情報保護學會論文誌
第20卷 第3號, 2010. 6

페르마 인수분해 방법의 확장과 검증에 대한 고찰*

정 서 현,† 정 수 환‡
숭실대학교

A Consideration on Verification and Extension of Fermat's Factorization*

Seohyun Jung,† Souhwan Jung‡
Soongsil University

요 약

인수분해에 관한 여러 가지 전수공격이 알려져 있다. 페르마의 인수분해 방법은 여러 가지 공격 중에 두 인수가 비슷한 크기인 경우에 가장 잘 동작한다고 알려져 있다. 본 논문에서는 페르마의 방법이 위와 같은 상황에서 잘 동작하는지 보이고, 그 해가 유일함을 증명한다. 이러한 증명을 이용하여 임의의 시작점에서 페르마의 정리를 시작 할 수 있다. 또한 본 증명은 "인수분해하다" 는 명제와 "제곱수를 찾다"라는 명제가 동일함을 의미한다.

ABSTRACT

There are some efficient brute force algorithm for factorization. Fermat's factorization is one of the way of brute force attack. Fermat's method works best when there is factor near the square-root. This paper shows that why Fermat's method is effective and verify that there are only one answer. Because there are only one answer, we can start Fermat's factorization anywhere. Also, we convert from factorization to finding square number.

Keywords: Fermat, factorization, square root

I. 서 론

빠른 인수분해 문제는 아직까지 풀리지 않은 난제로 남아 있다. 따라서 이를 기반으로 한 암호알고리즘들이 아직까지 상대적으로 안전하다고 알려져 있다. 현재까지 소수와 관련되어 소수 판정 알고리즘으로 Eratosthenes방법, Fermat방법, Wilson방법[1], APR방법, Solovay-Strassen방법[2], Lehman-Peralta 방법, Miller-Rabin 방법[3~4]이 있고, 소인수 분해 알고리즘으로는 Eratosthenes방법, Fermat방법, Pollard Rho방법[5], Pollard p-1 방법 등이 알려져 있다. 그중 페르마[6]의 인수분해 방법은 두 인수가 비슷할 때 빠른 인수분해 방법을 제시한다. 하지만 알고리즘이 가지는 장점에 대한 정확한 해석과 역 성립과정에 대한 검증이 충분하지 않다.

이미 몇몇 논문에서는 페르마의 알고리즘에서 요구하는 완전제곱수에 관한 연구를 개재한 바이지만, 완전제곱수 조건이 성립할 때 인수분해 성공여부에 관한 증명, 즉 역 성립에 관한 논리적 연결이 부족한 상태이다. 따라서 본 논문에서는 페르마 인수분해에서 변수가 가지는 의미를 상이한 방법으로 해석하고, 역으로 사용이 타당함을 보임으로써, 인수분해문제가 제곱근을 찾는 문제로 귀결될 수 있음을 보인다.

본 논문의 구성을 다음과 같다. 2장에서는 페르마 정리에 관해서 요약 및 분석하고 관련지식을 살펴보도록 한다. 이어서 3장에서는 분석을 위하여 사용될 수학적 알고리즘을 소개하고, 4장에서는 이를 이용하여 역이 성립함을 보인다. 마지막으로 5장에서 본 논문의

접수일(2009년 7월 13일), 수정일(1차: 2009년 11월 3일, 2차: 2009년 12월 21일), 게재확정일(2010년 4월 15일)
* 본 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행하였습니다.
(No. 2010-0000100)
† 주저자, iseohyun@cns.ssu.ac.kr
‡ 교신저자, souhwanj@cns.ssu.ac.kr

결말을 맺는다.

II. 관련 연구

2.1 페르마의 인수분해 방법

본 논문의 근간이 되는 페르마의 인수분해에 관하여 설명하면 다음과 같다[7~8]. $n=ab$ 로 정의 되는 합성수라 하면 n은 t^2-s^2 (t와 s는 정수) 와 같이 나타낼 수 있다. t와 s를 $t=(a+b)/2$, $s=(a-b)/2$ 로 정의 하면 $t^2-s^2=n$이다. 주어진 n을 인수분해하기 위하여 이들 t와 s를 구하는 알고리즘은 [표 1]과 같다.

