Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 24, 2023

What we have seen last time

- Division of polynomials
- Divisibility of polynomials
- Monic polynomials
- Greatest common divisor
- Least common multiple

Today's topics

Polynomials modulo p

- (Euclidean) division algorithm
- Units and irreducible polynomials
- Unique prime factorization
- Coprime polynomials
- Roots and degree

(Euclidean) division algorithm

(Euclidean) division algorithm

1. Start with two nonzero polynomials $f(T), g(T) \in \mathbb{F}_p[T]$, assume $\deg(f) \geq \deg(g)$.
2. Divide $f(T)$ by $g(T)$

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

3. If $r = \mathbf{0}$, ***halt***. Otherwise, repeat the previous steps with the pair (f, g) replaced by (g, r).
4. Continue until your remainder is the zero polynomial, this process will terminate in finite steps. Output the last nonzero remainder.

(Euclidean) division algorithm

Example 18.1

Over $\mathbb{F}_5$. Consider $\underbrace{T^4 + T^2 + \overline{3}T + \overline{1}}_{f}$ and $\underbrace{\overline{2}T^3 + \overline{4}T^2 + \overline{3}T + \overline{1}}_{g}$.

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

$$f = (\overline{3}T + \overline{4})g + \underbrace{T^2 + \overline{3}T + \overline{2}}_{r} \qquad g = (\overline{2}T + \overline{3})r + \underline{0}$$

(Euclidean) division algorithm

Theorem 18.2

Let $f(T), g(T) \in \mathbb{F}_p[T]$. Up to a nonzero constant factor, the output (last nonzero remainder) of the (Euclidean) division algorithm for $f(T)$ and $g(T)$ is their greatest common divisor.

Proof. Starting with the following lemma, basically the same as in Lecture 2. $\square$

Lemma 18.3

Let $f(T), g(T) \in \mathbb{F}_p[T]$. If there are polynomials $q(T)$ and $r(T)$ such that $f(T) = q(T)g(T) + r(T)$, then we have

$$\gcd(f, g) = \gcd(g, r).$$

$(\mathbb{F}_5)$

$\bar{2}T + \bar{3}$

$\downarrow$

$T + \bar{4}$

$\gcd(a, 0) = |a|$ $\quad$ $\gcd(f, 0) =$ monic-form of f

Corollary 18.4

Let $f(T), g(T) \in \mathbb{F}_p[T]$. Then $\gcd(f, g) = \bar{1}$ if and only if there are polynomials $h_1(T), h_2(T) \in \mathbb{F}_p[T]$ such that

$$f(T)h_1(T) + g(T)h_2(T) = \bar{1}.$$

If this is the case, we say $f(T)$ and $g(T)$ are ***coprime***.

We also have induction of coprime:

- If $f \mid h$, $g \mid h$, and f, g are coprime, then $fg \mid h$.
- If f, g are coprime, f, h are coprime, then f, gh are coprime.

Prime factorization

Definition 18.5

A ***unit*** in $\mathbb{F}_p[T]$ is a polynomial $f(T) \in \mathbb{F}_p[T]$ dividing the constant polynomial $\bar{1}$.

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

By theorem **??**, we must have $\deg(f) \leqslant \deg(\bar{1}) = 0$. Therefore, $f(T)$ must be a constant polynomial. Note that the zero polynomial cannot be a unit. Hence, units in $\mathbb{F}_p[T]$ are precisely the nonzero constant polynomials.

$\bar{1}, \bar{2}, \cdots, \overline{p-1}$

Prime factorization

Definition 18.6

A polynomial $f(T)$ in $\mathbb{F}_p[T]$ is ***irreducible*** if

1. it is neither zero nor a unit (equivalently, $\deg(f) > 0$);
2. if there are polynomials $g(T), h(T) \in \mathbb{F}_p[T]$ such that

$$f(T) = h(T)g(T),$$

   then one of them is a unit.

Example 18.7

For any $\alpha \in \mathbb{F}_p$, the linear polynomial $T - \alpha$ is irreducible.

$1 = \deg(T-\alpha) = \deg(hg) = \deg(h) + \deg(g) \Rightarrow$ one of h, g to be a unit.

