Congruence, Cosets and Lagrange's Theorem

R. C. Daileda

Congruences in Groups

Let $n \in \mathbb{N}_0$. Given integers a and b one says that a is *congruent to b modulo n* provided $a - b$ is divisible by n. We denote this relationship by $a \equiv b \pmod{n}$. It is well known that congruence modulo n is an equivalence relation on $\mathbb{Z}$ that respects the binary operation (addition) used to define it. A closer look at the condition $a \equiv b \pmod{n}$ reveals that congruence modulo n can be defined in entirely group theoretic terms, and can therefore be generalized in a very natural way to arbitrary groups.

Since $n|a - b$ if and only if $a - b = nk$ for some $k \in \mathbb{Z}$, we find that we can equivalently formulate congruence mod n as

$$a \equiv b \pmod{n} \iff a - b \in n\mathbb{Z}. \tag{1}$$

Notice that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. In fact, every subgroup of $\mathbb{Z}$ has this form. Therefore, up to the use of additive notation, we can generalize congruence modulo n in $\mathbb{Z}$ to an arbitrary group G as follows. First we replace $n\mathbb{Z}$ by a subgroup $H < G$. Because G need not be abelian, the additive expression $a - b$ has two possible multiplicative reformulations: ab^{-1} and $b^{-1}a$. We choose the latter and define *(left) congruence modulo H* by

$$a \equiv b \pmod{H} \iff b^{-1}a \in H \quad \text{for } a, b \in G.$$

Our choice here is more or less arbitrary, and every result that we prove for left congruence modulo H can also be proven, *mutatis mutandis*, using the condition $ab^{-1} \in H$ instead. We will therefore be content to only state (without proof) the "right handed" analogues of our main results.

Theorem 1. *If G is a group and $H < G$, then left congruence modulo H is an equivalence relation on G.*

Proof. Let $a, b, c \in G$. Since $a^{-1}a = e \in H$, we have $a \equiv a \pmod{H}$, proving that congruence modulo H is reflexive. If $b^{-1}a \in H$, then $a^{-1}b = (b^{-1}a)^{-1} \in H$ since H is a group. That is, $a \equiv b \pmod{H}$ implies $b \equiv a \pmod{H}$, and we conclude that congruence modulo H is symmetric. Finally, suppose $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$, so that $b^{-1}a \in H$ and $c^{-1}b \in H$. Since H is closed under the ambient binary operation, we have $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$, so that $a \equiv c \pmod{H}$. This proves that congruence modulo H is transitive, and completes the proof of Theorem 1. □

We remark that Theorem 1 remains true if we replace left congruence modulo H with *right* congruence, which for $a, b \in G$ is defined by the analogous condition $ab^{-1} \in H$. It should be noted, however, that if G is nonabelian, then these two equivalence relations are not the same, in general.

Example 1. If G is the dihedral group D_n $(n \geq 3)$, $f \in D_n$ is any flip and $H = \langle f \rangle = \{e, f\}$ then right and left congruence modulo H are *not* the same. To see why, let $r \in D_n$ be a rotation of order n. Set $s = rf$. Then $r^{-1}s = f \in H$ so that $s \equiv r \pmod{H}$. However, since $fr = r^{-1}f$ we have $rfr = f$ and hence $rf = fr^{-1}$. Thus $sr^{-1} = rfr^{-1} = r^2 f \notin H$ (since $n \geq 3$). So s is *not* right congruent to r modulo H.

On the other hand, if $H = \langle r \rangle$ and $s, t \in G$, then $t^{-1}s \in H$ if and only if $t^{-1}s$ is a rotation. This occurs if and only if s and t are either *both* rotations or are *both* flips (otherwise $t^{-1}s$ must be a flip). The exact same reasoning applies when $st^{-1} \in H$, which shows that left and right congruence modulo H coincide in this case.

Example 2. If G is abelian and $H < G$, then left and right congruence modulo H *always* agree, since $b^{-1}a = ab^{-1}$ for all $a, b \in G$. This is the case when $G = \mathbb{Z}$ and $H = n\mathbb{Z}$, for instance.

