

1187. 整数論ニ於ケル一定理ノ初等的
證明ニツイテ

東屋 五郎(名大)

a ヲ任意ノ有理整数(以下整数トイヘバ有理整数ノコト), p ヲ a ト素ナル素数トスレバ $a^m \equiv 1 \pmod{p}$ ナル自然数 m ガ存在シマスガ、 m ノ中最小ナルモノヲ a ノ \pmod{p} ニ関スル指数ト呼ビマス。ソレヲ n トスレバ $n|m$ デアリマス。特ニ $a^{p-1} \equiv 1 \pmod{p}$ デアル故ニ $n|p-1$ 従ツテ $(n, p) = 1$ デアリマス。逆ニ任意ニ整数 a ト自然数 n ヲ与ヘタトキニ a ト素ナル素数 p ノ中 $a \pmod{p}$ ニ関スル指数ガ丁度 n ニ等シクナルヤウナ p ガ存在スルカト云フニ $|a| > 1$, $n > 2$ ナラバ $a = 2, n = 6; a = -2, n = 3$ ナル場合ヲ除イテ、カ、ル p ガ常ニ存在スルトイフ定理ガ成立シマス。

コノ定理ハ実ハ C. Chevalley ガ東大ノ
*Sur la théorie du corps de classes dans les corps finis et. les corps locaux (1933)*ノ
432頁ニ於テ相互律ノ證明ノタメノ補助定理トシテ
證明シテ居リマスガ(尤モソレ大ノ為ナラ p ノ代リ
ニ p ノ巾ヲ取ツテ十分デアリ、従ツテソノ場合ノ証明ハ非常ニ簡單ニナルコトヲ彌永先生ガ指摘サレマ

シタガ、高木先生、代数的整数論 243 頁ノ定理ニ
 参照)、ソノ証明ハ透明デハアリマスガ、再分体ノ素
 「イデヤル」ノ問題ニ迄持ツテ行ツテ居ルノデ、初等的
 トハ申サレマセン。コ、ニソノ初等的ナ証明が得ラ
 レマシタノデソレヲ述ベテミマス。Chevalleyノ証
 明ト比ベテミマシタ所、証明ノ本質ハ同様デアリマ
 ス。

n ヲ自然数、 ζ ヲ一般ニ 1ノ原始 n 乗根ヲ表ハス
 トキ同前 n 分多項式

$$(1) \quad \Phi_n(x) = \prod_{\zeta} (x - \zeta) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

ハ $\varphi(n)$ 次ノ整係数(既約)多項式デアリマス。

$n > 2$ ノトキハ ζ ハ実ナラザル複素数ナル故 ζ ノ
 共軛複素数 ζ^{-1} モ原如 n 乗根デ、 ζ^{-1} キ ζ ダカラスヲ
 実数ト看ヘレバ $\Phi_n(x) = \prod_{\zeta} (x - \zeta) = \prod_{\zeta} |x - \zeta| = |\Phi_n(x)|$ トナ
 リマスガ、 $\Phi_n(x)$ ハ $x \geq 1$ ニ於テ單調増加、 $x \leq -1$ ニ
 於テ單調減少函数ヲ表ハシマス。

何トナレバ $1 \leq x < y$ 又ハ $x < y \leq -1$ ナレバ $|\zeta|$
 $= 1$ ナルコトカラ $|x - \zeta| < |y - \zeta|$ 、従ツテ

$$\Phi_n(x) = \prod_{\zeta} |x - \zeta| < \prod_{\zeta} |y - \zeta| = \Phi_n(y) \text{ナル故デアリマス。}$$

