数理解析研究所講究録
274巻 1976年 98-102



# Chevalley-Azumaya の定理

東京水産大学　竜沢周雄

問題　1より大きい自然数 $a$, $n$ を任意に与えたとき，

$$p \mid a^n - 1,\ \text{しかし}\ p \nmid a^{n'} - 1\ (1 \leqq n' < n)$$

を満足する少くとも1つの素数が存在するか。

この問題は Chevalley: Sur la théorie du corps de classes dans les corps finis et les corps locaux, Journ. of the Faculty of Science, Tokyo Univ. 1933 にあって，後に Azumaya: 整数論における一定理の初等的証明について，全国紙上数学談話会，265号 1944 が初等的証明を与えた。それは Chevalley の相互法則の証明に使われたものであるが，その目的のためならば Iyanaga [高木；代数的整数論，岩波 1971] による簡明な Lemma がある。東屋君の証明には教えられることの多い巧妙な手法が使われているが，多分その後発表されたこともないように思うので，Chevalley の方法も織りまぜながら，両者の相加平均によりえられる初等的証明を紹介する労をとらしていただこうと思うのである。しかし，

講演の際問題になつたArtinの原始根に関する予想問題やBakerの問題などに対しては使用目的が違うせいもあつて，ほとんど無力であることは止むをえない。

円分多項式

$$F_n(x)=\prod_{(a,n)=1}(x-\zeta^a) \qquad \zeta=e^{\frac{2\pi i}{n}}$$

は $\varphi(n)$ 次の有理整係数既約多項式で

$$\prod_{d\mid n}F_d(x)=x^n-1, \quad \text{したがって} \quad F_n(x)=\prod_{d\mid n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}$$

と表わされる。また $n=pf$，$p$ 素数，$(p,f)=1$ ならば

$$F_n(x)=\frac{F_f(x^p)}{F_f(x)}$$

となる。

[1] $p\mid F_n(a)$ かつ $p\nmid n$ なる素数 $p$ は問題の条件をみたす。

Proof　$p\mid F_n(a)\mid a^n-1$ だから $(a,p)=1$。$a$ の mod $p$ に関する指数を $f$ とすれば $f\mid n$。$p^\nu \parallel a^f-1$ $(\nu\geqq 1)$ とすれば $a^f=1+p^\nu c$，$(c,p)=1$ である。$n=bf$ とすれば $p\nmid n$ であるから $(b,p)=1$。また $a^n=(1+p^\nu c)^b=1+bp^\nu c+\cdots$ であるから $p^\nu\parallel a^n-1$。もし $n>f$ ならば

$$p^{\nu+1}\mid F_n(a)(a^f-1)\mid a^n-1$$

で矛盾がおきるから $f=n$ である。

[2] $F_n(a)$ と $n$ との共通の素因子はあるとしてもたゞ1つで、それを $p$ とすると

$n = p^e f$, $(f, p) = 1$ とかくとき $f < p$,

$(a, p) = 1$ で $F_n(a) = pk$ とすると, $(k, p) = 1$, $(k, n) = 1$,

が成立つ。

Proof $p \mid F_n(a) \mid a^n - 1$ だから $(a, p) = 1$。 $a$ の mod $p$ に関する指数を $f$ とすれば $f \mid n$。 Fermat の小定理より $f \mid p-1$ であるから $(p, f) = 1$。 したがって $n = p^e f m$, $(p, m) = 1$ とかける。 $f = n$ とすると Fermat の小定理より $n \mid p-1$ で $p \mid n$ に反するから $f < n$ である。

そこで $p^\nu \| a^{p^e f} - 1$ とすると, $n = p^e f m$, $(p, m) = 1$ であるから [1] の証明に述べたように $p^\nu \| a^n - 1$。 もしも $n > p^e f$ ならば

$$p^{\nu+1} \mid F_n(a)(a^{p^e f} - 1) \mid a^n - 1$$

となって矛盾がおきるから $n = p^e f$, $e \geqq 1$ とかける。

そこで, $p^\mu \| a^f - 1$, $p^\nu \| a^n - 1$ とすると

$$p^{\mu+1} \| a^{pf} - 1, \quad p^{\mu+2} \| a^{p^2 f} - 1, \cdots, \quad p^{\mu+e} \| a^{p^e f} - 1$$

