通信情報保護學會誌
第2卷, 第1號, 1992. 3

솟수 판별법(primality test)

최 영 주*

1. 서 론

우리는 종종 "주어진 큰 정수 n이 합성수인가 솟수인가"하는 질문을 하게 된다. 특히 최근들어 소인수 분해법(prime factorization)과 솟수 분별법(primality test)은 보안성 있는 pseudorandom generator, 또한 RSA 공용 키이 암호 시스템(public key cryptosystem)에서나 유한체(finite field) 위에서의 이산대수 문제(discretelog problem)에서의 응용 등 매우 중요한 위치를 차지하게 된다. 정수 n이 합성수 임을 증명하는 것은 비교적 쉬운 일이며 솟수 분별법(primalitiy test)이란 정수 n이 솟수가 아닌 것에 대한 판단 기준(criterion)이다. 솟수 분별법의 최종 목표는 물론 정수 n이 솟수임을 계산적으로 빠른 시간내에 증명하는 것이다.

솟수 분별법에는 크게 확률론적 솟수 분별법(probabilistic primality test)과 결정적인 솟수 분별법(deterministic primality test)이 있는데 확률론적 솟수 분별법은 어떠한 증명이 안된 가정하에서는 주어진 정수 n이 솟수임을 log n의 polynomial time하에 증명할 수 있으나, 일반적으로 어떠한 증명 안된 가정없이 큰 정수 n이 솟수임을 증명하는 것은 어려운 일이다. 현재 정수 n이 솟수임을 증명하는 가장 효과적인 솟수 분별법은 Jacobi sum 테스트와 타원 곡선을 이용한 솟수 분별법이다. 하지만 실질적으로 주어진 정수 n의 솟수 분별을 위해서는 확률론적 테스트를 적용하는 것이 실용적이다.

2. 확률론적 솟수 분별법 (probabilistic primality test)

어떻게 하면 합성수 n을 빨리 효과적으로 구분해 내느냐 하는 것이 이 테스트의 첫번째 목적이다. 정수 n이 솟수인지 아닌지 확인 할 수 있는 가장 기초적인 방법은 n 보다 작은 솟수로 나누어 보는 것이다(trivial division). 하지만 이것은 n이 커지면 trivial division으로 솟수를 구별하는 것은 $\sqrt{n}$ 정도까지의 솟수들로 나누어 보아야 하므로 아주 비효율적인 방법임을 알 수 있다. 일반적으로는 다른 테스트를 적용하기 전에 몇몇 작은 솟수로 나누어 본다. 또 가장 기초적인 확률론적 솟수분별법 중 하나는 Fermat의 little theorem을 이용한 방법인데 그것은 다음과 같다 : 만일 n이 솟수라면 어떠한 정수 a에 대해서도 $a^n \equiv a \pmod{n}$을 만족한다. 그러므로 만일 하나의 정수 a에 대하여 $a^n \not\equiv a$ (mod

* 포항공과대학, 수학과

n)이면 n이 합성수임을 알 수 있다. 이 a를 n이 합성수가 되기 위한 witness라고 부른다. 하지만 이 witness를 찾는 것은 계산적으로 어려울뿐더러 불가능할 경우도 있다. 이런 witness를 갖고 있지 않은 합성수 n을 Carmichael number라 하는데 $n=561=3\times 11\times 17$이 그 예이다.

이런 경우를 피할 수 있는 솟수 분별법이 Miller에 의해 발전 되었다 : 만일 n이 솟수이고 $(n-1=2^k t)$로 표시할 때(t는 홀수), 0과 n 사이의 양의 정수 a에 대해 $a^t\equiv 1 \pmod{n}$, 혹은 0과 k 사이의 수 어떤 i에 대해 $a^{t2^i}\equiv -1 \pmod{n}$이 성립한다함은 증명된 사실이다.

이 사실을 이용한 솟수 분별법을 Miller-Rabin 솟수 분별법이라 하는데 그것은 다음과 같다 :

$n-1=2^k t$로 표시하고(t는 홀수), 0과 n 사이의 양의 정수 a를 무작위로 축출한다. $a^t \pmod{n}$를 계산하여 $a^t\equiv \pm 1 \pmod{n}$을 얻으면 n이 a에 대하여 테스트를 통과한 것이므로 다른 a를 선택하여 되풀이 한다. 만일 $a^t\equiv \pm 1 \pmod{n}$일때 a^t의 제곱을 계속하여 $-1 \pmod{n}$을 얻으면 테스트를 통과한 것이고, 만일 0과 k 사이의 수 어떤 i에 대해 $a^{t2^i}\equiv 1 \pmod{n}$이고 $a^{t2^i}\not\equiv -1 \pmod{n}$이면 n이 합성수임을 보이는 것이다. 이 테스트에 합성수인 홀수 n이 패스할 확률은 $\frac{1}{4}$ 보다 작으므로 r번의 random하게 선택된 수 a에 대해 합성수 n이 패스할 확률은 $\frac{1}{4^r}$ 보다 작음이 알려져 있다. 그러므로 이 테스트를 통과한 정수 n은 솟수일 확률이 크지만 이것이 n이 솟수임을 증명하는 것은 아니다. 이러한 것을 확률적 솟수 분별법이라 하는데 수학적으로 증명이 안된 Generalized Riemann hypothesis하에서는 결정적인 polynomial time 솟수 분별법이 될 수 있다. 즉 Generalized Riemann hypothesis하에서는 만일 n이 합성수이면 witness를 $\{2, 3, \cdots, [2 \log n]^2\}$ 중에서 발견할 수 있다는 것을 증명할 수 있다. 그러나 실질적으로 n이 솟수임을 증명하기 위해서는 결정적인 테스트인 Jacobi sum 테스트와 complex multiplication 테스트가 빠른 것으로 알려져 있다.

