初等数论

吴 伊 涛

2021 年秋

Lecture 11. Primitive Roots and the order of an integer

Def: Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$, $g.c.d.(a, m) = 1$.

Then the least positive integer r s.t. $a^r \equiv 1 \pmod{m}$ is called the order of a modulo m, and denoted by $O_m(a)$.

So, $O_m(a) := \inf \{ t \in \mathbb{Z}^+ : a^t \equiv 1 \pmod{m} \}$.

E.g.

1. $m = 5$, $a = 2$.

   $2^1 \equiv 2 \pmod 5$, $2^2 \equiv 4 \pmod 5$, $2^3 \equiv 3 \pmod 5$, $2^4 \equiv 1 \pmod 5$

   $\therefore O_5(2) = 4$.

2. $m = 6$, $a = 5$

   $5^1 \equiv 5 \pmod 6$ $\quad$ $5^2 \equiv 1 \pmod 6$

   $\therefore O_6(5) = 2$.

3. $\forall m \in \mathbb{Z}^+$, $O_m(1) = 1$.

Remark: Note that the order of a modulo m is DIFFERENT from the order of a at (a prime) m. i.e.

$O_m(a) \neq \mathrm{ord}_m a$ (even if m is a prime).

Lemma: Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ and $g.c.d.(a,m)=1$.

If n is a positive integer s.t. $a^n \equiv 1 \pmod{m}$,

then $O_m(a) \mid n$.

Proof: ※1 Use Division Algorithm, $n = q \cdot O_m(a) + r$, $0 \le r < O_m(a)$.

It suffices to prove $r=0$.

Since $a^n = a^{q \cdot O_m(a) + r} = (a^{O_m(a)})^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{m}$

$\therefore\ a^r \equiv 1 \pmod{m}$

By definition of $O_m(a)$ and $r < O_m(a)$, we get $r=0$,

thus $O_m(a) \mid n$. $\square$

By this lemma, together with Euler's theorem, we get the following Corollary: (which also gives the existence of $O_m(a)$).

Cor1: Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ and $g.c.d.(a,m)=1$. Then

$$O_m(a) \mid \phi(m).$$

If we further assume m is a prime, then we get:

Cor 2: If p is a prime, $p \nmid a$, then

$$O_p(a) \mid p-1.$$

E.g. 1. $m = 7$,

$\forall a$ s.t. $7 \nmid a$, $O_7(a) \mid 6$, i.e. $O_7(a) \in \{1, 2, 3, 6\}$

2. $m = 11$.

$\forall a$, s.t. $11 \nmid a$, $O_{11}(a) \mid 10$, i.e. $O_{11}(a) \in \{1, 2, 5, 10\}$

3. $m = 18 = 2 \times 3^2$

$\forall a$, s.t. $g.c.d.(a, 18) = 1$, $O_{18}(a) \mid 6$. $(\phi(18) = 6)$.

$\therefore O_{18}(a) \in \{1, 2, 3, 6\}$

4. $m = 1001 = 7 \times 11 \times 13$

$\phi(m) = (7-1) \times (11-1) \times (13-1) = 720$.

$\forall a$, s.t. $g.c.d.(a, 1001) = 1$, $O_{1001}(a) \mid 720$.

5. $m = 108108 = 2^2 \times 3^3 \times 7 \times 11 \times 13$

$\phi(108108) = (2^2 - 2) \times (3^3 - 3^2) \times (7-1) \times (11-1) \times (13-1) = 25920$.

$\forall a$, s.t. $g.c.d.(a, 108108) = 1$, $O_{108108}(a) \mid 25920$.

However, we claim that: the bounds $\phi(m)$ in example 4 and 5 are by far not the best bound of $O_m(a)$. To see this, let's see the next proposition.

Prop. Let $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$ where $p_1, p_2, \cdots p_\ell$ are distinct primes, $\alpha_1, \alpha_2, \cdots \alpha_\ell$ are positive integers, $a \in \mathbb{Z}$, g.c.d.$(a, m) = 1$. Then

$$O_m(a) = \text{l.c.m.}\left(O_{p_1^{\alpha_1}}(a), O_{p_2^{\alpha_2}}(a), \cdots, O_{p_\ell^{\alpha_\ell}}(a)\right). \quad (*)$$

Proof:
For convenience, we denote the RHS of $(*)$ by n, we want to show: $n \mid O_m(a)$ and $O_m(a) \mid n$.

