CLASS 22, GIVEN ON 11/10/2010, FOR MATH 25

1. The group U_{2^e}

We have shown that U_{p^e} is cyclic for any prime power p^e where p is odd. In contrast, we will see that U_{2^e} is not cyclic, for $e \geq 3$, but we will be able to describe its group structure concretely.

First, notice that U_2, U_4 are cyclic, but U_8 is not, because $1, 3, 5, 7 \mod 8$ all have order 2. To prove that U_{2^e} is not cyclic for $e \geq 3$, we will use induction. First observe that $|U_{2^e}| = \phi(2^e) = 2^{e-1}$. Let $a \mod 2^e$ be an arbitrary element of U_{2^e}. This element has order dividing 2^{e-1}, so must have the form 2^i, for some $0 \leq i \leq e-1$. To show that U_{2^e} is not cyclic, we need to show that $a \mod 2^e$ has order 2^{e-2} or less for all $a \mod 2^e \in U_{2^e}$. Another way of saying this is that we want to show $a^{2^{e-2}} \equiv 1 \mod 2^e$ for all odd a.

First, we know this is true for U_8. Suppose this statement is true for e; we want to show it is also true for $e+1$. Since $a^{2^{e-2}} \equiv 1 \mod 2^e$, for every odd a, we can write $a^{2^{e-2}} = 1 + k2^e$ for some integer k. We want to show that $a^{2^{e-1}} \equiv 1 \mod 2^{e+1}$, so we square this expression for $a^{2^{e-2}}$:

$$(a^{2^{e-2}})^2 = a^{2^{e-1}} = (1 + k2^e)^2 = 1 + k2^{e+1} + k^2 2^{2e}.$$

Notice that the second and third terms are divisible by 2^{e+1} when $e \geq 3$. Therefore, $a^{2^{e-1}} \equiv 1 \mod 2^{e+1}$, as desired.

So U_{2^e} is not cyclic when $e \geq 3$. However, we will prove the following:

Proposition 1. *The numbers $\pm 5^i, 0 \leq i < 2^{e-2}$, give a complete set of representatives for U_{2^e}.*

One way of interpreting this proposition is that while U_{2^e} is not cyclic, it 'almost is', in the sense that while powers of 5 do not generate all of U_{2^e}, the powers of 5 along with their negatives do generate all of U_{2^e}.

Proof. The idea of the proof is to first show that the numbers $5^0, 5^1, \ldots, 5^{2^{e-2}-1}$ are all distinct, and then show that their negatives are also distinct, and not congruent to any of these powers of 5 mod 2^e. The first part is equivalent to showing that 5 has order 2^{e-2} in U_{2^e}. Since the order of 5 in U_{2^e} is a power of 2, this is equivalent to showing that $5^{2^{e-3}} \not\equiv 1$ mod 2^e.

We do this by induction. Indeed, for $e = 3$, notice that $5^{2^{3-3}} = 5^{2^0} = 5$, and clearly $5 \not\equiv 1 \mod 2^3$. Assume that $5^{2^{e-3}} \not\equiv 1 \mod 2^e$; we want to prove this statement with all the es replaced by $e+1$. First, notice that

$$5^{2^{e-2}} - 1 = (5^{2^{e-3}} - 1)(5^{2^{e-3}} + 1).$$

The second term on the right is $\equiv 2 \mod 4$, because $5^{2^{e-3}} \equiv 1^{2^{e-3}} \equiv 1 \mod 4$. Therefore the second term on the right hand side is divisible by 2 but not 4. On the other hand, $5^{2^{e-3}} - 1$ is not divisible by 2^e, by the inductive hypothesis. Therefore $5^{2^{e-2}} - 1$ is not divisible by 2^{e+1}, because if this were so, then $5^{2^{e-3}} - 1$ would be divisible by 2^e.

So we know that $5^0, 5^1, \ldots, 5^{2^{e-2}-1}$ are all incongruent mod 2^e. Consider $-5^0, -5^1, \ldots, -5^{2^{e-2}-1}$. These are all incongruent to each other mod 2^e, and they are also incongruent to any of the positive powers of 5. Indeed, if $5^i \equiv -5^j \mod 2^e$, then $5^i \equiv -5^j \mod 4$, which is impossible, because $5^i \equiv 5^j \equiv 1 \mod 4$, and $1 \not\equiv -1 \mod 4$. So the entire list $\pm 5^0, \pm 5^1, \ldots, \pm 5^{2^{e-2}-1}$ consists of 2^{e-1} integers which are all incongruent mod 2^e. But then these must be a complete set of representatives for U_{2^e}, because there are 2^{e-1} elements in U_{2^e}. □

Example. This proposition tells us that U_8 consists of $\pm 5^0, \pm 5^1$, which matches what we already know, because $-1 \equiv 7 \mod 8, -5 \equiv 3 \mod 8$.

