Discussion 4A

CS 70, Summer 2024

1 Euclidean Algorithm for Polynomials

(a) Let $f = \gcd(p, q)$. Then $f \mid p$ and $f \mid q$, so we have that $p = fk$ and $q = fj$ for some polynomials k and j.

We want to show that for some nonzero constant c, $cf \mid p$ and $cf \mid m$. That is, we must show that $p = cf\ell$ and $q = cfm$ for some polynomial ℓ and m.

Let $\ell = c^{-1}k$ and $m = c^{-1}j$; the resulting ℓ and m are still polynomials since we are scaling k and j by a finite constant.

Then,

$$p = cf\ell = cfc^{-1}k = fk \qquad \text{and} \qquad q = cfm = cfc^{-1}j = fj$$

We have shown that $p = cf\ell$ and $q = cfm$, as desired. So the polynomial cf is also a greatest common divisor of p and q.

(b) We will use the Euclidean algorithm and the division algorithm to show that $\gcd(\boldsymbol{x^3}, \boldsymbol{x^2 + 1}) = 1$.

$$\begin{aligned} \gcd(\boldsymbol{x^3}, \boldsymbol{x^2 + 1}) &= \gcd(\boldsymbol{x^2 + 1}, \boldsymbol{-x}) & \boldsymbol{-x} &= 1 \times \boldsymbol{x^3} - x \times (\boldsymbol{x^2 + 1}) \\ &= \gcd(\boldsymbol{-x}, \boldsymbol{1}) & \boldsymbol{1} &= 1 \times (\boldsymbol{x^2 + 1}) - (-x) \times (\boldsymbol{-x}) \\ &= \gcd(\boldsymbol{1}, \boldsymbol{0}) & \boldsymbol{0} &= 1 \times (\boldsymbol{-x}) - (-x) \times \boldsymbol{1} \\ &= 1. \end{aligned}$$

(c) In the same way we used the Euclidean algorithm for integer outputs, we start with the penultimate equation and work our way back.

$$\begin{aligned} \boldsymbol{1} &= 1 \times (\boldsymbol{x^2 + 1}) + x \times (\boldsymbol{-x}) \\ &= 1 \times (\boldsymbol{x^2 + 1}) + x \times (\boldsymbol{x^3} - x \times (\boldsymbol{x^2} + 1)) \\ &= x \times (\boldsymbol{x^3}) + (1 - x^2)(\boldsymbol{1 + x^2}). \end{aligned}$$

So for any x, $a(x) = x$ and $b(x) = 1 - x^2$.

(d) The following must hold for every x.

$$p(x)x^3 \equiv 1 \pmod{x^2 + 1}.$$

By part **(c)**, we know that

$$a(x)x^3 \equiv 1 \pmod{x^2 + 1}.$$

Therefore, we have that

$$\begin{aligned} p(x)x^3 &\equiv 1 && \pmod{x^2 + 1} \\ p(x)x^3a(x) &\equiv a(x) && \pmod{x^2 + 1} \\ p(x) &\equiv x && \pmod{x^2 + 1}. \end{aligned}$$

That is, $p(x)$ is x more than any multiple of $x^2 + 1$. Of course $p(x) = x$ works, but we know that $\deg p = 2$. Therefore we take the first nonzero multiple: for all x,

$$p(x) = 1(x^2 + 1) + x = x^2 + x + 1.$$

By the construction of p, the remainder when divided by $x^2 + 1$ is 1. However, $p(x)$ is a degree 2 polynomial, so we want to find a polynomial that is x more than some multiple of $x^2 + 1$.

If we pick the first nonzero multiple, $p(x) = x^2 + 1 + x = x^2 + x + 1$.

2 Polynomial Potpourri

(a) **(i)** The minimum number of roots for $f+g$ could be 0 if f and g both have no roots. As an example, let $f = x^2+1$ and $g = 2x^2+3$, $f+g$ will have no roots. However, if the highest degree of $f+g$ is odd, it has to cross the x-axis at least once, meaning that the minimum number of roots for odd degree polynomials is 1.

The maximum number of roots is $\max(d_f, d_g)$. The one exception to this expression is if $f = -g$. In that case, $f+g = 0$, so the polynomial has an infinite number of roots!

(ii) Again, the minimum number of roots for $f \cdot g$ would be 0 if f and g both have no roots. The maximum number of roots would be $d_f + d_g$ because $f \cdot g$ is of degree $d_f + d_g$.

(iii) Once again, the minimum number of roots for f/g would be 0 if f and g both have no roots. The maximum number of roots would be $d_f - d_g$ because if f/g is a polynomial, then it must be of degree $d_f - d_g$.

(b) We can show this by providing a counterexample. Here are a few:

Example 1: Let $f(x) = x^{p-1} - 1$ and $g(x) = x$, which are both non-zero polynomials in $\mathbb{F}_p$ for any prime p. Their product will be $x^p - x = x - x = 0$ in $\mathbb{F}_p$ by FLT.

Example 2: To satisfy $f \cdot g = 0$, all we need is $(\forall x \in S, f(x) = 0 \vee g(x) = 0)$ where $S = \{0, \ldots, p-1\}$. However, this is not equivalent to $(\forall x \in S, f(x) = 0)) \vee (\forall x \in S, g(x) = 0)$.

Example 3: We can also construct a concrete example.

Let $p = 2$, $f(x) = 1 - x$, and $g(x) = x$.