Since $a^{O_m(a)} \equiv 1 \pmod{m}$, it then follows that:

$a^{O_m(a)} \equiv 1 \pmod{p_1^{\alpha_1}}$, $a^{O_m(a)} \equiv 1 \pmod{p_2^{\alpha_2}}$, $\cdots$, $a^{O_m(a)} \equiv 1 \pmod{p_\ell^{\alpha_\ell}}$

So, by the lemma above, we get:

$O_{p_1^{\alpha_1}}(a) \mid O_m(a)$, $O_{p_2^{\alpha_2}}(a) \mid O_m(a)$, $\cdots$, $O_{p_\ell^{\alpha_\ell}}(a) \mid O_m(a)$

Thus $n \mid O_m(a)$.

Conversely,

Since $O_{p_1^{\alpha_1}}(a) \mid n$, thus $a^{\cancel{O_m(a)}\, n} \equiv 1 \pmod{p_1^{\alpha_1}}$;

Since $O_{p_2^{\alpha_2}}(a) \mid n$, thus $a^{\cancel{O_m(a)}\, n} \equiv 1 \pmod{p_2^{\alpha_2}}$;

$\vdots$

Since $O_{p_\ell^{\alpha_\ell}}(a) \mid n$, thus $a^{\cancel{O_m(a)}\, n} \equiv 1 \pmod{p_\ell^{\alpha_\ell}}$.

$\therefore$ $\cancel{a^{O_m(a)}}$ $a^n \equiv 1 \pmod{m}$, by the lemma on page 156 again, we get $O_m(a) \mid n$.

$\square$

Rmk. If we let $m = m_1 \cdot m_2 \cdots m_K$ where $m_1, m_2, \cdots m_K$ are pairwise coprime integers. The consequence then changes as:

$$O_m(a) = \text{l.c.m.}(O_{m_1}(a), O_{m_2}(a), \cdots, O_{m_K}(a)).$$

The proof is similar.

E.g. 1. $m = 1001 = 7 \times 11 \times 13$.

$\therefore \forall a \in \mathbb{Z}$, $\text{g.c.d.}(a, 1001) = 1$. Then we have:

$O_{1001}(a) = \text{l.c.m.}(O_7(a), O_{11}(a), O_{13}(a))$.

Now, $O_7(a) \mid 6$, $O_{11}(a) \mid 10$, $O_{13}(a) = 12$.

$\therefore O_{1001}(a) \mid \text{l.c.m.}(6, 10, 12) = 60$.

Now, if $a = 2$, we have:

$O_7(2) = 3$, $O_{11}(2) = 10$, $O_{13}(2) = 12$.

$\therefore O_{1001}(2) = \text{l.c.m.}(3, 10, 12) = 60$.

If $a = 10$, we have:

$O_7(10) = 6$, $O_{11}(10) = 2$, $O_{13}(10) = 6$

$\therefore O_{1001}(10) = \text{l.c.m.}(6, 2, 6) = 6$

If $a = 12$, we have:

$O_7(12) = 6$, $O_{11}(12) = 1$, $O_{13}(12) = 2$.

$\therefore O_{1001}(12) = \text{l.c.m.}(6, 1, 2) = 6$.

Eg 2. Calculate the order of 109 modulo 108108.

Sol:
$$108108 = 2^2 \times 3^3 \times 7 \times 11 \times 13, \quad g.c.d.(109, 108108) = 1.$$

$$O_{108108}(109) = l.c.m.\left(O_4(109), O_{27}(109), O_7(109), O_{11}(109), O_{13}(109)\right).$$

① $109 \equiv 1 \pmod 4$, $\therefore$ $\underline{O_4(109) = 1}$.

② $109 \equiv 1 \pmod{27}$. $\therefore$ $\underline{O_{27}(109) = 1}$.

③ $109 \equiv 4 \pmod 7$, and $O_7(109) = O_7(4) \mid 7-1 = 6$.

$\therefore O_7(109) \in \{1, 2, 3, 6\}$.

$4^1 \equiv 4 \pmod 7$, $4^2 \equiv 2 \pmod 7$, $4^3 \equiv 1 \pmod 7$

$\therefore$ $\underline{O_7(109) = O_7(4) = 3}$.

④ $109 \equiv -1 \pmod{11}$. $\therefore$ $\underline{O_{11}(109) = 2}$.

⑤ $109 \equiv 5 \pmod{13}$, $\therefore$ $O_{13}(109) = O_{13}(5) \mid 13-1 = 12$.

$\therefore O_{13}(109) = O_{13}(5) \in \{1, 2, 3, 4, 6, 12\}$

$5^1 \equiv 5 \pmod{13}$, $5^2 \equiv -1 \pmod{13}$, $5^3 \equiv -5 \pmod{13}$

$5^4 \equiv 1 \pmod{13}$

$\therefore$ $\underline{O_{13}(109) = O_{13}(5) = 4}$.

