Synopsis of cyclic groups

A group C is called *cyclic* if it is generated by one element. If x is a generator for C we write $C =< x >$. If G is any group and $x \in G$ then the cyclic subgroup generated by x is

$$C = \{x^n | n \in \mathbb{Z}\}$$

Clearly, $< x >$ must contain all these powers of x and they are closed in G :

$$x^n x^m = x^{n+m}$$
$$(x^n)^{-n} = x^{-n}$$
$$x^0 = e$$

Theorem The following statements about the cyclic group $C = \{x^n | n \in \mathbb{Z}\}$ are equivalent.

1. **a**) $x^n = x^m$ only if $m = n$.

   b) C is infinite.

Proof. We clearly have that a) implies b). Now assume that a) is false. That is, there are $m \neq n$ such that $x^m = x^n$. We may assume that $m > n$. Then $x^{m-n} = e$ and therefore the set $E = \{k | k > 0, x^k = e\}$ is non-empty. Let

$$n = \min E$$

Then $n > 0$ and $x^n = e$. We claim that for every $x^m \in C$ there is some $r, 0 \leq r < n$ such that

$$x^m = x^r, 0 \leq r < n$$

Indeed, $m = qn + r$ where $0 \leq r < n$. It follows that $x^m = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = x^r$. Thus in this case the group C is finite with at most n –many elements. Moreover, we have for $0 \leq s_1 < s_2 < n$ that $x^{s_1} \neq x^{s_2}$. Otherwise $x^{s_2 - s_1} = x^s = e$ where $0 \leq s < n$ But this is impossible, n was the smallest positive number for which $x^n = e$. Hence in this case we have that $C = \{x^0, x, x^2, \ldots, x^{n-1}\}$ and is a finite cyclic group of order n.

Corollary. Let $C =< x >$ be a cyclic group generated by some element x. Then we either have that

$$\mathbb{Z} \to C = \{x^n | n \in Z\}, n \mapsto x^n$$

Is an isomorphism between the additive group of integers and the infinite cyclic group C Or, in case that C is finite of order n then

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n \to C = \{x^0, x, \ldots x^{n-1}\}, [r]_n \mapsto x^r$$

is an isomorphism between the additive group of integers $\mathrm{mod}\, n$ and the finite group C of order n.

Facts on infinite cyclic groups. The additive group $\mathbb{Z}$ has only two generators 1 and -1. Therefore any infinite cyclic group $< x >$ has only two generators, namely x and x^{-1}.

Let H be a subgroup of the additive group $\mathbb{Z}$ of integers. Then H is cyclic and of the form $n\mathbb{Z}$. In case that $H = \{0\}$ then $n = 0$, otherwise let n be the smallest positive element in H. Clearly $n\mathbb{Z} \subseteq H$. For the converse inclusion, let $m \in H$. Then $m = qn + r, 0 \leq r < n$. Because $m \in H, qn \in H$ we have that $r = (m - qn) \in H$. The element r cannot be positive because $r < n$ and n was the smallest positive element in H. Thus $r = 0$ and m must be divisible by n, that is $H \subseteq nZ$. We have that $n\mathbb{Z} =< n >$, thus subgroups of the additive group $\mathbb{Z}$ are all cyclic.

Theorem Let $C =< x >$ be an infinite cyclic group. Then any subgroup H of C which is different from $\{e\}$ is infinite cyclic and $H =< x^n >$ where n is the smallest positive exponent n such that $x^n \in H$.

Corollary $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$ where k is the lowest common multiple of n and $.m$.

Indeed $nZ \supseteq kZ$ iff k is multiple of n. Thus $n\mathbb{Z} \cap m\mathbb{Z} \supseteq l\mathbb{Z}$ makes l a multiple of m as well as n. Any multiple l of m and n is a multiple of the lowest common multiple k. Thus kZ is the largest subgroup contained in $n\mathbb{Z}$ and $m\mathbb{Z}$.

Facts on finite cyclic groups.

Theorem Let $C =< x >$ be an finite cyclic group of order n. Then any subgroup of C is cyclic and if different from $\{e\}$ one has that $H =< x^m >$ where m is the smallest positive exponent k such that $x^k \in H$.

Theorem The subgroups H of $\mathbb{Z}_n$ are of the form $< [d]_n >$ where d is a divisor of n.

For the proof we only have to show that $< [m]_n >=< [d]_n >$ where $d = \gcd(m,n)$. We know that $d = xm + yn$. Therefore $[d]_n = [xm]_n + [yn]_n$. We obviously have $[yn]_n = [0]_n$. Thus $[d] \in< [m]_n >$. On the other hand, as the *gcd* of m and n we have that $d|m$ and therefore $[m]_n \in< [d]_n >$. This gives $< [m]_n >=< [d]_n >$.

If d is a divisor of n then $< [d]_n >$ has $\frac{n}{d}$ many elements

The order $o(x)$ of an element x is the order of the cyclic group $< x >$ in case that $< x >$ is finite. It is the smallest positive n where $x^n = e$.

Theorem If d is a divisor of n then $< [d]_n >$ has $\frac{n}{d}$ – many elements in $\mathbb{Z}_n$. Thus $o([m]_n) = \frac{n}{(m,n)}$.

Examples. Let $G = \mathbb{Z}_{12}$ What is the order of $[8]_{12.}$ Of course we can list the elements of $< [8] >$. They are $[8], [16] = [4], [12] = [0]$. Thus $ord[8]_{12} = 3$. We have $< [8] >=< [\gcd(8,12)] >=< [4] >$ and $ord[4]_{12} = \frac{12}{4} = 3$.

Exercise 4.15 in the book asks for $\gcd(123,321)$. Calculations lead to $(123,321) = 3 = 47 \bullet 123 - 18 \bullet 321$. Thus $< [123]_{321} >=< [3]_{321} >$and $ord < [3]_{321} >= \frac{321}{3} = 107$ and $< [321]_{123} >=< [3]_{123} >$ and $ord(< [3]_{123} >= \frac{123}{3} = 41$

Problem 5.21 in the book is the following. Given a cyclic group $G =< x >$ of order n. Find a condition on the integers r and s that is equivalent to $< x^r >\subseteq< x^s >$. We can identify G with $\mathbb{Z}_n$ and x^r with $[r]_n$ and x^s with $[s]_n$. We have that $< [r]_n >=< [(r,n)]_n >$ and $< [s]_n > = < [(s,n)]_n >$ We now have that $< [(r,n)]_n >\subseteq< [(s,n)]_n >$ is equivalent to $(s,n) |(r,n)$. This is the solution of the problem.