FORMALIZED MATHEMATICS
Vol. **19**, No. **3**, Pages 131–138, **2011**
DOI: 10.2478/v10037-011-0021-6

Set of Points on Elliptic Curve in Projective Coordinates[1]

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize a set of points on an elliptic curve over **GF**(**p**). Elliptic curve cryptography [10], whose security is based on a difficulty of discrete logarithm problem of elliptic curves, is important for information security.

MML identifier: `EC_PF_1`, version: `7.11.07 4.160.1126`

The notation and terminology used here have been introduced in the following papers: [15], [1], [16], [13], [3], [8], [5], [6], [19], [18], [14], [17], [2], [12], [4], [9], [22], [23], [20], [21], [11], and [7].

1. Finite Prime Field GF(p)

For simplicity, we use the following convention: x is a set, i, j are integers, n, n_1, n_2 are natural numbers, and K, K_1, K_2 are fields.

Let K be a field. A field is called a subfield of K if it satisfies the conditions (Def. 1).

(Def. 1)(i) The carrier of it $\subseteq$ the carrier of K,
(ii) the addition of it $=$ (the addition of K) $\restriction$ (the carrier of it),
(iii) the multiplication of it $=$ (the multiplication of K) $\restriction$ (the carrier of it),
(iv) $1_{\mathrm{it}} = 1_K$, and
(v) $0_{\mathrm{it}} = 0_K$.

We now state two propositions:

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

ISSN 1426–2630(p), 1898-9934(e)

(1) K is a subfield of K.

(2) Let S_1 be a non empty double loop structure. Suppose that

(i) the carrier of S_1 is a subset of the carrier of K,

(ii) the addition of $S_1 =$ (the addition of K) $\restriction$ (the carrier of S_1),

(iii) the multiplication of $S_1 =$ (the multiplication of K) $\restriction$ (the carrier of S_1),

(iv) $1_{(S_1)} = 1_K$,

(v) $0_{(S_1)} = 0_K$, and

(vi) S_1 is right complementable, commutative, almost left invertible, and non degenerated.

Then S_1 is a subfield of K.

Let K be a field. One can check that there exists a subfield of K which is strict.

In the sequel S_2, S_3 denote subfields of K and e_1, e_2 denote elements of K.

We now state several propositions:

(3) If K_1 is a subfield of K_2, then for every x such that $x \in K_1$ holds $x \in K_2$.

(4) For all strict fields K_1, K_2 such that K_1 is a subfield of K_2 and K_2 is a subfield of K_1 holds $K_1 = K_2$.

(5) Let K_1, K_2, K_3 be strict fields. Suppose K_1 is a subfield of K_2 and K_2 is a subfield of K_3. Then K_1 is a subfield of K_3.

(6) S_2 is a subfield of S_3 iff the carrier of $S_2 \subseteq$ the carrier of S_3.

(7) S_2 is a subfield of S_3 iff for every x such that $x \in S_2$ holds $x \in S_3$.

(8) For all strict subfields S_2, S_3 of K holds $S_2 = S_3$ iff the carrier of $S_2 =$ the carrier of S_3.

(9) For all strict subfields S_2, S_3 of K holds $S_2 = S_3$ iff for every x holds $x \in S_2$ iff $x \in S_3$.

Let K be a finite field. Observe that there exists a subfield of K which is finite. Then $\overline{\overline{K}}$ is an element of $\mathbb{N}$.

Let us mention that there exists a field which is strict and finite.

Next we state the proposition

(10) For every strict finite field K and for every strict subfield S_2 of K such that $\overline{\overline{K}} = \overline{\overline{S_2}}$ holds $S_2 = K$.

Let I_1 be a field. We say that I_1 is prime if and only if:

(Def. 2) If K_1 is a strict subfield of I_1, then $K_1 = I_1$.

Let p be a prime number. We introduce $\mathrm{GF}(p)$ as a synonym of $\mathbb{Z}_p^{\mathrm{R}}$. One can check that $\mathrm{GF}(p)$ is finite. One can check that $\mathrm{GF}(p)$ is prime.

