Exercise Worksheet 1

October 3, 2022

1 Exercise Workbook 1

1.1 Exercise 1

In handout 02 we covered computing the division with remainder of a polynomial a of degree n by a polynomial b of degree m but for simplicity assumed that the leading coefficient of b (denoted by $\mathrm{lc}(b)$) was 1.

The pseudocode for the division algorithm is:

$r := a$

for $i := n - m, n - m - 1, \ldots, 0$

  if $\deg(r) = m + i$ then

    $q_i := \mathrm{lc}(r)$

    $r := r - q_i \cdot x^i \cdot b$

  else

    $q_i := 0$

return $\sum_{i=0}^{n-m} q_i x^i$ as the quotient and r as the remainder

1.1.1 Part (a)

Modify the above algorithm so that it works for polynomials with $\mathrm{lc}(b) \neq 1$. You can assume that inverses of nonzero coefficients exist in the coefficient ring (i.e., the coefficient ring is a field).

1.1.2 Part (b)

Implement the updated algorithm in a programming language of your choosing.

1.1.3 Part (c)

Apply the algorithm to the polynomials $a = x^7$ and $b = 2x^2 - 1$ using the rational numbers $\mathbb{Q}$ as the coefficient field.

Demonstrate the values of i, q_i, and r after each loop iteration in a table.

1.1.4 Part (d)

Demonstrate the algorithm on at least two other pairs of nontrivial polynomials (a, b).

1.2 Exercise 2

Can you divide $a = x^2$ by $b = 2x + 1$ to get integer polynomials $q, r \in \mathbb{Z}[x]$ such that $a = bq + r$ with $\deg(r) < \deg(b)$?

If so, provide such q and r. If not, prove why not.

1.3 Exercise 3

In each part either find a solution (and explain how you found it) or state that no solution exists and explain why.

1.3.1 Part (a)

Solve $27s + 15t = 1$ for integers s and t.

1.3.2 Part (b)

Solve $27s + 16t = 1$ for integers s and t.

1.3.3 Part (c)

Solve $(x^2 - 1)s + (x - 1)t = 1$ for rational polynomials $s, t \in \mathbb{Q}[x]$.

1.4 Exercise 4

The version of Eulid's algorithm on polynomials presented in class works on polynomials in $\mathbb{Q}[x]$. In order to normalize the gcd (to have a leading coefficient of 1) we definitely require the coefficient ring to be a field. Say we drop the restriction that the gcd must have a leading coefficient of 1. Will Euclid's algorithm now be able to correctly work in $\mathbb{Z}[x]$? Why or why not?

1.5 Exercise 5

1.5.1 Part (a)

As part of the course assessment, choose a topic from one of the suggested textbooks (or a related textbook). Over the next few weeks you should prepare a worksheet that describes the topic in your own words and includes your own examples (ideally in a computer algebra system like Sage).

Right now you just need to select the topic. Potential topics include Gröbner bases, symbolic summation or integration, linear algebra, modular square roots, factorization, the Hermite normal form, lattices and their applications, elliptic curves and their applications, etc.

1.5.2 Part (b)

Select the research paper(s) that you will summarize in a final report (typically consisting of 10 to 15 pages).