2 = x^3 + 3$ modulo 5.

$$E : y^2 = x^3 + Ax + B, \tag{2.1}$$

with the discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$. Here the condition $\Delta \neq 0$ ensures that the elliptic curve is non-singular with no-repeated roots (equivalently, the partial derivatives do not vanish simultaneously for any point on E), which geometrically means the curve has no cusps or nodes (self-intersections). For an elliptic curve E there is an important invariant, called j-invariant which is defined as $j(E) = 1728\dfrac{4A^3}{4A^3 + 27B^2}$. Two elliptic curves defined over a field K and having the same j-invariant are isomorphic over

$\bar{K}$, where $\bar{K}$ is the algebraic closure of the ground field K. An elliptic curve is equipped with an abelian group structure and the group law is such that three points P, Q and R in $E(K)$ are collinear if and only if $P + Q + R = O$, with O being the identity element of the group, i.e., the point at infinity $(0, 1, 0)$.

An *isogeny* between E_1/K and E_2/K is a non-constant morphism $\phi\colon E_1 \to E_2$ defined over K such that $\phi(O_{E_1}) = O_{E_2}$. (I.e., ϕ is a morphism of curves given by rational functions with coefficients in K, which respects identity.) Elliptic curves E_1 and E_2 are called isogenous if there exists an isogeny $\phi\colon E_1 \to E_2$. Endomorphism ring of E/K, $\mathrm{End}_K(E)$ (or $\mathrm{End}(E)$, to ease notation) consists of all the isogenies $\phi\colon E \to E$, with natural addition and multiplication given by composition. For any integer m, there is a natural definition of an isogeny *multiplication by* m given as $[m] : E \to E$, with $[m]P = mP$. The kernel of the isogeny $[m]$ is denoted by $E[m]$ (i.e., $E[m] = \{P \in E \mid mP = 0\}$), and it is called the *m-torsion subgroup* of E.

Mordell proved that the group of rational points $E(Q)$ is finitely generated. Moreover, over a finite field $E(\mathbb{F}_q)$ is a finite abelian group of order $\#E(\mathbb{F}_q)$, where a bound for $\#E(\mathbb{F}_q)$ is given by Hasse's theorem.

Theorem 2 *(Hasse).*

$$\textit{Let } \#E(\mathbb{F}_q) = q + 1 - t. \textit{ Then } |t| \leq 2\sqrt{q}. \tag{2.2}$$

Next, we note a formula to determine the number $\#E(\mathbb{F}_q)$.

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right), \tag{2.3}$$

where $\left(\frac{x}{\mathbb{F}_q}\right)$ is the generalized Legendre symbol which takes the value 1 if x is a square in $\mathbb{F}_q^\times$, and -1 if x is not a square in $\mathbb{F}_q^\times$, otherwise, it takes the value 0 if $x = 0$.

Theorem 3 *(Deuring, [2]). Let E be an elliptic curve over the finite field $\mathbb{F}_q$. For each integer $m \geq 1$, let $\phi_m\colon E \to E^{(p^m)}$ and $\hat{\phi}_m\colon E^{(p^m)} \to E$ be the p^m-Frobenius map and its dual respectively. Then the following are equivalent.*

1. $E[p^m] = 0$ *for one (all)* $m \geq 1$.
2. $\mathrm{End}(E)$ *is an order in a quaternion algebra.*
3. $\hat{\phi}_m$ *is (purely) inseparable for one (all)* $m \geq 1$.
4. *The map* $[p]\colon E \to E$ *is purely inseparable and* $j(E) \in \mathbb{F}_{p^2}$.

Definition 1. An elliptic curve $E/\mathbb{F}_q$ is called supersingular if it satisfies any of the equivalent conditions given in Theorem 3. Otherwise, it is called an ordinary elliptic curve.

Another characterization of supersingular curves is that a curve is supersingular if and only if $t \equiv 0 \mod p$, where $\#E(\mathbb{F}_q) = q + 1 - t$.

The next result describes all the possible values of $\#E(q^n)$ that one can get by varying E over all the elliptic curves over $\mathbb{F}_q$.

Theorem 4 *(Schoof, [9]). Let $q = p^n$. There exists an elliptic curve $E/\mathbb{F}_q$ of order $q+1-t$ if and only if one of the following condition holds:*

1. *$t \not\equiv 0 \mod p$, and $t^2 \leq 4q$.*
2. *n is odd and one of the following holds:*
   - *$t = 0$.*
   - *$t^2 = 2q$, and $p = 2$.*
   - *$t^2 = 3q$, and $p = 3$.*
3. *n is even and one of the following holds:*
   - *$t^2 = 4q$.*
   - *$t^2 = q$ and $p \not\equiv 1 \mod 3$.*
   - *$t = 0$, and $p \equiv 1 \mod 4$.*

Corollary 1 *(of Theorem 4). Let E be as in Theorem 4. Then E is supersingular if and only if $t^2 = 0$, q, $2q$, $3q$, or $4q$.*

Theorem 5 *(Rück, [8]). Let $N = q + 1 - t$ such that it occurs as an order of an elliptic curve over $\mathbb{F}_q$. Let $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$, and $n_1 | n_2$ (possibly $n_1 = 1$). There is an elliptic curve $E/\mathbb{F}_q$ such that*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \tag{2.4}$$

if and only if

1. *$n_1 = n_2$ in the case n is even and $t^2 = 4q$ of Theorem 4.*
2. *$n_1 | q - 1$ in all other cases of Theorem 4.*

In view of Corollary 1 the following theorem characterizes the possible group structures of supersingular elliptic curves $E(\mathbb{F}_q)$.