補題 1. n ガ 2ヨリ大ナル自然数、 x ガ $|x| \geq 2$ ナ
 ル実数ナレバ、 n ノ任意ノ素因数 p ニ対シテ、

$\Phi_n(x) > p$ デアル。但シ $x=2$, $n=6$ ナル場合及ビ
 $x=-2$, $n=3$ ナル場合ヲ除ク。

証明： 上述ノ $\Phi_n(x)$ ノ 單調性 = ヨリ、 $x = \pm 2$ ナル
 場合ヲヤレバ十分デアルガ、

1) n ガ 平方因子ヲ有シナイ場合

イ) $n = p$ ガ 奇素数ノトキ、 $\Phi_n(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \dots$
 $+ x + 1$ トナル故 $\Phi_n(2) > \Phi_n(1) = p$, 又 $\Phi_n(-2) =$
 $\frac{2^p + 1}{3}$ ハ $p > 3$ ナラバ $> p$ デアルガ $p = 3$ ノト
 キダケハ $\Phi_3(-2) = 3$. シカシ、 $x < -2$ ナラバ
 $\Phi_3(x) > 3$ デアル。

ロ) n ガ 素数ナラザル奇数ノトキ、 $n = p_1 p_2 \dots p_s$,
 $p_1 > p_2 > \dots > p_s (> 2)$, ($s \geq 2$)ヲ n ノ 素因子分
 解トシ、 $n' = p_1 \dots p_{s-1}$ トオケバ (1) カラ容
 易 =

$$\Phi_n(x) = \frac{\Phi_{n'}(x^{p_s})}{\Phi_{n'}(x)} \quad \text{從ツテ} \quad \Phi_n(\pm 2) = \frac{\Phi_{n'}(\pm 2^{p_s})}{\Phi_{n'}(\pm 2)}$$

ヲ得ルガ ζ' ヲ一般 = 原始 n' 乗根トセバ

$$\Phi_{n'}(\pm 2^{p_s}) = \prod_{\zeta'} |\pm 2^{p_s} - \zeta'| \geq (2^{p_s} - 1)^{\varphi(n')} \geq 6^{\varphi(n')}$$

$$\Phi_{n'}(\pm 2) = \prod_{\zeta'} |\pm 2 - \zeta'| \leq 3^{\varphi(n')} \quad \text{トナル故} =$$

$$\Phi_n(\pm 2) \geq \frac{6^{\varphi(n')}}{3^{\varphi(n')}} = 2^{\varphi(n')} > p_1$$

ハ) n ガ 偶数ノトキ、 $n = 2n'$ トオケバ、 n ガ 平
 方因子ヲ有シナイ假定カラ n' ハ 1), ロ) ノ場
 合ノ n トナル故 $n' = 3$, $-x = -2$ 從ツテ $n = 6$,

$x=2$ の場合ヲ除イテ n の任意ノ素因子 $p =$
対シ

$$\Phi_n(x) = \Phi_{n'}(-x) > p$$

が成立ツ。

2) n が平方因子ヲ有スル場合

1) n が 2 の巾即チ $n = 2^e$ ($e \geq 2$) ナル形ノト

キハ $\Phi_n(x) = x^{2^{e-1}} + 1$ ナル故, $|x| > 1$ ナラ

$$\Phi_n(x) > \Phi_n(\pm 1) = 2$$

2) n が 2 以外ノ素因数ヲ含ムトキ, n ノ素因

子分解ヲ $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ ($s \geq 1$)

トスレバ $p_1^{e_1-1} p_2^{e_2-1} \dots p_s^{e_s-1} > 1$. シカル = (1)

カラ容易ニ $\Phi_n(x) = \Phi_{p_1 \dots p_s}(x^{p_1^{e_1-1} \dots p_s^{e_s-1}})$

ナル恒等式ヲ得ル故上記 1) ノ場合ニヨリ

$$\Phi_n(x) > \Phi_{p_1 \dots p_s}(x) \geq p_i \quad (|x| \geq 2)$$

(証明終)

補題 2. a が整数, p が素数デ, 且ツ $p^\nu \parallel a-1$, ($\nu \geq 1$)

