Connecting on the Lattice Based Reductions for Computing the Generators in the ISD Method

Ruma K K Ajeena*, Sanaa K Kamal
Mathematics Department, Education College for Pure Sciences, University of Babylon, Iraq.
ruma.usm@gmail.com

Abstract. In this paper, the generalized Lagrange-Gauss reduction method to generate the generators in ISD method has been proposed. The comparison results on using the generalized Lagrange-Gauss reduction method and generalized extended Euclidean algorithm have been determined. As well as, the connection between the generalized Lagrange-Gauss Reduction and generalized extended Euclidean Algorithm to compute reduced bases to form the ISD generators in ISD elliptic scalar algorithm is presented.

Keywords: Elliptic curve cryptography, scalar multiplication, efficiently computable endomorphisms, ISD method, lattice basis reductions methods

1. Introduction

On the lattice basis reduction methods, the transformations of the given lattice bases into good lattice bases have been presented. These good bases consist of linearly independent vectors that reduced into the shortest and closest to orthogonal vectors. Some efficient algorithms have been proposed to achieve this task and getting good bases which are depending on the lattices rank.

The lattice bases of rank 2 in \( \mathbb{R}^2 \) are reduced by the proposition of Lagrange and Gauss \([1,2,3]\). The Lagrange and Gauss algorithm (LGA) is implemented with the vectors \( v_1 \) and \( v_2 \) as inputs and returns the shortest vectors of \( v_1 \) and \( v_2 \). The LGA is closed to extended Euclidean algorithm (EEA) \([4,5]\). The EEA considered as another efficient way for reducing the lattice bases of rank 2. On the EEA, the reduction can be done with inputs \((n,\lambda)\) for positive integers \( n \) and \( \lambda \) with \( n \geq \lambda \), to get a sequence of integers \( f_i, g_i, \) and \( h_i \) such that \( nf_i + \lambda g_i = h_i \) for \( i = 0,1,2,...,l, l+1, l+2,...,w-1 \) with \( w > l \). These integers can be used to form the shortest vectors \( v_1 \) and \( v_2 \) which considered as the elements in good lattice basis \( \{v_1, v_2\} \).

Whereas, the lattice bases of rank 3 can be reduced using the Lenstra, Lenstra and Lovász algorithm, which is known by the LLL or L3 algorithm \([4,5]\). In this paper, our work focuses on the lattice bases of rank 2. The main idea of this research work is to generalize the Lagrange – Gauss algorithm (GLGA) for reducing 2-tuple of lattice bases that is employed to compute the generators in the ISD computation method \([7,8,9,10,11,12]\). The generalized extended Euclidean algorithm (GEEA) is presented as another efficient generalized algorithm to generate the ISD generators. Comparison results on using these generalized methods are explained by simple example. Based on these results, the connection between generalized methods, GLGA and GEEA can be done easily.
The rest of this paper is organized as follows: Section 2 reviews the mathematical background related to elliptic curves over finite fields and some important facts of lattices. Section 3 gives an explanation of the procedures of reducing the lattice basis in two dimensions. Section 4 discusses the generalized methods of two dimensional lattice bases reduction. Section 5 discusses the generators on the ISD computation method. Section 6 presents the comparison results on using these generalized methods, Lagrange-Gauss reduction method and extended Euclidean algorithm. Section 7 discusses the connection of the generalized Lagrange-Gauss reduction and generalized extended Euclidean algorithm. Finally, the conclusions are given in Section 8.

2. Mathematical background

This section discusses briefly some important mathematical concepts related to our research work in this paper. These concepts include the elliptic curve defined over prime fields and elementary fundamental definitions on lattices.

Definition 2.1.1. Suppose \( p > 2, 3 \). An elliptic curve \( E \) defined over \( F_p \) which is defined by

\[
y^2 = x^3 + cx + d \pmod{p}
\]

where \( c, d \in F_p \). The \( \Delta = 4c^3 + 27d^2 \not\equiv 0 \pmod{p} \) is defined to be a discriminant of \( E \). All points \((x,y)\) that satisfy elliptic curve equation (1) defined over \( F_p \) form a set that is given by

\[
E(F_p) = \{(x, y) : x, y \in F_p, y^2 = x^3 + cx + d \pmod{p}\} \cup \{\infty\},
\]

where \( \infty \) is a point at infinity [2,3,4].

