8 Domains

After fields, domains are the most common form of rings. In fact, certain domains best capture the features of our favourite rings: the ring $\mathbb{Z}$ of integers and the ring $\mathbb{K}[x]$ of univariate polynomials with coefficients in a field $\mathbb{K}$.

8.0 Recognizing Domains

How do we identify domains among all commutative rings? We first characterize domains via subrings.

Proposition 8.0.0. *Every commutative domain is isomorphic to a subring of a field.*

Proof. Let R be a commutative domain and set $D := R \setminus \{0_R\}$ to be the subset of nonzero elements in R. Since R is a domain, the subset D is multiplicative: the product of two nonzero elements in R is also nonzero. Theorem 7.0.2 shows that any nonzero fraction r/d in the ring $R[D^{-1}]$ of fractions is a unit, so $R[D^{-1}]$ is a field. Theorem 7.0.2 also provides the canonical ring homomorphism $\eta \colon R \to R[D^{-1}]$ such that, for any nonzero element d in D, the image $\eta(d) = d/1$ is a unit in $R[D^{-1}]$. It follows that $\operatorname{Ker}(\eta) = \langle 0_R \rangle$ and the map η is injective. We conclude that R is isomorphic to the subring $\eta(R)$ in $R[D^{-1}]$. □

Example 8.0.1. The ring $\mathbb{Z}$ of integers is a domain and the field $\mathbb{Q}$ of rational numbers is its field of fractions.

Example 8.0.2. The ring $\mathbb{K}[x]$ of univariate polynomials with coefficients in the field $\mathbb{K}$ is a domain. The field

$$\mathbb{K}(x) := \left\{ \tfrac{f}{g} \mid f, g \in \mathbb{K}[x] \text{ and } g \neq 0 \right\}$$

of rational functions is its field of fractions.

Problem 8.0.3. Show that the ring $\mathbb{Q}[\mathrm{i}] := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{Q}\}$ of Gaussian rationals is the field of fractions for the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers.

Solution. As a subring of the field $\mathbb{C}$ of complex numbers, we see that $\mathbb{Z}[\mathrm{i}]$ is a domain. Every element in the field of factions for $\mathbb{Z}[\mathrm{i}]$ can be expressed in the form

$$\begin{aligned} \frac{a + b\,\mathrm{i}}{c + d\,\mathrm{i}} &= \frac{(a + b\,\mathrm{i})(c - d\,\mathrm{i})}{(c + d\,\mathrm{i})(c - d\,\mathrm{i})} \\ &= \frac{(a\,c + b\,d) - (a\,d - b\,c)\,\mathrm{i}}{c^2 + d^2} = \left(\frac{a\,c + b\,d}{c^2 + d^2}\right) + \left(\frac{b\,c - a\,d}{c^2 + d^2}\right)\mathrm{i} \in \mathbb{Q}[\mathrm{i}] \end{aligned}$$

for some integers a, b, c, and d such that $(c, d) \neq (0, 0)$. □

As with fields, we determine when a quotient ring is a domain.

Theorem 8.0.4. *For any commutative ring R and any ideal I in R, the following are equivalent:*
(a) *The quotient ring R/I is a domain.*
(b) *We have $I \neq \langle 1_R \rangle = R$ and the product $f\,g$ being in ideal I implies that f is in I or g is in I.*
(c) *The ideal I is the kernel of a ring homomorphism of R to a field.*

Compare with Definition 1.2.7.

Proof.
(a) ⇔ (b): The quotient ring R/I is not the zero ring if and only if $I \neq \langle 1_R \rangle = R$. For any elements f and g in the ring R, the product $f\,g$ is in I if and only if the coset $f\,g + I = (f + I)(g + I)$ equals $0 + I$ in the quotient ring R/I. Hence, the quotient ring R/I is a domain if and only if $I \neq \langle 1_R \rangle = R$ and, the membership $f\,g \in I$ implies that $f + I = 0 + I$ or $g + I = 0 + I$ in R/I or equivalently that $f \in I$ or $g \in I$.
(a) ⇒ (c): Suppose that the quotient ring R/I is a domain. The canonical surjection $\pi\colon R \to R/I$ is a ring homomorphism and the canonical ring homomorphism η from the domain R/I into its field of fractions is injective. Hence, the ideal I is the kernel of the composite map $\eta\,\varphi$.
(c) ⇒ (a): Suppose that the ideal I is the kernel of a ring homomorphism from R into a field. The First Isomorphism Theorem 6.1.1 implies that the quotient ring R/I is isomorphic to a subring of the field. Since every subring of a domain is a domain, we see that the quotient ring R/I is a domain. □

Definition 8.0.5. An ideal I in commutative ring R is *prime* if it satisfies the equivalent conditions in Theorem 8.0.4.

