Module III

Finite Cyclic Groups and Conditions on n for Z_n^* to be Cyclic

In Module II we determined that Z_n^* is a finite group of order $\varphi(n)$ and that if $a \in Z_n^*$ then ord (a) $\mid \varphi(n)$. Of course, if ord (a) = $\varphi(n)$ then

$$Z_n^* = \left\{1, a, a^2, \ldots, a^{\varphi(n)-1}\right\}$$

and we say that Z_n^* is cyclic. Our purpose is to determine those values of n for which Z_n^* is cyclic. In preparation for that discussion we begin with a general definition of a cyclic group and a result regarding the structure of an arbitary finite cyclic group.

Definition 1. Let G be a finite group. If $\exists\, a \in G$ such that $G = (a) \underline{\underline{\Delta}} \left\{a^k \mid k \geq 0\right\}$ then G is said to be cyclic and a is called a generator of G.

Remark 1. Of course, if G = (a) then $\mathrm{ord}(a) = |G|$

Proposition 1. Let G be a finite group.

(i) if $a \in G$ and ord a = t then $\mathrm{ord}\,(a^k) = t / \gcd(k, t)$

(ii) if G is cyclic and $d \mid \mathrm{ord}\,(G)$ then G has $\varphi(d)$ elements of order d.

(iii) if G is cyclic and $H \subseteq_g G$ then H is cyclic. Moreover, if $d \mid \mathrm{ord}(G)$ then $\exists$ exactly one subgroup of G having order = d.

Proof (i) Observe that

$$(a^k)^{t/\gcd(k,t)} = a^{\frac{kt}{\gcd(k,t)}} = a^{\ell\mathrm{cm}(k,t)} = e$$

because $t \mid \ell\mathrm{cm}(k, t)$. Thus $\mathrm{ord}(a^k) \leq t / \gcd(k, t)$.

Next realize $\quad e = (a^k)^{\mathrm{ord}(a^k)} = a^{k\,\mathrm{ord}(a^k)}$

But then $\quad t \mid k\,\mathrm{ord}\,(a^k)$

and so $k\,\mathrm{ord}(a^k)$ is a common multiple of k and t;

whence $\quad \ell\mathrm{cm}(k, t) \mid k\,\mathrm{ord}(a^k)$.

Thus $\quad \mathrm{ord}(a^k) \geq \dfrac{\ell\mathrm{cm}(k,t)}{k} = \dfrac{t}{\gcd(k, t)}$.

(ii) Suppose α is a generator. We want $\text{ord}\,(\alpha^t) = d$

But $\text{ord}\,(\alpha^t) = \text{ord}\, G \;/\; \gcd(t, \text{ord}\, G)$ i.e. $\gcd(t, \text{ord}\, G) = \dfrac{\text{ord}\,(G)}{d}$.

Now this holds if and only if $\gcd\left(t \middle/ \dfrac{\text{ord}\,(G)}{d},\; d\right) = 1$.

But $t < \text{ord}\, G \Rightarrow t \big/ \frac{\text{ord}(G)}{d} < d$.

Conversely, suppose $1 \le a < d$ and set $t = a\left(\dfrac{\text{ord}(G)}{d}\right)$

if $\gcd(a, d) = 1$ then $\gcd\left(t \big/ \frac{\text{ord}\,(G)}{d}, d\right) = 1$

Thus $\exists$ 1-1 correspondence between the t's such that $t \le \text{ord}(G)$ and $\text{ord}(\alpha^t) = d$ and the $a\text{'s} \in [d]$ such that $\gcd(a, d) = 1$ thereby implying that $\exists\ \varphi\,(d)$ such t's.

(iii) Suppose α is a generator of G, i.e. $\text{ord}(\alpha) = |G|$. If $d \| G|$ then

$$\text{ord}\,(\alpha^{|G|/d}) = \frac{|G|}{\gcd\,(|G|, |G|_{/d})}$$

Of course with $t = |G|/d$

$$H_t \triangleq (\alpha^t)$$

is cyclic and has $|H_t| = d$ so for each divisior of ord G $\exists$ a cyclic subgroup of G having order d.

