Scientific Research Publishing

Advances in Pure Mathematics, 2017, 7, 649-659
http://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

# An Algebraic Proof of the Associative Law of Elliptic Curves

**Kazuyuki Fujii[1], Hiroshi Oike[2]**

[1]International College of Arts and Sciences, Yokohama City University, Yokohama, Japan
[2]Takado, Yamagata, Japan
Email: fujii@yokohama-cu.ac.jp, oike@docomonet.jp

**How to cite this paper:** Fujii, K. and Oike, H. (2017) An Algebraic Proof of the Associative Law of Elliptic Curves. *Advances in Pure Mathematics*, **7**, 649-659.
https://doi.org/10.4236/apm.2017.712040

**Received:** October 7, 2017
**Accepted:** December 9, 2017
**Published:** December 12, 2017



## Abstract

In this paper we revisit the addition of elliptic curves and give an algebraic proof to the associative law by use of MATHEMATICA. The existing proofs of the associative law are rather complicated and hard to understand for beginners. An "elementary" proof to it based on algebra has not been given as far as we know. Undergraduates or non-experts can master the addition of elliptic curves through this paper. After mastering it they should challenge the elliptic curve cryptography.

## Keywords

Elliptic Curve, Addition, Associative Law, MATHEMATICA, Elliptic Curve Cryptography

## 1. Introduction

Ciphering is essential for the security of internet. The RSA cryptography [1] [2] [3] is now commonly used. However, in the very near future the RSA cryptography will be replaced by the elliptic curve cryptography because of its efficiency; the RSA system is based on 2048 bits, while the elliptic system is based on 224 bits (2016, [4]).

The target reader of this note is undergraduates or non-experts. Those who are interested in cryptography are strongly encouraged to master the theory of elliptic curve cryptography as soon as possible. For this purpose they must study an additional structure of elliptic curves. However, it is not so hard except for **the associative law**.

As far as we know an algebraic proof to it has not yet been given[1]. Therefore, we give an "elementary" proof by use of MATHEMATICA for them.

[1]We don't admit usual geometric proofs in standard textbooks of elliptic curves.

## 2. Addition of Points of an Elliptic Curve

Let us start by recalling the definition of an elliptic curve [5] [6]

$$y^2 = x^3 + ax + b \tag{1}$$

where $a$ and $b$ are some real constants. In the following we consider only real category. The discriminant of the cubic equation

$$x^3 + ax + b = 0$$

is given by

$$D = -4a^3 - 27b^2 \tag{2}$$

(see for example [5]) and we assume $D < 0$ in the following, so the point crossing the real axis is just one.

For the graph of the elliptic curve (1)

$$E = \left\{ (x, y) \in \mathbf{R}^2 \mid y^2 = x^3 + ax + b \right\} \tag{3}$$

we want to introduce an addition, which is essential in the elliptic curve cryptography. For the purpose we must add the infinity point $O = (\infty, \infty)$ to (3). As a result, our space is not $\mathbf{R}^2$ but a two dimensional sphere $\mathbf{R}^2 \bigcup O = \mathbf{S}^2$. Later it turns out that $O$ is the identity element of the addition, see (10), (11). This justifies the notation $O$ for the infinity point.

Here we note

$$P = (x, y) \in E \Rightarrow -P = (x, -y) \in E \tag{4}$$

where we have adopted the notation $-P$ for the mirror image of $P$ with respect to the real axis, see (11).

Let us introduce the addition in $E$. For two points $P_1, P_2 \in E$ we associate another point $P_3 \in E$. Consider the straight line passing through $P_1$ and $P_2$. We set R the crossing point of the line and the elliptic curve.

A simple-minded candidate of the addition is

$$P_1 \oplus P_2 = R$$

Unfortunately, this is not good because the associative law does not hold. Instead, we take the reflection point of $R$

$$P_1 \oplus P_2 = -R \equiv P_3. \tag{5}$$

This is correct as shown in the paper. See the following **Figure 1**.

