BULLETIN OF THE
HELLENIC MATHEMATICAL SOCIETY
Volume 67, 2023 (59–72)

IMAGINARY QUADRATIC INTEGRAL POINTS ON A HYPERELLIPTIC CURVE OF CERTAIN TYPE

TORU KOMATSU

Abstract. In this paper we show that a hyperelliptic curve of certain type has only finitely many imaginary quadratic integral points, and also give an effective algorithm to determine all the imaginary quadratic integral points on the curve.

1. Introduction

For a subfield K of $\mathbb{C}$ we say that K is a number field if K is an algebraic extension of $\mathbb{Q}$ with finite degree. For a number field K let O_K denote the ring of all algebraic integers contained in K. For a polynomial $F(x)$ over $\mathbb{C}$ of positive degree let A_F be the algebraic curve defined by $Y^2 = F(X)$, and $A_F(R)$ be the set $\{(x, y) \in R \times R \mid y^2 = F(x)\}$ for a subring R of $\mathbb{C}$. For a polynomial $F(X) \in \mathbb{C}[X]$ we call $F(X)$ *nonsquare* if $F(X)$ is not the square of any polynomial over $\mathbb{C}$. Tzanakis [6], Poulakis [3] and Szalay [4] gave algorithms to calculate $A_F(\mathbb{Z})$ for a monic and nonsquare polynomial $F(X)$ over $\mathbb{Z}$ with even degree. In this paper we generalize their results to the cases of imaginary quadratic fields.

We prepare some invariants of a polynomial. For a polynomial $g(X)$ over $\mathbb{C}$ with positive degree m of the form $g(X) = g_m X^m + \cdots + g_1 X + g_0$, we define the *height* $\mathrm{ht}(g)$, the *subheight* $\mathrm{ht}'(g)$ and the *leading coefficient* $\ell(g)$ of $g(X)$ by $\mathrm{ht}(g) = \max\{|g_j| \mid 0 \le j \le m\}$, $\mathrm{ht}'(g) = \max\{|g_j| \mid 0 \le j < m\}$ and $\ell(g) = g_m$. For a constant polynomial $g(X) = g_0 \in \mathbb{C}$, we define $\mathrm{ht}(g) = |g_0|$, $\mathrm{ht}'(g) = 0$ and $\ell(g) = g_0$. For a polynomial $g(X)$ over $\mathbb{C}$ with positive degree, we define the *radius* $\mathrm{rad}(g)$ of $g(X)$ by $\mathrm{rad}(g) = 1 + \mathrm{ht}'(g)/|\ell(g)| \ge 1$.

Let $F(X)$ be a monic and nonsquare polynomial over $\mathbb{Z}$ with even degree $2k$. Due to Lemma 2.1 below there exist unique polynomials $B(X)$ and $C(X)$ over $\mathbb{Q}$ such that $B(X)$ is monic, $\deg(C(X)) \le k - 1$ and $F(X) = B(X)^2 + C(X)$. Let α be the least positive integer for which $\alpha B(X) \in \mathbb{Z}[X]$ as described by Szalay at §2 in [5]. Now put $r_F = 1 + \mathrm{ht}'(B) + \alpha\,\mathrm{ht}(C)$, $\tilde{r}_F = \max\{r_F, \mathrm{rad}(C)\}$ and $\mu_F = \min(\{F(s) \mid s \in \mathbb{Z}\} \cup \{0\})$. We define an important invariant δ_F of $F(X)$ by $\delta_F = \max\{4\tilde{r}_F^2, 4|\mu_F|\}$.

Theorem 1.1. *Let $F(X)$ be a monic and nonsquare polynomial over $\mathbb{Z}$ with even degree. Then there exist only finitely many imaginary quadratic fields K such that $A_F(O_K) \ne A_F(\mathbb{Z})$. More precisely, every imaginary quadratic field K with discriminant D_K of which absolute value $|D_K|$ greater than the invariant δ_F satisfies $A_F(O_K) = A_F(\mathbb{Z})$.*

Date: Received 30 March 2023. Accepted 6 September 2023.
2020 *Mathematics Subject Classification.* 11D41,11G30,11R11.
Key words and phrases. Hyperelliptic curve, Integral point, Imaginary quadratic field.

We present not only the invariant δ_F but also an algorithm to determine the sets $A_F(O_K)$ for all the imaginary quadratic fields K. In section 2 we prove Theorem 1.1 with δ_F. Our proof is elementary. In section 3 we give an algorithm to determine $A_F(O_K)$ over all imaginary quadratic fields K. In section 4 we exhibit numerical examples. In section 5 we describe a bit of generalization.

2. Effective bound for imaginary quadratic integral points

We recall the normal form of a polynomial introduced by Szalay.

Lemma 2.1 (Szalay [4, §4], Szalay [5, §2 Lemma])**.** *Assume that p and k are rational integers with $p \geq 2$ and $k \geq 1$, and $F(X) = X^{kp} + a_{kp-1}X^{kp-1} + \cdots + a_0$ is a polynomial over $\mathbb{Z}$. Then there exist unique polynomials $B(X) = X^k + b_{k-1}X^{k-1} + \cdots + b_0 \in \mathbb{Q}[X]$ and $C(X) \in \mathbb{Q}[X]$ with $\deg(C(X)) \leq kp - k - 1$ for which $F(X) = B(X)^p + C(X)$.*

Let $F(X)$ be a monic and nonsquare polynomial over $\mathbb{Z}$ of the form $F(X) = X^{2k} + a_{2k-1}X^{2k-1} + \cdots + a_0$. As in the Introduction, let A_F be the algebraic curve defined by $Y^2 = F(X)$, and $A_F(R)$ the set $\{(x, y) \in R \times R \mid y^2 = F(x)\}$ for a subring R of $\mathbb{C}$. Due to Lemma 2.1 there exist unique polynomials $B(X)$ and $C(X)$ over $\mathbb{Q}$ such that $B(X)$ is monic, $\deg(C(X)) \leq k - 1$ and $F(X) = B(X)^2 + C(X)$. Note that $C(X) \neq 0$ since $F(X)$ is nonsquare. Instead of $A_F(R)$, we consider its subset $A_F^+(R)$ such that

$$A_F^+(R) = \{(x, y) \in A_F(R) \mid |y + B(x)| \geq |y - B(x)|\}.$$

Then one has $A_F(R) = A_F^+(R) \cup A_F^-(R)$ where $A_F^-(R) = \{(x, -y) \mid (x, y) \in A_F^+(R)\}$.

To state an evaluation for the points in $A_F^+(R)$ we prepare some notation. For a real number $\rho > 0$ let $\mathfrak{B}(\rho)$ denote the open ball of radius ρ centered at 0 in $\mathbb{C}$, that is, the set of all the complex numbers z with absolute values $|z|$ less than ρ. Then we have

Theorem 2.2. *Let (x, y) be a point in $A_F^+(\mathbb{C})$, and c a positive number. Then $y - B(x)$ belongs to $\mathfrak{B}(c)$ or x belongs to $\mathfrak{B}(r)$ where $r = 1 + \mathrm{ht}'(B) + \mathrm{ht}(C)/c$.*

To prove Theorem 2.2 we use the following lemma.

