行政院國家科學委員會專題研究計畫成果報告

計畫編號：NSC 89-2115-M-002-031
執行期限：89年08月01日至90年08月30日

主持人：陳其誠 執行機構及單位名稱：台大數學系

一、中文摘要

本計畫中我們研究某些實數二次體之基本可逆元的特性。如果此二次體之判別數 d 為奇數且存在一質數 $p|d$，$p \equiv 3 \pmod 4$，則其基本可逆元 $\varepsilon = a + b\sqrt{d}$, $a>0$，必滿足 $1 < (a-1, d) < d$。我們亦嘗試利用此性質，以求 d 之質因數分解之可能性。

關鍵詞：實數二次體，判別數，基本可逆元，質因數分解，高斯虧格數，連分數，規化子，Diophantine 逼近。

Abstract: We study the fundamental units of certain real quadratic fields. If the discriminant d is odd and there is a prime number $p|d$, $p \equiv 3 \pmod 4$, then the fundamental unit $\varepsilon = a + b\sqrt{d}$, $a > 0$, satisfies

$$1 < (a-1, d) < d.$$

We also try to see the possibility of using this property to factorize d.

Keywords: real quadratic field, discriminant, fundamental unit, factorization, Gauss genus, continuous fraction, regulator, Diophantine approximation.

二 緣由與目的

古典的 Pell's equation

$$x^2 - dy^2 = \pm 1, \quad d \in \mathbb{N}, \ x, y \in \mathbb{Z}$$

可說是已被充分了解了，因為其解集合即為 $K=\mathbb{Q}(\sqrt{d})$ 中的 unit group（其 ring of integers, $\mathcal{O}_K$, 的 unit group）。而 Dirichlet 說這個 unit group 與 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}$ 同構。我們也知道，基本可逆元（the group 的 generator, up to ± 1）也可由連分數的方法求（算）出，而這似乎也是唯一的方法。

雖然事情已經是如此的清楚不過，但事實上如果往前一步更深入，則很容易就陷入廣泛未經系統化整理或甚至完全未知的領域之中。不用說關於解之計算 complexity，就連何時 $x^2-dy^2=-1$ 有解至今仍未有一完整的答案。而這個問題正與 K 之 class group 的 Sylow 2-subgroup 的 rank 有關。當然，如果談論到的是 strict class group 而非 class group，則 Gauss 的 genus 定理已經回答問題了。如果以 Class field theory 的觀點，則這個問題又可問到 K 上給定一個 ramification condition 的 maximal abelian Galois group 上面去，而答案似乎卻在那一個所謂的 fundamental unit 上。

近來數學日新月異，例如在各種複雜的系統上常有讓人意想不到的研究成果。但是在一個這樣簡單古老的二次体方面，我們卻像是一位糊塗的學究那樣，似乎看起來什麼都知道了，但又每次都被考倒。這對數學家而言，實為萬分尷尬的事。吾人忝為數學中人，見此情況於是自告奮勇，不揣淺薄而在此未知之領域做

探索，以期精解专業之進展. 本計劃行之多年，承貴会在本年度内给予经费補助，特此致谢.

三 结果与討論

在此計劃的研究过程当中，我們漸漸看到了，並驗证了下面的定理.

<u>Thm 1</u>: Suppose that $d = disc(K)$, the discriminant of K, is odd and there is a prime number $p \mid d$ such that $p \equiv 3 \pmod 4$. If $\varepsilon = a + b\sqrt{d}$, $a > 0$, is the fundamental unit, then

$$1 < (a-1, d) < d.$$

假設 $S = \{ p \mid p \mid d \}$, $S_0 = \{ p \mid p \mid (a-1, d) \}$
$S_1 = S \sim S_0$. 則 $d = \prod_{p \in S} p$

<u>Thm 2</u>:

Under the conditions of <u>Thm 1</u>, the followings are true.

① There exist $f_1, f_2 \in \mathcal{O}_K$ such that

$$N_{K|\mathbb{Q}}(f_1) = \prod_{p \in S_0} p \quad , \quad N_{K|\mathbb{Q}}(f_2) = \prod_{p \in S_1} p$$

② If $\exists f \in \mathcal{O}_K$, $S_2 \subset S$ such that

$$N_{K|\mathbb{Q}}(f) = \prod_{p \in S_2} p \quad , \text{ then } S_2 = S_0 \text{ or } S_2 = S_1$$

由此看來，$S = S_0 \amalg S_1$ 這一個 partition，或者等價的來說 $(a-1, d)$ 這一個 d 的因數，有其獨特之處。定理1已經告訴我們，這個特別的子集，或特別的因數，都可經由基本可逆元而求出。但這就像是說由台大坐捷運淡水線轉板南線再轉木柵線可達國科會一樣的令人迷惑。"到底有沒有更直接的路來描述 S 與 S_0，d 與 $(a-1, d)$ 的關連？" 這一個問題三不五時即浮現在吾人的思緒之中。然則就像歷史上的探險家一般，我們已被前面的未知所完全阻斷，越過前面是否有路？而我們是否有足夠的工具與生命去走完全程，則更是一個謎。

我們亦嘗試利用定理1做質因數分解。假設 $D = pq$，p, q 皆為大質因數。找 λ 使得 $d = \lambda \cdot D$ 滿足定理1的條件。再求出 ε，然後得到 $d_1 = (a-1, d)$。一般而言，如果 λ 為隨機取出，則 $(D, d_1) = p$ 的機率應為正。因為求公因數只用到 Euclidean Algorithm，故 p，在 ε 求出之後，應很容易得出。我們嘗試讓 λ 變動而看 ε 的計算複雜度。但是因為 ε 的計算只能使用連分數算法，經過實驗結果不理想。

四. 計畫成果自評

如果就數學上的成果而言，我們得到的比海風還輕，比海水更淺。

五. 參考文獻

1. 國科會專題研究計畫成果報告撰寫格式說明。中華民國行政院國家科學委員會。2001.