Lecture 17: Polynomials over Z/pZ

Friday, May 11, 2018 11:10 AM

In the previous lecture we showed:

- Theorem. Suppose F is a field and $f(x) \in F[x]$ is a poly. of deg. n. Then f has at most n distinct zeros in F.
- We also emphasized on distinguishing a poly. from the underlying function. For instance by Fermat's little theorem deg p polynomial $x^p - x$ gives us the zero function on $\mathbb{Z}_p$.

Next we see how fruitful it is to use poly. as functions!

Theorem. $x^p - x = x(x-1)\cdots(x-(p-1))$ in $\mathbb{Z}_p[x]$. (p: prime)

Pf. Since $x^p - x$ gives us the zero function on $\mathbb{Z}_p$, $0, 1, \ldots, p-1$ are distinct zeros of $x^p - x$. Hence by a result proved in the previous lecture $\exists\, g(x) \in \mathbb{Z}_p[x]$ ($\mathbb{Z}_p$ is a field and so we are allowed to use the mentioned result) s.t. $x^p - x = x(x-1)\cdots(x-(p-1))\, g(x)$.

Comparing degrees we get $\deg g = 0$; Comparing the

Lecture 17: Wilson's theorem

Friday, May 11, 2018 11:27 AM

leading coeff. we get $g(x)=1$. And so

$$x^p - x = x(x-1)\cdots(x-(p-1)). \quad \blacksquare$$

<u>Corollary</u> (Wilson's theorem)

Suppose p is prime. Then $(p-1)! \equiv -1 \pmod{p}$.

<u>Pf.</u> By the previous theorem

$$x^p - x = x(x-1)\cdots(x-(p-1)).$$

Compare coeff. of x: $-1 = (-1)^{p-1}(p-1)!$ in $\mathbb{Z}_p$.

$$\Rightarrow \quad (p-1)! \equiv (-1)^p \pmod{p}$$

- if $p=2$, then $(-1)^p = 1 \equiv -1 \pmod{2}$
- if $p \neq 2$, then $(-1)^p = -1$. $\blacksquare$

<u>Ex.</u> Show that $\binom{p-1}{i} \equiv (-1)^i \pmod{p}$ if p is an odd prime.

<u>Pf.</u> Since $p \mid \binom{p}{i}$, $(x+1)^p = x^p + 1$ in $\mathbb{Z}_p[x]$.

As $\mathbb{Z}_p$ is an integral domain, $\mathbb{Z}_p[x]$ is an integral domain.

So it has the cancelation property. Hence

$(x+1)^{p-1} = x^{p-1} - x^{p-2} + \cdots + (-1)^{i+1} x^{p-i} + \cdots + 1$. Compring

Lecture 17: Irreducible polynomials in F[x]

Friday, May 11, 2018 11:35 AM

coeff. of x^i we get $\binom{p-1}{i} \overset{p}{\equiv} (-1)^{p-i+1} = (-1)^i$ as $2 | p+1$.

∎

Let's go back to the study of irreducible polynomials:

<u>Lemma.</u> Suppose F is a field. Then $f(x) \in F[x]$ is irreducible if and only if $\deg f > 0$ and f cannot be written as a product of two non-constant polynomials.

<u>Pf.</u> ($\Rightarrow$) f is irreducible $\Rightarrow$ $f \neq 0$ and $f \notin U(F[x]) = U(F) = F \setminus \{0\}$.

$\Rightarrow \deg f > 0$

And if $f(x) = g(x)\, h(x)$, then either $g(x) \in U(F[x]) = F \setminus \{0\}$ or $h(x) \in U(F[x]) = F \setminus \{0\}$; and claim follows.

($\Leftarrow$) $\deg f > 0 \Rightarrow f \neq 0$ and $f \notin F \setminus \{0\} = U(F[x])$ is not a unit.

Since F is an integral domain, $F[x]$ is an integral domain.

Hence $f(x)$ is not a zero-divisor.

$f(x) = g(x)\, h(x)$ implies either $g(x) \in F$ or $h(x) \in F$. As $f \neq 0$, $g \neq 0$ and $h \neq 0$. Hence either $g \in F \setminus \{0\}$ or $h \in F \setminus \{0\}$. Since

Lecture 17: Irreducible

Friday, May 11, 2018 2:37 PM

$U(F[x]) = F \setminus \{0\}$, either $g \in U(F[x])$ or $h \in U(F[x])$

and claim follows. ■

<u>Ex.</u> $2x$ is irreducible in $\mathbb{Q}[x]$, but $2x$ is not

irreducible in $\mathbb{Z}[x]$

<u>Solution</u>... $\deg 2x \geq 1$

. $2x = g(x)\, h(x) \Rightarrow 1 = \deg g + \deg h$

$\Rightarrow$ either $\deg g = 0$ or $\deg h$

And so $2x$ is irredu. in $\mathbb{Q}[x]$.

- $2x = (2)(x)$, $2 \notin U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{\pm 1\}$ and

$x \notin U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{\pm 1\}$.

<u>Ex.</u> x^2+1 is reducible in $\mathbb{C}[x]$; but

x^2+1 is irreducible in $\mathbb{R}[x]$.

<u>Solution</u>.. $x^2+1 = (x+i)(x-i)$ and $x \pm i$ are not constant

And so x^2+1 is not irreducible in $\mathbb{C}[x]$.

- Since $\deg(x^2+1) \geq 1$ and $\mathbb{R}$ is a field, it is enough

Lecture 17: Zeros and irreducibility

Friday, May 11, 2018 2:45 PM

to show x^2+1 cannot be written as a product of two non-constant polynomials. Suppose to the contrary that $x^2+1 = g(x)\,h(x)$ and $\deg g, \deg h \geq 1$.

Then $2 = \deg g + \deg h \geq 1+1 = 2$. Since equality holds, $\deg g = \deg h = 1$. Hence g has a zero in $\mathbb{R}$. Therefore x^2+1 should have a zero in $\mathbb{R}$, which is a contradiction; because $\forall \alpha \in \mathbb{R}$, $\alpha^2+1 \geq 1$. ∎

<u>Lemma.</u> Suppose F is a field, $f(x) \in F[x]$, $\deg f \geq 2$, and f has a zero $c \in F$. Then f is reducible in $F[x]$.

<u>Pf.</u> By the factor theorem, $\exists\, q(x) \in F[x]$ s.t.

$$f(x) = (x-c)\,q(x).$$

So $\deg f = 1 + \deg q$; hence $\deg q = \deg f - 1 \geq 1$. Therefore f can be written as a product of two non-constant poly. which implies f is reducible in $F[x]$. ∎

Lecture 17: Irreducibility of degree 2 and 3

Friday, May 11, 2018 2:53 PM

In the next lecture we will show that the converse hold if $2 \leq \deg f \leq 3$.

The converse does not hold in general; for instance $(x^2+1)(x^2+1)$ is not irreducible in $\mathbb{R}[x]$, and it has no zero in $\mathbb{R}$.