高次合同式

文字は全て整数とする．p は素数とする．

定義 1 合同式

$$a_0x^n + a_1x^{n-2} + a_2x^{n-2} + \cdots + a_n = 0$$

において，$a_0 \not\equiv 0 \pmod{m}$ ならばこの合同式を n 次と呼ぶ．

定理 1 n 次合同式

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

は n 個より多くの解を有することはない．

［証明］(1) が解をもつとき，その解の一つを

$$x \equiv a \pmod{p}$$

とすると，

$$f(a) \equiv 0 \pmod{p}$$

$f(x)$ を $(x-a)$ で割ると，

$$f(x) = (x-a)f_1(x) + f(a)$$

よって (1) は

$$(x-a)f_1(x) + f(a) \equiv 0 \pmod{p}$$

と同値である．$f(a) \equiv 0 \pmod{p}$ であるので

$$(x-a)f_1(x) \equiv 0 \pmod{p}$$

p は素数なので，この合同式の解は $x - a \equiv 0$ または $f_1(x) \equiv 0 \pmod{p}$ の解である．$x \not\equiv a$ の解は

$$f_1(x) \equiv 0 \pmod{p}$$

の解である．この合同式は $n-1$ 次である．このように，次々に次数を下げていくとついには一次合同式となり，その解は 1 個である．よって，定理は証明された．［証明おわり］

［注］合成数を法とする場合はこの限りではない．例えば

$$x^2 \equiv 1 \pmod{12}$$

の解は

$$x \equiv 1, 5, 7, 11 \pmod{12}$$

の 4 個である．あるいは

$$x^2 \equiv 2 \pmod{3}$$

の解はない．

定理 2（**テイラーの定理**）関数 $f(x)$ はある区間において $n+1$ 回微分可能であるとする．この区間の 2 点 a, b に対して

$$f(b) = f(a) + f'(a)(b-a) + \frac{f''(a)}{2!}(b-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(b-a)^n + R_{n+1}$$

と表せば，$R_{n+1} = \dfrac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}$ となるような c が a と b の間にある．

ここで扱う $f(x)$ は整数係数の整式であり，有限回の微分においてその導関数は 0 となる．つまりこの級数展開は有限項数であり，テイラーの定理の後半はとくに必要ない．また各項は必ず整数となる．

定理 3

$$f(x) \equiv 0 \pmod{p} \tag{2}$$

の解の一つを x_0 とする．

$$f'(x_0) \not\equiv 0 \pmod{p}$$

のとき (1) の解のうち

$$x = x_0 + py \tag{3}$$

のなかで

$$f(x) = 0 \pmod{p^2} \tag{4}$$

を満たすものは唯一（p^2 を法として）である．

[証明]　p^2 で割り切れる数は必ず p でも割り切れる．つまり (4) の解は当然 (2) も満たすので，(2) の解のうち，どのような場合に (4) も満たすのかを調べきることにより，(4) の解の全体が判明するわけである．(3) を (2) に代入しテイラー展開を行うと，

$$\begin{aligned} f(x) &= f(x_0 + py) \\ &= f(x_0) + f'(x_0)py + \frac{f''(x_0)}{2!}p^2y^2 + \cdots \equiv 0 \pmod{p^2} \end{aligned}$$

前述のように各項は整数であるので，第三項以降は 0 である．つまり

$$f(x_0) + f'(x_0)py \equiv 0 \pmod{p^2}$$

また $f(x_0) \equiv 0 \pmod{p}$ より

$$\frac{f(x_0)}{p} + f'(x_0)y \equiv 0 \pmod{p} \tag{5}$$

この一次合同式は解を一つもち，その解を

$$y \equiv y_0 \pmod{p}$$

とする．つまり

$$y = y_0 + pk$$

であるので，これを (2) に代入すると，

$$x = x_0 + py_0 + p^2k$$

となるので

$$x \equiv x_0 + py_0 \pmod{p^2}$$

がその唯一の解である． [証明おわり]

定理 4

$$f(x) \equiv 0 \pmod{p}$$

の解の一つを x_0 とする．

$$f'(x_0) \equiv 0, \frac{f(x_0)}{p} \not\equiv 0 \pmod{p}$$

のとき (1) の解のうち

$$x = x_0 + py$$

のなかで

$$f(x) = 0 \pmod{p^2}$$

を満たすものはない．

[証明]　途中まで前定理の証明と同じである．仮定の条件において (4) を満たす y はない．[証明おわり]

定理 5

$$f(x) \equiv 0 \pmod{p}$$

の解の一つを x_0 とする．

$$f'(x_0) \equiv 0, \frac{f(x_0)}{p} \equiv 0 \pmod{p}$$

のとき (1) の解のうち

$$x = x_0 + py$$

のなかで

$$f(x) = 0 \pmod{p^2}$$

を満たす解は p 個ある．

[証明]　やはり途中まで前々定理の証明と同じである．仮定の条件において常に (4) を満たすので y は全ての整数値をとりうる．つまり

$$x = x_0, x_0 + p, x_0 + 2p, \cdots, x_0 + (p-1)p \pmod{p^2}$$

の p 個の解をもつ． [証明おわり]

同様の議論により，

$$f(x) \equiv 0 \pmod{p^{n+1}}$$

の解があればそれは

$$f(x) \equiv 0 \pmod{p^n}$$

の解から派生する．それはつきつめると

$$f(x) \equiv 0 \pmod{p}$$

から派生したものである．

定理 6

$$m = p^a q^b \cdots$$

とするとき，合同式

$$f(x) \equiv 0 \pmod{m}$$

の解は，

$$\begin{aligned} f(x) &\equiv 0 \pmod{p^a} \\ f(x) &\equiv 0 \pmod{q^b} \\ &\cdots\cdots\cdots \end{aligned}$$

の解の個数 $\nu, \nu', \cdots$ に対してその積である $\nu\nu' \cdots$ 個ある．それぞれの解の求め方は中国剰余定理あるいはガウスの方法による．

［証明略］

参考文献

[1] 熊原啓作『多変数の微積分』（放送大学，2003 年）

[2] 高木貞治『初等整数論講義第 2 版」（共立出版社，1997 年）

[3] 「ウィキペディア（Wikipedia）」<http://ja.wikipedia.org/wiki/>

[4] 「エンカルタ百科事典ダイジェスト」<http://jp.encarta.msn.com/>