Theorem 6 *(Schoof, [9]). Let $\#E(\mathbb{F}_q) = q + 1 - t$.*

1. *If $t^2 = q$, $2q$, or $3q$, then $E(\mathbb{F}_q)$ is cyclic.*
2. *If $t^2 = 4q$, then $E(\mathbb{F}_q)$ is of the form of $\mathbb{Z}_m \oplus \mathbb{Z}_m$ with $m = \sqrt{q} - 1$ if $t = 2\sqrt{q}$, otherwise if $t = -2\sqrt{q}$ then $m = \sqrt{q} + 1$.*
3. *If $t = 0$ and $q \not\equiv 3 \mod 4$, then $E(\mathbb{F}_q)$ is cyclic. If $t = 0$ and $q \equiv 3 \mod 4$, then either $E(\mathbb{F}_q)$ is cyclic, or $E(\mathbb{F}_q) \cong \mathbb{Z}_m \oplus \mathbb{Z}_2$, with $m = \frac{q+1}{2}$.*

Table 1
Elliptic curves over $\mathbb{F}_{2^n}$, where n is odd (see [5]).

Curve over 2^n	n	Order	Group
$y^2+y=x^3$	odd	$q+1$	cyclic
$y^2+y=x^3+x$	$n\equiv 1,7 \mod 8$	$q+1+\sqrt{2q}$	cyclic
	$n\equiv 3,5 \mod 8$	$q+1-\sqrt{2q}$	cyclic
$y^2+y=x^3+x+1$	$n\equiv 1,7 \mod 8$	$q+1-\sqrt{2q}$	cyclic
	$n\equiv 3,5 \mod 8$	$q+1+\sqrt{2q}$	cyclic

Table 2
Elliptic curves over $\mathbb{F}_{2^n}$, where n is even (see [5]).

Curve over 2^n	n	Order	Group
$y^2+y=x^3+\delta x$	even	$q+1$	cyclic
$y^2+\gamma y=x^3$	$n\equiv 0 \mod 4$	$q+1+\sqrt{q}$	cyclic
	$n\equiv 2 \mod 4$	$q+1-\sqrt{q}$	cyclic
$y^2+\gamma y=x^3+\alpha$	$n\equiv 0 \mod 4$	$q+1-\sqrt{q}$	cyclic
	$n\equiv 2 \mod 4$	$q+1+\sqrt{q}$	cyclic
$y^2+\gamma^2 y=x^3$	$n\equiv 0 \mod 4$	$q+1+\sqrt{q}$	cyclic
	$n\equiv 2 \mod 4$	$q+1-\sqrt{q}$	cyclic
$y^2+\gamma^2 y=x^3+\beta$	$n\equiv 0 \mod 4$	$q+1-\sqrt{q}$	cyclic
	$n\equiv 2 \mod 4$	$q+1+\sqrt{q}$	cyclic
$y^2+y=x^3$	$n\equiv 0 \mod 4$	$q+1-\sqrt{2q}$	$\mathbb{Z}_{\sqrt{q}-1}\oplus\mathbb{Z}_{\sqrt{q}-1}$
	$n\equiv 2 \mod 4$	$q+1+\sqrt{2q}$	$\mathbb{Z}_{\sqrt{q}+1}\oplus\mathbb{Z}_{\sqrt{q}+1}$
$y^2+y=x^3+\omega$	$n\equiv 0 \mod 4$	$q+1+\sqrt{2q}$	$\mathbb{Z}_{\sqrt{q}+1}\oplus\mathbb{Z}_{\sqrt{q}+1}$
	$n\equiv 2 \mod 4$	$q+1-\sqrt{2q}$	$\mathbb{Z}_{\sqrt{q}-1}\oplus\mathbb{Z}_{\sqrt{q}-1}$

The following theorem gives a simple method for determining whether an elliptic curve is supersingular.

Theorem 7 *(Deuring, [2]). Let $p>2$. The elliptic curve E over $\mathbb{F}_q$, with Weierstrass equation $y^2=f(x)$, is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$ is* 0.

Next, for a finite field with even characteristic we have the following results taken from [5] and listed in Table 1 and Table 2. For $q=2^n$, a representative curve $E/\mathbb{F}_q$ from each of the isomorphism classes of supersingular curve over $\mathbb{F}_q$ is listed. The order and the group structure of $E(\mathbb{F}_q)$ is also listed along with the curve for both the case when n is odd (see Table 1) and n even (see Table 2).

