

# Operations of Points on Elliptic Curve in Projective Coordinates

Yuichi Futa  
Shinshu University  
Nagano, Japan

Hiroyuki Okazaki<sup>1</sup>  
Shinshu University  
Nagano, Japan

Daichi Mizushima  
Shinshu University  
Nagano, Japan

Yasunari Shidama<sup>2</sup>  
Shinshu University  
Nagano, Japan

**Summary.** In this article, we formalize operations of points on an elliptic curve over  $\mathbf{GF}(\mathbf{p})$ . Elliptic curve cryptography [7], whose security is based on a difficulty of discrete logarithm problem of elliptic curves, is important for information security. We prove that the two operations of points: `compellprojCo` and `addellprojCo` are unary and binary operations of a point over the elliptic curve.

MML identifier: EC\_PF\_2, version: 7.12.02 4.176.1140

The terminology and notation used here are introduced in the following papers: [5], [17], [3], [1], [13], [4], [2], [12], [14], [10], [9], [16], [15], [8], [11], and [6].

## 1. ARITHMETIC IN $\mathbf{GF}(\mathbf{p})$

For simplicity, we adopt the following convention:  $i, j$  denote integers,  $n$  denotes a natural number,  $K$  denotes a field, and  $a_1, a_2, a_3, a_4, a_5, a_6$  denote elements of  $K$ .

One can prove the following propositions:

- (1) If  $a_1 = -a_2$ , then  $a_1^2 = a_2^2$ .
- (2)  $(1_K)^{-1} = 1_K$ .

---

<sup>1</sup>This work was supported by JSPS KAKENHI 21240001.

<sup>2</sup>This work was supported by JSPS KAKENHI 22300285.

- (3) If  $a_2 \neq 0_K$  and  $a_4 \neq 0_K$  and  $a_1 \cdot a_2^{-1} = a_3 \cdot a_4^{-1}$ , then  $a_1 \cdot a_4 = a_2 \cdot a_3$ .
- (4) If  $a_2 \neq 0_K$  and  $a_4 \neq 0_K$  and  $a_1 \cdot a_4 = a_2 \cdot a_3$ , then  $a_1 \cdot a_2^{-1} = a_3 \cdot a_4^{-1}$ .
- (5) If  $a_1 = 0_K$  and  $n > 1$ , then  $a_1^n = 0_K$ .
- (6) If  $a_1 = -a_2$ , then  $-a_1 = a_2$ .
- (7)  $a_1 + a_2 + a_3 + a_4 = a_4 + a_2 + a_3 + a_1$  and  $a_1 + a_2 + a_3 + a_4 = a_1 + a_4 + a_3 + a_2$ .
- (8)  $(a_1 + a_2 + a_3) + a_4 = a_1 + (a_2 + a_3 + a_4)$  and  $(a_1 + a_2 + a_3 + a_4) + a_5 = a_1 + (a_2 + a_3 + a_4 + a_5)$ .
- (9)  $(a_1 + a_2 + a_3 + a_4 + a_5) + a_6 = a_1 + (a_2 + a_3 + a_4 + a_5 + a_6)$ .
- (10)  $a_1 \cdot a_2 \cdot a_3 \cdot a_4 = a_4 \cdot a_2 \cdot a_3 \cdot a_1$  and  $a_1 \cdot a_2 \cdot a_3 \cdot a_4 = a_1 \cdot a_4 \cdot a_3 \cdot a_2$ .
- (11)  $(a_1 \cdot a_2 \cdot a_3) \cdot a_4 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4)$  and  $(a_1 \cdot a_2 \cdot a_3 \cdot a_4) \cdot a_5 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4 \cdot a_5)$ .
- (12)  $(a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5) \cdot a_6 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4 \cdot a_5 \cdot a_6)$  and  $a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5 \cdot a_6 = a_1 \cdot (a_2 \cdot a_3 \cdot a_4) \cdot a_5 \cdot a_6$ .
- (13)  $(a_1 \cdot a_2 \cdot a_3)^n = a_1^n \cdot a_2^n \cdot a_3^n$ .
- (14)  $a_1 \cdot (a_2 + a_3 + a_4) = a_1 \cdot a_2 + a_1 \cdot a_3 + a_1 \cdot a_4$  and  $a_1 \cdot ((a_2 + a_3) - a_4) = (a_1 \cdot a_2 + a_1 \cdot a_3) - a_1 \cdot a_4$  and  $a_1 \cdot ((a_2 - a_3) + a_4) = (a_1 \cdot a_2 - a_1 \cdot a_3) + a_1 \cdot a_4$  and  $a_1 \cdot (a_2 - a_3 - a_4) = a_1 \cdot a_2 - a_1 \cdot a_3 - a_1 \cdot a_4$  and  $a_1 \cdot (-a_2 + a_3 + a_4) = -a_1 \cdot a_2 + a_1 \cdot a_3 + a_1 \cdot a_4$  and  $a_1 \cdot ((-a_2 + a_3) - a_4) = (-a_1 \cdot a_2 + a_1 \cdot a_3) - a_1 \cdot a_4$  and  $a_1 \cdot ((-a_2 - a_3) + a_4) = (-a_1 \cdot a_2 - a_1 \cdot a_3) + a_1 \cdot a_4$  and  $a_1 \cdot (-a_2 - a_3 - a_4) = -a_1 \cdot a_2 - a_1 \cdot a_3 - a_1 \cdot a_4$ .
- (15)  $(a_1 + a_2) \cdot (a_1 - a_2) = a_1^2 - a_2^2$ .
- (16)  $(a_1 + a_2) \cdot ((a_1^2 - a_1 \cdot a_2) + a_2^2) = a_1^3 + a_2^3$ .
- (17)  $(a_1 - a_2) \cdot (a_1^2 + a_1 \cdot a_2 + a_2^2) = a_1^3 - a_2^3$ .

