

HW1

0.3 12

Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are not relatively prime then there is an integer b such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$

0.3 13

Let $n \in \mathbb{Z}$, $n > 1$ and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \pmod{n}$ (use the fact that g.c.d. of two integers is a \mathbb{Z} -linear combination of the integers)

Proof. By Euclidean algorithm, $\exists x, y \in \mathbb{Z}$ s.t. $ax + ny = (a, n) = 1$, so $1 - ax = yn$, hence $ax \equiv 1 \pmod{n}$ \square

1.3 15

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition

Proof. Let $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$ be cycle decomposition to product of k disjoint cycles. Suppose $|\sigma| = n$. Since disjoint cycles commutes,

$$\sigma^n = \gamma_1^n \gamma_2^n \cdots \gamma_k^n = 1 \quad \Longleftrightarrow \quad \gamma_1^n = \gamma_2^n = \cdots = \gamma_k^n = 1$$

Therefore n is a common multiple of length of $\gamma_1, \dots, \gamma_k$. By definition of order of σ , n is the smallest common multiple, i.e. the l.c.m. of the length of the cycles \square