Hilbert 第三問題與密鑰交換

學生：數三 高煌昌
指導教授：洪斌哲 教授

摘要：
迪菲-赫爾曼密鑰交換（Diffie–Hellman key exchange，縮寫為D-H） 是一種安全協定。它可以讓雙方在完全沒有對方任何預先資訊的條件下通過不安全信道建立起一個金鑰。這個金鑰可以在後續的通訊中作為對稱金鑰來加密通訊內容。公鑰交換的概念最早由瑞夫·墨克（Ralph C. Merkle）提出，而這個密鑰交換方法，由惠特菲爾德·迪菲（Bailey Whitfield Diffie）和馬丁·赫爾曼（Martin Edward Hellman）在1976年首次發表。馬丁·赫爾曼曾主張這個密鑰交換方法，應被稱為迪菲-赫爾曼-墨克密鑰交換（Diffie–Hellman–Merkle key exchange）。
在這個專題中，我們以Hilbert 第三問題為靈感，嘗試設計出一種密鑰交換的方法

Hilbert第三問題：

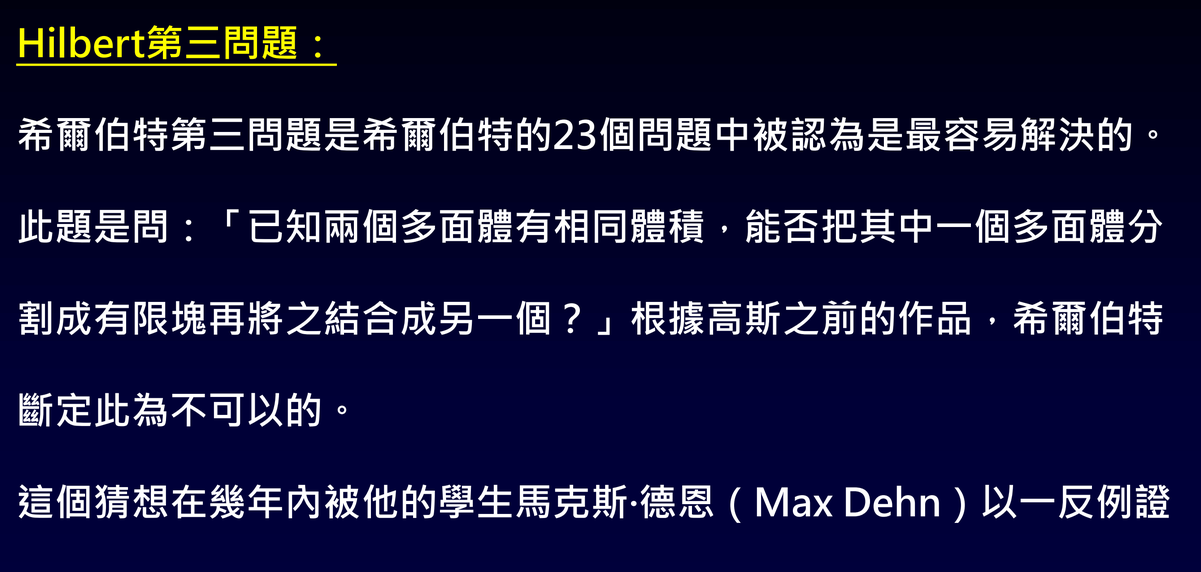
希爾伯特第三問題是希爾伯特的23個問題中被認為是最容易解決的。

此題是問：「已知兩個多面體有相同體積，能否把其中一個多面體分割成有限塊再將之結合成另一個？」根據高斯之前的作品，希爾伯特斷定此為不可以的。

這個猜想在幾年內被他的學生馬克斯·德恩（Max Dehn）以一反例證明了是不可以的了。但其在二維空間的情況，答案是肯定的。

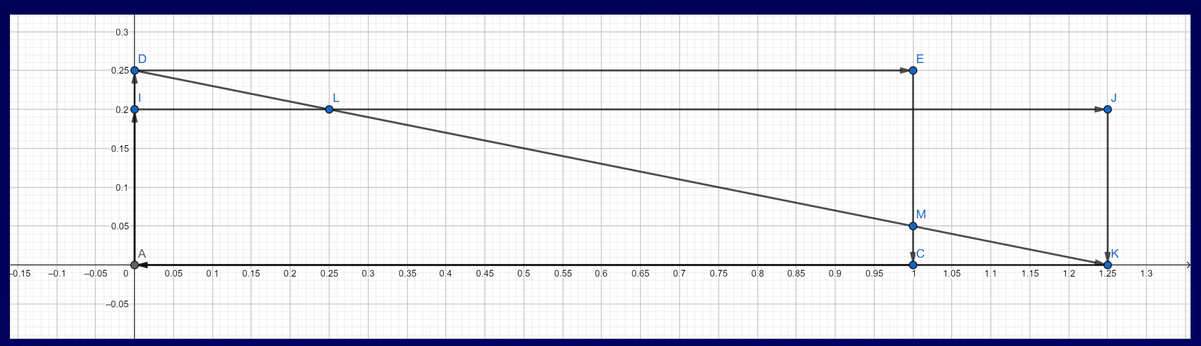
將一個三角形切割成另一個三角形：

步驟一、在三角形ABC（圖一）中切割出三角形BFH與BGH，將他們分別移至三角形AFD與CGE處。此時，三角形ABC變成矩形ADEC。



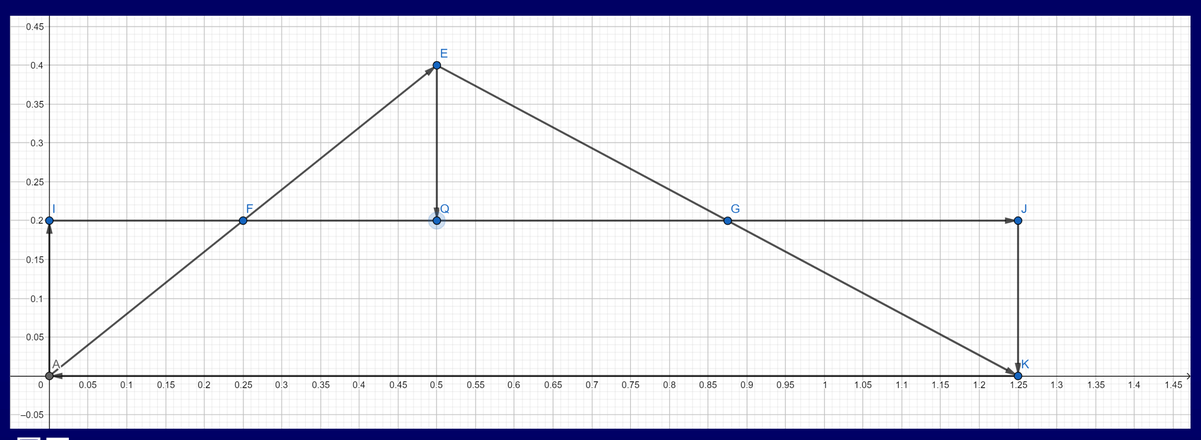
圖一