Example 8.0.6. Every maximal ideal I in a commutative ring R is prime because the quotient ring R/I is a field.

Example 8.0.7. The zero ideal $\langle 0 \rangle$ in a domain R is prime because the quotient ring $R/\langle 0 \rangle \cong R$ is a domain.

Example 8.0.8. The prime ideals in the ring $\mathbb{Z}$ of integers are the principal ideals generated by nonnegative prime integers (including the zero ideal).

Proposition 8.0.9. *For any prime ideal P in a commutative ring R, the subset $D := R \setminus P$ is multiplicative and the ring $R[D^{-1}]$ of fractions has a unique maximal ideal.*

Proof. Since P is prime, we have $R = \langle 1_R \rangle \neq P$ and $1_R \in D$. Moreover, the product of two elements in R belongs to P if and only if one of the factors belongs to the ideal P, so the product of any two elements in D is also in the subset D. Thus, the subset $D = R \setminus P$ is multiplicative.

Consider the subset $P[D^{-1}] := \{q/e \in R[D^{-1}] \mid q \in P \text{ and } e \in D\}$ in the ring $R[D^{-1}]$. For any elements p and q in P, any element r in

R, and any elements d and e in D, we have $p\,e + q\,d \in P$, $r\,q \in P$, $d\,e \in D$, $\frac{p}{d} + \frac{q}{e} = \frac{p\,e+q\,d}{d\,e} \in P[D^{-1}]$, and $\left(\frac{r}{d}\right)\left(\frac{q}{e}\right) = \frac{r\,p}{d\,e} \in P[D^{-1}]$, so $P[D^{-1}]$ is an ideal in $R[D^{-1}]$. By construction, any fraction r/d where $r \in D = R \setminus P$ is a unit in $R[D^{-1}]$. Hence, the only ideal containing a fraction not belonging to $P[D^{-1}]$ is the ideal $\langle 1_{R[D^{-1}]} \rangle = R[D^{-1}]$. We conclude that the ideal $P[D^{-1}]$ is the unique maximal ideal in the ring $R[D^{-1}]$. □

Proposition 8.0.10. *Let $\varphi\colon R \to S$ be a ring homomorphism between commutative rings. For any prime ideal J in the ring S, the preimage $\varphi^{-1}(J) := \{r \in R \mid \varphi(r) \in J\}$ is a prime ideal in the ring R.*

Proof. The Correspondence Theorem 6.2.0 demonstrates that the preimage $I := \varphi^{-1}(J)$ is an ideal in the ring R. As $\varphi(I) = J$, the Induced Map Lemma 6.1.0 establishes that the induce map $\widetilde{\varphi}\colon R/I \to R/J$ is well-defined ring homomorphism. Since

$$\widetilde{\varphi}(r + I) = \varphi(r) + J = 0 + J \quad \Leftrightarrow \quad \varphi(r) \in J \quad \Leftrightarrow \quad r \in \varphi^{-1}(J) = I$$

we see that $\operatorname{Ker}(\widetilde{\varphi}) = \langle 0_{R/I} \rangle$. The First Isomorphism Theorem 6.1.1 thereby shows that the quotient ring R/I is isomorphic to a subring of the domain R/J. Since every subring of a domain is a domain, we see that the quotient ring R/I is a domain. □

Exercises

Problem 8.0.11. Consider the subrings

$$\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \qquad \text{and}$$

$$\mathbb{Z}\left[\tfrac{1+\sqrt{5}}{2}\right] := \left\{a + b\left(\tfrac{1+\sqrt{5}}{2}\right) \,\middle|\, a, b \in \mathbb{Z}\right\}$$

of the field $\mathbb{R}$ of real numbers. For each subring, describe the elements in the field of fractions. Are these two fields the same? Is one contained in the other?

8.1 Euclidean Domains

Which rings have division with remainder? We naively start with the following declaration.

