Algorithmique de base

Master 1, Université de Rennes

17/10/2024 – TD 7

Exercise 1. Consider the following two polynomials

$$f = 5x^5 + 4x^4 + 3x^3 + 22 + x, \qquad g = x^2 + 2x + 3 \in \mathbb{Q}[x]$$

Apply the Euclidean division of f by g.

Exercise 2. We consider the following recursive algorithm for computing the gcd of two integers.

Algorithm 1 Binary Euclidean Algorithm

Require: $a, b \in \mathbb{N}_{>0}$
Ensure: $\gcd(a, b) \in \mathbb{N}$
if $a = 1$ or $b = 1$ **then**: **return** 1
if $a = b$ **then**: **return** a
if a and b are both even **then**: **return** $2 \cdot \gcd(a/2, b/2)$
if exactly one of a or b, say a, is even **then**: **return** $\gcd(a/2, b)$
if a and b are both odd and $a > b$ **then**: **return** $\gcd\left(\frac{a-b}{2}, b\right)$

1. Run the algorithm on the pairs $(34, 21)$ and $(136, 51)$.
2. Prove that the algorithm works correctly.
3. Find a "good" upper bound on the cost of the algorithm, and show that it takes $O(n^2)$ arithmetic operations on inputs $a, b < 2^n$.
4. Modify the algorithm so that it additionally computes $s, t \in \mathbb{N}$ such that $sa + tb = \gcd(a, b)$.

Exercise 3. Let

$$a = 30x^7 + 31x^6 + 32x^5 + 33x^4 + 34x^3 + 35x^2 + 36x + 37$$

and

$$b = 17x^3 + 18x^2 + 19x + 20$$

in $\mathbb{F}_{101}[x]$, and let $f \in \mathbb{F}_{101}[x]$ be the reversal of b.

(i) Compute $f^{-1} \mod x^4$.

(ii) Use (i) to find $q, r \in \mathbb{F}_{101}[x]$ with $a = qb + r$ and $\deg(r) < 3$.

Exercise 4. We consider the following property of a Euclidean function on an integral domain R:

$$\delta(ab) \geq \delta(b) \quad \text{for all } a, b \in R \setminus \{0\}. \tag{$*$}$$

Our two familiar examples, the degree on $\mathbb{F}[x]$ for a field $\mathbb{F}$ and the absolute value on $\mathbb{Z}$, both fulfill this property. This exercise shows that every Euclidean domain has such a Euclidean function.

(i) Suppose that R is a Euclidean domain and $D = \{\delta : \delta \text{ is a Euclidean function on } R\}$. Then D is nonempty, and we may define a function $d : R \to \mathbb{N} \cup \{-\infty\}$ by

$$d(a) = \min\{\delta(a) : \delta \in D\}.$$

Show that d is a Euclidean function on R (called the minimal Euclidean function).

(ii) Let δ be a Euclidean function on R such that $\delta(ab) < \delta(b)$ for some $a, b \in R \setminus \{0\}$. Find another Euclidean function δ^* that is smaller than δ. Conclude that the minimal Euclidean function δ satisfies (*).

(iii) Show that for all $a, b \in R \setminus \{0\}$ and a Euclidean function δ satisfying ($*$), we have $\delta(0) < \delta(a)$, and $\delta(ab) = \delta(b)$ if and only if a is a unit.

(iv) Let d be the minimal Euclidean function as in (i). Conclude that $d(0) = -\infty$ and the group of units of R is

$$R^\times = \{a \in R \setminus \{0\} : d(a) = 0\}.$$

(v) Prove that $d(a) = \deg(a)$ is the minimal Euclidean function on $\mathbb{F}[x]$ for a field $\mathbb{F}$ with $d(0) = -\infty$ cases.
