CLASS 20, GIVEN ON 11/05/2010, FOR MATH 25

1. Testing for primitive roots

The central question we want to answer right now is the following: when is U_n cyclic? If U_n is cyclic, we call any $g \mod n$ (which we might just write as g if the n is clear) which generates U_n a *primitive root* mod n. In particular, this means that $\langle g \rangle$ has the same size as U_n; in other words, the order of g is $\phi(n)$.

A question which immediately presents itself is the question of how you might actually determine whether a given $g \mod n$ is indeed primitive. One way is to directly verify that g has order $\phi(n)$, by calculating $g, g^2, g^3, \ldots, g^{\phi(n)}$, and checking that none of the elements equals $1 \mod n$ except the last. However, the following proposition shows that you actually only need to check a subset of powers of g to determine whether a number is a primitive root:

Proposition 1 (Lemma 6.4)**.** *Let n be any positive integer. Then $a \mod n$ is a primitive root mod n if and only if $a^{\phi(n)/q} \not\equiv 1 \mod n$ for all primes $q \mid \phi(n)$.*

Proof. If $a \mod n$ is a primitive root, then $a^{\phi(n)/q} \not\equiv 1 \mod n$ is clear, because $\phi(n)/q < \phi(n)$, so that $\phi(n)$ is the smallest positive power of a which is $\equiv 1 \mod n$. For the converse direction, suppose that $a \mod n$ is not a primitive root. Suppose $a \mod n$ has order d. Then $d \mid \phi(n), d \neq \phi(n)$. In particular, there is some prime q which divides $\phi(n)/d$. This prime also divides $\phi(n)$. On the other hand, since $q \mid \phi(n)/d$, we also have $d \mid \phi(n)/q$. Since $a^d \equiv 1 \mod n$, this implies $a^{\phi(n)/q} \equiv 1 \mod n$ as well. $\square$

Examples.

- Show that 2 is not a primitive root mod 17, but 3 is. First, $n = 17$ is prime, so $\phi(n) = 16$. Therefore a is a primitive root mod 17 if a has order 16 in U_{17}. One calculates that $2^4 = 16 \equiv -1 \mod 17$, so $2^8 \equiv 1 \mod 17$, so 2 is not a primitive root mod 17.

  The only prime dividing $\phi(17) = 16$ is 2, so to check that 3 is a primitive root it suffices to check that $3^8 \not\equiv 1 \mod 8$. We do this via three squarings: $3^2 \equiv 9 \mod 17, 3^4 \equiv 13 \equiv -4 \mod 17, 3^8 \equiv (-4)^2 \equiv 16 \mod 17$. So 3 is indeed a primitive root mod 17.
- Show that 2 is a primitive root mod 101. First, we check that 101 is prime. Therefore $\phi(101) = 100$. The only primes dividing 100 are $2, 5$, so to check that 2 is a primitive root mod 101 it suffices to check that $2^{20} \not\equiv 1 \mod 101, 2^{50} \not\equiv 1 \mod 101$. One can calculate these, say using fast exponentiation, or any other method you like, and check that $2^{20} \equiv 95 \mod 101, 2^{50} \equiv 100 \mod 101$. Therefore, 2 is a primitive root mod 101. In both this example and the previous example, notice that we save a substantial amount of work in using the above proposition.

2. U_p is cyclic

We now show that U_p is cyclic, when p is prime; ie, that there exist primitive roots mod p. The proof basically takes two steps. The first is the following seemingly unrelated result:

Proposition 2. *Let n be a positive integer. Then*

$$\sum_{d|n} \phi(d) = n,$$

where the summation runs over all positive divisors of n, including 1 and n.

Proof. We will group up all the numbers from $1, 2, \ldots, n$ into various sets depending on their gcd with n. Let S_d be the subset of $1, 2, \ldots, n$ which consists of all the integers whose gcd with n is exactly equal to n/d. In set theoretic notation, $S_d = \{a \mid 1 \leq a \leq n, \gcd(a, n) = n/d\}$.

The first claim is that the various sets S_d, as d ranges over divisors of n, partition $1, 2, \ldots, n$. First, notice every $a, 1 \leq a \leq n$, is a member of some S_d with $d \mid n$, since $\gcd(a, n) \mid n$. Furthermore, all these sets are disjoint, since $\gcd(a, n)$ is a fixed number, so that a can only belong to $S_{\gcd(a,n)}$.

This means that the sum of the sizes of S_d is equal to the size of the set $\{1, 2, \ldots, n\}$, which clearly is n. Therefore, to prove the proposition it is enough to show that each S_d has size $\phi(d)$.

