УДК 514.2

Studies on Systems of Six Lines on a Projective Plane over a Prime Field

Jiro Sekiguchi[*]
Department of Mathematics,
Tokyo University of Agriculture and Technology,
Koganei, Tokyo 184-8588,
Japan

Received 11.01.2008, received in revised form 20.02.2008, accepted 05.03.2008

A simple six-line arrangement on a projective plane is obtained by a system of six labelled lines $L_1, L_2, \dots, L_6$ with the conditions; (1) they are mutually different and (2) no three of them intersect at a point. We add the condition that (3) there is no conic tangent to all the lines. The main subject of this paper is to treat such arrangements on a projective plane over a finite prime field.

Keywords: projective plane, finite prime field, quadratic residue

Introduction

A simple six-line arrangement on a projective plane is obtained by a system of six labelled lines $L_1, L_2, \dots, L_6$ with the conditions; (1) they are mutually different and (2) no three of them intersect at a point. We add the condition that (3) there is no conic tangent to all the lines. The main subject of this paper is to treat such arrangements on a projective plane over a finite prime field.

Before entering into the main subject, we now explain some results on the real case. There are four types of simple six-line arrangements on a real projective plane (cf. B. Grünbaum [1]). Among the four types, one is characterized by the existence of a hexagon and one is characterized by the condition that the conic tangent to any five lines of the six lines does not intersect the remaining line. The totality of systems of six labelled lines with conditions (1), (2) admits the action of the sixth symmetric group by permutations among six lines. The advantage of the condition (3) is that the action of the sixth symmetric group on the totality of systems of six labelled lines with conditions (1), (2), (3) naturally extends to that of the Weyl group $W(E_6)$ of type E_6. It is shown in J. Sekiguchi and M. Yoshida [2] that $W(E_6)$ acts transitively on the set of systems of six labelled lines fixed by a group isomorphic to a fifth symmetric group and that this is decomposed into four orbits by the sixth symmetric group action. These four S_6-orbits are in a one to one correspondence with the four types of simple-six line arrangements mentioned above.

The purpose of this paper is to study what happens when we replace a real projective plane by a projective plane over a finite prime field. Let p be a prime number, $\mathbf{F}_p$ the field consisting of p points and $\mathbf{P}^2(\mathbf{F}_p)$ the projective plane over $\mathbf{F}_p$. Let $L_1, L_2, \dots, L_6$ be six lines on $\mathbf{P}^2(\mathbf{F}_p)$ with the conditions (1), (2), (3). Then we shall show the following theorems.

[*] e-mail: sekiguti@cc.tuat.ac.jp

© Siberian Federal University. All rights reserved

Theorem 1. *If* 5 *is a quadratic residue mod* p*, there is a system of six labelled-line arrangement on* $\mathbf{P}^2(\mathbf{F}_p)$ *fixed by a fifth symmetric group.*

It is easy to determine systems of six labelled lines fixed by a fifth symmetric group. They are related with the diagonal surface of Clebsch. In fact, if 5 is a quadratic residue mod p, the twenty-seven lines on it are defined over $\mathbf{F}_p$ and any system of six labelled lines fixed by a fifth symmetric group is obtained by blowing down the diagonal surface.

Theorem 2. *Now assume that there is* $n \in \mathbf{F}_p$ *such that* $n^2 \equiv 5\ (p)$*. Then there is a system of six labelled lines fixed by a fifth symmetric group such that the conic tangent to any five lines of the six lines does not intersect the remaining line if and only if* $\pm 2n - 5$ *is a non-quadratic residue mod* p*.*

It is well-known that for a prime p, 5 is a quadratic residue mod p if and only if $p = 10k+1$ or $p = 10k-1$ for a positive integer k. The following theorem was conjectured by the author and later proved by T.Ibukiyama.

Theorem 3. *For a prime* p *with* $5 < p$*, there is* $n \in \mathbf{F}_p$ *such that* $n^2 \equiv 5\ (p)$ *and there is no* $m \in \mathbf{F}_p$ *such that* $m^2 \equiv 2n - 5\ (p)$ *if and only if* $p = 10k - 1$ *for a positive integer* k*.*

We are going to explain the contents of this paper. In §1, we review geometry of six lines on a real projective plane and in §2, we do systems of six labelled lines fixed by S_5-action. The results of both sections are contained in [2]. In §3, we start to study six lines on a projective plane over a finite prime field.

1. Review on Geometry of Six Lines on a Real Projective Plane

In this section, we collect some results given in [2] and its references, necessary to our present study. A system of six labelled lines on a real projective plane consists of six labelled lines $L_1, L_2, \ldots, L_6$ on a real projective plane $\mathbf{P}^2(\mathbf{R})$. It defines an *arrangement of six-lines* (cf. [1]). An arrangement of six-lines is called *simple* if (C1) they are mutually different and (C2) no three of them intersect at a point.

In terms of a system of homogeneous coordinates $t_1 : t_2 : t_3$ on $\mathbf{P}^2(\mathbf{R})$, the six lines $L_1, L_2, \ldots, L_6$ are expressed by linear equations:

$$L_j\ :\ x_{j1}t_1 + x_{j2}t_2 + x_{j3}t_3 = 0 \quad (j = 1, 2, \ldots, 6).$$

Thus the system $\mathcal{S}$ of six labelled lines $L_1, L_2, \ldots, L_6$ is represented by a 3×6 matrix $X = (x_{ij})$. Then for any $a_i \in \mathbf{R} - \{0\}$ $(i = 1, 2, \ldots, 6)$, $X = (x_{ij})$ and $X' = (a_i x_{ij})$ define the same system of six labelled lines. Two systems of six labelled lines are equivalent if they are transformed into each other by a projective linear transformation. Since we are interested in the space of systems of six labelled lines with conditions (1), (2), we are led to define the configuration space

$$\mathbf{P}(2,6) = G\backslash M^*/H, \quad M^* = M^*(3,6), \quad G = GL(3,\mathbf{R}), \quad H = H_6,$$

where $M^*(3,6)$ is the set of real 3×6 matrices where no 3-minor vanishes, and H_6 is the subgroup of $GL(6, \mathbf{R})$ consisting of diagonal matrices. Any system of six labelled lines $\mathcal{S}$ is represented by a matrix of the form

$$X = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & x_1 & x_2 \\ 0 & 0 & 1 & 1 & y_1 & y_2 \end{pmatrix} \tag{1}$$

This implies that $\mathbf{P}(2,6)$ is identified with an affine open subset of $\mathbf{R}^4$.