Lemma 2.3 (Borwein–Erdélyi [1, Theorem 1.2.1])**.** *For a polynomial $g(X)$ over $\mathbb{C}$ with positive degree, every zero of $g(X)$ belongs to $\mathfrak{B}(\mathrm{rad}(g))$.*

Lemma 2.4. *Let $p(X)$ and $q(X)$ be polynomials over $\mathbb{C}$ with $\deg(p) > \deg(q)$, and c a positive number. If a complex number z satisfies $c|p(z)| \leq |q(z)|$, then z belongs to $\mathfrak{B}(r_{p,q,c})$ where $r_{p,q,c} = 1 + (\mathrm{ht}'(p) + \mathrm{ht}(q)/c)/|\ell(p)|$.*

Proof. Assume that $z \in \mathbb{C}$ and $c > 0$ satisfy $c|p(z)| \leq |q(z)|$. Then there exists a complex number κ with $|\kappa| \leq 1$ such that $cp(z) - \kappa q(z) = 0$. Put $g(X) = cp(X) - \kappa q(X) \in \mathbb{C}[X]$. It follows from $\deg(p) > \deg(q)$ and $c > 0$ that $\mathrm{ht}'(g) \leq c\,\mathrm{ht}'(p) + |\kappa|\mathrm{ht}(q) \leq c\,\mathrm{ht}'(p) + \mathrm{ht}(q)$ and $\ell(g) = c\ell(p)$. Thus one has

$$\mathrm{rad}(g) = 1 + \frac{\mathrm{ht}'(g)}{|\ell(g)|} \leq 1 + \frac{\mathrm{ht}'(p) + \mathrm{ht}(q)/c}{|\ell(p)|} = r_{p,q,c}.$$

Since $g(z) = 0$, Lemma 2.3 shows that $z \in \mathfrak{B}(\mathrm{rad}(g)) \subset \mathfrak{B}(r_{p,q,c})$. □

Proof of Theorem 2.2. Assume $(x, y) \in A_F^+(\mathbb{C})$. By $|y + B(x)| \geq |y - B(x)|$, one has $|y + B(x)| \geq |B(x)|$. It follows from $(x, y) \in A_F(\mathbb{C})$ that $C(x) = (y+B(x))(y-B(x))$. Now assume that $y - B(x) \notin \mathfrak{B}(c)$. Then one has $|y - B(x)| \geq c$ and $|C(x)| = |y + B(x)||y - B(x)| \geq c|B(x)|$. Lemma 2.4 shows that $x \in \mathfrak{B}(r)$ where $r = 1 + \mathrm{ht}'(B) + \mathrm{ht}(C)/c$. Indeed, $\ell(B)$ is equal to 1. Hence it satisfies that $y - B(x) \in \mathfrak{B}(c)$ or $x \in \mathfrak{B}(r)$. □

Through this section let K be an imaginary quadratic field with discriminant D_K.

Lemma 2.5. *We have* $O_K \cap \mathfrak{B}(1) = \{0\}$ *and* $O_K \cap \mathfrak{B}(\sqrt{|D_K|}/2) \subset \mathbb{Z}$.

Proof. If $z \in O_K \cap \mathfrak{B}(1)$, then the norm $N_{K/\mathbb{Q}}(z) = z\bar{z}$ of z from K to $\mathbb{Q}$ is a rational integer with $0 \leq N_{K/\mathbb{Q}}(z) < 1$ where $\bar{z}$ is the complex conjugate of z. Thus we have $N_{K/\mathbb{Q}}(z) = 0$ and $z = 0$. Assume $z \in O_K$ and $z \notin \mathbb{Z}$. When $D_K \equiv 1 \pmod 4$, one has that $|z| \geq |(1 + \sqrt{D_K})/2| > \sqrt{|D_K|}/2$. If $D_K \equiv 0 \pmod 4$, then $|z| \geq |\sqrt{D_K/4}| = \sqrt{|D_K|}/2$. Hence $z \in O_K$ and $|z| < \sqrt{|D_K|}/2$ imply $z \in \mathbb{Z}$. □

Let α be the least positive integer for which $\alpha B(X) \in \mathbb{Z}[X]$ as described by Szalay at §2 in [5]. Now put $r_F = 1 + \mathrm{ht}'(B) + \alpha\,\mathrm{ht}(C)$ and $\tilde{r}_F = \max\{r_F, \mathrm{rad}(C)\}$.

Proposition 2.6. *Let* (x, y) *be a point in* $A_F^+(O_K)$. *Then* x *is a zero of* $C(X)$ *or is contained in* $\mathfrak{B}(r_F)$. *In particular,* x *belongs to* $\mathfrak{B}(\tilde{r}_F)$.

Proof. Assume $(x, y) \in A_F^+(O_K)$. When $|y - B(x)| < 1/\alpha$, one has that $\alpha y - \alpha B(x) \in O_K \cap \mathfrak{B}(1) = \{0\}$ by Lemma 2.5. This means that $y = B(x)$ and thus $C(x) = 0$. Lemma 2.3 implies that $x \in \mathfrak{B}(\mathrm{rad}(C))$. If $|y - B(x)| \geq 1/\alpha$, then Theorem 2.2 with $c = 1/\alpha$ yields $x \in \mathfrak{B}(r_F)$. Hence x belongs to $\mathfrak{B}(\mathrm{rad}(C)) \cup \mathfrak{B}(r_F) = \mathfrak{B}(\tilde{r}_F)$. □

Now put $\mu_F = \min(\{F(s) \mid s \in \mathbb{Z}\} \cup \{0\})$ and define $\delta_F = \max\{4\tilde{r}_F^2, 4|\mu_F|\}$.

Proof of Theorem 1.1. Assume that $|D_K| > \delta_F$. Then one has that $\sqrt{|D_K|}/2 > \sqrt{\delta_F}/2 \geq \tilde{r}_F$ and $O_K \cap \mathfrak{B}(\tilde{r}_F) \subset \mathbb{Z}$ by Lemma 2.5. Let (x, y) be a point in $A_F^+(O_K)$. Proposition 2.6 yields that $x \in \mathfrak{B}(\tilde{r}_F)$ and thus $x \in \mathbb{Z}$. This means that $y^2 = F(x)$ is a rational integer. Now suppose $F(x) < 0$. Then one has that $\mu_F \leq F(x) = y^2 < 0$ and thus $|y| \leq \sqrt{|\mu_F|} \leq \sqrt{\delta_F}/2 < \sqrt{|D_K|}/2$. This implies that $y \in \mathfrak{B}(\sqrt{|D_K|}/2)$ and thus $y \in \mathbb{Z}$ by Lemma 2.5. It is contrary to the fact $y^2 < 0$. Thus one has that $F(x) \geq 0$ and $y \in \mathbb{Z}$ since $O_K \cap \mathbb{R} = \mathbb{Z}$. Hence we conclude $(x, y) \in A_F^+(\mathbb{Z})$, that is, $A_F^+(O_K) = A_F^+(\mathbb{Z})$ and $A_F(O_K) = A_F(\mathbb{Z})$. □

Remark 2.7. Note that μ_F is equal to the minimum of a finite set $\{F(s) \mid s \in \mathbb{Z} \cap \mathfrak{B}(\mathrm{rad}(F))\} \cup \{0\}$. Indeed, when $F(s) < 0$ for a rational integer s, there exist real zeros z_1 and z_2 of $F(X)$ such that $z_1 < s < z_2$ since F is monic and of even degree. Then one has $|s| \leq \max\{|z_1|, |z_2|\} < \mathrm{rad}(F)$ by Lemma 2.3. Thus every s with $F(s) < 0$ belongs to $\mathfrak{B}(\mathrm{rad}(F))$.

3. Algorithm for determining all imaginary quadratic integral points

For a monic and nonsquare polynomial $F(X)$ over $\mathbb{Z}$ with even degree, let

$$B(X), C(X), \alpha, r_F, \tilde{r}_F, \mu_F \text{ and } \delta_F$$

be as those in the previous section. Let $\square$ denote the set of all the squares of rational integers. For a subring R of $\mathbb{C}$ let $R[T,N]$ denote the polynomial ring in two indeterminates T and N over R. We define polynomials $D(T,N)$, $F_P(T,N)$ and $F_Q(T,N)$ in $\mathbb{Q}[T,N]$ such that $D(T,N) = T^2 - 4N$ and

$$F\left(\frac{T+\sqrt{T^2-4N}}{2}\right) = \frac{F_P(T,N) + F_Q(T,N)\sqrt{T^2-4N}}{2}.$$

The polynomials $F_P(T,N)$ and $F_Q(T,N)$ will prove to be defined over $\mathbb{Z}$. Before the proof we now present an algorithm to determine $A_F(O_K)$ for all the imaginary quadratic fields K.