In order to use supersingular elliptic curves and their group structure to solve the orchard problem on a projective plane over $\mathbb{F}_q$, we consider some representative supersingular elliptic curves. The results of the following lemma are well-known.

Lemma 1.

1. *Let q be odd and $q\equiv 2 \mod 3$. Let the elliptic curve $E\colon y^2=x^3+b$ be defined over $\mathbb{F}_q$, with $b\in\mathbb{F}_q^{\times}$. Then $E(\mathbb{F}_q)\cong\mathbb{Z}_{q+1}$.*

2. *Let* $q \equiv 3 \mod 4$. *Let the elliptic curve* $E\colon y^2 = x^3 - x$ *be defined over* $\mathbb{F}_q$. *Then* $E(\mathbb{F}_q) \cong \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$.
3. *Let* $q \equiv 3 \mod 4$. *Let the elliptic curve* $E\colon y^2 = x^3 + x$ *be defined over* $\mathbb{F}_q$. *Then* $E(\mathbb{F}_q) \cong \mathbb{Z}_{q+1}$.

Proof.

1. See Prop. 4.33, [12], Chap. V, Example 4.4, [10], and Example 2.17, [6].
2. See Example 2.18, [6].
3. See Example 2.18, [6]. □

As a side remark, we note that recently supersingular elliptic curves have found applications in cryptography. For example, the supersingular elliptic curve $y^2 = x^3 + 7$ is used in Bitcoin's public-key cryptography.

3. Orchard problem using elliptic curves over finite fields

Next we prove a lemma which will be essential for proving our main result.

Lemma 2. *Let* G *be a finite abelian group, such that* $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3} \oplus \cdots \mathbb{Z}_{n_k}$, *with* $n_i | n_{i+1}$ *for* $i = 1, 2, 3, \cdots k-1$. *If* $3 | n_k$, *then let* j *with* $1 \leq j \leq k$ *be the smallest index such that* $3 | n_j$, *i.e.,* j *is such that* $3 | n_j$ *but* $3 \nmid n_{j-1}$ *(with* $n_0 = 1$*). Let*

$$\Psi(G) = \begin{cases} 0 & \text{if } 3 \nmid n_k, \\ k - j & \text{if } 3 | n_j, 3 \nmid n_{j-1}. \end{cases} \tag{3.1}$$

Then the number of distinct solutions (where order does not matter) of $x + y + z = 0$ *in* G *is*

$$\frac{1}{6}\left(\left(\prod_{i=1}^{k} n_i^2\right) - 3\left(\prod_{i=1}^{k} n_i\right) + 2(3)^{\Psi(G)}\right). \tag{3.2}$$

Proof. Let $x = (\alpha_1, \alpha_2, \cdots \alpha_k)$, $y = (\beta_1, \beta_2, \cdots \beta_k)$, and $z = (\gamma_1, \gamma_2, \cdots \gamma_k)$, with $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_{n_i}$. Now $x + y + z = 0$ in $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3} \oplus \cdots \mathbb{Z}_{n_k}$ if and only if

$$\alpha_i + \beta_i + \gamma_i = 0 \qquad \text{in } \mathbb{Z}_{n_i}, \quad \text{for } i = 1, 2, 3, \cdots k. \tag{3.3}$$

In (3.3) α_i and β_i both can take n_i different values and corresponding to each of the pairs (α_i, β_i) there is a unique γ_i, giving n_i^2 solutions to $\alpha_i + \beta_i + \gamma_i = 0$, including solutions with α_i, β_i and γ_i non-distinct. Varying i from 1 to k yields $\prod_{i=1}^{k} n_i^2$ such solutions. Next in order to get distinct solutions, $\prod_{i=1}^{k} 3n_i$ needs to be subtracted, since for each of the cases $\alpha_i = \beta_i$, $\beta_i = \gamma_i$ and $\gamma_i = \alpha_i$, for $i = 1$ to k, there are $\prod_{i=1}^{k} n_i$ solutions; and to this twice the number of solution when $\alpha_i = \beta_i = \gamma_i$, for $i = 1$ to k, should be added.

Next we compute the number of solutions in case when $\alpha_i = \beta_i = \gamma_i$, for $i = 1$ to k. If $\alpha_i = \beta_i = \gamma_i$ and $3 \nmid n_i$, then there is a unique solution to $\alpha_i + \beta_i + \gamma_i = 0$, namely $\alpha_i = \beta_i = \gamma_i = 0$; otherwise if $3|n_i$, then there are 3 different solutions to $\alpha_i+\beta_i+\gamma_i = 0$, namely $\alpha_i = \beta_i = \gamma_i = 0, \frac{n_i}{3}$ and $\frac{2n_i}{3}$. Using this observation it is easy to see that as i varies form 1 to k, there are total $3^{\Psi(G)}$ such solutions.

