Solutions of Submitted Exercises from Module III

Exercise 1. Consider Z_{19}^* and realize $\varphi(19) = 18 = (2)(3^2)$

Now

$$2^6 = 64 \equiv 7 \pmod{19}$$

and

$$2^9 \equiv 56 \pmod{19} \equiv 18 \pmod{19}$$

so 2 is a generator. The others are given by

$$2^5 \equiv 13 \pmod{19}$$
$$2^7 \equiv 14 \pmod{19}$$
$$2^{11} \equiv 15 \pmod{19}$$
$$2^{13} \equiv 3 \pmod{19}$$

and $\quad 2^{17} \equiv 10 \pmod{19}$

Next we observe that there are unique cyclic subgroups of orders 2, 3, 6 and 9. First

$$H_2 = \{1, 18\}$$

To determine an element of order = 3 we require

$$3 = \frac{18}{\gcd(18, k)}$$

so $k = 6$. Now $2^6 \equiv 7 \pmod{19}$ and $7^2 \equiv 11 \pmod{19}$ so

$$H_3 = \{1, 7, 11\}$$

Next set $k = 3$ to get an element of order 6, i.e.

$$2^3 \equiv 8 \pmod{19}$$

The other element of order 6 is given by $8^5 \pmod{19}$

Now

$$8^5 (\mathrm{mod}\,19) \equiv (64)^2\, 8 \pmod{19} \equiv (11)(8) \bmod 19$$
$$\equiv 12 \pmod{19}$$

Thus

$$H_6 = \{1, 18, 7, 11, 8, 12\}$$

Obviously the remaining elements 4, 5, 6, 9, 16 and 17 have order = 9. Hence

$$H_9 = \{1, 7, 11, 4, 5, 6, 9, 16, 17\}$$

and the hierachical diagram is given below:

$$\begin{tikzcd} & Z^{*}_{19} \arrow[dl, dash] \arrow[dr, dash] & \\ H_9 \arrow[d, dash] & & H_6 \arrow[d, dash] \arrow[dll, dash] \\ H_3 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\ & \{1\} & \end{tikzcd}$$

Consider Z^*_{81} and observe that $\varphi(81) = 3^4 - 3^3 = 54 = (2)(3^3)$

Now

$$2^{18} = (512)^2 \equiv 28 \pmod{81}$$

and

$$2^{27} \equiv 80 \pmod{81}$$

so 2 is a generator. There are $\varphi(54) = 18$ generators:

$2^5 \equiv 32 \pmod{81}$

$2^7 \equiv 47$ (mod81)

$2^{11} \equiv 23 \pmod{81}$

$2^{13} \equiv 11 \pmod{81}$

$2^{17} \equiv 14 \pmod{81}$

$2^{19} \equiv 56 \pmod{81}$

$2^{23} \equiv 5 \pmod{81}$

$2^{25} \equiv 20 \pmod{81}$

$2^{29} \equiv 77$(mod 81)

$2^{31} \equiv 65 \pmod{81}$

$2^{35} \equiv 68 \pmod{81}$

$2^{37} \equiv 29 \pmod{81}$

$2^{41} \equiv 59 \pmod{81}$

$2^{43} \equiv 74 \pmod{81}$

$2^{47} \equiv 50 \pmod{81}$

$2^{49} \equiv 38 \pmod{81}$

$2^{53} \equiv 41 \pmod{81}$

We obtain the elements of order 27 by squaring the elements of order 54. There are $\varphi(27) = 18$ in total. Thus 4 has order 18. The rest are given by

