J. Korean Math. Soc. **34**(1997), No. 1, pp. 149-157

INTEGRAL POINTS ON HYPERBOLAS

JIN HONG, KYEONGHOON JEONG AND JAE-HOON KWON

1. Introduction

Finding all integers represented by the quadratic form $bx^2+cxy+ay^2$ is a classical problem in number theory. The closely related problem of finding all integral solutions to $bx^2+cxy+ay^2=k$ for a fixed $k \in \mathbb{Z}^\times$ is also of interest.

A number theoretical approach to this problem appears in [1]. But the solution involves finding a certain fundamental unit, which is not an easy thing to do.

In [2], as a by-product of the study of rank 2 hyperbolic Kac-Moody algebras, corresponding to the symmetric matrix $\begin{pmatrix} 2 & -a \\ -a & 2 \end{pmatrix}$, Kang and Melville find all integral solutions to $x^2-axy+y^2=-k$ when $a \geq 3$ and $k \geq -1$. There is a 1-1 correspondence between the imaginary roots of length k and the integral points of $x^2-axy+y^2=-k$. We also know that all imaginary roots are generated by the Weyl group action on a finite number of imaginary roots in an easily defined region. Using these two facts, Kang and Melville reduce finding all integral solutions of $x^2-axy+y^2=-k$ to finding them in a small region.

Motivated by the result above, we extend their result to a wider range of hyperbolas. Given $a, b, c, k \in \mathbb{Z}^\times$, satisfying $a|c$ and $b|c$, we shall give an explicit description for all integral solutions of $bx^2+cxy+ay^2=k$ analogous to that of Kang and Melville. Our method and the classical one appearing in [1] are similar in that both obtain all integral points of the hyperbola from that contained in some fundamental region, but our method will require much less work.

Received April 28, 1996. Revised November 30, 1996.
1991 AMS Subject Classification: 11D09.
Key words: quadratic form, Pell's equation, fundamental unit.

Finally, we apply our method to finding the minimal solution of the Pell's equation $X^2 - dY^2 = 1$ with $d = p^2 - q$, $q|2p$, and $q \neq 1$.

2. Fundamental Regions and Linear Transformations

Define $f(x,y) = bx^2 - abxy + ay^2$ with $a, b \in \mathbb{Z}^\times$. We assume $ab(ab-4) > 0$, so that $\mathfrak{H} = \{(x,y) \in \mathbb{R}^2 | f(x,y) = k\}$ with $k \in \mathbb{Z}^\times$ is a hyperbola.

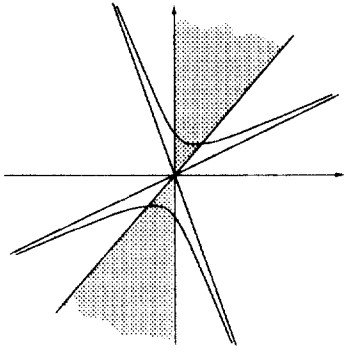
We split this into eight cases. We also define a region $\mathfrak{R}$ for each of the cases. It will be called the fundamental region for $\mathfrak{H}$.

Case 1. $ab < 0$, $a > 0$, and $k > 0$

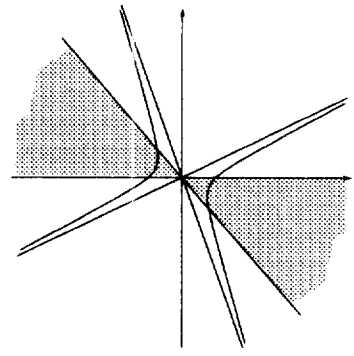
$\mathfrak{R} = \{(x,y) \in \mathbb{R}^2 | x \geq 0, y \geq \frac{2}{a}x\} \cup \{(x,y) \in \mathbb{R}^2 | x \leq 0, y \leq \frac{2}{a}x\}$

Case 2. $ab < 0$, $a > 0$, and $k < 0$

$\mathfrak{R} = \{(x,y) \in \mathbb{R}^2 | x \geq 0, \frac{b}{2}x \leq y \leq 0\} \cup \{(x,y) \in \mathbb{R}^2 | x \leq 0, 0 \leq y \leq \frac{b}{2}x\}$



