



**Lemma 1.** Let  $\mathcal{M}$  be a primitive integer norm pointset with characteristic  $D$ . If  $p$  is a rational prime that is also prime in  $\mathcal{O}_{-D}$ , and  $p$  divides the norm of some pairwise difference in  $\mathcal{M}$ , then  $p$  divides it with even multiplicity.

*Proof.* Translate and possibly reflect  $\mathcal{M}$  in the plane so that, of the two points whose pairwise distance's norm  $p$  divides, one lies at the origin and the other lies on the positive  $x$ -axis. Denote the latter point by  $\beta$ .

We will assume, for an contradiction, that  $p$  divides  $[\beta]$  with odd multiplicity - that is, there exist some positive integers  $c$  and  $k$  such that  $\beta = \sqrt{p^{2k-1}c}$ , but  $p$  does not divide  $c$ .

Now let  $\alpha$  be any other arbitrary point in  $\mathcal{M}$ . We will show that  $\alpha$  takes the form

$$\alpha = \frac{\delta\sqrt{p}}{2\sqrt{c}} \quad (1)$$

for some  $\delta \in \mathcal{O}_{-D}$ .

Since  $[\alpha]$ ,  $[\beta]$ , and  $[\alpha - \beta]$  are all integers, we know that

$$[\alpha] - [\beta] - [\alpha - \beta] = \alpha\bar{\beta} + \bar{\alpha}\beta = 2x\sqrt{p^{2k-1}c} = a$$

for some  $a \in \mathbb{Z}$  such that  $x = \frac{a}{2\sqrt{p^{2k-1}c}}$ .

The area of the triangle formed by 0,  $\alpha$ , and  $\beta$  is

$$\frac{1}{2}y\sqrt{p^{2k-1}c} = \frac{b}{4}\sqrt{D}$$

for some  $b \in \mathbb{Z}$  such that  $y = \frac{b\sqrt{D}}{2\sqrt{p^{2k-1}c}}$ .

Now, letting  $\gamma = a + b\sqrt{-D} \in \mathcal{O}_{-D}$ , we obtain the following expression for  $\alpha$ :

$$\alpha = x + y\sqrt{-D} = \frac{a + b\sqrt{-D}}{2\sqrt{p^{2k-1}c}} = \frac{\gamma}{2\sqrt{p^{2k-1}c}}.$$

Since  $\alpha$  has integer norm, the norm of its denominator must divide the norm of  $\gamma$ . So  $p^{2k-1} \mid \gamma\bar{\gamma}$ . Since  $p$  is prime in  $\mathcal{O}_{-D}$ , we must have either  $p^k \mid \gamma$  or  $p^k \mid \bar{\gamma}$ . Since  $p$  is rational, either case implies that  $p^k \mid \gamma$ . Thus there exists some  $\delta \in \mathcal{O}_{-D}$  such that  $\gamma = p^k\delta$ , hence proving  $\alpha$  takes the form given in (1).

First, assume that  $p \neq 2$ . Since  $p \nmid c$ , we must have  $2c \mid [\delta]$ , thus  $p \mid [\alpha]$ . Now, instead assume  $p = 2$ . Then  $\alpha = \frac{\delta}{\sqrt{2c}}$ , so  $2 \mid \delta\bar{\delta}$ , hence  $2 \mid \delta$  since we have assumed  $p = 2$  is prime. So  $\alpha = \frac{\delta'\sqrt{p}}{\sqrt{c}}$  for some  $\delta' \in \mathcal{O}_{-D}$ , and again  $p \mid [\alpha]$ .

Since

$$\begin{aligned} [\alpha - \beta] &= [\alpha] + [\beta] - \alpha\bar{\beta} - \bar{\alpha}\beta = [\alpha] + [\beta] - \sqrt{p^{2k-1}c} \left( \frac{\delta\sqrt{p}}{2\sqrt{c}} + \frac{\bar{\delta}\sqrt{p}}{2\sqrt{c}} \right) \\ &= [\alpha] + [\beta] - p^k \operatorname{Re}(\delta). \end{aligned}$$

Since  $p$  divides all three of these terms, it divides  $[\alpha - \beta]$ .

Now, since  $\alpha$  was an arbitrary point in  $\mathcal{M}$  other than 0 or  $\beta$ , we know if we take some other point  $\eta \in \mathcal{M}$ ,  $p$  will divide both  $[\eta]$  and  $[\eta - \beta]$ . It will also be of the form  $\eta = \frac{\varepsilon\sqrt{p}}{2\sqrt{c}}$  given in (1), thus

$$p \mid p \frac{[\delta - \varepsilon]}{4c} = [\alpha - \eta]$$

since  $p \nmid c$  and, again, if  $p = 2$  then  $p$  divides both  $\delta$  and  $\varepsilon$ . Therefore,  $p$  divides the norms of all pairwise differences in  $\mathcal{M}$ , contradicting our assumption that  $\mathcal{M}$  is primitive.  $\square$

**Lemma 2.** Let  $\mathcal{M}$  be an integer norm pointset with characteristic  $D$ , and let  $s$  be the greatest common divisor of the norms of all pairwise distances in  $M$ . The following are equivalent:

1. For every  $\alpha \in \mathcal{M}$  there exists an ideal  $L \subset \mathcal{O}_{-D}$ , not necessarily unique, such that  $\langle[\alpha]\rangle = L\bar{L}$
2. Every prime  $p$  which is also prime in  $\mathcal{O}_{-D}$  divides  $s$  with even multiplicity. In particular, this occurs if  $\mathcal{M}$  is primitive.

