Polynomials over $\mathbb{F}_p$.

1. What are polynomials?

S is a ring (i.e. It has addition/multiplication. 0, 1)

e.g. $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ...

$S = \mathbb{Z}/m$.

Defn. A **polynomial** over S is an expression

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

where the coefficents $a_0, \cdots, a_d \in S$.

The set of polynomials over S is denoted by $S[T]$.

The **degree** of f, denoted by **$\deg f$**, is the largest d s.t. $a_d \neq 0$ in S.

Convention: $\deg 0 = -1$.

- We will focus on $S = \mathbb{F}_p$. ($\mathbb{F}$ is for "field", which means nonzero = unit)

Defn. **$\mathbb{F}_p$** is the (ring) structure $(\mathbb{Z}/p, +, \cdot, \bar{0}, \bar{1})$.

e.g. $p = 5$ $\quad f(T) = \bar{4}T + \bar{2}$ $\quad g(T) = \bar{3}T^2 + \bar{2}T$

$\deg = 1$ $\quad\quad \deg = 2$

2. **Theorem.** $f(T), g(T) \in \mathbb{F}_p[T]$ are nonzero. Then

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

Proof. $f(T) = \bar{a}_{d_1} T^{d_1} +$ lower terms $\quad g(T) = \bar{b}_{d_2} T^{d_2} +$ lower terms

$$f(T)g(T) = \bar{a}_{d_1} \bar{b}_{d_2} T^{d_1+d_2} + \text{lower terms}$$

$$\bar{a}_{d_1} \neq \bar{0} \text{ and } \bar{b}_{d_2} \neq \bar{0} \Rightarrow \bar{a}_{d_1} \bar{b}_{d_2} = \overline{a_{d_1} b_{d_2}} \neq \bar{0}.$$

Since p is a prime.

Rmk: If we consider polynomials over $\mathbb{Z}/m$ where m is composite, then the thm fails.

e.g. $m = 6$ $\quad f(T) = \bar{2}T^2 + T$, $g(T) = \bar{3}T + \bar{2}$

$\deg f = 2$, $\deg g = 1$.

$$f(T)g(T) = (\bar{2}T^2 + T)(\bar{3}T + \bar{2}) = \bar{2}\cdot\bar{3}T^3 + \bar{2}\cdot\bar{2}T^2 + \bar{3}T^2 + \bar{2}T$$

$$= \bar{0}\cdot T^3 + \bar{4}T^2 + \bar{2}T. \qquad \deg fg = 2 \neq \deg f + \deg g.$$

3. Roots of a polynomial.

Defn. An element $a \in \mathbb{F}_p$ is called a **root** of $f(T) \in \mathbb{F}_p[T]$ if $f(a) = \bar{0}$.

e.g. $p=5$, $f(T) = \bar{3}T^2 + \bar{2}T$

Then $\bar{1}$ is a root of f: $\bar{3}\cdot\bar{1}^2 + \bar{2}\cdot\bar{1} = \bar{3}+\bar{2} = \bar{0}$.

$\bar{2}$ is NOT a root of f: $\bar{3}\cdot\bar{2}^2 + \bar{2}\cdot\bar{2} = \bar{2}+\bar{4} = \bar{1}$.

$\bar{3}$ is NOT a root of f: $\bar{3}\cdot\bar{3}^2 + \bar{2}\cdot\bar{3} = \bar{2}+\bar{1} = \bar{3}$

$\bar{4}$ is NOT a root of f: $\bar{3}\cdot\bar{4}^2 + \bar{2}\cdot\bar{4} = \bar{3}+\bar{3} = \bar{1}$

$\bar{0}$ is a root of f: $\bar{3}\cdot\bar{0}^2 + \bar{2}\cdot\bar{0} = \bar{0}$

Prop. Consider a linear polynomial $f(T) = aT + b \in \mathbb{F}_p[T]$ with $a \neq \bar{0}$ in $\mathbb{F}_p$.
Then $f(T)$ has a unique root in $\mathbb{F}_p$.

If $a \neq \bar{0}$, then it is a unit. Let a^{-1} be the multiplicative inverse of a.

Then $aT + b = \bar{0} \iff T + a^{-1}b = \bar{0} \iff T = -a^{-1}b$

4. Division algorithm in polynomials mod p.

Theorem. $f(T), g(T) \in \mathbb{F}_p[T]$. Assume $g(T)$ is nonzero.

Then there exist polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ s.t.

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

e.g. $p=5$ $f(T) = T^3 + \bar{4}T + \bar{2}$, $g(T) = T^2 + T + \bar{2}$

$$
\begin{array}{r|l}
 & T - \bar{1} \leftarrow q(T) \\
\hline
T^2 + T + \bar{2} & T^3 + \bar{0}\,T^2 + \bar{4}\,T + \bar{2} \\
 & T^3 + T^2 + \bar{2}\,T \\
\cline{2-2}
 & -T^2 + \bar{2}\,T + \bar{2} \\
 & -T^2 - T - \bar{2} \\
\cline{2-2}
 & \bar{3}\,T + \bar{4} \swarrow r(T)
\end{array}
$$

$f(T) = g(T)(T - \bar{1}) + (\bar{3}T + \bar{4})$

$\deg r(T) = 1 < \deg g = 2$

5. Divisibility of polynomials.

Defn. $f(T), g(T) \in \mathbb{F}_p[T]$

- Say f divides g if there is $h(T) \in \mathbb{F}_p[T]$ s.t.

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

$f \mid g$

By thm 2. $f \mid g \Rightarrow \deg f \leq \deg g$

- Say f is a unit polynomial if $f \mid \bar{1}$ ← the constant polynomial $\bar{1}$.