Definition 2.1.2. Let \( P = (x_1, y_1) \in E(F_p) \) and \( Q = (x_2, y_2) \in E(F_p) \), where \( P \neq \pm Q \). Then the sum of two points \( P \) and \( Q \) is \( P + Q = (x_3, y_3) \) [4], where

\[
\begin{align*}
x_3 &= \frac{(y_2 - y_1)(x_2 - x_1)^2}{x_2 - x_1} - x_1 - x_2 \pmod{p}, \\
y_3 &= \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1 \pmod{p}.
\end{align*}
\]

Whereas, doubling the point \( P \) which lies on \( E \) can be computed by \( 2P = P + P = (x_3, y_3) \), where

\[
\begin{align*}
x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \pmod{p}, \\
y_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \pmod{p}.
\end{align*}
\]

Definition 2.1.3. Suppose \( k \) is a positive integer such that \( k \in [1, n-1] \). The scalar multiplication \( kP \) on elliptic curve \( E \) can be defined by

\[
kP = P + P + \cdots + P,
\]

where \( P \) is a point lies on \( E \), which has a prime order \( n \), defined over a prime field \( F_p \) [2,3,4].
Definition 2.1.4. Let \( \{v_1, \ldots, v_n\} \) be a set of linearly independent vectors in \( \mathbb{Z}^n \), with \( m \geq n \). The set \( \{v_1, \ldots, v_n\} \) generates a lattice

\[
L = \left\{ \sum_{i=1}^{n} l_i v_i : l_i \in \mathbb{Z} \right\}
\]

(6)

of linear combinations which are integers \( v_i \). The vectors \( v_1, \ldots, v_n \) are called a lattice basis. The parameters \( n \) and \( m \) are the lattice rank and dimension respectively. A lattice has a full rank if \( n = m \) [1,3].

Definition 2.1.5. Let \( L \subset \mathbb{Z}^n \) be a lattice. A sub-lattice is a subset \( L' \subset L \) that is a lattice [1].

Definition 2.1.6. On a lattice \( L \), a basis matrix \( V \) is an \( n \times m \) matrix. It forms from the rows of the basis vectors \( v_i \). On the row \( v_i \), the \( \vdots \)th entry. So, \( L \) can be expressed by

\[
\{ x \in \mathbb{Z}^n : x V \}
\]

(7)

3. Two dimensional lattice basis reduction methods

Suppose \( v_1, v_2 \in \mathbb{Z}^2 \) are two linearly independent vectors, which are a basis for the lattice \( L \). The basic idea of the reduction methods on the lattice bases of rank 2 is to reduce the lengths of the basis vectors to be the shortest in compare with the original vectors. One of these reduction methods is Lagrange-Gauss method that will discuss as follows:

3.1 The Lagrange-Gauss lattice basis reduction method

With the vectors \( v_1, v_2 \in \mathbb{Z}^2 \), the Lagrange – Gauss reduction idea [1,3] has been explained through the following mathematical concepts.

Definition 3.1.1. An ordered basis \( \{v_1, v_2\} \) is Lagrange-Gauss reduced if

\[
\|v_1\| \leq \|v_2\| \leq \|v_2 + q v_1\| \text{ for all } q \in \mathbb{Z}.
\]

(8)

Theorem 3.1.1. Let \( \lambda_1, \lambda_2 \in \mathbb{Z} \) be the successive minima of \( L \). If \( L \) has an ordered basis \( \{v_1, v_2\} \) that is Lagrange-Gauss reduced, then \( \|v_i\| = \lambda_i \) for \( i = 1, 2 \). [1].

Definition 3.1.2. Let \( v_1, \ldots, v_n \) be the vectors in \( \mathbb{Z}^n \). We write \( V_i = \|v_i\|^2 = \langle v_i, v_i \rangle \).

On the Lagrange-Gauss algorithm, a crucial ingredient defines by

\[
\|v_2 - \mu v_1\|^2 = V_2 - 2 \mu \langle v_1, v_2 \rangle + \mu^2 V_1
\]

(9)

Which is minimised at \( \mu = \langle v_1, v_2 \rangle / V_1 \). Replacing \( v_2 \) by \( v_2 - \left[ \frac{\mu}{\mu} \right] v_1 \), where \( \left[ \frac{\mu}{\mu} \right] \) is the nearest integer to \( \mu \). On Algorithm (3.1.1), the size of \( v_2 \) can be reduced based on \( v_1 \), the reduction formula \( v_2 - \left[ \frac{\mu}{\mu} \right] v_1 \) is the familiar operation \( h_{i,i+1} = h_{i+1} - \left[ h_{i,i+1} / h_i \right] h_i \) that is computed from extended Euclidean algorithm [1].

Lemma 3.1.1. An ordered basis \( \{v_1, v_2\} \) is Lagrange-Gauss reduced if and only if

\[
\|v_1\| \leq \|v_2\| \leq \|v_2 + v_1\|.
\]

(10)
Algorithm 3.1.1. Lagrange-Gauss lattice basis reduction method
Input: Basis \( v_1, v_2 \in \mathbb{Z}^2 \) for a lattice \( L \).
Output: Reduced basis \( (v_1, v_2) \) for \( L \) such that \( \|v_i\| = \lambda_i \).
1: Compute \( V_1 = \|v_1\| \) and \( \mu = v_1, v_2 > N_1 \).
2: Calculate \( v_2 = v_2 - \left\lfloor \frac{\mu}{\|v_1\|} \right\rfloor v_1 \) and \( V_2 = \|v_2\| \).
3: While \( V_2 < V_1 \) do
   4: Swap \( v_1 \) and \( v_2 \)
   5: If \( V_2 = V_1 \) then
       6: Compute \( \mu = v_1, v_2 > N_1 \).
       7: Calculate \( v_2 = v_2 - \left\lfloor \frac{\mu}{\|v_1\|} \right\rfloor v_1 \) and \( V_2 = \|v_2\| \).
   8: Else
      9: Stop and go to choose other vectors \( v_1 \) and \( v_2 \).
   10: End if
   11: End while
12: Return \( (v_1, v_2) \).

