Solutions to Homework 2

Math 600, Fall 2007

5. (10 pts) Let $[m,n]$ denote the least common multiple of m and n. By definition both m and n divide $[m,n]$, therefore $x^{[m,n]}y^{[m,n]} = 1$. Using $xy = yx$ we see $(xy)^{[m,n]} = x^{[m,n]}y^{[m,n]} = 1$, whence $|xy|$ divides $[m,n]$. Two counterexamples when $xy \neq yx$:

i) Consider the group S_3 and set $x = (1,2)$ and $y = (1,3)$ then $|x| = |y| = |xy| = 2$ but $xy = (1,2,3)$ has order 3.

ii) Consider the upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. Let G be the group of transformations of $\mathbb{H}$ generated by $x : z \mapsto \frac{-1}{z}$ and $y : z \mapsto \frac{-1}{z+1}$. We have $|x| = 2$ and $|y| = 3$ but $xy : z \mapsto z+1$ has infinite order. (G is known as the modular group)

Example when $|xy| \neq [m,n]$: Take $x = y$ and $|x|$ even. Then $|xy| = |x|/2$ and $[|x|,|y|] = |x|$

6. (10 pts) 2.3.21-23 : Let $\mathrm{ord}_p\, n$ denote the highest power of p that divides n and let $\binom{n}{k}$ denote the binomial coefficient. The function ord_p extends naturally to rational numbers. We derive the following elementary formula:

$$\mathrm{ord}_p \binom{p^m}{k} = m - \mathrm{ord}_p k \quad \text{for } \ 1 \leq k \leq p^m$$

Writing $\binom{p^m}{k} = \frac{p^m \prod_{j=1}^{k-1}(p^m - j)}{k \prod_{j=1}^{k-1} j}$, and observing that $\mathrm{ord}_p\, j = \mathrm{ord}_p\,(p^m - j)$, we see that the ratio of the product terms is free of p, and so $\mathrm{ord}_p \binom{p^m}{k} = \mathrm{ord}_p \frac{p^m}{k}$ Using this formula, we get:

$$\mathrm{ord}_p\, p^k \binom{p^{n-1}}{k} = n + [k - 1 - \mathrm{ord}_p k] \tag{1}$$

$$\mathrm{ord}_p\, p^k \binom{p^{n-2}}{k} = n + [k - 2 - \mathrm{ord}_p k] \tag{2}$$

$$\mathrm{ord}_2\, 2^{2k} \binom{2^{n-2}}{k} = n + [2k - 2 - \mathrm{ord}_2 k] \tag{3}$$

$$\mathrm{ord}_2\, 2^{2k} \binom{2^{n-3}}{k} = n + [2k - 3 - \mathrm{ord}_2 k] \tag{4}$$

We assume $p \neq 2$ below. The expression in the square bracket in equations (1)-(4), are all non-negative with the exceptions of equations (2) and (4) for $k = 1$. This allows us to conclude:

$$\begin{aligned} (1+p)^{p^{n-1}} &\equiv 1 \pmod{p^n} \\ (1+p)^{p^{n-2}} &\not\equiv 1 \pmod{p^n} \\ (1+2^2)^{2^{n-2}} &\equiv 1 \pmod{2^n} \\ (1+2^2)^{2^{n-3}} \equiv 1+2^{n-1} &\not\equiv 1 \pmod{2^n} \end{aligned}$$

Therefore we deduce that:
(Problem 2.3.21) i) $1+p$ has order p^{n-1} in $(\mathbb{Z}/p^n\mathbb{Z})^\times$
(Problem 2.3.22) ii) the order of 5 in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is 2^{n-2}, when $n \geq 3$

Now, we answer **Problem 2.3.23**: We observe that if $\langle x \rangle$ is a cyclic group then, $x^{|x|/2}$ is the unique element of order two (if it exists). Applying this to $\langle 5 \rangle \subset G \stackrel{\text{def}}{=} (\mathbb{Z}/2^n\mathbb{Z})^\times$ we see that $5^{2^{n-3}}$ has order two in G. Thus, if G were cyclic then there would be no other element of order two in G. But, -1 has order two and is not identical to $5^{2^{n-3}}$ in G, because $5^{2^{n-3}} \not\equiv -1 \pmod 4$. This shows that G is not cyclic, when $n \geq 3$. [G has 3 elements of order 2 namely -1, $5^{2^{n-3}} = 2^{n-1}+1$ and $-5^{2^{n-3}} = 2^{n-1}-1$]