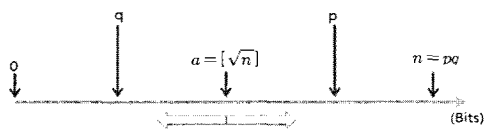
[표 1] 페르마의 인수분해 순서

1 단계 : n이 완전제곱수이면 끝내고, 아니면 t를 n의 제곱근 보다 큰 가장 작은 수라 하자.
2 단계 : $z=t^2-n$이라 놓자
3 단계 : z가 완전 제곱수이면 $n=t^2-s^2$ 이므로 끝내고 아니면 4단계로 간다. ($z=s^2$)
4 단계 : $t=t+1$로 놓고 2단계로 돌아간다.

2.1.1 변수의 의미와 구성

페르마의 인수분해 방법이 수행되는 방법에 대해서는 잘 알려져 있으나 두 수가 비슷할 때 알고리즘의 수행이 빠른 이유에 관한 해석이 없다. 따라서 두수가 비슷한 경우 인수를 찾는다는 가정에서부터 알고리즘의 설계를 시작하여, 비슷한 결론의 수식이 생성됨을 보이고, 결론적으로 페르마 알고리즘이 두수가 비슷할 때 효과적임을 보이도록 한다.

$p\times q=n$이고, a는 n의 제곱근에서 정수부($\lfloor\sqrt{n}\rfloor$)라고 정의 한다. [그림 1]에서 a와 p와의 사이를 x라고 정의 하였다. $n=a^2+c$로 표현 할 수 있다.



[그림 1] 변수의 정의

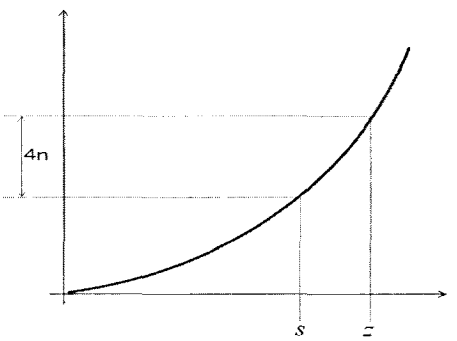
각 변수의 정의에 의하여 정의 된 식을 x에 대하여 정리하면 다음식이 성립한다.

$$c\equiv((a+x)-a)((a+x)+a)=x(2a+x)$$
$$x^2+2ax-c\equiv 0 \pmod p \quad (1)$$

식 1을 만족하는 해를 s라고 정의하고, 근의 공식으로 풀이한다. 우리가 구하고자 하는 방정식은 p와 q에 관한 식이므로 p에 관하여 정리하면 다음과 같다.

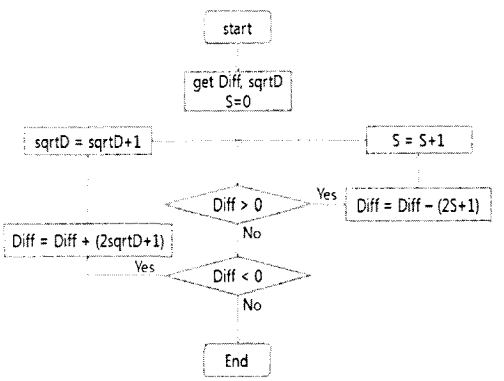
$$x^2+2ax-c=s(a+x)$$
$$x=\frac{-2a+s+\sqrt{D}}{2} \quad (2)$$
$$D=s^2+4n \ \in\text{어떤수}(z)\text{의제곱} \quad (3)$$
$$p=\frac{s+\sqrt{D}}{2} \quad (4)$$

식 3에 대하여 적당한 s값을 구해서 $4n$을 더한 값이 어떤 수의 제곱이 된다면, 구해진 두 수를 이용하여 근을 구할 수 있다.



