(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 $r = 0$, *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.

Example 5.3.1

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

(Euclidean) division algorithm

Example 5.3.1

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

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

Example 5.3.1

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

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

Theorem 5.3.2

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.

Theorem 5.3.2

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 Lemma 1.2.3. □

Lemma 5.3.3

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

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

Corollary 5.3.4

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

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

Corollary 5.3.4

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

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

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 5.3.5

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

Definition 5.3.5

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

By theorem 5.1.6, we must have $\deg(f) \leqslant \deg(\overline{1}) = 0$. 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.

Definition 5.3.6

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.

Definition 5.3.6

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 5.3.7

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

Example 5.3.8

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

Example 5.3.8

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.

Example 5.3.8

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.

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 $T^2 + \overline{2}$.

Theorem 5.3.9

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 $e_1, \cdots, e_n > 0$.*

Proof. Same as the fundamental theorem of arithmetic. □