IMO Training 2007: Order and Primitive Roots in Number Theory in the Context of Groups

July 11th: Afternoon Session

by: Adrian Tang

Let n be a positive integer. We define the following sets

$$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$
$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | gcd(a, n) = 1\}$$

To understand the multiplicative structure of the set $\mathbb{Z}_n^*$, it is helpful to view this set in terms of a group.

A group is a pair $(G, \cdot)$ where G is a set and $\cdot$ is an operation on G such that
(G1) For all $a, b \in G$, $a \cdot b \in G$. (**Closure Property**)
(G2) For all $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. (**Associative Property**)
(G3) There exists $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$. The element e is called the **identity** of G. (See Exercise 3 to show that this element is unique.)
(G4) For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1} \cdot a = a \cdot a^{-1} = e$. This element is called the **inverse** of a. (See Exercise 3 to show that this element is unique.)

Exercise 1: For each of the following sets and operations, determine whether it is a group. If it is a group, identify the identity and describe the inverse of each element. If it is not a group, explain which group property is not satisfied.

G	Group ?	Details
$(\mathbb{Z}, +)$		
$(\mathbb{Z}, -)$		
$(\mathbb{N}, +)$		
$(\mathbb{R}, \times)$		
$(\mathbb{R} - \{0\}, \times)$		
$(\mathbb{Z}_n, +)$		
$(\mathbb{Z}_n^*, \times)$		
$(\{(0,0), (0,1), (1,0), (1,1)\}, +)$		

Exercise 2: Give an example of a group G such that there exist $a, b \in G$ such that $a \cdot b \neq b \cdot a$. i.e. G is not commutative.

A group that satisfies the property that for all $a, b \in G$, $a \cdot b = b \cdot a$ is called an **abelian group**. Otherwise it is called a **non-abelian group**.

Exercise 3: Prove that the identity element of a group is unique. Prove that the inverse of an element in a group is also unique.

For the remainder of this paper, we will deal only with **finite and abelian** groups. We will use the following notation. Let G be a group with n elements. For $a \in G$ and $m \in \mathbb{Z}^+$, define $a^m = a \cdot a \cdot \cdots \cdot a$ (m times) If $m < 0$, define $a^m = (a^{-1})^{-m}$.

Proposition 0.1 *For all $a \in G$, $a^n = e$.*

Proof: Let $G = \{x_1, x_2, \cdots, x_n\}$. Note that ax_i, ax_j are distinct for distinct i, j. Hence,

$$\{x_1, \cdots, x_n\} = \{ax_1, \cdots, ax_n\}$$

.

Taking products of both sets and multiplying both sides by $x_1^{-1} \cdot x_2^{-1} \cdots x_n^{-1}$ yield this result. □

Exercise 4: Prove Fermat's Little Theorem. i.e. Let p be a prime and a be a positive integer relatively prime to p. Then

$$a^{p-1} \equiv 1 \bmod p$$

Exercise 5: Prove Euler's Theorem. i.e. Let n be a positive integer and a be a positive integer relatively prime to n. Then

$$a^{\varphi(n)} \equiv 1 \bmod n$$

where $\varphi(n)$ is the number of positive integers relatively prime to n. i.e. $\varphi_n = |\mathbb{Z}_n^*|$.

There are (finite abelian) groups where the entire group can be generated by a single element in the group. i.e. For all $a \in G$, there exists an element $g \in G$ and a positive integer m such that $g^m = a$. In other words, $\{g, g^2, \cdots, g^n\}$ are exactly all n elements of G. If such an element $g \in G$ exists, then G is said to be a **cyclic group**. It is named so because the sequence $g, g^2, g^3, \cdots, g^{n-1}, g^n(= e), g^{n+1}(= g^1), \cdots$ cycles through each element of the group periodically.

An easy example of a cyclic group is $(\mathbb{Z}_n, +)$. It has generator 1. An example of a group that is not cyclic is $(\{(0,0),(0,1),(1,0),(1,1)\}, +)$.

Exercise 6: Let p be a prime. Prove that $(\mathbb{Z}_p^*, \times)$ is cyclic. (While this problem is worth your time to solve , you can use this fact without proof on an olympiad.)

Let G be a finite abelian group with n elements. For $a \in G$, the **order** of a is defined to be the smallest positive integer m such that $a^m = e$. Clearly, the order of a is well-defined since $a^n = e$. This number is denoted by $ord(a)$.

Also note that G is a cyclic group if and only if there exists an element $g \in G$ with order n.

Exercise 7: Let $p = 7$. For each $a \in \{1, 2, 3, 4, 5, 6\}$, find $ord(a)$.

Exercise 8: For all $a \in G$, prove that $ord(a)$ divides n.

Exercise 9: Let p be a prime which is not 2 or 5 and $d = ord(10)$ modulo p and n be a positive integer such that $0 < n < p$. Prove that the decimal expansion of n/p is periodic with period d.

Exercise 10:
a.) Let G be a cyclic group with generator g. For each $1 \leq m \leq n$, find the order of g^m.

b.) Let G be a cyclic group with n elements. How many generators are there?