Next, we want to express the addition above by use of the coordinate system. For the purpose we set

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \text{ and } P_3 = (x_3, y_3).$$

**Formula** The addition formula

$$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$$

is given by

$$x_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - (x_1 + x_2),$$

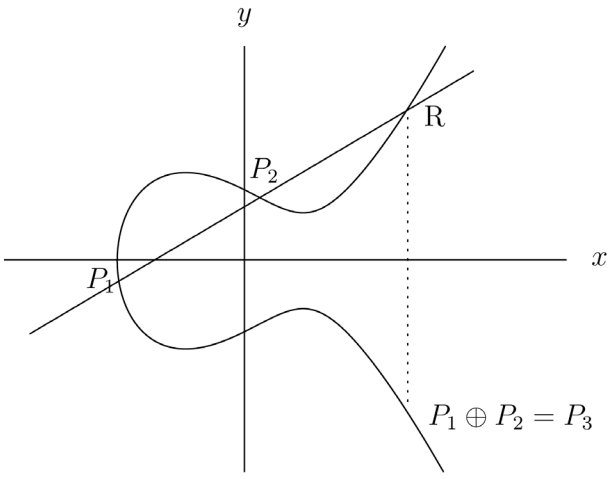


**Figure 1.** Addition $P_1 \neq P_2$.

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(2x_1 + x_2) - y_1. \tag{6}$$

**Proof** To give an elementary proof for undergraduates or non-experts is educational.

First of all we set the coordinate of the point $R = (x_r, y_r)$ and look for $x_r$ and $y_r$. The straight line passing through $P_1$ and $P_2$ is given by

$$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1.$$

By taking $x - x_1$ into consideration we have

$$\begin{aligned} y^2 &= x^3 + ax + b \\ &= (x - x_1 + x_1)^3 + a(x - x_1 + x_1) + b \\ &= (x - x_1)^3 + 3(x - x_1)^2 x_1 + 3(x - x_1)x_1^2 + a(x - x_1) + x_1^3 + ax_1 + b \\ &= (x - x_1)^3 + 3(x - x_1)^2 x_1 + 3(x - x_1)x_1^2 + a(x - x_1) + y_1^2. \end{aligned}$$

We substitute the straight line for the equation above

$$\begin{aligned} &\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 (x - x_1)^2 + 2\frac{y_2 - y_1}{x_2 - x_1}(x - x_1)y_1 + y_1^2 \\ &= (x - x_1)^3 + 3(x - x_1)^2 x_1 + 3(x - x_1)x_1^2 + a(x - x_1) + y_1^2. \end{aligned}$$

A short calculation gives

$$\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 (x - x_1) + 2\frac{y_2 - y_1}{x_2 - x_1}y_1 = (x - x_1)^2 + 3x_1(x - x_1) + 3x_1^2 + a$$

and

$$(x - x_1)^2 - \left\{\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 3x_1\right\}(x - x_1) + 3x_1^2 - 2\frac{y_2 - y_1}{x_2 - x_1}y_1 + a = 0.$$

This is a quadratic equation and it is easy to solve

$$x-x_1=\frac{1}{2}\left\{\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-3x_1\pm\sqrt{\left\{\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-3x_1\right\}^2-4\left(3x_1^2-2\frac{y_2-y_1}{x_2-x_1}y_1+a\right)}\right\}.$$

Here we set

$$(\#)=\left\{\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-3x_1\right\}^2-4\left(3x_1^2-2\frac{y_2-y_1}{x_2-x_1}y_1+a\right).$$

By expanding and arranging $(\#)$ we have

$$(\#)=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-6x_1\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+8\frac{y_2-y_1}{x_2-x_1}y_1-3x_1^2-4a.$$

