Armenian Journal of Mathematics
Volume 12, Number 5, 2020, 1–9

Canonical heights on Pell conics over number fields

M. Okazaki

Abstract. In [2], Lemmermeyer introduced the canonical heights on the groups of rational points on Pell conics, which are analogues of the canonical heights on elliptic curves. In this paper, we generalize this: We introduce the canonical heights on the groups of $\overline{\mathbb{Q}}$-rational points on Pell conics over number fields.

Key Words: canonical height, Pell conic
Mathematics Subject Classification 2010: Primary 11G50, Secondary 11D09, 14G05, 14H50, 20G30

Introduction

Let K be a number field, E be an elliptic curve over K, and $E(\overline{\mathbb{Q}})$ be the set of $\overline{\mathbb{Q}}$-rational points on E. It is well known that $E(\overline{\mathbb{Q}})$ is an abelian group. To study the group $E(\overline{\mathbb{Q}})$, it is useful to define a good function that measures a certain kind of arithmetic complexity of $P \in E(\overline{\mathbb{Q}})$. This function is called the *canonical height*, defined by

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{4^n},$$

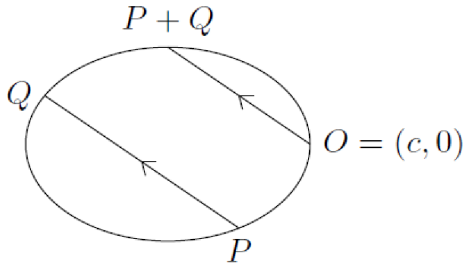
where $h(Q) := h(1, x(Q))$ for each $Q = (x(Q), y(Q)) \in E(\overline{\mathbb{Q}})$, and h is the logarithmic Weil height on the projective line $\mathbb{P}^1(\overline{\mathbb{Q}})$ (we will recall the definition of h in Section 1).

We set a *Pell conic* $C : X^2 - dY^2 = c^2$, where $c, d \in K$. We denote by $C(F)$ the set of F-rational points on C, where $F \subset \overline{\mathbb{Q}}$ is any subfield with $K \subset F$. For each $P = (x(P), y(P)), Q = (x(Q), y(Q)) \in C(F)$, we set

$$P + Q := \left(\frac{x(P)x(Q) + dy(P)y(Q)}{c}, \frac{x(P)y(Q) + x(Q)y(P)}{c} \right).$$

Under this binary operation $+$, $C(F)$ becomes an abelian group. The zero of $C(F)$ is $O = (c, 0)$ and $-(x, y) = (x, -y)$. $P + Q$ is the intersection of C

and the line which is through O and is parallel to the line PQ. If $Q = P$, then we regard the line PP as the tangent line of C at P. Thus, if $F \subset \mathbb{R}$, we can describe the addition as follow (see, *e.g.,* [2], [3], [4], [6]):



This figure implies that the addition of Pell conics is analogous to that of elliptic curves.

In [2], Lemmermeyer introduced an analogue of the canonical height $\hat{h}$ for Pell conics over $\mathbb{Q}$:

$$\tilde{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{2^n},$$

where $h(Q) := h(1, x(Q))$ for each rational point Q on the Pell conic. In this paper, we generalize this canonical heights to C, a Pell conic over a number field:

Theorem 1 (Canonical heights on Pell conics over $\overline{\mathbb{Q}}$) *For each $P \in C(\overline{\mathbb{Q}})$, set $h(P) := h(1, x(P))$.*

1. The limit

$$\tilde{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n}$$

does exist.

2. Fix $\sqrt{d} \in \overline{\mathbb{Q}}$ and set the group isomorphism

$$\varphi : C(\overline{\mathbb{Q}}) \ni (x, y) \longmapsto \frac{x + \sqrt{d}y}{c} \in \overline{\mathbb{Q}}^{\times}.$$

Then

$$\tilde{h}(P) = 2h(1, \varphi(P)).$$

We call $\tilde{h}$ the *canonical height on C*.

Further, we give some applications of Theorem 1 in Section 4: We will study the group $C(\overline{\mathbb{Q}})$ by using Theorem 1.

1 The Weil height

In this section, we recall the definition of the classical Weil height and summarize some basic properties of it which we will use later. Throughout the section, we employ the following notation:

- $\mathcal{O}_K$: the ring integers of K;
- $\mathcal{M}_K^0$: the set of all non-zero prime ideals of $\mathcal{O}_K$;
- $\mathcal{M}_K^\infty$: the set of all field homomorphisms from K to $\mathbb{C}$;
- $\mathcal{M}_K := \mathcal{M}_K^0 \cup \mathcal{M}_K^\infty$.