7. (10 pts) 2.3.25-26: Consider a finite cyclic group $\langle x \rangle$ and let $(k, |x|) = 1$, then we have $\langle x^k \rangle = \langle x \rangle$, therefore x is a k^{th} power. Now, let G be a finite group, and $\langle x \rangle$ a cyclic subgroup. Let $(k, n) = 1$ where $n = |G|$. By Lagrange's theorem $(k, n) = 1$ implies $(k, |x|) = 1$. Thus x is a k^{th} power. Since $x \in G$ was arbitrary we have shown that the map from g to itself given by $x \mapsto x^k$ is surjective.

Problem 2.3.26: Let g be a generator of the cyclic group Z_n. It is clear that $\sigma_a : Z_n \to Z_n$ is a group homomorphisms (because $\sigma_a(g^i g^j) = g^{a(i+j)} = \sigma_a(g^i)\sigma_a(g^j)$). Moreover, we observe that any homomorphism $\sigma : Z_n \to Z_n$ is equal to σ_a where a is determined by $\sigma(g) = g^a$. The kernel of σ_a is $\langle g^{n/(n,a)} \rangle$, thus we have proved (a) σ_a is an automorphism iff $(n, a) = 1$. (b) Next, $\sigma_a = \sigma_b$ iff they agree on the generator g, i.e., iff $a \equiv b \pmod n$. (c) We have already observed that any homomorphism of Z_n is given by σ_a, whence every automorphism is given by σ_a with $(a, n) = 1$. (d) $\sigma_a \circ \sigma_b$ sends g to g^{ab} whence $\sigma_a \circ \sigma_b = \sigma_{ab}$. Therefore we have a homomorphism $\Phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \text{Aut}(Z_n)$ given by $\Phi(a) = \sigma_a$. We have already shown in parts (b) and (c) that Φ is injective and surjective respectively.

9. (10 pts) a) We have $\phi : G \to \text{Perm}(G/H)$. An element $g \in G$ fixes a coset xH iff $g \in xHx^{-1}$ whence

$$\text{Ker}(\phi) = \bigcap_{x \in G} xHx^{-1}$$

(b) If $[\text{G} : \text{H}] = n$, then $\text{Perm}(G/H)$ is isomorphic to the symmetric group S_n. We have, $[\text{G} : \text{Ker}(\phi)] = |\text{im}(\phi))|$ and $\text{im}(\phi)$ being (isomorphic to) a subgroup of S_n has order dividing $n!$ Thus the normal subgroup $\text{Ker}(\phi) \subset G$ has index dividing $n!$
(c) Let $[\text{G} : \text{H}] = \text{r} > 1$, then $\text{Ker}(\phi)$ as defined in (a) is trivial, hence G is isomorphic to a subgroup of S_r, whence $|G|$ divides $r!$
(d)If G is simple and $|G| = 60$, by part (c) we have $60 \,|\, r!$ This needs $r \geq 5$ which is the same as $|H| \leq 12$.

10. (10 pts) We recall that when a group H acts on a set Y, the sum of the cardinalities of the H-orbits is the cardinality of Y. We will consider the orbits of X under the action of the subgroups $P_x \subset G$. The cardinality of such an orbit is either 1 or a power of p. Consider the P_x orbits of the set O_x: the P_x orbit of x is a singleton. Consider a P_x orbit of O_x different from the orbit of x, this will be the P_x orbit of gx for some $g \notin G_x$. This orbit cannot be a singleton, for then P_x would fix two distinct elements x and gx. Thus we have shown that $|O_x| \equiv 1 \pmod{p}$.
Suppose there is a $y \notin O_x$, then no P_y orbit of $gx \in O_x$ is a singleton, for otherwise P_y would fix two distinct elements y and gx. Thus $|O_x| \equiv 0 \pmod{p}$. This contradiction shows that there is no such y, which means $O_x = X$, or G acts transitively on X.