Example 18.8

Over $\mathbb{F}_5$, the polynomial $T^2 + \overline{2}$ is irreducible.

Suppose, for the sake of contradiction, there are polynomials $g(T), h(T) \in \mathbb{F}_p[T]$ such that

$$T^2 + \overline{2} = h(T)g(T),$$

but none of them is a unit. Then we must have $\deg(g), \deg(h) \geqslant 1$. But $\deg(g) + \deg(h) = \deg(gh) = 2$. Hence, both $g(T)$ and $h(T)$ are linear polynomials.

$T^2 + \bar{2} = (T + \bar{a})(T + \bar{b})$

If $g(T) = T + \overline{a}$, then from $g(T) \mid T^2 + \overline{2}$, we see that $\overline{-a}$ is a root of $T^2 + \overline{2}$ in $\mathbb{F}_5$. However, you can verify that none of the elements in $\mathbb{F}_5$ is a root of $T^2 + \overline{2}$.

$0^2 + 2 = 2$ $\quad 2^2 + 2 = 6 \equiv 1$ $\quad 4^2 + 2 = 18 \equiv 3$

$1^2 + 2 = 3$ $\quad 3^2 + 2 = 11 \equiv 1$

Theorem 18.9

Let $f(T) \in \mathbb{F}_p[T]$. Then it can be uniquely written as

$$f(T) = C \cdot P_1(T)^{e_1} \cdots P_n(T)^{e_n},$$

where C is a nonzero constant, each $P_i(T)$ is a ***monic irreducible polynomial****, and $e_1, \cdots, e_n > 0$.*

prime

Proof. Same as the fundamental theorem of arithmetic. $\square$

Roots and degree

Roots and degree

Lemma 18.10

$\bar{a} \in \mathbb{F}_p$ is a root of $f(T) \in \mathbb{F}_p[T]$ if and only if $T - \bar{a} \mid f(T)$.

Proof. By the division of polynomials over $\mathbb{F}_p$ (theorem **??**), there are polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ such that

$$f(T) = q(T) \cdot (T - \bar{a}) + r(T), \qquad \deg(r) < \deg(T - \bar{a}) = 1.$$

Therefore, r is a constant.

$T - \bar{a} \mid f \iff r = 0 \iff f(\bar{a}) = 0$

If we plug in $\bar{a}$, we get:

$$f(\bar{a}) = q(\bar{a}) \cdot (\bar{a} - \bar{a}) + r. \quad f(\bar{a}) = r$$

Hence, $\bar{a}$ is a root of $f(T)$ in $\mathbb{F}_p$ if and only if $r = 0$, which means $T - \bar{a} \mid f(T)$. ☐

Lemma 18.11

Let $\overline{a}$ and $\overline{b}$ be two congruence classes in $\mathbb{F}_p$. Then the polynomials $T-\overline{a}$ and $T-\overline{b}$ are coprime if and only if $\overline{a} \neq \overline{b}$.

Proof. ($\Rightarrow$) If there are polynomials $h_1(T), h_2(T) \in \mathbb{F}_p[T]$ such that

$$(T-\overline{a})h_1(T) + (T-\overline{b})(T)h_2(T) = \overline{1}.$$

as polynomials

Plug in $\overline{a}$, we get

$$(\overline{a}-\overline{b})(\overline{a})h_2(\overline{a}) = \overline{1}.$$

as elements

This means $\overline{a}-\overline{b}$ is a unit. Hence, $\overline{a} \neq \overline{b}$. ∎

Roots and degree

Lemma 18.11

Let $\overline{a}$ and $\overline{b}$ be two congruence classes in $\mathbb{F}_p$. Then the polynomials $T - \overline{a}$ and $T - \overline{b}$ are coprime if and only if $\overline{a} \neq \overline{b}$.

Proof. ($\Leftarrow$) If $\overline{a} \neq \overline{b}$, then $\overline{a} - \overline{b}$ is a unit. Suppose $\overline{c} \in \mathbb{F}_p$ is its inverse. Then we have

$$\overline{-c}(T - \overline{a}) + \overline{c}(T - \overline{b}) = \overline{1}.$$

This means $T - \overline{a}$ and $T - \overline{b}$ are coprime. $\square$

Roots and degree

Theorem 18.12

The number of roots of $f(T) \in \mathbb{F}_p[T]$ in $\mathbb{F}_p$ is at most $\deg(f)$.