Case 1



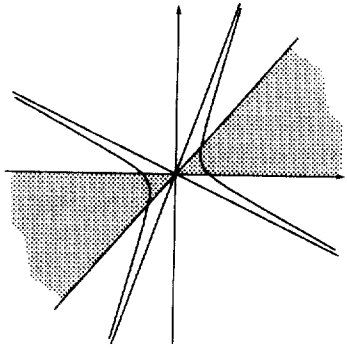
Case 2

Case 3. $ab < 0$, $a < 0$, and $k > 0$

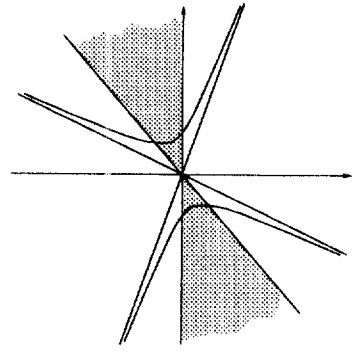
$\mathfrak{R} = \{(x,y) \in \mathbb{R}^2 | x \geq 0, 0 \leq y \leq \frac{b}{2}x\} \cup \{(x,y) \in \mathbb{R}^2 | x \leq 0, \frac{b}{2}x \leq y \leq 0\}$

Case 4. $ab < 0$, $a < 0$, and $k < 0$

$\mathfrak{R} = \{(x,y) \in \mathbb{R}^2 | x \geq 0, y \leq \frac{2}{a}x\} \cup \{(x,y) \in \mathbb{R}^2 | x \leq 0, \frac{2}{a}x \leq y\}$



Case 3



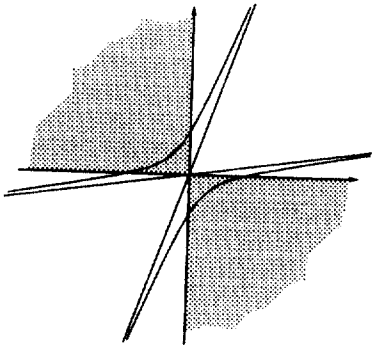
Case 4

Case 5. $ab > 4$, $a > 0$, and $k > 0$

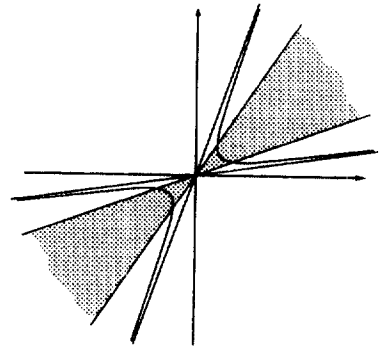
$\mathfrak{R} = \{(x, y) \in \mathbb{R}^2 | xy \leq 0\}$

Case 6. $ab > 4$, $a > 0$, and $k < 0$

$\mathfrak{R} = \{(x, y) \in \mathbb{R}^2 | x \geq 0, \frac{2}{a}x \leq y \leq \frac{b}{2}x\} \cup \{(x, y) \in \mathbb{R}^2 | x \leq 0, \frac{b}{2}x \leq y \leq \frac{2}{a}x\}$



Case 5



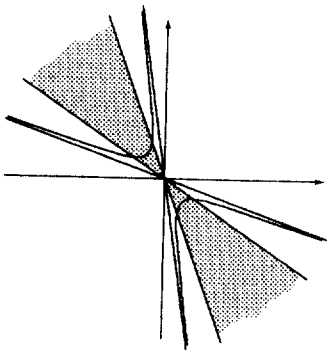
Case 6

Case 7. $ab > 4$, $a < 0$, and $k > 0$

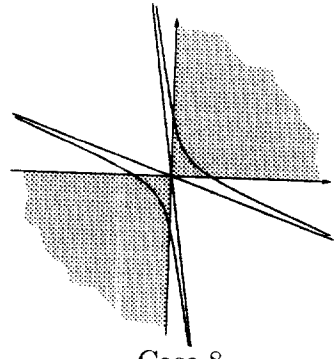
$\mathfrak{R} = \{(x, y) \in \mathbb{R}^2 | x \geq 0, \frac{b}{2}x \leq y \leq \frac{2}{a}x\} \cup \{(x, y) \in \mathbb{R}^2 | x \leq 0, \frac{2}{a}x \leq y \leq \frac{b}{2}x\}$

Case 8. $ab > 4$, $a < 0$, and $k < 0$

$\mathfrak{R} = \{(x, y) \in \mathbb{R}^2 | xy \geq 0\}$



Case 7



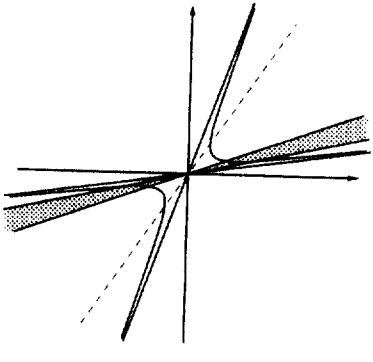
Case 8

We next define two matrices $A = \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ b & -1 \end{pmatrix}$. We view them as linear transformations of $\mathbb{R}^2$. The definitions of the matrices A and B were originated from simple reflections for the root space of the Kac-Moody algebras corresponding to matrices of the form $\begin{pmatrix} 2 & -b \\ -a & 2 \end{pmatrix}$.

