韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

연분수와 암호학

조 인 호*

1. 서 론

연분수는 두 정수의 최대공약수를 구하는 Euclidean algorithm을 적용할 때 자연스럽게 생겨나는 것으로서 방정식의 해와 관련하여 19C 정수론에서 중요한 도구가 되었으며 최근 암호학과 관련된 소인수분해의 응용[2], RSA 비밀키 발견에의 응용[5], 난수열의 발생 및 선형 복잡도 분석에의 적용[3,4] 때문에 새로이 주목받고 있는 정수론의 분야이다. 본 논문의 목적은 이와 관련하여 연분수를 소개하고 연분수의 몇가지 응용을 설명하는데 있다. 2절에서는 연분수의 개념과 중요 성질들을 소개하고 3절에서는 Eurocrypt'89에서 M. J. Wiener가 제시한 연분수를 이용한 RSA 비밀키 발견법을 설명하려 한다. 4절에서는 Legendre가 제시하고 Morrison, Brillhart 등에 의해서 개선 구현[2]된 연분수를 이용한 소인수분해법을 소개하고자 한다.

이 논문에서 소개하지는 않지만 Niederreiter가 Eurocrypt'88에서 제시한 연분수를 이용한 난수열의 선형복잡도 분석 또는 암호에 관심을 가진 분에게는 매우 흥미가 있을 것이다.

2. 연분수의 정의와 중요한 성질들

67과 24의 최대공약수를 구하는 Euclid법은 다음과 같다.

$$67=2\times 24+19$$
$$24=1\times 19+5$$
$$19=3\times 5+4$$
$$5=1\times 4+1$$

이제 이것들을 분수 형태로 고치면

$$67/24=2+(19/24)$$
$$24/19=1+(5/19)$$
$$19/5=3+(4/5)$$
$$5/4=1+(1/4)$$

이와 같이 된다. 따라서,

$$67/24=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+1/4}}}$$

와 같이 표시할 수 있다.

위와 같은 표현을 (67/24)의 연분수 전개(continued fraction expansion)라고 하며 편의상

$$2+\frac{1}{1+}\ \frac{1}{3+}\ \frac{1}{1+}\ \frac{1}{4+}$$

또는 [2, 1, 3, 1, 4]와 같이 표시한다. 또한 2, 1, 3,

* 정회원, 고려대학교 수학과

1, 4를 67/24의 부분 몫(partial quotient)라고 한다.

유리수는 연분수의 전개를 하면 위와 같이 유한개의 부분 몫을 갖는 유한 연분수 전개가 가능하지만 무리수(irrational number)의 경우에는 다양하게 나타난다.

예를 들면,

$\sqrt{3}=[1,\bar{1},\bar{2}]=[1,1,2,1,2,\cdots]$

$\pi=[3,7,15,1,292,1,292,1,\cdots]$

$e=[2,1,2,1,1,4,1,1,6,\cdots]$

와 같이 된다. $\sqrt{3}$과 같은 이차 무리수(quadratic irratioal)의 경우에는 위와 같이 주기성이 나타나지만(Lagrange) 일반적 무리수에 대해서는 중요성에도 불구하고 연분수전개에 대해 알려진 것이 별로 없다.

이제 일반적인 연분수를

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cdots}}}=[a_0,a_1,a_2,a_3,\cdots]$$

라 하면 다음 정리가 성립한다.

정리 1. 수열 $a_0, a_1, a_2, \cdots$가 주어졌을 때 $n=0,1,2,\cdots$에 대해

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix}\cdots\begin{bmatrix} a_n & 1 \\ 1 & 0 \end{bmatrix}=\begin{bmatrix} b_n & b_{n-1} \\ c_n & c_{n-1} \end{bmatrix} \quad \langle=\rangle\ b_n/c_n=[a_0,a_1,\cdots,a_n]$$

가 성립한다.

위에서 행렬식을 취하면 우리는,

$b_nc_{n-1}-b_{n-1}c_n=(-1)^{n-1}$ 또는

$b_n/c_n=b_{n-1}/c_{n-1}+(-1)^{n-1}/c_{n-1}c_n$

을 얻게 된다. 따라서 $b_n/c_n=a_0+1/c_0c_1-1/c_1c_2+\cdots+(-1)^{n-1}c_{n-1}c_n$이므로 우리는 수열 b_n/c_n이 $\alpha=a_0+\sum_{n=1}^{\infty}(-1)^{n-1}/c_{n-1}c_n$

에 수렴하는 것을 알 수 있다.

