

An Observation on the Hexagonal Lattice and Its Application to Néron-severi Groups

Mari Ohhira

Department of Mathematics, Faculty of Science,
Ochanomizu University

(Received October 2, 1993)

§ 0. Introduction

The Mordell-Weil lattice theory of Shioda ([7]) is a very powerful tool for the study of elliptic surfaces and gives many important results on algebraic surfaces, which include the complete classification of rational elliptic surfaces by their Mordell-Weil lattices ([4]). But in general the determination of the Mordell-Weil lattice of arbitrary elliptic surfaces is not so easy because of the bigness of their Picard numbers, and neither is the study of Néron-Severi groups which relate closely to the Mordell-Weil lattices.

Let X be a non-singular projective surface defined over an algebraically closed field k of positive characteristic p . X is called unirational if there exists a generically surjective rational mapping from the projective plane P^2 to X . Let $\pi: S \rightarrow C$ be a unirational elliptic surface defined over k . S is said to be of base change type if there exists a curve C' and a morphism f from C' to C such that the fiber product $S \times_C C'$ is rational. The classification of irrational unirational elliptic surfaces of base change type by singular fibers is given in [2, 5].

In [6], we calculate the determinant of Néron-Severi groups of unirational elliptic surfaces of base change type in characteristic 2 by using the results of Oguiso and Shioda mentioned above. The situation is greatly simplified due to the existence of generators of the Mordell-Weil lattices of short length.

The purpose of this paper is the same as that of [6], but we study in characteristic bigger than 3. We know that increasing of characteristics makes generators of Mordell-Weil lattices longer and longer. So, we must start from detailed study of generators of lattices.

So, the organization of this paper is as follows. In section 1, we observe the hexagonal lattice and give it the "shortest" representation by modulus p (Theorem 1.8).

In section 2, we review on Mordell-Weil lattices and unirational elliptic

surfaces of base change type, and then prepare to calculate the determinant of the Néron-Severi group of these unirational surfaces.

In section 3, we set up the algorithm of calculation for the determinant of the Néron-Severi group of unirational elliptic surfaces with specific Mordell-Weil lattices. Precisely, their Mordell-Weil lattice is included in the product of two hexagonal lattices. Finally, we analyze the determinant in characteristic $p \leq 41$, using a formula-transforming program "Mathematica" (Theorem 3.8).

§ 1. The shortest representation of the hexagonal lattice.

The main reference of this section is [1].

For the 2-dimensional real vector space \mathbf{R}^2 with a fixed basis, we define the following:

$P[x, y]$ or $[x, y]$: the coordinate of a point $P \in \mathbf{R}^2$,

$O[0, 0]$: the origin of \mathbf{R}^2 ,

$\langle, \rangle: \mathbf{R}^2 \times \mathbf{R}^2 \rightarrow \mathbf{R}; P[x, y] \times P'[x', y'] \mapsto xx' + yy' = |P||P'|\cos\theta$: the ordinary inner product where θ is the difference of arguments of P and P' .

DEFINITION 1.1. (1) The hexagonal lattice A is a lattice in \mathbf{R}^2 , spanned by $e=[1, 0]$ and $f=[1/2, \sqrt{3}/2]$:

$$(1.1) \quad A = \{[x, y] \in \mathbf{R}^2 \mid \alpha, \beta \in \mathbf{Z}, x = \alpha + \beta/2, y = \sqrt{3}\beta/2\},$$

with the ordinary inner product \langle, \rangle .

We denote the point $P[\alpha + \beta/2, \sqrt{3}\beta/2] \in A$ by $P(\alpha, \beta)$, or (α, β) and rewrite the formula of the ordinary inner product as follows:

$$(1.2) \quad \langle, \rangle; (\alpha, \beta) \times (\alpha', \beta') \mapsto \alpha\alpha' + \beta\beta' + (\alpha\beta' + \beta\alpha')/2.$$

(2) For an arbitrary positive integer N , we denote the quotient group A/NA by A_N .

We call $|P|^2 = \langle P, P \rangle$ the length of $P \in \mathbf{R}^2$ for convenience, although it is the power of its length exactly.

REMARK 1.2. In usual the notation of the hexagonal lattice is used for $A_2 = A(2)$, which is isomorphic to A as an Abelian group and its inner product equals 2 \langle, \rangle .

We denote by G the automorphism group of A which is the dihedral group of order 12, and fix its generators as follows:

$$(1.3) \quad \begin{aligned} G \ni \sigma: (\alpha, \beta) = [x, y] &\mapsto [(x - \sqrt{3}y)/2, (\sqrt{3}x + y)/2] = (-\beta, \alpha + \beta), \\ \tau: (\alpha, \beta) = [x, y] &\mapsto [-x, y] = (-\alpha - \beta, \beta). \end{aligned}$$

G acts canonically on \mathbf{R}^2 , and \mathbf{R}^2 is separated to twelve areas \mathcal{A}' ($1 \leq \iota \leq 12$) which are transitive each other :

$$(1.4) \quad \mathcal{A}' = \{[x, y] \in \mathbf{R}^2 \mid \tan((\iota-1)\pi/6)x \leq y \leq \tan(\iota\pi/6)x\}.$$

It is convenient to handle a point $P \in A$ and its orbits together.

DEFINITION 1.3. For a point $P(\alpha, \beta)$ in A , we define as follows :

$$(1.5) \quad \begin{aligned} AV(\alpha, \beta) &= \{\rho((\alpha, \beta))\}_{\rho \in G}, \\ av(\alpha, \beta) &= \text{Card. } AV(\alpha, \beta). \end{aligned}$$

LEMMA 1.4. Let α and β be a pair of integers.

(1) There exists a pair of integers, say, α' and β' , which satisfies that $\alpha' \geq \beta' \geq 0$ and that $AV(\alpha, \beta) = AV(\alpha', \beta')$.

(2) Assuming $\alpha \geq \beta \geq 0$, it follows that

$$AV(\alpha, \beta) = \begin{cases} 1 & \text{if } \alpha = \beta = 0. \\ 6 & \text{if } \alpha = \beta \neq 0, \text{ or } \alpha > \beta = 0, \\ 12 & \text{otherwise.} \end{cases}$$

PROOF. Immediate. □

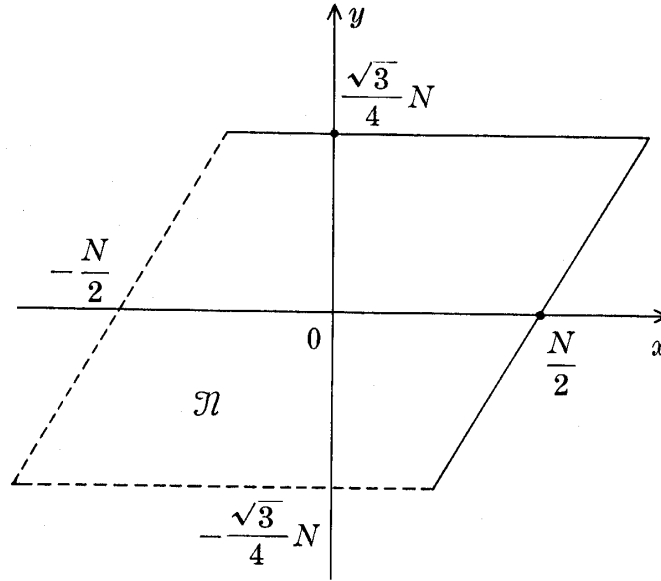
Let N be a fixed positive integer. It is trivial that the quotient group A_N has the following representation system, which is very naive and intuitive :

DEFINITION-LEMMA 1.5. Set the following notations :

$$\begin{aligned} \mathcal{A}_{\mathcal{N}(N)} &= \mathcal{A}_{\mathcal{N}} = \{[x, y] \in \mathbf{R}^2 \mid -\sqrt{3}N/4 < y \leq \sqrt{3}N/4, \\ &\quad \sqrt{3}(x - N/2) \leq y < \sqrt{3}(x + N/2)\}, \\ \mathcal{N} &= \mathcal{N}_N = \mathcal{A}_{\mathcal{N}} \cap A. \end{aligned}$$

Then \mathcal{N} gives a representation system of the quotient group $A_N = A/NA$.

PROOF. trivial (See Picture 1.1.)



Picture 1.1.

□

The main objective of this section is to give A_N the “best” representation. In our sense, such a representation satisfies the condition of the following definition:

DEFINITION 1.6. Let (L, \langle, \rangle) be any finite dimensional quadratic module with the inner product \langle, \rangle , L' be its subgroup, and \mathcal{S} be a representation system of L/L' . \mathcal{S} is called the shortest representation of L/L' if it satisfies the following condition (*) for all $s \in \mathcal{S}$.

(*) For any element $s' \in s + L'$, it holds that $\langle s, s \rangle \leq \langle s', s' \rangle$.

