FORMALIZED MATHEMATICS
Vol. 27, No. 3, Pages 315–320, 2019
DOI: 10.2478/forma-2019-0026

sciendo
https://www.sciendo.com/

Operations of Points on Elliptic Curve in Affine Coordinates[1]

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar [1], [2] a binary operation of points on an elliptic curve over **GF**(**p**) in affine coordinates. We show that the operation is unital, complementable and commutative. Elliptic curve cryptography [3], whose security is based on a difficulty of discrete logarithm problem of elliptic curves, is important for information security.

MSC: 14H52 14K05 68T99 03B35

Keywords: elliptic curve; commutative operation

MML identifier: EC_PF_3, version: 8.1.09 5.59.1363

1. Set of Points on Elliptic Curve in Affine Coordinates

From now on p denotes a 5 or greater prime number and z denotes an element of the parameters of elliptic curve p.

Now we state the propositions:

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

[1]This work was supported by JSPS KAKENHI Grant Numbers JP15K00183 and JP17K00182.

ISSN 1426–2630(Print), 1898-9934(Online)

PROOF: If $P = \langle 0, 1, 0 \rangle$, then the represent point of $P = P$. If $(P)_{\mathbf{3},3} = 1$, then the represent point of $P = P$ by [5, (2)], [6, (3)]. □

(2) Let us consider a 5 or greater prime number p, an element z of the parameters of elliptic curve p, and elements P, O of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $O = \langle 0, 1, 0 \rangle$. Then $(P)_{\mathbf{3},3} = 0$ if and only if $P \equiv O$. The theorem is a consequence of (1).

(3) Let us consider a 5 or greater prime number p, an element z of the parameters of elliptic curve p, and an element P of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. If $(P)_{\mathbf{3},3} = 0$, then $P \equiv (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)$. The theorem is a consequence of (2).

(4) Let us consider elements P, O of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $O = \langle 0, 1, 0 \rangle$. Then $(\mathrm{addell}_{\mathrm{ProjCo}}(z, p))(P, (\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)) \equiv O$. The theorem is a consequence of (2) and (3).

Let p be a 5 or greater prime number and z be an element of the parameters of elliptic curve p. The functor EC-SetAffCo(z, p) yielding a non empty subset of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$ is defined by the term

(Def. 1) $\{P$, where P is an element of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}}) : (P)_{\mathbf{3},3} = 1$ or $P = \langle 0, 1, 0 \rangle\}$.

Now we state the proposition:

(5) $\langle 0, 1, 0 \rangle$ is an element of EC-SetAffCo(z, p).

Let us consider a 5 or greater prime number p, an element z of the parameters of elliptic curve p, and an element P of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Now we state the propositions:

(6) The represent point of P is an element of EC-SetAffCo(z, p).

(7) If $P \in$ EC-SetAffCo(z, p), then the represent point of $P = P$. The theorem is a consequence of (1).

Let us consider elements P, O of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Now we state the propositions:

(8) If $O = \langle 0, 1, 0 \rangle$ and $P \not\equiv O$, then (the represent point of $P)_{\mathbf{3},3} = 1$. The theorem is a consequence of (2).

(9) Suppose $O = \langle 0, 1, 0 \rangle$ and the represent point of $P \equiv O$. Then

(i) the represent point of $P = O$, and

(ii) $P \equiv O$.

The theorem is a consequence of (2) and (1).

(10) Let us consider an element P of ProjCo(GF(p)). Then the represent point of the represent point of $P =$ the represent point of P. The theorem is a consequence of (1).

(11) Let us consider elements P, Q of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Suppose the represent point of $P \equiv$ the represent point of Q. Then the represent point of $P =$ the represent point of Q. The theorem is a consequence of (10).

Let p be a 5 or greater prime number and z be an element of the parameters of elliptic curve p. The functor compell-AffCo(z, p) yielding a unary operation on EC-SetAffCo(z, p) is defined by

(Def. 2) for every element P of EC-SetAffCo(z, p), $it(P) =$ the represent point of $(\mathrm{compell}_{\mathrm{ProjCo}}(z, p))(P)$.

Let F be a function from EC-SetAffCo(z, p) into EC-SetAffCo(z, p) and P be an element of EC-SetAffCo(z, p). Let us observe that the functor $F(P)$ yields an element of EC-SetAffCo(z, p). The functor addell-AffCo(z, p) yielding a binary operation on EC-SetAffCo(z, p) is defined by

(Def. 3) for every elements P, Q of EC-SetAffCo(z, p), $it(P, Q) =$ the represent point of $(\mathrm{addell}_{\mathrm{ProjCo}}(z, p))(P, Q)$.