Therefore, we obtain total

$$\left(\left(\prod_{i=1}^{k} n_i^2\right) - 3\left(\prod_{i=1}^{k} n_i\right) + 2(3)^{\Psi(G)}\right)$$

solutions, which should be divided by $3! = 6$ to obtain the total number of distinct solutions to (3.3) where order does not matter. □

As immediate corollaries to Lemma 2, we obtain the following results.

Corollary 2. *The number of distinct solutions (up to ordering) of $x + y + z = 0$ in $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, with $n_1|n_2$, is*

$$\begin{cases} \frac{n_1^2n_2^2-3n_1n_2+18}{6} & \text{if } 3|n_1, \\ \frac{n_1^2n_2^2-3n_1n_2+2}{6} & \text{if } 3 \nmid n_1, \\ \frac{n_1^2n_2^2-3n_1n_2+6}{6} & \text{if } 3 \nmid n_1, 3|n_2, \end{cases} = \begin{cases} \lfloor \frac{N(N-3)}{6} \rfloor + 3 & \text{if } 3|N, \\ \lfloor \frac{N(N-3)}{6} \rfloor + 1 & \text{if } 3 \nmid N, \end{cases}$$

where $N = n_1n_2$.

Corollary 3. *The number of distinct solutions (up to ordering) of $x+y+z = 0$ in $\mathbb{Z}_m \oplus \mathbb{Z}_m$ is*

$$\begin{cases} \frac{m^4-3m^2+18}{6} & \text{if } 3|m, \\ \frac{m^4-3m^2+2}{6} & \text{if } 3 \nmid m, \end{cases} = \begin{cases} \lfloor \frac{N(N-3)}{6} \rfloor + 3 & \text{if } 3|N, \\ \lfloor \frac{N(N-3)}{6} \rfloor + 1 & \text{if } 3 \nmid N, \end{cases}$$

where $N = m^2$.

Corollary 4. *The number of distinct solutions (up to ordering) of $x + y + z = 0$ in $\mathbb{Z}_N$ is*

$$\begin{cases} \frac{N^2-3N+6}{6} & \text{if } 3|N, \\ \frac{N^2-3N+2}{6} & \text{if } 3 \nmid N, \end{cases} = \left\{ \lfloor \frac{N(N-3)}{6} \rfloor + 1. \right.$$

Theorem 8. *Assume $\mathbb{F}_q$ to be a finite field of odd characteristic, with $q = p^n$.*

1. *Let $q \equiv 3 \mod 4$. There exist point-line arrangements $(N, \lfloor \frac{N(N-3)}{6} \rfloor + 1)$, with $N = q + 1$, in the projective plane over the finite field $\mathbb{F}_q$ with group models $\mathbb{Z}_{q+1}$ and $\mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$.*

2. *Let n be odd and $q \not\equiv 3 \mod 4$, or let n be even and $p \not\equiv 3 \mod 4$. There exists a point-line arrangement $(N, \lfloor \frac{N(N-3)}{6} \rfloor + 1)$, with $N = q+1$, in the projective plane over the finite field $\mathbb{F}_q$ with the group model $\mathbb{Z}_{q+1}$.*

In all the cases above

$$\mathcal{O}r(N) \geq \lfloor \frac{N(N-3)}{6} \rfloor + 1, \tag{3.4}$$

with $N = q+1$.

Proof.

1. Let $q \equiv 3 \mod 4$. Let $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 + x$ be elliptic curves defined over $\mathbb{F}_q$. Then from Lemma 1 we have $E_1(\mathbb{F}_q) \cong \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$, and $E_2(\mathbb{F}_q) \cong \mathbb{Z}_{q+1}$.
First, we consider $q+1$ points on $E_1(\mathbb{F}_q)$. Let $m = \frac{q+1}{2}$. It is given that $q \equiv 3 \mod 4$, so $2|m$. Since, $E_1(\mathbb{F}_q) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{\frac{q+1}{2}}$, there exist points P and Q in $E_1(\mathbb{F}_q)$ such that $2P = O$ and $mQ = O$, where O is the point at infinity. The three distinct points $A_i = \alpha_i P + \beta_i Q$, with $\alpha_i \in \mathbb{Z}_2, \beta_i \in \mathbb{Z}_m$, for $i = 1, 2, 3$, are collinear if and only if

$$\sum_{i=1}^{3} \alpha_i P + \beta_i Q = O \iff \alpha_1 + \alpha_2 + \alpha_3 = 0 \mod 2,$$
$$\text{and } \beta_1 + \beta_2 + \beta_3 = 0 \mod m. \tag{3.5}$$

Therefore, finding the number of 3-rich lines is equivalent to finding the number of distinct solutions (up to ordering) to the equation $x + y + z = 0$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_m$. Now the result follows from Corollary 2, with $n_1 = 2$ and $n_2 = m = \frac{q+1}{2}$.
Next we consider $q+1$ points on $E_2(\mathbb{F}_q) \cong \mathbb{Z}_{q+1}$. Let P be a generator of the underlying group of $E_2(\mathbb{F}_q)$. Let points $P_i \in E_2(\mathbb{F}_q)$, for $i = 1, 2, 3$. Then $P_1 = xP$, $P_2 = yP$ and $P_3 = zP$ for some $x, y, z \in \mathbb{Z}_{q+1}$. Clearly, P_1, P_2 and P_3 are collinear if and only if

$$P_1 + P_2 + P_3 = O \iff xP + yP + zP = O \iff x + y + z = 0 \mod q+1. \tag{3.6}$$