The shortest representation of the hexagonal lattice is given in the following:

DEFINITION-LEMMA 1.7. Set the following notations:

$$\mathcal{A}_{\mathcal{H}(N)} = \mathcal{A}_{\mathcal{H}} = \{[x, y] \in \mathbf{R}^2 \mid -N/2 < x \leq N/2, (x-N)/\sqrt{3} \leq y < (x+N)/\sqrt{3}, \\ -(x+N)/\sqrt{3} \leq y < -(x-N)/\sqrt{3}\},$$

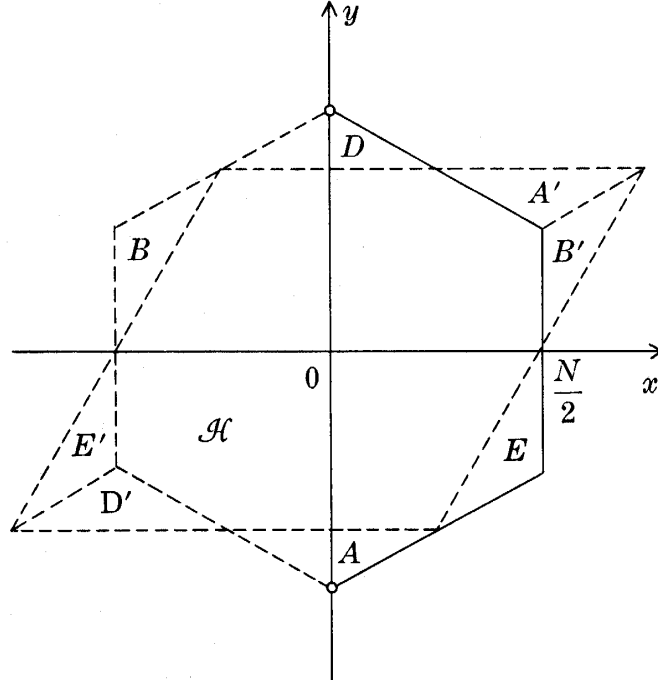
$$\mathcal{H} = \mathcal{H}_N = \mathcal{A}_{\mathcal{H}} \cap A,$$

$$\overline{\mathcal{H}} = \overline{\mathcal{A}_{\mathcal{H}}} \cap A,$$

$$\partial \mathcal{H} = (\partial \overline{\mathcal{A}_{\mathcal{H}}}) \cap A.$$

It holds that \mathcal{H} gives a representation system of the quotient group $A_N = A/NA$.

PROOF. \mathcal{H} and \mathcal{N} have 1:1-correspondence like Picture 1.2. ($A \leftrightarrow A'$, $B \leftrightarrow B'$, $D \leftrightarrow D'$, $E \leftrightarrow E'$.) Our lemma follows from this correspondence.



Picture 1.2.

□

THEOREM 1.8. \mathcal{H} gives the shortest representation of A , and the shortest representation of A is unique up to the choice of the boundary. Precisely, for all $P \in \mathcal{H}$ and for all $Q \in A \setminus \{0\}$, it hold that

$$(1.6) \quad |P + NQ|^2 \geq |P|^2,$$

where the equation holds when it suffices the following:

$$(1.7) \quad P, P + NQ \in \partial \mathcal{H}.$$

PROOF. Since it holds that $|P + NQ|^2 = |P|^2 + N^2|Q|^2 + 2N|P||Q|\cos\theta$ where θ is the difference of the argument of P and Q , it is sufficient to show the following (1.8):

$$(1.8) \quad N|Q| \geq -2|P|\cos\theta.$$

We remark that $|P| \leq N/\sqrt{3}$ for all $P \in \mathcal{H}$. If $|Q| \geq \sqrt{3}$, (1.8) holds without the sign of equality because $N|Q| \geq \sqrt{3}N \geq 2N/\sqrt{3} \geq -2|P| \geq |P|\cos\theta$. So we may assume that $|Q| = 1$.

If it also suffices that $|P| \leq N/2$, then we verify (1.8) at once, with the condition for the sign of equality, i. e.

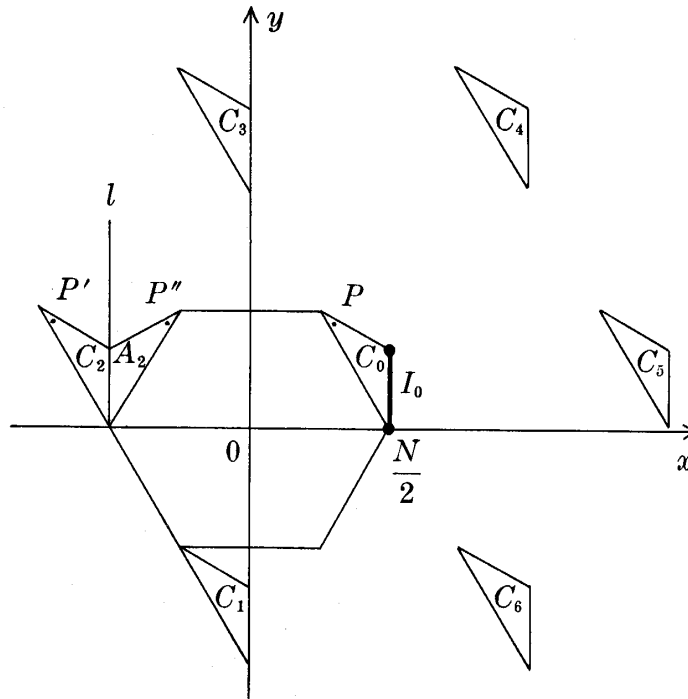
$$(1.9) \quad |P| = N/2, \text{ and } \cos \theta = \pi.$$

Remark that (1.9) yields that $NQ = -2P$, and we see that (1.7) holds.

Assume $N/2 < P \leq N/\sqrt{3}$ now. We can assume $P \in C_0$, where the closed triangle C_0 is as in Picture 1.3, due to the existence of many symmetry of the regular hexagon $\overline{\mathcal{A}_{\mathcal{H}}}$.

C_0 becomes C_1, C_2, \dots , or C_6 in Picture 1.3 after the translation by an elements of $NAV(1, 0)$. For $3 \leq i \leq 6$, it is evident that all the elements in $C_i \cap A$ are longer than any elements in $C_0 \cap A$.

Assume $P' \in (P + NA) \cap C_2$. It suffices to show that $|P'| \geq |P|$. Let P'' be the image of P by symmetry at y -axis. It holds that $|P''| = |P|$. P'' is also the image of P' by symmetry at the line l , and the origin O is at the same side as P'' . So, we see that $|P'| \geq |P''|$, and that the equality holds only when $P \in I_0 \subset \partial \mathcal{H}$.



Picture 1.3.

If $P' \in (P + NA) \cap C_1$, the proof is similar. □

COROLLARY 1.9. *Every element of A/NA can be represented by $P \in \mathcal{H}$, whose length $\langle P, P \rangle$ satisfies the following:*

$$(1.10) \quad \langle P, P \rangle \leq \begin{cases} N^2/3 & \text{if } N \equiv 0 \pmod{3}, \\ (N^2 - 2N + 4)/3 & \text{if } N \equiv 1 \pmod{3}, \\ (N^2 - N + 1)/3 & \text{if } N \equiv 2 \pmod{3}. \end{cases}$$

PROOF. Immediate. □

§ 2. Néron-Severi groups

In this section we use the following notations:

p : a rational prime number which satisfies the following (2.1):

$$(2.1) \quad p \geq 5 \quad \text{and} \quad p \equiv 2 \pmod{3},$$

k : an algebraically closed field of characteristic p ,

$K = k(t)$: the 1-dimensional rational function field over k ,

E/K : an elliptic curve over K with the following Weierstrass normal form:

$$(2.2) \quad y^2 = x^3 + t^4(t-1)^5(t-\alpha)^5,$$

where $\alpha \in k \setminus \{0, 1\}$.

$f: X \rightarrow \mathbf{P}^1$: the relatively minimal model of E ,

$NS(X)$: Néron-Severi Group of X with the quadratic form by intersection,

$\langle S = E(K), \langle, \rangle_s \rangle$: the Mordell-Weil lattice ([7]) of E with the height pairing \langle, \rangle_s ,

$K' = k(t^{1/p})$: the purely inseparable extension of degree p ,

$f_0: \mathbf{P}^1 \rightarrow \mathbf{P}^1$: the purely inseparable morphism of degree p corresponding to the field extension K'/K ,

$\langle S' = E'(K'), \langle, \rangle_{s'} \rangle$: the Mordell-Weil lattice of $E' = E \times K'$ over K' with the height pairing $\langle, \rangle_{s'}$,

$\iota: S \rightarrow S'$: the natural injection,

$\tilde{S} := \text{Im}(\iota)$.

E/K is our main object in this section, and the following lemma holds.

LEMMA 2.1. (1) S' is a Mordell-Weil lattice of an elliptic fibration of a rational surface over k and isomorphic to $(A(2/3))^{\oplus 2}$.

(2) The following equation holds:

$$(2.3) \quad [S' : \tilde{S}] = |\det NS(X)|^{1/2} p^2.$$

PROOF. From Katsura ([2]), we see that all the singular fibers of f are $f^{-1}(0)$ and $f^{-1}(\infty)$ which are of type C_6 (cf. Néron [3]), and $f^{-1}(1)$ and $f^{-1}(\alpha)$ which are of type C_8 (cf. *loc. cit.*). Katsura [2] also tells us that these fibers become, respectively, two fibers of type C_3 (cf. *loc. cit.*) and two fibers of type C_1 (cf. *loc. cit.*) of the elliptic surface $f': X' = X \times_{\mathbf{P}^1} \mathbf{P}^1 \rightarrow \mathbf{P}^1$. So, from the table of Main Theorem of [4], we see that $S' \cong (A(2/3))^{\oplus 2}$. This shows (1).

(2) is deduced from the following :

$$(2.4) \quad [S' : \tilde{S}] = \frac{|\det NS(X)|^{1/2} p^2 \#tor}{\det S' \prod m_v^{(1)}},$$

where $\#tor$ is the number of torsion points of S' , and $m_v^{(1)}$ is the number of irreducible components of multiplicity 1 of the fiber $f^{-1}(v)$ for $v \in \mathbf{P}^1$.

The proof of (2.4) is almost the same as that of Lemma 2.1 in [6]. \square

REMARK 2.2. Lemma 2.1 tells us that the calculation of $\det NS(X)$ is equivalent to that of $[S' : \tilde{S}]$.

From some experiments described in §3, we set the following conjecture.

CONJECTURE 2.3. *For every rational prime number p which satisfies (2.1), the following equation holds:*

$$(2.5) \quad |\det NS(X)| = p^4.$$

§3. Numerical experiments using “Mathematica”

In this section we use the same notations as in §2, unless otherwise mentioned.

