MA40238 NUMBER THEORY 2013/14 SEMESTER 1
HANDOUT ON PRIMITIVE ROOTS

ZIYU ZHANG

1. What you need to know from the lectures

You need to know everything from the lecture on Monday 13/10. This covers everything from Definition 3.1 to Corollary 3.5 in the lecture notes posted on the webpage.

From the lecture on Tuesday 14/10, you need to know the following (all numberings refer to the lecture notes posted on the webpage):

- The statement of Proposition 3.8:

For any odd prime p and any integer $l \geqslant 2$, $\mathbb{Z}_{p^l}^*$ is cyclic; i.e. there exist primitive roots modulo p^l.

- The statement in Remark 3.9 (which was proved in Proposition 3.8):

For any odd prime p and any integer $l \geqslant 2$, let $g \in \mathbb{Z}$ and $p \nmid g$. Suppose g is a primitive root modulo p and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then g is a primitive root modulo p^l.

  This provides a convenient way for finding primitive roots modulo high powers of odd primes.

- The statement of Proposition 3.6:

For any positive integer l, $\mathbb{Z}_{2^l}^*$ is not cyclic unless $l = 1, 2$.

- The statement of Theorem 3.10 (which I will explain on Friday 17/10):

For any integer $m \geqslant 2$, $\mathbb{Z}_m^*$ is cyclic (in other words, there exist primitive roots modulo m) iff $m = 2, 4, p^l$ or $2p^l$, where p is any odd prime and l is any positive integer.

  You should be able to use this theorem to rule out the numbers which do not possess primitive roots.

Date: October 15, 2014.

2. Hints to Exercise 3.1

Here is an example which shows how you might want to approach such a problem.

Suppose we want to find a primitive root modulo 17. Then we are looking for some $a \in \mathbb{Z}$, $\mathrm{hcf}(a, 17) = 1$, such that $\overline{a}$ is a generator of $\mathbb{Z}_{17}^*$. In other words, $\overline{a}$ has order $\phi(17) = 16$ in $\mathbb{Z}_{17}^*$. If we just pick an arbitrary a, $\overline{a}$ might not have order 16. Instead, its order could be any other positive divisor d of 16, namely, $1, 2, 4$ or 8. We want to rule out these situations. In other words, we want to find some $a \in \mathbb{Z}$, $\mathrm{hcf}(a, 17) = 1$, satisfying the requirement $a^d \not\equiv 1 \pmod{17}$ for $d = 1, 2, 4$ or 8.

The main idea to find such an a is test and error. We try small values of a coprime to 17 one by one until we find a right one. $a = 1$ is not worth trying since $1^1 \equiv 1 \pmod{17}$ which violates our requirement for a. Now we try $a = 2$. $2^1 \equiv 2 \pmod{17}$, good. $2^2 \equiv 4 \pmod{17}$, good. $2^4 \equiv 16 \equiv -1 \pmod{17}$, good. $2^8 \equiv (-1)^2 = 1 \pmod{17}$, which violates our requirement for a. We are sad because 2 is not a primitive root, so we have to start over and try $a = 3$. This time, $3^1 \equiv 3 \pmod{17}$, $3^2 \equiv 9 \pmod{17}$, $3^4 \equiv 9^2 \equiv 13 \equiv -4 \pmod{17}$, $3^8 \equiv (-4)^2 \equiv -1 \pmod{17}$. We are now happy because the order of 3 modulo 17 is not among $1, 2, 4$ and 8. So its order must be 16 (because its order has to be a positive divisor of 16). We conclude $a = 3$ is a primitive root modulo 17.

Suppose we want to go one step further and find all primitive roots modulo 17. We use Remark 3.2 (3) from lecture. We know $\overline{3}$ is a generator of $\mathbb{Z}_{17}^*$, hence all generators of $\mathbb{Z}_{17}^*$ are given by $\overline{3}^k$, where $0 \leqslant k < 16$, $\mathrm{hcf}(k, 16) = 1$; i.e., $k = 1, 3, 5, 7, 9, 11, 13, 15$. We can compute them explicitly one by one. $3^1 \equiv 3 \pmod{17}$, $3^3 = 27 \equiv 10 \pmod{17}$, $3^5 = 3^3 3^2 \equiv 10 \cdot 9 \equiv 5 \pmod{17}$, etc. In Exercise 3.1 you have much smaller numbers to work with, so the computation should not be too complicated. In this example, we can continue the calculation to get $3^7 \equiv 11 \pmod{17}$, $3^9 \equiv 14 \pmod{17}$, $3^{11} \equiv 7 \pmod{17}$, $3^{13} \equiv 12 \pmod{17}$, $3^{15} \equiv 6 \pmod{17}$. Conclusion: $a \in \mathbb{Z}$ is a primitive root modulo 17 iff a is congruent to any of the following numbers modulo 17: $3, 10, 5, 11, 14, 7, 12$ or 6.

