김일성종합대학학보
(자연과학)
주체104(2015)년 제61권 제8호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 61 No. 8 JUCHE104(2015).

한가지 형태의 초타원곡선의 야코비군위수계산

리학림, 최충혁

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《기초과학부문들을 발전시켜야 나라의 과학기술수준을 빨리 높일수 있고 인민경제 여러 분야에서 나서는 과학기술적문제들을 원만히 풀수 있으며 과학기술을 주체성있게 발전시켜나갈수 있습니다.》(《**김정일**선집》 증보판 제10권 485페지)

대수곡선을 리용한 공개열쇠암호계를 구성하는데서 나서는 중요한 문제의 하나는 야코비군의 위수를 구하기 위한 빠른 알고리듬을 얻는것이다.

선행연구[1, 2]에서는 대수곡선의 야코비군의 연산고속화를 위한 방법들과 야코비군의 위수를 구하는 지수시간알고리듬이 론의되였다. 이로부터 특수한 형태의 대수곡선들의 야코비군의 위수를 구하기 위한 결과들이 소개되였으며 일부 경우들에는 위수계산을 위한 준지수시간알고리듬들이 알려져있다.[3, 4]

론문에서는 $y^2=\gamma x^{k+1}+\delta x$ 형태의 초타원곡선에 대하여 그것의 야코비군의 위수를 준지수시간알고리듬으로 구하는 한가지 방법에 대하여 론의하였다.

p 를 씨수, F_p 를 위수가 p 인 씨체라고 하자.

정리 1 p 를 정의옹근수 k 에 대하여 $p\equiv 1 \pmod{2k}$ 인 씨수라고 하면 $\gamma,\ \delta\in F_p^*$ 에 대하여 초타원곡선 $y^2=\gamma x^{k+1}+\delta x$ 의 F_{p^r} -유리점개수는 다음과 같다.

$$N_r=1+p^r+\sum_{i=1}^{k-1}(-1)^{r-1}\cdot[\chi_{2k}^{2i+1}(-r^{-1})\chi_{2k}^{k+2i+1}(\delta)]^r\cdot J_{2k}(2i+1,\ k)^r$$

증명 $M(b)=|\{x\in F_p\,|\,x^k=b\}|$ 라고 하면 $M(b)=\sum_{i=0}^{k-1}\chi_k^i(b)$ 가 성립된다.

이때 $y^2=\gamma x^{k+1}+\delta x$ 의 F_p -유리점개수는 다음의 식으로 계산된다.

$$N_1=1+p+\sum_{x\in F_p}\chi_2(\gamma x^{k+1}+\delta x)=1+p+\sum_{x\in F_p}\chi_2(x)\chi_2(x)\chi_2(x^k+\gamma^{-1}\delta)=$$

$$=1+p+\sum_{b\in F_p}\chi_2(\gamma)\chi_{2k}(b)\chi_2(b+\gamma^{-1}\delta)\cdot M(b)=$$

$$=1+p+\sum_{b\in F_p}\chi_2(\gamma)\chi_{2k}(b)\chi_2(b+\gamma^{-1}\delta)\sum_{i=0}^{k-1}\chi_k^i(b)=$$

$$=1+p+\sum_{i=0}^{k-1}\sum_{x\in F_p}\chi_2(\gamma)\chi_{2k}(-\gamma^{-1}\delta x)\chi_2(-\gamma^{-1}\delta x+\gamma^{-1}\delta)\chi_k^i(-\gamma^{-1}\delta x)=$$

$$=1+p+\sum_{i=0}^{k-1}\chi_2(\delta)\chi_{2k}^{2i+1}(-\gamma^{-1}\delta)\sum_{x\in F_p}\chi_{2k}^{2i+1}(x)\chi_{2k}^k(1-x)=$$

$$=1+p+\sum_{i=0}^{k-1}\chi_{2k}^{2i+1}(-\gamma^{-1})\chi_{2k}^{k+2i+1}(\delta)J_{2k}(2i+1,\ k)=$$

$$=1+p+\sum_{i=1}^{k-1}\chi_{2k}^{2i+1}(-\gamma^{-1})\chi_{2k}^{k+2i+1}(\delta)J_{2k}(2i+1,\ k)$$

여기서 $b=-\gamma^{-1}\delta x$ 로 치환하였다.

따라서 확대체에서의 지표의 성질과 다벤포트－하쎄의 관계식에 의하여 정리는 증명된다.(증명끝)

실례로 $k=6$ 인 경우에 대하여 보기로 하자.