トスレバ $p=2, \nu=1$ ナル場合ヲ除イテ, $p^{\nu+1} \parallel a^n - 1$

デアル, 又 n が p ト素ナル自然数ナラバ $p^\nu \parallel a^n - 1$

デアル。 ($p^\nu \parallel a-1$ 小ハ $a-1$ ノ p -成分ガ p^ν ナルコト)

証明: $a = 1 + b$ トオケバ $p^\nu \parallel b$ デアル。シカラバ

$$a^p - 1 = pb + \binom{p}{2} b^2 + \dots + \binom{p}{p-1} b^{p-1} + b^p$$

トナルガ右辺ノ最初ノ項ハ $p^{\nu+1} \parallel pb$, 最後ノ項ハ

$p^{\nu} \parallel b^p$ デアリ、ソノ他ノ項ハ明ラカ $= p^{\nu+2}$ デ割り切レル。而シテ $p=2, \nu=1$, ノトキヲ除イテハ、
 $\nu+1 < p\nu$ トナル故 $= p^{\nu+1} \parallel a^p - 1$ ヲ得ル。

次 $= (n, p) = 1$ ノトキ

$$a^n - 1 = nb + \binom{n}{2} b^2 + \dots + \binom{n}{n-1} b^{n-1} + b^n$$

デアルガ：右辺ノ最初ノ項ハ $p^{\nu} \parallel nb$ デ、ソノ他ノ項ハ明ラカ $= p^{\nu+1}$ デ割り切レル故 $p^{\nu} \parallel a^n - 1$ デアル。

補遺3. 整数 a が与ヘラレタトキ素数 p が a と互ヒ素デ且ツ $a \pmod p$ = 關スル指数が n = 等シイタメノ必要且ツ十分ナル條件ハ、

$$p \mid \Phi_n(a) \text{ 且ツ } p \nmid n$$

ナルコトデアル。

証明： 先ヅ必要條件： $p \mid a^n - 1 = \prod_{d|n} \Phi_d(a)$ ナル故

$p \mid \Phi_d(a)$, $d|n$ トスレバ、 $a^d \equiv 1 \pmod p$ デアルカラ $d \equiv n$, 従ツテ $d = n$ 即チ $p \mid \Phi_n(a)$, 勿論 $p \nmid n$ デアル。

次 = 十分條件： $p \mid \Phi_n(a)$, $p \nmid n$ トセバ $a^n \equiv 1 \pmod p$ デアルガ、 $a \pmod p$ = 關スル指数ヲ f トオケバ $f|n$ デアル。

今 $p^{\nu} \parallel a^f - 1$ ($\nu \geq 1$) トオケバ $(\frac{n}{f}, p) = 1$ ナル故上ノ補題スカラ $p^{\nu} \parallel a^n - 1$ 従ツテ若シ $n > f$ ナ

ラバ $p^{\nu+1} \mid \Phi_n(a) \cdot (a^f - 1) \mid a^n - 1$ トナリ矛盾スル故
 $n = f$ デアル。

補題4. a ハ整数、 p ハ互素ナル素数デ且ツ $a \not\equiv 1 \pmod p$
 = 商スル指数ガ f ナルトキ $p \mid \Phi_n(a)$ オルタメノ必要且
 ツ十分ナル條件ハ、 n ガ $n = p^e f$ ($e \geq 0$) ナル形ニ表
 ハサレルコトデアル。

而シテソノ場合、 $n > f$ 、 $n \neq 2$ ナラバ $p \parallel \Phi_n(a)$
 デアル。

証明: 先ツ必要條件: $p^e \parallel n$ トセバ $p \nmid f \mid n$ ナル故、
 $p^e f \mid n$ デアルカラ、 $n = p^e f n'$ トオケバ $p \nmid n'$ 。