[그림 2] 두 값(s, $\sqrt{D}$)가 가지는 기하학적 해답

두 값을 구하기 위해 적당히 두 값을 늘리거나 줄일 필요가 있다. 알고리즘으로 나타내면 다음과 같다.



[그림 3] 전체 알고리즘

2.1.2 변수의 의미 해석

$0<q<a<p<n$인 관계에서 q에 대하여 다음 공식이 성립한다.

$$n \equiv a^2 + c \pmod{q} \tag{5}$$

같은 방식으로 $q=a-y$로 정의하고 식 5의 공식을 풀면 다음과 같은 결론을 얻을 수 있다.

$$c \equiv (q-a)(q+a) \equiv -y(2a-y) \pmod{q}$$

$$y^2 - 2ay - c = k(a-y) \ , k \in Z$$

$$q = a - y = \frac{k + \sqrt{D}}{2} \tag{6}$$

식 6에서 q가 양수이기 때문에 $\sqrt{D}$는 양수이다. 또한 $k=s$라면 $p=q=a$가 되므로 $p \neq q$가 성립하려면 $k \neq s$임을 알 수 있다. 식 6에서 $k < \sqrt{D} = \sqrt{k^2+4n}$이므로 $-k$에 대해서도 항상 q가 양수이다. $k=-s$로 정의 될 때 다음과 같이 정의 될 수 있다.

$$q = \frac{-s + \sqrt{D}}{2} \ , \ p = \frac{s + \sqrt{D}}{2} \tag{7}$$

$$s = p - q \ , \ \sqrt{D} = p + q \tag{8}$$

반드시 $k=-s$라는 정의를 성립 할 수 없으며, 본 논문에서는 p와 q가 소수일 때 식 3이 유일한 해를 가짐을 보임으로써, p와 q가 소수일 때 반드시 $k=-s$임을 증명하였다.

2.2 완전 제곱수를 찾는 알고리즘

페르마의 인수분해 방법이 제시하고 있는 단계 중 3 단계에서 Z가 완전 제곱수의 판별을 하나의 단계로 기술하고 있으나, 실제로 어떻게 판별 할 것인가에 대한 기술은 없다. 따라서 몇 가지 연구에서 완전제곱수를 찾는 방법을 제시하고 있다[9].

어떠한 수로 나머지 연산을 취했을 때 완전제곱수는 몇 개의 특정한 나머지를 갖는 특징을 보인다. 만약 나머지가 해당사항에 있지 아니할 때는 완전제곱수임을 확인하는 전체 알고리즘을 구현할 필요가 없어진다. 다음은 그 예를 모아둔 것이다.

〔표 2〕 나머지 연산을 적용했을 때, 완전제곱수의 나머지

modulo 20	0, 1, 4, 5, 9, 16
modulo 16	0, 1, 4, 9
module 9	0, 1, 4, 7

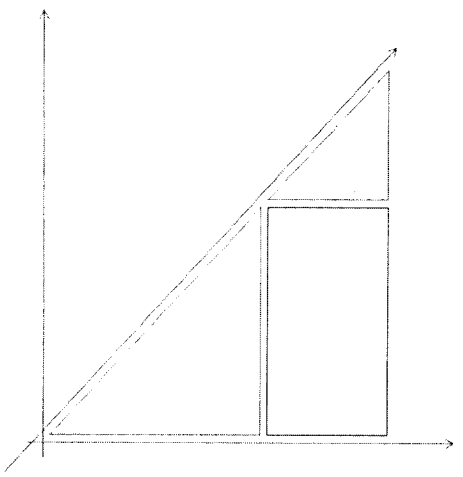
페르마의 인수분해 방법을 적용한다고 했을 때, n (mod 20, 16 또는 9)에 대한 값이 정해지므로 페르마의 인수분해 알고리즘의 2단계의 식에 들어갈 수 있는 수가 제한적이 된다.

III. 검증을 위한 수학적 도구

식을 분석하기에 앞서 완전 제곱수가 되는 수열들이 가지는 특징을 분석할 필요가 있다. 다음은 초기 수열이 가지는 특징을 분석한 표이다.

