Selected Solutions to HW 4:

[2.23] We have

$$\frac{|G|}{|P|} = \frac{|N|}{|P \cap N|} \frac{|G||P \cap N|}{|N||P|}.$$

Since $NP/N \cong P/P \cap N$, we have $|NP|/|N| = |P|/|P \cap N|$. Therefore

$$\frac{|G|}{|P|} = \frac{|N|}{|P \cap N|} \frac{|G|}{|NP|}.$$

In other words,

$$[G : P] = [N : P \cap N][G : NP].$$

All quantities in the last equation are integers and since p does not divide $[G : P]$, it cannot divide $[N : P \cap N]$. Hence $P \cap N$ is a p-Sylow subgroup of N.

The formula $|NP| = |N||P|$ is false: use $G = N = P = \mathbb{Z}_2$ under addition.

The formula $|NP| = \operatorname{lcm}(|N|, |P|)$ is true. Proof: Write $P = p^\alpha$, $|N| = p^\beta q$ where $\gcd(p, q) = 1$, and $|P \cap N| = p^\beta$ (which has to be the case because we proved above that $P \cap N$ is a p-Sylow subgroup of N). Since $P \cap N$ is a subgroup of P, $p^\beta | p^\alpha$, therefore $\alpha \geq \beta$. This implies $\operatorname{lcm}(|N|, |P|) = p^\alpha q$. On the other hand, by the formula above,

$$|NP| = (|P|/|P \cap N|)|N| = (p^\alpha/p^\beta)p^\beta q = p^\alpha q.$$

Hence $|NP| = p^\alpha q = \operatorname{lcm}(|N|, |P|)$.

Note: this proof of this formula depends in first establishing that $P \cap N$ is normal in N, so we cannot use the formula until we establish this fact.

3.1. The largest order of an element in $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ is $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. Proof: clearly, when you raise any element $(a_1, \ldots, a_k)$ to this order, you obtain $(\widehat{0}, \ldots, \widehat{0})$. Hence the largest order is $\leq \operatorname{lcm}(n_1, n_2, \ldots, n_k)$. On the other hand, $(\widehat{1}, \ldots, \widehat{1})$ has order $\operatorname{lcm}(n_1, \ldots, n_k)$ in a calculation very similar to the one on Exam 1, so this is the largest order. Using this one can quickly compute the largest order of each abelian group of order 72.

3.11. Technical point: there is nothing in the textbook to rule out the group $G = \langle e \rangle$ to be both simple and solvable. So we will assume without loss of generality that $|G| \geq 2$. Since G is solvable, it has a solvable series

$$\langle e \rangle = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G,$$

where we are assuming that no two subgroups in this series are equal. Since $H_{n-1} \lhd G$, by simplicity of G we must have $H_{n-1} = \langle e \rangle$. Therefore $G/\langle e \rangle$ is abelian, hence G is abelian. Now let $g \neq e$ be given in G. Then $\langle g \rangle$ is a non-trivial normal subgroup of G, so by simplicity $\langle g \rangle = G$. Hence G is cyclic. If $o(g) = \infty$ then $\langle g^2 \rangle$ is a proper normal subgroup of G since it doesn't contain g (if it did then $g = g^{2k}$ for some integer k, which implies that $g^{2k-1} = e$, which implies that $o(g)$ is finite, a contradiction). Therefore $o(g) = n$ for some positive integer n and $G \cong \mathbb{Z}_n$. If $n = ab$ is a non-trivial factorization of n then g^a has order b, which would make $\langle g^a \rangle$ a non-trivial proper normal subgroup of G, violating simplicity. Therefore n is prime.