MA 294: Applied Abstract Algebra / Spring 2022
Homework assignment #5 (final version)
~~(preliminary version: more problems may be added 2/24/2022)~~
Due Thursday 3/3/2022 by 4pm

2/24/22 edits in blue.

Turn in your work either in class or before 4pm in the envelope hanging on MCS 127.

- Please staple or otherwise connect the pages of your work. There is a stapler in the math department main office. Yes, this requires a tiny bit of planning — but I know we can do this! Our grader is anxious that homework set pages might get lost.
- Write your name on the front page. Plan ahead: perhaps you need to carry around a pen for this purpose on Thursdays?
- Consider using a pen rather than a pencil, especially if your pencilwork is smudgy.
- **Challenge problems:** Challenge problems are optional. Please write up your solutions to challenge problems separately. Alternatively, come tell me your solution during office hours. You may also do this later, anytime during the semester.

Let m be a positive integer and a any integer. If $\gcd(a, m) = 1$, figure out how to show that

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Hint: Use (6) on HW # 4. (No need to write this up or turn this in.)

This statement is called *Euler's theorem*. The special case where $m = p$ is prime is called *Fermat's little theorem*: if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Also read section 13.3 from the middle of p. 148 on, including Theorem 13.3.2.

Suppose $\gcd(a, m) = 1$. If you know $\varphi(m)$, then you may use Euler's theorem to find the multiplicative inverse of a modulo m. Alternatively, it's very efficient to use Euclid's algorithm to find solutions to $ax + my = 1$ as in the example after Theorem 8.4 and in Exercise 8.4.1; note that this method doesn't require knowing $\varphi(m)$.

(1) (a) In $\mathbb{Z}_{23}^{\times}$, compute $[3]^{47}$ and the inverse of $[17]$.

(b) Find all solutions to $13x \equiv 5 \pmod{23}$.

Read sections 20.6 and 20.7.

(2)–(5) Exercises 20.6.2, 20.7.2, 20.7.3, 20.7.4.

(Recall that $G_{\triangle}$ is what we've been calling $\mathrm{Symm}(\triangle)$.)

(6) (a) Show that $[a] \in \mathbb{Z}_m$ generates $\mathbb{Z}_m$ if and only if $\langle [a] \rangle$ contains $[1]$.

(b) Prove that $[a]_m$ is a generator of $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

(7) The group $\mathbb{Z}_{19}^{\times}$ is cyclic. Find all the generators.
(Hint: one option is to find *one* generator and then use (6b).)

(8) Let a be the smallest positive integer so that $[a]$ generates $\mathbb{Z}_{19}^{\times}$.

(a) Construct a "$\mathbb{Z}_{19}^{\times}$-$\log_a$" (discrete log) table: for every element $[b]$ of $\mathbb{Z}_{19}^{\times}$ find the smallest nonnegative power n so that $[a]^n = [b]$.

(b) First figure out how to use this table to solve an equation such as $2^x \equiv 12 \pmod{19}$, and then solve the following, showing your work:

(i) $3^x \equiv 4 \pmod{19}$ (ii) $5^x \equiv 7 \pmod{19}$.

Can you describe all the positive integers x that are solutions in each case?

More kinds of groups

(9) Let X be a set, and let G be the set of bijective functions $f : X \to X$. (Such a function is also called a *permutation* of X.) If X has n elements, how many elements does G have? Show that G forms a group under composition.

(10) Let $S = \{1, 2, 3\}$ and consider the group G of bijective functions $S \to S$.

(a) List the elements of G and make a group table.

(b) Is G isomorphic to another group that we have studied? Explain. (If yes, construct an isomorphism. If no, explain why not.)

(11) (a) Find all the subgroups of $\mathbb{Z}_{18}$ (this is an additive group). Explain. Draw the subgroup diagram.

(b) Find all the subgroups of $\mathbb{Z}_{13}^{\times}$ (this is a multiplicative group). Explain. Draw the subgroup diagram.

(12) Let G be a group and $H \leq G$ as subgroup. Consider the following relation on G: for $a, b \in G$ we have $a \sim b$ iff $a^{-1}b \in H$.

(a) Show that $\sim$ is an equivalence relation on G.

(b) What are the associated equivalence classes if $G = \mathrm{Symm}(\triangle)$ and $H = \{1, \mathrm{flip}(|)\}$?