96.35 Reflections on lattices

The problem

Recently, the following problem arose in the context of metric spaces. A grid point in the Euclidean plane $\mathbb{R}^2$ is a point $(x, y)$, where $x$ and $y$ are integers; equivalently, it is a point of $\mathbb{Z} \times \mathbb{Z}$, which we write as $\mathbb{Z}^2$. Take a grid point $(p, q)$, where $p$ and $q$ are positive and coprime, and let $L$ be the straight line through $(0, 0)$ and $(p, q)$. The problem is to find all pairs $(x, y)$ and $(u, v)$ in $\mathbb{Z}^2$ that are reflections of each other in $L$. We would also like to know what the set of such pairs looks like. So, if we let $R$ be the reflection across $L$, our task is to study the set

$$\mathcal{L} = \{(x, y) \in \mathbb{Z}^2 : R(x, y) \in \mathbb{Z}^2\}.$$  

Obviously, this set is symmetric about $L$, but what else can we say?

For typographical reasons we shall denote points in $\mathbb{R}^2$ by any of the symbols $A, B, C, \ldots$, $(a, b), \ldots$, as is most convenient at the time; in particular, we shall use row vectors and column vectors interchangeably.

The reflection $R$ across $L$

If we rotate the vector $(p, q)$ (which lies along $L$) by $\pi/2$ in each direction we obtain the vectors $(-q, p)$ and $(q, -p)$ (this can be seen by replacing $(p, q)$ by $p + iq$ and computing $i(p + iq)$ and $-i(p + iq)$), and these last two vectors are (i) orthogonal to $(p, q)$, and (ii) reflections of each other in $L$. In particular, $\mathcal{L}$ contains $(p, q), (-q, p)$ and $(q, -p)$.

Now take any $(x, y)$ in $\mathbb{R}^2$ (but not necessarily in $\mathbb{Z}^2$). Then there are unique real numbers $s$ and $t$ such that

$$\begin{pmatrix} x \\ y \end{pmatrix} = s \begin{pmatrix} p \\ q \end{pmatrix} + t \begin{pmatrix} -q \\ p \end{pmatrix}.$$  

If we now let $(u, v)$ be the reflection of $(x, y)$ across $L$, we have

$$\begin{pmatrix} u \\ v \end{pmatrix} = s \begin{pmatrix} p \\ q \end{pmatrix} - t \begin{pmatrix} -q \\ p \end{pmatrix}.$$  

We prefer to write these in matrix form, namely

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & -q \\ q & p \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} sp - tq \\ tp + sq \end{pmatrix}, \quad \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p & q \\ q & -p \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} sp + tq \\ sq - tp \end{pmatrix},$$  

(1)
so that

\[ \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p & q \\ q & -p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}^{-1}. \]

The important point here is that the reflection \( R \) across \( L \) is given by a \( 2 \times 2 \) real matrix; we do not need to know what this matrix is (although the reader may wish to find the explicit expression for it). Since \( R \) is given by a matrix, for all \( X \) and \( Y \) in \( \mathbb{R}^2 \), we have \( R(X + Y) = R(X) + R(Y) \) and \( R(-X) = -R(X) \), and this gives us our first piece of information about \( \mathcal{L} \).

**Lemma 1:** The set \( \mathcal{L} \) is a non-cyclic subgroup of the additive group \( \mathbb{Z}^2 \).

**Proof:** Certainly \( \mathcal{L} \) is a subset of the additive group \( \mathbb{Z}^2 \). We show that if \( X, Y \in \mathcal{L} \) then \( X + Y \in \mathcal{L} \). Suppose that \( X, Y \in \mathcal{L} \). Then \( X, Y \in \mathbb{Z}^2 \) so that \( X + Y \in \mathbb{Z}^2 \). Also \( R(X), R(Y) \in \mathbb{Z}^2 \), so that \( R(X) + R(Y) \in \mathbb{Z}^2 \). Thus \( R(X + Y) \in \mathbb{Z}^2 \); hence \( X + Y \in \mathcal{L} \). Essentially the same argument (using \(-X\) in place of \(X + Y\)) shows that if \( X \in \mathcal{L} \) then \(-X \in \mathcal{L} \) (we omit the details), so we conclude that \( \mathcal{L} \) is a subgroup of \( \mathbb{Z}^2 \). Since \( \mathcal{L} \) contains \((p, q)\) and \((-q, p)\), which are orthogonal, it is not cyclic.

