MATH 4573: HOMEWORK 6

INSTRUCTOR: TYLER GENAO

Due: March 22, 2024.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in this assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions.

Your solutions should not use theorems from sections which come after the day the homework was assigned. This HW should use what we've covered in Chapter 2 – especially §2.8 – as well as Chapter 4, §4.1 – 4.3.

1. Problems to Submit

Exercise 1. In parts a) and b), let G be a finite group of order n.

a) Show that for all $g \in G$, one has $|g| = n$ if and only if $g^d \neq e$ for all $1 \leq d < n$ with $d \mid n$. Thus, knowing the factorization of $|G|$ gives a way to check whether an element generates G.

b) Show that for any $g \in G$, one has $g^{\frac{n}{p}} \neq e$ for all primes $p \mid n$ if and only if g has order n. This gives a way to test whether g is a generator for G. (*Hint:* calculate the order of $g^{\frac{n}{p}}$ for suitably chosen $p \mid n$, using the formula from HW 5 Exercise 4.b).

c) Using part b), show that 2 is a primitive root modulo 19, and is *not* a primitive root modulo 17.

Exercise 2. Show that 2 is a primitive root modulo 61. Then determine with proof the solutions to $x^6 \equiv 6 \pmod{61}$, if they exist.

Exercise 3. This is a continuation of HW 3 Exercise 8. Let g be a primitive root modulo m. Recall that there exists a *discrete logarithm mod m with base g:* for each $a \in \mathbb{Z}$ coprime to m, there exists a unique exponent $0 \leq e < \phi(m)$ with $g^e \equiv a \pmod{m}$. Then we define the discrete logarithm as $\log_g(a) := e$.

a) Show that for $x, y \in \mathbb{Z}$ coprime to m, one has $\log_g(x \cdot y) \equiv \log_g(x) + \log_g(y) \pmod{\phi(m)}$.

b) Show that there is a "change of base" formula for discrete logarithms. More precisely, given another primitive root h modulo m, show that $\log_h(g)$ is coprime to $\phi(m)$, and that for all $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$ one has

$$\log_g(a) \equiv \frac{\log_h(a)}{\log_h(g)} \pmod{\phi(m)}$$

(here, $\frac{1}{\log_h(g)}$ represents the multiplicative inverse mod $\phi(m)$).

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

Exercise 4. Using de Polignac's formula, for any prime $p \in \mathbb{Z}^+$ and $n \in \mathbb{Z}^+$ one can compute the p-adic valuation[1] of $n!$ via

$$v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

This exercise gives an iterative way to compute each term $\left\lfloor \frac{n}{p^k} \right\rfloor$ in the sum.

a) Prove that for each $k \geq 1$, one has

$$\left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{p^{k-1}} \right\rfloor}{p} \right\rfloor.$$

Therefore, computing $\left\lfloor \frac{n}{p} \right\rfloor$ lets us compute $\left\lfloor \frac{n}{p^2} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor$, which then lets us compute $\left\lfloor \frac{n}{p^3} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{p^2} \right\rfloor}{p} \right\rfloor$, and so on.

b) Using the technique in part a), compute the 5-adic valuation of 3443!.

Exercise 5. In HW 4 Exercise 3, we showed that $\phi(x) = n$ has a finite number of solutions.

a) Show that $\sigma(x) = n$ has a finite number of solutions.

b) Show that $d(x) = n$ has an *infinite* number of solutions if $n > 1$.

Exercise 6. Define an arithmetic function $\lambda \colon \mathbb{Z}^+ \to \mathbb{C}$ via

$$\lambda(n) := (-1)^{\Omega(n)}.$$

This is called *Liouville's lambda function.*

a) Show that λ is totally multiplicative.

b) Show that

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a perfect square} \\ 0 & \text{otherwise.} \end{cases}$$

(*Hint:* for the case where n is a perfect square, fix a prime $p \mid n$ and write $n = p^e m$ with $p \nmid m$. Then show that $\sum_{d|n} \lambda(d) = \sum_{d|m} \lambda(d)$.)

Exercise 7.

a) Calculate the sum

$$\sum_{d|n} \mu(d)\phi(d)$$

for $n = 5, 6, 7, 8, 9, 10$.

[1]Recall that the *p-adic valuation of n,* denoted $v_p(n)$, is the largest power of p which divides n. This definition extends to rational numbers $\frac{a}{b}$ via $v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b)$.

b) Prove that for all even $n \in \mathbb{Z}^+$ one has

$$\sum_{d|n} \mu(d)\phi(d) = 0.$$

Exercise 8. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From the textbook, page 106: $\#1-3, 7-9, 12-14$.
Pages $184-185$: $\#1-4$.
Pages $191-192$: $\#1-4, 9$.
Page 195: $\#1, 2, 5$.

Bonus Exercise 9. 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 known Fermat primes are $3, 5, 17, 257$ and 65537. It is conjectured that these are the *only* Fermat primes.

Bonus Exercise 10. The following exercise outlines a proof of [NZM91, Theorem 2.41], on when primitive roots modulo m exist. It also gives some practice with products of groups.