Let  $n, p$  be natural numbers. We say that  $p$  is  $n$  or greater if and only if:

(Def. 1)  $n \leq p$ .

Let us note that there exists a natural number which is 5 or greater and prime.

The following propositions are true:

- (18) For all elements  $g_1, g_2, g_3, a$  of  $\text{GF}(p)$  such that  $g_1 = i \pmod p$  and  $g_2 = j \pmod p$  and  $g_3 = (i + j) \pmod p$  holds  $g_1 \cdot a + g_2 \cdot a = g_3 \cdot a$ .
- (19) For all elements  $g_1, g_2, a$  of  $\text{GF}(p)$  such that  $g_1 = i \pmod p$  and  $g_2 = j \pmod p$  and  $j = i + 1$  holds  $g_1 \cdot a + a = g_2 \cdot a$ .
- (20) For all elements  $g_4, a$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  holds  $a + a = g_4 \cdot a$ .
- (21) For all elements  $g_1, g_2, g_3, a$  of  $\text{GF}(p)$  such that  $g_1 = i \pmod p$  and  $g_2 = j \pmod p$  and  $g_3 = (i - j) \pmod p$  holds  $g_1 \cdot a - g_2 \cdot a = g_3 \cdot a$ .
- (22) For all elements  $g_1, g_2, a$  of  $\text{GF}(p)$  such that  $g_1 = i \pmod p$  and  $g_2 = j \pmod p$  and  $i = j + 1$  holds  $g_1 \cdot a - g_2 \cdot a = a$ .
- (23) For all elements  $g_1, g_2, a$  of  $\text{GF}(p)$  such that  $g_1 = i \pmod p$  and  $g_2 = j \pmod p$  and  $i = j + 1$  holds  $g_1 \cdot a - a = g_2 \cdot a$ .

- (24) For all elements  $g_4, a$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  holds  $g_4 \cdot a - a = a$ .
- (25) For all elements  $g_4, a, b$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  holds  $(a + b)^2 = a^2 + g_4 \cdot a \cdot b + b^2$ .
- (26) For all elements  $g_4, a, b$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  holds  $(a - b)^2 = (a^2 - g_4 \cdot a \cdot b) + b^2$ .
- (27) For all elements  $g_4, a, b, c, d$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  holds  $(a \cdot c + b \cdot d)^2 = a^2 \cdot c^2 + g_4 \cdot a \cdot b \cdot c \cdot d + b^2 \cdot d^2$ .
- (28) Let  $p$  be a prime number,  $n$  be a natural number, and  $g_4$  be an element of  $\text{GF}(p)$ . If  $p > 2$  and  $g_4 = 2 \pmod p$ , then  $g_4 \neq 0_{\text{GF}(p)}$  and  $g_4^n \neq 0_{\text{GF}(p)}$ .
- (29) Let  $p$  be a prime number,  $n$  be a natural number, and  $g_4, g_5$  be elements of  $\text{GF}(p)$ . If  $p > 3$  and  $g_5 = 3 \pmod p$ , then  $g_5 \neq 0_{\text{GF}(p)}$  and  $g_5^n \neq 0_{\text{GF}(p)}$ .