By ii) H_t contains $\varphi(d)$ elements of order d. But $d \| G|$ also implies G contains EXACTLY $\varphi(d)$ elements of order d. Thus H_t consists of all of the elements of G having order d. Now suppose $H \subseteq_g G$ such that $|H| = d$. It remains to show that $H = H_t$. Consider $a \in H$ so that $\text{ord}\,(a) | d$. But then $\text{ord}(a) \| G|$ implies that G contains exactly $\varphi(\text{ord}\,(a))$ elements of ord (a) and $\text{ord}\,(a) |\; d = |H_t|$ implies that H_t contains $\varphi(\text{ord}\, a)$ elements of ord(a). Hence H_t contains all of the elements of G having ord (a); in particular $a \in H_t$. Thus $H \subseteq H_t$. But $|H| = |H_t|$ forces $H = H_t$. Hence every subgroup of G is cyclic and for each $d |\; |G|$, $H_t = (\alpha^t)$ is the unique subgroup of G having order d.

Example1. Consider Z_9. Then $\varphi(9) = 9\left(1-\frac{1}{3}\right) = 6$

and

$$Z_9^* = \{a \in Z_9 \mid \gcd(a, 9) = 1\}$$
$$= \{1, 2, 4, 5, 7, 8\}.$$

Now Z_9^* is cyclic since $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 7 \pmod 9), 2^5 \equiv 5 \pmod 9)$ and it is easy to see that 5 is the other generator. But Z_9^* has two subgroups, one of order 2 and one of order 3. Since $\varphi(2) = 1$ there is one element of order 2 namely 8 so the unique subgroup of order 2 is $\{1,8\}$. Hence $\{1, 4, 7\}$ is the sole subgroup of order 3. In summary we have

	Subgroup	Order	Generators
	G	6	$\{2, 5\}$
	$\{1, 8\}$	2	$\{8\}$
	$\{1, 4, 7\}$	3	$\{4, 7\}$
AND	$\{1\}$	1	$\{1\}$

Corollary 1.1 a) $\alpha \in Z_n^*$ is a generator if and only if $\forall$ primes p

$$\left(p \mid \varphi(n)\right) \Rightarrow \alpha^{\varphi(n)/p} \not\equiv 1 \pmod n)$$

b) if α is a generator of Z_n^* then $b = \alpha^i \bmod n$ is also a generator if and only iff $\gcd(i, \varphi(n)) = 1$

Moreover, if Z_n^* is cyclic then the number of generators is $\varphi(\varphi(n))$

Proof i) if α is a generator then $\operatorname{ord}(\alpha) = \varphi(n) > \varphi(n)/p$

so $\alpha^{\varphi(n)/p} \not\equiv 1 \pmod n$.

If α is not a generator then $\operatorname{ord}(\alpha) = t < \varphi(n)$ and $t \mid \varphi(n)$. Let $p \left| \frac{\varphi(n)}{t} \right.$

i.e $\varphi(n) = \beta\, p\, t$ for some $\beta \in Z$. Thus $\alpha^{\varphi(n)/p} = \left(\alpha^t\right)^\beta \equiv 1 \pmod n$

ii) We know $\operatorname{ord} b = \dfrac{\operatorname{ord} \alpha}{\gcd(\operatorname{ord}\alpha, i)} = \operatorname{ord} \alpha = \varphi(n)$ if and only if

$\gcd(i, \varphi(n)) = 1$. Also the number of generators is just $\varphi\left(\operatorname{ord} Z_n^*\right) = \varphi\left(\varphi(n)\right)$.

Exercise 1 (Submit this exercise). Given that Z_{19}^* and Z_{81}^* are cyclic find all generators and all subgroups of each of them and draw hierarchical diagrams for each.

Two more preliminary results are required prior to proving that Z_n^* is cyclic whenever n is prime. As it happens the arguments required for this development are valid for the general case when F is a finite field. Accordingly we state and prove them in the general form and draw the immediate consequences for the finite field Z_p^* (see Corollary 2.2). First we require the notion of a polynomial.

Definition 2. Suppose F is a field. An expression of the form

$$\sum_{i=0}^{n} a_i \, x^i$$

where $n \geq 0$, $a_i \in F$ for each i $a_n \neq 0$ and x is an indeterminant (place holder) is called a polynomial of degree n with coefficients from F. The degenerate case where each $a_i = 0$ is referred to as the "zero" polynomial, is denoted by 0 and is assigned the degree $-\infty$.

Remark 2 Of course we allow the subsitution of any $a \in F$ for x, thereby producing a field element.

