Integer points on the ellipse

Consider on $\mathbf{R}^2$ an ellipse

$$ax^2 + 2bxy + cy^2 = 1, \quad (ac - b^2 > 0, a > 0) \tag{1}$$

such that

$$ac - b^2 = 1, \text{ and } a, c, b \in \mathbf{Z},$$

i.e. quadratic form $ax^2 + 2bxy + cy^2$ is defined by symmetric matrix in $SL(2, \mathbf{Z})^*$.

What about integer points (points with integer coordinates) on this ellipse, in the interior of this ellipse?

Fact 1 *The interior of the ellipse (2) possesses* 4 *points with integer coordinates (except the origin* $(0, 0)$ *). All these points are on the ellipse (1).*

Remark It is well-known that any domain M of the area 1 possesses at least two points $\mathbf{r}_1, \mathbf{r}_2$ such that vector $\mathbf{r}_2 - \mathbf{r}_1$ has integer coordinates (Minkovsky lemma). This implies the following

Fact 2 *Any central-symmetric convex domain* M *of the area* $S(M) = 4$ *possesses at least one point with integer coordinates except the point* $(0, 0)$.

It is evident that for an arbitrary $\varepsilon > 0$, there exists central-symmetric convex domain M_ε of the area $S(M) = 4 - \varepsilon$ which does not possess any point with integer coordinates except the point $(0, 0)$. On the other hand it follows from the Fact 1 that the ellipse (1) is a central-symmetric convex domain of the area $S(\Delta) = \pi < 4$ which possesses 4 integer points.

Proof of the Fact 1.

This is evident in the case if $a = b = 1$ and $b = 0$. Ellipse becomes circle which possesses exactly four integer points $(1, 0)$, $(1, 1)$, $(-1, 0)$ and $(1, 1)$ (on the boundary).

The Fact 1 follows from the following Proposition

Proposition *A matrix equation* $X^+X = B$ *has a solution* $X \in SL(2, \mathbf{Z})$ *if* B *is symmetric matrix in* $SL(2, \mathbf{Z})$.

Indeed let $X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $(\alpha, \beta\, \gamma, \delta \in \mathbf{Z})$ be a solution of the equation (3) where B is a matrix of quadratic form $ax^2+2bxy+cy^2$, which defines an ellipse (1): $B = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Then linear transformation $\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}$ transforms circle $x^2+y^2 = 1$ onto the ellipse (1). This linear transformation establishes one-one map of lattice of points

* A group $SL(2, \mathbf{Z})$ is a group of 2×2 matrices with integer entries.

with integer coordinates onto itself, since $\det X = 1$. Points with integer coordinates on the ellipse (1) are images of the points $(1,0)$, $(1,1)$, $(-1,0)$ and $(1,1)$. They are 4 points (α,γ), (β,δ), $(-\alpha,-\gamma)$ and (β,δ).

It remains to prove the Proposition.

Proof

Consider matrices $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ in $SL(2,\mathbf{Z})$, $S^2 = 1$ and $T^3 = 1^*$. Analyze the action of these matrices T and S on the quadratic form $ax^2 + 2bxy + cy^2$:

$$B = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \to S^+BS = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} c & -b \\ -b & a \end{pmatrix}$$

and

$$B = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \to T^+BT = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a+c-2b & a-b \\ a-b & a \end{pmatrix}.$$

It suffices to show that subsequent actions of these transformations a matrix $B = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ can be transformed to unity matrix $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, i.e.

$$M^+BM = E, \quad \text{where } M = S^{m_1}T^{n_1}S^{m_2}T^{n_2}\dots S^{m_{k-1}}T^{n_{k-1}}S^{m_k}T^{n_k}\,. \tag{2}$$

In this case matrix $B = X^+X$ and the matrix $X = T^{2n_k}S^{m_k}T^{2n_{k-1}}S^{m_{k-1}}\dots T^{2n_2}S^{m_2}T^{2n_1}S^{m_1}$ ∎ is a solution of equation in Proposition.

To prove the relation (2) note that if $b = 0$ (in matrix B) then $B = E$. If $B \to S^+BS$ then $b \to -b$, if $B \to T^+BT$ then $b \to a - b$ and if $B \to T^+T^+BTT$ then $b \to c - b$. On the other hand if $b > 0$ then $|a - b| < b$ or $|c - b| < b$. Therefore acting on B by one of the matrices T, or T^2, TST, ST, or ST^2 or $STST$ we decrease absolute value of b at lest on one. Repeating this procedure we come to $b = 0$ ** ∎

---

* Matrices T, S are generators of the group $SL(2,\mathbf{Z})$. The proof of Proposition is in the spirit of the proof of this statement.

** More puristic way to say it is following: For a given matrix B consider a set $\mathcal{M}$ of all matrices K^+BK where K is a matrix generated by matrices S and T ($K = S^{m_1}T^{n_1}S^{m_2}T^{n_2}\dots S^{m_{k-1}}T^{n_{k-1}}S^{m_k}T^{n_k}$). Consider in this set the matrix $B_0 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ such that entry $b = B_{12}$ is minimal. Show that $b = 0$, thus $B_0 = E$. Suppose that $b \neq 0$, then acting on B by matrices S and T we can decrease the value of $|b|$. Contradiction.