Lecture 10: residue maps; study Irreducibility

Monday, August 21, 2017 3:57 PM

In the previous lecture we mentioned that $c_n: \mathbb{Z}[x] \to \mathbb{Z}_n[x]$, $c_n\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} c_n(a_i) x^i$ is a ring homomorphism. So here is an immediate consequence:

Corollary Let $g(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_0$ and $h(x) = b_s x^s + b_{s-1} x^{s-1} + \cdots + b_0$. Suppose $g, h \in \mathbb{Z}[x]$, and p is a prime which does not divide $a_r b_s$.

Then $c_p(gh) = c_p(g)\, c_p(h)$ and $\deg(c_p(g)) = r$ and $\deg(c_p(h)) = s$.

Pf. By the previous lemma, $c_p: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is a ring homomorphism. So $c_p(gh) = c_p(g)\, c_p(h)$.

Since $c_p(g) = c_p(a_r) x^r + c_p(a_{r-1}) x^{r-1} + \cdots + c_p(a_0)$ and $c_p(a_r) \neq 0$ (notice $p \nmid a_r$), we have

$$\deg c_p(g) = r.$$

Similarly, since $c_p(h) = c_p(b_s) x^s + \cdots + c_p(b_0)$ and $c_p(b_s) \neq 0$ (notice $p \nmid b_s$), we have $\deg c_p(h) = s$. ∎

Lecture 10: residue maps; study Irreducibility

Monday, August 21, 2017 4:15 PM

Corollary. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ has a zero in $\mathbb{Q}$. Then it has a zero in $\mathbb{Z}_m$ for any integer $m \geq 2$. (Here it, in fact, refers to $c_m(f)$.)

Pf. If $f(\frac{b}{c}) = 0$, $b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(b,c) = 1$, then c divides the leading coefficient, which is 1. So $c = \pm 1$; and this implies f has a zero, say d, in $\mathbb{Z}$. So $d^n + a_{n-1}d^{n-1} + \cdots + a_0 = 0$, which implies $c_m(d)^n + c_m(a_{n-1})\, c_m(d)^{n-1} + \cdots + c_m(a_0) = 0$. Hence $c_m(d)$ is a zero of $c_m(f)$. ■

Let's use the above corollary to give a quick answer to the next question.

Ex. Is $x^3 - x + 2$ irreducible in $\mathbb{Q}[x]$?

Solution. Since $\deg(x^3 - x + 2) = 3$, it is irreducible exactly when it has no zero in $\mathbb{Q}$.

If it has a zero in $\mathbb{Q}$, then using the previous corollary

Lecture 10: residue maps; Fermat's theorem

Monday, August 21, 2017 4:29 PM

x^3-x+2 has a zero in $\mathbb{Z}_3$. But by Fermat's theorem $\forall a \in \mathbb{Z}_3$, $a^3=a$; and so $a^3-a+2=2\neq 0$. Hence x^3-x+2 does not have a zero in $\mathbb{Z}_3$; so it does not have a zero in $\mathbb{Q}$, which implies it is irreducible in $\mathbb{Q}[x]$. ■

Ex. Does $x^{(5^{10})}-x+2$ have a zero in $\mathbb{Z}_5$?

Solution. By the previous lemma, for any $a\in\mathbb{Z}_5$, we have $a^{(5^{10})}-a+2=a-a+2=2\neq 0$. So $x^{(5^{10})}-x+2$ does not have a zero in $\mathbb{Z}_5$. ■

Ex. Does $x^{(5^{10})}-x+2$ have a zero in $\mathbb{Q}$?

Solution. Since the leading coefficient is 1, if $x^{(5^{10})}-x+2$ has a zero in $\mathbb{Q}$, it has a zero in $\mathbb{Z}$. So $x^{(5^{10})}-x+2$ has a zero in $\mathbb{Z}_5$, which contradicts the previous example. ■

So far we learned how to use residue maps to show certain polynomials in $\mathbb{Z}[x]$ do not have a zero in $\mathbb{Q}$.

Lecture 10: Residue maps and Irreducibility

Sunday, August 20, 2017 11:23 PM

Proposition. Let p be a prime, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x].$$

Suppose $c_p(f)$ does not have a zero in $\mathbb{Z}_p$. Then f does not have a zero in $\mathbb{Q}$.

We proved the above proposition in two steps:

Step 1. Having a zero in $\mathbb{Q}$ $\Rightarrow$ Having a zero in $\mathbb{Z}$.

Step 2. Use the residue homomorphism to get a zero in $\mathbb{Z}_p$.

Next we will prove an irreducibility criterion.

Theorem. Let p be a prime, and

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x].$$

Suppose $c_p(f)$ is irreducible in $\mathbb{Z}_p[x]$. Then f is irreducible in $\mathbb{Q}[x]$.

