Consequences of Lagrange's Theorem

Last lecture we discussed Lagrange's Theorem: for any finite group G, and subgroup $H \subset G$, we have $[G : H] = |G|/|H|$. Recall here that $[G : H]$ is the number of right cosets of H in G. The most useful consequence of this theorem is the following:

▶ **If G is a finite group, and H is a subgroup of G, then $|H|$ divides $|G|$.**

This of course greatly constrains the possibilities for which subsets of G can be subgroups. A particular case is the following. Let $a \in G$ and consider the cyclic subgroup $\langle a \rangle \subset G$ generated by a. Recall that $\text{ord}(a)$ is equal to the size of this subgroup. We obtain:

▶ **If G is a finite group and $a \in G$ then ord(a) divides $|G|$.**

For example, S_3 can only have elements of orders $\{1, 2, 3, 6\}$, and 6 does not occur because S_3 is not cyclic. In fact, we know all of this from direct computation. But now we understand more about why the orders of elements are constrained to these numbers.

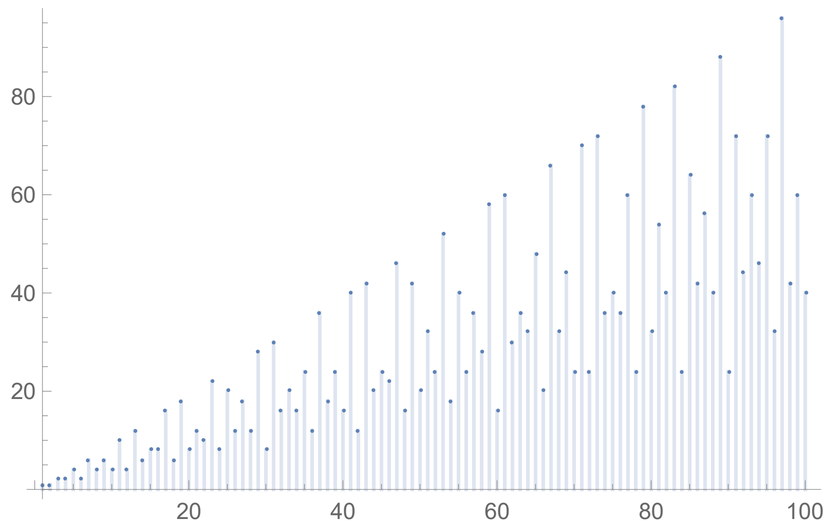
▶ **If G is a finite group and $a \in G$ then $a^{|G|} = e$.**

Indeed, writing $|G| = \text{ord}(a) \cdot n$, we have $a^{|G|} = a^{\text{ord}(a)\cdot n} = (a^{\text{ord}(a)})^n = e^n = e$, as claimed.

Next, we apply this last result to the group $(\mathbb{Z}_n^\times, \times)$ where n is a positive integer. Define

$$\phi(n) = |\mathbb{Z}_n^\times| = \#\{k \in \mathbb{Z} : 1 \leqslant k \leqslant n, \gcd(k, n) = 1\}$$

The function $\phi(n)$ is called *Euler's ϕ-function*, and sometimes *Euler's totient function*. For example, $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$ so $\phi(7) = 6$, while $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$ and so $\phi(10) = 4$. Below we show a graph of Euler's ϕ-function.



Euler's ϕ-function

▶ **(Euler's Theorem) For any integer k relatively prime to n, we have**

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

This result follows from the previous one: just view $k \pmod{n}$ as an element of $\mathbb{Z}_n^\times$, and note that the order of the group is by definition $\phi(n)$.

For example, let $n = 30$. We list the integers from 1 to 30 which are relatively prime to 30:

$$\mathbb{Z}_{30}^\times = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

Thus $\phi(30) = |\mathbb{Z}_{30}^\times| = 8$. Furthermore, Euler's Theorem tells us that for any one of the above 8 integers k (and their congruence classes mod 30) we have $k^8 \equiv 1 \pmod{30}$.

A special case of Euler's Theorem is when n is a prime number p. For in this case we have

$$\mathbb{Z}_p^\times = \{1, 2, \cdots, p-1\}$$

so in particular $\phi(p) = p - 1$. Therefore we obtain:

▶ **(Fermat's Little Theorem) For a prime p and integer k relatively prime to p:**

$$k^{p-1} \equiv 1 \pmod{p}$$

The conclusion of this result is often written as $k^p \equiv k \pmod{p}$.

For example, 97 is a prime number. Let's compute $5^{99} \pmod{97}$. Fermat's Little Theorem tells us that $5^{96} \equiv 1 \pmod{97}$. Using this we compute:

$$5^{99} \equiv 5^{96+3} \equiv 5^{96}5^3 \equiv 1 \cdot 5^3 \equiv 125 \equiv 28 \pmod{97}$$

Without the help of Fermat's Little Theorem, this would have taken much longer!

Another important consequence of Lagrange's Theorem is the following.

▶ **Suppose G is a finite group of prime order. Then G is cyclic.**

Let $H \subset G$ be a subgroup of G. Then Lagrange's Theorem tells us that $|H|$ divides $|G|$. Since $|G|$ is prime, $|H|$ must be 1 or $|G|$. In the first case, we must have $H = \{e\}$, and in the latter case, $H = G$. In particular, G has no non-trivial proper subgroups. Let $a \in G$ be a non-identity element. Then $\langle a \rangle$ is a non-trivial subgroup and thus must be all of G. In particular, $G = \langle a \rangle$ and so G is cyclic and generated by a.

We make two important remarks about Lagrange's Theorem. First, we could have used the notion of a *left* coset instead of a right coset: these are subsets $aH = \{ah : h \in H\}$. Lagrange's Theorem holds for left cosets, by the same arguments. A consequence is that the number of left cosets is equal to $[G : H]$, the number of right cosets.

Second, the converse to Lagrange's Theorem is false: if a positive integer d divides $|G|$, then it is not necessarily true that there is a subgroup of order d within G. The first instance of this phenomenon is the following:

▶ **In the alternating group A_4 of order 12, there is no subgroup of order 6.**

Let us prove this. First we write out the 12 elements of A_4:

$$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

Note we have 8 cycles of length 3, which have order 3, and 3 elements which are pairs of disjoint transpositions, each of order 2. Now suppose there is a subgroup $H \subset A_4$ of order 6. Let $\sigma \in A_4$ be a cycle of length 3. Consider the right cosets

$$H, \quad H\sigma, \quad H\sigma^2$$

Lagrange's Theorem tells us that $[A_4 : H] = |A_4|/|H| = 12/6 = 2$, so there are exactly 2 right cosets. So two of the cosets above must be equal. If $H = H\sigma$, then $\sigma \in H$, and similarly if $H = H\sigma^2$ then $\sigma^2 \in H$. But since $\sigma^2 = \sigma^{-1}$ and H is a subgroup, we must have $\sigma \in H$. The other possibility is that $H\sigma = H\sigma^2$. Multiplying on the right by σ gives $H\sigma^2 = H$, and again we conclude $\sigma \in H$. In conclusion, every length 3 cycle in A_4 must be in H. But there are 8 such cycles. Thus $6 = |H| \geqslant 8$, which is a contradiction. Thus A_4 cannot have a subgroup of order 6, as we claimed.