Step 1: If $\tilde{r}_F = r_F$, then skip this step and proceed to Step 2. Else, compute all monic irreducible factors of $C(X)$ with degree less than 3 over $\mathbb{Q}$, and
(1.1) if $X - x$ is a linear factor of $C(X)$ with $x \in \mathbb{Z}$, then $(x, \pm B(x)) \in A_F(\mathbb{Z})$.
(1.2) else if $X^2 - tX + n$ is a quadratic factor of $C(X)$ with $t, n \in \mathbb{Z}$ and $t^2 - 4n < 0$, then $(x, \pm B(x)) \in A_F(O_K)$ only for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{t^2-4n})$ where $x = (t \pm \sqrt{t^2-4n})/2$.
(1.3) else, other factors of $C(X)$ do not yield integral points over any imaginary quadratic field.

Step 2: For each x in a finite set $\{x \in \mathbb{Z} \mid -r_F < x < r_F\}$, compute $f := F(x)$ and
(2.1) if $f \in \square$, that is, $f = y^2$ for a rational integer y, then $(x, \pm y) \in A_F(\mathbb{Z})$.
(2.2) else if $f < 0$, then $(x, \pm\sqrt{f}) \in A_F(O_K)$ only for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{f})$.
(2.3) else, $(x, \pm\sqrt{f}) \in A_F(\mathbb{C})$ is not defined over any imaginary quadratic field.

Step 3: For each (t,n) in a finite set $\{(t,n) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \le n < r_F^2, |t| < 2\sqrt{n}\}$, compute $d := D(t,n)$, $f_1 := F_P(t,n)$ and $f_2 := F_Q(t,n)$, and
(3.1) if $f_2 = 0$ and $f_1/2 \in \square$, that is, $f_1 = 2y^2$ and $f_2 = 0$ for a nonnegative rational integer y, then $((t+\sqrt{d})/2, \pm y), ((t-\sqrt{d})/2, \pm y) \in A_F(O_K)$ only for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$.
(3.2) else if $f_2 = 0$ and $f_1 d/2 \in \square$, that is, $f_1 = 2b^2/d$ and $f_2 = 0$ for a positive rational integer b, then $((t+\sqrt{d})/2, \pm b/\sqrt{d}), ((t-\sqrt{d})/2, \pm b/\sqrt{d}) \in A_F(O_K)$ only for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$.
(3.3) else if $f_2 \neq 0$ and there exist positive rational integers ν and τ such that $4\nu^2 = f_1^2 - f_2^2 d$ and $\tau^2 = f_1 + 2\nu$, then

$$\left(\frac{t+\sqrt{d}}{2}, \pm\frac{\tau + (f_2/\tau)\sqrt{d}}{2}\right), \left(\frac{t-\sqrt{d}}{2}, \pm\frac{\tau - (f_2/\tau)\sqrt{d}}{2}\right) \in A_F(O_K)$$

only for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$.
(3.4) else, $(x, \pm\sqrt{F(x)})$ and $(\overline{x}, \pm\sqrt{F(\overline{x})}) \in A_F(\mathbb{C})$ are not defined over any imaginary quadratic field where $x = (t+\sqrt{d})/2$ and $\overline{x} = (t-\sqrt{d})/2$.

In the rest of this section we prove the correctness of the algorithm described above.

Remark 3.1. When $\alpha = 1$, it satisfies $\tilde{r}_F = r_F$. In fact, by $\alpha = 1$ one has that $B(X), C(X) \in \mathbb{Z}[X]$ and $\mathrm{rad}(C) = 1 + \mathrm{ht}'(C)/|\ell(C)| \leq 1 + \mathrm{ht}(C) \leq r_F$. This means $\tilde{r}_F = \max\{r_F, \mathrm{rad}(C)\} = r_F$. Fortunately we have $\tilde{r}_F = r_F$ at Examples 4.2 to 4.8 in the next section §4 even if $\alpha > 1$. Example 4.10 is an example with $\tilde{r}_F > r_F$ verifying that Step 1 is needed for the algorithm.

We define the polynomials $P_j(T,N)$ and $Q_j(T,N)$ in $\mathbb{Z}[T,N]$ for nonnegative rational integers j by the recurrence relations

$$\begin{aligned} P_{j+2}(T,N) &= TP_{j+1}(T,N) - NP_j(T,N), \\ Q_{j+2}(T,N) &= TQ_{j+1}(T,N) - NQ_j(T,N) \end{aligned}$$

with initial terms $P_0(T,N) = 2, P_1(T,N) = T, Q_0(T,N) = 0$ and $Q_1(T,N) = 1$, respectively.

Lemma 3.2. *The polynomials $F_P(T,N)$ and $F_Q(T,N)$ belong to $\mathbb{Z}[T,N]$. More precisely we have*

$$\begin{aligned} F_P(T,N) &= P_{2k}(T,N) + a_{2k-1}P_{2k-1}(T,N) + \cdots + a_1P_1(T,N) + a_0P_0(T,N), \\ F_Q(T,N) &= Q_{2k}(T,N) + a_{2k-1}Q_{2k-1}(T,N) + \cdots + a_1Q_1(T,N) + a_0Q_0(T,N) \end{aligned}$$

where $F(X) = X^{2k} + a_{2k-1}X^{2k-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$.

Proof. Let $X_\pm$ denote $(T \pm \sqrt{T^2 - 4N})/2 \in \mathbb{Q}[T, N, \sqrt{T^2 - 4N}]$, respectively. Then one has that $X_+ + X_- = T$, $X_+ - X_- = \sqrt{T^2 - 4N}$ and $X_+X_- = N$. By mathematical induction, it is seen that $P_j(T,N) = X_+^j + X_-^j$ and $Q_j(T,N) = (X_+^j - X_-^j)/(X_+ - X_-)$ for every rational integer $j \geq 0$. Here $F(X_+) = (F_P(T,N) + F_Q(T,N)\sqrt{T^2 - 4N})/2$ by definition. The Galois action of the quadratic extension $\mathbb{Q}(T, N, \sqrt{T^2 - 4T})/\mathbb{Q}(T,N)$ yields $F(X_-) = (F_P(T,N) - F_Q(T,N)\sqrt{T^2 - 4N})/2$. This implies

$$\begin{aligned} F_P(T,N) &= F(X_+) + F(X_-) \\ &= P_{2k}(T,N) + a_{2k-1}P_{2k-1}(T,N) + \cdots + a_1P_1(T,N) + a_0P_0(T,N), \\ F_Q(T,N) &= \frac{F(X_+) - F(X_-)}{X_+ - X_-} \\ &= Q_{2k}(T,N) + a_{2k-1}Q_{2k-1}(T,N) + \cdots + a_1Q_1(T,N) + a_0Q_0(T,N) \end{aligned}$$

and thus $F_P(T,N), F_Q(T,N) \in \mathbb{Z}[T,N]$. □

For a complex number z let $\bar{z}$ stand for the complex conjugate of z. Let Ω denote the set of all the imaginary quadratic integers. Note that Ω contains no rational integers. To study Ω in terms of rational integers, we define a set $W = \{(t,n) \in \mathbb{Z} \times \mathbb{Z} \mid n \geq 1, |t| < 2\sqrt{n}\}$ and a map $\Psi : \Omega \to W$, $z \mapsto (z + \bar{z}, z\bar{z})$. Then Ψ is surjective and two-to-one. In fact, for each $(t,n) \in W$, one has that $\{z \in \Omega \mid \Psi(z) = (t,n)\} = \{z_+, z_-\}$ where $z_\pm = (t \pm \sqrt{t^2 - 4n})/2 \in \Omega$, respectively.