One can check that there exists a field which is prime.

2. Arithmetic in GF(p)

In the sequel b, c denote elements of $\mathrm{GF}(p)$ and F denotes a finite sequence of elements of $\mathrm{GF}(p)$.

Next we state a number of propositions:

(11) $0 = 0_{\mathrm{GF}(p)}$.

(12) $1 = 1_{\mathrm{GF}(p)}$.

(13) There exists n_1 such that $a = n_1 \bmod p$.

(14) There exists a such that $a = i \bmod p$.

(15) If $a = i \bmod p$ and $b = j \bmod p$, then $a + b = (i + j) \bmod p$.

(16) If $a = i \bmod p$, then $-a = (p - i) \bmod p$.

(17) If $a = i \bmod p$ and $b = j \bmod p$, then $a - b = (i - j) \bmod p$.

(18) If $a = i \bmod p$ and $b = j \bmod p$, then $a \cdot b = i \cdot j \bmod p$.

(19) If $a = i \bmod p$ and $i \cdot j \bmod p = 1$, then $a^{-1} = j \bmod p$.

(20) $a = 0$ or $b = 0$ iff $a \cdot b = 0$.

(21) $a^0 = \mathbf{1}_{\mathrm{GF}(p)}$ and $a^0 = 1$.

(22) $a^2 = a \cdot a$.

(23) If $a = n_1 \bmod p$, then $a^n = {n_1}^n \bmod p$.

(24) $a^{n+1} = a^n \cdot a$.

(25) If $a \neq 0$, then $a^n \neq 0$.

(26) Let F be an Abelian add-associative right zeroed right complementable associative commutative well unital almost left invertible distributive non empty double loop structure and x, y be elements of F. Then $x \cdot x = y \cdot y$ if and only if $x = y$ or $x = -y$.

(27) For every prime number p and for every element x of $\mathrm{GF}(p)$ such that $2 < p$ and $x + x = 0_{\mathrm{GF}(p)}$ holds $x = 0_{\mathrm{GF}(p)}$.

(28) $a^n \cdot b^n = (a \cdot b)^n$.

(29) If $a \neq 0$, then $(a^{-1})^n = (a^n)^{-1}$.

(30) $a^{n_1} \cdot a^{n_2} = a^{n_1+n_2}$.

(31) $(a^{n_1})^{n_2} = a^{n_1 \cdot n_2}$.

Let us consider p. One can verify that $\mathrm{MultGroup}(\mathrm{GF}(p))$ is cyclic.

The following two propositions are true:

(32) Let x be an element of $\mathrm{MultGroup}(\mathrm{GF}(p))$, x_1 be an element of $\mathrm{GF}(p)$, and n be a natural number. If $x = x_1$, then $x^n = {x_1}^n$.

(33) There exists an element g of $\mathrm{GF}(p)$ such that for every element a of $\mathrm{GF}(p)$ if $a \neq 0_{\mathrm{GF}(p)}$, then there exists a natural number n such that $a = g^n$.

3. Relation between Legendre Symbol and the Number of Roots in GF(p)

Let us consider p, a. We say that a is quadratic residue if and only if:

(Def. 3) $a \neq 0$ and there exists an element x of $\mathrm{GF}(p)$ such that $x^2 = a$.

We say that a is not quadratic residue if and only if:

(Def. 4) $a \neq 0$ and it is not true that there exists an element x of $\mathrm{GF}(p)$ such that $x^2 = a$.

One can prove the following proposition

(34) If $a \neq 0$, then a^2 is quadratic residue.

Let p be a prime number. Observe that $1_{\mathrm{GF}(p)}$ is quadratic residue.

Let us consider p, a. The functor $\mathrm{Lege}_p\, a$ yields an integer and is defined as follows:

(Def. 5) $\mathrm{Lege}_p\, a = \begin{cases} 0, & \text{if } a = 0, \\ 1, & \text{if } a \text{ is quadratic residue}, \\ -1, & \text{otherwise}. \end{cases}$

Next we state several propositions:

(35) a is not quadratic residue iff $\mathrm{Lege}_p\, a = -1$.

