5. Subgroups, cosets, orders of elements

> *Every prime number divides necessarily one of the powers minus one of any [geometric] progression, and the exponent of this power divides the given prime minus one ...*
>
> Pierre Fermat, letter to Frénicle de Bessy, 1640. Translation Wikipedia (2016)

For a group G, we define a subset H of G to be a ***subgroup of*** G if

(1) The identity, 1, is in H.
(2) If $h \in H$, then $h^{-1} \in H$.
(3) If g and h are in H, then $g \times h$ is in H.

Problem 5.1. Let X be a set and let G be a finite group acting on X. For $x \in X$, show that $\mathrm{Stab}(x)$ is a subgroup of G.

Problem 5.2. Let G be a group and let H be a subgroup. Define a binary map $H \times G$ to G by sending (h, g) to $h \times g$.

(1) Check that this is an action of H on G.
(2) Show that, for any $g \in G$, the stabilizer of g is $\{e\}$.
(3) Suppose that H is finite. Show that every orbit has size $\#(H)$.
(4) Suppose that G and H are both finite. Show that $\#(H)$ divides $\#(G)$.

The orbits for this action are called the ***right cosets of*** H ***in*** G. In other words, for $g \in G$, the right coset of H containing g is $\{hg : h \in H\}$. We write this as Hg. Similarly, the ***left coset*** gH is $\{gh : h \in H\}$.

Problem 5.3. Let G be a group and let g be an element of G. We define $\langle g \rangle$ to be the set of all powers g^k for $k \in \mathbb{Z}$ (note that this includes negative values of k).

(1) Show that $\langle g \rangle$ is a subgroup of G.

We define the ***order*** of g to be the smallest positive integer N (WOP!) such that $g^N = 1$, or ∞ if there is no such N.

(2) Show that $\#\langle g \rangle$ is the order of g.
(3) Let G be a finite group and let g be in G. Show that the order of g is finite.

We now make some applications of these ideas to number theory.

Problem 5.4. Let G be a finite group with N elements and let g be in G. Show that $g^N = 1$.

Problem 5.5. **(**Fermat's Little Theorem, 1640, quoted above) Let p be a prime and let a be a nonzero element of $\mathbb{Z}_p$. Show that $a^{p-1} = 1$ in $\mathbb{Z}_p$.