1　オープンアドレス法に関する議論

補題 1. m, t を正整数とする。m, t が互いに素であるための必要十分条件は、任意の整数 s, g $(0 \leq s < m,\ 0 \leq g < m)$ に対して

$$g \equiv s + jt \mod m$$

を満たすような非負整数 j が存在することである。

証明. 最初に、十分性を示す。$(g, s) = (0, 0),\ (g, s) = (1, 0)$ を代入すると、

$$0 \equiv jt \mod m$$
$$1 \equiv j't \mod m$$

が成り立つから、ある整数 k を用いて、

$$mk + (j' - j)t = 1$$

が成り立つ。したがって、m, t は互いに素である。よって十分性が示された。

次に、必要性を示す。まず $s = 0$ のときを示す。

ある非負整数 j_0, j_1 $(0 \leq j_0 < j_1 < m)$ に対して

$$g \equiv j_0 t \mod m$$
$$g \equiv j_1 t \mod m$$

が成り立つと仮定すると，

$$0 \equiv (j_1 - j_0)t \mod m$$

である。t は m と互いに素であるから，両辺を t で割ることができ，

$$0 \equiv j_1 - j_0 \mod m$$

よって $j_0 = j_1$ であるが，これは $j_0 < j_1$ に矛盾する。したがって，非負整数 j を $0 \leq j < m$ の範囲で動かすとき，jt を m で割った余りはすべて相異なる。

このことと鳩の巣原理により，

$$g \equiv jt \mod m \tag{1}$$

を満たす非負整数 j が $0 \leq j < m$ の範囲に唯一つ存在する。

つぎに $s \neq 0$ のときを示す。(1) の両辺に s $(0 \leq s < m)$ を加え，さらに $g + s$ を m で割った余りを g' とおくと，

$$g' \equiv s + jt \mod m$$

であり，しかも $0 \leq g' < m$ であるから，必要性が示された。 □