~~Sheet 7~~

Extra exercises 2

1) From the proof of the Chinese Remainder Theorem in the lectures it follows that the map $\bar{\Theta}: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$ given by $\bar{\Theta}([m]_{\equiv_n}) = ([m]_{\equiv_{n_1}}, \dots, [m]_{\equiv_{n_k}})$ is an isomorphism of groups. We want to describe the inverse $\bar{\Theta}^{-1}$ explicitly.
For $j \in \{1, \dots, k\}$ put $n_j' = \prod_{l \neq j} n_l$. Then $\gcd(n_j, n_j') = 1 \ \forall j \in \{1, \dots, k\}$.
For each $j \in \{1, \dots, k\}$ let $r_j, s_j \in \mathbb{Z}$ with $r_j n_j + s_j n_j' = 1$.
Then $\bar{\Theta}^{-1}([i_1]_{\equiv_{n_1}}, \dots, [i_k]_{\equiv_{n_k}}) = \left[\sum_{j=1}^{k} s_j n_j' i_j\right]_{\equiv_n}$.
Convince yourself that the above is all correct and that this enables you to solve systems of simultaneous congruences as mentioned in the lectures.

2) Show that any two Sylow p-subgroups P_1 and P_2 of a finite group G are conjugate, i.e. $P_2 = g P_1 g^{-1}$ for some $g \in G$.
Alternatively, find a proof in a book or on the internet and try to understand it.

3) Try to determine the structure of $\mathbb{Z}_n^\times$ in general, by writing it as a direct product of cyclic groups. Here you may use that for p a prime $\mathbb{Z}_p^\times$ is cyclic (this was not mentioned in the lectures).
Hint: Using the isomorphism from the Chinese Remainder Theorem you can reduce to the case that n is a power of a prime p. Show that $|\mathbb{Z}_{p^r}^\times| = p^r - p^{r-1} = p^{r-1}(p-1)$. Now distinguish the cases $p=2$ and $p>2$

Solutions can be obtained on request.