

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,

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

を満足する少くとも 1 つの素数が存在するが。

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 にあつて、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 の方法も織り混ぜながら、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、

講演の際問題になった 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ふせいもあつて、ほとんど無力であることは止むをえない。

円分多項式

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

は $\varphi(n)$ 次の有理整係数既約多項式で

$$\prod_{d|n} F_d(x) = x^n - 1, \quad \text{したがつて } F_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$$

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

Proof $p \mid F_n(a) \mid a^n - 1$ したがつて $(a, p) = 1$ 。 a の mod p に
 關する指數を f とすれば $f \mid n$ 。 $p^y \parallel a^f - 1$ ($y \geq 1$) とすれば
 $a^f = 1 + p^y c$, $(c, p) = 1$ である。 $n = tf$ とすれば $p \nmid n$ であるから $(t, p) = 1$ 。 また $a^n = (1 + p^y c)^t = 1 + t p^y c + \dots$ であるから $p^y \parallel a^n - 1$ 。 もし $n > f$ ならば

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

で矛盾がよきるから $f = n$ である。

[2] $F_n(a)$ と n との共通の素因子はあるとしておたゞい
つて、それを p とすると

$$n = p^e f, (f, p) = 1 \text{ とかくと } f < p,$$

$$(a, p) = 1 \text{ で } F_n(a) = p^k \text{ とする } \text{と}, (k, p) = 1, (k, n) = 1,$$

が成立つ。

Proof $p \mid F_n(a) \mid a^n - 1$ 故に $(a, p) = 1$ 。 a の $\text{mod } p$ に
關する指數を 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。

よって $p^v \parallel a^{p^e f} - 1$ 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 $p^v \parallel a^n - 1$ 。 もしも $n > p^e f$
ならば

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

となつて矛盾がはきるから $n = p^e f$, $e \geq 1$ とかける。

よって, $p^\mu \parallel a^f - 1$, $p^v \parallel a^n - 1$ とする と

$$p^{\mu+1} \parallel a^{p^f} - 1, p^{\mu+2} \parallel a^{p^{2f}} - 1, \dots, p^{\mu+e} \parallel a^{p^{ef}} - 1$$

となるから $v = \mu + e$ である。 すなわち

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

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

て、 $p \parallel F_d(a)$ 。このとき $p \mid a^d - 1$ となる $x = a \mid d$ 。この
 故に $f' = f$ 、 $d = n$ 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 $f < p$ であり 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 だけ、1つである。

[3] [2] の場合が起きたとしても、 $d=2$ 、 $n=6$ 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。 $F_p(1) = p$ 故に $a > 1$ ならば $F_p(a) > p$ で $k > 1$ となる

(ii) $n = pf$ のとき。

$p \geq 3$ 、 $\varphi(f) \geq 2$ のときは

$$\begin{aligned} F_n(a) &= \frac{F_f(a^p)}{F_f(a)} \geq \frac{(a^p - 1)^{\varphi(f)}}{(a + 1)^{\varphi(f)}} > \frac{(ap)^{\varphi(f)}}{\left(\frac{3}{2}a\right)^{\varphi(f)}} = \left(\frac{2p}{3}\right)^{\varphi(f)} \\ &\geq \frac{4p^2}{9} \geq p \quad \text{で} \quad k > 1 \text{ となる。} \end{aligned}$$

$p = 2$ のときは $n = p$ で (i) の場合に戻る。

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

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

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) $n = p^e f$ $e \geq 2$ のとき。

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

であるから

$$\begin{aligned} F_n(a) &= \prod_{d|n} (a^d - 1)^{\mu(\frac{n}{d})} \geq \prod_{d|n} a^{d\mu(\frac{n}{d})} \left(\frac{1}{2}\right)^{1 + \binom{m}{2} + \binom{m}{4} + \dots} \\ &\geq a^{\varphi(n)} \left(\frac{1}{2}\right)^{2^{m-1}} \geq \frac{a^{\varphi(n)}}{2^f} \quad (m \text{ は } n \text{ の素因子の個数}) \end{aligned}$$

なぜなら, $\sum_{d|n} d\mu(\frac{n}{d}) = \varphi(n)$ であり, $n = p_1^{e_1} \dots p_m^{e_m}$, $p_1 = p$

と素因数分解するとき, $\frac{n}{d}$ が, 1 , p, p_2 型, p, p_2, p_3, p_4 型 $\dots$

になる場合の個数は

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

となるからである。 $f \mid p-1$ に注意すれば上記計算より

$$\begin{aligned} F_n(a) &= F_{p^e f}(a) \geq \frac{a^{p^{e-1}(p-1)\varphi(f)}}{2^f} \geq \frac{a^{p(p-1)\varphi(f)}}{a^{p-1}} \\ &= a^{(p-1)(p\varphi(f)-1)} \geq (1+p)^{p\varphi(f)-1} > p \end{aligned}$$

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, まを埋もれてしまっ
ては惜しいと思って紹介したわけである。