Challenge 2

Wednesday, 27 November 2024 01:00

One of the first similarities we can observe between $\mathbb{Z}$ and $\mathbb{F}[x]$ is that for any $a(x) \in \mathbb{F}[x]$, $a(\alpha) = \beta \Leftrightarrow R_{x-\alpha}(a(x)) = \beta$ $\left(\deg(x-\alpha) = 1 \Rightarrow R_{x-\alpha}(a(x)) \in \mathbb{F}\right.$ and $a(x) = q(x)(x-\alpha) + R_{x-\alpha}(a(x)) \Rightarrow a(\alpha) = R_{x-\alpha}(a(x))(\alpha)\left.\right)$

(This explains why interpolation breaks down when $\deg(a(x)) \geq |\mathbb{F}|$)

This brings Lagrange interpolation closer to the Chinese Remainder Theorem, which in the script is defined upon modular congruences, but, as its name may indicate, can easily be reformulated in terms of remainders:

$$\begin{cases} x \equiv_{m_1} a_1 \\ \quad \vdots \\ x \equiv_{m_n} a_n \end{cases} \Longleftrightarrow \begin{cases} R_{m_1}(x) = a_1' \\ \quad \vdots \\ R_{m_n}(x) = a_n' \end{cases} \quad \text{where } a_i' = R_{m_i}(a_i)$$

The definition of this system requires R to be a Euclidean domain, as $R_m(x) = a \Leftrightarrow x = q \cdot m + a$, with a "smaller than" m or $a = 0$.

This can be done with a degree function $d: R \to \mathbb{N}$.

(i) $\forall a, b \in R, \exists q, r \in R: \ a = b \cdot q + r$ with $d(r) < d(b)$

(ii) $\forall a, b \in R: d(a) \leq d(ab)$

Furthermore, for the Chinese Remainder Theorem to work, $m_1, \dots, m_n$ need to be coprime. To formalise this notion, we have to introduce a gcd function $\gcd: R^2 \to R$.

Consider, for any $a, b \in R$, the ideal (a, b):

$(a, b) = \{ua + vb \mid u, v \in R\}$

$a = 1 \cdot a + 0 \cdot b \Rightarrow a \in (a, b) \Rightarrow (a, b) \neq \emptyset$

Since $\mathbb{N}$ is well-ordered, $\{d(x) \mid x \in (a, b)\}$ has a least element, m.

Define $\gcd(a, b)$ as one of the elements with minimal degree m:

$$d(\gcd(a, b)) = \min_{x \in (a,b)} d(x)$$

We can now define:

$$\begin{aligned} n \text{ and } m \text{ coprime} &\overset{\text{def}}{\Leftrightarrow} \gcd(m, n) \sim 1 \\ &\Rightarrow \gcd(m, n) = s \quad \text{with } s \in R^* \ (\text{def of } \sim) \\ &\Rightarrow \text{there exists } u, v \in R \text{ s.t. } um + vn = s \ (\gcd(m, n) \in (m, n)) \\ &\Rightarrow s^{-1}um + s^{-1}vn = 1 \ (s \in R^*) \\ &\Rightarrow \exists u', v' \in R: u'm + v'n = 1 \quad (\Delta) \end{aligned}$$

We now see that n coprime integers, as well as n coprime polynomials of degree 1, uniquely define an integer or a polynomial whose degree is less than that of

We now see that n coprime integers, as well as n coprime polynomials of degree 1, uniquely define an integer or a polynomial whose degree is less than that of their product (for integers, we define degree as the absolute value). To be more precise, there exists one equivalence class $E \in R/\prod_{i=1}^{n} m_i R$ s.t. any $x \in E$ is a solution of the system.

The quotient group R/mR is equal to $R/\equiv_m$, but proving this isn't necessary, we can just accept R/mR as an alternative notation of $R/\equiv_m$.

We also define $a \equiv_m b \overset{\text{def}}{\Leftrightarrow} m \mid a-b \Leftrightarrow \exists k \in R: a-b = km$ (k is denoted $\frac{a-b}{m}$)

For all $a, b, k \in R$:

$a \mid b+ka \Leftrightarrow a \cdot \left(\frac{b+ka}{a}\right) = b+ka \Leftrightarrow a\left(\frac{b+ka}{a} - k\right) = b \Rightarrow a \mid b$

$\Leftrightarrow b+ka \equiv_a b$ $(\clubsuit)$

Consider for some coprime $m, n \in R$ the function:

$\varphi: R/mR \times R/nR \to R/mnR$

$\varphi(a,b) = a \cap b$

$\gcd(m,n) \sim 1 \Rightarrow$ There exist $u, v \in R$ s.t. $um + vn = 1$ (Δ)

$\Rightarrow um \equiv_n 1 \wedge vn \equiv_m 1$ $(\clubsuit)$

$\Rightarrow$ for any $([x]_m, [y]_n) \in R/mR \times R/nR$:

$yum + xvn \equiv_m x \wedge yum + xvn \equiv_n y$ $(\clubsuit)$

$\Rightarrow yum + xvn \in [x]_m \cap [y]_n$ (def of equivalence class)

$\Rightarrow \varphi([x]_m, [y]_n) \neq \emptyset$ $(\circledast)$

For any $u \in \varphi([x]_m, [y]_n), v \in R$:

If $v \in [u]_{mn}$:

$v \equiv_{mn} u \Rightarrow v \equiv_m u \wedge v \equiv_n u$ $(ab \mid c \Rightarrow a \mid c)$

$\Rightarrow v \in \varphi([x]_m, [y]_n)$ (def of φ)

If $v \in \varphi([x]_m, [y]_n)$:

$v \equiv_m u \wedge v \equiv_n u \Rightarrow v \equiv_{mn} u$ $(*)$

$\Rightarrow v \in [u]_{mn}$

$(*)$ $\gcd(m,n) \sim 1 \Rightarrow$ there exists $k, l \in R$ s.t. $km + ln = 1$ (Δ)

$\Rightarrow u-v = u-v \cdot (km + ln)$

$= km(u-v) + ln(u-v)$

$= kmn\frac{u-v}{n} + lnm\frac{u-v}{m}$ $(m \mid u-v \wedge n \mid u-v)$

$= mn\left(k\frac{u-v}{n} + l\frac{u-v}{m}\right)$

$\Rightarrow mn \mid u-v \Leftrightarrow u \equiv_{mn} v$

$\Rightarrow \varphi([x]_m, [y]_n) = [u]_{mn}$ for any $u \in \varphi([x]_m, [y]_n)$ $(\circledast)$

$\Rightarrow \varphi([x]_m, [y]_n) \in R/mnR$

$\Rightarrow \varphi$ maps to the codomain

φ is obviously totally and well-defined: the intersection of 2 sets is always defined and unique.

Furthermore, φ is surjective:

For all $[x]_{mn} \in R/mnR$:

$x \equiv_m x \wedge x \equiv_n x$

$\Rightarrow x \in [x]_m \cap [x]_n$

$x \equiv_m x \wedge x \equiv_n x$
$\Rightarrow x \in [x]_m \cap [x]_n$
$\Rightarrow \varphi([x]_m, [x]_n) = [x]_{mn}$ (✱)
$\Rightarrow \varphi$ surjective $(([x]_m, [x]_n) \in R/mR \times R/nR)$

Finally:
For all $([x]_m, [y]_n), ([w]_m, [z]_n) \in R/mR \times R/nR$:
If $\varphi([x]_m, [y]_n) = \varphi([w]_m, [z]_n)$:
There exists some $u \in \varphi([x]_m, [y]_n)$ (✱):
$u \equiv_m x \wedge u \equiv_m w \wedge u \equiv_n y \wedge u \equiv_n z$
$\Rightarrow x \equiv_m w \wedge y \equiv_n z$ (transitivity of $\equiv_x$)
$\Rightarrow [x]_m = [w]_m \wedge [y]_n = [z]_n$
$\Rightarrow ([x]_m, [y]_n) = ([w]_m, [z]_n)$
$\Rightarrow \varphi$ is injective

φ is thus bijective
$\Rightarrow$ the system $x \equiv_m a \wedge x \equiv_n b$ has exactly one set of solutions in R/mnR. (†)

We now only need to prove the uniqueness of the solution for an arbitrary amount of congruences. We do this by induction.
For all $n \in \mathbb{N}^*$, define the property:
$P(n) \Leftrightarrow \forall m_1, \dots, m_n, a_1, \dots, a_n \in R$:
$\gcd(m_i, m_j) \sim 1$ for all $\{i,j\} \in \{1, \dots, n\}$
$\rightarrow \exists! E \in R/\prod_{i=1}^{n} m_i R : x \in E \Leftrightarrow (\forall i \in \{1, \dots, n\} : x \equiv_{m_i} a_i)$

Trivially, $P(1)$ is true.
Assume $P(k)$ true for some $k \in \mathbb{N}$:
$\forall m_1, \dots, m_{k+1}, a_1, \dots, a_{k+1} \in R$ s.t. $\forall \{i,j\} \subseteq \{1, \dots, k+1\}: \gcd(m_i, m_j) \sim 1$:
$x \equiv_{m_k} a_k \wedge x \equiv_{m_{k+1}} a_{k+1} \Leftrightarrow x \equiv_{m_k m_{k+1}} b$ for some $[b]_{m_k m_{k+1}} \in R/m_k m_{k+1} R$ (†)
$\forall i \in \{1, \dots, k-1\}$:
$\gcd(m_i, m_k) \sim 1 \wedge \gcd(m_i, m_{k+1}) \sim 1$
$\Rightarrow$ There exists $u, v, u', v' \in R$ s.t. $um_i + vm_k = 1 \wedge u'm_i + v'm_{k+1} = 1$ (Δ)
$\Rightarrow (uu'm_i + uv'm_{k+1} + u'vm_k)m_i + vv'm_k m_{k+1} = 1$
$\Rightarrow d(\gcd(m_i, m_k m_{k+1})) \leq d(1)$ $(1 \in (m_i, m_k m_{k+1}))$
$\Rightarrow \gcd(m_i, m_k m_{k+1}) \sim 1$ ($d(1) \leq d(1 \cdot a)$ + antisymmetry of $\leq$)
By the induction hypothesis, the system is solvable for
$m_1, \dots, m_{k-1}, m_k m_{k+1}, a_1, \dots, a_{k-1}, b \Rightarrow P(k+1)$ holds

$m_1, \dots, m_{k-1}, m_k m_{k+1}, a_1, \dots, a_{k-1}, b \Rightarrow$ "$P(k+1)$" holds

We can thus generalise the Chinese Remainder theorem to any Euclidean domain D:

For any Euclidean domain D, the system of equations S:

$$S: \begin{cases} x \equiv_{m_1} a_1 \\ \vdots \\ x \equiv_{m_n} a_n \end{cases}$$

For some $n \in \mathbb{N}^*$, with $m_1, \dots, m_n, a_1, \dots, a_n \in D$ and $\gcd(m_i, m_j) \sim 1$ for any $\{i, j\} \subseteq \{1, \dots, n\}$

has exactly one solution $E \in D / \prod_{i=1}^{n} m_i D$ s.t. $x \in E \Leftrightarrow x$ solves S.