Some calculation (this is a key point) gives

$$\begin{aligned}(\#)&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-6x_1\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-4\frac{(y_2-y_1)^2}{x_2-x_1}\\&\quad+4\frac{(y_2-y_1)^2}{x_2-x_1}+8\frac{y_2-y_1}{x_2-x_1}y_1-3x_1^2-4a\\&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-\{6x_1+4(x_2-x_1)\}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2\\&\quad+4\frac{(y_2-y_1)\{(y_2-y_1)+2y_1\}}{x_2-x_1}-3x_1^2-4a\\&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-2(2x_2+x_1)\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+4\frac{y_2^2-y_1^2}{x_2-x_1}-3x_1^2-4a\\&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-2(2x_2+x_1)\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+4(x_2^2+x_2x_1+x_1^2+a)-3x_1^2-4a\\&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-2(2x_2+x_1)\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+4x_2^2+4x_2x_1+x_1^2\\&=\left(\frac{y_2-y_1}{x_2-x_1}\right)^4-2(2x_2+x_1)\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+(2x_2+x_1)^2\\&=\left\{\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-2x_2-x_1\right\}^2\end{aligned}$$

where in the process we have used the equation

$$\begin{aligned}y_2^2-y_1^2&=(x_2^3+ax_2+b)-(x_1^3+ax_1+b)\\&=(x_2-x_1)(x_2^2+x_2x_1+x_1^2+a).\end{aligned}$$

Therefore

$$\begin{aligned}x-x_1&=\frac{1}{2}\left\{\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-3x_1+\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-2x_2-x_1\right\}\\&=\frac{1}{2}\left\{2\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-4x_1-2x_2\right\}=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-(2x_1+x_2)\end{aligned}$$

and we finally obtain

$$x_r = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2),$$

which is symmetric in 1 and 2. Another solution is $x = x_2$ (check this).

This gives

$$\begin{aligned} y_r &= \frac{y_2 - y_1}{x_2 - x_1}(x_r - x_1) + y_1 \\ &= \frac{y_2 - y_1}{x_2 - x_1}\left\{\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (2x_1 + x_2)\right\} + y_1 \\ &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(2x_1 + x_2) + y_1. \end{aligned}$$

As a result we have

$$(x_3, y_3) = (x_r, -y_r)$$

and this gives the Formula (6).

**Comment** From the geometric definition of the addition (5) it is easy to see the commutativity

$$P_1 \oplus P_2 = P_2 \oplus P_1.$$

However, it is not clear to see this from the Formula (6). Then, a small change of $y_3$ in (6) gives

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 + x_2) + \frac{y_2 x_1 - y_1 x_2}{x_2 - x_1}, \tag{7}$$

which is anti-symmetric in 1 and 2. The commutativity is very clear. In our opinion this formula is best.

Next, we must define the addition $P \oplus P$ of the same point *P*. The definition is usually performed by differential. By noting

$$\lim_{2 \to 1} \frac{y_2 - y_1}{x_2 - x_1} = y_1'$$

the differential of $y^2 = x^3 + ax + b$ at $(x_1, y_1)$ gives

$$2y_1 y_1' = 3x_1^2 + a \Rightarrow y_1' = \frac{3x_1^2 + a}{2y_1}.$$

If we set for $P(x, y)$

$$P \oplus P = P_3 \text{ or } (x, y) \oplus (x, y) = (x_3, y_3) \tag{8}$$

then we obtain

$$x_3 = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x,$$

$$y_3 = -\left(\frac{3x^2 + a}{2y}\right)^3 + \left(\frac{3x^2 + a}{2y}\right)3x - y \tag{9}$$

by applying the argument above to (6). See the following Figure 2.

There are tasks left behind. Our tasks are to show

$$P \oplus O = O \oplus P = P \tag{10}$$

and

$$P \oplus (-P) = (-P) \oplus P = O. \tag{11}$$

**Exercise** Consider a proof with the geometric method.

Last, we must prove the associative law

$$(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3), \tag{12}$$

which is very hard for undergraduates (hard even for experts).

