1 Homomorphisms

Which of these are homomorphisms?

Either explain why, or give a counter-example to disprove it.

	$f(x)$	$a \star_1 b$	$a \star_2 b$
$f_1 : \mathbb{R} \to \mathbb{R}$	$-x$	$a + b$	$a + b$
$f_2 : \mathbb{Z} \to \mathbb{Z}$	x	$4b(a + b) + a^2$	$(a + 2b)^2$
$f_3 : \mathbb{P} \to \mathbb{P}$	1	a	a
$f_4 : \mathbb{Z}^+ \to \mathbb{R}$	$x/2$	$a + b$	$a + b$
$f_5 : \mathbb{Z}^+ \to \mathbb{R}$	$x/2$	$a \cdot b$	$a \cdot b$

1.1 General

$f : S \to S$ where:

- S is the set of elements of *any* group $G = (S, \star)$
- $f(x) = x^{-1}$ (i.e. $f(x) =$ the inverse of x in G)
- $a \star_1 b = a \star_2 b = a \star b$

2 Semi-Generator

Suppose g is a generator of a group G. (Recall: This means that the powers of g include every element in G.)

Show that g^{-1} "generates" at least half the elements of G.

(Hint: To convince yourself, try $G = (\mathbb{Z}_7, +)$ and $g = 3$. Use problem 1.1 to prove it for all groups.)

3 $\phi(N)$

Find a formula for finding $\phi(N)$ for any N given its prime factorization.

Calculate $\phi(N)$ for $N = 1$ to 30 and check that it works.

4 Groups

For each of these, make sure you can justify every step using definition of a group. As a refresher, here is the definition of a group G (often called the "group axioms"):

- Identity: There is an "identity" $e \in G$ such that $e \star x = x$ for every $x \in G$.
- Inverses: For every $x \in G$, there is a $y \in G$ such that $x \star y = e$.
- Associativity: If $x, y, z \in G$ then $(x \star y) \star z = x \star (y \star z)$
- Closed: If $\in G$ then $x \star y \in G$.

If $x \star y = y \star x$ for every $x, y \in G$, then G is *commutative*. Not every group is commutative, so *you can't switch the order of elements around* $\star$.

4.1

Suppose $a, b, x \in S$ are elements of any group $G = (S, \star)$. Prove that

$$a \cdot x = b \cdot x \quad \Rightarrow \quad a = b$$

4.2

Suppose G is *not* a commutative group: $a \star b$ may not be the same as $b \star a$ for every $a, b \in G$.

Try to prove the following:

- e is unique (Suppose there are two different identities. Show that they're the same.)
- $e \star a = a \Rightarrow a \star e = a$. (i.e. a "left identity" is also a "right identity")
- Suppose $x \in G$. Prove that $x \star y = e \Rightarrow y \star x = e$ (i.e. a "right inverse" is also a "left inverse").

For our course, we will usually be talking about commutative groups. If you ever take a group theory class, you will also see non-commutative groups.

5 Generators

- How many elements are there in $(\mathbb{Z}^*_{1001}, \cdot)$?
- How many generators are there in $(\mathbb{Z}^*_{1001}, \cdot)$?
- Find a generator for $(\mathbb{Z}_n, +)$ for each n from 1 to as high as you can (at least $n = 20$)
- Find all the generators mod 23. (First find one. Use it to find all the rest.)
- Can you find a generator for $(\mathbb{Z}_{24}, +)$?
- Pick two primes around 20 to 40. Can you find a number that is a generator mod both primes?

6 Using DLP to break CDH

The Discrete Log Problem (DLP) is at least as hard as the Computational Diffie-Hellman Problem (CDH). We'll show this by demonstrating that your ability so solve the DLP allows you to solve CDH.

Let's work with $G = (\mathbb{Z}^*_{19}, \cdot)$ and the generator $g = 14$.

Finish filling in the list of powers of g below. You can use it to solve the DLP (for base g in the group G): by looking up a value in the bottom row, you can find the discrete log in the top row.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
g^x	1	14	6															

(Why doesn't the table have a column for $x = 18$?)

Calculate the following:

- $DLOG_{14}(4) =$
- $DLOG_{14}(16) =$

- $DLOG_{14}(7) =$

Solve the Computational Diffie-Hellman (CDH) problem for these values:

- $(g, g^a, g^b) = (14, 8, 17) \Rightarrow g^{ab} =$
- $(g, g^a, g^b) = (14, 10, 8) \Rightarrow g^{ab} =$
- $(g, g^a, g^b) = (17, 2, 16) \Rightarrow g^{ab} =$
- $(g, g^a, g^b) = (13, 12, 8) \Rightarrow g^{ab} =$

Since you also found the values of a and b, check that $(g^a)^b = (g^b)^a = g^{ab}$ for your answers.

- 137
- 143
- 56191
- 890843293
- 561
- 1105.

In this class, we will learn methods for testing whether a number is prime or not without factoring the number. As has been suggested by this problem, the above test is not a reliable one.

7 FLT Primality Test

In class today we learned Fermat's Little Theorem, which says that if p is prime and a any integer, then

$$a^{p-1} = 1 \mod p.$$

We can sometimes use this to tell that a number isn't prime. For example, $2^{754128} = 64667 \mod 754129$, so we know that 754129 is not prime, without

even factoring $754129 = 19^2 \times 2089$ (doing the latter is a tougher computation). We say that g is a 'witness' for m if $g^{m-1} \neq 1 \mod m$ - telling us that m is not prime. So in the example, 2 is a witness for m. For the following numbers, determine whether the number is prime (you can do this by hand, but I would recommend using a computer - you can, for instance, ask your calculator or WolframAlpha 'factor x' if you want to factor x). If the number is not prime, try to find a witness for that number. You may again use a computer for this computation. If you don't think there are any witnesses for a given composite number, it is alright to stop.

- 137
- 143
- 56191
- 890843293
- 561
- 1105

8 RSA

Run the entire RSA algorithm using a friend:

- Select primes p and q and compute $N = p \cdot q$
- Pick an exponent e and find the inverse exponent d. (Find the inverse of e mod $\varphi(N)$. Recall that $\varphi(N) = (p-1) \cdot (q-1)$ and that you can use the Extended Euclidean Algorithm to find inverses).
- Ask your friend to select a message m and send you $c = m^e$.
- Compute c^d to decrypt the message.

9 Extra RSA Problems

Ask Lucas for extra RSA problems. ;-)

10 Montgomery's Ladder

The "obvious" way to calculate $g^y \mod n$ gives away some information about the number we are exponentiating. Can you characterize what information is given away?

Suppose the binary representation of x has x_i at the 2^i's place. Try the following for yesterday's homework problems:

- $a = g$, $b = x^2$
- For $i = k-2, k-3, ..., 0$:
  - If $x_i = 0$
    - $b = a \cdot b$
    - $a = a^2$
  - If $x_i = 1$:
    - $a = a \cdot b$
    - $b = b^2$
- Output the final value of a.

Can you explain why it swords?