이런 까닭에 b_n/c_n을 α의 convergent라 부른다.

무리수에 수렴하는 유리수열은 여러 방법으로 구할 수 있지만 연분수전개를 통하여 구한 convergent의 수열은 수렴 속도가 가장 빠르기에 중요하게 쓰인다. 예를 들어

$\pi=[3,7,15,1,292,1,\cdots]$에서 $[3,7]=22/7$

$[3,7,15,1]=355/113$이고 $|\pi-1355/113|<1/(292\cdot 113^2)$이므로 335/113은 π에 대한 유리 근사치(rational approximation)로 널리 쓰이고 있다.

다음의 정리는 3절에서 다루고 있는 Wiener의 RSA 비밀키 분석에 중요하게 쓰인다.

정리 2. $|c\alpha-b|<1/2c$이면 b/c는 α의 convergent이다.

3. 연분수의 RSA 비밀키 발견에의 응용

e를 공개키, d를 비밀키 그리고 $n=pq$를 갖는 RSA 암호계가 있다고 하자. M. J. Wiener는 Eurocrypto'89에서 $d<n^{1/4}$이면 $f=e/n$를 연분수 전개해 나가는 과정에서 d를 구할 수 있다는 것을 보였다. 이제 그 과정을 약술해 보겠다.

$ed\equiv 1 \pmod{\mathrm{lcm}(p-1,\ q-1)}$로 부터

$$ed=\frac{k}{g}(p-1)(q-1)+1 \quad (*),$$

$$g=\frac{(p-1,q-1)}{(K,(p-1,q-1))},$$

$$k=\frac{k}{(K,(p-1,q-1))},$$

$$K=\frac{ed-1}{\mathrm{lcm}(p-1,q-1)}$$

이 유도된다. 따라서, dn으로 나누면

$$\frac{e}{n}=\frac{k}{dg}(1-\varepsilon),$$

$$\varepsilon=\frac{p+q-1-g/k}{n}$$

가 된다.

여기에서 분수 $f'=e/n$는 $f=k/dg$에 아주 가깝고 $kd/g<<n^{1/2}$이면 정리 2에 의해서 f는 f'의 convergent가 된다. 따라서 $d<n^{1/4}$인 경우에는 f'의 연분수 전개를 통해서 convergent를 구해나가면 polynomial time내에 f 도달함으로서 d를 추정해 낼 수 있게 된다.

한편, $ed>n$이면 $k>g$이고 (*)로부터 edg를 k로 나누면 몫이 $(p-1)(q-1)$이고 나머지 g가 되므로 $(p-1)(q-1)$과 g를 추정할 수 있다. 또한 $1/2(n-(p-1)(q-1)+1)=1/2(p+q)$는 정수가 되어야 하고 $(1/2(p+q))^2-n=(1/2(p-q))^2$는 정수의 제곱이 되어야 한다. 이 조건들이 만족되지 않는다면 추정이 잘못된 것이므로 알고리즘을 반복해서 조건을 만족하는 것을 구하고 비밀키 d는 convergent의 분모가 dg이므로 분모를 g로 나누어서 구할 수 있게 된다. 연분수 알고리즘은 다음과 같다.

$f'=[a_0', a_1', \cdots, a_n']$라 하면,
repeat until f is obtained
  generate the next quotient a_n' of the continued fraction expansion of f;
  construct the fraction that equals
    $[a_0', a_1', \cdots, a_{n-1}, a_n'+1]$ for i even
    $[a_0', a_1', \cdots, a_{n-1}, a_n']$ for i odd
  check whether this fraction equal f.

이제 간단한 예를 들어 알고리즘을 설명해 보자.

예. $n=10541$, $e=4133$일 경우 d를 추정해 보자. $f'=4133/10541$의 연분수 전개를 통하여 d를 다음과 같이 추정한다.

