A mean value formula for elliptic curves *

Rongquan Feng[1], Hongfeng Wu[2] †

[1]LMAM, School of Mathematical Sciences, Peking University,
Beijing 100871, P.R. China

[2]Academy of Mathematics and Systems Science, Chinese Academy of Sciences,
Beijing 100190, P.R. China

fengrq@math.pku.edu.cn, whfmath@gmail.com

Abstract

It is proved in this paper that for any point on an elliptic curve, the mean value of x-coordinates of its n-division points is the same as its x-coordinate.

Keywords: elliptic curves, point multiplication, division polynomial

Let K be a field with $\mathrm{char}(K) > 3$. Every elliptic curve E/K can be written as a classical Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

with coefficients a, $b \in K$. A point Q on E is said to be smooth (or non-singular) if $\left(\frac{\partial f}{\partial x}|_Q, \frac{\partial f}{\partial y}|_Q\right) \neq (0,0)$, where $f(x,y) = y^2 - x^3 - ax - b$. The point multiplication is the operation of computing

$$nP = \underbrace{P + P + \cdots + P}_{n}$$

*Supported by NSF of China (No. 10990011)
†China Postdoctoral Science Foundation funded project.

for any point $P \in E$ and a positive integer n. The multiplication-by-n map

$$\begin{array}{rccc} [n]: & E & \to & E \\ & P & \mapsto & nP \end{array}$$

is an isogeny of degree n^2. For a point $Q \in E$, any element of $[n]^{-1}(Q)$ is called an n-division point of Q. Assume $(\mathrm{char}(K), n) = 1$. In this paper, the following result on the mean value of the x-coordinates of all the n-division points of any smooth point on an elliptic curve is proved.

Theorem 1. *Let E be an elliptic curve defined over K, and let $Q = (x_Q, y_Q) \in E$ be a point with $Q \neq \mathcal{O}$. Set*

$$\Lambda = \{P = (x_P, y_P) \in E(\bar{K}) \mid nP = Q\}.$$

Then

$$\frac{1}{n^2} \sum_{P \in \Lambda} x_P = x_Q.$$

Remark that, if $(\mathrm{char}(K), n) \neq 1$ then we have $\sum\limits_{P \in \Lambda} x_P = n^2 x_Q$. According to the theorem, let $P_i = (x_i, y_i), i = 1, 2, \cdots, n^2$ be all the points such that $nP = Q$. Let λ_i be the slope of the line through P_i and Q, then $y_Q = \lambda_i(x_Q - x_i) + y_i$. Therefore, $n^2 y_Q = \sum\limits_{i=1}^{n^2} \lambda_i \cdot (\sum\limits_{i=1}^{n^2} x_i)/n^2 - \sum\limits_{i=1}^{n^2} \lambda_i x_i + \sum\limits_{i=1}^{n^2} y_i$, thus we have

$$y_Q = \frac{\sum\limits_{i=1}^{n^2} \lambda_i}{n^2} \cdot \frac{\sum\limits_{i=1}^{n^2} x_i}{n^2} - \frac{\sum\limits_{i=1}^{n^2} \lambda_i x_i}{n^2} + \frac{\sum\limits_{i=1}^{n^2} y_i}{n^2} = \overline{\lambda_i} \cdot \overline{x_i} - \overline{\lambda_i x_i} + \overline{y_i},$$

where $\overline{\lambda_i}$, $\overline{x_i}$, $\overline{\lambda_i x_i}$, $\overline{y_i}$ be the average value of the variables $\lambda_i, x_i, \lambda_i x_i$ and y_i. Therefore, $Q = (x_Q, y_Q) = (\overline{x_i},\ \overline{\lambda_i} \cdot \overline{x_i} - \overline{\lambda_i x_i} + \overline{y_i})$.

