MATH 4573: HOMEWORK 6

INSTRUCTOR: TYLER GENAO

Due: March 6, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite up to §2.8 of our notes. Everything else must be proven.**

An extra warning: if you have already taken a course in abstract algebra, be careful not to use any results we have yet to prove in class!

1. Problems to Submit

For Exercises 1 and 2, we let $(R, +, \cdot)$ be a ring with additive identity $0 := 0_R$ and multiplicative identity $1 := 1_R$.

Exercise 1.

a) Show that for all $r \in R$ one has

$$r \cdot 0 = 0 \cdot r = 0.$$

b) Prove that the *unit group of* R, denoted as

$$R^\times := \{r \in R : \exists s \in R \text{ with } rs = 1\},$$

is a group under multiplication.

c) Show that for rings $R_1, R_2, \ldots, R_n$, one has

$$(R_1 \times R_2 \times \cdots \times R_n)^\times \cong R_1^\times \times R_2^\times \times \cdots \times R_n^\times.$$

Let S be another ring, and let $\varphi\colon R \to S$ be a ring homomorphism.

d) Show that φ induces a group homomorphism on unit groups,

$$\varphi\colon R^\times \to S^\times.$$

Exercise 2. Say that an element $r \in R$ is a **zero divisor** if for some nonzero $s \in R$ one has

$$rs = 0.$$

We call R an **integral domain** if it has no nonzero zero divisors.

a) Show that an integral domain R satisfies the *cancellation property:* for $r, s, t \in R$ with $r \neq 0$, if
$$rs = rt$$
then $s = t$. Similarly, show that if $sr = tr$ then $s = t$.
b) Show that a field is an integral domain.
c) Give an example of a ring which is not an integral domain, and an integral domain which is not a field.

Exercise 3. Let G be a finite group.

a) Show that an element $g \in G$ is a generator of G if and only if for all proper divisors d of $|G|$ one has $g^d \neq e$.
b) After proving part a), show that an element $g \in G$ is a generator of G iff for all primes $p \mid |G|$ one has $g^{\frac{|G|}{p}} \neq e$.
c) Without a calculator, use part b) to show that 2 is a primitive root modulo 29, and is *not* a primitive root modulo 31.

Exercise 4.

a) Use Exercise 3 to show that 3 is a primitive root modulo 43.
b) Without a calculator, determine with proof the solutions to $x^6 \equiv -2 \pmod{43}$ as powers of 3, if they exist.

Exercise 5. Let g be a primitive root modulo m. Let us define the **discrete logarithm (modulo m with base g)** as follows. For each element $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$, we know there exists unique $0 \leq k < \varphi(m)$ with
$$[g]^k = [a],$$
i.e.,
$$g^k \equiv a \pmod{m}.$$
We define the *discrete logarithm of a* as
$$\log_g(a) := k.$$
(Sometimes $\log_g^m(a)$ is used to emphasize the modulus m.)

a) Show that for any $a, b \in \mathbb{Z}$ coprime to m, one has
$$\log_g(a \cdot b) \equiv \log_g(a) + \log_g(b) \pmod{\varphi(m)}.$$
(*Hint:* HW 5 Exercise 4 will help.)
b) Prove the following *change of base formula* for discrete logarithms: given another primitive root h modulo m, show that $\log_h(g)$ is coprime to $\varphi(m)$, and that for all $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$ one has
$$\log_g(a) \equiv \frac{\log_h(a)}{\log_h(g)} \pmod{\varphi(m)},$$
where $\frac{1}{\log_h(g)} := \log_h(g)^{-1}$ is the multiplicative inverse of $\log_h(g)$ modulo $\varphi(m)$. (*Hint:* HW 5 Exercise 4 will help.)

c) Assume 3 and 5 are primitive roots modulo $4802 = 2 \cdot 7^4$, and that the discrete logarithm $\log_3^{4802}(5)$ is equal to 911. Use part b) to compute the discrete logarithm $\log_5^{4802}(81)$.

Exercise 6. For this computational exercise, **you will need to submit your associated code as a text file onto Carmen.** In particular, your code must run without error if pasted into SageCell by the class grader, and *automatically* print the output you claim in your answer. Note that when you copy-paste your code into Carmen, it might mess some of the formatting up, so you may need to fix it. The deadline for submitting the code is the same as this HW.

a) Use Exercise 3 to create a `Sage` function which for positive integers g and m, takes as input (m, g) and returns `True` if g is a primitive root modulo m. Have it return `False,` and print a message, if m has no primitive roots, or if g is not a primitive root mod m.

   Run output for this to check whether $g = 2$ is a primitive root modulo p, for primes $p \leq 163$.

b) Based on part a), can you come up with a conjecture on the primes p which have 2 as a primitive root? You can extend your search over larger p if necessary. (One point)

c) Use part a) to create a `Sage` function which for positive integers a, g and m with g a primitive root modulo m, takes as input (a, m, g) and outputs the discrete logarithm $\log_g(a) := \log_g^m(a)$, which is the integer $0 \leq \log_g(a) < m$ with

$$g^{\log_g(a)} \equiv a \pmod{m}.$$

   Have it return a message if any of the following hold: m does not have primitive roots; g is not a primitive root mod m; or a is not coprime to m.