Similar to the proof of the proposition, we prove the contrapositive of this theorem; and it is done in two steps:

Step 1. Reducibility over $\mathbb{Q}$ implies reducibility over $\mathbb{Z}$ (an slightly stronger version.)

Step 2. Using the residue homomorphism to get reducibility over $\mathbb{Z}_p$.

Before we start the proof, let's point out a few examples:

Ex. $2x$ is irreducible in $\mathbb{Q}[x]$. In fact any polynomial of degree 1 is irreducible in $\mathbb{Q}[x]$; Otherwise $\exists f, g \in \mathbb{Q}[x]$, $\deg f, \deg \geq 1$ and $2x = f(x)g(x)$. So $\deg(2x) = 1 = \deg f + \deg g \geq 2$ which is a contradiction.

- $2x$ is reducible in $\mathbb{Z}[x]$ as $2x = (2)(x)$ and $2, x \notin \mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{\pm 1\}$.

So the big difference is that $2 \in (\mathbb{Q}[x])^\times = \mathbb{Q} \setminus \{0\}$, but it is not a unit in $\mathbb{Z}[x]$.

Ex. $2x^2 + 4$ is irreducible in $\mathbb{Q}[x]$ as it is of degree 2 and does not have a zero in $\mathbb{Q}$.

Lecture 10: Towards Gauss's lemma

Wednesday, August 23, 2017 10:23 PM

- $2x^2+4 = (2)(x^2+2)$ and $2, x^2+2 \notin (\mathbb{Z}[x])^\times = \{\pm 1\}$

  imply that $2x^2+4$ is reducible in $\mathbb{Z}[x]$.

So the first thing we have to check, when we'd like to find out if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, is to find $\gcd(a_n, \cdots, a_0)$, and see if it is 1 or not.

Definition. For $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, $(f \neq 0)$, let $c(f) = \gcd_{i=1}^{n}(a_i)$.

Ex. • $c(2x) = 2$ • $c(2x^2+4) = 2$ • $c(x^3+3x+6) = 1$.

Let's recall three related properties of g.c.d.

Recall ① Let $d = \gcd(a_0, \cdots, a_n)$. Then $\gcd(\frac{a_0}{d}, \cdots, \frac{a_n}{d})$

② If $p \mid a_0, p \mid a_1, \cdots, p \mid a_n$, then $p \mid \gcd(a_0, \cdots, a_n)$

③ For $c \in \mathbb{Z}^+$, $\gcd(ca_0, ca_1, \cdots, ca_n) = c \gcd(a_0, \cdots, a_n)$.

Let's see what each one of the above properties implies about the defined c function.

Lecture 10: Towards Gauss's lemma

Wednesday, August 23, 2017 10:39 PM

• For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \setminus \{0\}$, let $c(f) = d$.

Then $f(x) = d \underbrace{\left(\frac{a_n}{d} x^n + \cdots + \frac{a_0}{d}\right)}_{f_1(x) \in \mathbb{Z}[x]}$ and

$$c(f_1) = \gcd\left(\frac{a_n}{d}, \ldots, \frac{a_0}{d}\right) = 1.$$

Def. $f(x) \in \mathbb{Z}[x] \setminus \{0\}$ is called primitive if $c(f) = 1$.

So for $f(x) \in \mathbb{Z}[x] \setminus \{0\}$, we have $f(x) = c(f) f_1(x)$

where $f_1(x)$ is primitive.

• $c_p(f) = 0 \iff p \mid a_0, \ldots, p \mid a_n \iff p \mid \gcd(a_0, \ldots, a_n) \iff p \mid c(f)$.

So $c_p(f) = 0 \iff p \mid c(f)$.

(Here $f(x) = a_n x^n + \cdots + a_1 x + a_0$ as before.)

• For $a \in \mathbb{Z}^+$, $c(af) = \gcd(aa_0, \ldots, aa_n) = a \gcd(a_0, \ldots, a_n)$.

So $c(af) = a\, c(f)$.

Now let's see how these can help.

Lemma. Suppose $f, g \in \mathbb{Z}[x]$ are primitive polynomials.

Then fg is primitive, too.

Lecture 10: Gauss's lemma

Monday, August 21, 2017 8:24 AM

We call this the 1^{st} version of Gauss's lemma. We start its proof and finish it in the next lecture.

Pf: Suppose to the contrary that $c(fg) \neq 1$. Then there is a prime p which divides $c(fg)$. So $p \mid c(fg)$, which implies $c_p(fg) = 0$. Since $c_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ is a ring homomorphism, $c_p(f)\, c_p(g) = 0$.

Since $\mathbb{Z}_p$ is a field, $\mathbb{Z}_p[x]$ is an integral domain. Hence $c_p(f)\, c_p(g) = 0$ implies that either $c_p(f) = 0$ or $c_p(g) = 0$. Therefore either $p \mid (f)$ or $p \mid (g)$, which contradicts the assumption that f and g are primitive. ∎