問1.1

「$\mathbb{Z}/m\mathbb{Z}$ が体になる $\Leftrightarrow$ $m$ が素数」を示す。

$\mathbb{Z}/m\mathbb{Z}$ の完全代表系を $\bar{0}, \bar{1}, \cdots, \overline{m-1}$ とする。

($\Rightarrow$)

$m$ は合成数であるとすると、$\exists a, b$ s.t. $ab=m$ $(1 \leq a, b \leq m-1)$

であるから、

$$\bar{0} = \bar{a} \cdot \bar{b} \quad \cdots ①$$

である。

$\bar{a}$ に逆元 $\bar{c}$ があるとすると $\bar{a} \cdot \bar{c} = \bar{1}$ となる。

①に $\bar{c}$ を作用すると

$$\bar{0} = \bar{c} \cdot \bar{a} \cdot \bar{b} = \bar{b}$$

となるが、これは $1 \leq b \leq m-1$ に矛盾する。

($\Leftarrow$)

$m$ は素数であるとする。$\bar{a} \neq \bar{0}$ であるすべての $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ に対し、逆元が存在することを示せばよい。

今、$a \cdot 0, a \cdot 1, \cdots, a \cdot (m-1)$ という $m$ 個の数を考える。

これらの数を $m$ で割った余りは、全て異なる…② ことを示す。

$\exists i, j$ s.t. $0 \leq i \leq j \leq m-1$ が $ai \equiv aj \bmod m$ となる $i, j$ が存在するとすると、

$a(j-i) \equiv 0 \pmod m$ となる。$0 \leq j-i \leq m-1$ であり、

$\gcd(a, m) = 1$ ($\because m$ は素数) だから $j-i = 0$。$\therefore i = j$

よって、②は真であり、$a \cdot 0, \cdots, a \cdot (m-1)$ の中に $m$ で割った余りが $1$ であるものが存在する。これを $a \cdot c$ とすると、

$\bar{a} \cdot \bar{c} = \bar{1}$。 ■