

(1)

$$f(\alpha) = \alpha^n + pa_{n-1}\alpha^{n-1} + \cdots + pa_1\alpha + \cdots + pa_0 = 0 \text{ より } -\alpha^n = p(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + \cdots + a_0) \text{ ——①}$$

①の右辺は p で割り切れるから、①の左辺 $-\alpha^n$ も p で割り切れる。

すなわち、 α^n が p で割り切れ、 α が p で割り切れる。(証明終)

(2)

a_0 が p で割り切れず、なおかつ $f(x) = 0$ が整数解 α を持つと仮定する。

$$\text{このとき、} f(\alpha) = 0 \text{ より } pa_0 = -(\alpha^n + pa_{n-1}\alpha^{n-1} + \cdots + pa_1\alpha)$$

$$(1) \text{ より、} \alpha \text{ は } p \text{ で割り切れるから、両辺を } p \text{ で割ると } a_0 = -\left(\frac{\alpha}{p} \cdot \alpha^{n-1} + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha\right) \text{ ——②}$$

$n \geq 2$ および α は p で割り切れることから、②の右辺は p で割り切れる。

ところが、 a_0 は p で割り切れないから、矛盾する。

したがって仮定は誤りであり、 a_0 が p で割り切れなければ、 $f(x) = 0$ は整数解を持たない。(証明終)