Lemma 1 Suppose f is a polynomial with coefficients from a field F and with degree $n \geq 1$. Then $f(a) = 0$ in F for $a \in F$ if and only if $\exists$ a polynomial $q(x)$ with coefficients from F having degree n-1 such that $f(x) = (x - a)\ q(x)$

Proof $(\Leftarrow)$: trivial

$(\Rightarrow)$: induction on n –

if $n = 1$, i.e. $f(x) = cx + b$ where $c \neq 0$. Then $f(a) = 0$ forces $c\,a + b = 0$ so $b = -ca$. Hence $f(x) = c\,x + b = c\,(x-a)$ and $q(x) = c$ does the job. Suppose the result is true for deg $f \leq n-1$ and consider deg $f = n$ with $f(a) = 0$.

Let $g(x) = f(x) - a_n\, x^{n-1}(x-a)$

where $f(x) = a_n\, x^n + \cdots + a_1\, x + a_0$

Then deg $g \leq n-1$. Also $g(a) = 0$

so the induction hypothesis yields $g(x) = (x-a)\,\hat{q}(x)$

where deg $\hat{q} \leq n-2$. Thus $(x-a)\,\hat{q}(x) = f(x) - a_n x^{n-1}(x-a)$

or, equivalently, $f(x) = (a_n x^{n-1} + \hat{q}(x))\,(x-a)$ with deg $(a_n\, x^{n-1} + \hat{q}(x)) = n-1$.

Lemma 2 If f is a polynomial with coefficients from F and with degree $n \geq 1$ then $f(x)$ has at most n distinct roots in F.

Proof If f has no roots then we are done. Otherwise let $f(a) = 0$ for $a \in F$. Then by Lemma 1, $f(x) = (x-a)\, q(x)$

where q has coefficients from F and degree $= n - 1$.

Suppose $f(b) = 0$ and $b \neq a$. Then $0 = f(b) = (b-a)\, q(b)$

But $b-a \in F$, and $b - a \neq 0$ so $q(b) = 0$ as $F^* = F - \{0\}$ is a group. Hence all other roots, if they exist, of $f(x)$ must be roots of $q(x)$. By the induction hypothesis q has at most $n-1$ distinct roots.

Proposition 2. If F is a finite field then $F^* = F - \{0\}$ is cyclic

Proof Let $t = \ell cm\{\text{ord } a \mid a \in F^*\}$. Of course $t \mid |F^*|$. Write

$$t = p_1^{c_1}\, p_2^{c_2} \cdots p_k^{c_k} \cdot \text{ where } p_1, p_2, \cdots, p_k \text{ are distinct primes.}$$

Consider $p_i^{c_i}$; $\exists\, a_i$, such that ord $a_i = p_i^{c_i} \beta$ where $\gcd(p_i^{c_i}, \beta) = 1$. Thus $\partial_i = a_i^{\beta}$ has order $p_i^{c_i}$. Since the $p_i^{c_i}$'s are pairwise relatively prime.

$$\text{ord}\left(\partial_1 \partial_2 \cdots \partial_k\right) = p_1^{c_1}\, p_2^{c_2} \cdots p_k^{c_k} = t$$

But $\text{ord}\, a \mid t\ \forall a \in F^* \Rightarrow$ every $a \in F^*$ satisfies $x^t - 1 = 0$.

Thus $|F^*| \leq t$ by Lemma 2 and $t = |F^*| \cdot$ Therefore $\partial_1 \partial_2 \cdots \partial_k$ is a generator of F^*, i.e. F^* is cyclic.

Corollary 2.1 Z_p^* is cyclic for all primes $p \geq 2$.

Our next result establishes the fact that Z_n^* is cyclic whenever $n = p^k$ where $p \geq 3$ and $k \geq 1$.

<u>Proposition 3</u>. $Z^*_{p^k}$ is cyclic $\forall$p prime $\geq$ 3 and $\forall k \geq 1$.