Let $v \in \mathcal{M}_K$ and $x \in K$. We set an absolute value $|\cdot|_v$ as

$$|x|_v := \begin{cases} \#(\mathcal{O}_K/v)^{-\mathrm{ord}_v(x)}, & v \in \mathcal{M}_K^0, \\ |v(x)|, & v \in \mathcal{M}_K^\infty, \end{cases}$$

where $\mathrm{ord}_v(x)$ is the order of $x \in K$ for each $v \in \mathcal{M}_K^0$, *i.e.*, if $x \neq 0$ and $(x) = \prod_{k=1}^n v_k^{e_k}$ is the prime factorization, then

$$\mathrm{ord}_v(x) := \begin{cases} e_k, & v = v_k \text{ for some } k, \\ 0, & v \neq v_k \text{ for any } k, \end{cases}$$

and $\mathrm{ord}_v(0) := \infty$ for all $v \in \mathcal{M}_K^0$. We note that $|\cdot|_v$ satisfies the product formula

$$\prod_{v \in \mathcal{M}_K} |x|_v = 1 \quad \text{for all } x \in K^\times.$$

For $(x_0, \ldots, x_n) \in K^{n+1}$, we set

$$h(x_0, \ldots, x_n) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} \log \max_{0 \leq i \leq n} \{|x_i|_v\}.$$

It is known that the value of $h(x_0, \ldots, x_n)$ is independent of the choice of K and, by the product formula, $h(cx_1, \ldots, cx_n) = h(x_0, \ldots, x_n)$ for all $c \in \overline{\mathbb{Q}}^\times$. Thus we can consider h to be a function on the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$. The function h is called the *logarithmic Weil height*.

Lemma 1 *Let $x, x_1, \ldots, x_n \in \overline{\mathbb{Q}}$ and $p, p_1, \ldots, p_n \in \mathbb{N}$ with $p_1 \leq \ldots \leq p_n$. Then:*

1. $h(1, x_1^p, \ldots, x_n^p) = p h(1, x_1, \ldots, x_n)$;
2. $h(1, x^{p_1}, \ldots, x^{p_n}) = h(1, x^{p_n})$;
3. $h(1, x_1 \cdot \ldots \cdot x_n) \leq h(1, x_1) + \cdots + h(1, x_n)$.

Proof. Fix an algebraic number field K such that $x, x_1, \ldots, x_n \in K$. Let $v \in \mathcal{M}_K$.

1. This is clear since
$$\max\{|1|_v, |x_1^p|_v, \ldots, |x_n^p|_v\} = \max\{|1|_v, |x_1|_v, \ldots, |x_n|_v\}^p.$$
2. If $|x|_v \leq 1$, then $|x|_v^{p_i} \leq 1$ for all $1 \leq i \leq n$. Hence we have
$$\max\{1, |x|_v^{p_1}, \ldots, |x|_v^{p_n}\} = 1 = \max\{1, |x|_v^{p_n}\}.$$
If $|x|_v > 1$, then $|x|_v^{p_i} \leq |x|_v^{p_n}$ for all $1 \leq i \leq n$, and therefore
$$\max\{1, |x|_v^{p_1}, \ldots, |x|_v^{p_n}\} = |x|_v^{p_n} = \max\{1, |x|_v^{p_n}\}.$$
3. The inequality holds since
$$\begin{aligned}\max\{|1|_v, |x_1 \cdot \ldots \cdot x_n|_v\} &= \max\{|1|_v, |x_1|_v \cdot \ldots \cdot |x_n|_v\} \\ &\leq \max\{|1|_v, |x_1|_v\} \cdot \ldots \cdot \max\{|1|_v, |x_n|_v\}.\end{aligned}$$

These complete the proof. □

Now we recall the definition of a morphism between projective spaces: A map $F : \mathbb{P}^m(\overline{\mathbb{Q}}) \to \mathbb{P}^n(\overline{\mathbb{Q}})$ is called a *morphism of degree d between projective spaces* if there exist homogeneous polynomials $F_0, F_1, \ldots, F_n \in \overline{\mathbb{Q}}[X_0, X_1, \ldots, X_m]$ of degree d such that $F(P) = (F_0(P), F_1(P), \ldots, F_n(P))$ for each $P \in \mathbb{P}^m(\overline{\mathbb{Q}})$ and $F_0(x_0, x_1, \ldots, x_m) = F_1(x_0, x_1, \ldots, x_m) = \cdots = F_n(x_0, x_1, \ldots, x_m) = 0$ implies that $x_0 = x_1 = \cdots = x_m = 0$. We shall frequently use the following fact:

Fact 1 ([5], p227, Theorem 5.6) *Let $F : \mathbb{P}^m(\overline{\mathbb{Q}}) \to \mathbb{P}^n(\overline{\mathbb{Q}})$ be a morphism of degree d between projective spaces. Then there exists a constant $C > 0$ such that for all $P \in \mathbb{P}^m(\overline{\mathbb{Q}})$,*
$$|h(F(P)) - dh(P)| \leq C.$$

Corollary 1 *Let $f_1(t), \ldots, f_n(t)$ be polynomials over $\overline{\mathbb{Q}}$ of degree d. Then there exists a constant $C > 0$ such that for all $x \in \overline{\mathbb{Q}}$,*
$$|h(1, f_1(x), \ldots, f_n(x)) - dh(1, x)| \leq C.$$

Proof. For each $1 \leq i \leq n$, we write
$$f_i(t) := a_{i0} + a_{i1}t + \cdots + a_{id}t^d, \quad (a_{id} \neq 0)$$
and set
$$F_i(t, u) := a_{i0}u^d + a_{i1}tu^{d-1} + \cdots + a_{id}t^d.$$
Then we know that
$$F : \mathbb{P}^1(\overline{\mathbb{Q}}) \ni [x : y] \longmapsto [y^d : F_1(x, y) : \cdots : F_n(x, y)] \in \mathbb{P}^n(\overline{\mathbb{Q}})$$
is a morphism of projective spaces of degree d. Thus we have
$$dh(1, x) - C \leq h(F([1 : x]) = h(1, f_1(x), \ldots, f_n(x)) \leq dh(1, x) + C$$
for a constant $C > 0$ in Fact 1. □

2 The naive height on C

In the statement of Theorem 1, we set

$$h(P) := h(1, x(P))$$

for each $P = (x(P), y(P)) \in C(\overline{\mathbb{Q}})$. We call this the *naive height on* C, as is the same case with elliptic curves.

The following lemma plays a crucial role in the proof of Theorem 1:

Lemma 2 *There exists a constant $D > 0$ such that for all $P \in C(\overline{\mathbb{Q}})$,*

$$|h(P) - 2h(1, \varphi(P))| \leq D,$$

where φ is the isomorphism in the statement of Theorem 1.

Proof. First, we consider φ to be the composition of some maps. We set:

$$\begin{aligned}
&\iota : C(\overline{\mathbb{Q}}) \ni (x, y) \longmapsto [x : y : 1] \in \mathbb{P}^2(\overline{\mathbb{Q}});\\
&F : \mathbb{P}^2(\overline{\mathbb{Q}}) \ni [x : y : z] \longmapsto [x + y\sqrt{d} : x - y\sqrt{d} : cz] \in \mathbb{P}^2(\overline{\mathbb{Q}});\\
&\pi : U \ni [u : v : w] \longmapsto u/w \in \overline{\mathbb{Q}}^{\times},
\end{aligned}$$

where $U := \{\, [u : v : w] \in \mathbb{P}^2(\overline{\mathbb{Q}}) \mid uv = w^2, w \neq 0 \,\}$. We can easily check that $F \circ \iota(C(\overline{\mathbb{Q}})) \subset U$ and $\varphi = \pi \circ F \circ \iota$: The following commutative diagram holds:

$$\begin{array}{ccc}
C(\overline{\mathbb{Q}}) & \xrightarrow{\varphi} & \overline{\mathbb{Q}}^{\times} \\
{\scriptstyle \iota}\downarrow & & \uparrow{\scriptstyle \pi} \\
\mathbb{P}^2(\overline{\mathbb{Q}}) & \xrightarrow[F]{} & U
\end{array} \tag{2.1}$$

By Corollary 1, there exists a constant $C_1 > 0$ such that for all $x \in \overline{\mathbb{Q}}$,

$$\left| h\left(1, x^2, \frac{x^2 - c^2}{d}\right) - 2h(1, x) \right| \leq C_1.$$

Now, note that for all $P \in C(\overline{\mathbb{Q}})$, it holds that $y(P)^2 = \dfrac{x(P)^2 - c^2}{d}$. Hence we have

$$\begin{aligned}
h\left(1, x(P)^2, \frac{x(P)^2 - c^2}{d}\right) &= h(1, x(P)^2, y(P)^2) \\
&= 2h(1, x(P), y(P)) \qquad \text{(by Lemma 1.1)} \\
&= 2h(\iota(P)).
\end{aligned}$$

Thus we obtain

$$|h(P) - h(\iota(P))| \leq C_2, \tag{2.2}$$

where $C_2 := C_1/2$.