Exercise 11: Let p be an odd prime and g be a generator for $(\mathbb{Z}_p^*, \times)$. Prove that

$g^{\frac{p-1}{2}} \equiv -1 \bmod p$.

A generator for the group $(\mathbb{Z}_n^*, \times)$ is called the **primitive root** modulo n. A primitive root in such a group does not always exist. In fact, it only exists when $n = 2, 4, p^m, 2 \cdot p^m$ where p is any odd prime and m is any positive integer. (The proof of this is not easy. However, you may use this fact without proof on an olympiad.)

Exercise 12: Prove that 2 is a primitive root modulo 101.

Exercise 13: Suppose $\mathbb{Z}_n^*$ has a primitive root. How many primitive roots are there in $\mathbb{Z}_n^*$?

Exercise 14: Let p be a prime.
(a) Prove that $x^2 \equiv -1 \bmod p$ has a solution in x if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

(b) Prove that $x^4 \equiv -1 \bmod p$ has a solution in x if and only if $p = 2$ of $p \equiv 1 \bmod 8$.

(c) Prove that $x^2 \equiv 2 \bmod p$ has a solution in x if and only if $p = 2$ or $p \equiv \pm 1 \bmod 8$.

(d) Let d be a positive divisor of $p-1$. Prove that $x^{\frac{p-1}{d}}$, over all $x \in \mathbb{Z}$, takes only exactly $d+1$ values modulo p.

(e) Let p be an odd prime and let $QR(p) = \{a \in \mathbb{Z}_p^* | a = x^2 \bmod p \text{ for some } x \in \mathbb{Z}_p^*\}$. Prove that $|QR(p)| = (p-1)/2$ and $(QR(p), \times)$ is a group. (These elements, along with 0, are called the **quadratic residues** modulo p. The other $\frac{p-1}{2}$ elements are called the **quadratic non-residues** modulo p.)

The results of Exercise 14 are extremely important in number theory. They are useful in solving various kinds of Diophantine equations. For examples, Exercises 14(a) and 14(c) tells us properties of perfect squares as it relates to certain modulus. Exercise 14(d) might tell us a suitable modulus to choose when solving a Diophantine equation. For example, if the exponents that appear in an equation are all of the form $\frac{p-1}{d}$ where d is small, then it might be helpful to analyze the equation modulo p since the number of distinct values of the equation modulo p is also small.

Exercise 15: Prove that there are no integer solutions to $y^2 = x^3 + 7$. (Can you generalize this?)

Exercise 16: Prove that there are no integer solutions to $x^3 + y^4 = 2^{2003}$.

IMO Training: Problem Set
July 11th: Afternoon Session

1. Prove that for all primes p, there exists a positive integer n such that $n^8 - 16$ is divisible by p.

2. Let p be an odd prime and m be a positive integer such that $1 \leq m \leq p-2$. Prove that
$$1^m + 2^m + \cdots + (p-1)^m$$
is divisible by p.

3. Let $p > 3$ be a prime and $QR(p) = \{j \in \mathbb{Z}_p^* | x^2 \equiv j \bmod p \text{ for some } x \in \mathbb{Z}_p^*\}$. Prove that
$$\sum_{j \in QR(p)} j$$
is divisible by p.

4. Let a, n be positive integers. Prove that $\varphi(a^n - 1)$ is divisible by n where $\varphi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

5. Let p be a prime greater than 3. Let
$$\frac{m}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$
where m, n are relatively prime positive integers. Prove that m is divisible by p^2.

6. Let n be a positive integer. Show that if $3 \leq d \leq 2^{n+1}$, then $a^{2^n} + 1$ is not divisible by d for all positive integers a.

7. Let a, n be positive integers with a odd. Prove that $a^{2^n} - 1$ is divisible by 2^{n+2}.

8. Find all integer solutions to $y^2 = x^3 + 23$.

9. Let p be a prime and q be a prime divisor of $2^p - 1$. Prove that $q > p$.

10. Prove that there are infinitely many positive integer solutions to $4ab - a - b = c^2 + 1$ but no positive integer solutions to $4ab - a - b = c^2$.

11. Let p be a prime such that $p \equiv 3 \bmod 4$. Prove that

$$\prod_{k=2}^{p-2}(k^2 + 1) \equiv 4 \bmod p.$$

12. Let n be the product of d distinct primes, each greater than 3. Prove that $2^n + 1$ has at least 4^d distinct positive divisors.

13. Let p be a prime greater than 3. Show that there exists a positive integer $n < p - 1$ such that $n^{p-1} - 1$ and $(n+1)^{p-1} - 1$ are not divisible by p^2.

14. Find all triples of positive integers (a, m, n) such that $(a+1)^n$ is divisible by $a^m + 1$.

15. a.) Prove that 2 is a primitive root modulo 3^n for all positive integers n.

    b.) Let k be any positive integer. Prove that if $2^n \equiv -1 \bmod 3^k$, then 3^{k-1} divides n.

    c.) Find all positive integers n such that $2^n + 1$ is divisible by n^2.