The symmetric group S_6 is generated by transpositions s_{ij} $(1 \leq i < j \leq 6)$. We may identify s_{ij} with the transposition between the lines L_i and L_j. This induces an S_6-action on the space $\mathbf{P}(2,6)$. Let $X \in M^*$ be a matrix representing a system $\mathcal{S}$ of six labelled lines. Regarding X as a linear map of $\mathbf{R}^6$ to $\mathbf{R}^3$, we choose a basis $\{y_1, y_2, y_3\}$ of its kernel. Then $s_r X =^t (y_1 y_2 y_3) \in M^*$ defines a system $s_r \mathcal{S}$. The map s_r induces a biregular involution on $\mathbf{P}(2,6)$. The following lemma is an easy consequence of the definition of s_r:

Lemma 1. *(i) The action s_r commutes with that of S_6 on $\mathbf{P}(2,6)$.*

(ii) A system of six labelled lines is fixed by s_r if and only if there is a conic tangent to all the six lines of the system.

Noting this lemma, we add a condition on systems of six labelled lines;

(C3) There is no conic tangent to all the six lines.

We define a subspace $\mathbf{P}_0(2,6)$ of $\mathbf{P}(2,6)$ consisting of systems of six labelled lines which are not fixed by the operation s_r. The space $\mathbf{P}_0(2,6)$ admits an action s_{123} which is not contained in S_6. Take a representative $X \in \mathbf{P}_0(2,6)$ defined in (1). Then s_{123} is defined by

$$X = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & x_1 & x_2 \\ 0 & 0 & 1 & 1 & y_1 & y_2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1/x_1 & 1/x_2 \\ 0 & 0 & 1 & 1 & 1/y_1 & 1/y_2 \end{pmatrix} = s_{123}X$$

By the condition (C3), $s_{123}X$ is also contained in $\mathbf{P}_0(2,6)$. The group generated by S_6 and s_{123} is nothing but the Weyl group $W(E_6)$ of type E_6 and the operation s_r is contained in $W(E_6)$. In this manner, the space $\mathbf{P}_0(2,6)$ admits the action of $W(E_6)$.

Let $\mathcal{P}_6(\mathbf{R})$ be the totality of connected components of $\mathbf{P}_0(2,6)$. Then the action of $W(E_6)$ on $\mathbf{P}_0(2,6)$ naturally extends to that on $\mathcal{P}_6(\mathbf{R})$.

We define p-gons for the system of six labelled lines $L_1, L_2, \ldots, L_6$. Each connected component of $\mathbf{P}^2(\mathbf{R}) - \cup_{j=1}^{6} L_j$ is called a polygon. If it is surrounded by p lines, it is called a p-gon. It is known (cf. [1]) that there are four types of simple six-line arrangements. They are characterized by numbers of p-gons and referred to as O, I, II, III.

Types	hexagon	pentagons	rectangles	triangles
O	1	0	9	6
I	0	2	8	6
II	0	3	6	7
III	0	6	0	10

In the case of systems of six labelled lines on a projective plane over a finite prime field, it is hard to define p-gons of a system. As a consequence, the characterizations of systems of types O, I, II, III above lose their meanings if we consider systems over a finite prime field. Instead, it is possible to characterize systems of types I and III in a different manner.

Lemma 2. *Let $\mathcal{S}$ be a system of six labelled lines $L_1, L_2, \ldots, L_6$ on a real projective plane. Let C_i be the conic tangent to five lines L_k $(k = 1, 2, \ldots, 6, k \neq i)$.*

(i) $\mathcal{S}$ is of type III if and only if the conic tangent to any five lines of $L_1, L_2, \ldots, L_6$ does not intersect the remaining line.

(ii) Suppose that $\mathcal{S}$ is of type O and that $L_1, L_2, \ldots, L_6$ bounds a hexagon in this order. Then one of the following holds:
(a) $C_i \cap L_i = \varnothing$ $(i = 1, 3, 5)$ and $C_i \cap L_i \neq \varnothing$ $(i = 2, 4, 6)$.
(b) $C_i \cap L_i \neq \varnothing$ $(i = 1, 3, 5)$ and $C_i \cap L_i = \varnothing$ $(i = 2, 4, 6)$.

(iii) Suppose that $\mathcal{S}$ is of type I and that $L_1, L_2, \ldots, L_5$ (resp. $L_1, \ldots, L_4, L_6$) bounds a pentagon. Then $C_i \cap L_i \neq \varnothing$ $(i = 1, 2, 3, 4)$ and $C_i \cap L_i = \varnothing$ $(i = 5, 6)$.

(iv) Suppose that $\mathcal{S}$ is of type II and that $L_1, L_2, \ldots, L_5$ (resp. $L_1, \ldots, L_4, L_6$, and L_1, L_2, L_3, L_5, L_6)) bounds a pentagon. Then $C_i \cap L_i \neq \varnothing$ $(i = 1, 2, 3)$ and $C_i \cap L_i = \varnothing$ $(i = 4, 5, 6)$.