Suppose we want to go one step further in another direction and find a primitive root for 17^5. We need to use Remark 3.9. That is, we need to find some $a \in \mathbb{Z}$ which is a primitive root modulo 17 and $a^{16} \not\equiv 1 \pmod{17^2}$. We already know 3 is a primitive root modulo 17. It remains to check whether $3^{16} \not\equiv 1 \pmod{17^2}$ holds. We have quite large numbers here, but in Exercise 3.1 you get numbers which are much more manageable. In this example we need the following calculation: $17^2 = 289; 3^4 = 81; 3^8 = 81^2 = 6561 \equiv 203 \pmod{289}; 3^{16} \equiv 203^2 = 41209 \equiv 171 \not\equiv 1 \pmod{289}$. Conclusion: 3 is a primitive root modulo 17^5. Indeed, 3 is a primitive root modulo 17^l for every $l \geqslant 2$ by Remark 3.9.

Finally, suppose we are asked to find any primitive root modulo 170 instead of 17. We need to check if 170 has one of the forms in the list in Theorem 3.10. The prime factorisation of 170 is $170 = 2 \times 5 \times 17$, which has two distinct odd prime factors, thus is not in the list. It follows that there is no primitive root modulo 170. In other words, $\mathbb{Z}_{170}^*$ is not cyclic.

3. Hints to Exercises 3.2 and 3.3

These two problems are simple yet important applications of primitive roots. Here are some hints, but you need to supply more details when writing down your own proofs.

Exercise 3.2:

For part (1), for any $a \in \mathbb{Z}$ coprime to p, "a has order d modulo p" means "$\overline{a}$ has order d in $\mathbb{Z}_p^*$". Equivalently, $a^d \equiv 1 \pmod{p}$ and $a^k \not\equiv 1 \pmod{p}$ for any $1 \leqslant k \leqslant d-1$. In this part of the problem we need to check these two conditions for $a = g^{\frac{p-1}{d}}$, both of which rely on the assumption that g is a primitive root modulo p (or equivalently, g has order $p-1$ modulo p).

Part (2) uses part (1). It is helpful to realise that $a^2 \equiv 1 \pmod{p}$ is equivalent to $p \mid (a^2-1) = (a+1)(a-1)$.

For part (3), assume g is a primitive root modulo 29, then $g^{28} \equiv 1 \pmod{29}$. We can use this to prove that $x \equiv g^{4k} \pmod{29}$ are always solutions. We can actually restrict ourselves to the values $k = 0, 1, 2, 3, 4, 5, 6$, because g^{4k} does not give new congruence class for any other $k \in \mathbb{Z}$. To prove there are no other solutions, you just need to realise that $\mathbb{Z}_{29}$ is a field. An equation of degree 7 can have at most 7 solutions in this field by Lemma 3.3 (or equivalently, at most 7 congruence classes modulo 29). If you have already found 7 solutions (as above), you should have found all.

Exercise 3.3:

For part (1), the "if" part is a simple observation. For the "only if" part, you need to realise that any solution x must be coprime to p, hence is in the congruence class of g^k for some $k \in \mathbb{Z}$.

Part (2) is extremely important because we will need to use this result next week. Using part (1), you only need to show that $a \equiv g^{dk} \pmod{p}$ iff $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$. This time the "only if" part is straightforward. For the "if" part, you need to realise that a is in the congruence class of g^l for some $l \in \mathbb{Z}$. And you just need to show l is a multiple of d.

For part (3), you need to use part (1) and the primitive root found in Exercise 3.1 (1). By allowing k to take various values you can get all values for a.

If you do everything correctly, then the values you found in parts (3) of these two exercises should agree. This is not a coincidence. Enthusiasts can try to figure out what the magic pattern is.

4. Hints to Exercise 3.4

There is, unfortunately, a typo in this problem. In the second line of part (3), g^l should be corrected to p^l. This exercise is a little more challenging. Some similar techniques were used in the proof of Proposition 3.8, but you can still do this exercise without reading that proof. Here are some hints, but you need to supply more details when writing down your own proofs.

For part (1), a hint is already given to you. If you take p-th powers on both sides of the equation in the hint and expand the right-hand side using binomial expansion, then you can see that every term on the right-hand side, except b^p, is divisible by p^{l+1}, which proves the statement.

For part (2), you can assume the order of g modulo p^m is d. The goal is to show $d = \phi(p^m)$. It suffices to prove that $d \mid \phi(p^m)$ and $\phi(p^m) \mid d$. For the first division, notice that $\mathbb{Z}_{p^m}^*$ has order $\phi(p^m)$, hence the order d of any element $\overline{g}$ is a positive divisor of $\phi(p^m)$. For the second division, you need to apply part (1) on the congruence $g^d \equiv 1 \pmod{p^m}$ repeatedly, more precisely, $n - m$ times. Then you will reach the congruence $g^{dp^{n-m}} \equiv 1 \pmod{p^n}$. Since g has order $\phi(p^n)$ modulo p^n (because g is a primitive root modulo p^n), we must have $\phi(p^n) \mid dp^{n-m}$. Using the formula for ϕ-function we can get the second division.

For part (3), the sufficiency is stated in Remark 3.9. For the necessity, you need to use part (2). More precisely, if g is a primitive root modulo p^l for some $l \geqslant 2$, then g is a primitive root modulo p and p^2, which give the two conditions in the statement.

Don't you think it's fun to play with the congruences? :-)