3.2 The extended Euclidean algorithm for reduction lattices
The extended Euclidean algorithm can be extended. Theorem (3.2.1) in [4, 5] is used to compute the tuples of variables \( g, f_i \) and \( h_i \) for \( i = 0, 1, 2, \ldots, l, l + 1, l + 2, \ldots, w - 1 \) with \( w > l \). On these tuples, some variables have been employed to form a two-dimensional reduced basis which is used to generate a lattice [5].

Theorem 3.2.1. (Extended Euclidean Algorithm (EEA)). If \( n \) and \( \lambda \) are two integers, not both zero, then there exist integers \( s \) and \( t \) such that:
\[
gcd (n, \lambda) = g, n + f_i, \lambda = h_i.
\] (11)

for \( i = 0, 1, 2, \ldots, l, l + 1, l + 2, \ldots, w - 1 \) with \( w > l \). That is, \( gcd (n, \lambda) \) can be expressed as a linear combination of \( n \) and \( \lambda \) [4,5].

Lemma 3.2.1 (Properties of the extended Euclidean algorithm [1,5]). Suppose tuples of variables \( s_i, t_i \) and \( r_i \) are defined by
\[
g, n + f_i, \lambda = h_i \quad \text{for} \quad i = 0, 1, 2, \ldots, l, l + 1, l + 2, \ldots, w - 1 \quad \text{with} \quad w > l.
\] (12)

Where \( g_0 = 1, f_0 = 0, h_0 = n, g_1 = 0, f_1 = 1, h_1 = \lambda \), are initial values. The values \( h_i \geq 0 \) for all \( i \) resulting from applying the EEA for given positive integers \( n \) and \( \lambda \). Then
i. \( h_i > h_{i+1} \geq 0 \) for all \( i \geq 0 \).
ii. \( g_i, i < 1 \) \( g_{i+1} \) for all \( i \geq 1 \).
iii. \( f_i, i \leq f_{i+1} + 1 \) for all \( i \geq 0 \).
iv. \( h_i, i \leq f_{i+1} + 1 \) \( h_{i+1}, i \leq n \) for all \( i \geq 1 \).
v. If \( f_i \) is odd then \( (i - 1) \), is even, so \( f_i < 0 \) and \( f_{i+1} > 0 \).

Assume \( i \) is a greatest index for \( h_i \geq \sqrt{n} \). On Lemma (3.2.1) then the property (iv) becomes
\[
h_i, i \leq f_{i+1} + 1 \quad h_{i+1}, i \leq n \quad \text{and} \quad |f_{i+1}| < \sqrt{n} \quad \text{with} \quad i = l + 1.
\]

Choose \( v_1 = (h_{i+1}, -f_{i+1}) \). The homomorphism \( T : Z \times Z \rightarrow Z_n \) defined by \( (a, b) \rightarrow a + b \lambda (mod \ n) \) then \( T (v_1) = 0 \). Further, \( |f_{i+1}| < \sqrt{n} \) and \( h_{i+1} < \sqrt{n} \), it is possible to compute \( \|v_1\| \leq \sqrt{n} \). A vector \( v_2 \) is also chosen as the shortest vector \( (h_1, -f_1) \) or \( (h_{i+2}, -f_{i+2}) \). Once again, from Equation (10) and
the homomorphism $T$, we have $T(v_2) = 0$. Experimentally, $v_2$ is also considered as a short vector. The $v_1$ and $v_2$ are linearly independent vectors. Otherwise, if $v_2 = (h_1, -f_1)$, then

$$\frac{h_{i+1}}{h_i} = \frac{-f_{i+1}}{-f_i} = \frac{f_{i+1}}{f_i}.$$ 

However, from Lemma (3.2.1)(i), $h_{i+1} = h_i < 1$, and from (iii), on the same Lemma, $f_{i+1} = f_i > 1$. This is contradictory. Hence, $v_1$ and $v_2$ are linearly independent [1].

4. The generalized lattice basis reduction methods in two dimensions

The generalization on the lattice reduction methods is discussed as follows.

4.1 The generalized computation of the extended Euclidean algorithm

The EEA has been used to form the generator in the GLV method. The generalized idea of the EEA can be used to form the ISD generators $\{v_1, v_2\}$ and $\{v_3, v_4\}$. The generalization of the EEA outputs 2-tuples of variables for $j = 1, 2$ as shown in the next lemma.