Remark 1. *Unfortunately, systems of types O and II are not distinguished by the lemma above.*

2. Systems of Six Labelled Lines Fixed by S$_5$-action

We begin with this section by defining an outer automorphism τ of S_6 defined as follows:

Permutation		Image by τ
(12)	→	(12)(34)(56)
(23)	→	(16)(24)(35)
(34)	→	(12)(36)(45)
(45)	→	(16)(25)(34)
(56)	→	(12)(35)(46)

Here we identify s_{ij} with the permutation (ij). Since $(i\,i+1)$ $(i = 1, 2, 3, 4, 5)$ generate S_6, τ is actually an automorphism of S_6. As in [2], we put $\tau(ij') = \tau((ij)) \circ s_r$. Define the matrix $X(\pm\sqrt{5}) \in M^*$ by

$$X(\pm\sqrt{5}) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & (-1 \mp \sqrt{5})/2 & (1 \mp \sqrt{5})/2 \\ 0 & 0 & 1 & 1 & (1 \mp \sqrt{5})/2 & (3 \mp \sqrt{5})/2 \end{pmatrix}$$

Then the following holds:

Proposition 1. *Let H be the subgroup of $W(E_6)$ generated by $\tau'((i\,i+1))$ $(i = 2, 3, 4, 5)$ (which is isomorphic to S_5). Then $X(\sqrt{5})$ is fixed by H as an element of $\mathbf{P}_0(2, 6)$.*

Remark 2 (cf. [2])**.** *(i) By blowing up $\mathbf{P}^2(\mathbf{C})$ at the six points*

$$(1:0:0),\ (0:1:0),\ (0:0:1),\ (1:1:1),$$
$$(1:(-1-\sqrt{5})/2:(1-\sqrt{5})/2),\ (1:(1-\sqrt{5})/2:(3-\sqrt{5})/2),$$

we obtain Clebsch diagonal surface in $\mathbf{P}^3(\mathbf{C})$.

(ii) We consider a regular icosidodecahedron in $\mathbf{R}^3$ whose center is the origin. There are six hyperplanes containing the origin in $\mathbf{R}^3$ which cut the edges. From these hyperplanes, we obtain a system $\mathcal{S}$ of labelled six lines on a real projective plane. Let $X \in M^*$ be the matrix obtained from $\mathcal{S}$. Then X is equivalent to $X(\sqrt{5})$ by choosing a label appropriately.

Proposition 2. *The system of six labelled lines defined by $X(\pm\sqrt{5})$ is of type III. Moreover, the systems of six labelled lines defined by $s_{123}X(\sqrt{5})$, $s_{145}s_{123}X(\sqrt{5})$, and $s_{123}X(-\sqrt{5})$ are of types O, I, II, repsectively, where $s_{145} = s_{35}s_{24}s_{123}s_{24}s_{35}$.*

3. Systems of Six Labelled Lines on a Projective Plane over a Prime Field

Let p be a prime number and let $\mathbf{F}_p$ be the prime field consisting of p elements. In this section, we study systems of six labelled lines on a projective plane defined over $\mathbf{F}_p$. Let $\mathbf{P}^2(\mathbf{F}_p)$ be a projective plane defined over $\mathbf{F}_p$. As before let $t_1 : t_2 : t_3$ be its homogeneous coordinate system.

First of all, we consider the conic tangent to five lines on $\mathbf{P}^2(\mathbf{F}_p)$. Let

$$t_1 = 0, t_2 = 0, t_3 = 0, a_1t_1 + a_2t_2 + a_3t_3 = 0, b_1t_1 + b_2t_2 + b_3t_3 = 0 \tag{2}$$

be equations of five lines. We assume that no three of them intersect at a point. Then it is easy to show that there is a unique conic tangent to the five lines (2) and it is defined by

$$p_1^2t_1^2 + p_2^2t_2^2 + p_3^2t_3^2 - 2p_2p_3t_2t_3 - 2p_3p_1t_3t_1 - 2p_1p_2t_1t_2 = 0, \tag{3}$$

where

$$p_1 = a_1b_1(a_2b_3 - a_3b_2),\ p_2 = a_2b_2(a_3b_1 - a_1b_3),\ p_3 = a_3b_3(a_1b_2 - a_2b_1).$$

A system $\mathcal{S}$ of six labelled lines on $\mathbf{P}^2(\mathbf{F}_p)$ is defined similarly to the real case. We consider conditions (C1), (C2), (C3). From the systems $\mathcal{S}$ with conditions (C1), (C2), (C3), we are naturally led to define the configuration space $\mathbf{P}_0(2,6)_{\mathbf{F}_p}$ over $\mathbf{F}_p$. The matrices of the form (1) with $x_1, x_2, y_1, y_2 \in \mathbf{F}_p$ are regarded as representatives of $\mathbf{P}_0(2,6)_{\mathbf{F}_p}$. Noting this, we may identify $\mathbf{P}_0(2,6)_{\mathbf{F}_p}$ with an affine open subset $S_{\mathbf{F}_p}$ of $\mathbf{F}_p^4$. In order to define $S_{\mathbf{F}_p}$ definitely, we introduce the fifteen polynomials f_j $(j = 1, 2, \dots, 15)$ by

$$\begin{aligned}
&f_1 = x_1,\ f_2 = x_2,\ f_3 = y_1,\ f_4 = y_2,\ f_5 = y_1 - x_1,\ f_6 = y_2 - x_2,\\
&f_7 = 1 - x_1,\ f_8 = 1 - x_2,\ f_9 = 1 - y_1,\ f_{10} = 1 - y_2,\\
&f_{11} = x_1 - x_2,\ f_{12} = y_1 - y_2,\ f_{13} = x_1y_2 - x_2y_1,\\
&f_{14} = x_1y_2 - x_2y_1 - x_1 + x_2 + y_1 - y_2,\\
&f_{15} = x_1y_1y_2 - x_2y_1y_2 + x_1x_2y_2 - x_1x_2y_1 - x_1y_2 + x_2y_1.
\end{aligned}$$

Then

$$S_{\mathbf{F}_p} = \{(x_1, x_2, y_1, y_2) \in \mathbf{F}_p^4\,;\ f_j \neq 0\ (j = 1, 2, \ldots, 15)\}.$$

Remark 3 (cf. [2], p.315)**.** *The fourteen polynomials f_j $(j < 15)$ are obtained as determinants of 3×3 minors of the matrix (1) and $f_{15} = 0$ corresponds to the condition that the system of six labelled lines defined by the matrix (1) does not satisfy (C3).*

It is easy to show that the Weyl group $W(E_6)$ acts on the space $S_{\mathbf{F}_p} \simeq \mathbf{P}_0(2, 6)_{\mathbf{F}_p}$ by the same manner as in the real case.

