FORMALIZED MATHEMATICS
Vol. 20, No. 1, Pages 87–95, 2012
DOI: 10.2478/v10037-012-0012-2

VERSITA
versita.com/fm/

Operations of Points on Elliptic Curve in Projective Coordinates

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki[1]
Shinshu University
Nagano, Japan

Daichi Mizushima
Shinshu University
Nagano, Japan

Yasunari Shidama[2]
Shinshu University
Nagano, Japan

Summary. In this article, we formalize operations of points on an elliptic curve over **GF(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: $\texttt{compell}_{\texttt{ProjCo}}$ and $\texttt{addell}_{\texttt{ProjCo}}$ 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 GF(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) $(1_K)^{-1} = 1_K$.

[1] This work was supported by JSPS KAKENHI 21240001.
[2] This work was supported by JSPS KAKENHI 22300285.

© 2012 University of Białystok
CC-BY-SA License ver. 3.0 or later
ISSN 1426–2630(p), 1898-9934(e)

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

(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 GF(p) such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $g_3 = (i + j) \bmod p$ holds $g_1 \cdot a + g_2 \cdot a = g_3 \cdot a$.

(19) For all elements g_1, g_2, a of GF(p) such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $j = i + 1$ holds $g_1 \cdot a + a = g_2 \cdot a$.

(20) For all elements g_4, a of GF(p) such that $g_4 = 2 \bmod p$ holds $a + a = g_4 \cdot a$.

(21) For all elements g_1, g_2, g_3, a of GF(p) such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $g_3 = (i - j) \bmod p$ holds $g_1 \cdot a - g_2 \cdot a = g_3 \cdot a$.

(22) For all elements g_1, g_2, a of GF(p) such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $i = j + 1$ holds $g_1 \cdot a - g_2 \cdot a = a$.

(23) For all elements g_1, g_2, a of GF(p) such that $g_1 = i \bmod p$ and $g_2 = j \bmod p$ and $i = j + 1$ holds $g_1 \cdot a - a = g_2 \cdot a$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

(24) For all elements g_4, a of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $g_4 \cdot a - a = a$.

(25) For all elements g_4, a, b of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ holds $(a+b)^2 = a^2 + g_4 \cdot a \cdot b + b^2$.

(26) For all elements g_4, a, b of $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ 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 $\mathrm{GF}(p)$ such that $g_4 = 2 \bmod p$ 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 $\mathrm{GF}(p)$. If $p > 2$ and $g_4 = 2 \bmod p$, then $g_4 \neq 0_{\mathrm{GF}(p)}$ and ${g_4}^n \neq 0_{\mathrm{GF}(p)}$.

(29) Let p be a prime number, n be a natural number, and g_4, g_5 be elements of $\mathrm{GF}(p)$. If $p > 3$ and $g_5 = 3 \bmod p$, then $g_5 \neq 0_{\mathrm{GF}(p)}$ and ${g_5}^n \neq 0_{\mathrm{GF}(p)}$.

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 (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) is defined as follows:

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

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 $z_{\mathbf{1}}$ is an element of $\mathrm{GF}(p)$. Then $z_{\mathbf{2}}$ is an element of $\mathrm{GF}(p)$.

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 $\mathrm{Disc}(z_{\mathbf{1}}) \neq 0_{\mathrm{GF}(p)}$.

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

Let p be a prime number, let a, b be elements of $\mathrm{GF}(p)$, and let P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$. The functor $P_{\mathbf{1}}$ yields an element of $\mathrm{GF}(p)$ and is defined as follows:

(Def. 3) If $P = \langle p_1, p_2, p_3\rangle$, then $P_{\mathbf{1}} = p_1$.

The functor $P_{\mathbf{2}}$ yielding an element of $\mathrm{GF}(p)$ is defined as follows:

(Def. 4) If $P = \langle p_1, p_2, p_3\rangle$, then $P_{\mathbf{2}} = p_2$.

The functor $P_{\mathbf{3}}$ yielding an element of $\mathrm{GF}(p)$ is defined by:

(Def. 5) If $P = \langle p_1, p_2, p_3\rangle$, then $P_{\mathbf{3}} = p_3$.

