1 Division with Remainders

Recall that if $a, b \in \mathbb{Z}$ with $b \neq 0$, then there exists unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ such that:

$$a = bq + r$$

As a consequence, we note that:

$$\mathbb{Z}/n\mathbb{Z} = \{ \underbrace{0, 1, \ldots, n-1}_{\text{Possible Remainders}} \}$$

If $a \in \mathbb{Z}$, then:

$$a = nq + r \equiv r \pmod{n}$$

The uniqueness of r in $[0, n]$ implies the equivalence classes $0, 1, \ldots, n-1$ are distinct.

1.1 Division Theorem over a Field

Theorem 1.1

Let F be a field and $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$. Then, there exists unique polynomials $q(x)$ and $r(x) \in \mathbb{F}[x]$ such that $f(x) = g(x)q(x) + r(x)$ and $\deg r(x) < \deg g(x)$, including $r(x) = 0$.

Remark: This is essentially the end result of polynomial long division.

1.1.1 Example 1: Polynomial Division

Consider $f(x) = x^6 + x$ and $g(x) = x^2 + 1$ where $f, g \int \cdots \int \mathbb{F}_3[x]$. Then, we have:

$$\frac{f(x)}{g(x)} = 1x^4 - x^2 + 1$$

With the remainder being $x - 1$. Therefore, the final answer is:

$$x^6 + x = (x^2 + 1)(x^4 - x^2 + 1) + (x - 1)$$

Remark: Since $\mathbb{F}_3 = \{0, 1, 2\} \pmod 3$, we *can* change the negative numbers to the corresponding numbers in $\mathbb{F}_3$. So, we could write the above like so:

$$x^6 + x = (x^2 + 1)(x^4 + 2x^2 + 1) + (x + 2)$$

Where $-1 \equiv 2 \pmod 3$.

1.2 Consequences

If $\deg f(x) = n$, then:

$$\frac{\mathbb{F}[x]}{\langle f(x) \rangle} = \{\overbrace{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}}^{\text{Possible Remainders}} + \langle f(x) \rangle\}$$

Since the remainders are unique, each of these cosets are distinct.

- If $\deg f(x) = 1$, so $f(x) = ax + b$ ($a \neq 0$), then:

  $$\frac{\mathbb{F}[x]}{\langle ax + b \rangle} = \{a_0 + \langle f(x) \rangle\} \xrightarrow{\sim} \mathbb{F}$$

  Where a_0 is a constant. So:

  $$a_0 + \langle f(x) \rangle \mapsto a_0$$

- If $\deg f(x) = 2$, then:

$$\frac{\mathbb{F}[x]}{\langle f(x) \rangle} = \{a + bx + \langle f(x) \rangle\}$$

Recall that:

$$\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle} = \{a + bx + \langle x^2+1 \rangle\} \cong \mathbb{C}$$

$$a + bx \mapsto a + bi$$

- If $\deg f(x) = 0$, then:

$$\frac{\mathbb{F}[x]}{\langle f(x) \rangle} = \{0 + \langle f(x) \rangle\} \cong \{0\}$$

This is because $\deg r(x) < \deg f(x) = 0$, so it follows that the possible remainders are none.

1.3 Proof of Division Theorem

Proof. We need to show two things. Let $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$.

- Existence: We use proof by induction.
  - Base Case: If $\deg f(x) < \deg g(x)$, then $f(x) = g(x) \cdot 0 + f(x)$ so we can choose $q(x) = 0$ and $r(x) = f(x)$.
  - Inductive Step: Assume q, r exist for all polynomial f of degree $\deg f(x) < n$. If $\deg f(x) = n \geq m = \deg g(x)$, then we write

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

with $a_n \neq 0$ and

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

with $b_m \neq 0$. We set

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

so by construction, the x^n-terms cancel out and $\deg f_1(x) \leq n - 1 < n$. By the inductive hypothesis, there exists a $q_1(x), r_1(x) \in \mathbb{F}[x]$ such that

$$f_1(x) = g(x)q(x) + r_1(x)$$

and

$$\deg r_1(x) < \deg g(x)$$

which implies that

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x) q_1(x) + r_1(x)$$

which further implies that

$$f(x) = g(x)(a_n b_m^{-1} x^{n-m} + q_1(x)) + r_1(x)$$

with $\deg r_1(x) < \deg g(x)$. So, take $q(x) = a_n b_m^{-1} x^{n-m} + q(x)$ and $r(x) = r_1(x)$ and we are done.

- Uniqueness: Suppose $f(x) = g(x)q(x) + r(x) = g(x)\overline{q}(x) + \overline{r}(x)$ with $\deg r(x), \deg \overline{r}(x) < \deg g(x)$. Then, subtracting the two equation gives us:

$$\begin{aligned} 0 &= (g(x)q(x) + r(x)) - (g(x)\overline{q}(x) + \overline{r}(x)) \\ \implies \overline{r}(x) - r(x) &= g(x)(q(x) - \overline{q}(x)) \end{aligned}$$

Suppose, towards a contradiction, that $q(x) \neq \overline{q}(x)$. Then, $q(x) - \overline{q}(x) \neq 0$ so $\deg(q(x) - \overline{q}(x)) \geq 0$, thus

$$\deg(g(x)(q(x) - \overline{q}(x))) = \deg g(x) + \deg(q(x) - \overline{q})(x) \geq \deg g(x)$$

However, note that

$$\deg r(x), \deg \overline{r}(x) < \deg g(x)$$

which implies that

$$\deg(\overline{r}(x) - r(x)) \leq \max\{\deg r(x), \deg \overline{r}(x)\} < \deg g(x)$$

But this is a contradiction. Thus, $q(x) = \overline{q}(x)$ and $\overline{r}(x) - r(x) = 0$, so $\overline{r}(x) = r(x)$.

This concludes the proof. □

1.4 More Properties

Definition 1.1

We say $g(x)$ **divides** $f(x)$, and write $g(x)|f(x)$, if $f(x) = g(x)q(x)$, i.e. has remainder 0. We say that $g(x)$ is a **factor** of $f(x)$.

Definition 1.2

A **zero** or **root** of $f(x)$ is some $a \in \mathbb{F}$ such that $f(a) = 0$ for some a.

Definition 1.3

The **multiplicity** of a root a of $f(x)$ is the largest value of $k \in \mathbb{Z}_{\geq 0}$ such that $(x-a)^k | f(x)$.

Corollary 1.1

Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then, $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Proof. Write $f(x) = q(x)(x-a) + r(x)$ for $\deg r(x) < \deg(x-a) = 1$. This implies that $r(x)$ is constant. Plug in $x = a$ to get $f(a) = q(a)(\underbrace{a-a}_{0}) + r(a) = r(a)$. Then, $r(a) = f(a)$ and $r(x)$ is constant implies that $r(x) = f(a)$. □

Corollary 1.2

$f(a) = 0$ if and only if $(x-a)|f(x)$.