Math 417 Homework 1 Solutions Due Friday, September 4, 2020

1a. ($\mathcal{E}$) Compute $g = \gcd(12, 20)$ by the Euclidean algorithm and find integers r, s so that $g = 12r + 20s$.

Solution:

$$20 = 1 \cdot 12 + 8$$
$$12 = 1 \cdot 8 + 4$$
$$8 = 2 \cdot 4$$

Thus $gcd(12, 20) = 4$, so $g = 4$ and

$$4 = 12 - 8 = 12 - (20 - 12) = 2 \cdot 12 - 20.$$

so one solution is $r = 2, s = -1$. If this were Math 453, you'd learn that the complete solution over integers is $r = 2 + 5t, s = -(1 + 3t)$, $t \in \mathbb{Z}$.

1b. Let $G = C_{20} = \langle a \rangle$ be a cyclic group of order 20. Using your answer from 1a., or any correct method, compute the number of elements in $H = \langle a^{12} \rangle$, the subgroup of powers of a^{12} in G.

Solution: By theorem, $gcd(12, 20) = 4$, so

$$H = \langle a^4 \rangle = \{e, a^4, a^8, a^{12}, a^{16}\}$$

If you just write down the powers of H, you get the same thing:

$$a^{12}, (a^{12})^2 = a^{24} = a^4, (a^{12})^3 = a^{36} = a^{16}, (a^{12})^4 = a^{48} = a^8, (a^{12})^5 = a^{60} = (a^{20})^3 = e^3 = e.$$

1c. List the elements in any **proper** subgroup of H (that is, give me *one* subgroup of H that is *not* $\{e\}$ or H.)

Solution: Bad problem, H is a cyclic group of order 5, 5 is prime, so no proper subgroups. I'll ask a correct version of this on hw 2.

2a. Determine $(\mathbb{Z}/14\mathbb{Z})^*$. (Hints: $14 = 2 \cdot 7$ and this set has 6 elements. It is ok in this problem to write your solution with, say "1" standing in for $[1]_{14}$.)

Solution: We want $[a]_{14}$ so that $gcd(a, 14) = 1$; that is, a is not divisible by 2 or 7. The first case rules out $\{2, 4, 6, 8, 10, 12\}$, the second case rules out $\{7\}$ and we are left with

$$(\mathbb{Z}/14\mathbb{Z})^* = \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}.$$

2b. Write down the multiplication table for $(\mathbb{Z}/14\mathbb{Z})^*$.

Solution: I'm lazy, so I'll drop the $[\cdot]_{14}$ and just write the a's.

	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	15	3	1

because, for example $5 \cdot 9 = 45 = 3 \cdot 14 + 3 \equiv 3 \mod 14$, etc.

2c. Which (if any) elements a have the property that the order of a is 6? That is, $a^6 \equiv 1 \mod 14$, but $a^j \not\equiv 1 \mod 14$ for $j \in \{1,2,3,4,5\}$.

Solution: Reading from the table, the powers of 1 are 1; the powers of 3 are 1,3,9,13,11,5,1; the powers of 5 are 1,5,11,13,9,3,1; the powers of 9 are 1,9,11,1; the powers of 11 are 1,11,9,1 and the powers of 13 are 1,13,1. So to answer the question, $a = 3, 5$; that is $[3]_{14}$ and $[5]_{14}$, and note that they are inverses: $3 \cdot 5 = 15 \equiv 1 \mod 14$.

3 ($\mathcal{E}$). The following is a bad (but accurate) multiplication table of a group G. You may assume this is a group, **you are not asked to prove this!** All questions can be answered by reading the table.

*	u	v	w	x
u	v	x	u	w
v	x	w	v	u
w	u	v	w	x
x	w	u	x	v

3a. Which element is the identity in the group? (Hint: it isn't u, even though it's the first element of the table, because this is a bad table.)

Solution: it has to be w, because for every z in the group, w*z = z*w = z.

3b. Determine the inverses of u, v, w, x.