步驟二、在矩形ACED（圖二）中切割出三角形MED與ILD，將它們分別移至三角形JKL與CKM處。此時，矩形ACED變成矩形AKJI。



圖二

步驟三、在矩形AKJI（圖三）中切割出三角形ANI與KOJ，將他們分別移至三角形NPQ與OPQ處。此時，矩形AKJI變成了三角形APK。



圖三

設計分割三角形的演算法：

步驟一、令三角形T0的三個頂點為：

(0, 0)，(x0, y0)，(1/(2*y0), 0)

將它切割成三角形T2，其三個頂點為：

(0, 0)，(x1, y1)，(1/(2*y1), 0)　（圖四）

步驟二、令 L1: x-x0/y0*y=0

L2: x+1/(y0*y1)*y=1/(2*y1)

求L1與L2的交點，令其為(x2, y2)

則 x2=x0 / (2*(x0*y1+1))

y2=y0 / (2*(x0*y1+1))

步驟三、對x2, y2的分子分母做模運算

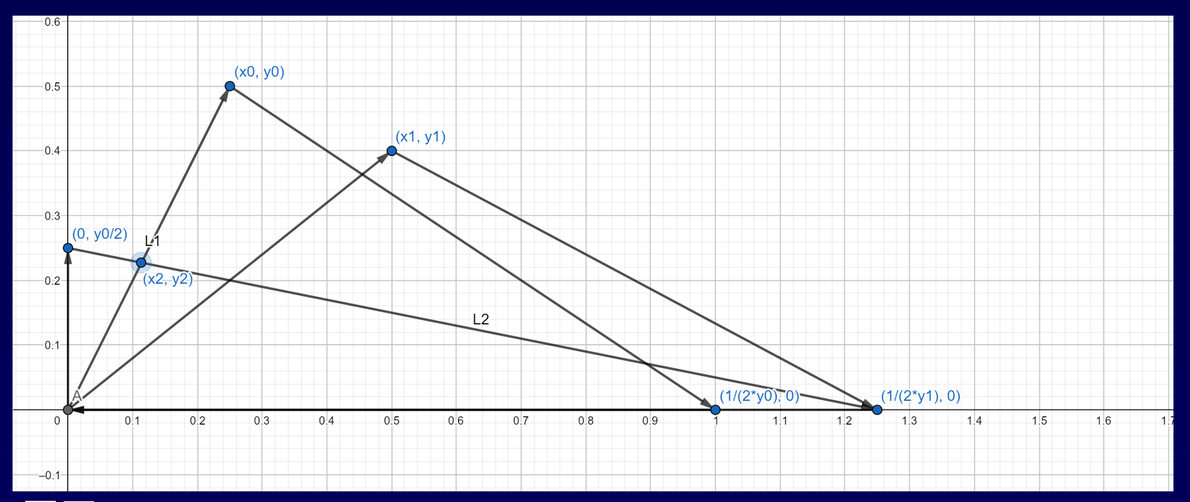
x2=x0 (mod p) / (2*(x0*y1+1)) (mod p)

y2=y0 (mod p) / (2*(x0*y1+1)) (mod p), p為大質數

令三角形T2的三個頂點為(0, 0)，(x2, y2)，(1/(2*y2), 0)

重複步驟一、二、三 (n-1) 次，得到三角形Tn的頂點：

(0, 0)，(xn, yn))，(1/(2*yn), 0)



圖四

密鑰交換：

公開(x0, y0), (x1, y1) 作為公鑰

Alice 選擇一個正整數n，運算得到Tn，並公開Tn

Bob 選擇一個正整數m，運算得到Tm，並公開Tm

Alice 將Tm運算(n-1)次，Bob將Tn運算(m-1)次

兩人會得到同樣的T(n+m)

密鑰交換之安全性：

此安全性相當於演算法的離散對數問題