Lemma 4.1.1. (The generalized extended Euclidean algorithm (GEEA)). Let $n$ be a positive integer and $\lambda = (\lambda_j)$ be two tuple of integers, where $j = 1, 2$ with $n \not\equiv O$ or $\lambda \not\equiv O$. For all $j$ and $\lambda = (\lambda_j)$ is a zero 2-tuple. Then, an 2-tuple of positive integers $D = (d_j) = (\gcd(n, \lambda_j))$ is a 2-tuple of the gcds. Furthermore, there exist two 2-tuples of the integers $G = (g_j)$ and $F = (f_j)$ such that $\gcd(n, \lambda_j) = g_j, f_j, \lambda_j$ for $j = 1, 2$ and $i = 1, 2, \ldots, l, l + 1, \ldots, w, w > l$. (13)

In other words, the expression of the 2-tuple $D$ is written by the linear combinations of the 2-tuple $\lambda$ and $n$ [7].

4.2 The generalized Lagrange - Gauss lattice basis reduction method

The generalization on the method of Lagrange-Gauss lattice basis reduction is illustrated as follows.

Definition 4.2.1. An ordered bases $v_1, v_2$ and $v_3, v_4$ in $\mathbb{Z}^2$ is a generalized Lagrange-Gauss reduced if

$$\|v_1\| \leq \|v_2\| \leq \|v_2 + qv_1\| \text{ and } \|v_3\| \leq \|v_3 + qv_4\| \forall q, q_2 \in \mathbb{Z}.$$ (14)

The reduced bases on the generalized Lagrange-Gauss (GLG) reduction method can be explained by following theorem.

Theorem 4.2.1. Let $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ be the successive minima of $L$. If $L$ has the ordered bases $(v_1, v_2)$ $(v_3, v_4)$ which are the generalized Lagrange-Gauss reduced, then $\|v_i\| = \lambda_i$ for $i = 1, 2, 3, 4$.

Definition 4.2.2. Let $v_1, v_2, v_3, v_4$ be the vectors in $\mathbb{Z}^2$. We write $V_i = \|v_i\|^2 = \{v_j, v_j\}$, for $i = 1, 2, 3, 4$. On the generalized Lagrange-Gauss algorithm, the crucial points are

$$\|v_2 - \mu_1v_1\|^2 = V_2 - 2\mu_1 <v_2, v_2> + \mu_1^2 V_1 \text{ and } \|v_4 - \mu_2v_3\|^2 = V_4 - 2\mu_2 <v_4, v_4> + \mu_2^2 V_3.$$ (15)

Are minimised at $\mu_1 <v_2, v_2> V_1$ and $\mu_2 <v_4, v_4> V_1$ respectively. The vectors $v_2$ and $v_4$ are replaced by $v_2 - [\mu_1] v_1$ and $v_4 - [\mu_2] v_3$ respectively, where $[\mu_1]$ and $[\mu_2]$ are the smallest integers to $\mu_1$ and $\mu_2$, the size of $v_2$ and $v_4$ are reduced based on the vectors $v_1$ and $v_3$. The reduced
formulas \( \nu_2 = \left[ \mu_1 \right] \nu_1 \) and \( \nu_4 = \left[ \mu_2 \right] \nu_3 \) are familiar the operations to \( r_{i+j} = r_{i} - \frac{r_{i+j}}{r_{j}} \nabla_j \) which are computed from the generalized Euclidean algorithm for \( j = 1, 2 \).

**Lemma 4.2.1.** The ordered bases \( (\nu_1, \nu_2) \) and \( (\nu_3, \nu_4) \) are Lagrange-Gauss reduced if and only if

\[
\|\nu_1\| \leq \|\nu_2\| \leq \|\nu_2 + \nu_1\| \quad \text{and} \quad \|\nu_3\| \leq \|\nu_4\| \leq \|\nu_4 + \nu_3\|. \tag{16}
\]

**Algorithm 4.2.1.** The generalized Lagrange-Gauss Algorithm (GLGA)

**Input:** The bases \( (\nu_1, \nu_2), (\nu_3, \nu_4) \in \mathbb{Z}^2 \) for a lattice \( L \).

**Output:** The shortest basis \( (\nu_1, \nu_2) \) and \( (\nu_3, \nu_4) \) for \( L \) such that \( \|\nu_i\| = \lambda_i \) for \( i = 1, 2, 3, 4 \).

1. Compute \( V_1 = \left\| \nu_1 \right\| \) and \( V_3 = \left\| \nu_3 \right\| \).
2. Calculate \( \mu_1 = \left< \nu_1, \nu_2 \right> > N_1 \) and \( \mu_2 = \left< \nu_3, \nu_4 \right> > N_3 \).
3. Reduce \( \nu_2 = \nu_2 - \left[ \mu_1 \right] \nu_1 \) and \( \nu_4 = \nu_4 - \left[ \mu_2 \right] \nu_3 \).
4. Check \( V_2 = \left\| \nu_2 \right\| \) and \( V_4 = \left\| \nu_4 \right\| \).
5. While \( \nu_2 < \nu_1 \) do
6. Swap \( \nu_1 \) and \( \nu_2 \).
7. If \( \nu_2 = \nu_1 \) then
8. Compute \( \mu_1 = \left< \nu_1, \nu_2 \right> > N_1 \).
9. Reduce \( \nu_2 = \nu_2 - \left[ \mu_1 \right] \nu_1 \).
10. Check \( V_2 = \left\| \nu_2 \right\| \).
11. Else
12. Stop and go to choose other vectors \( \nu_1 \) and \( \nu_2 \).
13. End if
14. End while
15. Return \( (\nu_1, \nu_2) \).
16. While \( \nu_4 < \nu_3 \) do
17. Swap \( \nu_3 \) and \( \nu_4 \).
18. If \( \nu_4 = \nu_3 \) then
19. Compute \( \mu_2 = \left< \nu_3, \nu_4 \right> > N_3 \).
20. Reduce \( \nu_4 = \nu_4 - \left[ \mu_2 \right] \nu_3 \).
21. Check \( V_4 = \left\| \nu_4 \right\| \).
22. Else
23. Stop and go to choose other vectors \( \nu_3 \) and \( \nu_4 \).
24. End if
25. End while
26. Return \( (\nu_3, \nu_4) \).