Lemma 3.3. *Let z be a number in Ω with $\Psi(z) = (t,n) \in W$. Then z^2 is contained in Ω if and only if $t \neq 0$. When $t \neq 0$, we have $\Psi(z^2) = (t^2 - 2n, n^2)$.*

Proof. By $\Psi(z) = (t, n)$, one has $z = (t \pm \sqrt{t^2 - 4n})/2$. This implies $z^2 = (t^2 - 2n \pm t\sqrt{t^2 - 4n})/2$. Note that $t^2 - 4n < 0$. Thus $z^2 \in \Omega$ if and only if $t \neq 0$. Since $z^2 + \overline{z^2} = (z + \overline{z})^2 - 2z\overline{z} = t^2 - 2n$ and $z^2\overline{z^2} = (z\overline{z})^2 = n^2$, we have $\Psi(z^2) = (t^2 - 2n, n^2)$. □

Proof of the Algorithm. Assume $(x, y) \in A_F^+(O_K)$ for an imaginary quadratic field K. Due to Proposition 2.6, we have two cases $C(x) = 0$ and $x \in \mathfrak{B}(r_F)$. Step 1 is the calculation for the first case $C(x) = 0$. The cases (1.1) and (1.2) correspond to $x \in \mathbb{Z}$ and $x \in \Omega$, respectively. The condition $\tilde{r}_F = r_F$ is equivalent to $\mathrm{rad}(C) \leq r_F$. When $\mathrm{rad}(C) \leq r_F$, we can find the numbers $x \in \mathbb{Z}$ (resp. $x \in \Omega$) with $C(x) = 0$ in Step 2 (resp. Step 3).

The second case $x \in \mathfrak{B}(r_F)$ is divided into two parts $x \in \mathbb{Z}$ and $x \in \Omega$. Step 2 is the calculation for $x \in \mathfrak{B}(r_F) \cap \mathbb{Z}$. The cases (2.1) and (2.2) correspond to $y \in \mathbb{Z}$ and $y \in \Omega$, respectively. By $x \in \mathbb{Z}$ and $y^2 = F(x) \in \mathbb{Z}$, the number $y \in \Omega$ has the shape in the case (2.2). Step 3 is the calculation for $x \in \mathfrak{B}(r_F) \cap \Omega$. Put a finite set $W_1 = \{(t, n) \in W \mid 1 \leq n < r_F^2, |t| < 2\sqrt{n}\}$. Then W_1 just yields all the numbers in $\mathfrak{B}(r_F) \cap \Omega$, that is, for every $x \in \mathfrak{B}(r_F) \cap \Omega$, there exists a unique $(t, n) \in W_1$ such that $x = (t \pm \sqrt{t^2 - 4n})/2$. Assume that $x = (t + \sqrt{d})/2 \in \mathfrak{B}(r_F) \cap \Omega$ with $(t, n) \in W_1$ where $d = t^2 - 4n < 0$. By the definition of $F_P(T, N)$ and $F_Q(T, N)$, it holds that

$$F(x) = (f_1 + f_2\sqrt{d})/2 \qquad (*)$$

where $f_1 = F_P(t, n)$ and $f_2 = F_Q(t, n)$. Lemma 3.2 means that f_1 and f_2 are rational integers. When $f_2 = 0$, one has $y^2 = F(x) = f_1/2 \in O_K \cap \mathbb{Q} = \mathbb{Z}$. The case $f_2 = 0$ is done in (3.1) and (3.2). The treatment of y in (3.1) and (3.2) are the same as those in (2.1) and (2.2), respectively. In (3.2) we have the condition $f_1 d/2 \in \square$ to satisfy that $y = \pm\sqrt{f_1/2} \in K = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{d})$. Let us consider the remaining case $f_2 \neq 0$, that is, (3.3). The condition $f_2 \neq 0$ implies $y^2 \in \Omega$ and thus $y \in \Omega$. Now put $(\tau, \nu) = \Psi(y) \in W$. Then one has $y = (\tau \pm \sqrt{\tau^2 - 4\nu})/2$. Lemma 3.3 means that $\tau \neq 0$ since $y^2 \in \Omega$. It is clear that $\nu \geq 1$. By $y^2 = F(x) = (f_1 + f_2\sqrt{d})/2$, Lemma 3.3 yields that $\Psi(y^2) = (\tau^2 - 2\nu, \nu^2) = (f_1, (f_1^2 - f_2^2 d)/4)$, which are equivalent to the equations in (3.3). Then it holds that $\tau^2(\tau^2 - 4\nu) = (\tau^2 - 2\nu)^2 - 4\nu^2 = f_1^2 - (f_1^2 - f_2^2 d) = f_2^2 d$. Thus $\sqrt{\tau^2 - 4\nu}$ is equal to $(f_2/\tau)\sqrt{d}$ or $-(f_2/\tau)\sqrt{d}$, and thus $y = (\tau \pm (f_2/\tau)\sqrt{d})/2$. This implies $F(x) = y^2 = (\tau^2 + (f_2/\tau)^2 d \pm 2f_2\sqrt{d})/4$. Comparing it with the equation (*), one can determine the sign $\pm$ in y, that is, $y = (\tau + (f_2/\tau)\sqrt{d})/2$. For all cases, if $(x, y) \in A_F(O_K)$, then $(x, \pm y), (\overline{x}, \pm\overline{y}) \in A_F(O_K)$ since $A_F : Y^2 = F(X)$ is defined over $\mathbb{Q}$. By $(-\tau + (f_2/(-\tau))\sqrt{d})/2 = -(\tau + (f_2/\tau)\sqrt{d})/2$, we may add the condition $\tau > 0$ for $\tau \neq 0$ in (3.3). □

4. Numerical examples

Remark 4.1. To compute the polynomials $F_P(T,X)$ and $F_Q(T,X)$ depending on $F(X)$, we may use $P_j(T,N)$ and $Q_j(T,N)$ not depending on $F(X)$.

j	$P_j(T,N)$	$Q_j(T,N)$
0	2	0
1	T	1
2	T^2-2N	T
3	T^3-3NT	T^2-N
4	$T^4-4NT^2+2N^2$	T^3-2NT
5	$T^5-5NT^3+5N^2T$	$T^4-3NT^2+N^2$
6	$T^6-6NT^4+9N^2T^2-2N^3$	$T^5-4NT^3+3N^2T$
7	$T^7-7NT^5+14N^2T^3-7N^3T$	$T^6-5NT^4+6N^2T^2-N^3$
8	$T^8-8NT^6+20N^2T^4-16N^3T^2+2N^4$	$T^7-6NT^5+10N^2T^3-4N^3T$

Examples 4.2, 4.3 and 4.4 below appear in [6] and [3], and Examples 4.5, 4.6 and 4.7 appear in [4] and [5], to calculate $\mathbb{Z}$-integral points. Examples 4.8 and 4.10 are original.

Example 4.2 (Tzanakis [6, §6 Example 1], Poulakis [3, §2 (1)] for $\mathbb{Z}$). Let us consider

$$F(X) = X^4 - 8X^2 + 8X + 1.$$

Then one has that $B(X) = X^2-4$, $C(X) = 8X-15$, $\alpha = 1$, $\mathrm{ht}'(B) = 4$, $\mathrm{ht}(C) = 15$, $r_F = 20$, $\mathrm{rad}(C) = 23/8 = 2.875$, $\tilde{r}_F = 20$, $\mu_F = -31$, $\delta_F = 1600$ and

$$\begin{aligned} F_P(T,N) &= T^4 - 4(N+2)T^2 + 8T + 2(N^2+8N+1), \\ F_Q(T,N) &= T^3 - 2(N+4)T + 8. \end{aligned}$$

In [3, §2 (1)] the range of x for $(x,y) \in A_F(\mathbb{Z})$ is $-33 \le x \le 30$. Our range is $|x| < r_F = 20$. By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points $(-6,\pm 31), (-3,\pm\sqrt{-14}), (-2,\pm\sqrt{-31}), (-1,\pm\sqrt{-14}), (0,\pm 1)$ and $(2,\pm 1)$ in Step 2 and no points in Step 3. Thus we conclude that

$$A_F(\mathbb{Z}) = \{(-6,\pm 31), (0,\pm 1), (2,\pm 1)\}$$

as in [3, §2 (1)],

$$\begin{aligned} A_F(O_{\mathbb{Q}(\sqrt{-14})}) &= \{(-3,\pm\sqrt{-14}), (-1,\pm\sqrt{-14}),\} \cup A_F(\mathbb{Z}), \\ A_F(O_{\mathbb{Q}(\sqrt{-31})}) &= \{(-2,\pm\sqrt{-31}),\} \cup A_F(\mathbb{Z}) \end{aligned}$$

and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K other than $\mathbb{Q}(\sqrt{-14})$ and $\mathbb{Q}(\sqrt{-31})$.