## 2. PARAMETERS OF AN ELLIPTIC CURVE

Let  $p$  be a 5 or greater prime number. The parameters of elliptic curve  $p$  yielding a subset of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$  is defined as follows:

- (Def. 2) The parameters of elliptic curve  $p = \{ \langle a, b \rangle; a \text{ ranges over elements of } \text{GF}(p), b \text{ ranges over elements of } \text{GF}(p): \text{Disc}(a) \neq 0_{\text{GF}(p)} \}$ .

Let  $p$  be a 5 or greater prime number. Observe that the parameters of elliptic curve  $p$  is non empty.

Let  $p$  be a 5 or greater prime number and let  $z$  be an element of the parameters of elliptic curve  $p$ . Then  $z_1$  is an element of  $\text{GF}(p)$ . Then  $z_2$  is an element of  $\text{GF}(p)$ .

The following proposition is true

- (30) Let  $p$  be a 5 or greater prime number and  $z$  be an element of the parameters of elliptic curve  $p$ . Then  $p > 3$  and  $\text{Disc}(z_1) \neq 0_{\text{GF}(p)}$ .

For simplicity, we adopt the following rules:  $p_1, p_2, p_3$  denote sets,  $P_1, P_2, P_3$  denote elements of  $\text{GF}(p)$ ,  $P$  denotes an element of  $\text{ProjCo}(\text{GF}(p))$ , and  $O$  denotes an element of  $\text{EC}_{\text{SetProjCo}}(a)$ .

Let  $p$  be a prime number, let  $a, b$  be elements of  $\text{GF}(p)$ , and let  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(a)$ . The functor  $P_1$  yields an element of  $\text{GF}(p)$  and is defined as follows:

- (Def. 3) If  $P = \langle p_1, p_2, p_3 \rangle$ , then  $P_1 = p_1$ .

The functor  $P_2$  yielding an element of  $\text{GF}(p)$  is defined as follows:

- (Def. 4) If  $P = \langle p_1, p_2, p_3 \rangle$ , then  $P_2 = p_2$ .

The functor  $P_3$  yielding an element of  $\text{GF}(p)$  is defined by:

- (Def. 5) If  $P = \langle p_1, p_2, p_3 \rangle$ , then  $P_3 = p_3$ .

We now state three propositions:

- (31) For every prime number  $p$  and for all elements  $a, b$  of  $\text{GF}(p)$  and for every element  $P$  of  $\text{EC}_{\text{SetProjCo}}(a)$  holds  $P = \langle P_1, P_2, P_3 \rangle$ .
- (32) Let  $p$  be a prime number,  $a, b$  be elements of  $\text{GF}(p)$ ,  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(a)$ , and  $Q$  be an element of  $\text{ProjCo}(\text{GF}(p))$ . Then  $P = Q$  if and only if the following conditions are satisfied:
- (i)  $P_1 = Q_1$ ,
  - (ii)  $P_2 = Q_2$ , and
  - (iii)  $P_3 = Q_3$ .
- (33) Let  $p$  be a prime number,  $a, b, P_1, P_2, P_3$  be elements of  $\text{GF}(p)$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(a)$ . If  $P = \langle P_1, P_2, P_3 \rangle$ , then  $P_1 = P_1$  and  $P_2 = P_2$  and  $P_3 = P_3$ .

Let  $p$  be a prime number, let  $P$  be an element of  $\text{ProjCo}(\text{GF}(p))$ , and let  $C_1$  be a function from  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$  into  $\text{GF}(p)$ . We say that  $P$  is on curve defined by an equation  $C_1$  if and only if:

(Def. 6)  $C_1(P) = 0_{\text{GF}(p)}$ .

