Section 10 — Primitive Roots

We learned that if $(a,m)=1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

However, it's possible that $a^k \equiv 1$ with $k < \varphi(m)$.

For example, working mod 7, we know that $\varphi(7)=6$, so if $(a,7)=1$, then $a^6 \equiv 1 \pmod{7}$.
But often an exponent smaller than 6 will do.

$\boxed{\text{mod } 7}$

a^1	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

$1^1 \equiv 1$

$2^3 \equiv 1$

$3^6 \equiv 1$

$4^3 \equiv 1$

$5^6 \equiv 1$

$6^2 \equiv 1$

<u>Def</u> If $m \in \mathbb{Z}^+$ and $(a,m)=1$, then the $\boxed{\text{smallest}}$ $k \in \mathbb{Z}^+$ such that $a^k \equiv 1 \pmod{m}$ is called the <u>order of a modulo m</u>, denoted $\text{ord}_m(a)$.

<u>Ex</u> Find the orders of the L.R. mod 7.

By the above table...

$\text{ord}_7(1)=1$

$\text{ord}_7(2)=3$

$\text{ord}_7(3)=6$

$\text{ord}_7(4)=3$

$\text{ord}_7(5)=6$

$\text{ord}_7(6)=2$

$\text{ord}_7(0)$ DNE

* Notice that $\text{ord}_m(a) \le \varphi(m)$ since $a^{\varphi(m)} \equiv 1$

* But more seems true — in the last example, the order of each (nonzero) element divided $6 = \varphi(7)$.

Ex Find all $n \in \mathbb{Z}^+$ s.t. $4^n \equiv 1 \pmod 9$. What is $\text{ord}_9(4)$?

a	a^2	a^3	a^4	a^5	a^6	a^7	
4	7	1	4	7	1	4	...

$\underbrace{n = 3, 6, 9, 12, \ldots}_{\text{mult. of order}}$ $\quad \text{ord}_9(4) = 3$

Theorem 1 Let $m \in \mathbb{Z}^+$. If $(a,m)=1$ and $t = \text{ord}_m(a)$, then $a^n \equiv 1 \pmod m$ if and only if t divides n.

Because we know $a^{\varphi(m)} \equiv 1$, we automatically get...

Theorem 2 Let $m \in \mathbb{Z}^+$. If $(a,m)=1$, then $\text{ord}_m(a)$ divides $\varphi(m)$.

pf of Thm 1

($\Longleftarrow$) Assume $t \mid n$, so $n = q \cdot t$ for $q \in \mathbb{Z}^+$. Since $t = \text{ord}_m(a)$, $a^t \equiv 1 \pmod m$, so $a^n = a^{q \cdot t} = (\overset{1}{\cancel{a^t}})^q \equiv 1^q \equiv 1 \pmod m$.

($\Longrightarrow$) Assume $a^n \equiv 1 \pmod m$. Use the division algorithm to write $n = qt + r$ with $0 \le r < t$. Now, we want to show $r = 0$.

$$1 \equiv a^n = a^{qt+r} = a^{qt} \cdot a^r = (\overset{1}{\cancel{a^t}})^q \cdot a^r \equiv a^r \pmod m$$

Thus $a^r \equiv 1 \pmod m$. Since $t = \text{ord}_m(a)$, t is the smallest, positive integer s.t. $a^t \equiv 1 \pmod m$. Since $r < t$ and $a^r \equiv 1$, r must not be positive, so as $r \ge 0$, $r = 0$. $\square$

Ex Find an a of the given order, if possible.

(a) $ord_9(a)=2$ $\quad$ $a\equiv -1$

(b) $ord_9(a)=4$ $\quad$ not possible — $4 \nmid \varphi(9)=6$

(c) $ord_9(a)=6$ $\quad$ trial + error $\quad a=2,-2$

Ex If $ord_m(a)=12$, what is $ord_m(a^3)$?

$a^{12}\equiv 1 \Rightarrow (a^3)^4\equiv 1 \Rightarrow ord_m(a^3)=\boxed{4}$.

Ex If $a^4\equiv 1 \pmod m$, must it be true that $ord_m(a)=4$?