(36) a is quadratic residue iff $\mathrm{Lege}_p\, a = 1$.

(37) $a = 0$ iff $\mathrm{Lege}_p\, a = 0$.

(38) If $a \neq 0$, then $\mathrm{Lege}_p(a^2) = 1$.

(39) $\mathrm{Lege}_p(a \cdot b) = \mathrm{Lege}_p\, a \cdot \mathrm{Lege}_p\, b$.

(40) If $a \neq 0$ and $n \bmod 2 = 0$, then $\mathrm{Lege}_p(a^n) = 1$.

(41) If $n \bmod 2 = 1$, then $\mathrm{Lege}_p(a^n) = \mathrm{Lege}_p\, a$.

(42) If $2 < p$, then $\overline{\overline{\{b : b^2 = a\}}} = 1 + \mathrm{Lege}_p\, a$.

4. Set of Points on an Elliptic Curve over GF(p)

Let K be a field. The functor $\mathrm{ProjCo}\, K$ yields a non empty subset of (the carrier of K) $\times$ (the carrier of K) $\times$ (the carrier of K) and is defined by:

(Def. 6) $\mathrm{ProjCo}\, K = $ ((the carrier of K) $\times$ (the carrier of K) $\times$ (the carrier of K)) $\setminus \{\langle 0_K, 0_K, 0_K \rangle\}$.

One can prove the following proposition

(43) $\mathrm{ProjCo}\, \mathrm{GF}(p) = $ ((the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$)) $\setminus \{\langle 0, 0, 0 \rangle\}$.

In the sequel P_1, P_2, P_3 are elements of $\mathrm{GF}(p)$.

Let p be a prime number and let a, b be elements of $\mathrm{GF}(p)$. The functor $\mathrm{Disc}(a, b, p)$ yields an element of $\mathrm{GF}(p)$ and is defined as follows:

(Def. 7) For all elements g_4, g_{27} of $\mathrm{GF}(p)$ such that $g_4 = 4 \bmod p$ and $g_{27} = 27 \bmod p$ holds $\mathrm{Disc}(a, b, p) = g_4 \cdot a^3 + g_{27} \cdot b^2$.

Let p be a prime number and let a, b be elements of $\mathrm{GF}(p)$. The functor EC WEqProjCo(a, b, p) yielding a function from (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) into $\mathrm{GF}(p)$ is defined by the condition (Def. 8).

(Def. 8) Let P be an element of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$). Then (EC WEqProjCo(a, b, p))$(P) = (P_{\mathbf{2}})^2 \cdot P_{\mathbf{3}} - ((P_{\mathbf{1}})^3 + a \cdot P_{\mathbf{1}} \cdot (P_{\mathbf{3}})^2 + b \cdot (P_{\mathbf{3}})^3)$.

We now state the proposition

(44) For all elements X, Y, Z of $\mathrm{GF}(p)$ holds (EC WEqProjCo(a, b, p))$(\langle X, Y, Z\rangle) = Y^2 \cdot Z - (X^3 + a \cdot X \cdot Z^2 + b \cdot Z^3)$.

Let p be a prime number and let a, b be elements of $\mathrm{GF}(p)$. The functor EC SetProjCo(a, b, p) yielding a non empty subset of ProjCo $\mathrm{GF}(p)$ is defined by:

(Def. 9) EC SetProjCo$(a, b, p) = \{P \in$ ProjCo $\mathrm{GF}(p)$: (EC WEqProjCo(a, b, p)) $(P) = 0_{\mathrm{GF}(p)}\}$.

One can prove the following two propositions:

(45) $\langle 0, 1, 0\rangle$ is an element of EC SetProjCo(a, b, p).

(46) Let p be a prime number and a, b, X, Y be elements of $\mathrm{GF}(p)$. Then $Y^2 = X^3 + a \cdot X + b$ if and only if $\langle X, Y, 1\rangle$ is an element of EC SetProjCo(a, b, p).