그 밖에 n이 특수한 성질을 갖을때, 예를 들어 n−1의 소인수가 알려져 있을 때, 혹은 $n\pm 1$, $n^2\pm 1$, $n^2\pm n+1$등의 소인수가 알려져 있을때 등, n이 솟수라는 것을 증명하는 것은 비교적 쉬운 일이다. 예를 들어 다음과 같은 테스트를 보자. 이 테스트는 n이 Miller-Rabin 테스트를 통과 했을때 주로 적용하는 테스트로 n−1의 소인수들이 알려졌다는 가정하에 이루어진다 : n−1을 나누는 각각의 솟수 p_i에 대해 0와 n 사이의 정수 중 $b_i^{n-1}\equiv 1 \pmod{n}$와 $b_i^{(n-1)/P_i}\equiv 1 \pmod{n}$를 만족하는 정수 b_i를 찾으면 n이 솟수임을 보일 수 있다. 이것은 primitive root를 이용한 것으로 n이 Miller-Rabin 테스트를 통과 했을때 n이 정말 솟수인지 증명하기 위하여 나온 테스트이다.

이런 종류의 테스트를 이용하여 William과 Dubner는 $\frac{(10^{1031}-1)}{9}$ 가 솟수라 함을 증명하였고, 6087 digit수인 $39181\times 2^{216193}-1$가 솟수임을 보일 수 있었으나 이런 방법들로 일반적으로 100 digit 근방의 솟수를 분별해 내는 것은 어려운 일이다.

3. 결정적 솟수 분별법 (deterministic test)

결정적 솟수 분별법이란 주어진 정수 n이 솟수임을 증명하는 것이다. 솟수 분별법으로 특수한 성질을 갖지 않는 일반적 정수 n에 적용할 수 있는 현재 알려진 가장 효율적인 결정적 솟수 분별법은 Jacobi sum 테스트와 타원 곡선을 (elliptic curve)을 이용하는 방법으로 complex multiplication 방법이 있다. 예를 들어 Jacobi sum 테스트는 여러가지 'Fermat-like' 테스트의 합성으로 알려져 있는 것으로 100~200 digit의 솟수를 쉽게 처리할 수 있으며 500 digit의 솟수들도 처리가 가능하다. 그의 running time은 약 $(\log n)^{O(\log\log\log n)}$으로 알려져 있어 현재 알려진 가장 빠른 결정적 솟수 분별법이다. 또 한가지 현재 알려진 효율적인 결정적 솟수 분별법은 타원 곡선을 사용하는 것이다.

타원곡선 E이란 $y^2=Ax^3+Bx+C$의 방정식으로

표시될 수 있는 곡선이다. 이 곡선의 중요성은 곡선위에 있는 유리점들의 집합이 더하기와 비슷한 작용(operation)에 의해 군(group)을 이룬다는 것이다. 곡선상의 유리점, (x, y), 들이란 $y^2=Ax^3+Bx+C$를 만족하고 x와 y의 비가 정수로 나타내질 수 있는 좌표를 의미한다. 만일 곡선 위에 있는 두 유리점들을 택하여 직선을 만들면 그 직선은 곡선 위에 제 삼의 유리점과 만나게 된다. 군의 작용(group operation)에 의해 이 한직선상에 있는 세 점(colinear point)을 더하면 O (identity)가 된다. 곡선 위에 있는 점 P_1과 P_2에 대하여 군의 작용 *를 적용하면, $P_1 * P_2$란 P_1과 P_2를 잇는 직선과 타원곡선의 제 3 의 만나는 점을 구해 그 점을 지나는 수직선을 그어 타원 곡선과 또 다시 만나는 점을 일컫는다. 유한체(finite field) 위에서 타원곡선의 군의 성질을 이용하여 솟수 분별법과 소인수 분해법이 발전하였다. 타원곡선을 이용한 솟수 분별법은 경험적 방식(heuristic argument)에 의해 running time이 log n의 polynomial time이 걸린다함을 알 수 있으나, 불행히도 이것이 아직 수학적으로 증명이 되지는 않았고, 적당한 양의 상수 c에 의존하는 솟수 분포의 가정하에서 running time이 약 $O(\log n)^{9+c}$이 됨을 알 수 있다. 또한 타원곡선 중 complex multiplication이라는 좋은 성질을 갖는 곡선이 있는데, 이것을 이용한 솟수 분별법을 complex multiplication 테스트라 부르며, 경험적 방식(heuristic argument)에 의해 running time이 lon n의 polynomial time이 걸린다함을 알 수 있으며, 즉 running time이 $O(\log n)^{6+\varepsilon}$, $\varepsilon>0$임을 알 수 있다.

참 고 문 헌

1. H. Cohnen and A. Lenstra, "Implementation of a new primality test," Math. Comp. 48, 103-121, 1987.
2. N. Koblitz, A course in number therory and cryptography, Springer-Verlag, 1987.
3. E. Kranakis, Primality and cryptography, John Wiley & Sons, 1986.
4. A. Lenstra, "Primality testing," Cryptology and computational number theory, proc. of symposia in applied math. Vol. 42, 13-25, 1990.
5. C. Pomerance, recent developments in primality testing, Math. Intelligencer 3, 1981.

□ 著者紹介

최 영 주

本 學會「論文誌」創刊號 參照