Therefore, the number of 3-rich lines is equal to the number of solutions of the equation $x + y + z = 0$ in $\mathbb{Z}_{q+1}$. Now, the result follows from Corollary 4, with $N = q+1$.
2. Let $q = p^n$ with n odd. Then from Theorem 4 there exist an elliptic curve such that $\#E(\mathbb{F}_q) = q+1$, i.e., $t = 0$ in Theorem 4. Then Theorem 6 implies that $F_{\mathbb{F}_q} \cong \mathbb{Z}_{q+1}$, as $q \not\equiv 3 \mod 4$. On the other hand, if $q = p^n$ with n even, then from Theorem 4 it follows that there exists an elliptic curve such that $\#E(\mathbb{F}_q) = q+1$ if and only if $p \equiv 1 \mod 4$. Once again, Theorem 6 implies that $F_{\mathbb{F}_q} \cong \mathbb{Z}_{q+1}$. Now the proof proceeds similar to the proof of part (1). □

Theorem 9. *Assume $\mathbb{F}_q$ to be a finite field with $q = 2^n$.*

1. *Let $q = 2^n$ with n odd. There exists a point-line arrangement $(N, \lfloor (N)(N-3)/6 \rfloor + 1)$ in the projective plane over the finite field $\mathbb{F}_q$ with the group model $\mathbb{Z}_N$ for each of the following values of N*
   (a) $N = q + 1$,
   (b) $N = q + 1 + \sqrt{2q}$,
   (c) $N = q + 1 - \sqrt{2q}$.
2. *Let $q = 2^n$ with n even. There exists a point-line arrangement $(N, \lfloor (N)(N-3)/6 \rfloor + 1)$ in the projective plane over the finite field $\mathbb{F}_q$ with the group models $\mathbb{Z}_N$ for $N = q+1$ and for $N = q + 1 \pm \sqrt{q}$.*
   For both the cases (1) and (2),

$$\mathcal{O}r(N) \geq \lfloor \frac{N(N-3)}{6} \rfloor + 1, \tag{3.7}$$

and it agrees with the Green-Tao bound.

Proof. From Table 1 one can pick the elliptic curves $y^2 + y = x^3$, $y^2 + y = x^3 + x$ and $y^2 + y = x^3 + x + 1$ to get the desired group models. Then the number of 3-rich lines can be calculated using Corollaries to Lemma 2, similar to the calculation carried out in Theorem 8. This proves part (1) of the theorem. Similarly, part (2) of the theorem follows from Table 2. □

Theorem 10. *Let $N = q + 1 + 2\sqrt{q}$ with either q odd or $q = 2^n$ with n even. There exist point-line arrangements (N, t) in the projective plane over the finite field $\mathbb{F}_q$ with*

1. *the group model $\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ for $N = q + 1 - 2\sqrt{q}$, and*

$$t = \begin{cases} \frac{1}{6}\left(q^2 - 4q^{\frac{3}{2}} + 3q + 2\sqrt{q} + 16\right), & \text{if } \sqrt{q} \equiv 1 \mod 3, \\ \frac{1}{6}\left(q^2 - 4q^{\frac{3}{2}} + 3q + 2\sqrt{q}\right), & \text{if } \sqrt{q} \not\equiv 1 \mod 3; \end{cases}$$

2. *the group model $\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$ for $N = q + 1 + 2\sqrt{q}$, and*

$$t = \begin{cases} \frac{1}{6}\left(q^2 + 4q^{\frac{3}{2}} + 3q - 2\sqrt{q} + 16\right), & \text{if } \sqrt{q} \equiv 1 \mod 3, \\ \frac{1}{6}\left(q^2 + 4q^{\frac{3}{2}} + 3q - 2\sqrt{q}\right), & \text{if } \sqrt{q} \not\equiv 1 \mod 3, \end{cases}$$

with

$$\mathcal{O}r(N) \geq \begin{cases} \lfloor \frac{N(N-3)}{6} \rfloor + 3 & \text{if } 3|N, \quad \textit{(Green-Tao bound is exceeded.)} \\ \lfloor \frac{N(N-3)}{6} \rfloor + 1 & \text{if } 3 \nmid N. \end{cases} \tag{3.8}$$

Table 3
Examples.

