Supplementary Materials for Chapter IV

Xu Gao

MATH 110 | Introduction to Number Theory | Summer 2023

July 11, 2023

Prerequisites

In order to succeed in this course, it is important to meet the following prerequisites:

(a). familiar with the style of proof-based mathematics;

(b). have a good understanding of proof formats and methods;

(c). have basic knowledge of set theory and combinatorics, which are covered in Math 100;

(d). solid grasp of lower division math courses, such as calculus and linear algebra.

In addition, you will meet some concepts which will be explored in greater depth in later courses. They will be used as terminology, and you should have ability to unpackage the abstract definitions.

What to expect in this document?

Definition important concepts which are not explicitly covered in the lectures. You are expected to be proficient in them.

Convenience conveniences used in this course. You should be able to reconginize them without mention.

Terminology useful terminology which are concepts from other courses. You are expected to be able to translate these terms into your own words, even without an in-depth understanding of the relevant theory.

Exercise non-mandatory exercises for practice and self-assessment. Highly recommended.

Further reading reading materials for further interest.

Problem homework problems and challenge problems.

† contents with † mark may be too deep or too off-topics.

Chapter IV

Modular World and Modular Dynamics

1 Modular structure

Terminology 1.1. A *(commutative) ring* is a set R equipped with two monoid structures $(R, +, 0)$ and $(R, \cdot, 1)$ such that:

(a). $(R, +, 0)$ is an abelian group;

(b). $(R, \cdot, 1)$ is an abelian monoid;

(c). The two operations $+$ and $\cdot$ are compatible in the sense of the following distributive laws:

- (left distributive law) $\forall a, b, c \in R$: $a \cdot (b + c) = a \cdot b + a \cdot c$;
- (right distributive law) $\forall a, b, c \in R$: $(a + b) \cdot c = a \cdot c + b \cdot c$.

Example 1.2. Let's clarify what does it mean by "the residue map π_m descends solutions"

- $(\mathbb{Z}, +, 0, \cdot, 1)$: the set of integers $\mathbb{Z}$ equipped with the *addition* and *multiplication* operations and their neutral elements 0 and 1 respectively, is a ring.
- $(\mathbb{Z}/m, +, 0, \cdot, 1)$: the residue set $\mathbb{Z}/m$ together with the *addition* and *multiplication* of congruence classes and their neutral elements $\mathbf{0} := [0]_m$ and $\mathbf{1} := [1]_m$ respectively, is another ring.
- The residue map $\pi_m \colon \mathbb{Z} \to \mathbb{Z}/m$ is a **surjective** homomorphism between rings.

2 Modular exponential

Theorem 2.1. Pingala's algorithm *on computing modular exponential* $b^x \pmod{m}$*:*

(a). *Write the exponent in binary digits:* $x = \sum_{i=0}^{n-1} a_i 2^i$

(b). *Instead of think* b^x *as* $\prod_{i=0}^{n-1} (b^{2^i})^{a_i}$*, we think it as*

$$b^x = (((b^2 \cdot b^{a_{n-2}})^2 \cdot b^{a_{n-3}})^2 \cdots)^2 \cdot b^{a_0}.$$

(c). *Then the algorithm can be understood as:*

- *Start with* b*;*
- *In each step* k*, take square (modulo* m*) of the previous one and then multiply it with* $b^{a_{n-k}}$ *(namely, multiply it with* b *if* $a_{n-k} = 1$ *and do nothing if not).*

Example 2.2. Find the natural representative of 2^{90} modulo 91.

exponent e	90	45	22	11	5	2	1
Binary	1011010	101101	10110	1011	101	10	1
$2^2 \pmod{91}$	64	57	23	46	32	4	2

Exercise 2.1. Is 119 a prime number?

Terminology 2.3. A group $(G, *, e)$ is called a *cyclic group* if it is isomorphic to $(\mathbb{Z}/m, +, \mathbf{0})$ for some m (called its *order*). The name comes from the fact that you can arrange elements in G in a single cycle $e \mapsto g \mapsto g^2 \mapsto \cdots \mapsto g^m = e$ under the function "$- * g$". Such an element g is called a *primitive root* of the cyclic group G.

Terminology 2.4. A congruence class $\overline{a} \in \mathbb{Z}/m$ is a primitive root of the additive group $(\mathbb{Z}/m, +, \mathbf{0})$ if and only if a coprime to m. (by Theorem 4.3.4)

An element $a \in \Phi(m)$ is a primitive root of the multiplicative group $(\Phi(m), \cdot, 1)$ if and only if a is a primitive root modulo m.