From Remark 2.2, Conjecture 2.3 is equivalent to the following :

CONJECTURE 3.1. *For every rational prime number p satisfying (2.1), the following two equivalent equation hold:*

$$(3.1) \quad [S' : \tilde{S}] = p^4,$$

or

$$(3.2) \quad \tilde{S}/pS' = 0,$$

PROOF OF EQUIVALENCE. Since the endomorphism of multiplication by p over E' is the composition of the Frobenius map over the prime field and its dual, we see that $\tilde{S} \supseteq pS'$. So, (3.1) is equivalent to (3.2). \square

To do all the computation on the hexagonal lattice A , we use the following relation between lattices.

LEMMA 3.2. *There exist the following injection ι and the isomorphism ϕ of lattices as in (3.3), whose quadratic forms relate to each other as in (3.4).*

$$(3.3) \quad (S, \langle, \rangle_s) \xrightarrow{\iota} (S', \langle, \rangle_{s'}) \xrightarrow{\phi} (A^{\oplus 2}, \langle, \rangle),$$

$$(3.4) \quad \langle \phi \circ \iota(P), \phi \circ \iota(Q) \rangle = \frac{3}{2} \langle \iota(P), \iota(Q) \rangle_{s'} = \frac{3p}{2} \langle P, Q \rangle_s,$$

where $P, Q \in S$.

PROOF. This is from the functoriality of height pairing (Proposition 8.12 in [7]) and Lemma 2.1. \square

Next we determine values of lengths of elements of $\text{Im}(\phi \circ \iota)$.

LEMMA 3.3. For $P \in S$, $\langle \phi \circ \iota(P), \phi \circ \iota(P) \rangle$ is in \mathfrak{L} , which is defined as follows:

$$(3.5) \quad \mathfrak{L} = \{jp \mid j \text{ is a natural number s.t. } j=5 \text{ or } j \geq 7\}.$$

PROOF. From the definition of the height pairing, the length of P in S is as follows:

$$(3.6) \quad \langle P, P \rangle_s = 2\chi + 2(P) \cdot (O) - \sum_{t \in P^1} \text{Contr}_v(P, P),$$

where χ is the arithmetic genus of X , $2(P) \cdot (O)$ is intersection of sections (P) and (O) which are corresponding to P and the zero point O respectively, $\text{Contr}_v(P, P)$ is contribution of the fiber $f^{-1}(v)$. From the facts in §2, table (8.16) in [7], and Lemma 3.2, we get (3.5). \square

By the way, since $A^{\oplus 2}/p$ has the representation system $\mathcal{H}^{\oplus 2}$, if there exists some non-zero elements of $\text{Im}(\phi \circ \iota)/(pA^{\oplus 2})$, it can be represented by the element whose length is equal to or less than $2(p^2 - p + 1)/3$ (cf. Corollary 1.9).

So, if the answer of the following Problem 3.4 is “yes”, Conjecture 3.1 holds.

PROBLEM 3.4. Assume there exists a subgroup H of $A^{\oplus 2}/p$ such that every element of H can be represented by $P \in A^{\oplus 2}$ which satisfies the following:

$$(3.7) \quad \langle P, P \rangle \in \mathfrak{L}',$$

where

$$(3.8) \quad \mathfrak{L}' = \{\ell \in \mathfrak{L} \mid \ell \leq 2(p^2 - p + 1)/3\}.$$

Then is H the zero-group?

To test Problem 3.4 for fixed p , we can apply the following algorithm.

ALGORITHM 3.5. (0) Collect the elements $P \in A^{\oplus 2}$ which satisfy (3.7).
(We denote the set of these collected elements by SET0).

(1) Collect the elements $P \in \text{SET0}$ which satisfy the following:

$$(3.9) \quad \exists Q \in \text{SET0}, \text{ s.t. } 2P \equiv Q \pmod{pA^{\oplus 2}}.$$

(We denote the set of these collected elements by SET1).

(2) Substitute SET1 for SET0.

(3) Repeat from (1) to (2) for $p-1/2$ times.

(4) Put SET0 into SET2.

(5) If SET2 equals $\{0\}$, we answer to Problem 3.4 positively.

If SET2 remains non-zero element, Conjecture 3.1 is still open.

NOTATION 3.6. Fix p satisfying (2.1). Let \mathfrak{S}_p be the family of subgroups of $A^{\oplus 2}/p$ which are generated by elements of SET2 mod p .

For $\mathfrak{s} \in \mathfrak{S}_p$, let $l(\mathfrak{s})$ the shortest positive length of elements of $\mathcal{H}_p^{\oplus 2}$ which represent elements of \mathfrak{s} .

We denote the set of $2l(\mathfrak{s})/3p$ by \mathfrak{T}_p :

$$(3.10) \quad \mathfrak{T}_p = \{2l(\mathfrak{s})/3p \mid \mathfrak{s} \in \mathfrak{S}_p\}.$$

When SET2 remains non-zero, to solve Conjecture 3.1 is reduced to solve the following Problem 3.7.

PROBLEM 3.7. Let \mathcal{E}_p be the set of points in S whose length belongs to \mathfrak{T}_p . Is \mathcal{E}_p empty?

Lists in §A are examples of the programs and outputs of "Mathematica" based on the above algorithm. From these results, we get the following:

THEOREM 3.8. (1) (3.1) holds for $p \leq 23$.

(2) $\mathfrak{T}_{29} = \{10/3\}$, $\mathfrak{T}_{41} \subset \{10/3, 14/3, 16/3, 20/3, 28/3\}$.

REMARK 3.9. The computation for $p=41$ takes about 13 hours on NEC PC-9821.

§ A. Lists

A.1. Program 1

```

Date[]>>\ohhira\out1
p=29
ip[a_,b_] :=a^2 + a*b + b^2
mbt=Sort[Flatten[
    Table[
        Table[
            {ip[a,b],{a,b}},
            {b,0,a}],
        {a,1,p/2}],1]
]>>>\ohhira\out1
dimbt=Dimensions[mbt][[1]]
hex1={};
Do[Block[
    {p1=mbt[[i]],a=mbt[[i,2,1]],b=mbt[[i,2,2]]},
    If[a<p/3,AppendTo[hex1,p1],
        If[
            (a<p/2) && (b<=p-2*a),AppendTo[hex1,p1]
        ]
    ],
    {i,1,dimbt}];
hex1>>>\ohhira\out1
cl={};
Do[
    Do[Block[{cle=p*(d+3*n)},If[cle<=2*(p^2-p+1)/3,
        AppendTo[cl,cl
e]
    ],
    {n,0,(2p-3d)/9}]
, {d,5,9,2}];
cl>>>\ohhira\out1
clv2={};clv1={};
Do[
    Do[
        Do[
            If[hex1[[j,1]]+hex1[[k,1]]==cl[[i]],
                If[FreeQ[clv2,{hex1[[k]],hex1[[j]]}],
                    clv2
                    =Union[clv2,{{hex1[[j]],hex1[[k]]}}]
                ];
            clv1=Union[clv1,{hex1[[j]]}];
            clv1=Union[clv1,{hex1[[k]]}];
        ],
        {k,Dimensions[hex1][[1]]}
    ],
    {j,Dimensions[hex1][[1]]}
, {i,Dimensions[cl][[1]]}];
clv1>>>\ohhira\out1
clv2>>>\ohhira\out1
clv3={};clv4={};
Do[

```

```

Block[{a=clv1[[1,2,1]],b=clv1[[1,2,2]],a2,b2},
If[ (a<p/6)
|((a>p/6)&&(a<p/4)&&(b<=p/2-2*a)),
a2=2*a;b2=2*b];
If[ ( (a>p/6)&&(a<p/4)&&(b>p/2-2*a)
&&(b<=(p-2*a)/4)
)
|((a>p/4)&&(b<=(p-2*a)/4)),
a2=p-2*a-2*b;b2=2*b];
If[ ((a>p/6)&&(a<p/4)&&(b>(p-2*a)/4))
|((a>p/4)&&(b>(p-2*a)/4)&&(b<=(p-2*a)/2)),
b2=p-2*a-2*b;a2=2*b];
If[(a>p/4)&&(b>(p-2*a)/2),
a2=p-2*a;b2=-p+2*a+2*b];
AppendTo[clv3,{clv1[[i]],{ip[a2,b2],{a2,b2}}}]
]
,{i,Dimensions[clv1][[1]]}};
clv4=clv3
clv4>>>\ohhira\out1
clv5={};clv6=clv2;
Do[Block[{dim2=Dimensions[clv2][[1]]},
clv5={};
Do[Block[{p1=clv2[[j]],q1=clv2[[j,1]],
r1=clv2[[j,2]],p2,q2,r2,
postb1
},
postb1=Position[clv4,q1];
If[postb1[[1,2]]==2
,q2=clv4[[postb1[[2,1]],2]]
,q2=clv4[[postb1[[1,1]],2]]
];
postb1=Position[clv4,r1];
If[postb1[[1,2]]==2
,r2=clv4[[postb1[[2,1]],2]]
,r2=clv4[[postb1[[1,1]],2]]
];
p2={q2,r2};
If[MemberQ[clv2,p2]||MemberQ[clv2,{r2,q2}]
,clv5=Union[clv5,{p2}]
];
],{j,dim2}};
clv2=clv5;
clv2>>>\ohhira\out1;
Print[clv2];
If[Dimensions[clv2][[1]]==0,Break[]];
],{i,(p-1)/2}};
clv5>>>\ohhira\out1
Date[]>>>\ohhira\out1

