Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 22, 2023

What we have seen last week

- Primality testing
- Modular exponential $\exp_a : (\mathbb{Z}/\varphi(m), +) \longrightarrow (\Phi(m), \times)$
- Primitive roots $\log_a$
- Discrete logarithm
- Some cryptography
- Properties of $\varphi(\,\cdot\,)$ multi. $\varphi(m) = m \prod_{\substack{p \mid m \\ \text{prime}}} \left(1 - \frac{1}{p}\right)$
- Dirichlet convolution

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

$$|\Phi_\ell(m)| \le \varphi(\ell)$$

Today's topics

Polynomials modulo p

- Division of polynomials $\leftrightsquigarrow$ $x = q \cdot y + r$
- Divisibility of polynomials $\leftrightsquigarrow$ $m \mid n$
- Monic polynomials $\leftrightsquigarrow$ positive integers
- Greatest common divisor
- Least common multiple

Polynomials

what we'll focus on

Definition 17.1

Let R be a ring (such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/m$, etc.). Then a ***polynomial over*** R (or, a ***polynomial with coefficients in*** R) is an expression

$$f(T) = a_d T^d + \cdots + a_1 T + a_0,$$

where T is the variable and the coefficients $a_0, a_1, \cdots, a_d$ belongs to R. The set of polynomials over R is denoted by $R[T]$.

The addition and multiplication of polynomials are defined in the obvious way. (So, using terminology from Algebra, $(R[T], +, 0, \cdot, 1)$ is a ring.)

Polynomials

Example 17.2

Try to simplify $(\overline{2}T^2 + \overline{1}T)(\overline{3}T + \overline{2})$ over $\mathbb{Z}/6$.

$$\begin{aligned}
(\overline{2}T^2 + T)(\overline{3}T + \overline{2}) &= \overline{2}T^2 \cdot \overline{3}T + T \cdot \overline{3}T + \overline{2}T^2 \cdot \overline{2} + T \cdot \overline{2} \\
&= \overline{2} \cdot \overline{3}T^3 + \overline{3}T^2 + \overline{2} \cdot \overline{2}T^2 + \overline{2}T \\
&= \overline{6}T^3 + \overline{3}T^2 + \overline{4}T^2 + \overline{2}T \\
&= \cancel{\overline{6}T^3} + \overline{3+4}T^2 + \overline{2}T \\
&= T^2 + \overline{2}T.
\end{aligned}$$

Polynomials

Polynomials over $\mathbb{Z}/m$ can be obtained from those over $\mathbb{Z}$ through the modulo reduction process:

$$\begin{array}{c} a_d T^d + \cdots + a_1 T + a_0 \\ \Big\downarrow \pmod{m} \\ \overline{a_d} T^d + \cdots + \overline{a_1} T + \overline{a_0} \end{array}$$

$$\begin{array}{c} a \in \mathbb{Z} \\ \downarrow \\ [a] \in \mathbb{Z}/m \end{array}$$

Such a process gives a surjective map respecting the addition, multiplication, and their neutral elements. (Using terminology from Algebra, it is a surjective homomorphism.)

Definition 17.3

Two integer polynomials $f(T)$ and $g(T)$ are ***congruence modulo*** m if for each exponent d, the coefficients of T^d in $f(T)$ and $g(T)$ are congruence modulo m.

This gives an equivalence relation on $\mathbb{Z}[T]$ and each equivalence class is called a ***polynomial modulo*** m.

Then the reduction map in previous slide identify the quotient set of $\mathbb{Z}[T]$ up to congruence modulo m (i.e. the set of polynomial modulo m) with $\mathbb{Z}/m[T]$. We'll thus not distinguish the two structures.

Polynomials

Polynomials over $\mathbb{Z}/m$ may behave very different from the usual ones (over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$). However, when p is a prime, polynomials modulo p behave well.

In what follows, we will use the notation $\mathbb{F}_p$ to denote the (ring) structure $\mathbb{Z}/p$ (where p is a prime). The letter $\mathbb{F}$ stands for "*field*", which means a ring in which nonzero = invertible.

$c_d T^{\deg}$ + lower terms

Definition 17.4

The ***degree*** of a polynomial $f(T)$ is the largest exponent d, for which the coefficient of T^d is nonzero.

Usually, the degree of the zero polynomial is by convenience -1.

Example 17.5

The degree of the integer polynomial $6T^3 + 7T^2 + 2T$ is 3, while the degree of the polynomial $\underset{\overline{0}}{\overline{6}}T^3 + \overline{7}T^2 + \overline{2}T$ over $\mathbb{Z}/6$ is 2.

