J Autom Reasoning (2013) 50:161–172
DOI 10.1007/s10817-012-9265-2

Formalization of Definitions and Theorems Related to an Elliptic Curve Over a Finite Prime Field by Using Mizar

Yuichi Futa · Hiroyuki Okazaki · Yasunari Shidama

Received: 24 August 2011 / Accepted: 10 October 2012 / Published online: 27 October 2012

Abstract In this paper, we introduce our formalization of the definitions and theorems related to an elliptic curve over a finite prime field. The elliptic curve is important in an elliptic curve cryptosystem whose security is based on the computational complexity of the elliptic curve discrete logarithm problem.

Keywords Elliptic curve · Prime field · Projective coordinate

1 Introduction

Mizar [1] is an advanced project of the Mizar Society, led by Andrzej Trybulec, which formalizes mathematics. The Mizar project, which was developed to describe mathematics formally, describes mathematical proofs in the Mizar language [2]. The Mizar proof checker operates on both Windows and UNIX environments and registers proven definitions and theorems in the Mizar Mathematical Library (MML).

This work was partly supported by JSPS KAKENHI 21240001 and 22300285.

Y. Futa (✉)
Interdisciplinary Graduate School of Science and Technology,
Shinshu University, Nagano 380-8553, Japan
e-mail: y-futa@cam.hi-ho.ne.jp

H. Okazaki
Graduate School, Division of Science and Technology,
Shinshu University, Nagano, Japan
e-mail: okazaki@cs.shinshu-u.ac.jp

Y. Shidama
Department of Computer Science & Engineering, Faculty of Engineering,
Shinshu University, Nagano, Japan
e-mail: shidama@shinshu-u.ac.jp

In this paper, we formalize the definitions and theorems related to an elliptic curve over a finite prime field [3]. An elliptic curve is a non-singular cubic curve defined by the equation $y^2 = x^3 + ax + b$. An operation on points on the elliptic curve is defined. A set of points has the structure of an Abelian group using this operation.

An elliptic curve is an important mathematical concept related to fields such as number theory, algebra, analysis, topology, and algebraic geometry. One of the most important applications of elliptic curves is in an elliptic curve cryptosystem (ECC) [4]. The ECC uses scalar multiplications of the $\mathbb{Z}$-module constructed using the Abelian group. The security of the ECC is based on the computational complexity of the elliptic curve discrete logarithm problem, in which s is computed from sP (multiplication of a scalar s and a point P).

Recently, it has become necessary to prove the security of cryptosystems. A mathematical proof checker is important for this purpose. However, the formalization of mathematical definitions and theorems of the elliptic curve is not yet included in the MML. Hence, we need to enrich the MML by including the definitions and theorems.

This paper is organized as follows. In Section 2, we explain a finite prime field $\mathbb{F}_p$ and its formalization. Section 3 introduces the definitions of projective coordinates and an elliptic curve. In Section 4, we describe the relationship between the number of points on an elliptic curve over $\mathbb{F}_p$ and Legendre symbols. Section 5 explains an operation on points on an elliptic curve. We conclude our discussion in Section 6. The definitions and theorems in this paper are described as formalizations in Mizar and have been verified for correctness using the Mizar proof checker.

2 Finite Prime Field $\mathbb{F}_p$

In this section, we describe the definition of a finite prime field. A finite prime field $\mathbb{F}_p$, where p is a prime number, is used as the definition field of an elliptic curve.

First, we introduce the definition of a subfield.

Definition 1 (Subfield)

```
definition let K be Field;
  mode Subfield of K -> Field means
  the carrier of it c= the carrier of K
  & the addF of it = (the addF of K) || the carrier of it
  & the multF of it = (the multF of K) || the carrier of it
  & 1.it = 1.K & 0.it = 0.K;
```

Here, “`the carrier of it`” is a set constructed by the subfield of a field K, and “`(the addF of K) || the carrier of it`” and “`(the multF of K) || the carrier of it`” are limitations of the addition and multiplication of K in the set, respectively. “`0.it`” and “`1.it`” refer to the identity elements of addition and multiplication in the subfield, respectively. Definition 1 defines a field satisfying the following conditions as a subfield of K:

- A set constructed by the field is included in a set constructed by K.
- Addition and multiplication of the field are limited to those of K in the set constructed by the field.

