Polynomial division

Exercises

Application of discrete models

Mathematical questions

1. Write down the division theorem for polynomials.

2. Define *divisors* in integral domains. Demonstrate the definition on polynomials.

3. Define *units*. What are the units in $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ and $\mathbb{R}$?

4. Define *associates*. Give *two* associates of $x^2 + x + 2$ in $\mathbb{R}[x]$.

5. Define *irreducible* elements in integral domains. What are these in $\mathbb{Z}$?

6. a) Give an irreducible polynomial in $\mathbb{R}[x]$.
b) Give a quadratic irreducible polynomial in $\mathbb{Z}[x]$.
c) Give a polynomial that is irreducible in $\mathbb{R}[x]$, but not in $\mathbb{C}[x]$.
d) Give a polynomial that is irreducible in $\mathbb{Z}[x]$, but not in $\mathbb{R}[x]$.

7. a) Define *greatest common divisor* in integral domains.
b) Define *least common multiple* in integral domains.

8. Define *formal derivative*. What is the formal derivative of $p = 5x^5 + 4x^3 - 3x^2 + 5x - 10 \in \mathbb{Z}[x]$?

9. If c is a triple root of $p \in \mathbb{Q}[x]$, and a double root of $q \in \mathbb{Q}[x]$, then what is its multiplicity in a) $\gcd(p, q)$; b) p'; c) $\gcd(p, p')$; d) $p \,/\, \gcd(p, p')$?

Programming exercises

10. Write a function that calculates both the quotient and the remainder of a polynomial p divided by $x - c$, using Horner's method. (Use only the coefficients of the polynomial.) Return the results in the same format as `p.quo_rem(x-c)`.

11. Implement CRC as follows, using the generator polynomial $g = x^4 + x + 1$.

a) Write a function that receives the message m (as a bit sequence), and calculates the transmitted codeword, i.e. it extends m with the CRC check value. You can use Sage's polynomial operations, but the input and output must be bit sequences (i.e. list of 0's and 1's), not polynomials.

b) Write a function that checks the received codeword, and returns whether it is valid.

c) Generate a random 16-bit message, and try function a) on it, then check the resulting codeword using b).

d) Change (corrupt) the codeword and check that too.

e) Change the codeword in such a way that it will be accepted by the check.

12. a) Adapt the Euclidean algorithm to polynomials. (Does it need to be changed at all?)

b) Adapt the extended Euclidean algorithm to polynomials. (And this?)

c) Try both algorithms for $2x^3 + x^2 - 2x - 1$ and $x^2 - 2x + 1$ in $\mathbb{Q}[x]$, and check the results using Sage functions.

d) Determine the common roots of $2x^3 + x^2 - 2x - 1$ and $x^2 - 2x + 1$ without calculating all of their roots individually.

13. Find an element $c \in \mathbb{Z}_{19}$ for which $x^2 + cx + c^2 \mid x^5 + x^3 + \overline{4}x + \overline{2}$, where both polynomials are in $\mathbb{Z}_{19}$.

14. Write a function that calculates the formal derivative of a polynomial. Do not use any polynomial operation, only the coefficients.

15. a) Create a polynomial $p \in \mathbb{Q}[x]$ of degree 6 for which 3 is a simple root, 5 is a double root, and 8 is a triple root. Check the roots of p using Sage.

b) Calculate the roots of p'. What is the relation to the roots of p?

c) Calculate the roots of $\gcd(p, p')$. What is the relation to the roots of p?

d) Calculate the roots of $p \,/\, \gcd(p, p')$. What is the relation to the roots of p?

16. Write a function that gets a polynomial p and a value c, and it calculates both $p(c)$ and $p'(c)$ simultaneously using Horner's method, without calculating the polynomial p'. (Use only the coefficients of the polynomial.)