CYCLIC UNIT GROUPS

LECTURE NOTES: MATH 422, CSUSM, SPRING 2009. PROF. WAYNE AITKEN

The goal of this document is to consider the concept of *order* in unit groups modulo m, and to prove the following important result (of Gauss): if p is a prime, then the unit group

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

is a cyclic group. Its generators are called *primitive roots*.

Remark. In this document, when we write 1, 2, 3, et cetera, as members of $\mathbb{Z}_m$, it is important to remember that we we are not referring to integers, but rather to equivalence classes of integers.

1. Orders

The ideas in this section are important not only in number theory, but more generally in group theory. So they warrant careful study. The group $\mathbb{Z}_m$ under addition is the prototypical additive cyclic group. What is striking is that $\mathbb{Z}_p^\times$ is a multiplicative cyclic group (at least when p is a prime).

Definition 1. If $a^k = 1$ where $a \in \mathbb{Z}_m$ then we say that k is an *i-exponent* for a.

Remark. Warning: *k is an integer.* Do not think of k as being an element of $\mathbb{Z}_m$. So $k \in \mathbb{Z}$ and $a \in \mathbb{Z}_m$.

Remark. The term *i-exponent* is short for *identity-exponent*. Some people use the simpler term *exponent*, but our terminology is more expressive.[1]

Remark. Euler's theorem implies that $\phi(m)$ is an i-exponent for every unit $a \in \mathbb{Z}_m^\times$:

$$a^{\phi(m)} = 1.$$

Exercise 1. Show that an element is a unit if and only if it has a positive i-exponent. Hint: if k is an i-exponent of a, what power of a is an inverse of a?

Definition 2. The *order* of an element $\mathbb{Z}_m^\times$ is defined to be the smallest positive i-exponent.

Remark. There are two *order* concepts used in this class, and they are much different. One concerns the power of p occurring in $n \in \mathbb{Z}$, while the other concerns i-exponents. When we are talking about units in $\mathbb{Z}_m^\times$ you can be sure that we mean Definition 2. (Definition 2 is the definition employed in group theory.)

Exercise 2. Find the order of all elements in $\mathbb{Z}_{11}^\times$. Repeat for units in $\mathbb{Z}_m^\times$ for each of $m = 2, 3, 4, 5, 6, 7, 8, 9, 10$. This is not as tedious as it sounds.

Date: Spring 2008. Version of March 18, 2009.

[1]Other terms I have used in the past are *neutralizing exponent* or *killing exponent*.

Proposition 1. *Let $a \in \mathbb{Z}_m^\times$ have order k, and let n be an integer. Then $a^n = 1$ if and only if $k \mid n$. In other words, n is an i-exponent if and only if n is a multiple of k.*

Proof. First suppose $a^n = 1$. Write $n = qk + r$ where $0 \le r < k$. Then

$$1 = a^n = a^{qk+r} = a^{qk}a^r = (a^k)^q\, a^r = 1^q\, a^r = a^r.$$

But k is defined as the smallest positive i-exponent. So $r = 0$. Thus k divides n.

Now suppose $k \mid n$. Then $n = qk$ for some q. So $a^n = \left(a^k\right)^q = 1^q = 1$. □

By Euler's Theorem we get the following.

Corollary 2. *Let $a \in \mathbb{Z}_m^\times$ have order k. Then $k \mid \varphi(m)$.*

Exercise 3. Go back to Exercise 2 and check that the corollary holds in every case.

Exercise 4. Show that any multiple of an i-exponent of $a \in \mathbb{Z}_m^\times$ is also an i-exponent of a.

The following gives a useful tool for finding a^s for large values of s.

Proposition 3. *Let $a \in \mathbb{Z}_m^\times$ have i-exponent k. Then $s \equiv t \bmod k$ implies $a^s = a^t$.*

Proof. From $s \equiv_k t$, we get $k \mid s - t$. So $a^{s-t} = 1$ by Exercise 4. Multiply both sides of the equation by a^t. This results in $a^s = a^t$. □

The following strengthens the above if we use the smallest i-exponent.

Proposition 4. *Suppose $a \in \mathbb{Z}_m^\times$ has order k. Then $a^s = a^t$ if and only if $s \equiv t \bmod k$.*

Proof. If $a^s = a^t$ then $a^{s-t} = 1$. Then $k \mid s - t$ by Proposition 1. So $s \equiv t \bmod k$.

The converse follows from the previous proposition. □

Remark. Notice how interesting this is: the exponents in $\mathbb{Z}_m^\times$ follow a different modulus than m.

