$m \in \mathbb{Z},\ m \neq 0, 1$ は平方因数をもたないとする．2次体の整数環

$$R = \begin{cases} \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\} & (\ m \equiv 2,\ 3 \pmod 4 \text{ のとき}) \\ \mathbb{Z}\left[\dfrac{1+\sqrt{m}}{2}\right] = \left\{a + b\dfrac{1+\sqrt{m}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\} & (\ m \equiv 1 \pmod 4 \text{ のとき}) \end{cases}$$

において 素数 $p \in \mathbb{Z}$ で生成される単項イデアル $(p) = pR = \{pr \mid r \in R\}$ は以下のように R の素イデアル（実は, 極大イデアル）の積で表される.

<table>
<tr><th colspan="3">素数 p ＼ $m \bmod 4$</th><th>2</th><th>3</th><th>1 $\left(\omega = \dfrac{1+\sqrt{m}}{2},\quad \omega^2 - \omega - \dfrac{m-1}{4} = 0\right)$</th></tr>
<tr><td colspan="3" rowspan="2">2</td><td rowspan="2">$(2) = (2,\ \sqrt{m})^2$</td><td rowspan="2">$(2) = (2,\ 1+\sqrt{m})^2$</td><td>$m \equiv 1 \pmod 8$ のとき $(2) = (2,\ \omega)(2,\ -1+\omega)$</td></tr>
<tr><td>$m \equiv 5 \pmod 8$ のとき $R/(2) \cong \mathbb{Z}[X]/(2,\ X^2 - X + 1)$
$\cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 - X + 1) \cong \mathbb{F}_4$ は体だから (2) は R の素イデアル</td></tr>
<tr><td rowspan="3">$p \geq 3$</td><td colspan="2">$p \mid m$</td><td colspan="2">$(p) = (p,\ \sqrt{m})^2$
$R/(p,\ \sqrt{m}) \cong \mathbb{Z}[X]/(p,\ X,\ X^2 - m)$
$\cong \mathbb{Z}[X]/(p,\ X) \cong \mathbb{Z}/p\mathbb{Z}$</td><td>$(p) = (p,\ -h+\omega)^2 \longleftarrow$ ($p \neq 2$ より $\exists h \in \mathbb{Z}$ s.t. $2h \equiv 1 \pmod p$)</td></tr>
<tr><td rowspan="2">$p \nmid m$</td><td>$\left(\dfrac{m}{p}\right) = 1$</td><td>$(p) = (p,\ a+\sqrt{m})(p,\ -a+\sqrt{m})$</td><td>$(p) = (p,\ ah-h+\omega)(p,\ -ah-h+\omega)$ $\longleftarrow$ ($p \neq 2$ より $\exists h \in \mathbb{Z}$ s.t. $2h \equiv 1 \pmod p$)</td></tr>
<tr><td>$\left(\dfrac{m}{p}\right) = -1$</td><td>$R/(p) \cong \mathbb{Z}[X]/(p,\ X^2 - m)$
$\cong (\mathbb{Z}/p\mathbb{Z})[X]/(\underbrace{X^2 - m}_{\text{既約}}) \cong \mathbb{F}_{p^2}$ は体だから
(p) は R の素イデアル</td><td>$R/(p) \cong \mathbb{Z}[X]\Big/\left(p,\ X^2 - X - \dfrac{m-1}{4}\right)$
$\cong (\mathbb{Z}/p\mathbb{Z})[X]\Big/\left(\underbrace{X^2 - X - \dfrac{m-1}{4}}_{\text{既約}}\right) \cong \mathbb{F}_{p^2}$ は体だから
(p) は R の素イデアル</td></tr>
</table>

上の表において

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & (\exists a \in \mathbb{Z} \text{ s.t. } a^2 \equiv m \pmod p) \\ -1 & (\text{その他}) \end{cases}$$

$\left(\dfrac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ $\left(\begin{array}{c|cc} & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}\right)$ は準同型写像, 即ち

$\forall m, n \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対し $\left(\dfrac{mn}{p}\right) = \left(\dfrac{m}{p}\right)\left(\dfrac{n}{p}\right)$