J. KSIAM **Vol.6**, No.2, 25-30, 2002

DISTRIBUTION OF RATIONAL POINTS IN THE REAL LOCUS OF ELLIPTIC CURVES

S. HAHN AND D. H. LEE

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve defined over rationals, $\mathbf{P}$ is a non-torsion rational point of E and

$$S = \{[n]\mathbf{P} | n \in \mathbb{Z}\}.$$

then S is dense in the component of $E(\mathbb{R})$ which contains the infinity in the usual Euclidean topology or in the topology defined by the invariant Haar measure and it is uniformly distributed.

Let g_2 and g_3 be two rational integers with non-zero discriminant $\Delta(E) = g_2^3 - 27g_3^2$ which defines an elliptic curve

$$E : y^2 = 4x^3 - g_2x - g_3.$$

Let ω_1 and ω_2 be a fundamental pair of periods for E, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and

$$F = \{\alpha_1\omega_1 + \alpha_2\omega_2 | 0 \leq a, b \leq 1\}$$

denote a fundamental region for the lattice Λ which can be identified with the complex locus $E(\mathbb{C})$ or the quotient $\mathbb{C}/\mathbf{\Lambda}$ by the isomorphism π

$$\pi : \mathbb{C}/\mathbf{\Lambda} \to E(\mathbb{C})$$

$$z \mapsto (\wp(z), \wp'(z))$$

where $\wp$ denotes the Weierstrass $\wp$ function defined by a lattice Λ. So the real locus $E(\mathbb{R})$ can be identified as a subset of F. For convenience we can further identify F with the unit square

$$I = \{(x, y) \in \mathbb{R}^2 | 0 \leq x, y \leq 1\}$$

on the Euclidean plane.

Consider the polynomial $f(x) = 4x^3 - g_2x - g_3$ which is the right side of the defining equation. If $f(x)$ has three distinct real roots $e_3 < e_2 < e_1$, that is $\Delta > 0$, then we may take

$$\omega_1 = \frac{\pi}{M(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})},\ \omega_2 = \frac{i\pi}{M(\sqrt{e_1 - e_3}, \sqrt{e_2 - e_3})}$$

where $M(a,b)$ denotes the arithmetic-geometric mean defined by Gauss. In this case, ω_1 is positive real and ω_2 is imaginary and $Im(\omega_2) > 0$ since $e_3 < e_2 < e_1$. If $f(x)$ has only one real root, e and two complex roots, that is $\Delta < 0$ we may take

$$\omega_1 = \frac{2\pi}{M(2\sqrt{\beta}, \sqrt{2\beta + \alpha})},\ \omega_2 = -\frac{\omega_1}{2} + \frac{i\pi}{M(2\sqrt{\beta}, \sqrt{2\beta - \alpha})}.$$

where $\alpha = 3e$ and $\beta = \sqrt{3e^2 - \frac{g_2}{4}}$. In this case ω_1 is also positive real and $Im(\omega_2) > 0, Re(\omega_2) = -\frac{1}{2}\omega_1$ since $\beta > 0$ and $2\beta \pm \alpha > 0$.

Without loss of generality, we may assume that $0 = Arg(\omega_1) < Arg(\omega_2) < \pi$. Schneider showed that ω_1 and ω_2 are both transcendental numbers. He also showed that the quotient ω_1/ω_2 is either a transcendental or an imaginary quadratic irrational. In the latter case E has complex multiplication.

Our aim in this paper is to study the distribution of the rational points $E(\mathbb{Q})$ inside the real locus $E(\mathbb{R})$. More precisely, we are interested in the question whether $E(\mathbb{Q})$ is dense in $E(\mathbb{R})$ in the Euclidean topology when $E(\mathbb{Q})$ has positive rank. In a similar fashion one might ask whether the sequence of rational points $[n]P$, $n = 0, \pm 1, \pm 2, \pm 3, \cdots$, is uniformly distributed inside $E(\mathbb{R})$ under the metric given by the invariant differential

$$\omega = \frac{dx}{2y} = \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}$$

when P is a non-torsion point of $E(\mathbb{Q})$. The above question is equivalent to whether the set $\{n\pi^{-1}(P) | n = 0, \pm 1, \pm 2, \cdots\}$ is uniformly distributed inside the inverse image of $\pi^{-1}(E(\mathbb{R}))$ under the usual Euclidean topology.
$E(\mathbb{R})$ has either two or one connected components depending on whether the cubic

equation

$$4x^3 - g_2 x - g_3 = 0$$

on the right side of the defining equation has three distinct real roots(if and only if $\Delta(E) = g_2^3 - 27g_3^2 > 0$) or one real root(if and only if $\Delta(E) = g_2^3 - 27g_3^2 < 0$). We will call the (possibly two) component(s) by finite component and infinite component depending upon whether the Euclidean length of the component is finite or infinite. Let P be a non-torsion point of $E(\mathbb{Q})$ corresponding to

