2010年6月8日配布
2010年6月15日提出
2010年6月29日返却

1. m を正の整数とし、$\mathbb{Z}/m\mathbb{Z}$ に演算 $\times$ を次のように定義することができる。

$$\times : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ \times([a],[b]) = [ab].$$

この写像 $\times$ は well-defined であることを示せ。

$$\begin{aligned}
[a]=[a'],[b]=[b'] \in \mathbb{Z}/m\mathbb{Z} &\implies m|(a-a'),\ m|(b-b') \\
&\implies m|(a-a')b,\ m|a'(b-b') \\
&\implies m|(a-a')b + a'(b-b') \\
&\implies m|(ab-a'b') \\
&\implies [ab]=[a'b'].
\end{aligned}$$

2. m を正の偶数とし、写像 $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/2m\mathbb{Z}$ を次のように定義することができる。

$$f([a]) = [a^2].$$

ただし、$[a] \in \mathbb{Z}/m\mathbb{Z}$, $[a^2] \in \mathbb{Z}/2m\mathbb{Z}$ である。この写像 f は well-defined であることを示せ。

$$\begin{aligned}
[a]=[a'] \in \mathbb{Z}/m\mathbb{Z} &\implies m|(a-a') \\
&\implies m|(a-a'),\ 2|(a-a') \qquad (m \text{ は偶数だから}) \\
&\implies m|(a-a'),\ 2|((a-a')+2a') \\
&\implies m|(a-a'),\ 2|(a+a') \\
&\implies 2m|(a-a')(a+a') \\
&\implies 2m|(a^2-a'^2) \\
&\implies [a^2]=[a'^2] \in \mathbb{Z}/2m\mathbb{Z}.
\end{aligned}$$