Groups and Group Actions, Sheet 4, HT18

Modular Arithmetic. Cosets and Lagrange's Theorem. Applications.

1. (i) Let x, n be integers with $n \geqslant 2$ and n not dividing x. Show that the order $\mathrm{o}(\bar{x})$ of $\bar{x} \in \mathbb{Z}_n$ is

$$\mathrm{o}(\bar{x}) = \frac{n}{\mathrm{hcf}(x,n)}.$$

(ii) Let G, H be finite groups with $g \in G$ and $h \in H$. Show that the order of (g,h) in $G \times H$ is given by

$$\mathrm{o}\left((g,h)\right) = \mathrm{lcm}\left\{\mathrm{o}\left(g\right), \mathrm{o}\left(h\right)\right\}.$$

2. $\bar{x} \in \mathbb{Z}_n$ is said to be a *unit* if there exists $\bar{y} \in \mathbb{Z}_n$ such that $\bar{x}\bar{y} = \bar{1} \pmod{n}$.
(i) Show that the units of $\mathbb{Z}_n$ form a group under multiplication. We denote this group $\mathbb{Z}_n^*$.
(ii) Use Bézout's Lemma to show that $\bar{x}$ is a unit of $\mathbb{Z}_n$ if and only if $\mathrm{hcf}(x,n) = 1$.
(iii) List the units in $\mathbb{Z}_9$ and write out the Cayley table for $\mathbb{Z}_9^*$.
(iv) Show that $\mathbb{Z}_9^*$ is cyclic. What are the generators of $\mathbb{Z}_9^*$?

3. (i) Use Fermat's Little Theorem to compute $5^{15} \pmod{7}$ and $7^{13} \pmod{11}$.
(ii) Use the Fermat-Euler Theorem to compute $4^{43} \pmod{15}$ and $2^{51} \pmod{21}$.
(iii) Show that $5^{14} = 10 \pmod{15}$. [You might try to find 5^{14} modulo 3 and modulo 5 first.]

4. Let p be a prime and let g, h be elements, both of order p, in a group G. What are the possible orders of $\langle g \rangle \cap \langle h \rangle$?

Show that if G is finite then the number of elements of order p in G is a multiple of $p-1$.

Deduce that a group of order 35 contains an element of order 5 and an element of order 7.

5. Suppose that every element x in a group G satisfies $x^2 = e$. Prove that G is Abelian.

Show also that if H is any subgroup of G and $g \in G \backslash H$ then $K = H \cup gH$ is a subgroup of G.

Show further that K is isomorphic to $H \times C_2$.

Deduce that if G is finite then G is isomorphic to $(\mathbb{Z}_2)^n$ for some non-negative integer n.

6. Let G_1 and G_2 be finite groups and let $K \leqslant G_1 \times G_2$.

(i) Set $H_1 = \{g \in G_1 : (g,e) \in K\}$ and $H_2 = \{g \in G_2 : (e,g) \in K\}$. Show that

$$H_1 \leqslant G_1; \qquad H_2 \leqslant G_2; \qquad H_1 \times H_2 \leqslant K.$$

(ii) Suppose that $|G_1|$ and $|G_2|$ are coprime. Show that $K = H_1 \times H_2$.

(iii) Show that this result need not follow if $|G_1|$ and $|G_2|$ are not coprime.