〔표 3〕 완전 제곱수 누적관계 예시

n	n^2	$i_n = n^2-(n-1)^2$	$\sum_{k=1}^{n} i_k$	=
1	$1^2=1$	1	1	1
2	$2^2=4$	3	1+3	4
3	$3^2=9$	5	1+3+5	9
4	$4^2=16$	7	1+3+5+7	16
5	$5^2=25$	9	1+3+5+7+9	25



〔그림 4〕 수학적 도구로써 기하학적 표현방법

〔표 3〕의 내용을 바탕으로 〔그림 4〕를 작성하였다. 〔그림 4〕에서 x축은 〔표 3〕의 n에 해당하고 y축은 n^2에 해당한다. 커다란 삼각형의 넓이는 완전 제곱수의

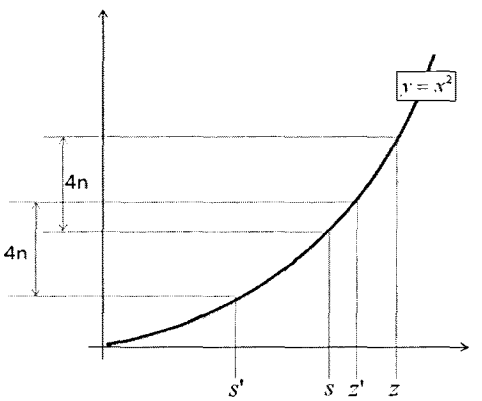
크기를 의미하고 x축은 제곱수의 제곱근을 의미한다. 커다란 삼각형은 두 개의 작은 삼각형과, 하나의 직사각형으로 이루어져 있고, 2개의 작은 삼각형은 커다란 삼각형과 닮음이므로, 작은 삼각형의 넓이는 완전제곱수가 된다. 각각의 작은 넓이들을 더하면 큰 넓이가 되므로 다음 식이 성립한다.

$$x^2 = y^2 + 2y(x-y) + (x-y)^2 \tag{9}$$

IV. 역 성립 과정 검증

알고리즘이 $s^2 = \sqrt{D}^2 - 4n$를 만족하는 수를 찾았을 때, 찾아진 s와 $\sqrt{D}$의 값으로 인수분해가 가능하다고 하였다. 하지만 찾은 두 값이 두 인수와 관계가 없을 수도 있다. 만약, 관계없는 두 수가 찾아진다고 했을 때, 제시된 알고리즘이 엉뚱한 결과를 초래할 수도 있기 때문에, 또 다른 해가 존재 하지 않음을 증명해야 한다.

다른 해가 존재할 경우에 대한 해석은 [그림 5]와 같다. 찾고자 하는 두 값 $(s, Z=\sqrt{D})$를 적당히 조절하여 $Z^2 - s'^2 = 4n$을 만족하는 경우이다.



[그림 5] 다른 해를 만족하는 경우

$(\frac{p+q}{2})^2 - (\frac{p-q}{2})^2 = pq$으로 정의 되므로 $Z^2 - s'^2 = 4n$이 되는 최소 1개의 식이 존재한다. 먼저 최소의 경우부터 시작하여 하나의 정당한 식을 찾았다고 가정하고 [그림 5]와 같이 s와 z를 적당하게 조절하여 또 다른 해를 찾는다고 가정해 보자. 찾은 해는 가장 작은 해가 된다. [그림 5]에서의 $s \to s$, $Z \to \sqrt{D}$로 치환되고, [식 3]에 의해서 다음이 성립한다.

$$4n = 2s(\sqrt{D}-s) + (\sqrt{D}-s)^2 \tag{10}$$

$\sqrt{D}-s=k$로 정의한다.

$$4n = 2sk + k^2 \tag{11}$$

조건이 만족하는 (k,s)쌍과 또 다른 조건을 만족하는 쌍 (k',s')가 있다고 가정할 때 두식의 좌변은 모두 $4n$이 되어야 하므로 다음식이 성립한다.