The following two propositions are true:

- (34)  $P$  is on curve defined by an equation  $\text{EC}_{\text{WEqProjCo}}(a)$  iff  $P$  is an element of  $\text{EC}_{\text{SetProjCo}}(a)$ .
- (35) Let  $p$  be a prime number,  $a, b$  be elements of  $\text{GF}(p)$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(a)$ . Then  $(P_2)^2 \cdot P_3 - ((P_1)^3 + a \cdot P_1 \cdot (P_3)^2 + b \cdot (P_3)^3) = 0_{\text{GF}(p)}$ .

Let  $p$  be a prime number and let  $P$  be an element of  $\text{ProjCo}(\text{GF}(p))$ . The represent point of  $P$  yields an element of  $\text{ProjCo}(\text{GF}(p))$  and is defined by:

- (Def. 7)(i) The represent point of  $P = \langle P_1 \cdot (P_3)^{-1}, P_2 \cdot (P_3)^{-1}, 1 \rangle$  if  $P_3 \neq 0$ ,
- (ii) the represent point of  $P = \langle 0, 1, 0 \rangle$  if  $P_3 = 0$ ,
  - (iii)  $P_3 = 0$ , otherwise.

The following propositions are true:

- (36) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then the represent point of  $P \equiv P$  and the represent point of  $P \in \text{EC}_{\text{SetProjCo}}(z_1)$ .
- (37) Let  $p$  be a prime number,  $a, b$  be elements of  $\text{GF}(p)$ , and  $P$  be an element of  $\text{ProjCo}(\text{GF}(p))$ . Suppose  $(\text{the represent point of } P)_3 = 0$ . Then the represent point of  $P = \langle 0, 1, 0 \rangle$  and  $P_3 = 0$ .
- (38) Let  $p$  be a prime number,  $a, b$  be elements of  $\text{GF}(p)$ , and  $P$  be an element of  $\text{ProjCo}(\text{GF}(p))$ . Suppose  $(\text{the represent point of } P)_3 \neq 0$ . Then the represent point of  $P = \langle P_1 \cdot (P_3)^{-1}, P_2 \cdot (P_3)^{-1}, 1 \rangle$  and  $P_3 \neq 0$ .
- (39) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $P \equiv Q$  if and only if the represent point of  $P =$  the represent point of  $Q$ .

3. OPERATIONS OF POINTS ON AN ELLIPTIC CURVE OVER  $\mathbf{GF}(p)$ 

Let  $p$  be a 5 or greater prime number and let  $z$  be an element of the parameters of elliptic curve  $p$ . The functor  $\text{compell}_{\text{ProjCo}}(z, p)$  yields a function from  $\text{EC}_{\text{SetProjCo}}(z_1)$  into  $\text{EC}_{\text{SetProjCo}}(z_1)$  and is defined as follows:

(Def. 8) For every element  $P$  of  $\text{EC}_{\text{SetProjCo}}(z_1)$  holds  $(\text{compell}_{\text{ProjCo}}(z, p))(P) = \langle P_1, -P_2, P_3 \rangle$ .

Let  $p$  be a 5 or greater prime number, let  $z$  be an element of the parameters of elliptic curve  $p$ , let  $F$  be a function from  $\text{EC}_{\text{SetProjCo}}(z_1)$  into  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and let  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $F(P)$  is an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ .

We now state a number of propositions:

- (40) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $O$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $O = \langle 0, 1, 0 \rangle$ , then  $(\text{compell}_{\text{ProjCo}}(z, p))(O) \equiv O$ .
- (41) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $(\text{compell}_{\text{ProjCo}}(z, p))((\text{compell}_{\text{ProjCo}}(z, p))(P)) = P$ .
- (42) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Suppose  $P_3 \neq 0$ . Then the represent point of  $(\text{compell}_{\text{ProjCo}}(z, p))(P) = (\text{compell}_{\text{ProjCo}}(z, p))(\text{the represent point of } P)$ .
- (43) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $P = Q$  if and only if  $(\text{compell}_{\text{ProjCo}}(z, p))(P) = (\text{compell}_{\text{ProjCo}}(z, p))(Q)$ .
- (44) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $P_3 \neq 0$ , then  $P \equiv (\text{compell}_{\text{ProjCo}}(z, p))(P)$  iff  $P_2 = 0$ .
- (45) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $P_3 \neq 0$ , then  $P_1 = Q_1$  and  $P_3 = Q_3$  iff  $P = Q$  or  $P = (\text{compell}_{\text{ProjCo}}(z, p))(Q)$ .
- (46) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $P \equiv Q$  if and only if  $(\text{compell}_{\text{ProjCo}}(z, p))(P) \equiv (\text{compell}_{\text{ProjCo}}(z, p))(Q)$ .
- (47) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $P \equiv (\text{compell}_{\text{ProjCo}}(z, p))(Q)$  if and only if  $(\text{compell}_{\text{ProjCo}}(z, p))(P) \equiv Q$ .
- (48) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Suppose  $P_3 \neq 0$  and  $Q_3 \neq 0$ . Then the represent point of  $P = (\text{compell}_{\text{ProjCo}}(z, p))(\text{the$