Example 4.3 (Tzanakis [6, §6 Example 2], Poulakis [3, §2 (2)] for $\mathbb{Z}$). Let us consider

$$F(X) = X^4 + 4X^3 + 10X^2 + 20X + 1.$$

Then one has that $B(X) = X^2 + 2X + 3$, $C(X) = 8X - 8$, $\alpha = 1$, $\mathrm{ht}'(B) = 3$, $\mathrm{ht}(C) = 8$, $r_F = 12$, $\mathrm{rad}(C) = 2$, $\tilde{r}_F = 12$, $\mu_F = -15$, $\delta_F = 576$ and

$$F_P(T,N) = T^4 + 4T^3 - 2(2N-5)T^2 - 4(3N-5)T + 2(N^2 - 10N + 1),$$
$$F_Q(T,N) = T^3 + 4T^2 - 2(N-5)T - 4(N-5).$$

In [3, §2 (2)] the range of x for $(x,y) \in A_F(\mathbb{Z})$ is $-34 \le x \le 28$ with $x \ne 1$. Our range is $|x| < r_F = 12$. By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points $(-4, \pm 9), (-3, \pm 2), (-2, \pm\sqrt{-15}), (-1, \pm 2\sqrt{-3}), (0, \pm 1)$ and $(1, \pm 6)$ in Step 2. In Step 3 we have

t	n	d	f_1	f_2	τ	ν	points (up to conj.)
-2	2	-4	-30	8	2	17	$(-1+\sqrt{-1}, \pm(1+4\sqrt{-1}))$
-1	2	-7	-27	9	3	18	$(\frac{-1+\sqrt{-7}}{2}, \pm\frac{3+3\sqrt{-7}}{2})$
-3	3	-3	-37	5	1	19	$(\frac{-3+\sqrt{-3}}{2}, \pm\frac{1+5\sqrt{-3}}{2})$
-3	5	-11	-45	9	3	27	$(\frac{-3+\sqrt{-11}}{2}, \pm\frac{3+3\sqrt{-11}}{2})$
-2	5	-16	-24	8	4	20	$(-1+2\sqrt{-1}, \pm(2+4\sqrt{-1}))$
-1	6	-23	-11	1	1	6	$(\frac{-1+\sqrt{-23}}{2}, \pm\frac{1+\sqrt{-23}}{2})$
0	6	-24	-46	-4	2	25	$(\sqrt{-6}, \pm(1-2\sqrt{-6}))$
-1	7	-27	3	-1	3	3	$(\frac{-1+3\sqrt{-3}}{2}, \pm\frac{3-\sqrt{-3}}{2})$
-2	8	-28	18	8	8	23	$(-1+\sqrt{-7}, \pm(4+\sqrt{-7}))$

The data of the table above are arranged in ascending order of the values with the first priority n and the second one t. Thus we conclude that

$$A_F(\mathbb{Z}) = \{(-4, \pm 9), (-3, \pm 2), (0, \pm 1), (1, \pm 6)\}$$

as in [3, §2 (2)] and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K other than the following 7 fields.

K	$A_F(O_K) \setminus A_F(\mathbb{Z})$
$\mathbb{Q}(\sqrt{-1})$	$(-1+\sqrt{-1}, \pm(1+4\sqrt{-1})), (-1-\sqrt{-1}, \pm(1-4\sqrt{-1}))$, $(-1+2\sqrt{-1}, \pm(2+4\sqrt{-1})), (-1-2\sqrt{-1}, \pm(2-4\sqrt{-1}))$
$\mathbb{Q}(\sqrt{-3})$	$(-1, \pm 2\sqrt{-3}), (\frac{-3+\sqrt{-3}}{2}, \pm\frac{1+5\sqrt{-3}}{2}), (\frac{-3-\sqrt{-3}}{2}, \pm\frac{1-5\sqrt{-3}}{2})$, $(\frac{-1+3\sqrt{-3}}{2}, \pm\frac{3-\sqrt{-3}}{2}), (\frac{-1-3\sqrt{-3}}{2}, \pm\frac{3+\sqrt{-3}}{2})$
$\mathbb{Q}(\sqrt{-6})$	$(\sqrt{-6}, \pm(1-2\sqrt{-6})), (-\sqrt{-6}, \pm(1+2\sqrt{-6}))$
$\mathbb{Q}(\sqrt{-7})$	$(\frac{-1+\sqrt{-7}}{2}, \pm\frac{3+3\sqrt{-7}}{2}), (\frac{-1-\sqrt{-7}}{2}, \pm\frac{3-3\sqrt{-7}}{2})$, $(-1+\sqrt{-7}, \pm(4+\sqrt{-7})), (-1-\sqrt{-7}, \pm(4-\sqrt{-7}))$
$\mathbb{Q}(\sqrt{-11})$	$(\frac{-3+\sqrt{-11}}{2}, \pm\frac{3+3\sqrt{-11}}{2}), (\frac{-3-\sqrt{-11}}{2}, \pm\frac{3-3\sqrt{-11}}{2})$
$\mathbb{Q}(\sqrt{-15})$	$(-2, \pm\sqrt{-15})$
$\mathbb{Q}(\sqrt{-23})$	$(\frac{-1+\sqrt{-23}}{2}, \pm\frac{1+\sqrt{-23}}{2}), (\frac{-1-\sqrt{-23}}{2}, \pm\frac{1-\sqrt{-23}}{2})$

Example 4.4 (Poulakis [3, §2 (3)] for $\mathbb{Z}$). Let us consider

$$F(X) = (X+1)^2(X^2+15) = X^4 + 2X^3 + 16X^2 + 30X + 15.$$

Then one has that $B(X) = X^2 + X + 15/2$, $C(X) = 15X - 165/4$, $\alpha = 2$, $\mathrm{ht}'(B) = 15/2$, $\mathrm{ht}(C) = 165/4$, $r_F = 91$, $\mathrm{rad}(C) = 15/4 = 3.75$, $\tilde{r}_F = 91$, $\mu_F = 0$, $\delta_F = 33124$ and

$$F_P(T,N) = T^4 + 2T^3 - 4(N-4)T^2 - 6(N-5)T + 2(N-15)(N-1),$$
$$F_Q(T,N) = T^3 + 2T^2 - 2(N-8)T - 2(N-15).$$

In [3, §2 (3)] the range of x for $(x,y) \in A_F(\mathbb{Z})$ is $-63 \le x \le 55$. Our range is $|x| < r_F = 91$. Excluding the square part, our range for $F(X) = X^2 + 15$ is $|x| < 16 = r_F = \tilde{r}_F$. By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points $(-7, \pm 48), (-1, 0), (1, \pm 8)$ and $(7, \pm 64)$ in Step 2. In Step 3 we have

