homework problems

1. Prove the lemmas 6, 7, and 8.
2. Prove the classical form of the Chinese Remainder Theorem, appearing as theorem 27.
   Deduce that $\mathbb{Z}_{13} \times \mathbb{Z}_{17}$ is cyclic (generated by one element). What is a generator for this group?
3. State and prove a formula for the number of r-cycles belonging to S_n.
4. Let p be a prime.
   (i) Using the binomial theorem (and not Fermat's theorem), prove that the function $\mathbb{Z}_p \to \mathbb{Z}_p$ specified by
   $$x \mapsto x^p$$
   is a homomorphism of the additive group $\mathbb{Z}_p$.
   (ii) Every non-zero element $c \in \mathbb{Z}_p$ corresponds to a function $\mathbb{Z}_p \to \mathbb{Z}_p$, multiplication by c:
   $$m_c(x) = cx$$
   Prove that m_c is an isomorphism of the additive group. (That is, $m_c \in \mathrm{Aut}(\mathbb{Z}_p)$. In fact, every $f \in \mathrm{Aut}(\mathbb{Z}_p)$ is of the form m_c for some $c \in \mathbb{Z}_p$.)
   Consider $\mathbb{Z}_{11}$. Note that $11 - 1 = 10 = 2 \cdot 5$.
   Find $c \in \mathbb{Z}_{11}$ such that m_c has order 5, so
   $$m_c \circ m_c \circ m_c \circ m_c \circ m_c = id$$
   Find $c \in \mathbb{Z}_{11}$ such that m_c has order 10.

5. Consult [Duzhin and Chebotarevsky], page 162.
For each of the crystallographic groups containing an element of order 3 (the five "hexagonal" ones), make a careful drawing of a figure with that symmetry group. On a separate diagram indicate all points of rotational symmetry, lines of reflective symmetry, and vectors generating all translational symmetries.
(Hint: Starting with any figure in the plane, the result of repeated application of all symmetries is a figure having at least the desired symmetry. Depending on the symmetry of the original figure, however, the result may have a strictly larger symmetry group!)

6. Prove theorem 57 (3): If a finite group G acts on a set X, the size of the orbit $O(x)$ of a given $x \in X$ and the size of the stabilizer subgroup $G_x \subset G$ are related by:

$$|O(x)| \cdot |G_x| = |G|$$

7. Use Euler's theorem to prove theorem 59:
If p and q are prime, and a and b are inverses mod $(p-1)(q-1)$, then

$$m \equiv c^a \bmod pq \Rightarrow c \equiv m^b \bmod pq$$

8. Prove proposition 63, that if $W \subset B^n$ is the subspace of codewords for a linear code, all words in a coset $u + W$ can be corrected with the same correction vector $e \in B^n$.

9. Give an explicit isomorphism $\mathrm{Aut}_+(\square) \to S_4$ by listing elements. Arrange them by conjugacy class

10. Prove that there is no isometry $\mathbb{R}^3 \to \mathbb{R}^3$ that puts the chiral symmetries of the cube and the symmetries of the tetrahedron into one-to-one correspondence.
(In fact, there is no invertible linear map $\mathbb{R}^3 \to \mathbb{R}^3$ accomplishing this; the two representations of S_4 are not isomorphic.)