Lecture Notes for International Mathematical Olympiad

ORDER THEORY AND PRIMITIVE ROOT

1. Basic notions

By Euler's theorem, whenever $(a, m) = 1$ and $m > 1$ we have $a^{\varphi(m)} \equiv 1 \bmod m$. Hence there exists a minimal positive integer $r \leqslant \varphi(m)$ such that $a^r \equiv 1 \bmod m$.

Definition 1. Suppose $(a, m) = 1$ and $m > 1$. The *order* of a modulo m,[1] denoted by $\delta_m(a)$, is the minimal positive integer r such that $a^r \equiv 1 \bmod m$.

Example 2. (1) Take $a = 2$ and $m = 7$. Then

$$2^1 \equiv 2 \bmod 7, \quad 2^2 \equiv 4 \bmod 7, \quad 2^3 \equiv 1 \bmod 7.$$

Hence $\delta_7(2) = 3$, whereas $\varphi(7) = 6$.

(2) Take $a = 2$ and $m = 11$. Then one can check that

n	1	2	3	4	5	6	7	8	9	10
$2^n \bmod 11$	2	4	8	5	-1	-2	-4	-8	-5	1

Hence $\delta_{11}(2) = 10 = \varphi(11)$.

Definition 3. If the order of a modulo m is exactly $\varphi(m)$, i.e.,

$$\delta_m(a) = \varphi(m),$$

then a is called a *primitive root* of m.

Remark 4. (1) Given a which is a primitive root of some m, we remark that m is not necessarily prime. For example, take $a = 5$ and $m = 6$. Then $\delta_6(5) = 2 = \varphi(6)$ but m is not prime.

(2) For fixed m, the primitive root of m is not necessarily unique, even if m is prime. For example, since $\varphi(2) = 1$ and $2k+1 \equiv 1 \bmod 2$, we see $\delta_2(2k+1) = \varphi(2)$; namely, all odd integers are primitive roots of 2.

2. Basic features of primitive root and order

In the upcoming context, if we have defined $\delta_m(a)$ then supposedly $(a, m) = 1$, which will be omitted as an indicated assumption.

Theorem 5. *Suppose $\delta = \delta_m(a)$. Then $1, a, \ldots, a^{\delta-1}$ have mutually distinct remainders modulo m.*

Proof. Assume there are k, l satisfying $0 \leqslant k < l \leqslant \delta - 1$, such that $a^k \equiv a^l \bmod m$. Since $(a, m) = 1$, we have $(a^k, m) = 1$. It follows that $a^{l-k} \equiv 1 \bmod m$ with $0 < l - k < \delta$. This contradicts to the assumption that $\delta = \delta_m(a)$ by the minimality. □

Date: August 28, 2022.

[1]Referring to some other materials, the order is also called the index of a modulo m.

Theorem 6. *If* $\delta = \delta_m(a)$, *then*

$$a^r \equiv a^{r'} \bmod m \iff r \equiv r' \bmod \delta.$$

In particular, $a^r \equiv 1 \bmod m$ *if and only if* $\delta \mid r$.

Proof. Write $r = \delta q + r_0$ and $r' = \delta q' + r_0'$ with $0 \leqslant r_0, r_0' \leqslant \delta - 1$. We first tackle with the "only if" part. For this,

$$a^\delta \equiv 1 \bmod m \implies a^r = (a^\delta)^q \cdot a^{r_0} \equiv a^{r_0} \bmod m,$$

and similarly $a^{r'} \equiv a^{r_0'} \bmod m$. Also, as $a^r \equiv a^{r'} \bmod m$, we have $a^{r_0} \equiv a^{r_0'} \bmod m$. This forces r_0 to equal to r_0'. Then $r \equiv r' \bmod \delta$.

Conversely, suppose $r \equiv r' \bmod \delta$, and hence $r_0 = r_0'$. Consequently,

$$a^r = (a^\delta)^q \cdot a^{r_0} \equiv a^{r_0} \equiv a^{r'} \bmod m$$

for the same reason. Hence we have finished the proof. In particular, $a^r \equiv 1 \bmod a^\delta \bmod m$ if and only if $\delta \mid r - \delta$, or equivalently $\delta \mid r$. □

From this we have a natural corollary:

Corollary 7. *Suppose* $\delta_m(a) = \delta$. *Then* $\delta \mid \varphi(m)$.

Theorem 8. *Suppose* $a, b > 0$. *We have*

$$\delta_m(x) = ab \implies \delta_m(x^a) = b,\ \delta_m(x^b) = a.$$

Proof. Since $(x, m) = 1$ we see $(x^a, m) = 1$. This implies the existence of $\delta := \delta_m(x^a)$. So it suffices to show $\delta = b$. On the one hand, $(x^a)^\delta \equiv 1 \bmod m$ renders $x^{a\delta} \equiv 1 \bmod m$. As $\delta_m(x) = ab$, by Theorem 6 above, $ab \mid a\delta$, and then $b \mid \delta$. On the other hand,

$$\delta_m(x) = ab \implies x^{ab} \equiv 1 \bmod m \implies (x^a)^b \equiv 1 \bmod m.$$

As $\delta_m(x^a) = \delta$, by Theorem 6 again, $\delta \mid b$. To conclude, we have $\delta = b$ and similarly, $\delta_m(x^b) = a$.[2] □

