平成２５年度卒業研究概要

平方剰余及び平方非剰余となる数について

中等教育教員養成課程　数学専攻　玉井 孝太

奇素数 p と, p で割り切れない整数 a に対して, $x^2 \equiv a \pmod{p}$ が $1 \leq x \leq p-1$ の範囲で解をもつとき, a を p の平方剰余という. また平方剰余でないとき, a を p の平方非剰余という. 例えば, $x^2 \equiv 5 \pmod{11}$ は, $1 \leq x \leq 10$ の範囲の整数において, $x = 4, 7$ を解にもつので, 5 は 11 の平方剰余であるのに対し, $x^2 \equiv 5 \pmod{13}$ は, $1 \leq x \leq 12$ の範囲の整数において, 解をもたないので, 5 は 13 の平方非剰余である. 平方剰余の性質の一つとしてガウスの補題というものがある.

命題 9 (ガウスの補題). p を奇素数, $h \in \mathbb{Z},\ p \nmid h$ とする. $(p-1)/2$ 個の数

$$h, 2h, \ldots, \frac{1}{2}(p-1)h$$

の中で, p を法とする最小の正の剰余が $p/2$ より大きいような数の個数を μ としたとき,

$$\left(\frac{h}{p}\right) = (-1)^{\mu}.$$

本論文では, ガウスの補題を利用し, ある整数がどのような素数の平方剰余及び, 平方非剰余であるかを考察する. ガウスの補題の h を $1, 2, -3, 5, -7, -11$ として μ の値を計算することにより, 以下の結果が得られた.

h	平方剰余となる素数の形	平方非剰余となる素数の形
1	すべての素数	
2	$8n \pm 1$	$8n \pm 3$
-3	$6n + 1$	$6n + 5$
5	$10n \pm 1$	$10n \pm 3$
-7	$14n + 1, 14n + 9, 14n + 11$	$14n + 3, 14n + 5, 14n + 13$
-11	$22n + 1, 22n + 3, 22n + 5$ $22n + 9, 22n + 15$	$22n + 7, 22n + 13, 22n + 17$ $22n + 19, 22n + 21$

本論文では, $h = 2, -3, 5$ の場合について詳しい証明を載せている.

また, 上記の結果から予想を立て, 次の定理を示すことができた.

定理 5. a を奇素数, $n \in \mathbb{Z}$ に対し, $2na + 1$ を奇素数とするとき,

$$\left(\frac{(-1)^{(a-1)/2}a}{2na+1}\right) = 1.$$

上の表からはさまざまな特徴がわかるので, その特徴について考察していくことが今後の課題である.