Definition 8.1.0. Let R be a commutative domain. A *Euclidean function* on R is a function $\nu\colon R \setminus \{0\} \to \mathbb{N}$ such that, for any element f in R and any element g in $R \setminus \{0\}$, there exists elements q and r in R such that $f = q\,g + r$ and either $r = 0$ or $\nu(r) < \nu(g)$. A *Euclidean domain* is a commutative domain which can be endowed with at least one Euclidean function.

A particular Euclidean function is *not* part of the definition of a Euclidean domain, as in general a Euclidean domain may admit many different Euclidean functions.

Remark 8.1.1. The defining property for a Euclidean function is equivalent to the following assertion: for any nonzero ideal $I = \langle g \rangle$ in R, every nonzero coset in the quotient ring R/I has a representative r such that $\nu(r) < \nu(g)$.

Example 8.1.2. Theorem 1.1.2 shows that the ring $\mathbb{Z}$ of integers is a Euclidean domain with the Euclidean function $\nu : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ defined by $\nu(m) := |m|$ for all nonzero integers m.

Example 8.1.3. Theorem 4.0.4 establishes that, for any field $\mathbb{K}$, the univariate polynomial ring $\mathbb{K}[x]$ is a Euclidean domain with the Euclidean function $\nu\colon \mathbb{K}[x] \setminus \{0\} \to \mathbb{N}$ defined by $\nu(f) := \deg(f)$ for all nonzero polynomials f.

Problem 8.1.4. Verify that any field $\mathbb{K}$ is a Euclidean domain with the Euclidean function $\nu\colon \mathbb{K} \setminus \{0\} \to \mathbb{N}$ defined by $\nu(k) = 1$ for all nonzero elements k in $\mathbb{K}$.

Solution. Let u be a nonzero element in $\mathbb{K}$. For any element k in $\mathbb{K}$, we have $k = (k\,u^{-1})\,u + 0$. □

In this pathological case, the remainder is always zero.

Problem 8.1.5. Confirm that the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers is a Euclidean domain with the Euclidean function $\nu\colon \mathbb{Z}[\mathrm{i}] \setminus \{0\} \to \mathbb{N}$ defined by $\nu(a + b\,\mathrm{i}) := a^2 + b^2$.

Geometric Solution. The elements of $\mathbb{Z}[\mathrm{i}]$ form a square lattice in the complex plane. For any element z in $\mathbb{Z}[\mathrm{i}]$, the ideal $\langle z \rangle$ forms a similar lattice: writing $z = r\,e^{\mathrm{i}\theta}$ where $r \in \mathbb{R}$ and $\theta \in [0, 2\pi)$, the lattice corresponding to $\langle z \rangle$ is obtained by rotating through the angle θ followed by stretching by the factor $r = |z|$. For any complex number w, there is at least one point of the lattice corresponding to $\langle z \rangle$ whose square distance from w is at most $\frac{1}{2}\,|z|^2 = \frac{1}{2} r^2$. Let $q\,z$ be that closed point and set $p := w - q\,z$. It follows that $|p|^2 \leqslant \frac{1}{2}\,|z|^2 < |z|^2$ as required. Since there may be more than one choice for $q\,z$, this division with remainder is not unique. □

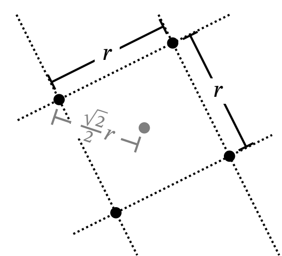

Figure 8.1: Nearest Gaussian integer in ideal

Algebraic Solution. Divide the complex number w by the complex number z; there is a complex number $c = x + y\,\mathrm{i}$ where $x, y \in \mathbb{R}$ such that $w = c\,z$. Choose a nearest Gaussian integer $a + b\,\mathrm{i}$, so $x := a + x_0$ and $y := b + y_0$ where $a, b \in \mathbb{Z}$ and $-\frac{1}{2} \leqslant x_0, y_0 < \frac{1}{2}$. The product $(a + b\,\mathrm{i})\,z$ is the required point in $\langle z \rangle$ because we have $|x_0 + y_0\,\mathrm{i}|^2 < \frac{1}{2}$ and $|w - (a + b\,\mathrm{i})\,z|^2 = |z\,(x_0 + y_0\,\mathrm{i})|^2 < \frac{1}{2}\,|z|^2$. □

We extend greatest common divisors to commutative domains in the most obvious way; compare with Definition 1.1.4.

