n 冪剰余

高校 3 年 2 組 40 番　西本将樹

1　Preface

次のような定理が知られている.

定理 1.1 (Hasse の定理) 多変数の同次 2 次方程式がすべて零以外の整数解をもつということと, その方程式が実数解をもち, 同次に各素数 p に関して p 真数解をもつということは同値である.

この定理の特別な場合として, 次の系が得られる.(初等的に)

系 1.2 $a \in \mathbb{Z}$ であり, 任意の素数 p に対して,$x^2 \equiv a \pmod{p}$ なる x が存在するならば,$x^2 = a$ なる $x \in \mathbb{Z}$ が存在する.

本文では, この系を少し強めた形で,Hasse の定理を経由せずに証明したいと思う. ある場面で, 系 1.2 の結果が重要になり, この結果に Hasse の定理のような定理を介する必要があるのかと疑問に思った事が動機です.

2　平方剰余の相互法則

この節では, 必要な定義や定理を挙げていく.

定義 2.1 (Legendre 記号) $n \not\equiv 0 \pmod{p}, p$: 素数 に対して,
$\left(\dfrac{n}{p}\right) = 1, \left(n \equiv x^2 \pmod{p} \text{ なる } x \text{ が存在する時.}\right)$
$\left(\dfrac{n}{p}\right) = -1, \left(n \equiv x^2 \pmod{p} \text{ なる } x \text{ が存在しない時.}\right)$
により,$\left(\dfrac{n}{p}\right) = 1$ を定義する. この記号 $\left(\dfrac{n}{p}\right) = 1$ は,***Legendre* 記号**と呼ばれる.

定理 2.2 (Fermat の小定理) 自然数 n と素数 p に対し,

$$n^p \equiv n \pmod{p}$$

が成り立つ. 特に,$p \nmid n$ であれば,$n^{p-1} \equiv 1 \pmod{p}$.

証明
$n=1$ で成り立つのは明らか。
$n=k$ で成り立つと仮定する。

$(k+1)^p=\sum_{i=0}^{p}{}_pC_ik^i$で,${}_pC_i$は $1\leq i\leq p-1$ に対して p の倍数になるから

$(k+1)^p\equiv k^p+1\equiv k+1 \pmod p$ よって $a=k+1$ でも成り立つ

よって数学的帰納法により任意の a に対して成立する。
また, 定理の後半部分はこれから直接分かる。
証明終

定理 2.3 (原始根の存在) 任意の素数 p に対し, ある g (**原始根**と呼ばれる) が存在して,$g^n\equiv 1 \pmod p \Leftrightarrow p-1\mid n$

証明は省略します. この定理より, $\pmod p$ で見た時,$1,g,g^2,g^3,\cdots,g^{p-2}$ は,$1,2,3,\cdots,p-1$ の並べ替えになっています.

定理 2.4 (Euler 規準) $\left(\dfrac{n}{p}\right)=n^{\frac{p-1}{2}}$

証明
定理 2.3 より, 原始根を g とすると, 任意の n に対して,$\exists e, n\equiv g^e \pmod p$
$n=x^2 \pmod p$ に解がある $\Leftrightarrow g^e=(g^d)^2$ に解がある $\Leftrightarrow e\equiv 2d \pmod{p-1}$ に解がある $\Leftrightarrow 2\mid e \Leftrightarrow n^{\frac{p-1}{2}}\equiv 1 \pmod p$
証明終

定理 2.5 $\left(\dfrac{n_1n_2\cdots}{p}\right)=\left(\dfrac{n_1}{p}\right)\left(\dfrac{n_2}{p}\right)\cdots$

Euler 規準より明らか.

さて, 次の定理でこの節は終わりである.

定理 2.6 (平方剰余の相互法則) 奇素数 p,q に対して

- $\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$(**平方剰余の第 1 補充則**)
- $\left(\dfrac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$(**平方剰余の第 2 補充則**)
- $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$(**平方剰余の相互法則**)

証明は省略する.

3　定理の証明

この節で, 次の定理を証明する.

定理 3.1 高々有限個以外の素数 p に対して $\left(\frac{n}{p}\right) = 1$ であるならば,n は平方数である.

n を割り切る最大の平方数を d とし,$n' = \frac{n}{d^2}$ とする. n について定理を示す事と n' について定理を示す事は同値だから, 始めから n として n を割り切る平方数が 1 以外に無い物を取っておけば良い. この時,$a, b = 0or1$ および奇素数 $p1, p2, \cdots, pn$ を用いて,$n = (-1)^a 2^b p_1 p_2 \cdots p_l$ または,$n = (-1)^a 2^b$ と書ける.

後者については $p \equiv 3 \pmod 4$ なる素数 p に対して $\left(\frac{-1}{p}\right) = -1$,$p \equiv \pmod 8$ なる素数 p に対して $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1$ である.

前者については $p \equiv 1 \pmod{8p_2 \cdots p_l}$ かつ,$p \equiv g \pmod{p_1}$(ただし g は $\pmod{p_1}$ の原始根) となる素数 p に対して,

$$\left(\frac{n}{p}\right) = \left(\frac{-1}{p}\right)^a \left(\frac{2}{p}\right)^b \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\cdots\left(\frac{p_l}{p}\right)$$

ここで,$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$ であり, さらに,

$$\left(\frac{p_1}{p}\right) = \left(\frac{p}{p_1}\right) = \left(\frac{g}{p_1}\right) = -1, \left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1, (i \geq 2)$$

であるから,$\left(\frac{n}{p}\right) = -1$

よって, いずれの場合にせよ,n がそれを割り切る 1 より大きな平方数を持たない時,$n = 1$ で無いならば, ある $a, M(a$ と M は互いに素) があって,$p \equiv a \pmod M$ なる素数 p に対して $\left(\frac{n}{p}\right) = -1$

最後に次の定理を用いれば証明が完結する.