Let $\mathcal{S}$ be a system of six labelled lines $L_1, \ldots, L_6$ in $\mathbf{P}^2(\mathbf{F}_p)$. Then as mentioned before, for each j $(j = 1, 2, \ldots, 6)$, there is a unique conic C_j in $\mathbf{P}^2(\mathbf{F}_p)$ tangent to the five lines L_k $(k = 1, \ldots, 6,\ k \neq j)$. Since systems of six labelled lines of type III play an important role in the study [2], we introduce the notion of systems of six labelled lines of type III.

Definition 1. *A system $\mathcal{S}$ is of type III if $C_j \cap L_j = \varnothing$ for $j = 1, 2, \ldots, 6$.*

Then it is interesting to study the following problems.

Problem 1. *(i) Find a condition for the prime p which implies the existence of a system of six labelled lines of type III.*

(ii) Fix a prime p for which there is a system of six labelled lines of type III. For any $(x_1, x_2, y_1, y_2) \in S$, does there exist $w \in W(E_6)$ satisfying the condition that w transforms (x_1, x_2, y_1, y_2) to $(u_1, u_2, v_1, v_2) \in S$ so that the system of six labelled lines corresponding to (u_1, u_2, v_1, v_2) is of type III?

Problem 2. *Find a condition for the prime p which implies the existence of a system of six labelled lines fixed by a subgroup H of $W(E_6)$ isomorphic to the symmetric group of degree five.*

In the next section, we shall study topics related to these problems.

4. Systems of Six Labelled Lines Fixed by $\mathbf{S_5}$-action over $\mathbf{F_p}$

In this section, we restrict our attention to such systems of six labelled lines that they are fixed by subgroups of $W(E_6)$ isomorphic to S_5.

We begin with this section with defining a subgroup $H(5)$ of $W(E_6)$ generated by $\tau(i\,i+1)'$ $(i = 2, 3, 4, 5)$. Clearly $H(5)$ is isomorphic to S_5. It is shown in [3] that there are forty five involutions in $W(E_6)$ conjugate to $\tau(i\,i+1)'$ $(i = 1, 2, \ldots, 5)$. As actions on $S_{\mathbf{F}_p}$, the explicit forms of $\tau(i\,i+1)'$ $(i = 2, \ldots, 5)$ are given in [2], Lemma 2. For example,

$$\tau(23)' : (x_1, x_2, y_1, y_2) \longrightarrow \left(\frac{x_2}{y_2}, x_2, \frac{x_2 y_1}{x_1 y_2}, \frac{x_2}{x_1}\right)$$

Noting this, we conclude that for $(x_1, x_2, y_1, y_2) \in S_{\mathbf{F}_p}$, (x_1, x_2, y_1, y_2) is fixed by $\tau(23)'$ if and only if $x_2 - x_1 y_2 = 0$. More generally we have the following lemma (cf. [2], Corollary 1 to Lemma 2).

Lemma 3. *For $i = 2, 3, 4, 5$, the fixed point set of $\tau(i\,i+1)'$ is given by $k_{i\,i+1} = 0$, where*

$$\begin{aligned} k_{23} &= -x_2 + x_1y_2, & k_{34} &= -(x_1 - x_2 - y_1 + x_2y_1), \\ k_{45} &= x_2y_1 - y_2, & k_{56} &= x_1 - x_2 + y_2 - x_1y_2. \end{aligned} \tag{4}$$

Theorem 4. *Let p be a prime number with $p > 5$. Then there is $(x_1, x_2, y_1, y_2) \in S_{\mathbf{F}_p}$ fixed by $H(5)$ if and only if there is $n \in \mathbf{Z}$ such that $n^2 \equiv 5\,(p)$.*

Proof. From the argument before the theorem, there is $(x_1, x_2, y_1, y_2) \in S_{\mathbf{F}_p}$ fixed by $H(5)$ if and only if $k_{23} = k_{34} = k_{45} = k_{56} = 0$ hold for (x_1, x_2, y_1, y_2). Since $(x_1, x_2, y_1, y_2) \in \mathbf{F}_p^4$ is contained in $S_{\mathbf{F}_p}$ if and only if $f_j \neq 0\,(j = 1, 2, \ldots, 15)$. Then it is easy to find that $(x_1, x_2, y_1, y_2) \in S_{\mathbf{F}_p}$ fixed by $H(5)$ if and only if

$$x_1^2 + x_1 - 1 = 0,\ \ x_2 = y_1 = x_1 + 1,\ \ y_2 + x_1 + 2. \tag{5}$$

If there is $n \in \mathbf{Z}$ such that $n^2 \equiv 5\,(p)$, we take x_1 as the residue class of $(p+1)/2 \cdot (n-1)$ in $\mathbf{F}_p$. Then $x_1^2 + x_1 - 1 = 0$ in $\mathbf{F}_p$. On the other hand, if $n^2 \not\equiv 5\,(p)$ for any $n \in \mathbf{Z}$, there is no solution of $x^2 + x - 1 = 0$ in $\mathbf{F}_p$. Hence the theorem follows. □

Let p be a prime number with $p > 5$. Then it follows from the reciprocity law for the Legendre symbol that 5 is a quadratic residue mod p if and only if $p+1$ or $p-1$ is divisible by 5. Noting that p is odd, this is equivalent to that there is an integer k such that $p = 10k + 1$ or $p = 10k - 1$.

In the rest of this section, we always assume that p is a prime number of the form $p = 10k + 1$ or $p = 10k - 1$. Moreover let n be an integer such that $n^2 \equiv 5\,(p)$ and fix it.