- Identity elements of addition and multiplication in the field are equal to those in K.

We now introduce the definition of a prime field.

Definition 2 (Prime field)

```
definition let IT be Field;
  attr IT is prime means
  K1 is strict Subfield of IT implies K1 = IT;
end;
```

Definition 2 indicates that a subfield of a prime field is the prime field itself.
For $\mathbb{F}_p$, where p is a prime number, the following theorem holds:

Theorem 1 (Prime field $\mathbb{F}_p$)

```
theorem
  for p be Prime holds GF(p) is prime;
```

Here, "`GF(p)`" denotes $\mathbb{F}_p$. Theorem 1 indicates that $\mathbb{F}_p$, where p is a prime number, is a prime field.

We introduce an outline of a proof of Theorem 1. The basic construction of the proof is as follows:

(1) proving that all elements in $K = \mathbb{F}_p$ are in a subfield K' of K, and
(2) proving that K is a subfield of K' and $K = K'$ because K' is the subfield of K.

(1) mentioned above can be proved by the inductive method. The detailed proof is as follows:

(a) 0 is included in K' because `0.it = 0.K`.
(b) When we assume that a natural number n ($0 \leq n < p - 1$) is included in K', $n + 1$ is included in K'.
(b) Because of the induction of (a) and (b), all elements of K ($0, 1, \cdots p - 1$) are included in K'.

(b) is proved by using the following theorem [5]:

```
theorem :: BINOP_1:17
  for f being Function of [:X,Y:],Z st x in X & y in Y &
  Z <> {} holds f.(x,y) in Z;
```

The inductive method used in (c) is as follows [6]:

```
scheme :: INT_1:sch 7
  FinInd{M, N() -> Element of NAT, P[Nat]} : for i being
  Element of NAT st M() <= i & i <= N() holds P[i]
provided
 P[M()] and
 for j being Element of NAT st M() <= j & j < N() holds
 P[j] implies P[j+1];
```

Here, “`P[j]`” indicates that a natural number j is included in K', and “`M()`” and “`N()`” are set to 0 and $p-1$, respectively.

3 Elliptic Curve

This section defines an elliptic curve.

We define the projective coordinates on which the elliptic curve is drawn.

Definition 3 (Projective coordinate)

```
definition let K be Field;
  func ProjCo(K) -> non empty Subset of
  [:the carrier of K, the carrier of K, the carrier of K:] equals
  [:the carrier of K, the carrier of K, the carrier of K:]
  \ {[0.K,0.K,0.K]};
end;
```

By Definition 3, when P is in “`ProjCo(K)`,” $P = [X_P, Y_P, Z_P] \in K^3 \backslash \{[0,0,0]\}$, where X_P, Y_P, and Z_P are the X, Y-, and Z-coordinates of P, respectively. The projective coordinates of P and Q are defined as follows such that their coordinates are equivalent:

Definition 4 (Equivalence of projective coordinates)

```
definition
  let p be Prime;
  let P,Q be Element of ProjCo(GF(p));
  pred P _EQ_ Q means
    ex a be Element of GF(p) st a <> 0.GF(p)
    & P`1 = a*Q`1 & P`2 = a*Q`2 & P`3 = a*Q`3;
  reflexivity;
  symmetry;
end;
```

Here, “``P`1(Q`1)``,” “``P`2(Q`2)``,” and “``P`3(Q`3)``” are the X, Y-, and Z-coordinates of $P(Q)$, respectively. “`_EQ_`” denotes the equivalence relation of the projective coordinates. Definition 4 indicates that P and Q are equivalent when $a(\neq 0)$ exists such that $X_P = a \times X_Q$, $Y_P = a \times Y_Q$, and $Z_P = a \times Z_Q$.