Let G and H be two finite abelian groups.

a) Show that the order of any element $(g, h) \in G \times H$ is equal to $\operatorname{lcm}(|g|, |h|)$. Then explain how this would generalize to a longer product $G_1 \times G_2 \times \ldots \times G_n$.
b) Given a group homomorphism $\varphi\colon K \to G \times H$, define two homomorphisms $\varphi_1\colon K \to G$ and $\varphi_2\colon K \to H$ as follows: $\varphi_1(k) := g_k$ and $\varphi_2(k) := h_k$ where $\varphi(k) = (g_k, h_k)$. Show that φ_1, φ_2 are homomorphisms, and that

$$\varphi(k) = (\varphi_1(k), \varphi_2(k)).$$

Thus, any homomorphism to a product is a product of homomorphisms.
c) Let $m \in \mathbb{Z}^+$ have the prime factorization $m = \prod_{i=1}^r p_i^{e_i}$. Show that for any $a \in \mathbb{Z}$, if a is coprime to m then

$$|\overline{a} \mod m| = \operatorname{lcm}\{|\overline{a} \mod p_i^{e_i}|\}_{i=1}^r.$$

d) Use part c) to give an alternate proof for the existence of primitive roots:

Theorem. [NZM91, Theorem 2.41] *There exists a primitive root modulo m if and only if $m = 1, 2, 4, p^e$ or $2p^e$ where p is an odd prime.*

Bonus Exercise 11. This exercise will prove the following result:

Theorem. *For any field F, one has that any finite subgroup G of $F^\times$ is cyclic.*

We will prove this the following way. Let us set $n := |G|$. Define for each $d \mid n$ the subset

$$G_d := \{g \in G : |g| = d\}.$$

We will show that $G_n \neq \emptyset$, which forces G to be cyclic.

a) Assume that $G_d \neq \emptyset$. Show that $|G_d| = \phi(d)$ by considering the roots of the polynomial $x^d - 1$ over F and applying the following generalization of [NZM91, Theorem 2.26]:

Proposition. *Over a field F, any nonzero polynomial $f \in F[x]$ has at most* $\deg(f)$ *roots.*

b) Using the fact that G is a disjoint union of the sets G_d (which are either empty or have size $\phi(d)$), prove using [NZM91, Theorem 4.6] that for each $d \mid n$ one must have $|G_d| = \phi(d)$. Show that this implies the theorem.

Bonus Exercise 12. This exercise will give a formula for computing the power of a prime which divides a binomial coefficient.

Fix a prime $p \in \mathbb{Z}^+$.

a) Show that every integer $n \geq 0$ can be uniquely written in "base p", with the form

$$n = n_0 + n_1 p + n_2 p^2 + \ldots + n_r p^r,$$

where the $n_i \in \mathbb{Z}$ each satisfy $0 \leq n_i < p^i$, and $n_r \neq 0$.

b) With notation as above, let $S(n) := n_0 + n_1 + \ldots + n_r$ be the sum of the base p digits of n. Then use de Polignac's formula to prove the following theorem.

Theorem (Kummer)**.** *Let $p \in \mathbb{Z}^+$ be a prime. Then for all integers $0 \leq m \leq n$, one has*

$$v_p\left(\binom{n}{m}\right) = \frac{S(m) + S(n-m) - S(n)}{p-1}.$$

Bonus Exercise 13. It is not hard to show that $\phi(n) < n$ for all integers $n > 1$. However, with the formula

$$\phi(n) = \prod_{p^e \| n} p^{e-1} \cdot (p-1),$$

it would seem that $\phi(n)$ should also be smaller than

$$n = \prod_{p^e \| n} p^{e-1} \cdot p$$

by a "consistently small amount." This exercise quantifies that: we will show that $\phi(n)$ is bigger than $n^{1-\epsilon}$ for any $\epsilon > 0$, provided that n is sufficiently large with respect to ϵ.

a) Let $f\colon \mathbb{Z} \to \mathbb{C}$ be a multiplicative arithmetic function such that

$$\lim_{p^k \to \infty} f(p^k) = 0$$

as p^k ranges through all prime powers. Prove that

$$\lim_{n \to \infty} f(n) = 0.$$

Thus, convergence to zero for a multiplicative function $f(x)$ can be checked using prime powers.

b) Show that for any $\epsilon > 0$, for all sufficiently large $n \in \mathbb{Z}^+$ one has

$$n^{1-\epsilon} < \phi(n) < n.$$

(*Hint:* for the inequality $n^{1-\epsilon} < \phi(n)$, it will suffice by part a) to show that

$$\lim_{p^k \to \infty} \frac{p^{k(1-\epsilon)}}{\phi(p^k)} = 0.)$$

Bonus Exercise 14. For each $n \geq 1$, let us define the *n-cyclotomic polynomial* $\Phi_n(x) \in \mathbb{Z}[x]$ recursively: for $n = 1$ we set $\Phi_1(x) := x - 1$, and for $n > 1$ we define $\Phi_n(x)$ as the unique monic[2] irreducible[3] polynomial in $\mathbb{Z}[x]$ that divides $x^n - 1$ and does not divide $x^k - 1$ for $1 \leq k < n$. As it turns out, one has