5. Generating the generators on the ISD computation method

The generators of the ISD computation method for computing a scalar multiplication \( kP \), which are called ISD generators, can be formed based on the following definition.

**Definition 5.1.** Suppose \( \nu_3, \nu_4 \) and \( \nu_5, \nu_6 \) are linearly independent vectors in the kernel of the homomorphism \( T \) that is defined by the formula:

\[
T: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} = n \quad (x, y) \rightarrow x + y \lambda j \pmod{n}. \tag{17}
\]
The bases of a lattice $L$, $\{v_1, v_2\}$ and $\{v_3, v_4\}$, are called ISD generators if each component of each vector is relatively prime to other and the components on these vectors are bounded by the range $[-\sqrt{n}, \sqrt{n}]$.

The existence of $v_1, v_2$ and $v_3, v_4$ in a sub-lattice $L_s$ as the linear independent vectors as well as the shortness of them considers as $kerT$ of a lattice $L = \mathbb{Z} \times \mathbb{Z}$. These vectors are computed by the GLGA (4.2.1) as the integer lattice points in two dimensions.

Algorithm 5.1. The ISD generators algorithm

Input: The bases $\{v_1, v_2\}$, $\{v_3, v_4\} \in \mathbb{Z}^2$ for a lattice $L$.

Output: The shortest bases $\{v_1, v_2\}$ and $\{v_3, v_4\}$ for $L$ such that $\|v_i\| = \lambda_i$ for $i = 1, 2, 3, 4$.

1: Run the GLGA (4.2.1).
2: Return reduced based $\{v_1, v_2\}$ and $\{v_3, v_4\}$.

6. Comparison studies on the GLG reduction and GEEA

The ISD generators are the fundamental points in the ISD computation method that uses to compute an elliptic scalar multiplication. So, the computation for these generators requires applying one of two generalized algorithms, the GLGA or GEEA. Our discussion will be beginning with using the GLGA.

With the vectors $v_1 = (1,39)$, $v_2 = (0,67)$ and $v_3 = (1,28)$, $v_4 = (0,67)$, the GLGA can be applied by the following computations.

$$
[\mu_1] = \left( \frac{v_1, v_2}{v_1, v_1} \right) = \frac{2613}{1522} = 1 \quad \text{and} \quad [\mu_2] = \left( \frac{v_1, v_3}{v_1, v_1} \right) = \frac{1876}{785} = 2.
$$

So, the first reduced vectors $v_2$ and $v_4$ are computed by

$$
v_2 = v_2 - [\mu_1] v_1 = (-1, 28) \quad \text{and} \quad v_4 = v_4 - [\mu_2] v_3 = (-2,11).
$$

Swapping $v_2, v_4$ with $v_1, v_3$ respectively. In other words, $v_1 = (-1, 28)$ and $v_2 = (1, 39)$ . Whereas, $v_3 = (-2,11)$ and $v_4 = (1,28)$. Now, the next values of $[\mu_1]$ and $[\mu_2]$ are

$$
[\mu_1] = \left( \frac{v_1, v_2}{v_1, v_1} \right) = \frac{1091}{785} = 1 \quad \text{and} \quad [\mu_2] = \left( \frac{v_1, v_3}{v_1, v_1} \right) = \frac{306}{125} = 2.
$$

So the new short vectors are

$$
v_2 = v_2 - [\mu_1] v_1 = (2,11) \quad \text{and} \quad v_4 = v_4 - [\mu_2] v_3 = (5,6).
$$

Second swapping of the vectors $v_2, v_4$ with $v_1, v_3$ respectively produces

$$
v_1 = (2,11), v_2 = (-1,28) \quad \text{and} \quad v_3 = (5,6), v_4 = (-2,11).
$$

New values of $[\mu_1]$ and $[\mu_2]$ are

$$
[\mu_1] = \left( \frac{v_1, v_2}{v_1, v_1} \right) = \frac{306}{125} = 2 \quad \text{and} \quad [\mu_2] = \left( \frac{v_1, v_3}{v_1, v_1} \right) = \frac{60}{61} = 1.
$$

New short vectors are

$$
v_2 = v_2 - [\mu_1] v_1 = (-5, 6) \quad \text{and} \quad v_4 = v_4 - [\mu_2] v_3 = (-7, 5).
$$
Now, the vectors \( v_3 = (5, 6) \) and \( v_4 = (-7, 5) \). Swapping operation is stopped at this point, since 

\[ |v_3| < |v_4| \]

therefore the shortest vectors are \( v_3 = (5, 6) \) and \( v_4 = (-7, 5) \).