We describe the definition equation of an elliptic curve as follows:

Definition 5 (Definition equation of an elliptic curve)

```
definition
  let p be Prime;
  let a, b be Element of GF(p);
  func EC_WEqProjCo(a,b,p) -> Function of
  [:the carrier of GF(p), the carrier of GF(p),
  the carrier of GF(p):], GF(p) means
  for P be Element of [:the carrier of GF(p),
  the carrier of GF(p), the carrier of GF(p):] holds
  it. P = ((P`2) |^2)*(P`3)-((P`1) |^3 +a*(P`1)*(P`3) |^2
  +b*(P`3) |^3);
end;
```

Definition 5 indicates that an elliptic curve is defined by the equation $Y^2Z - (X^3 + aXZ^2 + b\,Z^3) = 0$. Note that the equation $Y^2Z - (X^3 + aXZ^2 + b\,Z^3) = 0$ is valid for the definition field $\mathbb{F}_p$, where "$p > 3$." In this paper, we consider $p > 3$.

Because the elliptic curve is a non-singular cubic curve, the discriminant $\delta = 4a^3 + 27b^2$ ("Disc") is not equal to 0. The discriminant is defined as follows:

Definition 6 (Discriminant of an elliptic curve)

```
definition
  let p be Prime;
  let a, b be Element of GF(p);
  func Disc(a,b,p) -> Element of GF(p) means
  for g4, g27 be Element of GF(p) st g4 = 4 mod p &
  g27 = 27 mod p
  holds it = g4*a|^3 + g27*b|^2;
end;
```

A set of $\mathbb{F}_p$-rational points on the elliptic curve is defined as follows:

Definition 7 (Set of $\mathbb{F}_p$-rational points)

```
definition
  let p be Prime;
  let a, b be Element of GF(p);
  func EC_SetProjCo(a,b,p) -> non empty Subset of ProjCo(GF(p))
  equals {P where P is Element of ProjCo(GF(p)) :
  EC_WEqProjCo(a,b,p).P = 0.GF(p)};
end;
```

Definition 7 denotes that $\mathbb{F}_p$-rational points on the elliptic curve are points satisfying the definition equation "EC_WEqProjCo(a,b,p).P = 0."

4 Number of $\mathbb{F}_p$-Rational Points on an Elliptic Curve

In this section, we explain the definitions and theorems related to the number of $\mathbb{F}_p$-rational points on an elliptic curve over $\mathbb{F}_p$. The number of $\mathbb{F}_p$-rational points on an elliptic curve is counted without the equivalence of the projective coordinates.

4.1 Legendre Symbol

The number of $\mathbb{F}_p$-rational points on an elliptic curve can be calculated by using Legendre symbols. Legendre symbols are related to the quadratic residue defined as follows:

Definition 8 (Quadratic residue)

```
definition let p, a;
  attr a is quadratic_residue means
  a <> 0 & ex x being Element of GF(p) st x|^2 = a;
  attr a is not_quadratic_residue means
  a <> 0 & not ex x being Element of GF(p) st x|^2 = a;
end;
```

Definition 8 indicates that $a(\neq 0 \bmod p)$ is a quadratic residue when x exists such that $x^2 = a$, and is not a quadratic residue when x does not exist.

Legendre symbols $(\frac{a}{p})$ (“`Lege_p(a)`”) are defined as follows:

Definition 9 (Legendre symbol)

```
definition let p, a;
  func Lege_p(a) -> Integer equals
  0 if a = 0,
  1 if a is quadratic_residue
  otherwise -1;
end;
```

Definition 9 denotes that

- $(\frac{a}{p}) = 0$ when $a = 0 \bmod p$,
- $(\frac{a}{p}) = 1$ when $a(\neq 0 \bmod p)$ is a quadratic residue, and
- $(\frac{a}{p}) = -1$ when $a(\neq 0 \bmod p)$ is not a quadratic residue.