A number a is an element of S_d if and only if $1 \leq a \leq n$ and $\gcd(a, n) = n/d$. This in turn is equivalent to there being an a' such that $a = (n/d)a', 1 \leq a' \leq d$, and $\gcd(a', d) = 1$. The first two conditions are fairly clear; for the last, recall that if d is a common divisor of a, b, then $\gcd(a/d, b/d) = \gcd(a, b)/d$. How many choices of a' are there? Exactly $\phi(d)$. Therefore, S_d has size $\phi(d)$ as claimed. □

Example. As an illustration of the idea of the proof, let $n = 12$. Then S_{12} consists of the numbers from 1 to 12 which have gcd $12/12 = 1$ with n; we quickly see that $S_{12} = \{1, 5, 7, 11\}$. Similarly, S_6 consists of those numbers from 1 to 12 which have gcd $12/6 = 2$ with $n = 12$. One sees that $S_6 = \{2, 10\}$. For $d = 4, 3, 2, 1$, one checks that $S_4 = \{3, 9\}, S_3 = \{4, 8\}, S_2 = \{6\}, S_1 = \{12\}$. You can quickly check that every number from 1 to 12 lies in exactly one of these sets, and that the size of S_d is $\phi(d)$.

The following lemma gives some idea why the previous proposition will be helpful:

Lemma 1. *Let g have order d in a group G. Then exactly $\phi(d)$ of $g^1, g^2, \ldots, g^d$ have order d.*

Proof. Recall that $\langle g \rangle$ is isomorphic to $\mathbb{Z}/d\mathbb{Z}$, so to count the number of g^i with order d, it suffices to count the number of elements of $(\mathbb{Z}/d\mathbb{Z}, +)$ of order d. One can show (homework assignment) that the order of $a \mod d$ is $d/\gcd(a, d)$, so the number of elements of $(\mathbb{Z}/d\mathbb{Z}, +)$ with order exactly d is the number of elements relatively prime to d; this is $\phi(d)$. □

Example. Recall we computed that $2^8 \equiv 1 \mod 17$, and that $2^4 \equiv -1 \mod 17$, so that $2 \mod 17$ has order 8. Then four of the classes $2^1, 2^2, \ldots, 2^8 \mod 17$ have order 8 as well; as a matter of fact, the isomorphism in the proof above tells us that $2^1, 2^3, 2^5, 2^7$ are the powers of 2 which have order 8 mod 17.

Theorem 1 (Theorem 6.5). *Let p be a prime, and let $d \mid (p-1)$ be a positive integer. Then there are exactly $\phi(d)$ elements of U_p with order d.*

Proof. Let S_d be the set of elements of U_p with order exactly d, and let $n_d = |S_d|$. First, notice that the sets S_d, as d ranges across divisors of $p - 1$, partition U_p. Indeed, every element of U_p belongs to some S_d, because each element has an order d which divides $p-1$, and belongs to exactly one S_d, since an element cannot have two different orders. This means that $\sum_{d|(p-1)} n_d = p-1$.

On the other hand, we will show that $n_d \leq \phi(d)$. If there are no elements of order d, then this inequality is definitely true. If there is an element of order d, say g, consider the d distinct elements $g, g^2, \ldots, g^d$. These are all solutions to the polynomial congruence $x^d \equiv 1 \mod p$. On the other hand, by a theorem proven a few weeks ago, this polynomial congruence has at most d solutions. Therefore $g, g^2, \ldots, g^d$ are all the solutions of $x^d \equiv 1 \mod p$. In particular, any element of U_p which has order d appears in the list $g, g^2, \ldots, g^d$. On the other hand, the previous lemma tells us that exactly $\phi(d)$ elements in this list have order d. In this case, $n_d = \phi(d)$, so for all $d \mid (p-1)$, we have $n_d \leq \phi(d)$.

This implies the inequality

$$\sum_{d|(p-1)} n_d \leq \sum_{d|(p-1)} \phi(d).$$

On the other hand, notice that both the left hand side and the right hand side are equal to $p-1$. Therefore, this inequality is an equality. The only way this is possible is if $n_d = \phi(d)$ for all $d \mid (p-1)$, as desired. $\square$

A clear consequence of this is that U_p is cyclic, since there is not just one, but $\phi(p-1) \geq 1$ elements of order $p-1$ in U_p.

The next step, which we will look at next class, is to extend this analysis to U_{p^e}, for general $e \geq 1$.