```

A.2. Output for $p=17$.

```

{{1, {1, 0}}, {3, {1, 1}}, {4, {2, 0}}, {7, {2, 1}}, {9, {3, 0}},
 {12, {2, 2}}, {13, {3, 1}}, {16, {4, 0}}, {19, {3, 2}}, {21, {4, 1}},
 {25, {5, 0}}, {27, {3, 3}}, {28, {4, 2}}, {31, {5, 1}}, {36, {6, 0}},
 {37, {4, 3}}, {39, {5, 2}}, {43, {6, 1}}, {48, {4, 4}}, {49, {5, 3}},
 {49, {7, 0}}, {52, {6, 2}}, {57, {7, 1}}, {61, {5, 4}}, {63, {6, 3}},
 {64, {8, 0}}, {67, {7, 2}}, {73, {8, 1}}, {75, {5, 5}}, {76, {6, 4}},
 {79, {7, 3}}, {84, {8, 2}}, {91, {6, 5}}, {93, {7, 4}}, {97, {8, 3}},
 {108, {6, 6}}, {109, {7, 5}}, {112, {8, 4}}, {127, {7, 6}}, {129, {8, 5}},
 {147, {7, 7}}, {148, {8, 6}}, {169, {8, 7}}, {192, {8, 8}}}
{{1, {1, 0}}, {3, {1, 1}}, {4, {2, 0}}, {7, {2, 1}}, {9, {3, 0}},
 {12, {2, 2}}, {13, {3, 1}}, {16, {4, 0}}, {19, {3, 2}}, {21, {4, 1}},
 {25, {5, 0}}, {27, {3, 3}}, {28, {4, 2}}, {31, {5, 1}}, {36, {6, 0}},
 {37, {4, 3}}, {39, {5, 2}}, {43, {6, 1}}, {48, {4, 4}}, {49, {5, 3}},
 {49, {7, 0}}, {52, {6, 2}}, {57, {7, 1}}, {61, {5, 4}}, {63, {6, 3}},
 {64, {8, 0}}, {67, {7, 2}}, {73, {8, 1}}, {75, {5, 5}}, {76, {6, 4}},
 {79, {7, 3}}, {91, {6, 5}}}
{85, 136, 119, 170, 153}
{{9, {3, 0}}, {12, {2, 2}}, {21, {4, 1}}, {28, {4, 2}}, {36, {6, 0}},
 {37, {4, 3}}, {43, {6, 1}}, {48, {4, 4}}, {49, {5, 3}}, {49, {7, 0}},
 {52, {6, 2}}, {57, {7, 1}}, {61, {5, 4}}, {63, {6, 3}}, {64, {8, 0}},
 {67, {7, 2}}, {73, {8, 1}}, {75, {5, 5}}, {76, {6, 4}}, {79, {7, 3}},
 {91, {6, 5}}}
{{{9, {3, 0}}, {76, {6, 4}}}, {{12, {2, 2}}, {73, {8, 1}}},
 {{21, {4, 1}}, {64, {8, 0}}}, {{28, {4, 2}}, {57, {7, 1}}},
 {{28, {4, 2}}, {91, {6, 5}}}, {{36, {6, 0}}, {49, {5, 3}}},
 {{36, {6, 0}}, {49, {7, 0}}}, {{37, {4, 3}}, {48, {4, 4}}},
 {{43, {6, 1}}, {76, {6, 4}}}, {{52, {6, 2}}, {67, {7, 2}}},
 {{57, {7, 1}}, {79, {7, 3}}}, {{61, {5, 4}}, {75, {5, 5}}},
 {{63, {6, 3}}, {73, {8, 1}}}, {{79, {7, 3}}, {91, {6, 5}}}}
{{{9, {3, 0}}, {36, {6, 0}}}, {{12, {2, 2}}, {48, {4, 4}}},
 {{21, {4, 1}}, {67, {7, 2}}}, {{28, {4, 2}}, {61, {5, 4}}},
 {{36, {6, 0}}, {25, {5, 0}}}, {{37, {4, 3}}, {63, {6, 3}}},
 {{43, {6, 1}}, {19, {3, 2}}}, {{48, {4, 4}}, {73, {8, 1}}},
 {{49, {5, 3}}, {43, {6, 1}}}, {{49, {7, 0}}, {9, {3, 0}}},
 {{52, {6, 2}}, {21, {4, 1}}}, {{57, {7, 1}}, {7, {2, 1}}},
 {{61, {5, 4}}, {57, {7, 1}}}, {{63, {6, 3}}, {31, {5, 1}}},
 {{64, {8, 0}}, {1, {1, 0}}}, {{67, {7, 2}}, {13, {3, 1}}},
 {{73, {8, 1}}, {3, {1, 1}}}, {{75, {5, 5}}, {79, {7, 3}}},
 {{76, {6, 4}}, {49, {5, 3}}}, {{79, {7, 3}}, {27, {3, 3}}},
 {{91, {6, 5}}, {75, {5, 5}}}}
{{{36, {6, 0}}, {49, {5, 3}}}, {{57, {7, 1}}, {79, {7, 3}}},
 {{61, {5, 4}}, {75, {5, 5}}}, {{63, {6, 3}}, {73, {8, 1}}}}
{{{57, {7, 1}}, {79, {7, 3}}}}
{}
{}

```

A.3. Output for $p=29$.

```

(1993, 9, 30, 16, 48, 7)
{{(1, {1, 0}), {3, {1, 1}), {4, {2, 0}), {7, {2, 1}), {9, {3, 0}),
  {12, {2, 2}), {13, {3, 1}), {16, {4, 0}), {19, {3, 2}), {21, {4, 1}),
  {25, {5, 0}), {27, {3, 3}), {28, {4, 2}), {31, {5, 1}), {36, {6, 0}),
  {37, {4, 3}), {39, {5, 2}), {43, {6, 1}), {48, {4, 4}), {49, {5, 3}),
  {49, {7, 0}), {52, {6, 2}), {57, {7, 1}), {61, {5, 4}), {63, {6, 3}),
  {64, {8, 0}), {67, {7, 2}), {73, {8, 1}), {75, {5, 5}), {76, {6, 4}),
  {79, {7, 3}), {81, {9, 0}), {84, {8, 2}), {91, {6, 5}), {91, {9, 1}),
  {93, {7, 4}), {97, {8, 3}), {100, {10, 0}), {103, {9, 2}), {108, {6, 6}),
  {109, {7, 5}), {111, {10, 1}), {112, {8, 4}), {117, {9, 3}),
  {121, {11, 0}), {124, {10, 2}), {127, {7, 6}), {129, {8, 5}),
  {133, {9, 4}), {133, {11, 1}), {139, {10, 3}), {144, {12, 0}),
  {147, {7, 7}), {147, {11, 2}), {148, {8, 6}), {151, {9, 5}),
  {156, {10, 4}), {157, {12, 1}), {163, {11, 3}), {169, {8, 7}),
  {169, {13, 0}), {171, {9, 6}), {172, {12, 2}), {175, {10, 5}),
  {181, {11, 4}), {183, {13, 1}), {189, {12, 3}), {192, {8, 8}),
  {193, {9, 7}), {196, {10, 6}), {196, {14, 0}), {199, {13, 2}),
  {201, {11, 5}), {208, {12, 4}), {211, {14, 1}), {217, {9, 8}),
  {217, {13, 3}), {219, {10, 7}), {223, {11, 6}), {228, {14, 2}),
  {229, {12, 5}), {237, {13, 4}), {243, {9, 9}), {244, {10, 8}),
  {247, {11, 7}), {247, {14, 3}), {252, {12, 6}), {259, {13, 5}),
  {268, {14, 4}), {271, {10, 9}), {273, {11, 8}), {277, {12, 7}),
  {283, {13, 6}), {291, {14, 5}), {300, {10, 10}), {301, {11, 9}),
  {304, {12, 8}), {309, {13, 7}), {316, {14, 6}), {331, {11, 10}),
  {333, {12, 9}), {337, {13, 8}), {343, {14, 7}), {363, {11, 11}),
  {364, {12, 10}), {367, {13, 9}), {372, {14, 8}), {397, {12, 11}),
  {399, {13, 10}), {403, {14, 9}), {432, {12, 12}), {433, {13, 11}),
  {436, {14, 10}), {469, {13, 12}), {471, {14, 11}), {507, {13, 13}),
  {508, {14, 12}), {547, {14, 13}), {588, {14, 14})}}
{{(1, {1, 0}), {3, {1, 1}), {4, {2, 0}), {7, {2, 1}), {9, {3, 0}),
  {12, {2, 2}), {13, {3, 1}), {16, {4, 0}), {19, {3, 2}), {21, {4, 1}),
  {25, {5, 0}), {27, {3, 3}), {28, {4, 2}), {31, {5, 1}), {36, {6, 0}),
  {37, {4, 3}), {39, {5, 2}), {43, {6, 1}), {48, {4, 4}), {49, {5, 3}),
  {49, {7, 0}), {52, {6, 2}), {57, {7, 1}), {61, {5, 4}), {63, {6, 3}),
  {64, {8, 0}), {67, {7, 2}), {73, {8, 1}), {75, {5, 5}), {76, {6, 4}),
  {79, {7, 3}), {81, {9, 0}), {84, {8, 2}), {91, {6, 5}), {91, {9, 1}),
  {93, {7, 4}), {97, {8, 3}), {100, {10, 0}), {103, {9, 2}), {108, {6, 6}),
  {109, {7, 5}), {111, {10, 1}), {112, {8, 4}), {117, {9, 3}),
  {121, {11, 0}), {124, {10, 2}), {127, {7, 6}), {129, {8, 5}),
  {133, {9, 4}), {133, {11, 1}), {139, {10, 3}), {144, {12, 0}),
  {147, {7, 7}), {147, {11, 2}), {148, {8, 6}), {151, {9, 5}),
  {156, {10, 4}), {157, {12, 1}), {163, {11, 3}), {169, {8, 7}),
  {169, {13, 0}), {171, {9, 6}), {172, {12, 2}), {175, {10, 5}),
  {181, {11, 4}), {183, {13, 1}), {189, {12, 3}), {192, {8, 8}),
  {193, {9, 7}), {196, {10, 6}), {196, {14, 0}), {199, {13, 2}),
  {201, {11, 5}), {208, {12, 4}), {211, {14, 1}), {217, {9, 8}),
  {217, {13, 3}), {219, {10, 7}), {223, {11, 6}), {229, {12, 5}),
  {243, {9, 9}), {244, {10, 8}), {247, {11, 7}), {271, {10, 9}}
(145, 232, 319, 406, 493, 203, 290, 377, 464, 261, 348, 435, 522)