$k=6$ 이므로 $p\equiv 1(\mathrm{mod}\ 12)$ 이고 $y^2=\gamma x^7+\delta x$ 의 F_{p^r} －유리점개수는 정리 1에 의하여

$$N_r=1+p^r+\sum_{i=1}^{5}(-1)^{r-1}\cdot[\chi_{12}^{2i+1}(-r^{-1})\chi_{12}^{7+2i}(\delta)]^r\cdot J_{12}(2i+1,\ 6)^r$$

이다. 여기서 $(-1)^{r-1}\cdot[\chi_{12}^{2i+1}(-\gamma^{-1})\chi_{12}^{7+2i}(\delta)]^r\cdot J_{12}(2i+1,\ 6)^r,\ i=\overline{1,\ 5}$ 는 $r=1$ 일 때 초타원곡선 $y^2=\gamma x^7+\delta x$ 의 p제곱프로베니우스자기준동형넘기기의 특성다항식 $P(T)$ 의 뿌리 α_i 에 대응된다. 즉 $\alpha_i=\chi_{12}^{2i+1}(-\gamma^{-1})\chi_{12}^{7+2i}(\delta)J_{12}(2i+1,\ 6),\ i=1,\cdots,5$ 이다.

대수곡선의 야코비군의 위수는 $P(1)$ 로 구해지므로 α_i 를 구하면 위수를 계산할수 있다.

α_i 의 계산에서 $\chi_{12}^{2i+1}(-\gamma^{-1})\chi_{12}^{7+2i}(\delta)$ 의 계산은 F_p^* 에서 리산로그문제풀이를 위한 첨수계산법으로 준지수시간동안에 진행될수 있으므로 야코비합 $J_{12}(2i+1,\ 6),\ i=1,\cdots,5$ 만 계산하면 된다.

정리 2 a 를 $a\equiv 0(\mathrm{mod}\ 12)$ 인 정의옹근수, p 를 $p=a^4-a^2+1$ 인 씨수라고 하면 씨체 F_p 우에서의 야코비합 $J_{12}(3,\ 6),\ J_{12}(5,\ 6)$ 은 1의 원시12제곱뿌리 ζ_{12} 에 의하여 다음과 같이 표시된다.

$$J_{12}(3,\ 6)=J_{12}(5,\ 6)=-\zeta_{12}^6(a-\zeta_{12})(a-\zeta_{12}^5)$$

증명 $a\equiv 0(\mathrm{mod}\ 12)$ 이고 $p=a^4-a^2+1$ 이므로 $p\equiv 1(\mathrm{mod}\ 12)$ 임을 알수 있다.

$$p=a^4-a^2+1=(a-\zeta_{12})(a-\zeta_{12}^5)(a-\zeta_{12}^7)(a-\zeta_{12}^{11})$$

이므로 12차원주등분체 $Q(\zeta_{12})$ 의 대수적옹근수환 $\boldsymbol{Z}[\zeta_{12}]$ 에서 씨수 p 에 의하여 생성된 이데알의 분해는

$$<p>=<(a-\zeta_{12})(a-\zeta_{12}^5)(a-\zeta_{12}^7)(a-\zeta_{12}^{11})>=<a-\zeta_{12}><a-\zeta_{12}^5><a-\zeta_{12}^7><a-\zeta_{12}^{11}>$$

이다. 여기서 $<\cdot>$는 주이데알을 의미한다.

$I=<a-\zeta_{12}>,\ I_t=\sigma_t(I),\ t\in(\boldsymbol{Z}/12\boldsymbol{Z})^*$ 이라고 하면 대수적옹근수환 $\boldsymbol{Z}[\zeta_{12}]$ 에서 야코비합 $J_{12}(6,\ 4)$ 에 의해 생성된 이데알의 분해는 $<J_{12}(3,\ 6)>=I_1\cdot I_5,\ <J_{12}(5,\ 6)>=I_1\cdot I_5$.

따라서 $c\in\{1,\ -1\},\ 0\le s\le 9$ 가 있어서 $J_{12}(3,\ 6)=c\cdot\zeta_{12}^s\cdot(a-\zeta_{12})(a-\zeta_{12}^5)$ 이다.