Cosets

Given a group G and a subgroup $H < G$, the equivalence classes in G under congruence modulo H are called (left) *cosets* of H. These are easy to describe. Given $a \in G$, its coset is

$$\overline{a} = \{b \in G \,|\, b \equiv a \pmod{H}\} = \{b \in G \,|\, a^{-1}b \in H\} = \{b \in G \,|\, b \in aH\} = aH,$$

where

$$aH := \{ah \,|\, h \in H\},$$

as the notation is meant to suggest. Note that aH is just the image of H under the left translation $\lambda_a : G \to G$ given by $x \mapsto ax$. Since λ_a is a bijection, this implies that

$$|H| = |aH| \quad \text{for all } a \in G.$$

We also see that

$$aH = eH = H \iff a \equiv e \pmod{H} \iff a = e^{-1}a \in H.$$

In other words, H itself is the coset of the identity.

The collection of all (left) cosets of H in G (a subset of $\mathcal{P}(G)$) is called the associated *coset space* and is denoted G/H. In light of the description of cosets just given we have

$$G/H = \{aH \,|\, a \in G\}.$$

Taking into account well known properties of equivalence classes, we arrive at the following list of fundamental properties of cosets.

Theorem 2. *Let G be a group and let $H < G$. Then:*

(a) For all $a, b \in G$, either $aH = bH$ or $aH \cap bH = \varnothing$.

(b) The coset space G/H is a partition of G. That is, G is the disjoint union of the (left) cosets of H:

$$G = \coprod_{aH \in G/H} aH.$$[1]

(c) $aH = H$ if and only if $a \in H$.

(d) For all $a \in G$, $|aH| = |H|$.

Proof. We have already observed (c) and (d). Because congruence modulo H is an equivalence relation on G, its equivalence classes (cosets) are pairwise disjoint and their union is G. Since the equivalence class of $a \in G$ is precisely the coset aH, parts (a) and (b) now follow at once. □

Under *right* congruence modulo H, the equivalence classes in G are *right* cosets of H, which for $a \in G$ have the form

$$Ha = \{ha \,|\, h \in H\}.$$

The right coset space is sometimes denoted $H \setminus G$, and the properties of left cosets given in Theorem 2 hold just as well for the members of $H \setminus G$.

Example 3. In the case that $G = (\mathbb{Z}, +)$ and $H = n\mathbb{Z}$, the cosets of H have the form

$$a + n\mathbb{Z} = \{a + kn \,|\, k \in \mathbb{Z}\} = \{\ldots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \ldots\},$$

and are called *congruence classes* or *arithmetic progressions*. The term "arithmetic" refers to the fact that successive members of $a + n\mathbb{Z}$ have a common difference, namely n. If we use the division algorithm to write $a = qn + r$ with $r \in \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, then n divides $a - r$, so that $a \equiv r \pmod{n}$. Therefore every congruence class has the form $r + n\mathbb{Z}$ for some $r \in \mathbb{Z}_n$. Because two distinct members of $\mathbb{Z}_n$ can differ by at most $n - 1$, their difference cannot be divisible by n. That is, two distinct members of $\mathbb{Z}_n$ cannot be congruent modulo n. This implies that the congruence classes $r + n\mathbb{Z}$, $r \in \mathbb{Z}_n$, must all be distinct. So we see that we have a bijection

$$\begin{aligned} \phi : \mathbb{Z}_n &\to \mathbb{Z}/n\mathbb{Z}, \\ r &\mapsto r + n\mathbb{Z}. \end{aligned}$$

In particular, $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}_n| = n$.

Example 4. Let $G = D_n$ and $H = \langle f_0 \rangle = \{e, f_0\}$ where $f_0 \in D_n$ is any fixed flip. If $r \in D_n$ is any rotation, then $rH = \{r, f\}$, where f is the flip $f = rf_0$. If $f \in D_n$ is any flip, then $fH = \{f, r\}$, where r is the rotation $r = ff_0$. So every left coset of H has the form $\{r, f\} = rH = fH$, where r is a rotation, f is a flip, and the two are related by $r = ff_0$. Since there are n rotations in D_n and each coset of H contains exactly one of them, we conclude that $|D_n/H| = n$.

[1] The symbol $\coprod$ denotes the disjoint union of a family of sets.

On the other hand, similar reasoning shows that the right cosets of H also have the form $Hr = Hf = \{r, f\}$, but in this case r and f must be related by $r = f_0 f$. Nonetheless, note that we again have $|H \setminus D_n| = n$. As we shall see, this is not a coincidence.

Lagrange's Theorem

In general, the number of (left) cosets of a subgroup H of a group G is called the *index* of H in G and is denoted $[G : H]$. Thus,

$$[G : H] = |G/H|,$$

since G/H is the coset space. When G is infinite, the index $[G : H]$ can be finite or infinite, depending on G and H. For instance, $\mathbb{Z}$ is infinite, but we have just finished showing that

$$[\mathbb{Z} : n\mathbb{Z}] = n.$$

On the other hand, one can show that the map

$$\begin{aligned} S^1 &\to \mathbb{C}^\times/\mathbb{R}^+, \\ z &\mapsto z\mathbb{R}^+, \end{aligned}$$

is a bijection, so that $[\mathbb{C}^\times : \mathbb{R}^+]$ is (uncountably) infinite.