```

$\{(1, \{1, 0\}), \{3, \{1, 1\}), \{4, \{2, 0\}), \{7, \{2, 1\}), \{9, \{3, 0\}),$
 $\{12, \{2, 2\}), \{13, \{3, 1\}), \{16, \{4, 0\}), \{19, \{3, 2\}), \{21, \{4, 1\}),$
 $\{28, \{4, 2\}), \{31, \{5, 1\}), \{36, \{6, 0\}), \{37, \{4, 3\}), \{39, \{5, 2\}),$
 $\{43, \{6, 1\}), \{48, \{4, 4\}), \{49, \{5, 3\}), \{49, \{7, 0\}), \{52, \{6, 2\}),$
 $\{57, \{7, 1\}), \{61, \{5, 4\}), \{63, \{6, 3\}), \{64, \{8, 0\}), \{67, \{7, 2\}),$
 $\{73, \{8, 1\}), \{75, \{5, 5\}), \{76, \{6, 4\}), \{79, \{7, 3\}), \{81, \{9, 0\}),$
 $\{84, \{8, 2\}), \{91, \{6, 5\}), \{91, \{9, 1\}), \{93, \{7, 4\}), \{97, \{8, 3\}),$
 $\{100, \{10, 0\}), \{103, \{9, 2\}), \{108, \{6, 6\}), \{109, \{7, 5\}),$
 $\{111, \{10, 1\}), \{112, \{8, 4\}), \{117, \{9, 3\}), \{121, \{11, 0\}),$
 $\{124, \{10, 2\}), \{127, \{7, 6\}), \{129, \{8, 5\}), \{133, \{9, 4\}),$
 $\{133, \{11, 1\}), \{139, \{10, 3\}), \{144, \{12, 0\}), \{147, \{7, 7\}),$
 $\{147, \{11, 2\}), \{148, \{8, 6\}), \{151, \{9, 5\}), \{156, \{10, 4\}),$
 $\{157, \{12, 1\}), \{163, \{11, 3\}), \{169, \{8, 7\}), \{169, \{13, 0\}),$
 $\{171, \{9, 6\}), \{172, \{12, 2\}), \{175, \{10, 5\}), \{181, \{11, 4\}),$
 $\{183, \{13, 1\}), \{189, \{12, 3\}), \{192, \{8, 8\}), \{193, \{9, 7\}),$
 $\{196, \{10, 6\}), \{196, \{14, 0\}), \{199, \{13, 2\}), \{201, \{11, 5\}),$
 $\{208, \{12, 4\}), \{211, \{14, 1\}), \{217, \{9, 8\}), \{217, \{13, 3\}),$
 $\{219, \{10, 7\}), \{223, \{11, 6\}), \{229, \{12, 5\}), \{243, \{9, 9\}),$
 $\{244, \{10, 8\}), \{247, \{11, 7\}), \{271, \{10, 9\})\}$
 $\{(\{1, \{1, 0\}), \{144, \{12, 0\}), \{3, \{1, 1\}), \{229, \{12, 5\}),\}$
 $\{(\{4, \{2, 0\}), \{199, \{13, 2\}), \{7, \{2, 1\}), \{196, \{10, 6\}),\}$
 $\{(\{7, \{2, 1\}), \{196, \{14, 0\}), \{9, \{3, 0\}), \{223, \{11, 6\}),\}$
 $\{(\{12, \{2, 2\}), \{133, \{9, 4\}), \{12, \{2, 2\}), \{133, \{11, 1\}),\}$
 $\{(\{13, \{3, 1\}), \{219, \{10, 7\}), \{16, \{4, 0\}), \{129, \{8, 5\}),\}$
 $\{(\{19, \{3, 2\}), \{271, \{10, 9\}), \{21, \{4, 1\}), \{124, \{10, 2\}),\}$
 $\{(\{21, \{4, 1\}), \{211, \{14, 1\}), \{28, \{4, 2\}), \{117, \{9, 3\}),\}$
 $\{(\{28, \{4, 2\}), \{175, \{10, 5\}), \{31, \{5, 1\}), \{172, \{12, 2\}),\}$
 $\{(\{31, \{5, 1\}), \{201, \{11, 5\}), \{36, \{6, 0\}), \{109, \{7, 5\}),\}$
 $\{(\{36, \{6, 0\}), \{196, \{10, 6\}), \{36, \{6, 0\}), \{196, \{14, 0\}),\}$
 $\{(\{37, \{4, 3\}), \{108, \{6, 6\}), \{39, \{5, 2\}), \{193, \{9, 7\}),\}$
 $\{(\{43, \{6, 1\}), \{189, \{12, 3\}), \{43, \{6, 1\}), \{247, \{11, 7\}),\}$
 $\{(\{48, \{4, 4\}), \{97, \{8, 3\}), \{48, \{4, 4\}), \{271, \{10, 9\}),\}$
 $\{(\{49, \{5, 3\}), \{183, \{13, 1\}), \{49, \{7, 0\}), \{183, \{13, 1\}),\}$
 $\{(\{52, \{6, 2\}), \{93, \{7, 4\}), \{52, \{6, 2\}), \{151, \{9, 5\}),\}$
 $\{(\{57, \{7, 1\}), \{175, \{10, 5\}), \{61, \{5, 4\}), \{84, \{8, 2\}),\}$
 $\{(\{61, \{5, 4\}), \{171, \{9, 6\}), \{61, \{5, 4\}), \{229, \{12, 5\}),\}$
 $\{(\{63, \{6, 3\}), \{169, \{8, 7\}), \{63, \{6, 3\}), \{169, \{13, 0\}),\}$
 $\{(\{64, \{8, 0\}), \{81, \{9, 0\}), \{64, \{8, 0\}), \{139, \{10, 3\}),\}$
 $\{(\{67, \{7, 2\}), \{223, \{11, 6\}), \{73, \{8, 1\}), \{217, \{9, 8\}),\}$
 $\{(\{73, \{8, 1\}), \{217, \{13, 3\}), \{75, \{5, 5\}), \{157, \{12, 1\}),\}$
 $\{(\{75, \{5, 5\}), \{244, \{10, 8\}), \{76, \{6, 4\}), \{127, \{7, 6\}),\}$
 $\{(\{76, \{6, 4\}), \{156, \{10, 4\}), \{76, \{6, 4\}), \{243, \{9, 9\}),\}$
 $\{(\{79, \{7, 3\}), \{124, \{10, 2\}), \{79, \{7, 3\}), \{211, \{14, 1\}),\}$
 $\{(\{81, \{9, 0\}), \{151, \{9, 5\}), \{84, \{8, 2\}), \{148, \{8, 6\}),\}$
 $\{(\{91, \{6, 5\}), \{112, \{8, 4\}), \{91, \{6, 5\}), \{199, \{13, 2\}),\}$
 $\{(\{91, \{9, 1\}), \{112, \{8, 4\}), \{91, \{9, 1\}), \{199, \{13, 2\}),\}$
 $\{(\{93, \{7, 4\}), \{139, \{10, 3\}), \{97, \{8, 3\}), \{193, \{9, 7\}),\}$
 $\{(\{100, \{10, 0\}), \{103, \{9, 2\}), \{100, \{10, 0\}), \{219, \{10, 7\}),\}$
 $\{(\{103, \{9, 2\}), \{129, \{8, 5\}), \{108, \{6, 6\}), \{124, \{10, 2\}),\}$