한편 $J_{12}(3,\ 6)\equiv -1(\mathrm{mod}\,(1-\zeta_{12})^2)$ 이므로

$c\cdot\zeta_{12}^s\cdot(a-\zeta_{12})(a-\zeta_{12}^5)\equiv c\cdot\zeta_{12}^s\cdot\zeta_{12}^6\equiv c\cdot\zeta_{12}^{6+s}\equiv c(1-(6+s)(1-\zeta_{12}))\equiv -1(\mathrm{mod}\,(1-\zeta_{12})^2).$

그러므로 $c(-5-s)=-1,\ c(6+s)=0$ 이며 $c=-1,\ s=-6$ 이다.

따라서 $J_{12}(3,\ 6)=J_{12}(5,\ 6)=-\zeta_{12}^{-6}(a-\zeta_{12})(a-\zeta_{12}^{5})=-\zeta_{12}^{6}(a-\zeta_{12})(a-\zeta_{12}^{5})$ 이다.(증명끝)

정리 2를 리용하여 나머지 야코비합 $J_{12}(7,\ 6)$, $J_{12}(9,\ 6)$, $J_{12}(11,\ 6)$을 구하자.

$$J_e(-u,\ -v)=\sum_x \chi_e^{-u}(x)\chi_e^{-v}(1-x)=\sum_x \zeta_e^{-u\cdot \mathrm{ind}_g x}\cdot\zeta_e^{-v\cdot \mathrm{ind}_g (1-x)}=\sum_x (\zeta_e^{-1})^{u\cdot \mathrm{ind}_g x}\cdot(\zeta_e^{-1})^{v\cdot \mathrm{ind}_g (1-x)}$$

이므로 $J_e(-u,\ -v)$는 $J_e(u,\ v)$에서 ζ_e를 ζ_e^{-1}로 바꾸면 구할수 있다.

따라서 $J_{12}(3,\ 6)$의 표시식을 리용하면

$$J_{12}(7,\ 6)=J_{12}(-5,\ -6)=-(\zeta_{12}^{-1})^{6}(a-\zeta_{12}^{-1})(a-(\zeta_{12}^{-1})^{5})=-\zeta_{12}^{6}(a-\zeta_{12}^{11})(a-\zeta_{12}^{7}),$$

$$J_{12}(9,\ 6)=J_{12}(-3,\ -6)=-\zeta_{12}^{6}(a-\zeta_{12}^{11})(a-\zeta_{12}^{7}),$$

$$J_{12}(11,\ 6)=(-1)^{6(p-1)/12}J_{12}(-11-6,\ -6)=J_{12}(7,\ 6)=-\zeta_{12}^{6}(a-\zeta_{12}^{11})(a-\zeta_{12}^{7}).$$

이로써 야코비합 $J_{12}(2i+1,\ 6),\ i=1,\cdots,5$가 모든 ζ_{12}와 a에 의하여 표시되므로 야코비합계산을 쉽게 진행할수 있다.

우리는 씨수 p에 대하여 우와 같은 추가적인 가정을 줌으로써 야코비합들을 쉽게 결정하고 α_i의 계산에서 $\chi_{12}^{2i+1}(-\gamma^{-1})\chi_{12}^{7+2i}(\delta)$의 계산을 F_p^*에서 리산로그문제풀이를 위한 첨수계산법으로 준지수시간동안에 진행할수 있도록 하였다.

따라서 야코비군의 위수는 준지수시간동안에 구할수 있다.

우의 조건에 맞는 a와 p는 $120\ 000\le a\le 500\ 000$일 때만 해도 2 894개가 존재한다.

실례로 a=497 016으로 택할 때 $p=a^4-a^2+1$은

$$p=61\ 021\ 303\ 322\ 438\ 942\ 009\ 281(76\text{bit})$$

로서 씨수이다.

참 고 문 헌

[1] S. Flon et al.; LNCS, 2947, 55, 2004.

[2] S. D. Galbraith; Math. Comp., 71, 393, 2000.

[3] R. Blache et al.; Finite and Their Application, 13, 348, 2007.

[4] S. Canard et al.; LNCS, 8383, 167, 2014.

주체104(2015)년 4월 5일 원고접수

Counting Points on Jacobian Group of a Type of Hyperelliptic Curve

Ri Hak Rim, Choe Chung Hyok

We provide a subexponential-time method of counting points on Jacobian group of hyperelliptic curve $y^2=\gamma x^7+\delta x$. First we show that the order of Jacobian group is expressed by character and Jacobi sums. Then we divide the characteristic p with a^4-a^2+1 and calculate all Jacobian sums in subexponential-time.

Key words: hyperelliptic curve, Jacobian group