Lecture 41

Handout or Document Camera or Class Exercise

Compute the quotient and the remainder when

$$x^4 + 2x^3 + 2x^2 + 2x + 1$$

is divided by $g(x) = 2x^2 + 3x + 4$ in $\mathbb{Z}_5[x]$.

Solution:

$3x^2+4x+4$ quotient.

$$
\begin{array}{r}
2x^2+3x+4 \;\big|\; x^4+2x^3+2x^2+2x+1 \\
-(x^4+4x^3+2x^2) \\
\hline
3x^3+0x^2+2x \\
-(3x^3+2x^2+x) \\
\hline
3x^2+x+1 \\
-(3x^2+2x+1) \\
\hline
4x
\end{array}
$$

remainder

Instructor's Comments: This is the 10 minute mark

Proposition: Let $f(x), g(x) \in \mathbb{F}[x]$ be nonzero polynomials. If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = cg(x)$ for some $c \in \mathbb{F}$.

Proof: By definition, there exists $q(x)$ and $\hat{q}(x)$ in $\mathbb{F}[x]$ such that

$$\begin{aligned} f(x) &= g(x)q(x) \\ g(x) &= f(x)\hat{q}(x) \end{aligned}$$

Substituting the second equation into the first gives:

$$f(x) = f(x)\hat{q}(x)q(x) \quad \implies \quad f(x)(1 - \hat{q}(x)q(x)) = 0$$

As $f(x) \neq 0$, we see that $1 = \hat{q}(x)q(x)$. In fact, $\hat{q}(x)$ and $q(x)$ are nonzero. Now, note that $\deg(1) = 0$ and thus

$$0 = \deg(\hat{q}(x)q(x)) = \deg(\hat{q}(x)) + \deg(q(x))$$

(the last equality is an exercise - it holds in generality for nonzero polynomials). Therefore, $\deg(q(x)) = 0 = \deg(\hat{q}(x))$. Therefore, $q(x) = c \in \mathbb{F}$. Thus, substituting this into $f(x) = g(x)q(x)$ gives $f(x) = cg(x)$ completing the proof. ■

Instructor's Comments: This is the 25 minute mark

Theorem: (Remainder Theorem (RT)) Suppose that $f(x) \in \mathbb{F}[x]$ and that $c \in \mathbb{F}$. Then, the remainder when $f(x)$ is divided by $x - c$ is $f(c)$.

Proof: By the Division Algorithm for Polynomials, there exists unique $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = (x - c)q(x) + r(x)$$

with $r(x) = 0$ or $\deg(r(x)) < \deg(x - c) = 1$. Therefore, $\deg(r(x)) = 0$. In either case, $r(x) = k$ for some $k \in \mathbb{F}$. Plug in $x = c$ into the above equation to see that $f(c) = r(c) = k$. Hence $r(x) = f(c)$. ■

Example: Find the remainder when $f(z) = z^2 + 1$ is divided by

(i) $z - 1$

(ii) $z + 1$

(iii) $z + i + 1$

Solution:

(i) By the Remainder Theorem, the remainder is $f(1) = (1)^2 + 1 = 2$.

(ii) Note that $z + 1 = z - (-1)$. By the Remainder Theorem, the remainder is $f(-1) = (-1)^2 + 1 = 2$.

Note: $z^2 + 1 = (z - 1)(z + 1) + 2$

(iii) Note that $z + i + 1 = z - (-i - 1)$. By the Remainder Theorem, the remainder is $f(-i - 1) = (-i - 1)^2 + 1 = -1 + 2i + 1 + 1 = 2i + 1$.

Handout or Document Camera or Class Exercise

In $\mathbb{Z}_7[x]$, what is the remainder when $4x^3 + 2x + 5$ is divided by $x + 6$?

Solution: Since $x+6 = x-1$ in $\mathbb{Z}_7$, we see by the Remainder Theorem that the remainder is

$$4(1)^3 + 2(1) + 5 = 11 \equiv 4 \pmod 7$$

Instructor's Comments: Ideally this is the 40 minute mark.

Theorem: (Factor Theorem (FT)) Suppose that $f(x) \in \mathbb{F}[x]$ and $c \in \mathbb{F}$. Then the polynomial $x - c$ is a factor of $f(x)$ if and only if $f(c) = 0$, that is, c is a root of $f(x)$.

Proof: Note that $x - c$ is a factor of $f(x)$ if and only if $r(x) = 0$ via the Division Algorithm for Polynomials (DAP) which holds if and only if $r(x) = f(c) = 0$ via the Remainder Theorem (RT). $\blacksquare$

Handout or Document Camera or Class Exercise

Prove that there does not exist a real linear factor of

$$f(x) = x^8 + x^3 + 1.$$

Solution: By the factor theorem, it suffices to show that $f(x)$ has no real roots. We will show that $f(x) > 0$ for all $x \in \mathbb{R}$.

Case 1: Suppose that $|x| \geq 1$. Then $x^8 + x^3 \geq 0$ and hence $f(x) = x^8 + x^3 + 1 > 0$.

Case 2: Suppose that $|x| < 1$. Then $|x^3| < 1$ and so $x^3 + 1 > 0$ and hence $f(x) = x^8 + x^3 + 1 > 0$.

Instructor's Comments: Note here that $-1 < x^3 < 1$ and $x^8 \geq 0$. This is the 50 minute mark.