通信情報保護學會誌
第1卷, 第2號, 1991. 8

정수론 프로그램 및 데이타 베이스의 제안

한 상 근*

필자가 1990년 12월에 교토대학 수리해석연구소(RIMS)를 방문하였을 때 동경 도립대학의 나카무라 켄 교수와 만나서 그가 제안한「정수론의 프로그램과 계산결과에 관한 데이타 베이스」를 구축하는데 협조하기로 하였다.

이 사업의 주된 목적은 우선 쉽지 않은 각종 프로그램의 제작과 복잡한 계산결과를 많은 사람들이 공유하므로써 연구자들이 필요없는데에 시간을 낭비하지 않도록 도와주자는 것이고, 많은 양의 계산결과를 누구나 볼 수 있도록 하므로써 새로운 이론의 발전에 도움이 되고자 하는 것이다.

1991년 1월에 미국 수학회 정기총회에서 만난 A. Odlyzko, K. McCurley, C. Pomerance 등 많은 이들과 의견을 교환해 보았는데, 그들도 대부분의 프로그램을 자기자신, 혹은 조수가 몇개월에 걸쳐서 제작하였으며, 전혀 새로운 알고리듬을 프로그램으로 구현하는 것이 아니라면 이것은 대단한 시간과 노력의 낭비라고 느끼고 있었다.

실제로 필자와 한국과학기술원의 오운용 교수는 Decom이라는 소인수분해 프로그램을 1989년도에 당시 물리학과 4학년 학생이던 이준엽 군의 도움을 받아 제작해 본 경험이 있다. Decom에 사용된 알고리듬은 이미 잘 알려진 P. Montgomery의 효율적인 타원곡선법이었다. 그 당시에도 학생을 괜한 일에 부리는 것이 아닐까 의문을 가지고 있다가 다행하게도 같은 생각을 하고 있던 나카무라 켄 교수와 만나게 된 것이다.

이러한 작업의 필요성을 좀더 이야기하자면 우선 대부분의 논문에서는 프로그램이나 계산결과의 극히 일부분만을 수록하고 있고, 따라서 그런 프로그램이나 계산결과가 정확하다는 것을 보증해야 할 필요성이 대두되었다. 이미 학술지「Mathematics of Computation」에서는 Unpublished Mathematical Table이라는 데이타 베이스를 오래전부터 운영하고 있다.

또한, 이미 알고리듬의 배경이 되는 이론이 잘 알려져 있고, 소스코드 자체를 쉽사리 구해 볼 수 있는데 그런 기존의 알고리듬을 프로그램으로 구현하는 것이 도대체 연구에 무슨 의미가 있는지 생각해 볼 일이다.

상업적 목적을 가진 사람이나 교육적 목적을 가진 경우에만 그런데에 시간과 노력을 쏟는 것이 정당화될 수 있을 것이다. 그리고 그런 상업적 혹은 교육적 목적을 가지고 또다시 프로그램으로 기존 알고리듬을 구현한다고 해도 자신의 프로그램이 기존의

* 정회원, 한국과학기술원 수학과

프로그램보다 성능이 나은지 아니면 못한지를 알려면 기존의 프로그램을 많이 가지고 비교해 볼 수 있어야 할 것이다.

따라서 우리는 (소스코드가 있는) 각종 프로그램과 계산결과들을 수집하고 있으며, 원하는 모든 이들에게 실비로(우편료, 디스켓값 등) 제공하려고 한다.

우리가 요구하는 단 한가지 조건은 반드시 제작한 사람, 제공해준 사람, 수정 보완한 사람의 이름을 반드시 명기해야 한다는 것이다. 그래야만 제작한 사람들이 소스코드를 공개할 것이고, 추후에 저작권 등에 관한 시비가 일어나는 것을 방지할 수 있을 것이다.

현재까지 수집된 자료는 다음과 같다.

