Finite Groups We've Seen:

C_n The cyclic group of n elements:

$$C_n = \left\{1, r, r^2, \ldots, r^{n-1}\right\} \qquad r^n = 1.$$

D_n The dihedral group of $2n$ elements:

$$D_n = \left\{1, r, r^2, \ldots, r^{n-1}, m, mr, mr^2, \ldots, mr^{n-1}\right\} \qquad r^n = 1, m^2 = 1.$$

$\mathbf{Z}_n$ The additive group of integers modulo n:

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

with $a \oplus b$ is the remainder of $a + b$ when divided by n. The order of this group is $|\mathbf{Z}_n| = n$.

U_m The multiplicative group of integers modulo m:

$$U_m = \{k \in \mathbf{Z} : 0 < k < m, \gcd(k, m) = 1\}$$

with $a \otimes b$ is the remainder of ab when divided by m. (We called this group G_m, but I've seen U_m used more in texts.) The order of this group is $|U_m| = \phi(m)$. (See the next page for details of $\phi(m)$.)

S_n The symmetric group of permutation of n elements $\{1, 2, \ldots, n\}$. The group S_n has $n!$ elements.

A_n The alternating group: the subgroup of S_n of even permutations. From a homework problem, we know that $|A_n| = n!/2$.

- A few others: we've also seen the groups T (the tetrahedral group of symmetries of the tetrahedron), O (the octahedral group of symmetries of the cube or octahedron), and I (the icosahedral group of symmetries of the icosahedron or dodecahedron). These have orders $|T| = 12$, $|O| = 24$, and $|I| = 60$.
- Some new ones: let $\mathbf{R} = \{\pm 1\}$ using multiplication, and let $\mathbf{C} = \{\pm 1, \pm i\}$, where $i^2 = -1$, $(-i)^2 = -1$, and $(-1)^2 = +1$. Finally, let $\mathbf{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, and $ki = j$.

Some Useful (Mostly Familiar) Facts

Recall that the *order* of a group G is the number of elements of the group. On the other hand, the *order* of an element g of G is the smallest positive integer k with $g^k = 1$. We write $|G|$ and $|g|$ for the orders of G and g. The following fact is a corollary of Lagrange's theorem.

Fact: *For a finite group G, the order of an element g of G divides the order of G. That is, $|g|$ divides $|G|$.*

A finite group G is cyclic if and only if there is an element g in G with $|g| = |G|$. This element is called a *primitive root.*

Some Values of the Euler ϕ-Function

From a homework problem, we know that if $m = p_1^{k_1} p_2^{k_2} \cdots p_\ell k^\ell$ (where $p_1, \ldots, p_\ell$ are distinct primes and $k_1, \ldots, k_\ell$ are positive integers)

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_\ell}\right).$$

Here is a table of $\phi(m)$ for various values of m, with a companion table showing the values of m for a certain choice of $\phi(m)$.

m	$\phi(m)$
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8
31	30
32	16

$\phi(m)$	m
1	2
2	3, 4, 6
4	5, 8, 10, 12
6	7, 9, 14, 18
8	15, 16, 20, 24, 30
10	11, 22
12	13, 21, 26, 28
16	17
18	19, 27
20	25
22	23
28	29
30	31