Criterios de Irreducibilidad

Nos interesa poder determinar cuando un polinomio en $\mathbb{Z}[x]$ ó $\mathbb{Q}[x]$ es irreducible.

Criterio de Einsenstein: Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ y supongamos que existe un primo $p \in \mathbb{Z}$ tal que

(1) $p \nmid a_n$

(2) $p \mid a_i,\ 0 \leq i \leq n-1$

(3) $p^2 \nmid a_0$

Entonces $f(x)$ es irreducibe en $\mathbb{Q}[x]$.

Dem:

Por el lema de Gauss es suficiente probar que $f(x)$ es irreducible sobre $\mathbb{Z}$. Sup que hay una factorización $f(x) = p(x)q(x)$ con $1 \leq gr(p), gr(q) < n$. Escribimos:

$p(x)=b_0+b_1x+\cdots+b_rx^r$ y $g(x)=c_0+c_1x+\cdots+c_sx^s$, con $b_i,c_j\in\mathbb{Z}$, $0<r,s<n$ y $r+s=n$

Así $a_i=\sum_{j+k=i} b_jc_k$, en particular $a_0=b_0c_0$. Por hip $p\mid b_0c_0$, ent $p\mid b_0$ ó $p\mid c_0$. Notemos que no puede pasar que p divida a b_0 y a c_0 al mismo tiempo. Así p divide o solo a b_0 ó solo a c_0. S.p.g supongamos que $p\mid b_0$

Notemos que p no puede dividir a todos los coeficientes b_j de $p(x)$. De lo contrario dividiría a $a_n=\sum_{j+k=n} b_jc_k=b_0c_n+b_1c_{n-1}+\cdots+b_{n-1}c_1+b_nc_0$ lo cual es una contradicción. Por lo tanto p no divide a algun b_j $0\le j\le r$. Sea ℓ el menor indice tal que $p\nmid b_\ell$.

Notemos $0 \leq \underline{l \leq r < n}$.

$$a_l = \sum_{j+k=l} b_j c_k = (b_0 c_l + b_1 c_{l-1} + \cdots + b_{l-1} c_1) + b_l c_0$$

Tenemos que $p \mid (b_0 c_l + \cdots + b_{l-1} c_1)$ y además por hip. $p \mid a_l$. Esto implica que $p \mid b_l c_0$

Pero $p \nmid c_0$ así que $p \mid b_l$!

Por lo tanto $f(x)$ es irreducible en $\mathbb{Z}[x]$

Lema: Un polinomio $f(x) \in \mathbb{Z}[x]$ es irreducible si y solo si el polinomio $f(x+1) \in \mathbb{Z}[x]$ también lo es.

Dem:

Dado $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, $f(x+1) = a_0 + a_1(x+1) + \cdots + a_m(x+1)^m$. Los coeficientes de $f(x+1)$ son sumas y productos de los coeficientes $a_i \in \mathbb{Z}$. Por lo tanto $f(x+1) \in \mathbb{Z}[x]$. Además $f(x) = p(x) g(x)$ si y solo si

$$f(x+1) = p(x+1) g(x+1)$$

Ejemplo: Veamos que el polinomio $\varphi(x)=1+x+\cdots+x^{p-1}$ con $p\in\mathbb{Z}$ primo es irreducible. Al polinomio $\varphi(x)$ se le llama polinomio ciclotómico.

Notemos que así como está el polinomio $\varphi(x)$ no podemos aplicar el criterio de Einsenstein ya que $a_0=1$. Por el lema anterior $\varphi(x)$ es irreducible si y solo si $\varphi(x+1)$ lo es.

Consideremos $\varphi(x+1)=1+(x+1)+\cdots+(x+1)^{p-1}$. Notemos que el termino constante es $1+\cdots+1=p$, el grado del polinomio es $p-1$ y el termino de grado es 1.

Note que $\varphi(x)=\dfrac{x^p-1}{x-1}$

y así $\varphi(x+1)=\dfrac{(1+x)^p-1}{(1+x)-1}=\dfrac{1}{x}\sum_{i=1}^{p}\binom{p}{i}x^i=\dfrac{1}{x}\left(px+\sum_{i=2}^{p-1}\binom{p}{i}x^i+x^p\right)$

Entonces

$$\varphi(x+1) = p + \sum_{i=2}^{p-1} \binom{p}{i} x^{i-1} + x^{p-1}$$

$$\varphi(x+1) = p + \binom{p}{2} x + \cdots + \binom{p}{p-1} x^{p-2} + x^{p-1}$$

$$\binom{p}{i+1} = \frac{p!}{(p-i-1)!\,(i+1)!} = \frac{p\cdot(p-1)\cdots 2\cdot 1}{(p-i-1)!\,(i+1)!}$$

$$\downarrow$$

$$= \frac{p\cdot(p-1)\cdots(p-i)}{(i+1)!} \in \mathbb{Z}$$

Tenemos que p divide al numerador

pero p no divide al denominador porque $i+1<p$. Esto implica que $p \mid \binom{p}{i-1}$.