$$2^{10} \equiv (32)^2 (\mathrm{mod}\, 81) \equiv 52 \ (\mathrm{mod}\ 81)$$
$$2^{14} = (2^{13})(2) \equiv 22 \ (\mathrm{mod}\ 81)$$
$$2^{22} = (2^{19})(2^3) \equiv 43 \ (\mathrm{mod}\ 81)$$
$$2^{26} = (2^{25})(2) \equiv 40 \ (\mathrm{mod}\ 81)$$
$$2^{34} = (2^{31})(2^3) \equiv 34 \ (\mathrm{mod}\ 81)$$
$$2^{38} = (2^{37})(2) \equiv 58 \ (\mathrm{mod}\ 81)$$
$$2^{46} = (2^{43})(2^3) \equiv 25 \ (\mathrm{mod}\ 81)$$
$$2^{50} = (2^{49})(2) \equiv 76 \ (\mathrm{mod}\ 81)$$
$$2^{58} = (2^{19})^3 (2) \equiv 35 \ (\mathrm{mod}\ 81)$$
$$2^{62} = (2^{31})^2 \equiv 13 \ (\mathrm{mod}\ 81)$$
$$2^{70} = (2^{35})^2 \equiv 7 \ (\mathrm{mod}\ 81)$$
$$2^{74} = (2^{70})(2^4) \equiv 31 \ (\mathrm{mod}\ 81)$$
$$2^{82} = (2^{41})^2 \equiv 79 \ (\mathrm{mod}\ 81)$$
$$2^{86} = (2^{82})(2^4) \equiv 49 \ (\mathrm{mod}\ 81)$$
$$2^{94} = (2^{47})^2 \equiv 70 \ (\mathrm{mod}\ 81)$$
$$2^{98} = 2^{94}\, 2^4 \equiv 14 \ (\mathrm{mod}\ 81)$$
$$2^{106} = (2^{53})^2 \equiv 61 \ (\mathrm{mod}\ 81)$$

There are $\varphi(18) = 6$ elements of order 18. We obtain one by cubing 2, i.e. ord $8 = 18$. The others are given by -

$$8^5 = 2^{15} = (2^{14})(2) \equiv 44 \ (\mathrm{mod}\ 81)$$
$$8^7 = 2^{21} = (2^{19})(2^2) \equiv 62 \ (\mathrm{mod}\ 81)$$
$$8^{11} = 2^{33} = (2^{31})(2^2) \equiv 17 \ (\mathrm{mod}\ 81)$$
$$8^{13} = 2^{39} = (2^{38})(2) \equiv 35 \ \mathrm{mod}\ 81)$$

and

$$8^{17} = 2^{51} = (2^{49})(2^2) \equiv 71 \ (\mathrm{mod}\ 81)$$

There are $\varphi(9) = 6$ elements of order 9. We obtain one by considering $2^6 = 64$. The others are given by

$$64^2 = 2^{12} = (2^{11})\,(2) \equiv 46 \pmod{81}$$
$$64^4 = 2^{24} = (2^{23})\,(2) \equiv 10 \pmod{81}$$
$$64^5 = 2^{30} = (2^{29})\,(2) \equiv 73 \pmod{81}$$
$$64^7 = 2^{42} = (2^{41})\,(2) \equiv 37 \pmod{81}$$
$$64^8 = 2^{48} = (2^{47})\,(2) \equiv 19 \pmod{81}$$

There are $\varphi(6) = 2$ elements of order 6. We obtain one by considering $2^9 \equiv 26 \pmod{81}$.
The other one is given by $(2^9)^5 = 2^{45} = (2^{43})\,(2^2) \equiv 53 \pmod{81}$

There are $\varphi(3) = 2$ elements of order 3. One is given by $2^{18} = (2^{17})\,(2) \equiv 28 \pmod{81}$.
The other one is given by $(2^{18})^2 = 2^{36} = (2^{35})\,(2) \equiv 55 \pmod{81}$

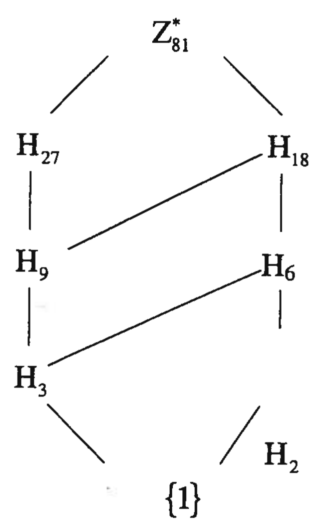
There is one element of order 2. Clearly $80 \equiv -1 \pmod{81}$, is the one. Thus

$$H_1 = \{1\}$$
$$H_2 = \{1, 80\}$$
$$H_3 = \{1, 28, 55\}$$
$$H_6 = \{1, 28, 55, 80, 26, 53\}$$
$$H_9 = \{1, 28, 55, 46, 10, 73, 37, 19, 64\}$$
$$H_{18} = \{1, 28, 55, 46, 10, 73, 37, 19, 64, 80, 18, 44, 62, 17, 35, 71, 53, 21\}$$

and

$$H_{27} = H_9 \cup \{28,32,47,23,11,14,56,5,20,77,65,68,29,59,74,50,38,41\}$$

The diagram is given below:



Exercise 2) If $m = 2^k$ $k \geq 2$ then $\varphi(m) = 2^{k-1}$, where $k - 1 \geq 1$, so $\varphi(m)$ is even. Otherwise $\exists\, p \geq 3$, prime, such that

$$m = p^k\, r$$

where $\gcd(p, r) = 1$ and $k \geq 1$. Then

$$\varphi(m) = \varphi(p^k)\, \varphi(r) = (p^k - p^{k-1})\, \varphi(r)$$

But $p^k - p^{k-1}$ is even so $\varphi(m)$ is even as well.

Exercise 3) Since $\varphi(11) = 10 = (2)(5)$ we must check α^2, α^5.

Consider $\alpha = 2$;

$$2^2 = 4 \pmod{11}$$

$$2^5 = 32 \equiv 10 \pmod{11}$$

so $\alpha = 2$ is a generator

Next consider

$$2^{10} = 1024 = 1 + (11)(93)$$

and $11 \chi\, 93$. Thus $\alpha = 2$ is a generator of $Z^*_{(11)^2}$

Finally, since $\alpha = 2$ is even we obtain

$$2 + 11^2 = 123$$

to be a generator of $Z^*_{2(11)^2}$

Ex 4 a) Suppose $\theta(1) = 0$

Then $\theta(n) = \theta(n \cdot 1) = \theta(n)\,\theta(1) = 0$

so $\theta \equiv 0$ $\times$

$\therefore$ $\theta(1) \neq 0$

Consider $\theta(1) = \theta((1)(1)) = (\theta(1))^2$.

Divide by $\theta(1)$, get $\theta(1) = 1$

b) Consider $x = p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}$ and

$\prod_{i=1}^{k} \sum_{j=0}^{e_i} \theta(p_i^j) =$

$(1 + \theta(p_1) + \cdots + \theta(p_1^{e_1}))(1 + \theta(p_2) + \ + \theta(p_2^{e_2})) \cdots (1 + \theta(p_k) + \cdot \cdot + \theta(p_k^{e_k}))$

This product can be expanded as the sum of all the terms obtained by selecting exactly one term from each of the parantheses and multiplying them (this is an application of a combinatorial theorem)

- if all 1's are selected get $(1)(1) \cdots (1) = 1$
- a typical term is obtained by selecting the parantheses in which 1 is not selected, say $i_1, i_2, \ldots, i_t$, and then a θ value within each of these parantheses, i.e

$$\Theta(p_{i_1}^{j_{i_1}})\,\Theta(p_{i_2}^{j_{i_2}})\cdots\Theta(p_{i_t}^{j_{i_t}}) = \Theta(p_{i_1}^{j_{i_1}} p_{i_2}^{j_{i_2}} \cdots p_{i_t}^{j_{i_t}})$$

Clearly each $p_{i_1}^{j_{i_1}} p_{i_2}^{j_{i_2}} \cdots p_{i_t}^{j_{i_t}}$ is a divisor of x and conversely each $d \mid x$ is of the above form so the expansion yields

$$\sum_{d \mid x} \Theta(d)$$

c) Consider

$$\sum_{j=0}^{e_i} \varphi(p_i^j) = 1 + (p_i - 1) + p_i(p_i - 1) + p_i^2(p_i - 1) + \cdots + p_i^{e_i - 1}(p_i - 1)$$

$$= 1 + (p_i - 1)(1 + p_i + \cdots + p_i^{e_i - 1})$$

$$= 1 + \cancel{(p_i - 1)}\frac{(p_i^{e_i} - 1)}{\cancel{p_i - 1}} = p_i^{e_i}$$

$$\therefore \sum_{d \mid n} \varphi(d) = \prod_{i=1}^{k} \sum_{j=0}^{e_i} \varphi(p_i^j) \quad (\text{by } (b))$$

$$= \prod_{i=1}^{k} p_i^{e_i} = n$$