Exercise 5. Find $3^{1000002}$ in $\mathbb{F}_{11}$ using Proposition 3.

Corollary 5. *Suppose $a \in \mathbb{Z}_m^\times$ has order k. Then the sequence $1, a, a^2, \ldots, a^{k-1}$ gives distinct elements of $\mathbb{Z}_m^\times$.*

Definition 3. Let $a \in \mathbb{Z}_m^\times$. Then

$$\langle a \rangle \stackrel{\text{def}}{=} \{1, a, \ldots, a^{k-1}\}.$$

Proposition 4 implies that every power of a is in the set $\langle a \rangle$.

Remark. The set $\langle a \rangle$ can easily be seen to be a subgroup of the unit group $\mathbb{Z}_m^\times$. It is called the *cyclic subgroup generated by a*.

Definition 4. Let $|\langle a \rangle|$ be the size of the set $\langle a \rangle$. The above corollary implies that $|\langle a \rangle|$ is the order of a. We sometimes write $|a|$ for $|\langle a \rangle|$. In other words,

$$|a| \;=\; \text{the order of } a.$$

Definition 5. If an element $g \in \mathbb{Z}_m^\times$ has order exactly equal to $\varphi(m)$, then we call g a *generator* or a *primitive root*. If $\mathbb{Z}_m^\times$ has a generator, then we say that it is *cyclic*.

Remark. The term *cyclic* refers to the fact that powers of the generator g cycles through all the elements of the group.

Remark. The term *cyclic group* applies to any finite group such that powers of a designated element give all elements of the group. (In an additive group, powers are not used, but integral multiples are used instead).

Exercise 6. Using the data of Exercise 2, find all the generators of $\mathbb{Z}_m^\times$ for $m \leq 11$. There might be no generators for some values of m.

Exercise 7. Show that g is a generator (primitive root) of $\mathbb{Z}_m^\times$ if and only if $\langle g \rangle = \mathbb{Z}_m^\times$. In other words, a generator really does generate all the units with powers of itself.

Remark. In the expression $|a|$, we have $a \in \mathbb{Z}_m$ and $|a| \in \mathbb{Z}$. This usages is not related to the traditional absolute value. However, absolute value notation is commonly used in mathematics to denote sizes, and $|a|$ denotes the size of the set $\langle a \rangle$.

An important theorem of Gauss, and the main theorem of this lecture, is that $\mathbb{F}_p^\times$ is cyclic if p is prime. In other words, $\mathbb{F}_p^\times$ has generators. We prove this later.

2. An Application

Trying to figure out the decimal expansions of rational numbers was a main stimulus for Gauss, then in his teens, to study the order of elements in $\mathbb{Z}_m^\times$. Here is a very amusing result.

Theorem 6. *Let n/m be a rational number in lowest terms with $\gcd(m, 10) = 1$ and $m > 1$. Then the decimal expansion of n/m is periodic (after the decimal point) with period equal to the order of 10 in $\mathbb{Z}_m^\times$.*

Remark. The element 10 occurs because we use base 10. We could generalize the above from base 10 to base B by making the obvious changes.

This theorem generalizes to denominators with $\gcd(b, 10) > 1$.

Theorem 7. *Let a/b be a rational number in lowest terms with positive b. Write*

$$b = 2^s 5^t m$$

where $\gcd(m, 10) = 1$. If $m = 1$ then a/b has a finite decimal expansion. If $m > 1$ then the decimal expansion of a/b is periodic (after some digit) with period equal to the order of 10 in $\mathbb{Z}_m^\times$.

Exercise 8. Predict what the behavior of the decimal expansion for 2/3, 1/9, 7/33, 3/5, 7/12, and 6/7. Now use a calculator to verify your predictions.

Exercise 9. Show that if m is relatively prime to 10 then there is a power of ten 10^k such that $m \mid (10^k - 1)$. For example, $7 \mid 999999$. Show that the period of the decimal expansion of $1/m$ is equal to the smallest such k.

3. Orders of powers and products

If an element $a \in \mathbb{Z}_m^\times$ has order k and if d divides k then you might expect a^d to have order k/d since when you raise a^d to the k/dth power you get a^k. This expectation turns out to be true:

Exercise 10. Suppose $a \in \mathbb{Z}_m^\times$ has order k and suppose d divides k. Show that a^d has order exactly k/d. Give a direct proof without using the following theorem.

What is the order of a^e if $e \in \mathbb{Z}$ is not a divisor of the order of a?