Proof. By lemma 18.10, for any root $\overline{a}$ of $f(T)$ in $\mathbb{F}_p$, we have $T - \overline{a} \mid f(T)$. By lemma 18.11, different roots give coprime factors of $f(T)$. Therefore, we have

$$\prod_{\overline{a} \text{ is a root of } f(T) \text{ in } \mathbb{F}_p} (T - \overline{a}) \mid f(T).$$

In particular, the degree of the left-hand side is at most $\deg(f)$. But each $T - \overline{a}$ is of degree 1. Hence, the degree of the left-hand side is the number of roots of $f(T) \in \mathbb{F}_p[T]$ in $\mathbb{F}_p$. $\square$

Roots and degree

Example 18.13

The theorem is not true for composite modulus m. For example, when the polynomial $T^2 - \overline{1}$ has degree 2, but has 4 roots in $\mathbb{F}_8$.

$$\overline{0}^2 - \overline{1} = \overline{0-1} = \overline{7} \qquad \overline{1}^2 - \overline{1} = \overline{1-1} = \overline{0}$$

$$\overline{2}^2 - \overline{1} = \overline{4-1} = \overline{3} \qquad \overline{3}^2 - \overline{1} = \overline{9-1} = \overline{0}$$

$$\overline{4}^2 - \overline{1} = \overline{16-1} = \overline{7} \qquad \overline{5}^2 - \overline{1} = \overline{25-1} = \overline{0}$$

$$\overline{6}^2 - \overline{1} = \overline{36-1} = \overline{3} \qquad \overline{7}^2 - \overline{1} = \overline{49-1} = \overline{0}$$

Finnishing proving primitive root theorem

Corollary 18.14

For each divisor ℓ *of* $p-1$*, we have either* $\Phi_\ell(p) = \varnothing$ *or* $|\Phi_\ell(p)| = \varphi(\ell)$.

Proof. Recall that

$$\Phi_\ell(p) := \{a \in \Phi(p) \mid \ell(a) = \ell\}.$$

Hence, any element $a \in \Phi_\ell(p)$ defines a root $\overline{a}$ of the polynomial $T^\ell - 1$ in $\mathbb{F}_p$. By theorem 18.12, there are at most ℓ roots in $\mathbb{F}_p$.

Suppose $\Phi_\ell(p)$ is nonempty. For $a \in \Phi_\ell(p)$, we know $\overline{a}^0, \cdots, \overline{a}^{\ell-1}$ are distinct congruence classes. In this way, we get ℓ distinct roots of $T^\ell - 1$ in $\mathbb{F}_p$. Hence, they are all the roots in $\mathbb{F}_p$. We thus have

$$\Phi_\ell(p) \subseteq \{a^e \pmod{p} \mid e = 0, \cdots, \ell - 1\} := \langle a \rangle.$$

Finnishing proving primitive root theorem

We can further identify $(\langle a \rangle, \cdot, 1)$ with the structure $(\mathbb{Z}/\ell, +, 0)$ through the modular exponential $[e]_\ell \mapsto a^e \pmod p$.

Then we see that

$\ell(a^e \pmod p) = \ell$ i.e. $a^e \in \Phi_\ell(p)$

$\iff$ the multiplicative dynamic of $a^e \pmod p$ on $\langle a \rangle$ consists of only one circle

$\iff$ the additive dynamic of $[e]_\ell$ on $\mathbb{Z}/\ell$ consists of only one circle

$\iff \gcd(e, \ell) = 1$ by theorem **??**

Namely, through above identification, $\Phi_\ell(p)$ is identified with the unit group $(\mathbb{Z}/\ell)^\times$ of $\mathbb{Z}/\ell$, or equivalently, the set $\Phi(\ell)$. Consequently, $|\Phi_\ell(p)| = \varphi(\ell)$. $\square$

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.

Exercise 18.1

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 18.2

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?

After Class Work

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