Exercise 2.2. Is there any primitive root modulo 8?

3 Properties of $\varphi(\,\cdot\,)$

Our argument of

$$\varphi(m) = |\Phi(m)| = \sum_{\ell | \varphi(m)} |\Phi_\ell(m)|$$

and

$$\sum_{\ell | \varphi(m)} \varphi(\ell) = \varphi(m)$$

works for any modulus m. So why the *primitive root theorem* may fail for general m? This could only because there are cases where

$$|\Phi_\ell(m)| > \varphi(\ell).$$

Exercise 3.1. Let $m = 20$ be the modulus.

(a). Compute $\ell(a)$ for all $a \in \Phi(20)$ and conclude that there is no primitive root modulo 20.

(b). However, compute $\varphi(\varphi(20))$. In particular, it is nonzero.

(c). Find all $\ell \mid \varphi(20)$ such that $|\Phi_\ell(20)| > \varphi(\ell)$.

The following algebraic result is used in the lecture.

Exercise 3.2. Show that

$$\prod_{i \in I} \left(1 - \frac{1}{x_i}\right) = \sum_{k \geqslant 1} (-1)^k \sum_{i_1, \cdots, i_k \in I} \frac{1}{x_{i_1} \cdots x_{i_k}}.$$

Problems

Problem IV.1. Prove that there are infinitely many positive integer triples (x, y, z) such that

$$x^2 + 2y^2 = 3z^2.$$

Hint. Find an appropriate rational point that will act as a "pivot", much like in the case of classifying Pythagorean triples that we saw in this lecture.

Problem IV.2. Let N be a positive integer, and A be the alternating sum of its digits. That is, if N has a decimal expansion with units digit u, tens digit t, hundreds digit h in units place, thousands digit s, then $A = u - t + h - s + \cdots$. Then $N \equiv A \pmod{11}$.

Problem IV.3. (a) Prove that a perfect square is congruent to 0, 1 or 4 modulo 8.

(b) Prove that there exists no integer solution (x, y, z) to the equation

$$x^2 + y^2 + z^2 = 31415926535897932384626433832 7.$$

(c) Demonstrate that there are infinitely many positive integers that *cannot* be written as a sum of three squares.

Problem IV.4. Let p be any prime number and let a and b be any two integers.

(a) Prove that if $a \equiv b \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
(b) Prove that if $a \equiv b \pmod{p}$, then $a^{p^2} \equiv b^{p^2} \pmod{p^3}$.
(b) (challenge) Can you generalise?

Problem IV.5. Compute (the natural representative of) $3^{10^{10^{10}}} \pmod{7}$.

Problem IV.6. Prove that a modulus m is even if and only if there exists an integer x such that $x \not\equiv 0 \pmod{m}$ and $x + x \equiv 0 \pmod{m}$.

Problem IV.7. Recall the Fibonacci numbers from Problem III.3.Prove that for all $n \geq 1$,

$$F_n \equiv 4^{n-1}(2^n - 1) \pmod{11}$$

Problem IV.8. (1) Find the multiplicative inverse of 15 modulo 49.

(2) Using (1), solve the linear equation/congruence $15x \equiv 8 \pmod{49}$.

Problem IV.9. Solve the congruences $5x \equiv 11 \pmod{37}$ and $11y \equiv 5 \pmod{37}$. If solutions exist, simplify $xy \pmod{37}$.

Problem IV.10. Consider the following modular dynamical system, which is neither additive nor multiplicative.

(a) Let $X = \mathbb{Z}/13$ and let $f : X \to X$ be given by

$$x \mapsto f(x) := x^2 + 3 \pmod{13}.$$

Draw the complete diagram for the dynamics of f.

(b) Let $A_0 = 0$ and let $A_{n+1} = f(A_n) \pmod{13}$ for all integers $n \geq 0$. What is $A_{2021} \pmod{13}$?

Problem IV.11.

(a) Compute the length of the cycles in the dynamics of $\boxed{\times a \pmod{8}}$ for every $a \in \Phi(8)$. Compare the length with $\varphi(8)$.
(b) Compute the length of the cycles in the dynamics of $\boxed{\times 3 \pmod{14}}$. Compare the length with $\varphi(14)$.

Problem IV.12. Compute (the natural representative of) $3^{10^{10^{10}}} \pmod{7}$.

