

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

### Lecture 6.

We have some loose ends to finish up.

**Homework question 7.1 number 11.** If  $(m, n) = 1$  and  $\text{ord}_m(x) = k$  and  $\text{ord}_n(x) = \ell$ , then  $\text{ord}_{mn}(x) = [k, \ell]$ .

**Proposition 7.2.12** If  $m = 2^d p_1^{a_1} \dots p_k^{a_k}$ , where  $p_1, \dots, p_k$  are distinct odd primes, then  $\lambda(m)$  is the least common multiple

$$[\lambda(2^d), \lambda(p_1^{a_1}), \dots, \lambda(p_k^{a_k})].$$

We proved this following the text.

**Remark.**  $\lambda(p^a) = \phi(p^a) = (p-1)p^{a-1}$ , and  $\lambda(2) = 1$ ,  $\lambda(4) = 2$  and  $\lambda(2^d) = 2^{d-2}$  if  $d > 2$ .

**Example.** Find an element of maximal order modulo 100.

$100 = 4 \cdot 5^2$  so  $\lambda(100) = [\lambda(4), \lambda(5^2)] = [2, 20] = 20$ . Now we already figured out the elements of order 20 modulo 25, they are 2, 3, 8, 12, 13, 17, 22, 23. In fact it is easy to see that the elements of order 20 modulo 100 are precisely the odd elements which have order 20 modulo 25. (They have to be odd to be relatively prime to 100, and since  $\text{ord}_{100}(x) = [\text{ord}_4(x), \text{ord}_{25}(x)]$ , they must have order 20 modulo 25.) The elements of order 20 modulo 100 are  $2 + 25 = 27$ ,  $2 + 75 = 77$ ,  $3 + 50 = 53$ , etc..

**Example.** Find an element of maximal order modulo 176.

$176 = 2^4 \cdot 11$  so  $\lambda(176) = [\lambda(2^4), \lambda(11)] = [4, 10] = 20$ . To find an element  $x$  of order 20 modulo 176, we need  $x$  to have order 4 modulo 32, (we know that  $x \equiv 3 \pmod{32}$  works, and  $x$  should have order 5 or 10 modulo 11. Now modulo 11, the possible orders for elements are 1, 2, 5, 10. Since the elements of order 1 and 2 are 1 and 10, the other elements all have order 5 and 10. Hence 3 has order 5 or 10 modulo 11 (actually order 5) and so 3 is primitive modulo 176.

### Discrete Logarithm.

**Recall:**

$$(*) \quad g^x \equiv g^y \pmod{m} \Leftrightarrow x \equiv y \pmod{\text{ord}_m(g)}.$$

Suppose that  $g$  is a primitive element modulo  $m$ . Then because  $g^0, g^1, \dots, g^{\phi(m)-1}$  are all distinct modulo  $m$ , they give all the elements modulo  $m$  which are relatively prime to  $m$ , i.e. every element  $k$  with  $(k, m) = 1$  can be written as  $k \equiv g^x \pmod{m}$  for some  $x$  with  $0 \leq x < \phi(m)$ . We define  $x$  to be the *discrete logarithm* or *index* of  $y$  (to the base  $g$ ). To repeat this, if  $0 \leq x < \phi(m)$ , then

$$\text{ind}_g(k) = x \quad \Leftrightarrow \quad k \equiv g^x \pmod{m}.$$

The book's notation is convenient. There is a distinction between

$$a \equiv b \pmod{n}, \quad \text{and} \quad a = b \pmod{n}.$$

The first means  $n|a - b$  while the second means that  $a$  is equal to the remainder when  $b$  is divided by  $n$ . By (\*), we have

$$\text{ind}_g(k) = x \pmod{\phi(m)}, \quad \Leftrightarrow \quad g^x \equiv k \pmod{m}.$$

In particular,  $g^{\text{ind}_g(k)} \equiv k \pmod{m}$ . We have the rules

**Proposition 7.3.3.**

- (a).  $\text{ind}_g(1) = 0$ .
- (b).  $\text{ind}_g(g) = 1$ .
- (c).  $\text{ind}_g(k\ell) = (\text{ind}_g k + \text{ind}_g \ell) \pmod{\phi(m)}$ .
- (d).  $\text{ind}_g(k^a) = a \text{ind}_g(k) \pmod{m}$ .