従ツテ、 $p^\nu \parallel a^{p^e f} - 1$ トオケバ、補題2ヨリ $p^\nu \parallel a^n - 1$ デアル故、若シ $n > p^e f$ ナラ $p^{\nu+1} \mid \Phi_n(a) \cdot (a^{p^e f} - 1) \mid a^n - 1$ トナリ矛盾スル。従ツテ $n = p^e f$ 逆ニ十分條件:
 $n = p^e f$ ($e \geq 0$) ナル形デアルトスル。 $e = 0$ 即チ $n = f$ ナラバ、補題3カラ $p \mid \Phi_n(a)$ ヲ得ル。ソユデ $e \geq 1$ 即チ $n > f$ ノ場合ヲ考へル。

$$p^\nu \parallel a^{p^{e-1} f} - 1 = \prod_{d \mid f} \Phi_d(a), \quad (\nu \geq 1)$$

トオケバ、補題2ニヨレバ $p = 2, \nu = 1$ ナル場合ヲ除イテ

$$p^{\nu+1} \parallel a^{p^e f} - 1 = \prod_{d \mid p^e f} \Phi_d(a)$$

得ル故、ユノニ式ヲ比較シテ、 $p \parallel \Phi_d(a), d \mid p^e f$,

$d \times p^e = f + \nu d$ が唯一つ存在シテレバナラナイコトが分カル。コ
ノ d ハ $d = p^e d'$ $d' \mid f$ ナル形ニ表ハサレルガ、
 $a^d \equiv 1 \pmod{p}$ ナル故ニ、 $f \mid d = p^e d'$ デナケレバ
ナラナイガ、 $(f', p) = 1$ ナル故、 $f \mid d'$ 、 従ツテ
 $f = d'$ 、 $d = p^e f = n$ 即チ $p \parallel \Phi_n(a)$ トナル。

$p = 2, \nu = 1$ ナル場合ハ $f \mid p-1 = 1$ ナル故 $f = 1$ 、
従ツテ $n = 2^e$ デアルガ、 $e > 1$ ナラバ $4 \mid a^{2^e} - 1$ ナ
ル故 $\nu > 1$ トナルカラ $e = 1$ 、即チ $n = 2$ デナケレ
バナラナイ。

コノ場合モ確カニ $2 \mid \Phi_2(a) = a + 1$ デアル。

以上ノ補題ヲ使ツテ、求ムル定理ガ簡單ニ証明サ
レル。

定理、 a ハ $|a| > 1$ ナル整数、 n ハ 2 ヨリ大ナル自
然数トスレバ、 a ト互ヒニ素ナル素数 p ノ中デ、 a
 $1 \pmod{p}$ = 離スル指数ガ丁度 n = 等シクナルヤウ
ナ p ガ少クトモ一ツ存在スル。但シ $a = 2, n = 6$ ナ
ル場合及ビ $a = -2, n = 3$ ナル場合ヲ除ク。

証明： 補題 2 = ヨレバ、 $p \mid \Phi_n(a)$ 且ツ $p \nmid n$ ナル
 p ノ存在ヲイヘバヨイワケデアル。ソコデ若シ、然
ラズトスル、即チ $p \mid \Phi_n(a)$ ナラバ $p \mid n$ ガ成立ツト
スル。ソノ p ヲトリ $a \not\equiv 1 \pmod{p}$ = 離スル指数ヲ f
トオケバ、 $n > f$ デ、 $n > 2$ デアルカラ、補題 4 =

ヨツテ、

$$n = p^e f, \quad p \parallel \Phi_n(a)$$

デナケレバナラナイ。

シカル $= f \mid p-1$ ナル故 $f < p$ 従ツテ p ハ n ノ
最大素因数トナル故、 $\Phi_n(a)$ ハ p 以外ノ素因数ヲ有
シナイコトニナリ、結局 $\Phi_n(a) = p$ デナケレバナラナ
イコトニナルガ、コレハ補題 1 ニヨレバ、ニツノ例
外ノ場合ヲ除イテハ不可能デアル。