*Proof.* Scale  $\mathcal{M}$  down by  $\sqrt{s}$  to obtain a primitive integer pointset, and let  $\alpha \in \mathcal{M}$ . By Lemma 1, every rational prime  $p$  which is also prime in  $\mathcal{O}_{-D}$  divides  $\frac{[\alpha]}{s}$  with even multiplicity, so factoring  $\langle[\alpha]\rangle$  into prime ideals gives

$$\begin{aligned} \left\langle \frac{[\alpha]}{s} \right\rangle &= \langle p_1 \rangle^{2k_1} \cdots \langle p_k \rangle^{2k_m} L_1 \bar{L}_1 \cdots L_n \bar{L}_n \\ &= \left( \langle p_1 \rangle^{k_1} \cdots \langle p_k \rangle^{k_m} L_1 \cdots L_n \right) \left( \langle p_1 \rangle^{k_1} \cdots \langle p_k \rangle^{k_m} \bar{L}_1 \cdots \bar{L}_n \right) \\ &= J\bar{J} \end{aligned}$$

where  $J = \langle p_1 \rangle^{k_1} \cdots \langle p_k \rangle^{k_m} L_1 \cdots L_n$ . Similarly, factoring  $s$  into prime ideals gives

$$\langle[\alpha]\rangle = \langle s \rangle \left\langle \frac{[\alpha]}{s} \right\rangle = \langle q_1 \rangle^{j_1} \cdots \langle q_k \rangle^{j_m} H_1 \bar{H}_1 \cdots H_n \bar{H}_n J\bar{J}.$$

This factorization becomes  $L\bar{L}$  for some ideal  $L$  if and only if each  $j_i$  is even.  $\square$

**Theorem.**  $\mathcal{O}_{-D}$  contains an element of norm  $[\alpha]$  if and only if  $\langle[\alpha]\rangle$  has such a factorization where  $L$  is principal for some  $\alpha \in \mathcal{M}$ .

*Proof.* Suppose assume the norm of some  $\alpha \in \mathcal{M}$  has such a factorization where  $L$  is principal, and let  $\beta$  be a generator of  $L$ . Then  $[\beta] = [\alpha]$ .

For the other direction, assume  $\beta$  has norm  $[\alpha]$ . Then  $[\langle \alpha \rangle] = \langle \beta \rangle \langle \overline{\beta} \rangle$  gives such a factorization where  $L$  is principal.  $\square$

**Corollary.** Suppose an integer norm pointset  $\mathcal{M}$  has characteristic  $D$ , where  $D$  is a Heegner number, and let  $s$  be the greatest common divisor of the norms of all pairwise distances in  $\mathcal{M}$ .  $\mathcal{M}$  embeds in  $\mathcal{O}_{-D}$  if and only if every prime  $p$  which is also prime in  $\mathcal{O}_{-D}$  divides  $s$  with even multiplicity.

In particular, every primitive integer norm pointset with characteristic  $D$  embeds in  $\mathcal{O}_{-D}$ .

*Proof.* If some prime  $p$  which is also prime in  $\mathcal{O}_{-D}$  does not divide  $s$  with even multiplicity, then no such factorization exists. So for every  $\alpha \in \mathcal{M}$ ,  $\mathcal{O}_{-D}$  contains no element of norm  $[\alpha]$ , thus  $\mathcal{M}$  cannot embed in  $\mathcal{O}_{-D}$ .

Now suppose every prime  $p$  which is also prime in  $\mathcal{O}_{-D}$  does divide  $s$  with even multiplicity. Then the norm of some  $\alpha \in \mathcal{M}$  has such a factorization, and since  $\mathcal{O}_{-D}$  is a principal ideal domain,  $L$  is principal. So there exists an element of norm  $[\alpha]$  for some  $\alpha \in \mathcal{M}$ . Thus  $\mathcal{M}$  embeds in  $\mathbb{Q}(\sqrt{-D})$ . Since the square of every ideal of  $\mathcal{O}_{-D}$  is principal,  $\mathcal{M}$  embeds in  $\mathcal{O}_{-D}$ .  $\square$

The following proposition, proven by Dantong, is the missing direction of Lemma 3 in the paper.

**Proposition.** If  $\mathcal{M}$  is primitive, then  $\langle K_1, \dots, K_n \rangle = \langle 1 \rangle$ .

*Proof.* Suppose some prime ideal  $H \subset \mathcal{O}_{-D}$  divides  $K_i$  for all  $i$ . We know that  $\left\langle \left[ \frac{\beta_i}{r} \right] \right\rangle = \langle [K_i] \rangle = K_i \overline{K_i}$  for all  $i$ . By Lemma 1,  $\left\langle \left[ \frac{\beta_i}{r} \right] \right\rangle = L_i \overline{L_i}$  for some ideal  $L \subset \mathcal{O}_{-D}$  as well. So, for all  $i$ ,  $H_i \mid L_i$  or  $H_i \mid \overline{L_i}$ . In either case,  $\langle [H] \rangle = H \overline{H} \mid L_i \overline{L_i} = \left\langle \left[ \frac{\beta_i}{r} \right] \right\rangle$  for all  $i$ . Thus  $[H] \mid \left[ \frac{\beta_i}{r} \right]$  for all  $i$ .  $\square$