Chapter 3 The Euclidean algorithms

3.1 Euclidean domains

Definition 1. *An integral domain* R *together with a function* $d : R \longrightarrow \mathbb{N} \cup \{-\infty\}$ *is a Euclidean domain if for all* $a, b \in R$ *with* $b \neq 0$, *we can divide* a *by* b *with remainder, so that there exist* $q, r \in R$ *such that*

$$a = q \cdot b + r, \quad d(r) < d(b) \tag{1}$$

$q = a \operatorname{quo} b$ *is the quotient and* $r = a \operatorname{rem} b$ *the remainder,* d *is called a Euclidean function.*

For example:

- $R = \mathbb{Z}$ and $d(a) = |a| \in \mathbb{N}$. Here the quotient and the remainder can be made unique by additional requirement that $r \geq 0$.

- $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field, and $d(a) = \deg a$. We define the degree of the zero polynomial to to ∞. It is easy to show uniqueness of the quotient and the remainder in this case.

Definition 2. *Let R be a ring and $a, b, c \in R$. Then c is a greatest common divisor of a and b if*

- $c \mid a$ *and* $c \mid b$,
- *if* $d \mid a$ *and* $d \mid b$, *then* $d \mid c$ *for all* $d \in R$

Definition 3. *Then c is a least common multiple of a and b if*

- $a \mid c$ *and* $b \mid c$,
- *if* $a \mid d$ *and* $b \mid d$, *then* $c \mid d$ *for all* $d \in R$

A unit $u \in R$ is any element with a multiplicative inverse $v \in R$, so that $u \cdot v = 1$.

The elements a and b are associate if $a = u \cdot b$ for a unit $b \in R$; written as $a \backsim b$.

Two integers a, b are coprime if $\gcd(a, b) = 1$.

Lemma 1. *The gcd in $\mathbb{Z}$ has the following properties, for all $a, b, c \in \mathbb{Z}$.*

1. $\gcd(a, b) = |a| \iff a|b$

2. $\gcd(a, b) = \gcd(b, a)$ (*commutativity*)

3. $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$ (*associativity*)

4. $\gcd(c \cdot a, c \cdot b) = |c| \cdot \gcd(a, b)$ (*distributivity*)

5. $|a| = |b| \Longrightarrow \gcd(a, c) = \gcd(b, c)$.

Algorithm 3.5 Classical Euclidean Algorithm

Input: $f, g \in R$ where R is a Euclidean domain with Euclidean function d.

Output: A greatest common divisor $h \in R$ of f and g.

1. $r_0 \longleftarrow f$, $r_1 \longrightarrow g$
2. $i \longleftarrow 1$
   while $r_i \neq 0$ do $r_{i+1} \longleftarrow r_{i-1}$ rem r_i, $i \longleftarrow i+1$
3. return r_{i-1}

Two disadvantages of the classical Euclidean algorithm:

- The denominators and numerators appear in the algorithm are considerably larger than the input polynomials. See page 175.
- It is unstable for numerical polynomials.

$$
\begin{aligned}
a(x) &= x^4 + x^3 + (1+\epsilon)x^2 + \epsilon x + 1, \\
b(x) &= x^3 - x^2 + 3x - 2, \\
c(x) &= \mathsf{rem}(a,b) = \epsilon x^2 + (\epsilon - 4)x + 5, \\
d(x) &= \mathsf{rem}(b,c) = \left(5 - \frac{17}{\epsilon} + \frac{16}{\epsilon^2}\right) x + \left(-2 + \frac{10}{\epsilon} - \frac{20}{\epsilon}^2\right) \\
e(x) &= \mathsf{rem}(c,d) = \frac{\epsilon^2(14\epsilon^3 - 39\epsilon^2 - 32\epsilon + 137)}{(5\epsilon^2 - 17\epsilon + 16)^2}
\end{aligned}
$$

We say that an element $a \in R$ in normal form if $\mathrm{lc}(a) = 1$.

