2. THE EUCLIDEAN ALGORITHM

More ring essentials

In this chapter: rings R commutative with 1.

An element $b \in R$ *divides* $a \in R$, or b *is a divisor of* a, or a *is divisible by* b, or a *is a multiple of* b, if there exists $c \in R$ such that $a = b \cdot c$. Elements a and b in R are *associates* if there exists a unit $u \in R$ such that $a = u \cdot b$ (so a is a multiple of b and b is a multiple of a).

The element b is a *proper divisor* of $a \in R$ if b is neither a unit nor an associate of a. An element is *irreducible* in R if it has no proper divisors in R; other wise it is *reducible*. Note that units are irreducible. The zero element is irreducible if and only if R is a domain.

Primes

A *prime element* is a non-unit $\pi \in R$ with the property that if π divides $a \cdot b$ then π divides a or b.

Lemma *If R is a domain then: $\pi \in R$ prime implies π is irreducible in R.*

For, if $\pi = \alpha \cdot \beta$, with α, β non-units, then π divides $\alpha \cdot \beta$, but if π divides α then $\alpha \cdot \beta \cdot \gamma = \alpha$ for some γ, so $\beta \cdot \gamma - 1 = 0$, contrary to β being non-unit.

Converse is false in general (z in $\mathbb{C}[x, y, z]/(z^2 - xy)$, or 2 in $\mathbb{Z}[\sqrt{-5}]$).

Unique factorization domains

A *unique factorization domain* (UFD) is a domain in which every non-zero non-unit can be written as a product of irreducible non-units in a way that is unique up to order and associates.

Lemma *If R is a UFD then every irreducible element α in R is prime.*

For, if α divides $a \cdot b$ but neither a nor b (non-units), then $a \cdot b$ would have two factorizations into irreducibles, one containing (an associate of) α, the other not.

Examples of unique factorization domains:

(i) $\mathbb{Z}$
(ii) any field F
(iii) any principal ideal domain
(iv) $D[x]$ for any UFD D, hence $D[x_1, x_2, \ldots, x_n]$

Common divisors

A *greatest common divisor* $g = \text{gcd}(S)$ of a finite set S of elements in a domain R is an element g that divides every element of S and has the property that if c also divides every element of S then c divides g.

Two elements a, b are called *relatively prime* (or *coprime*) if $\text{gcd}(a, b) = 1$.

In a UFD every finite set S has a greatest common divisor. Not true in general (6 and $2 + 2\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ have no gcd), and not necessarily unique.

Euclidean domains

A domain R is called *Euclidean* if there exists a *Euclidean function* $\phi : R \setminus \{0\} \to \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$

(i) $\phi(a) \leq \phi(a \cdot b)$ and
(ii) there exist $q, r \in R$ (*quotient* and *remainder*) such that $a = q \cdot b + r$, with either $r = 0$ or $\phi(r) < \phi(b)$.

Proposition *Every Euclidean domain is a principal ideal domain*

Given an ideal I, choose an element x in it minimizing $\phi(x)$. Then $\langle x \rangle \subset I$. But if $a \in I$ then $a = q \cdot x + r$ with $r = 0$ by minimality of $\phi(x)$, since $r = a - q \cdot x \in I$. Hence $a \in \langle x \rangle$.

Converse not true ($\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$).

Examples

(i) $\mathbb{Z}$, with $\phi(n) = |n|$;

(ii) $F[x]$ for any field F, with $\phi(f) = \deg f$.

(iii) $\mathbb{Z}[\sqrt{-1}]$, with $\phi(u + v\sqrt{-1}) = u^2 + v^2$.

Euclidean algorithm

An efficient procedure for finding greatest common divisors is Euclid's famous algorithm.

Input: $a, b \neq 0$
Output: $d = \text{gcd}(a, b)$

while $b \neq 0$:
    $r := a - q \cdot b$;
    $a := b$; $b := r$;
return a;

Correctness: if $a = q \cdot b + r$, then $\text{gcd}(a, b) = \text{gcd}(b, r)$.

Termination: $0 \leq \phi(r) = \phi(a - q \cdot b) < \phi(b)$, so $\phi(b)$ decreases.

Extended Euclidean algorithm

With a little more bookkeeping it is possible to obtain multipliers.

Input: $a, b \neq 0$
Output: $d = \text{gcd}(a, b)$, and multipliers s, t such that $d = s \cdot a + t \cdot b$

$s_1 := 1; \quad t_1 := 0;$
$s_2 := 0; \quad t_2 := 1;$
while $b \neq 0$:
    $s_0 := s_1; \quad t_0 := t_1;$
    $s_1 := s_2; \quad t_1 := t_2;$
    $r := a - q \cdot b;$
    $a := b; \quad b := r;$
    $s_2 := s_0 - q \cdot s_1; \quad t_2 := t_0 - q \cdot t_1;$
return $a, s_1, t_1;$

Termination and correctness as before.

