MULTIPLICATIVE ORDERS

Let $a \in \mathbb{Z}_m^*$ $(m \in \mathbb{N})$

$a, a^2, a^3, \ldots$ cannot all be distinct modulo m

$\exists\, i, j \in \mathbb{N}$, $i < j$, s.t. $a^j \equiv a^i \pmod m$

$a \in \mathbb{Z}_m^* \Rightarrow a^{-1}$ exists $\Rightarrow a^{j-i} \equiv 1 \pmod m$

$\exists$ positive integers e s.t. $a^e \equiv 1 \pmod m$

Consider the set $\mathcal{E}$ of all such exponents e.

$\mathcal{E} \subseteq \mathbb{Z}^+$ & hence has a least element.

(Defn) $a \in \mathbb{Z}_m^*$. The smallest $e \in \mathbb{N}$ s.t. $a^e \equiv 1 \pmod m$ is called the multiplicative order of a modulo m denoted $\operatorname{ord}_m a$.

Examples

→ $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

$4^2 \equiv 16 \equiv 7 \pmod 9$

$4^3 \equiv 7 \times 4 \equiv 28 \equiv 1 \pmod 9$

$\text{ord}_9 4 = 3$

→ $\text{ord}_m 1 = 1$

→ $\text{ord}_p -1 = 2$

Thm Let $a \in \mathbb{Z}_m^*$ & $e = \mathrm{ord}_m a$. Then $a^h \equiv 1 \pmod m$ iff $e \mid h$. In particular, $e \mid \phi(m)$.

Proof:

$\Leftarrow$ Suppose $e \mid h$. Then $h = ek$

$$a^h \equiv a^{ek} \equiv (a^e)^k \equiv 1^k \equiv 1 \pmod m$$

$\Rightarrow$ Suppose $a^h \equiv 1 \pmod m$

Let $h = qe + r \quad 0 \le r < e$

$$1 \equiv a^h \equiv (a^e)^q \cdot a^r \equiv 1^q a^r \equiv a^r \pmod m$$

But since $r < e$ & e is the <u>smallest</u> the integer s.t. $a^e \equiv 1 \pmod m$, we have

$$r = 0$$

$$\Rightarrow e \mid h.$$

By Euler's thm, $a^{\phi(m)} \equiv 1 \pmod m$ $\forall a \in \mathbb{Z}_m^*$ & hence $e \mid \phi(m)$.

(Defn) If $\operatorname{ord}_m a = \phi(m)$ for some $a \in \mathbb{Z}_m^*$, then a is called a primitive root mod m.

Example.

$\mathbb{Z}_{11} = \{0, 1, 2, \ldots, 10\}$

$3, 3^2, 3^3, 3^4, 3^5$ $\quad \operatorname{ord}_{11} 3 = 5$

$3, 9, 5, 4, 1$

$2, 2^2, \ldots$

$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$ $\quad \operatorname{ord}_{11} 2 = 10 = \phi(11)$

2 : primitive root modulo 11.

$\mathbb{Z}_{12}$ has no primitive roots.

Not all $m \in \mathbb{N}$ have primitive roots.

(Thm) Every prime p has a primitive root.

(Proof) $\mathbb{Z}_p$ is a field.

$x^{p-1} - 1$ has $(p-1)$ roots in $\mathbb{Z}_p$.
(follows from Fermat's little theorem)

Let d be a divisor of $(p-1)$. $(p-1) = kd$

$$(x^{p-1} - 1) = (x^d - 1)\underbrace{(1 + x^d + x^{2d} + \cdots + x^{(k-1)d})}_{f(x)}$$

$x^d - 1$ has at most d roots

degree of $f(x) = p-1-d$ $f(x)$ has $\leq p-1-d$ roots.

Since x^{p-1} has exactly $p-1$ roots,

$x^d - 1$ & $f(x)$ have exactly d & $p-1-d$ roots respectively.

$x^d - 1$ has exactly d roots

$\Rightarrow \exists$ exactly d elements of $\mathbb{Z}_p$ s.t. $x^d \equiv 1 \pmod{p}$

i.e., $\exists$ exactly d elements of $\mathbb{Z}_p$ with order dividing d.

Let $p-1 = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$. p_i's : pairwise distinct

$e_i \in \mathbb{N}$

$p_1^{e_1} \mid (p-1)$

$\exists$ exactly $p_1^{e_1}$ elements of order dividing $p_1^{e_1}$

$p_1^{e_1-1} \mid (p-1)$

$\exists$ exactly $p_1^{e_1-1}$ elements with order dividing $p_1^{e_1-1}$

elements with order exactly $p_1^{e_1}$

$= p_1^{e_1} - p_1^{e_1-1} > 0$ since $e_1 \in \mathbb{N}$

$\Rightarrow \exists\ a_1$ s.t. $\mathrm{ord}_p a_1 = p_1^{e_1}$.

