計算機数学への誘い

筑波大学数学域　西村　泰一

人間と計算との関わりは古いが、現在我々が computer で思い浮かべるような digital computer が出てくるのは 1940 年代の話で、比較的新しい。興味深いのは、そうした digital computer の出現に先立って、Church や Turing 等によって計算可能性の理論が作られていたことで（Gödel の不完全定理とその証明は大きな影を落としている）、そこで研究されたλ計算は、1950 年代後半に Lisp という計算機言語を生み出し、さらに 1970 年代には、その機能を必要最小限に絞って Scheme という言語も生み出している。計算可能性の理論は、計算機と発達と相俟って、計算量の理論へと発展し、Ｐ＝ＮＰ（？）という未解決問題は有名である。

Algorithm の概念と幾多の algorithms は、おそらく人類の誕生と同じくらいに古いのであろうが、文献に残る algorithm として有名なものは、Euclid の互除法あるいは中国剰余定理として知られているもので、紀元前数世紀に遡る。これと Gauss による連立一次方程式の解法として知られている掃き出し法は、20 世紀半ばに Gröbner 基底の理論として一般化され、計算機の発達と相俟って、計算代数学として爆発的な発展を示し、可換環論、代数幾何学、微分方程式、整数計画法等で不可欠な道具立てとなっている。

計算機で使用される言語の統語論の数学的基礎については、米国の著名な言語学者 Chomsky の生成文法の影響もあって、数理言語学という分野でよく研究されているが、その意味論についてはプログラム意味論として研究され、なかでも表示的意味論は 1960 年代末に英国の数学者 Dana Scott によって始められた領域理論によって基礎付けられる。1950 年代末にドイツの論理学者 Paul Lorenzen によって直観論理の意味論として導入された game 意味論は、Blass によって線形論理との関連が指摘され、この方向に研究を進めることで、Abramsky 等は長年の懸案であった計算機言語 PCF の完全に抽象的な model を与えることに成功している。20 世紀末の話である。

普通の digital computer では bit は 0 もしくは 1 であるが、このふたつの値を任意の割合で重ね合わせることのできる量子 computer の研究も 1980 年代に始まっている。最初は理論的な研究が主であったが、1994 年に米国の応用数学者 Shor によって（古典的な計算機では現実的な時間内に行えない）素因数分解を現実的な時間内に行う著名な Shor の algorithm が考案されると、研究は飛躍的に進展し、2011 年には D-Wave One という世界最初の商用量子計算機が市場に投入された。