The number of solutions of a second-degree equation $b^2 = a$ over $\mathbb{F}_p$ is related to the Legendre symbol as follows:

Theorem 2 (Number of solutions of the second-degree equation)

```
theorem
  2 < p implies card({b : b|^2 = a}) = 1 + Lege_p(a);
```

Theorem 2 indicates that the number of solutions of the equation $b^2 = a$ over $\mathbb{F}_p$ is equal to $1 + (\frac{a}{p})$.

4.2 Relationship Between Legendre Symbols and the Number of $\mathbb{F}_p$-Rational Points on an Elliptic Curve

An $\mathbb{F}_p$-rational point is equivalent to $[0, 1, 0]$ or $[X, Y, 1]$ $(X, Y \in \mathbb{F}_p)$ as per the following theorem:

Theorem 3 (Equivalence of points on an elliptic curve)

```
theorem
  for p be Prime, a, b be Element of GF(p), x be set st
  p > 3 & Disc(a,b,p) <> 0.GF(p)
  & x in Class (R_EllCur(a,b,p)) holds
  ( ex P be Element of ProjCo(GF(p)) st P in EC_SetProjCo(a,b,p)
  & P=[0,1,0]
  & x = Class(R_EllCur(a,b,p),P) ) or
  ex P be Element of ProjCo(GF(p)), X,Y be Element of GF(p)
  st P in EC_SetProjCo(a,b,p) & P=[X,Y,1]
  & x = Class(R_EllCur(a,b,p),P);
```

Here, “`Class(R_EllCur(a,b,p).P)`” is an equivalence class of P defined by the equivalence relation in Definition 4. “`Class(R_EllCur(a,b,p))`” denotes all the equivalence classes [8], that are a set of $\mathbb{F}_p$-rational points. By Theorem 3, the following theorem of equivalence classes holds:

Theorem 4 (Equivalence classes of points on an elliptic curve)

```
 theorem
  for p be Prime, a, b be Element of GF(p) st
  p > 3 & Disc(a,b,p) <> 0.GF(p) holds
  Class (R_EllCur(a,b,p)) = {Class(R_EllCur(a,b,p),[0,1,0])}
  \/ {Class(R_EllCur(a,b,p),P)
  where P is Element of ProjCo(GF(p)):
  P in EC_SetProjCo(a,b,p) & ex X,Y be Element of GF(p)
  st P=[X,Y,1]};
```

Theorem 4 indicates that the set of all equivalence classes of $\mathbb{F}_p$-rational points consists of an equivalence class including $[0, 1, 0]$ and equivalence classes including $[X, Y, 1]$.

We count the equivalence classes to calculate the number of $\mathbb{F}_p$-rational points on an elliptic curve (cardinality [7] of the equivalence classes). For this purpose, we prove the following:

(1) the equivalence class of $[0, 1, 0]$ and the equivalence classes of $[X, Y, 1]$ are disjoint, and
(2) the equivalence class of $[X_1, Y_1, 1]$ and the equivalence of class $[X_2, Y_2, 1]$ $(X_1 \neq X_2)$ are disjoint.

(1) is described by the following theorem:

Theorem 5 (Relationship of equivalence classes 1)

```
theorem
  for p be Prime, a, b be Element of GF(p),
  F1,F2 be set st p > 3 & Disc(a,b,p) <> 0.GF(p)
  & F1 = {Class(R_EllCur(a,b,p),[0,1,0])} &
  F2 = {Class(R_EllCur(a,b,p),P) where P is
  Element of ProjCo(GF(p)): P in EC_SetProjCo(a,b,p) &
  ex X,Y be Element of GF(p) st P=[X,Y,1]} holds F1 misses F2;
```

(2) is described by the following theorem:

Theorem 6 (Relationship of equivalence classes 2)

```
theorem
  for p be Prime, a, b, X1, Y1, X2, Y2 be Element of GF(p)
  st p > 3 & Disc(a,b,p) <> 0.GF(p)
  & [X1,Y1,1] in EC_SetProjCo(a,b,p)
  & [X2,Y2,1] in EC_SetProjCo(a,b,p) holds
  Class(R_EllCur(a,b,p),[X1,Y1,1]) =
  Class(R_EllCur(a,b,p),[X2,Y2,1]) iff X1=X2 & Y1=Y2;
```

Theorem 6 indicates that

$$\begin{aligned}&(\text{equivalence class of } [X_1, Y_1, 1]) = (\text{equivalence class of } [X_2, Y_2, 1])\\&\Leftrightarrow X_1 = X_2 \,\&\, Y_1 = Y_2.\end{aligned} \tag{4.1}$$

A contraposition of Theorem 6 is (2).

The number of equivalence classes of $[X, Y, 1]$ is equal to that of the solutions of the second-degree equation $Y^2 = X^3 + aX + b$ by the definition equation $Y^2Z - (X^3 + aXZ^2 + bZ^3) = 0$ of the elliptic curve. Therefore, the following theorem holds by Theorem 2:

Theorem 7 (Relationship between the X-coordinate and the number of points)

```
theorem
  for p be Prime, a, b, X be Element of GF(p)
  st p > 3 & Disc(a,b,p) <> 0.GF(p) holds
  card ({Class(R_EllCur(a,b,p),[X,Y,1])
  where Y is Element of GF(p) : [X,Y,1] in EC_SetProjCo(a,b,p)})
  = 1 + Lege_p(X|^3 + a*X + b);
```

By Theorems 5, 6, and 7,

$$1 + \sum_{X=0}^{p-1} \left\{ 1 + \left(\frac{X^3 + aX + b}{p} \right) \right\} = 1 + p + \sum_{X=0}^{p-1} \left(\frac{X^3 + aX + b}{p} \right). \tag{4.2}$$

Hence, the following theorem holds:

Theorem 8 (Number of $\mathbb{F}_p$-rational points on an elliptic curve)

```
theorem
  for p be Prime, a, b be Element of GF(p)
  st p > 3 & Disc(a,b,p) <> 0.GF(p)
  ex F be FinSequence of INT st len F = p &
  (for n be Nat st n in Seg p ex d be Element of GF(p)
  st X=n-1 & F.n = Lege_p(X|^3 + a*d + b)) &
  card(Class(R_EllCur(a,b,p))) = 1 + p + Sum(F);
```

5 Operation on Points on an Elliptic Curve

This section describes an operation on points on an elliptic curve. An addition operation of points on the elliptic curve that has an identity element $O = [0, 1, 0]$ is defined in this section.

An inversion element $-P = [X_P, -Y_P, Z_P]$ of $P = [X_P, Y_P, Z_P]$ is defined as follows:

Definition 10 (Inversion element of a point on an elliptic curve)

```
definition
  let p be greater_than_3 Prime;
  let z be Element of EC_WParam p;
  func compell_ProjCo(z,p) ->
  Function of EC_SetProjCo(z`1,z`2,p), EC_SetProjCo(z`1,z`2,p)
  means
  for P be Element of EC_SetProjCo(z`1,z`2,p)
  holds it.P = [P`1,-P`2,P`3];
end;
```

Here, "`compell_ProjCo(z,p).P`" denotes $-P$, and "`z`1`" and "`z`2`" denote a and b, respectively. `EC_WParam p` indicates the parameters a, b satisfying that the discriminant $\delta = 4a^3 + 27b^2 \neq 0 \bmod p$.

$Y_P = -Y_P$ and $Y_P = 0$ (because $p > 3$) hold in the following theorem since $P = -P \neq O \Rightarrow [X_P, Y_P, Z_P] = [X_P, -Y_P, Z_P]$:

Theorem 9 (2-torsion point)

```
theorem
  for p be greater_than_3 Prime, z be Element of EC_WParam p,
  P be Element of EC_SetProjCo(z`1,z`2,p) st P`3 <> 0 holds
  P _EQ_ compell_ProjCo(z,p).P iff P`2 = 0;
```

As $P = -P \Rightarrow P + P = 2P = O$, the above P is called a 2-torsion point.