{{108, {6, 6}}, {211, {14, 1}}}, {{109, {7, 5}}, {181, {11, 4}}},
 {{111, {10, 1}}, {121, {11, 0}}}, {{111, {10, 1}}, {208, {12, 4}}},
 {{117, {9, 3}}, {144, {12, 0}}}, {{121, {11, 0}}, {169, {8, 7}}},
 {{121, {11, 0}}, {169, {13, 0}}}, {{127, {7, 6}}, {163, {11, 3}}},
 {{127, {7, 6}}, {192, {8, 8}}}, {{129, {8, 5}}, {219, {10, 7}}},
 {{133, {9, 4}}, {157, {12, 1}}}, {{133, {9, 4}}, {244, {10, 8}}},
 {{133, {11, 1}}, {157, {12, 1}}}, {{133, {11, 1}}, {244, {10, 8}}},
 {{139, {10, 3}}, {151, {9, 5}}}, {{144, {12, 0}}, {175, {10, 5}}},
 {{147, {7, 7}}, {172, {12, 2}}}, {{147, {7, 7}}, {201, {11, 5}}},
 {{147, {11, 2}}, {172, {12, 2}}}, {{147, {11, 2}}, {201, {11, 5}}},
 {{148, {8, 6}}, {171, {9, 6}}}, {{148, {8, 6}}, {229, {12, 5}}},
 {{156, {10, 4}}, {163, {11, 3}}}, {{156, {10, 4}}, {192, {8, 8}}},
 {{163, {11, 3}}, {243, {9, 9}}}, {{169, {8, 7}}, {208, {12, 4}}},
 {{169, {13, 0}}, {208, {12, 4}}}, {{181, {11, 4}}, {196, {10, 6}}},
 {{181, {11, 4}}, {196, {14, 0}}}, {{183, {13, 1}}, {223, {11, 6}}},
 {{189, {12, 3}}, {217, {9, 8}}}, {{189, {12, 3}}, {217, {13, 3}}},
 {{192, {8, 8}}, {243, {9, 9}}}, {{193, {9, 7}}, {271, {10, 9}}},
 {{217, {9, 8}}, {247, {11, 7}}}, {{217, {13, 3}}, {247, {11, 7}}}
 {{1, {1, 0}}, {4, {2, 0}}}, {{3, {1, 1}}, {12, {2, 2}}},
 {{4, {2, 0}}, {16, {4, 0}}}, {{7, {2, 1}}, {28, {4, 2}}},
 {{9, {3, 0}}, {36, {6, 0}}}, {{12, {2, 2}}, {48, {4, 4}}},
 {{13, {3, 1}}, {52, {6, 2}}}, {{16, {4, 0}}, {64, {8, 0}}},
 {{19, {3, 2}}, {76, {6, 4}}}, {{21, {4, 1}}, {84, {8, 2}}},
 {{28, {4, 2}}, {112, {8, 4}}}, {{31, {5, 1}}, {124, {10, 2}}},
 {{36, {6, 0}}, {144, {12, 0}}}, {{37, {4, 3}}, {148, {8, 6}}},
 {{39, {5, 2}}, {156, {10, 4}}}, {{43, {6, 1}}, {172, {12, 2}}},
 {{48, {4, 4}}, {192, {8, 8}}}, {{49, {5, 3}}, {196, {10, 6}}},
 {{49, {7, 0}}, {196, {14, 0}}}, {{52, {6, 2}}, {208, {12, 4}}},
 {{57, {7, 1}}, {199, {13, 2}}}, {{61, {5, 4}}, {244, {10, 8}}},
 {{63, {6, 3}}, {223, {11, 6}}}, {{64, {8, 0}}, {169, {13, 0}}},
 {{67, {7, 2}}, {181, {11, 4}}}, {{73, {8, 1}}, {147, {11, 2}}},
 {{75, {5, 5}}, {271, {10, 9}}}, {{76, {6, 4}}, {217, {9, 8}}},
 {{79, {7, 3}}, {171, {9, 6}}}, {{81, {9, 0}}, {121, {11, 0}}},
 {{84, {8, 2}}, {133, {9, 4}}}, {{91, {6, 5}}, {219, {10, 7}}},
 {{91, {9, 1}}, {103, {9, 2}}}, {{93, {7, 4}}, {169, {8, 7}}},
 {{97, {8, 3}}, {127, {7, 6}}}, {{100, {10, 0}}, {81, {9, 0}}},
 {{103, {9, 2}}, {93, {7, 4}}}, {{108, {6, 6}}, {229, {12, 5}}},
 {{109, {7, 5}}, {175, {10, 5}}}, {{111, {10, 1}}, {67, {7, 2}}},
 {{112, {8, 4}}, {129, {8, 5}}}, {{117, {9, 3}}, {91, {6, 5}}},
 {{121, {11, 0}}, {49, {7, 0}}}, {{124, {10, 2}}, {61, {5, 4}}},
 {{127, {7, 6}}, {189, {12, 3}}}, {{129, {8, 5}}, {139, {10, 3}}},
 {{133, {9, 4}}, {97, {8, 3}}}, {{133, {11, 1}}, {39, {5, 2}}},
 {{139, {10, 3}}, {63, {6, 3}}}, {{144, {12, 0}}, {25, {5, 0}}},
 {{147, {7, 7}}, {211, {14, 1}}}, {{147, {11, 2}}, {37, {4, 3}}},
 {{148, {8, 6}}, {157, {12, 1}}}, {{151, {9, 5}}, {111, {10, 1}}},
 {{156, {10, 4}}, {73, {8, 1}}}, {{157, {12, 1}}, {19, {3, 2}}},
 {{163, {11, 3}}, {43, {6, 1}}}, {{169, {8, 7}}, {183, {13, 1}}},
 {{169, {13, 0}}, {9, {3, 0}}}, {{171, {9, 6}}, {133, {11, 1}}},
 {{172, {12, 2}}, {21, {4, 1}}}, {{175, {10, 5}}, {91, {9, 1}}},


```

{{181, {11, 4}}, {57, {7, 1}}}, {{183, {13, 1}}, {7, {2, 1}}},
{{189, {12, 3}}, {31, {5, 1}}}, {{192, {8, 8}}, {217, {13, 3}}},
{{193, {9, 7}}, {163, {11, 3}}}, {{196, {10, 6}}, {117, {9, 3}}},
{{196, {14, 0}}, {1, {1, 0}}}, {{199, {13, 2}}, {13, {3, 1}}},
{{201, {11, 5}}, {79, {7, 3}}}, {{208, {12, 4}}, {49, {5, 3}}},
{{211, {14, 1}}, {3, {1, 1}}}, {{217, {9, 8}}, {201, {11, 5}}},
{{217, {13, 3}}, {27, {3, 3}}}, {{219, {10, 7}}, {151, {9, 5}}},
{{223, {11, 6}}, {109, {7, 5}}}, {{229, {12, 5}}, {75, {5, 5}}},
{{243, {9, 9}}, {247, {11, 7}}}, {{244, {10, 8}}, {193, {9, 7}}},
{{247, {11, 7}}, {147, {7, 7}}}, {{271, {10, 9}}, {243, {9, 9}}}
({{28, {4, 2}}, {117, {9, 3}}}, {{31, {5, 1}}, {201, {11, 5}}},
{{36, {6, 0}}, {109, {7, 5}}}, {{39, {5, 2}}, {193, {9, 7}}},
{{43, {6, 1}}, {247, {11, 7}}}, {{48, {4, 4}}, {97, {8, 3}}},
{{49, {7, 0}}, {183, {13, 1}}}, {{52, {6, 2}}, {151, {9, 5}}},
{{64, {8, 0}}, {139, {10, 3}}}, {{73, {8, 1}}, {217, {13, 3}}},
{{76, {6, 4}}, {243, {9, 9}}}, {{81, {9, 0}}, {151, {9, 5}}},
{{84, {8, 2}}, {61, {5, 4}}}, {{93, {7, 4}}, {139, {10, 3}}},
{{97, {8, 3}}, {193, {9, 7}}}, {{103, {9, 2}}, {129, {8, 5}}},
{{112, {8, 4}}, {91, {6, 5}}}, {{112, {8, 4}}, {91, {9, 1}}},
{{121, {11, 0}}, {111, {10, 1}}}, {{124, {10, 2}}, {21, {4, 1}}},
{{124, {10, 2}}, {79, {7, 3}}}, {{127, {7, 6}}, {163, {11, 3}}},
{{133, {9, 4}}, {157, {12, 1}}}, {{139, {10, 3}}, {151, {9, 5}}},
{{144, {12, 0}}, {1, {1, 0}}}, {{144, {12, 0}}, {117, {9, 3}}},
{{144, {12, 0}}, {175, {10, 5}}}, {{147, {11, 2}}, {201, {11, 5}}},
{{148, {8, 6}}, {229, {12, 5}}}, {{156, {10, 4}}, {163, {11, 3}}},
{{157, {12, 1}}, {75, {5, 5}}}, {{157, {12, 1}}, {133, {11, 1}}},
{{163, {11, 3}}, {243, {9, 9}}}, {{169, {8, 7}}, {63, {6, 3}}},
{{169, {13, 0}}, {63, {6, 3}}}, {{169, {13, 0}}, {121, {11, 0}}},
{{171, {9, 6}}, {61, {5, 4}}}, {{172, {12, 2}}, {31, {5, 1}}},
{{172, {12, 2}}, {147, {7, 7}}}, {{175, {10, 5}}, {57, {7, 1}}},
{{181, {11, 4}}, {109, {7, 5}}}, {{183, {13, 1}}, {49, {5, 3}}},
{{189, {12, 3}}, {43, {6, 1}}}, {{189, {12, 3}}, {217, {13, 3}}},
{{192, {8, 8}}, {127, {7, 6}}}, {{192, {8, 8}}, {243, {9, 9}}},
{{196, {10, 6}}, {7, {2, 1}}}, {{196, {14, 0}}, {7, {2, 1}}},
{{199, {13, 2}}, {91, {9, 1}}}, {{201, {11, 5}}, {147, {7, 7}}},
{{208, {12, 4}}, {111, {10, 1}}}, {{208, {12, 4}}, {169, {8, 7}}},
{{211, {14, 1}}, {21, {4, 1}}}, {{211, {14, 1}}, {79, {7, 3}}},
{{217, {9, 8}}, {73, {8, 1}}}, {{217, {9, 8}}, {189, {12, 3}}},
{{217, {9, 8}}, {247, {11, 7}}}, {{217, {13, 3}}, {247, {11, 7}}},
{{219, {10, 7}}, {13, {3, 1}}}, {{219, {10, 7}}, {129, {8, 5}}},
{{223, {11, 6}}, {9, {3, 0}}}, {{223, {11, 6}}, {183, {13, 1}}},
{{229, {12, 5}}, {3, {1, 1}}}, {{229, {12, 5}}, {61, {5, 4}}},
{{244, {10, 8}}, {75, {5, 5}}}, {{244, {10, 8}}, {133, {9, 4}}},
{{244, {10, 8}}, {133, {11, 1}}}, {{271, {10, 9}}, {19, {3, 2}}},
{{271, {10, 9}}, {193, {9, 7}}}
({{7, {2, 1}}, {196, {10, 6}}}, {{9, {3, 0}}, {223, {11, 6}}},
{{19, {3, 2}}, {271, {10, 9}}}, {{21, {4, 1}}, {124, {10, 2}}},
{{21, {4, 1}}, {211, {14, 1}}}, {{31, {5, 1}}, {172, {12, 2}}},
{{43, {6, 1}}, {247, {11, 7}}}, {{49, {5, 3}}, {183, {13, 1}}},