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Each $\Phi_n(x)$ is irreducible, and its roots are of the form $e^{2\pi i \frac{a}{n}}$ where $\gcd(a, n) = 1$; these roots are called *roots of unity,* and have many applications in algebraic number theory. The first few cyclotomic polynomials are $\Phi_1(x) = x - 1, \Phi_2(x) = x + 1, \Phi_3(x) = x^2 + x + 1, \Phi_4(x) = x^2 + 1, \Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ and $\Phi_6(x) = x^2 - x + 1$.

Use the Möbius inversion formula to prove the following formula for $\Phi_n(x)$:

Theorem. *For each $n \geq 1$, one has*

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

(*Hint:* Fix $x \in \mathbb{R}$ with $|x| \neq 1$, so that $x^n - 1 \neq 0$ and $\phi_d(x) \neq 0$ for $d \mid n$; then take complex logarithms. Conclude that the relation is true by the identity theorem from complex analysis.)

Bonus Exercise 15. This exercise gives a more general version of arithmetic functions and the Möbius inversion formula, and an alternative proof for Bonus Exercise 14.

Let G be an abelian group, written multiplicatively. Call any map $f\colon \mathbb{Z}^+ \to G$ a *G-arithmetic function.*

a) Mimic the proof of the usual Möbius inversion formula [NZM91, Theorem 4.8] to prove the following "G-Möbius inversion formula" for G-arithmetic functions:

[2] A *monic* polynomial has a leading term coefficient of 1.

[3] A polynomial is *irreducible* if it is not a product of two polynomials with lower degree.

Theorem (G-Möbius inversion formula)**.** *For G-arithmetic functions $f, F\colon \mathbb{Z}^+ \to G$ with*

$$F(n) = \prod_{d|n} f(d),$$

one has

$$f(n) = \prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)}.$$

b) Use the G-Möbius inversion formula to give an alternative proof of Bonus Exercise 14:

Theorem. *For each $n \geq 1$, one has*

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

(*Hint:* Take $G := \mathbb{Q}(x)^\times$ as the unit group of the fraction field of $\mathbb{Z}[x]$, and apply the G-Möbius inversion formula to the relation $x^n - 1 = \prod_{d|n} \Phi_d(x)$.)

Bonus Exercise 16. In this exercise, you will explore an algebraic structure on the set $\mathcal{A}$ of arithmetic functions.

Given two arithmetic functions $f, g\colon \mathbb{Z}^+ \to \mathbb{C}$, their *convolution* is the function $(f * g)\colon \mathbb{Z}^+ \to \mathbb{C}$ defined by

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

a) For an arithmetic function $f\colon \mathbb{Z}^+ \to \mathbb{C}$, we have previously defined $F(n) := F_f(n) = \sum_{d|n} f(d)$. What is $\mu * F_f$?
b) Show that convolution is commutative: for any two arithmetic functions f and g, one has $f * g = g * f$.
c) show that if f and g are multiplicative functions, then so is $f * g$.
d) Show that convolution is associative: for arithmetic functions f, g and h, one has $(f * g) * h = f * (g * h)$.
e) Define a function $I\colon \mathbb{Z}^+ \to \mathbb{C}$ via

$$I(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Show that for any arithmetic function f, one has $f * I = I * f = f$.
f) Given an arithmetic function f with $f(1) \neq 0$, define a new arithmetic function $f^{-1}\colon \mathbb{Z}^+ \to \mathbb{C}$ recursively: set $f^{-1} := \frac{1}{f(1)}$, and for $n > 1$ define

$$f^{-1}(n) := \frac{-1}{f(1)} \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{-1}(d).$$

Show that $f * f^{-1} = I$.

The above steps show that the subset of $\mathcal{A}$ of functions f with $f(1) \neq 0$ is a *commutative group* under the convolution operation. However, there is a larger ring structure on $\mathcal{A}$ to consider.

g) For two arithmetic functions $f, g\colon \mathbb{Z}^+ \to \mathbb{C}$, define their sum $f+g\colon \mathbb{Z}^+ \to \mathbb{C}$ as their pointwise sum:

$$(f+g)(n) := f(n) + g(n).$$

Note that $f+g$ is an arithmetic function.

h) Show that $\mathcal{A}$ is a commutative group under the sum operation above.

i) Show that the distributive law holds for $+$ and $*$: more precisely, for arithmetic functions f, g and h, one has

$$f * (g+h) = f * g + f * h.$$

The conclusion is that $\mathcal{A}$ is a *commutative ring* under addition and convolution; it is called the **Dirichlet ring**. By the Möbius inversion formula, every element $f \in \mathcal{A}$ is a multiple of the Möbius function μ (see part a)). What other properties does $\mathcal{A}$ have as a ring?

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).