Math 305, Spring 2022, Test II

Dr. Holmes

April 6, 2022

This exam will be given on Thursday April 7, for the entire class period, 12-115 pm. At 115 I will actually give a five minute warning.

Do 10 of the following 12 questions to be assured of full credit.

You may bring and use a single sheet of notebook paper with whatever notes you want written on it. You may bring a non-graphing calculator, but I am not sure that there is any use for it.

1. Use Euler's theorem to determine the last decimal digit (i.e., the remainder mod 10) of $7^{5676545 28}$. Briefly explain your reasoning. Hint: you can compute $\phi(10)$ simply by inspecting the remainders mod 10.

$\cancel{0}$ 1 $\cancel{2}$ 3 $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ 9 $\quad \phi(10) = 4$

or $10 = 2 \cdot 5$

$\phi(10) = (2-1)(5-1) = 4$

$7^{587654528} \equiv_{10} 7^{587654528 \bmod 4} \equiv_{10} 7^{0} = 1$

2. Wilson's theorem asserts that for any prime p, $(p-1)! \equiv_p -1$. Prove that this is false if we do not assume that the modulus is prime, by showing that $(p-1)! \not\equiv_n -1$ if $n > 1$ is composite.

Suppose n is composite.

If $n = ab$ where $a \neq b$

then ~~$(p-1)!$ has a and b~~

the product $1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)$

includes both a, b as items so $(p-1)!$ is divisible by ab

$= n$ so $(p-1)! \equiv_n 0$.

~~If n~~ The only composite numbers which are not

~~so~~ ab for $a \neq b$ are of the form p^2, p a prime

If $n = 4$, $3! \bmod 4 = 2 \not\equiv_4 -1$

if $n = p^2$ for $p > 2$ then

the product $1 \cdot 2 \cdot 3 \cdots (p-1)(p-1) = (p-1)!$

includes both p and $2p$ as distinct items,

so ~~$n < p^2$~~ $(p-1)!$ is divisible by $p^2 = n$

so $(p-1)! \equiv_n 0$.

3. Show that if $a^2 = e$ for all elements of a group G, then G is abelian. Justify everything you do from the definition of a group.

~~Stuck~~

Let $a, b \in G$. We want to show $ab = ba$.

$(ab)^2 = abab = e$ by hypothesis

$a^2 b^2 = ee = e$ by hypothesis

Since $abab = aabb$, we also have

$a(abab)b = a(aabb)b$ ← using fact $aa = bb = e$

so $ba = ab$

4. List all the subgroups of $\mathbb{Z}_{12}$ [arithmetic mod 12 with addition as the operation] (listing all elements of each subgroup).

$\{0\}$

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$\{0, 2, 4, 6, 8, 10\}$

$\{0, 3, 6, 9\}$

$\{0, 4, 8\}$

$\{0, 6\}$

is a cyclic group, all of is subgroups are cyclic and the are the posibl[illegible]

5. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have? Explain why.

A generator of $\mathbb{Z}_n$ is an

m with $0 \le m < n$

and $\gcd(m, n) = 1$.

~~There are~~ ~~0 isn't a generator.~~

The positive remainders - there are $pq-1$ of them

$p-1$ of these are multiples of q

$q-1$ of these are multiples of p

$$(pq-1)-(p-1)-(q-1) = pq-1-p+1-q+1$$
$$= pq-p-q+1 = (p-1)(q-1)$$

6. Show that A_{10} contains an element of order 15 (there are two things to show: that there is an element of S_{10} of order 15, and that it belongs to A_{10}; you have to explain why these two things are true, not just present the permutation).

~~S_{10} (1 2 3)(4 5 6~~

$(1\,2\,3)(4\,5\,6\,7\,8)(9)(10)$

is of order 15. The order of a product of disjoint cycles is lcm of the orders, in this case relatively prime

as a product of transpositions

$(1\,3)(1\,2)(4\,8)(4\,7)(4\,6)(4\,5)$

a product of 6 transpositions so even so a member of A_{10}.

7. Find the left and right cosets of the cyclic subgroup generated by (12) in S_3.

The subgroup contains the identity and (12).

order 1, order 2, order 2, order 2, order 3, order 3

The group S_3 contains the identity, (12), (13), (23), (123) and (132).

Explain briefly why S_3 is not a cyclic group. (The explanation can be very brief!)

