通信情報保護學會論文誌
第2卷 第1號, 1992. 6

타원 곡선 $Y^2 = X^3 + DX$의 한 응용

한 상 근*

An application of the elliptic curves $Y^2 = X^3 + DX$

Sang-Geun Hahn

요 약

제목에 주어진 타원 곡선들 $Y^2 = X^3 + DX$은 허수 승법을 가진다. 이 곡선을 소수 증명과 소인수 분해에 응용하는 방법을 이 논문에서 고찰해 본다.

Abstract

The elliptic curves $Y^2 = X^3 + DX$ in the title have a complex multiplication. In this paper we consider its applications to the primality proof and prime factorization.

n이 합성수라고 하자. 이 수의 소인수 분해가 찾아내기 어렵다고 가정하자. 따라서 일반적으로 이 수 n은 홀수라고 놓을 수 있다. $n \equiv 1$ mod 4이면 Jacobi symbol$(-1/n)$의 값은 1이다. 그러나 Jacobi symbol$(-1/n)$의 값이 1이라고 해도 합동식

$$X^2 = -1 \bmod n$$

이 근을 가지지 않을 수 있다. 이러한 사실은 다음과 같은 간단한 합동식

$$X^2 = -1 \bmod 21$$

이 근을 가지지 않음을 확인해 보면 알 수 있다.

Jacobi symbol(a/n)의 값이 1인 정수 a가 주어졌을 때, a가 제곱잉여(quadratic residue, QR) 인지 비 제곱 잉여(quadratic non-residue, NR)인지를 알아내기 어렵다는 가정하에서 양자 암호(quantum cryptography)가 제안 되었다. 여기서 부터는 $a = -1$일 때를 살펴 보기로 하자. 합동식 $X^2 = -1 \bmod n$의 근을 알면 합동식

$$X^2 + Y^2 = 0 \bmod n$$

* 한국과학기술원 수학과 부교수 통신정보보호학회 종신회원

의 근을 하나 알 수 있고, 역으로 합동식 $X^2 + Y^2 = 0 \mod n$의 근 (x, y), $GCD(xy, n) = 1$을 하나 알면 합동식 $X^2 = -1 \mod n$의 근을 하나 찾아 낼 수 있다. 이변수 이차 형식 $X^2 + Y^2$으로 표시 가능한 정수는 분류가 되어 있고, 우리는 다음과 같은 간단한 동치 관계를 자명하게 얻는다.

n이 홀수이고 합동식 $X^2 = -1 \mod n$의 근이 Z/nZ에 존재한다.

$\longleftrightarrow$ n의 모든 소인수는 $4k+1$꼴이다.

다음의 사실도 이미 잘 알려져 있다.

두 정수 A와 B가 있어서 $n = A^2 + B^2$이다.

$\longleftrightarrow$ n의 소인수 분해에서 $q = 3 \mod 4$꼴의 소인수는 항상 짝수번 나온다, 즉 q의 지수가 항상 짝수이다.

p를 홀수인 소수라고 하자. 그리고 $p = 1 \mod 4$라고 가정하자. 이렇게 가정하는 이유는 유한체 Z/pZ에는 $X^2 = -1$의 근이 있기 때문이다. 이제 E를 다음식

$$E : Y^2 = X^3 + DX$$

으로 정의되는 유한체 Z/pZ위의 타원 곡선이라고 하자. 이 타원 곡선은 순 허수 i, $i^2 = -1$,를 포함하는 허수 승법(complex multiplication)을 가진다. 순허수 i에 대응하는 E의 사상을 $[i]$라고 하자. $[i]$는 곡선위의 점 $P = (x, y)$를 (x, iy)로 보낸다. 즉 $[i]$는 E를 E로 보내고

$$[i]([i](x, y)) = (x, -y) = -P$$

에서 $[i]^2 = -id$.이다. 또한 유한체 Z/pZ에는 $X^2 = -1$의 근이 있기 때문에 $[i]$는 Z/pZ 위에서 정의되어 있다.

Mordell-Weil 군 $E(Z/pZ)$의 원소의 갯수를 t로 표시하자. 그러면 t는 부등식

$$p + 1 - 2\sqrt{p} < t < p + 1 + 2\sqrt{p}$$

를 만족한다. 또한 t는 합동식

$t - 1 = [(X^3 + DX)^{(p-1)/2}$의 전개에서 X^{p-1}의 계수$]$ $\mod p$

를 만족한다. 위의 부등식과 합동식은 t를 유일하게 결정짓는다. $(X^3 + DX)^{(p-1)/2}$의 전개에서 X^{p-1}의 계수는 $(X^2 + D)^{(p-1)/2}$의 전개에서 $X^{(p-1)/2}$의 계수이고 이항계수를 써서

$$t = 1 + {}_{(p-1)/2}C_{(p-1)/4}\, D^{(p-1)/4} \mod p$$

이다. 여기에서 $D^{(p-1)/4} \mod p$는 $+1$과 -1을 포함해서 4가지가 있을 수 있고, 이항계수 ${}_{(p-1)/2}C_{(p-1)/4}$는 다음과 같이 다항식 시간에 계산이 가능하다.[7] p가 $p = 1 \mod 4$꼴이기 때문에

$$p = A^2 + B^2,$$

$A = 1 \mod 4$가 되는 두 정수쌍 A와 $B>0$가 유일하게 존재한다. 그리고 이 A와 B는 다항식 시간에 계산할 수 있다. 여기에서 A는 음수가 될수도 있다. 그리고 A와 B는 서로 소이다. 이 때에

$${}_{(p-1)/2}C_{(p-1)/4} = 2A \mod p$$

이다. 따라서

$$t = 1 + 2AD^{(p-1)/4} \mod p$$

이다.