The geometric method usually goes like Figure 3 ( $P_1 = P$ , $P_2 = Q$ and $P_3 = R$ in this figure)

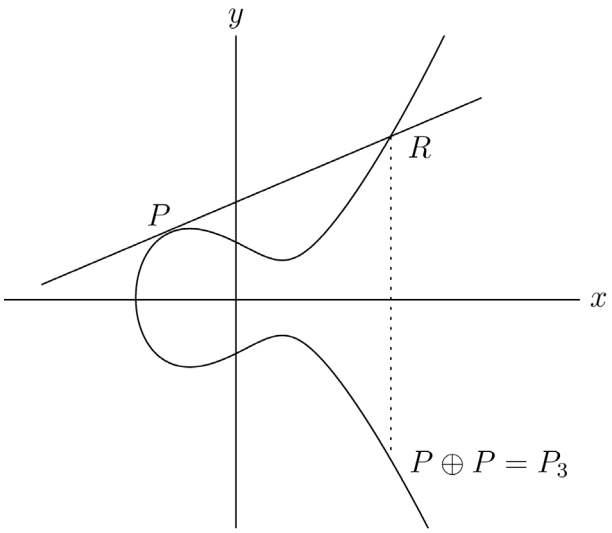


Figure 2. Addition $P_1 = P_2 = P$.

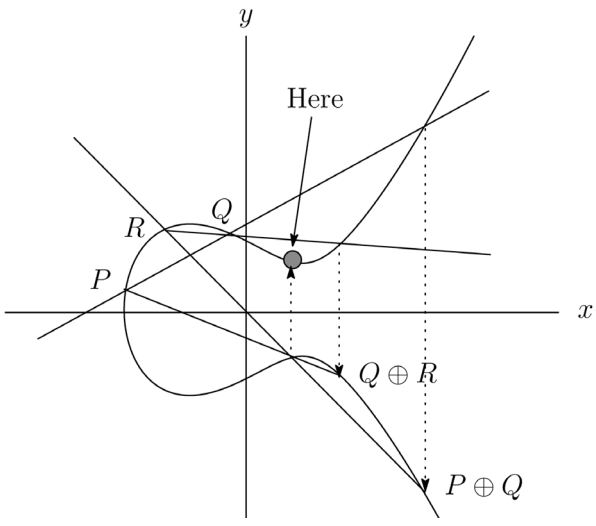


Figure 3. Associativity $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

However, this is not a proof but a circumstantial evidence. Therefore, we give an algebraic proof by use of MATHEMATICA[2].

For the purpose let us calculate the difference

$$\left(P_1 \oplus P_2\right) \oplus P_3 - P_1 \oplus \left(P_2 \oplus P_3\right) \tag{13}$$

by MATHEMATICA. In the following program we set

$$\left(P_1 \oplus P_2\right) \oplus P_3 - P_1 \oplus \left(P_2 \oplus P_3\right) = \left(CC - FF, DD - GG\right). \tag{14}$$

and use the Formula (7) because of its high symmetry. Associativity holds when the right hand side vanishes.

Beginning of MATHEMATICA

Readers must input and execute the following program in standard form of MATHEMATICA.

We set

$$s = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - \left(x_1 + x_2\right);$$

$$t = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)\left(x_1 + x_2\right) + \frac{\mathrm{Det}\left[\begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}\right]}{x_2 - x_1};$$

and

$$CC = \left(\frac{y_3 - t}{x_3 - s}\right)^2 - \left(s + x_3\right);$$

$$DD = -\left(\frac{y_3 - t}{x_3 - s}\right)^3 + \left(\frac{y_3 - t}{x_3 - s}\right)\left(s + x_3\right) + \frac{\mathrm{Det}\left[\begin{pmatrix} s & x_3 \\ t & y_3 \end{pmatrix}\right]}{x_3 - s};$$

and also set

$$u = \left(\frac{y_3 - y_2}{x_3 - x_2}\right)^2 - \left(x_2 + x_3\right);$$

$$v = -\left(\frac{y_3 - y_2}{x_3 - x_2}\right)^3 + \left(\frac{y_3 - y_2}{x_3 - x_2}\right)\left(x_2 + x_3\right) + \frac{\mathrm{Det}\left[\begin{pmatrix} x_2 & x_3 \\ y_2 & y_3 \end{pmatrix}\right]}{x_3 - x_2};$$

and

$$FF = \left(\frac{v - y_1}{u - x_1}\right)^2 - \left(x_1 + u\right);$$

$$GG = -\left(\frac{v - y_1}{u - x_1}\right)^3 + \left(\frac{v - y_1}{u - x_1}\right)\left(x_1 + u\right) + \frac{\mathrm{Det}\left[\begin{pmatrix} x_1 & u \\ y_1 & v \end{pmatrix}\right]}{u - x_1}.$$

[2]We expect that undergraduates in the world can use MATHEMATICA or MAPLE, etc.