---

let $H = \{id, (12)\}$

$id\,H = (12)H = \{id, (12)\}$

$(13)H = \{(13)\,id, (13)(12)\}$
$= (123)H = \{(13), (123)\}$

$(23)H = \{(23), (23)(12)\}$
$= (132)H = \{(23), (132)\}$

three left cosets

$H\,id = H(12) = \{id, (12)\}$

$H(13) = \{id\,(13), (12)(13)\}$
$= H(132) = \{(13), (132)\}$

$H(23) = \{id\,(23), (12)(23)\}$
$= H(123) = \{(23), (123)\}$

three right cosets

notice, they are different

S_3 is not cyclic because it has no element of order 6. also, it is not abelian

8. Give multiplication tables for each of the groups $U(5), U(10), U(12)$.

   Show that $U(5)$ is isomorphic to $U(10)$ (exhibit an isomorphism, an actual bijection from $U(5)$ to $U(10)$ with the right properties), but $U(12)$ is not (hint: talk about orders of elements of the groups).

$U(5) = \{1\ 2\ 3\ 4\}$ with multiplication mod 5

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 3$
$2^4 = 1$

$U(10) = \{1\ 3\ 7\ 9\}$ with multiplication mod 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

$3^0 = 1$
$3^1 = 3$
$3^2 = 9$
$3^3 = 7$
$3^4 = 1$

both groups cyclic,
$\{(1,1), (2,3), (4,9), (3,7)\}$
is an isomorphism

$U(12) = \{1\ 5\ 7\ 11\}$ with mult mod 12

1 2 4 3
1 7 9 3

65

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

not isomorphic
because $U(12)$
contains no element
of order 4 —
$5^2 = 7^2 = 11^2 = 1$

9. Exhibit the possible isomorphism types of abelian groups of order 36.

   For each type, say what the highest possible order of an element of the group is (this will help you to see that the isomorphism types are all different).

$36 = 2 \cdot 2 \cdot 3 \cdot 3$

$\cancel{\mathbb{Z}_{36}}$ ← ~~largs order~~ 36

$\mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_9$ ← largest ~~order~~ ~~[illegible]~~ 36 actually the same!

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$ largs order 18

$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ largs order 12

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ largest order 6

so we can see that all are different.

by theorem these are the only possibilities

10. Show that the map sending each nonzero complex number $a+bi$ to $a-bi$ is an automorphism of $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication. An automorphism of the group G is an isomorphism from G to G. Reminder: this isn't just showing that the map is a bijection – you have to show its relation to the group operation, too.

~~let~~ ~~a+b~~

Let $f(a+bi) = a-bi$

if $f(a+bi) = f(c+di)$ then

$a-bi = c-di$

so $a=c$

and $-b=-d$

so $b=d$

so $a+bi = c+di$, one to one

for any $a+bi$, $f(a-bi) = \cancel{a+} \; a-(-b)i = a+bi$

so onto

AND

$f(a+bi)f(c+di) = (a-bi)(c-di) = ac - adi - bci - bd$

$= (ac-bd) - (ad+bc)i = f((ac-bd)+(ad+bc)i)$

$= f((a+bi)(c+di))$

11. Show that $\{id, (123), (132)\}$ is a normal subgroup of S_3 (very briefly say what the factor group is), and that $\{id, (12)\}$ is not.

A subgroup is normal if it has the same left cosets and right cosets.

left or right

$\{id\ (123)(132)\}$ can only have one other coset, $\{(12), (13), (23)\}$,

so it has the same left cosets as right cosets so it is normal. Factor group is isomorphic to $\mathbb{Z}_2$.

$\{id, (12)\}$ has different left cosets and right cosets, as we showed in another problem, so it is not normal.

12. Prove that each subgroup of a cyclic group is cyclic. This will use the well-ordering principle and the division algorithm from number theory.

Suppose G is a cyclic group and H is a subgroup of G.

Since G is cyclic, ~~every element~~

G has a generator a and every element of G

is of the form a^h for some $h \in \mathbb{Z}$.

So every element of H is of the form a^h for some $h \in \mathbb{Z}$,

Let h be the smallest positive integer such that $a^h \in H$.

~~Let $a^j \in H$. We want to show that j must be~~

We show that a^h generates H.

Suppose $a^j \in H$. Then $j = qh + r$ for some $q \in \mathbb{Z}$ and

r nonnegative and less than h.

$$a^j = a^{qh} a^r$$

$$a^{qh} = (a^h)^q \in H \text{ (a power of an element of } H)$$

so $a^r = (a^{qh})^{-1} a^j \in H$

but this means $r = 0$, because h is the smallest positive integer with $a^h \in H$, so j is a multiple of h, a^j is a power of a^h, and a^h generates H, so H is cyclic.