DUKE MATH MEET- Power Round Solutions

1. (a) $3^{-1} = 5, 5^{-1} = 3, 6^{-1} = 6$ (1 pts)
   $Ord(3) = 6, Ord(5) = 6, Ord(6) = 2$ (1 pts)

   (b) $\langle 2 \rangle = \{1, 2, 4\}$ (1 pts)
   $\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\} = T$ (1 pts)

2. (a) Let $m = kn$, then $g^m = (m^k)^n = e^n = e$. (2 pts)

   (b) Let $ord_G(g) = n$, $d = kn + r, 0 \leqslant r < n$. (1 pts)
   $e = g^d = g^{kn+r} = (g^n)^k * g^r = e^k * g^r = g^r$.
   From the definition of n and $0 \leqslant r < n$, r must be 0 or d is divisible by n. (1 pts)

3. (a) Check criteria for a subgroup:
   i) For $a = g^i$ and $b = g^j \in \langle g \rangle$, $a * b = g^i * g^j = g^{i+j}$ which is also in H. (0.5 pts)
   ii) For each $a = g^i \in \langle g \rangle$, pick j such that i+j is a multiple of k. We have g^j is in G and $g^i * g^j = g^{i+j} = e$ (from 2a) or g^j is the inverse of a. (0.5 pts)
   Finally, we have $g^x = g^y$ iff $g^{x-y} = e$ or $x - y = 0$ mod k (from 2b). Since there are k residues modulo k, there are k distinct elements g^x or $|\langle g \rangle| = k$. (1 pts)

   (b) From a), $\langle g \rangle$ is a subgroup of G. By Theorem 1, $|\langle g \rangle| = k$ divides $|G|$. (0.5 pts)
   Now, from 2a, we have $g^{|G|} = e$. (0.5 pts)

   (c) Let $ord_G(g^i) = n$, then $(g^i)^n = g^{in} = e$. From 2b, we know in is divisible by k, but $(i, k) = 1$, so n is divisible by k. (1 pts)
   From the definition of order, n must be k. (1 pts)

   (d) We use contrapositive: if $\langle g \rangle \cap \langle b \rangle \neq \{e\}$, then there exist $g^i = b^j$, where $i, j \neq 0$ mod k. Here, we can pick m and n such that $im = jn = 1$ mod k, or $g^n = b^{jn} = b$ and $b^m = g^{im} = g$. (1 pts)
   Now, for each $g^k \in \langle g \rangle$, $b^{mk} = g^k$ implies $g^k \in \langle b \rangle$. Hence, $\langle g \rangle \subseteq \langle b \rangle$.
   Similarly, $\langle b \rangle \subseteq \langle g \rangle$ and we are done. (1 pts)

4. (a) $h * g_1 * g_2 * h^{-1} = (h * g_1 * h^{-1}) * (h * g_2 * h^{-1})$ (1 pts)

   (b) Let $r = f_h(g) = h * g * h^{-1}$ and $ord_G(r) = t$.
   $e = r^t = h * g * h^{-1} * h * g * h^{-1} * \ldots h * g * h^{-1}$
   $= h * g * (h^{-1} * h) * g * (h^{-1} * \ldots h) * g * h^{-1} = h * g^t * h^{-1}$ (1 pts)
   Hence, $h^{-1} * e * h = h^{-1} * (h * g^t * h^{-1}) * h = g^t = h^{-1} * h = e$.

From 2b, k divides t. (0.5 pts)

In addition, using similar transformation, $r^k = h * g^k * h^{-1} = h * e * h^{-1} = e$. From 2b, t divides k.

So t=k. (0.5 pts)

(c) Since the function is from G to G, it is enough to show injectivity. (1 pts)

$f_h(g_1) = f_h(g_2) \Rightarrow h * g_1 * h^{-1} = h * g_2 * h^{-1}$

$\Rightarrow h^{-1} * (h * g_1 * h^{-1}) * h = h^{-1} * (h * g_1 * h^{-1}) * h \Rightarrow g_1 = g_2$ (1 pts)

5. (a) From 3b, the order of g divides $|P| = p^k$ so it must be a power of p.

(b) From $|G| = 56 = 7.8$, by Sylow Theorem, $n_7(G)$ divides 8 and $n_7(G) = 1$ mod 7, so $n_7(G) = 1$ or 8. But $n_7(G)$ can not be 1 because this implies there is only 1 Sylow 7-subgroup in G, so it must be normal from Sylow Theorem iii) which means G is not simple. Hence, $n_7(G) = 8$. (1 pts)

Consider any element g of order 7, g is in $\langle g \rangle$ which is a Sylow 7-subgroup of G (from 3a), so g belongs to some Sylow 7-subgroup. From 3d, we know that the Sylow 7-subgroups in G either coincide or share only the identity element. From 3c, each Sylow 7-subgroup includes the identity and 6 distinct elements of order 7. Therefore, there are $8.6 = 48$ elements of order 7 in G. (1 pts)

(c) Assume G is simple, $|G| = 520 = 13.5.8$.

Since G is simple, for each $p = 13, 5, and 2$, G can not have just 1 Sylow p-subgroup since this implies this Sylow p-subgroup will be normal from Sylow iii) or G is not simple. (0.5 pts)

By Sylow Theorem, $n_{13}(G)$ divides 5.8 and $n_{13}(G) = 1$ mod 13, so it must be 1 or 40. From above, $n_{13}(G) = 40$. Similar to part b, there are 40.12 elements of order 13. (0.5 pts)

By Sylow Theorem, $n_5(G)$ divides 13.8 and $n_5(G) = 1$ mod 5, so it must be 1 or 26. From above, $n_5(G) = 26$. Similar to part b, there are 26.4 elements of order 5. (0.5 pts)

These elements of 2 different orders must be distinct so G has $\geqslant 26.4+40.12 > 520$ elements which is a contradiction. (0.5 pts)