Let $R \subset \mathbf{C}$ be an order of discriminant $\Delta < 0$. Let $p > 2$ be a prime not dividing Δ and let $t \in \mathbf{Z}$ strictly between 0 and p such that $t^2 \equiv \Delta \pmod{p}$ and $t \equiv \Delta \pmod{2}$. Let $I \subset R$ be the ideal generated by p and $t - \sqrt{\Delta}$. It has index p in R.

We define a sequence of elements $z_i \in I$ as follows:

$$\begin{aligned} z_0 &= p, \\ z_1 &= \frac{t - \sqrt{\Delta}}{2}, \\ z_{i+1} &= z_{i-1} - q_i z_i, \qquad \text{for } 2 \le i < m. \end{aligned}$$

Here q_i is the integral part of the quotient of $\operatorname{Re} z_{i-1}$ by $\operatorname{Re} z_i$ and $i = m$ is the smallest index for which $z_i = 0$. We have $m \ge 2$. The real parts of the z_i form a strictly decreasing sequence as do the numbers $(-1)^i \operatorname{Im} z_i$. Each successive pair z_i, z_{i+1} forms a $\mathbf{Z}$ basis for I.

Here are two examples: take $\Delta = -4$ and $p = 13$. We have $t = 10$ and $m = 6$. The sequence of the z_i is given by $13, 5 - i, 3 + 2i, 2 - 3i, 1 + 5i, -13i$. With $\Delta = -8$ and $p = 3$, we have $t = 2$ and $m = 4$ and the sequence of the z_i is given by $3, 1 - \sqrt{-2}, 3\sqrt{-2}$.

Definition. An a non-zero element $z \in I$ is called *minimal* if the only element $w \in I$ for which $|\operatorname{Re} w| < |\operatorname{Re} z|$ and $|\operatorname{Im} w| < |\operatorname{Im} z|$ is $w = 0$.

Lemma. *The elements $z_1, z_2, \ldots, z_{m-1}$ are precisely the minimal elements of I that have positive real part.*

Corollary. *If I is principal, then it is generated by z_i, where i is the smallest index for which $\operatorname{Re} z_i < \sqrt{p}$.*

Proof. Since p is not a square, a generator z of I cannot be purely imaginary or real. Multiplying z by -1 if necessary, we may assume that $\operatorname{Re} z > 0$. Then z is a minimal element of I. By the lemma it is therefore equal to one of the z_i. Since $|z_i|^2 = [R : I] = p$, clearly $\operatorname{Re} z_i < \sqrt{p}$. There may be more indices i for which z_i is a generator. Pick the one with largest real part. Then z_{i-1} is certainly *not* a generator of I and therefore $|z_{i-1}|^2 \ge 2|z_i|^2$. We have

$$(\operatorname{Re} z_{i-1})^2 = |z_{i-1}|^2 - (\operatorname{Im} z_{i-1})^2 \ge 2|z_i|^2 - (\operatorname{Im} z_i)^2 \ge |z_i|^2 = p.$$

This shows that i is the smallest index for which $\operatorname{Re} z_i < \sqrt{p}$ as required.

Proof of the lemma. Let z be minimal with $\operatorname{Re} z > 0$. Then z can be "seen" from the origin in between z_{i-1} and z_{i+1} say. In other words $z = (\lambda - \mu) z_{i+1} + \mu z_{i-1}$ for certain $\lambda, \mu \in \mathbf{R}$ satisfying $\lambda \ge \mu \ge 0$. Let $q \in \mathbf{Z}$ be the integral part of the quotient of $\operatorname{Re} z_{i-1}$ by $\operatorname{Re} z_i$. Then we have $z_{i+1} = z_{i-1} - q z_i$ and hence $z = \lambda z_{i+1} + \mu q z_i$. It follows that λ and $q\mu$ are in $\mathbf{Z}$.

Let $B \subset \mathbf{C}$ be the open box given by

$$B = \{w \in \mathbf{C} : |\operatorname{Re} w| < |\operatorname{Re} z| \text{ and } |\operatorname{Im} w| < |\operatorname{Im} z|.$$

By minimality of z we have $B \cap I = \{0\}$. If $\lambda = 0$ then $\mu = 0$ in contradiction with the fact that $z \neq 0$. So we have $\lambda \geq 1$. Recall

$$z = (\lambda - \mu)z_{i+1} + \mu z_{i-1}.$$

If $\mu > 1$, then z_{i-1} is in B. So we have $\mu \leq 1$. If $\lambda \geq 2$ then either $\lambda - \mu$ or μ exceeds 1 or we have $\lambda - \mu = \mu = 1$. In all cases the element z_{i+1} is in B. Therefore we have $\lambda = 1$.

This means that $z = z_{i+1} + \mu' z_i$ for some $\mu' \in \mathbf{Z}$ satisfying $0 \leq \mu' \leq q$. We observe that $|\mathrm{Im}\, z_{i+1}| = |\mathrm{Im}\, z_{i-1}| + q|\mathrm{Im}\, z_i|$. This shows that $q|\mathrm{Im}\, z_i| < |\mathrm{Im}\, z_{i+1}|$ so that $|\mathrm{Im}\, z_i| < |\mathrm{Im}\, z_{i+1}| - (q-1)|\mathrm{Im}\, z_i|$. It follows that z_i is in B whenever $\mu' \neq 0, q$. Therefore we have either $\mu' = 0$ and $z = z_{i+1}$ or $\mu' = q$ and $z = z_{i-1}$ as required.