MATH 111A, 30 Oct 2013

Exercise 11 on p. 33: Let $\sigma = (1\ 2\ 3\ \dots\ m) \in S_m$ and $i \in \mathbb{N}$. Set $\tau = \sigma^i$.

Claim: τ is an m-cycle $\iff \gcd(i, m) = 1$.

Proof.

Observation 1: From class we recall that for $\ell \in \mathbb{N}$ $\tau^\ell(k) = \sigma^{i\ell}(k) = [k + i\ell]$, where $[k+i\ell]$ is the unique element in $\{1, \dots, m\}$ which is congruent to $k + i\ell$ modulo m. Hence $\tau^\ell(k) = k$ iff $m \mid i\ell$.

Setting $\ell_0 := \min\{\ell \in \mathbb{N} \mid m \text{ divides } i\ell\}$, we thus obtain: For each $k \in \{1, \dots, m\}$, the smallest positive integer ℓ with $\tau^\ell(k) = k$ equals ℓ_0.

Observation 2: $\ell_0 = \dfrac{m}{\gcd(i,m)}$. This is immediate from the Fundamental Theorem of Arithmetic (Math 8 material), which we take as a given in this class.

Deriving the claim

τ is an m-cycle

$\iff \tau = (a_1, \dots\ a_m)$ with $\{a_1, \dots, a_m\} = \{1, \dots, m\}$

$\iff$ for each $k \in \{1, \dots, m\}$, the least integer ℓ with $\tau^\ell(k) = k$ equals m

$\iff \ell_0 = m$

Here the final equivalence follows from Observation 1.

By Observation 2, $\ell_0 = m \iff \gcd(i, m) = 1$,

which completes the proof.