It follows from the computation above that $((-1-n)/2, (1-n)/2, (1-n)/2, (3-n)/2)$ is the fixed point of $H(5)$ in $W(E_6)$. Let G_0 be the subgroup of $W(E_6)$ generated by s_{ij} $(1 \leq i < j \leq 6)$ and s_r. Then $G_0 \simeq S_6 \times \langle s_r \rangle$ and the G_0-orbit of $((-1-n)/2, (1-n)/2, (1-n)/2, (3-n)/2)$ in $S_{\mathbf{F}_p}$ consists of twelve points defined by

$$\begin{array}{cccccc}
(& (-1 \pm n)/2, & (1 \pm n)/2, & (1 \pm n)/2, & (3 \pm n)/2 &), \\
(& (-1 \pm n)/2, & (-1 \pm n)/2, & (3 \pm n)/2, & (1 \pm n)/2 &), \\
(& (1 \pm n)/2, & (3 \pm n)/2, & (-1 \pm n)/2, & (1 \pm n)/2 &), \\
(& (3 \pm n)/2, & (1 \pm n)/2, & (1 \pm n)/2, & (-1 \pm n)/2 &), \\
(& (-1 \pm n)/2, & (3 \mp n)/2, & (3 \mp n)/2, & (-1 \pm n)/2 &), \\
(& (3 \mp n)/2, & (-1 \pm n)/2, & (-1 \pm n)/2, & (3 \mp n)/2 &).
\end{array}$$

Put $a = (p+1)/2 \cdot (1-n)$. Then we find that

$$(a-1, a, a, a+1) = ((-1-n)/2, (1-n)/2, (1-n)/2, (3-n)/2)$$

and the corresponding matrix is

$$X_{\mathbf{F}_p}(n) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & a-1 & a \\ 0 & 0 & 1 & 1 & a & a+1 \end{pmatrix}.$$

This matrix is equivalent to

$$Y_{\mathbf{F}_p}(n) = \begin{pmatrix} 1 & 1 & -1 & 1 & 0 & 0 \\ 1 & -a & a-1 & 0 & 1 & 0 \\ -1 & a-1 & -a+2 & 0 & 0 & 1 \end{pmatrix},$$

namely, putting

$$U(n) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a-1 & a \\ 1 & a & a+1 \end{pmatrix},$$

we find that $\det(U(n)) = -1$ and $U(n)^{-1}X_{\mathbf{F}_p}(n) = Y_{\mathbf{F}_p}(n)$. Let $\mathcal{S}$ and $\mathcal{T}$ be the systems of six labelled lines defined by $X_{\mathbf{F}_p}(n)$ and $Y_{\mathbf{F}_p}(n)$, respectively. Namely, if the lines $L_i(n)$, $L'_i(n)$ $(i = 1, 2, \ldots, 6)$ are defined by

$$\begin{aligned} &L_j(n) : t_j = 0 \; (j = 1, 2, 3), \\ &L_4(n) : t_1 + t_2 + t_3 = 0, \\ &L_5(n) : t_1 + (a-1)t_2 + at_3 = 0, \\ &L_6(n) : t_1 + at_2 + (a+1)t_3 = 0, \end{aligned}$$

and

$$\begin{aligned} &L'_1(n) : t_1 + t_2 - t_3 = 0, \\ &L'_2(n) : t_1 - at_2 + (a-1)t_3 = 0, \\ &L'_3(n) : -t_1 + (a-1)t_2 + (-a+2)t_3 = 0, \\ &L'_j(n) : t_{j-3} = 0 \; (j = 4, 5, 6), \end{aligned}$$

then $\mathcal{S}$ is the system of six labelled lines $L_1(n), \ldots, L_6(n)$ and $\mathcal{T}$ is the system of six labelled lines $L'_1(n), \ldots, L'_6(n)$. Let $C_j(n)$ (resp. $C'_j(n)$) be the conic tangent to the five lines $L_k(n)$ $(k = 1, \ldots, 6, k \neq j)$ (resp. $L'_k(n)$ $(k = 1, \ldots, 6, k \neq j)$). Then it follows from the definition that $C_j(n) \cap L_j(n) = \varnothing$ (resp. $C_j(n) \cap L_j(n) \neq \varnothing$) if and only if $C'_j(n) \cap L'_j(n) = \varnothing$ (resp. $C'_j(n) \cap L'_j(n) \neq \varnothing$). By the computations in the previous section, the conic $C_6(n)$ is defined by

$$2t_1^2 + (7+3n)t_2^2 + (3+n)t_3^2 + 4(2+n)t_2t_3 - 2(1+n)t_1t_3 + 2(3+n)t_1t_2 = 0.$$

We consider the points of $C_6(n) \cap L_6(n)$. Then since $t_1 = -at_2 - (a+1)t_3$, we find that

$$(3+n)t_2^2 + 2t_2t_3 + 2t_3^2 = 0,$$

which is equivalent to

$$(t_2 + 2t_3)^2 + (5+2n)t_2^2 = 0.$$

This implies that $C_6(n) \cap L_6(n) \neq \varnothing$ if and only if there is $m \in \mathbf{F}_p$ such that $m^2 \equiv -2n-5 (p)$. Therefore $C_6(n) \cap L_6(n) = \varnothing$ if and only if $\left(\dfrac{-2n-5}{p}\right) = -1$. By computation similar to this, we find that

$$\begin{aligned} &C_4(n) \cap L_4(n) = \varnothing \text{ if and only if } \left(\frac{2n-5}{p}\right) = -1, \\ &C_5(n) \cap L_5(n) = \varnothing \text{ if and only if } \left(\frac{2n-5}{p}\right) = -1. \end{aligned}$$

Concerning the system $\mathcal{T}$, we find that
$C'_1(n) \cap L'_1(n) = \varnothing$ if and only if $\left(\dfrac{-2n-5}{p}\right) = -1$,
$C'_2(n) \cap L'_2(n) = \varnothing$ if and only if $\left(\dfrac{-2n-5}{p}\right) = -1$,
$C'_3(n) \cap L'_3(n) = \varnothing$ if and only if $\left(\dfrac{2n-5}{p}\right) = -1$.
Since $n^2 \equiv 5\,(p)$, it follows that $(-5+2n)(-5-2n) \equiv 5 \equiv n^2\,(p)$ and therefore the conditions $\left(\dfrac{2n-5}{p}\right) = -1$ and $\left(\dfrac{-2n-5}{p}\right) = -1$ are equivalent. We have thus proved the following theorem.

