1. (a) Let a be an arbitrary element in H since it is non-empty. We note that $a^{|G|} = e$ by Corollary 12.4, so $e \in H$. This implies that $a^{|G|-1} = a^{-1}$, so $a^{-1} \in H$. Lastly, for any $a, b \in H$, we get that $ab \in H$. Thus, we proved that H is a subgroup of G. $\square$

(b) **Claim 1:** Let $a \in G$. If $o(a) = d$, then if there exist a $k \in \mathbb{N}$ where $a^k = e$ then $d \mid k$.

By contradiction, $d \nmid k$, then by the Division Algorithm, there exist $q, r \in \mathbb{Z}$ where $a^k = a^{qd} \cdot a^r = e$ where $0 < r < d$. However, $a^{qd} = e^q = e$, so $a^r = e$. This contradicts the minimality of $o(a)$. Hence, r must be 0 and $d \mid k$.

Claim 2: Let $a \in G$. For any $k \in \mathbb{N}$, we have $o(a^k) = \frac{o(a)}{\gcd(o(a),k)}$. $\square$

Let $d = o(a)$ and $w = d/\gcd(d, k)$. Then $wk = d(k/\gcd(d, k))$ is divisible by d and so $a^{kw} = e$. Furthermore, suppose we have a $n \in \mathbb{N}$ where $a^{kn} = e$. By Claim 1, we get that $d \mid kn$, so:

$$\frac{d}{\gcd(k,d)} \mid \frac{k}{\gcd(k,d)} n$$

We note that $\gcd(d/\gcd(k, d), k/\gcd(l, d)) = 1$. By Corollary 2.20, $w \mid n$. This implies the smallest value for n is w. (Yes, this is just a re-write of the solution for HW3 2(b)) $\square$

Claim 3: For any positive integer $d \mid m$, there are exactly $\phi(d)$ elements of G with order d

Since G is cyclic, there exist some $g \in G$ with $o(g) = m$ where $G = \{g, g^2, \cdots, g^m\}$. For any $d \mid m$, there exist an integer q where $dq = m$. Let $a = g^q \in G$ thus $a^d = g^{dq} = e$ and $o(a) = d$. Otherwise, $o(a) < d$ implies $q \cdot o(a) < qd = m$, contradicting the minimality of m. Since $o(a) = d$, we note that $a, a^2, \cdots, a^d$ are all unique because if there exist $a^j = a^k$ for $1 \le j < k \le d$, then $e = a^{k-j}$, contradicting d's minimality. We apply Claim 2 to get that for $1 \le k \le d$ that $o(a^k) = d/\gcd(d, k)$. It is clear that if $o(a^k) = q$, then $\gcd(d, k) = 1$. We showed all of the a^k are unique, so there exist at least $\phi(d)$ elements with order d.

We now prove all orders $b \in G$ with order d must be in the form a^k. Let $b = g^r$ for $1 \le r \le m$. We apply Claim 2 again to get that $o(g^r) = m/\gcd(m, r)$ thus $\gcd(m, r) = d/m = q$. This further implies that $q \mid r$, so there exist an integer k where $1 \le k \le d$ that $qk = r$. Thus, $g^r = (g^q)^k = a^k$. This proves that there exist exactly $\phi(d)$ elements with order d. $\square$

Claim 4: For any positive integer $d \mid m$, there is a unique subgroup of G of order d.

Let $a \in G$ where $o(a) = d$ and $a = g^{m/d}$, which exits by Claim 3. We then denote the set $H = \{a, a^2, \cdots a^d\}$. For any $1 \le i, j \le d$, $a^i \cdot a^j = a^{i+j}$. If $i + j \le d$, then $a^{i+j} \in H$. Otherwise, we note that $a^{i+j} = a^{i+j-d} \cdot a^d = a^{i+j-d}$. Since $i + j \le 2j$ so $i + j - d \le d$, $a^{i+j} \in H$. By (a), H is a subgroup of G. Note that all elements in H are unique by our proof of Claim 3, so it is also order d.

It remains to prove H is the only subgroup of order d in G. Suppose there exist a subgroup $E \le G$ with order d. Let $b \in E$, then $b^d = e$ by Corollary 12.4. We note that $b = g^r$ for some $r \in \mathbb{N}$ and $g^{rd} = e$. By Claim 1, $m \mid rd$, which implies that $m/d \mid r$. Hence, there exist some integer k where $1 \le k \le d$ and $b = g^r = (g^{m/d})^k = a^k$. Hence, $b \in H$ and $E \subseteq H$. Since they have the same order, by the pigeonhole principle, $E = H$. $\square$