That thing you keep on forgetting

Let n and m be positive integers. Let $\varphi(x) = n \cdot x$ be a homomorphism on $\mathbb{Z}_m$.

Theorem 1 $|\ker \varphi| = (n, m)$

Proof Let k be the size of $\operatorname{im} \varphi$. Then k is the least positive integer such that $m|nk$.

So nk is the least positive integer that is a multiple of m and n. That is, $k = \operatorname{lcm}(m, n)/n$.

Hence $k = m/(n, m)$.

So $|\operatorname{im} \varphi| = m/(n, m)$.

Thus, $|\ker \varphi| = (n, m)$. $\square$

Example The multiplicative group $\mathbb{F}_q^*$ is cyclic of order $q - 1$. Hence it is isomorphic to $\mathbb{Z}_{q-1}$ and the subgroup of nth roots of unity has order $(n, q - 1)$.

Example Let n be an integer such that $\mathbb{Z}_n^*$ is cyclic. Then $\mathbb{Z}_n$ has $(\varphi(n), k)$ kth roots of unity.

Example Suppose that we have an n sided polygon and k colours of paint. We wish to count the number of distinct ways of painting the sides of the polygon.

The symmetry group of the polygon is $\mathbb{Z}_n$ and for each $x \in \mathbb{Z}_n$ the number of colourings invariant under rotation by x is $k^{(n,x)}$. Why?

Identify together edges of the polygon that are congruent under the action of x. So identify together elements a and b of $\mathbb{Z}_n$ if $x|a - b$.

Hence the set of equivalence classes is the set of cosets of the subgroup $x\mathbb{Z}_n$.

The subgroup $x\mathbb{Z}_n$ has size $n/(x, n)$.

Hence there are (x, n) different colours in a colouring invariant under x, so $k^{(x,n)}$ different colourings.

Hence the total number of colourings, by the orbit counting formula (Burnside's lemma) is

$$\frac{1}{n} \sum_{r=0}^{n-1} k^{(n,r)}$$

Now never forget it again.