Moreover, we set

$$P=(y_1-y_2)^2-(x_1-x_2)^2(x_1+x_2+x_3);$$

$$Q=(y_2-y_3)^2-(x_2-x_3)^2(x_1+x_2+x_3);$$

$$R=(x_2-x_3)y_1^2+(x_3-x_1)y_2^2+(x_1-x_2)y_3^2 +(x_1-x_2)(x_2-x_3)(x_3-x_1)(x_1+x_2+x_3).$$

Here, $P^2$ ($Q^2$) appears in the denominator of $CC$ ($FF$) and $P^3$ ($Q^3$) in the denominator of $DD$ ($GG$). The homogeneous polynomials $P$ and $Q$ are invariant under the permutation of $1,2,3$, whereas $R$ changes sign.

For

$$AA=\frac{P^2Q^2(CC-FF)}{R};\quad BB=\frac{P^3Q^3(DD-GG)}{R};$$

execute the following

$$\text{Factor}[AA]$$

$$\text{Factor}[BB]$$

Ending of MATHEMATICA

It takes about several seconds for a standard present day PC before MATHEMATICA outputs two huge *homogeneous polynomials* in $x_1$, $x_2$, $x_3$, $y_1$, $y_2$ and $y_3$ of *integer coefficients*. The "degrees" of $AA$ and $BB$ are 9 and 31/2, respectively, when "degree" 1 is assigned to $x_1$, $x_2$, $x_3$ and 3/2 for $y_1$, $y_2$ and $y_3$, see the curve Equation (1). In other words, $AA$ and $BB$ are universal polynomials of elliptic curves which are independent of the parameters *a* and *b*. More than 10 pages are required to write down the outputs. As we will see their explicit forms are irrelevant for the discussion of the associativity, we do not display them here. These polynomials have many interesting features.
From the program we have

$$CC-FF=\frac{AA}{P^2Q^2}R,\quad DD-GG=\frac{BB}{P^3Q^3}R. \tag{15}$$

It is very interesting and important that both have a common factor *R*. Note that we have not imposed the equations

$$\begin{cases} y_1^2=x_1^3+ax_1+b \\ y_2^2=x_2^3+ax_2+b \\ y_3^2=x_3^3+ax_3+b \end{cases} \tag{16}$$

up to this point.

Last, we show

$$R=0 \tag{17}$$

under the condition (16), which finishes the proof of associativity (14).

Here, let us give an educational proof for undergraduates. We treat the following determinant :

$$X = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ y_1^2 & y_2^2 & y_3^2 \end{vmatrix} \tag{18}$$

Direct calculation gives

$$\begin{aligned} X &= x_2y_3^2 + x_3y_1^2 + x_1y_2^2 - x_2y_1^2 - x_1y_3^2 - x_3y_2^2 \\ &= -\left\{(x_2 - x_3)y_1^2 + (x_3 - x_1)y_2^2 + (x_1 - x_2)y_3^2\right\}. \end{aligned} \tag{19}$$

On the other hand, from (16) we have

$$\begin{aligned} X &= \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^3 + ax_1 + b & x_2^3 + ax_2 + b & x_3^3 + ax_3 + b \end{vmatrix} \\ &= \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^3 + ax_1 & x_2^3 + ax_2 & x_3^3 + ax_3 \end{vmatrix} \\ &= \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^3 & x_2^3 & x_3^3 \end{vmatrix} \end{aligned}$$

by some fundamental operations.