Proposition 8. *Suppose $a \in \mathbb{Z}_m^\times$ has order k, and $e \in \mathbb{Z}$. Then the order of a^e is given by the following:*

$$|a^e| \;=\; \frac{k}{\gcd(e,k)}.$$

Proof. First we identify a condition for i-exponents of a^e. Suppose that $(a^e)^y = 1$. Then $a^{ey} = 1$. Thus ey is a multiple of k by Proposition 1. In particular, ey is a common multiple of e and k. By an earlier result, we know that every common multiple of e and k is a multiple of $\operatorname{lcm}(e,k) = ek/\gcd(e,k)$. Thus $ek/\gcd(e,k)$ divides ek. This implies that $k/\gcd(e,k)$ divides y. (If $e = 0$, you can't cancel, so argue directly).

So every i-exponent is a multiple of $k/\gcd(e,k)$. Now we just need to check that $k/\gcd(e,k)$ is an i-exponent, and so it must be the smallest positive i-exponent:

$$(a^e)^{k/\gcd(e,k)} = a^{ek/\gcd(e,k)} = \left(a^k\right)^{e/\gcd(e,k)} = 1^{e/\gcd(e,k)} = 1.$$

□

The next two corollaries illustrate the two extreme cases of the above proposition.

Corollary 9. *Suppose $a \in \mathbb{Z}_m^\times$ has order k, and that $\gcd(k,e) = 1$ then a^e has order k. In other words,*

$$|a^e| = |a|$$

Exercise 11. Give an example illustrating the above corollary. Now give a counter-example that shows that $\gcd(k,e) = 1$ is necessary in the above corollary.

Corollary 10. *Suppose $a \in \mathbb{Z}_m^\times$ has order k, and that d divides k. Then a^d has order k/d. In other words,*

$$\left|a^d\right| = \frac{|a|}{d}\ .$$

Exercise 12. Give an example illustrating the above corollary.

Corollary 11. *Suppose $a \in \mathbb{Z}_m^\times$. Then a and a^{-1} have the same order:*

$$\left|a^{-1}\right| = |a|.$$

Exercise 13. Gauss proved that the product of all the primitive roots modulo p, where $p > 3$ is a prime, is equal to 1. Prove this: hint use the ideas of Wilson's theorem.

Exercise 14. Verify that the above three corollaries are indeed simple consequences of the above proposition.

Here is another amusing corollary:

Corollary 12. *Suppose $\mathbb{Z}_m^\times$ has a generator. Then the number of generators is $\phi(\phi(m))$.*

Proof. Recall that an element is a generator if and only if its order is $\phi(m)$. Suppose one generator $g \in \mathbb{Z}_m^\times$ exists. Every element of $\mathbb{Z}_m^\times$ is of the form g^e for $e \in \{0, 1, \ldots, \phi(m) - 1\}$. By Proposition 8, a^e has order $\phi(m)$ if and only if e is relatively prime to $\phi(m)$. By definition of ϕ, there are $\phi(\phi(m))$ such elements. □

Exercise 15. According to the above corollary, how many generators of $\mathbb{Z}_9^\times$ are there? (Assume it has a generator). If you know one generator g, what e would you use such that a^e gives the others?

Exercise 16. According to the above corollary, how many generators of $\mathbb{F}_{11}^\times$ are there? If you know one generator a, what e would you use such that a^e gives the others?

Proposition 13. *Suppose $a \in \mathbb{Z}_m^\times$ has order k_1 and $b \in \mathbb{Z}_m^\times$ has order k_2. If $\gcd(k_1, k_2) = 1$ then ab has order $k_1 k_2$. In other words,*

$$|ab| = |a| \cdot |b|.$$

Proof. Clearly $k_1 k_2$ is an i-exponent for ab since

$$(ab)^{k_1 k_2} = a^{k_1 k_2}\, b^{k_1 k_2} = \left(a^{k_1}\right)^{k_2} \left(b^{k_2}\right)^{k_1} = 1 \cdot 1 = 1.$$

Now suppose that x is a positive i-exponent of ab. Then $a^x b^x = 1$. In other words, b^x is the inverse of a^x. By Corollary 11,

$$|a^x| = |b^x|$$

Now the order of a^x is a divisor of the order of a by Proposition 8. Likewise the order of b^x is a divisor of the order of b. Since $\gcd(k_1, k_2) = 1$, it follows that $|a^x|$ and $|b^x|$ are also relatively prime. But they are equal. Thus they both must be 1. Hence x is an i-exponent of both a and b. Thus x is a common multiple of k_1 and k_2. Since $\gcd(k_1, k_2) = 1$, the least common multiple is $k_1 k_2$. Thus $x \geq k_1 k_2$. In other words, $k_1 k_2$ is the least positive i-exponent of ab. □

Exercise 17. Give an example illustrating the above proposition. Give a counter-example that shows that $\gcd(k_1, k_2) = 1$ is necessary in the above proposition.