Definition 8.1.6. Let f and g be nonzero elements in a commutative domain R. An element d in R is a *greatest common divisor* of f and g, denoted by $\gcd(f, g)$, if

- the element d divides both f and g, and
- any element e in R, that divides both f and g, also divides d.

Two ring elements are *coprime* if 1 is a greatest common divisor.

A greatest common divisor may not exist. Moreover, when a greatest common divisor exists, it may not be unique.

Example 8.1.7. Consider the domain

$$R := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Observe that $9 = (3)(3) = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Both 3 and $2 + \sqrt{-5}$ divide 9, but neither divides the other. Hence, the ring elements 9 and $6 + 3\sqrt{-5}$ do not have a greatest common divisor in R.

Example 8.1.8. In any field, every nonzero element is a greatest common divisor for any pair of nonzero elements.

Lemma 8.1.9. *Let f and g be nonzero elements in commutative domain R. Assume that the element d in R is a greatest common divisor for f and g. A ring element e in R is also a greatest common divisor for f and g if and only if there exists a unit u in R such that $e = u\,d$.*

When $R = \mathbb{Z}$, we typically impose uniqueness by requiring the greatest common divisor to be positive. When $\mathbb{K}$ is field and $R = \mathbb{K}[x]$, we force uniqueness by requiring the greatest common divisor to be monic.

Proof.

$\Rightarrow$: Suppose that $e = \gcd(f, g)$. Since e divides f and g, it follows that e divides d. Similarly, d divides f and g, so d divides e. Hence, there exists elements u and v in R such that $d = u\,e$ and $e = v\,d$. It follows that $d = u\,e = u\,v\,d$. As R is a domain, we deduce that $1 = u\,v$.

$\Leftarrow$: Suppose there is a unit u such that $e = u\,d$. Since d divides f, there exists an element x in R such that $f = x\,d = x\,u\,e$, so e divides f. By symmetry, we see that e divides g. Assume that c divides f and g. Since d is a greatest common divisor for f and g, there exists an element w in R such that $d = w\,c$, so $e = u\,w\,c$. Thus, e is also a greatest common divisor for f and g. □

As with integers, greatest common divisors are computable in a Euclidean domain.

Algorithm 8.1.10 (Euclidean Algorithm)**.**
Input: Elements f and g in a Euclidean domain R.
Output: A greatest common divisor of f and g.

If $g = 0$ then return f.
Find q and r such that $f = q\,g + r$ where $\nu(f) < \nu(g)$ or $r = 0$.
Return $\gcd(g, r)$.

Proof of Correctness. It suffices to show that, when $f = q\,g + r$ and $r \neq 0$, there exists a unit u in R such that $\gcd(f, g) = u \gcd(g, r)$. Let d be a greatest common divisor of f and g, and let e be a greatest common divisor of g and r. Since d divides f and g, the ring element d also divides $r = f - q\,g$, so e divides d. Similarly, the ring element e divides $f = q\,g + r$, so d divides e. Hence, there exists ring elements u and v such that $d = u\,e$ and $e = v\,d$. It follows that $d = u\,e = u\,v\,d$. As R is domain, we deduced that $1 = u\,v$.

The algorithm terminates after finitely many iterations because $\nu(r) < \nu(g)$ and $\mathrm{Im}(\nu) \subseteq \mathbb{N}$. □

Problem 8.1.11. Find the greatest common divisor of $x^6 - 1$ and $x^4 - 1$ in $\mathbb{Q}[x]$.

Solution. The Euclidean Algorithm yields

$$
\begin{array}{r|l}
 & \quad\quad\quad\quad\quad\quad\quad\quad x^2 \\
\hline
x^4 - 1 & x^6 + 0\,x^5 + 0\,x^4 + 0\,x^3 + 0\,x^2 + 0\,x - 1 \\
 & x^6 + 0\,x^5 + 0\,x^4 + 0\,x^3 + x^2 \\
\hline
 & \quad\quad\quad\quad\quad\quad\quad\quad x^2 + 0\,x - 1
\end{array}
\qquad
\begin{array}{r|l}
 & \quad\quad\quad\quad\quad\quad x^2 + 0\,x + 1 \\
\hline
x^2 + 0\,x - 1 & x^4 + 0\,x^3 + 0\,x^2 + 0\,x - 1 \\
 & x^4 + 0\,x^3 - x^2 \\
\hline
 & \quad\quad\quad\quad x^2 + 0\,x - 1 \\
 & \quad\quad\quad\quad x^2 + 0\,x - 1 \\
\hline
 & \quad\quad\quad\quad\quad\quad\quad\quad\quad 0
\end{array}
$$

so $\gcd(x^6 - 1, x^4 - 1) = x^2 - 1$. □

Problem 8.1.12. Find a greatest common divisor for 10 and $4 + 3\,\mathrm{i}$ in the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers.

