Basics of polynomials

Exercises

Application of discrete models

Mathematical questions

1. What are the coefficients, leading coefficient, constant term, quadratic coefficient (i.e. coefficient of degree 2) and degree of the polynomial $2x^4 - 2x^3 + 3x + 1$?

2. Turn the following polynomials into canonical form:
a) $1 + x - x^2 + x - 2$; b) $(x+1)^3$; c) $(x^2+2)(2x-3)$; d) $(x+1)(x+2) - (x-1)(x-2)$.

3. Turn the polynomial p into the form used by Horner's method, and use it to evaluate it at c:
a) $p = 2x^3 - x^2 - 4x + 3,\ c = 2$;
b) $p = 2x^4 - 5x^3 - 6x^2 + 3x + 2,\ c = -1$;
c) $p = x^4 - 2x^3 - 2x - 20,\ c = 3$.

4. What is the condition for a polynomial p to have 5 as a double root?

5. a) At most how many roots can a polynomial of degree 6 have?
b) At most how many different roots can a polynomial of degree 6 have, if we know that it has two different double roots?

6. Write down the foundamental theorem of algebra.

7. Turn the polynomial $p = 4x^2 + 2x - 2$ into root factor form.

8. Calculate the polynomial p (in canonical form) for which:
a) $\deg p = 2,\ p(3) = 0,\ p(4) = 2,\ p(5) = 0$;
b) $\deg p = 2,\ p(1) = 1,\ p(2) = 0,\ p(3) = -3$;
c) $\deg p = 2,\ p(1) = 1,\ p(2) = 3,\ p(4) = 1$;
d) $\deg p = 2,\ p(0) = 1,\ p(1) = 4,\ p(-1) = 4$;
e) $\deg p = 1,\ p(5) = 7,\ p(7) = 5$;
f) $\deg p = 3,\ p(1) = 0,\ p(2) = 0,\ p(3) = 0,\ p(5) = 4$.
Check that the result indeed satisfies the given conditions.

Programming exercises

9. Create the following polynomials for arbitrary $n \in \mathbb{N}^+$. Print the results for $n = 4$.
(The type of the result must be polynomial, not general symbolic expression. This can be checked by `type(p)`, or by whether it supports operations like `p.degree()`.)

a) $nx^n + (n-1)x^{n-1} + (n-2)x^{n-2} + \ldots + 2x^2 + x$;

b) $x^{2n} + x^{2n-2} + \ldots + x^4 + x^2 + 1$;

c) whose roots are $1, 2, 3, \ldots, n$ (all simple);

d) whose only root is 2, with multiplicity n;

e) which has 1 as a simple root, 2 as a double root, ..., n as a root of multiplicity n, and has no other roots.

10. Write a function that calculates the value of a polynomial p at c using Horner's method. (Use only the coefficients of the polynomial.) Test it for the examples of exercise 3 above, and for $p = x^{1000000} - x^{999999} - \ldots - x^2 - x - 1$ at $c = 2$.

11. Find an integer c for which the polynomial $x^5 - cx^2 - cx + 1$ has a multiple root. You can use Sage's root finding function.

12. Implement Lagrange interpolation, i.e. write a function that receives $n+1$ points in a list: $[(x_1, y_1), (x_2, y_2), \ldots, (x_{n+1}, y_{n+1})]$ (where x_i's are all different), and returns the polynomial of degree $\leq n$ for which $p(x_1) = y_1$, $p(x_2) = y_2$, ..., $p(x_{n+1}) = y_{n+1}$. Don't use the interpolation functions of Sage (other than for testing).

13. Simulate Shamir's secret sharing in $\mathbb{Q}[x]$ as follows:

a) Write a function that receives the parameters n, k, S, and generates the n secret shares. It returns a list of length n containing the (x_i, y_i) points. Use the evaluation places $1, 2, 3, \ldots$, and generate the coefficients as random numbers between 1 and 100.

b) Write a function that receives exactly k of the above n shares (a list of length k of (x_i, y_i) points), and reconstructs the secret S. Check that different sets of k shares from the same total n shares produce the same secret value.

14. Shamir's secret sharing in $\mathbb{Q}[x]$ is not completely secure. To see this, generate secret shares for a fixed secret S for $n = 5$ participants and with the threshold value $k = 3$, and try to find out the secret from only *two* shares instead of the necessary three. More precisely, use the two known shares $(3, y_3)$ and $(4, y_4)$, and fill the "unknown" share $(5, y_5)$ with all possible y_5 values between 1 and 100. Calculate the supposed secret S for each of them, and examine S mod 12. If the method were secure, then each remainder would occur with equal probability, i.e. we couldn't learn anything about the secret by using only two secret shares. But what do we see instead? How does that bring closer to breaking S? (The mathematical explanation of the problem can be found at the end of the corresponding lecture notes, and the secure version will be given in the next document.)