represent point of  $Q$ ) if and only if  $P \equiv (\text{compell}_{\text{ProjCo}}(z, p))(Q)$ .

- (49) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $P \equiv Q$ , then  $P_2 \cdot Q_3 = Q_2 \cdot P_3$ .
- (50) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Suppose  $P_3 \neq 0$  and  $Q_3 \neq 0$ . Then  $P \equiv Q$  or  $P \equiv (\text{compell}_{\text{ProjCo}}(z, p))(Q)$  if and only if  $P_1 \cdot Q_3 = Q_1 \cdot P_3$ .
- (51) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $P_3 \neq 0$  and  $Q_3 \neq 0$  and  $P_2 \neq 0$ , then if  $P \equiv (\text{compell}_{\text{ProjCo}}(z, p))(Q)$ , then  $P_2 \cdot Q_3 \neq Q_2 \cdot P_3$ .
- (52) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ , and  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $P \not\equiv Q$  and  $P \equiv (\text{compell}_{\text{ProjCo}}(z, p))(Q)$ , then  $P_2 \cdot Q_3 \neq Q_2 \cdot P_3$ .
- (53) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_5$  be an element of  $\text{GF}(p)$ , and  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . If  $g_5 = 3 \pmod{p}$  and  $P_2 = 0$  and  $P_3 \neq 0$ , then  $z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2 \neq 0$ .
- (54) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_6, g_7, g_8$  be elements of  $\text{GF}(p)$ ,  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$ . Suppose that
- (i)  $g_4 = 2 \pmod{p}$ ,
  - (ii)  $g_6 = Q_2 \cdot P_3 - P_2 \cdot Q_3$ ,
  - (iii)  $g_7 = Q_1 \cdot P_3 - P_1 \cdot Q_3$ ,
  - (iv)  $g_8 = g_6^2 \cdot P_3 \cdot Q_3 - g_7^3 - g_4 \cdot g_7^2 \cdot P_1 \cdot Q_3$ , and
  - (v)  $R = \langle g_7 \cdot g_8, g_6 \cdot (g_7^2 \cdot P_1 \cdot Q_3 - g_8) - g_7^3 \cdot P_2 \cdot Q_3, g_7^3 \cdot P_3 \cdot Q_3 \rangle$ .
- Then  $g_7 \cdot P_3 \cdot R_2 = -(g_6 \cdot (R_1 \cdot P_3 - P_1 \cdot R_3) + g_7 \cdot P_2 \cdot R_3)$ .
- (55) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_6, g_7, g_8$  be elements of  $\text{GF}(p)$ ,  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$ . Suppose that
- (i)  $g_4 = 2 \pmod{p}$ ,
  - (ii)  $g_6 = Q_2 \cdot P_3 - P_2 \cdot Q_3$ ,
  - (iii)  $g_7 = Q_1 \cdot P_3 - P_1 \cdot Q_3$ ,
  - (iv)  $g_8 = g_6^2 \cdot P_3 \cdot Q_3 - g_7^3 - g_4 \cdot g_7^2 \cdot P_1 \cdot Q_3$ , and
  - (v)  $R = \langle g_7 \cdot g_8, g_6 \cdot (g_7^2 \cdot P_1 \cdot Q_3 - g_8) - g_7^3 \cdot P_2 \cdot Q_3, g_7^3 \cdot P_3 \cdot Q_3 \rangle$ .
- Then  $-g_7^2 \cdot (P_3 \cdot Q_3 \cdot R_1 + P_3 \cdot Q_1 \cdot R_3 + P_1 \cdot Q_3 \cdot R_3) + P_3 \cdot Q_3 \cdot R_3 \cdot g_6^2 = 0_{\text{GF}(p)}$ .