$D^{(p-1)/4} \mod p$이 $+1$이거나 -1이라고 하자. $t - p - 1$의 절대값이 $2\sqrt{p}$ 보다 작으므로 이때에는

$$t = p + 1 + 2A = (A + 1)^2 + B^2$$

이거나

$$t = p + 1 - 2A = (A - 1)^2 + B^2$$

이다. $D^{(p-1)/4} \mod p$이 $+1$도 -1도 아니라면 $D^{(p-1)/2} = -1 \mod p$이고 따라서

$$D^{(p-1)/4} = B/A \mod p$$

이므로 계산해 보면

$$t = p + 1 + 2A = A^2 + (B + 1)^2$$

이거나

$$t = p + 1 - 2A = A^2 + (B - 1)^2$$

임을 알 수 있다.

이제 임의의 소수 $p = 1 \mod 4$를 RSA에 사용한

다고 하자. 즉 $n=pq$인 공개 자료가 있고 또 이때에 n을 소인수 분해하기 위해서 타원 곡선 E : $Y^2=X^3+DX$을 사용하는 경우를 고려해 보자. 그러면 p를 찾아 낼 가능성은 Mordell-Weil군 $E(\mathbb{Z}/p\mathbb{Z})$의 지수(exponent)가 얼마나 smooth한지에 달려 있다.

어떤 경우에는 이 지수(exponent)가 t 보다 상당히 작아질 수 있다. 위에서 본 것처럼 t는 제곱수 두개의 합이고 따라서 t를

$$t=M^2N,$$

N은 제곱수로 나누어지지 않는다, 라고 쓸 때에 t의 소인수 분해에서 나오는 $q=3 \mod 4$꼴의 소인수는 모두 M의 약수이다. 이때에 $E(\mathbb{Z}/p\mathbb{Z})$의 지수는 기껏해야 MN이다.

Mordell-Weil군 $E(\mathbb{Z}/p\mathbb{Z})$의 구조는 다음의 형태임이 알려져 있다.[5] t의 소인수 분해가

$$t\prod_l l^{e(l)}$$

로 주어졌다고 하자. 그러면 $E(\mathbb{Z}/p\mathbb{Z})$는 $t=p$때에

$$\mathbb{Z}/p\mathbb{Z}$$

이거나, $t\neq p$때에

$$\prod(\mathbb{Z}/l^{a(l)}\mathbb{Z}\times\mathbb{Z}/l^{e(l)-a(l)}\mathbb{Z})$$

이다. 여기서 $a(l)$은 다음의 범위에 있는 임의의 정수가 될 수 있다.

$$l^{c(l)}\,\|\,p-1$$

이라고 하자. 그러면

$$0\le a(l)\le \min\{c(l),\ [e(l)/2]\}$$

이다.

이제 $q\equiv 3 \mod 4$이고

$$q^{e(q)}\,\|\,t$$

라고 하자. $E(\mathbb{Z}/p\mathbb{Z})$의 q-Sylow 부분군은

$$\mathbb{Z}/q^{a(q)}\mathbb{Z}\times\mathbb{Z}/q^{e(q)-a(q)}\mathbb{Z}$$

인데, 허수 승법 $[i]$를 q-Sylow 부분군에 국한시켜 생각해보면 $a(q)\ge 1$이 되어야 한다.

즉 다음과 같은 결론을 얻는다. 타원 곡선 E : $Y^2=X^3+DX$에서 t를 $E(\mathbb{Z}/p\mathbb{Z})$의 원소의 수라고 하자. t가 $q\equiv 3 \mod 4$인 소인수를 가지면 $E(\mathbb{Z}/p\mathbb{Z})$의 지수는 기껏해야 t/q이다. $q\equiv 3 \mod 4$인 t의 약수는 $GCD(A\pm 1,B)$나 $GCD(A,B\pm 1)$의 약수이다. 즉 $GCD(A\pm 1,B)$나 $GCD(A,B\pm 1)$이 많은 소인수 $q\equiv 3 \mod 4$를 가질수록 $E(\mathbb{Z}/p\mathbb{Z})$의 위수는 작아지고 좀더 smooth해진다. 따라서 p를 찾아내기가 상대적으로 쉬워진다. 물론 이러한 꼴의 소수는 그다지 많지 않을 것이다.

