Finnishing proving primitive root theorem

Corollary 5.4.5

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

Corollary 5.4.5

For each divisor $\ell \mid p-1$, 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 5.4.3, 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 $\mathbb{F}_p$.

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

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

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

$$\ell(a^e \pmod{p}) = \ell$$

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

Then we see that

$$\ell(a^e \pmod p) = \ell$$

$\iff$ 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

Then we see that

$$\begin{aligned}
&\ell(a^e \pmod p) = \ell \\
\iff &\text{the multiplicative dynamic of } a^e \pmod p \text{ on } \langle a \rangle \text{ consists of only one circle} \\
\iff &\text{the additive dynamic of } [e]_\ell \text{ on } \mathbb{Z}/\ell \text{ consists of only one circle} \\
\iff &\gcd(e, \ell) = 1 \qquad \text{(by theorem 4.3.4)}
\end{aligned}$$

Then we see that

$$\begin{aligned} & \ell(a^e \pmod p) = \ell \\ \iff & \text{the multiplicative dynamic of } a^e \pmod p \text{ on } \langle a\rangle \text{ consists of only one circle} \\ \iff & \text{the additive dynamic of } [e]_\ell \text{ on } \mathbb{Z}/\ell \text{ consists of only one circle} \\ \iff & \gcd(e,\ell) = 1 \qquad \text{(by theorem 4.3.4)} \end{aligned}$$

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, $|\Phi_\ell(p)| = \varphi(\ell)$. □

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

For instance,

Finnishing proving primitive root theorem

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

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

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

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 (monic)

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 (i.e. fractions of poly)

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

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.