となるから $\nu = \mu + e$ である。すなわち

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

である。したがって, $d = p^e f'$, $f' \mid f$ なる形のある $d$ につい

て、$p \parallel F_d(a)$。そのとき $p \mid a^d - 1$ となるから $f \mid d$。したがって $f' = f$, $d = n$ となる。すなわち

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

である。$f \mid p-1$ であるから $f < p$ で $p$ は $n$ の最大素因子である。故に $F_n(a)$ と $n$ との共通素因子は $p$ ただ1つである。

[3]　[2] の場合がおきたとしても、$a=2$, $n=6$ の場合を除いては $k>1$ となり [1] が適用され問題が解決される。

Proof

(i)　$n = p$ のとき。$F_p(1) = p$ だから $a > 1$ ならば $F_p(a) > p$ で $k > 1$ となる

(ii)　$n = pf$ のとき。

$p \geqq 3$, $\varphi(f) \geqq 2$ のときは

$$F_n(a) = \frac{F_f(a^p)}{F_f(a)} \geqq \frac{(a^p - 1)^{\varphi(f)}}{(a+1)^{\varphi(f)}} > \frac{(ap)^{\varphi(f)}}{\left(\frac{3}{2}a\right)^{\varphi(f)}} = \left(\frac{2p}{3}\right)^{\varphi(f)}$$

$$\geqq \frac{4p^2}{9} \geqq p$$

で $k > 1$ となる。

$p = 2$ のときは $n = p$ で (i) の場合に帰着。

$\varphi(f) = 1$, $f > 1$ ならば $f = 2$, $n = 2p$ そして $p \geqq 3$ の場合を検討すればよい

$$F_{2p}(a) = \frac{F_2(a^p)}{F_2(a)} = \frac{a^p + 1}{a+1} \geqq p \quad (a \geqq 2,\ p \geqq 3)$$

で等号が成立つのは $a = 2$, $p = 3$ の場合だけである。すなわち $a=2$, $n=6$ の場合を除いて $k > 1$

(iii) $n = p^e f$　$e \geqq 2$ のとき。

$$a^d - 1 \geqq \frac{1}{2}a^d, \quad \frac{1}{a^d - 1} \geqq \frac{1}{a^d}$$

であるから

$$F_n(a) = \prod_{d|n} (a^d - 1)^{\mu\left(\frac{n}{d}\right)} \geqq \prod_{d|n} a^{d\mu\left(\frac{n}{d}\right)} \left(\frac{1}{2}\right)^{1+\binom{m}{2}+\binom{m}{4}+\cdots}$$

$$\geqq a^{\varphi(n)}\left(\frac{1}{2}\right)^{2^{m-1}} \geqq \frac{a^{\varphi(n)}}{2^f} \qquad (m \text{ は } n \text{ の素因子の個数})$$

なぜなら，$\sum_{d|n} d\mu\left(\frac{n}{d}\right) = \varphi(n)$ であり，$n = p_1^{e_1} \cdots p_m^{e_m}$，$p_1 = p$ と素因数分解するとき，$\frac{n}{d}$ が，1，$p_1p_2$ 型，$p_1p_2p_3p_4$ 型 …… になる場合の個数は

$$1 + \binom{m}{2} + \binom{m}{4} + \cdots = 2^{m-1} \leqq p_2 \cdots p_m \leqq f$$

となるからである。$f \mid p-1$ に注意すれば上記計算より

$$F_n(a) = F_{p^e f}(a) \geqq \frac{a^{p^{e-1}(p-1)\varphi(f)}}{2^f} \geqq \frac{a^{p(p-1)\varphi(f)}}{a^{p-1}}$$

$$= a^{(p-1)(p\varphi(f)-1)} \geqq (1+p)^{p\varphi(f)-1} > p$$

となるから $k > 1$ である。

結局，初めの問題は $a=2$，$n=6$ の場合以外は解けるのである。例外の場合は $F_6(a) = a^2 - a + 1$，$F_6(2) = 3$ となって，成立しないのである。上述の(iii)が Chevalley の着想であり，あとは東屋君の着想である。そのような着想が我々の計算にも益することあるかも知れないと思って，また埋もれてしまっては惜しいと思って紹介したわけである。