That is,

$$\begin{aligned} f(0) &= 1 & \qquad g(0) &= 0 \\ f(1) &= 0 & \qquad g(1) &= 1 \end{aligned}$$

Then $f \cdot g = 0$ but neither f nor g is the zero polynomial.

(c) A degree d polynomial $f(x) = \sum_{k=0}^{d} c_k x^k$ will have $d+1$ coefficients that can take on any value $\{0, \ldots, p-1\}$.

However, there are two constraints we need to consider:

1. $f(0)$ is a fixed value a so there is only one value for c_0.
2. c_d can only take on values $\{1, \ldots, p-1\}$. If $c_d = 0$, our polynomial will not be degree d.

Hence we are left with $(p-1) \cdot p^{d-1}$ possibilities.

(d) **(i)** By Lagrange interpolation,

$$\begin{aligned} \Delta_0(x) &= \frac{(x-1)(x-4)}{(0-1)(0-4)} \bmod 5 = (x-1)(x-4)4^{-1} \bmod 5 = 4(x-1)(x-4) \bmod 5, \\ \Delta_1(x) &= \frac{(x-0)(x-4)}{(1-0)(1-4)} \bmod 5 = x(x-4)2^{-1} \bmod 5 = 3x(x-4) \bmod 5, \\ \Delta_4(x) &= \frac{(x-0)(x-1)}{(4-0)(4-1)} \bmod 5 = x(x-1)2^{-1} \bmod 5 = 3x(x-1) \bmod 5. \end{aligned}$$

Therefore

$$\begin{aligned} f(x) &= 1\Delta_0(x) + 2\Delta_1(x) + 0\Delta_4(x) \bmod 5 \\ &= 4(x-1)(x-4) + 6x(x-4) \bmod 5 \\ &= -4x + 1 \bmod 5. \end{aligned}$$

(ii) 5 points uniquely define a polynomial of degree at most 4. We have 3, so there are are $5 \cdot 5 = 25$ polynomials of degree at most four through these points.

3 Lagrange Interpolation in Finite Fields

(a) $p = 3p_{-1} + 1p_0 + 2p_1$

(b) We can construct $P_{-1}(x)$ by doing the following:

$$\begin{aligned} p_{-1}(x) &\equiv \frac{(x-0)(x-1)}{(-1-0)(-1-1)} \\ &\equiv \frac{(x-0)(x-1)}{2} \\ &\equiv (2)^{-1}x(x-1) \pmod 5 \\ &\equiv 3x(x-1) \pmod 5. \end{aligned}$$

(c) We can construct $P_0(x)$ by doing the following:

$$\begin{aligned} p_0(x) &\equiv \frac{(x+1)(x-1)}{(0+1)(0-1)} \\ &\equiv \frac{(x+1)(x-1)}{-1} \\ &\equiv (-1)^{-1}(x-1)(x+1) \pmod 5 \\ &\equiv 4(x-1)(x+1) \pmod 5. \end{aligned}$$

(d) We can construct $P_1(x)$ by doing the following:

$$\begin{aligned} p_1(x) &\equiv \frac{(x+1)(x-0)}{(1+1)(1-0)} \\ &\equiv \frac{(x+1)(x-0)}{2} \\ &\equiv (2)^{-1}x(x+1) \pmod 5 \\ &\equiv 3x(x+1) \pmod 5. \end{aligned}$$

(e) Using parts ***(a)*** through ***(d)***,

$$\begin{aligned} p(x) &= 3p_{-1}(x) + 1p_0(x) + 2p_1(x) \\ &= 3 \cdot 3x(x-1) + 1 \cdot 4(x-1)(x+1) + 2 \cdot 3x(x+1) \\ &= 9x(x-1) + 4(x-1)(x+1) + 6x(x+1) \\ &\equiv 4x^2 - 3x - 4 \pmod 5 \\ &\equiv 4x^2 + 2x + 1 \pmod 5. \end{aligned}$$

Our final polynomial will be $p = 4x^2 + 2x + 1$.

4 Secret

(a) Create a polynomial of degree 199 and give each enclave one point. Give the Secret Keeper $200 - 100 = 100$ distinct points, so that if they collaborate with 100 enclaves, they will have a total of 200 points and can reconstruct the polynomial. Without the Secret Keeper, the polynomial can still be recovered if all 200 enclaves come together.

Alternatively, we could have one scheme for condition (i) and another for condition (ii). We can fulfill the first condition by creating a single polynomial of degree 199, with each enclave receiving one distinct point and evaluating the polynomial at zero returns the combination s. For the second condition, we can create a polynomial f of degree 1 with $f(0) = s$, and give $f(1)$ to the Secret Keeper. Now, we can create a second polynomial g of degree 99, with $g(0) = f(2)$, and give one distinct point of g to each enclave. This way, any 100 enclaves can recover $g(0) = f(2)$, and then can consult with the Secret Keeper to recover $s = f(0)$ from $f(1)$ and $f(2)$.

(b) We'll layer an *additional* round of secret-sharing onto the scheme from part **(a)**. First, we construct a 199 degree polynomial f, where $f(0) = s$ and give each enclave one point t_i. Then, create a degree 9 polynomial f_i for each enclave with $f_i(0) = t_i$ and give each acolyte one point from f_i. Again, we give the Secret Keeper 100 distinct points so the secret combination can still be found if just 100 enclaves come together with 10 acolytes agreeing each. Without the Secret Keeper, the polynomial can still be recovered if all acolytes from all the enclaves come together.