Polynomials and the Extended Euclidean Algorithm - Exercises

01017

Discrete Mathematics

Date: 04 December 2025 **Semester:** Fall 2025

Rasmus Rosendahl-Kaa

Exercise 6.16

Let $p(x) = \sum_{k=0}^{n} c_k x^k$ be a polynomial if the coefficients $c_0, ..., c_n$ are all integers where $c_0 \neq 0$ as well as $c_n \neq 0$. Let $\mathbb{Q}$ denominate the set of rational number, meaning fractions with integers in the numerator and the denominator. Then the following theorem is true:

If $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a, b) = 1$, and if $p\left(\frac{a}{b}\right) = 0$, then it is true that $a \mid c_0$ and $b \mid c_n$.

a) Show by the help of the above that the polynomial $p(x) = x^2 - 2$ does not have any rational roots.

Solution:

For $a \mid c_0$ and $b \mid c_n$ to be true, $a = 1, 2$ and $b = 1$.

If $p(x)$ has integer roots, they would divide $c_0 \text{ and } c_n$

Here, we already have the only numbers that can divide $c_0 \text{ and } c_n$. But neither $P\left(\frac{2}{1}\right) \text{ nor } P\left(\frac{1}{1}\right)$ equals 0, so that must mean $p(x)$ does not have any rational roots. Only $a = b = 1$ would have $\gcd(a, b) = 1$, but $p\left(\frac{1}{1}\right)$ still doesn't equal 0, so that must mean that $p(x)$ doesn't have rational roots.

b) Conclude that $\sqrt{2} \notin \mathbb{Q}$

Solution:

$p(x)$ has roots: $-\sqrt{2}$ and $\sqrt{2}$. Because we have what values a, b ($a = b = 1$) could be in $p(x)$, we can see that $\frac{1}{1} \in \mathbb{Q}$, $\gcd(1, 1) = 1$, and that $a \mid c_0$ and $b \mid c_n$.

But since we know that $\sqrt{2}$ and $-\sqrt{2}$ are roots, this means $p\left(\sqrt{2}\right) = p\left(-\sqrt{2}\right) = 0$. But since we have that $\frac{1}{1} \neq \sqrt{2}$, we can conclude that $\sqrt{2} \notin \mathbb{Q}$.

c) Conclude in a similar fashion that $\sqrt{5} \notin \mathbb{Q}$

Solution:

We can observe a similar equation: $p(x) = x^2 - 5$. We can also observe that for the given theorem, then $a = b = 1$ are the only value that they could have. But for similar reasons as before, $\frac{1}{1} \neq \sqrt{5}$, so $\sqrt{5} \notin \mathbb{Q}$.

d) Is it possible that $\sqrt{5} - \sqrt{2} \in \mathbb{Q}$? We actually do not know that yet. Show that $\sqrt{5} - \sqrt{2}$ is a root of the polynomial $q(x) = x^4 - 14x^2 + 9$. Show that$\sqrt{5} - \sqrt{2} \notin \mathbb{Q}$.

Solution:

$$p\left(\sqrt{5} - \sqrt{2}\right) = \left(\sqrt{5} - \sqrt{2}\right)^4 - 14 \cdot \left(\sqrt{5} - \sqrt{2}\right)^2 + 9 \tag{1}$$

$$\left(\sqrt{5}-\sqrt{2}\right)\cdot\left(\sqrt{5}-\sqrt{2}\right)=\sqrt{5}^2+\sqrt{2}^2-2\cdot\sqrt{5}\cdot\sqrt{2} \\ =5+2-2\cdot\sqrt{10}=7-2\sqrt{10} \tag{2}$$

$$p\left(\sqrt{5}-\sqrt{2}\right)=\left(7-2\sqrt{10}\right)\cdot\left(7-2\sqrt{10}\right)-14\cdot\left(7-2\sqrt{10}\right)+9 \\ =49+4\sqrt{10}^2-28\sqrt{10}-14\cdot 7+28\sqrt{10}+9 \\ =49+40-14\cdot 7+9 \\ =98-98=0 \tag{3}$$

$\sqrt{5}-\sqrt{2}$ is a root.

The only a, b we can have are $a=b=1$. 1 is not a root:

$$q(1)=1^4-14+9=-4 \tag{4}$$

Therefore $\sqrt{5}-\sqrt{2}\notin\mathbb{Q}$

e) (Extra, not in the curriculum) Prove the theorem in the beginning of the exercise. (Tip: Consider $p(\frac{a}{b})=0$ and multiply by the common denominator, such that all terms are integers. Thereafter use modulus arithmetic.)

Exercise 6.17

We will examine the execution time of Euclid's algorithm

a) Prove as function of $\deg(f(x))$ and $\deg(g(x))$, how many iteration Euclid's algorithm uses at most, when it is executed on $f(x)$ and $g(x)$.

Solution:

Because we in the Euclidean Algorithm have that $\deg(R_i)<\deg(R_{i-1})$ aka the degree must always go down, and also have that $\deg(R_1)<\deg(M)$. Then the Euclidean Algorithm must use at most $\deg(g(x))$ iterations, where $\deg(g(x))<\deg(f(x))$

b) Let $D(n)$ be an upper limit for the number of arithmetic operations it takes to execute a division of $f(x)$ by $g(x)$ with a remainder if $\deg(f(x)),\deg(g(x))\leq n$. By arithmetic operations we mean $+,-,\cdot$ or $/$ of elements from the field, thus $\mathbb{R}$ or $\mathbb{C}$. Argue that $D(n)\leq 2n^2$.

Solution:

Imagine for the upper bound that $\deg(f(x))=\deg(g(x))=n$.

c)

d)

Exercise 6.18

As usual with fractions, they can be reduced such that given $\frac{p(x)}{q(x)}$ if you by chance know that there exists a $t(x)$ such that $p(x) = t(x)p_1(x)$ and $q(x) = t(x)q_1(x)$, then we have:

$$\frac{p(x)}{q(x)} = \frac{t(x)p_1(x)}{t(x)q_1(x)} = \frac{p_1(x)}{q_1(x)} \tag{5}$$

If you are just given a rational function $\frac{p(x)}{q(x)}$, describe a course of action to calculate the completely reduced fraction.

Solution:

Calculate the roots of each of the functions, then divide the two. You would be able to remove all their common roots, and be left with a completely reduced fraction

Exercise 6.19

Let $p(x)$ and $d(x)$ be polynomials both different from zero. Assume that $d(x) = d_1(x)d_2(x)$, where $\gcd(d_1(x), d_2(x)) = 1$, and assume that $\deg(p(x)) < \deg(d(x))$. Show that there exists polynomials $p_1(x)$ and $p_2(x)$ such that

$$\deg(p_1(x)) < \deg(d_1(x)) \text{ and } \deg(p_2(x)) < \deg(d_2(x)) \tag{6}$$

and

$$\frac{p(x)}{d(x)} = \frac{p_1(x)}{d_1(x)} + \frac{p_2(x)}{d_2(x)} \tag{7}$$

Tip: First multiply the wanted equation by $d(x)$

Solution:

$$p(x) = p_1(x)d_2(x) + p_2(x)d_1(x) \tag{8}$$