Solution. The Euclidean Algorithm yields

$$
\begin{aligned}
10 &= (2 - \mathrm{i})(4 + 3\,\mathrm{i}) + (-1 - 2\,\mathrm{i}) \\
4 + 3\,\mathrm{i} &= (-2 - \mathrm{i})(-1 - 2\,\mathrm{i}) + 0
\end{aligned}
$$

so $\gcd(10, 4 + 3\,\mathrm{i}) = -1 - 2\,\mathrm{i}$. □

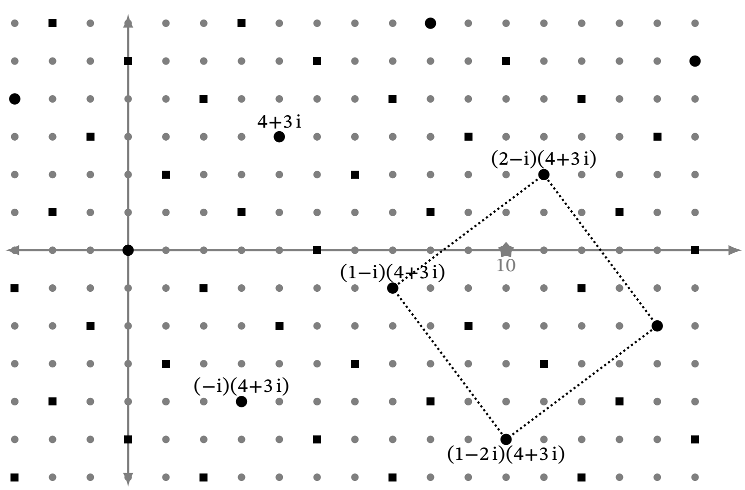

Figure 8.2: Gaussian division with remainder

Exercises

Problem 8.1.13. Let $\omega := \frac{1}{2}(-1 + \sqrt{3}\,\mathrm{i}) \in \mathbb{C}$ be one of the complex roots of the polynomial $x^2 + x + 1 \in \mathbb{C}[x]$. Prove that the commutative domain $\mathbb{Z}[\omega] := \{a + b\,\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a Euclidean domain with the function $\nu\colon \mathbb{Z}[\omega] \to \mathbb{N}$ is defined by $\nu(a + b\,\omega) = a^2 - a\,b + b^2$.

8.2 Extended Euclidean Algorithm

How can we improve on the Euclidean Algorithm? We want to write a greatest common divisor as a linear combination.

Algorithm 8.2.0 (Extended Euclidean Algorithm)**.**
Input: Elements f and g in a Euclidean domain R.
Output: Elements $d, s, t \in R$ such that $s\,f + t\,g = d = \gcd(f, g)$.

Set $(d_0, d_1, s_0, s_1, t_0, t_1) := (f, g, 1, 0, 0, 1)$.
While $d_1 \neq 0$ do
  Find $q, r \in R$ such that $d_0 = q\,d_1 + r$ and $\nu(r) < \nu(d_1)$.
  Set $(d_0, d_1, s_0, s_1, t_0, t_1) := (d_1, d_0 - q\,d_1, s_1, s_0 - q\,s_1, t_1, t_0 - q\,t_1)$.
Return (d_0, s_0, t_0).

Proof of Correctness. The remainders r produce a decreasing sequence $\nu(r)$ of nonnegative integers, so eventually a remainder will be zero. Thus, the while loop must terminate.