- For $R = \mathbb{Z}$, $\mathrm{lc}(a) = \mathrm{sgn}(a)$ if $a \neq 0$ and $\mathrm{normal}(a) = |a|$.
- For $R = \mathbb{Q}[x]$, $\mathrm{normal}(a) = a/\mathrm{lc}(a)$, ($\mathrm{lc}(0) = 1$).
- The normal form of a product is equal to the products of the normal forms.
- Two elements of R have the same normal form if and only if they are associate.
- $\gcd(0, 0) = 0$.

Algorithm 3.6 Extended Euclidean Algorithm(EEA)

Input: $f, g \in R$, where R is a Euclidean domain with a normal form.

Output: $l \in \mathbb{N}, \rho_i, r_i s_i, t_i \in R$ for $0 \leq i \leq l+1$ and $q_i \in R$ for $1 \leq i \leq l$.

1. $\rho_0 \longleftarrow$ lc$(f), r_0 \longleftarrow$ normal(f), $s_0 \longleftarrow \rho_0^{-1}, t_0 \longleftarrow 0$,
   $\rho_1 \longleftarrow$ lc(g), $r_1 \longleftarrow$ normal(g), $s_1 \longleftarrow 0, t_1 \longleftarrow \rho_1^{-1}$,

2. $i \longleftarrow 1$
   while $r_i \neq 0$ do

$$
\begin{aligned}
q_i &\longleftarrow r_{i-1}\ \mathsf{quo}\ r_i,\\
\rho_{i+1} &\longleftarrow \mathsf{lc}(r_{i-1}\ \mathsf{rem}\ r_i)\\
r_{i+1} &\longleftarrow \mathsf{normal}(r_{i-1}\ \mathsf{rem}\ r_i),\\
s_{i+1} &\longleftarrow (s_{i-1} - q_i s_i)/\rho_{i+1}\\
t_{i+1} &\longleftarrow (t_{i-1} - q_i t_i)/\rho_{i+1},\\
i &\longleftarrow i + 1.
\end{aligned}
$$

3. $l \longleftarrow i - 1$

return $l, \rho_i, r_i s_i, t_i \in R$ for $0 \le i \le l + 1$ and q_i for $1 \le i \le l$.

1. l is called the Euclidean length of the pair (f, g).

2. For all i: $s_i \cdot f + t_i \cdot g = r_i$.

3. In particular, $s_l \cdot f + t_l \cdot g = r_l = \gcd(f, g)$. The elements s_l, t_l are the Bezout coefficients of f and g.

Define the matrices:

$$R_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ \rho_{i+1}^{-1} & -q_i\rho_{i+1}^{-1} \end{pmatrix}, \; 1 \le i \le l$$

$$R_i = Q_i \cdots Q_1 R_0, \; 0 \le i \le l$$

Lemma 2. *For* $0 \le i \le l$, $\rho_{l+1} = 1$, $r_{l+1} = 0$, *we have*

$$R_i \cdot \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}, R_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}$$

Theorem 1. *The Extended Euclidean Algorithm 3.6 for polynomials* $f, g \in F[x]$ *with* $\deg f = n \geq \deg g = m$ *can be performed with*

- *at most* $m + 2$ *inversions and* $\frac{5}{2}nm + O(n)$ *additions and multiplications in* F *is only the quotients* q_i*, the remainders* r_i *and the coefficients* ρ_i *are needed*

- *at most* $m + 2$ *inversion and* $\frac{13}{2}mn + O(n)$ *additions and multiplications in* F *for computing all results.*

Theorem 2. *The Extended Euclidean Algorithm 3.6 for integers* $f, g \in N$ *with* $\lambda(f) = n \geq \lambda(g) = m$ *can be performed with* $O(mn)$ *word operations.*

Theorem 3. *The probability that two random integers are coprime:*

$$\frac{6}{\pi^2} + O\left(\frac{\log N}{N}\right)$$

Theorem 4. *The probability that a random integer is squarefree:*

$$\frac{6}{\pi^2} + O\left(\frac{1}{\sqrt{N}}\right)$$