Let F be a function from EC-SetAffCo$(z, p) \times$ EC-SetAffCo(z, p) into EC-SetAffCo(z, p) and Q, R be elements of EC-SetAffCo(z, p). Let us observe that the functor $F(Q, R)$ yields an element of EC-SetAffCo(z, p). Now we state the proposition:

(12) Let us consider elements P, O of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $O = \langle 0, 1, 0 \rangle$. Then

(i) $(\mathrm{addell}_{\mathrm{ProjCo}}(z, p))(P, O) \equiv P$, and

(ii) $(\mathrm{addell}_{\mathrm{ProjCo}}(z, p))(O, P) \equiv P$.

Let us consider elements P, O of EC-SetAffCo(z, p). Now we state the propositions:

(13) If $O = \langle 0, 1, 0 \rangle$, then (addell-AffCo$(z, p)$)$(O, P) = P$. The theorem is a consequence of (12) and (7).

(14) If $O = \langle 0, 1, 0 \rangle$, then (addell-AffCo$(z, p)$)$(P, O) = P$. The theorem is a consequence of (12) and (7).

(15) Let us consider an element O of EC-SetAffCo(z, p). Suppose $O = \langle 0, 1, 0 \rangle$. Then O is a unity w.r.t. addell-AffCo(z, p). The theorem is a consequence of (13) and (14).

(16) Let us consider elements P, O of EC-SetAffCo(z, p). Suppose $O = \langle 0, 1, 0 \rangle$. Then (addell-AffCo$(z, p)$)$(P,$ (compell-AffCo(z, p))$(P)) = O$. The theorem is a consequence of (7), (4), and (2).

2. Commutative Property of Operations of Points on Elliptic Curve

Now we state the propositions:

(17) Let us consider a 5 or greater prime number p, an element z of the parameters of elliptic curve p, and elements P, Q, O, P_3, Q_3 of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $O = \langle 0, 1, 0\rangle$ and $P \not\equiv O$ and $Q \not\equiv O$ and $P \not\equiv Q$. Suppose $P_3 = (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q)$ and $Q_3 = (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(Q,P)$. Then

(i) $(Q_3)_{\mathbf{1},3} = -(P_3)_{\mathbf{1},3}$, and

(ii) $(Q_3)_{\mathbf{2},3} = -(P_3)_{\mathbf{2},3}$, and

(iii) $(Q_3)_{\mathbf{3},3} = -(P_3)_{\mathbf{3},3}$.

Proof: Reconsider $g_2 = 2$ mod p as an element of $\mathrm{GF}(p)$. Set $gf_{1PQ} = (Q)_{\mathbf{2},3} \cdot ((P)_{\mathbf{3},3}) - (P)_{\mathbf{2},3} \cdot ((Q)_{\mathbf{3},3})$. Set $gf_{2PQ} = (Q)_{\mathbf{1},3} \cdot ((P)_{\mathbf{3},3}) - (P)_{\mathbf{1},3} \cdot ((Q)_{\mathbf{3},3})$. Set $gf_{3PQ} = {gf_{1PQ}}^2 \cdot ((P)_{\mathbf{3},3}) \cdot ((Q)_{\mathbf{3},3}) - {gf_{2PQ}}^3 - g_2 \cdot ({gf_{2PQ}}^2) \cdot ((P)_{\mathbf{1},3}) \cdot ((Q)_{\mathbf{3},3})$. Set $gf_{1QP} = (P)_{\mathbf{2},3} \cdot ((Q)_{\mathbf{3},3}) - (Q)_{\mathbf{2},3} \cdot ((P)_{\mathbf{3},3})$. Set $gf_{2QP} = (P)_{\mathbf{1},3} \cdot ((Q)_{\mathbf{3},3}) - (Q)_{\mathbf{1},3} \cdot ((P)_{\mathbf{3},3})$. Set $gf_{3QP} = {gf_{1QP}}^2 \cdot ((Q)_{\mathbf{3},3}) \cdot ((P)_{\mathbf{3},3}) - {gf_{2QP}}^3 - g_2 \cdot ({gf_{2QP}}^2) \cdot ((Q)_{\mathbf{1},3}) \cdot ((P)_{\mathbf{3},3})$. $gf_{3QP} = gf_{3PQ}$. $(Q_3)_{\mathbf{1},3} = -(P_3)_{\mathbf{1},3}$. $(Q_3)_{\mathbf{2},3} = -(P_3)_{\mathbf{2},3}$. $(Q_3)_{\mathbf{3},3} = -(P_3)_{\mathbf{3},3}$. □

