Problem 1. Let p be a prime. Prove that every group of order p^2 is abelian. Hint: Use problem 2 of homework 35.

Solution: Let P be a group of order p^2. We proved that every $p-$group has non-trivial, so the center $Z(P)$ of P is not trivial. Thus $|Z(P)|$ is either p or p^2. In the latter case, we have $P = Z(P)$, so P is abelian. In the former case, $P/Z(P)$ is a group of order p. We know that groups of prime order p are cyclic, so $P/Z(P)$ is cyclic. By problem 2 of homework 35 P is abelian so $Z(P) = P$, a contradiction (which shows that the former case is not possible). Thus P is abelian.

Remark. It is not hard to show that P as above is either cyclic of order p^2 or is isomorphic to the product of two cyclic groups of order p.

Problem 2. Let G be a finite group of order pq, where $p < q$ are primes.

a) Show that G has a normal Sylow $q-$subgroup.

b) Suppose that $p \nmid (q-1)$. Prove that G has a normal Sylow $p-$subgroup.

c) Suppose that $p \nmid (q-1)$. Let P be the Sylow $p-$subgroup of G and let Q be the Sylow $q-$subgroup of G. Prove that elements of P commute with elements of Q (problem 3b) from Test III can be useful). Conclude that G is a cyclic group.

Solution: a) Recall that the number t_q of Sylow $q-$subgroups of G satisfies $t_q|p$ and $t_q \equiv 1 \pmod{q}$. If $t_q \neq 1$ then $t_q \geq q+1 > p$ which contradicts the condition $t_q|p$. Thus $t_q = 1$, i.e. G has normal Sylow $q-$subgroup Q.

b) As in a), we have $t_p|q$ and $t_p \equiv 1 \pmod{p}$. The first condition implies that $t_p = 1$ or $t_p = q$. The latter case implies that $q \equiv 1 \pmod{p}$, which is excluded by our assumption that $p \nmid (q-1)$. Thus $t_p = 1$ and G has normal Sylow $p-$subgroup P.

c) Note that the order of $P \cap Q$ divides both the order of P and the order of Q. Since these orders are relatively prime, we have $P \cap Q = \{e\}$. Since both P, Q are normal, problem 3b) from Test III says that elements from P and Q commute. Note that P has order p, hence it is cyclic, $P =< a >$. Similarly, Q has prime order q, so it is cyclic, $Q =< b >$. Now the order of a is p, the order of b is q and a commutes with b. It follows that the order of ab is pq (since $\gcd(p,q) = 1$, see Problem 1 of hemework 35). Thus $< ab >$ has order pq, so $< ab >= G$, i.e. G is cyclic.

Problem 3. This problem sketches a different proof of existence of Sylow $p-$subgroups. Let p be a prime. Let G be a finite group and suppose that every group of order smaller than $|G|$ has a Sylow $p-$subgroup (so this proof goes by induction on $|G|$). If $p \nmid |G|$, there is nothing to prove, so we assume that $p||G|$. We use the action of G on itself by conjugation. Recall that the stabilizer of an elementa $a \in G$ is simply its centralizer $C(a)$ (and orbits are the conjugacy classes). In particular, the fixed points of this action are the elements of the center $Z(G)$.

a) Prove that if $p \nmid |Z(G)|$ then there is a non-central element a whose conjugacy class has size not divisible by p. Then justify the following claims:

- $C(a)$ is a proper subgroup of G so it has a Sylow $p-$subgroup P;
- the index $[G : C(a)]$ is prime to p;
- P is a Sylow P subgroup of G.

b) Suppose that $p||Z(G)|$ and that $Z(G)$ has an element g of order p. Show that $Q =< g >$ is a normal subgroup of G of order p. Conisder the canonical homomorphism $f : G \longrightarrow G/Q$. Since $|G/Q| < |G|$, G/Q has a Sylow $p-$subgroup P. Prove that $f^{-1}(P)$ is a Sylow $p-$subgroup of G.

c) Suppose that $p||Z(G)|$ and $Z(G)$ has no elements of order p (we know that this is not possible by Cauchy's Theorem, but I do not want to use this theorem, since we proved it using Sylow Theorem). Let $a \in Z(G)$ be a non-trivial element. Show that $p \nmid | < a > |$. Show that $Z(G)/ < a >$ has no elements of order p. Since $|Z(G)/ < a > | < |G|$, $Z(G)/ < a >$ has a Sylow $p-$subgroup P. Show that P is non-trivial and has an element of order p, a contradiction.

Solution: a) Conjugacy classes are the orbits. Note that $Z(G)$ is the set of fixed points so $|Z(G)|$ is the number of fixed points. If every orbit had either size 1 or size divisible by p, then (since orbits partition G) we would have $|G| \equiv |Z(G)| \pmod{p}$, which is false (since $p||G|$ and $p \nmid |Z(G)|$). Thus there is $a \in G$ whose orbit, i.e. conjugacy class, has size bigger than 1 and not divisible by p. In particular, a is non-central.

Since $C(a)$ is the stabilizer of a and a is not a fixed point, $C(a)$ is a proper subgroup of G so $|C(a)| < |G|$. Thus $C(a)$ has a Sylow $p-$subgroup P. Recall that $[G : C(a)]$ is equal to the size of the orbit of a, so $p \nmid [G : C(a)]$. Since $|G| = |C(a)|[G : C(a)]$, we see that the highest power of p which divides $|G|$ is the same as the highest power of p which divides $|C(a)|$, which equals the order of P. Thus P is a Sylow $p-$subgroup of G.

b) Since $g \in Z(G)$ has order p, the group $Q =< g >$ has order p. Since Q is in the center, Q is normal in G (every subgroup of the center is normal, since conjugation is trivial on the center). Let $|G| = p^a m$, $p \nmid m$. Then $|G/Q| = p^{a-1}m$. Thus G/Q has a Sylow $p-$subgroup P and its order is p^{a-1}. Note that the canonical homomorphism $f : G \longrightarrow G/Q$ maps the group $R = f^{-1}(P)$ onto P. It follows that R/Q is isomorphic to P. Thus $|R| = |P||Q| = p^{a-1}p = p^a$. It follows that $f^{-1}(P) = R$ is a Sylow $p-$subgroup of G.

c) Suppose that $p|| < a > |$. Then the order of a is pk for some k and the order of a^k is p, contrary to our assumption that $Z(G)$ has no elements of order p. This proves that no element of $Z(G)$ has order divisibleby p. Recall now that if f is a homomorphism of groups than the order of $f(g)$ divides the order of g for all g (see Problem 1 c) of homework 35). Applying this to the canonical homomorphism $f : Z(G) \longrightarrow Z(G)/ < a >$ (which is surjective), we see that $Z(G)/ < a >$ has no elements of order divisible by p. In fact, if p divides the order of $x \in Z(G)/ < a >$, then $x = f(y)$ for some $y \in Z(G)$ and p divides the order of y, a contradiction. On the other hand, since $p \nmid | < a > |$ and $p||Z(G)|$ we see that p divides the order of $Z(G)/ < a >$. Since $|Z(G)/ < a > | < |G|$, $Z(G)/ < a >$ has a non-trivial Sylow $p-$subgroup P. But every non-trivial element of P has $p-$power order, a contradiction. It follows that the assumptions of c) can not be realized.