Let p be a prime number and let P, Q be elements of ProjCo $\mathrm{GF}(p)$. We say that P EQ Q if and only if:

(Def. 10) There exists an element a of $\mathrm{GF}(p)$ such that $a \neq 0_{\mathrm{GF}(p)}$ and $P_{\mathbf{1}} = a \cdot Q_{\mathbf{1}}$ and $P_{\mathbf{2}} = a \cdot Q_{\mathbf{2}}$ and $P_{\mathbf{3}} = a \cdot Q_{\mathbf{3}}$.

Let us notice that the predicate P EQ Q is reflexive and symmetric.

We now state two propositions:

(47) For every prime number p and for all elements P, Q, R of ProjCo $\mathrm{GF}(p)$ such that P EQ Q and Q EQ R holds P EQ R.

(48) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, P, Q be elements of (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$) $\times$ (the carrier of $\mathrm{GF}(p)$), and d be an element of $\mathrm{GF}(p)$. Suppose $p > 3$ and $\mathrm{Disc}(a, b, p) \neq 0_{\mathrm{GF}(p)}$ and $P \in$ EC SetProjCo(a, b, p) and $d \neq 0_{\mathrm{GF}(p)}$ and $Q_{\mathbf{1}} = d \cdot P_{\mathbf{1}}$ and $Q_{\mathbf{2}} = d \cdot P_{\mathbf{2}}$ and $Q_{\mathbf{3}} = d \cdot P_{\mathbf{3}}$. Then $Q \in$ EC SetProjCo(a, b, p).

Let p be a prime number. The functor $\mathbb{R}$-ProjCo p yielding a binary relation on ProjCo $\mathrm{GF}(p)$ is defined by:

(Def. 11) $\mathbb{R}$-ProjCo $p = \{\langle P, Q\rangle; P$ ranges over elements of ProjCo $\mathrm{GF}(p), Q$ ranges over elements of ProjCo $\mathrm{GF}(p)$: P EQ $Q\}$.

One can prove the following proposition

(49) For every prime number p and for all elements P, Q of ProjCo GF(p) holds P EQ Q iff $\langle P, Q\rangle \in \mathbb{R}$-ProjCo p.

Let p be a prime number. Note that $\mathbb{R}$-ProjCo p is total, symmetric, and transitive.

Let p be a prime number and let a, b be elements of GF(p). The functor $\mathbb{R}$-EllCur(a,b,p) yielding an equivalence relation of EC SetProjCo(a,b,p) is defined as follows:

(Def. 12) $\mathbb{R}\text{-EllCur}(a,b,p) = \mathbb{R}\text{-ProjCo}\, p \cap \nabla_{\text{EC SetProjCo}(a,b,p)}$.

Next we state a number of propositions:

(50) Let p be a prime number, a, b be elements of GF(p), and P, Q be elements of ProjCo GF(p). Suppose $\text{Disc}(a,b,p) \neq 0_{\text{GF}(p)}$ and P, $Q \in$ EC SetProjCo(a,b,p). Then P EQ Q if and only if $\langle P, Q\rangle \in \mathbb{R}$-EllCur$(a,b,p)$.

(51) Let p be a prime number, a, b be elements of GF(p), and P be an element of ProjCo GF(p). Suppose $p > 3$ and $\text{Disc}(a,b,p) \neq 0_{\text{GF}(p)}$ and $P \in$ EC SetProjCo(a,b,p) and $P_{\mathbf{3}} \neq 0$. Then there exists an element Q of ProjCo GF(p) such that $Q \in$ EC SetProjCo(a,b,p) and Q EQ P and $Q_{\mathbf{3}} = 1$.

(52) Let p be a prime number, a, b be elements of GF(p), and P be an element of ProjCo GF(p). Suppose $p > 3$ and $\text{Disc}(a,b,p) \neq 0_{\text{GF}(p)}$ and $P \in$ EC SetProjCo(a,b,p) and $P_{\mathbf{3}} = 0$. Then there exists an element Q of ProjCo GF(p) such that $Q \in$ EC SetProjCo(a,b,p) and Q EQ P and $Q_{\mathbf{1}} = 0$ and $Q_{\mathbf{2}} = 1$ and $Q_{\mathbf{3}} = 0$.