Clearly, F is a morphism of degree 1 between projective planes. Therefore, by Fact 1, there exists a constant $C_3 > 0$ such that for all $A \in \mathbb{P}^2(\overline{\mathbb{Q}})$,

$$|h(A) - h(F(A))| \leq C_3. \tag{2.3}$$

For all $[u : v : w] \in U$, it holds that $v = w^2/u$. Therefore,

$$\begin{aligned} h(u, v, w) &= h\left(\left(\frac{u}{w}\right)^2, 1, \frac{u}{w}\right) \\ &= h\left(1, \left(\frac{u}{w}\right)^2\right) && \text{(by Lemma 1.2)} \\ &= 2h\left(1, \frac{u}{w}\right) && \text{(by Lemma 1.1)} \\ &= 2h(1, \pi([u : v : w])). && (2.4) \end{aligned}$$

Finally, for all $P \in C(\overline{\mathbb{Q}})$, we have

$$\begin{aligned} &|h(P) - 2h(\varphi(P))| \\ &\leq |h(P) - h(\iota(P))| + |h(\iota(P)) - h(F \circ \iota(P))| \\ &\quad + |h(F \circ \iota(P)) - 2h(1, \varphi(P))| \\ &\leq C_2 + C_3 + |2h(1, \pi \circ F \circ \iota(P)) - 2h(1, \varphi(P))| && \text{(by (2.2), (2.3), (2.4))} \\ &= C_2 + C_3. && \text{(by (2.1))} \end{aligned}$$

Therefore, setting $D := C_2 + C_3$, we complete the proof. □

3 The canonical height on C

In this section, first, we shall prove Theorem 1:

Proof. Let $n \in \mathbb{N}$ and $P \in C(\overline{\mathbb{Q}})$. Since φ is a group isomorphism, we have

$$\begin{aligned} h(1, \varphi(nP)) &= h(1, \varphi(P)^n) \\ &= nh(1, \varphi(P)). && \text{(by Lemma 1.1)} \end{aligned}$$

Thus, for a positive constant $D > 0$ in Lemma 2,

$$\lim_{n\to\infty} \left| \frac{h(nP)}{n} - 2h(1, \varphi(P)) \right| \leq \lim_{n\to\infty} \frac{D}{n} = 0.$$

This completes the proof. □

Further, we will give some corollaries of Theorem 1.

Corollary 2 *For all $P \in C(\overline{\mathbb{Q}})$ and $m \in \mathbb{N}$, it holds that*

$$\tilde{h}(mP) = m\tilde{h}(P).$$

Proof. Indeed,

$$\tilde{h}(mP) = \lim_{n\to\infty} \frac{h(nmP)}{n} = m \lim_{n\to\infty} \frac{h(mnP)}{mn} = m\tilde{h}(P).$$

□

Next, we will show that $\tilde{h}$ satisfies the subadditivity:

Corollary 3 *For all $P, Q \in C(\overline{\mathbb{Q}})$, it holds that*

$$\tilde{h}(P+Q) \leq \tilde{h}(P) + \tilde{h}(Q).$$

Proof. Since φ is a group isomorphism, we can write

$$\begin{aligned}
\tilde{h}(P+Q) &= 2h(1, \varphi(P+Q)) && \text{(by Theorem 1.2)} \\
&= 2h(1, \varphi(P)\varphi(Q)) \\
&\leq 2h(1, \varphi(P)) + 2h(1, \varphi(Q)) && \text{(by Lemma 1.3)} \\
&= \tilde{h}(P) + \tilde{h}(Q). && \text{(by Theorem 1.2)}
\end{aligned}$$

□

Finally, we will show that $C(K)$ has a kind of finiteness property relative to $\tilde{h}$:

Corollary 4 *1. There exists a constant $D > 0$ such that for all $P \in C(\overline{\mathbb{Q}})$,*

$$|\tilde{h}(P) - h(P)| \leq D;$$

2. For all algebraic number field K and constant $C > 0$, the set

$$\{\, P \in C(K) \mid \tilde{h}(P) \leq C \,\}$$

is a finite set.

Proof. 1. This immediately follows from Lemma 2 and Theorem 1.2.

2. This immediately follows from 1 and the Northcott finiteness theorem; see, *e.g.,* [1], Theorem 1.6.8. □

Remark. Corollary 4.2 holds not only for the algebraic number fields but also for the fields with the Northcott property; see, *e.g.,* [1], p117.

4 Two applications

In this section, we will apply Theorem 1 and its corollaries to study the group $C(\overline{\mathbb{Q}})$. However, what we will do in this section are only routines; we can see the same discussions in most of the books on elliptic curves (see, *e.g.,* [5]).