Theorem 9. *Suppose* $(a, b) = 1$. *Then*

$$\delta_m(x) = a,\ \delta_m(y) = b \implies \delta_m(xy) = ab.$$

Proof. Note that $(xy, m) = 1$ as $(x, m) = (y, m) = 1$. It suffices to show that $\delta := \delta_m(xy) = ab$. We have

$$(xy)^\delta \equiv 1 \bmod m \implies (xy)^{\delta b} \equiv 1 \bmod m \implies x^{\delta b} \cdot (y^b)^\delta \equiv 1 \bmod m.$$

Since $\delta_m(y) = b$, we see

$$y^b \equiv 1 \bmod m \implies x^{b\delta} \equiv 1 \bmod m \implies a \mid b\delta$$

because $\delta_m(x) = a$ by assumption. Also, $(a, b) = 1$ deduces $a \mid \delta$. For the same reason,

$$(xy)^{\delta a} \equiv 1 \bmod m \implies b \mid \delta.$$

As $(a, b) = 1$, we have $ab \mid \delta$ as required. On the other hand,

$$(xy)^{ab} \equiv (x^a)^b \cdot (y^b)^a \equiv 1 \bmod m \implies \delta \mid ab$$

[2] Be caution that the assumption $a, b > 0$ is finally applied. Because $a \mid b$ and $b \mid a$ implies only $|a| = |b|$.

because of $\delta_m(xy) = \delta$. Therefore, $\delta = ab$. □

The following is somehow the inverse of Theorem 9.

Proposition 10. *We have*

$$\delta_m(x) = a,\ \delta_m(y) = b,\ \delta_m(xy) = ab \implies (a, b) = 1.$$

Proof. We have $x^a \equiv 1 \bmod m$ and $y^b \equiv 1 \bmod m$. Then

$$x^{[a,b]} \equiv y^{[a,b]} \equiv 1 \bmod m.$$

So $(xy)^{[a,b]} \equiv 1 \bmod m$, and $ab \mid [a, b]$, which indicates that $ab = [a, b] = ab/(a, b)$. So we deduce $(a, b) = 1$. □

Theorem 11. *Assume $\lambda \geqslant 1$ and $\delta_m(a) = \delta$. Then*

$$\delta_m(a^\lambda) = \frac{\delta}{(\lambda, \delta)}.$$

Proof. First check that $(a^\lambda, m) = 1$ as $(a, m) = 1$. Hence we can denote $\nu = \delta_m(a^\lambda)$. Then $a^{\lambda\nu} \equiv 1 \bmod m$. Since $\delta_m(a) = \delta$, we see

$$\delta \mid \lambda\nu \implies \frac{\delta}{(\lambda, \delta)} \mid \frac{\lambda}{(\lambda, \delta)} \cdot \nu.$$

Moreover,

$$\left(\frac{\delta}{(\lambda, \delta)}, \frac{\lambda}{(\lambda, \delta)}\right) = 1 \implies \frac{\delta}{(\lambda, \delta)} \mid \nu.$$

On the other hand,

$$(a^\lambda)^{\frac{\delta}{(\lambda,\delta)}} = a^{\frac{\lambda\delta}{(\lambda,\delta)}} = (a^\delta)^{\frac{\lambda}{(\lambda,\delta)}} \equiv 1 \bmod m.$$

Again, because of $\delta_m(a^\lambda) = \nu$ by assumption, we have $\nu \mid \frac{\delta}{(\lambda,\delta)}$. To sum up, we have proved $\frac{\delta}{(\lambda,\delta)} = \nu$. □

Here are some corollaries of Theorem 11.

Theorem 12. *Let p be a prime. Suppose there exists $a \in \mathbb{Z}$ such that $\delta_p(a) = l$. Then there exist exactly $\varphi(l)$ integers that are mutually distinct modulo p, such that all of them share the same order l modulo p.*

Proof. Since $\delta_p(a) = l$, by Theorem 5, the set $S = \{a, a^2, \ldots, a^l\}$ contains l different elements modulo p. We are to prove that S is exactly the set of all solutions (up to modulo p) to

$$(*) \qquad x^l \equiv 1 \bmod p.$$

For any $x \in S$, there is $1 \leqslant \lambda \leqslant l$ such that $x = a^\lambda$. So $x^l = (a^\lambda)^l = (a^l)^\lambda \equiv 1 \bmod p$. Thus we have checked that each element of S is a solution to $(*)$. By Lagrange's theorem, there are at most l solutions to $(*)$. This proves that S is exactly the set of all solutions to $(*)$.

Now due to Theorem 11, $\delta_p(a^\lambda) = l$ if and only if $(\lambda, l) = 1$. Then there are exactly $\varphi(l)$ modulo-p-distinct integers with order l modulo p. □

3. A crash application to Mersenne integers

Problem 13. *Let p be an odd prime and q is a prime divisor of $2^p - 1$.*[3] *Show that $q \equiv 1 \bmod 2p$.*

Proof. By assumption $q \mid 2^p - 1$, and thus $2^p \equiv 1 \bmod p$. By the order theory we have $\delta_q(2) \mid p$ (c.f. Theorem 6). But p is an odd prime, which forces $\delta_q(2)$ to be p.

On the other hand, by Fermat's little theorem, $2^{q-1} \equiv 1 \bmod q$. So by Theorem 6, the given condition $p \mid q - 1$ is equivalent to $q \equiv 1 \bmod p$. This completes the proof because $(2, p) = 1$ and $q \equiv 1 \bmod 2$. □

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn

[3]Recall that the integer of the form $2^k - 1$ is called a Mersenne integer.