行政院國家科學委員會專題研究計畫　期中進度報告

橢圓曲線的質點問題(1/2)

計畫類別：個別型計畫
計畫編號：NSC91-2115-M-032-004-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：淡江大學數學系

計畫主持人：陳燕美

計畫參與人員：陳燕美 黃瓊儀 李嘉修

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 92 年 5 月 15 日

行政院國家科學委員會補助專題研究計畫 □成果報告 □期中進度報告

橢圓曲線的質點問題(1/2)

計畫類別：□ 個別型計畫 □ 整合型計畫
計畫編號：NSC 91－2115－M－032－004－
執行期間： 91 年 08 月 01 日至 92 年 07 月 31 日

計畫主持人：陳 燕 美 淡江大學數學系

計畫參與人員： 兼任助理 黃瓊儀 淡江大學數學系碩士生
兼任助理 李嘉修 淡江大學數學系大學部學生

成果報告類型(依經費核定清單規定繳交)：□精簡報告 □完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究

計畫、列管計畫及下列情形者外，得立即公開查詢

□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：淡 江 大 學　數 學 系

中　華　民　國　92　年　05　月　20　日

一、中文摘要：

令 E 為定義在 Q 上的橢圓曲線, 和 P 為曲線上具有無窮秩的有理點. 假設 E 擁有複乘數姐且其複乘數為複二次體 k 中的 零化子。令 M 為 具有下列性質的質數所形成的集合: p 在 k 中可分解, E 在 p 有好的約化, 而且 P 模 p 為一質點。假設一般化的黎曼猜想成立, 我們可以決定 M 的密度是否為一正數。

關鍵詞: 質點, 橢圓曲線, 複乘數, 密度。

二、　英文摘要(Abstract):

Let E be an elliptic curve defined over Q, and P a rational point of infinite order. Suppose that E has complex multiplication by an order in the quadratic imaginary field k. Denote by M the set of rational primes p such that p splits in k, E has good reduction at p, and P is a primitive point modulo p. Under the generalized Riemann hypothesis, we can determine the positivity of the density of the set M explicitly.

關鍵詞(Key Words): primitive points, elliptic curves, complex multiplication, density

三、　計畫緣由與目的:

The well-known Artin's primitive root conjecture was proved by Hooley in [6] under the assumption of the generalized Riemann hypothesis (GRH). There are various types of analogous primitive root problems. For example, the quadratic analogue in [2] and [10], the analogue for one-dimensional tori over the rational numbers in [3] and over the function fields in [4], and the r-rank analogue in [1] and

[9]. In this project we consider the analogue for elliptic curves following [5] and [8]. Let E be an elliptic curve defined over the rational numbers Q and P a rational point of infinite order. For a rational prime p, P is called a primitive point for the prime p if P *modulo* p generates $E(F_p)$. Lang and Trotter conjectured in [8] that the density of primes p for which P is a primitive point always exists. In that paper, only a necessary and sufficient condition for a prime q to divide the index $[E(F_p): \langle P \text{ modulo } p \rangle]$ was formulated which accomplished an algebraic step in line with Hooley's proof in [6]. The first break of this conjecture was struck by Gupta and Murty [5] in the case that E has complex multiplication (CM) by the maximal order O_k of a quadratic imaginary field k. In [5], they treated the splitting primes and proved the existence of the density in question under the assumption of the generalized Riemann hypothesis GRH. The positivity of density was also checked in their paper in some special cases. More precisely, they showed:

Theorem:(Gupta-Murty, [5])
Let E be an elliptic curve defined over $\boldsymbol{Q}$ with CM by O_k. Denote by M the set of rational primes p such that p splits in k, E has good reduction at p, and P is a primitive point for p. Assuming GRH, then
(a) The density of M exists.
(b) Suppose further that 2 or 3 are inert in k or $k= Q(\sqrt{-11})$. Then the density of M is positive.

It is not difficult to check that for these cases the Mordell-Weil group $E(Q)$ always has trivial torsion part, and furthermore $E_{tor}(k)$ is trivial. For the case $k= Q(\sqrt{-7})$ and E has CM by O_k. One checks that $E[2] \dot{C} E(k)$, hence the density of M is 0.

In this project we try to relate the positivity of the density with the torsion part of the Mordell-Weil group in all cases.

四、計畫結果與討論:

此一研究計畫中，我們得到以下的結果：

Theorem: Assume *GRH*. Suppose that E has CM by an order in k and P is a nontorsion rational point. Suppose further $E_{tor}(k)$ is cyclic. Then the density of M is positive if and only if for any prime $q | \#(E_{tor}(k))$, there exists no k-rational q-isogeny $\Phi: E' \to E$ such that $\Phi^{-1}(P) \dot{C} E'(k)$.

五、計畫成果自評

此一研究成果將Artin的質根猜想推廣至橢圓曲線的情況。其中需要大量地代數的理論支持以及相當繁瑣的計算，可是我們總算克服困難成功地得到上述的定理。但是我們將來會繼續此一研究，尤其是關於在 k 中不可分解的質數 p的情況。

六、參考文獻

[1] L. Cangelmi and F. Pappalardi, On the r-rank Artin Conjecture II, Journal of Number Theory 75(1999), 120-132.

[2] Y.-M. J. Chen, Y. Kitaoka, and J. Yu, Distribution of Units of Real quadratic Fields, Nagoya Math J. 158(2000), 167-184.

[3] Y.-M. J. Chen, On Primitive Roots of One Dimensional Tori, Journal of Number Theory 93(2003), 23-33.

[4] Y.-M. J. Chen, Y. Kitaoka, and J. Yu, On Primitive Roots of Tori: The Function Field Case, Mathematische Zeitschirft, to appear.

[5] R. Gupta and M. R. Murty, Primitive points on elliptic curves, Compositio mathematica 58(1986), 13-44.

[6] C. Hooley, On Artin's conjecture, J. reine angew Math. 225(1967), 209-220.

[7] D. S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. (3)33(1976), 193-237.

[8] S. Lang and H. Trotter, Primitive points on elliptic curves, Bull. Amer. Math. Soc. 83(1977), 289-292.

[9] F. Pappalardi, On the r-rank Artin Conjecture, Math. Comp. 66(1997), 853-868.

[10] H. Roskam, A quadratic analogue of Artin's conjecture on primitive roots, Journal of Number Theory 81(2000), 93-109, ERRATUM, 85(2000), page 108.

[11] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

[12] J. H. Silverman, The Arithmetic of Elliptic Curves}, Springer-Verlag, 1986.