Theorem 17.6

Let f, g be two nonzero polynomials over $\mathbb{F}_p$, then we have

$$\deg(fg) = \deg f + \deg g.$$

Proof. Suppose the leading terms of f and g are $\bar{a}T^{\deg(f)}$ and $\bar{b}T^{\deg(g)}$ respectively. Then we have

$$\begin{aligned} fg &= (\bar{a}T^{\deg(f)} + \text{lower terms})(\bar{b}T^{\deg(g)} + \text{lower terms}) \\ &= \overline{ab}T^{\deg f + \deg g} + \text{lower terms}. \end{aligned}$$

This is the only critical $\rightarrow$ $\neq \bar{0}$ $p \nmid a$ $p \nmid b$

Note that, from $\bar{a} \neq \mathbf{0}$ and $\bar{b} \neq \mathbf{0}$, we have $p \nmid ab$ since p is a prime. Therefore, the degree of fg is $\deg f + \deg g$. $\square$

Theorem 17.6

Let f, g be two nonzero polynomials over $\mathbb{F}_p$, then we have

$$\deg(fg) = \deg f + \deg g.$$

N.B. this is not true for $\mathbb{Z}/m$ with m composite.
E.g. over $\mathbb{Z}/6$, we have

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

But the degrees of them are $2 + 1 \neq 2$.

Definition 17.7

We say that a congruence class $\overline{a} \in \mathbb{Z}/m$ is a ***root*** of the integer polynomial $f(T) \in \mathbb{Z}[T]$, or the integer a is a ***root of*** $f(T)$ ***modulo*** m, if $f(a) \equiv 0 \pmod{m}$.

an integer

Example 17.8

Let's consider 5 and the polynomial $f(T) = 3T^2 + 2T$.

The congruence classes $\overline{0}$ and $\overline{1}$ are roots of f in $\mathbb{F}_5$, while $\overline{2}$, $\overline{3}$, and $\overline{4}$ are not.

$3 \cdot 0^2 + 2 \cdot 0 = 0 \equiv 0$

$3 \cdot 1^2 + 2 \cdot 1 = 5 \equiv 0$

$$\begin{cases} 3 \cdot 2^2 + 2 \cdot 2 = 16 \equiv 1 \not\equiv 0 \\ 3 \cdot 3^2 + 2 \cdot 3 = 33 \equiv 3 \not\equiv 0 \\ 3 \cdot 4^2 + 2 \cdot 4 = 56 \equiv 1 \not\equiv 0 \end{cases}$$

Theorem 17.9

Consider a linear integer polynomial $f(T) = aT + b$. If $p \nmid a$, then f has a unique root in $\mathbb{F}_p$.

Proof. If $p \nmid a$, then a is invertible modulo p. Hence, by its cancelling property, we get a unique congruence class $-[a]_p^{-1}[b]_p$ being the root of $f(T)$ in $\mathbb{F}_p$. $\square$