When G is finite, however, $[G : H]$ must also be finite (it cannot exceed $|G|$), and Theorem 2 has a powerful corollary.

Theorem 3 (Lagrange)**.** *If G is a finite group and $H < G$, then*

$$|G| = [G : H]\,|H|.$$

In particular, $|H|$ divides $|G|$.

Proof. Let $n = [G : H]$ and let $a_1H, a_2H, \ldots, a_nH$ be the distinct members (cosets) of G/H. By Theorem 2 we have

$$G = \coprod_{i=1}^{n} a_i H \quad \Rightarrow \quad |G| = \sum_{i=1}^{n} |a_i H| = \sum_{i=1}^{n} |H| = n|H| = [G : H]\,|H|.$$

□

Lagrange's Theorem itself has a number of important corollaries. If G is finite, $H < G$, and we utilize right cosets of H instead of left cosets in Lagrange's theorem, the same proof shows that $|G| = |H \setminus G|\,|H|$. Thus

$$|H \setminus G| = \frac{|G|}{|H|} = [G : H] = |G/H|.$$

In other words:

Corollary 1. *Let G be a finite group and $H < G$. The number of right cosets of H in G is the same as the number $[G : H]$ of left cosets of H in G.*

Example 5. Returning to Example 4, Corollary 1 immediately tells us that

$$|D_n/H| = |H \setminus D_n| = \frac{|D_n|}{|H|} = \frac{2n}{2} = n,$$

in agreement with our earlier computations.

We emphasize that although $[G : H]$ counts both the left and the right cosets of G, it is *not* generally true that every left coset of H is equal to a right coset. Subgroups satisfying $aH = Ha$ for all $a \in G$ are called *normal* and are of particular importance in the next section.

The next corollary generalizes a fact that we have so far only succeeded in proving for finite *abelian* groups.

Corollary 2. *Let G be a finite group and let $a \in G$. Then $|a|$ divides $|G|$.*

Proof. Let $H = \langle a \rangle < G$. Since $|\langle a \rangle| = |a|$, the conclusion follows from Lagrange's Theorem. □

Lagrange's theorem shows that just the *size* of a finite group puts certain limitations on its internal structure. The next corollary is a particularly strong example of this phenomenon.

Corollary 3. *Let G be a finite group. If $|G|$ is prime, then G is cyclic. In particular, G is generated by any of its nonidentity elements.*

Proof. Suppose $|G|$ is prime. Choose $a \in G$ so that $a \neq e$. Then $H = \langle a \rangle$ is nontrivial and

$$|G| = [G : H]\,|H|,$$

by Lagrange's theorem. Since $|G|$ is prime and $|H| \neq 1$, this implies $|H| = |G|$ and $[G : H] = 1$. Hence $G = H = \langle a \rangle$. □

Our final corollary generalizes Lagrange's theorem to a *tower* of subgroups $K < H < G$.

Corollary 4. *Let G be a finite group and let $K < H < G$ be a tower of subgroups. Then*

$$[G : K] = [G : H]\,[H : K].$$

Proof. According to Lagrange's theorem we have

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\,\frac{|H|}{|K|} = [G : H]\,[H : K].$$

□

Corollary 4 states that the index is *multiplicative in towers*. Using the tower $\{e\} < H < G$, multiplicativity of the index implies that

$$|G| = [G : \{e\}] = [G : H]\,[H : \{e\}] = [G : H]\,|H|.$$

This means that Corollary 4 includes the original statement of Lagrange's theorem as a special case.

Example 6. Let G be a group of order p, where p is prime, and let H be a nontrivial subgroup of G. Then H contains a nonidentity element of G, which must generate G by Corollary 3. It follows that $G < H < G$, so that $H = G$. It follows that a group of prime order has no nontrivial proper subgroups.

Example 7. Let G be a finite group. Suppose that p is a prime dividing $|G|$, and that H and K are subgroups of G with $|H| = |K| = p$. Let $J = H \cap K$, which is a subgroup of both H and K. If J is nontrivial, then $J = H$ and $J = K$ by the preceding exercise. Therefore $H = K$. This proves that any two subgroups of G with order p share only the identity or are identical.