(53) Let p be a prime number, a, b be elements of GF(p), and x be a set. Suppose $p > 3$ and $\text{Disc}(a,b,p) \neq 0_{\text{GF}(p)}$ and $x \in$ Classes $\mathbb{R}$-EllCur(a,b,p). Then

(i) there exists an element P of ProjCo GF(p) such that $P \in$ EC SetProjCo(a,b,p) and $P = \langle 0, 1, 0\rangle$ and $x = [P]_{\mathbb{R}\text{-EllCur}(a,b,p)}$, or

(ii) there exists an element P of ProjCo GF(p) and there exist elements X, Y of GF(p) such that $P \in$ EC SetProjCo(a,b,p) and $P = \langle X, Y, 1\rangle$ and $x = [P]_{\mathbb{R}\text{-EllCur}(a,b,p)}$.

(54) Let p be a prime number and a, b be elements of GF(p). Suppose $p > 3$ and $\text{Disc}(a,b,p) \neq 0_{\text{GF}(p)}$. Then Classes $\mathbb{R}$-EllCur$(a,b,p) = \{[\langle 0, 1, 0\rangle]_{\mathbb{R}\text{-EllCur}(a,b,p)}\} \cup \{[P]_{\mathbb{R}\text{-EllCur}(a,b,p)}; P$ ranges over elements of ProjCo GF(p) : $P \in \text{EC SetProjCo}(a,b,p) \wedge \bigvee_{X,Y\,:\,\text{element of GF}(p)} P = \langle X, Y, 1\rangle\}$.

(55) Let p be a prime number and a, b, d_1, Y_1, d_2, Y_2 be elements of GF(p). Suppose $p > 3$ and $\text{Disc}(a,b,p) \neq 0_{\text{GF}(p)}$ and $\langle d_1, Y_1, 1\rangle$, $\langle d_2, Y_2, 1\rangle \in$ EC SetProjCo(a,b,p). Then $[\langle d_1, Y_1, 1\rangle]_{\mathbb{R}\text{-EllCur}(a,b,p)} = [\langle d_2, Y_2, 1\rangle]_{\mathbb{R}\text{-EllCur}(a,b,p)}$ if and only if $d_1 = d_2$ and $Y_1 = Y_2$.

(56) Let p be a prime number, a, b be elements of $\mathrm{GF}(p)$, and F_1, F_2 be sets. Suppose that

(i) $p > 3$,

(ii) $\mathrm{Disc}(a,b,p) \neq 0_{\mathrm{GF}(p)}$,

(iii) $F_1 = \{[\langle 0, 1, 0\rangle]_{\mathbb{R}\text{-EllCur}(a,b,p)}\}$, and

(iv) $F_2 = \{[P]_{\mathbb{R}\text{-EllCur}(a,b,p)}; P$ ranges over elements of $\mathrm{ProjCo}\,\mathrm{GF}(p)$: $P \in \mathrm{EC\ SetProjCo}(a,b,p) \ \wedge \ \bigvee_{X,Y\,:\,\text{element of } \mathrm{GF}(p)} \ P = \langle X, Y, 1\rangle\}$.

Then F_1 misses F_2.

(57) Let X be a non empty finite set, R be an equivalence relation of X, S be a $\mathrm{Classes}\,R$-valued function, and i be a set. If $i \in \mathrm{dom}\, S$, then $S(i)$ is a finite subset of X.

(58) Let X be a non empty set, R be an equivalence relation of X, and S be a $\mathrm{Classes}\,R$-valued function. If S is one-to-one, then S is disjoint valued.

(59) Let X be a non empty set, R be an equivalence relation of X, and S be a $\mathrm{Classes}\,R$-valued function. If S is onto, then $\bigcup S = X$.

