定义1. 一个非零整系数多项式$g(x)$若各项系数互质,则称$g(x)$为本原多项式

$Q[x]$上$f(x)$不可约 $\Longleftrightarrow$ 与其相伴本原多项式不可约

性质1. 设$f(x), g(x)$为本原多项式 $f(x) \sim g(x) \Longleftrightarrow f(x) = \pm g(x)$

证: 设 $f(x) = \frac{q}{p} g(x)$, $((p,q)=1)$

则 $p\sum_{i=1}^{n} a_i x^i = q\sum_{i=1}^{n} b_i x^i$ $\qquad \therefore pa_i = qb_i$

$\therefore p \mid b_i \ (i=1,\cdots,n)$ $\qquad \therefore p = \pm 1$

同理, $q=\pm 1$ $\qquad \therefore f(x) = \pm g(x)$

性质2. (高斯引理)每个本原多项式乘积为本原多项式

证: 设$f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{i=0}^{m} b_i x^i$为本原多项式

$h(x) = f(x)g(x) = \sum_{s=0}^{n+m} \left(\sum_{i+j=s} a_i b_j\right) x^s$

若$h(x)$不是本原多项式,则 $\exists$素数p. s.t. $p \mid c_s$ $s=0,\cdots,m+n$

$\because f(x)$本原, $\therefore \exists k$, $0\le k\le n$, s.t. $p\mid a_0,\cdots, p\mid a_{k-1}, p\nmid a_k$.

同理 $\exists l$, $0\le l\le m$, s.t. $p\mid b_0,\cdots, p\mid b_{l-1}, p\nmid b_l$

$\because c_{k+l} = a_0 b_{k+l} + \cdots + a_{k-1}b_{l+1} + a_k b_l + a_{k+1}b_{l-1} + \cdots + a_{k+l}b_0$

$p\mid c_{k+l}$ $\quad \therefore p \mid a_k b_l$ $\quad \therefore p\mid a_k$ 或 $p\mid b_l$, 与假设矛盾

命题1. 次数大于0的本原多项式$g(x)$在Q上可约

$\Leftrightarrow g(x)$能分解为两个次数低于$g(x)$的本原多项式乘积

证: $\Rightarrow$ $g(x) = g_1(x)\, g_2(x)$, $\deg g_i(x) < \deg g(x)$, $i=1,2$

$g(x) = r_1 h_1(x) \cdot r_2 h_2(x)$, ($h_i(x)$为本原)

$= (r_1 r_2)(h_1(x) h_2(x))$

$\Downarrow$

$r_1 r_2 = \pm 1 \Rightarrow g(x) = \pm h_1(x)\cdot h_2(x)$ $\quad \deg h_i(x) < \deg g(x)$.

推论1. 次数大于0的本原多项式可分解为有限多个不可约本原多项式乘积.

推论2. 次数大于0整系数多项式$f(x)$在Q上可约
$\Longleftrightarrow$ 能分解为两个次数低于$f(x)$的整系数多项式乘积

定理1. 设$f(x)=\sum_{i=0}^{n}a_ix^i$为一次数为$n$整系数多项式. 若有一根$\frac{q}{p}$, $(p,q)=1$,
则 $p\mid a_n$, $q\mid a_0$.

证: $x-\frac{q}{p}\mid f(x) \Rightarrow px-q\mid f(x)$ $\quad f(x)=(px-q)g(x)$ $\quad g=\sum_{i=1}^{n-1}b_ix^i$

$\therefore a_n=pb_{n-1} \Rightarrow p\mid a_n$

$a_0=-qb_0 \Rightarrow q\mid a_n$

定理2. (Eisenstein判别法) 设$f(x)=\sum_{i=0}^{n}a_ix^i$, 为一次数为$n>0$整系数多项式.
若有一素数p满足:
1°. $p\nmid a_n$, $p\mid a_{n-1}$, $\cdots$, $p\mid a_0$
2°. $p^2\nmid a_0$
则$f(x)$在Q上不可约

证: 设$f(x)$在Q上可约, 则由推论2得
$f(x)=(b_mx^m+\cdots+b_0)(c_lx^l+\cdots+c_0)$ $\quad m<n, l<n$

$a_n=b_mc_l$, $\quad a_0=b_0c_0$
$p\nmid a_n \Downarrow$ $\quad p\mid a_0 \Downarrow$
$p\nmid b_m$, $p\nmid c_l$ $\quad p\mid b_0c_0 \Rightarrow p\mid b_0$或$p\mid c_0$ (设$p\mid b_0$)

$\exists k\ (0<k\le m<n)$, s.t. $p\mid b_0,\cdots,p\mid b_{k-1}$, $p\nmid b_k$

$a_k=b_0c_k+b_1c_{k-1}+\cdots+b_{k-1}c_1+b_kc_0$

$\because p\mid a_k$ $\quad\therefore p\mid b_kc_0$ $\quad\therefore p\mid c_0$ $\quad\therefore p^2\mid b_0c_0=a_0$, 矛盾

$\therefore f(x)$在Q上不可约

定理3、$Q[x]$中，存在任意次数不可约多项式

次数大于0的整系数多项式$f(x)$在Q上不可约

$\Leftrightarrow$ $f(x\pm1)$在Q上不可约

练练