Solutions

Math 187 Test IV

Dr. Holmes

December 4, 2008

1:40 pm 2:35 pm

The examination begins at ~~9:40 am~~ and ends at ~~10:35 am.~~ You may use a plain scientific calculator without graphing or symbolic computation capabilities. Cell phones must be turned off and out of sight.

You may expect that the question on which you do worst on this exam will be dropped.

8

1. Compute 38 `div` 10 and 38 `mod` 10. (`div` is integer division and `mod` is remainder.) That was easy!

38 div 10 = 3

38 mod 10 = 8

Compute -38 `div` 10 and -38 `mod` 10. That should be slightly less obvious.

−38 div 10 = −4

−38 mod 10 = 2

2. Present the multiplication table for mod 5 arithmetic.

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3. (a) Compute gcd(11, 37). Express gcd(11,37) in the form $37x + 11y$.

$37 = 3 \cdot 11 + 4$ R 4 $= 37 - 3 \cdot 11$

$11 = 2 \cdot 4 + 3$ R 3 $= 11 - 2 \cdot 4$

$4 = 1 \cdot 3 + 1$ R 1 $= 4 - 3$

	x	y
37	1	0
11	0	1
4	1	-3
3	-2	7
1	3	-10

$1 = 37 \cdot 3 - 10 \cdot 11$

(b) Compute the reciprocal of 11 in arithmetic mod 37. Be careful about signs. This uses the work of the previous part!

reciprocal of 11 mod 37 is -10 or $\boxed{27}$

(c) Solve the equation

$$11x \equiv 7 \bmod 37.$$

$x \equiv 27 \cdot 7 \bmod 37$

$\equiv \boxed{4} \bmod 37$

4. Chinese Remainder Theorem

Find the smallest positive integer solution to the system of equations

$$x \equiv 5 \bmod 37$$

$$x \equiv 32 \bmod 42$$

What fact about 37 and 42 guarantees that there is a solution?

The fact is that $\gcd(37, 42) = 1$.

$x = 5 + 37k$ for some integer k

$5 + 37k \equiv 32 \bmod 42$

$37k \equiv 27 \bmod 42$

find $37^{-1} \bmod 42$

$25 \cdot 37k \equiv k \equiv 25 \cdot 27 \bmod 42$

$\equiv 3 \bmod 42$

so $x = 5 + 37k$

$= 5 + 37 \cdot 3 = 116$

$116 \bmod 37 = 5$

$116 \bmod 37 = 32$

as desired.

it is smallest -

$116 \bmod (37 * 42) = 116$. so -17 is reprolal of 37 mod 42, i.e. $42 - 17 = 25$

$42 = 1 \cdot 37 + 5$ R 5

$37 = 7 \cdot 5 + 2$ R 2

$5 = 2 \cdot 2 + 1$ R 1

	x	y
42	1	0
37	0	1
5	1	-1
2	-7	8
1	15	-17

5. Permutation notation

Let π be the permutation (13)(245) and σ be the permutation (2354)(1).

Compute the composition $\pi \circ \sigma$ in table notation, then present it in cycle notation. Credit will be reduced if you compute $\sigma \circ \pi$ instead: be careful.

π ∘ σ

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$$

(132)(4)(5) in cycle notation

6. A specific group.

(a) Present the group table for $(\mathbb{Z}_{10}, \otimes)$ (multiplication in mod 10 arithmetic restricted to numbers relatively prime to 10).

① 2 ③ 4 5 6 ⑦ 8 ⑨ 10

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(b) Identify the identity element of this group and the inverse of each element of the group.

identity is 1

$1^{-1} = 1$

$3^{-1} = 7$

$7^{-1} = 3$

$9^{-1} = 9$

(c) Find a generator for this group (show work indicating why it is a generator).

$3^2 = 9$ $3^3 = 9 \cdot 3 = 7$ $3^4 = 7 \cdot 3 = 1$

The "powers" of 3 are the whole group

7 is also a generator

(d) Present an isomorphism between this group and the addition group in mod 4 arithmetic (this will be a 1-to-1 correspondence between elements of the two groups). I remind you that the elements of the addition group in mod 4 arithmetic are 0,1,2,3.

$(\mathbb{Z}_4, +)$ $(\mathbb{Z}_{10}^*, \otimes)$

$0 \longleftrightarrow 1$

$1 \longleftrightarrow 3$

$2 \longleftrightarrow 9$

$3 \longleftrightarrow 7$

or

$0 \longleftrightarrow 1$

$1 \longleftrightarrow 7$

$2 \longleftrightarrow 9$

$3 \longleftrightarrow 3$

7. Complete the given partial group table. Write a brief explanation for why you placed each element (this can be quite informal): the format can be $a * b = c$ because... You are allowed to say things like "a given element can appear no more than once in a given column".

   Give a reason why this group is *not* isomorphic to mod 4 addition.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This is not isomorphic to mod 4 addition because all elements are their own inverse here and this is not the in mod 4 addition. Another observation is that this group has no generators

a * b = c because it can't be a or e (already found in row) or b (found in column)

a * c = b because all other elb are found in row already

b * a = because a, e appear in col with it and b appears in row with it

b * c = a because it's the only elt not in the row yet

c * a = b by process of elimination

c * b = a in column by process of elim in both row and column

8. The operation table for the group S_3 is given below. (next page)

(a) Compute the order of each element of the group (the order of a group element is the smallest "power" of that group element which gives the identity).

$a^1 = 1$ order of a is 1

$b^2 = c$ $b^3 = a$ order of b is 3

$c^2 = b$ $c^3 = a$ order of c is 3

$d^2 = e^2 = f^2 = a$

d, e, f are all order 2s

(b) Present a subgroup of each of the following sizes, or give a brief explanation of why there cannot be one: 1,2,3,4.

{a} is a subgroup of size 1

{a, d} is a subgroup of size 2

{a, b, c} is a subgroup of size 3

There cannot be a subgroup of size 4 because 4 is not a divisor of 6

(c) State a reason why this group is not isomorphic to the addition group of mod 6 arithmetic (there are several ways to see this; any one will do).

either works by itself

[The group is not commutative

[It has no order 6 element (so no analogue of 1 in mod 6 arithmetic)

order 1 order 6 order 3 order 2 order 3 order 1

0 1 2 3 4 5 totally different distribution of orders

0
1
2
3
4
5

*	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a