Since $\gcd(d_0, d_1) = \gcd(d_1, r) = \gcd(d_1, d_0 - q\,d_1)$, it suffices to show that the equations $d_0 = s_0\,f + t_0\,g$ and $d_1 = s_1\,f + t_1\,g$ hold throughout the calculation. We verify these equalities for the initial conditions and each repetition of the loop:

$$s_0\,f + t_0\,g \leftrightsquigarrow 1(f) + 0(g) = f \leftrightsquigarrow d_0\,,$$
$$s_0\,f + t_0\,g \leftrightsquigarrow s_1\,f + t_1\,g = d_1 \leftrightsquigarrow d_0\,,$$
$$s_1\,f + t_1\,g \leftrightsquigarrow 0(f) + (1)(g) = g \leftrightsquigarrow d_1\,,$$
$$\begin{aligned} s_1\,f + t_1\,g &\leftrightsquigarrow (s_0 - q\,s_1)(f) + (t_0 - q\,t_1)(g) \\ &= (s_0\,f + t_0\,g) - q(s_1\,f + t_1\,g) = d_0 - q\,d_1 \leftrightsquigarrow d_1\,. \end{aligned}$$ □

Problem 8.2.1. In $\mathbb{Z}$, express $\gcd(1254, 1110)$ as an integer linear combination of 1254 and 1110.

Solution. Since we have

$$\begin{aligned} 1254 &= (1)(1110) + 144 & 102 &= (2)(42) + 18 \\ 1110 &= (7)(144) + 102 & 42 &= (2)(18) + 6 \\ 144 &= (1)(102) + 42 & 18 &= (3)(6) + 0\,, \end{aligned}$$

the Extended Euclidean Algorithm 8.2.0 gives

$$(54)(1254) + (-61)(1110) = 6 = \gcd(1254, 1110)\,.$$ □

d_0	d_1	s_0	s_1	t_0	t_1	q
1254	1110	1	0	0	1	1
1110	144	0	1	1	−1	7
144	102	1	−7	−1	8	1
102	42	−7	8	8	−9	2
42	18	8	−23	−9	26	2
18	6	−23	54	26	−61	3
6	0	54	−185	−61	209	

Table 8.1: Values of the local variables when using Algorihm 8.2.0 to compute $\gcd(1254, 1110)$

Problem 8.2.2. In $\mathbb{F}_3[x]$, express $\gcd(x^3 + 2\,x^2 + 2, x^2 + 2\,x + 1)$ as an $\mathbb{F}_3[x]$-linear combination of $x^3 + 2\,x^2 + 2$ and $x^2 + 2\,x + 1$.

Solution. Since we have

$$\begin{aligned} x^3 + 2\,x^2 + 2 &= (x)(x^2 + 2\,x + 1) + (x - 1) \\ x^2 + 2\,x + 1 &= (x)(x - 1) + (-1) \\ x - 1&(-x + 1)(-1) + 0\,, \end{aligned}$$

the Extended Euclidean Algorithm 8.2.0 gives

$$(1)(x^3 + 2x^2 + 2) + (2x)(x^2 + 2x + 1) = 2x + 2 = \gcd(f, g)\,.$$ □

d_0	d_1	s_0	s_1	t_0	t_1	q
x^3+2x^2+2	x^2+2x+1	1	0	0	1	x
x^2+2x+1	$2x+2$	0	1	1	$2x$	$2x+2$
$2x+2$	0	1	$x+1$	$2x$	$2x^2+2x+1$	

Table 8.2: Values of the local variables when using Algorithm 8.2.0 to compute $\gcd(x^3+2x^2+2, x^2+2x+1)$

The Extended Euclidean Algorithm 8.2.0 leads to an effective version of Sun Zi's Remainder Theorem 6.3.6.

Algorithm 8.2.3 (Effective Remainder Theorem)**.**

Input: Pairwise coprime elements $g_1, g_2, \dots, g_n$ and elements $f_1, f_2, \dots, f_n$ in a Euclidean domain R.
Output: An element $f \in R$ such that, for any $1 \leqslant j \leqslant n$, we have $f + \langle g_j \rangle = f_j + \langle g_j \rangle$ in $R/\langle g_j \rangle$.

Set $(j, g, f) := (2, g_1, f_1)$.
While $j \leqslant n$ do
  Find $s, t \in R$ such that $s\,g + t\,g_j = 1$.
  Compute $q, r \in R$, such that $(s\,g\,f_j + t\,g_j\,f) = q(g\,g_j) + r$
    and $\nu(r) < \nu(g\,g_j)$ or $r = 0$.
  Set $(j, g, f) := (j+1, g\,g_j, r)$.
Return f.