A set of $\mathbb{F}_p$-rational points on the elliptic curve has the structure of an Abelian group by the following operation:

Definition 11 (Addition operation on points on an elliptic curve)

```
definition
  let p be greater_than_3 Prime,
      z be Element of EC_WParam p;
  func addell_ProjCo(z,p) -> Function of
  [:EC_SetProjCo(z`1,z`2,p),EC_SetProjCo(z`1,z`2,p):],
  EC_SetProjCo(z`1,z`2,p) means
  for P, Q, O being Element of EC_SetProjCo(z`1,z`2,p)
  st O = [0,1,0]
  holds
  (P _EQ_ O implies it.(P,Q) = Q) &
  ((Q _EQ_ O & not P _EQ_ O) implies it.(P,Q) = P) &
  ((not P _EQ_ O & not Q _EQ_ O & not P _EQ_ Q) implies
  for g2, u, v, A being Element of GF(p) st g2 = 2 mod p &
  u = Q`2*P`3 - P`2*Q`3 &
  v = Q`1*P`3 - P`1*Q`3 &
  A = (u |^2)*P`3*Q`3 - (v |^3) - g2*(v |^2)*P`1*Q`3
  holds it.(P,Q) = [v*A, u*((v |^2)*P`1*Q`3-A) - (v |^3)*P`2*Q`3,
  (v |^3)*P`3*Q`3]) &
  ((not P _EQ_ O & not Q _EQ_ O & P _EQ_ Q) implies
  for g2, g3, g4, g8, w, s, B, h being Element of GF(p) st
  g2 = 2 mod p & g3 = 3 mod p & g4 = 4 mod p & g8 = 8 mod p &
  w = (z`1)*(P`3 |^2) + g3*(P`1 |^2) &
  s = P`2*P`3 &
  B = P`1*P`2*s &
  h = (w |^2) - g8*B
  holds it.(P,Q) = [g2*h*s, w*(g4*B-h) - g8*(P`2 |^2)*(s |^2),
  g8*(s |^3)]);
end;
```

Definition 11 indicates that the addition operation (+) for $P = [X_P, Y_P, Z_P]$, $Q = [X_Q, Y_Q, Z_Q]$, and $R = P + Q = [X_R, Y_R, Z_R]$ is defined as follows:

(1) in the case that $P = O$, $R = Q$;
(2) in the case that $P \neq O$ and $Q = O$, $R = P$;
(3) in the case that $P \neq O$, $Q \neq O$ and $Q \neq P$,

$$X_R = vA \tag{5.1}$$

$$Y_R = u(v^2 X_P Z_Q - A) - v^3 Y_P Z_Q \tag{5.2}$$

$$Z_R = v^3 Z_P Z_Q \tag{5.3}$$

where $u = Y_Q Z_P - Y_P Z_Q$, $v = X_Q Z_P - X_P Z_Q$, $A = u^2 Z_P Z_Q - v^3 - 2v^2 X_P Z_Q$; and

(4) in the case that $P \neq O,\ Q \neq O$ and $Q = P$,

$$X_R = 2hs \tag{5.4}$$

$$Y_R = w(4B - h) - 8Y_P^2 s^2 \tag{5.5}$$

$$Z_R = 8s^3 \tag{5.6}$$

where $w = aZ_P^2 + 3X_P^2,\ s = Y_P Z_P,\ B = X_P Y_P s,\ h = w^2 - 8B$.