To prove this result, define division polynomials [1] $\psi_n \in \mathbb{Z}[x, y, a, b]$ on an elliptic curve $E : y^2 = x^3 + ax + b$, inductively as follows:

$$\begin{aligned}
\psi_0 &= 0, \\
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \text{ for } n \geq 2, \\
2y\psi_{2n} &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \text{ for } n \geq 3.
\end{aligned}$$

It can be checked easily by induction that the ψ_{2n}'s are polynomials. Moreover, $\psi_n \in \mathbb{Z}[x, y^2, a, b]$ when n is odd, and $(2y)^{-1}\psi_n \in \mathbb{Z}[x, y^2, a, b]$ when n is even. Define the polynomial

$$\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}$$

for $n \geq 1$. Then $\phi_n \in \mathbb{Z}[x, y^2, a, b]$. Since $y^2 = x^3 + ax + b$, replacing y^2 by $x^3 + ax + b$, one have that $\phi_n \in \mathbb{Z}[x, a, b]$. So we can denote it by $\phi_n(x)$. Note that, $\psi_n\psi_m \in \mathbb{Z}[x, a, b]$ if n and m have the same parity.

Lemma 2. *The leading term of ψ_n is $nx^{(n^2-1)/2}$ when n is odd and is $nx^{(n^2-4)/2}y$ when is even.*

Proof. We give only the proof for the case where n is odd. The even case can be proved similarly. It is true for $n < 5$. Assume that it holds for all $n < 2k+1$. Now let $n = 2k+1$. If k is even, then by induction, the leading term of $\psi_{k+2}\psi_k^3$ is $(k+2)k^3y^4x^{\frac{(k+2)^2-4}{2}+\frac{3k^2-12}{2}}$, which is also $(k+2)k^3x^{\frac{(2k+1)^2-1}{2}}$ by substituting y^4 by $(x^3 + ax + b)^2$, and the leading term of $\psi_{k-1}\psi_{k+1}^3$ is $(k-1)(k+1)^3x^{\frac{(2k+1)^2-1}{2}}$. Thus, the leading term of ψ_{2k+1} is $(2k+1)x^{\frac{(2k+1)^2-1}{2}}$ when k is even. Similarly, if k is odd, then the leading term $\psi_{k+2}\psi_k^3$ is $(k+2)k^3x^{\frac{(2k+1)^2-1}{2}}$, and the leading term of $\psi_{k-1}\psi_{k+1}^3$ is $(k-1)(k+1)^3x^{\frac{(2k+1)^2-1}{2}}$. We have again the leading term of ψ_{2k+1} is $(2k+1)x^{\frac{(2k+1)^2-1}{2}}$ when k is odd. □

From Lemma 2, we have

$$\psi_n^2(x) = n^2x^{n^2-1} + \cdots,$$

and

$$\phi_n(x) = x^{n^2} + \cdots.$$

Lemma 3. *The coefficient of the x^{n^2-2} term of ψ_n^2 is 0, and the coefficient of the x^{n^2-1} term of $\psi_{n+1}\psi_{n-1}$ is 0.*

Proof. In order to prove the result, let us define the function F by

$$F(g) = (\text{the degree of } g, \text{the degree of the second leading term of } g)$$

for a polynomial $g \in \mathbb{Z}[x, a, b]$. In the following, set $F(g) = (m, \leq \ell)$, if the degree of g is m and the degree of the second leading term of g is less than or equal to ℓ.

Now we prove this lemma by induction. For $n \leq 4$, the statements are true from the definition of ψ_n. Now assume that the statements hold for all $n < 2k$ ($k > 2$), i.e., the coefficient of the x^{n^2-2} term of ψ_n^2 and that of the x^{n^2-1} term of $\psi_{n+1}\psi_{n-1}$ are 0's for $n < 2k$. Suppose that $n = 2k + 1$. Then

$$\psi_{2k+1}^2 = (\psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3)^2 = \psi_{k+2}^2\psi_k^6 + \psi_{k-1}^2\psi_{k+1}^6 - 2\psi_{k-1}\psi_{k+2}\psi_k^3\psi_{k+1}^3.$$