No: for example $(-1)^4\equiv 1 \pmod m$ but $ord_m(-1)=2$.

Let's revisit Theorem 1: if $(a,m)=1$ and $t=ord_m(a)$,

then $a^n\equiv 1 \pmod m \iff \cancel{t\mid n} \rightarrow n\equiv 0 \pmod t$

Thus,

$$a^r\equiv 1\equiv a^s \pmod m \iff r\equiv 0\equiv s \pmod t$$

what if $a^r\equiv a^s \pmod m$, do we still get $r\equiv s \pmod t$?

Recall the powers of 4 mod 9:

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
4	7	1	4	7	1	4	7	1	4	7

mod 9

Note: $ord_9(4)=3$

Thus $a^r\equiv a^s \pmod 9 \iff s-r$ is a multiple of 3

$a^5\equiv a^{11}$ $\quad$ $11-5$

$$\iff s\equiv r \pmod 3$$

optional

Theorem 4 If $(a,m)=1$ and $t=\text{ord}_m(a)$, then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

pf

Since $(a,m)=1$, a^{-1} exists — $a \cdot a^{-1} \equiv 1 \pmod{m}$.

We may assume that $s \geq r$.

$$a^r \equiv a^s \bmod m \iff \underbrace{a \cdot a \cdots a}_{r \text{ times}} \equiv \underbrace{a \cdot a \cdots a}_{s \text{ times}}$$

$$\iff \underbrace{a \cdot a \cdots a}_{r \text{ times}} \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{r \text{ times}} \equiv \underbrace{a \cdot a \cdots a}_{s \text{ times}} \underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{r \text{ times}}$$

$$\iff 1 \equiv \underbrace{a \cdot a \cdots a}_{(s-r) \text{ times}}$$

$$\iff 1 \equiv a^{s-r}$$

$$\iff t \mid s-r$$

Theorem 1

$$\iff r \equiv s \pmod{t} \quad \square$$

Ex Suppose that $(a,45)=1$. What are the possible values for $\text{ord}_{45}(a)$?

Let $k=\text{ord}_{45}(a)$. Then $k \mid \varphi(45)$. Now $\varphi(45) = \varphi(9 \cdot 5) = \varphi(9)\varphi(5) = 3 \cdot 2 \cdot 4 = 24$. Thus k must be a divisor of 24: 1, 2, 3, 4, 6, 8, 12, 24.

Question: is there an a with $\text{ord}_{45}(a) = 24$??

Def If a is a least residue $\pmod{m}$ for which $\text{ord}_m(a) = \varphi(m)$, we say that a is a <u>primitive root of m</u>.

* primitive roots have the largest possible order.

Ex 2 is a primitive root of 9

$\varphi(9) = 6$

a	a^2	a^3	a^4	a^5	a^6
2	4	8	7	5	1

all 6 numb. b/w 1 & 9 rel. prime to 9

Ex 2 is not a primitive root of 7, but 3 is

$\varphi(7) = 6$

a	a^2	a^3	a^4	a^5	a^6
2	4	1			
3	2	6	4	5	1

all 6 numbers b/w 1 & 7 rel. prime to 7

Notice that...

why we care ... application coming in next section

Theorem 5 If g is a primitive root of m, then the least residues of

$$g, g^2, g^3, \ldots, g^{\varphi(m)}$$

see above

are exactly the numbers b/w 1 and m that are relatively prime to m.

pf ... use Theorem 4 — see book.

Big Question: do primitive roots always exist?

Ex Show that there are no primitive roots of 8.

$\varphi(8) = 4$

a	a^2	a^3	a^4
1			
3	1		
5	1		
7	1		

$(a, 8) = 1 \Rightarrow a^2 \equiv 1 \bmod 8$

The situation is much better for primes...

Theorem 6 Every prime p has $\varphi(p-1)$ primitive roots.

existence but not how to find

... but we saw that non-primes may have primitive roots, e.g. 9, but not 8, ... maybe just prime powers?

Ex Show 18 has a primitive root.

