Homework #6. Solutions to selected problems.

1.

(a) Let $G_1, \ldots, G_k$ be finite groups. Prove that
$$\exp(G_1 \times \ldots \times G_k) = lcm(\exp(G_1), \ldots, \exp(G_k)),$$
where as usual $\exp(G)$ denotes the exponent of G.

(b) Give an example showing that if G is finite, but non-abelian, then $exp(G)$ may not equal to $o(g)$ for any $g \in G$.

Solution: (a) We start with a simple lemma:

Lemma: *Let G be a finite group and $n \in \mathbb{Z}$. Then the following are equivalent:*

(i) $\exp(G)$ *divides* n

(ii) $g^n = e$ *for all* $g \in G$.

Proof: The implication "(i)$\Rightarrow$(ii)" is clear. Conversely, assume (ii) holds, let $m = \exp(G)$ and write $n = mq + r$ where $0 \le r < m$. Since $g^m = e$ for all $g \in G$ by definition of $\exp(G)$, we get that $g^r = e$ for all $g \in G$. Since $0 \le r < \exp(G)$, this is only possible if $r = 0$, in which case $m \mid n$. $\square$

We proceed with the proof of (a). Let $G = G_1 \times \ldots \times G_k$, $m_i = \exp(G_i)$, let $m = \exp(G)$ and $m' = lcm(m_1, \ldots, m_k)$. Thus we are asked to prove that $m = m'$. We shall do this by first showing that $m \le m'$ and then that $m \ge m'$.

Any element of G has the form $(g_1, \ldots, g_k)$ for some $g_i \in G_i$. Then $(g_1, \ldots, g_k)^{m'} = (g_1^{m'}, \ldots, g_k^{m'})$. Since $m_i \mid m'$ for each i, Lemma applied to G_i implies that $g_i^{m'} = e_{G_i}$ for each i, and therefore $(g_1, \ldots, g_k)^{m'} = (e_{G_1}, \ldots, e_{G_k}) = e_G$. Now applying Lemma to G, we conclude that $m = \exp(G)$ divides m'; in particular, $m \le m'$. On the other hand, for any $(g_1, \ldots, g_k) \in G$ we have $(g_1^m, \ldots, g_k^m) = (g_1, \ldots, g_k)^m = e_G$. In particular, for each i we have $g_i^m = e_{G_i}$ for all $g_i \in G_i$, so by Lemma $m_i \mid m$. Thus m is a common multiple of $m_1, \ldots, m_k$, and in particular, $m \ge lcm(m_1, \ldots, m_k) = m'$

(b) $G = S_3$ is an example. It has one element of order 1, three elements of order 2 (transpositions) and two elements of order 3 (three-cycles). Hence $\exp(G) = lcm(1, 2, 3) = 6$, while there is no element of order 6.

3. Determine whether 67 is a primitive root mod 3^{2014}.

Solution: We know that x is a primitive root mod $3^{2014} \iff x$ is a primitive root mod $3^2 = 9$. Since $[67]_9 = [4]_9$ has order 3 in U_9 while $|U_9| = \phi(9) = 6 > 3$, we conclude that 67 is not a primitive root mod 3^{2014}.

An even simpler argument would be to observe that $[67]_3 = [1]_3$, so 67 is not even a primitive root mod 3, hence cannot be a primitive root mod 3^k for any $k \geq 1$ (the last implication follows, for instance, from the fact that the natural map $U_{3^k} \to U_3$ is surjective).

4. Let $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Find the order of the element $[67]_n \in U_n$.

Solution: We know that U_n is isomorphic to $U_2 \times U_3 \times U_5 \times U_7 \times U_{11}$ via the map $[x]_n \mapsto ([x]_2, [x]_3, [x]_2, [x]_5, [x]_7, [x]_{11})$. Hence

$$o([67]_n) = lcm(o([67]_2), o([67]_3), o([67]_5), o([67]_7), o([67]_{11})).$$

The elements $[67]_2, [67]_3$ and $[67]_{11}$ are trivial in the respective unit groups, $[67]_5 = [2]_5$ has order 4 and $[67]_7 = [4]_7$ has order 3. Therefore, $o([67]_n) = lcm(1, 1, 4, 3, 1) = 12$.

5. Find all $n \in \mathbb{N}$ for which the group U_n has exponent 4.

Solution: Let $n = p_1^{a_1} \dots p_k^{a_k}$ be the prime factorization of n. Then by Problem 1 and the isomorphism $U_n \cong U_{p_1^{a_1}} \times \dots \times U_{p_k^{a_k}}$ we know that $\exp(U_n) = lcm(\exp(U_{p_1^{a_1}}), \dots, \exp(U_{p_k^{a_k}}))$. The least common multiple of several positive integers is equal to $4 \iff$ each of those integers is equal to $1, 2$ or 4, and at least one is equal to 4.

Thus, to begin with we need to solve the equation $\exp(U_x) = 1, 2$ or 4 where x is a prime power. If p is an odd prime and $k \geq 2$, then U_{p^k} is cyclic, so $\exp(U_{p^k}) = |U_{p^k}| = \phi(U_{p^k}) = p^{k-1}(p-1)$ is divisible by p and cannot be a power of 2. Thus, x can only be an odd prime or a power of 2.

If x is an odd prime, then $\exp(U_x) = x - 1$, so the possible values are $x = 3$ or 5. We also know that $\exp(U_2) = 1$, $\exp(U_4) = 2$ and $\exp(U_{2^a}) = 2^{a-2}$ for $a \geq 3$. Hence the possibilities among powers of 2 are $2, 4, 8$ and 16.

Therefore, $\exp(U_n) = 4 \iff n$ is a product of prime powers chosen from $3, 5, 2, 4, 8, 16$, where we can pick at most one power for each prime and we must pick 5 and 16 (or both), as these are the only prime powers whose unit group has exponent 4.

Thus, there are 12 possibilities for n:

$$5,\ 5{\cdot}2,\ 5{\cdot}2^2,\ 5{\cdot}2^3,\ 5{\cdot}2^4,\ 5{\cdot}3,\ 5{\cdot}3{\cdot}2,\ 5{\cdot}3{\cdot}2^2,\ 5{\cdot}3{\cdot}2^3,\ 5{\cdot}3{\cdot}2^4,\ 2^4,\ 3{\cdot}2^4.$$