<u>Proof</u> Let g be a generator of Z^*_p so that $\exists$ T$\in$ Z such that

$$g^{p-1} = 1 + pT$$

Let $t \in$ Z and consider

$$\left(g + t\,p\right)^{p-1} = g^{p-1} + \sum_{i=1}^{p-1}\binom{p-1}{i}\left(t\,p\right)^{i}\; g^{p-1-i}$$

$$= 1 + p\,T + (p\text{-}1)\,t\,g^{p-2}p + \sum_{i=2}^{p-1}\binom{p-1}{i}\left(t\,p\right)^{i}\; g^{p-1-i}$$

$$= 1 + p\left[T + (p\text{-}1)\,t\,g^{p-2} + p\sum_{i=2}^{p-1}\binom{p-1}{i}\; t^{i}\; p^{i-2}\; g^{p-1-i}\right]$$

Set $u = T + (p\text{-}1)\; t\,g^{p-2} + p\;\sum_{i=2}^{p-1}\binom{p-1}{i}t^{i}\; p^{i-2}\; g^{p-1-i}$

Observe that $p\chi\; g^{p-2}$ and $p\;\chi\;p\text{-}1$ so $p\;\chi(p\text{-}1)\; g^{p-2}$

Thus

- if $p|T$ and we set $t = 1$ then $p\;\chi\;u$
- if $p\;\chi\;T$ and we set $t = 0$ then $p\;\chi\;u$

Hence $\exists$ $t_0 \in$ Z such that $\left(g + t_0 p\right)^{p-1} = 1 + p\,u_0$ where $p\;\chi\;u_0$.

Next consider

$$\left(g + t_0\; p\right)^{p(p-1)} = \left(1 + p\,u_0\right)^{p} = 1 + \sum_{i=1}^{p}\binom{p}{i}\; p^{i}\; u_0^{i}$$

$$= 1 + p^2\; u_0 + \sum_{i=2}^{p}\binom{p}{i}p^{i}\; u_o^{i}$$

Since $p \geq 3$, $\sum_{i=2}^{p}\binom{p}{i}\; p^{i}\; u_0^{i}$ is divisible by p^3

and so

$$\left(g + t_0\; p\right)^{p(p-1)} = 1 + p^2\; u_1 \text{ such that } p\;\chi\;u_1$$

By the same manipulation we obtain, by induction

$$\left(g + t_0\ p\right)^{p^{\alpha}(p-1)} = 1 + p^{\alpha+1}u_{\alpha} \text{ such that } p \not| u_{\alpha}.$$

Let

$$a_k \equiv g + t_0\ p \pmod{p^k}$$

and let $\delta_k = \text{ord}\,(a_k)$. Thus $a_k^{\delta_k} \equiv 1 \mod (p^k)$

and so, since

$$a_k^{p^{k-1}(p-1)} \equiv 1 \mod (p^k),$$

we have

$$\delta_k \mid \varphi\left(p^k\right) = p^{k-1}(p-1).$$

But

$$a_k^{\delta_k} \equiv 1 \pmod p$$

as well so $p-1 \mid \delta_k$ and therefore

$$\delta_k = p^{\beta}\ (p-1)$$

for some $0 \le \beta \le k-1$. However if $\beta \le k-2$ then

$$\left(a_k\right)^{p^{\beta}(p-1)} \equiv (g + t_0 p)^{p^{\beta}(p-1)} = 1 + p^{\beta+1}\ u_{\beta}, \quad p \not| u_{\beta}$$

$$\not\equiv 1 \pmod{p^k}$$

Consequently $\delta_k = p^{k-1}(p-1) = \varphi\left(p_k\right)$ and Z_{p^k} is cyclic.

One more positive result is possible:

<u>Proposition 4</u>. $Z^*_{2p^k}$ is cyclic $\forall$ primes $p \ge 3$ and all $k \ge 1$.

If fact, if g is a generator of $Z^*_{p^k}$ and g is odd then g is also a generator of $Z^*_{2p^k}$. If g is even then $g + p^k$ is a generator of $Z^*_{2p^k}$.

<u>Proof</u> First observe that $\varphi(p^k) = \varphi(2p^k) = p^{k-1}(p-1)\ \forall$ primes $p \geq 3$ and $k \geq 1$. Of course if x is odd

$$p^k \mid x^\alpha - 1 \iff 2\,p^k \mid x^\alpha - 1.$$

Thus

$$\text{ord}\,(x) \text{ in } Z^*_{p^k} = \text{ord}\,(x) \text{ in } Z^*_{2p^k}$$

Hence if g is odd

$$\text{ord}\,(g) \text{ in } Z^*_{2p^k} = p^{k-1}(p-1) = \varphi(2p^k)$$

Suppose g is even; then $g + p^k$ is odd (since $p \geq 3$) and $g + p^k \in Z_{2p^k}$. Furthermore, since $g + p^k \equiv g (\text{mod } p^k)$

$$\begin{aligned}(g + p^k)^\nu \equiv 1 \ (\text{mod } p^k) &\iff g^\nu \equiv 1 \ (\text{mod } p^k)\\ &\iff p^{k-1}(p-1) \mid \nu\end{aligned}$$

Thus, as above, the minimum value of ν that satisfies $(g+p^k)^\nu \equiv 1$ (mod 2 p^k) is just p^{k-1}(p-1) and so ord $(g + p^k) = \varphi(2\,p^k)$ in $Z^*_{2p^k}$.