```

{{57, {7, 1}}, {175, {10, 5}}}, {{61, {5, 4}}, {84, {8, 2}}},
 {{61, {5, 4}}, {171, {9, 6}}}, {{75, {5, 5}}, {244, {10, 8}}},
 {{79, {7, 3}}, {211, {14, 1}}}, {{91, {9, 1}}, {199, {13, 2}}},
 {{93, {7, 4}}, {139, {10, 3}}}, {{109, {7, 5}}, {36, {6, 0}}},
 {{112, {8, 4}}, {91, {6, 5}}}, {{117, {9, 3}}, {28, {4, 2}}},
 {{121, {11, 0}}, {111, {10, 1}}}, {{124, {10, 2}}, {79, {7, 3}}},
 {{127, {7, 6}}, {163, {11, 3}}}, {{129, {8, 5}}, {103, {9, 2}}},
 {{129, {8, 5}}, {219, {10, 7}}}, {{133, {9, 4}}, {244, {10, 8}}},
 {{133, {11, 1}}, {244, {10, 8}}}, {{144, {12, 0}}, {175, {10, 5}}},
 {{151, {9, 5}}, {52, {6, 2}}}, {{151, {9, 5}}, {139, {10, 3}}},
 {{156, {10, 4}}, {163, {11, 3}}}, {{157, {12, 1}}, {75, {5, 5}}},
 {{169, {8, 7}}, {63, {6, 3}}}, {{169, {13, 0}}, {63, {6, 3}}},
 {{172, {12, 2}}, {147, {7, 7}}}, {{183, {13, 1}}, {223, {11, 6}}},
 {{189, {12, 3}}, {43, {6, 1}}}, {{192, {8, 8}}, {127, {7, 6}}},
 {{193, {9, 7}}, {39, {5, 2}}}, {{193, {9, 7}}, {97, {8, 3}}},
 {{193, {9, 7}}, {271, {10, 9}}}, {{196, {14, 0}}, {7, {2, 1}}},
 {{201, {11, 5}}, {31, {5, 1}}}, {{201, {11, 5}}, {147, {7, 7}}},
 {{201, {11, 5}}, {147, {11, 2}}}, {{208, {12, 4}}, {111, {10, 1}}},
 {{217, {9, 8}}, {247, {11, 7}}}, {{217, {13, 3}}, {189, {12, 3}}},
 {{217, {13, 3}}, {247, {11, 7}}}, {{243, {9, 9}}, {76, {6, 4}}},
 {{243, {9, 9}}, {163, {11, 3}}}
 {{9, {3, 0}}, {223, {11, 6}}}, {{19, {3, 2}}, {271, {10, 9}}},
 {{21, {4, 1}}, {211, {14, 1}}}, {{28, {4, 2}}, {117, {9, 3}}},
 {{31, {5, 1}}, {172, {12, 2}}}, {{36, {6, 0}}, {109, {7, 5}}},
 {{39, {5, 2}}, {193, {9, 7}}}, {{61, {5, 4}}, {171, {9, 6}}},
 {{76, {6, 4}}, {243, {9, 9}}}, {{79, {7, 3}}, {124, {10, 2}}},
 {{79, {7, 3}}, {211, {14, 1}}}, {{84, {8, 2}}, {61, {5, 4}}},
 {{91, {6, 5}}, {112, {8, 4}}}, {{97, {8, 3}}, {193, {9, 7}}},
 {{111, {10, 1}}, {208, {12, 4}}}, {{124, {10, 2}}, {21, {4, 1}}},
 {{129, {8, 5}}, {219, {10, 7}}}, {{139, {10, 3}}, {93, {7, 4}}},
 {{139, {10, 3}}, {151, {9, 5}}}, {{163, {11, 3}}, {127, {7, 6}}},
 {{163, {11, 3}}, {156, {10, 4}}}, {{163, {11, 3}}, {243, {9, 9}}},
 {{169, {8, 7}}, {63, {6, 3}}}, {{172, {12, 2}}, {147, {7, 7}}},
 {{175, {10, 5}}, {144, {12, 0}}}, {{183, {13, 1}}, {223, {11, 6}}},
 {{189, {12, 3}}, {43, {6, 1}}}, {{196, {10, 6}}, {7, {2, 1}}},
 {{199, {13, 2}}, {91, {9, 1}}}, {{201, {11, 5}}, {147, {7, 7}}},
 {{217, {13, 3}}, {189, {12, 3}}}, {{244, {10, 8}}, {133, {9, 4}}},
 {{244, {10, 8}}, {133, {11, 1}}}, {{247, {11, 7}}, {43, {6, 1}}},
 {{247, {11, 7}}, {217, {9, 8}}}, {{271, {10, 9}}, {193, {9, 7}}}
 {{21, {4, 1}}, {211, {14, 1}}}, {{31, {5, 1}}, {172, {12, 2}}},
 {{36, {6, 0}}, {109, {7, 5}}}, {{43, {6, 1}}, {189, {12, 3}}},
 {{43, {6, 1}}, {247, {11, 7}}}, {{61, {5, 4}}, {84, {8, 2}}},
 {{63, {6, 3}}, {169, {8, 7}}}, {{76, {6, 4}}, {243, {9, 9}}},
 {{79, {7, 3}}, {211, {14, 1}}}, {{112, {8, 4}}, {91, {6, 5}}},
 {{117, {9, 3}}, {28, {4, 2}}}, {{124, {10, 2}}, {21, {4, 1}}},
 {{127, {7, 6}}, {163, {11, 3}}}, {{133, {9, 4}}, {244, {10, 8}}},
 {{139, {10, 3}}, {151, {9, 5}}}, {{144, {12, 0}}, {175, {10, 5}}},
 {{147, {7, 7}}, {172, {12, 2}}}, {{147, {7, 7}}, {201, {11, 5}}},
 {{156, {10, 4}}, {163, {11, 3}}}, {{171, {9, 6}}, {61, {5, 4}}},

```

    {{183, {13, 1}}, {223, {11, 6}}}, {{193, {9, 7}}, {39, {5, 2}}},
    {{193, {9, 7}}, {97, {8, 3}}}, {{217, {9, 8}}, {247, {11, 7}}},
    {{219, {10, 7}}, {129, {8, 5}}}, {{243, {9, 9}}, {163, {11, 3}}},
    {{244, {10, 8}}, {133, {11, 1}}}}
    {{{61, {5, 4}}, {84, {8, 2}}}, {{91, {6, 5}}, {112, {8, 4}}},
    {{97, {8, 3}}, {193, {9, 7}}}, {{124, {10, 2}}, {21, {4, 1}}},
    {{129, {8, 5}}, {219, {10, 7}}}, {{133, {11, 1}}, {244, {10, 8}}},
    {{144, {12, 0}}, {175, {10, 5}}}, {{151, {9, 5}}, {139, {10, 3}}},
    {{163, {11, 3}}, {127, {7, 6}}}, {{163, {11, 3}}, {156, {10, 4}}},
    {{172, {12, 2}}, {31, {5, 1}}}, {{172, {12, 2}}, {147, {7, 7}}},
    {{189, {12, 3}}, {43, {6, 1}}}, {{193, {9, 7}}, {39, {5, 2}}},
    {{201, {11, 5}}, {147, {7, 7}}}, {{211, {14, 1}}, {21, {4, 1}}},
    {{211, {14, 1}}, {79, {7, 3}}}, {{217, {9, 8}}, {247, {11, 7}}},
    {{223, {11, 6}}, {183, {13, 1}}}, {{244, {10, 8}}, {133, {9, 4}}},
    {{247, {11, 7}}, {43, {6, 1}}}}
    {{{21, {4, 1}}, {124, {10, 2}}}, {{21, {4, 1}}, {211, {14, 1}}},
    {{31, {5, 1}}, {172, {12, 2}}}, {{39, {5, 2}}, {193, {9, 7}}},
    {{43, {6, 1}}, {189, {12, 3}}}, {{61, {5, 4}}, {84, {8, 2}}},
    {{79, {7, 3}}, {211, {14, 1}}}, {{127, {7, 6}}, {163, {11, 3}}},
    {{139, {10, 3}}, {151, {9, 5}}}, {{147, {7, 7}}, {172, {12, 2}}},
    {{163, {11, 3}}, {156, {10, 4}}}, {{193, {9, 7}}, {97, {8, 3}}},
    {{201, {11, 5}}, {147, {7, 7}}}, {{219, {10, 7}}, {129, {8, 5}}},
    {{244, {10, 8}}, {133, {9, 4}}}}
    {{{79, {7, 3}}, {211, {14, 1}}}, {{84, {8, 2}}, {61, {5, 4}}},
    {{124, {10, 2}}, {21, {4, 1}}}, {{151, {9, 5}}, {139, {10, 3}}},
    {{156, {10, 4}}, {163, {11, 3}}}, {{163, {11, 3}}, {127, {7, 6}}},
    {{172, {12, 2}}, {31, {5, 1}}}, {{189, {12, 3}}, {43, {6, 1}}},
    {{193, {9, 7}}, {97, {8, 3}}}, {{211, {14, 1}}, {21, {4, 1}}},
    {{244, {10, 8}}, {133, {9, 4}}}}
    {{{21, {4, 1}}, {124, {10, 2}}}, {{31, {5, 1}}, {172, {12, 2}}},
    {{43, {6, 1}}, {189, {12, 3}}}, {{61, {5, 4}}, {84, {8, 2}}},
    {{133, {9, 4}}, {244, {10, 8}}}, {{163, {11, 3}}, {127, {7, 6}}},
    {{193, {9, 7}}, {97, {8, 3}}}}
    {{{43, {6, 1}}, {189, {12, 3}}}, {{84, {8, 2}}, {61, {5, 4}}},
    {{97, {8, 3}}, {193, {9, 7}}}, {{124, {10, 2}}, {21, {4, 1}}},
    {{163, {11, 3}}, {127, {7, 6}}}, {{172, {12, 2}}, {31, {5, 1}}},
    {{244, {10, 8}}, {133, {9, 4}}}}
    {{{21, {4, 1}}, {124, {10, 2}}}, {{43, {6, 1}}, {189, {12, 3}}},
    {{61, {5, 4}}, {84, {8, 2}}}, {{127, {7, 6}}, {163, {11, 3}}},
    {{133, {9, 4}}, {244, {10, 8}}}, {{172, {12, 2}}, {31, {5, 1}}},
    {{193, {9, 7}}, {97, {8, 3}}}}
    {{{21, {4, 1}}, {124, {10, 2}}}, {{84, {8, 2}}, {61, {5, 4}}},
    {{97, {8, 3}}, {193, {9, 7}}}, {{163, {11, 3}}, {127, {7, 6}}},
    {{172, {12, 2}}, {31, {5, 1}}}, {{189, {12, 3}}, {43, {6, 1}}},
    {{244, {10, 8}}, {133, {9, 4}}}}
    {{{21, {4, 1}}, {124, {10, 2}}}, {{31, {5, 1}}, {172, {12, 2}}},
    {{43, {6, 1}}, {189, {12, 3}}}, {{84, {8, 2}}, {61, {5, 4}}},
    {{127, {7, 6}}, {163, {11, 3}}}, {{133, {9, 4}}, {244, {10, 8}}},
    {{193, {9, 7}}, {97, {8, 3}}}}