So,
$$\begin{aligned} O_{108108}(109) &= l.c.m.\left(O_4(109), O_{27}(109), O_7(109), O_{11}(109), O_{13}(109)\right) \\ &= l.c.m.(1, 1, 3, 2, 4) \\ &= 12. \end{aligned}$$

(1640,Frenicle to Fermat)

Find a perfect number between 10^{20} and 10^{22}.

Recall that an even perfect number should have a form $2^{p-1}(2^p-1)$ where 2^p-1 is a prime(the so called Mersenne prime), and we haven't found any odd perfect number now.

Hence we need to find:

$$10^{20} \leq 2^{p-1}(2^p-1) \leq 10^{22} \qquad (*)$$

with 2^p-1 is a prime.

It's easy to get $34 \leq p \leq 37$ from (*). Clearly, 2^p-1 is a prime only if p is a prime.

Thus Frenicle's problem is equivalent to the following problem:

Is $2^{37}-1$ a prime or a composite?

Prop. All prime factors of $2^{37}-1$ are 74k+1type integers.

Proof

Let p be a prime factor of $2^{37}-1$, then

$$2^{37} \equiv 1 (mod \;\; p)$$

Thus $o_p(2)|37$, $o_p(2) = 1$ or 37.

If $o_p(2) = 1$, then $2 \equiv 1(mod \;\; p)$, a contradiction.

If $o_p(2) = 37$, since $o_p(2)|(p-1)$, we have $37|(p-1)$.

Also, since $2^{37}-1$ is odd, so p is odd too, we also have $2|(p-1)$.

Hence $74|(p-1)$, i.e. p is a 74k+1type integers. $\square$

By the above proposition, we list all 74k+1type integers:

$$75, 149, 223, \cdots$$

75 is not a prime, pass.

Use repeated squaring method, we find $2^{37}(mod \;\; 149) = 105 \neq 1$, so 149 is not a prime factor of $2^{37} - 1$.

Use repeated squaring method, we find $2^{37}(mod \;\; 223) = 1$, so 223 is a prime factor of $2^{37} - 1$!

Thus $2^{37} - 1$ is a composite number.

Hence there is no perfect number between 10^{20} and 10^{22}.

Another Story of Fermat Numbers

Recall:

Numbers of the form $2^{2^n}+1$ are called Fermat Numbers, denoted by $F_n = 2^{2^n}+1$. Let's write out the first few terms of $\{2^{2^n}+1\}_{n\geq 1}$:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

Clearly, these are all primes, so Fermat made a conjecture:

For all natural numbers n, F_n is a prime.

However, Euler gave a contradiction:

$$F_5 = 641 \times 6700417$$

Let's see how to get this factorization.

Prop. All prime factors of $2^{2^5}+1$ are 64k+1 type integers.

Proof Let p be a prime factor of $2^{2^5}+1$, then

$$2^{32} \equiv -1(mod \ \ p)$$

Squaring both sides, we get $2^{64} \equiv 1(modp)$. Thus $o_p(2)|64$.

We claim $o_p(2)$ doesn't divides 32, otherwise, $2^{32} \equiv 1(mod \ \ p)$, thus $p|2$, we get $p=2$, but $2^{2^5}+1$ is odd, a contradiction.

So $o_p(2)=64$.

Also, $o_p(2)|(p-1)$, thus $64|(p-1)$, Thus p is a $64k+1$ type integer. It follows that all primes factors of $2^{2^5}+1$ are $64k+1$ type integers. $\square$

By the above proposition, we list all 64k+1 type integers:

$$65, 129, 193, 257, 321, 385, 449, 513, 577, 641 \cdots$$

65 is not a prime, pass.

129 is not a prime, pass.

Use repeated squaring method, we find $2^{32}(mod \;\; 193) = 108 \neq 192$, so 193 is not a prime factor of $2^{32} + 1$.

Use repeated squaring method, we find $2^{32}(mod \;\; 257) = 1 \neq 256$, so 257 is not a prime factor of $2^{32} + 1$.

321 is not a prime, pass.

385 is not a prime, pass.

Use repeated squaring method, we find $2^{32}(mod \;\; 449) = 324 \neq 448$, so

449 is not a prime factor of $2^{32}+1$.

513 is not a prime, pass.

Use repeated squaring method, we find $2^{32}(mod\ \ 577) = 287 \neq 576$, so 577 is not a prime factor of $2^{32}+1$.

Use repeated squaring method, we find $2^{32}(mod\ \ 641) = 640$, so 641 is a prime factor of $2^{32}+1$!

Primitive Root.

Def: Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ and $g.c.d.(a, m) = 1$.

If $O_m(a) = \phi(m)$, then a is called a primitive root modulo m.