(56) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_6, g_7, g_8$  be elements of  $\text{GF}(p)$ ,  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$ . Suppose that

(i)  $g_4 = 2 \pmod{p}$ ,

(ii)  $g_6 = Q_2 \cdot P_3 - P_2 \cdot Q_3$ ,

(iii)  $g_7 = Q_1 \cdot P_3 - P_1 \cdot Q_3$ ,

(iv)  $g_8 = g_6^2 \cdot P_3 \cdot Q_3 - g_7^3 - g_4 \cdot g_7^2 \cdot P_1 \cdot Q_3$ , and

(v)  $R = \langle g_7 \cdot g_8, g_6 \cdot (g_7^2 \cdot P_1 \cdot Q_3 - g_8) - g_7^3 \cdot P_2 \cdot Q_3, g_7^3 \cdot P_3 \cdot Q_3 \rangle$ .

Then  $z_2 \cdot g_7^2 \cdot (P_3)^2 \cdot Q_3 \cdot R_3 = -g_7^2 \cdot P_3 \cdot P_1 \cdot Q_1 \cdot R_1 + (g_7 \cdot P_2 - g_6 \cdot P_1)^2 \cdot Q_3 \cdot R_3$ .

(57) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_6, g_7, g_8$  be elements of  $\text{GF}(p)$ ,  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$ . Suppose that

(i)  $g_4 = 2 \pmod{p}$ ,

(ii)  $g_6 = Q_2 \cdot P_3 - P_2 \cdot Q_3$ ,

(iii)  $g_7 = Q_1 \cdot P_3 - P_1 \cdot Q_3$ ,

(iv)  $g_8 = g_6^2 \cdot P_3 \cdot Q_3 - g_7^3 - g_4 \cdot g_7^2 \cdot P_1 \cdot Q_3$ , and

(v)  $R = \langle g_7 \cdot g_8, g_6 \cdot (g_7^2 \cdot P_1 \cdot Q_3 - g_8) - g_7^3 \cdot P_2 \cdot Q_3, g_7^3 \cdot P_3 \cdot Q_3 \rangle$ .

Then  $z_1 \cdot g_7^2 \cdot P_3 \cdot Q_3 \cdot R_3 = g_7^2 \cdot (P_1 \cdot Q_1 \cdot R_3 + P_3 \cdot Q_1 \cdot R_1 + P_1 \cdot Q_3 \cdot R_1) + g_4 \cdot g_6 \cdot Q_3 \cdot R_3 \cdot (g_7 \cdot P_2 - g_6 \cdot P_1)$ .

(58) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_6, g_7, g_8$  be elements of  $\text{GF}(p)$ ,  $P, Q$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$ . Suppose that

(i)  $g_4 = 2 \pmod{p}$ ,

(ii)  $g_6 = Q_2 \cdot P_3 - P_2 \cdot Q_3$ ,

(iii)  $g_7 = Q_1 \cdot P_3 - P_1 \cdot Q_3$ ,

(iv)  $g_8 = g_6^2 \cdot P_3 \cdot Q_3 - g_7^3 - g_4 \cdot g_7^2 \cdot P_1 \cdot Q_3$ , and

(v)  $R = \langle g_7 \cdot g_8, g_6 \cdot (g_7^2 \cdot P_1 \cdot Q_3 - g_8) - g_7^3 \cdot P_2 \cdot Q_3, g_7^3 \cdot P_3 \cdot Q_3 \rangle$ .

Then  $g_7^2 \cdot (P_3)^2 \cdot Q_3 \cdot ((R_2)^2 \cdot R_3 - ((R_1)^3 + z_1 \cdot R_1 \cdot (R_3)^2 + z_2 \cdot (R_3)^3)) = 0_{\text{GF}(p)}$ .