Curve	q	Group	N	t	Green-Tao bound
$y^2 + y = x^3 + x$	8	$\mathbb{Z}_5$	5	2	2
$y^2 + y = x^3 + x$	128	$\mathbb{Z}_{145}$	145	3432	3432
$y^2 = x^3 + 1$	5	$\mathbb{Z}_6$	6	4	4
$y^2 = x^3 + 1$	49	$\mathbb{Z}_{48}$	48	361	361
$y^2 = x^3 + x$	7	$\mathbb{Z}_8$	8	7	7
$y^2 = x^3 + x$	13	$\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$	20	57	57
$y^2 + y = x^3 - x^2 - 10x - 20$	19	$\mathbb{Z}_{20}$	20	57	57
$y^2 + y = x^3$	4	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	9	12	10
$y^2 + y = x^3$	16	$\mathbb{Z}_9 \oplus \mathbb{Z}_9$	81	1056	1054
$y^2 + y = x^3$	256	$\mathbb{Z}_{15} \oplus \mathbb{Z}_{15}$	225	8328	8326
$y^2 = x^3 + 1$	25	$\mathbb{Z}_6 \oplus \mathbb{Z}_6$	36	201	199
$y^2 = x^3 + 1$	7	$\mathbb{Z}_2 \oplus \mathbb{Z}_6$	12	19	19

Proof. The proof is very similar to the previous Theorem and follows from Table 1 and Table 2. We omit the details. □

Theorem 11. *Assume $|t| \leq 2\sqrt{p}$. Let $N = p + 1 + t$ such that $N = n_1 n_2$, with $n_1 | n_2$. Then there exists an elliptic curve E over the finite field $\mathbb{F}_p$, such that $E(\mathbb{F}_p) = N$. Then there exists a point-line arrangement (N, t) in the projective plane over the finite field $\mathbb{F}_p$ with the group model $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, with*

$$\mathcal{O}r(N) \geq \begin{cases} \lfloor \frac{N(N-3)}{6} \rfloor + 3 & \text{if } 3|n_1, \quad \textit{(Green-Tao bound is exceeded.)} \\ \lfloor \frac{N(N-3)}{6} \rfloor + 1 & \text{if } 3 \nmid n_1. \end{cases} \tag{3.9}$$

Proof. There exists an elliptic curve with $\#E(\mathbb{F}_p) = N$ for each integer N in the interval $[p+1-2\sqrt{p}, p+1+\sqrt{p}]$ is well-known (for example, it follows from the work of Deuring [2]). The statement about the group-structure of $E(\mathbb{F}_p)$ follows form Theorem 5. It is clear from the proof of Theorem 8 that the number of 3-rich lines depends upon the underlying group-structure of $E(\mathbb{F}_p)$, and more precisely, the number of distinct solutions to the equation $x + y + z = 0$ in the underlying group of $E(\mathbb{F}_p)$. Now, the result follows from the Corollaries of Lemma 2. □

Remark 1. *Some examples of orchard group models are shown in Table 3.*

4. Realization on a real projective plane

Let us consider the example of the elliptic curve $E : y^2 = x^3 + 5x^2 + 4x$ over $\mathbb{F}_7$. It can be checked that $\#E(\mathbb{F}_7) = 8$ and $E(\mathbb{F}_7)$ contains the following 8 points:

$$A = (0,0), \quad B = (2,1), \quad C = (2,6), \quad D = (3,0),$$
$$E = (5,2), \quad F = (5,5), \quad G = (6,0), \quad H = (0,1,0) \text{ (the point at infinity).}$$

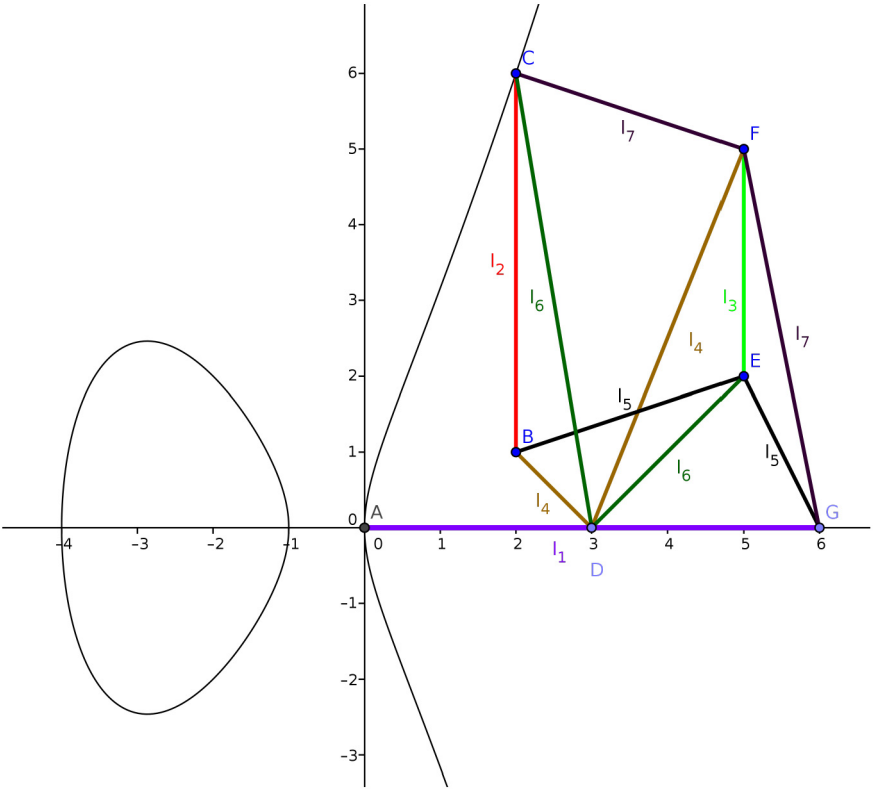


Fig. 3. Orchard configuration with (8 points, 7 lines) using elliptic curve given by a minimal Weierstrass equation $y^2 = x^3 + 5x^2 + 4x$ over $\mathbb{F}_7$. The point at infinity $(0, 1, 0)$ is not shown.