$$4n = 2sk + k^2 = 2s'k' + k'^2 \tag{12}$$

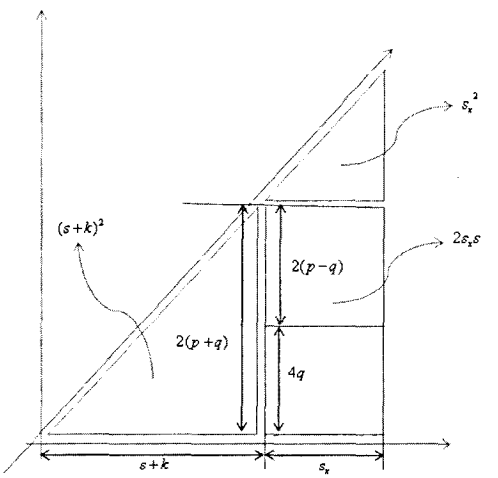
k'과 s'은 각각 k와s에서의 이동이므로 $k' = k + k_x$, $s' = s + s_x$으로 정의한다. 각각을 대입해서 n으로 정리하면 다음과 같다. 단, $k_x, s_x \neq 0$이라고 가정한다.

$$k_x = -(s + s_x + k) + \sqrt{(s+s_x)^2 + 2sk + k^2} \tag{13}$$

식 12에서 (k',s')쌍이 존재하기 위해서는 식 13에서 우변 2항인 $\sqrt{(s+s_x)^2+2sk+k^2}$가 정수이어야 한다. 식 13의 우변 2항이 정수이기 위한 조건을 만족하는지 알아보기 위하여 다음과 같이 식을 수정할 필요가 있다.

$$\sqrt{(s+s_x)^2+2sk+k^2} = \sqrt{(s+k)^2 + 2s_x s + s_x^2} \tag{14}$$

s와 k에 관하여 $s+k=p+q$, $s=p-q$ 이므로 다음 [그림 6]이 성립한다.



[그림 6] $\sqrt{(s+k)^2+2s_x s+s_x^2}$ 해석

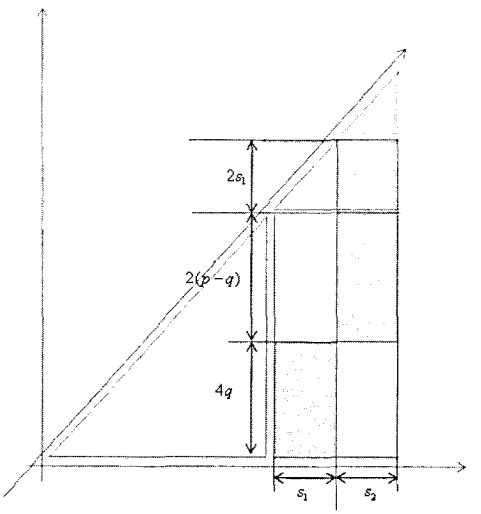
$4q=2(p+q)-2(p-q)$이고 [그림 7]과 같이 $s_x=s_1+s_2$ 라고 정의 될 때,

$$4qs_1=2s_1s_2+2s_2(p-q)+s_2^2 \quad (15)$$

식 15에서 $\gcd(s_1,s_2)=t$ $(t\geq 1, t\in Z)$라고 정의하고, $s_1'=ts_1$, $s_2'=ts_2$로 대입한다.

$$4qs_1'=s_2'(2ts_1'+2(p-q)+ts_2') \quad (16)$$

식 16에서 s_2'는 s_1'와 서로소이므로 s_1'인자를 갖지 않는 q,2q 또는 4q의 값을 가져야만 한다. 각각의 경우에 다음과 같이 요약되는데, 식 17, 18, 19는 각각 $s_2'=q$일 때, $s_2'=2q$일 때, $s_2'=4q$일 때이다.