Theorem 5. *Let p be a prime number and suppose that $p = 10k-1$ or $p = 10k+1$ for an integer k. Then the system of six labelled lines defined by the matrix $X_{\mathbf{F}_p}(n)$ is of type III if and only if* $\left(\dfrac{2n-5}{p}\right) = -1$.

5. Systems of Other Types

Let p be a prime number. In this section, we always assume that
(A1) There is $n \in \mathbf{F}_p$ such that $n^2 \equiv 5\ (p)$.
(A2) For any $m \in \mathbf{F}_p$, $m^2 \not\equiv 2n-5\ (p)$, where n is an integer given (A1).

It is easy to show that $s_{123}(a-1, a, a, a+1) = (a, a-1, a-1, -a+2)$ as elements of $S_{\mathbf{F}_p}$. The corresponding matrix is

$$X_{\mathbf{F}_p}(n)^{s_{123}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & a & a-1 \\ 0 & 0 & 1 & 1 & a-1 & -a+2 \end{pmatrix}.$$

This matrix is equivalent to

$$Y_{\mathbf{F}_p}(n)^{s_{123}} = \begin{pmatrix} (1-2a)/5 & (1-2a)/5 & (3+4a)/5 & 1 & 0 & 0 \\ (1-2a)/5 & (1+3a)/5 & (-2-a)/5 & 0 & 1 & 0 \\ (3+4a)/5 & (-2-a)/5 & (-1-3a)/5 & 0 & 0 & 1 \end{pmatrix}.$$

Let $s_{123}\mathcal{S}$ and $s_{123}\mathcal{T}$ be the systems of six labelled lines defined by $X_{\mathbf{F}_p}(n)^{s_{123}}$ and $Y_{\mathbf{F}_p}(n)^{s_{123}}$, respectively. Lines $L_i(n)^{s_{123}}$, $L'_i(n)^{s_{123}}$ $(i = 1, 2, \ldots, 6)$ and conics $C_j(n)^{s_{123}}$, $C'_j(n)^{s_{123}}$ are defined by using $X_{\mathbf{F}_p}(n)^{s_{123}}$ and $Y_{\mathbf{F}_p}(n)^{s_{123}}$ as the lines $L_i(n)$, $L'_i(n)$ $(i = 1, 2, \ldots, 6)$ and conics $C_i(n)$ $C'_i(n)$ $(i = 1, 2, \ldots, 6)$ by $X_{\mathbf{F}_p}(n)$ and $Y_{\mathbf{F}_p}(n)$. From $X_{\mathbf{F}_p}(n)^{s_{123}}$, $Y_{\mathbf{F}_p}(n)^{s_{123}}$, we compute the condition for which $C_i(n)^{s_{123}} \cap L_i(n)^{s_{123}} \neq \varnothing$ $(i = 4, 5, 6)$ and $C'_i(n)^{s_{123}} \cap L'_i(n)^{s_{123}} \neq \varnothing$ $(i = 1, 2, 3)$. As a consequence, we easily find that
(i) $(t_1 : t_2 : t_3) \in C_4(n)^{s_{123}} \cap L_4(n)^{s_{123}}$ if and only if $t_2(t_2 + t_3) = 0$.
(ii) $(t_1 : t_2 : t_3) \in C_6(n)^{s_{123}} \cap L_6(n)^{s_{123}}$ if and only if $t_3(2t_2 + (3+n)t_3) = 0$.
(iii) $(t_1 : t_2 : t_3) \in C_6(n)^{s_{123}} \cap L_6(n)^{s_{123}}$ if and only if $t_3(2t_1 + nt_2) = 0$.
(iv) $C'_1(n)^{s_{123}} \cap L'_1(n)^{s_{123}} \not\equiv \varnothing$ if and only if $2n-5 \equiv m^2\ (p)$ for some $m \in \mathbf{F}_p$.
(v) $C'_2(n)^{s_{123}} \cap L'_2(n)^{s_{123}} \not\equiv \varnothing$ if and only if there is $(t_2 : t_3) \in \mathbf{P}^1(\mathbf{F}_p)$ such that $2t_2^2 + (-1+n)t_2t_3 + 2t_3^2 = 0$.
(vi) $C'_3(n)^{s_{123}} \cap L'_3(n)^{s_{123}} \not\equiv \varnothing$ if and only if $2n-5 \equiv m^2\ (p)$ for some $m \in \mathbf{F}_p$.

We continue the computation in the case (v). Since

$$(n-1)^2(2n+5) \equiv 10+2n \quad (p),$$

it follows that

$$\begin{aligned} 8\{2t_2^2+(-1+n)t_2t_3+2t_3^2\} &\equiv \{4t_2+(n-1)t_3\}^2+(10+2n)t_3^2 \\ &\equiv \{4t_2+(n-1)t_3\}^2-(n-1)^2(-2n-5)t_3^2 \qquad (p). \end{aligned}$$

Then we find from (A2) that there is no point $(t_2:t_3) \in \mathbf{P}^1(\mathbf{F}_p)$ satisfying the condition $2t_2^2+(-1+n)t_2t_3+2t_3^2=0$. Summarizing the computation above and noting that $C_i(n)^{s_{123}} \cap L_i(n)^{s_{123}} = \varnothing$ if and only if $C_i'(n)^{s_{123}} \cap L_i'(n)^{s_{123}} = \varnothing$, we conclude the following:

(i) $C_i(n)^{s_{123}} \cap L_i(n)^{s_{123}} = \varnothing$ $(i=1,2,3)$,

(ii) $C_i(n)^{s_{123}} \cap L_i(n)^{s_{123}} \neq \varnothing$ $(i=4,5,6)$.