We now state three propositions:

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

(31) For every prime number p and for all elements a, b of $\mathrm{GF}(p)$ and for every element P of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$ holds $P = \langle P_{\mathbf{1}}, P_{\mathbf{2}}, P_{\mathbf{3}} \rangle$.

(32) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$, and Q be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. Then $P = Q$ if and only if the following conditions are satisfied:

(i) $P_{\mathbf{1}} = Q_{\mathbf{1}}$,

(ii) $P_{\mathbf{2}} = Q_{\mathbf{2}}$, and

(iii) $P_{\mathbf{3}} = Q_{\mathbf{3}}$.

(33) Let p be a prime number, a, b, P_1, P_2, P_3 be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$. If $P = \langle P_1, P_2, P_3 \rangle$, then $P_{\mathbf{1}} = P_1$ and $P_{\mathbf{2}} = P_2$ and $P_{\mathbf{3}} = P_3$.

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

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

The following two propositions are true:

(34) P is on curve defined by an equation $\mathrm{EC}_{\mathrm{WEqProjCo}}(a)$ iff P is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$.

(35) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(a)$. Then $(P_{\mathbf{2}})^2 \cdot P_{\mathbf{3}} - ((P_{\mathbf{1}})^3 + a \cdot P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + b \cdot (P_{\mathbf{3}})^3) = 0_{\mathrm{GF}(p)}$.

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

(Def. 7)(i) The represent point of $P = \langle P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^{-1}, P_{\mathbf{2}} \cdot (P_{\mathbf{3}})^{-1}, 1 \rangle$ if $P_{\mathbf{3}} \neq 0$,

(ii) the represent point of $P = \langle 0, 1, 0 \rangle$ if $P_{\mathbf{3}} = 0$,

(iii) $P_{\mathbf{3}} = 0$, 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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then the represent point of $P \equiv P$ and the represent point of $P \in \mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$.

(37) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. Suppose (the represent point of $P)_{\mathbf{3}} = 0$. Then the represent point of $P = \langle 0, 1, 0 \rangle$ and $P_{\mathbf{3}} = 0$.

(38) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and P be an element of $\mathrm{ProjCo}(\mathrm{GF}(p))$. Suppose (the represent point of $P)_{\mathbf{3}} \neq 0$. Then the represent point of $P = \langle P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^{-1}, P_{\mathbf{2}} \cdot (P_{\mathbf{3}})^{-1}, 1 \rangle$ and $P_{\mathbf{3}} \neq 0$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P \equiv Q$ if and only if the represent point of $P =$ the represent point of Q.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

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 $\mathrm{compell}_{\mathrm{ProjCo}}(z, p)$ yields a function from $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ and is defined as follows:

(Def. 8) For every element P of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ holds $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) = \langle P_{\mathbf{1}}, -P_{\mathbf{2}}, P_{\mathbf{3}} \rangle$.

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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and let P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $F(P)$ is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$.

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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $O = \langle 0, 1, 0 \rangle$, then $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(O) \equiv O$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))((\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)) = P$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Suppose $P_{\mathbf{3}} \neq 0$. Then the represent point of $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))$(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P = Q$ if and only if $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P_{\mathbf{3}} \neq 0$, then $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)$ iff $P_{\mathbf{2}} = 0$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P_{\mathbf{3}} \neq 0$, then $P_{\mathbf{1}} = Q_{\mathbf{1}}$ and $P_{\mathbf{3}} = Q_{\mathbf{3}}$ iff $P = Q$ or $P = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P \equiv Q$ if and only if $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$ if and only if $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P) \equiv Q$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Suppose $P_{\mathbf{3}} \neq 0$ and $Q_{\mathbf{3}} \neq 0$. Then the represent point of $P = (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))$(the

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

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

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P \equiv Q$, then $P_{\mathbf{2}} \cdot Q_{\mathbf{3}} = Q_{\mathbf{2}} \cdot P_{\mathbf{3}}$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Suppose $P_{\mathbf{3}} \neq 0$ and $Q_{\mathbf{3}} \neq 0$. Then $P \equiv Q$ or $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$ if and only if $P_{\mathbf{1}} \cdot Q_{\mathbf{3}} = Q_{\mathbf{1}} \cdot P_{\mathbf{3}}$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P_{\mathbf{3}} \neq 0$ and $Q_{\mathbf{3}} \neq 0$ and $P_{\mathbf{2}} \neq 0$, then if $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$, then $P_{\mathbf{2}} \cdot Q_{\mathbf{3}} \neq Q_{\mathbf{2}} \cdot P_{\mathbf{3}}$.