(59) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10}$  be elements of  $\text{GF}(p)$ ,  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of  $(\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p)) \times (\text{the carrier of } \text{GF}(p))$ . Suppose that  $g_4 = 2 \pmod{p}$  and  $g_5 = 3 \pmod{p}$  and  $g_{11} = 4 \pmod{p}$  and  $g_9 = 8 \pmod{p}$  and  $g_6 = z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2$  and  $g_7 = P_2 \cdot P_3$  and  $g_8 = P_1 \cdot P_2 \cdot g_7$  and  $g_{10} = g_6^2 - g_9 \cdot g_8$  and  $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_2)^2 \cdot g_7^2, g_9 \cdot g_7^3 \rangle$ . Then  $g_4 \cdot g_7 \cdot P_3 \cdot R_2 = -(g_6 \cdot (P_3 \cdot R_1 - P_1 \cdot R_3) + g_4 \cdot g_7 \cdot P_2 \cdot R_3)$ .

- (60) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10}$  be elements of  $\text{GF}(p)$ ,  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ ). Suppose that  $g_4 = 2 \pmod p$  and  $g_5 = 3 \pmod p$  and  $g_{11} = 4 \pmod p$  and  $g_9 = 8 \pmod p$  and  $g_6 = z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2$  and  $g_7 = P_2 \cdot P_3$  and  $g_8 = P_1 \cdot P_2 \cdot g_7$  and  $g_{10} = g_6^2 - g_9 \cdot g_8$  and  $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_2)^2 \cdot g_7^2, g_9 \cdot g_7^3 \rangle$ . Then  $g_{11} \cdot g_7^2 \cdot P_3 \cdot R_1 = R_3 \cdot (g_6^2 \cdot P_3 - g_9 \cdot g_7^2 \cdot P_1)$ .
- (61) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10}$  be elements of  $\text{GF}(p)$ ,  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ ). Suppose that  $g_4 = 2 \pmod p$  and  $g_5 = 3 \pmod p$  and  $g_{11} = 4 \pmod p$  and  $g_9 = 8 \pmod p$  and  $g_6 = z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2$  and  $g_7 = P_2 \cdot P_3$  and  $g_8 = P_1 \cdot P_2 \cdot g_7$  and  $g_{10} = g_6^2 - g_9 \cdot g_8$  and  $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_2)^2 \cdot g_7^2, g_9 \cdot g_7^3 \rangle$ . Then  $g_{11} \cdot g_7^2 \cdot (P_3)^2 \cdot (z_2 \cdot R_3) = R_3 \cdot (g_4 \cdot g_7 \cdot P_2 - g_6 \cdot P_1)^2 - g_{11} \cdot g_7^2 \cdot (P_1)^2 \cdot R_1$ .
- (62) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10}$  be elements of  $\text{GF}(p)$ ,  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ ). Suppose that  $g_4 = 2 \pmod p$  and  $g_5 = 3 \pmod p$  and  $g_{11} = 4 \pmod p$  and  $g_9 = 8 \pmod p$  and  $g_6 = z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2$  and  $g_7 = P_2 \cdot P_3$  and  $g_8 = P_1 \cdot P_2 \cdot g_7$  and  $g_{10} = g_6^2 - g_9 \cdot g_8$  and  $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_2)^2 \cdot g_7^2, g_9 \cdot g_7^3 \rangle$ . Then  $g_4 \cdot g_7^2 \cdot (P_3)^2 \cdot (z_1 \cdot R_3) = g_6 \cdot P_3 \cdot R_3 \cdot (g_4 \cdot g_7 \cdot P_2 - g_6 \cdot P_1) + g_7^2 \cdot (g_{11} \cdot P_1 \cdot P_3 \cdot R_1 + g_4 \cdot (P_1)^2 \cdot R_3)$ .
- (63) Let  $p$  be a 5 or greater prime number,  $z$  be an element of the parameters of elliptic curve  $p$ ,  $g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10}$  be elements of  $\text{GF}(p)$ ,  $P$  be an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and  $R$  be an element of (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ )  $\times$  (the carrier of  $\text{GF}(p)$ ). Suppose that  $g_4 = 2 \pmod p$  and  $g_5 = 3 \pmod p$  and  $g_{11} = 4 \pmod p$  and  $g_9 = 8 \pmod p$  and  $g_6 = z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2$  and  $g_7 = P_2 \cdot P_3$  and  $g_8 = P_1 \cdot P_2 \cdot g_7$  and  $g_{10} = g_6^2 - g_9 \cdot g_8$  and  $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_2)^2 \cdot g_7^2, g_9 \cdot g_7^3 \rangle$ . Then  $g_{11} \cdot g_7^2 \cdot (P_3)^2 \cdot ((R_2)^2 \cdot R_3 - ((R_1)^3 + z_1 \cdot R_1 \cdot (R_3)^2 + z_2 \cdot (R_3)^3)) = 0_{\text{GF}(p)}$ .

