MATH1022, INTRODUCTORY GROUP THEORY
Question Sheet 4: Cosets, Lagrange's Theorem, Wilson's Theorem

To be handed in by Friday 16th March

Q1. Find all the right cosets of the subgroup $H := \{1, 4, 13, 16\}$ of $\mathbb{Z}_{17}^*$, the group of units of $\mathbb{Z}_{17}$ (under $\times$ mod 17).

Q2. Find the right cosets of the subgroup $\{I, a^2\}$ of Q, the quaternion group (defined in the lectures as $\{I, a, a^2, a^3, b, ab, a^2b, a^3b\}$ where $a^4 = I$, $b^2 = a^2$, $ba = a^3b$).

Q3. Prove that a finite group of composite order contains a proper non-trivial subgroup. (Note that a subgroup is *non-trivial* if it is not just $\{e\}$, the identity subgroup, and it is *proper* if it is not G.)
Hint: Consider the possibilities for a subgroup generated by an element not equal to the identity. A *composite* integer is an integer which is greater than 1 and not prime.

Q4. (a) By considering the smallest non-zero element of a subgroup, find all subgroups of $G := \mathbb{Z}_8$ under + mod 8. First list all the subgroups, then write out your proof that all the subgroups are in your list formally, starting: Let H be a subgroup of $\mathbb{Z}_8$..... Answers considering all possible subsets of $\mathbb{Z}_8$ and checking one-by-one which are subgroups and which are not are not acceptable.
Determine the right cosets of the subgroup $H := \{0, 4\}$ of $\mathbb{Z}_8$.
Hint: the operation in this group is addition, so the right cosets are of the form $H + x$ for $x \in G$.

Q5. Let G be a group of order 105 and H a subgroup of G. Show that if $|H| \geq 36$ then $H = G$, stating clearly any results that you use.

Q6. Let G be a group, and H a subgroup of G. For $x, y \in G$, let us write $x \sim y$ if $xy^{-1} \in H$. Show that:
(i) For all $x \in G$, $x \sim x$.
(ii) For all $x, y \in G$, $x \sim y$ implies $y \sim x$.
(iii) For all $x, y, z \in G$, $x \sim y$ and $y \sim z$ implies $x \sim z$.

Remark: We say that $\sim$ is an *equivalence relation* on H, as it satisfies (i), (ii) and (iii). We shall look at these again later in the course.

Q7. Let p be a prime number, and let G be the group $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ under $\times$ mod p. Show that $p-1$ is the only element of G of order 2. Deduce that all elements of G apart from 1 and $p-1$ come in pairs a, b such that b is the inverse of a in G. By using this, and multiplying together all group elements, prove 'Wilson's Theorem', that $(p-1)! + 1 \equiv 0 \bmod p$.

MATH1022, INTRODUCTORY GROUP THEORY
Tutorial Exercises 4: Cosets, Lagrange's Theorem, Wilson's Theorem

To be discussed in the tutorial in the week 12 March – 16 March

T1. Find all the right cosets of the subgroup $H := \{1, 7\}$ of $\mathbb{Z}_{16}^*$, the group of units of $\mathbb{Z}_{16}$ (under $\times$ mod 16).

T2. Find the right cosets of the subgroup $\{I, H\}$ of D_4, the group of symmetries of a square (considered in Question 2 on Question Sheet 1).

T3. Prove that if A and B are finite subgroups of a group G whose orders are coprime, then $A \cap B = \{e\}$.

T4. (a) By considering the smallest non-zero element of a subgroup, find all subgroups of $G := \mathbb{Z}_6$ under $+$ mod 6. First list all the subgroups, then write out your proof that all the subgroups are in your list formally, starting: Let H be a subgroup of $\mathbb{Z}_6$..... Answers considering all possible subsets of $\mathbb{Z}_6$ and checking one-by-one which are subgroups and which are not are not acceptable.
Determine the right cosets of the subgroup $H := \{0, 3\}$ of $\mathbb{Z}_6$.
Hint: the operation in this group is addition, so the right cosets are of the form $H + x$ for $x \in G$.

T5. Let H be a subgroup of the symmetric group S_4. Prove that if $|H| > 8$ then $|H| \geq 12$, stating clearly any results that you use.

T6. Let G be a group and H a subgroup of G. A *left coset* of G is a subset of G of the form $xH = \{xh : h \in H\}$, where $x \in G$. Prove that, for $x, y \in G$, $xH = yH$ if and only if $x^{-1}y \in H$.

T7. Show that if $n \in \mathbb{N}$, $n > 1$ is composite and $n \neq 4$ then $(n-1)! \equiv 0 \bmod n$. Verify that $(4-1)! \equiv 2 \bmod 4$. Conclude that $(n-1)! + 1 \not\equiv 0 \bmod n$.
Remark: See Question Q3 overleaf for the definition of composite. The contrapositive of the statement shown here is that for integers greater than 1, if $(n-1)! + 1 \equiv 0 \bmod n$ then n is prime. We have therefore shown that the converse of Wilson's Theorem (see Q7 overleaf) is true.