1. 소프트웨어 이름 : PARI-GP 용도 : 범용 정수론 팩키지, 정수론의 각종 함수들, 소인수 분해, 타원곡선 위에서의 연산 등등, 사용한 프로그래밍 언어 C, 제작자 : C. Batut, D. Bernardi, H. Cohen, M. Olivier

2. Decomprime, 타원곡선을 이용한 소인수 분해 소프트웨어, 소소코드 없음, 제작자 불명

3. Decom, Pollard 방법과 타원곡선을 이용한 소인수 분해법, FORTRAN과 C, 오윤용, 한상근

4. Numbdroid, 범용 정수론-소수판정, 타원곡선을 이용한 소인수 분해, Shank의 소인수 분해, 연분수 전개, 선형 디오판틴 방정식의 풀이 등등, Turbo Pascal 혹은 UBASIC, D. Malm

필자는 한국과학재단의 지원으로 1991년 6월 중순에 한달 예정으로 동경대학을 방문할 계획이다. 이 때에 동경 도립대의 나카무라 켄 교수와 만나서 이 사업에 대해서 좀더 자세한 이야기를 할 예정이며, 그가 이미 수집해 놓은 자료들을 가지고 올 예정이다. 또한 리쿄 대학의 컴퓨터 연구팀과도 이 사업에 관해서 협의해 볼 예정이다. 귀국한 후 올해 8월부터 배포 가능한 자료는 다음과 같다.

1. KANT, 대수체의 각종 불변량 계산, FORTRAN, M. Pohst, J. Schmettow

2. Multi-precision Package, UBASIC 86(version 8.12)와 소인수 분해 등 응용 프로그램, 키다 유지

3. 각종 암호의 제작 및 해독 프로그램, UBASIC, C, 야마무라 켄

4. 이차체의 아이디얼 클라스 그룹의 계산, VAX/VMS 위의 FORTRAN, 사이토 미치요

5. Multi-precision Package, FORTRAN, R. Brent

6. Pure Cubic Field의 불변량 계산, FORTRAN, 나카무라 켄

7. Real Quadratic Field의 아이디얼 클라스 그룹의 3-Sylow group, FORTRAN, 나카하라 토무

이글을 쓰고 있는 현재 시점에서 수집하려고 연락중인 자료는 다음과 같다.

1. LISP interpreter in the form of algebraic equation, Gödel의 불완전성 정리를 randomness로 증명, C, G. Chaitin

2. CAYLEY, 이산수학 특히 유한군론, C, J. Cannon

3. UBASIC(version 8.15), multi-precision을 포함한 BASIC interpreter, 키다 유지

4. Multi-precision package, 68000 Assembly, D. Bernardi

5. BigNum, 범용 정수론, C, DEC

올해 9월부터는 Number Field Sieve를 이용한 소인수 분해법, Self-initializing Multiple Polynomial Quadratic Sieve를 이용한 소인수 분해법, 타원곡선을 이용한 소수 판정법, Jacobi Sum을 이용한 소수 판정법, 유한체 위에서의 Discrete Logarithm 계산법, Number Field Sieve를 이용한 Discrete Logarithm 계산법, 유한체 위에서의 Sparse Matrix의 연산법, 유한환 위에서의 Sparse Matrix의 연산법 등에 관한 소스코드를 수집할 예정이다.

간혹 RSA나 Discrete Log 암호에 사용할 목적으로 Modular Exponentiation에 대해서 문의하는 분들이 계신데, 그 분들을 위해서 간단히 접할 수 있는 프로그램을 소개하면 먼저 Mathematica라는 범용 팩키지가 있다. 범용인 이상 속도가 그리 빠르지는 않지만 Symbolic Computation이 가능하고 따라서 프로그램을 제작하기가 아주 쉽다. 필자가 영어를장을 RSA 방식으로 암호화하는 프로그램을 만들어 보았는데 Subroutine까지 다 합해도 100줄이

되지 않았다. 좀더 빠른 속도를 원하는 분들에게는 UNIX의 /user/lib에 있는 mp(multiple precision)를 사용해 보기를 권한다.

각종 문의나 요망사항은 필자에게 연락하면 된다. 필자는 컴퓨터 전문가가 아니기 때문에 각종 프로그램들을 컴파일하고 실행해보고 사용 설명서를 만들어 내는데 익숙하지 않다. 따라서 이런 부문에서 필자에게 도움을 줄 수 있는 분들도 언제라도 연락해 주기 바란다.

- 연 락 처 : 대전직할시 유성구 구성동
  한국과학기술원 수학과
  한 상 근
- 우편번호 : 305-701
- 전 화 : 042) 829-2727(사무실)
  042) 829-2702(과사무실)

□ 著者紹介

한 상 근(정회원)

1979年 서울大學 數學科(學士)
1982年 美國 뉴멕시코주립대학 數學科(碩士)
1987年 美國 오하이오주립대학 數學科(博士)
1988年 美國 오하이오주립대학 講師
現 韓國科學技術院 數學科 助教授

관심분야 : 정수론과 그 응용(암호, 부호)