Solution: Based on this u*x=x*u = w, v*v = w*w = w, so the inverse of u is x, the inverse of v is v, the inverse of w is w and the inverse of x is u.

3c. Find a specific isomorphism Φ from G to your favorite C_4.

Solution. If you look at powers of elements, the powers of u are u,v,x,w and the powers of x are x,v,u,w, so either u or x generate the group. There are two corresponding multiplication tables:

*	w	u	v	x
w	w	u	v	x
u	u	v	x	w
v	v	x	w	u
x	x	w	u	v

*	w	x	v	u
w	w	x	v	u
x	x	v	u	w
v	v	u	w	x
u	u	w	x	v

These correspond to two natural isomorphisms to C_4, which I will take to be $(\mathbb{Z}/4\mathbb{Z}, \oplus)$

$$\Phi_1(w) = [0]_4,\ \Phi_1(u) = [1]_4,\ \Phi_1(v) = [2]_4,\ \Phi_1(x) = [3]_4$$
$$\Phi_2(w) = [0]_4,\ \Phi_2(x) = [1]_4,\ \Phi_2(v) = [2]_4,\ \Phi_2(u) = [3]_4.$$

4. ($\mathcal{E}$) Find two sets of integers (a_i, b_i, c_i), $i = 1, 2$ so that $\gcd(a_i, b_i) = 4$ and $\gcd(a_i, c_i) = 6$, but $\gcd(b_1, c_1) \neq \gcd(b_2, c_2)$.

Solution. There are many correct solutions. To find one pair: if $gcd(a, b) = 4$ and $gcd(a, c) = 6$, then both 4 and 6 divide a, so 12 divides a as well. Let's take $a_1 = a_2 = 12$. As a first guess, if we take $b_1 = 4$ and $c_1 = 6$, then $(a_1, b_1, c_1) = (12, 4, 6)$ and

$$gcd(12, 4) = 4, \qquad gcd(12, 6) = 6, \qquad gcd(4, 6) = 2$$

To make a change, I'll give b and c a common factor that won't involve a, say 5. So take $(a_2, b_2, c_2) = (12, 20, 30)$ and

$$gcd(12, 20) = 4, \qquad gcd(12, 30) = 6, \qquad gcd(20, 30) = 10.$$

There are a lot of correct solutions!

5. Use your imagination and invent a situation in which one of the objects is a cyclic group of order 7. (But not simply adding integers mod 7 or rotating a regular 7-gon.) I have no specific answer in mind. Surprise me!

XX Gatsby inherited wealth from his father, who invented the idea of turning a computer off and then turning it back on to fix all its problems. He gets a royalty of a few cents from every computer sold in the world. His son, resented that his parents named him "XX", but he appreciated the family money.

XX mastered his addition table so quickly that his family told him he had to become a math major in college. He didn't like it and he never paid attention in his classes and didn't bother to work very hard.

So when he heard about the wonderful theorem that a regular 7-sided polygon cannot be constructed by straightedge and compass (according to the strict rules of Euclidean geometry), he mis-heard that as meaning that nobody could construct a regular 7-sided polygon at all (even though that is not the case if you use different rules; look up "Heptagon" on wikipedia!)

When XX (inevitably) was asked to leave school, he decided that he needed to build an underground mansion to protect himself against killer hornets. And to show up his advisors and professors, he decided to construct a regular 7-sided underground lair with 7 large rooms, all completely protected from the outside, and numbered 0,1,2,3,4,5,6 in order.

For security reasons, each room was only accessible from a central cylindrical elevator. For security reasons, the elevator has no controls. It automatically opens, closes and rotates $\frac{2\pi}{7}$ radians clockwise, to the next room, taking exactly one minute to do so.

If you stay on the elevator for k minutes, you rotate $\frac{2\pi k}{7}$ radians and move k rooms. This gives both rotations of a regular 7-gon for the motions of the elevator and $(\mathbb{Z}/7\mathbb{Z}, \oplus)$ for the number of the room you are in.

Well that's my story. I hope you wrote a better one!