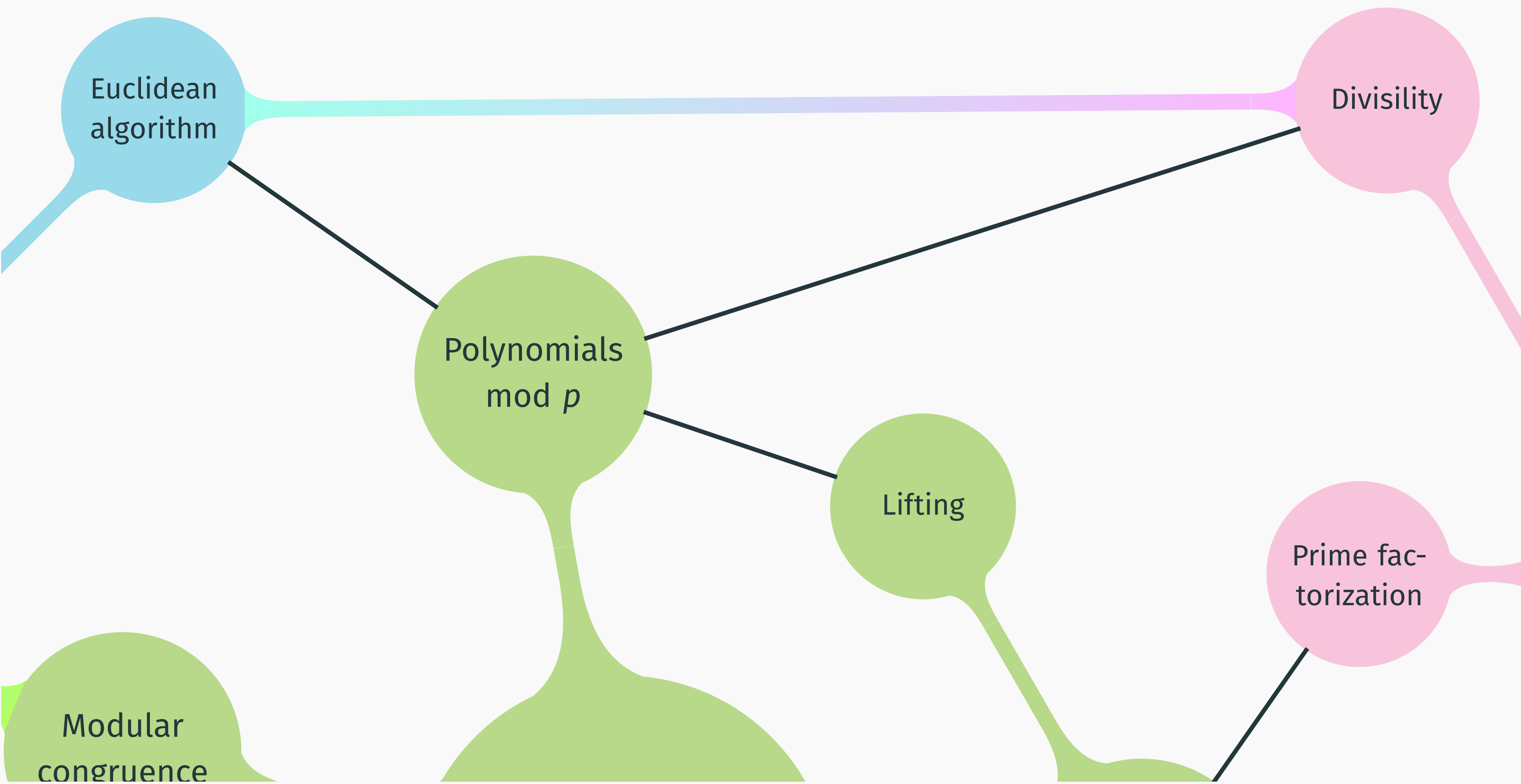
Theorem 17.9

Consider a linear integer polynomial $f(T) = aT + b$. If $p \nmid a$, then f has a unique root in $\mathbb{F}_p$.

N.B. this is not true for $\mathbb{Z}/m$ with m composite.
E.g. in $\mathbb{Z}/6$, the linear polynomial $3T + 1$ has no roots, while $3T + 3$ has three roots: $\overline{1}$, $\overline{3}$, and $\overline{5}$.

Division of polynomials mod p

Division of polynomials mod p



Division of polynomials mod p

Theorem 17.10 (Division of polynomials)

Let $f(T)$ and $g(T)$ be two polynomials over $\mathbb{F}_p$, then there are polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ such that

$$f(T) = q(T)g(T) + r(T), \qquad \deg(r) < \deg(g).$$

Proof. Suppose the leading terms of f and g are $\overline{a}T^{\deg(f)}$ and $\overline{b}T^{\deg(g)}$ respectively. Since p is a prime, we can always solve the equation $a = xb$ in $\mathbb{F}_p$. Then $f(T) - (xT^{\deg(f)-\deg(g)})g(T)$ has degree strictly less than $\deg(f)$. Replace $f(T)$ by it and repeat this process, we will get a polynomial of degree less than $\deg(g)$ in the last step. $\square$

Division of polynomials mod p

Example 17.11

Over $\mathbb{F}_5$. Consider the polynomials $T^3 + \overline{4}T + \overline{2}$ and $T^2 + T + \overline{3}$.

