Chapter 12

Orders of Abelian groups

Given a set X, the number of elements of X (which could be infinity) will be denoted by $|X|$. When X is an abelian group, $|X|$ is called it's order. One of the most basic principles of counting is the following:

Lemma 12.1. *If X can be written as a union of two disjoint subsets $Y \cup Z$ (disjoint means their intersection is empty), then $|X| = |Y| + |Z|$.*

A *partition* of X is a decomposition of X as a union of subsets $X = Y_1 \cup Y_2 \cup \ldots Y_n$ such that Y_i and Y_j are disjoint whenever $i \neq j$.

Corollary 12.2. *If $X = Y_1 \cup Y_2 \cup \ldots Y_n$ is a partition, then $|X| = |Y_1| + |Y_2| + \ldots |Y_n|$.*

Theorem 12.3 (Lagrange). *Let A be an abelian group of finite order. Then for any subgroup B, $|A| = |B||A/B|$*

Proof. Since A is finite, there are only a finite number of cosets. Let $A/B = \{e*B, a_1*B, \ldots a_n*B\}$. Every element $a \in A$ lies in one of these cosets, namely $a*A$. Exercise 3 of the previous chapter shows that $A = e*B \cup a_1*B \cup \ldots a_n*B$ is a partition. Therefore $|A| = |e*B| + |a_1*B| + \ldots |a_n*B|$. The map from $B \to a_i*B$ given by $x \mapsto a_i*x$ is one to one and onto since it has an inverse given $y \mapsto a_i y$. Therefore $|a_i*B| = |B|$ which implies that $|A| = |A/B||B|$. □

Corollary 12.4. *The order of any subgroup divides the order of A.*

The order of an element $a \in A$ is the order of the subgroup generated by a.

Lemma 12.5. *The order of n is the least $n > 0$ such that $a^n = e$.*

Corollary 12.6. *The order of $a \in A$ divides the order of A.*

An abelian group A is called cyclic if there is an element $a \in A$ (called a generator) such that every element of A is a power of A. For example $\mathbb{Z}_n$ is cyclic with 1 as it is generator.

Lemma 12.7. *If $|A| = p$ is prime then it's cyclic. In fact, every element different from the identity is a generator.*

Proof. The order of $a \in A$ is either 1 or p. If it's 1, $a = e$, otherwise a is a generator. □

Corollary 12.8. $a^{|A|} = 1$

Proof. Write $|A| = mn$ where m is the order of a. Then $a^{mn} = (a^m)^n = e$. □

An important special case is the following:

Lemma 12.9. *(Fermat's little theorem). If p is prime and $0 < a < p$ then $\overline{a}^{p-1} = 1$.*

This leads to a simple test for compositness (nonprimeness) which we call the Fermat test to the base a.

Corollary 12.10. *If $a^{p-1} \not\equiv 1\, (mod\, p)$ for some $0 < a < p$ then p is not prime.*

It may seems strange that one even needs a test other than the obvious one of attempting to divide by successive integers. The point is that for very large integers (which arise in applications to cryptography), the obvious test is so slow as to be useless. A more practical method would be to might pick several bases at random. If it passes each Fermat test, then p is "probably" prime, but if it fails once it's definitely composite. Most primality tests used in practice, including Maple's *isprime*, procedure use a more accurate variation of this idea.

Fermat had conjectured that integers of the form $P = 2^{2^n} + 1$ were always prime. This was shown to be false by Euler, when $n = 5$, by explicitly factoring it. Let's test the next one, with $n = 6$, using the above method. In this case $P = 18446744073709551617$ is big enough that Maple will be unable to compute a^{P-1} directly:

```
>  P := 2^(2^6)+1:
>  2^(P-1);
```

```
Error, integer too large in context
```

However, we only need a^{P-1} in the ring $\mathbb{Z}_P$, and Maple can do this if we tell it to compute $Power(a, P-1)\, mod\, P$. Trying the Fermat test with base 2 is inconclusive, but base 3 shows us that P isn't prime.

```
>  Power(2, P-1) mod P; Power(3,P-1) mod P;
```

```
                         1

                 8752249535465629170
```

12.11 Exercises

1. Calculate the orders of all elements of $\mathbb{Z}_{12}$
2. Show that $\mathbb{Z}_p^*$ is cyclic for $p = 3, 5, 7, 11$.
3. Is $\mathbb{Z}_8^*$ cyclic (explain)?
4. Suppose that n passes the Fermat test to base 2 i.e. $2^{n-1} \equiv 1\ (mod\, n)$. Prove that n must be odd.
5. Calculate all the between 3 and 25 which pass the Fermat test to base 2. Are these all prime? (Use Maple.)