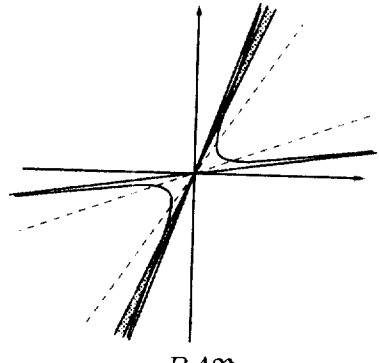
Let us see what the matrices do to the region $\mathfrak{R}$. We take Case 6 as an example. With the help of the observation,

$$\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x - t \\ \frac{2}{a}x \end{pmatrix} = \begin{pmatrix} x + t \\ \frac{2}{a}x \end{pmatrix},$$

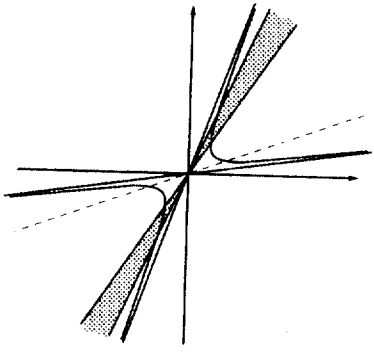
we can visualize A as "horizontal reflection in the line $y = \frac{2}{a}x$". Similarly we view B as "vertical reflection in the line $y = \frac{b}{2}x$". Keeping this in mind, we draw the following sequence of pictures.



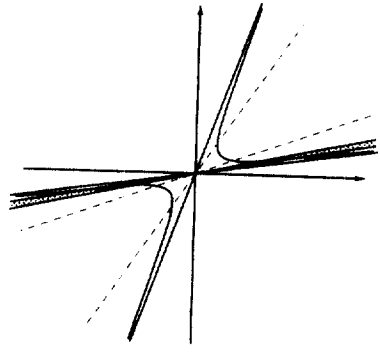
$A\mathfrak{R}$



$BA\mathfrak{R}$



$B\mathfrak{R}$



$AB\mathfrak{R}$

This suggests that the hyperbola $\mathfrak{H}$ lies inside

$$(\cup_{i=1}^{\infty}(BA)^i\mathfrak{R})\cup(\cup_{i=0}^{\infty}B(AB)^i\mathfrak{R})\cup\mathfrak{R}\cup(\cup_{i=0}^{\infty}A(BA)^i\mathfrak{R})\cup(\cup_{i=1}^{\infty}(AB)^i\mathfrak{R}).$$

Let us prove this. Starting with an arbitrary initial value, we define the sequence $\{m_i\}_{i=0}^{\infty}\subset\mathbb{R}\cup\{\infty\}$ so that AB sends the line of slope m_i passing through the origin to a line of slope m_{i+1}. Similarly, we define $\{n_i\}_{i=0}^{\infty}$ using BA. Let $\gamma=\frac{ab+\sqrt{(ab)^2-4ab}}{2a}$ and $\delta=\frac{ab-\sqrt{(ab)^2-4ab}}{2a}$. The asymptotes of the hyperbola are given by $y=\gamma x$ and $y=\delta x$.

LEMMA 1. *The sequences $\{m_i\}_{i=0}^{\infty}$ and $\{n_i\}_{i=0}^{\infty}$ are convergent regardless of the initial values. The limit values are either γ or δ.*

Proof. We have $AB=\begin{pmatrix} ab-1 & -a \\ b & -1 \end{pmatrix}$.

