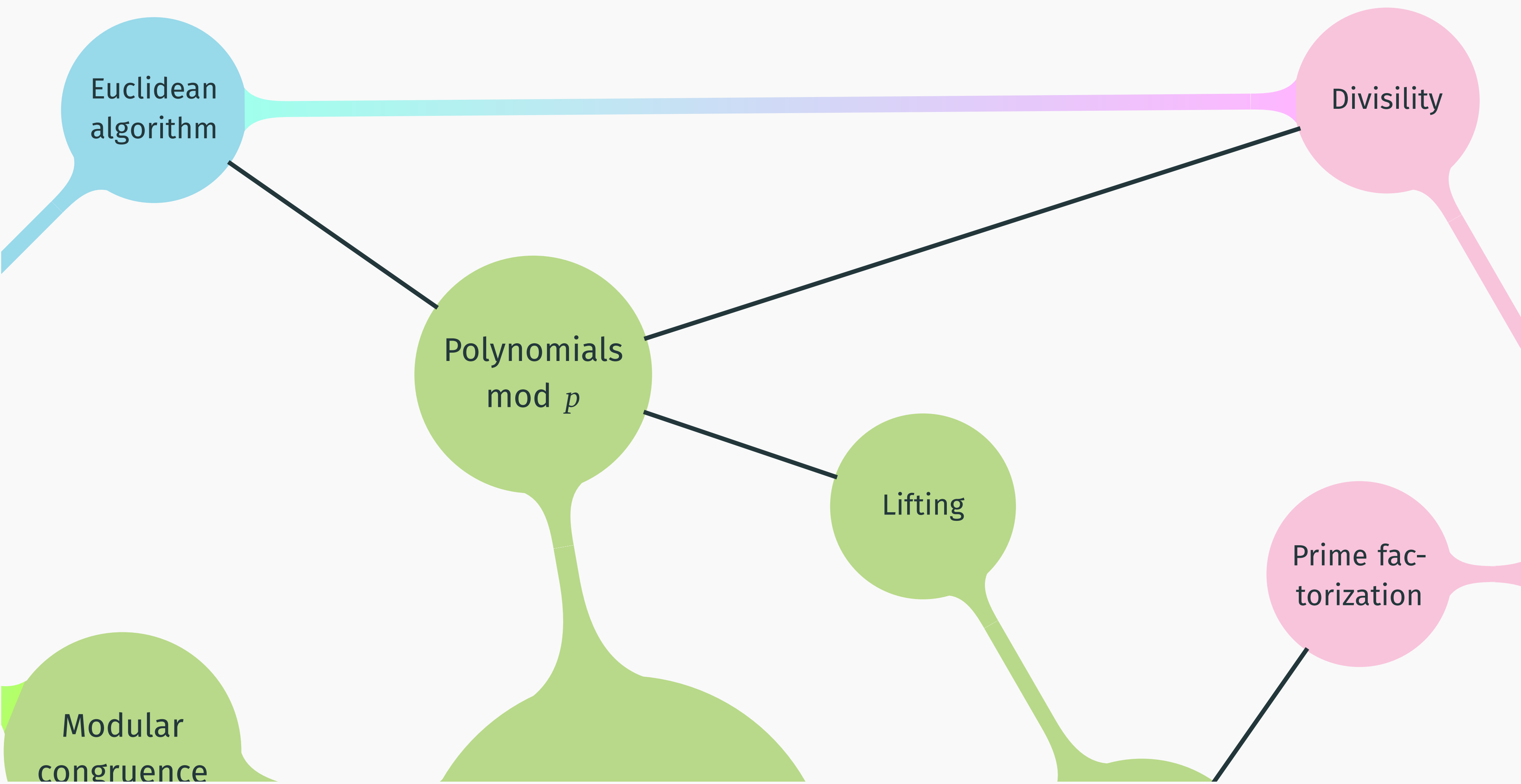
Division of modular polynomials

Division of modular polynomials



Theorem 5.2.1 (Division of polynomials)

Let $f(T)$ and $g(T)$ be two polynomials over $\mathbb{F}_p$, then there are polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ such that

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

Theorem 5.2.1 (Division of polynomials)

Let $f(T)$ and $g(T)$ be two polynomials over $\mathbb{F}_p$, then there are polynomials $q(T), r(T) \in \mathbb{F}_p[T]$ such that

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

Proof. Suppose the leading terms of f and g are $\overline{a}T^{\deg(f)}$ and $\overline{b}T^{\deg(g)}$ respectively. Since p is a prime, we can always solve the equation $a = xb$ in $\mathbb{F}_p$. Then $f(T) - (xT^{\deg(f)-\deg(g)})g(T)$ has degree strictly less than $\deg(f)$. Replace $f(T)$ by it and repeat this process, we will get a polynomial of degree less than $\deg(g)$ in the last step. $\square$

