MATH 25 CLASS 26 NOTES, NOV 21 2011

Contents

1. Calculations involving primitive roots

Let's look at a few concrete calculations involving primitive roots. First, let's consider the question of finding primitive roots for unit groups mod (odd) prime powers, or prime powers times 2.

Examples.

- Find a primitive root for U_{125}. One way to approach this problem is to start by finding a primitive root for U_5, and then work our way up powers of 5. Clearly 2 is primitive mod 5, because $2^2 = 4, 2^3 = 8, 2^4 = 16$, and only $16 \equiv 1 \mod 5$. We know, based on the proofs from last class, that either 2 or $2 + 5$ is primitive mod 25. Furthermore, because 2 is primitive mod 5, the order of 2 in U_{25} is either 4 or $4(5) = 20$. And since $2^4 \not\equiv 1 \mod 25$, it is clear that 2 has order 20 in U_{25}, so is primitive in U_{25}. Finally, we saw that if g is primitive mod p^e, and if p is an odd prime, $e \geq 2$, then it is also primitive mod p^{e+1}, so applied to this situation, 2 is primitive mod $5^3 = 125$.
- Suppose we know that g is a primitive root mod p^e, where p is an odd prime, $e \geq 1$. How do we find a primitive root mod $2p^e$? Recall that we have an isomorphism

  $$U_{2p^e} \simeq U_2 \times U_{p^e}$$

  given by the CRT. The group U_2 is trivial. So to find a generator for U_{2p^e}, we should find a generator for $U_2 \times U_{p^e}$, which is essentially the same as finding a generator for U_{p^e}. Since we know g is primitive mod p^e, g is a generator of U_{p^e}. Then we want to find an element, say g', of U_{2p^e}, which corresponds to the element $(1, g)$ under the isomorphism given by the CRT. More concretely, we are looking for a $g' \mod 2p^e$ which satisfies $g' \equiv 1 \mod 2, g' \equiv g \mod p^e$. But this is easy to solve; if g is odd, just let $g = g'$, and if g is even, let $g' = g + p^e$, which is odd because p^e is.

  For instance, if we want to find a primitive root for U_{250}, we already know that 2 is a primitive root for U_{125}. Therefore we want to find a g' which is odd and $g' \equiv 2 \mod 125$, so $g' = 127$ works. (Notice that 2 cannot possibly be a primitive root for U_{250} because it is not even an element of U_{250}.)

Primitive roots can also sometimes make finding 'roots' of numbers mod p^e a little easier.

Examples.

- We know that 2 is a primitive root mod 25. Find all solutions of $x^4 \equiv 1 \mod 25$. Clearly $1, -1$ solve this congruence, but there could be up to two additional solutions. Let's use primitive roots to help us. Suppose $x^4 \equiv 1 \mod 25$ is true. Then we can write $x = 2^k$ for some integer k; as a matter of fact if we restrict $1 \leq k \leq 20 = \phi(25)$ then this k is unique. Therefore $2^{4k} \equiv 1 \mod 25$. But this is true if and only if $20 \mid 4k$, or if $5 \mid k$. So we see that $k = 5, 10, 15, 20$ give the values $x = 2^5, 2^{10}, 2^{15}, 2^{20}$ which solve $x^4 \equiv 1 \mod 25$. Indeed, $2^5 \equiv 7 \mod 25, 2^{10} \equiv -1 \mod 25, 2^{15} \equiv -7 \mod 25, 2^{20} \equiv 1 \mod 25$, so $\pm 1, \pm 7$ are the solutions of $x^4 \equiv 1 \mod 25$.
- For any integer a not divisible by 11, show that $x^3 \equiv a \mod 11$ always has exactly one solution mod 11. Since U_{11} is cyclic, there exists a primitive root g mod 11. (For instance one checks that 2 works.) Therefore, any $x \mod 11$ can be written in the form g^k for some integer k; uniquely if we restrict $1 \leq k \leq 10$. Then we want to solve $g^{3k} \equiv a \mod 11$. On the other hand, we can write $a \equiv g^m \mod 11$ for some integer $m, 1 \leq m \leq 10$, and since a, g are coprime to 11, we obtain

$$g^{3k} \equiv a \mod 11 \Rightarrow g^{3k} \equiv g^m \mod 11 \Rightarrow g^{3k-m} \equiv 1 \mod 11.$$

  The last congruence is true if and only if $10 \mid (3k - m)$. In other words, we want to know how many solutions (k, l) there are of the equation $3k - m = 10l$, where m is some constant. Since $\gcd(3, 10) = 1$, we know that any solution (k, l) satisfies $k = k_0 + 10n$, where n is any integer; in other words, $k \equiv k_0 \mod 10$ where k_0 is the k-coordinate of some solution. In particular, this means that there is exactly one value of k with $1 \leq k \leq 10$ which makes $g^{3k} \equiv a \mod 11$ true, and therefore $x^3 \equiv a \mod 11$ has exactly one solution for any value of a. (Actually, this is true even if $a \equiv 0 \mod 11$.)
- One can check that 6 is a primitive root mod 13. Suppose we want to solve $x^3 \equiv 6^3 \equiv 8 \mod 13$. Writing $x \equiv 6^k$ for a unique $k, 1 \leq k \leq 12$, this is equivalent to $6^{3k} \equiv 6^3 \mod 13$, or $6^{3k-3} \equiv 1 \mod 13$, or $12 \mid (3k - 3)$. We know that this has exactly three solutions mod 12: $k = 1, 5, 9$. So $x = 6, 6^5, 6^9$ solves the original congruence.

The key principle behind each of the previous three examples is that solving equations of the form $x^k \equiv a \bmod n$ can be reduced to questions on linear congruences, if U_n is cyclic. Even if U_n is not cyclic, we can use the CRT to examine $x^k \equiv a \bmod p^e$ for the various prime powers p^e which make up the factorization of n, and then use this technique on each congruence, and then reassemble the answers to find solutions to $x^k \equiv a \bmod n$, if there are any.