Let  $p$  be a 5 or greater prime number and let  $z$  be an element of the parameters of elliptic curve  $p$ . The functor  $\text{addell}_{\text{ProjCo}}(z, p)$  yields a function from  $\text{EC}_{\text{SetProjCo}}(z_1) \times \text{EC}_{\text{SetProjCo}}(z_1)$  into  $\text{EC}_{\text{SetProjCo}}(z_1)$  and is defined by the condition (Def. 9).

(Def. 9) Let  $P, Q, O$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$  such that  $O = \langle 0, 1, 0 \rangle$ .

Then

- (i) if  $P \equiv O$ , then  $(\text{addell}_{\text{ProjCo}}(z, p))(P, Q) = Q$ ,
- (ii) if  $Q \equiv O$  and  $P \not\equiv O$ , then  $(\text{addell}_{\text{ProjCo}}(z, p))(P, Q) = P$ ,



- (iii) if  $P \neq O$  and  $Q \neq O$  and  $P \neq Q$ , then for all elements  $g_4, g_6, g_7, g_8$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  and  $g_6 = Q_2 \cdot P_3 - P_2 \cdot Q_3$  and  $g_7 = Q_1 \cdot P_3 - P_1 \cdot Q_3$  and  $g_8 = g_6^2 \cdot P_3 \cdot Q_3 - g_7^3 - g_4 \cdot g_7^2 \cdot P_1 \cdot Q_3$  holds  $(\text{addell}_{\text{ProjCo}}(z, p))(P, Q) = \langle g_7 \cdot g_8, g_6 \cdot (g_7^2 \cdot P_1 \cdot Q_3 - g_8) - g_7^3 \cdot P_2 \cdot Q_3, g_7^3 \cdot P_3 \cdot Q_3 \rangle$ , and
- (iv) if  $P \neq O$  and  $Q \neq O$  and  $P \equiv Q$ , then for all elements  $g_4, g_5, g_{11}, g_9, g_6, g_7, g_8, g_{10}$  of  $\text{GF}(p)$  such that  $g_4 = 2 \pmod p$  and  $g_5 = 3 \pmod p$  and  $g_{11} = 4 \pmod p$  and  $g_9 = 8 \pmod p$  and  $g_6 = z_1 \cdot (P_3)^2 + g_5 \cdot (P_1)^2$  and  $g_7 = P_2 \cdot P_3$  and  $g_8 = P_1 \cdot P_2 \cdot g_7$  and  $g_{10} = g_6^2 - g_9 \cdot g_8$  holds  $(\text{addell}_{\text{ProjCo}}(z, p))(P, Q) = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_2)^2 \cdot g_7^2, g_9 \cdot g_7^3 \rangle$ .

Let  $p$  be a 5 or greater prime number, let  $z$  be an element of the parameters of elliptic curve  $p$ , let  $F$  be a function from  $\text{EC}_{\text{SetProjCo}}(z_1) \times \text{EC}_{\text{SetProjCo}}(z_1)$  into  $\text{EC}_{\text{SetProjCo}}(z_1)$ , and let  $Q, R$  be elements of  $\text{EC}_{\text{SetProjCo}}(z_1)$ . Then  $F(Q, R)$  is an element of  $\text{EC}_{\text{SetProjCo}}(z_1)$ .

## REFERENCES

- [1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(1):91–96, 1990.
- [2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(1):175–180, 1990.
- [3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [5] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [6] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Set of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 19(3):131–138, 2011, doi: 10.2478/v10037-011-0021-6.
- [7] G. Seroussi I. Blake and N. Smart. *Elliptic Curves in Cryptography*. Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.
- [8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [9] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(5):887–890, 1990.
- [10] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(5):829–832, 1990.
- [11] Christoph Schwarzweiler. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(3):559–564, 2001.
- [12] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(1):115–122, 1990.
- [13] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(1):97–105, 1990.
- [14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [15] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(5):821–827, 1990.
- [16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.

Received November 3, 2011