定理 0.1 (Eisenstein's criterion)**.**

$$f(x) = \sum_{0 \le k \le n} a_k x^k \in \mathbb{Z}[x]$$

について、ある素数 p が存在して、整数 $a_0, a_1, \ldots, a_n$ が

1. $i \neq n$ の場合は a_i は p で割り切れる
2. a_n は p で割り切れない
3. a_0 は p^2 で割り切れない

を満たすならば、$f(x)$ は有理数体上既約である。

(証明). 多項式 g, h を $f(x) = g(x)h(x)$ を満たすものとおき、多項式 f, g, h の各係数を

$$g(x) = \sum_{0 \le i \le n} g_i x^i, h(x) = \sum_{0 \le j \le n} h_j x^j$$

と置く。

この時、単純な計算で

$$a_k = \sum_{i+j=k} g_i h_j$$

が成り立つと分かる。記法を簡単にするため、$P = (p) \subset \mathbb{Z}$ とおく。これが素イデアルであることを何度も使う。

a_0 を考える。

$$a_0 = g_0 h_0$$

前提条件 1. より a_0 は p の倍数である。さらに前提条件 3. から、a_0 には素因数として p がただ一つ含まれる。その p は g_0 か h_0 のどちらか一方に含まれている。そこで仮定 (*) として $g_0 \in P, h_0 \notin P$ とする。この議論全体で g と h を単純に入れ替えても議論は破綻しない。

帰納法で $g_0, g_1, \ldots, g_{n-1} \in P$ を示す。まず、$k = 1$ で示す。

$$a_1 = g_0 h_1 + g_1 h_0 \in P$$

P はイデアルだから $g_0 h_1 \in P, h_0 \notin P$。特に P は素イデアルだから $g_1 \in P$。

次に、$0 \le N + 1 < n$ を満たす自然数 N について $g_0, g_1, \ldots, g_N \in P$ が成り立つとする。

$$a_{N+1} = g_{N+1} h_0 + g_N h_1 + \sum_{1 \le j \le N+1} g_{N+1-j} h_j$$

そして前提条件 1. より $a_{N+1} \in P$ が成り立つ。帰納法の仮定より、$g_N h_1, \sum_{2 \le j \le N+1} g_{N+1-j} h_j \in P$。仮定 (*) より $h_0 \notin P$ だから $g_{N+1} \in P$。

さて、最後に a_n を考える。

$$a_n = g_n h_0 + \sum_{1 \le j \le n} g_{n-j} h_j$$

前提条件 2. より $a_n \notin P$。すでに示したとおり、$g_0, g_1, \ldots, g_{n-1} \in P$ が成り立つ。したがって、仮定 (*) と合わせて $g_n \notin P$ が成立する。

$0 \in P$ だから、このことから $g_n \neq 0$。よって $\deg g = n, \deg h = n - n = 0$。これで f の既約性が示された。 ∎

これと以下の命題を組み合わせると、多くの多項式の既約性が示せる。

命題 0.2. 多項式 $f(x) \in \mathbb{Z}[x]$ について、「任意の定数 $a \in \mathbb{Z}$ について $f(x+a)$ が既約」と「$f(x)$ も既約」は同値。

(証明). $f(x)$ が既約だとする。定数 a に対し、1 次以上の多項式 g, h（これは a によって変化する）が存在して $f(x+a) = g(x)h(x)$ が成り立つ ($f(x+a)$ が既約でない) ならば、$f(x) = g(x-a)h(x-a)$ となり、$g(x-a), h(x-a)$ は一次以上の多項式。これは前提に矛盾。よって $f(x+a)$ も既約。

$f(x)$ が既約でないとする。すると 1 次以上の多項式 g, h が存在して $f(x) = g(x)h(x)$ が成り立つが、$f(x+a) = g(x+a)h(x+a)$ となり、$g(x+a), h(x+a)$ は一次以上の多項式。よって $f(x+a)$ も既約でない。 ∎