$$\alpha_1\omega_1 + \alpha_2\omega_2$$

in $\mathbb{C}/\Lambda$(or to (α_1, α_2) in I). Then α_1 and α_2 can not be both rational, since otherwise P will be a torsion point. Kronecker's classical theorem on simultaneous Diophantine approximation is as follows: If 1, α_1, $\cdots$, and α_k are linearly independent over the rationals $\mathbb{Q}$, then the set

$$\left\{(\{n\alpha_1\}, \{n\alpha_2\}, \cdots, \{n\alpha_k\}) \middle| \ n \in \mathbb{Z}\right\}$$

is dense in the k-dimensional unit box $[0,1]^k$ where $\{x\} = x - [x]$ denotes the fractional part of x. So Kronecker's theorem tells that the numbers 1, α_1, and α_2 can not be linearly independent over the rationals $\mathbb{Q}$, since otherwise the sequence S,

$$S = \big\{[n]P | n = 0, \pm 1, \pm 2, \pm 3, \cdots\big\} \subseteq E(\mathbb{Q})$$

will be dense in the whole $E(\mathbb{C})$. Hence we have an equation

$$r + s\alpha_1 + t\alpha_2 = 0$$

for some relatively prime integers r, s, and t which are not zeroes simultaneously.

Computing α_1 and α_2 is called the elliptic logarithm problem. And it is possible to compute α_1 and α_2 to any prescribed precision for any elliptic curve with a non-torsion point P.

Algorithm 1. *For a given elliptic curve $E : y^2 = f(x) = 4x^3 - g_2x - g_3$, and $P = (x, y)$ be a non-torsion point of $E(\mathbb{Q})$, we calculate the given sufficiently accurate approximation of the inverse image z of $\pi^{-1}(P)$.*

- `CASE 1` :$\Delta(E) > 0$ *and* $e_3 < e_2 < e_1$ *are real roots of* $f(x)$.
  1. *Set* $a_1 = \sqrt{e_1 - e_3}, b_1 = \sqrt{e_1 - e_2}$.
  2. *If P is contained in the finite component, that is* $e_3 < x < e_2$

     $$\lambda = \frac{y}{(x - e_3)}, X = \frac{\lambda^2}{4} - x - e_3$$

     Otherwise $X = x$. *Finally set* $c_1 = \sqrt{X - e_3}$.
  3. *Compute* $a_{n+1} = \frac{1}{2}(a_n + b_n), b_{n+1} = \sqrt{a_n b_n}, c_{n+1} = \frac{1}{2}(c_n + \sqrt{c_n^2 + b_n^2 - a_n^2})$.
  4. *If* $a = \lim a_n, c = \lim c_n$ *then*

     $$z = \begin{cases} \frac{1}{a}\sin^{-1}(\frac{a}{c}), & \textit{if } y \geq 0 \textit{ and } x \geq e_1 \\ \omega_1 - \frac{1}{a}\sin^{-1}(\frac{a}{c}), & \textit{if } y < 0 \textit{ and } x > e_1 \\ \frac{1}{a}\sin^{-1}(\frac{a}{c}) + \frac{1}{2}w_2, & \textit{if } y < 0 \textit{ and } e_3 < x < e_2 \\ \omega_1 - \frac{1}{a}\sin^{-1}(\frac{a}{c}) + \frac{1}{2}w_2, & \textit{if } y \geq 0 \textit{ and } e_3 < x \leq e_2 \end{cases}$$

- `CASE 2` : $\Delta(E) < 0$ *and e is the unique real root of* $f(x)$.
  1. *Set* $\alpha = 3e, \beta = \sqrt{3e^2 - \frac{g_2}{4}}, a_1 = 2\sqrt{\beta}, b_1 = \sqrt{2\beta + \alpha}, c_1 = \frac{(x-e+\beta)}{\sqrt{x-e}}$
  2. *Compute* $a_{n+1} = \frac{1}{2}(a_n + b_n), b_{n+1} = \sqrt{a_n b_n}, c_{n+1} = \frac{1}{2}(c_n + \sqrt{c_n^2 + b_n^2 - a_n^2})$.
  3. *If* $a = \lim a_n, c = \lim c_n$ *then*

     $$z = \begin{cases} \frac{1}{a}\sin^{-1}(\frac{a}{c}), & \textit{if } y < 0 \textit{ and } (x-e)^2 - \beta^2 > 0 \\ \frac{1}{2}\omega_1 - \frac{1}{a}\sin^{-1}(\frac{a}{c}), & \textit{if } y < 0 \textit{ and } (x-e)^2 - \beta^2 \leq 0, \textit{ or } y = 0 \\ \frac{1}{2}\omega_1 + \frac{1}{a}\sin^{-1}(\frac{a}{c}), & \textit{if } y > 0 \textit{ and } (x-e)^2 - \beta^2 < 0 \\ \omega_1 - \frac{1}{a}\sin^{-1}(\frac{a}{c}), & \textit{if } y > 0 \textit{ and } (x-e)^2 - \beta^2 \geq 0 \end{cases}$$

By the above algorithm, we can decide the distribution of S.

