

Math 104B, Number Theory, Winter 2003.

Lecture 3.

Proposition 3. See Cor. 7.2.9. The number of elements of order d modulo m in the set $\{a, a^2, \dots, a^{\text{ord}_m(a)}\}$ is $\phi(d)$ if $d \mid \text{ord}_m(a)$ and 0 if $d \nmid \text{ord}_m(a)$. In particular, if there exists a primitive root modulo m then the number of invertible elements of order d is $\phi(d)$ if $d \mid \phi(m)$ and 0 if $d \nmid \phi(m)$, so if there exists a primitive root modulo $m > 2$ then there is exactly one element of order 2 modulo m .

Theorem. See Props. 7.1.13 and 7.1.14, and Ths. 7.2.8 and 7.2.10. There exists a primitive root modulo m if and only if m is of the form $2, 4, p^k$, or $2p^k$ where p is an odd prime.

Lemma. (a). If $m = 2^k$ with $k \geq 3$, then there is no primitive root modulo m . (b). If $m > 2, n > 2$ and $(m, n) = 1$, then there is no primitive root modulo mn .

Proof. In both cases we show that there is more than one element of order 2 contradicting Prop. 3. To do this we need to exhibit more than 2 elements satisfying $x^2 \equiv 1$. (a). If $m = 2^k$ with $k \geq 3$, it is easy to check that the 4 elements

$$1, -1, 2^{k-1} + 1, 2^{k-1} - 1$$

all satisfy $x^2 \equiv 1 \pmod{2^k}$, (in fact they are the only elements which do).

(b). We can obtain 4 elements satisfying $x^2 \equiv 1 \pmod{mn}$ by using the Chinese Remainder Theorem to solve the following pairs of congruences.

$$\left\{ \begin{array}{l} x \equiv 1 \pmod{m} \\ x \equiv 1 \pmod{n} \end{array} \right\}, \quad \left\{ \begin{array}{l} x \equiv -1 \pmod{m} \\ x \equiv 1 \pmod{n} \end{array} \right\}, \quad \left\{ \begin{array}{l} x \equiv 1 \pmod{m} \\ x \equiv -1 \pmod{n} \end{array} \right\}, \quad \left\{ \begin{array}{l} x \equiv -1 \pmod{m} \\ x \equiv -1 \pmod{n} \end{array} \right\}.$$

We also gave the proof in 7.1.14.

It remains to show that there are primitive roots modulo p^k and $2p^k$ for p odd. We start by showing that there is a primitive root modulo p for p prime. For this we introduce

Notation. Set $M(m) = \max\{\text{ord}_m(a) : (a, m) = 1\}$.

Definition. See 7.2.2. Set $\lambda(m) = \min\{k : a^k \equiv 1 \pmod{m} \text{ for all } a \text{ with } (a, m) = 1\}$. Then $\lambda(m)$ is called the *minimal universal exponent modulo m* .

We will show $M(m) = \lambda(m)$.

Proposition. See Prop 7.2.5. If a has order j modulo m and b has order k modulo m , then there exists an element of order $[j, k]$ modulo m .

Proof. First suppose $(j, k) = 1$. Then we claim that ab has order jk . Indeed, let ℓ be the order of ab . Then since $(ab)^{jk} = a^{jk}b^{jk} \equiv 1 \pmod{m}$ we have that $\ell|jk$. Conversely since ℓ is the order of ab we have $(ab)^\ell \equiv 1 \pmod{m}$. Raising this to the power j gives

$$b^{j\ell} \equiv a^{j\ell}b^{j\ell} \equiv ((ab)^\ell)^j \equiv 1 \pmod{m},$$

and so $k|j\ell$. Since $(j, k) = 1$, we have $k|\ell$. Similarly we get $j|\ell$ and so $jk|\ell$. Hence $jk = \ell$.

In the case when $(j, k) \neq 1$ we can find u, v, x, y such that $j = ux$, $k = vy$, $(x, y) = 1$, and $xy = [j, k]$. For example we can take $x = j$ and $y = x/(x, y)$. Then since a^u has order x and b^v has order y , by the previous case we obtain an element of degree $xy = [j, k]$ modulo m .

We showed that $M(m) = \lambda(m)$ by following the proof of Proposition 7.2.7.

We followed the proof of *Proposition 7.2.8*, showing that there exists a primitive root modulo p .