t	n	d	f_1	f_2	τ	ν	points (up to conj.)
0	6	−24	−90	18	6	63	$(\sqrt{-6}, \pm(3 + 3\sqrt{-6}))$
−4	8	−16	−154	−18	4	85	$(-2 + 2\sqrt{-1}, \pm(2 - 9\sqrt{-1}))$
4	8	−16	−42	110	20	221	$(2 + 2\sqrt{-1}, \pm(10 + 11\sqrt{-1}))$
0	11	−44	−80	8	4	48	$(\sqrt{-11}, \pm(2 + 2\sqrt{-11}))$
0	14	−56	−26	2	2	15	$(\sqrt{-14}, \pm(1 + \sqrt{-14}))$
0	15	−60	0	0	−	−	$(\sqrt{-15}, 0)$
0	16	−64	30	−2	8	17	$(4\sqrt{-1}, \pm(4 - \sqrt{-1}))$
−2	17	−64	0	32	16	128	$(-1 + 4\sqrt{-1}, \pm(8 + 8\sqrt{-1}))$
2	17	−64	−256	−24	8	160	$(1 + 4\sqrt{-1}, \pm(4 - 12\sqrt{-1}))$
0	20	−80	190	−10	20	105	$(2\sqrt{-5}, \pm(10 - \sqrt{-5}))$
−4	22	−72	−322	66	18	323	$(-2 + 3\sqrt{-2}, \pm(9 + 11\sqrt{-2}))$
4	22	−72	−882	−30	6	459	$(2 + 3\sqrt{-2}, \pm(3 - 15\sqrt{-2}))$
0	27	−108	624	−24	36	336	$(3\sqrt{-3}, \pm(18 - 2\sqrt{-3}))$
0	64	−256	6174	−98	112	3185	$(8\sqrt{-1}, \pm(56 - 7\sqrt{-1}))$

Thus we conclude that $A_F(\mathbb{Z}) = \{(-7, \pm 48), (-1, 0), (1, \pm 8), (7, \pm 64)\}$ as in [3, §2 (3)] and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K other than the following 8 fields.

K	$A_F(O_K) \setminus A_F(\mathbb{Z})$
$\mathbb{Q}(\sqrt{-1})$	$(-2+2\sqrt{-1}, \pm(2-9\sqrt{-1}))$, $(-2-2\sqrt{-1}, \pm(2+9\sqrt{-1}))$, $(2+2\sqrt{-1}, \pm(10+11\sqrt{-1}))$, $(2-2\sqrt{-1}, \pm(10-11\sqrt{-1}))$, $(4\sqrt{-1}, \pm(4-\sqrt{-1}))$, $(-4\sqrt{-1}, \pm(4+\sqrt{-1}))$, $(-1+4\sqrt{-1}, \pm(8+8\sqrt{-1}))$, $(-1-4\sqrt{-1}, \pm(8-8\sqrt{-1}))$, $(1+4\sqrt{-1}, \pm(4-12\sqrt{-1}))$, $(1-4\sqrt{-1}, \pm(4+12\sqrt{-1}))$, $(8\sqrt{-1}, \pm(56-7\sqrt{-1}))$, $(-8\sqrt{-1}, \pm(56+7\sqrt{-1}))$
$\mathbb{Q}(\sqrt{-2})$	$(-2+3\sqrt{-2}, \pm(9+11\sqrt{-2}))$, $(-2-3\sqrt{-2}, \pm(9-11\sqrt{-2}))$, $(2+3\sqrt{-2}, \pm(3-15\sqrt{-2}))$, $(2-3\sqrt{-2}, \pm(3+15\sqrt{-2}))$
$\mathbb{Q}(\sqrt{-3})$	$(3\sqrt{-3}, \pm(18-2\sqrt{-3}))$, $(-3\sqrt{-3}, \pm(18+2\sqrt{-3}))$
$\mathbb{Q}(\sqrt{-5})$	$(2\sqrt{-5}, \pm(10-\sqrt{-5}))$, $(-2\sqrt{-5}, \pm(10+\sqrt{-5}))$
$\mathbb{Q}(\sqrt{-6})$	$(\sqrt{-6}, \pm(3+3\sqrt{-6}))$, $(-\sqrt{-6}, \pm(3-3\sqrt{-6}))$
$\mathbb{Q}(\sqrt{-11})$	$(\sqrt{-11}, \pm(2+2\sqrt{-11}))$, $(-\sqrt{-11}, \pm(2-2\sqrt{-11}))$
$\mathbb{Q}(\sqrt{-14})$	$(\sqrt{-14}, \pm(1+\sqrt{-14}))$, $(-\sqrt{-14}, \pm(1-\sqrt{-14}))$
$\mathbb{Q}(\sqrt{-15})$	$(\sqrt{-15}, 0)$, $(-\sqrt{-15}, 0)$

Example 4.5 (Szalay [4, §3 Example 1], [5, §3 Example 1] for $\mathbb{Z}$). Let us consider

$$F(X) = X^8 + X^7 + X^2 + 3X - 5.$$

Then one has that $B(X) = X^4 + \frac{1}{2}X^3 - \frac{1}{8}X^2 + \frac{1}{16}X - \frac{5}{128}$, $C(X) = \frac{7}{128}X^3 + \frac{505}{512}X^2 + \frac{3077}{1024}X - \frac{81945}{16384}$, $\alpha = 128$, $\mathrm{ht}'(B) = 1/2$, $\mathrm{ht}(C) = 81945/16384$, $r_F = 82137/128 = 641.6\ldots$, $\mathrm{rad}(C) = 82841/896 = 92.4\ldots$, $\tilde{r}_F = 82137/128 = 641.6\ldots$, $\mu_F = -7$, $\delta_F = 6746486769/4096 = 1647091.4\ldots$ and

$$\begin{aligned} F_P(T,N) &= T^8 + T^7 - 8NT^6 - 7NT^5 + 20N^2T^4 + 14N^2T^3 \\ &\quad -(16N^3-1)T^2 - (7N^3-3)T + 2(N^4 - N - 5), \\ F_Q(T,N) &= T^7 + T^6 - 6NT^5 - 5NT^4 + 10N^2T^3 + 6N^2T^2 \\ &\quad -(4N^3-1)T - (N^3-3). \end{aligned}$$

In [4, §3 Example 1] the range of x for $(x, y) \in A_F(\mathbb{Z})$ is $-4 \le x \le 10$. Our range is $|x| < r_F = 641.6\ldots$. By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points $(-2, \pm 11), (-1, \pm\sqrt{-7}), (0, \pm\sqrt{-5})$ and $(1, \pm 1)$ in Step 2. In Step 3 we have

t	n	d	f_1	f_2	τ	ν	points (up to conj.)
1	2	-7	-54	8	2	29	$(\frac{1+\sqrt{-7}}{2}, \pm(1+2\sqrt{-7}))$

Thus we conclude that $A_F(\mathbb{Z}) = \{(-2, \pm 11), (1, \pm 1)\}$,

$$\begin{aligned} A_F(O_{\mathbb{Q}(\sqrt{-5})}) &= \{(0, \pm\sqrt{-5})\} \cup A_F(\mathbb{Z}), \\ A_F(O_{\mathbb{Q}(\sqrt{-7})}) &= \{(-1, \pm\sqrt{-7}), (\tfrac{1+\sqrt{-7}}{2}, \pm(1+2\sqrt{-7})), (\tfrac{1-\sqrt{-7}}{2}, \pm(1-2\sqrt{-7}))\} \\ &\quad \cup A_F(\mathbb{Z}) \end{aligned}$$

and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K other than $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-7})$.