It is clear that $F(\psi_k\psi_{k+2}) = (k^2 + 2k + 1, \leq k^2 + 2k - 1)$ since $k + 2 < 2k$ and the coefficient of the $x^{(k+1)^2-1} = x^{k^2+2k}$ term of $\psi_k\psi_{k+2}$ is 0 from the assumption. So $F((\psi_k\psi_{k+2})^2) = (2k^2 + 4k + 2, \leq 2k^2 + 4k)$. Furthermore, $F(\psi_k^4) = F((\psi_k^2)^2) = (2k^2 - 2, \leq 2k^2 - 4)$ since $F(\psi_k^2) = (k^2 - 1, \leq k^2 - 3)$ from the induction assumption. Thus

$$F(\psi_{k+2}^2\psi_k^6) = F((\psi_k\psi_{k+2})^2\psi_k^4) = (4k^2 + 4k, \leq 4k^2 + 4k - 2).$$

Similarly,

$$F(\psi_{k-1}^2\psi_{k+1}^6) = F((\psi_{k-1}\psi_{k+1})^2\psi_{k+1}^4) = (4k^2 + 4k, \leq 4k^2 + 4k - 2),$$

and

$$F(2\psi_{k-1}\psi_{k+2}\psi_{k+1}\psi_k^3) = F(\psi_{k-1}\psi_{k+1}\psi_k\psi_{k+2}\psi_k^2\psi_{k+1}^2) = (4k^2+4k, \leq 4k^2+4k-2).$$

Therefore,

$$F(\psi_{2k+1}^2) = (4k^2 + 4k, \leq 4k^2 + 4k - 2).$$

Similarly, when $n = 2k$, we have that $F(\psi_{2k}^2) = (4k^2 - 1, \leq 4k^2 + 4k - 3)$.

For the polynomial $\psi_{n-1}\psi_{n+1}$, when $n = 2k$, from

$$\begin{aligned}
\psi_{2k-1}\psi_{2k+1} &= \psi_{2(k-1)+1}\psi_{2k+1} = (\psi_{k+1}\psi_{k-1}^3 - \psi_{k-2}\psi_k^3)(\psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3) \\
&= \psi_{k+1}\psi_{k-1}\psi_{k+2}\psi_k\psi_{k-1}^2\psi_k^2 - \psi_{k-1}^4\psi_{k+1}^4 - \psi_{k-2}\psi_k\psi_k\psi_{k+2}\psi_k^4 \\
&\quad +\psi_{k-2}\psi_k\psi_{k-1}\psi_{k+1}\psi_k^2\psi_{k+1}^2,
\end{aligned}$$

we have that $F(\psi_{2k-1}\psi_{2k+1}) = (4k^2, \leq 4k^2 - 2)$ from the assumption. The case for the polynomial $\psi_{n-1}\psi_{n+1}$, where $n = 2k+1$ can be treated similarly. This completes the proof. □

The following corollary follows immediately from Lemma 3.

Corollary 4. *The coefficient of the x^{n^2-1} term of $\phi_n(x)$ is* 0.

Proof of Theorem 1: Define ω_n as

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2.$$

Let $P = (x_P, y_P) \in E$. Then ([1])

$$nP = \left(\frac{\phi_n(x_P)}{\psi_n^2(x_P)}, \frac{\omega_n(x_P, y_P)}{\psi_n(x_P, y_P)^3} \right).$$

If $nP = Q$, then $\phi_n(x_P) - x_Q\psi_n^2(x_P) = 0$. Therefore, for any $P \in \Lambda$, the x-coordinate of P satisfies the equation $\phi_n(x) - x_Q\psi_n^2(x) = 0$. From Corollary 4, we have that

$$\phi_n(x) - x_Q\psi_n^2(x) = x^{n^2} - n^2 x_Q x^{n^2-1} + \text{lower degree terms}.$$

Since $\sharp\Lambda = n^2$, every root of $\phi_n(x) - x_Q\psi_n^2(x)$ is the x-coordinate of some $P \in \Lambda$. Therefore $\sum\limits_{P\in\Lambda} x_P = n^2 x_Q$ by Vitae Theorem. $\square$

References

[1] J.H. Silverman. The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, Berlin, 1986.