[그림 7] 제곱수 만족을 위한 조건
(보라색 영역의 넓이 = 붉은색 영역의 넓이)

$$(4-2t)s_1'=2p+(t-2)q \quad (17)$$

$$(1-t)s_1'=p+(t-1)q \quad (18)$$

$$(1-2t)s_1=2p+(4t-2)q \quad (19)$$

최소의 해로부터의 거리 s_x는 항상 양수이므로 s_1'는 항상 양수이고, $p>q$이므로 식 17에서 t=1일 경우를 제외하고는 모두 성립하지 않는다. 식 17에서 t=1일 경우

$$s_1'=p-\frac{q}{2} \quad (20)$$

이므로 s_1'이 정수가 아니므로 해가 존재하지 않는다. 따라서 모든 $s^2=\sqrt{D}^2-4n$에 관하여 단 한 개의 해만이 존재한다.

V. 결 론

근래에 많이 쓰이는 RSA를 바탕으로 하는 PKI 시스템은 인수분해라는 난제를 기반으로 설계되었다. 본 논문에서 많은 인수분해 방법 중에서 페르마의 인수분해 방법에 대하여 고찰하였다. 페르마의 인수분해 방법은 두 인수가 비슷한 경우에 인수분해가 빠르다고 알려져 있다. 페르마의 인수분해 방법은 "인수는 특정 제곱식으로 주어진다."라는 명제에서 시작하는데 본 논문에서는 이를 역을 증명함으로써 페르마 정리에 사용된 인수분해 과정과 제곱수 찾기라는 문제가 동치임을 보였다. 또한 본 논문에서는 제곱수와 또 다른 제곱수와의 관계를 기하학적으로 기술하여 정확하면서도 빠르게 제곱수의 조건을 판별하는 방법을 제시하였다. 이와 같은 논리적 기반은 페르마의 인수분해 방법이 임의의 시작점 설정이 가능함을 제시한다. 한 발 더 나아가 임의의 시작점 보다 작거나 큰 부분에 해가 존재하지 않는다는 것을 증명한다면 보다 효율적인 인수분해가 가능하게 된다는 결론을 얻게 된다.

참고문헌

[1] G. Wilson, "Factorization of the covariance generating function of a pure moving average process," SIAM J. Numer. Anal. pp. 1-7, Mar. 1969.

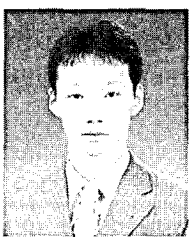
[2] R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," SIAM Journal on Computing, vol. 6. no. 1 pp. 84-85, 1977.

[3] O. Rabin, "Probabilistic algorithm for testing primality," Journal of Number Theory, vol. 12, no. 1, pp. 128-138, Feb. 1980.

[4] C. Mcintosh, "Finding prime numbers : Miller rabin and beyond," Furman University Electronic, vol. 12, pp. 1-4, 2007.

[5] E. Bach, "Toward a theory of Pollard's rho method," Information and Computation, vol. 90, no. 2, pp. 139-155, Feb. 1991.
[6] 김종국, "Fermat의 定理에 關한 硏究," 박사학위 논문, 성균관대학교, 1989년 8월.
[7] 이민섭, 현대암호학, 2판, 敎友社, pp. 272-292, 2007년 3월.
[8] J. McKee, "Speeding Fermat's factoring method," Mathematics of Computation, pp. 1729-1737, Mar. 1999.
[9] D.M. Burton, Elementary number theory, McGRAW HILL, pp. 82-88, Sep. 1998.

〈著者紹介〉



정 서 현 (Seohyun Jung) 정회원
2009년 2월: 한국대학교 전자공학과 졸업
2009년 3월~현재: 숭실대학교 전자공학과 석사과정
〈관심분야〉 정보보호, 차량 네트워크 보안, IPTV 보안

정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 학사
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임 연구원
1996년 6월: University of Washington 박사
1996년~1997년: Stellar One S/W Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 교수
2009년 3월~현재: 지식경제부 지식정보보안 PD
〈관심분야〉 이동 네트워크 보안, VoIP보안, 차량 네트워크 보안, RFID/USN 보안