Supplementary Materials for Chapter V

Xu Gao

MATH 110 | Introduction to Number Theory | Summer 2023

July 23, 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 V

Modular Polynomials

1 Polynomials

Terminology 1.1. A homomorphism of rings $\phi\colon R \to S$ induces a homomorphism

$$\phi_*\colon R[T] \longrightarrow S[T]$$

mapping a polynomial

$$f(T) = a_n T^n + \cdots + a_1 T + a_0 \in R[T],$$

to a polynomial

$$\phi_* f(T) = \phi(a_n)T^n + \cdots + \phi(a_1)T + \phi(a_0) \in S[T].$$

If this is the case, we say $f(T)$ **descends** to $\phi_* f(T)$, or $f(T)$ is a **lifting** of $\phi_* f(T)$.

Usually, we do not distinguish the polynomial $f(T)$ and $\phi_* f(T)$ in notations. Rather, when we treat $f(T)$ as a polynomial over S, we actually work with $\phi_* f(T)$.

When we say $s \in S$ is a *root of* $f(T)$ *in* S, what we actually mean is $\phi_* f(s) = 0$, not $f(s) = 0$, which a priori doesn't make sense.

Example 1.2. $\overline{1}$ is a root of $3T^2 + 2T$ in $\mathbb{F}_5$.

Terminology 1.3. Suppose we have a homomorphism of rings $\phi\colon R \to S$. Let $f(T)$ be a polynomial over R. Then any root x of $f(T)$ in R *descends* to a root $\phi(x)$ in S:

$$\begin{aligned}\phi_* f(\phi(x)) &= \phi(a_d)\phi(x)^d + \cdots + \phi(a_1)\phi(x) + \phi(a_0)\\ &= \phi(a_d x^d + \cdots + a_1 x + a_0)\\ &= \phi(f(x)) = \phi(0) = 0.\end{aligned}$$

However, the converse is not true. Eventhrough ϕ is surjective, it doesn't imply that any root of $f(T)$ in S can be *lifted* to a root in R.

Example 1.4. $T^2 + 1$ has a root $\overline{1}$ in $\mathbb{F}_2$, but there is no root of $T^2 + 1$ in $\mathbb{Z}$.

2 Arithmetic on modular polynomials

The analogy between $\mathbb{Z}$ and $\mathbb{F}_p[T]$ is outstanding. Try to transplant results about arithmetic of integers to polynomials.

For instance,

- absolute value (size) of integers $\rightsquigarrow$ degree of polynomials
- ± 1 (the units) $\rightsquigarrow$ nonzero constant polynomials
- positive integers $\rightsquigarrow$ monic polynomials
- prime numbers $\rightsquigarrow$ irreducible polynomials
- rational numbers $\rightsquigarrow$ rational functions
- rational solutions of equations $\rightsquigarrow$ rational family solutions of equations
- etc.

3 polydiv

Please find the "polydiv" files (a .pdf, a .sty, and a .tex) on Canvas.

- The "polydiv.sty" provides LaTeX commands to deal with arithmetic of polynomials modulo p.
- Read the "polydiv.pdf" for how to use it.
- To use this package, put both the "polydiv.sty" and "polydiv.tex" in your LaTeX working folder.
- The purpose of this package is to half-automatically generate exercises on arithmetic of polynomials.

Exercise 3.1. Choose a modulus p and then pick up two polynomials f and g over $\mathbb{F}_p$. Practice the long division and the Euclidean algorithm for them and then verify your answer by the "polydiv" program. (Refer "polydiv.pdf" for how to use it.)

Exercise 3.2. If you try to run this program with non-prime modulus, you may get some nonsense results. Can you explain why we shouldn't expect the program to work in that situation?

Problems

Problem V.1.

(a) Let $f(T)$ be an irreducible polynomial modulo p, and consider any $a \in \mathbb{F}_p$ such that $a \neq \overline{0}$. Prove that $g(T) := af(T)$ is also irreducible.

(b) Let $f(T)$ be a polynomial modulo p, a prime, of degree 2 or 3. Prove that $f(T)$ is irreducible if and only if $f(T)$ has no roots modulo p.

Hint: prove the contrapositive, look at the degrees of the factors of $f(T)$ and invoke a theorem from class.

Give an example illustrating why this reasoning does not help us determine if a given polynomial (modulo p) of degree ≥ 4 is irreducible.

Problem V.2. Let $p = 5$ and consider two polynomials mod p:

$$f(T) = T^3 + \overline{3}T^2 + \overline{2}T + 1$$

$$g(T) = \overline{2}T^4 + \overline{4}T^3 + T^2 + \overline{3}T + \overline{4}.$$

(a) Find the two polynomials mod p: $q(T)$ and $r(T)$, such that $\deg r < 3$ and

$$g(T) = f(T)q(T) + r(T).$$

(b) Apply the Division Algorithm to find the greatest common divisor of $f(T)$ and $g(T)$. Show your work. As in the case with integers, the gcd is the last non-zero remainder.

(c) Prove or disprove: The gcd that you have found in (b) is irreducible.

Hint: use Problem V.1.

(d) Find the unique factorizations of $f(T)$ and $g(T)$ into irreducible polynomials mod p.