At the beginning of the while loop: $s_1 a + t_1 b = a$.

Application: modular inverses

Proposition *Let R be a Euclidean domain, $S = R/mR$. Then $\bar{a} \in S$ is a unit if and only if* gcd$(a, m) = 1$*, and extended Euclidean algorithm produces $\bar{a}^{-1}$.*

$\bar{a}$ is unit $\iff$
there exists $s \in R$ with $a \cdot s \equiv 1 \bmod m \iff$
there exist $s, t \in R$ with $a \cdot s + m \cdot t = 1 \iff$
gcd$(a, m) = 1$ and $\bar{s} = \bar{a}^{-1}$.

Hence inverses in

(i) $\mathbb{Z}/m\mathbb{Z}$
(ii) finite fields $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$
(iii) finite fields $\mathbb{F}_{p^k} \cong \mathbb{F}_p[x]/f\mathbb{F}_p[x]$
(iv) number fields $\mathbb{Q}[x]/g\mathbb{Q}[x]$.

Continued fractions

The Euclidean algorithm is closely related to the continued fraction expansion of rational numbers. If we let a and b be positive integers with $a > b$, the Euclidean algorithm determines positive integers q_i, r_i with $a = q_0 b + r_0$,
$b = q_1 r_0 + r_1$,
$r_0 = q_2 r_1 + r_2$,
$\vdots$
$r_{k-2} = q_k r_{k-1}$, so $r_k = 0$. But then

$$\frac{a}{b} = q_0 + \frac{r_0}{b} = q_0 + \frac{1}{\dfrac{b}{r_0}} = q_0 + \frac{1}{q_1 + \dfrac{r_1}{r_0}} =$$

$$= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k}}}}.$$

An expansion of the kind on the right is called a (*finite*) *regular continued fraction*, and is usually denoted by $[q_0; q_1, \dots q_k]$.

The positive integers q_i are called *partial quotients*; note that $q_k > 1$. Conversely, it is clear that every such continued fraction determines a rational number. The main importance of finite continued fractions lies in the possibility to generalize to expansions of arbitrary real numbers, by allowing *infinite* expansions $[q_0; q_1, \dots]$. Such an infinite expansion can be obtained from a positive real x by setting $x_0 = x$ and $q_i = \lfloor x_i \rfloor$, where $x_{i+1} = 1/(x_i - q_i)$, for $i \geq 1$. It can be shown that the rational numbers $c_k = [q_0; q_1, \dots, q_k]$ form a sequence of increasingly good rational approximations to x, converging to x; the c_k are called the *convergents* to x. Right now we will only use infinite continued fraction in a worst case analysis of Euclid's algorithm, for which purpose it suffices to look at one special case.

Lemma *Let ϕ be the positive real root of $f = x^2 - x - 1$, so $\phi = \frac{\sqrt{5}+1}{2}$. Then $\phi = [1; 1, 1, \ldots]$ and the convergents to ϕ are the rational numbers $c_k = F_{k+1}/F_k$, where F_k is the k-th Fibonacci number, given by $F_0 = F_1 = 1$, and $F_j = F_{j-1} + F_{j-2}$ for $j \geq 2$. Moreover*

$$F_k = \frac{1}{\sqrt{5}}(\phi^{k+1} - \bar{\phi}^{k+1}),$$

where $\bar{\phi} = \frac{-\sqrt{5}+1}{2}$ is the conjugate of ϕ.

Proof Since ϕ is a root of $x^2 - x - 1$, we have $\phi \cdot (\phi - 1) = 1$, hence $(\phi - 1)^{-1} = \phi$. But since $f(1) = -1 < 0 < 1 = f(2)$ we see that $1 < \phi < 2$, so for the continued fraction development we find $x_0 = \phi$, $q_0 = 1$ and $x_1 = 1/(x_0 - 1) = x_0$. That proves the first part. For the second assertion one proceeds by induction: clearly $c_0 = 1, c_1 = 2$ and

$$c_{i+1} = 1 + \frac{1}{c_i} = 1 + \frac{F_{k-1}}{F_k} = \frac{F_k + F_{k-1}}{F_k} = \frac{F_{k+1}}{F_k}.$$

The final statement follows easily by induction, using that ϕ and $\bar{\phi}$ satisfy $x^n = x^{n-1} + x^{n-2}$.

Theorem *The Euclidean algorithm on input a, b less than N takes at most $\lceil \log_\phi(\sqrt{5}N) \rceil - 2$ division steps.*

Proof The maximum number of division steps occurs when $a = F_n$ and $b = F_{n+1}$ with n maximal such that $F_{n+1} < N$. The result follows from the expression for F_k in the Lemma, using that $\bar{\phi} < 1$.