**Demonstrations**

Cyclically permuting $\mathbb{Z}/p\mathbb{Z}$ illustrated with cards.

The Rubik’s cube group.

**Recall**

$\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ consists of multiplication maps $l_m$ where $\gcd(m,n) = 1$, and so can be identified with the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of integers coprime to $n$, taken modulo $n$.

*Example.* $(\mathbb{Z}/10\mathbb{Z})^\times = \{ 1, 3, 7, 9 \}$ and $3 \cdot 7 = 21 = 1$ in $(\mathbb{Z}/10\mathbb{Z})^\times$.

The order of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is denoted by $\varphi(n)$. The function $\varphi$ is called *Euler’s phi function*.

**Discussion**

A gift shop sells necklaces with $p$ beads where each bead is available in $a$ colors. How many possible such necklaces are offered by the gift shop?

**Problems**

1. Determine the subgroups of $(\mathbb{Z}/15\mathbb{Z})^\times$.

2. If $p$ is prime, then $\varphi(p) = p - 1$. What is $\varphi(p^n)$?

3. If $a \not\equiv 0 \pmod{n}$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

4. Let $a, n \in \mathbb{Z}_{>0}$. Then $n$ divides $\varphi(a^n - 1)$.
   
   [Hint: Use Lagrange’s theorem. What are the relevant subgroup and group?]

5. Fermat conjectured that the numbers $F_n = 2^{2^n} + 1$ are prime for all $n$. In 1732, Euler refuted this by checking that $F_5 = 2^{2^5} + 1$ is composite (641 is a factor). To do this, Euler first proved:

   *Theorem.* Every prime factor of $F_n$ has the form $k2^{n+1} + 1$.

   Reason as in previous problem to prove this.

**Food for thought**

$1/7 = 0.\overline{142857}$ has period $\varphi(7) = 6$.

$1/17 = 0.0588235294117647$ has period $\varphi(17) = 16$. 