By direct computation, we find that $s_{145}s_{123}(a-1,a,a,a+1)=(a-1,3a-4,a,-a+3)$ as elements of $S_{\mathbf{F}_p}$. The corresponding matrix is

$$X_{\mathbf{F}_p}(n)^{s_{145}s_{123}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & a-1 & 3a-4 \\ 0 & 0 & 1 & 1 & a-1 & -a+3 \end{pmatrix}.$$

This matrix is equivalent to

$$Y_{\mathbf{F}_p}(n)^{s_{145}s_{123}} = \begin{pmatrix} 3+4a & -1-2a & -1-2a & 1 & 0 & 0 \\ 3+4a & -2-3a & -1-a & 0 & 1 & 0 \\ -5-8a & 3+5a & 2+3a & 0 & 0 & 1 \end{pmatrix}.$$

Let

$$L_i(n)^{s_{145}s_{123}},\ L_i'(n)^{s_{145}s_{123}}\ (i=1,2,\ldots,6)$$

be the lines constructed from $X_{\mathbf{F}_p}(n)^{s_{145}s_{123}}$, $Y_{\mathbf{F}_p}(n)^{s_{145}s_{123}}$, respectively defined similarly to the cases $L_i(n)$, $L_i'(n)$. Then it follows from direct computation that

(i) $(t_1:t_2:t_3) \in C_4(n)^{s_{145}s_{123}} \cap L_4(n)^{s_{145}s_{123}} \iff t_2\{2t_2+(n-1)t_3\}=0.$

(ii) $(t_1:t_2:t_3) \in C_5(n)^{s_{145}s_{123}} \cap L_5(n)^{s_{145}s_{123}} \iff t_3\{2t_2+(n-1)t_3\}=0.$

(iii) $(t_1:t_2:t_3) \in C_6(n)^{s_{145}s_{123}} \cap L_6(n)^{s_{145}s_{123}} \iff (2t_2+t_3)^2-(2n-5)t_3^2=0.$

(iv) $(t_1:t_2:t_3) \in C_1'(n)^{s_{145}s_{123}} \cap L_1'(n)^{s_{145}s_{123}} \iff \{2nt_2+(2-n)t_3\}^2 -(2n-5)t_3^2=0.$

(v) $(t_1:t_2:t_3) \in C_2'(n)^{s_{145}s_{123}} \cap L_2'(n)^{s_{145}s_{123}} \iff t_2(t_2-t_3)=0.$

(vi) $(t_1:t_2:t_3) \in C_3'(n)^{s_{145}s_{123}} \cap L_3'(n)^{s_{145}s_{123}} \iff (t_2-t_3)\{2t_2+(n-3)t_3\}=0.$

By the condition (A2), $C_6(n)^{s_{145}s_{123}} \cap L_6(n)^{s_{145}s_{123}} = \varnothing$ and $C_1'(n)^{s_{145}s_{123}} \cap L_1'(n)^{s_{145}s_{123}} = \varnothing$.

Summarizing the computation above and noting that $C_i(n)^{s_{145}s_{123}} \cap L_i(n)^{s_{145}s_{123}} = \varnothing$ if and only if $C_i'(n)^{s_{145}s_{123}} \cap L_i'(n)^{s_{145}s_{123}} = \varnothing$, we conclude the following:

(i) $C_i(n)^{s_{123}} \cap L_i(n)^{s_{123}} = \varnothing$ $(i=1,6)$,

(ii) $C_i(n)^{s_{123}} \cap L_i(n)^{s_{123}} \neq \varnothing$ $(i=2,3,4,5)$.

By direct computation, we have $s_r(a-1,a,a,a+1)=(-a,1-a,1-a,2-a)$ as elements of $S_{\mathbf{F}_p}$. The corresponding matrix is

$$X_{\mathbf{F}_p}(n)^{s_r} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & -a & 1-a \\ 0 & 0 & 1 & 1 & 1-a & 2-a \end{pmatrix}.$$

Next we have $s_{123}s_r(a-1, a, a, a+1) = (1-a, -a, -a, 1+a)$ as elements of $S_{\mathbf{F}_p}$. The corresponding matrix is

$$X_{\mathbf{F}_p}(n)^{s_{123}s_r} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1-a & -a \\ 0 & 0 & 1 & 1 & -a & 1+a \end{pmatrix}.$$

This matrix is equivalent to

$$Y_{\mathbf{F}_p}(n)^{s_{123}s_r} = \begin{pmatrix} -1+2a & -1+2a & 7-4a & 5 & 0 & 0 \\ -1+2a & 4-3a & -3+a & 0 & 5 & 0 \\ 7-4a & -3+a & -4+3a & 0 & 0 & 5 \end{pmatrix}.$$

As before, let $L_i(n)^{s_{123}s_r}$, $L'_i(n)^{s_{123}s_r}$ $(i = 1, 2, \dots, 6)$ be the lines constructed from $X_{\mathbf{F}_p}(n)^{s_{123}s_r}$, $Y_{\mathbf{F}_p}(n)^{s_{123}s_r}$, respectively defined similarly to the cases $L_i(n)$, $L'_i(n)$. Then it follows from direct computation that

(i) $(t_1 : t_2 : t_3) \in C_4(n)^{s_{123}s_r} \cap L_4(n)^{s_{123}s_r} \iff t_2(t_2+t_3) = 0.$

(ii) $(t_1 : t_2 : t_3) \in C_5(n)^{s_{123}s_r} \cap L_5(n)^{s_{123}s_r} \iff t_3\{(3+n)t_2 + t_3\} = 0.$

