MAT 312/AMS 351
Applied Abstract Algebra
Midterm 2 – Solutions

1. (15 points) A toy public-key code is constructed with the public "unfactorable" number $n = 55$ and the exponent $e = 9$. A number a is encoded as 4. What was a?

   The Euler ϕ-function of 55 is $\phi(55) = \phi(5 \cdot 11) = 4 \cdot 10 = 40$. To decode, we calculate the multiplicative inverse of the exponent mod 40.

   $$40 = 4 \times 9 + 4$$

   $$9 = 2 \times 4 + 1$$

   gives

   $$1 = 9 - 2 \times 4 = 9 - 2(40 - 4 \times 9) = 9 \times 9 - 2 \times 40$$

   so the multiplicative inverse of 9 mod 40 is 9.

   The next step is to raise the received word 4 to the power 9, mod 55

   $$4^3 = 64 \equiv 9 \text{ mod } 55$$

   $$4^6 = 4^3 \cdot 4^3 \equiv 81 \equiv 26 \text{ mod } 55$$

   $$4^9 = 4^6 \cdot 4^3 = 234 \equiv 14 \text{ mod } 55$$

   so 14 was the word transmitted.

2. Consider the group G_9 of invertibles *mod* 9. It has $\phi(9) = 6$ elements.

   (a) (15 points) Show that G_9 is cyclic of order 6, by constructing an explicit isomorphism $\varphi : \mathbf{Z}_6 \to G_9$. ($\varphi$ will have to take sums to products).

   Consider the powers of the elements $1, 2, 4, 5, 7, 8$ in G_9.
   1 has order 1

   $$2^1 = 2 \;\; 2^2 = 4 \;\; 2^3 = 8 \;\; 2^4 = 7 \;\; 2^5 = 5 \;\; 2^6 = 1$$

   $$4^1 = 4 \;\; 4^2 = 7 \;\; 4^3 = 1$$

   $$5^1 = 5 \;\; 5^2 = 7 \;\; 5^3 = 8 \;\; 5^4 = 4 \;\; 5^5 = 2 \;\; 5^6 = 1$$

   $$7^1 = 7 \;\; 7^2 = 4 \;\; 7^3 = 1$$

   $$8^1 = 8 \;\; 8^2 = 1$$

   Since exponents add in a multiplicative group, we can use $\varphi(k) = 2^k$ as an isomorphism: $\mathbf{Z}_6 \to G_9$.

   $$\varphi(0) = 1, \varphi(1) = 2, \varphi(2) = 4, \varphi(3) = 8, \varphi(4) = 7, \varphi(5) = 5.$$

(b) (10 points) Can this construction be done differently? I.e., is φ unique?

We can also use 5, the multiplicative inverse of 2 mod 9, as our generator:

$$\varphi(0) = 1, \varphi(1) = 5, \varphi(2) = 7, \varphi(3) = 8, \varphi(4) = 4, \varphi(5) = 2.$$

3. In the symmetric group $S(5)$ of permutations of 5 objects, consider the cyclic subgroup $\langle(15)(234)\rangle$ made up of the permutation $(15)(234)$ and all its powers.

(a) (10 points) List all the elements of $\langle(15)(234)\rangle$.

these are the identity e and all the powers of $(15)(234)$:

$$\begin{gathered}(15)(234)\\ (15)(234)(15)(234) = (243)\\ (243)(15)(234) = (15)\\ (15)(15)(234) = (234)\\ (234)(15)(234) = (15)(243)\end{gathered}$$

(b) (10 points) List all the elements of the left coset $(12345)\langle(15)(234)\rangle$.

These are the products of (12345) with the six elements listed above:

$$\begin{gathered}(12345)\\ (12345)(15)(234) = (2435)\\ (12345)(243) = (125)\\ (12345)(15) = (2345)\\ (12345)(234) = (12435)\\ (12345)(15)(243) = (25)\end{gathered}$$

4. (a) (10 points) What are the possible orders of elements in a group of order 27 (i.e. with 27 elements)?

The order of an element is the order of the cyclic subgroup it generates; this number must divide 27 (Lagrange's Theorem). The only possibilities are 1, 3, 9, 27.

(b) (10 points) Give an example of a group G of order 27 with no element of order 27.

Examples are $\mathbf{Z}_3 \times \mathbf{Z}_6$, $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$.

(c) (10 points) Can a group of order 27 have elements of order 9 but no elements of order 3?

No, because if $a^9 = 1$, then $(a^3)^3 = 1$. If an element has order 9, its cube has order 3.

5. (10 points) Show that a group of even order must have at least one element of order 2. *Hint:* consider the set of all elements which are not equal to their inverses.

Let S be the set of all elements which are not equal to their inverses (equivalently, the set of all elements which are *not* the identity, and *not* of order 2). Then each element of S other than the identity can be associated with another element of S namely, its inverse. Consequently the number of elements of S is an even number, plus one. This accounts for an odd number of elements; since the group has even order, there must be some elements which are not in S. These elements have order 2.