The following seven 3-rich lines could be formed using the points in $E(\mathbb{F}_7)$ (see Fig. 3):

$$\begin{aligned} l_1 &: \text{ containing } \{A, D, G\}, & l_2 &: \text{ containing } \{O, B, C\}, \\ l_3 &: \text{ containing } \{O, E, F\}, & l_4 &: \text{ containing } \{B, D, F\}, \\ l_5 &: \text{ containing } \{B, E, G\}, & l_6 &: \text{ containing } \{C, D, E\}, \\ l_7 &: \text{ containing } \{C, F, G\}. \end{aligned}$$

It can be verified that $E(\mathbb{F}_7) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ and the generators of the group are $C = (2, 6)$ and $D = (3, 0)$. Thus, we have a model showing that $\mathcal{O}r(8) \geq 7$. The orchard configuration with (8 points, 7 lines) in a projective plane over $\mathbb{F}_7$ is shown in Fig. 3. Some lines, for example, l_4 going through points B, D and F, 'visually' does not appear to be a straight line. Is it possible to 'straightened' these lines by picking some other equivalent points in the projective plane over $\mathbb{F}_7$, i.e., can this point-line configuration be embedded into a real projective plane to give an orchard model? The answer in this case is in affirmative, as shown in Fig. 4.

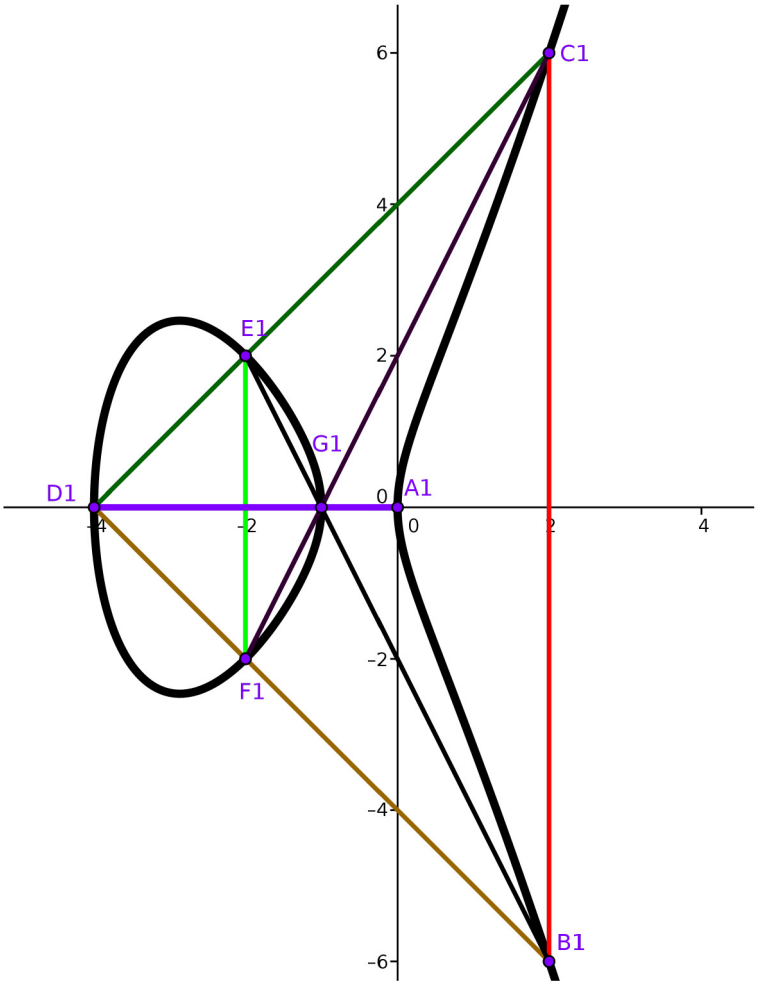


Fig. 4. Orchard configuration with (8 points, 7 lines) using elliptic curve given by a minimal Weierstrass equation $y^2 = x^3 + 5x^2 + 4x$ on a projective plane over $\mathbb{R}$. The point at infinity $(0, 1, 0)$ is not shown.