(18) Let us consider elements P, Q, O, P_3, Q_3 of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$, and an element d of $\mathrm{GF}(p)$. Suppose $O = \langle 0, 1, 0\rangle$ and $d \neq 0_{\mathrm{GF}(p)}$ and $(Q)_{\mathbf{1},3} = d \cdot ((P)_{\mathbf{1},3})$ and $(Q)_{\mathbf{2},3} = d \cdot ((P)_{\mathbf{2},3})$ and $(Q)_{\mathbf{3},3} = d \cdot ((P)_{\mathbf{3},3})$ and $P \not\equiv O$ and $Q \not\equiv O$ and $P \equiv Q$ and $P_3 = (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q)$ and $Q_3 = (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(Q,P)$. Then

(i) $(Q_3)_{\mathbf{1},3} = d^6 \cdot ((P_3)_{\mathbf{1},3})$, and

(ii) $(Q_3)_{\mathbf{2},3} = d^6 \cdot ((P_3)_{\mathbf{2},3})$, and

(iii) $(Q_3)_{\mathbf{3},3} = d^6 \cdot ((P_3)_{\mathbf{3},3})$.

(19) Let us consider elements P, Q of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$.
Then $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q) \equiv (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(Q,P)$. The theorem is a consequence of (17) and (18).

(20) Let us consider elements P, Q of EC-SetAffCo(z,p).
Then (addell-AffCo(z,p))$(P,Q) =$ (addell-AffCo(z,p))(Q,P). The theorem is a consequence of (19).

Let p be a 5 or greater prime number and z be an element of the parameters of elliptic curve p. One can verify that addell-AffCo(z,p) is non empty, commutative, and unital.

The functor 0-EC(z,p) yielding an element of EC-SetAffCo(z,p) is defined by the term

(Def. 4) $\langle 0, 1, 0\rangle$.

Let us consider p and z. Let us observe that $\langle$EC-SetAffCo(z,p), addell-AffCo $(z,p)\rangle$ is Abelian and $\langle$EC-SetAffCo(z,p), addell-AffCo(z,p), 0-EC$(z,p)\rangle$ is left zeroed and right zeroed and $\langle$EC-SetAffCo(z,p), addell-AffCo(z,p), 0-EC$(z,p)\rangle$ is complementable.

Let p be a 5 or greater prime number and z be an element of the parameters of elliptic curve p. One can verify that $\langle$EC-SetAffCo(z,p), addell-AffCo$(z,p)\rangle$ is unital.

Now we state the proposition:

(21) Let us consider a 5 or greater prime number p, and an element z of the parameters of elliptic curve p. Then $\mathbf{1}_{\langle \text{EC-SetAffCo}(z,p),\text{addell-AffCo}(z,p)\rangle} =$ 0-EC(z,p). The theorem is a consequence of (15).

Let p be a 5 or greater prime number and z be an element of the parameters of elliptic curve p. One can check that $\langle$EC-SetAffCo(z,p), addell-AffCo$(z,p)\rangle$ is commutative, group-like, and non empty.

Now we state the propositions:

(22) Let us consider elements P_1, P_2, Q of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $P_1 \equiv P_2$. Then $(\text{addell}_{\text{ProjCo}}(z,p))(P_1,Q) \equiv (\text{addell}_{\text{ProjCo}}(z,p))(P_2,Q)$. The theorem is a consequence of (19).

(23) Let us consider elements P, Q_1, Q_2 of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $Q_1 \equiv Q_2$. Then $(\text{addell}_{\text{ProjCo}}(z,p))(P,Q_1) \equiv (\text{addell}_{\text{ProjCo}}(z,p))(P,Q_2)$. The theorem is a consequence of (19) and (22).

(24) Let us consider elements P_1, P_2, Q_1, Q_2 of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $P_1 \equiv P_2$ and $Q_1 \equiv Q_2$. Then $(\text{addell}_{\text{ProjCo}}(z,p))(P_1,Q_1) \equiv$ $(\text{addell}_{\text{ProjCo}}(z,p))(P_2,Q_2)$. The theorem is a consequence of (22) and (23).

(25) Let us consider elements P, O of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $O = \langle 0, 1, 0\rangle$. Then $P \equiv O$ if and only if $(\text{compell}_{\text{ProjCo}}(z,p))(P) \equiv O$.