Quantity	Iteration		
	i=0	i=1	i=2
a_i'	0	2	1
r_i'	4133/10541	2275/4133	1858/2275
n_i'/d_i'	0/1	1/2	1/3
guess of k/dg	1/1	1/2	2/5
guess of edg	4133	8266	20665
guess of $(p-1)(q-1)$	4133	8266	10332
guess of g	0	0	1
guess of $(p+q)/2$	3204.5	1138	105
guess of $[(p-q)/2]^2$ d		1133.36	$484=22^2$ $5/1=5$

따라서, $d=5$, $p=127$, $q=83$이고 $k=2$, $q=1$임을 알 수 있다.

위와 같은 공격법을 피하기 위해서는 Wiener는 $edf\simeq kn$이므로 $e>n^{1.5}$를 택하면 k가 커져서 위의 방법의 시행시간이 polynomial time을 넘게 할 것을 제안하였다.

4. 연분수의 소인수분해에의 응용

큰 정수 n이 주어졌을 때 n을 소인수분해하는 대표적인 방법은 facter base를 정한 후 이것을 이용하여 이차합동식 $x^2\equiv y^2 \bmod n (x>>y)$을 만들어서 $(x\pm y, n)$을 구하는 것으로 평가받고 있는 MPQS, NFS 등이 이 계열에 속한다.

이 점에서는 1975년 Morrison과 Brillhart가 개선 구현한 연분수를 이용한 factor base 계열의 알고리즘을 설명하려고 한다.

정리 3. n이 양의 정수이고 b_i/c_i가 $\sqrt{n}$의 convergent라면,
$b_i^2 \bmod n (-n/2<b_i \bmod n<n/2)$은 $2\sqrt{n}$ 보다 작다.

정리 1에 의해서 b_i와 $b_i^2 \bmod n$을 구할 수 있고 $b_i \bmod n$은 정리 3에 의해서 아주 작은 잉여가 되므로 적당한 것들을 곱해서 이차합동식을 만들 수 있다.

예를 들어 설명해 보자.

예) $n=9073$을 소인수분해하기 위해서 $\sqrt{n}$의 연분수 전개를 하면 다음과 같다.

i	0	1	2	3	4
a_i	95	3	1	26	2
b_i	95	286	381	1119	2619
$b_i^2 \bmod n$	−48	139	−7	87	−27

$-48=(-1)\times 2^4\times 3$ $-27=(-1)\times 3^3$이므로
$(95\times 2619)^2=95^2\times 2619^2\equiv(-1)^2\times 2^4\times 3^4\equiv(2^2$

$\times 3^2)^2 \bmod n$이 된다.

$x=95\times 2619 \equiv 3834 \bmod 9073$, $y=2^2\times 3^2=36$으로 택하면 $x^2 \equiv y^2 \bmod n$이고 $x \not\equiv \pm y \bmod n$이다.

그리고 $(3834+36, 9093)=43$이다. 이렇게 하여 $9073=43\times 211$을 얻게 된다.

참 고 문 헌

1. H. Darenport, The Higher Arithmatic, 5nd ed., Cambridge University Press, 1982.

2. M.A. Morrison and J. Brillhart, A mothod of factoring and the factorization of F*, Mathematics of Computation, Vol. 29, 1975, 183-205.

3. H. Niederreiter, The probabilistic theory of linear complexity, Advances in cryptology, Eurocrypt' 88, Lecture Note in Computer Science 330, 1988, 191-209, Springer-Verlag, Berlin.

4. H. Niederreiter, The linear complexity profile of keystream sequences, Proc. workshop on Stream Ciphers, 1989 Karlstruhe.

5. M.J. Wiener, Cryptanalysis of short RSA secret exponents, Eurocrypt'89, 1989, Houthalen, Belgium.

□ 著者紹介

趙 寅 鎬(正會員)

高麗大學校 理科大學 數學科(學士)
高麗大學校 大學院 數學科(代數學 碩士)
高麗大學校 理科大學 講師/독일 뮌헨대학교 수학과(Dr. rer. nat)
서울大學校 大學院 講師/梨花女子大學校 數學科 助教授
大韓數學會 無任所 理事
大韓數學會 會誌 編輯委員/大韓數學會 監査
現 高麗大學校 理科大學 數學科 教授/韓國通信情報保護學會 副會長