高橋秀俊，石橋善弘: 電子計算機によるexactな計算の新方法（mod p 演算の応用）

情報処理，Vol.1, No.2（1960-9），pp.78-86

H. Takahasi and Y. Ishibashi: A New Method for "Exact Calculation" by a Digital Computer（An Application of Modulo p Arithmetics）

Information Processing in Japan, Vol.1（1961），pp.28-42

現在ではmodular arithmeticとかChinese remainder theoremとかいう言葉は計算機科学，数値計算の世界ではよく知られているが，そんなものが単なる数学（整数論）の世界の浮世離れした観念的な遊戯であるかと多くの人が思っていた頃公表された上記の論文は，非常に新鮮な感じを当時我々に与えたのではなかろうか．日本語版，英語版とも表題に示すところにそれぞれ掲載されている．2つの論文は本質的には同内容であるが，説明の仕方や誤植は微妙に両者で異なるところもある（実はそれより前“プログラミングシンポジウム報告集”にもその原型が発表されているそうである）．

ここに展開されている手法は，基本的には，大きな整数の和，差，積をとる演算がそれらを整数pで割ったときの剰余についても同じ形をしているということに注目すれば，剰余を扱うことによってすべてp以下の数だけの計算に帰着できること，そしてpが素数ならばもとの数が割り切れるものならその商の剰余が剰余の方の商に一致するという，数論ではよく知られた事実を高精度計算に利用しようという着想から出発している．pが1つでは仕方ないが，いくつもの素数（それも1語長に収まる範囲でなるべく大きいもの）を使って同時並行に計算するとその結果からもとの数が復活できるという事実があるので嬉しいことになる．この復活法が，Chinese remainder theoremと呼ばれるもので，近頃では“孫氏の定理”という人もいる．ちなみに，和算の“百五算盤”の原理と同じだそうである．斯界では知らない人のない有名なD. E. Knuth: The Art of Computer ProgrammingのVol.2にも「modular arithmeticのいくつかの応用が高橋・石橋の論文にある」というような通り一遍の紹介がある．

しかし，私には，この論文にはそのような通り一遍の理解，紹介で済ますのにはもったいない多くの内容，あるいは示唆が含まれているように見える．さすがに高橋先生は高橋先生である．当時だって，modular arithmeticおよびその応用について似たような着想を持った人がなかったとは言えまい．しかし，この論文には“参考文献”がない．つまり，ごく当たり前の数論の基礎だけ知っていれば分かるように書かれている．故高橋先生はよく言っておられた：「あなたは自分の考えが新しいと思っているかもしれないが，そんなことは文献に書いてあろうがなかろうが誰でもちょっと考えれば分かることですよ．既発表の論文がないということは，その考えが新しいからではなく，あまりにも当たり前のことだからでしょう．」などと．しかし，この論文は違う．ここにはChinese remainder theoremなどと言わずに，より具体的に最も効率よくいくつかの剰余からもとの数を復活する方法が，計算の複雑さの評価とともに，挙げられている．応用として取り上げられている主題は，（1）逆行列の正確な計算法，（2）多項式の積や多項式要素の行列式の高精度計算，（3）整数論的調和解析（これは後にFFTと組み合わせて“Numerical FFT”などと呼ばれるようになる），（4）複素数を用いない複素数計算，であるが，そのいずれについても，慣用的な“多倍長計算”と比べてこの方法がどのように優れているかが具体的に論じられている．つまり，通り一遍の理解を超えて，実際の計算をするときに遭遇する問題点が具体的に簡潔に論じられている．

今でも，いや今だからこそ，このような論文を一読する余裕を我々は持ちたいものである．

（平成14年4月4日受付）

伊理正夫/中央大学理工学部
iri@ise.chuo-u.ac.jp