Roots and degree

Lemma 5.4.1

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

Lemma 5.4.1

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

Proof. By the division of polynomials over $\mathbb{F}_p$ (theorem 5.2.1), there are polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ such that

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

Therefore, r is a constant.

□

Lemma 5.4.1

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

Proof. By the division of polynomials over $\mathbb{F}_p$ (theorem 5.2.1), there are polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ such that

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

Therefore, r is a constant.

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

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

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

Lemma 5.4.2

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 $\overline{a} \neq \overline{b}$.

Lemma 5.4.2

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

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

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

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

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

Lemma 5.4.2

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. □

$\bar{c}(\bar{a} - \bar{b})$

Theorem 5.4.3

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

Theorem 5.4.3

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

Proof. By lemma 5.4.1, for any root $\overline{a}$ of $f(T)$ in $\mathbb{F}_p$, we have $T - \overline{a} \mid f(T)$. By lemma 5.4.2, 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 $\mathbb{F}_p$. $\square$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

$$\overline{4}^2 - \overline{1} = \qquad \overline{5}^2 - \overline{1} =$$

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

$$\overline{4}^2 - \overline{1} = \qquad \overline{5}^2 - \overline{1} =$$

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

$$\overline{4}^2 - \overline{1} = \qquad \overline{5}^2 - \overline{1} =$$

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

$$\overline{4}^2 - \overline{1} = \qquad \overline{5}^2 - \overline{1} =$$

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

$$\overline{4}^2 - \overline{1} = \qquad \overline{5}^2 - \overline{1} =$$

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

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

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

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

$$\overline{6}^2 - \overline{1} = \qquad \overline{7}^2 - \overline{1} =$$

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

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

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

Example 5.4.4

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 $\mathbb{F}_8$.

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

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

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

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