Lecture 21: Mod p irreducibility criterion

Wednesday, May 23, 2018 10:52 AM

We were in the middle of proof of the following result:

Theorem. Suppose $f(x) \in \mathbb{Z}[x]$ is primitive, and p is prime. Suppose $c_p(f)$ is irreducible in $\mathbb{Z}_p[x]$ and $\deg f = \deg c_p(f)$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Pf. Suppose to the contrary that $f(x)$ is not irred. in $\mathbb{Q}[x]$. Since $c_p(f)$ is irred. in $\mathbb{Z}_p[x]$, $\deg c_p(f) \geq 1$. And so $\deg f \geq 1$. Hence the contrary assumption implies $\exists g_1, g_2 \in \mathbb{Q}[x]$ s.t. $f(x) = g_1(x) g_2(x)$, and $\deg g_i \geq 1$. Then $\exists a_i \in \mathbb{Q} \setminus \{0\}$, (1) $a_1 a_2 = 1$ (2) $\overline{g}_i(x) = a_i g_i(x)$ is primitive; and so $f(x) = \overline{g}_1(x) \overline{g}_2(x)$. Hence $c_p(f) = c_p(\overline{g}_1) c_p(\overline{g}_2)$. $(*)$

Since $\deg f = \deg c_p(f)$ and $\deg \overline{g}_i \geq \deg c_p(\overline{g}_i)$, we deduce that $\deg c_p(\overline{g}_i) = \deg \overline{g}_i \geq 1$; and so $(*)$ implies $c_p(f)$ is reducible in $\mathbb{Z}_p[x]$ which is a contradi. $\blacksquare$

Ex. (a) $x^4 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

(b) $5x^4 + 2x^3 - 2018x^2 + 103x + 109$ is irred. in $\mathbb{Q}[x]$.

Lecture 21: Irreducibility criteria

Wednesday, May 23, 2018 11:08 AM

Solution. (a)

x	x^4+x+1
0	1
1	1

it has no zero in $\mathbb{Z}_2$. So if it is reducible it should have a factor of deg 2:

$\underbrace{x^2}_{\text{has a zero}}$ ✗, $\underbrace{x^2+1}_{\text{has a zero}}$ ✗, $\underbrace{x^2+x}_{\text{has a zero}}$ ✗, $x^2+x+1 \downarrow$ let's use long division:

$$
\begin{array}{r|l}
 & x^2+x \\ \hline
x^2+x+1 & x^4+x+1 \\
 & x^4+x^3+x^2 \\ \hline
 & x^3+x^2+x+1 \\
 & x^3+x^2+x \\ \hline
 & 1
\end{array}
$$

$\to$ x^2+x+1 is not a factor of x^4+x+1.

Hence x^4+x+1 has no deg. 2 factor.

And so it is irreducible.

(b) Notice that $c_2(f) = x^4+x+1$ is irreducible in $\mathbb{Z}_2[x]$. And so by Mod p Irreducibility Criterion f is irreducible in $\mathbb{Q}[x]$. ■

The next criterion is extremely useful, and easy to use.

Eisenstein's irreducibility criterion. Suppose $f(x)=a_nx^n+\cdots+a_1x+a_0 \in \mathbb{Z}[x]$, p is prime, and

$$p \nmid a_n,\ p \mid a_{n-1},\ p \mid a_{n-2}, \ldots, p \mid a_0,\ p^2 \nmid a_0.$$

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

Lecture 21: Eisenstein's irreducibility criterion

Wednesday, May 23, 2018 11:20 AM

To prove Eisenstein's criterion, I use the following result:

<u>Theorem</u>. Suppose F is a field. Then any polynomial in $F[x]$ can be written as a product of irreducible polynomials in a unique way (up to reordering the factors.)

<u>Corollary</u>. Suppose F is a field, $g(x), h(x) \in F[x]$, $c \in F\setminus\{0\}$, and $g(x)\, h(x) = c\, x^n$. Then $g(x) = c_1 x^{n_1}$ and $h(x) = c_2 x^{n_2}$.

<u>Pf</u>. g and h can be written as prod. of irred.. Since the only irred. factor of $g(x)\,h(x)$ is x, the only irred. factor of $g(x)$ and $h(x)$ can be x; and claim follows. ■

The following lemma is a weaker result than the above Corollary; but we give an easier argument.

<u>Lemma</u>. Suppose F is a field, $g(x), h(x) \in F[x]$, $c \in F\setminus\{0\}$, and $g(x)\,h(x) = c\, x^n$, and $\deg g, \deg h \geq 1$. Then $g(0) = h(0) = 0$.

<u>Pf</u>. Suppose to the contrary that $g(0) \neq 0$. Let $g(x) = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0, b_0 \neq 0$ and $h(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_\ell x^\ell$
$c_k \neq 0$, $c_\ell \neq 0$.

Then $g(x)h(x) = (b_m x^m + \cdots + b_1 x + b_0)(c_k x^k + \cdots + c_\ell x^\ell)$

$$= b_m c_k x^{m+k} + \underbrace{\cdots}_{\substack{\text{terms of deg.} \\ \ell < \quad < m+k}} + b_0 c_\ell x^\ell$$

$$b_m c_k \neq 0, \; b_0 c_\ell \neq 0, \; \left.\begin{matrix} m > 0 \\ k \geq \ell \end{matrix}\right\} \Rightarrow m+k > \ell.$$

So $g(x)h(x)$ has at least two terms, which contradicts our assumption. ∎

Pf of Eisenstein's criterion. Let $d := \alpha(f)$. Since $p \nmid a_n$, $p \nmid d$.

Let $a_i' := \frac{a_i}{d}$. Then $p \nmid a_n'$, $p \mid a_i'$ if $i < n$, $p^2 \nmid a_0'$.

And $\overline{f}(x) = a_n' x^n + \cdots + a_1' x + a_0'$ is primitive, and $f(x) = \alpha(f)\,\overline{f}(x)$.

Suppose to the contrary that $f(x)$ is reducible in $\mathbb{Q}[x]$. Hence $\overline{f}(x)$ is reducible in $\mathbb{Q}[x]$. So $\overline{f}(x) = g_1(x) g_2(x)$ for some $g_i(x) \in \mathbb{Q}[x]$ with $\deg g_i \geq 1$. Hence $\exists\, \overline{g}_i(x) \in \mathbb{Z}[x]$ that are primitive and $\deg \overline{g}_i = \deg g_i \geq 1$, and $\overline{f}(x) = \overline{g}_1(x)\, \overline{g}_2(x)$. Hence

$$c_p(\overline{f}) = c_p(\overline{g}_1)\, c_p(\overline{g}_2) \quad \text{in } \mathbb{Z}_p[x].$$

Lecture 21: Eisenstein's criterion

Wednesday, May 23, 2018 11:37 AM

Since $p \nmid a_n$, $p \mid a_i$ for $i<n$, $c_p(\bar{f}) = c_p(a_n)\, x^n$. Since $\deg c_p(\bar{f})$ is equal to $\deg f$, we deduce $\deg c_p(\bar{g}_i) = \deg \bar{g}_i \geq 1$; and $c_p(a_n')\, x^n = c_p(\bar{g}_1)\, c_p(\bar{g}_2)$. Hence by the above lemma:

$c_p(\bar{g}_1)(0) = c_p(\bar{g}_2)(0)$; and so $p \mid \bar{g}_1(0)$ and $p \mid \bar{g}_2(0)$. Then

$p^2 \mid \bar{g}_1(0)\, \bar{g}_2(0) = \bar{f}(0) = a_0'$, which is a contradiction. ∎