Note that

$$A_1 = A = (0,0), \quad B_1 = (2,-6) \equiv B = (2,1) \mod 7, \quad C_1 = C = (2,6)$$
$$D_1 = (-4,0) \equiv D = (3,0) \mod 7, \quad E_1 = (-2,2) \equiv (5,2) \mod 7$$
$$F_1 = (-2,-2) \equiv F = (5,5,) \mod 7, \quad G_1 = (-1,0) \equiv G = (6,0) \mod 7.$$

In Fig. 4 seven points A_1, B_1, C_1, D_1, E_1, F_1 and G_1 are arranged so that they yield total 7 'straight' 3-rich lines. In fact, the configuration shown in Fig. 4 gives an orchard model with (8 points, 7 lines) for $y^2 = x^3+5x^2+4x$ over any finite $\mathbb{F}_p$, for all prime $p \geq 7$. Moreover, it is easy to check that the above points on $y^2 = x^3 + 5x^2 + 4x$ also give an orchard model on a real projective plane. This is nice, as one obtains a classical orchard

model (8 points, 7 lines) with integral points (i.e., points with integral coordinates) and the group structure $\mathbb{Z}_4 \times \mathbb{Z}_2$ over real projective plane.

A natural question arises: is it always possible to obtain an orchard group model on a real projective plane corresponding to an orchard model on a projective plane over a finite field? Of course, for orchard group model with (n points, t lines), such that $t = \lfloor \frac{n(n-3)}{6} \rfloor + 3$, i.e., where the Green-Tao bound is exceeded, the answer to this question would be no for sufficiently large n, otherwise it will contradict Theorem 1. Indeed, the answer is no for even a small $n = 9$, as evident from the following example.

Consider the elliptic Curve defined by $y^2 = x^3 + 2$ over $\mathbb{F}_7$. It can be checked that $\#E(\mathbb{F}_7) = 9$ and $E(\mathbb{F}_7)$ contains the following 9 points:

$$A = (0,3), \quad B = (0,4), \quad C = (3,1), \quad D = (3,6), \quad E = (5,1),$$
$$F = (5,6), \quad G = (6,1), \quad H = (6,6), \quad O = (0,1,0) \text{ (the point at infinity)}.$$

The following twelve 3-rich lines could be formed using the points in $E(\mathbb{F}_7)$

$$\begin{aligned}
l_1 &: \text{ containing } \{O,A,B\}, & l_2 &: \text{ containing } \{O,C,D\},\\
l_3 &: \text{ containing } \{O,E,F\}, & l_4 &: \text{ containing } \{O,G,H\},\\
l_5 &: \text{ containing } \{A,C,H\}, & l_6 &: \text{ containing } \{A,D,E\},\\
l_7 &: \text{ containing } \{A,F,G\}. & l_8 &: \text{ containing } \{B,C,F\},\\
l_9 &: \text{ containing } \{B,D,G\}, & l_{10} &: \text{ containing } \{B,E,H\},\\
l_{11} &: \text{ containing } \{C,E,G\}, & l_{12} &: \text{ containing } \{D,F,H\}.
\end{aligned}$$

It can be verified that $E(\mathbb{F}_7) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ and the generators of the group are $C = (6,6)$ and $D = (6,0)$. Thus, we have a model showing that $\mathcal{O}r(9) \geq 12$. The orchard configuration with (9 points, 12 lines) in a projective plane over $\mathbb{F}_7$. But, this configuration can not be realized over the real projective plane as it is known that an optimal configuration of 9 points can yield at most 10 3-rich lines (see [7]).

References

[1] Stefan A. Burr, Branko Grünbaum, N.J.A. Sloane, The orchard problem, Geom. Dedic. 2 (1974) 397–424.
[2] Max Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272.
[3] Ben Green, Terence Tao, On sets defining few ordinary lines, Discrete Comput. Geom. 50 (2) (2013) 409–468.
[4] John Jackson, Rational Amusement for Winter Evenings, or, a Collection of Above 200 Curious and Interesting Puzzles and Paradoxes Relating to Arithmetic, Geometry, Geography, &c: With Their Solutions, and Four Plates, Designed Chiefly for Young Persons, Longman, Hurst, Rees, Orme, and Brown, 1821.
[5] Alfred Menezes, Isomorphism classes of elliptic curves over finite fields of characteristic 2, Util. Math. (1990).

[6] Alfred Menezes, Elliptic Curve Public Key Cryptosystems, The Kluwer International Series in Engineering and Computer Science, vol. 234, Kluwer Academic Publishers, Boston, MA, 1993. With a foreword by Neal Koblitz, Communications and Information Theory.
[7] OEIS Foundation Inc., The on-line encyclopedia of integer sequences, http://oeis.org/A003035, 2020.
[8] Hans-Georg Rück, A note on elliptic curves over finite fields, Math. Comput. 49 (179) (1987) 301–304.
[9] René Schoof, Nonsingular plane cubic curves over finite fields, J. Comb. Theory, Ser. A 46 (2) (1987) 183–211.
[10] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[11] J. Sylvester, Mathematical question 2571, Educational Times (1868).
[12] Lawrence C. Washington, Elliptic curves, in: Number Theory and Cryptography, second edition, in: Discrete Mathematics and Its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008.