확률론적 소수 판정법은 여러가지가 있다. Fermat 판정법이나 Strong pseudo-prime판정법이 그중에서 가장 자주 쓰이는 방법이라 할 수 있다.

n이 합성수인데 모든 $GCD(a,n)=1$인 a에 대해서

$$a^{n-1}=1 \mod n$$

인 합동식을 만족하면, 이 n을 카미카엘(Charmicael)수라고 한다. 최근에 Pomerance등이 카미카엘 수는 무한히 많다는 사실을 증명하였다.[1] 또한 고정된 유한번의 Strong pseudo-prime 판정법을 통과하는 카미카엘(Charmicael) 수도 무한히 많다는 사실이 증명된다는 주장이 있다.

소수판정을 해주는 대부분의 프로그램에서는 실제로 소수임을 증명하지 않고, 몇번의 Strong pseudo-prime 판정법을 통과할 때에 소수라고 답을 내는 것들이 많다. 사용자는 이런 프로그램과 실제로 소수임을 증명해주는 프로그램의 차이점에 주의해야 할 것이다.

그들의 결과에 따르면

$$f(x)=x \text{ 보다 작은 카미카엘 수의 갯수}$$

라고 할때

$$f(x)>cx^{2/7},$$

c는 0보다 큰 상수, 임을 보였다. 그리고 여기에 나오는 지수 2/7을 1에 가까운 수로 바꿀 수 있을 것이라고 예상하고 있다.

유한개의 밑(base)을 고정시켰을 때, 이 모든 밑에 대해서 Strong pseudo-prime 판정법을 통과하는 합

성수가 무한히 많은지는 아직 알려져있지 않고 해석적 정수론(analytic number theory) 연구가들은 대체로 유한개의 밑의 갯수가 아무리 많아도, Strong 판정법을 통과하는 합성수가 무한히 많으리라 예상한다.

Bosma와 Chudnovsky등이 타원곡선을 소수 증명에 이용할 수 있다는 사실을 최초로 발견하였고 그 이유는 다음과 같다.[3)]

n을 $n>1$, $GCD(n, 6)=1$인 정수라고 하자. E가 Z/nZ 위의 타원 곡선이고 $E(Z/nZ)$의 원소의 수는 rs, s는 소수, 라고 하자. $E(Z/nZ)$에 어떤 원소 P가 있어서 $rP=(x;y;z)$로 쓸때 $\gcd(z, n)=1$이라고 하자. 만일 $s>(n^{1/4}+1)^2$이면 n이 소수이다.

이 소수증명법은 Pocklington의 $p-1$의 소인수 분해를 이용하는 소수증명법과 거의 비슷하다. 다만 증명에 사용된 군이 $(Z/pZ)^{\times}$ 대신에 $E(Z/pZ)$인 것이 차이점이다.

Pocklington의 방법에서는 사용 가능한 수가 $n-1$ 한 개밖에 없지만 $n=1 \bmod 4$일때 타원곡선 $E: Y^2=X^3+DX$를 사용하면 사용 가능한 수가 4가지가 있다. 즉, n이 소수임을 증명할 수 있는 기회가 Pocklington의 방법의 4배이다. 대신에 $n=1 \bmod 4$일 것이 요구된다. 이 약점은 허수승법을 가지는 다른 타원곡선을 사용해서 보완할 수 있다. E가 일반형태의 타원곡선일 때에는 $E(Z/pZ)$의 원소의 수를 계산해 내는 것이 쉬운 문제가 아니다. 다만 E가 허수승법을 가질 경우에는 원소의 수를 상대적으로 쉽게 계산해 낼 수 있다. 아직까지는 일반형태의 E를 써서 소수증명을 하는 프로그램은 제작되지 못했다. Atkin이 제안하고 Morain이 제작한 소수증명 프로그램 ECPP(elliptic curves and primality proving)을 사용해 보면 SUN4에서 150자리의 수는 증명하는데 약 3~10분 정도 걸리고 350자리의 수는 증명하는데 약 10~30시간 걸린다. 현재의 컴퓨터로 이 방법을 써서 일반형태의 소수에 대해 소수증명을 할 수 있는 최대치는 약 1500자리 정도라고 알려져 있다. ECPP 는 ftp로 가져올 수도 있고 아니면 필자에게서 얻을 수도 있다. 위에서 언급한 CPU running time은 필자의 경험이다.

참 고 문 헌

1. W. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, preprint.
2. Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.
3. H. W. Lenstra, Jr., *Elliptic curves and number-theoretic algorithms*, Proc. ICM 1986, AMS(1987).
4. F. Morain, *Courbes elliptiques tests de primalité*, Thése, Université de Lyon I, 1990.
5. Hans-Georg Rück, *A note on elliptic curves over finite fields*, Math. Comp. Vol. 49, No. 179(1987), 301-304.
6. Joseph Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.
7. Kit Ming Yeung, *On congruences for binomial coefficients*, Journal of Number Theory 33 (1989), 1-17.

□ 著者紹介

한 상 근(종신회원)

서울대학교 수학과 졸업(학사)
미국 오하이오 주립대학교 수학과 졸업(박사)
현 재 한국과학기술원 수학과 부교수
통신정보보호학회 종신회원