Homework #6. Solutions to selected problems.

3. Let $G_1, \ldots, G_k$ be finite groups.

(a) Prove that if each G_i is abelian, then

$$o_{max}(G_1 \times \ldots \times G_k) = lcm(o_{max}(G_1), \ldots, o_{max}(G_k)),$$

where as before $o_{max}(G) = \max\{o(g) : g \in G\}$. State clearly how you use that G_i are abelian.

(b) Give an example showing that assertion of (a) maybe false without the assumption that G_i are abelian.

Solution: (a) Let $G = G_1 \times \ldots \times G_k$. Consider an arbitrary element $g = (g_1, \ldots, g_k) \in G$. An easy computation shows that $o(g) = lcm(o(g_1), \ldots, o(g_k))$. Since each G_i is abelian, by Problem 3(d) in HW#4, $o(g_i)$ divides $o_{max}(G_i)$. Hence $o(g) = lcm(o(g_1), \ldots, o(g_k))$ divides $lcm(o_{max}(G_1), \ldots, o_{max}(G_k))$; in particular, $o(g) \leq lcm(o_{max}(G_1), \ldots, o_{max}(G_k))$. Since this is true for any $g \in G$, we get $o_{max}(G) \leq lcm(o_{max}(G_1), \ldots, o_{max}(G_k))$.

The opposite inequality $lcm(o_{max}(G_1), \ldots, o_{max}(G_k)) \leq o_{max}(G)$ is even easier to prove and does not use the fact that G_i's are abelian. Indeed, for each i choose $g_i \in G_i$ with $o(g_i) = o_{max}(G_i)$. Then as before

$$lcm(o_{max}(G_1), \ldots, o_{max}(G_k)) = lcm(o(g_1), \ldots, o(g_k)) = o((g_1, \ldots, g_k)) \leq o_{max}(G).$$

(b) Let $k = 2$ and $G_1 = G_2 = S_3$, the symmetric group on 3 elements $\{1, 2, 3\}$. The possible orders of elements of S_3 are 1,2,3 (and all of them do occur), so $o_{max}(S_3) = 3$ and hence $lcm(o_{max}(G_1), o_{max}(G_2)) = 3$. On the other hand, if g_1 is an element of G_1 of order 3 and g_2 is an element of G_2 of order 2, then $o((g_1, g_2)) = lcm(3, 2) = 6$; in particular, $o_{max}(G_1 \times G_2) \geq 6$ (in fact, it is easy to see that $o_{max}(G_1 \times G_2) = 6$).

4. Prove that the equation

$$x_1^{11} + x_2^{11} + \ldots + x_{10}^{11} = 230000000000011$$

has no integer solutions. **Hint:** reduce modulo a suitable prime.

Solution: By Fermat's little theorem, for any prime p and any x with $p \nmid x$ we have $x^{p-1} \equiv 1 \mod p$, so $(x^{(p-1)/2})^2 \equiv 1 \mod p$, and therefore $x^{(p-1)/2} \equiv \pm 1 \mod p$. And if $p \mid x$, then of course $x^{(p-1)/2} \equiv 0 \mod p$.

Observing that $11 = (23-1)/2$, we reduce both sides of the original equation mod $p = 23$. The right-hand side is clearly congruent to 11. On the other hand, as shown above, $x^{11} \equiv 0$ or ± 1 mod 23 for any x, so the left-hand side is congruent to c for some $-10 \leq c \leq 10$. None of the numbers in this interval is congruent to 11 mod 23, so we reached a contradiction.

5. Find the smallest positive integer m such that

$$x^m \equiv 1 \mod 120 \text{ for all } x \text{ which are coprime to 120.}$$

Note that $120 = 3 \cdot 5 \cdot 8$.

Solution: We can immediately reformulate the problem in terms of unit groups: find the smallest integer m such that $g^m = e$ for all $g \in U_{120}$. We claim that $m = o_{max}(U_{120})$. The inequality $m \geq o_{max}(U_{120})$ is clear; on the other hand, since U_{120} is abelian, by Problem 3(d) in HW#4, $g^{o_{max}(U_{120})} = e$ for all $g \in U_{120}$, so $m \leq o_{max}(U_{120})$.