Note that, by the example in page 159, $\forall a \in \mathbb{Z}$, $g.c.d.(a, 1001) = 1$, $O_{1001}(a) \mid 60$, thus $O_{1001}(a) \neq \phi(1001) = 720$. Thus, only for a few positive integers m, there exists a primitive root modulo m. In fact, we have the following theorem:

Thm. There exists a primitive root modulo m if and only if $m = 2, 4, p^l$ or $2p^l$, where p is an odd prime.

(Proof: Omitted).

E.g. 1. $m = 8$

$\forall a \in \mathbb{Z}$, $g.c.d.(a, 8) = 1$, then $a \equiv 1, 3, 5, 7 \pmod 8$

$O_8(1) = 1$, $O_8(3) = 2$, $O_8(5) = 2$, $O_8(7) = 2$.

Thus, $O_8(a) = 1$ or 2.

We verified the Thm.

Eg 2. $m = 11$,

$2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^5 \equiv -1 \pmod{11}$

$\therefore O_{11}(2) = 10$. 2 is a primitive root modulo 11.

Prop. Assume there exists a primitive root modulo m, i.e. $m = 2, 4, p^l$ or $2p^l$, where p is an odd prime. $g \in \mathbb{Z}$ and $g.c.d.(g, m) = 1$. Then:

g is a primitive root modulo $m \iff g^{\frac{\phi(m)}{p_i}} \not\equiv 1 \pmod{m}$

where p_i runs through all prime factors of $\phi(m)$.

Proof:

"$\Rightarrow$" By definition.

"$\Leftarrow$" If g is not a primitive root modulo m, then $O_m(g) \neq \phi(m)$.

However, by the corollary in page 156, $O_m(g) \mid \phi(m)$.

Thus $\phi(m)/O_m(g) \neq 1$.

So $\phi(m)/O_m(g)$ has a prime factor q, obviously, q is also a prime factor of $\phi(m)$.

Since $q \mid \frac{\phi(m)}{O_m(g)}$, thus $O_m(g) \mid \frac{\phi(m)}{q}$.

So $g^{\frac{\phi(m)}{q}} \equiv 1 \pmod{m}$, where q is a prime factor of $\phi(m)$, a contradiction.

Thus g is a primitive root modulo m.

$\square$

Eg 1. Check if 2 is a primitive root modulo 29.

Sol: 29 is an odd prime, thus there exists a primitive root modulo 29.

$\phi(29) = 29-1 = 28 = 2^2 \times 7$.

We have to check $2^{\frac{\phi(m)}{q}} \not\equiv 1 \pmod{29}$? where $q = 2$ or 7.

$2^{\frac{\phi(m)}{2}} = 2^{14} = (2^7)^2 = 128^2 \equiv 12^2 = 144 \equiv 28 \pmod{29}$

$2^{\frac{\phi(m)}{7}} = 2^4 \equiv 16 \pmod{29}$

So, Both $2^{\frac{\phi(m)}{2}}$ and $2^{\frac{\phi(m)}{7}}$ are not congruent to 1 modulo 29. Thus 2 is a primitive root modulo 29.

Eg 2. Check if 3 is a primitive root modulo 121.

Sol: $121 = 11^2$ is a square of an odd prime, so there exists a primitive root modulo 121.

$\phi(121) = 11^2 - 11 = 110 = 2 \times 5 \times 11$.

We have to check $3^{\frac{\phi(121)}{q}} \not\equiv 1 \pmod{121}$? where $q = 2, 5, 11$.

$3^{\frac{\phi(121)}{2}} = 3^{55} = (3^5)^{11} = 243^{11} \equiv 1^{11} \equiv 1 \pmod{121}$

Thus 3 is not a primitive root modulo 121.

Remark

In case l is large, then it's hard to compute $a^{\frac{\phi(p^l)}{q}}(mod p^l)$. The following theorem is useful.

Theorem Let p be an odd prime, g is an integer coprime to p. The following statements are equivalent:

(1)g is a primitive root modulo p^2.

(2)For all $l \geq 2$, g is a primitive root modulo p^l.

Example Check if 2 is a primitive root modulo 5^{2002}.

Solution

5^{2002} is a power of odd prime, so there exists a primitive root modulo 5^{2002}.

By the above theorem, it suffices to check if 2 is a primitive root modulo 5^2.

Since $\phi(5^2) = 5^2 - 5 = 20 = 2^2 \times 5$. We have to check $2^{\frac{20}{q}}(mod\ \ 5^2) \neq 1$? where $q = 2$ or 5.

$$2^{\frac{20}{2}} \equiv 24(mod\ \ 5^2)$$

$$2^{\frac{20}{5}} \equiv 16(mod\ \ 5^2)$$

Thus 2 is a primitive root modulo 5^2, hence 2 is a primitive root modulo

5^{2002} too.

谢谢！