**Lattices**

The group \( \mathbb{Z}^2 \) is the set of all integral linear combinations of \((1, 0)\) and \((0, 1)\), and a lattice is a generalisation of this idea. Explicitly, a lattice \( \Lambda \) is the set of all integral linear combinations of a pair of points \( A \) and \( B \) that do not lie on a line through the origin; thus \( \Lambda = \{mA + nB : m, n \in \mathbb{Z}\} \). Clearly, a lattice is an additive group, and if \( A, B \in \mathbb{Z}^2 \), then \( \Lambda \subset \mathbb{Z}^2 \). Our next step is to show that \( \mathcal{L} \) is a lattice and, since \( \mathbb{Z}^2 \) is a lattice, this follows immediately from Lemma 1 and the next well-known result.

**Lemma 2:** A non-cyclic subgroup of a lattice is a lattice.

**Proof:** Let \( G \) be a non-cyclic subgroup of a lattice \( \Lambda \). Then \( G \) contains a non-zero vector, say \( A \), of smallest positive length among all non-zero vectors in \( G \). Now let \( L_A \) be the line through \( 0 \) and \( A \). Then it is easy to see that \( G \cap L_A \) is \( \{mA : m \in \mathbb{Z}\} \) and, as \( G \) is not cyclic, \( G \) contains vectors not on \( L_A \). Thus \( G \) contains a vector \( B \) which has the shortest length among all vectors in \( G \) which are not on \( L_A \). We shall now show that \( G = \{mA + nB : m, n \in \mathbb{Z}\} \).

For distinct points \( U, V \) and \( W \) in \( \mathbb{R}^2 \), let \( T(U, V, W) \) be the closed triangular region (including its boundary) with vertices \( U, V \) and \( W \). Also, let \( \theta = (0, 0) \). Now, by construction, the only points of \( G \) that lie in \( T(\theta, A, B) \) are its three vertices. Since \( X \in G \) if, and only if, \(-X \in G \), we deduce that the only points of \( G \) that lie in \( T(\theta, -A, -B) \) are also its three vertices. Since \( G \) is mapped onto itself by the translation by the vector
$A + B$ it follows that the only points of $G$ that lie in $T(A + B, B, A)$ are (again) its three vertices. These facts imply that the only points of $G$ that lie in the parallelogram with vertices $0, A, A + B$ and $B$ are its four vertices, and it follows easily from this that $G = \{mA + nB : m, n \in \mathbb{Z}\}$.

The complete solution

We know that $\mathcal{L}$ is a sub-lattice of $\mathbb{Z}^2$, and it only remains to identify a pair of generators of $\mathcal{L}$. We have already seen that $\Gamma \subset \mathcal{L}$, where $\Gamma = \{s(p, q) + t(-q, p) : s, t \in \mathbb{Z}\}$, but there need not be equality here. In Figure 1 we have illustrated the cases $(p, q) = (2, 1)$ and $(p, q) = (3, 1)$. In each case the square has vertices $(0, 0), (p, q), (-q, p)$ and $(p - q, p + q)$. In the first case, the centre of the square is not in $\mathcal{L}$; in the second case, the centre is in $\mathcal{L}$ but it is not in $\Gamma$. We shall now show that this is typical of the cases when $p^2 + q^2$ is odd and when it is even.

![Figure 1](https://www.cambridge.org/core)

**Theorem 1**: Suppose that $p$ and $q$ are coprime positive integers.

(i) If $p^2 + q^2$ is odd then $\mathcal{L}$ is the square lattice $\Gamma$.

(ii) If $p^2 + q^2$ is even then $\mathcal{L}$ is the square lattice $\Sigma$ generated by $(h, k)$ and $(k, -h)$, where $h = (p - q)/2$ and $k = (p + q)/2$.