Since $120 = 3 \cdot 5 \cdot 8$, we have $U_{120} \cong U_3 \times U_5 \times U_8$, so by Problem 3, $o_{max}(U_{120}) = lcm(o_{max}(U_3), o_{max}(U_5), o_{max}(U_8))$. The groups U_3 and U_5 have orders $3-1=2$ and $5-1=4$, respectively, and as we explicitly checked in class, $g^2 = e$ for all $g \in U_8$, so $o_{max}(U_8) = 2$. Therefore, $m = o_{max}(U_{120}) = lcm(2,4,2) = 4$.

We shall also give a different solution, which is more ad hoc, but does not use any results about the quantity o_{max}. Indeed, as above, the equality $g^4 = e$ identically holds in each of the groups U_3, U_5, U_8, hence it also holds in their direct product $U_3 \times U_5 \times U_8 \cong U_{120}$. Therefore, $m \leq 4$.

On the other hand, since 7 is coprime to 1, and none of the numbers $7, 7^2 = 49$ and $7^3 = 343$ is congruent to 1 mod 120, we have $m > 3$. Therefore, $m = 4$.

6. Let p be an odd prime and a a (fixed) integer not divisible by p. Find the number of solutions mod p^3 to the following congruence

$$x^3 - a^2x^2 + p^2 \equiv 0 \mod p^3.$$

Solution: Let $f(x) = x^3 - a^2x^2 + p^2$. We start by solving the congruence $f(x) \equiv 0 \mod p$. We get $p \mid (x^3 - a^2x^2) = x^2(x - a^2)$, so $p \mid x$ or $p \mid (x - a^2)$; equivalently, $x \equiv 0$ or a^2 mod p. To determine possible lifts of these solutions, we evaluate $f'(0)$ and $f'(a^2)$.

We have $f'(x) = 3x^2 - 2a^2x$, so $f'(a^2) = 3a^4 - 2a^4 = a^4 \not\equiv 0 \mod p$ since $p \nmid a$. Thus, by Hensel's lemma, $x = a^2$ lifts to unique mod p^k solution to $f(x) \equiv 0 \mod p^k$ for any k; in particular, this is true for $k = 3$.

On the other hand, $f'(0) = 0$, so the lifting theorem is not applicable in this case, and we have to analyze potential solutions of the form $x \equiv 0 \mod p$ (or equivalently, $x = pk$) directly. Rather than starting with solving $f(x) \equiv 0 \mod p^2$, we plug in $x = pk$ directly into the congruence $f(x) \equiv 0 \mod p^3$.

We get $(pk)^3 - a^2(pk)^2 + p^2 \equiv 0 \mod p^3$. This simplifies to $(ak)^2 \equiv 1 \mod p$, which is equivalent to $ak \equiv \pm 1 \mod p$. Since $gcd(a, p) = 1$, each of the congruences $ak \equiv 1 \mod p$ and $ak \equiv -1 \mod p$ has unique solution mod p, call them k_0 and k_1; hence an arbitrary solution has the form $k = k_1 + pn$ or $k = k_2 + pn$ with $n \in \mathbb{Z}$. Moreover, $k_1 \not\equiv k_2 \mod p$ since $a(k_1 - k_2) = ak_1 - ak_2 \equiv 1 - (-1) = 2 \mod p$ and p is odd, so these two families are distinct.

The corresponding solutions to $f(x) \equiv 0 \mod p^3$ are $x = pk_1 + p^2n$ and $x = pk_2 + p^2n$. We may be tempted to say that there are two non-congruent solutions (namely pk_1 and pk_2), but not that these are the only solutions mod p^2 (not mod p^3). The number of mod p^3 solutions is equal to $2p$ (explicitly, solutions to $f(x) \equiv 0 \mod p^3$ which are pairwise non-congruent mod p^3 are $pk_1, pk_1 + p^2, \ldots, pk_1 + (p-1)p^2$, $pk_2, pk_2 + p^2, \ldots, pk_2 + (p-1)p^2$).

Thus, the number of mod p^3 solutions to $f(x) \equiv 0 \mod p^3$ satisfying $x \equiv 0 \mod p$ is equal to $2p$. Therefore, the total number of mod p^3 solutions to $f(x) \equiv 0 \mod p^3$ is equal to $2p + 1$.