Proposition 14. *Suppose $a_1, \ldots, a_r \in \mathbb{Z}_m^\times$ have orders $n_1, \ldots, n_r$ respectively. Suppose also that the n_i are pairwise relatively prime. Then $a_1 \cdots a_r$ has order $n_1 \cdots n_r$. Thus*

$$|a_1 \cdots a_r| = |a_1| \cdots |a_r|.$$

Proof. This follows from Proposition 13 by induction on r. □

4. Connections between i-exponents and polynomials

Here is an easy proposition. It is so easy, you should do the proof in your head.

Proposition 15. *Let $a \in \mathbb{Z}_m^\times$. Then a has i-exponent k if and only if a is a root of the polynomial*

$$x^k - 1.$$

We will now use prime modulus p so that we can use Lagrange theorem.

Proposition 16. *Let k be a positive integer, and let p be a prime. There are at most k elements of $\mathbb{F}_p^\times$ that have i-exponent k.*

Proof. Use Proposition 15. By Lagrange's theorem, the polynomial $x^k - 1$ has at most k roots. □

An example of this is that there are at most two elements of i-exponent 2. These elements are roots of $x^2 - 1 = (x-1)(x+1)$ and are 1 and -1. For larger k, there might not be k elements of i-exponent k. For example, if $3 \nmid p-1$ then there are no elements of order 3 by a previous result (since $\phi(p) = p-1$). Thus the only element of i-exponent 3, if $3 \nmid p-1$, is the identity 1. In other words $x^3 - 1$ has only one root if $3 \nmid p-1$. If, on the other hand, $p \equiv 1 \bmod 3$ then $x^3 - 1$ has three roots: it factors into linear factors.

Exercise 18. Find two elements of $\mathbb{F}_7^\times$ of order 3, and use them to factor $x^3 - 1$.

5. The Primitive Root Theorem

Now we prove Gauss' famous, and important, Primitive Root Theorem. First a lemma:

Lemma 17. *Suppose p is a prime, and suppose q is a prime dividing $p-1$. Suppose that q^e is a power of q dividing $p-1$, and write*

$$p - 1 = q^e n.$$

If $a \in \mathbb{F}_p^\times$ does not have i-exponent $q^{e-1}n$ then a^n has order q^e.

Proof. By Fermat's Little Theorem,

$$(a^n)^{q^e} = a^{q^e n} = a^{p-1} = 1.$$

Thus a^n has i-exponent q^e. This means that the order of a^n is equal to a divisor of q^e. In other words, the order of a^n is q^l for some $l \leq e$.

We wish to show that a^n has order q^e. Suppose on the contrary that a^n has order q^l where $l \leq e-1$. Then a^n must have i-exponent q^{e-1} since q^{e-1} is a multiple of q^l. Thus

$$1 = (a^n)^{q^{e-1}} = a^{q^{e-1}n}.$$

This means that a has i-exponent $q^{e-1}n$, a contradiction. □

Corollary 18. *Suppose p is a prime, and suppose q is a prime dividing $p-1$. Suppose that q^e is a power of q dividing $p-1$. Then there is an element of $\mathbb{F}_p^\times$ of order q^e.*

Proof. Write $p - 1 = q^e n$. By proposition 16 there are at most $q^{e-1}n$ elements of i-exponent $q^{e-1}n$, but there are $q^e n = p-1$ elements of $\mathbb{F}_p^\times$. So there is an $a \in \mathbb{F}_p^\times$ that does not have i-exponent $q^{e-1}n$. By the above lemma, this means that a^n has order q^e. □

Theorem 19 (Gauss)**.** *There is an element of $\mathbb{F}_p^\times$ of order $p-1$. In other words, $\mathbb{F}_p^\times$ is cyclic.*

Proof. Factor $p-1$ into prime powers:

$$p - 1 = q_1^{e_1} \cdots q_r^{e_r}.$$

By Corollary 18, there is an element a_i of order $q_i^{e_i}$. So

$$a_1 a_2 \cdots a_r$$

has order

$$q_1^{e_1} \cdots q_r^{e_r} = p - 1$$

by Proposition 14. □