$f \mid \bar{1} \Rightarrow \deg f \leq 0$

But $f \neq 0 \Rightarrow \deg f = 0$

Note that: unit polynomial = nonzero constant polynomials.

$\bar{a} \in \mathbb{F}_p \quad \bar{a} \neq \bar{0}$

- Say f is an irreducible polynomial if

(Irr1) $\deg f \geq 1$. Namely f is nonzero and non-unit; and

(Irr2) If g, h are polynomials s.t.

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

then either g or h is a unit polynomial.

e.g. For any $a \in \mathbb{F}_p$, $T - a \in \mathbb{F}_p[T]$ is irreducible.

$\deg(T-a) = 1$ If $g, h \neq 0$ s.t. $gh = f (= T-a)$

By thm 2, $\underset{\underset{1}{\parallel}}{\deg f} = \deg gh = \underset{\geq 0}{\deg g} + \underset{\geq 0}{\deg h}$. $\Rightarrow$ either $\deg g = 0 \leadsto$ unit!
or $\deg h = 0$

e.g. $p = 5$ $f(T) = T^2 + \bar{2} \in \mathbb{F}_5[T]$ is irreducible.

$\deg f = 2$. If g, h s.t. $\deg g, \deg h \geq 1$ and $gh = f$.

By thm 2, $\underset{\underset{2}{\parallel}}{\deg f} = \deg gh = \underset{\geq 1}{\deg g} + \underset{\geq 1}{\deg h}$. $\Rightarrow \deg g = \deg h = 1$.

Assume $g = T + a$ and $h = T + b$

$f = gh = (T+a)(T+b) = T^2 + (a+b)T + ab$ $\left(f = T^2 + \bar{2} \right)$

$\Rightarrow \begin{cases} a+b = \bar{0} \\ ab = \bar{2} \end{cases} \Rightarrow \begin{cases} b = -a \\ a^2 = -\bar{2} = \bar{3} \end{cases} \not\Leftarrow$ $\boxed{\begin{matrix} \bar{0}^2 = \bar{0} & \bar{2}^2 = \bar{4} & \bar{4}^2 = \bar{1} \\ \bar{1}^2 = \bar{1} & \bar{3}^2 = \bar{4} & \end{matrix}}$

Defn. Suppose $\deg f = d$. Write
$$f(T) = a_d T^d + \cdots + a_1 T + a_0.$$
Then a_d is called the leading coefficient of f.
When $a_d = \bar{1}$, f is called a monic polynomial.

Lemma. For any nonzero $f \in \mathbb{F}_p[T]$, there is a monic irreducible polynomial P dividing it. "prime divisor"

Proof. We prove it by induction on degree.

- $\deg f = 0$, Saying $f(T) = aT + b$.
  Then $T + a^{-1}b$ is a monic irreducible polynomial dividing f.

- Suppose the lemma is true for all f with $\deg f < k$.
  For a f with $\deg f = k$. Either f is irreducible. Then $f/_{\text{leading coeffiect of } f}$ is a monic irreducible polynomial dividing f.

Or $f = gh$ with $\deg g, \deg h \geq 1$.

Then by thm 2., $\underset{\substack{\shortparallel \\ k}}{\deg f} = \deg gh = \underset{\geq 1}{\deg g} + \underset{\geq 1}{\deg h}$.

Hence, $\deg g < k$.

By Induction Hypothesis, there is a monic irreducible polynomial p s.t. $p \mid g$.

Then $p \mid f$ since $g \mid f$. $\boxtimes$

6. Theorem (Unique prime factorization.)

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

$$f(T) = c \cdot P_1(T)^{e_1} \cdot P_2(T)^{e_2} \cdot \cdots \cdot P_r(T)^{e_r}$$

where

- c is the leading coefficient of f;
- $P_1, \cdots, P_r$ are monic irreducible polynomials over $\mathbb{F}_p$; and
- $e_1, \cdots, e_r > 0$.

Proof. 1) What are P_i?

For each monic irreducible polynomial P with $\deg \leq \deg f$, test if $P_i \mid f$. (There are only finitely many candidates)

2) What are e_i?

For each P_i, consider

$$\bar{1},\ P_i,\ P_i^2,\ \cdots$$

Let e_i be the largest exponent s.t. $P_i^{e_i} \mid f$

3) Why $f = c \cdot P_1^{e_1} \cdots P_r^{e_r}$?

We have $P_i^{e_i} \mid f$. By a lemma we'll see next time, $P_1^{e_1} \cdots P_r^{e_r} \mid f$

Let $g \in \mathbb{F}_p[T]$ s.t. $f = g \cdot P_1^{e_1} \cdots P_r^{e_r}$.

Suppose $\deg g \geq 1$ (nonzero, non-unit).

Then there is a monic irreducible polynomial $P_0 \mid g$.

But either $P_0 \notin \{P_1, \cdots, P_r\}$ or $P_0 = P_i$ and hence $P_i^{e_i+1} \mid f$

leads to a contradiction!

Next time:

Defn. Say f and g are coprime if there are $h_1(T), h_2(T) \in \mathbb{F}_p[T]$ s.t.

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

Lem: If $f \mid h$, $g \mid h$ and f, g are coprime, then $fg \mid h$.

Lem: If f, g are coprime and f, h are coprime, then f, gh are coprime.

Coro: If $p_i^{e_i} \mid f$, then $p_1^{e_1} \cdots p_r^{e_r} \mid f$.

Prop. $\bar{x} \in \mathbb{F}_p$ is a root of $f(T) \in \mathbb{F}_p[T]$ iff $T - \bar{x} \mid f(T)$

Thm. $\#\{\text{roots of } f(T) \text{ in } \mathbb{F}_p\} \leq \deg f.$