The remaining results regarding the existence of a generator in Z_n^* exclude all n other than those we have considered above, except $n = 4$. Of course $Z_4^* = (3)$, which is cyclic.

Case (1) $n = 2^k, k \geq 3$

First consider $Z_8^* = \{1, 3, 5, 7\}$. Each $a \neq 1$ has ord $= 2$ so Z_8^* is not cyclic. Now realize that $Z_{2^k}^* = \left\{a \in \left[2^k\right] \middle| \text{ a is odd}\right\}$ and $\varphi(2^k) = 2^{k-1}$.

Claim $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ so a is not a generator and $Z_{2^k}^*$ is NOT cyclic for $k \geq 3$.

Proof Realize

$$a^{2^\alpha} - 1 = \left(a^{2^{\alpha-1}} + 1\right)\left(a^{2^{\alpha-1}} - 1\right)$$

Of course if $\alpha \geq 1$ then $2 \mid a^{2^{\alpha-1}} + 1$ because a is odd.

Observe that for $a = 2b + 1, b \geq 1$

$$a^2 - 1 = 4(b^2 + b)$$

so that

$$8 \mid a^2 - 1$$

Thus $16 \mid a^4 - 1$.

Next

$$a^8 - 1 = (a^4 + 1)(a^4 - 1)$$

so

$$32 \mid a^8 - 1$$

By induction

$$2^k \mid a^{2^{k-2}} - 1, \quad k \geq 3$$

so

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Case (2) all other n: Since $n \neq p^k$ or $2\,p^k$ for $k \geq 1$ and $n \neq 2^k$ for $k \geq 3$ it follows that $n = n_1\, n_2,\ n_1,\ n_2 > 2$ and $\gcd(n_1,\ n_2) = 1$.

Thus

$$\varphi(n) = \varphi(n_1)\ \varphi(n_2)$$

Claim If $m > 2$ then $2 \mid \varphi(m)$

Proof Exercise 2 (Submit this one)

Thus $\gcd\left(\varphi(n_1),\ \varphi(n_2)\right) \geq 2$

and

$$c = \ell\text{cm}\left(\varphi(n_1),\ \varphi(n_2)\right) < \varphi(n_i)\varphi(n_2) = \varphi(n).$$

Now suppose $a \in Z_n^*$, i.e $\gcd(a, n) = 1$.

Then $\gcd(a, n_1) = \gcd(a, n_2) = 1$ and so

$$a^{\varphi(n_1)} \equiv 1 \pmod{n_1}$$

and

$$a^{\varphi(n_2)} \equiv 1 \pmod{n_2}$$

But then

$$a^c \equiv 1 \pmod{n_1}$$

and

$$a^c \equiv 1 \pmod{n_2}$$

i.e. $n_1, n_2 \mid a^c - 1$

But $\gcd(n_1, n_2) = 1 \Rightarrow n_1\, n_2 = n \mid a^c - 1$

and so

$$a^c \equiv 1 \pmod{n}$$

As $c < \varphi(n)$, a is not a generator of Z_n^*.

Summarizing this extensive development we have the following theorem:

Theorem 1. Z_n^* is cyclic if and only if $n = 2, 4, p^k$ or $2\,p^k$ for $p \geq 3$ and $k \geq 1$.

Prior to doing an example we summarize the procedural aspects of the development.

Procedure for Finding Generators of Z_p^*, $Z_{p^k}^*$ and $Z_{2p^k}^*$ $(p \geq 3)$.

