

**Math 104B, Number Theory, Winter 2003.**

**Lecture 4.**

**Lemma.** For  $k \geq 3$ ,  $\lambda(2^k) = 2^{k-2}$ .

**proof.** We already showed that there is no primitive root modulo  $2^k$ , hence  $\lambda(2^k) \neq \phi(2^k) = 2^{k-1}$ . Hence  $\lambda(2^k) | 2^{k-2}$ . Now we will show that 3 has order  $2^{k-2}$  modulo  $2^k$ , and hence  $\lambda(2^k) = 2^{k-2}$ . In order to show this, we just need to show that  $3^{2^{k-3}} \not\equiv 1 \pmod{2^k}$ . When  $k = 3$  this is clear, since  $3 \not\equiv 1 \pmod{8}$ . We will show by induction that for  $k \geq 4$ ,

$$(*) \quad 3^{2^{k-3}} = 1 + s_k 2^{k-1}, \quad s_k \text{ odd.}$$

Hence we immediately see that  $2^k$  does not divide  $3^{2^{k-3}} - 1$ , which proves the result. In the case  $k = 4$ , we have

$$3^2 = 1 + 2^3,$$

so the result holds with  $s_4 = 1$ . Now assume the result holds for  $k$ . Then

$$3^{2^{k-2}} = \left(3^{2^{k-3}}\right)^2 = (1 + s_k 2^{k-1})^2 = 1 + (s_k + s_k^2 2^{k-2})2^k.$$

But we see that  $s_{k+1} = s_k + s_k^2 2^{k-2}$  is odd, and hence the result holds for  $k + 1$ . By induction, the result holds for all  $k$ .

**Theorem 7.2.10** Let  $p$  be an odd prime.

- (a). If  $g$  is a primitive root modulo  $p$ , then either  $g$  or  $g + p$  is a primitive root modulo  $p^2$ .
- (b). If  $g$  is a primitive root modulo  $p^2$ , then it is a primitive root modulo  $p^k$  for  $k \geq 2$ .
- (c). Suppose  $g$  is a primitive root modulo  $p^k$ . If  $g$  is odd, then it is a primitive root modulo  $2p^k$ . If  $g$  is even then  $g + p^k$  is a primitive root modulo  $2p^k$ .

Before going on, let's see how this helps us find primitive roots. Let us first remark that if  $a$  is a primitive root modulo  $p^2$  then it must be a primitive root modulo  $p$ . Indeed, suppose that  $a$  is not a primitive root modulo  $p$ , so that  $a^r \equiv 1 \pmod{p}$  where  $r < p - 1$ . Then  $a^r = 1 + sp$  for some  $s$ . But then

$$a^{rp} = (1 + sp)^p = 1 + \binom{p}{1} sp + \binom{p}{2} s^2 p^2 + \dots \equiv 1 \pmod{p^2},$$

but  $rp < (p - 1)p = \phi(p^2)$ , so  $a$  is not a primitive root modulo  $p^2$ .

**Examples.** Modulo 3, we see that 2 is a primitive root.

Modulo 9: The elements congruent to 2 modulo 3 are 2, 5, 8. We want to know which ones have order  $\phi(9) = 6$ . Since  $8 \equiv -1$  has order 2 modulo 9, we know 8 doesn't work. Since the number of primitive roots is  $\phi(6) = 2$ , the primitive roots are 2 and 5.

Modulo 18: The primitive roots are  $2 + 9 = 11$  and  $5$ .

Modulo 5: Primitive roots have order  $\phi(5) = 4$ , and there are  $\phi(4) = 2$  of them. Since  $0, 1, 4$  cannot be primitive roots, the primitive roots are  $2$  and  $3$ .

Modulo 25: The primitive roots have order  $\phi(25) = 20$ , and there are  $\phi(20) = 8$  of them. They must all be congruent to  $2$  or  $3$  modulo  $5$ . The possibilities are

2	3
7	8
12	13
17	18
22	23

We just have to eliminate two of these possibilities.

We proved Theorem 7.2.10 (a). The proof used the fact that if  $g$  is a primitive root modulo  $p$ , then  $g$  is a primitive root modulo  $p^2$  if and only if  $g^{p-1} \not\equiv 1 \pmod{p^2}$ . Applying this to the case of computing the primitive roots modulo  $25$ , we see that we wish to eliminate the solutions of

$$\begin{cases} x^4 \equiv 1 \pmod{25}, \\ x \equiv 2 \text{ or } 3 \pmod{5} \end{cases}.$$

We solve this in the usual way.

$x$	2	3
$f = x^4 - 1$	15	80
$f' = 4x^3$	32	108

One solution is  $x = 2 + 5t$  where  $t$  satisfies

$$\begin{aligned} 15 + 5t \cdot 32 &\equiv 0 \pmod{25} \\ \Rightarrow 3 + 32t &\equiv 0 \pmod{5} \\ \Rightarrow 2t &\equiv 2 \pmod{5} \\ \Rightarrow t &\equiv 1 \pmod{5}. \end{aligned}$$

The solution is  $x = 7$ . The other solution is  $x = 3 + 5t$  where  $t$  satisfies

$$\begin{aligned}80 + 5t \cdot 108 &\equiv 0 \pmod{25} \\ \Rightarrow 16 + 108t &\equiv 0 \pmod{5} \\ \Rightarrow 3t &\equiv 4 \pmod{5} \\ \Rightarrow t &\equiv 3 \pmod{5}.\end{aligned}$$

The solution is  $x = 18(\equiv -7)$ . Hence the twelve primitive roots modulo 25 are 2, 3, 8, 12, 13, 17, 22, 23.

We proved Theorem 7.2.10 (b).