Third swapping of the vectors \( v_2 \) with \( v_1 \) produces

\[ v_1 = (-5, 6), \ v_2 = (2, 11) \]

New value of \( \mu_1 \) is

\[ \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} = 1 \]

New short vector is

\[ v_2 = v_2 - \mu_1 v_1 = (7, -5) \]

Now, the vectors \( v_1 = (-5, 6) \) and \( v_2 = (7, -5) \). Swapping operation is stopped at this point, since 

\[ |v_1| < |v_2| \]

therefore the shortest vectors are \( v_1 = (-5, 6) \) and \( v_2 = (7, -5) \). Thus, the ISD generators can be formed by

\[ \{v_1, v_2\} = \{(h_{i, z_1}, -f_{i, z_1}), (h_{i, z_2}, -f_{i, z_2})\} \{(6, -5), (-7, 5)\} \]

and

\[ \{v_3, v_4\} = \{(h_{i, z_1}, -f_{i, z_1}), (h_{i, z_2}, -f_{i, z_2})\} \{(16, 5), (5, -7)\} \]

On the other hand, the application of the GEEA for the same values \((n, \lambda_1, \lambda_2) = (67, 39, 28)\) is achieved as follows.

With \( \lambda_1 = 39, n = 67 \) and \( f_{i, z_1} \leftarrow 1, g_{i, z_1} \leftarrow 0, f_{i, z_2} \leftarrow 0, g_{i, z_2} \leftarrow 1 \). 

\[ q \leftarrow \left[ 67/39 \right] = 1, h \leftarrow 67 - 1(39) = 28, f \leftarrow 0 - 1(1) = -1, g \leftarrow 1 - 1(0) = 1 \]

\[ n \leftarrow 39, \lambda_1 \leftarrow 28, f_{i, z_1} \leftarrow 1, f_{i, z_2} \leftarrow -1, g_{i, z_1} \leftarrow 0, g_{i, z_2} \leftarrow 1 \]

\[ q \leftarrow \left[ 39/28 \right] = 1, h \leftarrow 39 - 1(28) = 11, f \leftarrow 1 - 1(-1) = 2, g \leftarrow 0 - 1 = -1 \]

\[ n \leftarrow 28, \lambda_1 \leftarrow 11, f_{i, z_1} \leftarrow 1, f_{i, z_2} \leftarrow 2, g_{i, z_1} \leftarrow 1, g_{i, z_2} \leftarrow -1 \]

\[ q \leftarrow \left[ 28/11 \right] = 2, h \leftarrow 28 - 2(11) = 6, f \leftarrow -1 - 2(-2) = -5, g \leftarrow 1 - 2(-1) = 3 \]

\[ n \leftarrow 11, \lambda_1 \leftarrow 6, f_{i, z_1} \leftarrow 2, f_{i, z_2} \leftarrow -5, g_{i, z_1} \leftarrow -1, g_{i, z_2} \leftarrow 3 \]

\[ q \leftarrow \left[ 11/6 \right] = 1, h \leftarrow 11 - 1(6) = 5, f \leftarrow -2 - 1(-5) = 7, g \leftarrow -1 - 1(3) = -4 \]

\[ n \leftarrow 6, \lambda_1 \leftarrow 5, f_{i, z_1} \leftarrow -5, f_{i, z_2} \leftarrow 7, g_{i, z_1} \leftarrow 3, g_{i, z_2} \leftarrow -4 \]

\[ q \leftarrow \left[ 6/5 \right] = 1, h \leftarrow 6 - 1(5) = 1, f \leftarrow -5 - 1(-4) = -12, g \leftarrow 3 - 1(-4) = 7 \]

\[ n \leftarrow 5, \lambda_1 \leftarrow 1, f_{i, z_1} \leftarrow 7, f_{i, z_2} \leftarrow -12, g_{i, z_1} \leftarrow -4, g_{i, z_2} \leftarrow 7 \]

\[ q \leftarrow \left[ 5/1 \right] = 5, h \leftarrow 5 - 5(1) = 0, f \leftarrow 7 - 5(-12) = 67, g \leftarrow -4 - 5(7) = -39 \]

\[ n \leftarrow 5, \lambda_1 \leftarrow 1, f_{i, z_1} \leftarrow 7, f_{i, z_2} \leftarrow -12, g_{i, z_1} \leftarrow -4, g_{i, z_2} \leftarrow 7 \]

So, \( h = \{28, 11, 6, 5, 1, 0\}, f = \{-1, 2, -5, 7, -12, 67\} \) and \( g = \{1, 1, 3, 4, 7, -39\} \).

