1 オープンアドレス法に関する議論

補題 1. 正整数 m, t が互いに素であるならば，任意の整数 s, g $(0 \le s < m,\ 0 \le g < m)$ 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。

証明. まず $s = 0$ のときを示す。

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

$$\begin{aligned} g &\equiv j_0 t \mod m \\ g &\equiv j_1 t \mod m \end{aligned}$$

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 $0 \le j < m$ 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 $0 \le j < m$ の範囲に唯一つ存在する。

つぎに $s \ne 0$ のときを示す。(1) の両辺に s $(0 \le s < m)$ 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 $0 \le g' < m$ であるから，補題 1 が成り立つ。 □