(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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $P \not\equiv Q$ and $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(Q)$, then $P_{\mathbf{2}} \cdot Q_{\mathbf{3}} \neq Q_{\mathbf{2}} \cdot P_{\mathbf{3}}$.

(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 $\mathrm{GF}(p)$, and P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. If $g_5 = 3 \bmod p$ and $P_{\mathbf{2}} = 0$ and $P_{\mathbf{3}} \neq 0$, then $z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2 \neq 0$.

(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 $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8, g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}}, {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}}\rangle$.

Then $g_7 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{2}} = -(g_6 \cdot (R_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot R_{\mathbf{3}}) + g_7 \cdot P_{\mathbf{2}} \cdot R_{\mathbf{3}})$.

(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 $\mathrm{GF}(p)$, P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8, g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}}, {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}}\rangle$.

Then $-{g_7}^2 \cdot (P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{1}} + P_{\mathbf{3}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{3}} + P_{\mathbf{1}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}}) + P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} \cdot {g_6}^2 = 0_{\mathrm{GF}(p)}$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

(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 GF(p), P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of GF(p)) $\times$ (the carrier of GF(p)) $\times$ (the carrier of GF(p)). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8, g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}}, {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then $z_{\mathbf{2}} \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} = -{g_7}^2 \cdot P_{\mathbf{3}} \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{1}} + (g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}})^2 \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}}$.

(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 GF(p), P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of GF(p)) $\times$ (the carrier of GF(p)) $\times$ (the carrier of GF(p)). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8, g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}}, {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then $z_{\mathbf{1}} \cdot {g_7}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} = {g_7}^2 \cdot (P_{\mathbf{1}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{3}} + P_{\mathbf{3}} \cdot Q_{\mathbf{1}} \cdot R_{\mathbf{1}} + P_{\mathbf{1}} \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{1}}) + g_4 \cdot g_6 \cdot Q_{\mathbf{3}} \cdot R_{\mathbf{3}} \cdot (g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}})$.

(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 GF(p), P, Q be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of GF(p)) $\times$ (the carrier of GF(p)) $\times$ (the carrier of GF(p)). Suppose that

(i) $g_4 = 2 \bmod p$,

(ii) $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$,

(iii) $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$,

(iv) $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$, and

(v) $R = \langle g_7 \cdot g_8, g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}}, {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$.

Then ${g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot Q_{\mathbf{3}} \cdot ((R_{\mathbf{2}})^2 \cdot R_{\mathbf{3}} - ((R_{\mathbf{1}})^3 + z_{\mathbf{1}} \cdot R_{\mathbf{1}} \cdot (R_{\mathbf{3}})^2 + z_{\mathbf{2}} \cdot (R_{\mathbf{3}})^3)) = 0_{\mathrm{GF}(p)}$.

(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 GF(p), P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of GF(p)) $\times$ (the carrier of GF(p)) $\times$ (the carrier of GF(p)). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2, g_9 \cdot {g_7}^3 \rangle$. Then $g_4 \cdot g_7 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{2}} = -(g_6 \cdot (P_{\mathbf{3}} \cdot R_{\mathbf{1}} - P_{\mathbf{1}} \cdot R_{\mathbf{3}}) + g_4 \cdot g_7 \cdot P_{\mathbf{2}} \cdot R_{\mathbf{3}})$.

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

(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 $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2, g_9 \cdot {g_7}^3\rangle$. Then $g_{11} \cdot {g_7}^2 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{1}} = R_{\mathbf{3}} \cdot ({g_6}^2 \cdot P_{\mathbf{3}} - g_9 \cdot {g_7}^2 \cdot P_{\mathbf{1}})$.