`Case 1 :` Assume that $\Delta(E) > 0$ and P is a non-torsion point of $E(\mathbb{Q})$. Let

$$V = \{\alpha_1\omega_1 | 0 \leq \alpha_1 \leq 1\}.$$

Then $\pi^{-1}(E(\mathbb{R})) = V \cup V + \frac{1}{2}\omega_2$ and V is the inverse image of the infinite component. If P is contained in the infinite component, then $z = \alpha_1\omega_1$ for some irrational number α_1 since P is non-torsion. Hence $\pi^{-1}(S) \subset V$ and it is dense in V. Moreover it is uniformly distributed. Therefore S is dense in the infinite component and uniformly distributed.

If P is contained in the finite component, then $z = \alpha_1\omega_1 + \frac{1}{2}\omega_2$ for some irrational number α_1 since P is non-torsion. In this case $\{2kz/\Lambda | k \in \mathbb{Z}\}$ is dense in V and $\{(2k-1)z/\Lambda | k \in \mathbb{Z}\}$ is dense in $V + \frac{1}{2}\omega_2$. And they are uniformly distributed respectively. Therefore S is dense in the whole component of $E(\mathbb{R})$ and uniformly distributed. In particular $\{[2k]P | k \in \mathbb{Z}\}$ is dense in the infinite component and $\{[2k-1]P | k \in \mathbb{Z}\}$ is dense in the finite component.

`Case 2 :` Assume that $\Delta(E) < 0$ and P is a non-torsion point of $E(\mathbb{Q})$. Then $\pi^{-1}(E(\mathbb{R})) = V$ and $z = \alpha_1\omega_1$ for some irrational number α_1 since P is non-torsion. Since $\{kz/\Lambda | k \in \mathbb{Z}\}$ is dense in V and uniformly distributed, S is dense in $E(\mathbb{R})$ and uniformly distributed.

So we get

Proposition 2. *Suppose that $E/\mathbb{Q}$ is an elliptic curve defined over the rationals, P is a non-torsion rational point of E. Then the set S is dense in the component of $E(\mathbb{R})$ which contains the infinity and uniformly distributed.*

Example. Let $E : y^2 = 4x^3 - 624x + 2240$ and $P_1 = (13, 54), P_2 = (2, 32) \in E(\mathbb{Q})$, hence P_1 is contained in the infinite component and P_2 is contained the finite component.

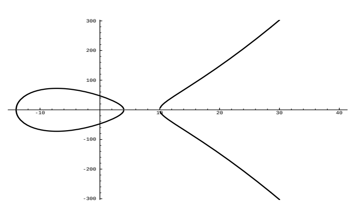

FIGURE 1. $E : y^2 = 4x^3 - 624x + 2240$

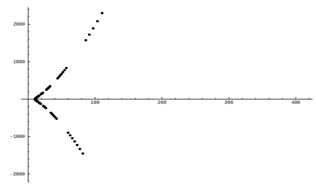

FIGURE 2. $[n]P_1$ points $(1 \leq n \leq 140)$

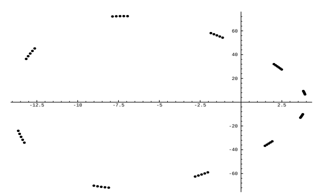

FIGURE 3. $[2n-1]P_2$ points $(1 \leq n \leq 51)$

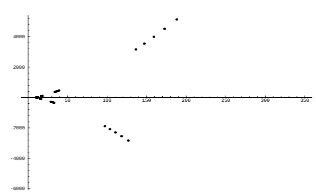

FIGURE 4. $[2n]P_2$ points $(1 \leq n \leq 50)$

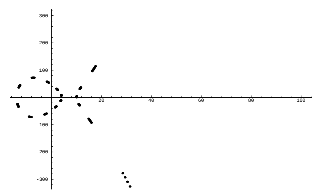

FIGURE 5. $[n]P_2$ points $(1 \leq n \leq 101)$

REFERENCES

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.
[2] A. Knapp, *Elliptic Curves*, Princeton University Press, 1992.
[3] J. Silverman, *The Arithmetic of Elliptic Curves*,Springer-Verlag, 1986.
[4] A. Schidlovski ,*Transcendental Numbers*, Walter de Gruyter , 1989.
[5] R. Tijdeman , *On the Gel'fond-Baker method and its applications* , Proc. Sympo. Pure Math. **28**(1976), 242–268.

Department of Mathematics
KAIST
Taejon, 305-701 KOREA
E-mail: sghahn@mathx.kaist.ac.kr

National Security Research Institute (NSRI)
Taejon 305-350, KOREA
e-mail : dlee@etri.re.kr