MATH 1025: Introduction to Cryptography

Bonus 2

𐃺 𐃱 𐃹 𐃲 𐃶 𐃸 𐃺 𐃻 𐃳 𐃺 𐃴 𐃺 𐃵 𐃺 𐃻 𐃺 𐃸
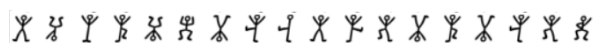
exhaustive rotation

Problem [3 **pts**] By a necklace we understand a circular arrangement of colored beads. The necklaces consist of p beads (prime number) and there are $0 < a < p$ colors. We say that two necklaces are equivalent if one can be obtained from the other via rotation. Show that the equivalence classes either contain one element (all beads of the same color) or p elements (otherwise).[1]

---

[1]**Hint:** number the beads and suppose the necklace coincides with its rotation by $\frac{2k\pi}{p}$ for some $0 < k < p$. Then the color of the bead with index 0 is the same as of the one with index k, but then the color of the bead with index k is the same as of the one with index $2k$...