(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 $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2, g_9 \cdot {g_7}^3\rangle$. Then $g_{11} \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot (z_{\mathbf{2}} \cdot R_{\mathbf{3}}) = R_{\mathbf{3}} \cdot (g_4 \cdot g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}})^2 - g_{11} \cdot {g_7}^2 \cdot (P_{\mathbf{1}})^2 \cdot R_{\mathbf{1}}$.

(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 $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2, g_9 \cdot {g_7}^3\rangle$. Then $g_4 \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot (z_{\mathbf{1}} \cdot R_{\mathbf{3}}) = g_6 \cdot P_{\mathbf{3}} \cdot R_{\mathbf{3}} \cdot (g_4 \cdot g_7 \cdot P_{\mathbf{2}} - g_6 \cdot P_{\mathbf{1}}) + {g_7}^2 \cdot (g_{11} \cdot P_{\mathbf{1}} \cdot P_{\mathbf{3}} \cdot R_{\mathbf{1}} + g_4 \cdot (P_{\mathbf{1}})^2 \cdot R_{\mathbf{3}})$.

(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 $\mathrm{GF}(p)$, P be an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and R be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Suppose that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ and $R = \langle g_4 \cdot g_{10} \cdot g_7, g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2, g_9 \cdot {g_7}^3\rangle$. Then $g_{11} \cdot {g_7}^2 \cdot (P_{\mathbf{3}})^2 \cdot ((R_{\mathbf{2}})^2 \cdot R_{\mathbf{3}} - ((R_{\mathbf{1}})^3 + z_{\mathbf{1}} \cdot R_{\mathbf{1}} \cdot (R_{\mathbf{3}})^2 + z_{\mathbf{2}} \cdot (R_{\mathbf{3}})^3)) = 0_{\mathrm{GF}(p)}$.

Let p be a 5 or greater prime number and let z be an element of the parameters of elliptic curve p. The functor $\mathrm{addell}_{\mathrm{ProjCo}}(z, p)$ yields a function from $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}}) \times \mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ and is defined by the condition (Def. 9).

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

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

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM

(iii) if $P \not\equiv O$ and $Q \not\equiv O$ and $P \not\equiv Q$, then for all elements g_4, g_6, g_7, g_8 of GF(p) such that $g_4 = 2 \bmod p$ and $g_6 = Q_{\mathbf{2}} \cdot P_{\mathbf{3}} - P_{\mathbf{2}} \cdot Q_{\mathbf{3}}$ and $g_7 = Q_{\mathbf{1}} \cdot P_{\mathbf{3}} - P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$ and $g_8 = {g_6}^2 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} - {g_7}^3 - g_4 \cdot {g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}}$ holds $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q) = \langle g_7 \cdot g_8,\ g_6 \cdot ({g_7}^2 \cdot P_{\mathbf{1}} \cdot Q_{\mathbf{3}} - g_8) - {g_7}^3 \cdot P_{\mathbf{2}} \cdot Q_{\mathbf{3}},\ {g_7}^3 \cdot P_{\mathbf{3}} \cdot Q_{\mathbf{3}} \rangle$, and

(iv) if $P \not\equiv O$ and $Q \not\equiv O$ 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 GF(p) such that $g_4 = 2 \bmod p$ and $g_5 = 3 \bmod p$ and $g_{11} = 4 \bmod p$ and $g_9 = 8 \bmod p$ and $g_6 = z_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + g_5 \cdot (P_{\mathbf{1}})^2$ and $g_7 = P_{\mathbf{2}} \cdot P_{\mathbf{3}}$ and $g_8 = P_{\mathbf{1}} \cdot P_{\mathbf{2}} \cdot g_7$ and $g_{10} = {g_6}^2 - g_9 \cdot g_8$ holds $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q) = \langle g_4 \cdot g_{10} \cdot g_7,\ g_6 \cdot (g_{11} \cdot g_8 - g_{10}) - g_9 \cdot (P_{\mathbf{2}})^2 \cdot {g_7}^2,\ g_9 \cdot {g_7}^3 \rangle$.

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 $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}}) \times \mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$ into $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$, and let Q, R be elements of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$. Then $F(Q,R)$ is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}(z_{\mathbf{1}})$.

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 Schwarzweller. 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

Brought to you by | Biblioteka Uniwersytecka w Bialymstoku
Authenticated
Download Date | 12/8/15 12:24 PM