Whereas, with \( \lambda_2 = 28, n = 67 \) and \( f_{i, z_1} \leftarrow 1, g_{i, z_1} \leftarrow 0, f_{i, z_2} \leftarrow 0, g_{i, z_2} \leftarrow 1 \).

\[ q \leftarrow \left[ 67/28 \right] = 2, h \leftarrow 67 - 2(28) = 56, f \leftarrow 0 - 2(1) = -2, g \leftarrow 1 - 2(0) = 1. \]
Since the shortest vectors \( v_1 \) of So, extended Euclidean algorithm produces a sequence of integers, \( g \) and extended Euclid algorithm have been discussed. If,

7. Connecting between the GLGA and GEEA

algorithms are same. So, it is easy to connect between these generalized algorithms. Next section will Based on the comparison results on the GLGA and GEEA, one can conclude that the outputs on these algorithms are same. So, it is easy to connect between these generalized algorithms. Next section will discuss this connection.

\[
\begin{align*}
n & \leftarrow 28, \lambda_2 \leftarrow 11, f_0 \leftarrow 1, f_1 \leftarrow -2, g_0 \leftarrow 0, g_1 \leftarrow 1. \\
q & \leftarrow \frac{28}{11} = 2, h \leftarrow 28 - 2(11) = 6, f_1 \leftarrow 0 - 2(1) = -2.
\end{align*}
\]

\[
\begin{align*}
n & \leftarrow 11, \lambda_2 \leftarrow 6, f_0 \leftarrow -2, f_1 \leftarrow 5, g_0 \leftarrow 1, g_1 \leftarrow -2. \\
q & \leftarrow \frac{11}{6} = 1, h \leftarrow 11 - 1(6) = 5, f_1 \leftarrow -2 - 1(5) = -7, g_1 \leftarrow -1(\cdot 2) = 3.
\end{align*}
\]

\[
\begin{align*}
n & \leftarrow 6, \lambda_2 \leftarrow 5, f_0 \leftarrow 5, f_1 \leftarrow -7, g_0 \leftarrow 1, g_1 \leftarrow -2. \\
q & \leftarrow \frac{6}{5} = 1, h \leftarrow 6 - 1(5) = 1, f_1 \leftarrow -2 - 1(3) = -5.
\end{align*}
\]

\[
\begin{align*}
n & \leftarrow 5, \lambda_2 \leftarrow 1, f_0 \leftarrow -7, f_1 \leftarrow 12, g_0 \leftarrow -3, g_1 \leftarrow -5. \\
q & \leftarrow \frac{5}{1} = 5, h \leftarrow 5 - 5(1) = 0, f_1 \leftarrow -7 - 5(12) = -67, g_1 \leftarrow -3 - 5(5) = 28.
\end{align*}
\]

So, \( h = [11, 6, 5, 1, 0], f = [-2, 5, -7, 12, -67] \) and \( g = [1, -2, 3, -5, 28] \).

Since the shortest vectors \( v_1 \) and \( v_2 \) on the GEEA are defined by

\[
\begin{align*}
v_1 &= (h_{(\cdot + 1)\cdot}, -f_{(\cdot + 1)\cdot}) = (6, -5), \quad v_2 &= (h_{(\cdot + 2)\cdot}, -f_{(\cdot + 2)\cdot}) = (-5, 7) \quad \text{and} \quad v_3 &= (h_{(\cdot + 3)\cdot}, -f_{(\cdot + 3)\cdot}) = (6, 5), \quad v_4 &= (h_{(\cdot + 5)\cdot}, -f_{(\cdot + 5)\cdot}) = (5, -7).
\end{align*}
\]

Based on the comparison results on the GLGA and GEEA, one can conclude that the outputs on these algorithms are same. So, it is easy to connect between these generalized algorithms. Next section will discuss this connection.

7. Connecting between the GLGA and GEEA

In this section, some similarities and differences on the generalization of the Lagrange-Gauss algorithm and extended Euclid algorithm have been discussed. If \( n, \lambda_j \in \mathbb{Z} \) for \( j = 1, 2 \), then the generalized extended Euclidean algorithm produces a sequence of integers \( h_{ij}, g_{ij} \) and \( f_{ij} \) such that

\[
n_{g_{ij}} + \lambda_j f_{ij} = h_{ij} \quad \text{(18)}
\]

Where \( |h_{ij}| < |n_j| \) and \( |g_{ij}| < |\lambda_j| \). The precise formulae are \( h_{0,ij} = h_{0,0j} - q_j h_{ij} \) and \( f_{0,ij} = f_{0,0j} - q_j f_{ij} \), where \( q_j = \lfloor f_{0,0j} / f_{ij} \rfloor \). The sequence \( |h_{ij}| \) is strictly decreasing. The initial values are \( h_0 = n, h_1 = \lambda_j, g_0 = 1, g_1 = 0, f_0 = 0, f_1 = 1 \). In other words the lattice with basis matrix

\[
V_j = \begin{bmatrix} 0 & \lambda_j \\ 1 & f_{ij} \\ n & h_{ij} \end{bmatrix} \quad \text{(19)}
\]

contains the vectors

\[
(f_{ij}, h_{ij}) = (g_{ij}, f_{ij}) V_j.
\]