Example 4.6 (Szalay [4, §3 Example 2] for $\mathbb{Z}$). Let us consider

$$F(X) = X^4 - 2X^3 + 2X^2 + 7X + 3.$$

Then one has that $B(X) = X^2 - X + \frac{1}{2}$, $C(X) = 8X + \frac{11}{4}$, $\alpha = 2$, $\mathrm{ht}'(B) = 1$, $\mathrm{ht}(C) = 8$, $r_F = 18$, $\mathrm{rad}(C) = 43/32 = 1.3\ldots$, $\tilde{r}_F = 18$, $\mu_F = 0$, $\delta_F = 1296$ and

$$F_P(T,N) = T^4 - 2T^3 - 2(2N-1)T^2 + (6N+7)T + 2(N^2 - 2N + 3),$$
$$F_Q(T,N) = T^3 - 2T^2 - 2(N-1)T + (2N+7).$$

In [4, §3 Example 2] the range of x for $(x,y) \in A_F(\mathbb{Z})$ is $-6 \le x \le 9$ after correction. Our range is $|x| < r_F = 18$. By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points $(-1, \pm 1)$ and $(2, \pm 5)$ in Step 2 and no points in Step 3. Thus we conclude that $A_F(\mathbb{Z}) = \{(-1,\pm 1), (2, \pm 5)\}$ as in [4, §3 Example 2] after correction, and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K.

Example 4.7 (Szalay [4, §3 Example 3] for $\mathbb{Z}$). Let us consider

$$F(X) = X^2 - 5X - 11.$$

Then one has that $B(X) = X - \frac{5}{2}$, $C(X) = -\frac{69}{4}$, $\alpha = 2$, $\mathrm{ht}'(B) = 5/2$, $\mathrm{ht}(C) = 69/4$, $r_F = 38$, $\mathrm{rad}(C) = 1$, $\tilde{r}_F = 38$, $\mu_F = -17$, $\delta_F = 5776$ and

$$F_P(T,N) = T^2 - 5T - 2(N+11), \quad F_Q(T,N) = T - 5.$$

In [4, §3 Example 3] the range of x for $(x,y) \in A_F(\mathbb{Z})$ is $-15 \le x \le 20$. Our range is $|x| < r_F = 38$. By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points

$$(-15, \pm 17), (-4, \pm 5), (-1, \pm\sqrt{-5}), (0, \pm\sqrt{-11}), (1, \pm\sqrt{-15}), (2, \pm\sqrt{-17}),$$
$$(3, \pm\sqrt{-17}), (4, \pm\sqrt{-15}), (5, \pm\sqrt{-11}), (6, \pm\sqrt{-5}), (9, \pm 5), (20, \pm 17)$$

in Step 2. In Step 3 we have

t	n	d	f_1	f_2	τ	ν	points (up to conj.)
-3	4	-7	-6	-8	4	11	$(\frac{-3+\sqrt{-7}}{2}, \pm(2-\sqrt{-7}))$
1	5	-19	-36	-4	2	20	$(\frac{1+\sqrt{-19}}{2}, \pm(1-\sqrt{-19}))$
5	12	-23	-46	0	–	–	$(\frac{5+\sqrt{-23}}{2}, \pm\sqrt{-23})$
9	25	-19	-36	4	2	20	$(\frac{9+\sqrt{-19}}{2}, \pm(1+\sqrt{-19}))$
13	44	-7	-6	8	4	11	$(\frac{13+\sqrt{-7}}{2}, \pm(2+\sqrt{-7}))$
5	97	-363	-216	0	–	–	$(\frac{5+11\sqrt{-3}}{2}, \pm 6\sqrt{-3})$

Thus we conclude that $A_F(\mathbb{Z}) = \{(-15, \pm 17), (-4, \pm 5), (9, \pm 5), (20, \pm 17)\}$ as in [4, §3 Example 3] after correction, and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K

other than the following 8 fields.

K	$A_F(O_K) \setminus A_F(\mathbb{Z})$
$\mathbb{Q}(\sqrt{-3})$	$(\frac{5+11\sqrt{-3}}{2}, \pm 6\sqrt{-3}), (\frac{5-11\sqrt{-3}}{2}, \pm 6\sqrt{-3})$
$\mathbb{Q}(\sqrt{-5})$	$(-1, \pm\sqrt{-5}), (6, \pm\sqrt{-5})$,
$\mathbb{Q}(\sqrt{-7})$	$(\frac{-3+\sqrt{-7}}{2}, \pm(2-\sqrt{-7})), (\frac{-3-\sqrt{-7}}{2}, \pm(2+\sqrt{-7}))$, $(\frac{13+\sqrt{-7}}{2}, \pm(2+\sqrt{-7})), (\frac{13-\sqrt{-7}}{2}, \pm(2-\sqrt{-7}))$
$\mathbb{Q}(\sqrt{-11})$	$(0, \pm\sqrt{-11}), (5, \pm\sqrt{-11})$
$\mathbb{Q}(\sqrt{-15})$	$(1, \pm\sqrt{-15}), (4, \pm\sqrt{-15})$
$\mathbb{Q}(\sqrt{-17})$	$(2, \pm\sqrt{-17}), (3, \pm\sqrt{-17})$
$\mathbb{Q}(\sqrt{-19})$	$(\frac{1+\sqrt{-19}}{2}, \pm(1-\sqrt{-19})), (\frac{1-\sqrt{-19}}{2}, \pm(1+\sqrt{-19}))$, $(\frac{9+\sqrt{-19}}{2}, \pm(1+\sqrt{-19})), (\frac{9-\sqrt{-19}}{2}, \pm(1-\sqrt{-19}))$
$\mathbb{Q}(\sqrt{-23})$	$(\frac{5+\sqrt{-23}}{2}, \pm\sqrt{-23}), (\frac{5-\sqrt{-23}}{2}, \pm\sqrt{-23})$

Example 4.8. Let us consider

$$F(X) = X^6 + 2X^5 + 3X^4 + 4X^3 + 5X^2 + 6X + 7.$$

Then one has that $B(X) = X^3 + X^2 + X + 1$, $C(X) = 2X^2 + 4X + 6$, $\alpha = 1$, $\mathrm{ht}'(B) = 1$, $\mathrm{ht}(C) = 6$, $r_F = 8$, $\mathrm{rad}(C) = 4$, $\tilde{r}_F = 8$, $\mu_F = 0$, $\delta_F = 256$ and

$$\begin{aligned} F_P(T,N) &= T^6 + 2T^5 - 3(2N-1)T^4 - 2(5N-2)T^3 + (9N^2 - 12N + 5)T^2 \\ &\quad +2(5N^2 - 6N + 3)T - 2(N^3 - 3N^2 + 5N - 7), \\ F_Q(T,N) &= T^5 + 2T^4 - (4N-3)T^3 - 2(3N-2)T^2 + (3N^2 - 6N + 5)T \\ &\quad +2(N^2 - 2N + 3). \end{aligned}$$

By the algorithm, omitting Step 1 due to $r_F = \tilde{r}_F$, we find points $(-1, \pm 2)$ in Step 2. In Step 3 we have

t	n	d	f_1	f_2	τ	ν	points (up to conj.)
2	2	-4	-30	8	2	17	$(1+\sqrt{-1}, \pm(1+4\sqrt{-1}))$
-2	3	-8	32	0	$-$	$-$	$(-1+\sqrt{-2}, \pm 4)$

Thus we conclude that $A_F(\mathbb{Z}) = \{(-1, \pm 2)\}$,

$$\begin{aligned} A_F(O_{\mathbb{Q}(\sqrt{-1})}) &= \{(1+\sqrt{-1}, \pm(1+4\sqrt{-1})), (1-\sqrt{-1}, \pm(1-4\sqrt{-1}))\} \cup A_F(\mathbb{Z}), \\ A_F(O_{\mathbb{Q}(\sqrt{-2})}) &= \{(-1+\sqrt{-2}, \pm 4), (-1-\sqrt{-2}, \pm 4)\} \cup A_F(\mathbb{Z}) \end{aligned}$$

and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$.

Remark 4.9. In [2, §2.4] the sextic polynomial $F(x)$ of Example 4.8 is known to have Galois group S_5, not S_6, where S_n is the symmetric group of degree n.

