計畫名稱: 橢圓曲線上的漢斯-魏爾函數

計畫編號: NSC 87-2115-M-032-006

執行期限: 86 年 8 月 1 日至 87 年 7 月 31 日

主持人: 陳燕美

淡江大學數學系

一、中文摘要:

在本計畫中,我們可以利用布林代數來決定一組(係數是有限體的元素)多變數多項式方程組是否有解。此結果能夠幫助我們瞭解橢圓曲線的同次空間質的局部表現。

關鍵詞: 布林代數,有限體,多變數多項式,橢圓曲線,同次空間。

二、英文摘要(Abstract):

In this project, we can determine the solvability of a system of multivariate polynomials over the finite field of 2 elements in terms of Boolean algebras. This can help decide the local behavior of homogeneous spaces of an elliptic curve at the rational prime 2.

關鍵詞(Key Words): Boolean algebra, finite field, multivariate polynomials, elliptic curves, homogeneous spaces.

三、計畫緣由與目的:

The computation of the rank of an elliptic curve is usually very complicate. One way to do it is by the method of descend—this can be done by computing its Selmer group which consists of lots of homogeneous spaces. A homogeneous space of an elliptic curve itself is a smooth curve. Roughly speaking, a homogeneous space will be an element of a Selmer group if and only if it has a local rational point everywhere which can be reduced to finite field cases by Hensel's lemma. And mostly a homogeneous space can be defined by a finite set polynomials in more than one variables.

To check the local behavior at the places lying over the rational prime 2 turns out can be reduced to check the existence of solutions of a system of multivariate polynomials over the finite fields of 2 elements. Therefore, we try to study the properties of the polynomial rings and hope it might help us on computing the Selmer group of an elliptic curve.

四、計畫結果與討論:

First, we set the following notations.
F = the finite field of 2 elements.
R = the polynomial ring of n variables $x_1, x_2, \dots, x_n$ with coefficients in F.
I= the ideal of R generated by $x_1^2 - x_1, x_2^2 - x_2, \dots, x_n^2 - x_n$.
B= the Boolean algebra of the power set of F^n.

Given f and g in R, we define $f+I \cup g+I = fg+I$, $f+I \cap g+I = fg+f+g+I$. And $(f+I)' = f+1+I$. It is easy to check that $(R/I, \cup, \cap, ', 0+I, 1+I)$ is a Boolean algebra which has the same cardinality with B.

Finally, we can show the following proposition.

Proposition: R/I and B are isomorphic Boolean algebras.

Proof: Given any f in R, denote the zero set of f by Z_f . Consider the map $\varphi : R/I \to B$ defined by $\varphi(f+I) = Z_f$. It is routine to check that the map φ is a homomorphism of Boolean algebras. Also we can show by induction on n that Z_f is empty if and only if $f+I=1+I$, this will implies that φ is injective, and thus it is bijective since R/I and B have the same cardinality. □

Corollary 1: For any f in R, Z_f is empty if and only if $f+I=1+I$.

Proof: (←) Clear.
(→) By induction on n.
Write $f \equiv x_n q + r \bmod x_n^2 - x_n$, where q, r are polynomials in $x_1, x_2, \dots, x_{n-1}$ only. If r is not congruent to 1 modulo $x_1^2 - x_1, x_2^2 - x_2, \dots, x_{n-1}^2 - x_{n-1}$, then r has a solution, say $(a_1, a_2, \dots, a_{n-1})$ in $F^{n-1}$and thus f has a solution $(a_1, a_2, \dots, a_{n-1}, 0)$ in F^n, this is a contradictions! Therefore r is congruent to 1 modulo $x_1^2 - x_1, x_2^2 - x_2, \dots, x_{n-1}^2 - x_{n-1}$. Again if q is not congruent to 0 modulo $x_1^2 - x_1, x_2^2 - x_2, \dots, x_{n-1}^2 - x_{n-1}$, then $q+1$ has a solution, say $(b_1, b_2, \dots, b_{n-1})$ in $F^{n-1}$and thus f has a solution $(b_1, b_2, \dots, b_{n-1}, 1)$ in F^n,

this is a contradictions too! Therefore q is congruent to 0 modulo $x_1^2 - x_1, x_2^2 - x_2, \ldots, x_{n-1}^2 - x_{n-1}$ and $f+I = x_n q+r+I = 1+I$. □

Corollary 2-4 follow immediately from the proposition.

Corollary 2: For any f, g in R, $Z_f = Z_f$ if and only if $f+I = g+I$.

Corollary 3: For any $\underline{a}=(a_1, a_2, \ldots, a_n)$ in F^n, let $t_{\underline{a}} = \Pi(x_1+a_1+1)$, then $\underline{a}$ is the unique solution of $t_{\underline{a}}$.

Corollary 4: For any f in R, it is congruent to $\Pi\, t_{\underline{a}}$ where the product runs thought the set Z_f.

Corollary 5: Given any f in R, let $f_1^{(0)} = fx_1+f+x_1$ and $f_1^{(1)} = fx_1+x_1+1$, then f has a unique solution if and only if for every $i=1, 2, \ldots, n$, either $f_1^{(0)}+I = 1+I$ or $f_1^{(1)}+I = 1+I$ but not both.

Proof: (←) Let $\delta : \{1, 2, \ldots, n\} \to \{0, 1\}$ be the function which satisfies that $f_1^{(\delta(1))}$ is not congruent 1 modulo I. Then $(\delta(1), \delta(2), \ldots, \delta(n))$ is the only solution of f.
(→) Let $\underline{a}=(a_1, a_2, \ldots, a_n)$ be the unique solution of f. For every i, ie easy to check that if $a_1=0$, then $f_1^{(1)} \equiv 1$ and if $a_1=1$, then $f_1^{(0)} \equiv 1$. □

五、計畫成果自評:

Proposition tells that the set of F-rational points of a variety over F is the set of F-rational points of a hypersurface. Corollary 1 can determine the existence of F-rational points of a hypersurface and Corollary 5can determine the uniqueness of F-rational points of a hypersurface .

六、參考文獻:

[1] Joseph Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.
[2] Yen-Mei J. Chen, *The Selmer Groups and the Ambiguous Ideal Class Groups of Cubic Fields*, Bull. Austral. Math. Soc., Vol(54)267-274,1996.
[3] Yen-Mei J. Chen, *The Selmer Groups of Elliptic Curves and the Ideal Class Groups of Quadratic Fields*, Communication in Algebra, 25(7), 2157-2167,1997.
[4] Rudolf Lidl & Harald Niederreiter, *Introduction to finite fields and their applications*, revised ed., Cambridge University Press,1994.