First, as a simple application, we give a criterion for torsion points:

Proposition 1 *$P \in C(\overline{\mathbb{Q}})$ is a torsion point if and only if $\tilde{h}(P) = 0$.*

Proof. Suppose that P is a torsion point. Then there are only finitely many possibilities for the value of $h(nP)$. Thus, $\tilde{h}(P) = 0$.

Conversely, suppose that $\tilde{h}(P) = 0$. Fix an algebraic number field K such that $c, d, x(P), y(P) \in K$. Note that $x(mP), y(mP) \in K$ for all $m \in \mathbb{N}$. By Corollary 2, we have

$$\tilde{h}(mP) = m\tilde{h}(P) = 0.$$

According to Corollary 4.2, the set

$$\Omega_0 := \{\, Q \in C(K) \mid h(Q) = 0 \,\}$$

is finite. Therefore, $\{\, mP \mid m \in \mathbb{N} \,\} \subset \Omega_0$ is also a finite set. Thus, for some $k \in \mathbb{N}$, it holds that $kP = O$. □

Next, we will apply the subadditivity of $\tilde{h}$ to decent.

Proposition 2 *Assume that the weak Mordell–Weil theorem holds for a subgroup $G \subset C(\overline{\mathbb{Q}})$, i.e., for some natural number $m \geq 2$, it holds that $\#(G/mG) < \infty$. Then G is finitely generated.*

Proof. Let $\Gamma := \{Q_1, \ldots, Q_r\}$ be a complete system of representatives of G/mG, $M := \max_{1 \leq i \leq r}\{\tilde{h}(Q_i)\}$, and $\Omega := \{\, R \in G \mid \tilde{h}(R) \leq 1 + M \,\}$. Note that Ω is a finite set by Corollary 4.2. We claim that G is generated by $\Omega \cup \Gamma$. Take any $P = P_0 \in G$. Then there exist $1 \leq i_1 \leq r$ and $P_1 \in G$ such that $P_0 - Q_{i_1} = mP_1$. Repeating this, we have $\{P_0, \ldots, P_n\}$ and $\{i_1, \ldots, i_n\}$ with

$$P_{j-1} - Q_{i_j} = mP_j \quad (\text{for all } 1 \leq j \leq n) \tag{4.1}$$

for each $n \in \mathbb{N}$. Further,

$$\begin{aligned} \tilde{h}(P_j) &= \frac{1}{m}\tilde{h}(P_{j-1} - Q_{i_j}) && (\text{by Corollary 2}) \\ &\leq \frac{1}{m}(\tilde{h}(P_{j-1}) + \tilde{h}(Q_{i_j})) && (\text{by Corollary 3}) \\ &\leq \frac{1}{2}(\tilde{h}(P_{j-1}) + M). && (4.2) \end{aligned}$$

Using (4.2) repeatedly, we obtain

$$\tilde{h}(P_n) \leq \left(\frac{1}{2}\right)^n \tilde{h}(P) + M.$$

Letting n be sufficiently large such that $\left(\frac{1}{2}\right)^n \tilde{h}(P) \leq 1$, we achieve $P_n \in \Omega$. By (4.1), we have

$$P = P_0 = 2^n P_n + (Q_{i_1} + 2Q_{i_2} + \cdots + 2^{n-1}Q_{i_n}) \in \langle \Omega \cup \Gamma \rangle.$$

This completes the proof. □

Acknowledgement

I thank my advisor Yuichiro Takeda for his continued support. I am also grateful to the anonymous referee for reading my draft carefully and giving me valuable comments.

References

[1] E. Bombieri and W. Gubler, Heights in Diophantine Geometry, New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006.

[2] F. Lemmermeyer, *Higher descent on Pell conics. III. The first 2-descent*, preprint, available at: https://arxiv.org/abs/math/0311310

[3] P. Shastri, *Integral points on the unit circle*, J. Number Theory **91** (2001), no. 1, 67–70.

[4] S. A. Shirali, *Groups associated with conics*, Math. Gaz. **93** (2009), no. 526, 27–41.

[5] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[6] L. Tan, *The group of rational points on the unit circle*, Math. Mag. **69** (1996), no. 3, 163–171.

Masao Okazaki
Graduate School of Mathematics,
Kyushu University
Motooka 744, Nishi-ku, Fukuoka 819-0395, Japan.
m-okazaki@math.kyushu-u.ac.jp

Please, cite to this paper as published in
Armen. J. Math., V. **12**, N. 5(2020), pp. 1–9