```

```

({{84, {8, 2}}, {61, {5, 4}}}, {{97, {8, 3}}, {193, {9, 7}}},
  {{124, {10, 2}}, {21, {4, 1}}}, {{133, {9, 4}}, {244, {10, 8}}},
  {{163, {11, 3}}, {127, {7, 6}}}, {{172, {12, 2}}, {31, {5, 1}}},
  {{189, {12, 3}}, {43, {6, 1}}}}
({{21, {4, 1}}, {124, {10, 2}}}, {{31, {5, 1}}, {172, {12, 2}}},
  {{43, {6, 1}}, {189, {12, 3}}}, {{61, {5, 4}}, {84, {8, 2}}},
  {{97, {8, 3}}, {193, {9, 7}}}, {{127, {7, 6}}, {163, {11, 3}}},
  {{133, {9, 4}}, {244, {10, 8}}}}
({{21, {4, 1}}, {124, {10, 2}}}, {{31, {5, 1}}, {172, {12, 2}}},
  {{43, {6, 1}}, {189, {12, 3}}}, {{61, {5, 4}}, {84, {8, 2}}},
  {{97, {8, 3}}, {193, {9, 7}}}, {{127, {7, 6}}, {163, {11, 3}}},
  {{133, {9, 4}}, {244, {10, 8}}}}
{1993, 9, 30, 17, 31, 40}

```


A.5. Output from Program 2 for $p=41$.

```

{1993, 10, 2, 17, 29, 57}
{{(7, {2, 1}), {403, {14, 9}}}, {(28, {4, 2}), {259, {13, 5}}},
  {(112, {8, 4}), {175, {10, 5}}}, {(331, {11, 10}), {448, {16, 8}}},
  {(193, {9, 7}), {381, {19, 1}}}}
14/3
{{(9, {3, 0}), {196, {10, 6}}}, {(36, {6, 0}), {333, {12, 9}}},
  {(144, {12, 0}), {307, {17, 1}}}, {(39, {5, 2}), {289, {17, 0}}},
  {(49, {7, 0}), {156, {10, 4}}}, {(196, {14, 0}), {337, {13, 8}}},
  {(169, {13, 0}), {241, {15, 1}}}, {(103, {9, 2}), {225, {15, 0}}},
  {(121, {11, 0}), {412, {18, 4}}}, {(49, {5, 3}), {361, {19, 0}}}}
10/3
{{(9, {3, 0}), {196, {14, 0}}}, {(36, {6, 0}), {169, {13, 0}}},
  {(144, {12, 0}), {225, {15, 0}}}, {(121, {11, 0}), {289, {17, 0}}},
  {(49, {7, 0}), {361, {19, 0}}}}
10/3
{{(13, {3, 1}), {397, {12, 11}}}, {(52, {6, 2}), {399, {17, 5}}},
  {(79, {7, 3}), {208, {12, 4}}}, {(217, {9, 8}), {316, {14, 6}}},
  {(157, {12, 1}), {417, {16, 7}}}, {(151, {9, 5}), {259, {15, 2}}},
  {(93, {7, 4}), {399, {13, 10}}}, {(325, {15, 5}), {372, {14, 8}}},
  {(111, {10, 1}), {217, {13, 3}}}, {(171, {9, 6}), {403, {19, 2}}}}
14/3
{{(19, {3, 2}), {268, {14, 4}}}, {(76, {6, 4}), {129, {8, 5}}},
  {(304, {12, 8}), {475, {15, 10}}}, {(273, {16, 1}), {301, {11, 9}}},
  {(67, {7, 2}), {343, {18, 1}}}}
10/3
{{(19, {3, 2}), {432, {12, 12}}}, {(76, {6, 4}), {457, {17, 7}}},
  {(147, {7, 7}), {304, {12, 8}}}, {(273, {16, 1}), {547, {14, 13}}},
  {(67, {7, 2}), {507, {13, 13}}}, {(268, {14, 4}), {511, {15, 11}}},
  {(129, {8, 5}), {363, {11, 11}}}, {(427, {19, 3}), {475, {15, 10}}},
  {(27, {3, 3}), {301, {11, 9}}}, {(108, {6, 6}), {343, {18, 1}}}}
16/3
{{(27, {3, 3}), {301, {15, 4}}}, {(97, {8, 3}), {108, {6, 6}}},
  {(388, {16, 6}), {432, {12, 12}}}, {(117, {9, 3}), {457, {17, 7}}},
  {(147, {7, 7}), {427, {17, 6}}}, {(109, {7, 5}), {547, {14, 13}}},
  {(436, {14, 10}), {507, {13, 13}}}, {(309, {13, 7}), {511, {15, 11}}},
  {(211, {14, 1}), {363, {11, 11}}}, {(147, {11, 2}), {427, {19, 3}}}}
10/3
{{(27, {3, 3}), {547, {14, 13}}}, {(108, {6, 6}), {507, {13, 13}}},
  {(432, {12, 12}), {511, {15, 11}}}, {(363, {11, 11}), {457, {17, 7}}},
  {(147, {7, 7}), {427, {19, 3}}}}
28/3
{{(37, {4, 3}), {291, {14, 5}}}, {(139, {10, 3}), {148, {8, 6}}},
  {(351, {15, 6}), {469, {13, 12}}}, {(133, {11, 1}), {441, {15, 9}}},
  {(247, {11, 7}), {327, {17, 2}}}}
14/3
{{(39, {5, 2}), {412, {18, 4}}}, {(49, {5, 3}), {156, {10, 4}}},
  {(196, {10, 6}), {337, {13, 8}}}, {(241, {15, 1}), {333, {12, 9}}},
  {(103, {9, 2}), {307, {17, 1}}}}
10/3

```

$\{ \{43, \{6, 1\}\}, \{367, \{13, 9\}\}, \{172, \{12, 2\}\}, \{279, \{15, 3\}\},$
 $\{91, \{6, 5\}\}, \{237, \{13, 4\}\}, \{169, \{8, 7\}\}, \{364, \{12, 10\}\},$
 $\{349, \{17, 3\}\}, \{471, \{14, 11\}\} \}$
 $16/3$
 $\{ \{63, \{6, 3\}\}, \{388, \{16, 6\}\}, \{117, \{9, 3\}\}, \{252, \{12, 6\}\},$
 $\{229, \{12, 5\}\}, \{427, \{17, 6\}\}, \{109, \{7, 5\}\}, \{219, \{10, 7\}\},$
 $\{343, \{14, 7\}\}, \{436, \{14, 10\}\}, \{183, \{13, 1\}\}, \{309, \{13, 7\}\},$
 $\{199, \{13, 2\}\}, \{211, \{14, 1\}\}, \{147, \{11, 2\}\}, \{181, \{11, 4\}\},$
 $\{273, \{11, 8\}\}, \{301, \{15, 4\}\}, \{97, \{8, 3\}\}, \{313, \{16, 3\}\} \}$
 $16/3$
 $\{ \{79, \{7, 3\}\}, \{372, \{14, 8\}\}, \{217, \{13, 3\}\}, \{316, \{14, 6\}\},$
 $\{157, \{12, 1\}\}, \{171, \{9, 6\}\}, \{259, \{15, 2\}\}, \{397, \{12, 11\}\},$
 $\{93, \{7, 4\}\}, \{399, \{17, 5\}\} \}$
 $16/3$
 $\{ \{97, \{8, 3\}\}, \{436, \{14, 10\}\}, \{309, \{13, 7\}\}, \{388, \{16, 6\}\},$
 $\{117, \{9, 3\}\}, \{211, \{14, 1\}\}, \{147, \{11, 2\}\}, \{427, \{17, 6\}\},$
 $\{109, \{7, 5\}\}, \{301, \{15, 4\}\} \}$
 $16/3$
 $\{ \{127, \{7, 6\}\}, \{283, \{13, 6\}\}, \{189, \{12, 3\}\}, \{508, \{14, 12\}\},$
 $\{223, \{11, 6\}\}, \{433, \{13, 11\}\}, \{277, \{12, 7\}\}, \{379, \{15, 7\}\},$
 $\{163, \{11, 3\}\}, \{247, \{14, 3\}\} \}$
 $20/3$
 $\{10/3, 14/3, 16/3, 20/3, 28/3\}$
 $\{1993, 10, 2, 17, 35, 30\}$

References

- [1] J.H. Conway and N. J. A. Sloane: Sphere Packings, Springer Verlag, Berlin-Heidelberg-London-Tokyo, 1989.
- [2] T. Katsura, Unirational elliptic surfaces in characteristic p , Tôhoku. Math. J. 33 (1981), 521-553.
- [3] A. Néron: Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I.H.E.S. 21 (1964).
- [4] K. Oguiso and T. Shioda: The Mordell-Weil Lattice of a Rational Elliptic Surface, Comment. Math. Univ. St. Pauli, 40 (1986), 83-99.
- [5] M. Ohhira: Unirational elliptic surfaces in characteristic 2, Journal of Math. Soc. Japan 44 (1992), 709-738.
- [6] M. Ohhira: Supersingular K3 surfaces with various values of the Artin invariant in characteristic 2, Nat. Sci. Rep, Ocha. Univ. 44 (1993), 7-15.
- [7] T. Shioda: On the Mordell-Weil Lattices, Comment. Math. Univ. St. Pauli. 39 (1990), 211-240.
- [8] J.H. Silverman: The arithmetic of elliptic curves, Grad. Texts in Math. 106, Springer-Verlag, Berlin-Heidelberg-New York, 1986.