Lecture 19: Fermat's little theorem and having no zeros

Monday, May 14, 2018 11:42 AM

In the previous lecture we showed:

Lemma. Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If f has a zero in $\mathbb{Q}$, then, for any $m \in \mathbb{Z}^{\geq 2}$, f has a zero in $\mathbb{Z}_m$.

Pf. Since f is monic, if b/c is a zero of f, $\gcd(b,c)=1$, and $c>0$, then $c=1$; and so $f(b)=0$. Hence $f(b) \equiv 0 \pmod{m}$; which implies f has a zero in $\mathbb{Z}_m$. ∎

Using the above lemma and Fermat's little theorem we can find out whether certain poly. (of large degree) has a rational zero or not.

Ex. $x^3 - x + 2018$ has no zero in $\mathbb{Q}$.

Solution. $x^3 - x + 2018$ modulo 3 is $x^3 - x + 2$; and by Fermat's little theorem, $\forall a \in \mathbb{Z}_3$, $a^3 - a + 2 = 2 \neq 0$; and so $x^3 - x + 2018$ has no zeros in $\mathbb{Z}_3$; therefore by the above lemma it has no zero in $\mathbb{Q}$. ∎

(Since $\deg(x^3 - x + 2018) = 3$, we can deduce that it is irred.

Lecture 19: Fermat's little theorem and having no zeros

Friday, May 18, 2018 11:01 AM

in $\mathbb{Q}[x]$.)

<u>Ex.</u> $x^{(5^{103})} - x^5 + 2018$ has no zero in $\mathbb{Q}$.

<u>Pf.</u> Suppose to the contrary that it does have a zero in $\mathbb{Q}$. Then by the previous lemma, it has a zero in $\mathbb{Z}_5$. $(*)$

By Fermat's little theorem, $\forall a \in \mathbb{Z}_5$, $a^5 = a$. And so by induction on n, one has $a^{5^n} = a$. Hence

$$a^{(5^{103})} - a^5 + 2018 = a - a + 3 = 3 \neq 0 \quad \text{in } \mathbb{Z}_5;$$

which contradicts $(*)$. ∎

<u>Ex.</u> Show that $x^{50} - x + 2017$ has no zero in $\mathbb{Z}_5$ and $\mathbb{Q}$.

<u>Pf.</u> By the previous lemma, it is enough to show this poly. has no zeros in $\mathbb{Z}_5$.

$$\forall a \in \mathbb{Z}_5, \quad a^{50} - a + 2017 = a^{(2)(5^2)} - a + 2$$

$$= (a^2)^{(5^2)} - a + 2$$

$$\xrightarrow{\text{As a conseq. of Fermat's little theorem}} = a^2 - a + 2.$$

Lecture 19: Fermat's little theorem and having no zeros

Friday, May 18, 2018 11:14 AM

a	0	1	2	3	4
a^2-a+2	2	2	4	3	4

. And so $x^{50}-x+2017$ has no zeros in $\mathbb{Z}_5$. ∎

Next we will use the residue maps to get an <u>irreducibility criterion</u>.

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 $\mathbb{Q}[x]$.

To prove this criterion we follow the same steps as for finding zeros: assuming f is reducible; we have to show $c_p(f)$ is reducible:

Step 1. Going from $\mathbb{Q}$ to $\mathbb{Z}$;

Step 2. Going from $\mathbb{Z}$ to $\mathbb{Z}_p$.

Step 1 is rather hard and it is a consequence of Gauss's lemma.

Lecture 19: The content of an integer polynomial

Friday, May 18, 2018 11:24 AM

As we have seen earlier, there is a subtle difference between irreducibility in $\mathbb{Q}[x]$ and irreducibility in $\mathbb{Z}[x]$.

<u>Ex</u>. $2x^2+4$ is irreducible in $\mathbb{Q}[x]$ as it is of deg. 2 and it has no zero in $\mathbb{Q}$. But $2x^2+4 = (2)(x^2+2)$ and $2, x^2+2 \notin U(\mathbb{Z}[x])$; and so $2x^2+4$ is reducible in $\mathbb{Z}[x]$.

So to find out if $f(x) \in \mathbb{Z}[x]$ is irreducible, the first thing that we have to do is to calculate the g.c.d. of its coeff.

<u>Def</u>. For $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \setminus \{0\}$, the content of f is $\alpha(f) := \gcd(a_0, a_1, \ldots, a_n)$.

<u>Ex</u>. $\alpha(2x) = 2$, $\alpha(2x^2+4) = 2$, $\alpha(x^3+2x+6) = 1$.

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

1. Let $d = \gcd(a_0, \ldots, a_n)$. Then $\gcd\left(\frac{a_0}{d}, \ldots, \frac{a_n}{d}\right) = 1$.
2. If $p \mid a_0, p \mid a_1, \ldots, p \mid a_n$, then $p \mid \gcd(a_0, \ldots, a_n)$.
3. For $c \in \mathbb{Z}^+$, $\gcd(c a_0, \ldots, c a_n) = c \gcd(a_0, \ldots, a_n)$.

Lecture 19: The content of an integer polynomial

Friday, May 18, 2018 11:34 AM

Here are immediate consequences of these properties:

Proposition (Basic properties of content).

① $\forall f(x) \in \mathbb{Z}[x] \setminus \{0\}$, $f(x) = \alpha(f)\, \bar{f}(x)$ for some

$\bar{f}(x) \in \mathbb{Z}[x]$ such that $\alpha(\bar{f}) = 1$.

(we say $\bar{f}$ is primitive.)

② $\forall f(x) \in \mathbb{Z}[x] \setminus \{0\}$, $\quad c_p(f) = 0 \iff p \mid \alpha(f)$.

③ $\forall f(x) \in \mathbb{Z}[x] \setminus \{0\}$, $\forall c \in \mathbb{Z}^+$, $\alpha(cf) = c\,\alpha(f)$.

Pf. ① $f(x) = a_n x^n + \cdots + a_0$. Then $\alpha(f) = \gcd(a_0, \ldots, a_n)$.

Say $d = \alpha(f)$. So $\gcd(\frac{a_0}{d}, \ldots, \frac{a_n}{d})$. Let $\bar{f}(x) = \frac{a_n}{d} x^n + \cdots + \frac{a_0}{d}$.

Hence $\alpha(\bar{f}) = 1$ and $f(x) = d \cdot \bar{f}(x) = \alpha(f)\, \bar{f}(x)$.

② $c_p(f) = 0 \iff p \mid a_0, p \mid a_1, \ldots, p \mid a_n \iff p \mid \gcd(a_0, \ldots, a_n)$

$\iff p \mid \alpha(f)$.

③ $cf(x) = c\,a_n x^n + c\,a_{n-1} x^{n-1} + \cdots + c a_0 \Rightarrow$

$\alpha(cf) = \gcd(ca_0, \ldots, ca_n) = c \gcd(a_0, \ldots, a_n) = c\,\alpha(f)$. ∎

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