Example 5.2.2

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

Example 5.2.2

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

$$
\begin{array}{r|rrrr}
 & & & T & -\overline{1} \\
\hline
T^2 + T + \overline{3} & T^3 & +\overline{0}T^2 & +\overline{4}T & +\overline{2} \\
 & T^3 & + \quad T^2 & +\overline{3}T & \downarrow \\
\cline{2-4}
 & & - \quad T^2 & + \quad T & +\overline{2} \\
 & & - \quad T^2 & - \quad T & -\overline{3} \\
\cline{3-5}
 & & & \overline{2}T & +\overline{5}
\end{array}
$$

Example 5.2.2

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

$$
\begin{array}{r|l}
 & T - \overline{1} \\
\hline
T^2+T+\overline{3} & T^3+\overline{0}T^2+\overline{4}T+\overline{2} \\
 & \underline{T^3+\ T^2+\overline{3}T} \quad \downarrow \\
 & -\ T^2+\ T+\overline{2} \\
 & \underline{-\ T^2-\ T-\overline{3}} \\
 & \overline{2}T+\overline{5}
\end{array}
\qquad
\begin{array}{r|l}
 & T + \overline{4} \\
\hline
T^2+T+\overline{3} & T^3+\overline{0}T^2+\overline{4}T+\overline{2} \\
 & \underline{T^3+\ T^2+\overline{3}T} \quad \downarrow \\
 & \overline{4}T^2+\ T+\overline{2} \\
 & \underline{\overline{4}T^2+\overline{4}T+\overline{2}} \\
 & \overline{2}T+\overline{0}
\end{array}
$$

Example 5.2.3

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

Example 5.2.3

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

$$
\begin{array}{r}
\overline{4}T+\overline{3} \\
\overline{3}T^2+T+\overline{2}\;\big)\;\overline{2}T^3+\overline{3}T^2+T+\overline{1} \\
\underline{\overline{2}T^3+\overline{4}T^2+\overline{3}T\quad\downarrow} \\
\overline{4}T^2+\overline{3}T+\overline{1} \\
\underline{\overline{4}T^2+\overline{3}T+\overline{1}} \\
0
\end{array}
$$

Note that we cannot do division of integer polynomials this time.

Definition 5.2.4

Let $f(T)$ and $g(T)$ be two polynomials over $\mathbb{F}_p$. Then we say f *divides* g, or f is a *divisor* of g, or g is a multiple of f, written as $f \mid g$ if there is another $h(T) \in \mathbb{F}_p[T]$ such that

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

Example 5.2.5

Over $\mathbb{F}_5$, $\overline{3}T^2 + T + \overline{2}$ divides $\overline{2}T^3 + \overline{3}T^2 + T + \overline{1}$.

Division of modular polynomials

It is possible that two distinct polynomials divides each other, this is due to the fact that every nonzero element of $\mathbb{F}_p$ is a unit. Hence, any two polynomials different only by a nonzero constant factor would divide each other.

It is possible that two distinct polynomials divides each other, this is due to the fact that every nonzero element of $\mathbb{F}_p$ is a unit. Hence, any two polynomials different only by a nonzero constant factor would divide each other.

Among the polynomials over $\mathbb{F}_p$, the following ones play as the role of positive integers.

Definition 5.2.6

A polynomial $f(T)$ over $\mathbb{F}_p$ is *monic* if its leading term (the term of degree $\deg(f)$) has coefficient $\overline{1}$.

So a monic polynomial looks like this: T^n+ lower terms.

You can verify that the divisibility of *monic* polynomials is also a *partial order* satisfying the *2-out-of-3 principle*.

We also have the notions of $\gcd$ and lcm.

Definition 5.2.7 (Greatest common divisor)

Let $a(T)$ and $b(T)$ be two nonzero polynomials over $\mathbb{F}_p$. Then a monic polynomial $g(T)$ is called a *greatest common divisor* of them if it satisfies the following two defining properties:

1. $g \mid a$ and $g \mid b$, i.e. g is a common divisor of a and b; and
2. if d is any common divisor of a and b, then $d \mid g$.

We will use $\gcd(a, b)(T)$ to denote the greatest common divisor of $a(T)$ and $b(T)$.

Definition 5.2.8 (Least common multiple)

Let $a(T), b(T)$ be two nonzero polynomials over $\mathbb{F}_p$. Then a monic polynomial $l(T)$ is called a *least common multiple* of them if it satisfies the following two defining properties:

1. $a \mid l$ and $b \mid l$, i.e. l is a common multiple of a and b; and
2. if m is any common multiple of a and b, then $l \mid m$.

We will use $\operatorname{lcm}(a, b)(T)$ to denote the least common multiple of $a(T)$ and $b(T)$.

Theorem 5.2.9

$$\gcd(a, b)(T) \cdot \operatorname{lcm}(a, b)(T) = a(T) \cdot b(T)$$