Preliminaries

- $\mathcal{O}_K$: The ring of integers.
- ect.

Circle Correspondence

We define S_K as the Schmidt Arrangement of $\mathcal{O}_K$, where $K = \left|\sqrt{\Delta}\right|$. Assume that Δ is a negative integer and that 0 divides itself.

We have a triple $(r, x, y) \in \mathbb{Z}^3$, which must adhere to

$$r \mid x^2 + y + y^2. \tag{1}$$

The triple results in a circle with curvature $2ir$, and a curvature-center $2(x + iy) + i$. We can represent the circle in S_K by the matrix

$$\begin{pmatrix} a + a'i & c + c'i \\ b + b'i & d + d'i \end{pmatrix} \tag{2}$$

which results in the the triple

$$(m, n, l) = \begin{cases} (bd' - b'd, bc' - a'd, a'd' - b'c'), & \text{if } \Delta = -1 \\ (b'd - bd', a'd - bc', bc - ad), & \text{otherwise} \end{cases}$$

Case 1. $r = 0$. To find the corresponding circle in S_K we let $a' = -\gcd(x, y)$. Then

$$a = \frac{-a'(1 + \|i\|\, y)}{x}, \quad c = c' = 0, \quad b = d = \frac{-x}{a}, \quad b' = d' = \frac{y}{a'}.$$

- If $x = 0$ and $y = 0$ then $(r, x, y) = (0, 0, 0)$. This yields a 2×2 identity matrix.
- (IGNORE for now) If $x \neq 0$ then we find $a', a, b', b, c', c, d', d$ from the equations above, and where (1) is satisfied.

Case 2. $r \neq 0$. Let p be a prime that divides r, $p \mid r$, and let e be the exponent of the largest power of p dividing a particular variable.

We define $e_{b'}$, e_d, and $e_{d'}$ as

$$e_d = \begin{cases} 0 & e_{1+y} = 0 \\ \min(e_r, e_x) & \text{otherwise} \end{cases} \quad \text{and} \quad e_{b'}, e_{d'} = \begin{cases} 0 & e_y = 0 \\ \min(e_r, e_x) & \text{otherwise} \end{cases} \tag{3}$$

To find d' we have that

$$d' = \prod_{p \mid r} p^{e_{d'}}. \tag{4}$$

Then the following systems of congruences can be solved

$$dy \equiv -d'x \bmod p^{e_r} \qquad dx \equiv d'(1 + y) \bmod p^{e_r}, \tag{5}$$

and

$$b'(dy + d'x) \equiv -ry \bmod p^{e_r + e_{d'}} \qquad b'\left(dx - d'(1 + y)\right) \equiv -rx \bmod p^{e_r + e_{d'}}. \tag{6}$$

We can then find the following variables

$$b = \frac{r + b'd}{d'} \qquad a = \frac{bx - b'(1 + y)}{r}$$

$$a' = \frac{by + b'x}{r} \qquad c = \frac{dx - d'(1 + y)}{r}$$

$$c' = \frac{d'x + dy}{r}.$$

– **Example 1:** Let $(r, x, y) = (3, 2, 1)$ with $p = 3$. Then from (3), $e_d = 0$, $e_{b'} = 0$, $e_{d'} = 0$. We also have that $e_r = 1$, since the largest power $p \mid r$ is 1. Then, by (4),

$$d' = \prod_{1} p^{e_{d'}} = \prod_{1} 3^0 = \prod_{1} 1 = 1.$$

By (5),

$$\begin{aligned} d &\equiv -2 \bmod 3 \\ 2d &\equiv -6 \bmod 3, \end{aligned}$$

which $d = 1$ satisfies. By (6),

$$\begin{aligned} 3b' &\equiv -3 \bmod 3 \\ 0 &\equiv -6 \bmod 3. \end{aligned}$$

which yields no solution for b' (this is not a problem though). Solving for each variable

$$\begin{aligned} b &= 3 + b' & a &= \frac{2(3+b') - 2b'}{3} = \frac{6}{3} = 2 \\ a' &= \frac{3 + b' + 2b'}{3} = 1 + b' & c &= 2 - 2 = 0 \\ c' &= \frac{2+1}{3} = 1. \end{aligned}$$

Substituting into the matrix from (2),

$$\begin{pmatrix} 2 + i + ib' & i \\ 3 + b' + ib' & 1 + i \end{pmatrix}.$$

We can exclude b' in the following way

$$\begin{pmatrix} 2 + i + ib' & i \\ 3 + b' + ib' & 1 + i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -b' & 1 \end{pmatrix} = \begin{pmatrix} 2 + i + ib' - ib' & i \\ 3 + b' + ib' - b' - ib' & 1 + i \end{pmatrix} = \begin{pmatrix} 2 + i & i \\ 3 & 1 + i \end{pmatrix}$$

– **Example 2:** Let $r, x, y) = (2, 4, 2)$ with $p = 2$. Then from (3), $e_d = 0$, $e_{b'} = 1$, $e_{d'} = 1$. We also have that $e_r = 1$, since the largest power of $p \mid r$ is 1. Then, by (4),

$$d' = \prod_{2|2} p^{e_{d'}} = \prod_{1} 2^1 = \prod_{1} 2 = 2.$$

By (5),

$$\begin{aligned} 2d &\equiv -4 \bmod 2 \\ 4d &\equiv 6 \bmod 2, \end{aligned}$$

which $b' = 0$ satisfies. Solving for each variable

$$\begin{aligned} b &= \frac{2+0}{2} = 1 & a &= \frac{4-0}{2} = 2 \\ a' &= \frac{2+0}{2} = 1 & c &= \frac{0-6}{2} = -3 \\ c' &= \frac{8+0}{2} = 4. \end{aligned}$$

Substituting into the matrix from (2),

$$\begin{pmatrix} 2 + i & -3 + 4i \\ 1 & 2i \end{pmatrix}.$$

– **Example 3:** space for one more example, maybe another odd situation like example 1, if one is to arise.

Algorithm

We present the following algorithm used in our program.

Function 1 : Check condition (1) and the $p \mid r$.

if $r \mid x^2 + y + y^2$ is not True **then**
    Raise an exception.
if (p is prime) is True **then**
    if $p \mid r$ is not True **then**
        Raise an exception.
else
    Raise an exception.

Function 2 : Find e_d.

Require: Function 1 to hold true.

if $p \mid (1 + y) = 0$ **then**
    $e_d \leftarrow 0$
else
    $e_r \leftarrow r/p$ ▷ Want number of times $p \mid r$ and $p \mid x$
    $e_x \leftarrow x/p$
    $e_d = \min(e_r, e_x)$