Problem IV.13. A *Sophie Germain prime* is a prime number p such that $2p+1$ is also a prime. For example, $p = 2, 3, 5$ are Sophie Germain primes, but $p = 7$ is not (since $15 = 2 \cdot 7 + 1$ is not a prime).
Prove that if p is a Sophie Germain prime, then $2p+1$ is a divisor either of $2^p - 1$ or of $2^p + 1$, but not of both.

Problem IV.14. Suppose that p is a prime and $p \equiv 2 \pmod 3$. Prove that every integer is a cube modulo p. That is, prove that for every integer x there exists an integer a such that $x \equiv a^3 \pmod p$.

Problem IV.15. Consider the recursive sequence given by

$$a_0 = 3, \quad a_n = 3^{a_{n-1}}, \text{ for } n \geq 1$$

That is, $a_0 = 3,\ a_1 = 3^3,\ a_2 = 3^{3^3}, \ldots$. What is the last digit of a_{1000}?

Problem IV.16. Let $f(n)$ and $g(n)$ be two complex-valued functions of positive integers $n > 0$. Recall the definition of convolution

$$(f * g)(n) = \sum_{d \in \mathscr{D}(n)} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{ab=n \\ a,b>0}} f(a)g(b).$$

(a) Prove that the two functions $f * g$ and $g * f$ are one and the same.
(In other words: the convolution product is commutative.)

(b) Let $\epsilon(n)$ be the function defined by the rule

$$\epsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}.$$

Prove that $f = \epsilon * f$. Combined with (a), this tell us $f * \epsilon = f = \epsilon * f$.
(In other words: ϵ acts as the neutral element for the convolution.)

(c) Let $h : \mathbb{Z}_+ \to \mathbb{C}$ be a third function. Prove that

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

(In other words, the convolution product is associative.)

(d) Suppose that $f(1) \neq 0$. Define the function $i_f(n)$ by induction on the divisibility of n as follows. First define

(12.1.d.1) $$i_f(1) := \frac{1}{f(1)}.$$

Given an integer $n > 1$, assume we have defined $i_f(d)$ for all the proper positive divisors d of n, this is the set $\mathscr{D}_{\text{pr}}(n) := \mathscr{D}(n) \setminus \{n\}$. Then proceed to define

(12.1.d.2) $$i_f(n) := -\frac{1}{f(1)} \sum_{d \in \mathscr{D}_{\text{pr}}(n)} i_f(d) f\left(\frac{n}{d}\right).$$

Compute $i_f(n)$ for $n = 2, 3, 4, 5, 6$ in the particular case where f is the identity function: $f(n) = n$.

(e) Return to the general case where $f(n)$ is any function such that $f(1) \neq 0$, and i_f is defined by the formulae (12.1.d.1) and (12.1.d.2).

Prove that $i_f * f = \epsilon$.

Prove that if $j(n)$ is any other complex valued function such that $j * f = \epsilon$, then we necessarily have $j = i_f$.

Hint: look back to our proof of “uniqueness" of multiplicative inverses modulo m.

Problem IV.17.

(a) Compute $\ell(a)$ in the 3×4 cases: $a = 2, 3, 6$ and $p = 7, 11, 13, 17$.
(b) For the primes $p = 7, 11, 13, 17$, list all the primitive roots modulo p.

Problem IV.18. Let $a \in \Phi(m)$ for a modulus m, and define $\ell(a)$ to be the smallest positive integer such that

$$a^{\ell(a)} \equiv 1 \pmod{m};$$

that is, $\ell(a)$ is the length of the cycles in the multiplicative modular dynamics given by

$$\boxed{\times a \pmod{m}} : \Phi(m) \to \Phi(m).$$

We have already seen that $\ell(a) \mid \varphi(m)$.

(a) Prove that if e is any integer such that $a^e \equiv 1 \pmod{m}$, then $\ell(a) \mid e$.
Hint: use the division algorithm with respect to e and $\ell(a)$ arriving at a contradiction to the minimality of $\ell(a)$.
(b) Suppose p is an odd prime and q is a prime factor of $2^p - 1$. Prove that $q \equiv 1 \pmod{2p}$.

Problem IV.19. Find the smallest positive integer a such that $2^a \equiv 11 \pmod{p}$, for the two primes: $p = 23$ and $p = 37$.

Problem IV.20. Find Alice and Bob's secret number S, if $g = 3$, $p = 17$, $A = 8$ and $B = 7$.

Problem IV.21. Prove that if p is any prime and a and b are any nonzero integers such that $a \equiv b \pmod{p^2 - p}$, then $a^a \equiv b^b \pmod{p}$.