Corollary 1. *As a group, for $e \geq 3$, U_{2^e} is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$.*

Proof. Consider the map $f : U_{2^e} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$ given by $f(5^i) = (0 \mod 2, i \mod 2^{e-2}), f(-5^i) = (1 \mod 2, i \mod 2^{e-2})$. The previous proposition tells us that this map is well-defined and a bijection. This map also clearly respects the group operation on the respective groups. □

2. The general case: U_n

We are now in a position to understand when U_n is cyclic, for general n. Recall that we know when U_{p^e} is cyclic: if p is odd this is always cyclic, while if $p = 2$, this is only cyclic for $e = 1, 2$, and otherwise is not cyclic. A homework exercise, which is an application of the CRT, tells us that if a, b are relatively prime, then U_{mn} is isomorphic to $U_m \times U_n$. One can apply this repeatedly to see that

$$U_{p_1^{e_1} \cdots p_r^{e_r}} \simeq U_{p_1^{e_1}} \times \ldots \times U_{p_r^{e_r}}.$$

So to understand when U_n is cyclic, we should try to understand when a direct product of groups is cyclic or not. This is the content of the following sequence of lemmas.

Lemma 1. *If m, n are not coprime, then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is not cyclic. More generally, given two groups G, G' of orders m, n, if m, n are not coprime, then $G \times G'$ is not cyclic.*

Proof. The first part is a homework assignment. The second part is an easy generalization, although we will not need to use it. □

Lemma 2. *If G is not cyclic, and G' is any group, then $G \times G'$ is not cyclic.*

Proof. Suppose that $G \times G'$ were cyclic, and had generator (g, g'). Then the elements (g^i, g'^i) as i ranges over integers cover all the elements of $G \times G'$. In particular, every element of G can be written in the form g^i for some integer i, which would imply that g is a generator of G, contradicting the fact that G is not cyclic. □

We can now completely determine when U_n is cyclic:

Theorem 1. *U_n is cyclic if and only if $n = 1, 2, 4, p^e$, or $2p^e$, where p is any odd prime, $e \geq 1$ any positive integer.*

Proof. First we check that if $n = 1, 2, 4, p^e, 2p^e$, then U_n is cyclic. For $n = 1, 2, 4$, this is clear. We also know this already for $n = p^e$, so we need only check $n = 2p^e$. In this case, $U_{2p^e} \simeq U_2 \times U_{p^e}$. Since U_2 is the identity group (the group consisting of exactly one element), this means that $U_{2p^e} \simeq U_{p^e}$, which we know is cyclic, so U_{2p^e} is cyclic as well.

Now we prove the converse. If n is not of the form above, then n is either equal to $2^e, e \geq 3, 2^f p^e, f \geq 2, e \geq 1$, or has two distinct odd prime divisors. In the first case, we already know that U_{2^e} is not cyclic. In the second case, we know that $U_{2^f p^e} \simeq U_{2^f} \times U_{p^e}$. If $f \geq 3$, we are done, because then U_{2^f} is not cyclic and the second lemma tells us that U_n will not be cyclic either. If $f = 2$, then $U_4 \simeq \mathbb{Z}/2\mathbb{Z}$. On the other hand, we know that U_{p^e} is cyclic and of order $p^{e-1}(p-1)$, so is isomorphic to $\mathbb{Z}/p^{e-1}(p-1)\mathbb{Z}$. Since p is an odd prime, $p^{e-1}(p-1)$ is even, so is divisible by 2. But $U_4 \times U_{p^e} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^{e-1}(p-1)\mathbb{Z}$, and the orders of the two groups in the direct product are not coprime, so their direct product is not cyclic by the first lemma.

Finally suppose we are in the final case, where n is divisible by two distinct odd primes, say p, q. Then $U_n \simeq \dots U_{p^e} \times U_{q^f} \times \dots$, where the missing parts of the product on the right correspond to the unit groups mod other prime powers in the factorization of n (if there are any). Then $2 \mid \phi(p^e), \phi(q^f)$, so $U_{p^e} \times U_{q^f}$ is not cyclic (since the relevant orders are not coprime), which in turn means that $U_{p^e} \times U_{q^f} \times \dots$ is not cyclic.

□