1. Use the theorem:

$\alpha \in Z_p^*$ is a generator if and only if $\forall$ q primes

$$q \mid (p\text{-}1) \Rightarrow \alpha^{\frac{(p-1)}{q}} \not\equiv 1 \pmod p$$

to find a generator g of Z_p^*

2. Method 1: Use the theorem

$\alpha \in Z_{p^k}^*$ is a generator if and only if $\forall$ primes q

$$q \mid \varphi(p^k) = p^{k-1}(p-1) \Rightarrow \alpha^{\frac{p^{k-1}(p-1)}{q}} \not\equiv 1 \pmod{p^k}$$

to find a generator of $Z_{p^k}^*$

Method 2: Take the g of 1. (i.e. a generator of Z_p^*)

- write $g^{p-1} = 1 + pT$ (i.e. find T)
- if $p \nmid T$ declare g to be a generator of $Z_{p^k}^*$
- if $p \mid T$ declare $g + p$ to be a generator of $Z_{p^k}^*$

3. Let g' be a generator of $Z_{p^k}^*$

- if g' is odd it is also a generator of $Z_{2p^k}^*$
- if g' is even then $g + p^k$ is a generator of $Z_{2p^k}^*$

Remark (3.a) I have not found an example where $p \mid T$ so that it is therefore necessary to use $g + p$ for $Z_{p^k}^*$

b) The method shows that a generator for $Z_{p^2}^*$ is a generator for all $Z_{p^k}^*$, $k \geq 2$.

<u>Example 2.</u> Find a primitive (generator) of Z_p^* where p = 41

Solution: Here p - 1 = 40 = (2^3) (5). Consider

$\alpha = 2$ $\quad 2^{\varphi(p)/2} = 2^{20} = (32)^4 = (1024)^2 \equiv (-1)^2 (\text{mod } 41)$

$\alpha = 3$ $\quad 3^{20} = (81)^5 \equiv (-1)^5 \equiv -1 \ (\text{mod } 41)$

$\quad 3^8 = (81)^2 \equiv (-1)^2 \equiv 1 \ (\text{mod } 41)$

$\alpha = 4$ $\quad 4^{20} = (256)^5 \equiv 10^5 \equiv 1 \text{mod } 41$

$\alpha = 5$ $\quad 5^{20} = (625)^5 \equiv (10)^5 \equiv 1 \text{ mod } 41$

$\alpha = 6$ $\quad 6^{20} = (1296)^5 \equiv (25)^5 \equiv (625)^2 \ 25 \equiv 40 \ (\text{mod } 41)$

$\alpha = 6$ $\quad 6^8 = (1296)^2 \equiv (25)^2 \equiv 625 \equiv 10 \ (\text{mod } 41)$

SO $\alpha = 6$ is a primitive.

The others are $\alpha^3, \alpha^7, \alpha^9, \alpha^{11}, \alpha^{13}, \alpha^{17}, \alpha^{19}, \alpha^{21}, \alpha^{23}, \alpha^{27}, \alpha^{29}, \alpha^{31}, \alpha^{33}, \alpha^{37}, \alpha^{39}$.

<u>Continuation</u> Consider $6^{40} = 1 + 41T$. As $41 \chi\ 6^{20} - 1$ since 6 is a generator of Z_{41}^*, it must be that $41 \mid 6^{20} + 1$. Indeed, $6^{20} + 1 = (41)\hat{T}$ and T = $\left(6^{20} = 1\right)$ $\hat{T}$.

Now $41 \chi\ \hat{T}$= 89174596099097 and $41 \chi\ 6^{20}$-1 so 41χ T. Thus 6 is a generator of $Z^*_{(41)^2}$.

A generator for $Z^*_{2(41)^2}$ is given by $6 + (41)^2$ since g is even.

Exercise 3. (Submit this one) Find generators of Z_{11}^*, $Z_{(11)}^*$ and $Z_{2(11)^2}^*$.

Exercise 4. (Extra Credit) A function

$$\Theta\colon Z^+ \to \text{reals}$$

is multiplicative if and only if $\Theta \not\equiv 0$ and

$\forall\, n_1, n_2 \in Z^+ \; (\gcd(n_1, n_2) = 1 \;\Rightarrow\; \Theta(n_1 n_2) = \Theta(n_1)\Theta(n_2))$

a) Prove: $\Theta(1) = 1$

b) Prove if $x = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k} \geq 2$ where $p_1, \ldots, p_k$ are distinct primes then

$$\sum_{d \mid x} \Theta(d) = \prod_{i=1}^{k} \sum_{j=0}^{c_i} \Theta(p_i^j)$$

c) Prove: $\sum_{d \mid n} \varphi(d) = n.$