(26) Let us consider elements P, Q of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$, and an element a of GF(p). Suppose $a \neq 0_{\text{GF}(p)}$ and $(P)_{\mathbf{1},3} = a \cdot ((Q)_{\mathbf{1},3})$ and $(P)_{\mathbf{2},3} = a \cdot ((Q)_{\mathbf{2},3})$ and $(P)_{\mathbf{3},3} = a \cdot ((Q)_{\mathbf{3},3})$. Then $P \equiv Q$.

(27) Let us consider elements P, Q of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$, and elements g_2, gf_1, gf_2, gf_3 of GF(p). Suppose $P \not\equiv Q$ and $(P)_{\mathbf{3},3} = 1$ and $(Q)_{\mathbf{3},3} = 1$ and $g_2 = 2 \bmod p$ and $gf_1 = (Q)_{\mathbf{2},3} - (P)_{\mathbf{2},3}$ and $gf_2 = (Q)_{\mathbf{1},3} - (P)_{\mathbf{1},3}$ and $gf_3 = {gf_1}^2 - {gf_2}^3 - g_2 \cdot ({gf_2}^2) \cdot ((P)_{\mathbf{1},3})$. Then $(\text{addell}_{\text{ProjCo}}(z,p))(P,Q) = \langle gf_2 \cdot gf_3,\ gf_1 \cdot ({gf_2}^2 \cdot ((P)_{\mathbf{1},3}) - gf_3) - {gf_2}^3 \cdot ((P)_{\mathbf{2},3}),\ {gf_2}^3\rangle$. The theorem is a consequence of (2).

(28) Let us consider elements P, Q of $\text{EC}_{\text{SetProjCo}}((z)_{\mathbf{1}})$, and elements g_2, g_3, g_4, g_8, gf_1, gf_2, gf_3, gf_4 of GF(p). Suppose $P \equiv Q$ and $(P)_{\mathbf{3},3} = 1$ and $(Q)_{\mathbf{3},3} = 1$ and $g_2 = 2 \bmod p$ and $g_3 = 3 \bmod p$ and $g_4 = 4 \bmod p$ and $g_8 =$

8 mod p and $gf_1 = (z)_{\mathbf{1}} + g_3 \cdot (((P)_{\mathbf{1},3})^2)$ and $gf_2 = (P)_{\mathbf{2},3}$ and $gf_3 = (P)_{\mathbf{1},3} \cdot ((P)_{\mathbf{2},3}) \cdot gf_2$ and $gf_4 = {gf_1}^2 - g_8 \cdot gf_3$. Then $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q) = \langle g_2 \cdot gf_4 \cdot gf_2,\ gf_1 \cdot (g_4 \cdot gf_3 - gf_4) - g_8 \cdot (((P)_{\mathbf{2},3})^2) \cdot ({gf_2}^2),\ g_8 \cdot ({gf_2}^3) \rangle$. The theorem is a consequence of (2).

Let us consider elements P, Q of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Now we state the propositions:

(29) Suppose $(P)_{\mathbf{3},3} = 1$ and $(Q)_{\mathbf{3},3} = 1$.
Then $(\mathrm{compell}_{\mathrm{ProjCo}}(z,p))((\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q)) \equiv (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))((\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(P), (\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(Q))$. The theorem is a consequence of (27), (28), and (26).

(30) $(\mathrm{compell}_{\mathrm{ProjCo}}(z,p))((\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,Q)) \equiv (\mathrm{addell}_{\mathrm{ProjCo}}(z,p))((\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(P), (\mathrm{compell}_{\mathrm{ProjCo}}(z,p))(Q))$. The theorem is a consequence of (25), (8), (29), (24), and (2).

(31) Let us consider elements P, O of $\mathrm{EC}_{\mathrm{SetProjCo}}((z)_{\mathbf{1}})$. Suppose $O = \langle 0,\ 1,\ 0 \rangle$ and $P \not\equiv O$. Then $(P)_{\mathbf{2},3} = 0_{\mathrm{GF}(p)}$ if and only if $(\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,P) \equiv O$.
Proof: Reconsider $g_8 = 8 \bmod p$ as an element of $\mathrm{GF}(p)$. $((\mathrm{addell}_{\mathrm{ProjCo}}(z,p))(P,P))_{\mathbf{3},3} = 0$. $g_8 \neq 0_{\mathrm{GF}(p)}$. $(P)_{\mathbf{3},3} \neq 0$ by [4, (23)], [5, (28)]. □

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.

[4] 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.

[5] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Operations of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 20(**1**):87–95, 2012. doi:10.2478/v10037-012-0012-2.

[6] Artur Korniłowicz. Recursive definitions. Part II. *Formalized Mathematics*, 12(**2**):167–172, 2004.

Accepted August 29, 2019