10/1/07 Fall 07, Intro to Modern Algebra I Test I Solutions Sitaraman

1. Prove by induction: The sum of the first n odd numbers for any n given by $1+3+\ldots+(2n-1)$ equals n^2.

We want to show that $1+3=2^2, 1+3+5=3^2, 1+3+5+7=4^2$ and so on.

Step 1: Showing it is true for $n=1$: We have $1=1^2$. So it is true for $n=1$.

Step 2: Assume it is true for $n=k$. So $1+3+\ldots+(2k-1)=k^2$.

Step 3: Use step 2 to prove for $n=k+1$. i.e, we need to show that $1+3+5+\ldots+(2(k+1)-1)=(k+1)^2$. We have $1+3+\ldots+(2k-1)+(2(k+1)-1)=(1+3+5+\ldots(2k-1))+(2k+1)$. But from Step 2, we have $1+2+\ldots+(2k-1)=k^2$. Plugging this into the above, we get $k^2+(2k+1)=k^2+2k+1=(k+1)^2$. So we have proved the statement for $k+1$.

2. Show that the relation $a \sim b$ if $a+b$ is even where a, b are integers is an equivalence relation on the set of integers, and describe the equivalence classes. What is the equivalence class of 0? How many equivalence classes are there?

Soln: The equivalence class of any integer n is all m such that $m+n$ is even. Thus, if m belongs to (0) – the equivalence class of 0 – then $m+0=m$ is even. Thus all even integers are in (0). Similarly, the equivalence class of 1 is all m such that $m+1$ is even which is true for all odd integers. So there are just two equivalence classes – the whole set of integers is divided into even and odd integers.

3. Find 12345678^6 mod 9 by using the divisibility test for 9 (same as used in the checksum procedure) and the fact that products of remainders are the same as remainders of products. (in this case, that helps you to find the remainder of the power by taking the power of the remainder).

$12345678 \equiv 1+2+3+\ldots+8=36 \equiv 0$ modulo 9. So $12345678^6 \equiv 0^6=0$ modulo 9.

4. Describe $U(20)$ and write the Cayley table for it. Read off the inverse of each element from the Cayley table.

Soln: U(20) consists of the integers relatively prime to 20 under multiplication mod 20. Thus we get 1,3,7,9,11,13,17,19, a set of eight

elements. The Cayley table is constructed by multiplying pairs mod 20. From the table, we can see that $1^{-1} = 1, 3^{-1} = 7$, (thus $7^{-1} = 3$) $9^{-1} = 9, 11^{-1} = 11, 13^{-1} = 17$, (thus $17^{-1} = 13$) $19^{-1} = 19$.

5. Prove that in any dihedral group D_n with $n \geq 3$, the rotation taking each vertex to its adjacent vertex (i.e, 1 to 2, 2 to 3, etc.,) does not commute with reflection through any of the diagonals. This shows that D_n is never commutative (or abelian).

Soln: This (as is problem 2) is from the exercises in the book. See the figure under problem 12 following chapter 1. It shows why the rotation and reflection through the vertex 1 don't comute. Since there is nothing special about the choice of 1, it is true for any such reflection.

6. Give an example of each of the following:

(a) An infinite group that is not commutative (Hint: matrices). (b) A finite group with more than 3 elements that is commutative (c) An element of finite order in an infinite group.

Soln: (a) The set of 2×2 matrices with non-zero determinant and real number entries is a group (note that same is true for integer entries – i.e, $GL(2, \mathbf{Z})$ is not a group because inverses may not be integer matrices . But $SL(2, \mathbf{Z})$ is a group because if det is 1, the inverses are integer matrices as well). This has an infinite number of elements in it, and it is non-commutative. For example, the matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ do not commute.

(b) The group $U(10)$ has four elements and it is abelian.

(c) The matrix A above has order 4, i.e, A^4 is the identity matrix in the group $GL(2, \mathbf{R})$ and the matrix B has order 2. A much simpler example is -1 in the group of positive real numbers under multiplication.

7. Show that the set of 2×2 matrices whose entries are from $\mathbf{Z}_5$ and the operation is matrix addition (modulo 5, of course) is a finite, abelian group. How many elements does it have?

Soln: Checking that it is a group is easy. Matrix addition results in elements in the same set, and it is associative. Inverses exist in $\mathbf{Z}_5$, so inverse of a matrix under addition is just the matrix whose entries are

inverses of the entries of the given matrix. Identity is the zero matrix with all entries zero. It is abelian because addition mod 5 is commutative. It has $5^4 = 625$ elements because there are 5 possibilities for each entry.

8. For any element g in any group G, show that the inverse of g^k is the same as $(g^{-1})^k$, where k is a positive integer.

Soln: We see that $g^k(g^{-1}.g^{-1}\ldots.g^{-1})$ (where g^{-1} is multiplied k times) reults in identity because the g^{-1} entries cancel the $g's$ successively. [This is just a special case of hw problem 20 from chapter 2, with all the elements a_i being equal to g.)