Discussion 4A

CS 70, Summer 2024

1 Euclidean Algorithm for Polynomials

We saw in lecture that the division algorithm holds for polynomials. That is, for any two polynomials a and $b \neq 0$, there exist polynomials q and r such that

$$a(x) = q(x)b(x) + r(x) \qquad \text{for all } x$$

and $\deg r < \deg b$. If $r = 0$, we say that $b \mid a$. Typically, we will work with $\deg b \leq \deg a$.

This theorem allows us to extend our theory of modular arithmetic to polynomials. We define the *greatest common divisor* $\gcd(a, b)$ of two polynomials a and b to be the polynomial d satisfying the following.

(1) d is a *common divisor* of a and b: $d \mid a$ and $d \mid b$.

(2) d is the *greatest* such divisor: for any other c such that $c \mid a$ and $c \mid b$, we have that $c \mid d$.

(a) Prove that the polynomial gcd is only unique up to constants. That is, prove that if some polynomial f is the greatest common divisor of two polynomials p and q, then for $c \in \mathbb{Z} \setminus \{0\}$, the polynomial cf is also a greatest common divisor of p and q.

(b) We can use the Euclidean algorithm for polynomials exactly the same way we did for integers. This requires proving that $\gcd(a, b) = \gcd(b, r)$, where $a = bq + r$ by the polynomial division algorithm, which we will not do.

Use the Euclidean algorithm to show that $\gcd(x^3, x^2 + 1) = 1$. Note that since the polynomial gcd is unique up to constants, we will typically scale the gcd so that the leading term has coefficient 1.

(c) Extend the Euclidean algorithm from part **(b)** to find two polynomials a and b such that

$$1 = x^3 a(x) + (x^2 + 1)b(x) \qquad \text{for all } x.$$

(d) Use part **(c)** to find a degree 2 polynomial p such that for all x, $p(x)x^3$ has a remainder of 1 when divided by $x^2 + 1$.

2 Polynomial Potpourri

(a) Let f and g be two nonzero real polynomials with degrees $d_f = \deg f$ and $d_g = \deg g$. Determine the minimum and maximum number of roots each of the following polynomials could have.

(i) $f + g$.

(ii) $f \cdot g$.

(iii) f/g, given that f/g is a polynomial.

(b) Let f and g be polynomials over $\mathbb{F}_p$. Show that if $f \cdot g = 0$, it is not necessarily the case that $f = 0$ or $g = 0$.

(c) Let p be a prime and fix $a \in \{0, \ldots, p-1\}$. Determine exactly how many degree exactly d polynomials f over $\mathbb{F}_p$ there are such that $f(0) = a$.

(d) Consider the polynomials f over $\mathbb{F}_5$ such that.

$$f(0) = 1, \qquad f(1) = 2, \qquad f(4) = 0.$$

(i) Find a polynomial f satisfying the constraints.

(ii) Determine how many polynomials of degree at most 4 satisfy the constraints.

3 Lagrange Interpolation in Finite Fields

Consider the unique polynomial p over $\mathbb{F}_5$ which passes through the points $(-1, 3)$, $(0, 1)$, and $(1, 2)$.

(a) Suppose you had three polynomials p_{-1}, p_0, and p_1 over $\mathbb{F}_5$ such that

$$\begin{aligned} p_{-1}(-1) &\equiv 1 \pmod 5 & p_0(-1) &\equiv 0 \pmod 5 & p_1(-1) &\equiv 0 \pmod 5 \\ p_{-1}(0) &\equiv 0 \pmod 5 & p_0(0) &\equiv 1 \pmod 5 & p_1(0) &\equiv 0 \pmod 5 \\ p_{-1}(1) &\equiv 0 \pmod 5 & p_0(1) &\equiv 0 \pmod 5 & p_1(1) &\equiv 1 \pmod 5. \end{aligned}$$

Explain how you could construct the polynomial p using these polynomials.

(b) Find a polynomial p_{-1} over $\mathbb{F}_5$ such that

$$\begin{aligned} p_{-1}(-1) &\equiv 1 \pmod 5 \\ p_{-1}(0) &\equiv 0 \pmod 5 \\ p_{-1}(1) &\equiv 0 \pmod 5. \end{aligned}$$

(c) Find a polynomial p_0 over $\mathbb{F}_5$ such that

$$\begin{aligned} p_0(-1) &\equiv 0 \pmod 5 \\ p_0(0) &\equiv 1 \pmod 5 \\ p_0(1) &\equiv 0 \pmod 5. \end{aligned}$$

(d) Find a polynomial p_1 over $\mathbb{F}_5$ such that

$$\begin{aligned} p_1(-1) &\equiv 0 \pmod 5 \\ p_1(0) &\equiv 0 \pmod 5 \\ p_1(1) &\equiv 1 \pmod 5. \end{aligned}$$

(e) Construct the unique polynomial p over $\mathbb{F}_5$ as a linear combination of p_{-1}, p_0, and p_1.

4 Secret

A secret vault in secret headquarters of the Secret League™ can only be opened with a secret combination $s \in \mathbb{Z}$. The vault should only be opened in the following two situations.

(1) All 200 secret enclaves agree to open the vault.

(2) At least 100 secret enclaves and the Secret Keeper agree to open the vault.

(a) Propose a secret scheme which gives secret information to the secret enclaves and the Secret Keeper so that the secret combination s can only be recovered in either one of the two situations.

(b) The Secret League™ decides to add an additional layer of secrecy. Each of the 200 secret enclaves has a secret delegation of 10 secret acolytes. The Secret League™ requires that a secret enclave will only agree to open the vault if all 10 secret acolytes agree to open the vault.

Propose a secret scheme which gives secret information to the the secret acolytes and the Secret Keeper so that the secret combination s can only be recovered in either one of the two situations with this additional requirement.