These vectors are shorter than the original vectors of the lattice. Now, If we suppose that the value of \( f_{ij} \) is sufficiently small compared with \( h_{ij} \) then one step of the generalized Lagrange-Gauss algorithm on \( V_j \) corresponds to one step of the generalized extended Euclidean algorithm. To see this, let \( v_1 = (f_{0,0j}, h_{0,0j}) \), \( v_2 = (f_{0,0j}, h_{0,0j}) \) and consider the GLGA with \( v_2 = (f_{ij}, h_{ij}) \), \( v_4 = (f_{ij}, h_{ij}) \) respectively. First compute the value
If \( f_{ij} \) is a small value relative to \( h_{ij} \), for instance, in the first step, when \( f_{ij} = 1 \) then

\[
| \mu_j | = \left| \frac{h_{i,ai} h_{ij} / h_{i,ai}^2}{h_{ij}} \right| = q_j, \quad \text{for} \quad j = 1, 2.
\]

The reduced operations \( v_2 = v_2 - \left[ \mu_1 \right] v_1 \) is \( v_2 = (f_{ij} - q f_{i,ai} h_{ij} - q h_{i,ai} h_{ij}^2) \) and \( v_4 = v_4 - \left[ \mu_2 \right] v_3 \), is \( v_4 = (f_{ij} - q f_{i,ai} h_{ij} - q h_{i,ai} h_{ij}^2) \) which agree with the GEEA. Finally, the GALA compares the lengths of the vectors \( v_2, v_4 \) with \( v_1, v_3 \) respectively to check if these vectors should be swapped. When \( f_{i,ai} \) is small compared with \( h_{i,ai} \), then \( \| v_2 \| \) and \( \| v_4 \| \) are smaller than \( \| v_1 \| \) and \( \| v_3 \| \). So, the vectors are swapped and the matrix becomes

\[
\begin{bmatrix}
  f_{ij} - q f_{i,ai} & h_{ij} - q h_{i,ai} \\
  h_{i,ai} & h_{i,ai}^2
\end{bmatrix},
\]

as shown in the GEEA. The generalized algorithms start to deviate once \( f_{ij} \). Further, the GEEA runs until \( h_{ij} = 0 \), in this case \( f_{ij} \approx n \), whereas the GLGA stops \( h_{ij} \approx f_{ij} \).

8. Conclusions

For applying some efficient algorithms to compute a scalar multiplication \( kP \) on elliptic curves \( E \) defined over a prime fields \( F_p \), the generators should be found. One of these generators are the ISD generators which consist of the linearly independent vectors \( v_2, v_4 \) and \( v_3, v_4 \). These vectors are the shortest vectors that form the bases on lattice \( L \) of rank 2. In this work, the generalization on the Lagrange-Gauss reduction method of basis lattice of rank 2 is proposed. On this generalization, the reduction of 2-tuple of integer vectors has been computed to give the good shortest bases lattice which are used to form the ISD generators \( \{ v_2, v_4 \} \) and \( \{ v_3, v_4 \} \).

The numerical results by simple example on the GLGA to generate ISD generators are compared with the numerical results that resulting from applying the GEEA. Based on the comparison results, the GLGA and GEEA can be connected to give the same numerical results of the ISD generators.

References
[1] Galbraith Steven D 2012 Mathematics of public key cryptography Cambridge University Press
[2] L C Washington 2006 Elliptic curves: number theory and cryptography CRC press
[3] J Hoffstein, J Pipher and J H Silverman 2008 An introduction to mathematical cryptography Springer
[4] G Robert P, L Robert J and V Scott A 2001 Faster point multiplication on elliptic curves with efficient endomorphisms Advances in Cryptology-CRYPTO pp 190-200
[5] K Dongryeol and L Seongan 2003 Integer decomposition for fast scalar multiplication on elliptic curves Selected Areas in Crypto pp 13-20
[7] R K K Ajeena 2015 Integer sub-decomposition (ISD) method for elliptic curve scalar multiplication
             *Diss. Universiti Sains Malaysia* pp 1-453
[8] R K K Ajeena and H Kamarulhaili 2013 Analysis on the elliptic scalar multiplication using integer
    sub decomposition method *Int. J. of Pu. and App. Math.* 87 1 pp 95-114
[9] R K K Ajeena and H. Kamarulhaili 2014 Point Multiplication using Integer Sub- Decomposition
    for Elliptic Curve Cryptography *Appl. Math. & Inf. Sci.* 8 2 pp 517-525
[10] R K K Ajeena and H Kamarulhaili 2014 Comparison Studies on Integer Decomposition Method
    for Elliptic Scalar Multiplication *Adva. Sci. Lett.* 20 2 pp 526-530
[11] R K K Ajeena 2015 Upper Bound of Scalars in the Integer Sub-decomposition Method: The
    Theoretical Aspects *J. of Cont. Sci. and Eng.* 2 pp 91-101
[12] R K K Ajeena and H Kamarulhaili Two dimensional Sub-decomposition method for point
    multiplication on elliptic curves *J. of Math. Sci. : Adva. and Appl.* 25 pp 43-56