$$
\begin{array}{r|rrrr}
 & & & T & -\overline{1} \\
\cline{2-5}
T^2 + T + \overline{3} & T^3 + & \overline{0}T^2 + & \overline{4}T + & \overline{2} \\
 & T^3 + & T^2 + & \overline{3}T & \downarrow \\
\cline{2-4}
 & & -T^2 + & T + & \overline{2} \\
 & & -T^2 - & T - & \overline{3} \\
\cline{3-5}
 & & & \overline{2}T + & \overline{5}
\end{array}
\qquad\qquad
\begin{array}{r|rrrr}
 & & & T & +\overline{4} \\
\cline{2-5}
T^2 + T + \overline{3} & T^3 + & \overline{0}T^2 + & \overline{4}T + & \overline{2} \\
 & T^3 + & T^2 + & \overline{3}T & \downarrow \\
\cline{2-4}
 & & \overline{4}T^2 + & T + & \overline{2} \\
 & & \overline{4}T^2 + & \overline{4}T + & \overline{2} \\
\cline{3-5}
 & & & \overline{2}T + & \overline{0}
\end{array}
$$

Example 17.12

Over $\mathbb{F}_5$. Consider the polynomials $\overline{2}T^3 + \overline{3}T^2 + T + \overline{1}$ and $\overline{3}T^2 + T + \overline{2}$.

$$
\begin{array}{r|l}
 & \overline{4}T + \overline{3} \\
\hline
\overline{3}T^2 + T + \overline{2} & \overline{2}T^3 + \overline{3}T^2 + T + \overline{1} \\
 & \underline{\overline{2}T^3 + \overline{4}T^2 + \overline{3}T} \quad \downarrow \\
 & \overline{4}T^2 + \overline{3}T + \overline{1} \\
 & \underline{\overline{4}T^2 + \overline{3}T + \overline{1}} \\
 & 0
\end{array}
$$

Note that we cannot do division of integer polynomials this time.

Division of polynomials mod p

Definition 17.13

Let $f(T)$ and $g(T)$ be two polynomials over $\mathbb{F}_p$. Then we say f ***divides*** g, or f is a ***divisor*** of g, or g is a multiple of f, written as $f \mid g$ if there is another $h(T) \in \mathbb{F}_p[T]$ such that

$$\cancel{f}\,g(T) = h(T)\,\cancel{g}\,f(T).$$

Example 17.14

Over $\mathbb{F}_5$, $\overline{3}T^2 + T + \overline{2}$ divides $\overline{2}T^3 + \overline{3}T^2 + T + \overline{1}$.

Division of polynomials mod p

It is possible that two distinct polynomials divides each other, this is due to the fact that every nonzero element of $\mathbb{F}_p$ is a unit. Hence, any two polynomials different only by a nonzero constant factor would divide each other.

Among the polynomials over $\mathbb{F}_p$, the following ones play as the role of positive integers.

Definition 17.15

A polynomial $f(T)$ over $\mathbb{F}_p$ is ***monic*** if its leading term (the term of degree $\deg(f)$) has coefficient $\overline{1}$.

So a monic polynomial looks like this: T^n+ lower terms.

Division of polynomials mod p

poly ⟷ integers
monic poly ⟷ positive integers

You can verify that the divisibility of ***monic*** polynomials is also a ***partial order*** satisfying the ***2-out-of-3 principle***.

We also have the notions of $\gcd$ and lcm.

Definition 17.16 (Greatest common divisor)

Let $a(T)$ and $b(T)$ be two nonzero polynomials over $\mathbb{F}_p$. Then a monic polynomial $g(T)$ is called a ***greatest common divisor*** of them if it satisfies the following two defining properties:

1. $g \mid a$ and $g \mid b$, i.e. g is a common divisor of a and b; and
2. if d is any common divisor of a and b, then $d \mid g$.

We will use $\gcd(a, b)(T)$ to denote the greatest common divisor of $a(T)$ and $b(T)$.

Definition 17.17 (Least common multiple)

Let $a(T), b(T)$ be two nonzero polynomials over $\mathbb{F}_p$. Then a monic polynomial $l(T)$ is called a ***least common multiple*** of them if it satisfies the following two defining properties:

1. $a \mid l$ and $b \mid l$, i.e. l is a common multiple of a and b; and
2. if m is any common multiple of a and b, then $l \mid m$.

We will use $\mathrm{lcm}(a, b)(T)$ to denote the least common multiple of $a(T)$ and $b(T)$.

Theorem 17.18

$$\gcd(a, b)(T) \cdot \mathrm{lcm}(a, b)(T) = a(T) \cdot b(T)$$

After Class Work

After Class Work

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

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

After Class Work

Exercise 17.1

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 17.2

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?

Terminology

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 $\phi_* f(T)$.

Terminology

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.

E.g. $\bar{1}$ is a root of $3T^2 + 2T$ in $\mathbb{F}_5$.

After Class Work

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.

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

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.

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