We must prove that "addell_ProjCo(z,p).(P,Q)" (called "R") is in "EC_SetPorjCo(z`1,z`2,p)" to show that the above operation "addell_ProjCo(z,p)" is defined on points on the elliptic curve over $\mathbb{F}_p$. This is shown by proving the following propositions:

(a) R is included in ProjCo(GF(p)), i.e., addell_ProjCo(z,p).(P,Q) is not equal to [0, 0, 0], and
(b) R satisfies EC_WEqProjCo(z`1,z`2,p).R = 0.GF(p).

(a) naturally holds in cases (1) and (2) in Definition 11. In case (3), (a) is satisfied as follows:

- in the case that $P = -Q$, as $v = 0$ and $u \neq 0$ by Definition 11, $Y_R \neq 0$, and
- in the case that $P \neq -Q$, as $v \neq 0$ by Definition 11, $Z_R \neq 0$.

In case (4), (a) is satisfied as follows:

- in the case that $Y_P = 0$ (that is P is a 2-torsion point), as $w \neq 0$, $Y_R \neq 0$, and
- in the case that $Y_P \neq 0$, as $s \neq 0$, $Z_R \neq 0$.

Here, $w \neq 0$ holds in the case that $Y_P = 0$ by the following theorem:

Theorem 10 (Discriminant of an elliptic curve and a 2-torsion point)

```
theorem
  for p be greater_than_3 Prime, z be Element of EC_WParam p,
  g3 be Element of GF(p), P be Element of EC_SetProjCo(z`1,z`2,p)
  st g3 = 3 mod p & P`2 = 0 & P`3 <> 0 holds
  (z`1)*(P`3 |^2) + g3*(P`1 |^2) <> 0;
```

Theorem 10 indicates that for $P \neq O$ satisfying $Y_P = 0$, $w \neq 0$ holds. The theorem is proved by using the characteristic that the discriminant $\delta \neq 0$(a 2-torsion point P is non-singular).

As (b) mentioned above (R satisfies EC_WEqProjCo(z`1,z`2,p).R = 0.GF(p)) is proved by using complicated transformation of equations, we omit its explanation.

6 Conclusion and Future Work

In this paper, we introduced our formalization of the definitions and theorems related to an elliptic curve over a finite prime field $\mathbb{F}_p$. We explained in detail the definitions and theorems of a finite prime field, an elliptic curve over $\mathbb{F}_p$, and an operation of points on the elliptic curve. The correctness of our formalization of the definitions and theorems was proved using a formal verification tool in the Mizar proof-checking system. Our formalizations are very important to prove the security of the ECC.

The operation on points on the elliptic curve can construct an Abelian group from a set of $\mathbb{F}_p$-rational points on the elliptic curve. For the construction, we need to prove the commutative law ($P + Q = Q + P$) and the associative law ($P + (Q + R) = (P + Q) + R$) of the operation. However, we have not formalized these laws yet. We plan to formalize these laws and complete the formalization of the Abelian group constructed from the set of $\mathbb{F}_p$-rational points on the elliptic curve in the near future. We will also formalize other definitions and theorems related with cryptosystems, particularly those used in the ECC.

References

1. Mizar proof checker: http://mizar.org/ (1973). Accessed 7 May 2011
2. Bonarska, E.: An introduction to PC mizar. Mizar Users Group, Fondation Philippe le Hodey, Brussels (1990)
3. Futa, Y., Okazaki, H., Shidama, Y.: Set of points on elliptic curve in projective coordinates. Formal. Math. **19**(3), 131–139 (2011)
4. Blake, I., Seroussi, G., Smart, N.: Elliptic Curves in Cryptography. London Mathematical Society Lecture Note Series, No. 265. Cambridge University Press (1999)
5. Byliński, C.: Binary operations. Formal. Math. **1**(1), 175–180 (1990)
6. Trybulec, J.: Integers. Formal. Math. **1**(3), 501–505 (1990)
7. Bancerek, G.: Cardinal numbers. Formal. Math. **1**(2), 377–382 (1990)
8. Raczkowski, K., Sadowski, P.: Equivalence relations and classes of abstraction. Formal. Math. **1**(3), 441–444 (1990)