Week3, Challenge2

Take $C_9 = \{\mathrm{id}, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\}$ for example. The subgroups generated by each element of C_9 are

$\langle id \rangle = \{id\}$
$\langle x \rangle = \{x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, \mathrm{id}\}$
$\langle x^2 \rangle = \{x^2, x^4, x^6, x^8, x, x^3, x^5, x^7, \mathrm{id}\}$
$\langle x^3 \rangle = \{x^3, x^6, \mathrm{id}\}$
$\langle x^4 \rangle = \{x^4, x^8, x^3, x^7, x^2, x^6, x, x^5, \mathrm{id}\}$
$\langle x^5 \rangle = \{x^5, x, x^6, x^2, x^7, x^3, x^8, x^4, \mathrm{id}\}$
$\langle x^6 \rangle = \{x^6, x^3, \mathrm{id}\}$
$\langle x^7 \rangle = \{x^7, x^5, x^3, x, x^8, x^6, x^4, x^2, \mathrm{id}\}$
$\langle x^8 \rangle = \{x^8, x^7, x^6, x^5, x^4, x^3, x^2, x, \mathrm{id}\}$

We see that x^k is a generator of C_9 if and only if the order of x^k (i.e. the smallest positive integer m for which $(x^k)^m = \mathrm{id}$) is 9.

Continued

More generally, x^k is a generator of C_n if and only if ord$(x^k) = n$.

(1) If ord$(x^k) < n$, elements in $\langle x^k \rangle$ starts repeating before all elements appear in the list, which means that there exist elements in C_n that will not be generated by x^k.
(2) If ord$(x^k) > n$, then there have to be some duplicate items in $\langle x^k \rangle$. Thus, $\exists$a ,b with $1 \leq a < b < n$ such that $(x^k)^a = (x^k)^b$ $\implies (x^k)^{a-b} = id \implies ord(x^k) = a - b < n$ which contradicts with our assumption.
Combining (1) and (2), we see that if x^k is a generator of C_n, then $ord(x^k) = n$.
(3) If ord$(x^k) = n$, then ord$(\langle x^k \rangle) =$ ord(C_n). Thus $\langle x^k \rangle = C_n$ since $\langle x^k \rangle$ is a subgroup of C_n. It follows that x^k is a generator of C_n .

Continued

Furthermore, x^k is a generator of C_n

$\iff ord(x^k) = n$

$\iff x^{[kb]_n} \neq id \qquad \forall 1 \leq b < n$

$\iff kb \ mod \ n \neq 0 \qquad \forall 1 \leq b < n$

$\iff lcm(k, n) = kn$

$\iff gcd(k, n) = 1$

Therefore, the elements of C_n that generate it as a cyclic group are exactly those elements of the form x^k where gcd(k,n) = 1 (i.e. the number of these is Φ(n), where Φ is the Euler's totient function).