AlgebraNotes07 Euler's ϕ function.

A theorem about cyclic groups that we have been using.

Theorem 7.1 Suppose that each of G and H is a cyclic group of order n with generators a and b respectively. Then $\varphi : G \to H$ defined by

$$\varphi(a^k) \quad = \quad b^k \qquad \text{for each } k \in \mathbb{Z}$$

is an isomorphism.

Theorem 7.2. Suppose that G is a cyclic group of order n with generator a. Then a^k generates G if and only if $k = 1$ or n and k are relatively prime.

Theorem 7.3. Consider $(\mathbb{Z}_n, \cdot_n)$; let $M_n = \{x \in \mathbb{Z}_n \mid x \text{ has a multiplicative inverse}\}$. Then $(M_n, \cdot_n)$ is a group.

Definition [Euler's ϕ function]. Let n be a positive integer, then the Euler phi-function, written as $\phi(n)$, is the number of positive integers less than or equal to n that have a greatest common divisor of 1 with n.

Theorem 7.4. [Euler's theorem]. If each of a and n are positive relatively prime integers, then

$$a^{\phi(n)} \quad \equiv_n \quad 1.$$

Equivalently

$$n \Big| a^{\phi(n)} - 1.$$

I think the following is a corollary to 7.5: If each of a and n are positive relatively prime integers, then for any positive integer k:

$$n \Big| (a^{k\phi(n)} - 1).$$

Let's test this out with 5 and 9; and then with 8 and 10.

I also think the following is a corollary to 7.5: If k is a positive integer then

$$n \Big| \phi(k^n - 1).$$

Again let's test this out with some values.

Exercise 7.5. Argue that if p and q are relatively prime, then $\phi(pq) = \phi(p)\phi(q)$.

Another important theorem of Group Theory:

Theorem 7.6. [Cayley's Theorem.] If G is a group and $|G| = m$, then G is isomorphic to a subgroup of the permutation group on m elements, S_m.

Hints:

a. For each $g \in G$, define $f_g : G \to G$ by $f_g(x) = gx$. Show that f_g is a permutation of the elements of G.

b. Show that $S(G) = \{f_g | g \in G\}$ is a group with the composition operator $\circ$.

c. Show that $S(G)$ is isomorphic to G.

Exercise 7.7. Suppose $\gamma : G \to G$ is one-to-one and onto. Show that $\gamma = f_g$ for some $g \in G$. Where f_g is as defined in 7.5a. above.

Exercise 7.8. Suppose that G is a group and $|G| = 2p$ for some prime number p. Show that

a. G has a subgroup of order p.

b. Show that the subgroup of order p from part (a) is normal.

c. What can you say if $|G| = pq$ where p and q are distinct primes.

Helpful observations regarding Exercise 7.8.

Part a. Assume that G is a group and $|G| = 2p$ with p a prime number. [Note: by the order of a group is meant the cardinality of the group. By the order of an element g of a group G we mean the smallest positive integer n so that $g^n = e$.]

Observation 1. If g and h are two elements of G, the order of g is p, h is not in the subgroup generated by g and for some i we have an integer j so that $h^i = g^j \neq e$. Then G is cyclic and h generates G.

Observation 2. G contains a subgroup of order p.

Observation 3. If J is a group and g and h are elements of J with $g \neq h$ and so that $g^2 = h^2 = (gh)^2 = e$, then J contains a subgroup of order 4.

Part b. Stay tuned.

Part c. Find a generalization of observation 1 above useful for the case that $|G| = pq$ with both p and q prime.