

Math 104B, Number Theory, Winter 2003.

Lecture 2.

Proposition 1. See Prop. 7.1.3. If $a^k \equiv 1 \pmod{m}$ then $\text{ord}_m(a) | k$, in particular by Euler's Theorem, $\text{ord}_m(a) | \phi(m)$.

Corollary. See Cor. 7.1.4. If $(a, m) = 1$ then $a^i \equiv a^j \pmod{m} \Leftrightarrow i \equiv j \pmod{\text{ord}_m(a)}$.

Corollary. See Cor. 7.1.6. The elements $a, a^2, \dots, a^{\text{ord}_m(a)}$ are distinct modulo m .

Proposition 2. See Lem. 7.1.8. If $(a, m) = 1$, then

$$\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{(k, \text{ord}_n(a))}.$$

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 $d | \text{ord}_m(a)$ and 0 otherwise. In particular, if there exists a primitive root modulo m then the number of invertible elements of order d is $\phi(d)$ if $d | \phi(m)$ and 0 otherwise.

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.

Proof of Proposition 2. We first consider the example when a has order 12 modulo m . We compute the orders of a^3 and a^8 . (See 7.1.9.) Working modulo m ,

$$a^3 \not\equiv 1, \quad a^6 \not\equiv 1, \quad a^9 \not\equiv 1, \quad a^{12} \equiv 1,$$

so a^3 has order 4.

$$a^8 \not\equiv 1, \quad a^{16} \equiv a^4 \not\equiv 1, \quad a^{24} \equiv 1,$$

so a^8 has order 3. In general, if a has order O_1 modulo m and a^k has order O_k modulo m , then the powers of a^k are

$$a^k, \quad a^{2k}, \quad a^{3k}, \dots, a^{O_k k} \equiv 1 \pmod{m}.$$

By Proposition 1, O_k is the smallest positive number such that O_1 divides $O_k k$. Then $O_k k = [k, O_1]$, and

$$O_k = \frac{[k, O_1]}{k} = \frac{k O_1}{k(k, O_1)} = \frac{O_1}{(k, O_1)}.$$

We also gave the proof in the book, see 7.1.8..

Proof of Proposition 3. Set $\text{ord}_m(a) = O_1$. Using Proposition 2,

$$\begin{aligned}
 (*) \quad \{j : 1 \leq j \leq O_1, O_m(a^j) = d\} &= \{j : 1 \leq j \leq O_1, O_1/(j, O_1) = d\} \\
 &= \{j : 1 \leq j \leq O_1, (j, O_1) = O_1/d\}
 \end{aligned}$$

Now $(j, O_1) = O_1/d \Rightarrow (O_1/d)|j \Rightarrow j = \ell O_1/d$ for some ℓ , and replacing j by this, (*) is equal to

$$\{\ell O_1/d : 1 \leq \ell \leq d, (\ell O_1/d, O_1) = O_1/d\},$$

but $(ac, bc) = (a, b)c$, so $(\ell O_1/d, O_1) = (\ell, d)O_1/d$, and the set (*) equals

$$\{\ell O_1/d : 1 \leq \ell \leq d, (\ell, d) = 1\}.$$

The number of such elements is $\#\{\ell : 1 \leq \ell \leq d, (\ell, d) = 1\} = \phi(d)$.

From Proposition 3, we see in particular that if $m > 2$ and there exists a primitive root modulo m , then there exists precisely one element of order 2.

(Note, we can check that if $m > 2$ then 2 divides $\phi(m)$, in two ways. Either write down the formula for $\phi(m)$ in terms of the prime factorization of m , or we can note that the number -1 has order 2 modulo m , and hence $2|\phi(m)$ by Proposition 1.)