Entonces si $\varphi(x+1) = a_0 + a_1 x + \dots + a_{p-1} x^{p-1}$ con $a_0 = p$, $a_i = \binom{p}{i-1}$ $1 \leq i \leq p-1$ y $a_{p-1} = 1$ entonces $p \mid a_0$ y $p^2 \nmid a_0$, $p \mid a_i$ $0 \leq i \leq p-1$ y $p \nmid a_{p-1}$. Por el criterio de Einsenstein $\varphi(x+1)$ es irreducible. y así $\varphi(x)$ también lo es.

Ejemplo: Si $p \in \mathbb{Z}$ es un primo y $n > 1$ el polinomio $f(x) = x^n - p \in \mathbb{Z}[x]$ es irreducible, por el criterio de Einsenstein. $a_n = 1$, $a_i = 0$ $1 \leq i \leq n-1$ y $a_0 = p$. En particular $f(x)$ no tiene un factor linial de la forma $x - a$ con $a \in \mathbb{Z}$. Es decir no hay $a \in \mathbb{Z}$ tal que $a^n = p$. $\therefore$ $a = \sqrt[n]{p} \notin \mathbb{Q}$

Existen otros criterios de irreducibilidad. Consideremos un entero q y el morfismo de anillos canónico $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$. Entonces, este morfismo se extiende a un morfismo
$$n \mapsto n + q\mathbb{Z}$$
de anillos $\mathbb{Z}[x] \xrightarrow{\overline{(\ )}} \mathbb{Z}/q\mathbb{Z}[x]$.

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \longmapsto \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$$

donde $\bar{a}_i = a_i + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$. Este morfismo es un morfismo de anillos. Si $f(x)$ y $g(x) \in \mathbb{Z}[x]$ $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ y $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ ent $f(x)g(x) = \sum c_k x$ $f(x) + g(x) = \sum d_\ell x^\ell$ donde $d_\ell = a_\ell + b_\ell$ y $c_k = \sum_{i+j=\ell} a_i b_j$. $\overline{(f(x)+g(x))} = \sum \overline{d_\ell} x^\ell$

$= \overline{f(x)} + \overline{g(x)}$ ya que $\overline{d_\ell} = \overline{a_\ell} + \overline{b_\ell}$

$$\overline{c_k} = \overline{\sum_{i+j=k} a_i b_j} = \sum_{i+j=k} \overline{a_i}\,\overline{b_j}$$

$$\overline{\left(f(x)g(x)\right)} = \overline{f(x)}\,\overline{g(x)}$$

$$\therefore\ \overline{(\ \ )} : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/q\mathbb{Z}[x]$$

es un morfismo de anillos $\forall q \in \mathbb{Z}$

Prop. Sea $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$. Si existe un entero $q>1$ tal que $q\nmid a_n$ y tal que $\bar{f}(x)\in\mathbb{Z}/q\mathbb{Z}[x]$ es irreducible, entonces $f(x)$ es irreducible en $\mathbb{Z}[x]$.

Dem:

Si $f(x)=g(x)h(x)$ con $gr(g), gr(h)\geq 1$ entonces para todo entero $m>1$, $\bar{f}(x)=\bar{g}(x)\bar{h}(x)$ en $\mathbb{Z}/m\mathbb{Z}[x]$. En particular, si $q\nmid a_n$ ent $\bar{f}(x)=\bar{g}(x)\bar{h}(x)\in\mathbb{Z}/q\mathbb{Z}[x]$ con $gr(\bar{g})\geq 1$ y $gr(\bar{h})\geq 1$ ya que si

$$g(x)=b_0+b_1x+\cdots+b_mx^m$$
$$h(x)=c_0+c_1x+\cdots+c_rx^r$$

Se tiene $a_n = b_m c_r$. Como $q \nmid a_n$,
$q \nmid b_m$ y $q \nmid c_r$ i.e $\underline{b_m} \not\equiv 0 \mod q$
ni $c_r \not\equiv 0 \mod q$. Por lo tanto
el termino de grado de $\overline{g(x)}$ es
$\overline{b_m}$ y el de $\overline{h(x)} = \overline{c_r}$. Por lo tanto
$f(x)$ no es irreducible en $\mathbb{Z}/q\mathbb{Z}[x]$.