(60) Let X be a non empty finite set, R be an equivalence relation of X, S be a $\mathrm{Classes}\,R$-valued function, and L be a finite sequence of elements of $\mathbb{N}$. Suppose S is one-to-one and onto and $\mathrm{dom}\, S = \mathrm{dom}\, L$ and for every natural number i such that $i \in \mathrm{dom}\, S$ holds $L(i) = \overline{\overline{S(i)}}$. Then $\overline{\overline{X}} = \sum L$.

(61) Let p be a prime number, a, b, d be elements of $\mathrm{GF}(p)$, and F, G be sets. Suppose that

(i) $p > 3$,

(ii) $\mathrm{Disc}(a,b,p) \neq 0_{\mathrm{GF}(p)}$,

(iii) $F = \{Y \in \mathrm{GF}(p)\colon Y^2 = d^3 + a \cdot d + b\}$,

(iv) $F \neq \emptyset$, and

(v) $G = \{[\langle d, Y, 1\rangle]_{\mathbb{R}\text{-EllCur}(a,b,p)}; Y$ ranges over elements of $\mathrm{GF}(p)$: $\langle d, Y, 1\rangle \in \mathrm{EC\ SetProjCo}(a,b,p)\}$.

Then there exists a function from F into G which is onto and one-to-one.

(62) Let p be a prime number and a, b, d be elements of $\mathrm{GF}(p)$. Suppose $p > 3$ and $\mathrm{Disc}(a,b,p) \neq 0_{\mathrm{GF}(p)}$.

Then $\overline{\overline{\{[\langle d, Y, 1\rangle]_{\mathbb{R}\text{-EllCur}(a,b,p)}; Y \text{ ranges over elements of } \mathrm{GF}(p)\colon \langle d, Y, 1\rangle \in \mathrm{EC\ SetProjCo}(a,b,p)\}}} = 1 + \mathrm{Lege}_p(d^3 + a \cdot d + b)$.

(63) Let p be a prime number and a, b be elements of $\mathrm{GF}(p)$. Suppose $p > 3$ and $\mathrm{Disc}(a,b,p) \neq 0_{\mathrm{GF}(p)}$. Then there exists a finite sequence F of elements of $\mathbb{N}$ such that

(i) $\mathrm{len}\, F = p$,

(ii) for every natural number n such that $n \in \mathrm{Seg}\, p$ there exists an element d of $\mathrm{GF}(p)$ such that $d = n - 1$ and $F(n) = 1 + \mathrm{Lege}_p(d^3 + a \cdot d + b)$, and

(iii) $\overline{\overline{\{[P]_{\mathbb{R}\text{-EllCur}(a,b,p)}; P \text{ ranges over elements of } \mathrm{ProjCo}\,\mathrm{GF}(p) : P \in \mathrm{EC\ SetProjCo}(a,b,p) \ \wedge \ \bigvee_{X,Y\,:\,\text{element of } \mathrm{GF}(p)} \ P = \langle X, Y, 1\rangle\}}} = \sum F$.

(64) Let p be a prime number and a, b be elements of $\mathrm{GF}(p)$. Suppose $p > 3$ and $\mathrm{Disc}(a, b, p) \neq 0_{\mathrm{GF}(p)}$. Then there exists a finite sequence F of elements of $\mathbb{Z}$ such that

(i) $\mathrm{len}\, F = p$,

(ii) for every natural number n such that $n \in \mathrm{Seg}\, p$ there exists an element d of $\mathrm{GF}(p)$ such that $d = n - 1$ and $F(n) = \mathrm{Lege}_p(d^3 + a \cdot d + b)$, and

(iii) $\overline{\overline{\mathrm{Classes}\, \mathbb{R}\text{-}\mathrm{EllCur}(a, b, p)}} = 1 + p + \sum F$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[8] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[9] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[10] G. Seroussi I. Blake and N. Smart. *Elliptic Curves in Cryptography.* Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.
[11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[12] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[13] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.
[14] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[15] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
[16] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[17] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[18] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[19] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[20] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[22] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[23] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.

Received December 21, 2010