

Math 104B, Number Theory, Winter 2003.

Lecture 5.

Theorem 7.2.10 Let p be an odd prime.

(b). If g is a primitive root modulo p^2 , then it is a primitive root modulo p^k for $k \geq 2$.

Before going on, let's see how this helps us find primitive roots. The primitive roots modulo $9 = 3^2$ are 2 and 5. The primitive roots modulo $27 = 3^3$ are those numbers which are congruent to 2 or 5 modulo 9, namely 2, 11, 20, 5, 14, 23.

Remark. We should also remark that we are taking for granted that if g is a primitive root modulo p^k with $k > 2$ then g is a primitive root modulo p^2 . To show this, if g is not primitive modulo p^2 then there exists r with $0 < r < (p-1)p$ with $g^r \equiv 1 \pmod{p^2}$. Then

$$g^r = 1 + sp^2.$$

Now $\phi(p^k) = (p-1)p^{k-1}$ and so $0 < rp^{k-2} < \phi(p^k)$, but by the Binomial Theorem,

$$(*) \quad g^{rp^{k-2}} = (1 + sp^2)^{p^{k-2}} = 1 + sp^k + \binom{p^{k-2}}{2} (sp^2)^2 + \dots$$

Claim I. For $r > 1$,

$$p^k \mid p^{2r} \binom{p^{k-2}}{r}.$$

This says that all the terms in the binomial expansion (*) after the first term are divisible by p^k . Hence we see that $g^{rp^{k-2}} \equiv 1 \pmod{p^k}$, so g is not primitive modulo p^k .

Proof of Theorem 7.2.10(b). (Be warned that the book uses the variable k for two different quantities. The proof given below is an explanation of the short proof given in the book.) Suppose g is primitive modulo p^2 and let ℓ be the order of g modulo p^k . Then $g^\ell \equiv 1 \pmod{p^k}$, so $g^\ell \equiv 1 \pmod{p^2}$ and hence $(p-1)p \mid \ell$. On the other hand, since $\phi(p^k) = (p-1)p^{k-1}$, we see that $\ell \mid (p-1)p^{k-1}$. We conclude that $\ell = (p-1)p^j$ for some j with $1 \leq j \leq k-1$, and g is primitive modulo p^k if and only if

$$g^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}.$$

Now by Fermat's Theorem,

$$g^{p-1} = 1 + sp$$

for some s , and since g is primitive modulo p^2 , $p \nmid s$. Raising this to the power p^{k-2} , by the Binomial Theorem we get

$$(**) \quad g^{(p-1)p^{k-2}} = (1 + sp)^{p^{k-2}} = 1 + sp^{k-1} + \binom{p^{k-2}}{2} (sp)^2 + \dots$$

Claim II. If $r > 1$ then

$$p^k \mid p^r \binom{p^{k-2}}{r}.$$

Using this, we see that all the terms in the binomial expansion in (***) after the second term vanish, and so

$$g^{(p-1)p^{k-2}} \equiv 1 + sp^{k-1} \not\equiv 1 \pmod{p^k}.$$

Hence g is a primitive root modulo p^k .

It remains to prove the two claims, and since the second one clearly implies the first, it remains to prove Claim II.

Lemma. Suppose $0 \leq r \leq 2^{k-2}$. Write $r = p^\ell s$ with $p \nmid s$, so that p^ℓ is the largest power of p which divides r . Then the largest power of p which divides $\binom{p^{k-2}}{r}$ is $p^{k-2-\ell}$.

Example. Compute the power of 3 which divides $\binom{81}{18}$.

$$\binom{81}{18} = \frac{64 \ 65 \ \dots \ 81}{1 \ 2 \ \dots \ 18} = \frac{81}{18} \frac{80}{1} \frac{79}{2} \frac{78}{3} \frac{77}{4} \frac{76}{5} \frac{75}{6} \frac{74}{7} \frac{73}{8} \frac{72}{9} \frac{71}{10} \frac{70}{11} \frac{69}{12} \frac{68}{13} \frac{67}{14} \frac{66}{15} \frac{65}{16} \frac{64}{17}$$

We know that this rational number is actually an integer, and we are interested in finding the largest power of 3 which divides it. To compute this, let's replace each of the integers in the above expression by the largest power of 3 which divides it. We get

$$\frac{3^4}{3^2} \frac{1}{1} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3^2}{3^2} \frac{1}{1} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3}{3} \frac{1}{1} \frac{3}{3} \frac{1}{1}$$

We notice that all the powers of 3 cancel from the top and bottom except those in the first fraction

$$\frac{3^4}{3^2} = 3^2$$

and so this is the largest power of 3 which divides $\binom{81}{18}$. Notice that $81 = 3^4$ and $18 = 3^2 \cdot 2$ and the answer is $3^{4-2} = 3^2$. The idea that we gave in this example can be used to prove the Lemma in general. We will omit the formal proof.

Once we have the Lemma, Claim II becomes: If $r = p^\ell s > 1$ where $\ell \geq 0$, then

$$(***) \quad p^k \mid p^{r+k-2-\ell}.$$

Now (***) is equivalent to $\ell + 2 \leq r$, so what we want to prove is

Claim II': (All variables are integers) If $\ell \geq 0$ and $r = p^\ell s > 1$, then $\ell + 2 \leq r$.
 In the case when $\ell = 0$, the claim says that if $r = s > 1$ then $2 \leq r$, which is true.
 In the case when $\ell > 0$, the result is equivalent to the fact that for $\ell \geq 1$ we have $\ell + 2 \leq p^\ell$. This holds for $\ell = 1$ since the smallest odd prime is 3, and it is easily checked for larger values of ℓ by induction on ℓ . (There is a lot of room in this result, in general $\ell + 2$ is much smaller than p^ℓ .)

Discrete Logarithm. We finish the lecture with something a little less heavy. Let's see how we can solve the equation

$$8k^5 \equiv 3 \pmod{17}.$$

We have that 3 is a primitive root modulo 17, so we write a table of powers of 3:

k	1	2	3	4	5	6	7	8
$3^k \pmod{17}$	3	9	10	13	5	15	11	16
k	9	10	11	12	13	14	15	16
$3^k \pmod{17}$	14	8	7	4	12	2	6	1

Writing $x \equiv 3^k \pmod{17}$, since $8 \equiv 3^{10} \pmod{17}$ and $3 \equiv 3^1 \pmod{17}$,

$$8k^5 \equiv 3^{10} 3^{5x} \equiv 3^{10+5x} \equiv 3^1 \pmod{17}$$

and so by the Lemma from Lecture 1,

$$10 + 5x \equiv 1 \pmod{\text{ord}_{17}(3) = 16}.$$

Solving this, we have that the inverse of 5 is -3 modulo 16 and so

$$5x \equiv -9 \pmod{16} \quad \Rightarrow \quad x \equiv 27 \equiv 11 \pmod{16}.$$

Hence $k \equiv 3^x \pmod{17} \equiv 7 \pmod{17}$.