- $\varphi(18) = (2-1)\cdot 3(3-1) = 6$
- need to find an element a with $\mathrm{ord}_{18}(a) = 6$
- only chance is with $(a,18)=1$

  use trial + error:

a	a^2	a^3	a^4	a^5	a^6
1					
5	7	-1	-5	-7	1
7					
11					
13					
$-1 \equiv 17$	1				

try next?

yes: $\boxed{\mathrm{ord}_{18}(5) = 6}$

nope: $\mathrm{ord}_{18}(17) = 2$

try first?

Theorem Let $m \in \mathbb{Z}^+$. Then m has a primitive root if and only if $m = 1, 2, 4, p^e$, or $2\cdot p^e$ for p an odd prime.

existence but not how to find

Ingredients for the proof of Thm 6

* Remember, in Thm 6, the modulus is prime.

Lemma 2 If $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_n \not\equiv 0 \pmod p$, then $f(x)$ has at most n roots modulo p.

pf idea

Either
- $f(x)$ is linear: $f(x) = a_1 x + a$. Then $(a_1, p) = 1$
  so $a_1 x + a \equiv 0 \pmod{p}$ has 1 sol.
- $\deg f(x) \geq 2$: if $f(x)$ has a root r, then

$$f(x) \equiv (x-r) \cdot g(x) \pmod{p}$$

and

$$f(x) \equiv 0 \pmod{p} \Longrightarrow x = r \text{ or } g(x) \equiv 0 \pmod{p}$$

b/c p is prime!

now this has fewer roots than $f(x)$ — use induction

Ex Show that $x^2 + x \equiv 0 \pmod{6}$ has 4 solutions.

$x \equiv 0, -1, 2, 3$

Lemma 3 If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

pf
- By Fermat's Thm, $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions (namely $1, 2, \ldots, p-1$)
- $x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + x + 1)$

general form of $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

$$= \underbrace{(x^d - 1)}_{\text{at most } d \text{ roots by Lemma 2}} \cdot \underbrace{h(x)}_{\text{at most } p-1-d \text{ roots}}$$

- LHS has $p-1$ roots mod p

$\Longrightarrow x^d - 1$ has d roots (and $h(x)$ has $p-1-d$ roots)

$\square$

pf idea for Thm 6

WTS that there are $\varphi(p-1)$ primitive roots of p.

Consider the set $A = \{1, 2, \dots, p-1\}$.

Every element of A has an order, and the order must be a divisor of $p-1$. Let

$$\psi(t) = \# \text{ of elements of } A \text{ that have order } t.$$

Note that
$$\boxed{\sum_{t \mid p-1} \psi(t) = p-1.}$$

Also we learned in the last chapter that

$$\boxed{\sum_{t \mid p-1} \varphi(t) = p-1}$$

Thus
$$\boxed{\boxed{\sum_{t \mid p-1} \psi(t) = \sum_{t \mid p-1} \varphi(t).}} \quad \star$$

The goal is to show that $\psi(t) = \varphi(t)$, because then $\psi(p-1) = \varphi(p-1)$.

Since $\star$ is true, it suffices to show that $\underline{\psi(t) \le \varphi(t)}$ for all $t \mid p-1$.

want to prove

case 1: $\psi(t) = 0$

Then clearly $\psi(t) \le \varphi(t)$ ✓

case 2: $\varphi(t) \neq 0$.

we aim to show $\psi(t) = \varphi(t)$, and all we know right now is $\psi(t) > 0$. Let a be an element of order t.

Now, every element of order t is a solution to

$$x^t \equiv 1 \pmod{p}$$

and by Lemma 3, there are exactly t solutions, of which a is one. Notice that

$$a^t \equiv 1 \Rightarrow (a^k)^t \equiv (a^t)^k \equiv 1$$

so

$$a, a^2, a^3, \ldots, a^t$$

are the t solutions to $x^t \equiv 1 \pmod{p}$. So, the elements of order t are on this list — which ones are they?

see book

Lemma 2: if a has order t, then a^k has order t iff $(k,t) = 1$.

Thus,

$$\psi(t) = \#\text{ elem. of order } t = \varphi(t)$$

$\square$