Non-fixed points

KAIST 201[redacted] Myeongjae Lee

April 10, 2012

Let X be a finite non-empty set. Suppose that there is a function $f : X \to X$ such that $f^{20120407}(x) = x$ for all $x \in X$. Prove that the number of elements x in X such that $f(x) \neq x$ is divisible by 20120407

Proof. Since $f^{20120407}(X) = X$, $f(X) = X$. That is, f is surjective. Then f is bijective because X is finite. Define $Y = \{x \in X | f(x) \neq x\}$. Let the number of elements of Y is n. Since 20120407 is prime, let's denote 20120407 by p.

If Y is empty, $n = 0$ so it's divisible. If not, suppose $y_1, y_2 \in Y$. Define a relation $\sim$ by $y_1 \sim y_2$ iff $\exists k \in N$ such that $y_1 = f^k(y_2)$. Then we can choose such $k < p$ since f^p is identity. This relation becomse an equivalence relation.
- $a \sim a$ by $k = 0$
- $a \sim b$ implies $b \sim a$ because $a = f^k(b)$ implies $f^{p-k}(a) = f^p(b) = b$
- $a \sim b$ and $b \sim c$ implies $a \sim c$ because $a = f^{k_1}(b), b = f^{k_2}(c)$ implies $a = f^{k_1+k_2}(c)$

Claim : each equivalent class has p elements.
Let $y \in Y$. $\forall k < p, f^k(y) \neq y$ because if so, since $(p, x) = 1, \exists m_1, m_2 \in Z$ such that $m_1 p + m_2 k = 1$. Then, $f(y) = f^{m_1 p + m_2 k}(y) = y$ since f is bijective. This is contradiction to $y \in Y$. That is, if $k_1 < k_2 < p$, $f^{k_1}(y) \neq f^{k_2}(y)$ since $f^{k_2}(y) = f^{k_2 - k_1}(f^{k_1}(y))$ and $k_2 - k_1 < p$. So all $f^k(y)$ for $k < p$ are distict. By this fact and because f^p is identity, each equivalent class has p elements in the form of $< y >= \{f^k(y) : 0 \leq k \leq p-1\}$

If Y is divided to r equivalent classes, then $n = pr$. Therefore, p divides n.