Moreover, we have

$$\begin{aligned} X &= \begin{vmatrix} 1 & 0 & 0 \\ x_1 & x_2 - x_1 & x_3 - x_1 \\ x_1^3 & x_2^3 - x_1^3 & x_3^3 - x_1^3 \end{vmatrix} \\ &= (x_2 - x_1)(x_3 - x_1)\begin{vmatrix} 1 & 0 & 0 \\ x_1 & 1 & 1 \\ x_1^3 & x_2^2 + x_2x_1 + x_1^2 & x_3^2 + x_3x_1 + x_1^2 \end{vmatrix} \\ &= (x_2 - x_1)(x_3 - x_1)\begin{vmatrix} 1 & 0 & 0 \\ x_1 & 1 & 0 \\ x_1^3 & x_2^2 + x_2x_1 + x_1^2 & (x_3 - x_2)(x_3 + x_2 + x_1) \end{vmatrix} \\ &= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)(x_3 + x_2 + x_1) \\ &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_1 + x_2 + x_3) \end{aligned} \tag{20}$$

by some fundamental operations. As a result, we obtain

$$\begin{aligned} R &= (x_2 - x_3)y_1^2 + (x_3 - x_1)y_2^2 + (x_1 - x_2)y_3^2 \\ &\quad + (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_1 + x_2 + x_3) \\ &= -X + X = 0 \end{aligned}$$

by (19) and (20).

As shown in the paper the elementary proof of the associative law of the points of an elliptic curve is not easy. However, it is not necessarily a bad thing for the encryption system.

In this section we reproved the following

**Theorem** The system $\{E, \oplus\}$ becomes an additive (abelian) group.

## 3. Concluding Remarks

We conclude the paper by making some comments on the elliptic curve cryptography [7] [8].

Let $p$ be a huge prime number and $\mathbf{F}_p$ be the finite field

$$\mathbf{F}_p = \{0,1,2,\cdots,p-1\},$$

see for example [5].

Our target is an elliptic curve on $\mathbf{F}_p$

$$E_p = \{(x,y) \mid y^2 = x^3 + ax + b \pmod p\}.$$

For this case $E_p$ becomes a finite set. We assume that $P$ and $Q \in E_p$ satisfy the relation

$$Q = n_{\oplus} P \pmod p$$

where

$$n_{\oplus} P = P \oplus P \oplus \cdots \oplus P \ (n\text{-times}).$$

**Problem** For given $P$ and $Q$ is it possible to find $n$ in polynomial time?

This is called the **discrete logarithm problem** and it is known as a very hard one to solve [9]. The security of the elliptic curve cryptography (which is worth studying for undergraduates or non-experts) is based on this hard problem.

## Acknowledgements

We wishes to thank Ryu Sasaki for useful suggestions and comments.

## References

[1] Diffie, W. and Hellman, M. (1976) New Directions in Cryptography. *IEEE Transactions on Information Theory*, **22**, 644-654. https://doi.org/10.1109/TIT.1976.1055638

[2] Rivest, R.L., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, **21**, 120-126. https://doi.org/10.1145/359340.359342

[3] ELGamal, T. (1985) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31**, 469-472. https://doi.org/10.1109/TIT.1985.1057074

[4] Nakanishi, T. (2017) Mechanisms of Modern Cryptography. Kyoritsu Smart Selection 12, Kyoritsu Shuppan.

[5] Silverman, J.H. (2006) A Friendly Introduction to NUMBER THEORY. 3rd Edition, Pearson Education, London.

[6] Silverman, J.H. and Tate, J. (1992) Rational Points on Elliptic Curves. Springer-Verlag, Berlin. https://doi.org/10.1007/978-1-4757-4252-7

[7] Koblitz, N. (1987) Elliptic Curve Cryptosystems. *Mathematics of Computation*, **48**, 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

[8] Fujii, K. (2014-2016) Public-Key Cryptography and Its Decoding by Quantum Computation (in Japanese). Lecture Note at Yokohama City University, Yokohama, 39.

[9] Shor, P.W. (1999) Polynomial—Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, **41**, 303-332. https://doi.org/10.1137/S0036144598347011