   Run output for this function for $g = 2$, $a = 3$ and over primes $p \leq 163$.

Exercise 7. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From [NZM91, §2.11], page 127: $\#14 - 16, 19 - 21$.
From [NZM91, §2.8], page 106: $\#1 - 3, 7 - 9, 12 - 14$.

Bonus Exercise 8. This exercise studies *Fermat numbers,* which are integers of the form 2^n+1 for $n \geq 0$. The first few Fermat numbers are listed here: https://oeis.org/A000215.

A prime number which is a Fermat number is called a *Fermat prime.* More information about them can be found here: https://oeis.org/A019434.

a) Show that if a Fermat number is prime, then it is of the form $2^{2^k} + 1$ for some $k \geq 0$. (*Hint:* consider how to factorize the difference of odd a'th powers of two numbers, $x^a - y^a$.)

b) Show that 2 is a primitive root modulo any Fermat prime p.

c) More generally, show that if a is not a square modulo a Fermat prime p (so $x^2 \equiv a \pmod{p}$ has no solutions), then a is a primitive root modulo p.

The only known Fermat primes are $3, 5, 17, 257$ and 65537.

Bonus Exercise 9. This exercise explores the *characteristic* of an integral domain.

a) Prove that for a ring R, there exists exactly one ring homomorphism

$$\iota\colon \mathbb{Z} \to R.$$

b) Show that in part a), ι is injective if and only if 1_R has infinite additive order.
c) Show that in part a), if ι is not injective, then *assuming that R is an integral domain* the additive order of 1_R is prime.

When ι is injective, we say that R has **characteristic zero.** When ι is not injective, we say that the integral domain R has **positive characteristic** p**,** where p is the additive order of 1_R. As it turns out, any field with characteristic zero contains $\mathbb{Q}$, and any field with positive characteristic p contains $\mathbb{Z}/p\mathbb{Z}$.

Bonus Exercise 10 (Examples of rings)**.** For each set R below, determine whether:

1. R is a ring;
2. R is commutative;
3. R is an integral domain;
4. R is a field.

If R is a ring, then determine its group of units $R^\times$ if possible.

a) The set $\mathbb{Z}[x]$ of polynomials with integer coefficients.
b) The set $C([0,1])$ of continuous real-valued functions $f\colon [0,1] \to \mathbb{R}$.
c) For $n \in \mathbb{Z}^+$, the set $\mathrm{Mat}_{n\times n}(\mathbb{R})$ of $n \times n$ matrices with real entries.
d) For $n \in \mathbb{Z}^+$, the set $\{c_0 + c_1x + \ldots + c_nx^n : c_i \in \mathbb{Z}\}$ of degree $\leq n$ polynomials over $\mathbb{Z}$.
e) The set of Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.
f) The set of squares of rational numbers, $\{\frac{a^2}{b^2} : a, b \in \mathbb{Z}, b \neq 0\}$.
g) The set of real-valued functions $f\colon \mathbb{R} \to \mathbb{R}$ with $\lim_{x\to 0} f(x) = 0$.

Bonus Exercise 11. Prove that for any prime $p > 2$, writing

$$1 + \frac{1}{2^3} + \ldots + \frac{1}{(p-1)^3} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}$, one has $p \mid a$. (*Hint:* Interpret this sum modulo p, and use the identity $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.)

Bonus Exercise 12. The following exercise outlines a proof of [NZM91, Theorem 2.41] on when primitive roots modulo m exist.

a) Let G and H be finite abelian groups. Show that the order of any element $(g, h) \in G \times H$ is equal to $\mathrm{lcm}(|g|, |h|)$. (*Hint:* HW 5 Exercise 5 should help.)
b) Explain how part a) should generalize to a product $G_1 \times G_2 \times \ldots \times G_n$ of finite abelian groups.
c) Let an integer $m > 1$ have prime factorization

$$m = \prod_{i=1}^{r} p_i^{e_i}.$$

Show that for any element $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$, one has

$$|[a]|^\times = \operatorname{lcm}\{|[\pi_{p_i^{e_i}}(a)]|^\times\}_{i=1}^r.$$

(Here, we use $|[a]|^\times$ to denote the multiplicative order of $[a]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, and for $d \mid m$ we let $\pi_d \colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$ denote the mod-d reduction map.)

d) Finally, use the previous parts to give an alternate proof for the existence of primitive roots:

Theorem. [NZM91, Theorem 2.41] *For an integer $m \in \mathbb{Z}^+$, there exists a primitive root modulo m if and only if $m = 1, 2, 4, p^k$ or $2p^k$, where p is an odd prime.*

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).