Proof of Correctness. For each repetition of the loop, we show that $f + \langle g_k \rangle = f_k + \langle g_k \rangle$ for all $1 \leqslant k \leqslant j$. Before the loop, we have $f = f_1$, so $f + \langle g_1 \rangle = f + \langle g_1 \rangle$ in $R/\langle g_j \rangle$. At the j-th iteration of the loop, we have $g = g_1 g_2 \cdots g_{j-1}$, so $\gcd(g, g_j) = 1$. Given that $s\,g + t\,g_j = 1$, we see that $(s\,g\,f_j + t g_j f) + \langle g_k \rangle = f + \langle g_k \rangle = f_k + \langle g_k \rangle$ in $R/\langle g_k \rangle$ for any $1 \leqslant k \leqslant j-1$ and $(s\,g\,f_j + t g_j f) + \langle g_j \rangle = f_j + \langle g_j \rangle$ in $R/\langle g_j \rangle$. Since $(s\,g\,f_j + t\,g_j\,f) = q(g\,g_j) + r$ in $R/\langle g_k \rangle$, we deduce that $r + \langle g_k \rangle = f_k + \langle g_k \rangle$ for any $1 \leqslant k \leqslant j$. □

Problem 8.2.4. Find an integer m such that $m \equiv 7 \mod 11$ and $m \equiv 5 \mod 17$.

Solution. The first iteration in the Effective Remainder Algorithm 8.2.3 gives $(-3)(11) + (2)(17) = 1$ and

$$(-3)(11)(5) + (2)(17)(7) = 73 = (0)(187) + (73)\,.$$

We confirm that $73 = (6)(11) + 7$ and $73 = (4)(17) + 5$, so integer 73 meets the requirements. □

Problem 8.2.5. Find a polynomial f in $\mathbb{F}_5[x]$ such that

$$\begin{aligned} f + \langle x \rangle &= 1 + \langle x \rangle && \text{in } \mathbb{F}_5[x]/\langle x \rangle, \\ f + \langle x+2 \rangle &= 3 + \langle x+2 \rangle && \text{in } \mathbb{F}_5[x]/\langle x+2 \rangle, \text{ and} \\ f + \langle x^2+x+2 \rangle &= (x+1) + \langle x^2+x+2 \rangle && \text{in } \mathbb{F}_5[x]/\langle x^2+x+2 \rangle. \end{aligned}$$

Solution. The first iteration in the Effective Remainder Algorithm 8.2.3 gives $(2)(x) + (3)(x+2) = 1$ and

$$(2)(x)(3) + (3)(x+2)(1) = 4\,x + 1 = (0)(x^2 + 2\,x) + (4\,x + 1)\,.$$

The second iteration gives

$$(3\,x+4)(x^2+2\,x) + (2\,x+3)(x^2+x+2) = 1$$

$$\begin{aligned} (3\,x+4)(x^2+2\,x)(x+1) + (2\,x+3)(x^2+x+2)(4\,x+1) &= x^4 + x^2 + 4\,x + 1 \\ &= (1)(x^4 + 3\,x^2 + 4\,x^2 + 4\,x) + (2\,x^3 + 2\,x^2 + 1)\,. \end{aligned}$$

Finally, we verify that

$$\begin{aligned}
2\,x^3 + 2\,x^2 + 1 &= (2\,x^2 + 2\,x)(x) + 1\,,\\
2\,x^3 + 2\,x^2 + 1 &= (2\,x^2 + 3\,x + 4)(x + 2) + 3\,,\\
2\,x^3 + 2\,x^2 + 1 &= (2\,x)(x^2 + x + 2) + (x + 1)\,.
\end{aligned}$$

Therefore, the desired polynomial is $2\,x^3 + 2\,x^2 + 1$. □

Exercises

Problem 8.2.6. Let $\mathbb{F}_2 := \mathbb{Z}/\langle 2\rangle$ be the field with two elements. Find a polynomial f in $\mathbb{F}_2[x]$ such that

$$\begin{aligned}
f + \langle x\rangle &= 1 + \langle x\rangle && \text{in } \mathbb{F}_2[x]/\langle x\rangle,\\
f + \langle x\rangle &= (x + 1) + \langle x^2 + x + 1\rangle && \text{in } \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle,\\
f + \langle x^4 + x^3 + 1\rangle &= (x^3 + x + 1) + \langle x^4 + x^3 + 1\rangle && \text{in } \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle.
\end{aligned}$$