

楊一帆教授 / 應用數學系

數論

數論是數學最古老的分支之一，一開始主要是研究整數的性質及其之間的關係，像是質數的性質、整係數多項式的整數解等等皆是數論的研究課題，例如著名的費馬最後定理（當為大於二的整數而為方程式的整數解，則中必有一個數為零）即是數論中最為耳熟能詳的問題。為了解決數論中的問題，數學家發展了許多工具，刺激了數學其他領域的發展，也與各領域互動密切，像是代數、幾何、複變、微分方程、離散數學、數學物理等等皆與數論密切相關。

傳統上，數論被視為一個純數學的領域，但在過去三十餘年間，數學家發現許多數論在實際生活的應用。由於資訊科技的迅速發展，人們對於密碼及編碼有強烈需求，此時數學家們發現許多數論中的理論可以用來建構好的密碼系統及編碼，如目前應用廣泛的RSA 密碼及橢圓曲線密碼系統皆是數論的應用。因此，時至今日，數論已經不僅是人們基於好奇心而產生的數學領域，它也跟現代人的生活密不可分。

特色研究介紹

本人主要是研究方向為模形式（modular forms）的構造及應用，以及模曲線（modular curve）及志村曲線（Shimura curve）的研究。簡單的講，模形式是一個擁有很多對稱性的解析函數。可想而知，一個擁有很多對稱性的函數一定是非常特別，數學家們發現這些模形式有豐富的算術性質，可以用來解決數論中的問題，一個著名的例子即是上述提到的費馬最後定理。費馬最後定理一直到1995年才由Andrew Wiles給出一個完整的證明，但其證明並不是直接的。Wiles真正證明的事實上是一個有關橢圓曲線跟模形式算術性質之間的對應關係。

模形式的研究從十九世紀中期開始，至今仍是數學中最熱門的研究課題之一，跟表現理論、算術幾何、微分方程、物理裡的弦論、量子場論等皆有關聯，其高階的推廣仍有許多問題等待數學家去解決，非常值得年輕學者投入研究。