Before we give the proof of Theorem 1, we obtain some preliminary information about points $(x, y)$ in $\mathcal{L}$. Take $(x, y)$ in $\mathcal{L}$ and, as in (1), let $(u, v)$ be the reflection of $(x, y)$ across $L$; thus $(u, v) \in \mathbb{Z}^2$. Now (1) gives

$$u + x = 2sp, \quad y + v = 2sq, \quad u - x = 2tq, \quad y - v = 2tp.$$ 

Since $p, q, x, y, u$ and $v$ are all integers, we see that $s$ and $t$ are rational. Now let $s = a/b$, where $a$ and $b$ are coprime and $b > 0$. Then $2pa = b(u + x)$ and $2qa = b(y + v)$, so that $b$ divides $2p$ and $2q$. As $p$ and $q$ are coprime, this implies that $b$ divides 2. Thus $b$ is 1 or 2. Similarly, we may write $t = c/d$ where $c$ and $d$ are coprime, and $d$ is 1 or 2. We have now shown that we can write $s = [s] + r/2$ and $t = [t] + r'/2$, where $[s]$ and $[t]$ are integers (the integral parts of $s$ and $t$), and $r$ and $r'$ are either 0 or 1. We shall now show that $r = r'$. 

---

**Core terms of use, available at** [https://www.cambridge.org/core/terms](https://www.cambridge.org/core/terms). [https://doi.org/10.1017/S0025557200004563](https://doi.org/10.1017/S0025557200004563)
We recall from (1) that \( x = ps - qt \) and \( y = sq + pt \). If \( s \) is an integer then, as \( t = c/d \), we see that \( d \) divides \( pc \) and \( qc \); thus \( d = 1 \) and \( t \) is an integer. Similarly, if \( t \) is an integer, then so is \( s \), and we have proved the next lemma.

**Lemma 3:** Suppose that \((x, y) \in \mathcal{L}\), and that (1) holds. Then \( s = [s] + r/2 \) and \( t = [t] + r/2 \), where \( r \) is 0 or 1. In particular, \( s + t \) and \( s - t \) are integers.

The proof of Theorem 1: First, we consider the case when \( p^2 + q^2 \) is odd. In this case one of \( p \) and \( q \) is even and the other is odd, so that \( p - q \) is odd. As \( x = sp - tq = ([s]p - [t]q) + \frac{1}{2}r(p - q) \), we see that \( \frac{1}{2}r(p - q) \) is an integer; hence \( r = 0 \). Thus \( s \) and \( t \) are integers, and (1) now shows that \( \mathcal{L} \subset \Gamma \). Since (in all cases) \( \Gamma \subset \mathcal{L} \), we have \( \mathcal{L} = \Gamma \) and (i) is proved.

Finally, we consider the case when \( p^2 + q^2 \) is even. Then \( p \) and \( q \) are both odd, and \( p - q \) and \( p + q \) are both even. In this case we write \( h = \frac{1}{2}(p - q), \quad k = \frac{1}{2}(p + q), \quad p = h + k, \quad q = k - h; \) thus \((h, k)\) and \((k, -h)\) are in \( \mathbb{Z}^2 \). Since these two points are reflections of each other across \( \mathcal{L} \) (see (1) with \( s = t = \frac{1}{2} \)), we see that \( \Sigma \subset \mathcal{L} \). Finally, we show that \( \mathcal{L} \subset \Sigma \). If \((x, y) \in \mathcal{L} \) then
\[
\begin{pmatrix} x \\ y \end{pmatrix} = s \begin{pmatrix} p \\ q \end{pmatrix} + t \begin{pmatrix} -q \\ p \end{pmatrix} = s \begin{pmatrix} h + k \\ k - h \end{pmatrix} + t \begin{pmatrix} h - k \\ k + h \end{pmatrix} = (s + t) \begin{pmatrix} h \\ k \end{pmatrix} + (s - t) \begin{pmatrix} h \\ -k \end{pmatrix}
\]
which is in \( \Sigma \) since \( s + t \) and \( s - t \) are integers. Thus \( \mathcal{L} = \Sigma \) as required.

A. F. BEARDON

Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge CB3 0WB
e-mail: afb@dpmms.cam.ac.uk

96.36 Prime and irreducible elements of the ring of integers modulo \( n \)

**Introduction**

Divisibility is an important concept in number theory and it generalises to rings, here always assumed commutative with multiplicative identity element 1, where concepts such as factorisation of elements, prime elements, and irreducible elements can be defined. Although these concepts are most important in integral domains, nonetheless they are of some interest in more general rings also.