定理 3.2 (Dirichlet の算術級数定理) a と n が互いに素な整数である時,$p \equiv a \pmod n$ なる素数が無限に多く存在する.

以上により,n が平方数でないならば,$\left(\frac{n}{p}\right) = -1$ なる素数 p が無限に多く存在する事が分かる. これによって, 定理 3.1 の証明が完了する.

4　n 乗数の場合

これを証明した後で, 次のような予想を立てた.

予想 4.1 $a \in \mathbb{Z}, n \in \mathbb{N}$ であり, 高々有限個以外の素数 p に対して,$x^n \equiv a \pmod{p}$ なる x が存在するならば,$x^n = a$ なる $x \in \mathbb{Z}$ が存在する.

実は, これは成り立つのだ！証明には, 類体論を使った. 類体論の細部をここで説明するのは不可能なので, ここではそのおおまかな流れを書く事にする.

a が,n 乗数では無いとして, どんな x に対しても $x^n \not\equiv a \pmod{p}$ なる p が無限に多く存在する事を示せば良い。

定理 4.2 $p \equiv 1 \pmod{n}, p \nmid m$ の時,
$x^n \equiv m$ なる x が存在する $\Leftrightarrow m^{\frac{p-1}{n}} \equiv 1 \pmod{p}$

証明
原始根の存在から簡単に導かれる.
証明終

定理 4.3 K/k を H 上の類体とし,A/H を k のイデアル全体の類別とする. この時

$$A/H \cong Aut(K/k)$$

が成り立ち, その対応は,

$$C(\mathfrak{p}) \longleftrightarrow z$$

ただし,z は,

$$A^{N(p)} \equiv A^z \pmod{\mathfrak{p}} (\forall A \in K)$$

なる置換.

これが, 類体論で非常に有名な **Artin の相互律**である.

定理 4.4 A/H の各類に,1 次の, つまり $N(\mathfrak{p}) = p$ なる素イデアル $\mathfrak{p}$ が, 無限に多く存在する.

これは, いわば Dirichlet の算術級数定理を一般の代数体に拡張した物である.

定理 4.5 p を m に含まれない素数とし,f を

$$p^f \equiv 1 \pmod{m}$$

なる最小の正指数,$\phi(m) = fg$ とすれば,m 分体 $Q(\zeta)$ において,

$$p = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g$$

と分解される. 各素因子 $\mathfrak{p}_i$ は f 次である.

さて, 準備が整った. 示したいのは次の定理だ.

定理 4.6 $a \in \mathbb{Z}, n \in \mathbb{N}$ であり, 高々有限個以外の素数 p に対して,$x^n \equiv a \pmod{p}$ なる x が存在するならば,$x^n = a$ なる $x \in \mathbb{Z}$ が存在する.

証明

a を n 乗数では無いとする.d を,n の約数で $\sqrt[d]{a}$ が整数になる物のうち最大の整数とする.$N = \dfrac{n}{d}, A = \sqrt[d]{a}$ とする.a が n 乗数でないので,$N \geq 2$

1 の原始 N 乗根を ζ, $\sqrt[N]{A} = \alpha$ として, 体拡大

$$\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \alpha)$$

を考える.

$\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}(\zeta)$ は Abel 体であり

$$Aut\left(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}(\zeta)\right) = \{\alpha \to \alpha\zeta^k \mid k = 0, 1, \cdots, N-1\}$$

従って, 任意の k に対し,$\mathbb{Q}(\zeta)$ の 1 次の素イデアル $\mathfrak{p}$ であって,$N(\mathfrak{p}) = p$,

$$\alpha^p \equiv \alpha\zeta^k \pmod{\mathfrak{p}}$$

なる物が無限に多く存在する. 特に $k = 1$ とすると,

$$\alpha^p \equiv \alpha\zeta^k \pmod{\mathfrak{p}}$$

$$A^{\frac{p-1}{N}} \equiv \zeta \pmod{\mathfrak{p}}$$

$$a^{\frac{p-1}{n}} \equiv \zeta \pmod{\mathfrak{p}}$$

よって,

$$a^{\frac{p-1}{n}} \not\equiv 1 \pmod{p}$$

さらに,p は N 分体において 1 次の素イデアルを因子に持つので,

$p \equiv 1 \pmod{N}$ 従って $p \equiv 1 \pmod{n}$

これらは,a が p を法として n 乗数で無い事を意味している. さらに, このような p は無限に多く取れるので, 定理が成り立つ.

証明終

5　後書き

この結果は, いかにも成り立ちそうではあったが, 証明は大変だった. 実際はもっと初等的に出来るのかもしれない. 得られた定理は, なかなか綺麗な物だと思った.

n 乗数の場合に挑んで, 暫く何も見えてこなかったので, ヒントを求めて類体論を少し勉強してみたら, 証明出来た. この証明を通して, かなり類体論に興味を持ったので, もっと勉強してみようと思います. 皆さんも, この文を読んで, なんとなく興味が沸いたなら, 是非勉強してみて下さい

参考文献としては, **代数的整数論 (高木貞治　著)** などがあります.

質問や感想などは,nisimotomasaki@funifuni.net へ御願いします.