So $m_{i+1}=\frac{b-m_i}{ab-1-am_i}$ with natural interpretations when $m_i=\infty$. Solving

$$\begin{cases} y=\frac{b-x}{ab-1-ax} \\ y=x \end{cases}$$

gives two solutions (γ,γ) and (δ,δ). Substituting $\gamma=\frac{b-\gamma}{ab-1-a\gamma}$ into the equation $m_{i+1}-\gamma=\frac{b-m_i}{ab-1-am_i}-\gamma$, we get

$$m_{i+1}-\gamma=\frac{m_i-\gamma}{(ab-1-am_i)(ab-1-a\gamma)}.$$

Using this and a similar equation with δ in place of γ, we get

$$\frac{m_{i+1}-\gamma}{m_{i+1}-\delta}=\frac{ab-1-a\gamma}{ab-1-b\delta}\cdot\frac{m_i-\gamma}{m_i-\delta}$$

We can show $|\frac{ab-1-a\gamma}{ab-1-b\delta}| \neq 1$ so that $|\frac{m_i-\gamma}{m_i-\delta}|$ always approaches either 0 or ∞. The convergence of m_i is now clear. Convergence of $\{n_i\}_{i=0}^{\infty}$ may be taken care of similarly. □

This lemma is enough to show what has been suggested. Noting $A^{-1} = A$ and $B^{-1} = B$, we write this as:

PROPOSITION 1. *The hyperbola $\mathfrak{H}$ lies inside the region*

$$\mathfrak{D} = (\cup_{i\in\mathbb{Z}}(AB)^i\mathfrak{R}) \cup (\cup_{i\in\mathbb{Z}}B(AB)^i\mathfrak{R}).$$

From Lemma 1, we know that $\mathfrak{D}$ is the region bounded by the two asymptotes of the hyperbola $\mathfrak{H}$. Proposition 1 says that given any point (x, y) in $\mathfrak{D}$, there exists a point (x_0, y_0) in $\mathfrak{R}$ and an integer i such that, $\binom{x}{y} = (AB)^i\binom{x_0}{y_0}$ or $B(AB)^i\binom{x_0}{y_0}$.

3. Integral Points on the Hyperbola

Define $\mathfrak{F} = \mathfrak{H}\cap\mathfrak{R}\cap\mathbb{Z}^2$ to be the integral points on the hyperbola lying inside the fundamental region $\mathfrak{R}$. By direct calculation, we can see that both A and B leave $\mathfrak{H}$ invariant. $(AB)^i$, $B(AB)^i$, and their inverses, which are also of the same form, send integral points to integral points. This together with Proposition 1 yields:

PROPOSITION 2. *The integral points on the hyperbola, i.e. $\mathfrak{H}\cap\mathbb{Z}^2$, are given by, $(\cup_{i\in\mathbb{Z}}(AB)^i\mathfrak{F}) \cup (\cup_{i\in\mathbb{Z}}B(AB)^i\mathfrak{F})$.*

So all the integral solutions to a given hyperbola are generated by the integral solutions inside the fundamental region. We must add that the intersection of $\mathfrak{H}$ and $\mathfrak{R}$ is only a finite segment so that $\mathfrak{F}$ is a finite set which may be found explicitly.

To write the solutions to $\mathfrak{H}$ more explicitly, we define the sequences $\{a_n\}_{n\in\mathbb{Z}}$, $\{b_n\}_{n\in\mathbb{Z}}$, $\{c_n\}_{n\in\mathbb{Z}}$, and $\{d_n\}_{n\in\mathbb{Z}}$ by,

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = (AB)^n\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} c_n \\ d_n \end{pmatrix} = (AB)^n\begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Their explicit values are given by:

LEMMA 2.

$$a_n = \frac{\alpha+1}{\alpha-\beta}\alpha^n + \frac{\beta+1}{\beta-\alpha}\beta^n,$$
$$b_n = \frac{b}{\alpha-\beta}(\alpha^n - \beta^n),$$
$$c_n = \frac{a}{\beta-\alpha}(\alpha^n - \beta^n),$$
$$d_n = \frac{\beta+1}{\beta-\alpha}\alpha^n + \frac{\alpha+1}{\alpha-\beta}\beta^n,$$

where α and β are the two roots of $x^2 - (ab-2)x + 1 = 0$.

With this, we can rewrite Proposition 2 as:

THEOREM. *The integral points on the hyperbola $bx^2 - abxy + ay^2 = k$ are given by:* $\{(xa_n + yc_n, xb_n + yd_n), (xa_n + yc_n, x(ba_n - b_n) + y(bc_n - d_n))|(x,y) \in \mathfrak{F}, n \in \mathbb{Z}\}$.

REMARK. We can now find the complete set of integral solutions to $bx^2 - cxy + ay^2 = k$ when $a|c$ and $b|c$. We multiply it by $\frac{c}{ab}$, so that it is equivalent to solving $\frac{c}{a}x^2 - \frac{c^2}{ab}xy + \frac{c}{b}y^2 = \frac{c}{ab}k$. If $\frac{c}{ab}k$ is not an integer, this has no integral solution. If $\frac{c}{ab}k$ is an integer, this is of the form we have discussed.

