§3.5 # 13, 14, 16, 18, 20

(13) Show that in a finite cyclic group of order n, the equation $x^m = e$ has exactly m solutions for each $m \mid n$.

Proof: Let $G = \langle a \rangle$, $o(a) = n < \infty$. If $d = n/m$ then $(a^{jd})^m = a^{jn} = e$ for each $j \in \mathbb{Z}$. Since $a^{jd} = a^{kd} \iff jd \equiv kd \ (n) \iff j \equiv k \ (m)$, the set $\langle a^d \rangle$ contains exactly m solutions to $x^m = e$. No other elements of G solve $x^m = e$ since $(a^i)^m = e \Rightarrow im \equiv 0 \ (n) \Rightarrow i \equiv 0 \ (d) \Rightarrow a^i = a^{jd} \in \langle a^d \rangle$ for some j. //

(14) A cyclic group with more than two elements has at least two generators

Proof: If $G = \langle a \rangle$ then $G = \langle a^{-1} \rangle$ as well, since $a^k = (a^{-1})^{-k}$. If $a = a^{-1}$ then $a^2 = e$ and $|G| = 2$, so if $|G| > 2$ then a and a^{-1} are distinct. //

(16) If G is a group of order >1 with no proper subgroups then $G \cong \mathbb{Z}_p$, p prime.

Proof: Let $g \in G$, $g \neq e$. Then $\langle g \rangle$ is a subgroup of G so $\langle g \rangle = G$. If $o(g) = \infty$ then $\langle g^2 \rangle$ is a proper subgroup, so $o(g) < \infty$. If $o(g) = nm$, $n > 1$ and $m > 1$, then $\langle g^n \rangle$ is a proper subgroup. Hence $o(g)$ is prime. //

(18) $$\sum_{d \mid n} \phi(d) = n$$

Proof: Since any $[k] \in \mathbb{Z}_n$ has order $d \mid n$, the set $\mathbb{Z}_n$ can be partitioned according to the order of the subgroup generated:

$$\mathbb{Z}_n \cong \coprod_{d \mid n} \{ [k]_n \mid o([k]_n) = d \}.$$

Now
$$\begin{array}{ccc} \{ [k]_n \mid o(k) \mid d \} & \cong & \mathbb{Z}_d \\ \cup\!\!| & & \cup\!\!| \\ \{ [k]_n \mid o([k]_n) = d \} & \cong & \mathbb{Z}_d^\times \end{array}$$
and so
$$n = \sum_{d \mid n} \left| \{ [k]_n \mid o([k]_n) = d \} \right| = \sum_{d \mid n} \phi(d). \ //$$