論文審査の結果の要旨

氏　名　張　祺　智

張氏は、提出論文において、有限体上の離散対数問題を研究した。有限体の乗法群 $\mathbf{F}_q^{\times}$は巡回群であり、その生成元 g がある。$F_q^{\times}$の元 a に対し、$a=g^m$をみたす整数 m を求める問題を離散対数問題といい、コンピュータ暗号への応用が知られている。

Hwang 氏と Raskind 氏は離散対数問題の解法として、実2次体の単数を用いる方法を提案した。張氏は本論文でこの方法の一般化について研究した。p と l を相異なる奇素数とし、K を実2次体とする。K は p で不分岐かつ l で完全分解と仮定する。u を p の上にある素点、v を l のうえにある素点とする。u の剰余体の位数 q=Nu が $q\equiv 1 \bmod l$ をみたすと仮定する。また K の類数は l で割れないと仮定する。K の素点 w に対し $\langle\ ,\ \rangle_w : H^1(K, \mathbf{F}_l) \times K^{\times} \to \mathbf{F}_l$ で類体論の相互写像が定める標準ペアリングを表す。K の l 次巡回拡大で u, v の外で不分岐で、u, v で分岐するものをとり、χ を対応するガロワ群の指標とする。α を K の単数とすると、類体論の相互法則より $\langle \chi, \alpha \rangle_u + \langle \chi, \alpha \rangle_v = 0$ となる。

Hwang と Raskind の方法は、この事実に基づき乗法群 $\mathbf{F}_q^{\times} = \kappa(u)^{\times}$における離散対数問題を、有限体の加法群 $\mathbf{F}_q = \kappa(v)$での除法という、より簡単な問題に帰着させようというものである。しかしその際、$\langle \chi, g \rangle_u$ と $\langle \chi, 1+l \rangle_v$ の比を求めることが必要となり、分岐符号とよばれるこの比を求める問題と、離散対数問題が同等という結論が得られる。

Hwang と Raskind は、この方法を K が p で完全分解の場合、すなわち q=p の場合に考察した。張氏は、この方法が K で p が分解しない場合、すなわち $q=p^2$ の場合にも適用できることを示した。論文の主結果は次のとおりである。

主結果 p と l を相異なる奇素数とし、$p^2 \equiv 1 \bmod l$ と仮定する。q=p, p^2に対し，p で不分岐かつ l で完全分解する実2次体 K とその単数 α で、K の p の上にある素点と l の上にある素点に関する分岐符号問題が、$\mathbf{F}_q^{\times}$における離散対数問題と同値であるものを構成できる。

ただし、構成した実 2 次体 K の類数は 1 と素であると仮定する。また、構成した単数 α が条件をみたす確率は 50%でありこの構成をくり返すことで、条件をみたすものが確率的に得られる。

証明の方法は基本的には Hwang と Raskind の議論をなぞるものではあるが、次のような点で改良も加えている。この方法を適用するためには、$\langle \chi, \alpha \rangle_v$ が 0 でない単数 α を構成することが必要である。Hwang と Raskind の論文ではこのような単数の存在は仮定とされていたが、単数の構成を工夫することで、この仮定を少なくとも確率論的には取り除

くことができた。Hwang と Raskind の論文と同じく、類数が 1 で割れないという仮定は除くことができない。

以上のように、本論文において論文提出者張祺智氏は有限体上の離散対数問題に関する Hwang 氏と Raskind 氏の方法を考察し、それをさらに進めることに成功している。これは、博士（数理科学）の学位を与えるにふさわしいものである。