Example 4.10. Let us consider

$$F(X) = X^6 + X^4 + X.$$

Then one has that $B(X) = X^3 + \frac{1}{2}X$, $C(X) = -\frac{1}{4}X^2 + X$, $\alpha = 2$, $\mathrm{ht}'(B) = 1/2$, $\mathrm{ht}(C) = 1$, $r_F = 7/2$, $\mathrm{rad}(C) = 5$, $\tilde{r}_F = 5$, $\mu_F = 0$, $\delta_F = 100$ and

$$F_P(T,N) = T^6 - (6N-1)T^4 + N(9N-4)T^2 + T - 2(N-1)N^2,$$
$$F_Q(T,N) = T^5 - (4N-1)T^3 + N(3N-2)T + 1.$$

Note that $r_F = 7/2 < 5 = \tilde{r}_F$. In Step 1 the polynomial $C(X)$ is factored into $-\frac{1}{4}X(X-4)$ over $\mathbb{Q}$. The linear factors X and $X-4$ of $C(X)$ yield points $(0,0)$ and $(4,\pm 66)$, respectively. We find points $(-1,\pm 1)$ and $(0,0)$ in Step 2. In Step 3 we have

t	n	d	f_1	f_2	τ	ν	points (up to conj.)
1	1	-3	2	0	$-$	$-$	$(\frac{1+\sqrt{-3}}{2}, \pm 1)$

Thus we conclude that $A_F(\mathbb{Z}) = \{(-1,\pm 1), (0,0), (4,\pm 66)\}$,

$$A_F(O_{\mathbb{Q}(\sqrt{-3})}) = \{(\tfrac{1+\sqrt{-3}}{2}, \pm 1), (\tfrac{1-\sqrt{-3}}{2}, \pm 1)\} \cup A_F(\mathbb{Z})$$

and $A_F(O_K) = A_F(\mathbb{Z})$ for all imaginary quadratic fields K other than $\mathbb{Q}(\sqrt{-3})$. This example verifies that Step 1 is needed for the algorithm. Indeed, $(4,\pm 66)$ are found only at Step 1.

5. Small generalization

We have a bit of generalization on the condition with respect to the coefficients of $F(X)$. By using the following map Λ we can show a similar statement for a nonsquare polynomial of even degree over $\mathbb{Q}$ with the leading coefficient being a square. For a prime number p and an $a \in \mathbb{Q}$ let $v_p(a)$ denote the additive valuation at p of a with $v_p(p) = 1$ and $v_p(0) = \infty$. Let $F(X)$ be a nonsquare polynomial over $\mathbb{Q}$ with even degree $2k > 0$ of the form $F(X) = a_{2k}X^{2k} + a_{2k-1}X^{2k-1} + \cdots + a_0$ where a_{2k} is the square of a rational number. Now put $J = \{j \in \mathbb{Z} \mid a_j \neq 0, 0 \leq j \leq 2k\}$ and $J' = J \setminus \{2k\}$. Let P denote the set consisting of prime numbers p with $v_p(a_j) \neq 0$ for some $j \in J$. If $P = \emptyset$, then $F(X)$ is monic and defined over $\mathbb{Z}$, and thus it has been settled. Assume $P \neq \emptyset$. For each $p \in P$ we take a nonnegative integer l_p such that $l_p \geq \max(\{v_p(a_{2k})/(2k)\} \cup \{(v_p(a_{2k}) - v_p(a_j))/(2k-j) \mid j \in J'\})$ and put $m_p = kl_p - v_p(a_{2k})/2$. Here m_p is a nonnegative integer since a_{2k} is square in $\mathbb{Q}$ and $l_p \geq v_p(a_{2k})/(2k)$. Now define rational integers $\lambda = \prod_{p\in P} p^{l_p}$, $\mu = \prod_{p\in P} p^{m_p}$ and a polynomial $\tilde{F}(X) = \mu^2 F(X/\lambda) = \mu^2 a_{2k}\lambda^{-2k}X^{2k} + \cdots + \mu^2 a_j \lambda^{-j}X^j + \cdots + \mu^2 a_0$.

Lemma 5.1. *The polynomial $\tilde{F}(X)$ is monic and defined over $\mathbb{Z}$ and there exists an injection $\Lambda : A_F(R) \to A_{\tilde{F}}(R)$, $(x,y) \mapsto (\lambda x, \mu y)$ where R is a subring of $\mathbb{C}$ containing $\mathbb{Z}$.*

Proof. The additive valuation at each $p \in P$ of the leading coefficient of $\tilde{F}(X)$ is equal to $v_p(\mu^2 a_{2k}\lambda^{-2k}) = 2m_p + v_p(a_{2k}) - 2kl_p = 0$. The number $\mu^2 a_{2k}\lambda^{-2k}$ is square in $\mathbb{Q}$. Thus $\tilde{F}(X)$ is monic. For $p \in P$ and $j \in J'$, one has $v_p(\mu^2 a_j \lambda^{-j}) = 2m_p + v_p(a_j) - jl_p = 2kl_p - v_p(a_{2k}) + v_p(a_j) - jl_p \geq (2k-j)(v_p(a_{2k}) - v_p(a_j))/(2k-j) - v_p(a_{2k}) + v_p(a_j) = 0$. Hence $\tilde{F}(X)$ is defined over $\mathbb{Z}$. Since R is a subring of $\mathbb{C}$ containing $\mathbb{Z}$, if x and y belong to R, then so do λx and μy by $\lambda, \mu \in \mathbb{Z}$. Due to the definition of $\tilde{F}(X)$, if $(x,y) \in A_F(R)$,

that is, $y^2 = F(x)$, then $(\mu y)^2 = \tilde{F}(\lambda x)$, that is, $(\lambda x, \mu y) \in A_{\tilde{F}}(R)$. Since λ and μ are nonzero, the map Λ is injective. □

Applying our algorithm to $\tilde{F}(X)$, we calculate $A_{\tilde{F}}(O_K)$ and see a similar result on the $A_F(O_K)$. The set $A_{\tilde{F}}(O_K)$ tells us the whole of $A_F(O_K)$ via Λ. Indeed, if $A_F(O_K) \neq A_F(\mathbb{Z})$, then $A_{\tilde{F}}(O_K) \neq A_{\tilde{F}}(\mathbb{Z})$ since Λ is an injection over $\mathbb{Z}$. Hence $A_{\tilde{F}}(O_K) = A_{\tilde{F}}(\mathbb{Z})$ yields $A_F(O_K) = A_F(\mathbb{Z})$.

Corollary 5.2. *Let $F(X)$ be a nonsquare polynomial over $\mathbb{Q}$ with even degree of which the leading coefficient is the square of a rational number. Then there exist only finitely many imaginary quadratic fields K such that $A_F(O_K) \neq A_F(\mathbb{Z})$. That is, there exists a constant $\tilde{\delta}_F > 0$ such that every imaginary quadratic field K with discriminant D_K of which absolute value $|D_K|$ greater than $\tilde{\delta}_F$ satisfies $A_F(O_K) = A_F(\mathbb{Z})$.*

References

[1] P. Borwein, T. Erdélyi, *Polynomials and polynomial inequalities*, Grad. Texts in Math., **161**, Springer-Verlag, New York, 1995.

[2] C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Math. Sci. Res. Inst. Publ., **45**, Cambridge University Press, Cambridge, 2002.

[3] D. Poulakis, A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$ (German summary), Elem. Math., **54**, 1999, 32–36.

[4] L. Szalay, Fast algorithm for solving superelliptic equations of certain types (English summary), Acta Acad. Paedagog. Agriensis Sect. Math. (N.S.), **27**, 2000, 19–24.

[5] L. Szalay, Superelliptic equations of the form $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, Bull. Greek Math. Soc., **46**, 2002, 23–33.

[6] N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations, Acta Arith., **75**, 1996, 165–190.

Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, 2641 Yamazaki, Noda-shi, Chiba-ken, 278-8510, Japan

Email address: komatsutoru.math@gmail.com