数理統計学特論

199X223X 綿岡晃輝

神戸大学大学院 システム情報学研究科 計算科学専攻

1　BIBD(11, 11, 5, 5, 2) と BIBD(13, 13, 4, 4, 1) を作れ.

1.1　BIBD(11, 11, 5, 5, 2)

$V := \mathbb{Z}/11\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ とする.
V = {
{2, 4, 7, 10, 0 },
{5, 6, 7, 9, 0 },
{4, 5, 8, 9, 10 },
{1, 6, 8, 10, 0 },
{3, 4, 6, 7, 8 },
{2, 3, 6, 9, 10 },
{1, 3, 4, 9, 0 },
{2, 3, 5, 8, 0 },
{1, 3, 5, 7, 10 },
{1, 2, 7, 8, 9 },
{1, 2, 4, 5, 6 },
}

1.2　BIBD(13, 13, 4, 4, 1)

$V := \mathbb{Z}/13\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ とする.
V = {
{1, 2, 5, 7 },
{3, 5, 10, 11 },
{5, 6, 12, 0 },
{7, 9, 10, 12 },
{7, 8, 11, 0 },
{1, 6, 8, 10 },
{4, 5, 8, 9 },
{3, 4, 6, 7 },
{1, 4, 11, 2 },
{1, 3, 9, 0 },
{2, 4, 10, 0 },
{2, 6, 9, 11 },
{2, 3, 8, 12 },
}

2 $z^2 = 6x^2 - y^2$ は自明な解しか持たないことを示せ.

$z^2 = 6x^2 - y^2$ は自明な解以外を持つと仮定し, 矛盾を導く.
任意の整数 k に対して,

$$(3k+1)^2 = 9k^2 + 6k + 1 \equiv 1 \ (mod.3) \tag{1}$$
$$(3k+2)^2 = 9k^2 + 12k + 4 \equiv 1 \ (mod.3) \tag{2}$$

が言える.

$$x = 3^{\alpha}x' \ (\alpha \in 0 \cup \mathbb{N}, x' : 3 \text{ の倍数でない整数})$$
$$y = 3^{\beta}y' \ (\beta \in 0 \cup \mathbb{N}, y' : 3 \text{ の倍数でない整数})$$
$$z = 3^{\gamma}z' \ (\gamma \in 0 \cup \mathbb{N}, z' : 3 \text{ の倍数でない整数})$$

とおき, 一般性を失わないので, $\beta \geq \gamma$ とすると,

$$\begin{aligned} 6x^2 &= 6(3^{\alpha}x')^2 \\ &= 3^{2\alpha+1}\{2(x')^2\} \end{aligned}$$

となり,

$$\begin{aligned} y^2 + z^2 &= (3^{\beta}y')^2 + (3^{\gamma}z')^2 \\ &= 3^{2\gamma}\{(3^{\beta-\gamma}y')^2 + (z')^2\} \end{aligned}$$

となる.
ここで, x' は 3 の倍数ではないため, (1),(2) より $2(x'^2) \equiv 2 \ (mod.3)$ となる.
また, $(3^{\beta-\gamma}y')^2 \equiv 0, (z')^2 \equiv 1 \ (mod.3)$ なので, $(3^{\beta-\gamma}y')^2 + (z')^2 \equiv 1 \ (mod.3)$ となる.
つまり, $2(x')^2$ も $(3^{\beta-\gamma}y')^2 + (z')^2$ も 3 の倍数にはならない.
故に, $6x^2$ と $y^2 + z^2$ を素因数分解した時, 3 の累乗が同じにならないため,

$$6x^2 \neq y^2 + z^2$$

となり, 矛盾.
従って,$z^2 = 6x^2 - y^2$ は自明な解しか持たない.