Let $a_i \in \mathbb{Z}_p$ s.t. $\operatorname{ord}_p a_i = p_i^{e_i}$ for $1 \le i \le r$

$$a = \prod_{i=1}^{r} a_i$$

Lemma: Let $a, b \in \mathbb{Z}_m$ & $\operatorname{ord}_m a = k$ $\operatorname{ord}_m b = l$.
If $\gcd(k, l) = 1$, then $\operatorname{ord}_m ab = kl$.

From the lemma, we have

$$\operatorname{ord}_p a = \prod_{i=1}^{r} \operatorname{ord}_p a_i$$

$\left[p_1^{e_1}, p_2^{e_2}, \dots, p_r^{e_r} \text{ are co-prime} \right]$

$$= \prod_{i=1}^{r} p_i^{e_i}$$

$$= p - 1 \quad (= \phi(p))$$

$\therefore$ a is a primitive root modulo p.

Proof of Lemma

$\text{ord}_m a = k \qquad \text{ord}_m b = l$

Let $\text{ord}_m(ab) = h$

To show $h = kl$.

$$(ab)^{kl} \equiv (a^k)^l \cdot (b^l)^k \equiv 1^l \cdot 1^k \equiv 1 \pmod m$$

$$h \mid kl \quad \text{---} (1)$$

$$(ab)^h \equiv 1 \pmod m$$

$$(ab)^{hk} \equiv 1 \pmod m$$

$$(a^k)^h b^{kh} \equiv 1 \pmod m$$

$$b^{kh} \equiv 1 \pmod m$$

$$\Rightarrow l \mid kh \Rightarrow l \mid h \quad (\because \gcd(k,l) = 1)$$

Similarly we can show that $k \mid h$.

We have $l \mid h$, $k \mid h$

& $\gcd(l,k) = 1$

$\therefore lk \mid h$ --- (2)

(1) & (2) $\Rightarrow h = kl$

(Thm) The only positive integers > 1 that have primitive roots are $2, 4, p^e, 2p^e$ where $p \in \mathbb{P} \setminus \{2\}$ & $e \in \mathbb{N}$

COMPUTING ORDERS ($\mathbb{Z}$ elements in $\mathbb{Z}_m$)

When complete prime factorisation of m is not known: no efficient algorithm exists

Let $\phi(m) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $\quad p_i$'s: pairwise distinct, $e_i \in \mathbb{N}$

$a \in \mathbb{Z}_m$

$\operatorname{ord}_m a \mid \phi(m)$

$\operatorname{ord}_m a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ $\quad 0 \le k_i \le e_i$

Sufficient to compute k_i's.

Algorithm Order (a, m)

Running time $O(\log^4 m)$

i/p : $m \in \mathbb{N}$ $a \in \mathbb{Z}_m^*$ o/p $\operatorname{ord}_m a$

$\phi(m) = p_1^{e_1} \cdots p_r^{e_r}$

Initialise $h \leftarrow 1$

for $i \leftarrow 1$ to r, do

→ compute $b \leftarrow a^{\phi(m)/p_i^{e_i}} \pmod m$ $\quad O(\log^4 m)$

while $b \not\equiv 1 \pmod m$ do

$b \leftarrow b^{p_i} \pmod m$ $\quad O(\log m)(\log^3 m) = O(\log^4 m)$

$h \leftarrow h \cdot p_i$

end while

end for

return h

Total cost $= O(\log^4 m)$

$a^{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}} \equiv 1 \pmod m$

Running Times of Algorithms for Integer Arithmetic

Operation	Running Time
$a+b,\ a-b,\ a \overset{?}{=} b$	$O(\max(\log a, \log b))$
$x \leftarrow a$	$O(\log a)$
ab	$O(\log a \log b)$ ($\exists$ improvements)
a quot b, a rem b	$O(\log^2 a)$
(Extended) GCD (a, b)	$O(\log^2 a)$
$a+b \pmod m$, $a-b \pmod m$	$O(\log m)$
$ab \pmod m$, $a^{-1} \pmod m$	$O(\log^2 m)$
$a^e \pmod m$	$O(\log^3 m)$
CRT	$O(t \log^2 M)$
$\left(\frac{a}{p}\right)$, $a \in \mathbb{Z}_p$	$O(\log^3 p)$
$\operatorname{ord}_m a$	$O(\log^4 m)$