(iii) $(t_1 : t_2 : t_3) \in C_6(n)^{s_{123}s_r} \cap L_6(n)^{s_{123}s_r} \iff t_2 t_3 = 0.$

(iv) $(t_1 : t_2 : t_3) \in C'_1(n)^{s_{123}s_r} \cap L'_1(n)^{s_{123}s_r} \iff \{2t_2 - (2+n)t_3\}^2 - (-2n-5)t_3^2 = 0.$

(v) $(t_1 : t_2 : t_3) \in C'_2(n)^{s_{123}s_r} \cap L'_2(n)^{s_{123}s_r} \iff \{4t_2 - (n+1)t_3\}^2 - (2n-5)(n+1)^2 t_3^2 = 0.$

(vi) $(t_1 : t_2 : t_3) \in C'_3(n)^{s_{123}s_r} \cap L'_3(n)^{s_{123}s_r} \iff (2t_2 - t_3)^2 - (-2n-5)t_3^2 = 0.$

By the condition (A2), $C_i(n)^{s_{123}s_r} \cap L_i(n)^{s_{123}s_r} = \varnothing$ if and only if $C'_i(n)^{s_{123}s_r} \cap L'_i(n)^{s_{123}s_r} = \varnothing$, we conclude the following:

(i) $C_i(n)^{s_{123}s_r} \cap L_i(n)^{s_{123}s_r} = \varnothing$ $(i = 1, 2, 3)$,

(ii) $C_i(n)^{s_{123}s_r} \cap L_i(n)^{s_{123}s_r} \neq \varnothing$ $(i = 4, 5, 6)$.

6. Some Results on Prime Numbers

In this section, we study prime numbers satisfying the conditions (A1), (A2) introduced in §5.

Let p be a prime integer. If p satisfies (A1), then $p = 10k+1$ or $p = 10k-1$ for an integer k. In the sequel, we always assume that p is a prime satisfying (A1) and let $n \in \mathbf{Z}$ be so taken that $n^2 \equiv 5\,(p)$.

It is interesting to determine such prime numbers satisfying the condition in Theorem 5. The following theorem answers this question.

Theorem 6. *Let p be a prime number with $5 < p$. Then there is $n \in \mathbf{F}_p$ such that $n^2 \equiv 5\,(p)$ and there is no $m \in \mathbf{F}_p$ such that $m^2 \equiv 2n-5\,(p)$ if and only if $p = 10k-1$ for a positive integer k.*

The outline of his proof is as follow. By the assumption of the theorem, we get an equation of degree 4 over $\mathbf{Q}$. The field generated by one of the roots of this equation is nothing but the cyclotomic field $\mathbf{Q}(\zeta)$ generated by the fifth root ζ of unity. It is well known that a rational prime splits completely if and only if $p \equiv 1(5)$. This is rougly the condition that there exists the number m in Theorem 6. But $p \equiv \pm 1(5)$ by the existence of n (if p is not 2). So we have $p \equiv -1(5)$. Since we assumed the p is odd, we have $p \equiv -1(10)$, too.

Remark 4. *The author proved Theorem 6 for such primes that $p < 1000$ by direct computation. Later T. Ibukiyama proved for an arbitrary prime p $(5 < p)$.*

7. Concluding Remarks

(1) The condition for a prime number p that there is $n \in \mathbf{Z}$ such that $n^2 \equiv 5 \ (p)$ is equivalent to the condition that the twenty seven lines on the Clebsch diagonal surface $x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 = 0$, $x_1 + x_2 + x_3 + x_4 + x_5 = 0$ are defined over the prime number field $\mathbf{F}_p$.

(2) Let p be a prime number such that $\left(\dfrac{5}{p}\right) = -1$. In this case, we consider a field extension $\mathbf{F}_p(\boldsymbol{n})$ over $\mathbf{F}_p$ attaching $\boldsymbol{n}$ such that $\boldsymbol{n}^2 = 5$ in $\mathbf{F}_p$. Let $\mathbf{P}^2(\mathbf{F}_p(\boldsymbol{n}))$ be a projective plane over $\mathbf{F}_p(\boldsymbol{n})$. Then it is possible to define systems of six labelled lines on $\mathbf{P}^2(\mathbf{F}_p(\boldsymbol{n}))$ with conditions (C1), (C2), (C3). In this case, by direct computation, the condition for the existence of a system of six labelled lines of type III and fixed by the group $H(5)$ is equivalent to that there is no pair $(a, b) \in \mathbf{Z}^2$ such that $(a\boldsymbol{n} + b)^2 = 2\boldsymbol{n} - 5$ in $\mathbf{F}_p(\boldsymbol{n})$, which is also equivalent to the condition that there is no pair $(a, b) \in \mathbf{Z}^2$ such that $5a^2 + b^2 \equiv -5$, $ab \equiv 1 \ (p)$. It is easy to show that if $p \not\equiv \pm 1 \ (5)$, then there is no pair (a, b) of integers satisfying the conditions $5a^2 + b^2 \equiv -5$, $ab \equiv 1 \ (p)$. As a consequence, we conclude that there is a system of six labelled lines of type III and fixed by the group $H(5)$ on $\mathbf{P}^2(\mathbf{F}_p(\boldsymbol{n}))$.

The author thanks his colleague Professor H. Maeda for the discussion between them on number theory being very useful to formulate Theorem 5 in §4 and Professor T. Ibukiyama for proving it and kindly explaining the proof to the author. The author was partially supported by Grand-in-Aid for Scientific Research (No. 17540013), Japan Society for the Promotion of Science.

References

[1] B.Grünbaum, Convex Polytopes. Interscience (1967).

[2] J.Sekiguchi, M.Yoshida, $W(E_6)$-action on the configuration space of 6 points of the real projective plane. *Kyushu J. Math.*, **51**(1997), 297-354.

[3] I.Naruki, Cross ratio variety as a moduli space of cubic surfaces. *Proc. London Math. Soc.* **45**(1982), 1-30.