Before ending this section, we will talk about finding $\mathfrak{F}$. Suppose, as in Case 3, that $\mathfrak{H}$ passes through $(\pm\sqrt{\frac{k}{b}}, 0)$. To find $\mathfrak{F}$, we substitute each integer in the range $[-\sqrt{\frac{k}{b}}, \sqrt{\frac{k}{b}}]$ into the x slot of $bx^2 - abxy + ay^2 = k$ and solve for y. For Case 6, the x coordinate for the intersection of the line $y = \frac{2}{a}x$ with $\mathfrak{H}$ is $\pm\sqrt{\frac{ak}{4-ab}}$. So we have only to substitute integers in the range $[-\sqrt{\frac{ak}{4-ab}}, \sqrt{\frac{ak}{4-ab}}]$ to find all integral points of $\mathfrak{H}$ lying in $\mathfrak{R}$. It should now be obvious as to what should be done for other cases. For Case 6, we can actually show that $\frac{ak}{4-ab} \leq \frac{-5k}{b}$, so that in all cases a bound for the number of integers to be checked in order to find $\mathfrak{F}$, proportional to $\sqrt{|\frac{k}{a}|}$ or $\sqrt{|\frac{k}{b}|}$, can be given.

REMARK. The approach in [1] also reduces finding all integral solutions of a binary form to finding them in some fundamental region. Complete integral solution is then generated by applying to them all proper integral automorphs of the binary form. In that approach, both the fundamental region and the finding of proper integral automorphs involves finding a fundamental unit. So our method is much more explicit and requires much less work in finding all integral solutions.

4. Application to Solving the Pell's equation

In this section, we apply our results to solving the Pell's equation, $X^2 - dY^2 = 1$, when d is of the form $p^2 - q > 0$ with $p, q \in \mathbb{Z}^\times$, $q|2p$, and $q \neq 1$.

We use the linear transformation $P = \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix}$. Its determinant is 1, so that solving the above Pell's equation is equivalent to solving

$$(x - py)^2 - dy^2 = 1.$$

Substituting $d = p^2 - q$, this is just

$$x^2 - 2pxy + qy^2 = 1,$$

or equivalently,

$$\frac{2p}{q}x^2 - \frac{4p^2}{q}xy + 2py^2 = \frac{2p}{q}.$$

Considering each of the eight cases, we find cases 1,4,6, and 7 not applicable and $\mathfrak{F} = \{(\pm 1, 0)\}$ in all the other cases. We use the Theorem and apply the matrix P to the resulting set. After some calculations, we are able to write the complete solution to $X^2 - dY^2 = 1$ as,

$$\left\{ \left(\pm\frac{1}{2}(\alpha^n + \beta^n), \pm\frac{1}{2\sqrt{d}}(\alpha^n - \beta^n) \right) \middle| n \in \mathbb{Z} \right\}.$$

Here, α and β are the two roots of $x^2 - (\frac{4p^2}{q} - 2)x + 1 = 0$.

We summarize this as:

PROPOSITION 3. *The minimal solution of* $X^2 - dY^2 = 1$ *for* $d = p^2 - q > 0$ *with* $q|2p$ *and* $q \neq 1$ *is given by* $(\frac{2p^2}{q} - 1, \frac{2p}{q})$.

REMARK. (a) The result of this section, along with some other similar results, has been obtained by Richaud [4], but he has left no proof.

(b) Under some conditions, for example $q < -1$, it is possible to show that $X^2 - dY^2 = -1$ has no solution, so that $(\frac{2p^2}{q} - 1) + \frac{2p}{q}\sqrt{d}$ is actually a fundamental unit.

ACKNOWLEDGMENT. We would like to thank our advisor, Professor Seok-Jin Kang, for suggesting this problem and for the many helpful remarks.

References

1. J. W. S. Cassels, *Rational quadratic forms*, Academic Press Inc., 1978.
2. S.-J. Kang and D. J. Melville, *Rank 2 symmetric hyperbolic Kac-Moody algebras*, Nagoya Math. J. **140** (1995), 41-75.
3. L. K. Hua, *Introduction to number theory*, Springer-Verlag, 1982.
4. M. C. Richaud, Atti Dell' Accademia Pontificia De' Nuovi Lincei **19** (1866), 177-182.

Department of Mathematics
Seoul National University
Seoul 151-742, Korea